cherwell®

Acquired by Ivanti

CSM 2022.3 Administration

Legal Notices

The Cherwell Software product suite includes:

- Cherwell Service Management
- Cherwell Asset Management

Contact Cherwell Software

Contents

System Administration

CSM provides a number of powerful administrative features that help you install, configure, secure, automate, and extend your system.

Installing

The installer provides all the elements and tools needed to successfully install or update CSM.

Installation

Installation steps vary depending on which installers are run (Server, Portal and Browser Apps, and Client), whether you are installing a new instance of CSM or upgrading an existing instance, and whether or not Auto-Deploy is used.

For more information about installation/upgrade steps, see Steps to Install or Update CSM.

Installation configurations also vary. A typical installation is called a *single-server installation* because the Cherwell Application Server and supporting services are all installed on one machine. A typical single-server installation involves three tiers:

- **(Tier 1) Database server**: Houses the CSM database (SQL database).
- **(Tier 2) Cherwell Server (main server)**: Houses the Cherwell Application Server and supporting services, and the Portal and Browser applications.
- **(Tier 3) Client machines**: Houses the client-only files/administrator tools (the CSM Desktop Client, CSM Administrator, and all the supporting tools/utilities).

The following figure shows a typical single-server installation.
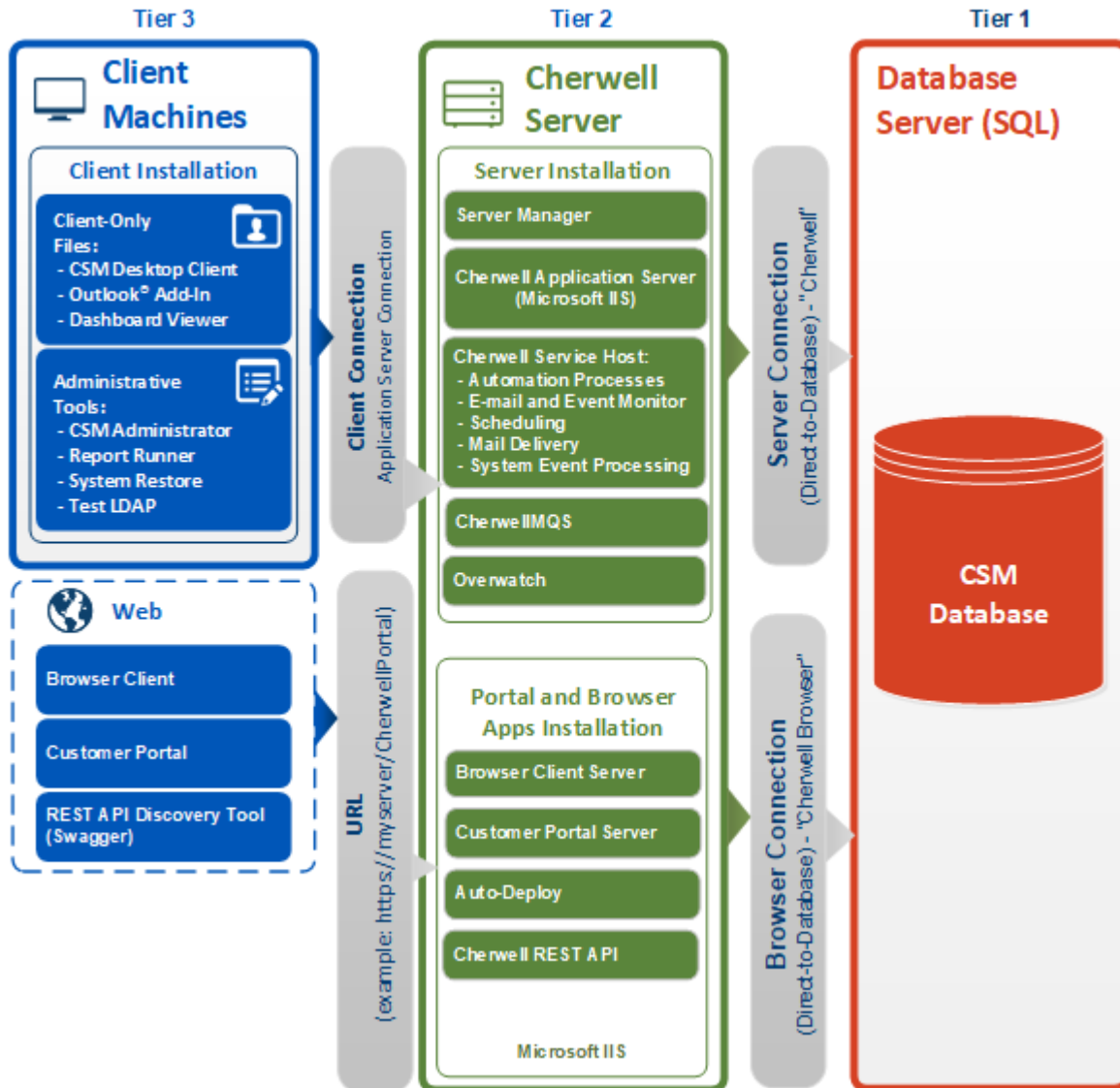
Multi-Language Installers

The CSM installer is available in English, German, French, Spanish, and Brazilian Portuguese.

Download the CSM installer for your preferred language to step through the installation process in that language.

Platform code-level support for all five languages is included with each installer. Each multi-language installer follows the same sequence of steps to complete the Server, Web Applications, and Client installations.

Content support for all five languages is included in the Demo and Starter databases by default.

Globalization features enable you to translate platform and content strings into multiple languages. Globalization is enabled by default.

Considerations for CSM SaaS Implementation

Using a hosted implementation of CSM has benefits that on-premises installations do not have. However, there are a few differences in users' ability to control the product.

Some features described in the Cherwell Product Documentation are only available to users on an on-premises system. To ensure the security of the hosted environment, some other features require users with software as a service (SaaS) implementations of CSM to coordinate with Cherwell Support.

The following CSM functionality is not available for SaaS customers:

- Database server object management, including accessing, creating, editing, or deleting
- Configuring database file settings
- Creating CSM database views
- Performing database system maintenance, which includes:
    ◦ Shrinking the event log
    ◦ Rebuilding full-text search catalog
- Modifying or deleting the CSDAdmin or CherwellServices accounts in the User Manager
- Linking new Business Objects to an external database

The following actions must be coordinated with Cherwell Support:

- Configuring the Log Viewer
- Installing the Trusted Agent Hub
- Restoring a database
- Configuring a SAML integration
- Penetration testing
- Upgrading CSM
- Creating encryption keys

> **Note:** SaaS users must sign a Field-Level Encryption addendum before working with Cherwell Support to create encryption keys.

The following activities are available for SaaS customers after Cherwell installs and configures the Trusted Agent Hub:

- Using Trusted Agent to provide secure access between private network and Cherwell data center
- Configuring a Trusted Agent to use printers on their remote network
- Using One-Step™ Actions with Trusted Agent to perform the following tasks:
    ◦ Run a program
    ◦ Write to a file
    ◦ Excel merge

- ◦ Call a web service

SaaS customers can start/stop/restart CSM services and restart CSM Web Applications from the Cherwell Self-Service Portal. For more information, see Start/Stop/Restart a CSM Server, or Restart a Web Application from the Server Manager.

Related concepts

Database Server Objects Security Rights

About Encrypted Fields

Trusted Agent Components

Installations

Use the Server, Web Applications, and Client installations to install the groups of components that make up Cherwell Service Management.

CSM provides the following installations:

- **Server**: Installs the Server Manager, the Cherwell Application Server, and the Cherwell Service Host.
- **Portal and Browser Applications**: (Also called Web Apps) Installs the CSM Browser Client, CSM Portal, Cherwell REST API, and Auto-Deploy.
- **Client**: Installs the main Client applications (client-only files) and administrator tools (optional). (You can optionally install the server files as well, but it is not typical). For most users, the Client applications will be installed via Auto-Deploy.

> **Note:** Run the Server installation first, then the Web Applications installation. Client installations are run last and are typically pushed out to client computers using the Auto-Deploy feature (Auto-Deploy is configured separately to push out a preconfigured Client installation and connection).

The following tables describe the installation components in each installation.

Server Installation

Item	Description
Cherwell Application Server	The Cherwell Application Server is a CSM service that runs programs and handles application operations between users and their databases. The Application Server is the middle tier of the Cherwell 3-tier application. Client applications connect to the Application Server.

Item	Description
Cherwell Service Host	The Cherwell Service Host includes these microservices: • Automation Processes • E-mail and Event Monitoring • Mail Delivery Service • Scheduling • System Even Processing Service The Mail Delivery Service is automatically installed, along with the Cherwell Message Queue Service (CherwellMQS) message broker application. Since the installation is automatic, Mail Delivery Service does not appear as an installation option. **Note:** Along with RabbitMQ, Erlang is automatically installed to power CherwellMQS. Erlang shows up in the **Start** menu of any computer where CSM is installed.
Database Options	The installer prompts users to either: • Install a new database (Starter or Demo): Installs the most recent version of a CSM Demo or Starter database, including any required internal system definitions. • Update an existing database: Installs new internal system definitions (required for new functionality) to your existing CSM database. Updating does not affect current system definitions.

Web Applications Installation

Item	Description
Customer Portal	The CSM Customer Portal is a highly configurable web application that enables customers to securely and conveniently access their CSM data (example: Incidents, company news, documents, the Service Catalog, etc.) using a browser. A Portal supports multiple sites (for different types of users), and also allows managers to access their team's data.
Browser Client	The CSM Browser Client is a web application that enables users to access most of the features available from the CSM Windows-based Desktop Client using a browser. The CSM Browser Client supports most major modern browsers on desktop machines and tablets.

Item	Description
Auto-Deploy	Cherwell Auto-Deploy is an installation tool that allows system administrators to automatically distribute preconfigured Desktop Client and or CSM Administrator installations and connections to client machines. Auto-Deploy is configured using the stand-alone Auto-Deploy Configuration Utility and is deployed using the Auto-Deploy web page.
Cherwell REST API	The Cherwell REST API provides programmatic access to many CSM functions via an HTTP-based RESTful API. Methods are available for finding, creating, and updating Business Objects; finding and running saved search queries; managing users; and more. Comprehensive API documentation is available in the Cherwell REST API Discovery Tool, which enables you to discover and test methods using your CSM data.

Client Installation

Item	Description
Client-Only Applications	CSM Desktop Client, Outlook® Add-in (Installer), Report Runner, and the Dashboard Viewer.
Administrator Applications	CSM Administrator, System Upgrade/Restore, and Test LDAP Tool.
Server Applications	See Server installation.

Connections

A connection is the means by which a CSM application connects to another tier of the CSM suite.

A client is a tier, a Cherwell Server is a tier, and the database is a tier.

CSM has two different types of connections that are used in different ways and from different places. Both types of connections are configured through the Connection Wizard:

	• **Direct-to-Database connection (2-tier):** A direct-to-database connection is a connection between one or more CSM applications and a CSM database. Typically, only CSM Servers (example: Cherwell Application Server) use this type of connection, although Client applications can use direct-to-database connections under special circumstances, bypassing the Cherwell Application Server. • A direct-to-database connection is also referred to as a "2-tier connection" because only two tiers are involved: The Cherwell Server (Tier 2) connects to the database (Tier 1). • Since a direct-to-database connection does not use the Cherwell Application Server, it does not use compression or encryption. • Most CSM Services use a direct-to-database connection, but end users generally should connect via an App Server connection when using the CSM clients. • Although end users should usually avoid using a direct-to-database connection, it can be helpful in troubleshooting. In some situations, users are able to see more detailed error messages when using a direct-to-database connection, and by bypassing the Cherwell Application Server it can help to isolate the source of a problem. • Direct-to-database connections for end users are not available for Cherwell SaaS customers.
	• **App Server connection (3-tier):** An App Server connection is a connection between one or more CSM applications (example: CSM Desktop Client) and the Cherwell Application Server. • An App Server connection is also referred to as a "3-tier connection" because three tiers are involved: The CSM application (Tier 3) connects to the CSM database (Tier 1) through the Cherwell Application Server (Tier 2).

For a new installation, configure the following three connections:

• **Server connection**: The Server connection is a configured *direct-to-database (2-tier)* connection between any Cherwell Server (primarily the Cherwell Application Server and the Cherwell Service Host.) and a CSM database. During the Server installation, you are prompted to create this connection which, by default, is named Cherwell.

- **Browser connection**: The Browser connection is a configured *direct-to-database (2-tier)* connection between the CSM Browser Applications and a CSM database. CSM Browser Applications use a different connection than the desktop clients because they run inside IIS, and the connection needs to work with the IIS security options. During the Portal and Browser Applications installation, you are prompted to create this connection which, by default, is (and should remain) named "Cherwell Browser."

- **Client connection:** A Client connection is a configured *App Server connection (3-tier)* that allows a user to connect to the CSM database through the Cherwell Application Server. Although users can manually configure this connection, we recommend that the system administrator configure the client connection as part of the Auto-Deploy configuration, and then push the client connection out to all users using the Auto-Deploy process. A client connection pushed out by Auto-Deploy is also referred to as an "Auto-Deployed Client connection."

The configuration steps vary by the type of connection. Typically, a system administrator configures all three connections during the installation process. To help with the configurations, CSM provides the Connection Wizard, which is launched automatically by the Installation Wizard during the Server and Browser/Portal Apps installations, and manually by the system administrator during the Auto-Deploy configuration.

Related concepts
Default Port Numbers
Configure the Server Connection
Configure the Client Connection
Related tasks
Configure the Browser Connection

Default Port Numbers

Discover the ports that Cherwell Service Management uses by default.

The following list describes the default ports that CSM uses.

Connection	Protocol	Default Port
Client Connection	HTTPS (Recommended for all production environments.) HTTP (Not recommended for production environments.) **Note:** CSM versions installed before 9.5.0 can run on TCP; however, TCP connections are a legacy configuration. HTTPS is the recommended protocol. For TCP connections, the default port is 8001.	443 (HTTPS) 80 (HTTP)
Internet	HTTPS (Recommended for all production environments.) HTTP (Not recommended for production environments.)	443 (HTTPS) 80 (HTTP)
LDAP	LDAP	389
CherwellMQS (RabbitMQ)	AMQP (Transport by TCP)	5672 15672
Email	SMTP SMTP SSL POP3 POP3 SSL IMAP4 IMAP4 SSL	25 465 110 995 143 993

Connection	Protocol	Default Port
Microsoft SQL Server	TCP	1433
Redis (optional for load balancing)	TCP	6379
Splunk (optional)	HTTP	8089

Related concepts

Server Installation Options

Configure the Application Server

Define General Directory Service Properties

Define Global POP or IMAP Account Settings

Troubleshooting Application Server Installations Using IIS

Sizing and Scalability Considerations

When planning your CSM installation, use these recommendations for sizing, database and server installations, and more.

Sizing Variables

Variable	Notes
Total number of users	• 1 CPU core per 75 concurrent users. 2 minimum: 1 for OS, 1 for CSM. • 50 MB of memory per session for application and web servers.
Concurrent licenses used	• Use a 1:3 ratio for Desktop Client and Browser Client users. Example: 50 to 100 licenses = 150-300 Desktop Client and Browser Client users, 30 percent Desktop Client and Browser Client users concurrent (1:3). • 5 percent concurrent coverage for CSM Portal users. Example: 900 Portal users = 18,000-20,000 user pool. • Consider factoring 600 MB of storage per license per year.
Number of records created (example. Incidents or Changes)	If the record count is especially high, consider increasing the memory and processors on both servers.
Number and type of CSM reports run	If running multiple reports frequently, or reporting historical/trend data for extended periods of time, consider increasing the memory and processors on both servers.
Number and type of CSM attachments used	If using many large attachments, consider doubling the amount of storage.

Database Installation Considerations

CSM uses Microsoft SQL Server as a back-end database (see the System Requirements for supported versions). Organizations typically host CSM on a centralized database server. This setup is efficient because it simplifies management and ensures that CSM data participates in an existing backup/recovery plan.

Consider the following:

- Network activity exists between the CSM server and database server. There is typically a fast connection between the two machines, though firewalls might require configuration to allow this communication.
- CSM servers must have appropriate security access to the database. This is accomplished by either providing SQL credentials for the database to the CSM server or ensuring that the account used by the CSM servers has appropriate rights on the database server (and also has appropriate local rights on the CSM server machine).

Server Components Installation Considerations

By default, servers and server components are installed on a single server. However, the components can be separated onto additional servers if necessary.

Consider the following reasons for separating components:

- **Support of existing infrastructure**: Customers commonly have separate servers set up for specific functionality. Typically, this includes either the database or the web server.
- **Scalability**: When the number of concurrent users increases substantially or when the automation load is high, separating secondary services might improve efficiency. Typically, this includes secondary services expected to use a significant amount of data. For guidance, see Scaling CSM.
- **Server Farms**: The Cherwell server and CSM Web Applications support server farms using a Redis cache to handle state management between multiple servers when used with a hardware load balancer. For guidance, see Scaling the CSM Web Applications.

Deployment Considerations

Prior to deployment, consider factors that might affect performance, such as:

- Network performance.
- Database performance.
- Complexity of the SQL database network configuration.
- Use of CSM on a shared or dedicated server.
- Use of CSM in a high availability environment.

Trusted Agent Considerations

Prior to deployment, consider the impact of Trusted Agents on scalability and system performance. In most cases, the use of Trusted Agents adds only a marginal amount of overhead, but in the case of the Trusted Agents for email, the impact can be as much as a 40 percent reduction in the throughput of emails. For guidance, see Trusted Agent.

Before Installing CSM

Consult these resources to prepare for Cherwell Service Management's installation process.

Before installing CSM for the first time:

1. Verify that the system meets the system requirements. See System Requirements.
2. Complete the installation worksheet. See Installation worksheet.
3. Configure IIS. See Internet Information Services (IIS).
4. Read the steps to install CSM. See steps to install CSM.

Related concepts
Securing Your CSM Environment

Gather Information Required for Installation

Before installing CSM, gather these worksheet items so you are prepared with the required server information, account details, license keys, and URLs.

Table 1. Worksheet Items

Installation Item	Description
Cherwell® Server	This is the machine where the Cherwell Application Server and the supporting services are installed. The account used to launch the services on this machine is called the Cherwell Server account (Network account or Services account). The Cherwell Server account must have rights to the registry and file system on the local machine, and must be allowed to communicate via TCP. Often the account is a local administrator. If you want the services to use the same account to connect to the CSM database, you must use a domain account that has rights to SQL Server. • Server Name: *Example: CherwellServer* • Location: *Example: \\domain\CherwellServer* For Cherwell Server Account Credentials: • Username: *Example: domain\henri* • Password: *Example: Colorado719* For CherwellMQS: • Password: *Example: Colorado719*

Installation Item	Description
Database Server (SQL Server Machine)	This is the machine where the CSM database (SQL database) is installed. The account used to access the CSM database is often called the Database Login account (SQL Login). The Database Login account must have rights to insert, update, and delete rows within tables. If you are planning to use this account for the administrative functions that modify that database, this account must also have rights to create, drop, and alter tables, and to create views, indexes, and stored procedures. When the CSM services use this connection, the account under which the service is running is the account whose credentials are used to connect to the database. If the Cherwell Application Server is installed in the same domain as the database server and the service account has rights to the database, use Windows Authentication to provide the credentials. This information is needed when creating connections. • Server Name: *Example: CSMDatabaseServer* • IP Address: *Example: 168.212.225.204* Database Login Account Credentials: • Username: *Example: sa* • Password: *Example: Colorado719*
Cherwell Application Server	This is the location of the Cherwell Application Server. HTTPS is the recommended protocol. URL: *Example:https://<Cherwellserver>:<Port#>*
Web Applications Server	CSM Web Applications must be contacted using a URL that includes a fully qualified Domain Name System (DNS) and this must also be resolved on the server. CSM SaaS systems are configured to use the fully qualified domain name by default; on-premises customers can use one of these methods to ensure the web applications server can resolve to a fully qualified domain name: • Add the fully qualified domain name mapped to 127.0.0.1 entry to the host file on the web server used by CSM. • Create internal DNS entries for the servers to resolve the name to the internal correct IP address.

Installation Item	Description
Browser Application Account	The Browser App Database Login account must have rights to insert, update, and delete rows in database tables. We recommend that you use a SQL Account with sufficient rights here, rather than Windows credentials. Otherwise, IIS will need to be specially configured to use a Windows account that has appropriate rights to the database. • Username: *Example: sa* • Password: *Example: Colorado719*
License	• Organization Name: *Example: Cherwell Software* • Cherwell License Key: *Example: 3SKPFM-PC9ZM-PD4MK-FPG90-RLUW8*
REST API URL	The base REST API URL is required for authenticating users for CSM applications, third-party reporting tools, and webhooks. System administrators can configure the URL in the **Security** section of CSM Administrator. The URL must be in the following format: https://*[servername]*/CherwellAPI/api/

Related concepts

Set the Base URL for the Cherwell REST API

Configure IIS for CSM

As a prerequisite to installing CSM, on-premises customers must enable certain features for the Internet Information Services (IIS) server that is used with CSM. This includes adding HTTP activation features for the .NET Framework, enabling dynamic compression, and enabling support for the WebSocket Protocol (IIS 8.0 and later only).

Enable HTTP Activation for the .NET Framework

To enable HTTP Activation:

1. On the IIS server, open the **Windows Server Manager**.

2. Select **Manage>Add Roles and Features**.

3. Select **Next** until the Features page opens.

4. For .NET Framework 4.5 verify that **HTTP Activation** is selected.
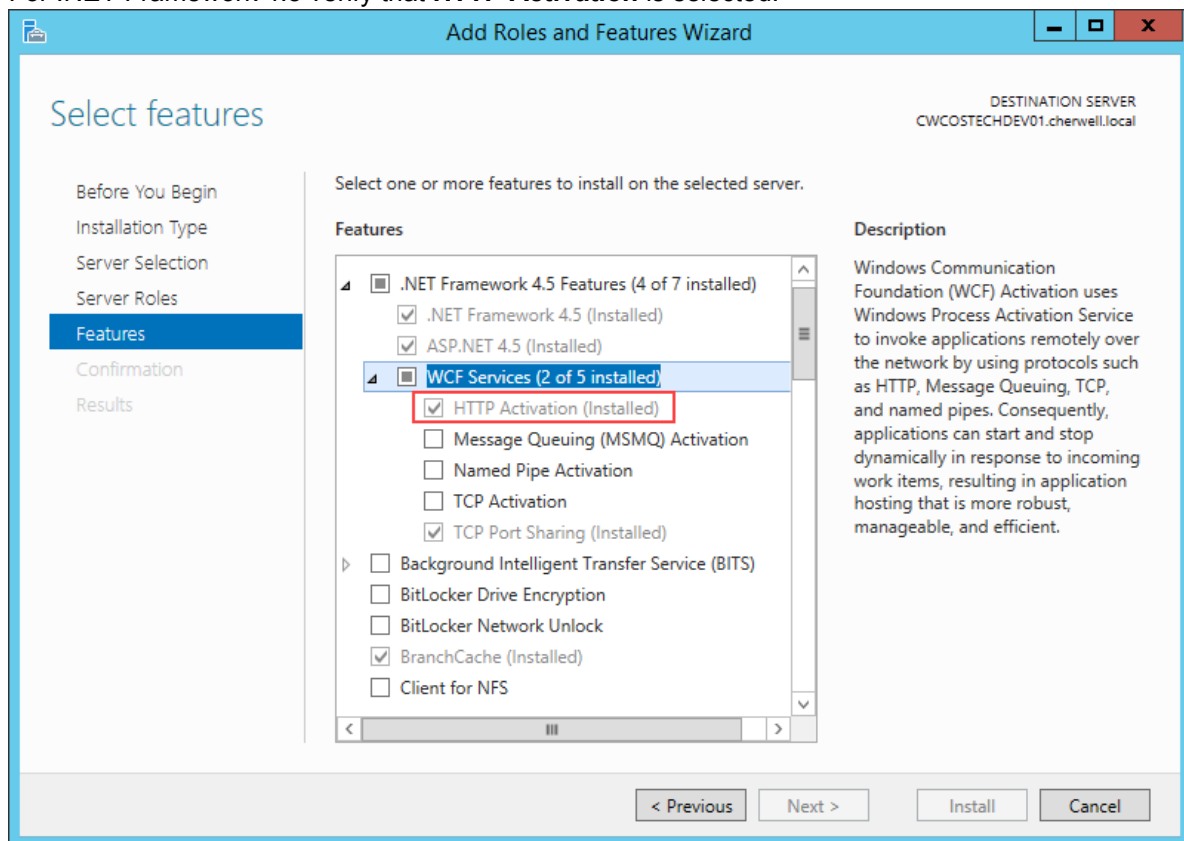
Improve Response Time for CSM Web Applications

Enable dynamic compression to potentially improve response times for CSM Web Applications, particularly the Browser Client and CSM Portal. In many cases, the performance improvements are dramatic, so Cherwell highly recommends that you enable dynamic compression for all IIS instances.

To learn more about dynamic compression and how to enable it, see https://docs.microsoft.com/en-us/iis/configuration/system.webserver/httpcompression/#setup.

Enable the WebSocket Protocol

WebSockets establish an efficient 2-way connection between IIS and CSM web applications. You can enable the WebSocket Protocol in IIS 8.0 and later; if you use an older version of IIS, polling is used and users may experience issues with CSM web applications, particularly when multiple tabs are used in the same browser session.

To enable the WebSocket Protocol, see https://docs.microsoft.com/en-us/iis/get-started/whats-new-in-iis-8/iis-80-websocket-protocol-support.

Related concepts

Steps to Install CSM

Troubleshooting Application Server Installations Using IIS

Steps to Install CSM

The installation steps vary depending on which installations are run (Server, CSM Web Applications, and Client), whether it is a new installation or an upgrade, and whether Auto-Deploy is used.

Important: Using a proxy server during configuration is not supported or recommended. Proxy servers can change request headers and cache information, both of which can cause unknown and unexpected issues with the CSM Client Applications and CSM Web Applications.

Complete the following high-level steps to install the CSM suite for the first time. Run the installation as a system administrator so that all installation steps can execute successfully.

Task	Notes
1. Add Windows Features to the IIS Server.	See Add Windows Features to the IIS Server.
2. Run the Server installation.	See Run the Server Installation to install the Server application and services files. Download and install any third-party tools as prompted by the installer.
3. Configure the Server connection.	See Configure the Server connection. This is a direct-to-database (2-tier) connection between the Cherwell Application Server and the CSM database.
4. Run the Portal and Browser Apps installation.	See Run the Portal and Browser Apps installation to install the Browser application files.
5. Configure the Browser connection.	See Configure the Browser connection when prompted by the Portal and Browser Apps installation. This is a direct-to-database (2-tier) connection between the Cherwell Browser Apps and the CSM database.
6. Configure and start the Cherwell Service Host and CSM services.	See Configure and start the Cherwell Service Host and CSM services.
7. Configure Auto-Deploy.	See Configure Auto-Deploy to push out the Client installation and connection to client machines. **Note:** During the Auto-Deploy configuration, the configure the Client connection that are auto-deployed must be configured.
8. Reboot the installation server.	If you installed CSM and Portal and Browser Apps on different servers, reboot both servers.
9. License CSM.	See License CSM

Task	Notes
10. Log in to CSM Administrator.	Use the default credentials (username = CSDAdmin, password = CSDAdmin), and complete these configuration tasks: 1. Set up the user and customer profiles so that people in the organization can log in to other CSM applications. 2. The base URL for the Cherwell REST API is automatically set when you install CSM. The URL is required for user authentication, third-party reporting tools, and webhooks. If you need to change the default URL, see Set the Base URL for the REST API.
Push out Client installations using Auto-Deploy.	See Using Auto-Deploy. **Note:** New users must access the system administrator designated web page to run Auto-Deploy. Existing users are prompted to install the new version when they next run CSM locally.

Related concepts

Configure IIS for CSM

Run the Web Applications Installation

Configure the Cherwell Service Host

Configuring Auto-Deploy

Related tasks

Run the Server Installation

Log in to the CSM Desktop Client or CSM Administrator

Run the Server Installation

Launch the installation on the server to install the Server application files. Use the Cherwell Service Management installation wizard to begin the installation and the Cherwell Configuration Manager to configure the services.

Remember: Run the installation as a system administrator so that all installation steps can execute successfully.

1. In the CherwellDiskImage-English folder, right-click the Cherwell_Service_Managment_Installation.exe file and select **Run as Administrator**. The **Cherwell Service Management installation** window opens.
2. Select **Install** in the **Server** section of the Cherwell Service Management installation wizard. The **Cherwell Service Management Server Setup** window opens.
3. Select **Install** in the **Cherwell Service Management Server Setup** window. The install begins and the Cherwell Service Management Server Setup Wizard opens.
4. Review the introductory text, and then select **Next**.
5. Select **I accept the terms in the license agreement**, and then select **Next**.
6. Use the default location folder in which to install the Server installation files or select **Change** to browse to another location. We recommend accepting the default installation folder. See Folder Selection Options. Select **Next**.
7. Select **Install** to start the installation. After the installation begins, the **Cherwell Configuration Manager** opens.
8. Select **Start** on the **Cherwell Configuration Manager**.
9. Select the database components to install, and then select **Next**. See Database Selection Options.
10. Select which CSM services to enable by default, and then select **Next**. See Server Selection Options.
11. Provide the Cherwell Server account credentials that will be used to launch the CSM services, then select **Finish**. See Server Log in Information.
12. The next page depends on selections made on the **Database Selection** page:
    ◦ **Cherwell demo database**: The Connection Wizard opens to help configure the Server connection (the connection between the CSM Application Server and the CSM database).
    ◦ **Update an existing database**: A prompt appears to select an existing CSM database to update. Select a database, log in, and then approve the update. Select **OK** when the wizard shows that the update is complete.
    ◦ **Not update any data**: Installation is complete. A database update is typically necessary, so there might be a prompt to update the database upon first run of the applications.
    ◦ If prompted, select an installation environment:
        ◦ Development: The database file is being used to configure functionality.
        ◦ Production: The database file meets all requirements, has been tested, and is ready for business use.
        ◦ Test: The database file is being used for testing purposes.

Note: The environment type provides visibility into the environment you are working with while managing your system. Once this value is selected, it displays in the client login windows, window titles for the CSM Desktop Client and CSM Administrator (when configured), the Health Check Results window, and the Company Information drop-down in the CSM Browser Client and CSM Portal. You can leverage these values in your configurations using their associated System Functions.

13. Provide a default password for the Cherwell Message Queue Service, and then select **Finish**.

14. The base URL of the Cherwell REST API is automatically populated. If you need to edit it, see Set the Base URL for the Cherwell REST API.

15. Select **Close** on the **Cherwell Configuration Manager**.

16. Select **Finish** on the **Cherwell Service Management Setup Wizard**.

17. Select **Close** on the **Cherwell Service Management Server Setup** window.

Related concepts

Server Installation Options

Configure the Server Connection

Use the Connection Wizard to configure the Server connection.

The Connection Wizard is automatically launched by the Installation Wizard during the Server installation. The server connection is a direct-to-database/2-tier connection between the Cherwell Application Server and the CSM database.

> **Note:** Using a proxy server during configuration is not supported or recommended. Proxy servers can change request headers and cache information, both of which can cause unknown and unexpected issues with the Cherwell Client and Web Applications.

To configure the Server connection:

1. Open the Connection Wizard in one of the following ways:
    - Automatically opens during installation If installing the Demo or Starter database (new user).
    - Manually open the Connection Wizard from Cherwell Server Manager by selecting **Add**.
    - For an existing user with a CSM connection already configured, the Connection Wizard does not appear, but there is a prompt to update the database either during the installation process or on first run of an application if an update is required.

2. Review the introductory text.

3. Select **Next**.

4. Select a connection type:
    - **Connect to a Cherwell** Server. This option takes you to the Server Location page next to provide the URL for the Cherwell Application Server.
    - **Connect directly to a Cherwell** database (this is a direct-to-database/2-tier connection).

5. Select **Next**.

6. Select a location to install the CSM database to.

7. Select **Next**.

8. Provide a name and owner for the database, or select **Browse** to see a list of available databases. If unsure of the database name or owner, accept the default values.

9. Select **Next**.

10. Specify the Database Login account credentials.

11. Select **Next**.

12. Select the connection pooling and security or failover options.

13. Select **Next**.

14. Accept the **default connection name (Cherwell)** and provide an optional description.

    > **Note:** If the default connection name (Cherwell) is not accepted, the CSM Server (service) connections have to be manually configured.

15. Select **Next**.

16. Select **Test Connection** to verify the connection to the database. If the test fails, check settings or choose to finish the installation.

17. Select **Finish**.

CSM creates the Server connection, and then imports the database. If this is an upgrade, CSM imports any new, required internal system definitions.

If there is a message that the database needs to be upgraded to work with the latest version of CSM, select **Yes**, and then perform the upgrade.

Related concepts

Connections

Default Port Numbers

Related reference

CSM Server and Browser Connection Options

Server Installation Options

Explore the available options for folder selection, database selection, server selection, and server log in when installing servers.

Folder Selection Options

The default folder for the Server installation files is C:\Program Files\Cherwell Service Management. Select **Change** to browse to another location.

Note: CSM does not install to C:\Inetpub because IIS sometimes removes files in this directory in certain scenarios.

Database Selection Options

Select the data to install. The following table describes each of the database options.

Option	Description	Notes
Cherwell Demo Database	Installs the Cherwell Demo database (contains structure and sample data/users).	Recommended for evaluating CSM. When **Install** is selected, the Connection Wizard opens, prompting you to configure the database connection.
Cherwell Starter (Empty) Database	Installs the Cherwell Starter database (contains structure but no data).	Recommended for using CSM in a production environment. This option opens the Connection Wizard, prompting you to configure the database connection.
Upgrade an existing database	Updates an existing database to the most recent version.	If the database is not updated here, there is a prompt later if an update is required. Select **Install**, and then select a database to update.
Do not load any data	Skips installing or updating the database.	Use this option when a database is not needed on the machine where you are installing server applications. For example, select this option if you are installing CSM on distributed servers.

Server Selection Options

During the server installation, the Server Manager and all servers and services are installed. You must select which to enable by default. The following table describes each server option.

Option	Description	Notes
Application Server	Select this option to enable the Application Server as a web application under IIS.	Windows Communication Foundation (HTTP and Non-HTTP Activation) components are also required.

Option	Description	Notes
Automation Process Service	Select this option to enable the Automation Process Service.	Configure the Automation Process Service in the Server Manager after installation.
Scheduling Service	Select this option to enable the Scheduling Service.	Configure the Scheduling Service in the Server Manager after installation.
E-mail and Event Monitor	Select this option to enable the E-mail and Event Monitor service.	Configure the E-mail and Event Monitor in the Server Manager installation.
Mail Delivery Service	This service enables email message queuing, which provides increased throughput of messages.	Configure the Mail Delivery Service in the Server Manager after installation. The Mail Delivery Service is automatically installed and enabled, along with the Cherwell Message Queue Service message broker application. Since the installation is automatic, Mail Delivery Service will not appear as an installation option. • When you install CSM for the first time and select the **Don't load any data** option instead of the Starter or Demo database, you must set the connection information manually; credentials will be set to use CSDAdmin. • When you install CSM for the first time and use the demo or starter database, the Mail Delivery Server uses that database as its connection; credentials will be set to use CSDAdmin.

Server Log in Information

Specify a name and password for Cherwell Service Host and microservice configuration. You can choose a specific Windows domain account or a special Windows service account.

Option	Description	Notes
Specific account	Provide a User name (should be in the format *DOMAIN\UserAcct*) and Password.	Select **Browse** to locate domains and accounts on each domain.
Confirm that User name & Password are legal	Select this check box to confirm that legal credentials were entered.	By default, the installer confirms that the credentials are legal.

Option	Description	Notes
Use Special Account	Select this check box to use a Windows account for the Cherwell Service Host and its four microservices. If a special account is selected, the Application Server is installed using the built-in AppPoolIdentity account.	You must select one of the following options: • Local System Account • Local Service Account • Network Service Account
Local System Account	This account has extensive administrative privileges on the local computer and acts as the computer on the network. With unrestricted access to local resources, it is capable of doing things that could bring down the entire system.	Enabled when the **Use Special Account** check box is selected. **Important:** The local system account should not be used in production environments.
Local Service Account	This account has minimum privileges on the local computer and presents anonymous credentials on the network. The user privileges are limited to the local computer. Use this service for processes that do not require access outside the server on which it is running.	Enabled when the **Use Special Account** check box is selected.
Network Service Account	This account has minimum privileges on the local computer and acts as the computer on the network. The service is authenticated to other computers on the network by using the computer's account in the domain.	Enabled when the **Use Special Account** check box is selected.

Related concepts

Default Port Numbers

Using Databases with CSM

Configure the Application Server

CSM Server and Browser Connection Options

When configuring browser and server connections during your CSM installation, specify a location for the database, the database login account credentials, administrative login options, connection pooling options, and additional advanced options.

Database Location Options

The following table describes database location options.

Option	Description	Notes
Database is on this machine	Connect to a local database.	Typically, this option is only for evaluation systems.
Specific server	Connect to a database that is installed on a named server.	Provide the database server name, or select the name of the database server in the drop-down list. The list might take a few seconds to populate, and the desired server may not be listed. **Note:** If installing on an alternative instance of SQL Server, specify the instance as part of the name: CSMDatabaseServer\Instance.
IP Address	Connect to a database installed on a server referenced by an IP address.	Provide the database server IP address.

Database Login Account Credentials

The database login account must have *DBReader* and *DBWriter* SQL permissions with rights to insert, update, and delete rows within tables. If you also plan to use this account for the administrative functions, the account must also have *DBOwner View Server State* permissions (although these permissions are not recommended for production environments).

Option	Description	Notes
Windows authentication	Use the stored Windows credentials (user name and password) for authentication.	Not recommended for browser connections.
User ID and Password	Select this option to log in by providing the user ID and password of SQL Server.	Recommended for browser connections.

We strongly recommend that you use a SQL account with sufficient rights rather than Windows Authentication to connect to the CSM database for the following reasons:

- The database connection must work with the security options for Internet Information Sevices (IIS). When connecting using SQL credentials, a different connection is used so that the CSM browser applications can run inside IIS. However, when connecting using Windows Authentication, IIS must be specially configured to use a Windows account that has appropriate rights to the database.

- When using Windows Authentication credentials, the Windows account that must be authenticated against SQL Server is the account that is used by the IIS application pool running the CSM browser applications. This account is usually a special local account, which does not have rights beyond the machine, and usually does not have rights to SQL Server running on the same server. This impact to connection pooling may also impact performance.

    Note: Setting up Windows Authentication requires configuration of both IIS and SQL Server and is beyond the scope of this document.

When using SQL account credentials, note the following requirements:

- The *View server state* privilege must be set for the SQL database login account. In SQL Server Management Studio, this privilege is located on the **Securables** tab of the **Login Properties** window.
- SQL Server must be configured for mixed mode authentication to support the use of SQL credentials.
- The SQL account must have rights to insert, update, and delete rows in the database.

Administrative Login Options for Server Connection

Specify the account credentials that the administrative functions use to log in to the CSM database when the database is being modified during the publishing of a CSM Blueprint.

The administrative login account must have *DBOwner* permission and *View Server State* privileges with rights to create, drop, and alter tables, as well as insert, update, and delete rows within tables. When the CSM services use this connection, the account under which the service is running is the account whose credentials will be used to connect to the database. If the Cherwell Application Server is installed in the same domain as the database, and the service account has rights to the database, then you can use Windows Authentication to provide the credentials.

Administrative Login Options

Option	Description	Notes
Same as standard login	Select this option to use the same login options as the system.	Not recommended for production environments.
Windows authentication	Select this option to use the stored Windows credentials (user name and password) for authentication.	
User ID and Password	Select this option to login in using a specific user name and password.	Provide the user ID and password.

Connection Pooling and Advanced Options

The **Connection Options** page includes sections for connection pooling options and advanced settings.

Connection Pooling and Advanced Options

Option	Description	Notes
Use default pooling options	Select this option to use the default pooling options.	This option is appropriate for most systems with 30 or fewer concurrent CSM licenses.
Customize pooling options	Select this advanced option to specify custom pooling options.	Specify the pool sizes to customize the caching options. To improve performance, set the maximum pool size to three times the number of concurrent CSM licenses that are used in your organization. You may need to adjust this value, depending on usage of your system.
SQL Server is configured as an AlwaysOn group	Sets the MultiSubnetFailover property on the connection string, which allows for a faster detection and connection to the active server.	In the instance of a failed server, instead of attempting to reconnect one IP address at a time sequentially, SQL attempts using all addresses simultaneously to re-establish the connection.
Encrypt connection with SQL Server	This option sets the Encrypt property within the connection string.	In a server with a certificate installed, the property gets or sets a Boolean value. In turn, the value informs SQL whether to use the SSL encryption when sending and receiving data between the client and server application.
Always trust SQL Server's SSL certificates	This option sets the TrustServerCertificate property on the connection string.	This option is enabled when **Encrypt connection** option is selected. When this property is selected, the transport layer uses the SSL to encrypt (to the level specified by the server) the channel. The channel bypasses going through the certificate chain to validate trust.
Change Connection Packet Size	Allows users to specify the packet size of the connection.	

Related concepts
Configure the Server Connection
Related tasks
Configure the Browser Connection

Run the Web Applications Installation

Logged in as system administrator, install Browser Applications, update Auto-Deploy, and configure the browser connection to the CSM database.

Launch the installation on the server where you want to install the Portal and Browser applications files. Use the Cherwell Browser Applications Setup Wizard to install the applications and the Cherwell Configuration Manager to configure the applications.

Remember: Run the installation as a system administrator so that all installation steps can execute successfully.

To run the Portal and Browser Apps installation:

1. In the CherwellDiskImage-Enlish folder, right-click the Cherwell_Service_Managment_Installation.exe file and select **Run as Administrator**.

   The Cherwell Service Management installation window opens.

2. Select **Install** in the Portal and Browser Apps section.

   The Cherwell Browser Applications Setup Wizard opens.

3. Select **Install**.
4. Review the introductory text, and then select **Next**.
5. Read the license agreement. The license agreement can also be printed. If you accept the license terms, select the **I accept the terms in the license agreement** check box, and then select **Next**.
6. Use the default location/folder in which to install the Browser installation files, or select **Change** to select another location. Select **Next**.
7. Review the text, and then select **Install**.

   The Cherwell Configuration Manager opens to set up the Browser applications.

8. Select **Start**.
9. Select which Browser applications to install.

   Note: The Cherwell REST API is installed regardless of the selections made on this page. If no selection is made, only the REST API is installed.

   Select **Next**.

10. Choose Auto-Deploy options, then select **Finish**.
11. The next page depends on previous selections:
    ◦ If Auto-Deploy is not yet configured and the user wants to update it: The installer prompts to configure Auto-Deploy installation. Select **Yes** and configure it now, or configure it later by

selecting **Windows Start > Cherwell Browser Applications > Auto-Deploy Config** or **Windows Start > Programs > Cherwell Service Management > Tools > Configure Auto-Deploy**, depending on the Server.

- ◦ If browser connection (new user) is not yet configured: The Connection Wizard opens to help configure the connection between the CSM Browser applications and the CSM database. This is a different connection than the one for CSM because the Browser Apps run inside IIS and the connection needs to work with the IIS security options. Follow the instructions in the wizard.

- ◦ If the Cherwell Browser connection (existing user) is already configured: Installation is complete.

12. Select **Close**.

13. Select **Finish** on the Cherwell Browser Applications Setup window.

14. Select **Close** on the Cherwell Browser Applciations Setup window.

Configure the Browser Connection

Use the Connection Wizard, which is automatically launched by the Installation Wizard during the Portal and Browser App installation, to configure the Browser connection. The Browser connection is a direct-to-database/2-tier connection between the web applications and the CSM database.

Most options are assumed or set by default to assist with decision making. For example, the connection type is assumed to be a direct-to-database connection and the database connection is named Cherwell Browser. Wizard page examples are in Configure the Server Connection.

Important: Using a proxy server during configuration is not supported or recommended. Proxy servers can change request headers and cache information, both of which can cause unknown and unexpected issues with the CSM Web Applications.

To configure the Browser connection:

1. Open the Connection Wizard in one of the following ways:
    ◦ If installing the Demo or Starter database (new user), the Connection Wizard automatically opens during the installation process.
    ◦ Manually open the Connection Wizard from the Connect to CSM window by selecting the **Add** button.

    > **Tip:** If the Connection Wizard is manually opened, be sure to name the connection `Cherwell Browser`.

    ◦ If an existing user already has a CSM connection configured, the Connection Wizard does not appear but instead you are prompted to update your database either during the installation process or on first run of an application if an update is required.

2. Review the introductory text, and then select **Next**.

    > **Note:** If the wizard is automatically launched by the Installation Wizard, this window does not appear because CSM already knows that it is a direct-to-database connection.

3. Select **Connect directly to a Cherwell database** because this is a direct-to-database/2-tier connection, then select **Next**.

4. Specify where to find the CSM database, this is the name of the SQL Server machine where the CSM database was installed, then select **Next**. For information on the database location options, see CSM Server and Browser Connection Options.

5. Provide the name and owner of the installed database to connect to. If unsure, leave the default values. Select **Next**.

    > **Note:** The last page of the wizard enables you to test the database connection.

6. Specify the Browser App Database Login account credentials that the Browser applications use to log in to the CSM database, then select **Next**. For more information on the options and requirements for these credentials, see CSM Server and Browser Connection Options.

7. Select connection pooling and security/failover options, then select **Next**. For more information on these options, see CSM Server and Browser Connection Options.

8. Accept the default connection name (Cherwell Browser), provide an optional description for the Browser connection, and then select **Next**.

> **Note:** If the default connection name (Cherwell Browser) is not accepted, manually edit configuration files for the Browser applications. For more information, refer to Troubleshoot the Web Applications

9. Select **Test Connection** to verify the connection to the database.

> **Note:** If the test fails, the installation can continue.

10. Select **Finish**.

Related concepts
Connections
Default Port Numbers
Related reference
CSM Server and Browser Connection Options

Web Applications Installation Options

Explore the available options for Auto-Deploy and folder selection when you install the Web Applications.

Folder Selection Options

The default folder location for the browser installation files is C:\Program Files\Cherwell Browser Applications. Select **Change** to browse to another location.

Note: CSM does not install to C:\Inetpub because IIS sometimes removes files in this directory in certain scenarios.

Auto-Deploy Options

When you run the Web Applications installation, you need to specify auto-deploy options. The following table describes each auto-deploy option:

Option	Description	Notes
Update Auto-Deploy	Update the Auto-Deploy feature. Updating Auto-Deploy wraps the latest version of the installer so that users can then install CSM by clicking a link on a web page, or automatically after being prompted to upgrade when running an older version of CSM.	If this is the first time setting up Auto-Deploy, there will be a prompt to configure Auto-Deploy after selecting Install (later in the installation).
Don't Update Auto-Deploy	Does not update the Auto-Deploy configuration.	If not updated now, Auto-Deploy can be configured/updated later by selecting either of these options depending on the server: • **Windows Start>Cherwell Browser Applications>Auto-Deploy Config** • **Windows Start>Programs>Cherwell Service Management>Tools>Configure Auto-Deploy**

Run the Client Installation

Launch the installation on the Client machine to install the Client application files.

Remember: Run the installation as a system administrator so that all installation steps can execute successfully.

Tip: Client installations are run last and are typically pushed out to users using the Auto-Deploy feature (configured separately).

To run the Client installation:

1. Right-click the Cherwell_Service_Management_Installation.exe file and select **Run as Administrator**.

   The **Cherwell Service Management Installation** window opens.

2. Select **Install** in the Client section.

   The **Cherwell Client Setup Wizard** opens.

3. Review the introductory text, and then select **Next**.

4. Read the license agreement. The license agreement can also be printed. If the license terms are accepted, select the **I accept the terms in the license agreement** radio button, and then select **Next**.

5. Select **Install** to start the Client installation.

6. When the install is complete, select **Finish**.

Configure the Client Connection

Use the Connection Wizard to configure the Client connection (App Server/3-tier connection between the Client machine and the Cherwell Application Server).

In most cases, the Connection Wizard is launched and the Client connection configured during the Auto-Deploy configuration so that it can be pushed out to users using the Auto-Deploy feature. See Configure the Server Connection.

⭐ **Important:** Using a proxy server during configuration is not supported or recommended. Proxy servers can change request headers and cache information, both of which can cause unknown and unexpected issues with the CSM Desktop Client and web applications.

To configure the Client connection:

1. Open the Connection Wizard in one of the following ways:
    ◦ Manually open the Connection Wizard from the **Auto-Deploy Configuration** window by selecting **Connection**.

    ◦ Manually open the Connection Wizard from the **Connect to CSM** window by selecting **Add**.

    ◦ If an existing user and a CSM connection is already configured, the Connection Wizard does not appear but there is a prompt to update the database either during the installation process or on first run of an application if an update is required.

2. Review the introductory text, and then select **Next**.

3. Select **Connect to a Cherwell Server** (because this is an Application Server/3-tier connection), and then select **Next**.

4. Specify where to find the Cherwell Application Server, and then select **Next**. For details on specifying the server location, refer to Client Connection Options.

5. Provide a name and description for the Client connection, and then select **Next**.

   ✏️ **Note:** There cannot be two connections with the same name, so we recommend a name like *Company* Cherwell.

6. (Optional) Select **Test Connection** to verify that the connection to the server/database.

   ✏️ **Note:** The Cherwell Application Server must be running in order to successfully test a 3-tier connection. If the Application Server is not running (if this is a first-time install or or the Application Server is paused), manually start it using the Server Manager. (Select **Start > All Programs > Cherwell Service Management > Tools > Server Manager**. Then select the Cherwell Application Sever and select Start Server).

   ✏️ **Note:** It is possible to finish creating the connection without testing the connection.

7. Select **Finish**.

CSM creates the Client connection.

Related concepts
Connections
Related reference
Client Connection Options

Client Connection Options

Explore the server location options for configuring the client connection.

Server Location Options

In the course of configuring your client connection, you will be required to specify the location of the Cherwell Application Server. The following table describes each option.

Field	Description	Notes [optional]
URL	Provide the URL of the server where the CSM Application Server was installed.	Provide a URL using the HTTP protocol. TCP connections are a legacy configuration and are only available for systems upgraded from a version earlier than CSM 9.5.0. For new installations of CSM, only HTTP connections are supported. The connection type must match the configuration on the server, however.
Advanced	Select this link to specify Certificate Validation Mode settings. This option is for advanced users.	If the Security Mode is unknown, leave the option set to Server Determines Mode, and CSM reads the settings from the server.

Client Installation Options

Explore default folder and client setup type options for Client installation.

Folder Selection Options

The default folder for the Client installation files is C:\Program Files\Cherwell Browser Applications. Select **Change** to browse to another location.

> **Note:** CSM does not install to C:\Inetpub because IIS sometimes removes files in this directory in certain scenarios.

Client Setup Types

In the course of your Client installation, you are required to specify a setup type. The following table describes each option:

Options	Description	Notes
Client-only	Installs the CSM Desktop Client, Outlook Add-in (Installer), and the Dashboard Viewer.	
Client and Administrator tools	Installs the client-only applications and the Administrator tools (CSM Administrator, Report Runner, System Upgrade/Restore, and Test LDAP).	

Logging in to CSM Applications

When logging in to CSM applications, select a connection, provide credentials, and select a role.

The main CSM applications require users to log in to access the system. These applications include:

- CSM Desktop Client or CSM Administrator
- CSM Browser Client
- Cherwell Portal

To Log in to a CSM Application:

1. **Select a connection**: Either directly to the database or to the Cherwell Application Server, which is connected to the database.
2. **Provide CSM credentials**: User ID and password.
3. **Select a Role for the session (if the User has access to multiple Roles)**: For example, an administrator could have the Role of IT Service Desk or IT Service Desk Manager.

Using Auto-Deploy

Auto-Deploy is an installation tool that allows system administrators to automatically distribute preconfigured Client installations and connections to client machines.

When working with the Auto-Deploy feature, Users can:

- Configure Auto-Deploy.
- Run Auto-Deploy.

Use the Auto-Deploy Configuration window to configure Auto-Deploy to push out Client installations. When configuring Auto-Deploy, the system administrator defines:

- Which Client connection to push out.

  Important: For first-time installations, the Client connection must be configured during the Auto-Deploy configuration. Refer to Configure the Client Connection.

- Where to place the installation files.
- Connection and minor release options.
- Which CSM applications to install.
- Installation account options.

Run Auto-Deploy

Users must download and install Auto-Deploy the first time they open the Desktop Client. After the initial installation, Users are prompted to install the new version.

  Note: Auto-Deploy requires Microsoft .NET Framework 4.8. Before installation, Auto-Deploy verifies that Microsoft .NET Framework 4.8 exists on the client machine. If it does not exist, Auto-Deploy downloads and installs it.

To run Auto-Deploy:

1. Type the URL into the Auto-Deploy installation.
2. To install CSM, select the **Cherwell Service Management** link.
   The Open/Save download box appears for the download.
3. Run the file.
   Auto-Deploy launches. The Auto-Deploy options vary depending on how the system administrator configured Auto-Deploy.

     Note: The Auto-Deploy file is generated dynamically by the local server and is unsigned. An unsigned file can trigger malware alerts.

4. After the installation finishes, reboot your machine.

Configuring Auto-Deploy

Configure Auto-Deploy to distribute Client installations to client machines.

To configure Auto-Deploy:

1. Open Auto-Deploy:

   Important: Due to commonly used components in Auto-Deploy technologies, an error may appear cautioning against running the Auto-Deploy application. An error may also appear depending on your Operating System and anti-virus settings. If the error appears, select **Run Anyway**.

   ◦ If Cherwell Application Server is installed: select **Windows Start > All Programs > Cherwell Service Management > Tools > Auto-Deploy Config**.

   ◦ If Cherwell Browser is installed: select Windows **Start > All Programs > Cherwell Browser Apps > Auto-Deploy Config**.

2. Optional: Configure the client connection if this is a first-time installation.

3. Select the **Ellipses** button to select an existing client connection if this is not a first-time installation. The **Database Manager** window opens.

4. Select an existing connection.

   Note: Do not use the connections created for the Cherwell Servers or Browser Applications because these are direct-to-database connections. Connect to the Cherwell Application Server.

5. Select **OK**.

6. Provide the Auto Deploy Site URL.

7. Select the **Ellipses** button to select a Target folder. The Target folder is a directory location on the server that specifies where the install files are stored.

8. Select desired check boxes to configure additional options:
   ◦ Overwrite Client Connection

   ◦ Make Connection Be Default

   ◦ Require Users to Install Minor Releases

   ◦ Connect Without Prompting

   ◦ Display Debug Messages

9. Select **OK** to close the **Auto-Deploy Configuration** window.

Related concepts
Configure the Client Connection

Configure Auto-Deploy Options

Explore options for Auto-Deploy configuration.

The table below describes the details of the Configure Auto-Deploy options.

Option	Description
Connection	The Client connection that is pushed out to all clients during installation. This must be an Application Server connection (3-tier connection).
Auto Deploy Site	The URL of the website housing the Auto-Deploy installation. If the defaults are selected during the installation, then it is called CherwellAuto-Deploy (example: http://MyServer/CherwellAutoDeploy).
Target Folder	The directory on the server where the install files are stored. This should be the directory where Auto-Deploy is installed (the physical directory that is pointed to by the Auto-Deploy site). If defaults were selected during the installation, this should be C:\Program Files (x86)\Cherwell Browser Applications \CherwellAutoDeploy. **Important:** Change the default value to remove `(x86)` from the file path, or update the target folder to where you want to install Auto-Deploy.
Options	
Overwrite client connection	Overwrites any defined Client database connections with the same name. For example, if the Auto-Deploy connection was [Common]Cherwell and the user already had a connection named [Common]Cherwell, it is overwritten.
Make connection be default	Makes the installation connection the default Auto-Deploy connection for users.
Require users to install minor releases	Requires users to install minor releases (example: CSM 10.1.1 on top of CSM 10.0.0) even if the current version is compatible with the server. If this check box is cleared, users are given the option.
Connect without prompting	Automatically connects to the installation connection without prompting users.
Display Debug messages	Use for troubleshooting only. A series of message boxes appear during deployment. Leave this check box cleared.
Installation Options	The CSM applications to install on the Client machines.
Run Installer on client without providing any options to user	Does not give the user any options during the installation. Users are prompted whether or not to install, but are not allowed to change the install directory or files to install, and then select what to install.
Install only the Cherwell client application	Installs the CSM Desktop Client, Outlook Add-in (Installer), and the Dashboard Viewer.
Install the Cherwell client and Administrative tools	Installs both the Client application and the Administrator tool.

Option	Description
Allow user to choose what to install	Allows the user to select whether or not to install the Administrator tool. **Note:** This option is disabled if the Run Installer check box is selected.

Licensing CSM

CSM uses a concurrent or floating license model to control how many users can log in at the same time. This means that a fixed number of licenses are shared among a group of users/customers, and that a fixed number of people can simultaneously access the product.

License codes determine the number of people who can log in at any given time.

Example: If 100 licenses are purchased (100-person concurrent license), 100 people can log into CSM at any given time; the 101st person is prohibited. When any one of the 100 people logs out, the next person can log in.

License consumption varies depending on the product, who logs in (user or customer), and what tasks each person performs.

License keys are valid for a set time period. Keys expire at 12 AM on the expiration date. For example, a key that has an expiration date of September 24, 2020, expires at the beginning of September 24 rather than at the end of that day. Expiration time is based on the time zone of the Cherwell Application Server server.

Related concepts
Add a License Key
Reserve a License for a User
Related information
Reserve Licenses for a Department

Add a License Key

License keys, also known as license codes, determine the number of people who can log in at any given time.

Use the Licensing window in CSM Administrator to provide a license code.

Note: You may be prompted to provide a license code when you attempt to log in to CSM.

To license CSM:

1. Open the Licensing window (CSM Administrator>Security>Licensing).
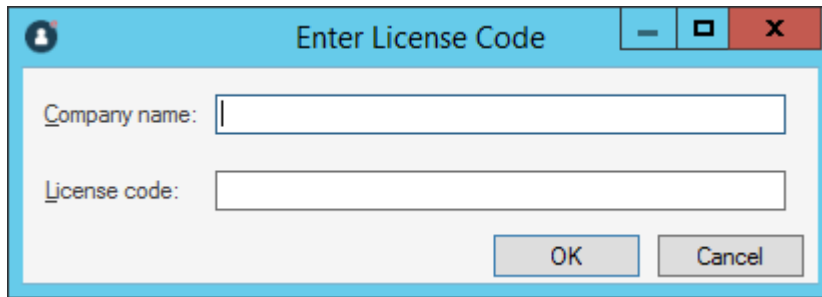
2. Click the **Enter Code** button.

   The Enter License Code window opens.

3. Provide a **company name** and **license code**. If you need a license code, contact Cherwell Software.

4. Select **OK**.

Related concepts
Reserve a License for a User

Automatically Release a License
Related information
Reserve Licenses for a Department

Reserve a License for a User

Reserve a license for a specific user to ensure they always have access to your system. A license can be freed by removing it from user. This allows it to be reserved for a different user.

Tip: We recommend that you reserve a license for the system administrator to ensure permanent access.

To reserve a license for a user and remove it from the set of available concurrent licenses:

1. In CSM Administrator, select **Security**.

2. Select **Licensing**.

   The **Reserved Licenses** area lists the reserved licenses by user and department.

3. To reserve a license for a particular user:
   a. Select **Add user**.

      The **Add Reserved License** window opens, listing users who do not currently have a reserved license.

   b. Select one or more users for whom to reserve a license.

      Tip: Press **Ctrl** to choose a non-contiguous selection of users. Press **Shift** to select a contiguous list of users. Select **New User** to create a new User Profile. See Create a User Profile.

   c. Select **OK**.

      The **Has reserved license** check box in the User's Profile updates to show a reserved license.

      Tip: Reserve or free a license by selecting or clearing the **Has reserved license** check box on the User's Profile (**Security > Edit Users**).

4. To free a license, select the **User**, and then select **Remove**.

5. Select **OK**.

Related concepts
Automatically Release a License
License Consumption
Related information
Reserve Licenses for a Department

Reserve Licenses for a Department

You can group licenses for a department to use. This means that concurrent licenses are segmented for use by different organizations within a company.

When you reserve a license for a user or a department, you take that license out of circulation. Any licenses left over can be used as and when needed. Reserving licenses guarantees a certain number of licenses are always available for a department by removing those licenses from the general set of licenses available. This does not limit the department to only those licenses if there are additional non-reserved licenses available.

Note: Reserve two licenses for the IT department so that members of that department can always access CSM.

Note: Reserving licenses for a department is available only if the **Holds** property is set on a **Department** field in the UserInfo Business Object. To find the **Holds** property:

1. Open the CSM Administrator
2. Edit a Blueprint containing the UserInfo Business Object.
3. Go to the **General** page and you see the **Holds** drop-down list.

We also recommended that this field is validated with a list of legal departments.

Examples of License Use

1. You reserve 30 licenses for the HR department out of 100 available licenses. 30 HR staff log in. More HR staff can still log in because the remaining 70 licenses are not reserved for anyone else. However a maximum of 70 non-HR users can log in at any one time because 30 licenses are always reserved for HR.
2. You have 100 licenses with 20 reserved for Accounting and 25 reserved for HR, leaving 55 licenses available for general use. If 30 users from Accounting and 30 users from HR are logged in, consuming a total of 60 licenses, 40 are available for any other users what want to use CSM.

To reserve one or more licenses for a particular department:

1. In CSM Administrator, select **Security**.
2. Select **Licensing**.

   The **Reserved Licenses** area lists the reserved licenses by user and department.

3. Select **Add department**.

   The **Add Department Licenses** window opens.

4. Enter the **Department name** for which you wish to reserve a license.

5. Select the number of **Licenses to reserve** for that department.

6. Select **OK**.

To modify licenses reserved for a department:

1. To free a license, select the **Department**, and then select **Remove**.

2. To change the number of reserved licenses for a department, select the **Department**, and then select **Edit**.

3. Enter the new number of licenses.

4. Select **OK**.

Related concepts

Reserve a License for a User

Automatically Release a License

License Consumption

Automatically Release a License

Use the **Automatically Release a License** option in the **Licensing** window to automatically release idle licenses.

Licenses become idle for the following reasons:

- User inactivity (example: Walked away with CSM open).
- The CSM Desktop Client crashes.

Good to know:

- Configure the system to automatically log out idle Users, thus releasing licenses (**CSM Administrator > Security > Edit Security Settings > Desktop Client > Logout inactive users from Cherwell Client**). See Configure Login, Authentication, and Inactivity Settings for Each Client/
- The CSM Browser Client and CSM Portal automatically log out users/customers after a period of inactivity based on browser application settings and IIS configuration. See Configure CSM Web Application Settings (URLs, Timeouts, RSS Feeds).

    Note: Closing a browser window without logging out of CSM does not release the license. The license is released when the user/customer logs out or the session times out. If an IIS Reset is performed, the license will be released only if the auto-release option is enabled.

To automatically release a license:

1. Open the Licensing window (**CSM Administrator > Security > Licensing**).
2. Select **If Client Stops Responding, Auto-release License After x Minutes**.
3. Minutes: Specify the number of minutes to wait before releasing the license.

    Tip: We recommend setting the auto-release period to 90 minutes.

4. Select **OK**.

Related concepts
License Consumption

License Consumption

License consumption varies depending on the application, who logs in (user or customer), and which operations each person performs.

The following operations affect license consumption:

- Only the following Cherwell applications require a license:
  - Desktop Client
  - Browser Client
  - Outlook® Add-In
  - Under special circumstances, the CSM Portall might also require a license

- A user consumes one and only one license when logging into a license-consuming Cherwell application, regardless of the number of applications or instances of Cherwell that are accessed. In other words, a user can simultaneously access multiple Cherwell applications and multiple instances of Cherwell using one license.

  Example: Andrew logs into CSM via his computer; Andrew consumes one license. Andrew then logs into CSM through his mobile device; Andrew still consumes only the one license.

- Customers logging into CSM Portal to view/edit their own records typically do not consume a license (example: A customer owns the record, is the requestor, and is associated with the record). Certain editing tasks require that the customer log in and consume a license. CSM notifies the customer when a license is necessary. Customers who do do not have rights to consume a license cannot edit the record.

- A customer logging into the CSM Portal to access someone else's records does not consume a license to view the record but does consume a license to edit a record. After a license is acquired, it is held for the remainder of the customer's session.

The following table shows license consumption by item:

Item	Consumes License
Client Applications	
CSM Desktop Client	✓
CSM Browser Client	✓
Cherwell Mobile™ for iOS®	✓
Cherwell Mobile™ for Android™	✓

Item	Consumes License
Cherwell Portal™	✔ Sometimes (see People)
CSM Administrator	✖
Supporting Applications	
Auto-Deploy	✖
Cherwell® REST API	✔
Dashboard Viewer	✖
Import Utility (legacy)	✖
Outlook® Add-in	✔
Outlook Add-in Installer	✖
Report Runner	✖
System Restore/Upgrade	✖
Test LDAP	✖
Server applications	✖
Server Manager	✖
People	
User logging into a license-consuming application	✔
User logging into a second license-consuming application	✖
User logging into a second instance of a licensing-consuming application	✖
Customer logging into the CSM Portal to view/create/edit their own record (Requestor/record owner)*	✖
Customer logging into the CSM Portal to *view* someone else's record (not the requestor/record owner but has extended rights to manage another customer's records)*	✖

Item	Consumes License
Customer logging into the CSM Portal to *edit* someone else's record (not the requestor/record owner but has extended rights to edit another customer's records). **Exceptions:** Sometimes, a One-Step Action can edit another dustomer's records without consuming a license (example: Send an Email, Create a Journal, or Rating a Record).	✔ (with exceptions)
* Some Portal Sites and activities require use of a license. CSM prompts the customer if a license is required.	

Related concepts

Add a License Key

Reserve a License for a User

Related information

Reserve Licenses for a Department

Troubleshooting Application Server Installations Using IIS

If you are unable to log in to any CSM Client using an HTTP or HTTPS server connection, follow these troubleshooting steps.

Verify the Server Installation

1. Open the Cherwell Server Manager, and then select Application Server from the **Server** list.
   a. If the Cherwell Server Manager is started in IIS, **Browser application found** is shown on the dialog box.
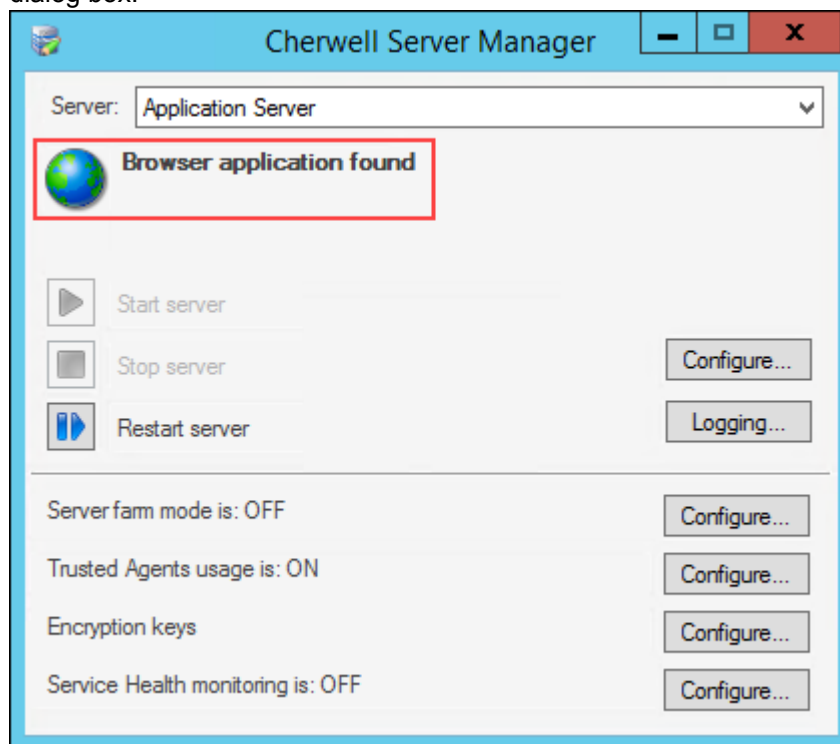
   b. Select **Configure**.
   c. Select the **Connection** ellipsis icon.
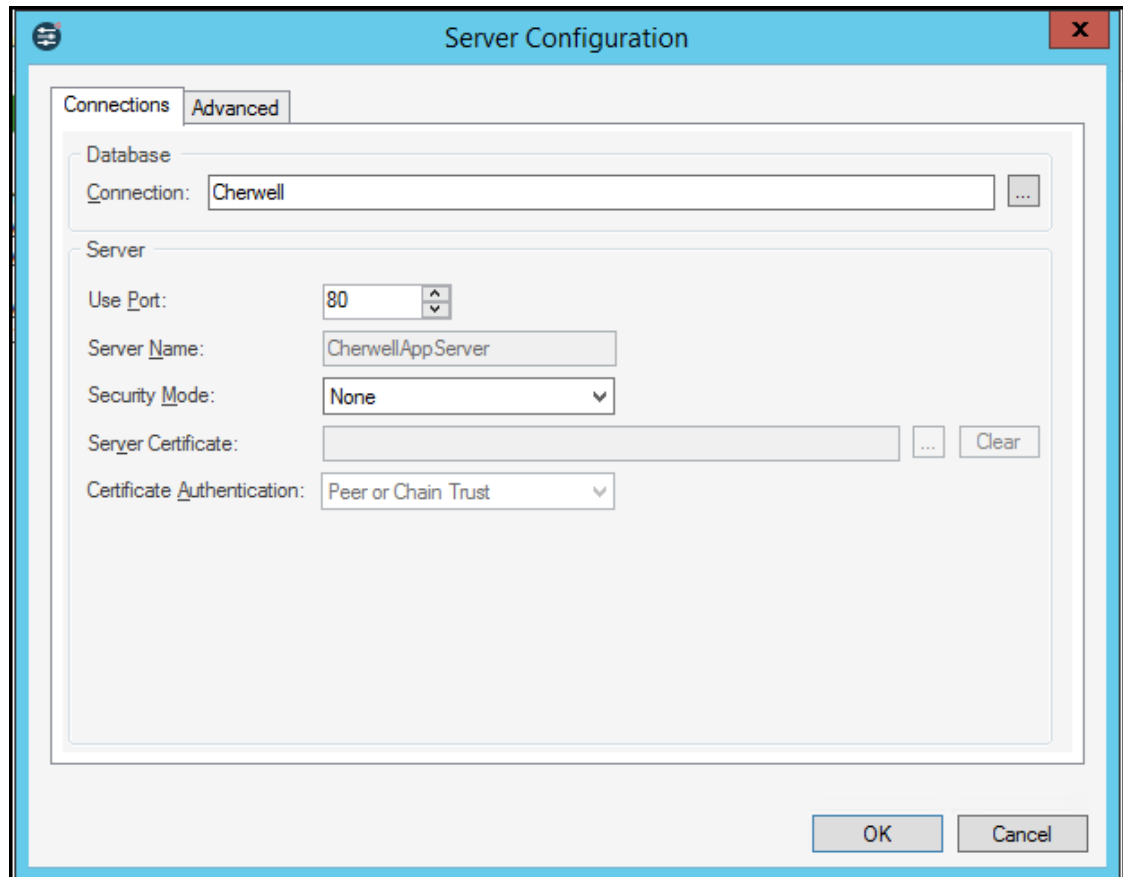
d. Select a connection, and then select **Edit**.

e. Step through Connection Wizard by selecting **Next**. Do not change any options.

f. On the summary page, select **Test Connection**.
   If the connection fails, the issue is with the database connection and not IIS.
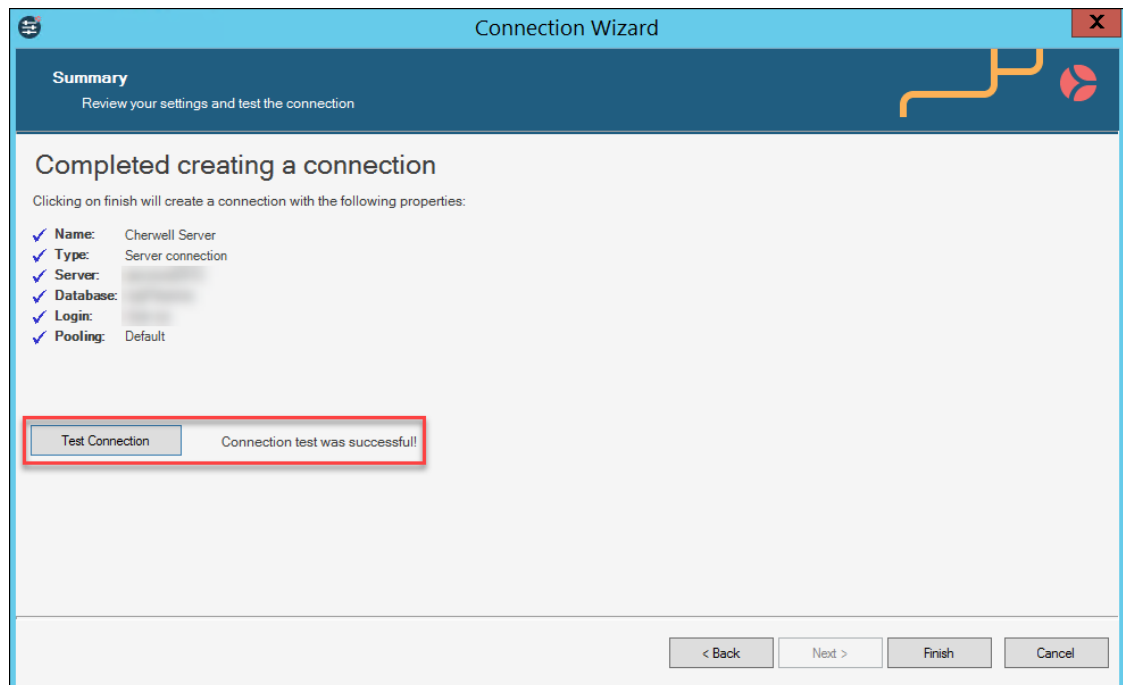
2. Cancel the test connection and close the Connection Wizard.

Verify Port and Security Settings

1. Open the Cherwell Server Manager, and then select Application Server from the **Server** list.
   a. Select **Configure**.

   b. Verify these settings:
      ◦ **Port**: Defaults ports are 80 for HTTP or 443 for HTTPS. (HTTPS should be used for all production environments.)

      ◦ **Security Mode**: **Encrypted** must selected for environments using HTTPS.

      ◦ **Sever Certificate**: If this field is not auto-populated, select the ellipsis icon to browse and select the certificate.

2. Select the **Connection** ellipsis icon.

3. Select **Add**.

   Note: Do not use an existing connection to test, as this can cause issues.

4. Select these options in the Connection Wizard:
   a. **Connection Type**: Select **Connect to Cherwell Server**.

   b. **Server Location**: Provide the **URL** to the server being used. For example, http://cherwell.company.

   c. **Connection Name**: Provide a name and description.

        d. Select **Test connection**.

If the test connection succeeds, CSM and IIS are configured correctly. You can cancel the test connection.

Verify that Windows Features are Enabled on the IIS Server

Verify that HTTP activation features are enabled for the IIS server that will be used with CSM. See Configure IIS for CSM.

Verify Application Pool (AppPool) Settings in IIS

1. Open IIS.
2. Expand the Connections tree to verify the CherwellAppServer is listed as a site.
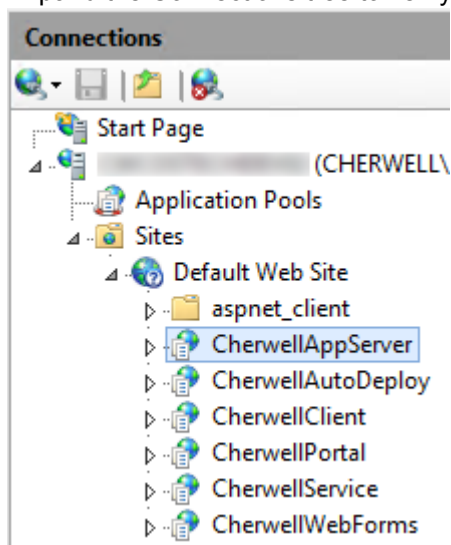
3. Select **Application Pools** in the Connections Tree.
4. Verify that the CherwellAppServer Identity field is ApplicationPoolIdentity or a domain account.
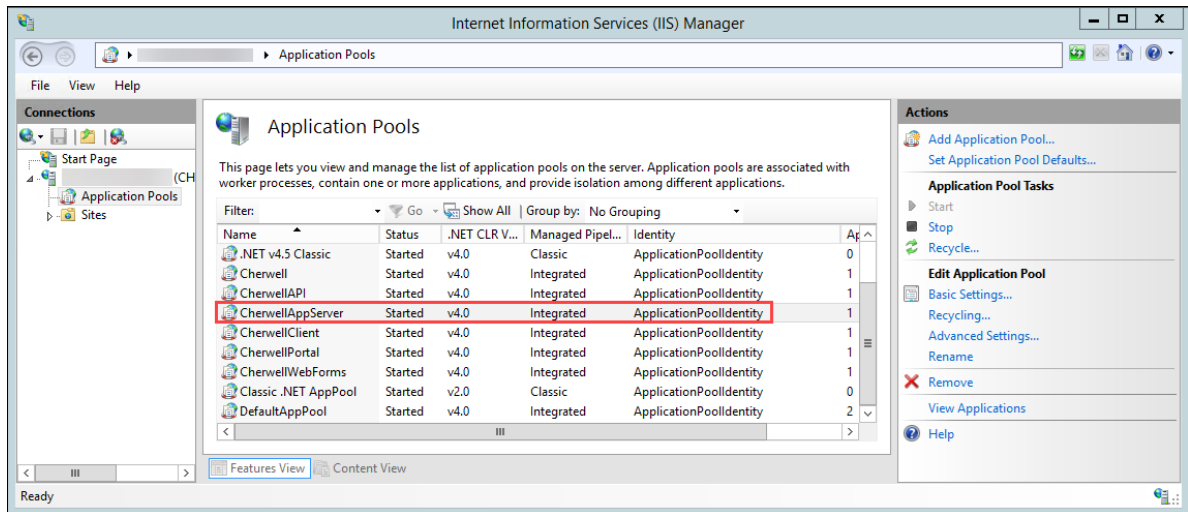
Verify Application Pool (AppPool) Settings for the Folder

1. On the IIS server, navigate to Application Server installation directory. The default location is C:\Program Files\Cherwell Service Management\Cherwell Application Server.

2. Right-click inside the directory, and then select **Properties**.

3. Select the **Security** tab, and then select **Edit**.

4. On the Permissions tab, select **Add**, and then select **Locations**.

5. Select the server name from the Locations dialog.
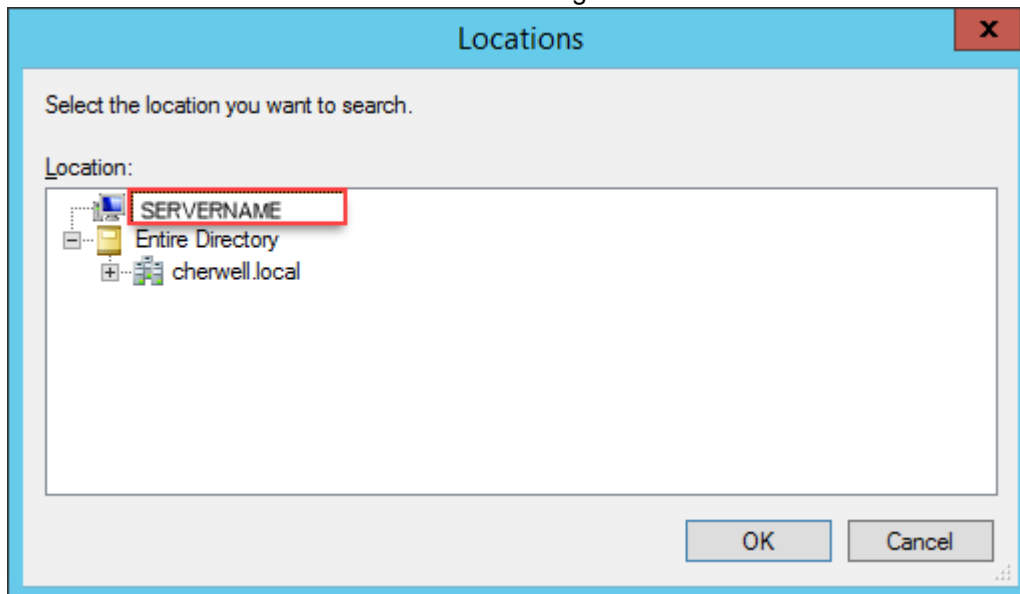
6. Select **OK**.

7. On the Select Users or Groups dialog, enter `iis AppPool\CherwellAppServer` in the Object Names box, and then select **Check Names**.
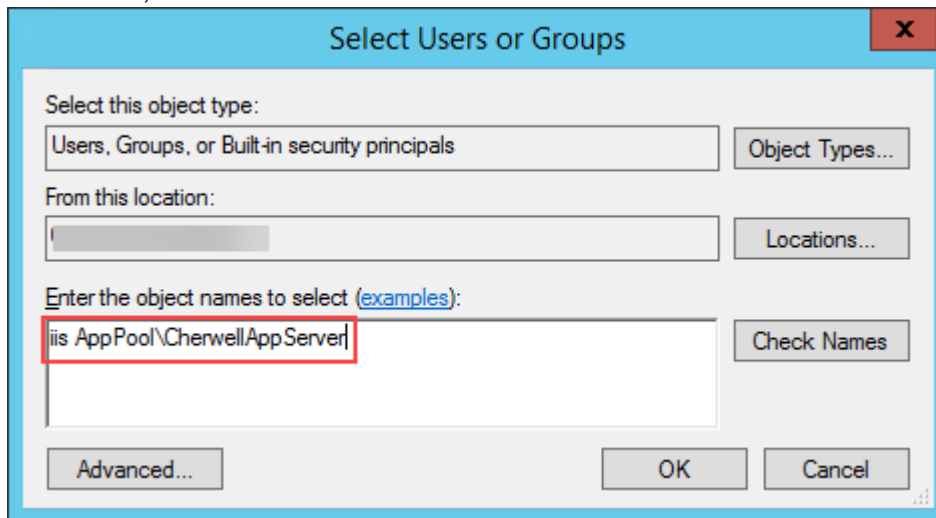
8. Select **OK**.

9. On the Permissions page, select **CherwellAppServer**, and then select the **Allow** check box for all permissions.
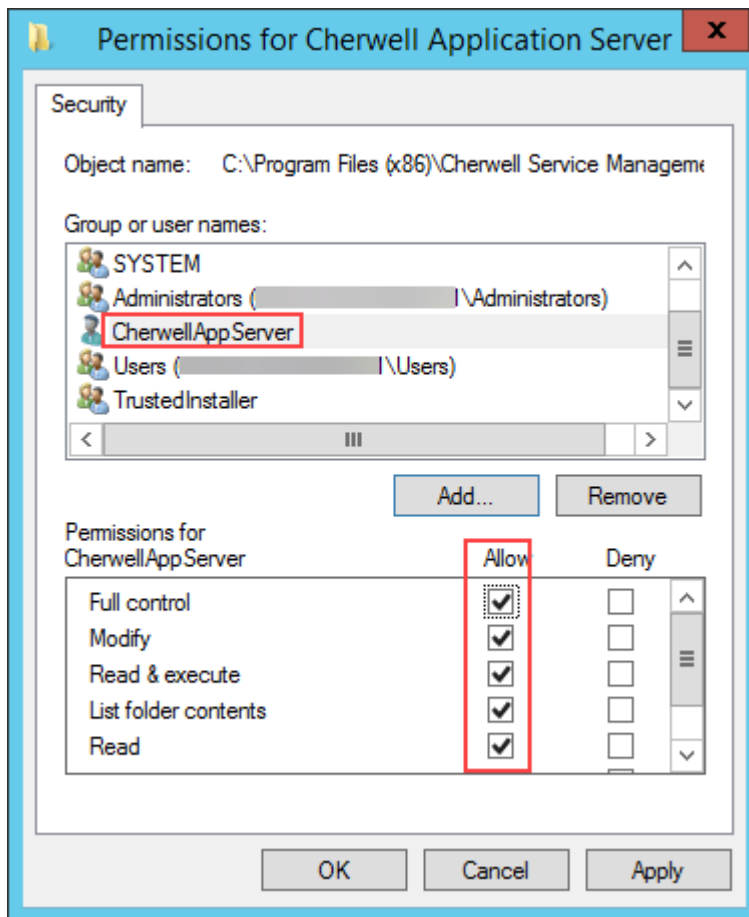
10. Select **OK**.

Verify the Application Server Connection Using a URL

In a browser, navigate to this address:

```
HTTPS://YourServer/CherwellAppServer/Rest.svc
```

Use HTTPS or HTTP in the URL based on your environment's security protocols.

A web page should open that shows *Service*. If this does not happen, contact Cherwell Support.
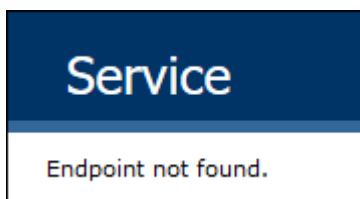
Related concepts

Default Port Numbers

Configure the Application Server

Installing CSM from the Command Line

Use command-line options to silently install CSM Client, server, and web applications. After installation, you can configure CSM servers using the Server Manager or Command-Line Configuration utility.

Each of the following sections contains commands and examples for running the silent installer.

When creating a command, you must use two variables: the directory where CSM will be installed (INSTALLDIR) and all other parameters (PARAMS) in a list. Remember the following rules for commands in CSM:

- Values that include spaces must be wrapped in double quotation marks. Since PARAMS includes multiple parameters, its values always require quotes. INSTALLDIR requires quotes only if any of the directories in the filepath have spaces in their names (example: INSTALLDIR:"C:\Program Files\CSM").
- A final backslash is not required for the INSTALLDIR filepath. If the INSTALLDIR filepath ends with a backslash, it must be escaped (example: INSTALLDIR:"C:\Program Files\CSM\\").
- Parameter values inside of double quotes must be separated by a pipe (|) or a semi-colon (;).
- CSM includes .exe files for CSM Server installation, CSM Web Applications installation, and Cherwell Server Manager installation.
- CSM Client is installed using an .msi file.
- Silent installation of an .exe file can be achieved using either /quiet or /silent switch commands. These can be shortened to /q or /s. The examples in the following sections use /q.

CSM Client Installation

The CSM Client installer uses an .msi file, so the command to launch the CSM Client installer requires a different format than all other CSM installers. In addition to INSTALLDIR, the CSM Client installation command uses INSTALLLEVEL.

Use the following command to install CSM Clients:

```
msiexec /i "Cherwell Client.msi" /qn <Install parameters here>
```

The following example installs the Desktop Client and administrator tools (CSM Administrator, Report Runner, System Upgrade/Restore, and Test LDAP) for all users:

```
msiexec /i "Cherwell Client.msi" /qn INSTALLLEVEL=10
```

Options	Definition	Values
INSTALLDIR	Location/folder in which to install the Client application files.	[ProgramFilesFolder]Cherwell Service Management (default)

INSTALLLEVEL	Install the CSM Desktop Client only or both CSM Desktop and CSM Administrator.	• 1 = Client component only installed. • 10 = Client and Administrator components installed.

CSM Server Installation

During the server installation, the Server Manager and all servers and services are installed. You must select which servers and services to enable by default.

Use the following command to install the Cherwell Server:

```
"Cherwell Server.exe" /q INSTALLDIR="<File path to directory for installation>" PARAMS="<Formatted list of parameters and values>"
```

The following example command is completely silent, which means it avoids opening a wizard and therefore does not install data or configure services. The command installs the Cherwell Application server, the Automation microservice, the Scheduling microservice, and the E-mail and Event Monitoring microservice. It also sets the local Windows account to launch CSM services and does not install the Cherwell Application server as a web application under IIS:

```
"Cherwell Server.exe" /quiet INSTALLDIR="C:\Program Files\CSM" PARAMS="DATABASETYPE=4|SERVERSERVICE=1|BUSINESSPROCSERVICE=1|SCHEDULINGSERVICE=1|EMAILSERVICE=1|USE_SP_ACCOUNT=1|CWSPECIALACCOUNT=LocalSystem|CWAPPSERVERIIS=0|CFGSRVS=0"
```

Options	Definition	Values
INSTALLDIR	Location/folder in which to install the server installation files.	[ProgramFilesFolder]Cherwell Service Management (default)
Database Options **Note:** The Connection Wizard is launched when DATABASETYPE is set to 1, 2, or 3. For a silent install, set DATABASETYPE to 4.		
DATABASETYPE	Select the database components to install.	Cherwell Demo Database = 1 (default)
		Cherwell Starter (empty) Database = 2
		Upgrade an existing database = 3
		Don't load any data = 4

Service Options		
`SERVERSERVICE`	Enable the Application Server.	• 1 = Enable (default) • 0 = Disable
`BUSINESSPROCSERVIC E`	Enable the Automation Process microservice.	• 1 = Enable (default) • 0 = Disable
`SCHEDULINGSERVICE`	Enable the Scheduling microservice.	• 1 = Enable (default) • 0 = Disable
`EMAILSERVICE`	Enable the E-mail and Event Monitoring microservice.	• 1 = Enable (default) • 0 = Disable
Logon Information		
`IS_NET_API_LOGON_U SERNAME`	Cherwell Server account username that will be used to launch the CSM services. Must be in the form Domain/ username.	Blank (default), but information is required. Format: DOMAIN\Username if the server is joined by a domain. Example: Cherwell\Henri.Bryce
`IS_NET_API_LOGON_P ASSWORD`	Cherwell Server account password that will be used to launch the CSM services.	Blank (default), but information is required.
`USE_SP_ACCOUNT`	Use special account (Windows account) to launch the CSM services.	• 1 = True • 0 = False (default)
`CWSPECIALACCOUNT`	Name of special account that will be used to launch the CSM services.	• LocalSystem (default) • LocalService • NetworkService
`CWAPPSERVERIIS`	Install the Application Server as a web application under IIS.	• 2 = True (default) • 0 = False

CFGSRVS	Allow auto-configuration of services including the Application Server and Service Host. For a completely silent install, set to 0. The installation process will complete without service configuration, and the services must be configured after installation. **Note:** If this option is left out or set to 1, the installation attempts to automatically configure the services and displays the Connection wizard if no suitable connection is found.	• 1 = True • 0 = False

CSM Web Applications

Use the following command to install the CSM Web Applications:

```
"Cherwell Browser Apps.exe" /q INSTALLDIR="<File path to directory for installation>" PARAMS="<Formatted list of parameters and values>"
```

The following example does not install the Portal, but it installs Auto-Deploy:

```
"Cherwell Browser Apps.exe" /q INSTALLDIR="C:\Program Files\CSM" PARAMS="CWPORTAL=0|CWAUTODEPLOY=1"
```

Options	Definition	Values
CWPORTAL	Install Cherwell Portal.	• 1 = Install (default) • 0 = Do not install
CWBROWSERCLIENT	Install Cherwell Browser client.	• 1 = Install (default) • 0 = Do not install

`CWAUTODEPLOY`	Install Auto-Deploy.	• 1 = Install (default) • 0 = Do not install
`CWCFGMGR`	Select whether or not to display the Connection wizard during install.	• 1 = Display the Connection wizard during install (default) • 0 = Do not display the Connection wizard during install
`INSTALL_AUTO DEPLOY`	Select whether or not to update the Auto-Deploy configuration. **Note:** If Auto-Deploy is not installed (CWAUTODEPLOY=0), then this option is ignored.	• 2 = Do not run Auto-Deploy configuration **Note:** Before Auto-Deploy is ready for use, you must manually configure Auto-Deploy. • 1 = Run Auto-Deploy configuration (default)
`INSTALLDIR`	Location/folder in which to install the Browser application files.	[ProgramFilesFolder]Cherwell Browser Applications (default)

Related concepts

Server Installation Options

Web Applications Installation Options

Command-Line Configuration (CLC) Options

Related reference

Client Installation Options

Securing Your CSM Environment

When preparing for overall security of your on-premises CSM environment, follow recommendations for individual CSM components, including the database, the Cherwell® Service Host, and Internet Information Services (IIS). Also, adhere to recommendations when to plan testing your CSM environment.

Securing CSM Applications

Security configuration recommendations for on-premise CSM installations are provided for the Cherwell Application Server, CSM Web Applications, and CSM Administrator.

Recommendations for Cherwell Application Server

- Install the Cherwell Application Server with Internet Information Services (IIS) with the Cherwell REST API enabled.
- Configure Secure Sockets Layer (SSL) using a Trusted Agent.
- Change the default password for the CSDAdmin account.
- Configure database security with separate database accounts for the 2-tier connection.

Recommendations for CSM Web Applications

- Configure SSL using a Trusted Agent.
- Use the `/updatebrowserclientsettings/RedirectHttptoHttps` command in the Command-Line Configure utility to set a value of **true**.

Recommendations for CSM Administrator

🖉 **Note:** Recommendations for CSM Administrator apply to both on-premise and SaaS environments.

- Set the number of allowed failed customer login attempts before lockout to five (**Security > Edit security settings > Cherwell Credentials > Lockout customers after 5 failed login attempts**).
- Adhere to Open Web Application Security Project (OWASP) best practices for attachments (**Security > Attachments**) and password complexity (**Security > Cherwell Credentials**).
- Validate Windows security accounts (navigate to **Security > Desktop** and then select **Validate Windows/LDAP credentials on Server**).
- Disable client auto-login (navigate to **Security > Desktop**, and then clear the **Allow users to have system remember last password** option).
- Set URLs for CSM Web Applications to use HTTPS (**Browser Settings > Portal and Browser Client URLs**).
- Disable iFrame embedding (navigate to **Browser Settings** and select **Do not allow browser applications to be embedded within iFrame**).
- Disable detailed error messages (navigate to **Browser Settings** and select **Do not send detailed error information to client**).
- Disable linked attachments (navigate to **Browser Settings** and select **Disable linked attachments in the browser applications**).

- Disable password auto-complete on the login page (navigate to **Browser Settings** and select **Disable password auto-complete on login page**).

Securing the CSM Database

Cherwell® Service Management uses two accounts for database access: an application-level account and an administrator user account. These two accounts are configured when a 2-tier database connection is created to control the level of database access given for the application.

Create the following two accounts before you run the scripts in this procedure:

- CSMAdminUser (administrator account)
- CSMUser (application-level user)

The application and administrator accounts control different aspects of CSM.

By configuring each account separately, CSM uses the appropriate security context for advanced operations that CSM Portal and technician users do not typically perform. These advanced actions usually occur during Blueprint publishes, system restore, and system upgrade. For a multi-tenant environment (multiple databases on a single database server), do not share database accounts if access to these databases is restricted between instances of CSM. Integrated security for connections is not recommended.

> **Note:** When configuring connection options, do not use a single `sa` account for both account values.

To grant the appropriate permissions, run scripts against the target database for the CSMAdminUser and CSMUser accounts.

To grant permissions:

1. On the command line, navigate to the target database.
2. Run the following script to grant permission to create tables and perform DDL operations to an Administrator user named CSMAdminUser.

```
DEFAULT_DATABASE=[master], DEFAULT_LANGUAGE=[us_english], CHECK_EXPIRAT
ION=OFF, CHECK_POLICY=OFF
GO


GRANT VIEW SERVER STATE TO [CSMAdminUser]
GO


CREATE USER [CSMAdminUser] FOR LOGIN [CSMAdminUser] WITH DEFAULT_SCHEMA
=[dbo]
GO
```

```
EXEC sp_addrolemember N'db_owner', N'CSMAdminUser'
GO
```

3. Run the following script to grant permission to access table data to an application-level user named CSMUser.

```
CREATE USER [CSMUser] FOR LOGIN [CSMUser] WITH DEFAULT_SCHEMA=[dbo]
GO


EXEC sp_addrolemember N'db_datareader', N'CSMUser'
GO


EXEC sp_addrolemember N'db_datawriter', N'CSMUser'
GO
```

Related concepts
Using Databases with CSM

Securing the Cherwell Service Host

Assign network service-level security access and permissions on the Cherwell® Service Host to support its microservices Automation Process Service and Scheduling Service.

For back-end processes that run One-Step™ Actions, you should allow only permissions that are required for performing the actions. Granting more advanced permissions is not recommended.
To configure security:

1. Start the Windows Services Manager, and locate the Cherwell Service Host.
2. Right-click the Cherwell Service Host, and then select **Properties**.
3. Select the **Log On** tab.
4. Select the **This account** option, and then select the **Browse** button.
5. In the **Select User** window, type `Network Service` in the **Enter the object name to select** field, and then select **Check Names** to resolve the name.

   > **Note: Network Service** is the recommended account for all Cherwell services. Do not use **Local Service**.

6. Select **OK**.
7. Select **Apply** to save your updates, and then select **OK** to close the **Properties** window.

Related concepts
About the Cherwell Service Host

Securing IIS

Internet Information Services (IIS) uses application pools to coordinate the identity of the website that is running on the server.

For Cherwell® applications, only one application pool is allowed per virtual directory. Application pools cannot be shared across virtual directories.

To confirm your IIS configuration:

1. To verify how an IIS application pool is used for Cherwell applications, open the Windows IIS Manager and view the connection information.

2. To check if a virtual directory has a specific application pool assigned, right-click the virtual directory, select **Manage Application > Advanced Settings**, and view the **Application Pool** value. Close the window.

3. To verify the identity of the application pool, right-click the name of the application pool in the **Connections** pane, and select **Advanced Settings**. If configured, **ApplicationPoolIdentity** is listed as the identity of the application pool. The **ApplicationPoolIdentity** identity is recommended for Cherwell applications running under IIS.

4. To assign a direct permission to the application pool identity, still in the IIS Manager, right-click the site folder, and then navigate to **Edit Permissions > Security > Edit > Add**. Search for the local application pool (example: IIS AppPool*CherwellClient*). Select the **Check Names** button to resolve the name.

5. Use the following information as a reference for assigning security permissions for the CSM Browser Client:
   - Cherwell Application Server
     - Log to file directory: Create, Read, and Write/Modify
     - C:\ProgramData\Trebuchet\Trebuchet.AppServerRecovery.dat: Create, Read, and Write/Modify
     - HKLM\SOFTWARE\Trebuchet\ServerSetup Access: Read
     - General file access: Not applicable
     - Right to act as service: Not applicable
     - Permissions to [Programs]\Cherwell Browser Applications\Portal\dist\Bundles\Portal\css: Not applicable
   - Browser Client
     - Log to file directory: Create, Read, and Write/Modify
     - C:\ProgramData\Trebuchet\Trebuchet.AppServerRecovery.dat: Not applicable
     - HKLM\SOFTWARE\Trebuchet\ServerSetup Access: Read
     - General file access: Not applicable
     - Right to act as service: Not applicable
     - Permissions to [Programs]\Cherwell Browser Applications\Portal\dist\Bundles\Portal\css: Not applicable
   - CSM Portal
     - Log to file directory: Create, Read, and Write/Modify

- C:\ProgramData\Trebuchet\Trebuchet.AppServerRecovery.dat: Not applicable
- HKLM\SOFTWARE\Trebuchet\ServerSetup Access: Read
- General file access: Not applicable
- Right to act as service: Not applicable
- Permissions to [Programs]\Cherwell Browser Applications\Portal\dist\Bundles\Portal\css: Create, Read, and Write/Modify
- Cherwell REST API
  - Log to file directory: Create, Read, and Write/Modify
  - C:\ProgramData\Trebuchet\Trebuchet.AppServerRecovery.dat: Not applicable
  - HKLM\SOFTWARE\Trebuchet\ServerSetup Access: Read
  - General file access: Not applicable
  - Right to act as service: Not applicable
  - Permissions to [Programs]\Cherwell Browser Applications\Portal\dist\Bundles\Portal\css: Not applicable
- Cherwell Service
  - Log to file directory: Create, Read, and Write/Modify
  - C:\ProgramData\Trebuchet\Trebuchet.AppServerRecovery.dat: Not applicable
  - HKLM\SOFTWARE\Trebuchet\ServerSetup Access: Read
  - General file access: Not applicable
  - Right to act as service: Not applicable
  - Permissions to [Programs]\Cherwell Browser Applications\Portal\dist\Bundles\Portal\css: Not applicable
- Cherwell Auto-Deploy
  - Log to file directory: Not applicable
  - C:\ProgramData\Trebuchet\Trebuchet.AppServerRecovery.dat: Not applicable
  - HKLM\SOFTWARE\Trebuchet\ServerSetup Access: Not applicable
  - General file access: Not applicable
  - Right to act as service: Not applicable
  - Permissions to [Programs]\Cherwell Browser Applications\Portal\dist\Bundles\Portal\css: Not applicable

Enable HTTP Strict Transport Security (HSTS)

HSTS helps protect websites against man-in-the-middle attacks by informing a browser that it should contact the website only through HTTPS connections and should automatically convert all attempts to access the site using HTTP to HTTPS requests instead.

On-premise CSM customers need to enable HSTS, but the process is different depending on which version of Internet Information Services (IIS) you have.

Earlier Versions of IIS 10.0 1709

Before IIS 10.0 version 1709, the process to enable HSTS requires one of the two following configurations:

- HTTP Redirect Module + Custom Headers
- URL Rewrite Module

HTTP Redirect Module + Customer Headers

Before IIS 10.0, use the HTTP Redirect Module to configure settings to redirect client requests to a new location. See https://docs.microsoft.com/en-us/iis/configuration/system.webserver/httpredirect/. Use two separate websites, one for HTTP and the other for HTTPS, to avoid an infinite redirect loop.

For more details on this configuration, see **Solution 1: HTTP Redirect Module + Custom Headers** in the Microsoft documentation: https://docs.microsoft.com/en-us/iis/get-started/whats-new-in-iis-10-version-1709/iis-10-version-1709-hsts#challenges-on-enabling-hsts-before-iis-100-version-1709.

URL Rewrite Module

Before IIS 10.0, install the URL Rewrite Module and configure rewrite rules for a single website with both HTTP and HTTPS bindings. See https://docs.microsoft.com/en-us/iis/extensions/url-rewrite-module/using-the-url-rewrite-module. You can specify the HTTP and HTTPS redirection by an inbound rule and you can add the STS header to the HTTPS replies by an outbound rule.

For more details on this configuration, see **Solution 2: URL Rewrite Module** in the Microsoft documentation: https://docs.microsoft.com/en-us/iis/get-started/whats-new-in-iis-10-version-1709/iis-10-version-1709-hsts#challenges-on-enabling-hsts-before-iis-100-version-1709.

IIS 10.0 Version 1709 Native HSTS Support

For IIS 10.0 and later, HSTS is supported natively. You can enable HSTS at site-level by configuring the attributes of the `<hsts>` element under each `<site>` element. See https://docs.microsoft.com/en-us/iis/configuration/system.applicationhost/sites/site/hsts.

For more details on this configuration, see **IIS 10.0 Version 1709 Native HSTS Support** in the Microsoft documentation: https://docs.microsoft.com/en-us/iis/get-started/whats-new-in-iis-10-version-1709/iis-10-version-1709-hsts#iis-100-version-1709-native-hsts-support.

Application Security

CSM application security provides powerful, granular, and set-in layers to secure people, functionality, data, environment, and sharing.

About Security

CSM provides a default security design (complete with Security Groups, Roles, Teams/Workgroups, and system security settings). You can implement the default design (and just add users and customers, assigning them to other default Security Groups, Roles, and Team/Workgroups), edit it, or create a new security design.

Note: Security is configured and managed in CSM Administrator, typically by a system administrator.

Security components include:

- Security Group: A collection of CSM security rights that controls access to CSM functionality and data (Business Objects/fields).
- Role: A user or customer's current function/responsibility in CSM, and controls how data is presented in that person's CSM environment.
- User: A service desk professional who logs in and uses CSM to manage service desk data (example: A technician, manager, designer, system administrator, etc.).
- Team: A collection of CSM users that can share CSM items (such as Dashboards), record ownership, and assignments.
- Customer: An end user, either an internal employee or an external individual, who relies on CSM to initiate/fulfill a Service or Product (example: A person reporting a lost password or requesting a new phone).
- Customer Workgroup: A collection of CSM customers who can share CSM items (such as Dashboards).
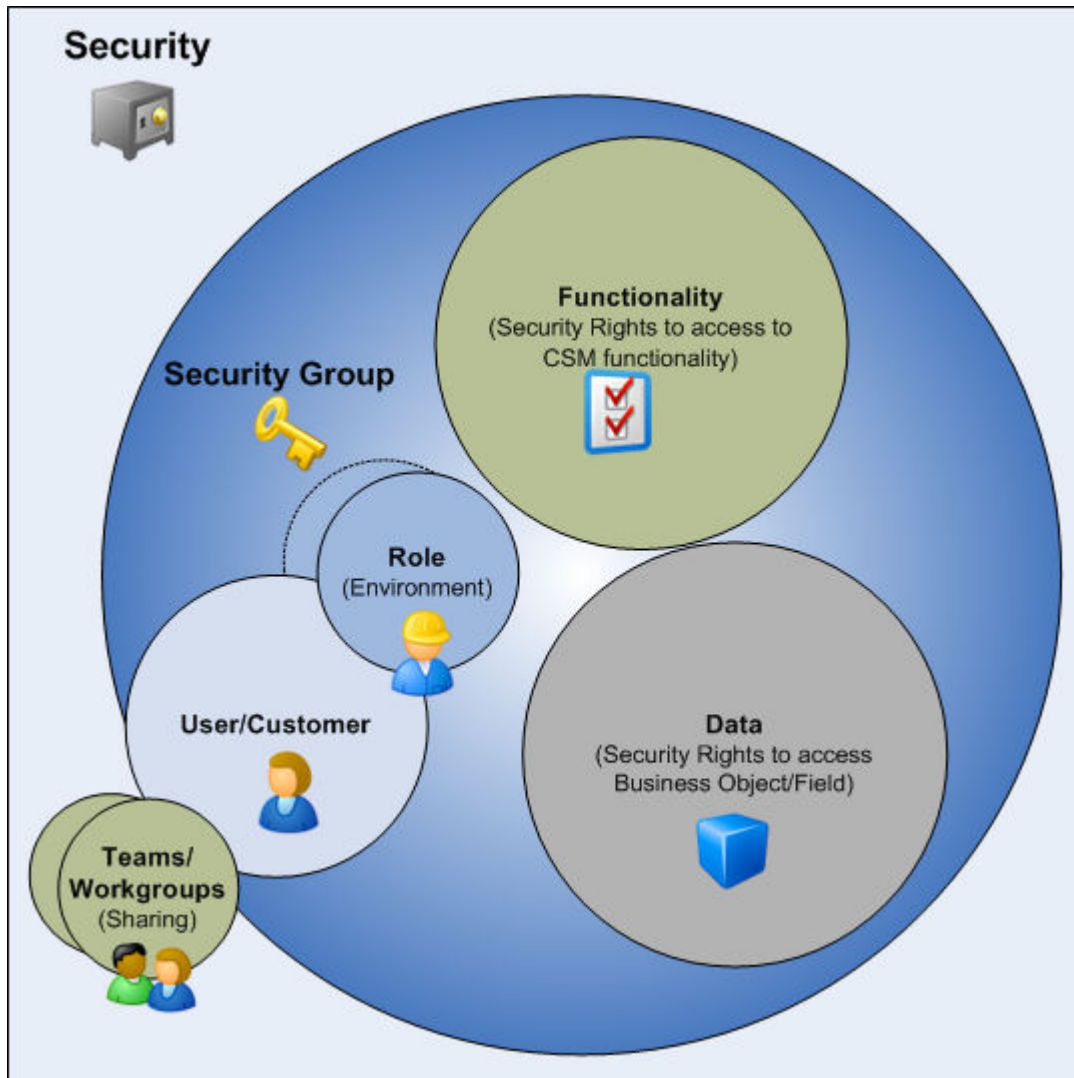
Related concepts

About Security Groups

About Roles

About Users

About Teams and Workgroups

About Customers

Security Rights

Security rights control access to CSM functionality and data.

For example, to create a Dashboard, you must have security rights to access the Dashboard Manager (functionality). To view, add, edit, or delete the Description Field in an Incident record, you must have security rights to access the Incident Business Object and the Description field (data).

For a detailed explanation of each Security right, see Security Rights Reference.

Security rights are set at the Security Group level in CSM Administrator using the Rights and Business Object tabs (**Security > security groups > Edit**.

- Use the **Rights** tab to configure access to functionality; specifically View, Add, Edit, Delete, Allow, Run, and Open rights.
- Use the **Business Objects** tab to configure access to Business Object/Field data; specifically View, Add, Edit, Delete, Limit, Edit in final state, and Change final state. Business Objects rights can be set for different types of Business Object Owners (example: Record Owner, Manager of Owner).

Each Security Group has a defined set of security rights (access to functionality and data). Each user or customer is assigned to one and only one Security Group. The user or customer then inherits the security rights of that Security Group.

Related concepts
Security Rights Reference
About Security Groups
Related tasks
Define Functionality Security Rights (Access to Functionality)
Related information
Define Business Object Rights (Access to Data)

Security Considerations

When designing a security strategy, consider security rights, licenses, users and customers, record ownership, and scope.

Like everything in CSM, access to Security functionality is controlled through security rights (that is, you need security rights to manage security rights). If you cannot View, Add, Edit, or Delete Security functionality, check your security functionality rights in CSM Administrator (**Security > Edit Security Groups > security group > Rights > security group**).

License consumption varies depending on the product, who logs in (user or customer), and which tasks each person performs. Consider your licensing needs when setting up security (especially when considering record ownership rights and reserving licenses).

Users (service desk professionals working in CSM) and customers (end users using the CSM Portal to conduct self-service activities) perform different functions in CSM and, therefore, require different security. Users require access to functionality and data based on their Role as workers in the CSM system. Customers require access to functionality and data based on their Role as initiators of a Service or Product. To facilitate this, CSM provides User *and* Customer Security Groups.

Different record ownership rights can be set to extend/deny access to users and customers, managers, departments, Teams/Workgroups, and Team/Workgroup managers. Be sure to consider the implications of Relationships and setting different rights based on ownership.

Scope is the intended audience for a CSM item (example: the Dashboard is intended for everyone on a specific Team). CSM scopes include User, Role, Team, Global, System, Blueprint, and Site. When creating CSM Items and defining default settings, be sure to consider how scope affects access.

Related concepts
Security Rights
Related information
License Consumption

Differences Between Users and Customers

Users and customers perform different functions in CSM and, therefore, require different security.

A user is a service desk professional who logs in and uses CSM to manage service desk data (example: A technician, manager, designer, system administrator, etc.). A user is assigned to only one Security Group (so they can access specific functionality and data), can log in using one or more Roles (so they can have a personal viewing environment), and can belong to one or more Teams (so they can share CSM items, such as Dashboards).

A customer is an end user, either an internal employee or an external individual, who relies on CSM to initiate/fulfill a Service or Product (example: A person reporting a lost password or requesting a new phone). If configured, a customer can access CSM data and perform self-service activities using the CSM Portal. A customer is assigned to one, and only one, Security Group (so they can access specific functionality and data) can log in using their default Role (so they can have a personal Customer View) and can belong to one or more Workgroups (so they can share CSM items, such as Dashboards).

Often, a user functions as both a user and a customer in CSM. For example, a Service Desk Technician performs user functions but is a customer of the HR Department. If the user is also a customer, they must have a Customer Profile, as well as a User profile.

Users and customers operate very differently in CSM. Below are some of the differences:

Difference	User	Customer
Profile information (personal information, security information, credentials, etc.)	Information is stored in the User Profile in CSM Administrator (**Security > Edit users**. Personal user information is a subset of the User Profile, is configurable, and is stored in the User Info Business Object (called User Info in the Starter database).	Customer information is stored in the Customer Record. The Customer Record is configurable and is stored in the Customer Business Object (called Customer - Internal in the Starter database).
Licensing	Users consume a license when logging in to CSM (Desktop Client or Browser Client).	A customer logging in to CSM through the CSM Portal to access her own records (she is the customer owner) typically does NOT consume one of the concurrent licenses. A customer logging in to CSM through the CSM Portal to access someone else's records (she is NOT the customer owner but has been granted access rights), DOES consume a license.
Security group	Assigned to a User Security Group.	Assigned to a Customer Security Group.

Team	Member of a Team.	Member of a Customer Workgroup.
Ownership	A record usually has a user owner. Record access rights can be extended to the user's manager and department.	A record might have a customer owner. Access rights can be extended to the customer's manager and department.
Web Applications	Accesses the Browser Client through a browser.	Accesses the CSM Portal through a browser.

Related concepts
User and Customer Security Groups
About Teams and Workgroups
Record Ownership
Related information
License Consumption

Record Ownership

Record ownership is an important concept in CSM because it affects security and licensing.

It affects security because ownership controls who has particular rights to a record, and it affects licensing because non-owners typically require a license to edit a record via the CSM Portal. Moreover, it differs depending on whether the record owner is a user or a customer.

The following people can be record owners:

- Primary User: A record is usually owned by a single user.
- Customer: A record might also be owned by a customer if the customer is the requestor (is assigned to the record) and has rights.
- Team: A record might also be owned by a Team it if it is explicitly assigned to the Team.
- Customer Workgroup: A record might also be owned by a Workgroup it if it is explicitly assigned to the Workgroup.

Record ownership rights can be extended to the following people:

- Department Member: Any person assigned to the same department as the record owner. Typically, this is just for a user.
- Manager of owner: Person designated as the manager of the record owner. This is for a user or customer.
- Team/Workgroup Member: Any member of the Team/Workgroup owning the record.
- Team/Workgroup Manager: Person designated as the manager of the Team/Workgroup owning the record.

Set Record Ownership

To set record ownership in a new or existing Blueprint, activate ownership tracking for a Business Object, set the record ownership Holds property, and set the Business Object rights based on the ownership.

1. To open the **Business Object Properties** window:
   a. In the CSM Administrator main window, select the **Blueprints** category, and then select the **Create a New Blueprint** task.

      Note: If working on a saved Blueprint, open the existing Blueprint.

   b. In the Object Manager, select **(New Object)** in the Object tree, and then select the **New Business Object** task from the Structure area.

      Note: If working on an existing Business Object, open the Business Object Editor for that Business Object, and then select the **Bus Ob Properties** button.

2. To open the Business Object Editor:
   a. In the CSM Administrator main window, select the **Blueprints** category, and then select the **Create a New Blueprint** task.

      Note: If working on a saved Blueprint, open the existing Blueprint.

      The Blueprint Editor opens, showing the Object Manager in its main pane. The Object Manager lists the existing Business Objects.

   b. In the Object Manager, select a Business Object in the Object tree, and then select the **Edit Business Object** task in the Structure area (or double-click a Business Object in the Object tree).

      Tip: You can also select the **Edit Business Object** button on the Blueprint Editor Toolbar to open the Business Object Editor.

3. To activate ownership tracking for a Business Object:
   a. Select the **Track owner** check box to track Business Object ownership by user.
   b. Select the **Track team owner** check box to track Business Object ownership by Team.

      CAUTION: Clearing either check box deletes the **Owned by** and **Owned by ID** Fields for the *Track owner* selection, and the **Owned by Team** and **Owned by Team ID** Fields for the *Track team owner* selection. Users are prompted to continue upon clearing the check boxes.

4. Set the Record Ownership Holds property.

      Tip: To simplify your setup, CSM set the ownership property on some standard Fields in your Starter database.

5. Set Business Object rights based on ownership. Business Object rights are set at the Business Object level in a Security Group in CSM Administrator (**Security > Edit security group > User/Customer Security Group > Business Objects > Business Object**. Rights are typically View, Add, Edit, and Delete. Rights can be set for all owners/extended owners, or they can be set differently for record owner, department member, manager of owner, Team/Workgroup member, and Team/Workgroup manager.

Related concepts

Open an Existing Blueprint

Blueprint Editor

Blueprint Editor Toolbar

Related tasks

Create a Blueprint

Record Ownership Holds Property

Record ownership is identified by the Holds property on a Field. The Hold property identifies that a person listed in a Field is the record owner.

The property value tells CSM the type of owner (User, Customer, Team, Workgroup, Department, or Manager). For example, in the Starter database, the **Owner ID Holds** value is set on the **Owner ID** Field and tells CSM that the person listed in that Field is the official user record owner.

Because many ID Fields (example: Owner ID) work in tandem with and are populated by more user friendly Fields (example: Owner ID works with Owner Name), a second Holds property should be set on the exposed Field. In the example above, Owner Name is also set on the **Owned By** Field to tell CSM that April Hawkins is the display name of the official User record owner.

Set an ownership value in the **Holds** drop-down list on the Field's **General** tab.
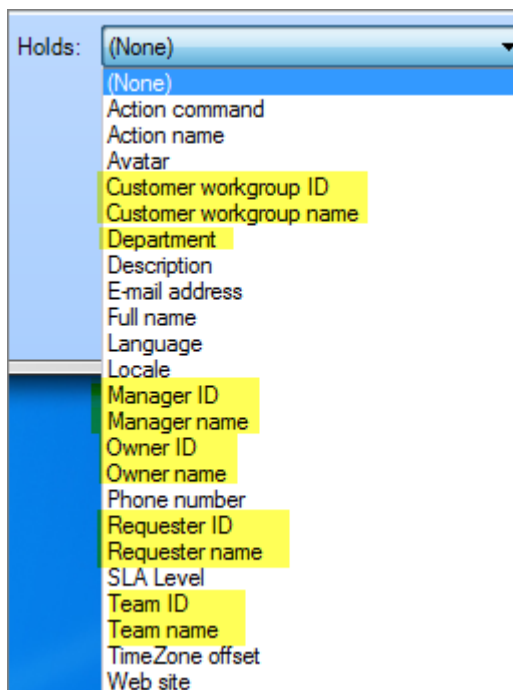
Record Ownership Value Considerations

- Most record ownership values are tied to a record type and are set on the Fields in a Business Object (example: They are set in the Incident Business Object).

- Department and Manager are tied to a person and are set on the Fields in the User Info and Customer Business Objects.

- To simplify your setup, CSM provides the record ownership property on some standard Fields in the Starter database. It is assumed that certain Relationships are based on CSM's User Profile and Customer Record. For example, we assumed that the record owner manager is the manager listed

on the User Profile in CSM Administrator (**Security > Edit users**). Because CSM is highly configurable, your system might vary.

- CSM does not set any Workgroup ownership attributes. They must be configured Workgroup attributes.

Record Ownership Values

CSM uses the following values to identify record owners and extended owners. If the value typically works in tandem with another value, it is listed as well.

Record Owner Values

Holds Value	Description
Owner ID Owner name	Identifies User record owner. **Note:** Typically, the **Owned By ID** and **Owned By** Fields hold the ownership values.
Requester ID Requester name	Identifies Customer record owner. **Note:** Typically, the **Requested By ID** and **Requested By** Fields hold the ownership values.
Team ID Team name	Identifies Team record owner. **Note:** Typically, the **Owned By Team ID** and **Owned By Team** Fields hold the ownership values.
Customer Workgroup ID Customer Workgroup name	Identifies Workgroup record owner. **Note:** Typically, the **Owned By Workgroup ID** and **Owned By Workgroup** Fields hold the ownership values. Currently, these Fields are not part of the Starter database, but you can add them manually,

Extended Record Owner

Holds Value	Description
Department	Identifies any person assigned to the same department as the record owner. **Note:** Typically, the **Department** Field holds the ownership value (example: in User Info and Customer-Internal). Unlike the other specialized Fields, the **Department** Field holds the name of the department, not an ID identifying the department.
Manager ID Manager name	Identifies the person designated as the manager of the record owner. Remember, a record owner can be a user and/or customer, and a Team and/or Workgroup. **Note:** Typically, the **Manager ID** and **Manager** Fields hold the ownership value (example: in User Info and Customer-Internal).

Record Ownership Values Matrices

The following tables list the record ownership values by owner type.

User Record Owner

Record Owner	Description	Holds Value	Example Business Obect.Fields
Record owner (User)	Identifies the User who owns the record.	Owner name Owner ID	Incident.Owned By Incident.Owner ID
Manager	Identifies the manager of the User who owns the record.	Manager name Manager ID	User Info.Manager User Info.Manager ID
Department	Identifies the User owner's department.	Department	User Info.Department Customer-Internal.Department

Team Owner Record

Record Owner	Description	Holds Value	Example Business Object.Fields
Team owner	Identifies the Team who owns the record.	Team name Team ID	Incident.Owned By Team Incident.Owner Team ID
Team owner manager	Identifies the manager (or managers) of the Team who owns the record.	Not applicable. Team owner manager is assumed to be the manager (or managers) selected on the Team Profile.	Not applicable.

Custom Record Owner

Record Owner	Description	Holds Value	Example Business Object.Fields
Record owner (Customer/ requester)	Identifies the Customer who owns the record.	Requester name Requester ID	Change Request.Requested By Change Request.Requested By ID
Manager	Identifies the manager of the Customer who owns the record.	Manager name Manager ID	Customer-Internal.Manager Customer-Internal.Manager ID
Department	Identifies the Customer owner's department.	Department	Customer-Internal.Department Field

Workgroup Record Owner

Record Owner	Description	Holds Value	Example Business Object.Fields
Workgroup owner	Identifies the Customer Workgroup who owns the record.	Customer Workgroup name Customer Workgroup ID	Change Request.Owned By Workgroup Change Request.Owner Workgroup ID
Workgroup owner manager	Identifies the manager (or managers) of the Customer Workgroup who owns the record.	Not applicable. Workgroup owner manager is assumed to be the manager (or managers) selected on the Workgroup Profile.	Not applicable.

Related tasks
Set a Record Ownership Holds Property Example

Set a Record Ownership Holds Property

Set the record ownership Holds property. To simplify your setup, CSM set the ownership property on some standard Fields in your Starter database.

1. Open the Business Object that contains the Field you want to tag as an ownership Field:
   a. In a Blueprint, select the Business Object.
   b. Select **Edit business object**.
2. Set the property on the **Ownership** field:
   a. Double-click the icon in front of the Field.
   b. Select the **General** page.
   c. In the **Holds** drop-down list, select a record ownership value.
   d. Select **OK**.

Set a Record Ownership Holds Property Example

In this example, you want a Customer Workgroup to have ownership rights to a Change Request. You need to add the Workgroup ID and Workgroup Name attributes to a Field on your Change Request form.

Because the Change Request Business Object does not have any appropriate Fields to house the attributes, you need to add two new Fields (**Workgroup ID** and **Owned By Workgroup**) to the Form.

To set a record ownership Holds property:

1. Open the Object Manager.
2. Select **Change Request**, and then select **Edit business object**.
3. Add a Field named **Owned By Workgroup**:
   a. Name: Owned By Workgroup
   b. Type: Text
   c. Length (of text): 30
4. Define Field properties:
   a. Select the **Field Properties** button.
   b. On the **General** page, in the **Holds** drop-down list, select the **Customer Workgroup name** ownership attribute. This selection tells CSM that the Workgroup in this Field is a record owner.
   c. On the the **Validation/Auto-populate** page, select the **Other validation types** check box to expand the section.
   d. Select the **Valid Team or Workgroup** radio button, and then select **All customer workgroups**. This selection tells the Field to list all the valid Customer Workgroups.
   e. Define additional Field properties as necessary: Full-Text Search, default values, etc.
   f. Select **OK**.
5. Add a Field named **Owner Workgroup ID**:
   a. Name: Owner Workgroup ID
   b. Type: Text
   c. Length (of text): 42
6. Define Field properties:
   a. Select the **Field Properties** button.
   b. On the **General** page, in the **Holds** drop-down list, select the **Customer Workgroup ID ownership attribute**. This selection tells CSM that the Workgroup in this Field is a record owner.
   c. On the **Validation/Auto-populate** page, select the **Auto-populate** check box to expand the section.
   d. In the **Populate when there is a change in table: [ITEM] field** drop-down list, select **Owned By Workgroup**.
   e. Select the **Customer workgroup ID** radio button.
   f. Define additional Field properties as necessary: Full-Text Search, default values, etc.
   g. Select **OK**.

7. Add the **Owned By Workgroup** field to the Form.

8. Publish the Blueprint to commit the changes (**File > Publish Blueprint**).

9. In the Customer Security Group, set the different ownership rights for the Change Request Business Object.

Related concepts

Record Ownership Holds Property

Publish a Blueprint

Set Different Business Object Rights Based on Ownership

Scope

Scope is the intended audience for a CSM Item (example: A Dashboard is intended for everyone on a specific Team).

CSM uses the following Out of the Box (OOTB) scopes:

- **User:** Audience is a specific User/Customer (example: User can access his Dashboards).
- **Role:** Audience is every member assigned to a Role (example: Every User/Customer logging in through the Role can access that Role's Dashboards).
- **Team:** Audience is every User on a Team, or every Customer in a Workgroup (example: Every User/Customer assigned to a specific Team/Workgroup can access that Team/Workgroup's Dashboards).
- **Global:** Audience is all Users/Customers who can log in to CSM (example: All CSM Users/Customers can access Global Dashboards).
- **System:** Audience is the CSM system itself. Any User/Customer who can log in to CSM can use a system item; however, editing is available only in CSM Administrator, typically by a system administrator. A Document Repository is an example of a System item.
- **Blueprint:** Audience is any User/Customer who can log in to CSM; however, use is typically automated and editing is available only in a Blueprint, typically by a system administrator. A One-Step™ Action that runs when a User clicks a button on a form is an example of an item in a Blueprint scope.
- **Site:** Audience is a Portal Customer (example: Dashboard is available only on a specific Portal Site). Site-only items must be created within the Site Manager (Site Manager>Menu).

  Note: If you want items to be widely available, do not limit them to a Site scope; rather store the items with the other CSM items in their perspective Managers.

  Note: CSM Browser Clients support limited functionality so some CSM items and operations are not applicable in the Portal and/or Browser Client.

When setting security rights for CSM items for security groups (example: Administrator, Service Desk Technician, Manager, etc.), access to functionality can be limited by scope. For example, an Anonymous Browser (not logged-in Portal Customer) might not be able to see a Calendar that a logged-in Customer has access to.

Note: When creating CSM Items and defining default settings, be sure to consider how scope affects access.

Scopes are used by most CSM items (Calendars, Dashboards, Attachments, One-Step Actions, etc.) to apply a range of use. As a result, most CSM Managers organize their items at the root level in the Manager tree by scope.

OOTB Security Design

CSM provides an OOTB security design to get new systems started. This design has all the Security Groups, Roles, and Teams/Workgroups to successfully access CSM features and CSM data. We recommend implementing this OOTB design and adding Users and Customers by creating User and Customer Profiles. Later, edit the security design or create a new security design to meet specific organizational needs.

> **Note:** Use the User/Customer Worksheet to determine to which Security Group and Teams/Workgroups each User/Customer is assigned.

Below is a high-level summary of the OOTB security design. For a detailed design spreadsheet, refer to the CSM OOTB Security Design Spreadsheet (posted to our Support Portal).

Security Groups					
	Administrator	**Service Desk Manager**	**Service Desk Level 1, 2, or 3**	**Portal Workgroup Manager**	**Portal Customer**
Roles	Service Desk Technician Service Desk Manager	Service Desk Manager	Portal End-User	Portal End-User	Portal End-User
Typical Rights	• Viewer: Access to data (General Customer, Executives, etc.). • Service desk: Access to record logging. • Design: Access to design functionality (example: Can create, edit, or delete Dashboards). • Administrator: Access to administrative functions and tools (example: Security and settings).				
Functionality					
View, Add, Edit, Delete, Allow, Run, Open	Full	Most service desk, some design, some administrator.	Some service desk, limited design, no administrator.	Limited service desk, no design, no administrator.	Very limited service desk, no design, no administrator.
Data					
View, Add, Edit, Delete, Allow, Run, Open	Full	Most	Some	Limited	Very limited

Security Scenario

Below is an example security scenario. Remember that CSM is highly configurable, so individual Users/Customers, Security Groups, Roles, and Teams/Workgroups will vary.

Andrew, Gina, Sawyer, Tracy, and John work at the River T Corp. organization:

- **Andrew is a System Administrator** and is assigned to the Admin User Security Group. As a member of this group, Andrew has security rights to access all data and functionality in the system. This means Andrew has Allow, Run, View, Add, Edit, and Delete rights for all CSM Administrator functionality (security, Blueprints, e-mail setup, etc.), CSM functionality (Dashboards, One-Step Actions, etc.), and Business Object data (Incidents, Problems, etc.). In short, Andrew is a *superuser* and has rights to do just about anything in CSM. Because Service Desk and Service Desk Manager are legal Roles for the Admin Security Group, Andrew can log in using either of those Roles, and therefore has access to different environments (Dashboards, Forms, etc.).

  Andrew is also a member of two User Teams (2nd Level Support and Knowledge Management), and can therefore share CSM Items (example: Dashboards), support processes (Queues and Knowledge Article publishing/approvals), and record ownership (if configured) with the other members of those Teams. Andrew can use either the Desktop Client to access data or the Browser Client to log in via his web browser.

  Note: Andrew can also function as a Customer to other parts of the organization (example: HR). As a Customer, Andrew is a member of the Portal Customer Security Group and the Information Technology Customer Workgroup. See below for more details about Customers.

- **Gina is the Service Desk Manager** and is assigned to the Service Desk Manager User Security Group. As a member of this Security Group, Gina has security rights to Allow, View, Add, Edit, and Delete most data in the system (Incidents, Problems, etc.) but has limited security rights to functionality (example: Gina can View, Add, Edit, and Delete Team and User Dashboards but cannot edit system security). Because Service Desk Manager is the only legal Role for the Service Desk Manager Security Group, Gina can log in using only that Role. Her default environment (Dashboards, Forms, etc.) is appropriate for her managerial Role.

  Gina is also a member of two User Teams (CAB and IT Management) and can therefore share CSM Items (example: Dashboards), support processes (example: Queues), and record ownership (if configured) with the other members of that Team. Gina can use either the Desktop Client to access data or the Browser Client to log in via her web browser.

  Note: Gina can also function as a Customer to other parts of the organization (example: HR). As a Customer, Gina is a member of the Portal Workgroup Manager Security Group and the Information Technology Customer Workgroup. See below for more details about Customers.

- **Sawyer is a Service Desk Worker** who reports to Gina and is assigned to the Service Desk User Security Group. As a member of this Security Group, Sawyer has limited security rights to both data and functionality. For example, Sawyer can View but cannot Add, Edit, or Delete Team Dashboards;

Sawyer can, however, View, Add, Edit, and Delete User Dashboards. Because Service Desk is the only legal Role for the Service Desk Security Group, Sawyer can log in using only that Role. His default environment (Dashboards, Forms, etc.) is appropriate for his troubleshooting Role.

Sawyer is also a member of the 1st Level Support User Team and can therefore share CSM Items (example: Dashboards), support processes (example: Queues), and record ownership (if configured) with other members of that Team. Sawyer can use either the Desktop Client to access data or the Browser Client to log in via his web browser.

> **Note:** Sawyer can also function as a Customer to other parts of the organization (example: HR). As a Customer, Sawyer is a member of the Portal Customer Security Group and the Information Technology Customer Workgroup. See below for more details about Customers.

- **Tracy is a Shipping Specialist and a Customer**, meaning she is an employee but not a licensed CSM User. Tracy is a Customer who uses the CSM Customer Portal to find company information and log Incidents for a service or product (example: She can log an Incident that her printer is not working). Tracy logs in to the Customer Portal using her default assigned Portal Customer Security Group, which has very limited security rights. Tracy can view and edit her own records (example: Incidents) but has *very* limited access to functionality.

  Tracy is a member of the Shipping Customer Workgroup and can therefore share CSM Items and record ownership (if configured) with other members of that Workgroup.

- **John is the Production Manager and a Customer Manager**, meaning he is an employee but not a licensed CSM User. John is Tracy's manager and also a Customer. John can log in to the Customer Portal to log Incidents using his default assigned Portal Workgroup Manager Security Group, which has very limited security rights. Like most Customers, John can view and edit his own records (example: Incidents) but has *very* little access to functionality; however, unlike Tracy, John is a manager, so he has extended rights to view and edit Tracy's records, as well.

  John is also a member of the Shipping Customer Workgroup and can therefore share CSM Items and record ownership (if configured) with other members of that Workgroup.

The following table provides a nice visual to see how the layers trickle down the security rights.

Person/ Security Needs	Security Group	Functionality Rights	Business Object Rights	Roles	Team/Workgroup
Andrew System Administrator	Admin	Full security rights for all. Example: Allow, Run, View, Add, Edit, and Delete for all CSM Administrator functionality (security, Blueprints, e-mail setup, etc.) and all Cherwell Service Management functions (Calendars, Dashboards, One-Step Actions, etc.).	Full security rights for all. Example: View, Add, Edit, and Delete Incident.	Service Desk Service Desk Manager	Teams: • 2nd Level Support Knowledge Management
Gina Service Desk Manager	Service Desk Supervisor	No security rights for system administrator functionality, nearly full security rights for CSM functionality. Example: View, Add, Edit, and Delete Team Dashboards but does not have security rights to access system security.	Full security rights for all. Example: View, Add, Edit, and Delete Incidents.	Service Desk Manager	Teams: • CAB • IT Management
Sawyer Service Desk worker	Service Desk	No security rights for system administrator functionality, limited security rights for CSM functionality. Example: View Team Dashboards but cannot Add, Edit, or Delete. View, Add, Edit, and Delete User Dashboards.	Limited security rights for some. Example: View and Add Incidents but cannot Edit or Delete.	Service Desk	Team: • 1st Level Support

Person/ Security Needs	Security Group	Functionality Rights	Business Object Rights	Roles	Team/Workgroup
Tracy Customer (employee but not a licensed Cherwell User; she logs service requests as a Customer)	Portal Customer	No security rights for system administrator functionality, very limited security rights for CSM functionality. Example: View Dashboards but cannot Add, Edit, or Delete.	Limited security rights to most. Example: View and Edit her own Incidents but cannot Delete.	Portal End-User	Workgroup: • Shipping
John Customer Manager (employee but not a licensed Cherwell User; he logs service requests as a Customer)	Portal Workgroup Manager	No security rights for system administrator functionality, very limited security rights for CSM functionality. Example: View Team Dashboards but cannot Add, Edit, or Delete.	Limited security rights to most. Example: View and Edit his own Incidents, as well as Tracy's Incidents.	Portal End-User	Workgroup: • Shipping

About Security Groups

A Security Group is a collection of CSM security rights that controls access to CSM functionality and data (Business Objects/fields).

You can use Security Groups to implement different levels of security. Each user or customer is assigned to only one Security Group. The user or customer then inherits the security rights of that Security Group, as well as access to the Roles assigned to the Security Group.

CSM provides several Security Groups. The following are examples of Security Groups:

- **Administrator Security Group:** Might have full rights to all CSM functionality and data (view, add, edit, and delete).
- **Service Desk Manager:** Might have limited rights to CSM functionality and data (view, add, edit, but not delete).
- **Service Desk Worker:** Might have very limited to limited rights to CSM functionality and data (view or edit only) depending upon Service Desk level (not required).
- **Customer (via the Customer Portal):** Might have no rights to CSM functionality and limited rights (view only) to CSM data.

> **Note:** To accommodate the differences between Users and Customers, CSM provides two kinds of Security Groups: User and Customer Security Groups.

Security Group properties include:

- **Info:** Name and description
- **Rights:** Security rights to access CSM functionality
- **Business Objects:** Security rights to access CSM data (example: Business Objects/Fields)
- **File Attachments:** Attachment security rights (example: Import/link and global overrides)
- **Roles:** Roles assigned to the Security Group
- **Users:** Users assigned to the Security Group

> **Note:** The Users tab only displays for User Security Groups. Customers are assigned as part of their Customer Profile, and only if they require Portal login credentials.

Related concepts
Differences Between Users and Customers
User and Customer Security Groups
OOTB Security Groups
Create a Security Group
Users Security Rights

OOTB Security Groups

CSM provides the following OOTB Security Groups:

- **Admin:** Used for CSM System Administrators. Typically, these Users can delete groups of records and administer the system.
- **Anonymous Browser:** Used for CSM Users/Customers who need to access CSM Browser and Mobile Applications without logging in.
- **IT Service Desk Level 1:** Used for CSM Service Desk Technicians. Typically, these Users can add/edit/delete items in their User Folders but cannot modify records in their final state, delete records, or administer the system.
- **IT Service Desk Level 2 & 3:** Used for CSM Service Desk Technicians. Typically, these Users can add/edit/delete items in their User Folders but cannot modify records in their final state, delete records, or administer the system.
- **IT Service Desk Manager:** Used for CSM Service Desk Managers. Typically, these Cherwell Users can add/edit/delete items in their Team's Folder and in their User Folders but cannot modify records in their final state, delete groups of records, or administer the system.
- **Portal Customer:** Used for Customers accessing CSM via the Portal. Typically, these Customers have rights to view and edit their own records.
- **Portal Workgroup Manager:** Used for Customers accessing CSM via the Portal who manage teams in their organizations. Typically, these Customers have rights to view and edit their own records, as well as the ability to view and edit their Workgroup members' records.

Use these OOTB Security Groups as-is, edit them, or create new Security Groups using the Security Group Manager in CSM Administrator.

User and Customer Security Groups

Users (Service Desk professionals working in CSM) and Customers (End-Users using the CSM Portal to conduct self-service activities) perform different functions in CSM and, therefore, require different security. Users require access to functionality and data based on their Role as workers in the CSM system. Customers require access to functionality and data based on their Role as initiators of a Service or Product. To facilitate this, CSM provides User *and* Customer Security Groups.
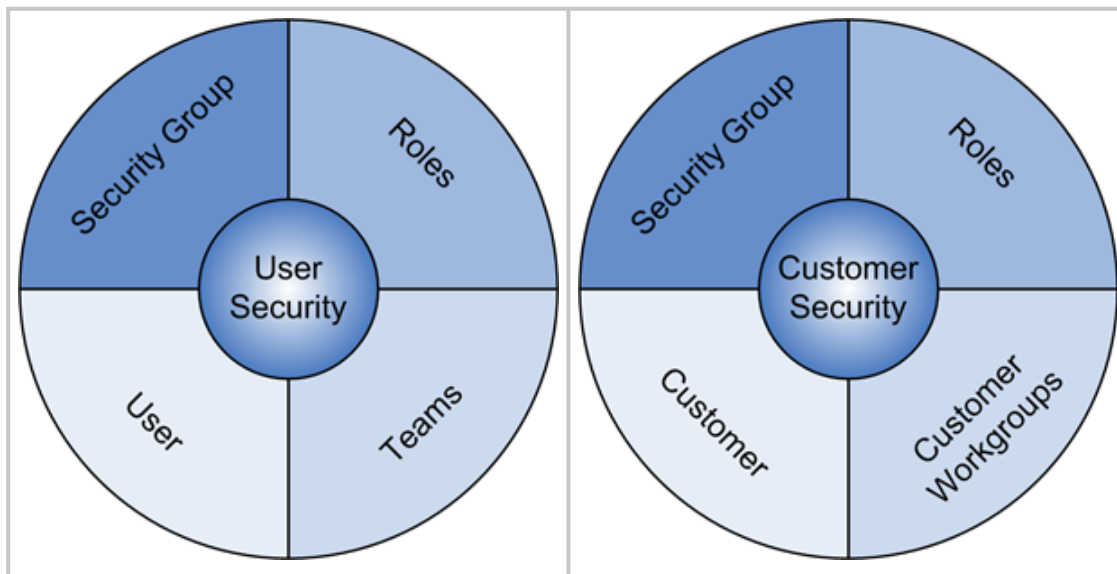
Note: CSM provides several OOTB Security Groups, both User (Admin, IT Service Desk, IT Service Desk Manager) and Customer (Portal Customer and Manager). You can use these OOTB Security Groups as-is, edit them, or create your own using the Security Group Manager.

When creating a Security Group (CSM Administrator>Security>Edit Security Groups), select one of the following:

- New Cherwell User Security Group.
- New Customer Security Group.

User Security Groups have a Users tab to assign Users to the Security Group. Customer Security Groups do not have a Users tab.

A Customer is assigned to a Customer Security Group when you create Customer login credentials (CSM>Customer>Portal Settings>Current Customer Credentials or Batch Customer Credentials).

Note: For more information about the differences between Users and Customers, refer to Differences Between Users and Customers in the Security documentation.

Anonymous Security Group

The Anonymous Security Group (OOTB: *Anonymous Browser*) is required for CSM Web Applications to read basic setup information from the system. The Anonymous Security Group can also be configured to allow Users/Customers in the group to view (or not view) the CSM Portal and a variety of items on the CSM Portal, including Business Objects, Form Controls, Dashboards, Widgets, and Actions.

OOTB Anonymous Security Group

The CSM Starter Database provides an OOTB Security Group named *Anonymous Browser*.

Initial Configuration for Anonymous Access

The following initial configurations must be set for the Anonymous features to work:

- **Security Settings**: Configure Anonymous Login Settings for CSM Web Applications. This is required for CSM Web Applications to read basic setup information from the system.
- **Site Settings**: Configure the Site to Allow Anonymous Access.

Enable Searching Rights for Anonymous access

Users in the Anonymous Security Group can be enabled for specific Searching Rights in the CSM Portal.

- Enable Anonymous Searching Rights

Enable specific Business Objects for Anonymous access

Users in the Anonymous Security Group can be enabled to view specific Business Objects in the CSM Portal. Any Business Objects associated with Form Controls, Dashboards, Widgets, and Actions enabled for Anonymous access will also need to be enabled for Anonymous access.

- Enable Anonymous View of a Specific Business Object
    - Examples
        - Knowledge Articles
        - Service Catalog
    - Anonymous Users can execute a direct link (also known as deep link) to Business Objects that have been configured for anonymous access.

Enable a Dashboard for Anonymous View

Users in the Anonymous Security Group can be enabled to view specific Dashboards in the CSM Portal. When not configured, the Anonymous User is prompted to login to view the Dashboard.

Note: The configured Startup Dashboard is automatically visible to Anonymous Users regardless of the configured setting.

- Enable Anonymous View of a Dashboard.
- Anonymous Users can execute a direct link (also known as deep link) to Dashboards that have been configured for Anonymous view.
- If a Form or Dashboard is configured to be visible to Anonymous Users, each control on the Form or Dashboard is also enabled to be visible to Anonymous Users. Anonymous Users have view access only. If an Anonymous User selects a control to execute an action, they are prompted to login. After successful login, the action runs.

Note: You can add a Button or Link with a **Portal Login** Command to a CSM Portal Form or Dashboard or a **Portal Login** Command to the CSM Portal Menu. The **Portal Login** Command immediately prompts an Anonymous User with the Login modal. See Add a Portal Login Command to a Customer Portal Dashboard, Menu, or Form.

Enable the Service Catalog for Anonymous Access

Users in the Anonymous Security Group can be enabled to view the Service Catalog in the CSM Portal in a variety of ways. See Enable Anonymous Access of the Service Catalog for specific information.

Restrict a Specific Form Control or Widget from Anonymous View

Use the ViewAnonymous() System Function to restrict Anonymous User visibility of a specific Form Control or Widget by setting the Value to *false* for that control. If the Value is set to *False*, the control is not visible to Anonymous Users.

Note: If a Form or Dashboard is configured to be visible to Anonymous Users, each control on the Form or Dashboard is also enabled to be visible to Anonymous Users.

The *ViewAnonymous()* System Function is a visibility expression for an item on a Form or Dashboard. It can be set as a Boolean Property wherever a System Function can be accessed (e.g., One-Step Action, Expression, etc.).

Limit Anonymous Access to Records

Anonymous Users can be limited in their access to records. When enabling Anonymous view of a specific Business Object, select **Limit records based on criteria** and **Browse** to configure a custom query to limit the records available to Anonymous Users.

Related concepts
Configure Anonymous Login Settings for CSM Web Applications
Enable Anonymous Searching Rights
Enable Anonymous View of a Specific Business Object
Enable Anonymous View of a Dashboard
Restrict Anonymous User Visibility for a Form Control
Restrict Anonymous User Visibility for a Dashboard Widget
Related tasks

Configure the CSM Portal Site to Allow Anonymous Access
Enable Anonymous View of the Service Catalog

Enable Anonymous View of a Specific Business Object

The CSM Portal can be configured to allow Anonymous Users to view specific Business Objects and associated fields. Any Business Objects associated with Form Controls, Dashboards, Widgets, and Actions enabled for Anonymous access will also need to be enabled for Anonymous access.

Note: Anonymous access requires some initial configuration. See Anonymous Security Group for specific information.

To enable anonymous view of a specific Business Object:

1. In CSM Administrator, select **Security > Edit security groups**.
2. In the **Group** drop-down list, select the Anonymous Security Group (OOTB: *Anonymous Browser*).
3. Select the **Business Objects** tab.
4. In the **Business Object** drop-down list, select the specific Business Object (Example: Knowledge Articles) you want to allow Anonymous Users to view.
5. Select the **View** check box for the Business Object and all associated fields you want the Anonymous User to be able to view. You must also grant **View** permissions to any Business Objects associated with the selected Business Object. For example, if the Knowledge Articles Business Object is associated with the *Journal - Comment* Business Object, you would additionally provide View access to *Journal - Comment*).
6. *Optional*: Select **Limit records based on criteria** and **Browse** to configure a custom query to limit the records available to Anonymous Users.
7. Select **Save**.

Note: Anonymous users can only *view* the selected Business Object(s). Login is required for Users who want to interact with or edit records in the Portal.

Related concepts

Anonymous Security Group

Configure Anonymous Login Settings for CSM Web Applications

Enable Anonymous Searching Rights

Enable Anonymous View of a Dashboard

Restrict Anonymous User Visibility for a Form Control

Restrict Anonymous User Visibility for a Dashboard Widget

Related tasks

Configure the CSM Portal Site to Allow Anonymous Access

Enable Anonymous View of the Service Catalog

Example: Enable Anonymous View of Knowledge Articles

The CSM Portal can be configured to allow Anonymous Users to view knowledge articles without having to log in to the CSM Portal.

Note: This is only one example of how Anonymous Security Group Users can be granted view access to a Business Object in the Portal. The specific Business Object used in this example may appear differently or not at all in your unique database. Click here for more generic instructions.

To enable anonymous view of knowledge articles:

1. In CSM Administrator, select **Security > Edit security groups**.
2. In the **Group** drop-down list, select the Anonymous Security Group (OOTB: **Anonymous Browser**).
3. Select the **Business Objects** tab.
4. In the **Business Object** drop-down list, select **Knowledge Article**.
5. Select the **View** check box for Knowledge Article and all associated fields you want the anonymous user to be able to view.
6. In the **Business Object** drop-down list, select **Journal**.
7. Select the **View** check box for Journal and all associated fields you want the anonymous user to be able to view.
8. In the **Business Object** drop-down list, select **Journal - Comment**.
9. Select the **View** check box for Journal - Comment and all associated fields you want the anonymous user to be able to view.
10. Select **Save**.

Note: Anonymous Users can only *view* the knowledge articles. Users who want to interact with or edit records must log in.

Enable Anonymous Searching Rights

The CSM Portal can be configured to allow Anonymous Users to run searches that reference fields to which the User doesn't have rights.

Note: Anonymous access requires some initial configuration. See Anonymous Security Group for specific information.

To enable anonymous searching rights:

1. In CSM Administrator, select **Security > Edit security groups**.
2. In the **Group** drop-down list, select the Anonymous Security Group (OOTB: *Anonymous Browser*).
3. Select the **Rights** tab.
4. In the **Category** drop-down list, select **Searches**.
5. Select the applicable option and select the **Allow** check box. Specific options are described in the following table:

Option	Description	Example
Can run searches that reference fields to which the user doesn't have rights.	If you select the **Allow** check box, the Anonymous User can run searches that reference fields to which the User doesn't have rights.	If the User has been enabled to view the Knowledge Articles Business Object and a Knowledge Article has associated *Journal - Comments*, but the user does not have View access for *Journal - Comment*, the user could still perform the search and view the Knowledge Article.
Perform Global Searches?	If you select the **Run** check box, applicable Saved Searches can run for the Anonymous User. Enable **Run** if appropriate for the scope of the Saved Search.	
Perform Role Searches?	If you select the **Run** check box, applicable Saved Searches can run for the Anonymous User. Enable **Run** if appropriate for the scope of the Saved Search.	
Perform Site Searches?	If you select the **Run** check box, applicable Saved Searches can run for the Anonymous User. Enable **Run** if appropriate for the scope of the Saved Search.	

Option	Description	Example
Perform Team Searches?	If you select the **Run** check box, applicable Saved Searches can run for the Anonymous User. Enable **Run** if appropriate for the scope of the Saved Search.	
Perform User Searches?	If you select the **Run** check box, applicable Saved Searches can run for the Anonymous User. Enable **Run** if appropriate for the scope of the Saved Search.	

6. Select **Save**.

Related concepts

Anonymous Security Group

Configure Anonymous Login Settings for CSM Web Applications

Enable Anonymous View of a Specific Business Object

Enable Anonymous View of a Dashboard

Restrict Anonymous User Visibility for a Form Control

Restrict Anonymous User Visibility for a Dashboard Widget

Related tasks

Configure the CSM Portal Site to Allow Anonymous Access

Enable Anonymous View of the Service Catalog

Managing Security Groups

When managing Security Groups, you can define business object rights, assign roles and users, create new Groups, edit existing Groups, and more.

Security Groups are managed using the Security Group Manager.
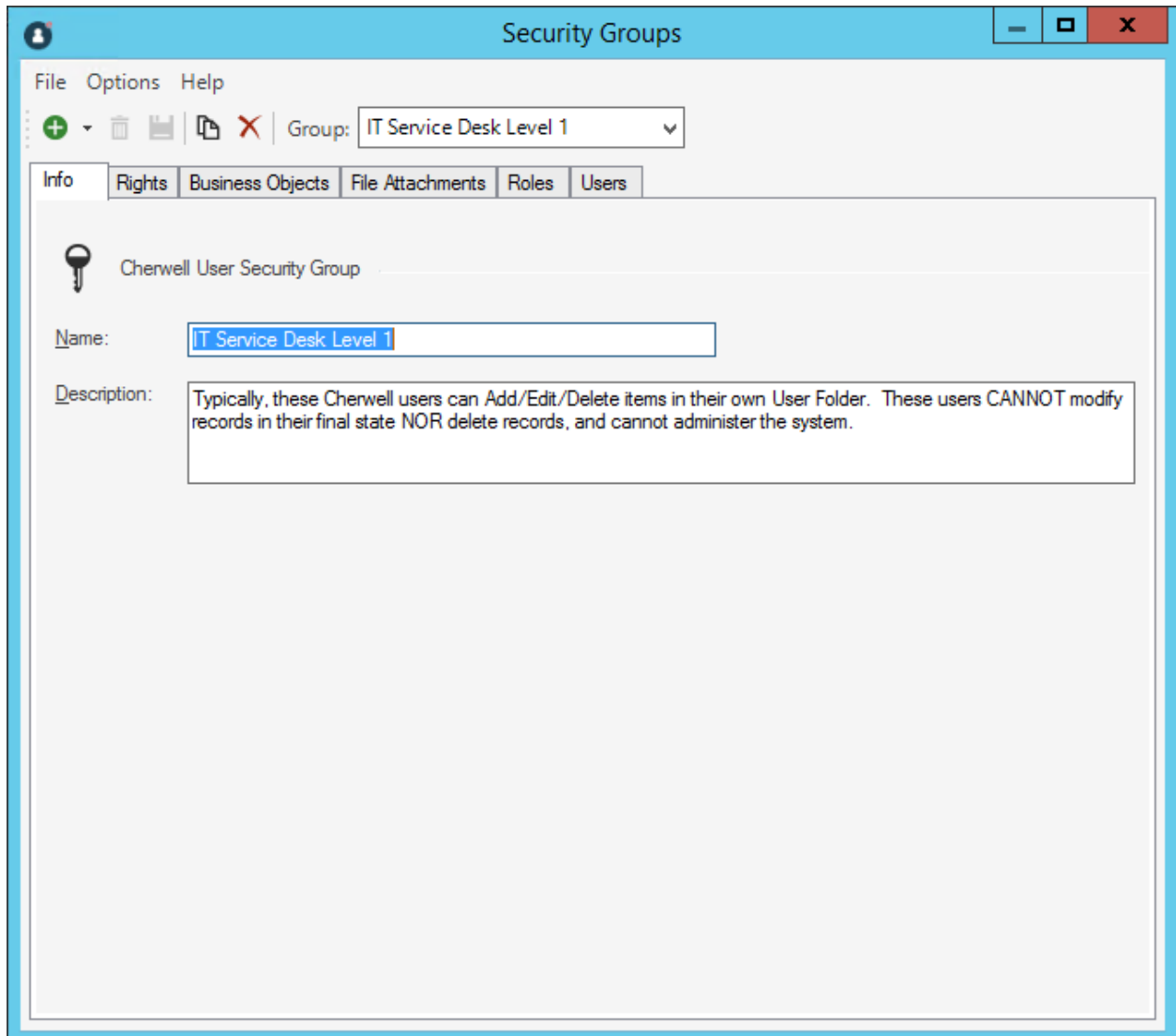
Use the Security Group Manager to:

- Create or edit Security Groups:
    - Define general information for a Security Group.
    - Define functionality security rights.
    - Define Business Object rights.

- ◦ Define File Attachment rights for a Security Group.
- ◦ Assign Roles to a Security Group.
- ◦ Assign Users to a Security Group.
- ◦ Move Users to a different Security Group.
- Delete a Security Group.
- Copy a Security Group.

Note: After editing Security Groups, the changes take effect immediately in the database. However, the changes may be delayed in other CSM applications (CSM Desktop Client, CSM Browser Client, and Cherwell REST API) due to a synchronization service that pulls database changes at designated intervals for maximum performance. The default value for both client and server checks is 15 seconds, but you can change this value by navigating to **Settings > Edit system settings > Advanced Settings** and updating the fields in the **Notifications** section.

Related concepts
Configure Global Advanced Settings

Open the Security Group Manager

Open the Security Group Manager from CSM Administrator.

From the CSM Administrator main window, select the **Security** category, and then select the **Edit Security Groups** task.

Create a Security Group

Use the Security Group Manager in CSM Administrator to create a Security Group.

When creating a Security Group, define the following properties:

- **Info:** Name and description.
- **Rights:** Security rights to access CSM functionality.
- **Business Object:** Security rights to access CSM data (Business Objects/Fields).
- **File Attachments:** Attachment security rights (ex: Import/link and global overrides).
- **Roles:** Roles assigned to the Security Group. You can also designate a default Role for the Security Group.
- **Users:** Users assigned to the Security Group.

To create a Security Group:

1. Open the Security Group Manager. See Open the Security Group Manager.

2. Select the **Create New** button **Down** arrow ⊕▾ , and then select the **type of Security Group** (User or Customer):
   - New Cherwell User Security Group: Creates a Security Group for a user (technician).
   - New Customer Security Group: Creates a Security Group for a customer (end-user).

   🖉 **Note:** Users and customers require different levels of security, and therefore, different User and Customer Security Groups.

3. Define general information (Info tab): Name and description.

4. Define security rights (Rights tab): Access to CSM functionality.

5. Define Business Objects rights (Business Objects tab): Access to CSM Business Object/Field data.

6. Define File Attachment rights (File Attachments tab): Attachment security rights (ex: Import/link and global overrides).

7. Assign Roles to the Security Group (Roles tab): You can assign an existing Role or create a new Role.

8. Assign people to the Security Group:
   - Assign users if it is a User Security Group (Users tab). You can reassign an existing user or create a new User Profile.
   - Assign Customers if it is a Customer Security Group. This is done when you create Portal credentials (CSM Desktop Client>Customer).

9. Assign LDAP or SAML groups (for systems configured to use LDAP or SAML authentication and automatic user imports only). See Map LDAP Groups to CSM Security Groups and Map SAML Security Groups to CSM Security Groups

10. Select **Save**.

Related concepts

Users Security Rights

Define General Information for a Security Group

Use the **Info** tab to define properties.

To define general information for a Security Group:

1. Open the Security Group Manager
2. In the **Group** drop-down list, select the Security Group for which you want to define rights (example: Admin).
3. Select the **Info** tab.
4. Define the general properties:
   a. Provide a name and description (both properties can be searched in CSM Item Managers). The description should be the type of user that belongs to the new Security Group and an explanation of when it should be used.
   b. From the drop-down list, select an email address to set as the default email address. This is the default email account for this Security Group. The account must be accessible to that Security Group to be set as the default. Select **Delete** to delete the email address.
   If no email address is set as the default, the global default email address is used.

   > **Note:** If a Security Group's default email address is provided, it will override the global default address. However, if a user's default email address is provided, that address will override the Security Group default address.

5. Select **Save**.

Define Functionality Security Rights (Access to Functionality)

Use the Rights tab in the Security Group Manager to define the access to CSM functionality for a Security Group.

Good to know:

- Functionality security rights control access to CSM functionality (example: Allowing a user/customer in a Security Group access to global dashboards).
- To make items easy to find, functionality is organized by category/subcategory (example: dashboards/global dashboards).
- For a detailed description of each security right, see Security Rights Reference.

To define functionality security rights:

1. Open the Security Group Manager.
2. From the **Group** drop-down list, select the **Security Group** that you want to define rights for (example: Admin).
3. Select the **Rights** tab.
4. Select the CSM functionality **Category** that you want to set rights for (example: Dashboards, Calendars). Notable categories include:

Option	Description
Default right	Sets default rights for all functionality in a Security Group. This default is also used for any new functionality that is added in future versions of CSM. **Note:** The defaults only affect untouched functionality; if you have already set specific functionality rights, those rights override the default. You can override the default at any time by manually setting functionality rights.
Application rights	Houses basic CSM functionality rights, such as Table Management, Grid/Toolbar/Task Pane, and personalization.
E-mail Accounts	Defaults all new accounts to allow for all groups. You can deny permissions on a per account basis.

Option	Description
Security features	Houses security feature rights, such as system settings, role/team management, and SAML settings.
Sites	Houses Portal Site rights.

A list of associated subcategories displays below the category.

5. **Subcategory**: Select the functionality that you want to set permissions for. The available rights show as check boxes below the subcategory. Rights vary by functionality but include a combination of the following:

Option	Description
View	Item can be viewed
Add	New item can be added
Edit	Existing item can be modified
Delete	Item can be deleted
Allow	Action/access is allowed
Run	Item can be run
Open	Item can be opened
View rights expression	Item has conditional rights based on an Expression
Use default	Item uses default rights

> **Note:** Many rights are scope-related (user, role, team, global), meaning they allow/deny access to an item based on an intended audience.

6. Select the **rights** check box to allow this Security Group permission to perform the action. Clear the check box to deny permission.

7. Select **Save**.

Example: To deny the Service Desk Security Group access to the Cherwell Administrator module:

1. Open the Security Group Manager.

2. Select the **Rights** tab.

3. Select the **Security features** category.

4. Select the **Run the administrator tool?** security right.

5. Clear the **Allow** check box.

Related concepts

Users Security Rights

About Security Groups

Define Business Object Rights (Access to Data)

Use the **Business Objects** tab in the **Security Group Manager** to define access to CSM data for a Security Group. Business Object security rights control access to:

- **General data:** Security Group can access (view, add, edit, delete) data in a Business Object. Business Object rights can be set at the Business Object or field level.
- **File Attachments:** Security Group can access (view, add, edit, and delete) Business Object record Attachments.

Different record ownership rights (both user and customer) can be set to extend/deny access to managers, departments, teams/workgroups, and team/workgroup managers.

To define Business Object security rights:

1. Open the **Security Group Manager**.

2. In the **Group** drop-down list, select the **Security Group** for which you want to define rights (example: Admin).

3. Select the **Business Objects** tab.

4. In the **Business Object** drop-down list, select the **Business Object** for which you want to set rights. You can also select individual fields within the Business Object.

   Tip: To set default rights for all Business Objects/fields in a Security Group, use the **New Business Objects** and **New Field Rights** options. These defaults are also used for any new Business Object/field created in a Blueprint. The defaults only affect untouched Business Objects/fields; if you have already set specific rights for a Business Object/field, those rights override the defaults. To override the defaults at any time, manually set rights for a Business Object/field. To restore a Business Object so that it uses default rights, use the Reset Rights options on the **Options** menu.

   The available Business Object rights show as check boxes to the right of Business Object/fields.

5. Define **General** rights:
   a. Select a check box to give a user permission to perform the operation. Clear the check box to deny permission. Rights include any combination of the following:
      ◦ **View:** Data/record can be viewed.

         Important: General View rights must be given to the Approval Business Object to allow approvals to be displayed.

      ◦ **Add:** Data/record can be added.

      ◦ **Edit:** Data/record can be modified.

      ◦ **Delete:** Data/record can be deleted.

      ◦ **Can edit Closed:** Data/record can be edited when it is in a Closed state of a lifecycle that was created using the About Business Object Lifecycles.

Note: If your Business Object has a legacy lifecycle attached, this check box is named **Can edit final state**. Either of these options are only available if the Business Object has a final state, such as Closed.

◦ **Can change Closed to Reopened:** Data/record can be changed from Closed to Reopened for a lifecycle that was created using the About Business Object Lifecycles.

Note: If your Business Object has a legacy lifecycle attached, this check box is named **Can change the final state to the recall state**. The data/record can be changed from its final defined state to a different lifecycle state. This option is only available if the Business Object has a final state (example: Closed) and a recall state (example: Reopened). The main reason to force users to change from a final state to a specific recall state is to ensure that changes are logged, and to trigger any special Automation Processes that need to be run when a record is recalled. Field rights are limited to View and Edit; Business Object rights vary depending on the lifecycle support.

Tip: It is a very common mistake to set view/edit rights for a Business Object but forget to set view/edit rights for fields, so the user still cannot edit any fields. The most straightforward way is to edit the **New Field** option for a Business Object, because that applies to any fields for which rights have not been set.

◦ **Limit records based on criteria:** Data is limited based on a defined criteria. Even though you can define complex queries, it is recommended that you limit the queries to ones using only fields from the Business Object being limited, or fields in 1-1 Related Objects (example: Members of the network Security Group might be limited to seeing Incidents with the category of **Networking**. If a criteria is applied, then only records that meet that criteria are seen by the user. Not only are searches limited, but Dashboard Widgets show only included records, as do reports, and all other features of the system).

6. Define **Encrypted Fields** rights:
   ◦ **View:** Encrypted fields can be viewed (can run the decrypt command on encrypted fields).

   ◦ **Edit:** Data can be entered into encrypted fields in new records.

7. Define **File Attachment** rights:
   a. Select a check box to give a user permission to perform the operation. Clear the check box to deny permission. Rights include any combination of the following:
      ◦ **View:** Attachments can be viewed.

      ◦ **Add:** Attachments can be added.

      ◦ **Edit:** Attachments can be modified.

      ◦ **Delete:** Attachments can be deleted.

8. **(Optional) Different rights based on ownership:** Select this check box to set different rights based on ownership.

Note: Record ownership is an important concept in CSM because it affects security and licensing, and it differs depending on whether the owner is a user or a customer. Be sure to understand the complexities of ownership.

9. Select **Save** .

Related concepts

Users Security Rights

Set Different Business Object Rights Based on Ownership

Business Object rights take effect when CSM can identify who each owner is (record owner, department member, manager of owner, Team/Workgroup member, and Team/Workgroup manager). Be sure that each entity is identified with an ownership attribute; otherwise, CSM ignores ownership.

To set different Business Object rights based on ownership:

1. Open the Security Group Manager

2. In the Group drop-down, select the **Security Group** for which you want to define rights (ex: Admin).

3. Click the **Business Objects** tab.

4. In the Business Object drop-down, select the **Business Object** for which you want to set rights. You can also select individual Fields within the Business Object.

5. Select the **Different rights based on ownership** check box. The rights expand.

    Note: A Customer Security Group displays Workgroup Member and Workgroup Manager instead of Team.

6. Set the **Business Object rights** for each entity.

7. Click **Save** .

Define File Attachment Rights for a Security Group

Use the File Attachments tab in the Security Group Manager to define the following File Attachments rights for a Security Group.

You can define:

- Which Attachment operations the Security Group can perform (example: Can import file attachments, link file attachments, and link URLs).
- Override system defaults for attachments: Whether or not the Security Group can override global Attachments settings (example: Maximum file size limit and allowable file types).

Global File Attachments rights are defined as part of system security settings. For more information, refer to Configure Global File Attachment Settings.

To define File Attachment rights:

1. Open the Security Group Manager.

2. In the **Group** drop-down, select the Security Group for which you want to define rights (example: Admin).

3. Click the **File Attachments** tab.

4. Define which Attachment operations the Security Group can perform (select all that apply):
   a. **Can import files**:

      Select this check box to allow the Security Group to import files as Attachments.

   b. **Can link files**:

      Select this check box to allow the Security Group to link files that are on a network drive directly to CSM.

   c. **Can link URLs**:

      Select this check box to allow the Security Group to link a website directly to CSM.

5. (Optional) Override system defaults for attachments: Select this check box to allow the Security Group to override the default settings with its own settings. Then, define the Security Group's settings:
   ◦ Select the **Limit Imported File Size** to check box to specify a maximum allowable file size to import, in MB. Then, provide the file size limit, in MB. If not selected, there is no limit and any size file can be imported.
   ◦ Define allowable file types to be imported as attachments (select one option):
     ◦ **Allow any files**:

        Select this option to allow all file types.

     ◦ **Only allow files with the following extensions**:

Select this option to import only explicit extensions. Then, provide the extensions to include (example: pdf), separated by a comma, either by typing directly in the

Extensions box, or by selecting **Choose File Types** to open the **Select File Types** window.

- **Allow files with any extension except**:

Select this option to exclude explicit extensions. Then, provide the extensions to exclude, separated by a comma, either by typing directly in the **Extensions** box, or by selecting

the **Choose File Types** button to open the **Select File Types** window.

 Tip: To restore the default file types, select **Restore to Cherwell defaults** .

6. Click **Save** .

Related concepts
Users Security Rights

Select Allowed File Attachment Types for Attachments

Use the Select File Types window to select the types of files to include or exclude as Attachments.

To select allowed file types for Attachments:

1. Open the Security Group Manager (CSM Administrator>Security>Edit Security Groups).

   The Manager lists the existing Security Groups.

2. Select a **Security Group**.
3. Click the **File Attachments** tab.
4. Select the **Override system defaults for attachments** check box.
5. Select the **Only allow files with the following extensions** radio button to limit the allowed Attachment file types.

   OR

   Select the **Allow files with any extension except** radio button to exclude certain file types from being Attachments.

6. Click the **Select file types** button.

   The Select File Types window opens.

   > **Note:** If you selected to only allow certain file types, the Allowed File Types window opens. If you selected to exclude certain file types, the File Types to Prohibit window opens. Both windows appear and function the same; however, one will allow certain file types while the other prohibits their use.

7. Select or clear the **File types** check boxes to add or remove file types to/from the list. Beneath the File Types list is the file extension(s) included in the file type (ex: Adobe Photoshop Files have .psd file extensions).

   File extensions are automatically added or removed from the File Extensions list at the bottom of the window as you select/clear file types. You can also type the file extensions directly into this File Extensions list.

8. Click the **Reset to Default** button to reset the file types to Cherwell defaults.

9. Click the **Uncheck all file types** button to clear all file type selections.

10. Click the **Check all files types** button to select all file types.

11. Select **OK**.

Reset Security Group Rights

To reset the rights of a Security Group, perform the following steps:

1. In the CSM Administrator main window, click the **Security** category, and then click the **Edit Security Groups** task.
   The Security Group Manager opens.
2. While on the Rights or Business Objects tab, select **Options > Reset Rights...**
3. Choose a reset option:
   - **Reset all standard rights - these are the rights that appear on the "Rights" tab**
   - **Reset all business object rights - these are the rights that appear on the "Business Objects" tab**
4. Click **OK**.

Assign Roles to a Security Group

Use the Roles tab in the Security Group Manager to assign Roles to a Security Group.

Good to know:

- A Role can be assigned to one or more Security Groups at a time.
- A User can access any of the Roles in his Security Group, but can only log in using one Role at a time.
- If the Security Group supports only one Role, Users in that Security Group will be assigned to that Role without being asked. Otherwise, they will have the option of choosing the Role they want to use when they log in to one of the main client products.
- Customers are automatically logged into their Security Group's default Role when logging in.

To assign a Role to a Security Group:

1. Open the Security Group Manager.
2. In the Group drop-down list, select the **Security Group** for which you want to define rights (example: Admin).
3. Select the **Roles** tab.
   A list of assigned Roles (legal Roles) opens.
4. Select the **Add** button.
   The **Add Role to Security Group** window opens, listing the available CSM Roles (Roles not already in the Security Group).
5. Select the **Role** you want to assign to the Security Group or select the **New Role** button to create an ad hoc Role.
6. Select **OK**.
7. Designate a default Role by selecting a **Role**, and then selecting the **Make default** button.

   Note: When a User logs into CSM, their default Role is selected, but they can select any Role. When a Customer logs into CSM, they log in using their default Role.
   Select the **Remove** button to remove a Role from the Security Group.

8. Select **Save**.

Related concepts
About Security Groups
About Roles
Open the Security Group Manager
Related tasks
Create a Role

Assign Users to a Security Group

You can manually add users to a Security Group. If you have SAML or LDAP configured for your system, you can map Active Directory groups to a Security Group and automatically add users to CSM from those groups.

Users can be assigned to only one Security Group at a time. When you reassign an existing user to a Security Group, you remove that user from the first Security Group. The Security Group is stored in the user's profile. You can assign a user to a Security Group when you edit a user profile or when you edit a Security Group.

> **Note:** If you have SAML or LDAP configured, you can mapping Active Directory groups to CSM Security Groups. See Map LDAP Groups to CSM Security Groups and Map SAML Security Groups to CSM Security Groups.

To assign a user to a Security Group:

1. Open the Security Group Manager.
2. In the **Group** drop-down list, select the **Security Group** for which you want to define rights (example: Admin).
3. Select the **Users** tab.
4. Select **Add**. The **Add user to security group** window opens, listing the available Users (Users not already in the Security Group).
5. Select the **User** you want to assign to the Security Group, or select **New User** to create a new User Profile.
6. Select **OK**.
   - Select the **Move To** button to move a User from the Security Group to another Security Group.
   - Select the **Import** button to import a User from Windows or AD/LDAP.
7. Select **Save**.

Related concepts
Import Directory Service Users
Related tasks
Create a User Profile
Map SAML Security Groups to CSM Security Groups
Move a User to a Security Group

Move a User to a Security Group

To move a User to a Security Group, perform the following steps:

1. In the CSM Administrator main window, click the **Security** category, and then click the **Edit Security Groups** task.
   The **Security Groups Manager** opens.

2. In the **Users** tab, choose the User you wish to reassign, then select the **Move to**button.
   The Move User to a Different Security Group dialog opens.

3. Select the new Security Group and click **OK**.

About Roles

A Role is a user or customer's current function/responsibility in CSM, and controls how data is presented in that person's CSM environment.

For example, a Role determines which Home Dashboard is displayed and how the Incident form looks (example: Which fields are exposed, required, etc.). A Role is assigned to a Security Group and can be assigned to more than one Security Group at a time. A user or customer can access any of the Roles in his Security Group, but can only log in using one Role at a time. Examples of Roles include Service Desk Manager and Portal Customer.

Related concepts
About Security Groups

OOTB Roles

CSM provides the following OOTB Roles:

- Service Desk
- Service Desk Manager
- Portal Customer

Use these OOTB Roles as-is, edit them, or create new Roles using the Role Manager in CSM Administrator.

Managing Roles

Roles are managed using the Role Manager.

Use the Role Manager to:

- Create or edit a Role.
- Delete a Role.
- Copy a Role.
- Clear Settings.

Open the Role Manager

To open the Role Manager in CSM Administrator main window, click the **Security** category, and then click the **Edit Roles** task.

Create a Role

Use the Role Manager in CSM Administrator to create a role.

A role controls how data is presented in that person's CSM environment. For more information, see About Roles.

When you create a role, you define:

- Name and description.
- Primary Business Object: A Primary Object is the Business Object that the system defaults to for any newly added items (if there is not some other default). For example, if a role's default Business Object is Incident, when a new dashboard widget is created, it defaults to being an Incident Widget. In many cases, the system remembers the last selected Business Object for an option (example: Quick Search on the Task Pane defaults to searching the last selected Business Object). However, if there is no previous value, or a particular option does not remember the last choice, CSM uses the Primary Object.
- Available Business Objects: Business Objects that the role can access from the New menu, Quick Search, and Item Managers; cleared roles will be suppressed (not visible from those locations) but not restricted (that is, the UI will not be cluttered with the Business Object but the role can still access the Business Object when in a Relationship with accessible objects). For example, if Problem is not selected, Problem will not be on the New menu but users of this role will still be able to access Problems through Incidents.
- Default system items for the role:
  - Dashboard
  - Dashboard Theme
  - Heads-Up Display (HUD)
  - Calendar
  - Visualization
- Custom Views: View to use when members of this role log into the CSM Desktop Client (applicable for users only) and the CSM Web Applications (Portal for Customers and Browser Client for users).
- Culture: Determines the cultures available for users assigned to the role.

Good to know:

- If no default role dashboard/HUD is selected, the Global defaults are used.
- With security rights, a user can override the role defaults and select their own defaults. For more information, see Security Rights.
- Customers have limited options and cannot override defaults in the Portal.
- A system administrator can clear role and user defaults (for a specific user/role or all), resetting the defaults to the global-defined settings (**File > Clear Settings** in the User Manager or Role Manager).

To create a role:

1. Open the Role Manager. For more information, see Open the Role Manager.
   The Manager lists the existing roles.

2. Select **Create New**.
   A [New] role is added to the list.

3. Define general information for the role:
   a. Name: Specify a **name** for the role.

   b. Image:

   Select the image to open the **Image Manager**, and then select an existing image or import a new image to represent the item in the UI.

   c. Primary Object: From the drop-down list, select a **primary Business Object** for the role.

   d. Description:

   Provide a description to use within CSM (search this property in CSM Item Managers).

   e. Control Business Objects available with this role: Select the **Ellipses** to select **Business Objects** that the role can access.

4. Select **default CSM Items** for the role (dashboard/Heads-Up Display/calendar/visualization):
   ◦ Use default: Select this option to have the role use the Global defaults.

   ◦ Dashboard/Dashboard Theme/Heads-Up Dashboard (HUD)/Calendar/Visualization: Select these options to select specific default CSM items for the role. The Managers open to select an existing item or create a new item. Be sure to select items that everyone in that role can access (that is, the item must be in scope). For more information, see Scope.

   > **Note:** For dashboard theme, you can select to use the Global Dashboard Theme, the dashboard's default theme, or a specifically-selected theme.

   Most defaults can be overridden by a user assuming they have security rights. For example, a user can right-click a displayed dashboard and choose to make it their default Home dashboard instead of the system administrator-chosen default. Also, for most options, there is a Global default that is displayed if the role does not explicitly override it. Customers have limited options and cannot override defaults in the Portal. System administrators can clear user defaults by selecting **File>Clear Settings**.

5. Select the **Views** to use when members of this role log into the CSM Desktop Client (applicable for users only) and the CSM Web Applications (Portal for Customers and Browser Client for users). Typically, Customers will have a limited Portal view.

6. Select culture options for the role. For more information, see Set Cultures for Roles.

7. Select **Save**.

Related concepts
Dashboards
Dashboard Themes
Heads-Up Display (HUD)

About Calendars
About Visualizations

Exclude Business Objects from a Role

You can specify which Business Objects a Role can access from the New menu, Quick Search, and Item Managers; excluded Roles will be suppressed (not visible from those locations) but not restricted (that is, the UI will not be cluttered with the Business Object but the Role can still access the Business Object when in a Relationship with accessible objects). For example, if Problem is not selected, Problem will not be on the New menu but Users of this Role will still be able to access Problems through Incidents.

To exclude a Role's access to certain Business Objects, perform the following steps:

1. In the CSM Administrator main window, click the **Security** category, and then click the **Edit Roles** task.
   The Roles Manager opens.

2. Select the **Ellipses** button to control Business Objects available within a Role.
   The Available Business Objects dialog opens.

3. Uncheck the Business Objects you wish to exclude from the Role.
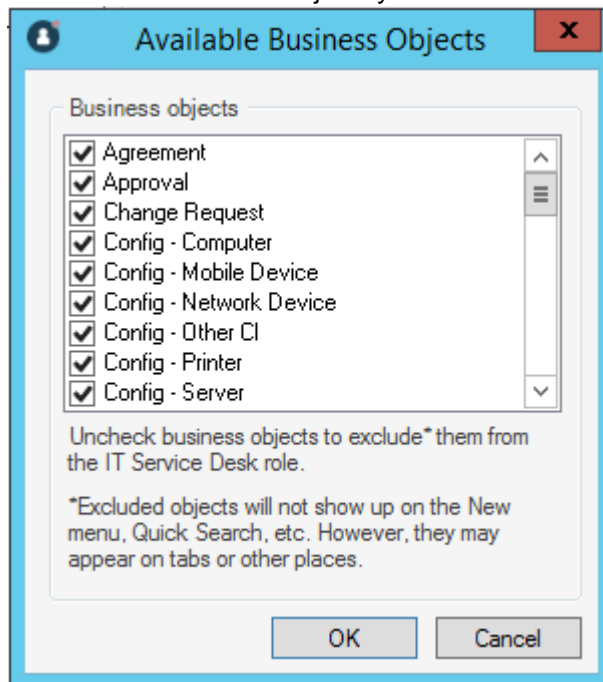
Click **OK**.

About Teams and Workgroups

CSM provides several default Teams and Workgroups. Use these Teams/Workgroups as-is, edit them, or create your own using the Team and Workgroup Manager.

A Team is a collection of CSM users that can share CSM items (such as Dashboards), record ownership, and assignments. Examples include Support, Management, and Knowledge Management. A Team plays an important part in record ownership because members of the Team can have additional rights to view and edit records.

A Workgroup is a collection of CSM customers who can share CSM items (such as Dashboards). Examples include Sales, HR, and Operations. A Workgroup plays an important part in record ownership because members of the Workgroup can have additional rights to view and edit records.

Team/Workgroup properties include:

- Information: Name and description, and defaults for sending e-mails to Workgroup members.
- Members: Users on the Team and Customers in the Workgroup.

> **Note:** If configured, record ownership rights (View, Add, Edit, Delete rights) can be extended to managers, departments, and Teams/Workgroups, so carefully consider the implications of these relationships.

Related concepts
Record Ownership

Default Teams and Workgroups

CSM provides several default Teams and Workgroups.

Default User Teams:

• 1st Level Support • 2nd Level Support • 3rd Level Support • Change Advisory Board (CAB) • Facilities	• HR • IT Management • Knowledge Management Teams • Reporting

Default Customer Workgroups:

• Accounting • Business Development • Customer Service • Design • Executive • Finance • Human Resources	• Information Technology • Marketing • Office • Operations • Sales • Shipping • Telesales

Use these default Teams/Workgroups as-is, edit them, or create your own using the Team and Workgroup Manager in CSM Administrator.

Managing Teams and Workgroups

Teams and Workgroups are managed using the Teams and Workgroups Manager and the Team Manager. Use these managers to view, edit, and delete a team or workgroup, create a customer workgroup, and create a team.

Open the Team and Workgroup Manager

The Team and Workgroup Manager is available from the **Security** category in CSM Administrator.

1. Open the CSM Administrator.
2. In the main window, select the **Security** category.
3. Select the **Edit Teams and Workgroups** task.

View Team Information

You can access Team Info from a Blueprint Lookup table or Security Teams and Workgroups in CSM Administrator or Table Management in the CSM Desktop Client.

The Team Info Business Object creates a lookup table based on the information in Security Teams and Workgroups.

🖉 **Note:** The ability to edit and create Team Info is set through security rights.

- To view Team Info from a Blueprint in CSM Administrator:
    1. Create a Blueprint.

    2. Select the **Lookup tables** radio button.

    3. Select **Team Info Business Object**.

    4. Select the **Edit data** task.
       The **Edit Blueprint Data - Team Info objects** window opens.

    5. Double-click a Team Info object to view the details.

- To view Team Info from the **Security** category in the CSM Administrator, open the Team and Workgroup Manager.

- To view Team Info in the Desktop Client:
    1. Open the Table Management Interface.

    2. In the **Type** drop-down list, select **Team Info**.

    3. Double-click a Team Info object to view the details.

Related concepts
Using Blueprints
Related tasks
Create a Blueprint

Team Information Synchronization

Manually synchronize Team Info to keep information current across locations. When the system is synced, the Team Info Business Object is updated from the Team Info Definitions.

If a Team info Business Object is found, then the Team definition is updated. Otherwise, a new Team Info Business Object is created.

To manually synchronize Team Info:

1. In CSM Administrator, select the **Database** category, and then select the **System maintenance** task.
   The **System Maintenance** window opens.
2. Select the **Synchronize Team Info Business objects with team list** check box.
3. Select **OK**.

Create a Team

Create a Team/Workgroup to define name, description, and email information for the Team (Info) and Users on the Team (Members).

Use the Team and Workgroup Manager in CSM Administrator to create a Team or Customer Workgroup.

Note: If configured, record ownership rights (View, Add, Edit, Delete rights) can be extended to managers, departments, and Teams/Workgroups, so carefully consider the implications of these relationships.

To create a Team:

1. Open the Team and Workgroup Manager.
2. Select the **User Teams** radio button.
   The Manager lists the existing Teams.
3. Select the **Create New** button to add a new team to the list.
4. Define general information for the Team:
   a. Select the **Info** tab.
   b. Provide a name for the Team.
   c. Select the **Image** button to open the Image Manager, and then select an existing image or import a new image to represent the item in the UI.
   d. Provide a description to use within CSM (this property can be searched in CSM Item Managers).
5. Define options for determining how emails are sent to the Team (when the Team is chosen as the email recipient).
   a. **Send to All Members Who Have a Valid E-mail Address**: Select this radio button to send emails to all of the addresses for all members of the Team (based on the member list created in the next step).
   b. **Send to This Alias**: Select this radio button, and then provide the email alias (example: Admins@mycompany.com) to send emails to an already defined email alias. This option is useful if a company has created an email alias (example: Company Administrators) that mirrors the membership of the Team.
6. Add Users to the Team:
   a. Select the **Members** tab.
   b. Select the **Add** button.
      The **Add Team Member** window opens.
   c. Select one or more Users to add to the Team.
   d. To designate a Team manager, select a User (member), and then select the **Team manager** check box. You can designate more than one manager, if needed.
   e. Select **OK** to add User(s) to the team.
7. Select **Save**.

Related concepts
[About Teams and Workgroups](#)

Record Ownership

Select Email Recipients from the CSM Address Book

About Users

Related tasks

Create a User Profile

Add a User to a Team

To add a user to a Team:

1. In the CSM Administrator main window, select the **Security** category.
2. Select **Edit Teams and Workroups**.
   The Team and Workgroup Manager opens.
3. Select the **User Teams** radio button and choose the Team you wish to add users to. Select the **Members** tab.
4. Select the **Add** button to open the **Add Team Member** window.
5. Select team member(s) to add, close the dialog, then close the Teams and Workgroups Manager.

   Tip: Select **New user** to create a new User Profile or use the search bar to search for User names.

6. Select **OK**.

To designate a user as the Team Manager, select a User (member) in the Teams and Workgroups Manager, and then select the **Team Manager** check box. You can designate more than one manager, if needed.

   Note: If configured, record ownership rights (View, Add, Edit, Delete rights) can be extended to managers, departments, and Teams/Workgroups, so carefully consider the implications of these relationships.

Related concepts
Add a License Key
Record Ownership
Related tasks
Create a User Profile

Create a Customer Workgroup

Using the **Team and Workgroup Manager**, create a Customer Workgroup by defining the name, description, and email information about the Workgroup (Info) and the customers in the Workgroup (Members).

If configured, record ownership rights (View, Add, Edit, Delete rights) can be extended to managers, departments, and Teams/Workgroups, so carefully consider the implications of these relationships.
To create a Customer Workgroup:

1. Open the Team and Workgroup Manager.
2. Select the **Customer workgroups** option.
   The Manager lists the existing Workgroups.
3. Select **Create New** to add a new workgroup to the list.
4. Define general information for the Workgroup:
   a. Select the **Info** tab.
   b. Provide a name for the Workgroup.
   c. Select the **Image** button to open the **Image Manager**, and then select an existing image or import a new image to represent the item in the UI.
   d. Provide a description to use within CSM (this property can be searched in CSM Item Managers).
5. Select an option to determine how emails are sent to the Workgroup (when the Workgroup is chosen as the email recipient).
   ◦ **Send to All Members Who Have a Valid E-mail Address**: Select this option to send emails to all of the addresses for all customers in the Workgroup (based on the member list created in the next step).
   ◦ **Send to This Alias**: Select this option, and then provide the email alias (example: Admins@mycompany.com) to send emails to an already-defined email alias. This option is useful if a company has created an email alias (example: Company Administrators) that mirrors the membership Workgroup.
6. Add customers to the new (or an existing) Workgroup:
   a. Select the Workgroup (if not already selected).
   b. Select the **Members** tab.
   c. Select **Add** to open the **Contact Manager**.
   d. Select a customer from the list of contacts, and then select **OK**.
   e. Repeat steps *c* and *d* above to add more customers.

   Note: If a customer you want to add is not in the **Contact Manager** lists, select **New** on the **Contact Manager** toolbar, and then create a new Customer Record, see Create a Customer Record. After adding the new customer to the **Contact Manager**, follow the steps above to add them to the Workgroup.

7. Select **Save** in the **Teams and Workgroups** window.

Related concepts

About Teams and Workgroups

Select Email Recipients from the CSM Address Book

About Customers

Record Ownership

Create an Approver Workgroup

Using the Team and Workgroup Manager, create an approver workgroup that you can reuse across multiple Approval blocks. Approver workgroups can contain teams, other workgroups and users and don't impact existing team or customer workgroups.

If configured, record ownership rights (View, Add, Edit, Delete rights) can be extended to managers, departments, and teams/workgroups, so carefully consider the implications of these relationships.

Note: You can also edit and remove one or more members from a workgroup and copy or delete the workgroup using this **Teams and Workgroups** window.

Tip: You can see any approver workgroups you create by configuring an Approval Block.

To create an approver workgroup:

1. In CSM Administrator, select **Security > Edit teams and workgroups** to open the Team and Workgroup Manager.
2. Select the **Approver Workgroup** option.
   The Manager lists the existing workgroups.
3. Select **Create New** and select **Approver Workgroup** to add a new workgroup to the list.
4. Define general information for the workgroup:
   a. Select the **Info** tab.
   b. Provide a name for the workgroup.
   c. Select to open the Image Manager, and then select an existing image or import a new image to represent the item in the UI.
   d. Provide a description to use within CSM (this property can be searched in CSM Item Managers).
5. Define options for determining how emails are sent to the workgroup (when the workgroup is chosen as the email recipient).
   a. **Send to all members who have a valid e-mail address**: Select to send emails to all of the addresses for all users and customers in the Workgroup (based on the member list created in the next step).
   b. **Send to this alias**: Select and then provide the email alias (example: Admins@mycompany.com) to send emails to an already-defined email alias. This is useful if a company has created an email alias (example: Company Administrators) that mirrors the membership workgroup.
6. Add users/customers/teams to the workgroup:
   a. Select the **Members** tab.
   b. Select **Add** to open the **Choose Approvers** window.
   c. Using the expanding tree or the search box, find and select a user/customer/team/workgroup to add to the workgroup, and then select **OK**.
   d. Continue to add more members to your list until finished.

Tip: Select `Ctrl + A` to select all members in a list and then select the left or right arrow to move them from selected to deselected or vice versa. Double-click a member to add them to the workgroup and close the window at the same time.

   e. Select **OK**.

7. Select **Save**.

Note: When teams and customer workgroups are part of an approver workgroup, the values set for votes required for approval is for all the users and customers within those teams. Voting thresholds cannot be set per team. See Define Approver Properties.

Related concepts

About Approvals

Approvals Good to Know

Add an Approval to a Business Object

About Users

A user is a service desk professional who logs in and uses CSM to manage service desk data (example: A technician, manager, designer, system administrator, etc.).

A user is assigned to only one Security Group (so they can access specific functionality and data), can log in using one or more Roles (so they can have a personal viewing environment), and can belong to one or more Teams (so they can share CSM items, such as Dashboards).

Note: Although a User can belong to one or more Teams, they must have a default team assigned. To add a User to a Team, see Create a User Profile.

Each User has a User Profile that stores the pertinent details and properties for that User, including:

- Login credentials: Username and password, and authentication method
- Culture settings
- User information: Name, department, title, manager, and other contact information

    Note: The User Information fields are configurable and are stored in the User Info Business Object.

- Account details: Password resets, reserved licenses, and other account details
- Assigned Security Group
- Assigned Teams

User Profiles are managed (created, viewed, imported, deleted) as part of Security in CSM Administrator using the User Manager. For more information, see View User Accounts.

Note: A User often functions as both a User and a Customer in CSM. For example, a service desk technician performs User functions but is a Customer of the HR Department. If the User is also a Customer, he/she must have a User Profile AND a Customer record. A Customer record does NOT store account credentials, so any Customer requiring a Portal login must also have Portal credentials. For more information, see Create Portal Login Credentials (for a Customer).

Related concepts
About Security Groups
About Roles
About Teams and Workgroups
User Manager
Related tasks
Set Cultures for Users

User Manager

The User Manager is used to create or modify user profiles.

Use the User Manager to:

Operation	Description
Create	Create new users.
Import	Import existing users.
Edit	Edit existing users.
Copy	Copy the settings for existing users into new files.
Delete	Remove selected user(s).
Clear Settings	Clears all custom settings/defaults defined for the selected user, resetting the custom settings/defaults to the Global settings/defaults. An option is also available to clear all custom settings for all users.

Note: When using a hosted services license (SaaS), if you try to modify or delete the CSDAdmin or CherwellServices accounts, you will receive the following message: "This account is used for hosting services and cannot be modified." The only user account that can modify these accounts is CSDAdmin.

Open the User Manager by using the Security category in the CSM Administrator Task Pane.

To open the User Manager:

1. In the CSM Administrator main window, select the **Security** category, and then select the **Edit Users** task.
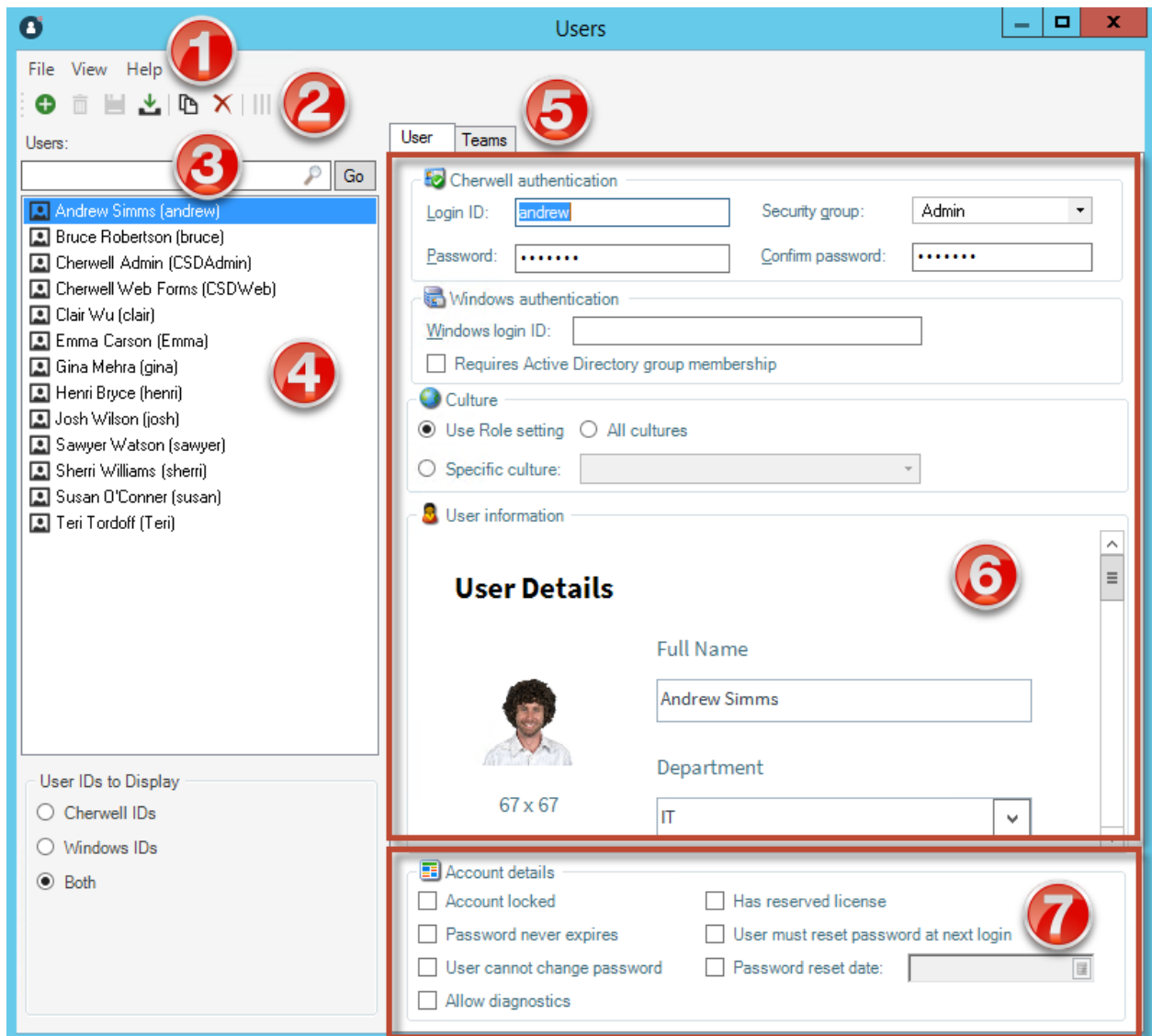
1. Menu bar:

   Displays a row of drop-down menus available in the Manager.

2. Toolbar:

   Displays a row of buttons for operations available in the Manager.

3. Search Control:

   Displays a search box to find specific words or phrases in the Manager.

4. User list:

Displays a list of available users.

5. Tabs:
   - User: Details about the user, separated into login credentials, culture settings, User Information, and Account Details.
   - Teams: Teams of which the User is a member.

6. User Information:

Personal information about the user.

📝 **Note:** The User Information fields are configurable and are stored in the User Info Business Object.

7. Account Details:

Details about account locking, password resets, and reserved licenses.

User Manager Menu Bar

File Menu

Action	Description
New	Creates a new item.
Abandon	Abandons changes to the current item.
Save	Saves changes to the current item.
Clear Settings	Clears all custom settings/defaults defined for the current item, resetting the settings/defaults to the Global settings. An option is also available to clear all custom settings for all items. Cleared settings include: Default Dashboard/Dashboard Theme, HUD, Calendar, Visualization, Mobile Configuration, window sizes, and some Grid settings.
Import User	Imports users from Windows NT, AD/LDAP. **Note:** This option only appears if your system has been appropriately configured.
Copy	Creates a new item whose properties are the same as the copied item. The new item can then be named and customized.
Delete	Deletes the current selection.
Close	Closes the Manager.

View Menu

Action	Description
User Account List..	View list of user accounts and their details.

Help Menu

Action	Description
Help	Opens the online help.
Contents	Opens the online help.
About	Displays information about the application.

Manager Menu Bar

Button	Action	Description
⊕	**Create New**	Creates a new item.
🗑	**Abandon**	Abandons changes to the current item.
💾	**Save**	Saves changes in the active window.
⭳	**Import User**	Imports users from Windows NT, AD/LDAP.
🗐	**Copy**	Creates a new item whose properties are the same as the copied item. The new item can then be named and customized.
✕	**Delete**	Deletes the current selection.
|||	**Show Legal Values (Lookup)**	Displays a list of legal values (for lookup fields only).

Open the User Manager

To open the User Manager in the CSM Administrator main window, click the **Security** category, and then click the **Edit Users** task.

Create a User Profile

Use the User Manager in CSM Administrator to create a User Profile for each CSM user.

The User Profile stores the pertinent details and properties for the user such as:

- Login credentials: Username and password, and authentication method.
- User information: Name, department, title, manager, contact information.
- Account details: Password resets, reserved licenses.
- Assigned Security Group.
- Assigned Teams.

Good to know:

- To save time, import users already stored in a Service Directory.
- Login credentials (either Cherwell or Windows/Lightweight Directory Access Protocol [LDAP]), Security Group, and Full Name are required fields on a User Profile. Department, Email, and Manager are highly recommended because some features (record ownership, One-Step™ Actions/ Actions, Automation Processes), if configured, use them.
- If the user's Security Group does not yet exist, you must create it before creating the User Profile. You can create the Teams before, or on the fly.
- The user information fields are configurable and are stored in the User Info Business Object.
- If configured, record ownership rights (view, add, edit, delete rights) can be extended to managers, departments, and Teams/Workgroups, so carefully consider the implications of these relationships.

To create a User Profile:

1. Open the User Manager.
2. Select **Create New**.
   A [New] user is added to the list.
3. Select the **User** tab.

Setting User Authentication Options

4. Define login credentials for the User (either Cherwell authentication or Windows/LDAP authentication):

Field	Description
Login ID	Provide a Cherwell login ID for the user (example: First initial + last name). The login is limited to 60 characters and must be unique.
Security Group	Select a Security Group.

Field	Description
Password	Provide a Cherwell password for the user, and then enter it again to confirm it.
(Optional) Windows authentication	◦ Windows login ID: Uses Windows credentials for login (instead of Cherwell credentials). Provide the user's Windows Login ID. **Note:** To use this feature, Windows or LDAP must be a supported login mode (**CSM Administrator > Security > Edit security settings**) and select the **Windows** check box. ◦ Requires Active Directory group membership: Select this check box to further validate the Windows login by authenticating it against Microsoft® Active Directory® (AD). If users are created on the fly from AD, this option will be set automatically. **Note:** To use this feature, AD must be configured and LDAP must be a supported login mode (**CSM Administrator > Security > Edit security settings**) and select the **LDAP** check box.
Culture	Choose the culture option. See Set Cultures for users.

Adding User Information

5. Provide personal user Information:

Field	Description
Full name	Provide the user's full name.

Field	Description
Set Image	Select the image to open the **Image Manager**, and then select an existing image or import a new image to represent the item in the UI. **Tip:** A person's image is often called an avatar because it can be a photo or a character representation.
Department	Select the user's department. **Note:** If configured, record ownership rights (View, Add, Edit, Delete rights) can be extended to managers, departments, and teams/workgroups, so carefully consider the implications of these relationships.
E-mail	Provide the user's email address. If email is configured, CSM can send emails to this address. Note that Automation Processes and Actions/One-Step Actions can also use an email address. **Tip:** When testing a system, consider using a test email account to avoid unnecessary emails.
Manager	Select the **Selector** button to open the **User Selector** window. Then, select the user's manager. Browse, search, or create a new user, if needed. **Tip:** If configured, record ownership rights (View, Add, Edit, Delete rights) can be extended to managers, departments, and teams/workgroups, so carefully consider the implications of these relationships.

Field	Description
Manager E-mail	Auto-populates with the selected manager's email address (if defined in the manager's User Profile). If email is configured, CSM can send email to this address. Automation Processes and Actions/One-Step Actions can also use a user's email address.
Other	Phone numbers, fax number, availability (example: Day shift), scheduled time-off, comments.

Note: The user information fields are configurable and are stored in the User Info Business Object.

Setting User Account Details

6. Define account locking, password reset, and reserved license options:

Field	Description
Account locked	Select this to lock the user account. **Note:** Accounts can also be locked using the **View Logged-in Users** window (**CSM Administrator > Security > View currently logged-in users**).
Password never expires	Select this to waive password expiration. This overrides any system setting to reset the password. **Note:** If this is selected, the *User must reset password at next login* and *Password reset date* settings are hidden.
User cannot change password	Select this to restrict a user from changing their password. If a password reset is required by the system, the system administrator must reset the password.
Allow diagnostics	Select this to grant a user permission to run the Network Health Check test.

Field	Description
Has reserved license	Select this to reserve one of your company's concurrent licenses for this user. **Tip:** Use the **Licensing** window to manage all reserved licenses.
User must reset password at next login	Select this to prompt the customer to change their password at their next login. This check box is cleared after the customer changes their password. **Note:** This restarts any administrator-scheduled password reset. This is an immediate reset. Use this setting if the user forgot their password.
Password reset date	Select this to prompt a user to change their password on a specific date. Then, use the **Date Selector** to choose a reset date.

Adding Users to Teams

7. Add the user to one or more existing teams. If the team does not yet exist, create the team:
   a. Select the **Teams** tab.
   b. Select the **Add**.
      The **Add User to Team** window opens.
   c. Select one or more teams and select **OK**.
      The user is added to the team(s).
   d. To select a default team, select the **Team**, and then select **Default Team**.
8. Select **Save**.

Related concepts
Import User and Customer Information Using Microsoft Active Directory
Open the User Manager
Windows Credentials
Related tasks
Network Health Check Results

View User Accounts

With the User Accounts List, system administrators can view the current account status of the Users in the CSM database, including:

- User names.
- Account creation dates.
- Locked status of the account.
- If the User can change their password.
- If the User's password is set to expire.
- The date of a User's last password reset.
- The date of a User's next password reset.

To access the User Accounts List:

1. Open the User Manager

2. In the User Manager menu bar, click **View>Select User Account List**.

   The User Account List opens.

3. Double-click a **User Profile** in the User Account List.

   The User Profile window opens.

   Note: The Add User window is the same form as the User tab of the User Manager when you create a User profile.

Profiles can also be edited by clicking the profile once to highlight it in the User Account List, and then clicking the Edit... button. From the User Account List, new profiles can also be added and existing profiles deleted by clicking the Add... (to open the Add User window) and Delete buttons.

Import User and Customer Information Using Microsoft Active Directory

Active Directory is a special-purpose database that stores data for objects in a network, including User and Customer information. User and Customer data from Active Directory can be imported into CSM to readily view information such as full names, e-mail addresses, etc. for internal Users and Customers.

To import Users and Customers using Active Directory:

1. Complete the Directory Services worksheet.
2. Configure CSM Directory Services Settings.
3. Configure Users for Directory Services.
4. Configure Customers for Directory Services.

> **Tip:** Alternatively, configure these settings using the Getting Started Page in CSM Administrator (Help>Go to Getting Started Page).

About Customers

A customer is an end user, either an internal employee or an external individual, who relies on CSM to initiate/fulfill a Service or Product (example: A person reporting a lost password or requesting a new phone).

If configured, a customer can access CSM data and perform self-service activities using the CSM Portal. A customer is assigned to one, and only one, Security Group (so they can access specific functionality and data) can log in using their default Role (so they can have a personal Customer View) and can belong to one or more Workgroups (so they can share CSM items, such as Dashboards).

Each customer has a Customer Profile (called a Customer record) that stores the pertinent details and properties for the customer, including:

- Identification information: Name, department, title, manager, etc.
- Details: Contact information, SLA level, social media information, etc.

> **Note:** The Customer record Fields are configurable and are stored in the Customer Info Business Object (called *Customer - Internal* in the Starter Database).

Customer records are created in the CSM Desktop Client and are managed (searched for, edited, deleted, etc.) using the Contact Manager. A Customer record does NOT store account credentials, so any customer requiring a CSM Portal login must also have credentials to store:

- CSM Portal login credentials (username and password).
- Assigned Security Group.
- Account details (password resets, etc.).

Related concepts

About Security Groups

Create a Customer Record

Add Customers to the CSM Portal

Contact Manager

The **Contact Manager** allows you to quickly manage customer records.

Use the Contact Manager to:

- View: View a grid list or card view of customer records, or view a specific record in detail. In grid and card view, customer records are listed alphabetically by last name, organized by lettered tabs (example: ABC, DEF, etc.).
- Find a specific customer record using filtering and searching options.
- Create, edit, or delete a customer record.

The **Contact Manager** can be opened several ways in the CSM Desktop Client or CSM Browser Client.

To open the Contact Manager:

- From the CSM Desktop Client menu bar, select **Customer > Contact Manager**.
- From the CSM Browser Client menu bar, select **Tools > Contact Manager**.
- From a Business Object record, select the **Customer Selector** button .
- From the **Team and Workgroup Manager** in CSM Administrator (**Security > Edit Teams and Workgroups**, select the **Customer Workgroup** radio button, select the **Members** tab, and then select the **Add** button.
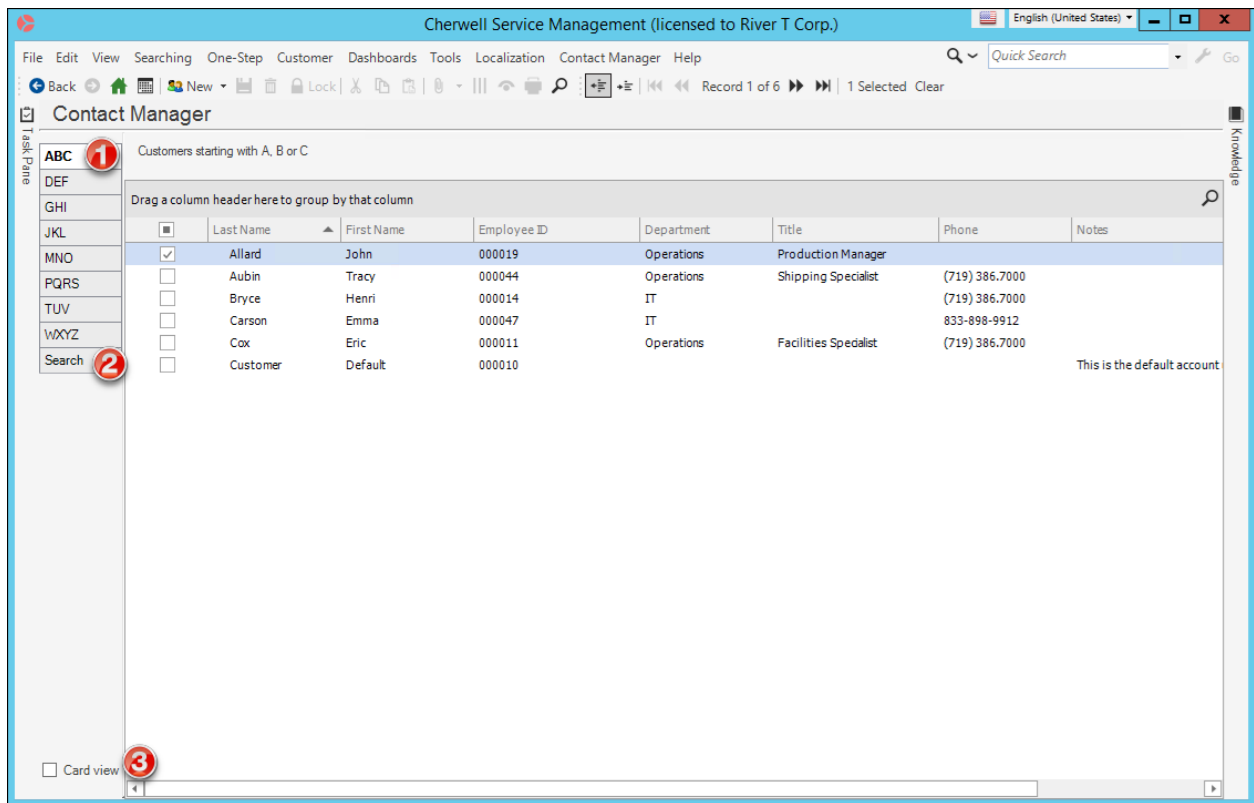
1. Tabs: View customer records, organized alphabetically by last name on lettered tabs.

2. Search: Shows/hides search and filtering options:
   - Search: Search for a specific customer record (example: Search any searchable field, such as First Name, Last Name, etc.).
   - Changed: Displays a time frame filter to refine your search (example: Anytime, Today, Previous Month, etc.).

3. Record View: Displays a Grid list or card view of customer records, or a specific customer record in detail.

Good to know:

- From the grid, you can print, export, run an Action, sort, filter, group, size, move/reorder, and add/ remove columns. Double-click a record to display it.

- See Contact Manager Behaviors for tips on working with customer records in the **Contact Manager**.

Open the Contact Manager

To open the Contact Manager:

- From the CSM Desktop Client menu bar, click **Customer>Contact Manager**.

- From the CSM Browser Client menu bar, click **Tools>Contact Manager**.

- From a Business Object record, click the **Customer Selector** button .

- From the Team and Workgroup Manager in CSM Administrator (CSM Administrator>Security>Edit Teams and Workgroups), select the **Customer Workgroup** radio button, click the **Members** tab, and then click the **Add** button.

Contact Manager Behaviors

Menu Bars and Toolbars

Use the CSM Desktop Client menu bar/toolbar and Browser Client menu bar/toolbar to access Table Management operations, such as:

- Navigating records.
- Switching between Grid view and Current Record view.
- Adding, editing, and deleting Customer Records.

Context Menu (Desktop Client Only)

Use the Contact Manager context (right-click) menu to quickly access common Contact Manager operations.

Menu Item	Description
Go to Record	Displays the selected Customer Record.
New	Creates a new Customer Record.
Delete	Deletes the selected Customer Record.
Print Grid	Prints the active Grid.
Export Grid	Exports the active Grid to a file.
Tip: If Context Menu Actions are defined, an Actions menu item is also displayed to run Actions.	

Record Views

There are several ways to view records in the Contact Manager:

- Grid list: Select the **Show Results Grid** button on the toolbar to display a Grid list of Customer Records.

- Current record: Select the **Show Current Record** button on the toolbar to display the selected Customer Record.

- Card: Select the **Card view** check box in the Navigation pane to display the Customer Records in a user-friendly business card format.

Grid Capabilities

When Contact Records are displayed in Grid view, use the CSM Grid capabilities (ex: Print, export, run an Action, sort, filter, group, size, move/reorder, and add/remove columns) to display only the data you want and in a way that is meaningful to you.

Find Records

Use the filter and search options to find Customer Records.

Create a Customer Record

Create a Customer record using the **Customer - Internal** form in the CSM Desktop Client. The Customer record stores the pertinent details and properties for the Customer, including:

- Identification information: Name, Department, Title, Manager.
- Details: Contact information, SLA level, organizational information.

Good to know:

- To save time, import Customers already stored in a Service Directory. See Import User and Customer Information Using Microsoft Active Directory.
- Department, Manager, Phone, E-mail, and SLA Subscription Level are highly recommended because some features (record ownership, One-Step Actions/Actions, Automation Processes, etc.), if configured, use them.
- SAM Account Name (a unique Microsoft® username attribute) is used for Customer information imported from Microsoft® Active Directory®.

- If configured, record ownership rights (View, Add, Edit, Delete rights) can be extended to Managers, Departments, and Teams/Workgroups. Carefully consider the implications of these relationships.

The following image shows the Customer - Internal form.

To create a Customer record:

1. From the toolbar in CSM Desktop Client or CSM Browser Client, select **New > New Customer - Internal**.

2. (Optional) In the Default Form, click the Image to add a photo or graphic to the Customer Record.

3. Select **Change Status** in the Default Form. The **Select Status** dialog box opens.

4. Select a status from the drop-down menu.

5. Click **OK**.

6. Complete the following fields in the **General** section of the Form Area:

Field	Description
First Name	(Required) Customer's first name.
Middle	Customer's middle initial.
Last Name	(Required) Customer's last name.
Employee Type	Customer's type of employment. The drop-down menu includes the following options: ◦ Contractor ◦ Full-Time ◦ Part-Time ◦ Temporary
SLA Subscription Level	Customer's Service Level Agreement subscription level.
Site Name	The name of the site where the customer is located. Use the **Related Item** button to open the **Site Selector** dialog box.
Building	The building where the customer is located. The drop-down menu offers building names dynamically based on the **Site Name** field.
Location ID	The name or number of the customer's location within the Site and Building.

7. Complete the following fields in the **Contact** section:

Field	Description
Primary Phone	Customer's primary phone number. Use the **Type** drop-down menu to select the type of phone: ◦ Home ◦ Mobile ◦ Work
Secondary Phone	Customer's secondary phone number. Use the **Type** drop-down menu to select the type of phone: ◦ Home ◦ Mobile ◦ Work
E-mail	Customer's primary email address. (Example, work email address.) If email is configured, CSM can send emails to this address. Note that Automation Processes and Actions/One-Step Actions can also use an email address.
Secondary E-mail	Customer's secondary email address. (Example, private email address.)

8. Provide organization information:

Field	Description
Department	Customer's work department.
Title	Customer's job title.
Manager	Immediate manager of the customer.
Notes	Text field to enter notes about the customer.

9. Click **Save**.

> **Note:** Unlike a User Profile, a Customer record does not store account credentials or Workgroup information. If the Customer requires a Portal login, you must also create portal login credentials to store username and password, assigned Security Group, and account details (password resets, etc.). Refer to create Portal credentials. If the Customer needs to share information with a team, you must assign the Customer to a Customer Workgroup.

The **Create an Incident** action in the **Actions List** allows you to create an Incident that is associated with the Customer. When you select **Create an Incident**, the Incident Form opens. See Create an Incident.

Related concepts
About Customers
Add Customers to the CSM Portal

Add Customers to the CSM Portal

Before customers can access the CSM Portal, you must create login credentials for them. Customer credentials are configured for customer records because it is usually a support desk task to manage customer accounts.

You can also schedule an automatic action to assign credentials on a regular basis using the Scheduling Service. This is commonly used to import customers from LDAP.

Customers can log in to the CSM Portal using assigned CSM credentials or using Windows/LDAP credentials. You must specify a supported login mode in CSM Administrator (**Security > Edit Security settings > Browser Portal**). This is intended for situations when your Active Directory users access the CSM Portal.

Create customer credentials:

- For a single customer.
- For a batch of customers.

For a batch of customers, passwords can be generated randomly and sent to each customer by email or can be assigned through Active Directory.

> **Note:** If configured, customers can access the CSM Portal anonymously using CSM's Anonymous Security Group. Anonymous customers do not require credentials, but their access is limited to the features configured for Anonymous access.

Related concepts
Create a Customer Record
Related tasks
Add a Customer to the CSM Portal
Add a Batch of Customers to the CSM Portal

Add a Customer to the CSM Portal

Use the CSM Desktop Client to create login credentials for an individual CSM Portal customer or user.

Good to know:

- Configuration is required to use Windows credentials. For more information, see Windows Credentials.
- If you provide a Windows/LDAP ID, omit the CSM login ID and password.

To create login credentials for an individual customer:

1. In the CSM Desktop Client, open the **Contact Manager** (**Customer > Contact Manager**).
2. Create or select a customer record.
3. On the menu bar, select **Customer > Portal Settings > Current Customer Credentials**. The **Portal Credentials** window opens.
4. Select the **Customer configured to use Cherwell Portal** check box to enable the customer to log in to the Portal.
5. Select a **Customer Group**. The Security Group you select controls access to CSM functionality and data. Customers have their own Security Group, called Portal Customer, in the Starter Database.
6. Provide a login ID:
   - To use CSM credentials, provide a unique login ID.
   - To use Windows credentials or LDAP credentials instead of CSM credentials, provide the **Windows Login ID**.
7. Provide a password or select the **Auto-generate a new password for this Customer** check box to have the system randomly generate a password.
8. Select the **Email customer new credential information** check box to send the customer credentials by email. Select **Edit email** to customize the text that is sent.

   > **Note:** If you randomly generate a password, select the **Email customer new credential information** check box; otherwise, there is no way for the customer to retrieve the password.

9. Define account locking and password reset options:
   - Select **Account locked** to lock an account and prevent the customer from logging in to the CSM Portal).
   - Select the **Password never expires** check box to remove password expiration for this user. This overrides any system setting to reset the password. If this option is selected, the **User must reset password at next login** and **Password reset date** settings are hidden.
   - Select **User cannot change password** to restrict a customer from changing a password. If a password reset is required, the system administrator must reset the password.
   - Select **User must reset password at next login attempt** to force a password when the customer next logs in. This is an immediate reset. Use this setting if customers forget their passwords.

◦ Select the **Password reset date** check box to prompt customers to change their password on a specific date. Then, select a reset date.

10. Select **OK**.

Related concepts

Create a Customer Record

Add Customers to the CSM Portal

Related tasks

Add a Batch of Customers to the CSM Portal

Add a Batch of Customers to the CSM Portal

Use the CSM Desktop Client to create login credentials for a batch of CSM Portal customers or users.

Good to know:

- To batch-assign both CSM and Windows credentials, you must run the batch process twice, once for standard, and once for Windows credentials.
- The easiest way to assign credentials to all customers is to open the **Contact Manager** and switch to the **Search** tab. Leave the **Search** text blank, make sure that **Changed** is set to **Any time**, and then select **Go**.
- Configuration is required to use Windows credentials. For more information, see Windows Credentials.

To create CSM Portal login credentials for a batch of customers:

1. In the CSM Desktop Client, open the **Contact Manager Customer > Contact Manager**.
2. Select a group of customers either by running a saved search or by using the **Search** tab in the **Contact Manager**.
3. Select **Customer > Portal Settings > Batch Customer Credentials**.
   The **Batch Portal Credentials** window opens.
4. From the **Field with Login ID** drop-down list, select a field that provides the value to use for each customer's login ID. The value must be unique.

   Note: For CSM credentials, this field is used as a source for the new User ID. For Windows/ LDAP credentials, this is the field that holds the customer's Windows or LDAP ID. When using Active Directory, this field is usually *SAMAccountName*. The value is combined with a domain to create the full Windows/LDAP User ID.

   Tip: If you do not have a field that contains the value that you want, consider creating a calculated field in the Customer Business Object to automatically create the value you want. For example, use First letter of First name + Last name.

5. Select a **Customer Group**. The Security Group you select controls access to CSM functionality and data. Customers have their own Security Group, called **Portal Customer**, in the Starter Database.
6. Set passwords for the customers. You have several options:
   - Select **Randomly generate a password for each customer** to generate passwords that adhere to the password setting specified in CSM Administrator. If you select this option, you must select the option to email credentials to each customer; otherwise there is no way for customers to retrieve the password.
   - Select **Set password the same for all** to provide an identical password for everyone in the group. This is typically not recommended.
   - Select **Password is value from Field** to pull the value from a field in the customer record. For example, use a phone number or office number, or use a more complex calculated field.

- Select **Set Login ID Field as Windows/LDAP Login** to authenticate customers using Windows credentials instead of CSM credentials. If the field being used to provide the credentials is fully qualified in the form of domain\user-id, that identifier is assumed to be the full Windows ID and is used as-is. However, if the field only contains the User ID, there are several options for how the system should try to determine the domain to use. The first two options are only available if customers have been imported from LDAP. When importing from Active Directory, the SAMAccountName does not usually contain the domain, and so one of the following options should be selected. If multiple options are selected, the system tries them each in order until a domain can be determined. You can then select options for determining the domain:

7. If you selected **Set Login ID Field as Windows/LDAP Login**, select the option for determining the domain:
    - **Attempt to determine domain from LDAP distinguished name**: Select this check box to have the system determine if the customer's distinguished name is stored in a field in the customer record and contains a domain that can be used.
    - **Attempt to use domain associated with LDAP customer mapping**: Select this check box to use the domain specified in the settings used to import this particular customer.
    - **Use this domain**: Select this check box, and then provide a domain name.

8. Define account locking and password reset options:
    - Select **Account locked** to lock accounts and prevent customers from logging in to the CSM Portal).
    - Select **Password never expires** to remove password expiration for the users. This overrides any system setting to reset the password. If this option is selected, the **User must reset password at next login** and **Password reset date** settings are hidden.
    - Select **User must reset password at next login attempt** to force a password when customers next log in. This is an immediate reset. Use this setting if customers forget their passwords.
    - Select the **User must reset password at next login attempt** check box to restrict customers from changing their password. If a password reset is required by the system, the system administrator must reset the password. This restarts any system administrator-scheduled password reset and is an immediate reset.
    - Select the **Password reset date** check box to prompt customers to change their password on a specific date. Then, select a reset date.

9. Select the **Email customer new credential information** check box to send the customer credentials by email. Select **Edit email** to customize the text that will be sent.

    Note: If you randomly generate a password, select the **Email customer new credential information** check box; otherwise, there is no way for the customer to retrieve the password.

10. Select **Skip customers with no email addresses** to skip assigning credentials to customers who do not have known email addresses.

11. Select **Skip customers who already have login IDs assigned** to assign credentials only to new customers. For example, to change everyone's credentials at once, clear this check box. If you add new customers or import new records from Active Directory in bulk and want to assign credentials to the newly added customers, select this check box.

12. Select **OK**.

Related concepts
Create a Customer Record
Add Customers to the CSM Portal
Related tasks
Add a Customer to the CSM Portal

Assign a Customer to a Workgroup

Use the Security Group Manager Members tab to add Customers to a Workgroup so that Customers can share CSM Items and, if configured, record ownership rights.

> **Note:** By default, Customers can share record ownership with their Customer and Manager; however, our Out-of-the-Box (OOTB) system in not configured to share with Workgroup members.

To add a Customer to a Security Group:

1. Open the Team and Workgroup Manager (CSM Administrator>Security>Edit Teams and Workgroups).

2. Select the **Customer Workgroup** radio button.

   The Manager lists the existing Workgroups.

3. Click the **Customer Workgroup** to which you want to assign a Customer (ex: Accounting)

4. Click the **Members** tab.

5. Click the **Add** button.

   The Contact Manager opens.

6. Click a **Customer** to add to the Workgroup, and then click **OK**.

7. To designate one of the members as a Workgroup manager, select a **Customer (member)**, and then select the **Customer Workgroup Manager** check box. You can designate more than one manager, if needed.

   > **Note:** If configured, record ownership rights (View, Add, Edit, Delete rights) can be extended to managers, departments, and Teams/Workgroups, so carefully consider the implications of these relationships.

8. Select **OK**.

   The Customer is added to the Workgroup.

9. Click **Save** .

Implementing Security

The steps to implement security vary depending on whether you:

- Implement the OOTB security design.
- Create a custom security design.

Steps to Implement the OOTB Security Design

CSM is shipped with an OOTB security design complete with OOTB Security Groups, OOTB Roles, OOTB Teams/Workgroups, and OOTB security settings. Complete the following steps to implement the OOTB security design.

To implement the OOTB security design:

1. Review the OOTB security design: Understand the OOTB Security Groups, Roles, and Teams/Workgroups.

2. Complete the User/Customer Worksheet to determine which Security Group and Teams/Workgroups to assign each User/Customer to.

3. Add your people:
   a. Create User Profiles: Create a User Profile for each CSM User (CSM Administrator>Security>Edit Users). During this process, you will assign each person to one Security Group, and one or more Teams.

   b. Create Customer Profiles (Customer Records): Create a Customer Record for each Customer you support (from the CSM Desktop Client toolbar, click the **New** button and select **Customer-Internal**).

      Unlike a User Profile, a Customer Record does not store account credentials or Workgroup information.

      Tip: To save time, you can import users already stored in a Directory Service (ex: Active Directory). Refer to import Users/Customers.

4. Explore Security design ideas.

5. (Optional) Configure Security: CSM provides numerous system security settings (ex: Login, authentication, inactivity, password enforcement, etc.); you can change these, if needed, but it is not required.

Security Design Ideas

CSM provides an OOTB security design to get you started. This design has Security Groups, Roles, and Teams/Workgroups. You can use this design as-is or tailor it to meet the needs of your organization. Design ideas include:

- Create new Security Groups and define specific functionality and data security rights for each.
- Define new Roles, and then assign them to Security Groups.
- Create new Teams/Workgroups, and then add Users/Customers.
- Configure the Scheduler to regularly import Active Directory data.
- Integrate with SAML.

> **Note:** Detailed step-by-step instructions for the above is beyond the scope of this document. Refer to the online help for this detailed information.

Steps to Create a Custom Security Design

Complete the following steps to create a custom security design.

🚩 **Tip:** CSM is shipped with an OOTB security design complete with OOTB Security Groups, OOTB Roles, OOTB Teams/Workgroups, and OOTB security settings. We recommend that you start with this design, and then tailor it to meet your needs.

To create a custom security design:

1. Review the OOTB security design: To understand the OOTB Security Groups, Roles, and Teams/Workgroups.
2. Design your security model:
    a. Identify which Security Groups you will need and the defined set of security rights (access to functionality and data) for each.

    b. Identify which Roles you will need.

    c. Identify which Teams/Workgroups you will need.

    🚩 **Tip:** Complete the User/Customer Worksheet to determine which Security Group and Teams/Workgroups to assign each User/Customer to.

3. Create Security Groups.
4. Create Roles.
5. Create Teams (for Users) and Workgroups (for Customers).
6. Add your people:
    ◦ Create User Profiles: Create a User Profile for each CSM User.

    ◦ Create Customer Profiles (Customer Records): Create a Customer Record for each Customer you support. If a Customer requires login access to a CSM Customer Portal, you must also create Portal login credentials.

    🚩 **Tip:** To save time, you can import Users/Customers already stored in a Directory Service (example: Active Directory®).

7. Configure Security: Configure rights to access security functionality, as well as system security settings (ex: Login, authentication, inactivity, password enforcement, etc.).

Security Worksheets

CSM provides the following worksheets to help you implement and/or design your system security:

User/Customer Worksheet

Use the following worksheet to determine to which Security Group and Teams/Workgroups each User/Customer is assigned.

Good to know:

- A User often functions as both a User and a Customer in CSM. For example, a service desk technician performs User functions but is a Customer of the HR Department. If the User is also a Customer, he must have a User Profile AND a Customer record.

- If configured, record ownership rights (View, Add, Edit, Delete rights) can be extended to managers, departments, and Teams/Workgroups, so carefully consider the implications of these relationships.

> **Important:** Our OOTB system is configured so that Users can share records with managers, departments, and Team members. However, Customers are configured to share only with managers and departments.To extend rights to Workgroup members, you must configure extended ownership rights on the records you want to share.

User/Customer Worksheet: Make applicable role selections for each person.			
Name:			
Role: User		**Role: Customer**	
Security Group	**Teams**	**Security Group**	**Workgroups**

(Select One per User) • Admin • Service Desk Manager • Service Desk Level 1 • Service Desk Security Group Level 2&3	(Select All That Apply) • 1st Level Support • 2nd Level Support • 3rd Level Support • IT Management • Knowledge Management • Reporting	(Select One per Customer) • Portal Customer • Portal Workgroup Manager	(Select All That Apply) • Accounting • Business Development • Customer Service • Design • Executive • Finance • Human Resources • Information Technology • Marketing • Office • Operations • Sales • Shipping
Example: Name: Andrew Simms			
User		**Customer**	
Security Group	**Teams**	**Security Group**	**Workgroups**
• Admin	• 2nd Level Support • Knowledge Management	• Portal Customer	• Information Technology

Directory Services Worksheet

To integrate CSM with a Directory Service, gather the information provided in this worksheet.

Account Information

Note: Search and read capability for the Directory Service account is needed.

- User name
- Password
- Domain name

Server Information

- Server operating system (example: Windows Server 2008 R2)
- Server name (example: Server-AD)
- Server long name (example: Server-1.DNS.Domain.local)
- IP address (example: 10.1.2.3)
- AD domain name (example: AD-Domain)
- RootDSE Path
- Schema path
- Search start

- **Note:** Custom filters (contact the Active Directory/LDAP administrator)

The **Map Default Object Properties** window becomes the Map LDAP/Active Directory Object window depending on which Directory Service is selected.

Managing Security

Security is managed in CSM Administrator. In CSM Administrator, Users can:

Lock/Unlock the System

Use the Lock/Unlock feature to prevent Users from logging into CSM Clients while administrative work is being done. System administrators will still be able to log in to CSM Administrator, but no Users will be able to log in to clients. Users already logged in will not be automatically logged out of the system.

> **Tip:** Use the Unlock feature to manually unlock the system if the system gets automatically locked. Automatic locking can occur, for example, during a failed Blueprint publish.

To lock/unlock the system:

1. In the CSM Administrator main window, click the **Security** category, and then click the **Lock the System** task.

   The Lock/Unlock System window opens.

2. Select the **Lock system** check box.

3. Provide a **reason** for the lockout (example: Locked for maintenance). This is displayed to any User who attempts to log in.

4. Select **OK**.

> **Note:** To unlock the system, repeat the above steps, but select the **Unlock System** check box.

Authentication Whitelist

The Authentication Whitelist includes the acceptable hosts to redirect to upon a successful login for internal CSM Web Applications (example: Portal sites).

Overview

When using the Cherwell REST API as an OAuth provider, users must maintain a whitelist of acceptable hosts to redirect to upon a successful login. Whitelisting redirect hosts is a way to prevent bad actors from hijacking the authentication flow via redirects to unsafe hosts. Separate whitelists can be maintained for each custom Cherwell REST API client, and a single whitelist will apply for each of Cherwell's internal clients (example: Portal sites). The whitelists can be managed by launching the CSM Administrator.

CSM Administrator Whitelist Manager

The Whitelist Manager can be opened from **CSM Administrator > Security > Authentication Whitelist**.

- **Client**: Select a custom Cherwell REST API client or an entry to represent all the internal Cherwell REST API clients.
- **New**: Add a new whitelisted host to the selected Client.
- **Save**: Save a new or modified whitelisted host on the selected Client.
- **Delete**: Delete a whitelisted host from the selected Client.
- **Cancel**: Cancel the changes made without saving.

Logging into the Browser Client or Portal

By default, the system will allow login redirects to the Browser Client, Portal, or other internal Cherwell clients if they are hosted on the same server as the Cherwell REST API. If they are hosted on different servers, users must add those hosts to the whitelist for internal Cherwell clients.

Using Cherwell API as an authentication provider for 3rd party applications

Some users may have 3rd party applications configured to use the Cherwell REST API as an authentication provider. If this is the case, they will have Cherwell REST API client keys defined for their applications. Users must add any hostname used by their 3rd party applications to the authentication whitelist for those clients. This will allow redirects back to those 3rd party applications to work.

View the Audit Log

Use the Security Audit log to track successful logins and logouts, and all attempted logins. This might be required in your environment for compliance reasons.

To view the Audit log:

1. In the CSM Administrator main window, select the **Security** category, and then select **Audit Log**.

   The Audit Log window opens.

2. Users can then choose from the following:
   - View: Filter the type of record audit logs you want to view by selecting one of the following (the list varies depending on which actions you select to track/log):
     - All records: Displays audit logs for all records.
     - Failed attempts: Displays audit logs for all failed login attempts.

       Note: The values in the User Name column will be blank until after successful authentication.

     - Particular application: Displays audit logs for a specified Cherwell product.
     - Particular login ID: Displays audit logs for a specified login ID.
     - Particular user: Displays audit logs for a specified User.
     - Still logged in: Displays audit logs for all Users currently logged in.
     - Successful attempts: Displays audit logs for all successful login attempts.
   - Refresh: Select this button to refresh the data in the list.
   - Configure: Select this button to select the actions to track. Select the box next to the item to track:
     - Login
     - Logout
     - Failed login attempts
   - File>Clear Log: Clears either all entries from the log or all entries earlier than a specified date. It is recommended that you regularly clear log files because the log can get very large.
   - File>Export/Print: Exports or print the audit log.

Note: Date/Time stamps in the audit log are shown in UTC (Coordinated Universal Time). If your installation is on-premises, Date/Time stamps are shown in the server time zone.

Configure the Audit Log

To configure the audit log, perform the following steps:

1. In the CSM Administrator main window, click the **Security** category, and then click the **Audit Log** task .
2. Click the **Configure** button.

   The Audit Options dialog opens.

3. Select the options you wish to track:
   ◦ **Track login**
   ◦ **Track logout**
   ◦ **Track failed login attempts**
4. Click **OK**.

View/Manage Logged-In Users/Customers

CSM Administrator provides the ability to see all users currently logged in to CSM and perform actions on them.

To view/manage logged-in users/customers:

1. In the CSM Administrator main window, select the **Security** category, and then select **View currently logged-in users**.

   The **Logged-In Users** window opens. All currently logged-in users are listed alphabetically by login ID. Customers logged into the CSM Portal will also be listed if they are using licenses. Regular customers using the CSM Portal (those not logged in) are not shown.

2. Select one or more users.
3. Select an action:
   - **Logout of module**: Logs the user(s) out of the selected Cherwell product.
   - **Logout all modules**: Logs the user(s) out of all the Cherwell products the user is currently logged in to.

     Note: If the Cherwell Service Host is running and you select this option for the user that the Cherwell Service Host is logged in as, the user will be logged back in after a few seconds. To avoid this happening, stop the Cherwell Service Host before selecting this option.

   - **Lock user out**: Locks the user(s) out of the selected module after they log out.

Configuring Security

Complete the following procedures to configure Security. Configuration procedures are completed in CSM Administrator.

To configure Security:

1. Configure System Settings security rights: Configure who can configure system settings.
2. Configure Application security rights: Configure who can access general application functionality (ex: Who can access Table Management, who can create custom toolbars etc.).
3. Configure System Security settings: Configure general security settings (default domain and anonymous login); login modes, authentication, and inactivity settings for each client; login settings for mobile applications (Cherwell Mobile); and password enforcement rules.

Configure System Security Settings

Use the **Security Settings** window in CSM Administrator (CSM Administrator> **Security > Edit System Settings**) to configure the following system security settings:

- General: Configure the default domain and anonymous login settings.
- File Access: Configure File Access Settings.
- Attachments: Configure global Attachment settings.
- Desktop Client, Browser Client, and Browser Portal: Configure login modes, authentication, and inactivity settings for each client.
- Mobile Applications: Configure login settings for Cherwell Mobile applications (whether or not to remember the User ID and password).
- Cherwell Credentials: Configure User/Customer Password rules.

Configure the Default Domain, Anonymous Login, and Lookup Table Security Settings

Use the General page in the Security Settings window (in CSM Administrator) to configure the following general system security settings for all clients:

- Default domain
- Anonymous login settings
- Lookup Table security

Configure the default domain and anonymous login settings:

1. Open CSM Administrator and select **Security > Edit security settings**.

2. Select **General**.

3. Provide the default domain name for your network. This is used any place where a domain is needed but not otherwise provided, such as automatically assigning credentials to Customers.

   Tip: Select **Arrow** (⬅) to have CSM auto-populate the name.

4. Configure anonymous login settings:
   a. **Allow Anonymous Login**: Select this check box to allow CSM Web Applications to read basic setup information from the system without User login and to enable the Anonymous Security Group access to items specifically configured for Anonymous view.

   b. **Security group when not logged in**: Select the Anonymous Security Group (OOTB: *Anonymous Browser*) that should be used by CSM Web Applications before any User/ Customer has logged in.

5. Select the **Enforce Lookup Table Security for Validated Fields** check box to require that security rights be set for validation Fields in Lookup Objects before Users and Customers can access values in those Fields. For example, if you enforce security for Lookup Tables, Users cannot see values for validated Fields on Forms and in the Query Builder unless you grant them rights to these Fields in the Lookup Tables.

   If you select this check box, be sure to review and modify Lookup Object security rights for all security groups in your system. For more information, see Define Business Object Rights (Access to Data).

6. Select **OK**.

Configure File Access Settings

Use the **File Access** page in the **Security Settings** window (in CSM Administrator) to configure the following global file access settings for any file operations (and therefore all users):

- File Types.
- Folder Access.

Configure file access settings:

1. Open CSM Administrator and select **Security > Edit security settings**.
2. Select **File Access**.
3. Select the checkbox for **Enable file access configuration**.
   The settings for **File Types** and **Folder Access** are now available.

Configure access to file types:

4. Choose one of the following options:
   - **Allow any files**: Select this option to allow CSM to access and use all files regardless of type.
   - **Only allow files with the following extensions**: Select this option to restrict CSM (and therefore its users) solely to files with specific extensions. Enter a list of file extensions separated by commas (example: .txt, .csv, .docx, .xlsx).
   - **Allow files with any extension except:** Select this option to allow CSM (and therefore its users) to access all files except for those with specific extensions
     (example: .config, .db, .mdf, .ldf). Enter a list of file extensions separated by commas.

Configure access to folders:

5. Select **Add** to enter folder paths that CSM is allowed to access (example: c:\temp, c:\data).
6. Select **OK**.

Related concepts
Configure the Default Domain, Anonymous Login, and Lookup Table Security Settings
Configure Global File Attachment Settings
Configure Cherwell Mobile Login Settings
Configure Cherwell Credential Settings (User/Customer Password Rules)
Related tasks
Configure Login, Authentication, and Inactivity Settings for Each Client

Configure Global File Attachment Settings

Use the **Attachments** page in the **Security Settings** window (in CSM Administrator) to configure Global Attachments settings, including:

- Maximum allowable file size to import, in MB.

- Which file types can be imported (example: All, explicit include list, or explicit exclude list).

Each Security Group can be configured to override the global settings.

To configure the default Attachment security settings:

1. In the CSM Administrator main window, click the **Security** category, and then click the **Edit Security Settings** task.
2. Click the **Attachments** page.
3. Select the **Limit Imported File Size** to check box to specify a maximum allowable file size to import, in MB. Then, provide the file size limit, in MB. If not selected, there is no limit and any size file can be imported.
4. Define allowable file types to be imported as attachments (select one option):
   - **Allow any files**:

     Select this option to allow all file types.

   - **Only allow files with the following extensions**:

     Select this option to import only explicit extensions. Then, provide the extensions to include (example: pdf), separated by a comma, either by typing directly in the **Extensions** box, or by selecting **Choose File Types** to open the **Select File Types** window.

   - **Allow files with any extension except**:

     Select this option to exclude explicit extensions. Then, provide the extensions to exclude, separated by a comma, either by typing directly in the **Extensions** box, or by selecting the **Choose File Types** button to open the **Select File Types** window.

    Tip: To restore the default file types, select **Restore to Cherwell defaults** .

5. Select **OK**.

Configure Login, Authentication, and Inactivity Settings for Each Client

Configure login, authentication, and inactivity settings for the CSM Desktop Client, CSM Browser Client, and CSM Portal.

By default, the Browser Client and CSM Portal use the same settings as the Desktop Client. To specify unique settings for the Browser Client and CSM Portal, clear the **Use Same Settings as Desktop Client** check box on their respective pages, and then define the unique settings.

To configure login, authentication, and inactivity settings:

1. In the CSM Administrator main window, select **Security > Edit Security Settings**.
   The **Security Settings** window opens.
2. Select the **Desktop Client** page.
3. In the **Supported login modes** area, select the login modes that you want to allow.

   > **Note:** You can enable multiple login modes so that if one authentication fails or the user or customer cancels the process, the next configured login method is invoked (SAML, then external authentication server, then LDAP, then Windows, then Internal). Not all of these options will necessarily be in your system if they have not been configured.

4. Select general login option check boxes as applicable:
   - **Display last logged-in User on Login page** (Desktop Client only). If enabled, the user ID is stored in the registry on the user's computer, which might be considered a security risk.
   - **Allow Users to have system remember last password (auto-login)** (Desktop Client only). If enabled, the password is stored in an encrypted format in the registry on the user's computer, which might be considered a security risk.
   - **Validate Windows/LDAP credentials on server**. We recommend that you configure your server to use encrypted communication before enabling this feature so that credentials are not passed to the server in a potentially sniffable format.
   - **Allow logging of authentication code (for troubleshooting)**. To assist with troubleshooting and debugging, select this option to write authentication-related messages to your log file. Log messages begin with the prefix `AuthLog`.

     > **Note:** To display authentication messages, enable logging in the Cherwell Server Manager and set the level to Info, Stats, or Debug.

5. In the **Default domain for login** field, provide a default domain to use when users log in.
6. Select **Validate credentials via external authentication server**.
7. Select **Require user to enter credentials** to require users and customers to provide their credentials each time they log in.

   > **Note:** If this option is not selected, and users and customers are on the same domain as the Cherwell Authentication Server, then the user or customer's current Windows credentials are

used to determine the person's identity. Otherwise, users and customers must provide their Windows domain/user ID and password on the login window.

8. In the **Authentication server URI** field, provide the URI (location) of the external authentication server.

> **Note:** Both client applications and the Cherwell Application Server must have access to this URL.

9. In the **Select Logout Inactive Users from Cherwell Client** area (Desktop Client only):
   ◦ Specify the minutes to wait before logging out an inactive user.
   ◦ Select the warning period to warn users before they are automatically logged out and specify the minutes before the logout to send a warning where users can select stay logged in or log out.
10. Select **OK**.

Related concepts

Configure Logging for a CSM Service, Web Application, and Cherwell REST API

Logging Options

Configure Cherwell Mobile Login Settings

Use the Mobile Apps page in the **Security Settings** window (n CSM Administrator to configure login settings for Cherwell Mobile applications (Cherwell Mobile for iOS and Cherwell Mobile for Android.

- Whether or not to store the user's Cherwell Mobile login user ID and password. When stored, those login values are saved (remembered) so that the next time the user logs in, the login Fields will be automatically populated.

- Whether or not to enable SAML.

> **Note:** Cherwell Mobile does not support Windows login mode.

To configure login settings for the Cherwell Mobile applications:

1. In the CSM Administrator main window, click the **Security** category, and then click the **Edit Security Settings** task.
2. Click the **Mobile Apps** page.
3. Select a login option for all Cherwell Mobile applications:
   ◦ **Store both User ID and Password**: Select this radio button to store the user's Login ID and password on each user's mobile device, auto-populating the login Fields.

   > **Note:** This might be considered insecure because any person who gets access to a user's mobile device will be able to view CSM data without any prompt for identity. Also, while the device stores the user ID and Password in the correct, secure manner, there are techniques for retrieving this information.

   ◦ **Store User ID, but prompt for Password**: Select this radio button to store the user's Login ID but not the password.
   ◦ **Prompt for User ID and Password**: Select this radio button to prompt for the User's Login ID and password every time they log in to a Cherwell Mobile application.
   ◦ **Allow SAML Login**: Select this check box to enable users to log into Cherwell Mobile applications using SAML.

   > **Note:** SAML is supported on Cherwell Mobile for Android, as well as Cherwell Mobile for ioS version 2.0 or greater.

4. Select **OK**.

Configure Cherwell Credential Settings (User/Customer Password Rules)

Use the Cherwell Credentials page in the Security Settings window (in CSM Administrator) to configure the following User/Customer password enforcement rules:

- Complexity
- Character length

Note: The maximum password length is 200 characters.

- Reset
- Lockout

Notes: Password resets should only be configured if (1) the User/Customer has security rights to change their password and (2) the system administrator has not prevented the User/Customer from changing their password in their User Profile/Customer Credentials. Individual Customer and User password settings can override some of these settings, if needed. User password settings are defined in the User Profile (CSM Administrator>Security category>Edit Users task); Customer password settings are defined in the Customer Credentials window (CSM Desktop Client>Customer>Portal Settings).

To configure User/Customer password enforcement rules:

1. In the CSM Administrator main window, click the **Security** category, and then click the **Edit Security Settings** task.
2. Click the **Cherwell Credentials** page.

3. Configure enforcement rules for User and Customer credentials:

   Note: The settings selected apply to individual User/Customer account creation, individual User/Customer password changes, and batch generated User/Custer credentials.

   a. Enforce Windows complexity rules: Select this check box to require that the password be complex (six (6) characters, a combination of at least three (3) of the following: uppercase letters, lowercase letters, numbers, symbols/punctuation marks, and cannot contain the User's/Customer's login ID).

      Note: If *Enforce Windows complexity rules* is selected, the minimum number of characters must be at least six (6).

   b. Enforce minimum password length: Select this check box to require that a minimum number of characters be in a password. Then, select the **minimum number of characters**.

    c. Enforce maximum password age: Select this check box to require a password reset every *x* days. Then, schedule the reset by selecting the **number of days between resets**.

    d. Days before required password change to warn customers: Select this check box to warn Users/Customers ahead of time that a password reset is required. Then, select **how many days in advance to send the warning**. Users/Customers receive daily warnings of the impending reset when they log in.

    e. Lockout Customers After *X* Failed Login Attempts: Specify the number of times Users/Customers can attempt to login using the incorrect credentials before CSM locks them out of the system.

4. Select **OK**.

Security Rights Reference

View detailed information for security rights in each category.

Security rights control access to functionality and are configured in the Security Group Manager in CSM Administrator (**Security > Edit Security Groups**).

Use the Rights tab to configure rights for different features and functions.

Good to know:

- Security design strategy is very important. Carefully consider the level of access to each scope. For more information, see the OOTB Security Design documentation.
- Manager security rights control who can access the individual CSM Item Managers and are set separately (Managers category).
- Security rights control who can access CSM functionality. The Business Object tab of the Security Groups window allows users to configure access to Business Object/field data. While a user may have access to functionality, data may not be visible without Business Object rights.

Action Block Security Rights

Action Block rights are selected from the **Category** field on the **Rights** tab (**CSM Administrator > Security > Edit Security Groups**).

Right	Description (when selected)	Grant To:
Blueprint One-Steps Action Block?	Allows people working with Action Blocks to: • Run: Run Action Blocks. • Add: Create Action Blocks. • Edit: Edit Action Blocks. • Delete: Delete Action Blocks.	View/Run Only: • Users/Customers • Managers All rights: • System administrators
Can edit Action Block Category	Allow: Allows users to add or select a category for an Action Block.	• System administrators
Global One-Steps Action Block?	Allows people working with Action Blocks to: • Run: Run Action Blocks. • Add: Create Action Blocks. • Edit: Edit Action Blocks. • Delete: Delete Action Blocks.	View/Run Only: • Users/Customers • Managers All rights: • System administrators

Application Security Rights

Application rights are selected from the **Category** drop-down list on the **Rights** tab in CSM Administrator (**Security > Edit security groups**).

Right	Description (when selected ☑)	Grant To:
Attachments? Rights are organized by scope: Blueprint, Global, Role, Site, Team, and User.	Allows people working with Attachments on Business Objects and within the Attachment Manager in CSM to: • View: Access Attachments. • Add: Create Attachments. • Edit: Edit attachments. • Delete: Delete Attachments.	View/Run Only: • Users/Customers All rights: • System administrators • Managers
Can customize Grids even if they don't support customization?	Allow: Allows selected users to customize Grids (add/remove Fields and move columns) even if the Grid does not support customization.	• System administrators • Managers • Advanced Users (Level 2 and 3 technicians)
Can customize Grids that support customization?	Allow: Allows selected users to customize Grids that support customization.	• System administrators • Managers • Users
Can import definitions from inside Managers?	Allow: Allows selected users to import definitions (.ced files) into Managers so that you can share definitions between systems.	• System administrators • Advanced Users (Level 2 and 3 technicians)
Can override the Task Pane definition?	Allow: Allows selected users to override the default Task Pane options and configure your own personal user options.	• System administrators • Managers • Advanced Users (Level 2 and 3 technicians) • Users
Can export definitions from inside Item Managers?	Allow: Allows selected users to export definitions (.ced files) into Managers so that you can share definitions between systems.	• System administrators • Advanced Users (Level 2 and 3 technicians)

Right	Description (when selected ☑)	Grant To:
Can delete all records in a group?	Allow: Allows selected users to delete all records in the current Search results group (example: All Incidents).	• System administrators
Can export data from grids?	Allow: Allows you to export data in a Grid to use CSM data in other applications for reporting or display purposes.	• System administrators • Managers • Advanced Users (Level 2 and 3 technicians)
Run application?	Allow: Allows selected users to run the Desktop Client and Browser Client.	• System administrators • Managers • Users
Can modify settings governing scaling of Business Object forms?	Allow: Allows selected users to edit the default scaling settings of Business Object forms (**Form > Scale Form**).	• System administrators • Managers • Users
Table management?	Allow: Allows selected users to access Table Management so that you can manage (create, edit, and delete) table/Field values directly from the Desktop Client.	• System administrators • Managers • Advanced Users (Level 2 and 3 technicians)
Can define custom toolbars?	Allow: Allows selected users to create personal User toolbars.	• System administrators • Managers • Advanced Users (Level 2 and 3 technicians)
Can rank Business Objects that have ranking enabled?	Allow: Allows selected users to rank records for Business Objects that have ranking enabled.	• System administrators • Managers • Users

Right	Description (when selected ✔)	Grant To:
Images? Rights are organized by scope: Blueprint, Global, Role, Site, Team, and User.	Allows people working with application images in CSM to: • View: Access images. • Add: Import images. • Edit: Edit image properties. • Delete: Delete images.	View Only: • Users/Customers All rights: • System administrators • Managers

Related concepts

Scope

Related tasks

Export a Grid in the Desktop Client

Automation Process Blueprints Security Rights

Automation Process Blueprints rights are selected from the **Category** drop-down on the **Rights** tab in CSM Administrator (**Security > Edit Security Groups**).

Right	Description (when selected ☑)	Grant To:
Create Automation Process Blueprints?	Allow: Allows selected users to create Automation Processes in CSM Administrator (Edit Automation Processes window>File>New or Edit Automation Processes window>Create New button).	• System administrators
Publish Automation Process Blueprints?	Allow: Allows selected users to publish Automation Process Blueprints in CSM Administrator (Automation Processes window>File>Publish Blueprint).	• System administrators

Automation Process Service Security Rights

Automation Process Service rights are selected from the **Category** drop-down on the **Rights** tab in CSM Administrator (**Security > Edit Security Groups**).

Right	Description (when checked ☑)	Grant To:
Enable/disable individual processes?	Allow: Allows selected users to enable or disable individual Automation Processes in CSM Administrator (Automation Process Status window and Edit Automation Process window).	• System administrators
Allow viewing of running/completed processes?	Allow: Allows selected users to view running and/or completed Automation Processes in CSM Administrator (Automation Process Status window and Edit Automation Process window).	• System administrators • Managers • Users
Check status of Automation Processes?	Allow: Allows selected users to check the status of Automation Processes (Automation Process Status window and Edit Automation Process window).	• System administrators • Managers • Users
Clear Automation Processes?	Allow: Allows selected users to clear all scheduled Automation Processes or a history of all completed Automation Processes (Automation Process Status window>File>Clear all processes).	• System administrators
Retrieve/update events from the Event Queue?	Allow: Allows API users to read/update Automation Processes in the Automation Process event queue. The account used by the Automation Process Service must have this right.	• System administrators
Pause/resume service?	Allow: Allows selected users to pause and resume the Automation Process microservice using the Pause/Resume Automation Process Service window from within CSM Administrator.	• System administrators

Browser and Mobile Device Security Rights

Browser and Mobile Device rights are selected from the **Category** drop-down list on the **Rights** tab in CSM Administrator (**Security > Edit Security Groups**).

Right	Description (when selected ☑)	Grant To:
Assign login information to groups of customers (batch)?	Allow: Allows selected users to create Portal login credentials for a batch of customers in the CSM Desktop Client (**Customer > Portal Settings > Batch Customer Credentials**).	• System administrators • Advanced users (Level 2 and 3 technicians)
Configure mobile devices? Rights are organized by scope: Global, role, and user.	Allow: Allows selected users to configure default Cherwell Mobile settings (example: Default Mobile Dashboards, Business Objects, and Actions/One-Step Actions). The default Cherwell Mobile settings (either global or role) are initially configured in CSM Administrator. If users have security rights, they can override user (personal) Cherwell Mobile settings from **Tools > Options > Dashboard Options**	• System administrators • Managers • Users
Edit Self-Service settings?	Allow: Allows selected users to edit Self-Service settings on the Browser and Mobile page in CSM Administrator.	• System administrators
Login information for customers?	Allows people working with the CSM Portal to: • View: View Portal login credentials for customers in the CSM Desktop Client (**Customer > Portal Credentials**>). • Edit: Create/edit Portal login credentials for customers in the CSM Desktop Client (**Customer > Portal Credentials**	• System administrators • Managers • Users
Portal Right 1-5 Arbitrary right that can be assigned to the Portal.	Allow: Allows selected users to set up to five (5) arbitrary rights assigned to the Portal.	• System administrators • Managers • Users

Business Hours Security Rights

Business Hours rights are selected from the Category drop-down on the Rights tab in CSM Administrator (**Security > Security Groups**).

Right	Description (when checked ☑)	Grant To:
Business Hours? Rights are organized by scope: Blueprint, Business Intelligence, global, role, team, and user. **Note:** The Business Intelligence scope is available only for Automation Processes.	Allows people working with the Business Hours Manager to: • View: Access Business Hours. • Add: Create Business Hours. • Edit: Edit Business Hours. • Delete: Delete Business Hours.	• System administrators • Managers

Calendar Security Rights

Calendar rights are selected from the **Category** drop-down on the **Rights** tab in CSM Administrator **Security > Edit Security Groups**).

Right	Description (when checked ☑)	Grant To:
Calendars? Rights are organized by scope: Blueprint, global, role, user, and team.	Allows people working with Calendars to: • View: View Calendars. • Add: Create Calendars. • Edit: Edit Calendars. • Delete: Delete Calendars.	View/Run Only: • Users • Customers All rights: • System administrators • Managers

CAM Security Rights

Security rights control access to Cherwell Asset Management (CAM) functionality and are configured in the Security Group Manager in CSM Administrator (CSM Administrator>Security>Edit Security Groups). Use the **Rights** tab to configure the following functionality rights under the CAM Administrator, CAM Purchasing, and CAM Reporting Categories.

Table 1. CAM Administration

Right	Description (when selected ☑)	Grant To:
Configure all aspects of the CAM system (CAM system administrator)?	Allows the Security Group to run CAM Administrator, Reporting, License Analytics, and Purchasing. Only users with this permission are able to do the following: • Run the Setup Wizard • Configure baselines • Reset data • Change the license key • View all panels • View and configure all tabs and options in the Options dialog box	• System administrators
Configure and manage recognized software characteristics?	Allows the Security Group to: • View the License Units, Unconfigured Applications, and Files panels • Add, delete, or modify license units • View and modify the license unit template • Automatically configure applications into license units • Mark any unconfigured applications that you don't want to configure into license units • Enable metering • Configure control profiles • Add, delete, or modify license unit groups • Organize files • Run administrative reports related to license units	• System administrators

Right	Description (when selected ☑)	Grant To:
Configure hardware assets other than computers?	Allows the Security Group to: • View the Network Devices and Other Assets panels • Discover network devices • Delete network devices • Add, delete, or modify other assets • Import asset data • View and modify the network device template • View and modify the asset template • Add, delete, or modify network device groups and asset groups • Run reports related to network devices and other assets	• System administrators
Configure managed computers and users?	Allows users to: • View the Machines and Users panels • Inventory machines • Install the CAM Agent on machines • Uninstall the CAM Agent from machines • Run remote inventory • Discover machines and users • Launch the Remote Desktop Connection • Open the Agent Options dialog box • Check licenses in and out for selected machines • Import user-defined data • Add, delete, or modify machine groups • Add, delete, or modify user groups • Delete and restore machines • Delete and restore users • Run administrative reports related to machines and users	• System administrators

Right	Description (when selected ☑)	Grant To:
Configure purchasing access profiles, orders, and contracts?	Users with Purchasing administrator permissions have full access to Purchasing and all panels and commands are available. Specifically, purchasing administrators can run Purchasing and use all functionality, including: • Use its Administration panel • Configure email notifications for access profiles • Move orders and contracts from one access profile to another	• System Administrators

Table 2. CAM Purchasing

Right	Description (when selected ☑)	Grant To:
Run the purchasing application?	Allows users to: • Run Purchasing, Reporting, and License Analytics • View orders and contracts available for the relevant access profile	• System Administrators • Managers

Table 3. CAM Reporting

Right	Description (when selected ☑)	Grant To:
Run the reports and license analytics applications?	Allows users to run Reporting and License Analytics.	• System Administrators • Managers

Chat Service Integration Features Security Rights

Chat Service Integration Features rights are selected from the **Category** drop-down list on the Rights tab in CSM Administrator (**Security > Edit Security Groups**).

Right	Description (when checked ☑)	Grant To:
Add chat session history to Business Objects?	Allow: Allows selected users to manually add a remote support session history to Business Objects using the Add Chat Session History command in the CSM Desktop Client.	• System administrators • Managers • Users/customers
Can process chat session events and create and modify Business Objects in web service?	Allow: Allows CSM to automatically process remote support session events as well as create and modify Business Objects by logging into Cherwell as a user specified in the **General** page of the Chat and Remote **Support Connector Settings** window. **Note:** This setting is for users who are configured to process BeyondTrust remote support session end notifications. If this privilege is not allowed, BeyondTrust events are ignored.	• System administrators • Managers • Users
Chat settings?	Edit: Allows selected users to edit remote support service settings in CSM Administrator (**Security > Edit Chat and Remote Support Connector Settings**).	• System administrators • Managers • Users
Request a new chat session?	Allow: Allows selected users to initiate new remote support sessions using the New Chat Session command.	• System administrators • Managers • Users/customers
Request a new device administrator session?	Allow: Allows selected users to remotely control a device using the Remotely Administer a Device command.	• System administrators • Managers • Users
Request chat service information?	Allow: Allows selected users to access information about the BeyondTrust remote support service (using the Display Chat Service Information command), such as API version information.	• System administrators • Managers • Users/customers

Command Manager Security Rights

Command Manager rights are selected from the **Category** drop-down on the **Rights** tab in CSM Administrator (**Security > Edit Security Groups**).

Right	Description (when checked ✔)	Grant To:
View Command Manager?	View: Allows selected users to access the Command Manager and select commands for use where appropriate.	• System administrators • Managers • Users

Configuration Management Security Rights

Configuration Management rights are selected from the **Category** drop-down on the **Rights** tab in CSM Administrator (**Security > Edit Security Groups**).

Right	Description (when checked ☑)	Grant To:
Device Manager?	Allows people working with the Device Manager to: • View: Access devices in the Device Manager. • Add: Create devices in the Device Manager. • Edit: Edit devices in the Device Manager. • Delete: Delete devices in the Device Manager.	View/Run Only: • Managers • Users All rights: • System administrators
Discovery Rules Manager?	Allows people working with the Discovery Rules Manager to: • View: Access the Discovery Rules Manager. • Add: Create Discovery Rules. • Edit: Edit Discovery Rules. • Delete: Delete Discovery Rules.	View/Run Only: • Managers • Users All rights: • System administrators
Run Discovery and Inventory?	Allow: Allows selected users to create a scheduled Action to run Discovery and Inventory. Otherwise, the Config Discovery and Config Inventory items do not show as Actions when scheduling an item.	• System administrators • Managers • Users

Counter Security Rights

Counter rights are selected from the **Category** drop-down on the **Rights** tab in CSM Administrator (**Security > Edit Security Groups**).

Right	Description (when checked ☑)	Grant To:
Counters? Rights are organized by scope: Blueprint, global, role, team, and user.	Allows people working with Counters to: • View: View Counters. • Add: Create Counters. • Edit: Edit (reset or change) Counters. • Delete: Delete Counters.	View/Run Only: • Managers • Users All rights: • System administrators

Dashboard Security Rights

Dashboard rights are selected from the **Category** drop-down on the **Rights** tab in CSM Administrator (**Security > Edit Security Groups**).

Right	Description (when checked ✅)	Grant To:
Dashboards? Rights are organized by scope: Blueprint, global, role, site, team, and user.	Allows people working with dashboards to: • View: View dashboards. • Add: Create dashboards. • Edit: Edit dashboards. • Delete: Delete dashboards.	View/Run Only: • Users/customers All rights: • System administrators • Managers • Advanced Users (Level 2 and 3 technicians)
Mobile Dashboards? Rights are organized by scope: Blueprint, global, role, site, team, and user.	Allows people working with mobile dashboards to: • View: View mobile dashboards. • Add: Create mobile dashboards. • Edit: Edit mobile dashboards. • Delete: Delete mobile dashboards.	View/Run Only: • Managers • Users All rights: • System administrators • Advanced Users (Level 2 and 3 technicians)
Slideshows? Slideshows are accessed from within the Dashboard Viewer. Rights are organized by scope: Blueprint, global, role, site, team, and user.	Allows people working with dashboard slideshows to: • View: Access dashboard slideshows. • Add: Create dashboard slideshows. • Edit: Edit dashboard slideshowss. • Delete: Delete dashboard slideshows.	View/Run Only: • Users All rights: • System administrators • Managers • Advanced Users (Level 2 and 3 technicians)

Right	Description (when checked ✅)	Grant To:
Widgets? Rights are organized by scope: Blueprint, global, role, site, team, and user.	Allows people working with widgets to: • View: Access widgets. • Add: Create widgets. • Edit: Edit widgets. • Delete: Delete widgets.	View/Run Only: • Users/customers View/Run/Add/Edit Only: • Managers • Advanced users (Level 2 and 3 technicians) All rights: • System administrators
Can set a default Dashboard Theme?	Allow: Allows selected users to select a default theme for all dashboards.	• System administrators • Managers • Users

Database Options Security Rights

Database rights are selected from the **Category** drop-down on the **Rights** tab in CSM Administrator (**Security > Edit Security Groups**).

Right	Description (when checked ☑)	Grant to:
Allow system restore?	Allow: Allows selected users to perform a system restore on the database.	• System administrators
Database transaction log settings?	Allow: Allows selected users to view and edit the Database Transaction Log settings in the Tools>Options window of a Blueprint.	• System administrators
Export system data?	Allow: Allows selected users to export system data from the database.	• System administrators
Import data from CSV files?	Allow: Allows selected users to import data from .csv files into CSM.	• System administrators
Perform maintenance on the database?	Allow: Allows selected users to perform maintenance on the database.	• System administrators
Saved import definitions?	Allows people working with .csv import definitions to: • Run: Create and run imported definitions stored on the system. • Delete: Delete import definitions.	• System administrators

Database Server Objects Security Rights

Database Server Objects rights are selected from the **Category** drop-down on the **Rights** tab in CSM Administrator (**Security > Edit Security Groups**).

Right	Description (when checked ☑)	Grant to:
Database server object management?	Allows people working with Database Server Objects (triggers, views, and stored procedures) in CSM Administrator to: • View: Access Database Server Objects. • Add: Create Database Server Objects. • Edit: Edit Database Server Objects. • Delete: Delete Database Server Objects. **Note:** All Database Server Management operations take place within a Blueprint and are not available for SaaS users.	• System administrators

Directory Service (LDAP) Security Rights

Directory Service (LDAP) rights are selected from the **Category** drop-down on the **Rights** tab in CSM Administrator (**Security > Edit Security Groups**).

Right	Description (when checked ✅)	Grant To:
Associate LDAP Groups with Security Groups?	Allow: Allows selected users to associate LDAP Groups with Security Groups in order to allow users to log in to CSM using LDAP authentication.	• System administrators
Change LDAP settings?	Allow: Allows selected users to configure/edit directory service settings. **Note:** Directory services in the Tools menu of a Blueprint cannot be accessed without this right.	• System administrators
Import LDAP data into Business Objects?	Allow: Allows selected users to import Customer data into Business Objects rather than manually inputting it. **Note:** The Import from Active Directory task in the Database category in CSM Administrator cannot be accessed without this right.	• System administrators
Import LDAP Users?	Allow: Allows selected users to import user data into the User Information Business Object.	• System administrators
Map Business Objects to LDAP objects?	Allow: Allows selected users to map Business Objects to LDAP objects so that directory service data can be imported into CSM Business Objects.	• System administrators

Document Repository Items Security Rights

Document Repository Items rights are selected from the **Category** drop-down on the **Rights** tab in CSM Administrator (**Security > Edit Security Groups**).

Right	Description (when checked ☑)	Grant To:
Default rights?	Allows users working with Document Repository Items in the CSM Desktop and Browser Clients to: • View: Access Document Repository Items. • Add: Create Document Repository Items. • Edit: Edit Document Repository Items. • Delete: Delete Document Repository Items. The default Document Repository rights will be applied to any Document Repository that does not have specific rights set (which can be determined by the **Use default** checkbox for each repository).	View/Run Only: • Users All rights: • System administrators • Managers
Default Portal Documents (for each defined Document Repository)?	Allows people working with the default documents in the Document Repository in the CSM Portal to: • View: Access documents. • Add: Create documents. • Edit: Edit documents. • Delete: Delete documents. • Use Default: Uses the same security rights set for the Default Sites rights (above). **Note:** For each Document Repository, you can also define Expressions that limit access. For example, you can limit add/edit rights to a particular Repository based on whether the Team Lead checkbox is checked on the customer's record. The type of Expression (user or customer) will differ depending on the type of security group.	View/Run Only: • Users/customers All rights: • System administrators • Managers

Document Repository Manager Security Rights

Document Repository Manager rights are selected from the **Category** drop-down on the **Rights** tab in CSM Administrator (**Security > Edit Security Groups**).

Right	Description (when checked ☑)	Grant To:
Document Repository Manager?	Allows people working with the Document Repository Manager: • View: Access the Document Repository Manager. • Add: Create items in the Document Repository Manager. • Edit: Edit items in the Document Repository Manager. • Delete: Delete items from the Document Repository Manager.	View/Run Only: • Users All rights: • System administrators • Managers

E-mail and Event Monitor Security Rights

E-mail and Event Monitor rights are selected from the **Category** drop-down on the **Rights** tab in CSM Administrator (**Security > Edit Security Groups**).

Right	Description (when checked ☑)	Grant To:
Allow to import emailmonitor.ini?	Allow: Allows selected users to import an emailmonitor.ini file using the E-mail and Event Monitoring Manager. This feature has been deprecated.	• System administrators
E-mail and Event Monitor item management?	Allows people working with e-mail monitors in the E-mail and Event Monitoring Manager in CSM Administrator to: • View: Access Monitors. • Add: Create Monitors. • Edit: Edit Monitors. • Delete: Delete Monitors.	View/Run Only: • Managers All rights: • System administrators • Advanced users (Level 2 and 3 technicians)
Pause/resume the E-mail and Event monitor?	Allow: Allows selected users to pause or resume the E-mail and Event Monitoring microservice using the pause/resume task in CSM Administrator (E-mail and Event Monitoring>Pause/Resume Monitoring).	• System administrators

Email Security Rights

Security rights control access to CSM functionality and are configured in the Security Group Manager in CSM Administrator (**Security > Edit Security Groups**). Use the **Rights** tab to configure the following functionality rights.

Right	Description (when checked)	Grant To:
Can override server and account settings on locked accounts?	Allow: Allows selected users to override the email account server settings and account information for a global account configured in CSM Administrator (example: Allows users in CSM to override the global account settings configured in CSM Administrator, even if the padlock is set to locked in the server and account information sections).	• System administrators
Can send email from the system?	Allow: Allows selected users to send emails from within the system. This includes emails sent through One-Step Actions as well as those sent directly from the CSM clients.	• System administrators • Managers • Users
Can add user email accounts?	Allow: Allows selected users to add and personalize your own email account and settings.	• System administrators • Managers • Advanced users (Level 2 and 3 technicians)
Can email teams?	Allow: Allows selected users to email teams (example: IT Service Desk Level 1).	• System administrators • Managers • Users
Can administrate email credentials?	Allow: Allows selected users to create and edit email credentials using the Email Credentials Manager or the Email Options dialog.	• System administrators
Can administrate global email settings?	Allow: Allows selected users to configure global email accounts in CSM Administrator.	• System administrators
Can email workgroups?	Allow: Allows selected users to email CSM workgroups.	• System administrators • Managers • Users

Right	Description (when checked)	Grant To:
Show teams in address book?	Allow: Allows selected users to view and select CSM teams in the CSM address book.	• System administrators • Managers • Users
Show the address book?	Allow: Allows selected users to access and use the CSM address book.	• System administrators • Managers • Users
Show workgroups in address book?	Allow: Allows selected users to view and select CSM workgroups in the CSM address book.	• System administrators • Managers • Users
Can specify arbitrary FROM addresses even if not allowed for users?	Allow: Allows selected users to specify arbitrary From addresses even if this option has been disabled for users	• System administrators

External Data Options Security Rights

External Data Options rights are selected from the **Category** drop-down on the **Rights** tab in CSM Administrator (**Security > Edit Security Groups**).

Right	Description (when checked ☑)	Grant to:
Create connections to external data?	Allows selected users to link to external data from CSM Administrator.	• System administrators
Import external data?	Allows selected users to import external data using CSM Administrator into a CSM database.	• System administrators

HTML Pages Security Rights

HTML pages rights are selected from the **Category** drop-down on the **Rights** tab in CSM Administrator (**Security > Edit Security Groups**).

Right	Description (when checked ☑)	Grant To:
HTML pages? Rights are organized by scope: Blueprint, global, role, site, team, and user.	Allows people working with HTML pages in the CSM Browser Client and Portal to: • View: Access HTML pages. Allows users working with HTML pages in CSM Administrator to: • Add: Create HTML pages. • Edit: Edit HTML pages. • Delete: Delete HTML pages.	View/Run Only: • Users/customers All rights: • System administrators • Managers

Knowledge Security Rights

Use CSM Administrator Security Groups to define Knowledge Security Rights.

You can view Knowledge Security Group Rights in CSM Administrator > **Security > Edit Security Groups**. Select the **Group** from the drop-down list and select the **Rights** tab. In the **Category** drop-down list, select **Knowledge**. See Configure Knowledge Security Group Permissions for specific steps on how to configure Security Group permissions for Knowledge.

The following are suggested settings for Knowledge Security Rights using the default Security Groups:

Right	Description (when selected ☑)	Grant To (Default Security Groups):
Change Knowledge Search options?	Allow: Allows selected Users to change Knowledge Search options in the CSM Desktop Client from the default options to either expand or limit the search as necessary.	• Admin • IT Service Desk Level 2 & 3 • IT Service Desk Manager • Knowledge Manager • Service Desk - KM Tier 1
Import Knowledge?	Allow: Allows selected to import Knowledge using third-party Knowledge bases through the Knowledge Import Wizard.	• Admin • IT Service Desk Level 2 & 3 • Knowledge Manager
Knowledge mapping?	Allows people working with Knowledge Mapping in CSM Administrator (Settings>Knowledge Mapping) to: • View: Access the Knowledge Mapping window. • Add: Add Knowledge Sources to a specified type of search (ex: General search) using the Knowledge Mapping window. • Edit: Edit Knowledge Sources for a specified type of search (ex: General search) using the Knowledge Mapping window. • Delete: Remove Knowledge Sources from a specified type of search (ex: General search) using the Knowledge Mapping window.	View/Run Only: • IT Service Desk Level 1 • IT Service Desk Level 2 & 3 • Service Desk - KM Tier 1 View/Add/Edit: • Knowledge Manager View/Add/Edit/Delete: • Admin

Right	Description (when selected ✔)	Grant To (Default Security Groups):
Knowledge sources?	Allows people working with Knowledge Sources in CSM Administrator (Settings>Knowledge Sources) to: • View: Access Knowledge Source Manager. • Add: Create Knowledge Sources using the Knowledge Source Manager. • Edit: Edit Knowledge Sources using the Knowledge Source Manager. • Delete: Delete Knowledge Sources using the Knowledge Source Manager.	View/Run Only: • IT Service Desk Level 1 • IT Service Desk Level 2 & 3 • Service Desk - KM Tier 1 View/Add/Edit: • Knowledge Manager View/Add/Edit/Delete: • Admin

Manager Security Rights

Manager rights are selected from the **Category** drop-down on the **Rights** tab in CSM Administrator (**Security > Edit Security Groups**).

Right	Description (when selected ☑)	Grant To:
Can pin/unpin items from all users' pinboards?	Allow: Allows you to pin or unpin an item to/from all users' pinboards (example: Pinning a new dashboard to all users' pinboards for easy access).	• System administrators
Can pin/unpin items from any role pinboard?	Allow: Allows you to pin or unpin an item to/from any role's pinboard (example: Pinning a report to any role's pinboard for easy access).	• System administrators
Can pin/unpin items from current role pinboard?	Allow: Allows you to pin or unpin an item to/from the pinboards of all users in the current user's role (example: Pinning a One-Step Action to all users' pinboards within the currently logged-in role so that they can run the same One-Step Action).	• System administrators • Managers
Can view items in Managers for all users?	Allow: Allows you to view items in the Managers for all users. Normally, you can only edit items in a Manager for your current role. When this right is set, you can edit items for any role.	• System administrators
Can view items in Managers for all Sites?	Allow: Allows you to view items in the Managers for all Sites. Normally, you can only edit items in a Manager for your current role. When this right is set, you can edit items for any role.	• System administrators
Can view items in Managers for all Customer Workgroups?	Allow: Allows you to view items in the Managers for all customer workgroups. Normally, you can only edit items in a Manager for your current role. When this right is set, you can edit items for any role.	• System administrators

Right	Description (when selected ☑)	Grant To:
Can view items in Managers for all roles?	Allow: Allows you to view items in the Managers for all roles. Normally, you can only edit items in a Manager for your current role. When this right is set, you can edit items for any role.	• System administrators
Can view items in Managers for all Teams?	Allow: Allows you to view items in the Managers for all Teams. Normally, you can only edit items in a Manager for your current role. When this right is set, you can edit items for any role.	• System administrators

Mergeable Applications (mApps) Security Rights

mApps rights are selected from the Category drop-down on the Rights tab (CSM Administrator>Security>Edit Security Groups).

Right	Description (when checked ✔)	Grant To:
Create mApp Solutions?	Allow: Allows selected Users to create mApp Solutions.	• System administrators
Apply mApp Solutions?	Allow: Allows selected Users to apply mApp Solutions.	• System administrators
View installed mApp Solutions?	Allow: Allows selected Users to view a list of mApp Solutions that have already been installed on a CSM system.	• System administrators
View mApp Solutions development history?	Allow: Allows selected Users to view available history records for all definitions within a CSM system that were modified by a mApp Solution.	• System administrators

Metrics Security Rights

Metrics rights are selected from the Category drop-down on the Rights tab (CSM Administrator>Security>Edit Security Groups).

Right	Description (when checked ☑)	Grant To:
Metrics? Rights are organized by scope: Blueprint, Global, Role, Team, and User.	Allows people working with Metrics to: • View: View Metrics. • Add: Create Metrics. • Edit: Edit Metrics. • Delete: Delete Metrics.	View/Run Only: • Users All rights: • System administrators • Managers

Prompts Security Rights

Prompt rights are selected from the Category drop-down on the Rights tab (CSM Administrator>Security>Edit Security Groups).

Right	Description (when checked ✔)	Grant To:
Prompts? Rights are organized by scope: Blueprint, Global, Role, Team, and User.	Allows people working with Prompts to: • View: View Prompts. • Add: Create Prompts. • Edit: Edit Prompts. • Delete: Delete Prompts.	View/Run Only: • Users • Customers All rights: • System administrators • Managers

One-Step Security Rights

One-Step rights are selected from the Category drop-down on the Rights tab (CSM Administrator>Security>Edit Security Groups).

Right	Description (when selected)	Grant To:
One-Step Actions? Rights are organized by scope: Blueprint, Business Intelligence, Global, Role, Site, Team, and User. **Note:** The Business Intelligence scope is available only for Automation Processes.	Allows people working with One-Step Actions to: • Run: Run One-Step Actions. • Add: Create One-Step Actions. • Edit: Edit One-Step Actions. • Delete: Delete One-Step Actions. For the Site scope, the following additional options are available: • Run other Users: Run Site One-Step Actions (from the One-Step Action Manager) that were created by other Users. • Add other Sites: Create One-Step Actions for Sites that belong to other Security Groups. • Edit other Sites: Edit One-Step Actions for Sites that belong to other Security Groups. • Delete other Sites: Delete One-Step Actions for Sites that belong to other Security Groups.	View/Run Only: • Users/Customers • Managers All rights: • System administrators
Can configure One-Step Actions to run through a Trusted Agent?	Allow: Allows Users to configure One-Step Actions to run on a remote network using Trusted Agents. This right controls the configuration of One-Step Actions with Trusted Agents, but does not control a User's ability to view or run One-Step Actions configured to use Trusted Agents.	• System administrators
Can edit One-Step Actions set to explicitly run under any Security Group?	Allow: Allows Users to edit One-Step Actions, regardless of the Security Group they are configured to run under.	• System administrators

Right	Description (when selected)	Grant To:
Can edit One-Step Actions set to explicitly run under this Security Group?	Allow: Allows Users to edit One-Step Actions if their Security Group is the same as the Security Group the One-Step Actions are configured to run under.	• System administrators • Managers • Users
Can set One-Step Actions to run under any Security Group?	Allow: Allows Users who create and edit One-Step Actions to select any Security Group for One-Step Actions to run under.	• System administrators
Can set One-Step Actions to run under this Security Group?	Allow: Allows Users who create and edit One-Step Actions to select only their current Security Group for One-Step Actions to run under.	• System administrators • Managers • Users
Can a User work with the Web Service One-Step Action Action?	Allows people working with Web Service One-Step Action Actions to: • View: Access Web Service One-Step Action Actions. • Add: Create Web Service One-Step Action Actions. • Edit: Edit Web Service One-Step Action Actions. • Delete: Delete Web Service One-Step Action Actions. **Note:** The ability to set up and use web services also requires security rights.	View/Add/Edit Only: • Advanced Users (Level 2 and 3 technicians) All rights: • System administrators
One-Step Actions can access values for fields for which the Security Group doesn't have rights?	Allow: Allows One-Step Actions to access values for Fields even if the Security Group the One-Step Action is configured to run under does not have rights to the Field values.	• System administrators
Run One-Step Actions for groups?	Allow: Allows you to run One-Step Actions against groups of records.	• System administrators • Managers

Outlook Integration Security Rights

Outlook Integration rights are selected from the Category drop-down on the Rights tab (CSM Administrator>Security>Edit Security Groups).

Right	Description (when checked ☑)	Grant To:
Can set the default configurations for the system and for Roles?	Allow: Allows selected Users to configure default Outlook Integration Configurations for all Users and/or for each Role.	• System administrators
Can a User run the Outlook integration?	Allow: Allows selected Users to run the Outlook Add-In within Microsoft Outlook.	• System administrators • Managers • Users
Outlook integration item management?	Allows people working with the Outlook Integration Manager to: • View: Access Outlook Integration Configurations. • Add: Add Outlook Integration Configurations. • Edit: Edit Outlook Integration Configurations. • Delete: Delete Outlook Integration Configurations.	View/Add/Edit Only: • Users • Managers All rights: • System administrators

Queues Security Rights

Queues rights are selected from the Category drop-down on the Rights tab (CSM Administrator>Security>Edit Security Groups).

Right	Description (when checked ✅)	Grant To:
Queue Manager? Rights are organized by scope: Blueprint, Global, Role, Team, and User.	Allows people working with the Queue Manager in the CSM Desktop Client (Tools>Queues>Queue Manager) to: • Open: Open the Queue Manager. • Add: Create Queues using the Queue Manager. • Edit: Edit Queues using the Queue Manager. • Delete: Delete Queues using the Queue Manager.	View/Run Only: • Users • Managers All rights: • System administrators
Queues - remove items? Rights are organized by scope: Blueprint, Global, Role, Team, and User.	Allow: Allows selected Users to remove items from the Queues of the specified scope.	• System administrators • Managers • Users
Queues - suspend/unsuspended items? Rights are organized by scope: Blueprint, Global, Role, Team, and User.	Allow: Allows selected Users to suspend/unsuspend records in the Queue for the scope.	• System administrators • Managers • Users
Can remove items from other User's Queues?	Allow: Allows selected Users to remove items from another User's Queue.	• System administrators • Managers • Advanced Users (Level 2 and 3 technicians)
User Queue settings?	Allow: Allows selected Users to define User Queue settings in CSM Administrator (Settings>Edit user queue settings).	• System administrators • Managers

Record Locking Security Rights

Record Locking rights are selected from the **Category** drop-down on the **Rights** tab in CSM Administrator(**Security > Edit Security Groups**).

Right	Description (when checked ☑)	Grant To:
Can edit record locking settings?	Allow: Allows selected users to configure the Record Locking settings in CSM Administrator to control how record locking behaves globally or per Business Object.	• System Administrators
Global User lock list?	Allows users working with the **Global Record Locking Manager** in CSM Administrator to: • View: View Global locks (all locked records for all users). • Delete: Unlock records (all locked records for all users).	• System Administrators

Reports Security Rights

Reports rights are selected from the Category drop-down on the Rights tab (CSM Administrator>Security>Edit Security Groups).

Right	Description (when checked ☑)	Grant To:
Report styles? Rights are organized by scope: Blueprint, Global, Role, Team, and User.	Allows people working with Report styles in CSM Desktop to: • View: Access Report styles. • Add: Create Report styles. • Edit: Edit Report styles. • Delete: Delete Report styles.	View/Run Only: • Users • Managers All rights: • System administrators
Report can be run against all records in a system?	Allows people working with Reports to create a Report that uses all records in the system to generate the new Report in the Cherwell Report Wizard. **Note:** This is not recommended as there is no way to tell how many records a table will have upon generating the Report.	• Users • Managers • System administrators
Reports? Rights are organized by scope: Blueprint, Global, Role, Team, and User.	Allows people working with Reports in the CSM Desktop Client, Browser Client, and Customer Portal to: • View: Access Reports. • Run: Run Reports. • Edit: Edit Reports. • Delete: Delete Reports.	View/Run Only: • Users/Customers • Managers All rights: • Advanced Users (Level 2 and 3 technicians) • System administrators

Scheduler Security Rights

Scheduler rights are selected from the Category drop-down on the Rights tab (CSM Administrator>Security>Edit Security Groups).

Right	Description (when checked ✅)	Grant To:
Edit Scheduled Items?	Allow: Allows selected Users to edit Scheduled Items (example: Scheduled imports or reports).	• System administrators
Pause/resume scheduling service?	Allow: Allows selected Users to pause and resume Scheduling microservice processing from CSM Administrator. **Note:** The scheduling process will still run, but no Scheduled Items will execute if processing is paused.	• System administrators

Searches Security Rights

Searches rights are selected from the Category drop-down on the Rights tab (CSM Administrator>Security>Edit Security Groups).

Right	Description (when selected)	Grant To:
Can access the Quick Search Builder?	Allow: Allows selected Users to access to: • Quick Search Query Builder • Edit Current Search menu option • Save Current Search as menu option • Open Advanced Editor • Filters menu option (available on filtered Search results) **Tip:** Grant this right to disable Quick Search features at all levels. You can then use **Perform Searches** rights to enable Quick Search features at various levels. For example, you can grant Add rights to enable Users to create Quick Searches for specific Roles.	• System administrators • Managers • Users
Can edit searches that reference fields to which the User doesn't have rights.	Allow: Allows selected Users to edit Searches that reference Fields which they do not have rights to access. Users cannot view restricted Fields, but Searches can use them to retrieve data.	• System administrators • Managers • Users
Can run searches that reference fields to which the User doesn't have rights.	Allow: Allows selected Users to run Searches that reference Fields which they do not have rights to access. Users cannot view restricted Fields, but Searches can use them to retrieve data.	• System administrators • Managers • Users
Change Full-Text Search options?	Allow: Allows selected Users to change Full-Text Search options for Business Objects and Fields.	• System administrators

Right	Description (when selected)	Grant To:
Perform Searches? Rights are organized by scope: Blueprint, Global, Role, Site, and Business Intelligence. **Note:** The Business Intelligence scope is available only for Automation Processes.	Allows people working with Searches in the CSM Desktop Client (Searching>Search Manager) to: • Run: Run Searches. • Add: Create Searches. • Edit: Edit Searches. • Delete: Delete Searches.	View/Run/Add/Edit Only: • Users/Customers • Managers All rights: • System administrators
Perform Full-Text Search?	Allow: Allows selected Users to run a Full-Text Search.	• System administrators • Managers • Users/Customers

Security Features Security Rights

Security Features rights are selected from the Category drop-down on the Rights tab in CSM Administrator (**Security > Edit Security Groups**).

Right	Description (when selected ☑)	Grant To:
Advanced system settings?	Edit: Allows selected users to edit advanced system settings.	• System administrators
Audit log?	Allows people working with the audit log in CSM Administrator to: • View: Access the audit log. • Edit: Edit audit log settings. • Delete: Delete entries from the audit log.	• System administrators
Credential Management?	Allows people working with credentials in CSM Administrator to: • View: Access credentials. • Add: Create credentials. • Edit: Edit existing credentials. • Delete: Delete credentials.	View/Run Only: • Users • Managers All rights: • System administrators
In a Portal, can request a license to edit records owned by other users?	Allow: Allows selected users to request a license to edit records owned by other users.	• Managers
License products?	Allow: Allows selected users to provide Cherwell licenses into the system.	• System administrators
Lock system so users cannot log in?	Allow: Allows selected users to lock the CSM system so that users cannot log in (ex: During scheduled maintenance).	• System administrators
Publish log?	Allows people working with Blueprint publish logs to: • View: Access logs in order to publish. • Delete: Deletes previous publish logs.	• System administrators

Right	Description (when selected ☑)	Grant To:
REST API client management?	Allows users working with Rest API client keys to: • View: Access client keys. • Add: Create client keys. • Edit: Modify client key settings. • Delete: Delete client keys.	• System administrators
Role management?	Allows people working with roles to: • View: Access roles. • Add: Add roles. • Edit: Edit existing roles. • Delete: Delete roles.	• System administrators
Run the Administrator tool?	Allow: Allows selected users to run the CSM Administrator.	• System administrators
SAML Cherwell Service Provider settings?	Edit: Allows selected users to edit the service provider settings to configure CSM as a SAML Service Provider.	• System administrators
SAML Identity Provider settings?	Edit: Allows users to edit the identity provider settings to configure the SAML Identity Provider.	• System administrators
Security group management?	Allows people working with Security Groups in CSM Administrator to: • View: Access Security Groups. • Add: Add Security Groups. • Edit: Edit existing Security Groups. • Delete: Delete Security Groups.	• System administrators
Security settings?	Allows people working with Security settings in CSM Administrator to: • View: Access the Security settings. • Edit: Edit the Security settings.	• System administrators

Right	Description (when selected ✔)	Grant To:
System settings?	Edit: Allows selected users to edit default system settings in CSM Administrator.	• System administrators
Team management?	Allows people working with Teams in CSM Administrator to: • View: Access Teams. • Add: Add Teams. • Edit: Edit existing Teams. • Delete: Delete Teams.	• System administrators
Twitter Account Management?	Allows people working with their Twitter account in CSM Administrator and the Desktop Client to: • View: Access affiliated Twitter accounts. • Add: Add Twitter accounts. • Edit: Edit existing Twitter accounts. • Delete: Delete Twitter accounts.	View/Add/Edit Only: • Advanced users (Level 2 and 3 technicians) • Managers All rights: • System administrators
Unlock a system that has been locked?	Allow: Allows selected users to unlock a system that has been locked.	• System administrators
View logged-in users?	View: Allows selected users to view logged-in users.	• System administrators • Managers

Sites Security Rights

Sites rights are selected from the Category drop-down on the Rights tab (CSM Administrator>Security>Edit Security Groups).

View rights are only used for Sites that require login.

Right	Description (when checked ☑)	Grant To:
Default rights?	View: The default view rights assigned to any site when the security group does not explicitly specify view rights. **Note:** This does not apply to sites that do not require a login (anonymous sites and browsers).	Customers
For each defined Site (ex: CompanyHomepage)?	Allows Customers working in the CSM Portal to: • View: View the Site. • Use Default: Uses the same security rights set for the Default Sites rights (above). **Note:** This can also be conditional upon information in the Customer's record. For example, access can be limited to only full-time employees.	Customers

Sites Manager Security Rights

Sites Manager rights are selected from the Category drop-down on the Rights tab (CSM Administrator>Security>Edit Security Groups).

Right	Description (when checked ☑)	Grant To:
Sites Manager?	Allows people working with the Sites Manager: • View: Access the Sites Manager. • Add: Create items in the Sites Manager. • Edit: Edit items in the Sites Manager. • Delete: Delete items from the Sites Manager.	• System administrators

Stored Expressions Security Rights

Stored Expressions rights are selected from the Category drop-down on the Rights tab (CSM Administrator>Security>Edit Security Groups).

Right	Description (when checked ☑)	Grant To:
Stored Expressions? Rights are organized by scope: Global, Role, and User.	Allows people working with Stored Expressions in CSM Administrator and the Desktop Client to: • View: Access and use Stored Expressions. • Add: Create Stored Expressions. • Edit: Edit Stored Expressions. • Delete: Delete Stored Expressions.	• System administrators • Managers • Advanced Users (Level 2 and 3 technicians)
Notes:		

Stored Values Security Rights

Stored Values rights are selected from the Category drop-down on the Rights tab (CSM Administrator>Security>Edit Security Groups).

Right	Description (when checked ✅)	Grant To:
Stored Values? Rights are organized by scope: Global, Role, Team, and User.	Allows people working with Stored Values in CSM to: • View: Access and use Stored Values. • Add: Create Stored Values. • Edit: Edit Stored Values. • Delete: Delete Stored Values.	• System administrators • Managers • Users

System Blueprints Security Rights

System Blueprints rights are selected from the Category drop-down on the Rights tab (CSM Administrator>Security>Edit Security Groups).

Right	Description (when checked ☑)	Grant To:
Create System Blueprints?	Allow: Allows selected Users to create System Blueprints in CSM Administrator.	• System administrators
View details of current Field when in application?	Allow: Allows selected Users to view the details of the current Field in CSM Administrator.	• System administrators • Advanced Users (Level 2 and 3 technicians)
Publish System Blueprints?	Allow: Allows selected Users to publish System Blueprints in CSM Administrator.	• System administrators

System Settings Security Rights

System settings rights are selected from the **Category** drop-down on the **Rights** tab in CSM Administrator (**Security > Security Groups**).

Right	Description (when selected ☑)	Grant To:
Can choose a custom form when configuring the Create New Command from the Command Selector?	Allow: Allows selected users to choose a custom form when configuring the Create New Command from the Command Selector. Example: When creating Portal menus, users can define a Create New command that runs a One-Step Action before or after creating the object and also have an alternate form be displayed instead of the main form. This is useful to create a custom New Incident form that is different for different types of requests.	• System administrators
Can clear role settings?	Allow: Allows selected users to clear settings and remembered information (example: toolbar and window positions) for a particular role or all roles in CSM Administrator.	• System administrators • Managers • Users
Can configure definition for custom toolbars for roles?	Allow: Allows selected users to create custom toolbars for roles.	• System administrators • Managers
Can configure definition for Task Panes for roles?	Allow: Allows selected users to create custom Task Panes for roles.	• System administrators • Managers
Can configure global definition for custom toolbars?	Allow: Allows selected users to create Global toolbars.	• System administrators • Managers
Can configure global definition for Task Panes?	Allow: Allows selected users to create Global Task Panes.	• System administrators

Right	Description (when selected ☑)	Grant To:
Group maps?	Allows people working with Group Maps in CSM Administrator? to: • View: Access Group Maps. • Add: Create Group Maps. • Edit: Edit existing Group Maps. • Delete: Delete Group Maps.	• System administrators
Stored Field formats?	Allows people working with Stored Field formats (example: Telephone numbers, zip codes) in CSM Administrator to: • View: Access Stored Field formats. • Add: Add Stored Fields? • Edit: Edit existing Stored Field formats? • Delete: Delete Stored Field formats?	• System administrators
Views?	Allows people working with the View Manager to: • View: Access the View Manager. • Add: Create Views. • Edit: Edit Views. • Delete: Delete Views.	• System administrators

Theme Security Rights

Themes rights are selected from the Category drop-down on the Rights tab (CSM Administrator>Security>Edit Security Groups).

Right	Description (when checked ☑)	Grant To:
Theme management?	Allows people working with the Theme Manager in CSM Administrator (Create a Blueprint>Managers>Themes) to: • View: Access the Theme Manager. • Add: Create Themes. • Edit: Edit Themes. • Delete: Delete Themes.	• System administrators

Third-party Chat Integration Security Rights

Third-party chat integration rights are granted from the **Category** drop-down on the **Rights** tab (**CSM Administrator > Security > Edit Security Groups**.

Right	Description (when selected ☑)	Grant to:
Can manage chat settings?	**Allow**: Allows users to edit chat configuration settings in CSM Administrator.	System administrators.
Chat conversations?	• **View**: Allows users to view existing chat conversations. • **Add**: Allows users to add existing chat conversations.	Users who will participate in existing chat conversations.
Create new chat?	**Allow**: Allows users to create a new chat conversation or channel and add other users to the conversation.	Users who will create new chat conversations.
Store chat history?	**Allow**: Allows users to store conversations in Business Object records.	Users who participate in chat conversations.

Related information
Related Item Navigation

Tools Security Rights

Tools rights are selected from the Category drop-down list on the Rights tab (CSM Administrator>Security>Edit Security Groups).

Tools include:

- Health Check.
- System Analyzer.
- Trusted Agents
- Client-side Logger.

Right	Description (when selected ✅)	Grant To:
Change client-side logger settings?	Allow: Allows selected Users to change Client-side logger settings in the CSM Desktop Client (Tools>Options>Other).	• System administrators
Configure Trusted Agents?	Allow: Allows Users to set Trusted Agent configuration options in CSM Administrator.	• System administrators
Manage encryption keys via Server Manager?	Allow: Allows selected Users to manage (add and edit) encryption keys for servers and web applications using the Server Manager.	• System administrators
Run Health Check?	Allow: Allows selected Users to run the Health Check in CSM Administrator.	• System administrators
Run System Analyzer?	Allow: Allows selected Users to run the System Analyzer in the CSM Desktop Client.	• System administrators

Users Security Rights

Set a whole range of access rights for users, customers and managers.

Users rights are selected from the **Category** drop-down list on the **Rights** tab (**CSm Administrator > Security > Edit Security Groups**).

Right	Description (when checked ☑)	Grant To:
Can clear User settings?	Allow: Allows selected users to clear user settings and remembered information (example: toolbar and window positions).	• System administrators • Advanced users (Level 2 and 3 technicians)
Can see logged in/out data for other Users/ Customers (via the User Data Expression)?	Allow: Allows selected users to see login/ logout information for other users or customers using the user/customer data expression.	• System administrators • Managers • Users
Can set password reset options?	Allow: Allows selected users to set password reset options in CSM Administrator.	• System administrators
Can view delegate history?	Allow: Allows selected users to view all delegations in the system.	• System administrators • Managers • Users
Change password?	Allow: Allows selected users to change their passwords.	• System administrators • Managers • Users/Customers
Change User ID?	Allow: Allows selected users to change a CSM user's Login ID.	• System administrators
Change Windows ID?	Allow: Allows selected users to change a CSM user's Windows ID.	• System administrators
Import Users from Windows?	Allow: Allows selected users to import users into CSM from Windows.	• System administrators

Right	Description (when checked ✔)	Grant To:
Lock/unlock User Accounts?	Allow: Allows selected users to lock or unlock user accounts.	• System administrators
Manage delegates for other users?	Allow: Allows managers and administrators to view all the active and historical delegations in the system.	• System administrators • Managers
Manage delegates?	Allows selected managers and administrators to: • View: Access delegate accounts. • Add: Create new delegates. • Edit: Edit existing delegates. • Delete: Delete delegates.	• System administrators • Managers • Users
User management?	Allows selected users who are working with User accounts in CSM Administrator to: • View: Access user accounts. • Add: Create new users. • Edit: Edit existing users. • Delete: Delete users.	• System administrators

Visualizations Security Rights

Visualizations rights are selected from the Category drop-down on the Rights tab (CSM Administrator>Security>Edit Security Groups).

Right	Description (when checked ☑)	Grant To:
Visualizations? Rights are organized by scope: Blueprint, Global, Role, Site, Team, and User.	Allows people working with Visualizations to: • View: Access Visualizations. • Add: Create Visualizations. • Edit: Edit Visualizations. • Delete: Delete Visualizations.	View/Run Only: • Users/Customers View/Add/Edit • Managers All rights: • System administrators

Webhooks Security Rights

Webhooks rights are selected from the Category drop-down on the Rights tab (CSM Administrator>Security>Edit Security Groups).

Right	Description (when selected ☑)	Grant To:
Allow Users to manage webhooks?	Allow: Allows selected Users to view, add, edit, and delete webhooks in CSM Administrator.	• System administrators

Related concepts

About Webhooks in CSM

Manage Webhooks

Web Services Security Rights

Web Services security rights are selected from the **Category** drop-down list on the **Rights** tab in CSM Administrator (**Security > Edit Security Groups**).

Right	Description (when selected ☑)	Grant To:
Allow calling web services from client machine (if allowed by system)?	Allow: Allows selected users to call web services (using a Call a Web Service Action in a One-Step™ Action) from a client machine if global settings are set to "allow" or "allow based on security." These settings are located in CSM Administrator (**System Settings > Advanced**). See Configure Global Advanced Settings.	• System administrators • Managers • Users
Web Services? Rights are organized by scope: Global, role, team, and user.	Allows people working with web services in CSM Administrator and the CSM Desktop Client to: • View: Access web services. • Add: Create web services. • Edit: Edit web services. • Delete: Delete web services.	View/Add Only: • Users/customers View/Add/Edit Only: • Managers All rights: • System administrators

Authentication Methods

CSM provides four methods for authenticating users: internal, LDAP/Active Directory, Security Assertion Markup Language (SAML), and Windows authentication.

You can enable multiple login modes so that if one authentication fails or the user/customer cancels the process, the next configured login method is invoked (example: SAML, then external authentication server, then Windows, then LDAP, then Internal). Not all of these options will necessarily be configured in your system.

Depending on which authentication methods you have enabled, which client you are using, where you have CSM installed, and where your authentication is implemented, you may be able to use pass-through authentication or single sign-on (SSO) when authenticating in CSM.

LDAP, Windows, and SAML authentication can be implemented as client-side or server-side authentication, meaning that the authentication request can be configured to come from either the client or the server. In general, client-side authentication is easier to use, but server-side authentication is more secure.

- **Internal**
  CSM authenticates using the login ID and password that is defined in either CSM Administrator or CSM Desktop Client.
    - In the CSM Administrator User Profile, select **Security > Edit Users** to edit users' credentials.

    - In the Desktop Client, first select **Customer > Contact Manager**, select a customer, and then select **Customer > Portal Settings > Current Customer Credentials** to edit customers' credentials.

    - **Important:** If Internal authentication is disabled, any services that are configured to use an internal account for authentication will be disabled.

      Note: Users may need to type `CHERWELL\` in front of the user name (example: CHERWELL\Bob). For more information, see Define the Default Domain and Anonymous Login Settings.

- **LDAP/Active Directory**
  CSM authenticates login credentials stored in an LDAP directory service such as Active Directory. Depending on configuration, user/customer data can be imported based on LDAP data.
    - Client-side LDAP authentication allows both SSO and pass-through authentication. Server-side LDAP authentication allows SSO, but not pass-through authentication.

    - For installations in which the LDAP service is on a different network from the CSM server, LDAP authentication requires the use of a Trusted Agent. This will be the case for all SaaS environments.

- **SAML**
  Allows SAML authentication. SAML authentication can be service provider initiated or identity provider initiated, and it allows both SSO and pass-through authentication.

- ◦ Since SAML is web-based, it does not require a Trusted Agent as long as the identity provider is reachable by the CSM client via the Internet.
- **Windows**

  CSM authenticates using Windows login credentials. Usernames must be manually defined in CSM Administrator, but passwords are defined by Windows credentials.
  - ◦ In on-premises, exclusively Windows environments, client-side Windows authentication allows both SSO and pass-through authentication. Server-side Windows authentication allows SSO, but not pass-through authentication.

  - ◦ In SaaS environments, client-side Windows authentication allows both SSO and pass-through authentication in the Desktop Client. In the CSM Browser Client, SSO is possible, but not pass-through authentication. Server-side Windows authentication is not possible in SaaS environments.

  - ◦ For installations in which the CSM server is not in the customer's network domain, Windows authentication requires the use of a Trusted Agent. This will be the case for all SaaS environments.

Related concepts

Create a Customer Record

Windows Credentials

Directory Services

SAML

Related tasks

Create a User Profile

Configure Login, Authentication, and Inactivity Settings for Each Client

Windows Credentials

If enabled, CSM can use Windows/LDAP credentials to authenticate users and customers.

To use Windows credentials:

- Windows or Active Directory must be enabled for each client in CSM Administrator. Navigate to **Security > Edit security settings**, select **Desktop Client**, **Browser Client**, or **Browser Portal**, and finally select **Windows** or **LDAP** as the login mode. See Configure Login Authentication for Each Client.

- The Windows login ID must be provided for each user's CSM. See Create a User Profile or Create a Customer Record.

Note: In the CSM Desktop Client, Windows credentials are automatically used, if enabled. In the Edge browser, the CSM Browser Client can automatically retrieve the user's/customer's credentials from the system and pass them to the server. In other browsers, users and customers might be prompted to provide Windows credentials. The browser validates the credentials before passing them to the server. If users or customers have previously provided credentials to the browser, they might not be prompted to provide their credentials.

If users or customers are not currently logged in to their standard Windows system (example: they are logging in from a mobile device or from outside the network), or their system is configured to use an alternate LDAP provider that does not provide direct Windows validation, they can still use their Windows/LDAP Credentials for single sign-on.

Users and customers provide their Windows (or LDAP) credentials in the **User Name** field and their Windows (or LDAP) credentials in the **Password** field. When the **Login** button is selected, CSM confirms that the specified credentials are valid, and if so, logs the user or customer in.

The user/customer must specify a fully qualified ID in the format `domain\user-id`.

CAUTION: HTTPS is the recommended protocol for production environments. When HTTP is used instead, credentials are visible when they are passed from the browser to the server and may pose security risks.

Related concepts
Create a Customer Record
Related tasks
Configure Login, Authentication, and Inactivity Settings for Each Client
Create a User Profile

Use the Windows Login for the CSM Portal

The WinLogin clause is an addition to the CSM Portal URL that allows the system to automatically log customers in with their Windows credentials.

Normally, customers access the CSM Portal with a URL like this:

http://MyServer/CherwellPortal

This URL redirects automatically to the default CSM Portal site, such as:

http://MyServer/CherwellPortal/IT

Customers can also go directly to a particular CSM Portal site:

http://MyServer/CherwellPortal/SomeSite

Depending on the configuration of the site, customers might then be prompted to log in, or they might have to select the **Login** link to be prompted for credentials. However, if the WinLogin clause is added to the URL (example: http://MyServer/CherwellPortal/WinLogin/IT), the system attempts to automatically log customers in using their Windows credentials, and then take them to the startup page. Note that, if the credentials are not legal, an error message is displayed.

Note: Using a URL with the WinLogin clause is equivalent to going to the CSM Portal, selecting **Login**, and then selecting **Use Windows Login**.

Related concepts
Windows Credentials
Related tasks
Configure Login, Authentication, and Inactivity Settings for Each Client

Directly Provide Windows/LDAP Credentials

If users/customers are not currently logged in to their standard Windows system, they can still use their Windows/LDAP credentials for single sign-on.

For example, if users/customers have logged in from a mobile device or outside their network, or their system is configured to use an alternate LDAP provider that does not provide direct Windows validation, they can still use their Windows/LDAP credentials for single sign-on.

Users/customers can provide their Windows (or LDAP) credentials in the **User Name** field and Windows (or LDAP) credentials in the **Password** field. When the **Login** button is selected, CSM confirms that the specified credentials are valid, and then logs the user/customer in to the system.

Note: The user/customer must specify a fully qualified ID in the format `domain\user-id`.

CAUTION: HTTPS is the recommended protocol for production environments. When HTTP is configured, credentials are visible when they are passed from the browser to the server and may pose security risks.

Directory Services

You can authenticate Users from a Directory Service such as LDAP or Active Directory.

Related concepts

Windows Credentials

SAML

Create a Customer Record

Related tasks

Configure Login, Authentication, and Inactivity Settings for Each Client

Create a User Profile

About Directory Services

On the **General Options** page of the **Map an Object** window, the **Directory Service** drop-down list shows a complete list of available vendors.

The following list of vendors are available:

- Active Directory Domain Service (Microsoft)
- LDAP: Generic and OpenLDAP (open source implementation)
- eDirectory (NetIQ)
- IBM Tivoli Directory Server
- iPlanet Directory Server
- Netscape Directory

> **Note:** After a particular vendor is chosen, CSM displays that name (example: Active Directory) throughout the system.

User Mapping Wizard Field Information

The **User Mapping Wizard** is used in all directory services to map the CSM User Business Object and user information to the directory service object that represents users. LDAP is used in this example, but the information is the same for any type of directory service.

To open the **User Mapping Wizard**, log in to CSM Administrator, navigate to **Create a New Blueprint > Tools > Directory Services**, and edit the desired service. Select **Users** in the left navigation pane, and then select the **Wizard** button.

The Wizard automatically maps CSM fields to directory service fields. The Wizard also creates some common fields. Since fields in the directory service standard are sometimes cryptic, CSM assigns more obvious names to them. For example, the **co** field in LDAP holds the name of the country, so CSM calls its field **Country**.

The **Map LDAP Object** page is where objects are selected to map to each other. Select the **Add** button to see all of the directory service fields that were not mapped and add any additional fields. There no maximum number of fields allowed. Select the **Delete** button to remove any fields that are not necessary.

Note: Be sure to map the field that holds the user ID of each LDAP user. This field is needed to synchronize when a re-import is done for users.

- **Cherwell Service Management Business Object:** Shows the name of the CSM User Business Object that holds the LDAP data.
- **LDAP object:** The name of the LDAP object that is mapped to a CSM Business Object.

  Active Directory uses the User object to hold user information. The LDAP standard uses INetOrgPerson to hold user information. Each vendor may have its own name that it uses for the INetOrgPerson object.

- **Additional Filters on User:** The filter limits the search results to the specified path and filters. For example, set filters to show only active users, only users with an email attribute, and more. To set up additional filters, select the **Add** button. The **Add Filter** window opens.

  The **Filter** window offers three types of filters:

  - **Filter for attribute that equals a certain value:** Filters on an attribute that has a particular value.
  - **Enter a custom filter string:** Filter LDAP directly. For example: (&(objectClass=user)(objectCategory=person)(!userAccountControl:1.2.840.113556.1.4.803:=2))
  - **Special Filters:** Choose special filters that CSM provides for certain objects.

Integration with Directory Services Workflow

You can configure the integration between CSM and a directory service. Most configuration procedures are completed in CSM Administrator.

> ✏️ **Note:** CSM provides a directory service with example settings selected. Use the Directory Services Worksheet to access the required configuration values that are specific to an organization.

Using a directory service with CSM consists of both configuring Users and Customers, as shown in the figure.

Configuring Users and Customers
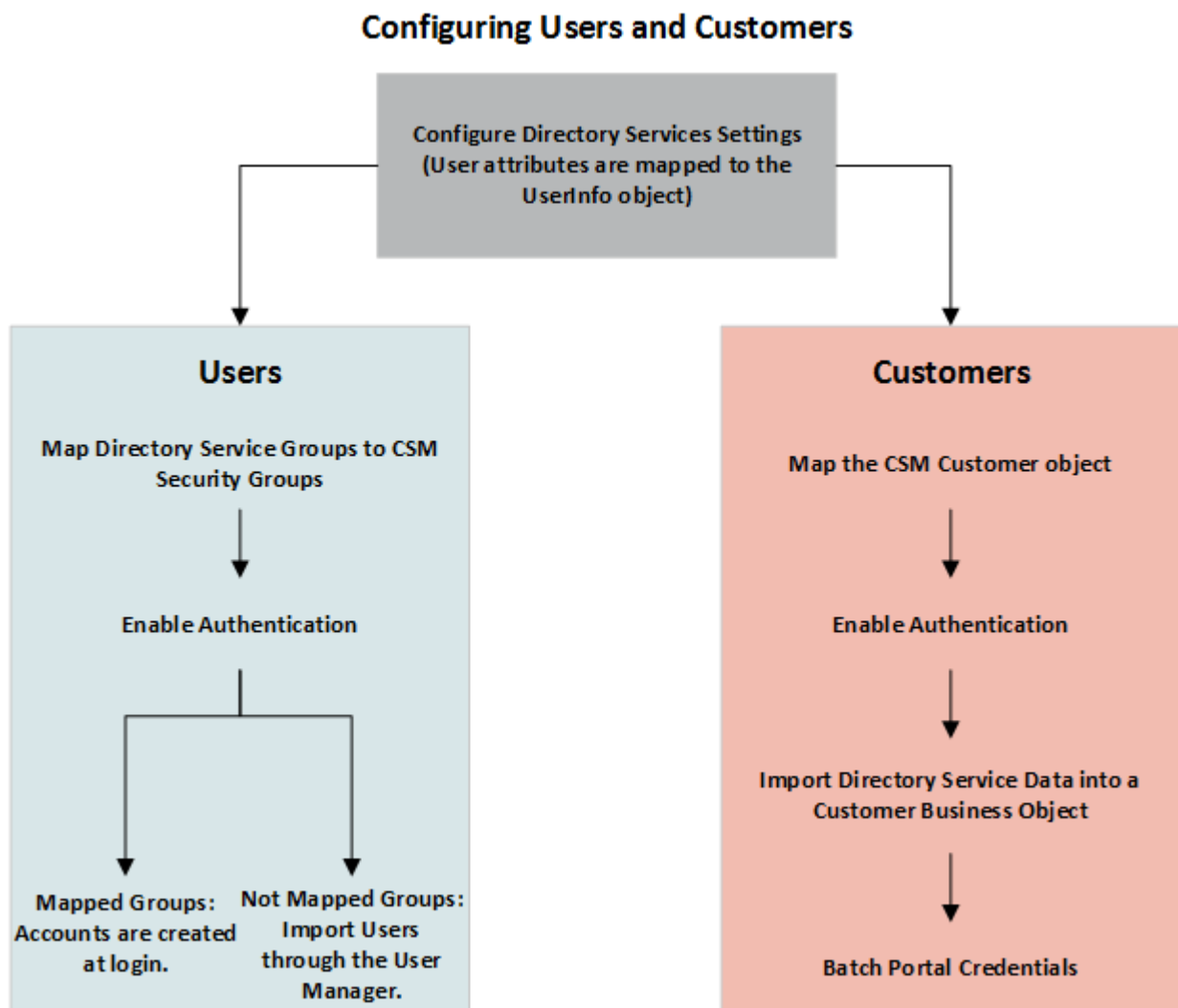
To configure the LDAP integration:

1. Configure CSM Directory Service settings
    a. Configure users for Directory Services.
        i. Enable authentication for users

    b. Configure customers for Directory Services.
        i. Enable authentication for customers

2. Use the Test LDAP tool. This tool is only available for LDAP connections.

Configuring CSM Directory Services Settings

Use the **Directory Services** window in CSM Administrator to configure a directory service.

Before authentication can be set up, the **Directory Services Settings** window must be completed. This process is the same for configuring both Users and Customers. For example, the CSM User Business Object must be mapped on the **Users** page.

To configure a directory service:

1. In the CSM Administrator main window, select the **Blueprints** category, and then select the **Create a new Blueprint** task.

2. In the menu bar, select **Tools > Directory Services (Active Directory, LDAP)**.

3. In the **Directory Services (Active Directory, LDAP, etc.)** window, select **Add** to set up a new directory service.

   The **Map LDAP Object** window opens.

4. In the **Directory Service** drop-down list, select the directory service (example: **Active Directory** or **LDAP**). The name of the **Map LDAP Object** window updates with the name of the new directory service.

5. Select the options in the left navigation pane to define properties on the **General**, **Schema**, **Users**, **Groups**, and **Trusted Agents** pages.

   Note:
   - The **Groups** page is available only when users are allowed to log in to the system and/or when users are allowed to be imported into the system. These settings are available on the **Users** page.

   - The **Trusted Agents** page is available only when Trusted Agents are configured for the CSM system.

Related concepts
Configuring Trusted Agent

Define General Directory Service Properties

The **General** page in the **Map Object** window in a Blueprint includes options for general information, settings for Security, Configuration, and Searching, and a series of check boxes for mapping options.

To define General properties:

1. Open the **Map Object** window.
2. Select the **General** page.
3. Define General properties.
4. Define Security properties.
5. Define Configuration properties.
6. Define Use Paged Searching properties.
7. Define the Miscellaneous properties.

General Properties

- **Name**: The name of the service.
- **Directory Service**: The type of directory service.
- **Domain**: The domain name of the network.
- **Server**: The host name of the LDAP directory server.

> **Note:** If you are using Secure LDAP (LDAPS), specify the host name of the SSL/TLS certificate used by your LDAP directory to establish a secure connection. If your certificate is self-signed or from a non-standard Root CA, you may need to install the certificate on the machines that are connecting directly to the LDAP directory. This may include your CSM Application Servers and machines running the CSM Administrator and CSM Trusted Agent Server if they directly connect to the LDAP directory.

Security Properties

- **Authentication type**: The type of authentication required to access LDAP.
    - **No Encryption**: No login is required and all data is transferred in plain text.
    - **Basic**: User ID and password are required, but no confidentiality is provided. Data is transferred in plain text.
    - **Secure**: User ID and password is authenticated through NTLM or Kerberos, depending on the service selected. The data between LDAP and CSM is not encrypted.
    - **SSL**: User ID and password are required and data between LDAP and CSM is encrypted. This changes the path to LDAP and the default port to 636.
- **Search User ID**: The User ID used for all LDAP searches. The User ID can be set in a variety of formats:

- **Windows Only**: domain\user, user@domain, cn=user.dc=company.ddc=com
- **Other**: cn=user.ou=company.c=US.

> **Tip:** Select the question mark to see the list of valid formats. Ask an LDAP administrator which format is used at a specific organization.

- **Search Password**: The password assigned to the User ID.

Configuration Properties

- **Port**: The standard LDAP ports are 389 and 636 (secure LDAP). If unsure of the port number, try these two first.
- **RootDSE Path**: The RootDSE is the root of the LDAP directory server. Some examples are:
    - LDAP://192.168.0.123/RootDSE
    - LDAP://192.168.0.123:389/RootDSE (when port number is included)
    - LDAP://ServerName/RootDSE

> **Note:** If you are using any port besides 389, type the port number in the RootDSE path (example: LDAP://www.mycompany.com:389/RootDSE).

- **Schema Path**: The schema contains a definition of all of the objects on the LDAP server (User, Group, etc.).
  The easiest way to set up the schema path is to select the **Locate** button. Before doing this, go to the **Security** section on the **General** properties page and verify that the encryption type, User ID, and password are set up. When the RootDSE and security information is entered, CSM Administrator should be able to find the schema. If the schema is not found, Users should ask an LDAP administrator for assistance.

  Some common schema paths include:

    - LDAP:// 192.168.0.123/CN=Schema,CN=Configuration,DC=Cherwell,DC=com
    - LDAP://ServerName/CN=Schema,CN=Configuration,DC=Cherwell,DC=com
      (these are the formats used by Active Directory)
    - LDAP://192.168.0.123/cn=schema
    - LDAP://www.mycompany.com/cn=Subschema
    - LDAP://www.openldap.com:389/cn=Subschema

- **Search Start**: This is the location where LDAP searches begin. Using only the server location can slow the data transfer. Enter a path more specific to the location of the data to increases data-transfer efficiency. For example, to search for only Users in Colorado Springs the path might be: LDAP://Cherwell/DC=ColSpgs,DC=Cherwell,DC=Com

> **Tip:** DC stands for domain context (used by Microsoft computers with domains). The LDAP standard also suggests some prefixes that are used by most vendors – OU (Organizational

Unit), O (Organization), CN (Common Name), and C (Country). The prefixes are case insensitive.

More examples include:
- LDAP://Cherwell/OU=ColSpgs,DC=Cherwell,DC=com

- LDAP://192.168.0.123/ou=Administrators,ou=TopologyManagement,o=NewspapeRing

- LDAP://ServerName/O=Cherwell,c=US

- LDAP://www.mycompany.com/o=Cherwell

- LDAP://www.mycompany.com /dc=site

- **Follow Server Referrals**: Data can be stored on multiple LDAP servers. Selecting this check box allows the initial-contact server to continue searching for data beyond the initial server to secondary servers for information. Users should consult an LDAP administrator or IT staff member to verify if this should be selected.

> **Note:** Allowing referral services can cause delays during data transfer.

Page Searching Properties

The **Use Paged Searching** option is recommended because it allows you to set the maximum page size and server time limit. Using paged searching increases the speed of searching by grouping search results into pages set by the Max page size limit. The time limit is set so that the server stops searching after the entered time if there are no results to the search.

Recommended settings: Max page size - 100; Server Time Limit - 120 seconds.

> **Note:** Some vendors do not support this functionality. Select **Test Paged Search** to see if the feature is supported.

Miscellaneous Options

- **Allow Business Objects to be mapped to objects**: Select the check box to map CSM Business Objects to Active Directory Objects.

- **Allow Business Objects to be imported from data:** Select the check box to import Active Directory data into CSM.

- **Client-Side LDAP (for SaaS)**: When using an application server and a 3-tier connection, select the check box to allow data to be shared from CSM to LDAP without going through the Cherwell Application Server. Do not select this check box unless specifically directed.

Related concepts
Default Port Numbers

Define Directory Service Schema Properties

The **Schema** page (in the **Map LDAP Object** window) is where Users set the Schema Attributes, and the page is used to map directory service objects to CSM objects. The schema contains the structure of all objects stored in a directory service.

To define Schema properties:

1. Open the **Map LDAP Object** window.
2. Select the **Schema** page.
3. Select the **Save schema first time it is read in** check box.
4. Define the following Schema Attributes:

Save schema first time it is read in	The field in schema objects that contains the ID. When selected, the LDAP schema is cached the first time an LDAP-mapped Business Object is created. This improves performance because mappings can be done without accessing the LDAP server.
ID	The ID attribute.
Path	The field in schema objects that holds the path to an object. Microsoft calls this field *distinguishedName*.
Attributes that Hold Name	The standard has several fields that can be used to hold a name – cn (common name), ou (organizational unit) and o (organization). Active Directory adds *name*. Have the most commonly used name at the top (*name* for Active Directory and *cn* for other vendors). ◦ Select the **Add** button to add attributes. ◦ Select an attribute, and then select **Delete** to un-associate the attribute. ◦ Use the arrows to order the attributes.

Define Directory Service Users Properties

The directory service **Users** page (in the **Map LDAP Object** window in a Blueprint) maps CSM users to LDAP Users. Once the mapping is done, users log in using a Directory Service authentication and/or are imported directly into CSM.

To define Active Directory users:

1. Open the **Map LDAP Object** window.
2. Select the **Users** page.
3. Define the users properties.

Allow LDAP Users to Login to the System	Use LDAP authentication when users log in. **Note:** In CSM Administrator, go to the **Security** page, select the **Edit System Settings** and the **LDAP** check boxes under **Supported Login Modes**.
Allow Users to be imported	Import users directly into CSM. To import users, open CSM Administrator and select **Database > Import from LDAP**.
Wizard	Opens the Wizard to map Active Directory fields to CSM Business Object Fields. If LDAP fields change in the future, use the **Add**, **Edit**, and **Delete** buttons to modify the field mappings. **Note:** For more information about how to use filters, refer to User Mapping Wizard.
Name of Active Directory User Class	Specify the ObjectClass attribute of users.
Field that Holds User ID	After the Wizard, select the field that holds the User ID for each LDAP user. This is used for synchronization when users are re-imported.
Start of User Searches	Specify the path where user searches should start or provide the same path specified for Search Start on the **General** page. **Note:** LDAP searches can be slow, it is best to pick the LDAP directory that contains all of the users and provide that path. Select the **Test** button to verify the directory specified is correct.

Additional Filters When Pulling Active Directory Data:	Select **Add** to open a window to add additional criteria that are applied to LDAP objects when an import is done.

Define Directory Service Groups Properties

If the **Allow LDAP Users to login to the system** or **Allow LDAP Users to be imported** check boxes are selected on the **Users** page, then the **Groups** page option is shown on the **Map Object** window.

The group information is used to associate LDAP Users with a CSM Security Group.

For options with Browse, select the **Browse** button to verify the object is available, even if the group name is known. If the object is not there, Users should ask an LDAP administrator if a security setting is preventing it from being shown.

To define the LDAP Groups:

1. Open the **Map Active Directory Object** window.
2. Select the **Groups** page.
3. Define the Groups properties.

Name of Group Object	The name of the directory service object that holds group information. In directory services, this is called Group. Select the **Browse** button to see the list of objects available.
Location of Group Membership	The standard has two options that Users can be associated with a group. Many vendors allow both methods. ◦ The User object holds the name of the group. ◦ The Group object holds a list of group members (Users). If both options are available, select **User object holds name of group member**. LDAP authentication is faster if this method is used.
Start of Group Searches	The **Wizard** button maps directory services fields to CSM Business Object Fields. If directory service fields change in the future, use the **Add**, **Edit**, and **Delete** buttons to modify the field mappings. **Note:** For more information about how to use filters and run the wizard, refer to User Mapping Wizard.
Name of Active Directory User Class	Specify the ObjectClass attribute of Users.
Field that Holds User ID	After the Wizard is run, select the field that holds the User ID for each directory service User. This is used for synchronization when Users are re-imported.

Start of User Searches	Provide the path where group searches should start. The same path entered for **Search Start** (on the **General** page) can be used. Although LDAP searches can be slow, pick the LDAP directory that contains all groups and enter that path. Select the **Test** button to confirm the directory is correct.
Test	Select **Add** to provide additional criteria that are applied to LDAP objects when an import is done.

Define Trusted Agents Properties for Directory Services

Use the **Trusted Agents** page to assign the Active Directory connection to a Trusted Agents Group. This scenario is used to scale out Trusted Agents for request routing.

To assign service groups to a connection, you must first:

1. Configure Trusted Agents.
2. Connect to the Trusted Agents Hub from CSM Administrator.
3. Configure Trusted Agents Service Groups.

For more information, see Scaling Trusted Agents for Request Routing.

To define Trusted Agents properties:

1. Open the **Map LDAP Object** window.
2. Select the **Trusted Agents** page.
3. Select the **Use Trusted Agents** check box.
4. Select one of these options:
    - **Any Trusted Agent Group**: Allows any group to handle requests for this Active Directory connection.
    - **Trusted Agent Group**: A specific group to handle requests for this Active Directory connection.

Workflow for Configuring Users for Directory Services

The process to configure users in CSM to integrate with Directory Services differs slightly from configuring customers. Complete the steps for configuring CSM Directory Services settings before configuring users.

To configure users:

1. Map Directory Service groups to CSM security groups.
2. Order Directory Service groups.
3. Enable authentication for users.
4. Import users:
   - If groups are mapped, the account is created when users log in to Cherwell using their Active Directory/LDAP credentials.
   - If groups are not mapped, or the users are entered manually, accounts are imported using the User Manager in CSM Desktop Client.

Map LDAP Groups to CSM Security Groups

When users log in to CSM, the assigned security rights are based on the CSM Security Group. For LDAP users, security rights are assigned only in an Active Directory Group. Active Directory Groups must be mapped to CSM Security Groups.

Use the **Security Groups** window to define:

- The Security Groups for LDAP Groups
- The order of Security Groups

To map LDAP Groups to CSM Security Groups:

1. In the CSM Administrator main window, select **Security > Edit security groups**.
2. Select the **Users** tab on the **Security Groups** window (the directory service must be configured in the database).
3. Select **Order groups**. If no groups are shown in the **Groups** section, select **Add** to open the **Associate LDAP Groups** window.
4. To show available groups. provide a group or set of characters in the text field, and select **Search**.
5. Select the groups that should be associated with this CSM Security Group and select **OK**.

The window closes and the group appears in the **Associated LDAP Groups** section of the **Security Groups** window.

> **Tip:** If the LDAP Groups are not visible, go to the **Map LDAP Object** window and select the **Groups** page to verify the Search Start settings.

Related concepts
Order Directory Service Groups

Order Directory Service Groups

Once all directory service Groups are associated with CSM Security Groups, the groups need to be ordered.

Users can belong to more than one directory service Group, so CSM requires groups to be ordered. This ensures the correct directory service Group is used for the User's CSM Security Group.

For example, Joe belongs to the Administrators and Developers Groups. When he logs in to CSM, he is assigned to the Security Group that is associated with Administrators. He is assigned to that group because the Administrators Group has the most rights out of the list.

To order directory service Groups:

1. In CSM Administrator, select **Security > Edit security groups > Users > Order groups** to open the **Order LDAP Groups** window.

2. Select the arrows to order the directory service Groups.

   Note: Put the Directory Service Groups in the order they should be verified when picking the associated CSM Security Group.

3. Select **OK**.

Enabling LDAP Authentication for Users

Before a directory service can work with CSM, LDAP must be enabled as a supported login mode in CSM Security Settings.

Regardless of the type of directory service being used, the selections for this setting all refer to LDAP in the user interface.

Note: LDAP authentication does not fall back to Windows authentication if LDAP authentication is unsuccessful. Enable Windows authentication to verify credentials with a Windows domain using native Windows APIs.

To enable LDAP authentication:

1. In the CSM Administrator main window, select **Security > Edit security settings**.
2. In the **Security Settings** window, select **Desktop Client**.
3. Under **Supported login modes**, select the **LDAP** check box.
4. Select **OK**.

Import Directory Service Users

To import Directory Service Users, ensure that Windows login is allowed in CSM. Enable Windows login in the CSM Administrator.

If Security Groups are already configured, importing Users is not necessary, as Users are added to the system when they log in.

Use the Import Users window to define:

- Directory service to import
- Users to import
- Default domain
- Security Group to assign to imported Users
- LDAP Key field

To import Users:

1. To open the User Manager in CSM Administrator, select **Security > Edit Users**.

2. In the toolbar, select the **Import Users** button ⬇ .

3. In the **Import Users** window, select the **Directory Service Users** radio button and provide the following User information:
    ◦ **LDAP Directory Service:** Select the created LDAP Blueprint in the list.
    ◦ **Starts With**: Leave blank or provide a few characters to narrow the search, and then select **Search** to see a list of all LDAP Users.
    ◦ **Default domain:** Provide the domain that the imported Users belong to and select a default domain-option radio button.
    ◦ **Security Group for imported Users:** Select the CSM Security Group in the list.

        Tip: If the LDAP Users are not shown, go to the **Map LDAP Object** window. Select the **Users** page to verify the Search Start setting.

    ◦ **LDAP Key Field:** Select the **Key Field** for the LDAP import in the list.
4. Select **OK**.

Import Active Directory Image Data into CSM

The Active Directory import allows images to be added to a User or Customer Internal Business Objects in CSM by mapping the fields to an Active Directory image attribute.

To import Active Directory image data into CSM:

1. In the CSM Administrator main window, select **Create a new Blueprint**.
2. In the Object Manager, verify that the **Major** radio button is selected.
3. Select **Customer > Customer-Internal**.

   🖉 **Note:** This process can also be done on the User-Info Lookup table Object for Users.

4. Select the **Edit Business Object** task to open the **Edit Customer - Internal Business Object Group Member** page.
5. Select the **Bus Ob Properties** button.
6. Select the **Active Directory** page.
7. Select **Add** to open the **Map Active Directory Field** window.
8. Under **User Attributes**, select the **Active Directory attribute** that holds the image. The default attribute is **thumbnailPhoto**.
9. Select **Add**.
10. Select the attribute for the image in the **Map Active Directory Field** window.
11. Select the **Existing field** radio button, and select **Avatar**.
12. Select **OK**.
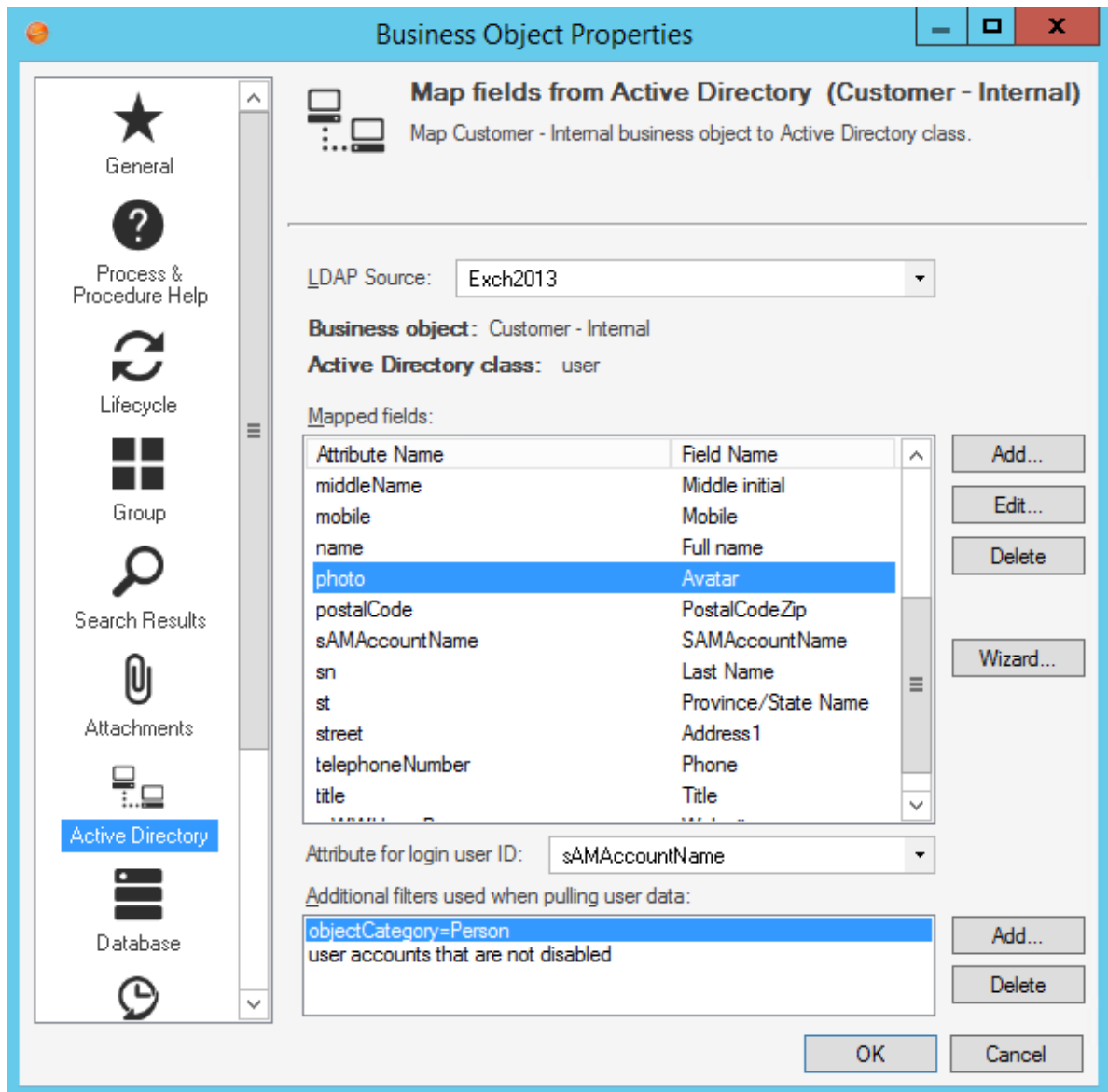
13. Select **Object Manager** in the Blueprints task pane.

14. Select the **Lookup tables** radio button.

15. Select **UserInfo**.

16. Select the **Edit Business Object** task.

17. Select the **Bus Ob Properties** button.

18. Select the **Active Directory** page.

19. Select **Add** to open the **Map Active Directory Field** window.

20. Under **User Attributes**, select the Active Directory attribute that holds the image.

21. Select the **Existing field** radio button, and select **Avatar**.

22. Select **OK**.

23. Save and publish the Blueprint.

Workflow for Configuring Customers for Directory Services

The process to configure Customers in CSM to integrate with Directory Services differs slightly from configuring Users.

Complete the steps for Configuring CSM Directory Services settings before configuring Customers.

To configure Customers for LDAP:

1. Map the CSM Customer Object to a Directory Service (this can be used for any Business Object).
2. Enable Authentication for Customers.
3. Import Directory Service Data into the Customer Business Object using the Import Data Wizard or a Scheduled LDAP Import Action.
4. Batch Updating Customer Credentials after the Customer records are imported.

Map the CSM Customer Object to a Directory Service

After the **General properties** window is complete, map Customers to the CSM Business Object.

Use the LDAP Mapping Wizard to define:

- Directory services
- Group information
- Business Objects to use LDAP data
- Fields to map to LDAP attributes

To map a CSM Business Object to Directory Service objects:

1. In a newly created Blueprint, go to the Object Manager.
2. Select **Customer-Internal Business Object**. Under **Structure**, select **Map to Active Directory** to open the LDAP Mapping Wizard.
3. Select **Next**.
4. Select the LDAP directory service to use for the mapping, and then select **Next**.
5. Select if the new LDAP Business Object is part of a group.

    🖉 **Note:** This step is shown only if mapping a New Object.

    - **Not a Member of a Group**: The Business Object is not a member of a group.
    - **Group Leader**: The Business Object is a group leader. A group leader is an object that has other Business Objects as its children and holds the common fields shared by the children Business Objects.
    - **Member of Group**: The association to a group. When selected, the drop-down list is enabled. Select an item.
    - **Group Members**: Select a list item to select the group members (only one item can be selected).

6. Set up the CSM Business Object to use directory service data:
    a. **Cherwell Service Management Business Object**: Provide a name for the CSM Business Object. This autopopulates with the Object that is selected in the Blueprint.
    b. **Directory Service object**: Scroll down and select **User**.
    c. **Reload Schema** button: Select the **Reload Schema** button to reload the Active Directory objects. A warning appears that this function can take a while.
    d. **Additional Filters on User**: The following Out-of-the-Box (OOTB) filters are in place. The filters are applied to filter out the records returned.
        i. **ObjectCategory=Person**: Ensures that computers are not included along with people in the records returned.

      ii. **User accounts that are not disabled**: Ensures that disabled User accounts are not included in the records returned.

To add additional filters, select **Add**.

> **Note:** Be sure to map the field that holds the User ID of each User. In Active Directory, this is usually SAMAccountName. This field is needed to synchronize when performing a User re-import action.

7. Select **Next**.

8. Select **Add** to add fields to map on the **Map fields to LDAP attributes** page to open the **Map LDAP Field** window.

9. Select **User Attribute**.

10. Select either:
    - **New field**: Creates a new field. Select an option in the **Data Type** drop-down list and provide the size.
    - **Existing field**: Select this radio button, and then select an already existing field in the drop-down list.

> **Note:** The System_LDAPPath field is a reserved system field and is not for Customer mapping.

11. Select the **Auxiliary attribute** radio button and provide the attribute name. The **Auxiliary attribute** text box extends the mapping functionality to allow entry of an attribute name that is not structurally defined on the selected LDAP class but should be included in the mapping process.

12. Select **Finish**.

The Map Wizard closes, and the **Business Object Properties** window opens.

13. Publish the Blueprint.

14. Import Customers by Importing Directory Services Data into the Business Object.

Enable Authentication for Customers

Regardless of the type of directory service being used, the selections for this setting all refer to LDAP in CSM. Before a directory service can work with CSM, the CSM Security Settings must be configured.

To enable authentication:

1. In the CSM Administrator main window, select the **Security** category, and then select the **Edit security settings** task.

2. Select the **Browser Portal** page.

3. Verify the **Use Same Settings as Desktop Client** check box is selected.

4. Under **Supported login modes**, select **Internal** and **LDAP**.

Import LDAP Data into Business Objects

The LDAP Import Wizard assists with importing LDAP data into CSM. Before importing data, create a Business Object to import the data into, and then complete importing customers using the Customer-Internal Business Object. The Scheduler can be used to import LDAP data at scheduled times.

Due to read-only settings, you may need to assign a new value to the Exempt User from Read Only AD Import Stored Value (under the Blueprint folder). You must enter the full name for the User account under which the import runs or the import may fail. The read-only settings are related to how your content is configured, so this may not apply to your customizations.

To import LDAP data into Business Objects:

> **Note:** The Wizard and page names depend on the Directory Service selected on the **General** page.

1. In the CSM Administrator main window, select the **Database** category, and then the **Import from Active Directory** task (or other directory service) to open the Import Wizard.
2. Select **Next**.
3. Select the Directory Service that was configured to import Active Directory Users/Customers in the Customer - Internal Business Object.
4. Select **Next**.
5. On the **Select Business Object** page, select the Business Object that is mapped to Active Directory, and then select **Next** to continue.
6. Import all items or only particular ones.
   - **Import Option**: Select **Import All** (the Business Object selected in the previous step appears next) or select **Choose items to import**.
   - **Existing items**: Select **Update existing items**, and then select the key in the drop-down list. If any existing items should be refreshed, select **Do not update existing items**.
   - If CSM data should not be overwritten when the LDAP field is empty, select **Do not overwrite CSM Service Management field when the LDAP field is empty**.
   a. If the **Import All** option is selected, the **filter** page opens.
      - **Start Import at**: Shows where CSM searches to import Active Directory Users.
      - **Additional Filters on Customer-Internal**: Applies filters to filter out the records returned. The example uses two filters:
         - ObjectCategory=Person: Ensures that computers are not included along with people in the records returned.
         - User accounts that are not disabled: Ensures that disabled User accounts are not included in the records returned.
      - Select **Add** to set up additional filters or **Delete** to delete filters.

      b. If the **Choose items to import** option is selected, the **Select Active Directory Data** page opens. To view items, either leave the **Starts with** text field empty or enter a few characters to narrow the search.

          i. Select **Search**.

          ii. Select **Customer-Internal items**.

7. Select **Finish** to complete the import.

> **Tip:** In CSM Administrator, select **Scheduling > Edit Schedule** to open the Scheduler and import Customer data consistently at a defined date and time.

Related concepts

Create a Scheduled Item

Import External Data into a New External Business Object

Assign a Value to a Stored Value

Batch Updating Customer Credentials for a Directory Service

After using the Import Wizard, use the Contact Manager in the CSM Desktop Client to view, edit, and manually batch update Customer credentials.

The Contact Manager feature takes all imported Customers and assigns them Portal IDs. CSM allows a Customer to log in using assigned Cherwell credentials or using Windows/LDAP credentials.

Note: Ensure that Windows or LDAP Login is allowed in CSM. To do this, open CSM Administrator, and select **Security > Edit security settings**, and select either **Windows** or **LDAP** as a supported login mode.

To batch Customer credentials for a Directory Service:

1. Open the Contact Manager.

2. In the **Customer type to show** drop-down list, select the Business Object that is mapped and has the imported data.

3. Select **Go** to allow all Users that are imported from the directory service.

4. On the menu bar, select **Customers > Select Portal Settings > Batch Portal Credentials**.

    Note: This menu option only appears when the search returns Users.

5. Define the login credentials for the Customers:
    a. **Field with Login ID**: Select **User ID Field**. This is usually SAMAccountName (depending on the directory service).

    b. **Customer Group**: Select the security group to assign Users that are included in the batch.

6. Define the Password options:
    a. Select the **Set Login ID Field as Windows/LDAP login** radio button.

    b. Select the **Use this domain** check box and provide the domain.

    c. Leave all other options cleared.

7. Define Account details options:
    a. **Account locked**: Select to lock the Customer's account (preventing her from logging in to the Portal).
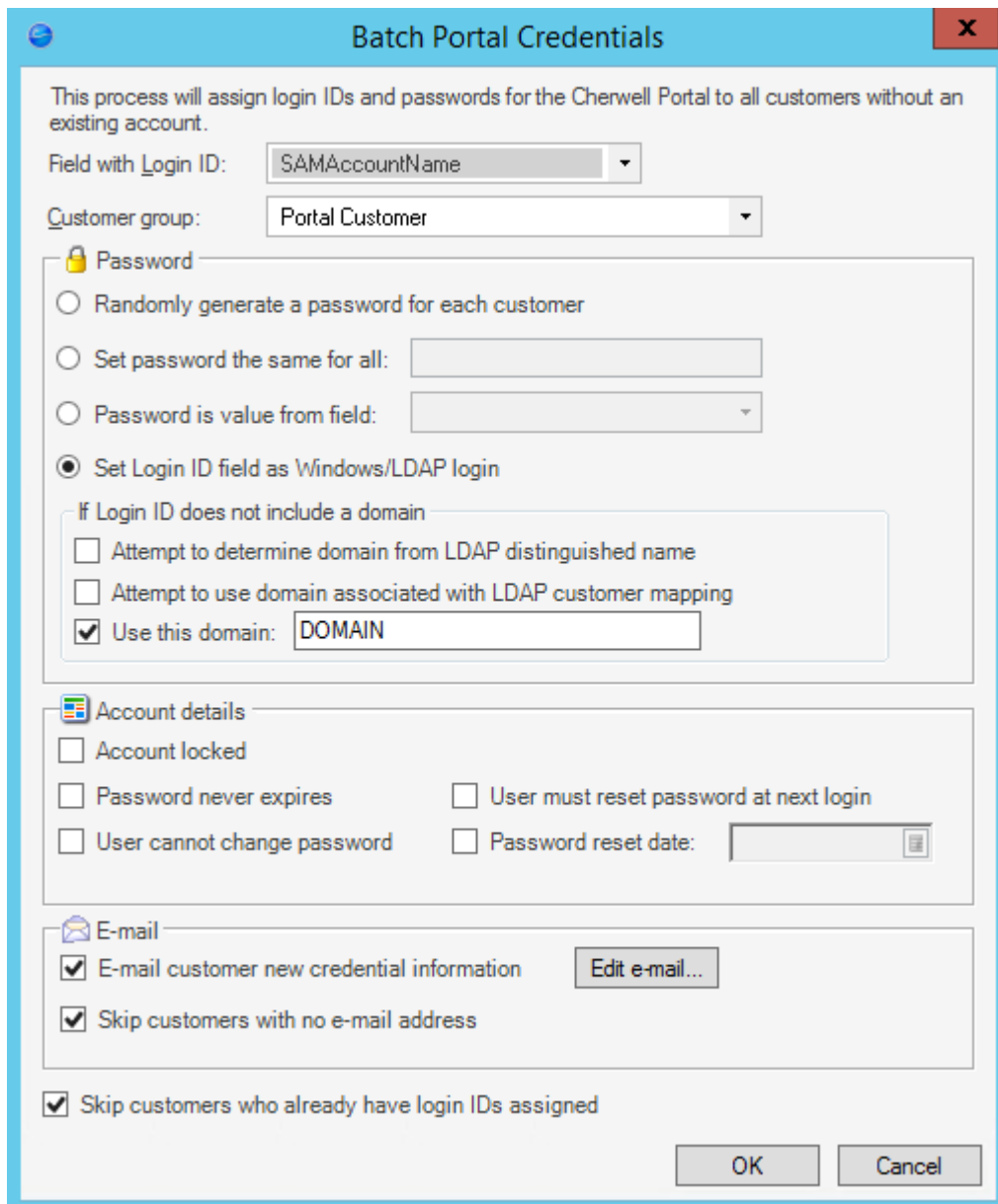
    Note: A Customer can be automatically locked out of the system because of too many failed login attempts (depending on system settings).

    b. **Password never expires**: Select to forgo password expiration. This overrides any system setting to reset the password.

> **Note:** If selected, the **User must reset password at next login** and **Password reset date** settings are hidden.

    c. **User cannot change password**: Select to restrict a Customer from changing the password. If a password reset is required by the system, the system administrator must reset the password.

    d. **User must reset password at next login attempt**: Select force users to reset their passwords at their next login attempt.

    e. **Password reset date**: Select to prompt a Customer to change the password on a specific date. Select the **Date Selector** button [icon] to select a reset date.

8. Select E-mail options:

    a. Select **E-mail customer new credential information** so that Customers receive an email with their User ID/password for credentials.

    b. Select **Skip customers with no e-mail addresses**. This option is used when using Cherwell Internal Authentication, LDAP, Windows Authentication, and domain credentials that do not require an email address.

9. Select **Skip the customers who already have login IDs assigned** to assign credentials only to new Customers (that is, skip assigning credentials to Customers who already have them).

10. Select **OK** to generate the IDs.

Related concepts
Open the Contact Manager

Using the Test LDAP Tool

When working with the LDAP testing tool, Users can test LDAP and directory service browsing for connectivity, search streams, servers, and authentication in some instances.

The tabs allow Users to search or browse for containers and objects.
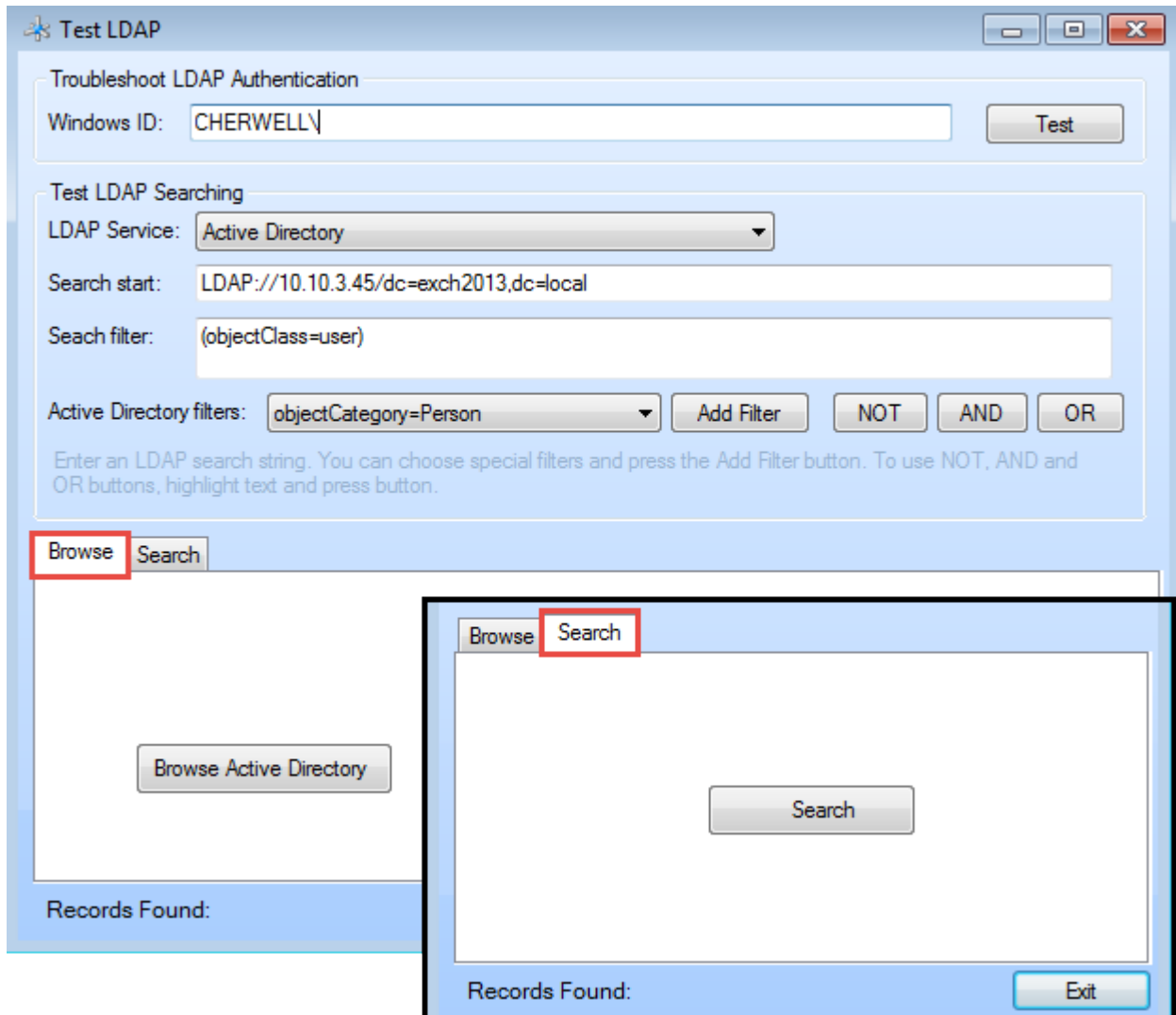
To use the Test LDAP tool:

1. Go to **Start > All Programs > [variable here] Service Management > Tools > Test LDAP**.

   The **Connect to Cherwell Service Management** window opens.

2. Select a connection and select **OK** to open the **Test LDAP** login window.

3. Provide the user ID and password.

4. Select **OK** to open the **Test LDAP** window.

5. Troubleshoot LDAP Authentication:
   ◦ **Windows ID**: Searches LDAP for the account in field and auto-populates with the account of the person logged in to the workstation.

   ◦ **Test**: Takes the account and verifies in the LDAP service if account exists. If no account exists, an error window opens.

6. Test LDAP Searching:
   ◦ **LDAP Service**: Select the directory service loaded in CSM.

   ◦ **Search start**: Shows the location of where the LDAP search begins.

   ◦ **Search filter**: Shows the filter syntax to narrow search results. This field is required to run the search.

   ◦ **Active Directory Filters**: Contains predefined filters.

   ◦ **Add Filter**: Adds the Active Directory filter to the **Search Filter** path.

   ◦ **NOT**, **AND**, **OR**: Inserts operators into the **Search Filter** field.

7. Select either:
   ◦ **Browse**: Runs a directory service browser and shows the different containers in a tree. Select a container to view the objects in the container.

   > **Note:** Verify that the account you are using has the required permissions for the Browse function to work.
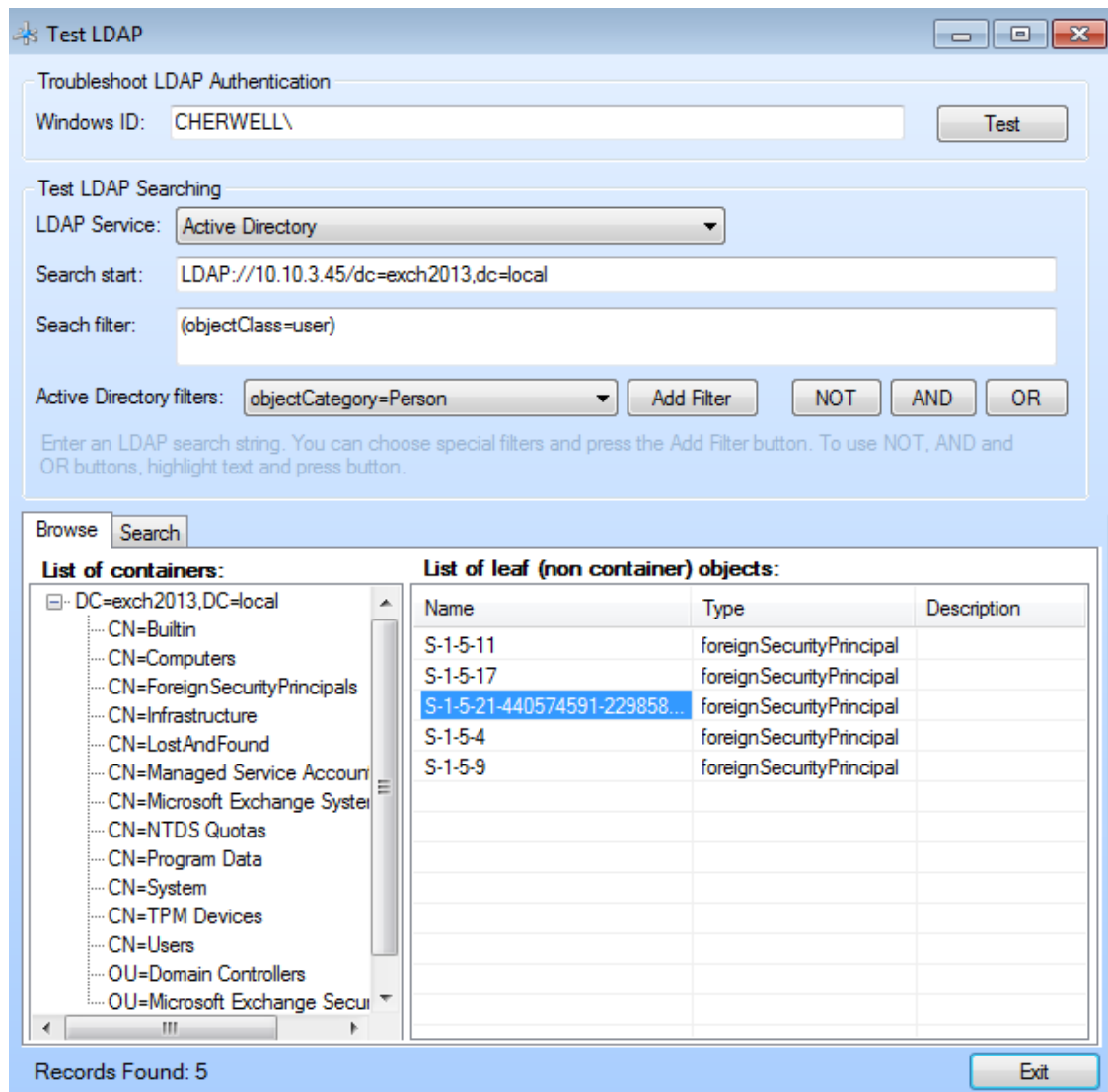
◦ **Search**: Runs a search against the value provided in the Search filter. The results show in the **Search** section.

About Active Directory Integrations

Microsoft Active Directory® is a special-purpose database that stores data for objects in a network, including Customer information.

Customer data from Active Directory can be imported into CSM to readily view account information such as full names and email addresses for internal Customers. CSM integrates with Active Directory by connecting to the directory service, mapping objects, and enabling security settings to import Users and data.

About LDAP Integrations

Lightweight Directory Access Protocol (LDAP) is a protocol used to access information in a directory service (a directory stored on a server).

LDAP integrates by connecting to the directory service, mapping objects, and enabling security settings to import the Users and data into CSM.

Troubleshooting Directory Services

You can troubleshoot issues with Directory Services by answering a series of questions.

- **Who is responsible for integrating CSM with Directory Services?**

  Users should consult an LDAP administrator, IT staff member, or the Cherwell Professional Consulting Services team for assistance with LDAP.

- **Why are Users not able to login using LDAP authentication?**

  If Users are not able to login using LDAP authentication, try these tips:

  - Ensure the Domain value in LDAP General settings matches the domain specified by Users in the login dialog. This is how CSM matches User accounts with the correct LDAP settings.
  - Ensure the selected directory service value matches the type of LDAP directory being configured. The LDAP (generic) settings may be tried for unlisted directories, but LDAP functionality within CSM may be limited or non-functional.
  - Ensure all accounts within the LDAP General settings Search Start scope are unique. CSM expects that, within the configured Search scope for an LDAP settings definition, duplicate User accounts (ex. SAMAccountNames) do not exist. There are two options available for this:
    - Enter a Search start path in the **General** page of LDAP settings that is limited to a single domain or OU that contains unique User accounts.
    - Ensure that all User accounts that are found in the configured Search scope have unique User accounts (ex.SAMAccountNames). Multiple LDAP settings can be created to cover multiple domains or OUs.

SAML

Security Assertion Markup Language (SAML) is an XML-based open standard for exchanging authentication and authorization data between identity providers and service providers to support Single-Sign-On (SSO) capability.

SAML uses:

- Identity Providers: Manage User Identities and interact with data stores containing User credentials. Identity providers normally provide interfaces allowing Users to log in to SAML sessions.
- Service Providers: Provide applications and act as *Relying Parties* for SAML identity information.

Related concepts
Configure SAML in CSM
Related tasks
Configure Login, Authentication, and Inactivity Settings for Each Client

About SAML

CSM supports SAML 2.0 as a service provider. Before SAML can be used, the integration must be configured in CSM Administrator and in the identity provider.

Note: The CSM Outlook add-in does not currently support SAML authentication.

When a user starts CSM, including the CSM Desktop Client or CSM Browser Client, a Cherwell Service sends an authentication request to the user's identity provider. Users who are not already logged in to an identity provider are presented a log in window so they can enter their credentials, which are authenticated by the identity provider. If the authentication is successful, the identity provider passes a response containing one or more assertion statements to the Cherwell assertion consumer Service.

An assertion indicates that the identity provider has successfully authenticated the user and includes a user name ID (example: email address or Windows login ID) and possibly additional optional attributes about the user (example: Name, department, and more). The Cherwell Service uses the Name ID to find the user information in CSM (the user can be either a customer or an internal user), and then logs the user in to the Cherwell application without requiring further user interaction.

Note: SAML is designed for browsers. Desktop Client applications open a browser window when initiating support of the SAML authentication process. After SAML authentication has completed successfully, this window automatically closes. Each Desktop Client application maintains its own separate session information, so every time users log in to the Desktop Client, they are prompted to log in to the identity provider (with the exception of ADFS, which uses the current Windows session information).

The figure shows the CSM SAML SSO process.

User navigates to Cherwell site or starts Desktop Client. → Is SAML enabled and configured? — No → Use standard configured login process

Yes ↓

Redirect to SAML authentication service.

↓

Create SAML Authentication Request to IdP and return as auto-post form

↓

Auto post form containing SAML Authentication request to IdP.

↓

Has the User been authenticated? — Yes / No

No → Redirect browser to IdP login page. → User enters credentials on login page.

Yes ↓

Return authentication response (containing User ID) ← Yes — Can User be authenticated against User store? — No → Have number of login attempts been exceeded? — Yes → Display error page or return failure response (IdP-dependent)

No ↑

↓

Auto post form containing assertion response to SP. → Was authentication successful and User ID returned? — No → Return failure. → Display error

Yes ↓

Validate User information and authentication result. ← Return success with User information.

↓

E-mail/Windows login found in database? — No → Return failure. → Display error

Yes ↓

Create Cherwell session → Start Application

Key

| Cherwell Service |
| Client Application |
| Identtity Provider (IP) |
| Cherwell Service Provider (SP) |

The figure shows the CSM SAML IdP Initiated process.
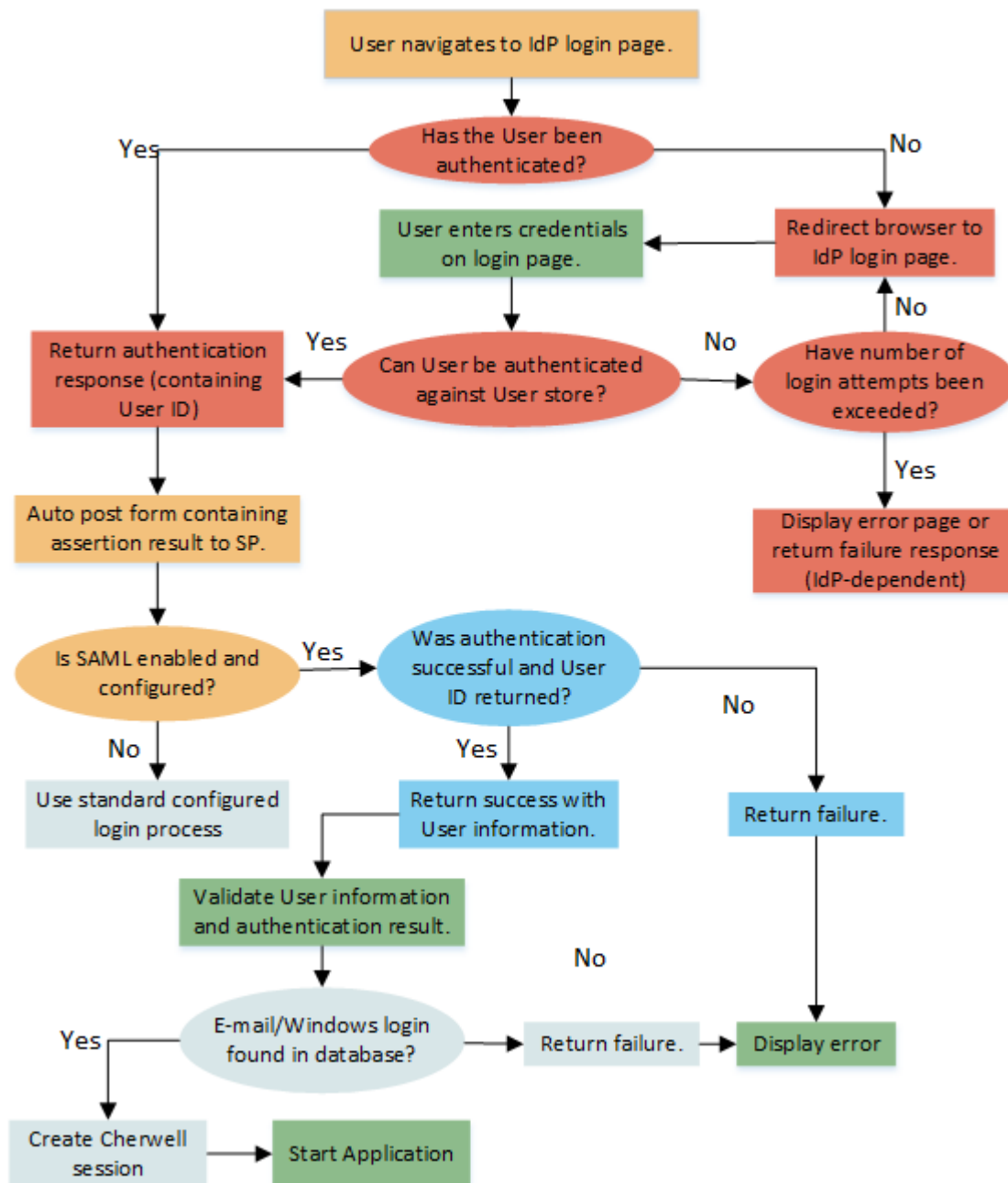
Related concepts
Configure SAML in CSM

SAML Good to Know

When using SAML, note the following integration considerations.

- Before you can use SAML, configure the integration in CSM Administrator and in the identity provider.

- Use the `/updatebrowserclientsettings/RedirectHttptoHttps` command in the Command-Line Configure utility to set a value of **true**. Redirecting HTTP requests to HTTPS provides a better, more secure logon experience.

Related concepts
Configure SAML in CSM
Configure SAML Security Rights
Related tasks
Prevent Browsing HTTP from HTTPS

SAML Configuration Components

SAML configuration components include SAML user identities, metadata, single sign-on (SSO), single logout, and identity providers.

SAML User Identities (Name IDs)

CSM supports the following types of user identities (Name IDs) in SAML assertions:

- Email addresses
- Windows login IDs

All identity providers should support email addresses and some also support Windows login IDs. Using either of these identity types allows for easy association with CSM user information because these types are already supported by CSM. Users only need to select which type to use, verify that the identity provider supports it, and verify that information is populated for all users in the CSM Database and that the ID is unique across all users.

> **Note:** For users on Windows environments, the recommended solution is to use ADFS and Windows account names. This solution is known to work well and potentially requires less logging in. Using account names also avoids issues where multiple users share the same email address. When using other identity providers, particularly those that are hosted outside the organization's network, email addresses might be the only solution available.

SAML Metadata

SAML defines a format for metadata, which is provided in the form of an XML document that describes what is supported and required by an identity or service provider. Metadata is a convenient way to set up providers without having to enter complex information manually. CSM provides the ability to import metadata for identity providers and to export metadata for the CSM Service Provider.

SAML SSO

SAML was intended to be used primarily with browser-based applications. The authentication process is implemented through page posts and redirects through the user's browser. This normally is automatic and transparent and does not require any interaction with the user, with the exception of the initial login at the identity provider. After the user is authenticated, the user credentials are kept in the browser session. If the user logs in again or logs into a different SAML-based application, the authentication process is normally automatically complete without further prompting.

SAML is designed for browsers. CSM Desktop Client applications open a browser window when initiating support of the SAML authentication process. After SAML authentication has completed successfully, this window automatically closes. Each Desktop Client application maintains its own separate session information, so every time a user logs in to a Desktop Client, they are prompted to log in to the identity provider (with the exception of ADFS, which uses the current Windows session information).

Note: User credentials are kept in the browser session, so it is very important for the user to close all browser applications when logging out to prevent someone else from using their credentials.

SAML Single-Logout

SAML defines a single-logout protocol. SAML single-logout is not supported by CSM because of its limited support by identity providers.

The single-logout allows a user to select a global logout feature in a SAML application, which logs out the user from the current application, and also sends notifications to all SAML applications running in the current session to log out the user. There are a number of issues with this feature, and it is not always supported by identity providers. For example, Shibboleth does not support the logout feature at all, and Microsoft ADFS only supports it in a limited way.

SAML Identity Providers

You can configure a SAML service provider such as Microsoft ADFS to work with CSM. Microsoft ADFS supports SAML with Active Directory and is the best choice for organizations where users are internal employees using Windows. For ADFS, the most commonly configured SAML name ID type would be the Windows login ID, although email addresses can also be used. As long as a user is logged into the same network as the ADFS service, the user should be able to use any configured SAML application without ever being prompted for a login. If the user is not directly logged into the network, the user is prompted to login through ADFS.

CSM supports an identity-provider initiated SAML feature. Users log in to the identity provider page using their login information and select CSM as the desired service provider, which transfers users to CSM after login.

SAML Signing Certificates

Security is one of the most important concerns when using an SSO framework like SAML. Ensure that messages are actually coming from the expected identity and service provider rather than a malicious third party.

To ensure the identity of message originators, signing certificates are used within messages. These certificates are stored in both the identity and service providers at the time of configuration. In addition, some data might be optionally encrypted.

To use Cherwell SAML SSO, gather a number of standard x.509 certificates for use by the Cherwell Server. A self-signed certificate can be used temporarily during initial testing. For production, use a publicly trusted X.509 certificate from a public third-party certification authority (CA).

Identity Provider Token Signing and Encryption Certificates

The identity provider uses a certificate to verify the source of its communications to CSM (referred to as a token-signing certificate). The identity provider's public certificate needs to be imported into CSM. The easiest approach is to import the metadata provided by the identity provider as a file into CSM. The metadata includes configuration information as well as certificates. If configuring the identity provider manually, copy and import its public certificate manually into Cherwell. In addition to the signing certificate, the identity provider may optionally also use a separate token encryption certificate. To import this certificate into CSM, import the identity provider's metadata file.

Service Provider Token Signing Certificate

Like the identity provider, CSM (acting as a service provider) must use a token signing certificate, and the public certificate must be imported into the identity provider. For this purpose, both a public certificate (typically with a .cer file extension) and matching private key certificate (typically with a .pfx file extension) must be created. The private key certificate must be imported into the CSM using the Administrator SAML settings. The public certificate needs to be imported into the identity provider. The easiest way to do this is to export the CSM settings as metadata, and then import the metadata (which includes the certificate) into the identity provider.

Note: Network IT staff normally manage signing certificates and should be knowledgeable about the procedure for obtaining new certificates. Certificates must be obtained from trusted certificate authorities (such as VeriSign, Thawte, GoDaddy, and more).

Configure SAML in CSM

SAML is configured in CSM Administrator and in the identity provider.

Follow this general process to configure SAML in CSM.

Task	Notes
1. Obtain and apply a self-signed certificate on your CSM server. This task is typically performed by an organization's IT department.	See SAML Signing Certificates.
2. In CSM Administrator, grant security rights to system administrators so they can configure SAML.	See Configure SAML Security Rights.
3. In CSM Administrator, set SAML identity provider options, and then import the identity provider metadata file.	See Configure the SAML Identity Provider.
4. In CSM Administrator, set SAML service provider options, and then export the CSM service provider metadata file.	See Configure CSM as a SAML Service Provider.
5. Complete the steps to configure the SAML identity provider.	See Configure Microsoft ADFS for CSM.
6. In CSM Administrator, configure automatic user account creation and updates in CSM. This option only applies when Microsoft ADFS is used and when Windows logins are used as the SAML name ID.	See Configure Automatic User Imports From SAML.
7. In CSM Administrator, enable SAML as a supported login mode.	See Enable SAML.

Related concepts
Configure the SAML Identity Provider

Configure SAML Security Rights

Security rights control access to CSM functionality and are configured in the Security Group Manager in CSM Administrator.

To configure security rights:

1. In CSM Administrator, open the **Security Group Manager** (**Security > Edit security groups**).
2. In the **Info** tab, provide the name of the Security Group (example: Admin).
3. Select the **Rights** tab.
4. In the **Category** menu, select **Security features**.
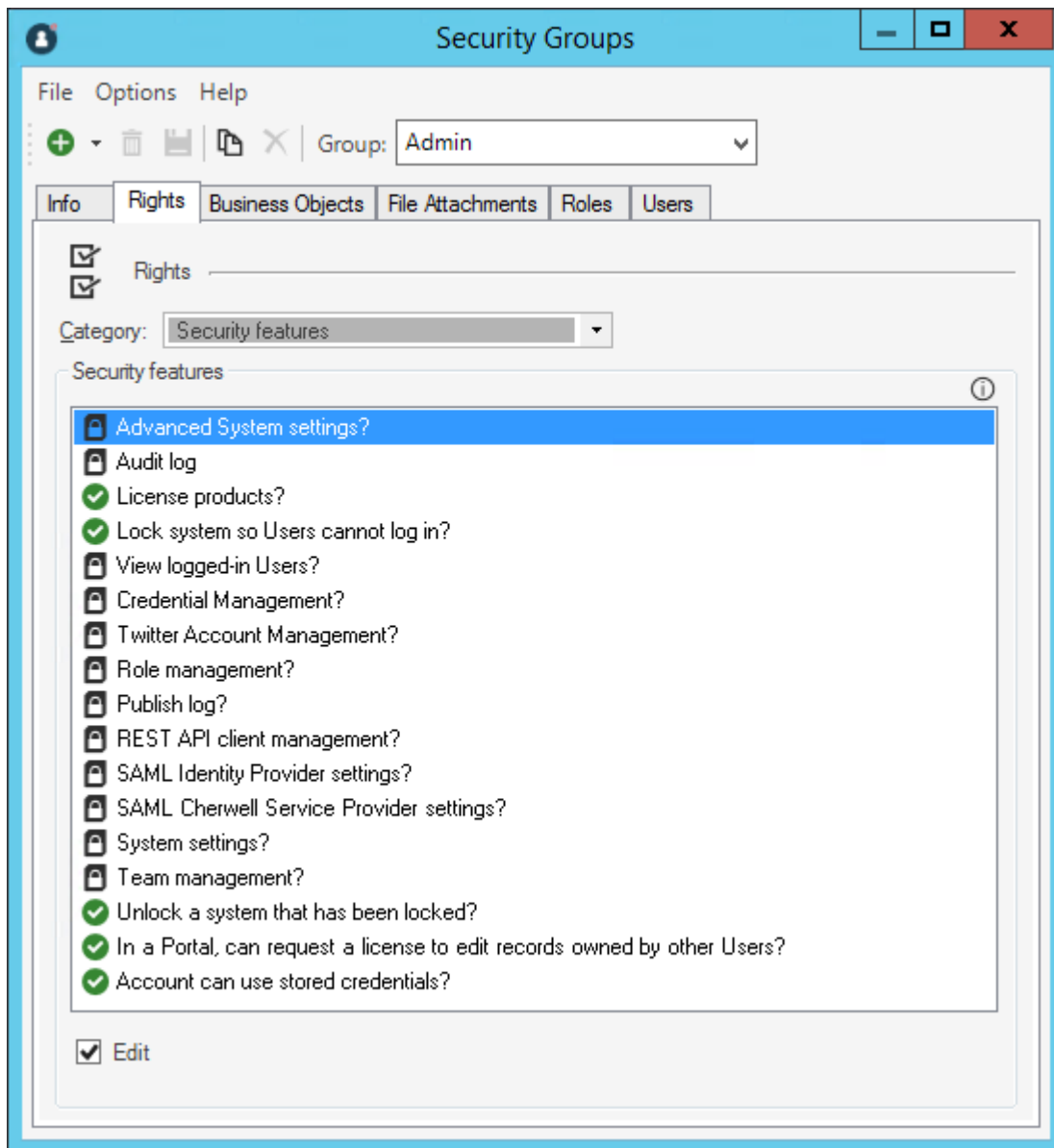
5. Select each security feature right, and then select the appropriate check box to (example: Allow, View, Add, Edit, and Delete). Use the following descriptions as a guide:
   ◦ **SAML Cherwell Service Provider settings?**: When **Edit** is selected, system administrators can edit the service provider settings and configure CSM as a SAML Service Provider.
   ◦ **SAML Identify Provider settings?**: When **Edit** is selected, system administrators can edit the identity provider settings and configure the SAML Identity Provider.
   ◦ **System settings?**: When **Edit** is selected, system administrators can edit system settings and enable SAML.

Related concepts

Security Rights

Configure the SAML Identity Provider

Integrate CSM with a SAML-compliant identity provider such as Microsoft Active Directory Federation Services (ADFS).

Each identity provider uses a different procedure for integrating with CSM. The procedures in this section provide some sample guidelines on how to configure CSM with each identity provider. Refer to the specific identity provider documentation for guidelines on installing and initially configuring the identity provider, and to ensure that the correct configuration steps are followed for the desired implementation.

Tip: A convenient way to create the configuration is to import the identity provider's metadata. This configures all the required settings except for the selection of the type of ID. However, you can manually enter all the data and import the signing certificate, if needed.

To configure the SAML identity provider:

1. In CSM Administrator, create a Blueprint.
2. From the toolbar menu, select **Tools > Edit SAML Settigs**.
3. Select the **Identity Provider** page.
4. Select **Import Metadata**.
5. When prompted for a file name, select the Service Provider's metadata .xml file. For example, use the metadata file from ADFS.
   The following information is automatically imported from the metadata file. If it is not, you can manually enter information into the writable fields.

Option	Description
Entity URL	A URL that uniquely identifies the identity provider. This is provided by the identity provider.
Organization Name	(Optional) The name of the identity provider, used only for display.
Organization URL	(Optional) The main URL of the identity provider, used only for display.
Single-Sign-On URL	The URL of the identity provider's authentication service. This should always be a secure URL (beginning with https:).

Option	Description
Certificate	The identity provider signing certificate (a standard .cer file) is used to verify messages from the identity provider. **Note:** Signing certificates are normally managed by network IT staff; IT should be knowledgeable about the procedure for obtaining new certificates. Certificates must be obtained from trusted certificate authorities (such as VeriSign, Thawte, GoDaddy, and more).

6. If you have changed the SSO URL or are re-routing requests to a SSO URL outside the CSM environment, you must list proxy SSO URLs here. Select **Add** and provide the URL(s). They are added to the safe URLs list in the form-action attribute in the Content Security Policy header.

7. From the **Type of ID** options, select the type of ID (SAML Name ID) to request from the identity provider:
   ◦ **Email Address**: Select this option to use email addresses as the SAML Name ID. See Use E-mail Address as the Name ID.

     Note: When using email address, ensure that the Email Attribute is set on the Email Address Field of the User/Customer Business Objects (User Info and Customer-Internal).

   ◦ **Windows Login**: Select this option to use the Windows login ID as the SAML Name ID. This option must be selected if you want to automatically update user imports from SAML. See Use Windows Login as the Name ID.

8. Select the **Hide SAML authentication window** check box to hide the SAML authentication window used by the CSM Desktop Client.

     Note: This should be used only with ADFS and when users are normally logged into the same network, in which case users are never prompted to log in and so the browser window might be considered an unnecessary distraction.

9. Select the appropriate signing options to configure SAML signing certificates according to your identity provider's parameters. When an authentication response is returned, it may consist of many SAML assertions. Identity providers may sign the entire response, sign individual assertions, or both. For example, ADFS signs individual assertions but not entire responses. Consult documentation from your identity provider to determine the appropriate settings. You must select at least one option.

10. Optionally, select the **Force** check box to disable Force Authentication. Authentication is forced by default; this means users are required to enter their credentials each time they access CSM.

Warning: Cherwell strongly recommends that you do not disable Force Authentication, as it decreases security. If you are considering disabling Force Authentication (due to network/ physical server environments, or to make it easier for users to maintain a session), please contact Cherwell Support to ensure you understand the implications.

Optional web.config settings:

- Adjust the server time allowance to allow for differences in clocks on the identity provider and local servers. This setting will default to 60 seconds but can be overridden by a setting in the web.config files for both Cherwell Service and the REST API. To override the default setting, specify a value in seconds in the web.config files as follows:

```
<add key="SAMLServerTimeAllowance" value="90" />
```

- If using SAML and a non-ADFS identity provider, you must add this setting to the web.config file in the Cherwell Service folder. Specify the setting under the <appSettings> section as follows:

```
<add key="IdpIsAdfs" value="false"/>
```

If you have upgraded and are using ADFS, you do not need to add the setting.

Related concepts
SAML Signing Certificates
Related tasks
Create a Blueprint

Configure CSM as a SAML Service Provider

Use the **Service Provider** page in the **SAML Settings** window to configure CSM as a SAML Provider.

To configure CSM as a SAML Service Provider:

1. In CSM Administrator, create a Blueprint.
2. From the menu, select **Tools > Edit SAML settings**.
3. Select the **Service Provider** page.
4. Provide CSM identity information:

Option	Description
Entity URL	Provide the URL that identifies the service provider. The entity and service URLs should use the same domain as specified in the signing certificates.
Organization name	(Optional) Provide the service provider organization name used only for display.
Organization URL	(Optional) Provide the URL of the service provider organization used only for display.
Web service URL	Provide the Cherwell web service URL (example: https://host.domain/CherwellAPI). If you are upgrading CSM, the existing SAML web service URL is automatically updated to match the Cherwell REST API URL that us entered in the upgrade prompt. For example, if the REST API URL is https://host.domain/CherwellAPI/api/, the web service URL will be updated to https://host.domain/CherwellAPI (without the /api at the end of the path).
CSM default startup URL	Provide the CSM Client or CSM Portal URL for the site to be redirected to after logging in using SAML Identity-Provider initiated authentication.

Option	Description
Validate SAML authentication	After a user is successfully authenticated through SAML, CSM receives a response that the user is valid. To verify that the user valid response is itself is valid, CSM sends a request to a CSM web service to authenticate the response. Select whether the request is sent: **From Server (recommended)** **From Client**: Provided for backwards compatibility and in cases where the *from server* option might be incompatible with the network configuration. This is a less secure option. **Note:** In most configurations, this option only impacts the behavior of the CSM Desktop Client.
Signature algorithm	Select the Secure Hash Algorithm to use for signing SAML messages between CSM applications and your identity provider. SHA-1 and SHA-256 are supported, but SHA-256 is the default and recommended option, particularly for customers who operate under General Data Protection Regulation (GDPR) jurisdiction.

5. Import the Private Certificate: Personal Information Exchange Format (.pfx) file containing a certificate with a private key. This certificate must be issued by a trusted certificate authority. To import a private certificate, select **Import** and select the **.pfx file**. There is a prompt to enter the password for the file.

> **Note:** Signing certificates are normally managed by network IT staff; IT should be knowledgeable about the procedure for obtaining new certificates. Certificates must be obtained from trusted certificate authorities (such as VeriSign, Thawte, Go Daddy, and more).

6. Export the service provider settings to a metadata file.

> **Tip:** Use this file later to import the service provider metadata into the identity provider.

   a. Select **Export Metadata** to open the **Export File** window.
   b. Select a name and location for the metadata .xml file.

Related concepts
SAML Signing Certificates

Configure Automatic User Imports From SAML

You can configure automatic user account creation and updates in CSM when users log in using SAML. Control the user data and group membership passed to CSM by mapping ADFS attributes to Business Object fields and Active Directory security groups to CSM Security Groups.

This feature is only supported when SAML is configured with Microsoft ADFS.

The process for configuring automatic user updates requires setup in ADFS and in CSM Administrator.

Task	Notes
1. In Microsoft ADFS, verify that Windows login IDs are used as the SAML name ID that identifies users.	See Use Windows Login as the Name ID.
2. In Microsoft ADFS, verify that email addresses are not used as the SAML name ID that identifies users.	See Use E-mail Address as the Name ID.
3. In Microsoft ADFS, configure user attributes that will be passed to CSM. For example, create attributes such as first name, last name, email address, etc.	See Configure User Attributes in ADFS.
4. In Microsoft ADFS, add a rule for every Active Directory security group that you want to map to a CSM Security Group.	See Map SAML Security Groups to CSM Security Groups.
5. In CSM Administrator, verify that the type of ID set for the identity provider is **Windows Login**.	See Configure the SAML Identity Provider.
6. In CSM Administrator, add the **SAMLImport** general attribute to the User Business Object.	See Add SAMLImport Attribute to User Business Object.
7. In CSM Administrator, map attributes in the Business Object that stores user information to ADFS attributes.	See Map Active Directory User Attributes to CSM User Fields.
8. In CSM Administrator, map Active Directory groups to CSM Security Groups.	See Map SAML Security Groups to CSM Security Groups.

Related concepts
Windows Credentials
Related tasks
Configure User Attributes in ADFS
Map Active Directory User Attributes to CSM User Fields
Configure Groups in ADFS
Map SAML Security Groups to CSM Security Groups

Add SAMLImport Attribute to User Business Object

Before you can automatically create and update user accounts from SAML, you must apply a special general attribute to the Business Object used to store user data.

To apply the SAMLImport attribute:

1. Create a Blueprint.
2. From the **Object Manager**, select the Business Object used to store user data. For example, select the UserInfo Lookup Table.
3. Select **Edit Business Object**, and then select **Bus Ob Properties**.
4. Select the **Advanced** page.
5. Expand **General Attributes**.
6. Add **SAMLImport** to the **Attribute** column.
7. Select **OK**.
8. Publish the Blueprint.

Map Active Directory User Attributes to CSM User Fields

Map Active Directory user attributes to User Business Object fields so that data is copied to the user record when the user logs in to CSM through SAML.

You need the list of Active Directory attributes added in the AD FS Management tool. See Configure User Attributes in ADFS.

To map Active Directory User Attributes:

1. In CSM Administrator, create a Blueprint.
2. From the toolbar menu, select **Tools > Edit SAML Settigs**.
3. Select the **User Mapping** page.
4. Select the **Create or update users when logging in users SAML** check box.
5. Select **Add**.
6. In the Attribute name box, type the exact name of the Active Directory attribute.
7. Select one of these options:
   - **New Field**: Add a new Business Object field to map to the Active Directory attribute. You must also select a data type and size.
   - **Existing Field**: Select an existing field in the User Business Object.
8. Repeat for each Active Directory attribute added to ADFS.
9. Publish the Blueprint.

Map SAML Security Groups to CSM Security Groups

Map SAML groups to CSM Security Groups to ensure that new and updated user accounts are added to the correct CSM Security Group when users log in using SAML.

You need the list of groups you added in the AD FS Management tool. See Configure Groups in ADFS.

Keep in mind that users can belong to multiple SAML groups but only one CSM Security Group. You can associate multiple SAML groups to a single CSM Security Group, but you cannot assign a single SAML group to multiple CSM Security Groups.

For example, a user may belong to two SAML groups:

- Domain Admins
- Network Admins

In this case, you must choose one CSM Security Group for the user, such as the Admin group.

1. In CSM Administrator, open the **Security Group Manager** (**Security > Edit security groups**).
2. From the **Group** drop-down list, select the CSM Security Group you want to map to a SAML group.
3. Select the **Users** page.
4. In the SAML Groups area, select **Add**.
5. Type the name of the SAML group to associate with the selected CSM Security Group.
6. Select **OK**.

   🖉 **Note:** If you have already mapped the SAML group to a different CSM Security Group, you are given the option to change the assignment to the group you are currently modifying.

7. Repeat this step for each SAML group that should be mapped to the CSM Security Group.
8. Select **Order Groups**.
9. Order the list to determine the assignment priority for users who belong to multiple SAML groups. When these users log in using SAML, the first SAML group found determines which CSM group the users are assigned to.
10. Select **OK**.

Enable SAML

Before SAML can be used, SAML must be enabled as a supported login mode. The other login types can also be enabled so that if SAML authentication fails, or the user cancels the process, the next configured login method is invoked.

By default, the CSM Web Applications use the same security settings as those configured for the CSM Desktop Client Applications; however, configure the system to use different login modes for each. Select **Browser Client** or **Browser Portal**, and then clear **Use Same Settings as Desktop Client**, and then enable or disable SAML authentication separately for each type of application.

To enable SAML:

1. In the CSM Administrator main window, select **Security > Edit security setting**.
2. Select **Desktop Client**.
3. Under **Supported login modes**, select **SAML**.

   SAML authentication is now enabled and, if configured, is now invoked for users logging in.

4. Select **OK**.

Note: There might be a delay (up to 15 minutes or so) before the new configuration is loaded and made available by the SAML Web Services.

Configure Microsoft ADFS for CSM

Configure Microsoft Active Directory Federation Services (ADFS), an add-on product for Active Directory that supports identity federation protocols, including SAML 2.0.

Note: CSM provides integration with third-party identity providers, not support. For more information about your AD/ADFS setup, work with an AD/ADFS Administrator.

Note: This topic applies to versions of ADFS that are currently supported by Microsoft.

Task	Notes
1. In CSM, follow steps 1-4 in Configure SAML in CSM.	
2. In Microsoft ADFS, verify DNS and certificate settings.	See Verify DNS and Certificate Properties in ADFS.
3. In Microsoft ADFS, import or manually add CSM as a relying party trust.	See Manually Add CSM as a Relying Party.
4. In Microsoft ADFS, configure the type of SAML Name ID. **Note:** To automatically import new and updated user accounts in CSM, you must use Windows login IDs.	See Use E-mail Address as the Name ID or Use Windows Login as the Name ID.
5. In Microsoft ADFS, configure user attributes if you want to automatically import new and updated user accounts in CSM.	See Configure User Attributes in ADFS.
6. In Microsoft ADFS, configure groups if you want to automatically import new and updated user accounts in CSM.	See Configure Groups in ADFS.
7. In Microsoft ADFS, configure ADFS as the SAML Identity Provider.	See Configure the SAML Identity Provider.

Verify DNS and Certificate Properties in ADFS

Before you configure SAML for CSM, verify that the general properties of ADFS are configured correctly.

1. Open the ADFS x.x Manager.
2. Right-click **Service** and select **Edit Federation Service Properties**.
3. Verify that the settings on the **General** tab match the correct DNS and certificate common names.

Import the CSM Service Provider Metadata File into ADFS

1. Start the ADFS x.x Manager.

2. Select **Add Relying Party Trust**.

3. Select **Import data about the relying party from a file**.

4. Select the **CSM Service Provider metadata file** exported when CSM was configured as a service provider.

5. Provide a display name, and then select **Next**.

6. Select **Permit all users to access this relying party**, and then select **Next**.

7. Ensure that the **Open the Edit Claim Rules dialog for this relying party when the Wizard closes** check box is selected, and then select **Close**.

Manually Add CSM as a Relying Party

Add CSM Service Provider to Microsoft Active Directory Federation Services (ADFS) as a relying party.

🖉 **Note:** This topic applies to versions of ADFS that are currently supported by Microsoft.

To manually add CSM as a relying party:

1. Start the ADFS x.x Manager.
2. Under **Trust Relationships** (left of the window), select **Relying Party Trusts**.
3. On the right, select **Add Relying Party Trust**.
4. Select **Start**.
5. Select **Enter data about the relying party manually**, and then select **Next**.
6. Provide a display name, and then select **Next**.
7. Select **ADFS x.x profile**, and then select **Next**.
8. Import an encryption certificate:
   a. Select **Browse**, and then select the **certificate (.cer file)** that was used when setting up the CSM Service Provider.
   b. Select **Next**.
9. Select **Enable support for the Saml 2.0 WebSSO protocol**, and enter the URL to the Cherwell web service page that is used as the assertion consumer. This is the domain followed by CherwellAPI/saml/assertion (example: https://www.mycompany.com/CherwellAPI/saml/assertion).
10. Select **Next**.
11. Provide a URL for the relying party trust identifier. The URL must match what was entered in CSM as the service provider entity ID.
12. Select **Add**, and then **Next**.
13. Select **Permit all users to access this relying party**, and then select **Next**.
14. Verify the selections, and then select **Next**.
15. Ensure that the **Open the Edit Claim Rules dialog for this relying party when the Wizard closes** option is selected, and then select **Close**.
16. On the **Issuance Transform Rules** tab, select **Add Rule**, and then follow the instructions for the desired type of ID.
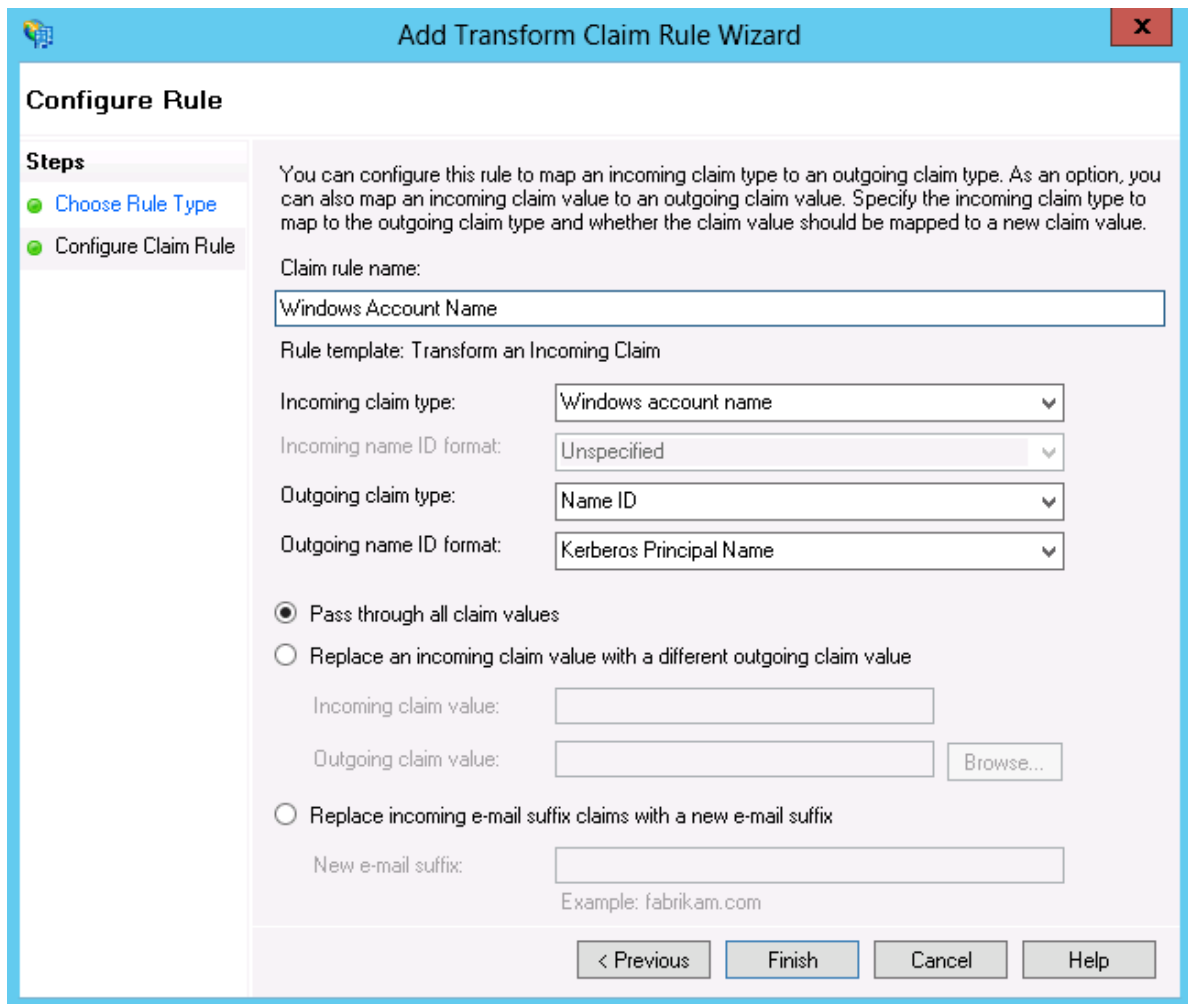
Use Windows Login as the Name ID

For users on Windows environments, the recommended solution is to use ADFS and Windows account names. Windows logins are required if you intend to automatically create and update user accounts from SAML.

If the Add Transform Claim Rule Wizard is not already open, select **CSM Relying Party**, and then select **Edit Claim Rules** (on the right), and then select **Add Rule** on the **Issuance Transform Rules** tab.

To use Windows Login as the Name ID:

1. For Claim rule template, select **Transform an Incoming Claim**, and then select **Next**.
2. Provide a name for the claim rule (example: Windows account name).
3. In the **Incoming claim type** field, select **Windows account name**.
4. In the **Outgoing claim type** field, select **Name ID**.
5. In the **Outgoing name ID format** field, select **Kerberos Principal Name**.
6. Select **Select Pass through all claim values**.

7. Select **Finish**.

Use E-mail Address as the Name ID

Before you choose to use email addresses as the SAML Name ID, verify that your identity provider can return the desired type of ID. For some identity providers, particularly those that are hosted outside the organization's network, email address might be the only solution available.

To use E-mail Address as the Name ID:

1. For Claim rule template, select **Send LDAP Attributes as Claims**, and then select **Next**.

2. Provide a claim rule name (example: E-mail Attribute).

3. In the **Attribute store** field, select **Active Directory**.

4. Under **Mapping of LDAP attributes to outgoing claim types**, select **E-mail-Addresses** in the **LDAP Attribute** column and **E-mail Address** in the **Outgoing Claim Type** column.

5. Select **OK**.

6. Select **Add Rule**.

7. For Claim rule template, select **Transform an Incoming Claim**, and then select **Next**.

8. Provide a claim rule name (example: E-mail Address).

9. In the **Incoming claim type** field, select **E-mail Address**.

10. In the **Outgoing claim type** field, select **Name ID**.

11. In the **Outgoing name ID format** field, select **Email**.

12. Select the **Select Pass through all claim values** radio button.

13. Select **OK**.

After completing the above steps, change the following:

1. Under **Trust Relationships** (left-hand side), select **Relying Party Trusts**, and then double-click the entry for the CSM Relying Party.

2. Select the **Advanced** tab.

3. Select the Secure Hash Algorithm specified on the **SAML Settings - Service Provider** page. SHA-1 and SHA-256 are supported, but SHA-256 is the default and recommended option, particularly for customers who operate under General Data Protection Regulation (GDPR) jurisdiction.

4. Select **OK**.

Related tasks
Configure CSM as a SAML Service Provider

Configure User Attributes in ADFS

Create or configure Active Directory user attributes that you want to map to fields in the CSM User Business Object. This is typically the CSM User Info Lookup Object, but it could be a different table based on your user implementation.

To configure Active Directory user attributes:

1. Open the AD FS Management tool.
2. From the navigation pane, expand **Trust Relationships**, and then select **Relying Party Trusts**.
3. Select the CSM server that is configured for SAML.
4. Select **Edit Claims Rules**, and then select **Add Rule**.
5. From the **Add Transform Claim Rule Wizard**, select the **Send LDAP Attributes as Claims** rule template, and then select **Next**.
6. Add the following claim rule properties:

Property	Value
Claim rule name	Provide a name, such as User Attributes.
Attribute Store	Select Active Directory.
LDAP Attribute	Add an entry for each attribute you want to pass to CSM. For example, add Given Name, Surname, E-mail Addresses, and Department.
Outgoing Claim Type	Type (do not select) a name for each attribute. For example, add First Name for the Given Name attribute.

7. Record the Outgoing Claim Type entries you make so have the names when you map them to Business Object fields in CSM.

8. Select **Finish**.

9. Map the Outgoing Claim Types to Business Object fields. See Map Active Directory User Attributes to CSM User Fields.

Configure Groups in ADFS

Create or configure Active Directory groups that you want to map to Security Groups in CSM. Users are automatically added to the mapped CSM Security Group when their account is created or updated.

To configure groups in ADFS:

1. Open the AD FS Management tool.
2. From the navigation pane, expand **Trust Relationships**, and then select **Relying Party Trusts**.
3. Select the CSM server that is configured for SAML.
4. Select **Edit Claims Rules**, and then select **Add Rule**.
5. From the **Add Transform Claim Rule Wizard**, select the **Send Group Membership as a Claim** rule template, and then select **Next**.
6. Add the following claim rule properties:

Property	Value
Claim rule name	Provide a name, such as Admin or IT Service Desk Level 1. For easier maintenance, choose a name that matches Security Group names in CSM.
User's Group	Select Browse, and then add the domain name group you want to map to CSM Security Groups. For example, add Domain Admins if you want to automatically add users in this group to the Admins Security Group in CSM.
Outgoing Claim Type	Select Group.
Outgoing Claim Value	Provide a name for the group. This is the name you will use to map the ADFS group to a CSM Security Group.

7. Record the group names you added so have the names when you map them to Security Groups in CSM.

8. Select **Finish**.

9. Repeat this process for each ADFS group you want to map to a CSM Security Group.

10. Map the ADFS groups to CSM Security Groups. See Map SAML Security Groups to CSM Security Groups.

SAML Diagnostics

SAML logging is included with general CSM logging features and is configured using the Server Manager.

The following sections discuss how to test and troubleshoot SAML.

Troubleshoot SAML

When SAML is enabled and correctly configured, a web page initially opens after the CSM Desktop Client or CSM Browser Client are opened. The web page indicates that a SAML authentication request has been sent to the identity provider (this might appear very briefly), and then the identity provider's login page can be seen.

If the web page does not open or other issues are experienced related to SAML, try the following suggestions.

1. After SAML settings have been changed, it might take a while before the settings are reloaded into the Application Server. Ensure the latest settings are active by restarting the IIS Web Server and the Cherwell server (through the Cherwell Server Manager application). Also, clear the local browser cache.

2. Verify that the selected identity provider ID type (email address or Windows login) matches the type of ID that the identity provider is configured to return.

3. If settings were manually configured in the CSM Administrator for an identity provider (rather than by importing a metadata file), verify that the entity and SSO URLs exactly match what is specified by the identity provider. The URLs for some identity providers are case sensitive.

4. Verify that the domains contained in certificates match the domains of the identity and service provider URLs and are issued by a recognized Certificate Authority and have not expired.

5. Recheck the SAML settings in CSM and the identity provider to ensure that they are correct and consistent.

6. Ensure that the date and time are synchronized on the Cherwell and identity provider servers.

To access CSM clients without SAML authentication, select **Cancel** in the SAML window that is initially displayed. This skips the SAML authentication step and displays the login window (or whatever the next login option that is configured).

Test SAML With a Browser

Run a simple test using a web browser and view the results of a SAML authentication without running a client application by following the steps below.

To test SAML through a browser:

> **Note:** In the steps below, the URL saml.cherwell.com should be replaced with the actual URL. This can also be done as an easy way to generate debug logs.

1. Navigate to `https://MyServer/Service/SAML/login.aspx`. The browser redirects to the identity provider and prompts a login.

2. Provide the User credentials.
   After the identity provider response has been processed, a page opens and displays the important information returned to the service provider, such as result status codes, the user name ID, session ID, and the authentication and assertion xml body.

Bypass SAML for Individual Users

If you are using a login method other than SAML (external, LDAP, Windows, internal), bypass SAML authentication and log in using a different method. For example:

- For the Desktop Client, select **Cancel** on the SSO dialog after SAML authentication has begun and the next login method is invoked.

- For CSM Web Applications, use a special URL to bypass SAML authentication and display the standard login dialog, which also includes a link to initiate SAML authentication. Add `CherwellLogin` to the end of the URL normally used to access the technician or Portal site, such as:
  ```
  http://myserver/CherwellPortal/CherwellLogin
  ```
  or
  ```
  http://myserver/CherwellClient/CherwellLogin
  ```

If the CSM Portal site is configured to allow Anonymous access, select **Click to Login** to start the SAML authentication. SAML authentication can also be started immediately by adding `SamlLogin` to the URL (similar to adding `CherwellLogin` as described above). To go directly to the login page, add `CherwellLogin` to the URL.

Bypass SAML for All Users

To bypass the initial SAML authentication for all users for either the Browser Client or CSM Portal, use the Command-Line Configure utility to pass the following command to Overwatch:

```
/updateportalsettings /defaultauthmode=CherwellLogin
```

This setting bypasses SAML authentication and forces the login dialog to be displayed instead. SAML authentication is available using the link provided on the login dialog.

Diagnose Microsoft ADFS Errors

If an error is displayed by Active Directory Federation Services (ADFS) during SAML authentication, more information about the error is available in the Windows Event Viewer on the ADFS server.

Note: This topic applies to versions of ADFS that are currently supported by Microsoft.

To open the Event Viewer on the ADFS server:

1. Open the Event Viewer by navigating to **Start > Programs > Administrative Tools > Event Viewer or Control Panel > Administrative Tools**.

2. In the console tree, expand **Applications and Service Logs > ADFS**, and select **Admin**.

To enable a debug trace viewer for more detailed information:

1. On the menu bar, select **View > Show Analytic and Debug Logs**.
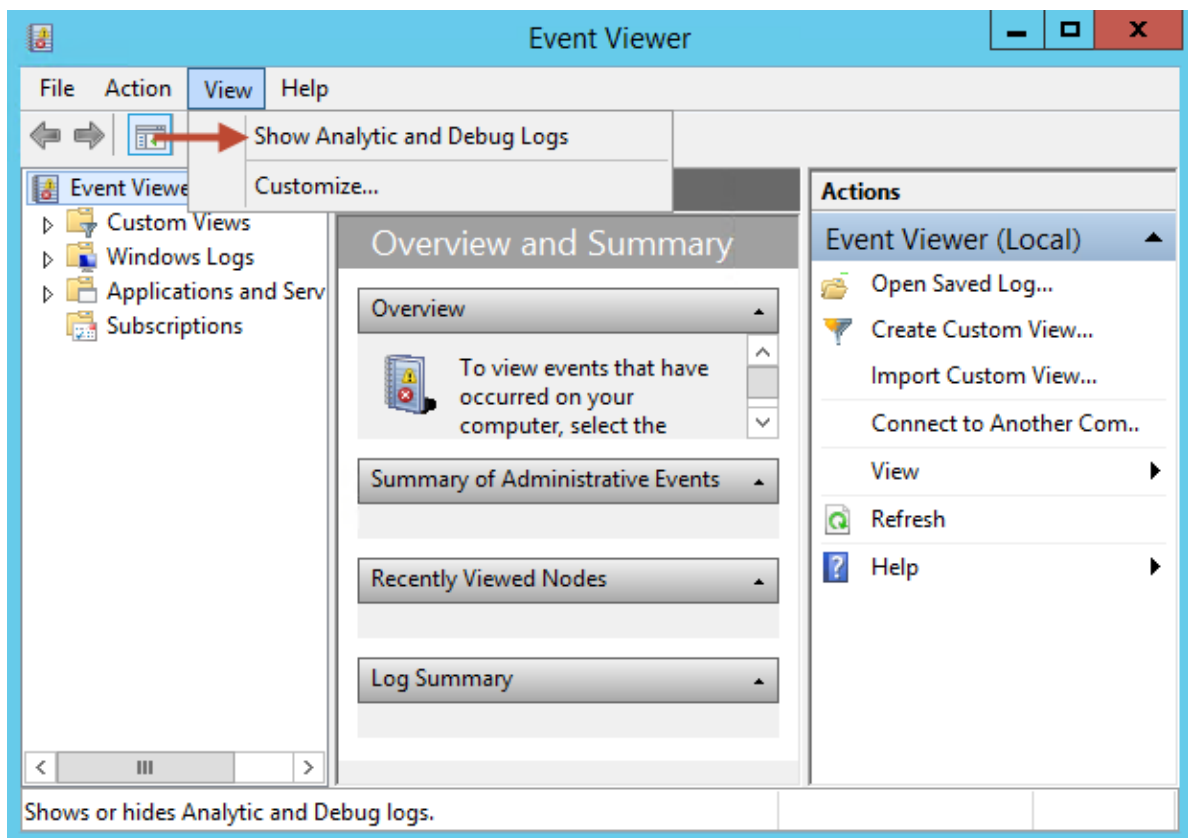
2. In the console tree, expand **Applications and Services Logs > ADFS x.x Tracing**, and then select **Debug**.

3. In the **Actions** pane, select **Enable Log**. Tracing for ADFS x.x is now enabled.

4. Restart the ADFS x.x Windows Service.

Resolve Problems Using ADFS with Chrome or Firefox Browsers

If Microsoft Active Directory Federation Services (ADFS) appears to be working with Internet Explorer but problems occur when using Chrome, Firefox, Safari, or other browsers (example: Continuously seeing the ADFS login prompt), the ExtendedProtectionTokenCheck on the ADFS server might need to be disabled.

Disabling this feature lessens security somewhat against man-in-the-middle attacks. If turning off this feature is not acceptable (check with your AD/ADFS administrator), Internet Explorer might be the only browser available.

Note: This feature is disabled only on the ADFS server; Users do not have to change anything with their browser.

Note: This topic applies to versions of ADFS that are currently supported by Microsoft.

To disable the ExtendedProtectionTokenCheck on the ADFS server:

1. Open the **Windows PowerShell** window (under **Administrative Tools**).
2. Provide the following command: Set-ADFSProperties -ExtendedProtectionTokenCheck None.
3. Close the **PowerShell** window.
4. Open the Internet Information Services (IIS) Manager (under **Administrative Tools**).
5. Expand **Web Server node** (left side), and then expand **Sites > Default Web Site > adfs**. Select **ls node**.
6. Double-click **Authentication under IIS**.
7. Right-click **Windows Authentication**, and then select **Advanced Settings**.
8. Change the selection under **Extended Protection** to **Off**.
9. Close the IIS Manager.
10. Restart both the IIS and ADFS Services.

Global Settings

Global settings control how CSM looks and behaves by default for all users or in some cases, users assigned to specific Roles. Configure Global settings from CSM Administrator.

Configure Global System Settings

Configure Global system settings for Search, Display, Dashboards/Calendar/Visualization, Catalog, Rich Text, Record Locking, Help, and more. Most of these settings can be configured Globally, by Role, and by user.

To configure the Global System Settings:

1. In the CSM Administrator main window, select the **Settings** category, and then select the **Edit System Settings** task.
2. Select the **Search** page and configure the Global Search settings: Full Text Search, Quick Search, and Knowledge Search settings.
3. Select the **Display** page and configure the Global Display settings: Multiple Monitor settings and a default application skin.
4. Select the **Dashboards** page and configure these Global settings: default Dashboard, Calendar, and Visualization settings.
5. Select the **Catalog** page and configure the Global Catalog settings: Whether or not to store primary system definitions in a local catalog file on a user's machine, to allow users to decide whether to use a definition catalog, and to force catalog files to be rebuilt each time a user restarts a CSM application.
6. Select the **Rich Text** page and configure the Global Rich Text settings: Determines how images are stored and shown in Rich Text Fields, size limits, and the custom default font for Rich Text.
7. Select the **Locking** page and configure the Global Record Locking settings: General Record Locking settings, OOTB Record Locking settings for all Major Business Objects, and Portal Record Locking settings.
8. Select the **Globalization** page and configure the Global Globalization settings: Determines culture settings for your system. You can override these settings for Roles or for individual users.
9. Select the **Help** page and configure the Global Help settings: Help system settings, and whether to globally enable/display Process and Terminology Help for Business Objects and Fields. Also configure a custom Support phone number and a custom report error email address.
10. Select the **Advanced** page and configure the Global Advanced settings: Dashboard Widget refresh, system notifications, web service call settings, and Google Analytics settings.

Related concepts
Configure Global Search Settings

Configure Global Search Settings

Global search settings are the foundational default search settings when these preferences are not modified by users and/or saved searches. Global search settings are configured in **CSM Administrator > System Settings > Search**.

Setting	Description
Text Search (only applies to the Query Builder)	Select the default setting for how the Query Builder searches fields: • **All Search Words Should Exist in the Same Field**: Returns records only when both words are found in a single field (example: *CSM* and *software* are found in the same field). • **Search Words Can Be Found in Different Fields**: Returns records if both words are found in different fields in the same Business Object (example: *CSM* is found in one field and *software* is found in another field). • **Search For Different Forms of the Word**: Returns records that have plural and past tense forms of the word and different verb tenses. For example, if the search is for *find*, the records found will be those with *find*, *finds*, and *found*.
Quick Search should default to using (only applies to Quick Search)	Select the default setting for how Quick Search searches fields: • **All Words**: Search uses all words (AND is used to separate words in search). With the relevancy ranking, "noise" words are included in the search (example: "the" and "will"). An **All Words** search is better at finding records where users are looking for records containing all of the words in the search string. • **Any Words**: Search uses any of the words (OR is used to separate words in search). With the Relevancy ranking, this option ranks records higher that have more of the search words. An **Any Words** search is better at ranking records by those containing the most instances of any words in the search string. 📝 **Note:** These settings only apply to Quick Searches run from the **Searching > Quick search builder** menu.
Knowledge Search should default to using (only applies to Knowledge Search)	Select the default setting for how Knowledge Search searches fields: • **All Words**: Search uses all words (AND is used to separate words in search). With the Relevancy ranking, "noise" words are included in the search (example: "the" and "will"). An **All Words** search is better at finding records where users are looking for records containing all of the words in the search string. • **Any Words**: Search uses any of the words (OR is used to separate words in search). With the Relevancy ranking, this option ranks records higher that have more of the search words. An **Any Words** search is better at ranking records by those containing the most instances of any words in the search string.

Related concepts

Query Builders

About Quick Search

Search Knowledge

Configure User Task Pane and Search Control Settings

Configure Global Display Settings

Use the **Display** page in the **System Settings** dialog to configure global display settings for the CSM Desktop Client. Global display settings are configured in **CSM Administrator > System Settings > Display**.

Application Skin

Select a default application skin from the **Skin** list to control the appearance of the Desktop Client and CSM Administrator. Options are Cherwell Light (default), Cherwell Blue, or Cherwell Dark.

The skin selected affects all users by default. However, users can change the application skin in the Desktop Client, which only affects their personal interface.

Note: You may need to close and reopen the CSM Administrator for this change to take effect.

Title Bar Info

To configure window title settings, select the **Display connection information** check box, then select an option from the drop-down list. The available window title types are:

- **Connection name**: Displays as *<connection name> connection*.
- **Database name**: Displays as *<database name> database*.
- **Environment name**: Displays as *<environment name> environment* (Production, Development, or Test).
- **Connection and database name**: Displays as *<connection name> connection, <database name> database*.
- **Connection and environment name**: Displays as *<connection name>, <environment> name*.
- **Database and environment name**: Displays as *<database name> database*, *<connection name> connection name*.
- **Connection, database, and environment**: Displays as *<connection name> connection, <database name> database, <environment name> environment*.

  If no environment value is selected, the content displays as *Unknown environment*.

Note: This setting applies to the current database only. If the user has set the window title to a different setting in the Desktop Client, that setting will override this one.

Web Appearance

You can choose to display form controls with right-angled or rounded corners.

Related concepts
Configure User Display Settings
Connections

Configure Global Dashboard, Calendar, and Visualization Settings

Configure global default dashboards, calendars, and visualization settings for all CSM Desktop Client users. Global settings are configured in **CSM Administrator > System Settings > Dashboards, etc.**.

Setting	Description
Default Dashboard	Select the **Dashboard** button to open the **Dashboard Manager**, and then select an existing dashboard or create a new dashboard to use as the system default.
Default Heads-up Display	Select the **Dashboard** button to open the **Dashboard Manager**, and then select an existing dashboard or create a new dashboard to use as the global heads-up display.
Default Dashboard Theme	From the drop-down list, select a dashboard theme to apply to all dashboards in the system.
Default Calendar	Select the **Calendar** button to open the **Calendar Manager**, and then select an existing calendar or create a new calendar to use as the default.
Default config visualization	Select the **Visualization** button to open the **Visualization Manager**, and then select an existing visualization or create a new visualization to use as the default.

Related concepts

Dashboards

Heads-Up Display (HUD)

About Calendars

About Visualizations

Related tasks

Configure User Dashboard and Calendar Settings

Configure Global Catalog Settings

Use global catalog settings to determine how core system definitions are retrieved. Global catalog settings are configured in **CSM Administrator > System Settings > Catalog**.

When the CSM Desktop Client is initially launched, core system definitions are retrieved from the server and stored in a local catalog file. Definitions do not need to be retrieved again unless a Blueprint is published. You can configure how users receive updated definitions.

Setting	Description
Store Primary System Definition in a Local Catalog File on Users' Machines	Select this option to retrieve core system definitions from the server when the Desktop Client is initially launched, and then store them in a local definition catalog file. Definitions do not need to be retrieved again unless a Blueprint is published.
Allow Users to Decide Whether or Not to Use a Definition Catalog	Select this option to allow users to override the above default and set their own personal datalog defaults in the Desktop Client (**Tools > Options > General**).
Invalidate all Current Catalogs	Select this option to force all local catalog files to be built the next time each user starts a CSM application.

Related concepts

About Blueprints

Configure User General Settings

Configure Global Rich Text Settings

Use Rich Text settings to determine how images are stored and shown in Rich Text fields, set size limits, and use a default custom font. Global Rich Text settings are configured in **CSM Administrator > System Settings > Rich Text**.

Setting	Description
Image Format	Select either JPEG or PNG. Images not in a default format are converted to the image format you select.
Form Images Are Displayed As	Determines how embedded images are shown in Rich Text fields: • **No Image Support** (no image is shown). • **Small Thumbnails** • **Medium Thumbnails** (default). • **Large Thumbnails** • **Full Images**
Zoomed Images Are Displayed As	Select an option to determine how embedded images in Rich Text fields are shown in the Rich Text Zoom window: • **No Image Support** (no image is shown). • **Small Thumbnails** • **Medium Thumbnails** • **Large Thumbnails** • **Full Images** (default).

Size limits	• **Maximum size per image** (default is 500 kilobytes)
	
	  Note: If the image size exceeds the maximum size, the image will automatically be resized to fit within the maximum size limits.
	
	• **Maximum total size for images** (default is 3 megabytes)
	
	  Note: If the total image size exceeds the maximum size, the images will automatically be resized to fit within the maximum size limits.

Setting	Description
Custom Default Font	Select the **Ellipses** button to open the Font window. Select a default font, style, and size. **Note:** The **Rich Text Editor** uses a default font based on the following settings, shown in priority order: • Field properties for a specific field in a Business Object (example: Resolution fields in Problems). • Default font selected in the Global Rich Text settings. • Default theme form control font. • CSM global system font (not configurable).

Related concepts

About Rich Text

Global Record Locking Setting Options

Define the options for record locking settings, such as default lock type and when a lock expires. Global search settings are configured in **CSM Administrator > System Settings > Search**.

Setting	Description
Unlock records when User session ends (Recommended)	Automatically unlocks all of a user's records when the user logs out of a session. If cleared, the record remains locked until the record is saved (if configured), until the lock expires (if configured), or until the record is manually unlocked.
Update lock status and notify of any changes, when possible	Automatically shows status and change notifications (example: Reload and merge) to the lock holder and any other user who might be viewing a locked record. If not selected, users are notified only if they attempt to edit a record. **Note:** Automatic notifications are not available in the CSM Browser Client.
Default lock type	• **None**: Does *not* enforce or inform record locking even though it is enabled for the system. **Tip:** Use this option to enable record locking for the system but not use it for most Business Objects, then enable/configure record locking settings on a per Business Object basis. • **Enforced**: Prevents users from editing a record when it is locked by another user (the lock holder). • **Informational**: Warns users when a record is currently locked by another user, so users do not attempt to edit the same record. If two users do edit the same record, CSM gives them the option to merge the edits.
Lock record upon editing	Automatically locks the record when a user attempts to edit the record. If cleared, users must manually lock records.
Unlock record upon saving	Automatically unlocks the record when a user saves the record. If cleared, the record remains locked until the user ends their session (if configured), until the lock expires (if configured), or until the record is manually unlocked.
Lock expires after	Enables lock expiration and specifying the time limit in minutes (example: 30). If cleared, the record remains locked until the user ends their session (if configured), until the record is saved (if configured), or until the record is manually unlocked. **Note:** In some environments, when you change the time limit for the lock setting expiration, it may take up to 30 minutes for the change to take effect.

Setting	Description
Minutes before lock expiration to notify Users	Notifies users of impending expiration and allow renewal before expiration. Users can specify the number of minutes before expiration to notify users (example: 3 minutes).
Maximum number of records a User can have locked at one time (per Business Object type)	Specify the maximum number of records a user can have locked at one time, per Business Object (example: Each user can lock only ten Incidents at a time).
Portal participates in record locking (hidden from portal users where possible)	Allows customers working in the CSM Portal to lock records and see locks on records. **Note:** When a customer attempts to edit a record, the record is automatically locked; and, when the customer saves the record, the record is automatically unlocked. This prevents users from editing records at the same time as customers. However, the customer does not see messages about locks unless they attempt to edit a record that is locked by another user or customer. If the CSM Portal does not participate in record locking (or record locks are informational), the customer is able to edit records even if a user has the record locked. The user is given the option to merge the customer's edits.

Related concepts

About Record Locking

Configure Global Help Settings

Use Global Help system settings to provide an alternate help site to your users and customize support contact settings. Access Global Help settings from CSM Administrator (**Settings > Edit System Settings > Help**).

Setting	Description
Alternate Help Site	Define a custom Help System or site. After selecting the **Alternate Help Site** checkbox, provide an alternate help system URL.
Pass Parameters	Select the **Pass Parameters** checkbox to enable passing parameters for the provided help system URL.
Show Process and Terminology Help	Enables Process and Terminology Help in CSM. Process and terminology Help text is defined in the Process and Terminology pages in the Business Object Properties or Field Properties windows.
Disable Reporting Error	By default, CSM allows users to send a Report Error email to Cherwell. Select the **Disable Reporting Error** checkbox to disable the send error reports feature.
Alternate Report Error E-mail	Provide a custom email address for error reports to be sent to instead of the default Cherwell email address.
Alternate Support Phone Number	Provide a custom Support Team phone number instead of the default Cherwell phone number. **Note:** The Cherwell phone number will remain in several error messages when directly contacting Cherwell is the best way to solve those problems.

Related concepts

Define Process and Procedure Help Properties for a Business Object

Define Process and Procedure Help Properties for a Field

Configure Global Advanced Settings

Use the **Advanced** page in the CSM Administrator **System Settings** window (**Edit System Settings > Advanced**) to configure the number of dashboard widgets to simultaneously refresh, the time span between notification checks, and more.

Setting	Description
Max simultaneous widget refresh	Define the maximum number of widgets that can be refreshed simultaneously (default is 5). Use the up/down arrows to increase/decrease the number. When a dashboard is set to reload its data, it will combine refresh requests. Increasing this number might make dashboards update more smoothly, but might also increase network traffic and slow down other users and operations.
Configure Notification Settings	The Cherwell Application Server sends messages to clients regarding updates (example: Definitions need to be reloaded, queues need to be updated, or records have been locked). This information is attached to regular requests from the client to the server. However, if the client has not communicated with the server within the maximum notification time, the client checks for updates. You can set the maximum amount of time between client notification checks and server notification checks. Decreasing these values can make clients get updated data more frequently, but also increase network traffic.
Web Services	The settings defined here might override some of the settings defined when you set up a web service.
Calling Web Services from Client	Select an option for allowing web service calls from a client. • Select **Allow** to allow web services to be called from a client. • Select **Don't Allow** to prevent web services from being called by clients. Users who try calling a web service from a client will receive an error. • Select **Force to Server** to force client web service calls to the server. • Select **Based on Security** to determine whether a client can call a web service based on security rights.

Setting	Description
Unsecured Calls (HTTP)	Select an option for unsecured web service calls. • Select **Allow** to allow unsecured (HTTP) web service calls. • Select **Don't Allow** to prevent unsecured web service calls. Users who try making unsecured calls receive an error. • Select **Force to HTTPS** to have all unsecured web service calls forced to HTTPS.
Allow self-signed certificates (HTTPS)	Select this check box to allow calls to web services with self-signed certificates (certificates not signed through a signing authority such as VeriSign). If this box is cleared, users receive an error when they try to call a self-signed web service.
Auditing	Select an option for determining what to audit (log). • Select **None** to disable auditing. • Select **Based on Service Settings** to audit based on the web service's auditing setting. • Select **All Web Service Calls** to audit all web service calls. • Select **Server-Based Calls** to only audit web service calls made from the server. **Note:** Web service calls are audited by writing an entry into the Cherwell Application Server log, which can write to a file, to the event log, or to an external logging tool such as Splunk. The log must be configured for web service calls to be captured.
Analytics	Select the **Google Analytics Tracking ID (Portal)** check box and provide your Google Analytics Tracking ID to enable the tracking of data for your CSM Portal sites. See Tracking Portal Use with Google Analytics.
Use legacy rules for related data retrieval	We do not recommend setting the **Use legacy rules for related data retrieval** check box. This setting causes relationships to load beyond the second level and can severely degrade system performance or cause recursion problems.
Timeout on request cache	Set a cache timeout of up to 5 minutes for expressions and dashboard chart queries in the CSM Web Applications. This setting helps reduce the database load when the same expression is run multiple times. The default is 4 minutes. Use 0 to disable the cache.

Related information

Track Portal Use With Google Analytics
Tips for Using Google Analytics with CSM

Configure Global User Queue Settings

Configure default options for each automatically created User Queue, including defining a History Record to track Queue options and enabling ownership transfer if records in a User Queue.

User Queue settings are defined in CSM Administrator.

Open the User Queue Settings Window

To open the User Queue Settings window from the CSM Administrator main window, click the **Settings** category, and then click the **Edit User Queue Settings** task.

Define User Queue History Settings

Use the User Queue History Settings window to define Queue History Journal records to track Queue operations (example: Add to Queue, check in, check out, reassign, suspend, unsuspend, remove).

To define User Queue History settings:

1. .

2. Select Queue History Journal options for Queue operations (Add to Queue, Check Out, Check In, Reassign, Suspend, Unsuspend, Remove): Select one of the following options from the corresponding drop-down:
   - **Auto-generate:** Select this option to automatically create a Queue History Journal record containing default text when the action takes place.
   - **No History:** Select this option to create no Queue History Journal record when the action takes place.
   - **Optional:** Select this option to prompt the User to add notes to the Queue History Journal record when the action takes place. It also allows the User to select not to create a Queue History Journal record.
   - **Prompt:** Select this option to prompt the User to add notes to the Queue History Journal record when the action takes place, but does not allow the User to cancel the Queue History record.

     Notes: Canceling the prompt will cancel the entire Queue operation. If a record is added to a Queue using an automated process (example: Automation Process), the Optional and Prompt options will add History, but use default text.

3. Select **OK**.

Transfer Ownership When Record is Placed in User Queue

Use the User Queue History Settings window to define if Users can transfer record ownership to a specific User when a record is placed in a User Queue.

To transfer record ownership when a record is placed in a User Queue:

1. Open the User Queue Settings window.

2. Select the **Transfer ownership to User when record put on User Queue** check box.

3. Select **OK**.

Configure Global Task Pane and Search Control Settings

Configure which items appear in the Task Pane or which Search Control is used on the CSM menu bar. These settings can be applied globally to all users or for users assigned to specific roles.

To configure Global/Role Task Pane and Search Control settings:

1. In the CSM Administrator main window, click the **Settings** category, and then click the **Edit Default Task Panes and Menu Search** task.

   Note: *Default* is a Global default and applies for all users/roles unless overridden. The small green check mark indicates that Task Pane and Search Settings have been defined for a particular role. If no defaults are defined for a role, members of that role see the Task Pane and Search Settings for the Global default, if defined.

2. Select **Default** (Global) or a role, and then click the **Edit** button.

   The Global or Role Task Pane and Search Settings window opens (our example shows how to edit the OOTB task pane and search settings, which applies to all users and becomes the *Default Task Pane Setup*).

3. Configure Task Pane settings:
   - View or hide sections.

   - Add new sections.

   - Configure sections (only applicable to new sections).

   - Delete sections (only applicable to new sections).

   - Organize sections.

4. View or hide the following sections in the Task Pane (select or clear the corresponding box):
   - Quick Search

   - Common Tasks

   - Actions

   - Queues

   - Process and Terminology

   - Customer Information

5. Add Sections to the Task Pane:

   Note: Any items added to the Global Task Pane become part of the Global default task pane setup. If editing the Task Pane and Search settings for a role, select the **Use default task pane setup** check box to use the settings defined for the Global default. This check box must be cleared to add items to a Role Task Pane.

   a. Select **Add**.

    b. Provide a **title** for the Task Pane section.

    c. Select **Add** to open the Action Manager.

    d. Select the CSM Items to show in the Task Pane (Calendars, Commands, Dashboards, Document Repositories, One-Step Actions, Reports, Searches, or Visualizations).

    e. Select **OK**.

> **Tip:** Select **Configure** to edit the title and list of Actions for a newly added section. Select **Delete** to delete a newly added Task Pane section. Use the up/down arrows to change the order of Task Pane sections.

6. Customize the CSM Search Control in the Menu bar Search Options:
   - Use Default: Uses the OOTB Search Menu Search Widget, which allows users to run a Quick Search on multiple Business Objects simultaneously (example: Knowledge Article, Incident, Problem, and Change Request). Users can also select a Business Object in the drop-down to search one item at a time (example: Specific Search).
   - Use Search Widget: Uses a specific Search Widget. Select the **Ellipses** button to open the Widget Manager, and then select an existing Search Widget or create a new Search Widget.
   - No Menu Bar Search: Removes the Search Control from the menu bar.

Configure Custom Global Toolbars

Create and configure custom Desktop Client toolbars to provide quick access to CSM operations for all users or users assigned to particular Roles.

🖉 **Note:** Custom Global toolbars are not available in the Browser Client.

To configure a custom Global toolbar:

1. In the CSM Administrator main window, select the **Settings** category, and then select the **Edit Custom Toolbars** task.
   The **Configure Toolbars** window opens. *Default* is a Global default and applies for all users/roles unless overridden. The small green check mark indicates that a custom toolbar has been defined for a particular Role. If no defaults are defined for a Role, members of that Role see the custom toolbar for the Global default, if defined.

2. Select **Default** (Global) or a **Role**, and then select the **Edit** button.
   The toolbar for <Global/Role> opens.

3. Select the **Add** button.

4. Define general properties and Actions for the toolbar:
   a. Name: Provide a name for the toolbar. This is the name that shows in the toolbar context menu (in the Desktop Client, right-click toolbar to show a context menu of available toolbars to display).

   b. Show by Default: Shows the custom toolbar in the Desktop Client by default. Otherwise, users have to manually show it (right-click toolbar>select a toolbar to display).

   c. Add Action: Select this button and select the type of **Action** to add to the custom toolbar
   A CSM Item Manager opens (varies by type of Action selected in the previous step), and then select/create the CSM Item to initiate through the Action.

   d. Select a **CSM Item** (example: A specific Dashboard).

   e. Define properties for the Action:
      ◦ Action: Shows the name of the Action as it is recognized by CSM (example: Name of the Dashboard or Report).

      ◦ Display text: Provide the **text** to show on the toolbar button if *Show text on button* (below) is selected.

      ◦ Image button:

         Select the image to open the **Image Manager**, and then select an existing image or import a new image to represent the item in the UI.

      ◦ Help text: Provide a tooltip to show when the cursor is on the menu item.

      ◦ Begin group: Shows a horizontal line before the menu item, separating it from other menu items.

      ◦ Show text on button: Shows the Display Text on the toolbar button.

   f. Add additional Actions to the toolbar.

5. (Optional) Create additional custom toolbars.

Configure CSM Remote Support Settings

Use the Chat and Remote Support Connector Settings window in CSM Administrator to configure how CSM accesses and initiates remote support systems, how CSM identifies Customers requesting remote support, and which Business Objects are linked to remote support sessions.

You can use the BeyondTrust Remote Support mApp Solution to easily configure a remote services integration.

For detailed information, see:

- Define General Settings
- Define Identify Customer Settings
- Define Business Object Settings

To configure CSM remote support settings:
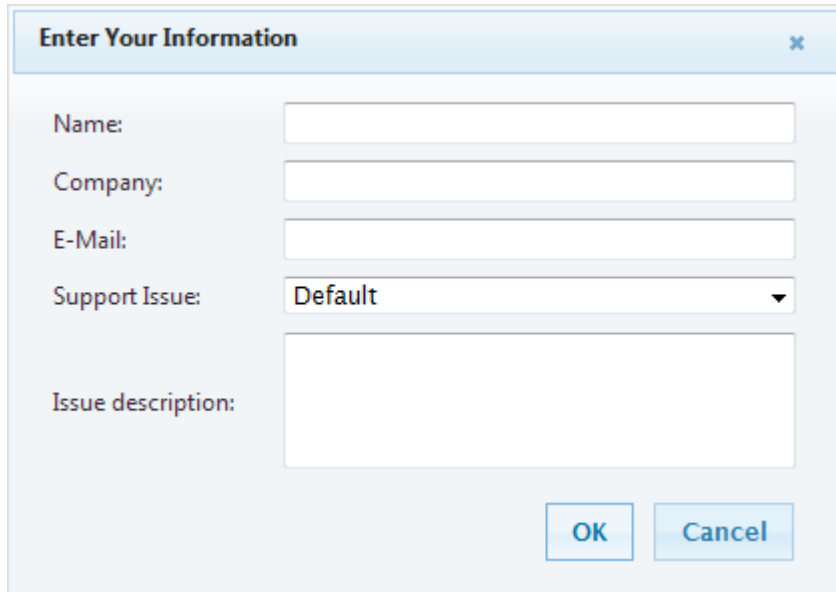
1. In CSM Administrator window, select the **Settings** category, and then the **Edit Chat and Remote Support Connector Settings** task.

   The Chat and Remote Support Connector Settings window opens.

2. Define General page settings for remote support:
   a. Enable Chat and Remote Control Services.

   b. Define Chat Service Credentials.

   c. Define Cherwell Credentials for Processing Chat Service Events.

   d. Define Chat Service Technician Queue options.

   e. Define Chat Service Support Issue Queue options.

   f. (Optional) Create a remote support session invitation e-mail template that CSM technicians can use to invite Customers to remote support sessions.

3. Define Identify Customer page settings: Define how CSM identifies Customers requesting a support session from the Portal.
   a. Define options for Self-Service Portal Customers Logged In.

   > **Note:** If no options are selected and the Customer is not prompted to select a support issue, no window opens for the Customer to provide information.

Enter Your Information   ✖

Name:

Company:

E-Mail:

Support Issue: Default   ▼

Issue description:

                                    OK   **Cancel**

b. Define options for Self-Service Portal Customers Not Logged In.

When any or all of these options are selected, a window opens to prompt the Customer to provide the specified information when a new remote support session is requested.

4. Define Objects page settings: Define which Business Objects are linked to remote support sessions and create One-Step Actions for processing session information.

5. Select **Add**, **Edit** (Add and Edit open the Chat Actions window), or **Remove** for existing Business Objects in the list, or **Clear Default**.

6. From the Chat Actions Window:
   a. Specify the Chat Action Behavior (Create or Update):

   Note: The CSM Desktop Client and Portal both support creating new Business Objects at the end of a remote support session. In the Desktop Client, if a Business Object is currently in focus, the new Business Object is created under the Customer that owns the current Business Object. If no Business Object is in focus, the new Business Object is created under the default Customer designated in the Chat and Remote Support Connector Settings. When a Customer launches a remote support session from the Portal, a new Business Object can be created under the currently logged-in Customer, the Customer identified by email address, or a default Customer if the Customer could not be identified. If no default Customer is configured and a Customer cannot be identified, a new Business Object might not be created.

   Note: The option to create a new Business Object to associate with the remote support session must also be selected in the New Chat Session command options in order for a new Business Object to be created at the end of a remote support session, and to have remote support session history attached to it.

     b. Select **Add** and select the Action from a list: **Create New**, **Update**, **Add to a Queue, Run a One-Step Action**.

7. Specify the Actions that should be performed when the selected Business Object type is created at the end of a remote support session: Select **Add**, **Edit**, **Copy**, or **Delete**.

> **Note:** When a remote support session is not launched from CSM, CSM does not have any information about the type of Business Object to create after a session ends. By setting a Business Object as the default, CSM creates a new object of the specified type if no Business Object information is available when a remote support session has ended. If no default Business Object is selected and a remote support session is not initiated through CSM, the event is ignored and no action taken.

8. Select **OK**.

Define General Settings

The General Settings define how CSM accesses and initiates remote support (the URL for the remote service, login information, queue selection, and email invitation template).

Setting	Description
Enable Chat and Remote Control Services	Enables remote support (example: BeyondTrust) through CSM. When this option is selected, the Remote Support Service commands appear in the menu bar of the CSM Desktop Client under **Tools>Chat**. **Note:** Clear this check box to temporarily disable remote support integration while still keeping other settings.
Service URL	Provide the base URL for the remote support service API. **Security Warning:** Use HTTPS for this URL to ensure security.
Chat Server IP Address	(Optional) Provide the IP address of the remote support server. If specified, remote support event notifications are allowed only when originating from this IP address.
Chat Service Credentials	Provide the User Name and Password for a remote support service user authorized to perform API requests.
Cherwell Credentials for Processing Chat Service Events	These are the credentials used to log in to CSM to process information from the remote support service after a remote support session ends. **Use Active Web Service Credentials:** Current Windows login credentials are used. Create a corresponding Windows User in CSM using the same Windows user name. This User must have the proper security rights to process events, run One-Step Actions, and create or modify Business Objects and Customer Records. Typically, this user name is IIS AppPool\DefaultAppPool or something similar. **Use Specific Cherwell User:** Use a CSM User login (internal or Windows user). Provide the User name and Password of the CSM User that is used for logging in to process remote support events. This User must have the proper security rights to process events, run One-Step Actions, and create or modify Business Objects and Customer Records.

Setting	Description
Chat Service Technician Queue	These options (only supported in the CSM Desktop Client) allow CSM technicians to have remote support sessions placed in their personal queues in the BeyondTrust Representative Console. **Select Technician Queue Using Current User Login:** Match the user name for the currently logged-in CSM technician against the usernames of all CSM technicians who are currently logged into the BeyondTrust Representative Console. If a match is found, the remote support session is created within that technician's queue **Select Technician Queue Using Login Stored In Current User Business Object:** Match the user name stored in a Field in the User Business Object (UserInfo) for the currently logged-in technician against the user names of all technicians who are currently logged into the remote support system. If a match is found, the remote support session is created within that technician's queue. To indicate which Field contains the technician's user name, add an attribute with the name ChatUserName to the Field. For more information about Field attributes, see Define Advanced Properties for a Field.
Chat Service Support Issue Queue	These options determine whether a Customer can select from a list of support issues when launching a remote support session, or whether all remote support sessions launched by Customers are categorized under a specified support issue. **Prompt for Support Issue:** Select this option to have a pop-up open for the Customer to select from a list of issues downloaded from the remote support system. **Always Use a Specific Support Issue:** Automatically use a specified issue. Default indicates that the request should be placed in the general queue in the remote support system. **Select Issue:** Select a specific issue to use, which determines the queue the request is placed in. **Note:** If the Technician queue options described above are enabled and a Technician match is found, the support issue queue options are ignored and the remote support session is created in the technician's personal queue.
Chat Invitation E-mail	(Optional) Create a remote support session invitation e-mail template that CSM technicians can use to invite Customers to remote support sessions.

Create the Remote Support Session Invitation E-mail Template

In the CSM Desktop Client, when a technician selects the command for a new remote support session, an email message is constructed and sent to Customers to invite them to participate in the session. In the Portal, a remote support session is immediately started when a Customer selects the New Chat Session command.

To create a remote support session invitation e-mail template:

1. In CSM Administrator, select the **Settings** category, and then the **Edit Chat and Remote Support Connector Settings** task.

   The Chat and Remote Support Connector Settings window opens.

2. On the General page, click the **Chat Invitation E-mail** button.

3. Use the following options to design an email template:
   a. Select the **Selector** button or right-click in the e-mail template to insert Expressions, functions, and variables into the template.

      Tip: Use Expressions, functions, and variables to insert conditional/actual values into the email when it is created.

   b. Select **Variables** in this list to view a list of variables associated with remote support session requests. The following variables are available:

Variable Name	Description
Chat Session URL	URL that can be used to initiate the remote support session.
E-mail Address	Email address of Customer.
Object Name	Name of Business Object with which a remote support session is associated.
Object Plural Name	Plural name of Business Object with which a remote support session is associated.
Provider E-mail Body	Text for the body of the email returned by the remote support system. The body of a Customer invitation email is configured the remote system. The generated email body can be passed to CSM through the API and used in lieu of the remote support session invitation email template in CSM.
Provider E-mail Subject	Text for the email subject returned by BeyondTrust.
Support Issue	Name of the support issue selected by the Customer (if any).
Team Name	Name of the team queue the remote support session request is submitted to (if any).

Define Identify Customer Settings

At the end of remote support sessions, Business Objects can be created or updated and associated with remote support session histories. Use the Identify Customer page to define how to identify Customers under whom Business Objects can be created at the completion of remote support sessions.

In the Portal, when a command to start a remote support session is selected, an optional window can open to prompt the Customer for a user name, company, e-mail address, support issue (if enabled on the General page in the Chat Service Support Issue Queue area), and issue description. This information is passed to a support technician in the remote support system at the start of the remote support session. If the Customer is not currently logged into the Portal, the e-mail address she enters (if any) is used in an attempt to identify her.

Self-Service Portal Customers Logged In	Select the check boxes next to the types of information a Customer who is logged into the Portal should be prompted to enter when they launch a new remote support session. This information is passed to the remote support system with the request to start a session. • Name: Prompts the Customer to enter her name. • E-mail Address: Prompts the Customer to enter her e-mail address. • Company: Prompts the Customer to enter her company name. • Issue description: Prompts the Customer to enter a description of the problem she is experiencing. When any or all of these options are selected, a window appears to prompt the Customer to provide the specified information when a new remote support session is launched.

Self-Service Portal Customers Not Logged In	Select the check boxes next to the types of information a Customer who is not logged into the Portal should be prompted to provide when they launch a new remote support session. This information is passed to the remote support system with the request to start a remote support session. In addition, the e-mail address is used to attempt to identify the Customer in CSM. • **Name:** Select this check box to prompt the Customer to enter her name. • **E-mail Address:** Pompts the Customer to specify her e-mail address. If the Customer provides an e-mail address, the e-mail address is matched against CSM User Records according to the additional Identify options in an attempt to identify the Customer. • **Company:** Prompts the Customer to provide her company name. • **Issue description:** Prompts the Customer to provide a description of the problem. **Identify Customer by Matching E-mail Address to Default E-mail Address Fields:** If this option is selected and no current Customer is logged into the CSM Portal, the e-mail address entered by the Customer (if any) is matched against the default e-mail Business Objects and Fields. **Search All Contact Manager Objects:** If this option is selected and no current Customer is logged into the CSM Portal, in addition to searching the default Business Objects and Fields, the e-mail address entered by the Customer (if any) is also matched against Fields having the E-mail Address attribute in all Contact Manager Objects. **Identify Customer by Matching E-mail Address to Specific Business Object and Field:** If this option is selected and no current Customer is logged into the CSM Portal, the e-mail address entered by the Customer (if any) is matched against the e-mail Business Object and Field selected in the drop-downs. **Note:** If no options are selected and the Customer is not being prompted to select a support issue, no window opens for the Customer to provide information.
If no Customer identified or associated with chat session use default	Select the **Customer Identified or Associated with Chat Session, Use Default** check box to select a default Customer from the Contact Manager. Click the **Ellipses** button (shows Default if check box is selected or select Customer if cleared). In the following cases, CSM creates Business Objects at the end of a remote support session under a default Customer: • Customer is not prompted to provide an e-mail address. • CSM could not find a match to the Customer's e-mail address in Customer Records. • The remote support session was not initiated through CSM (example: sessions launched from the remote support system). **Note:** If this option is not selected, and no Customer information for a completed remote support session is available, the session event is ignored and no processing takes place.

Define Business Object Settings

Business Objects must be defined for Business Object Records to be created or updated and associated with remote support session history.

Add	Select to add the highlighted Action. See Chat Actions window options below.
Edit	Select to edit the highlighted Action. See Chat Actions window options below.
Remove	Select to remove the highlighted Action.
Up/Down Arrow buttons	Select to change the order of the selected Actions.
Clear Default	Select or clear **Business Object defaults** to determine what type of Business Object CSM creates after the end of a remote support session that was not launched from CSM (example: sessions launched from the BeyondTrust Web Portal or BeyondTrust Representative Console). • If the currently selected Business Object type is not the default, select **Make Default** to make it the default. • If the currently selected Business Object type is already the default, select **Clear Default** to change it to no longer be the default. **Note:** When a remote support session is not launched from CSM, CSM does not have any information about the type of Business Object to create after a session ends. By setting a Business Object as the default, CSM creates a new object of the specified type if no Business Object information is available when a remote support session has ended. If no default Business Object is selected and a remote support session is not initiated through CSM, the event is ignored and no action taken.

Configure Cherwell Mobile Settings

The Cherwell Mobile applications for iOS and Android were deprecated in March 2019 and are no longer available in their respective application stores. CherwellMobile applications that are already installed should continue to work as expected, however.

To replace Cherwell Mobile and accommodate users on any device, including mobile devices, use Adaptive Layouts to design forms and dashboards that adapt to different dimensions.

Cherwell Mobile settings define which:

- Mobile dashboard (home) to display by default.
- Mobile dashboard (alert) to display by default.
- Business Objects to make available. Associated Saved Searches will also be available.
- Actions/One-Step Actions to allow for each Business Object.

The default Cherwell Mobile settings (either Global or Role) are initially configured in CSM Administrator. Users with security rights can configure their personal Cherwell Mobile settings.

Configure Global/Role Cherwell Mobile Settings

Use the Mobile Configuration window in CSM Administrator to configure how Cherwell Mobile looks and behaves on mobile devices, Globally or by Role. You can configure which:

- Mobile Home Dashboard to display by default.
- Mobile Alert Dashboard to display by default.
- Business Objects to make available. Associated Search Groups will also be available.
- Actions/One-Step Actions to make available for each Business Object.

To configure Global/Role Cherwell Mobile settings:

1. In the CSM Administrator main window, click the **Browser and Mobile** category, and then click the **Edit Mobile Configuration** task.

   The Mobile Configuration window opens, listing the available Roles (*Default* is a global default, is always defined, and applies for all Users/Roles unless overridden). The small green check mark indicates that settings have been configured for a particular Role.
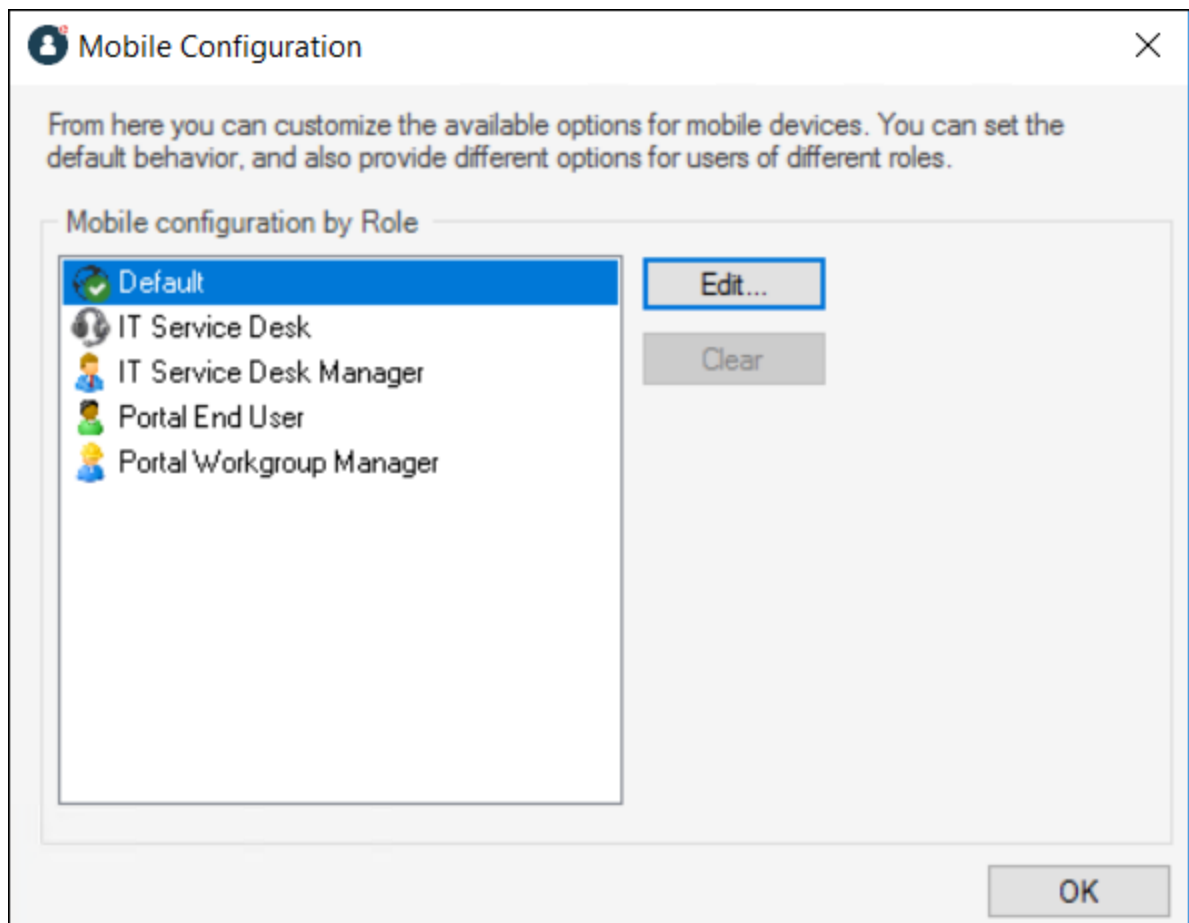
2. Click **Default** (Global) or a **Role**, and then click the **Edit** button.

> **Note:** Our example uses Global. If you select a Role, you have the option to override the Global default and configure Cherwell Mobile settings from scratch.

Tip: Click the **Clear** button to clear configured settings for a selected Role. If no defaults are configured for a Role, members of that Role see the Global default settings (which cannot be cleared).

The Mobile Access Setup window opens, listing the objects (Dashboards and Business Objects) currently being displayed on mobile devices.

3. Select default Mobile Dashboards (Home and Alert):

Tip: If you do not want to display any Dashboards, remove the Dashboard item from the *List of Objects to Display on Mobile Device* list.

   a. Home Page: Select a default Mobile Home Dashboard.
      ◦ Click the drop-down to select from a list of recently used Mobile Dashboards.

      ◦ Click the **Mobile Dashboard** button to open the Mobile Dashboard Manager, and then select an existing Mobile Dashboard or create a new Mobile Dashboard.

   b. Alerts Page: Select a default Mobile Alert Dashboard.
      ◦ Click the drop-down to select from a list of recently used Mobile Dashboards

      ◦ Click the **Mobile Dashboard** button to open the Mobile Dashboard Manager, and then select an existing Mobile Alert Dashboard or create a new Mobile Alert Dashboard.

4. Select the Business Objects to make available in Cherwell Mobile:

> **Important:** In order for a Business Object to be available, it must have the *Show in Search Manager* property set (in the Business Object properties within a Blueprint).

   a. Override List of Objects to Display on Mobile Device: Select this check box to override the current Global default list of Business Objects. This check box does not appear when configuring Global defaults because there is nothing above them to override.

   b. Click **Add**, and then select the **Business Object** to make available on mobile devices.

   Tip: Click **Edit** to edit a selected item. Click **Remove** to remove the selected item from the list.

c. Define how to display the Business Object in Cherwell Mobile:
  ◦ Custom Name: Provide a **display name** to use in Cherwell Mobile. If blank, the Business Object name is displayed.

  ◦ Custom Image:

    Select the image to open the **Image Manager**, and then select an existing image or import a new image to represent the item in the UI.

    If no image (None) is selected, the default image for the Business Object is displayed.

    Android: Android devices use standard color images. For the best results, use the images in the BusObs>32x32 folder in the Image Manager. If you are setting up a mobile configuration for use on both Android and iOS devices, use the iPhone-specific images. They will be automatically mapped to equivalent standard images for non-iOS devices.

d. Select the Actions/One-Step Actions to make available in Cherwell Mobile:
  i. Click **Add** to add a new Action/One-Step Action to the list.

    Tip: Click **Edit** to edit a selected item. Click **Remove** to remove the selected item from the list. Use the **Up/Down** arrows to change the order of the Actions/One-Step Actions when displayed in Cherwell Mobile (ex: In the Actions list).

      ii. Define additional options for the list of Actions:

- Also Show Default Business Object Actions: Select this check box to also make available any default Actions for the Business Object. This option is only available if the Business Object has default Actions available (ex: Approvals have built-in functionality to approve, deny, and abstain).

- Also Show Global Actions: Select this check box to make available any Actions that were defined for the Business Object as part of the Global default settings.

           Note: This option is available only if you are configuring settings for a Role.

5. Configure the order of the Actions when displayed in Cherwell Mobile (ex: On the Actions popup list):
   a. Use the **Up/Down arrows** to order the Actions.

6. Select **OK**.

Suggested Timeout Settings for CSM

Learn about the many timeout settings in CSM and its supporting services. You can implement our suggested timeout settings for improved performance.

We suggest a timeout of 90 minutes as a baseline. You'll base many of your timeout settings throughout the system on this value. The following information describes how CSM uses the various timeout settings in CSM, Cherwell Application Server, and IIS. You'll also find suggested timeout values based on the 90-minute baseline.

CSM Desktop Client

You can implement an inactivity timeout for the CSM Desktop Client using the **Logout inactive users from Cherwell after** option under Security Settings. The Desktop Client keeps track of the "last touched" time, which is updated by user activity. The Desktop Client checks every minute to see if a logged-in user has been inactive for longer than the configured timeout. If the Desktop Client does not detect any activity within the specified timeout, it sends a "logout" request to the application server, and displays a dialog box telling the user they have been logged out due to inactivity.

To implement our suggested Desktop Client timeout settings:

1. In CSM Administrator, navigate to **Security > Security Settings > Desktop Client**.
2. Set **Logout inactive users from Cherwell after** to 90 minutes.

> **Note:** You can also set a **Warning period**, which dictates how long before the inactivity timer expires users will get a warning before being disconnected.

CSM Browser Client and CSM Portal

The same inactivity timeout setting is available for the CSM Browser Client and CSM Portal. This session timeout must be smaller than the IIS Application Pool Idle Timeout-out setting.

To implement our suggested CSM Browser Client and CSM Portal timeout settings:

1. In CSM Administrator, navigate to **Browser and Mobile > Browser Application Settings**.
2. Under the Session Timeout section, set **Timeout** to 90 minutes.

> **Note:** Remember to ensure the IIS Application Pool timeout setting is 5-10 minutes higher than this setting. The IIS Session State timeout setting should match the CSM session timeout setting.

Cherwell Application Server

The Cherwell Application Server has a variety of settings dealing with timeouts and inactivity. The Cherwell Application Server timestamps the last action registered for a given user, and periodically reviews all logged-in users to see if any user has not reported activity within the designated timeframe. If

not, the user is removed from the cache of logged-in users, causing clients to log the user out and display a log-out message.

The application server keeps track of users using a key constructed of three parts:

- User ID
- Module (client) the user is logged into
- A unique session key that is assigned to the user when they log in, which is stored in the logged-in users cache/table

When the application server applies a timestamp to a user's activity, it stores the timestamp using the most recent session key created for the user, which means that only activity on the user's most recent login should be tracked.

To implement our suggested Application Server timeout settings:

1. Navigate to **Security > Licensing**.
2. Set **If the client stops responding, auto-release license after** to 90 minutes.

IIS

You can set **Idle Time-out (minutes)** in Application Pools in IIS to the your desired timeout plus 10 minutes. The IIS Idle Time-out setting controls when the IIS application pool is shut down if no activity is detected within the configured interval. When the application pool is shut down, the Application Server and Web clients will lose their sessions, which can cause users to be logged out. It is recommended that this be set to at least your desired inactivity timeout plus ten minutes, to ensure that the application pool is never recycled while users are still logged in.

By default, the **Regular Time Interval (minutes)** is set to 1740 minutes (29 hours). We suggest setting this to 0, then setting a **Specific Time** to recycle the Application Pool. We suggest recycling at 0200; if there are multiple servers separate the recycle times by 15 minutes.

🖉 **Note:** Be sure to coordinate your recycle time with your scheduled tasks and adjust if there are conflicts.

When the application pool is recycled, the Application Server and web clients will lose their current sessions, causing users to be logged out. Schedule this to run during expected down times, such as at 0200.

To implement our suggested IIS timeout settings for a server farm with Redis:

1. Open IIS and access the Application Pools.
2. Right-click the Application pool you want to edit and select **Advanced Settings**. Set the following values:

Setting Name	Suggested Value
Idle Time-out (minutes)	100 minutes
Regular Time Interval (minutes)	0
Specific Time	0200 (if multiple servers, separate recycle times by 15 minutes)

3. For the Portal and Browser Client sites, double-click **Session State** and adjust the **Time-out (in minutes)** to 90 minutes.

Related concepts
Automatically Release a License
Related tasks
Configure CSM Web Application Settings (URLs, Timeouts, RSS Feeds)
Configure Login, Authentication, and Inactivity Settings for Each Client
Configure Server Farms in Cherwell Server Manager

Developing in CSM

CSM allows for concurrent development. This means multiple designers can simultaneously work on system changes, which is an essential technique for increasing the productivity of large IT organizations. In CSM, simple and complex system configuration is done using Blueprints or mApp® Solutions.

Concurrent development has several advantages:

- Complex changes can be developed and expanded over a long period of time without affecting current users.
- The changes themselves can be applied during downtime without requiring the actual design work to be done after hours.
- Designers can experiment with various independent changes or work on different design projects.
- The same set of changes can be applied to a test system, and then later be applied to the production environment.

However, when multiple designers are working on system configurations at the same time, conflicts, overwrites, errors, and other undesirable results can occur. For example, if one designer works on Incident fields and then another designer modifies the Incident form with additional fields, the work of the second designer could overwrite the work of the first designer.

Use the guidelines and best practices in this section to enable multiple designers to work simultaneously on system changes.

Setting up Environments for Concurrent Development

Concurrent development works best with a well organized set of development and test environments, in order to ensure that changes are properly tested before being applied to the production environment.

Overview

We recommend having at least one shared development environment and one shared test environment, either on premises or hosted by Cherwell SaaS, in addition to the shared production environment. Additionally, each developer should have a local development environment in order to keep your concurrent development strategy running smoothly. Each environment should be a full server with its own instance of a CSM database, onto which all configuration and record information is stored. Before beginning development, the development and test environments should be replicated from the production environment as completely as possible.
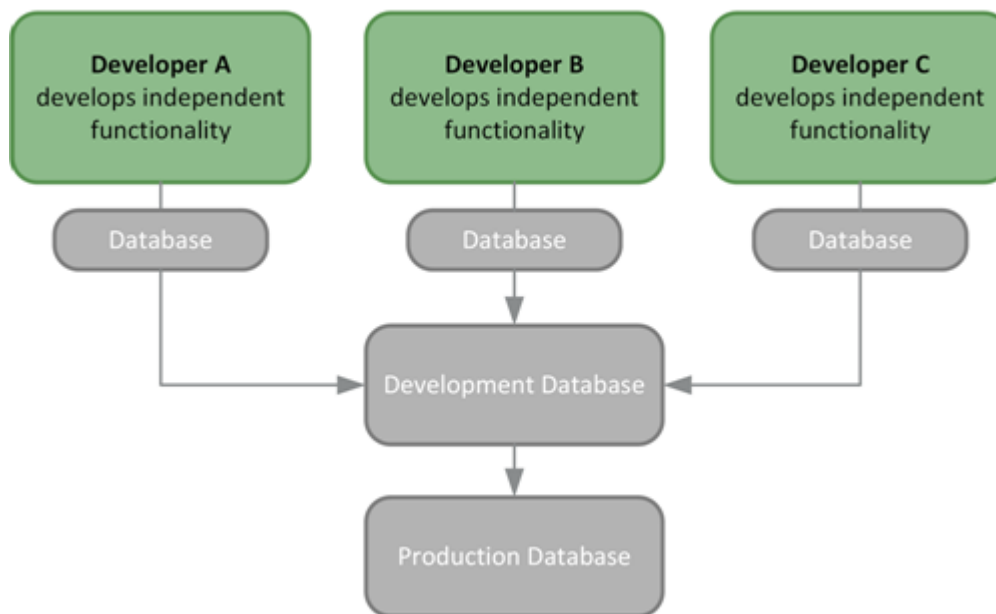
Create Multiple Working Databases

Use multiple CSM databases when implementing concurrent development using Blueprints or mApp Solutions:

- Have one independent development database for each designer.
- Have one master development database where one or more gatekeepers are allowed to make changes.

Designers can use their independent development databases (which are restored using the master CSM development database) to develop their individual system configurations. Only approved changes are applied to the master development database (which is restored using the current production environment).

Using Blueprints or mApp Solutions for Concurrent Development

Use the following workflows to accommodate multiple designers simultaneously working on system changes using Blueprints or mApp® Solutions.

Use Blueprints for Concurrent Development

When you use Blueprints for concurrent development, you use two or more Blueprints to develop the functionality and then apply each Blueprint to the production environment.

To use Blueprints for concurrent development:

1. The project manager creates a rollout document. The document should be detailed and include the following minimum information:
   - A list of stakeholders, including:
     - Business Object owners who are the sole developers assigned to work on a particular Business Object, including its views (example: Portal view) and features (example: dashboards, widgets, One-Step™ Actions, etc.).
     - Feature owners who are the sole developers assigned to work on a particular feature (example: Calendar) that does not have an associated Business Object.
     - A gatekeeper who ensures that the Blueprint adheres to requirements and follows team standards (example: naming conventions, design guidelines, etc.) before being published.
     - A product manager who is responsible for the scope and outcome of the project.
   - Required external connections (example: SCCM, Outlook, Active Directory, etc.). See Import Data from External Databases
   - Impacted CSM services (example: Cherwell Application Server, Automation Process Service, etc.).
   - System configurations that must be done outside the Blueprint. These might include changes to security, the Scheduler, the Email and Event Monitor Service, etc.
   - Test plans, including any user acceptance test requirements.
   - A backup and recovery plan.
2. Create a development environment for the project by restoring the master development server from the current production environment. When creating this environment, consider the following:
   - Create one copy of the production environment and store it in a shared location.
   - You do not need to include attachments in the file unless you are specifically testing their functionality.
   - Ensure that all impacted CSM services (example: Cherwell Application Server, Automation Process Service, etc.) are disabled. If you need to test Email Monitor functionality, make sure to configure the test email account. See Configure Test and Production Accounts.
3. Develop the functionality.
   a. Designers make individual copies of the master development database.

  b. Designers communicate which Business Objects and features they intend to work on.

  c. Designers develop the functionality using individual databases.

4. Conduct internal testing on the first Blueprint:
  a. Reference the rollout document to ensure that:
   ◦ The current Blueprint is intended to be published first.

   ◦ The Blueprint includes all of the required system configurations.

  b. Publish the Blueprint using the master development environment.

  c. Test the Blueprint.

  d. Edit the Blueprint or create a new Blueprint based on test results.

  e. Repeat internal testing (steps *a* through *d*) until the gatekeeper approves the Blueprint.

  f. Update the rollout document. Make sure to include any additional system configurations that were done outside of the Blueprint.

5. Conduct internal testing on the second Blueprint using the development environment that includes the first published Blueprint:
  a. Reference the rollout document to ensure that:
   ◦ The current Blueprint is intended to be published second.

   ◦ The Blueprint includes all of the required system configurations.

  b. Publish the Blueprint using the master development environment.

  c. Test the Blueprint.

  d. Edit the Blueprint or create a new Blueprint based on test results.

  e. Repeat internal testing (steps *a* through *d*) until the gatekeeper approves the Blueprint.

  f. Update the rollout document. Make sure to include any additional system configurations that were done outside of the Blueprint.

6. Conduct internal testing on subsequent Blueprints by repeating the instructions in step five.

7. Release the Blueprint into the production environment:
  a. Gatekeeper applies the first Blueprint while referencing the rollout document.

  b. Gatekeeper applies the second Blueprint while referencing the rollout document.

  c. Gatekeeper applies subsequent Blueprints while referencing the rollout document.

  d. Gatekeeper conducts a final review and publishes the Blueprints to the master development database.

  e. Quality assurance engineers complete regression testing.

  f. Publish the Blueprints in the production environment.

> **Important:** The order in which the Blueprints are published is critical. Ensure that the Blueprints are published in the same order that they were applied to the master development database.

8. Conduct a post-implementation review.

Use mApp Solutions for Concurrent Development

When you use mApp Solutions for concurrent development, you have two options:

- Use two or more Blueprints to develop the functionality and then create a mApp Solution to apply the functionality into the production environment. (Process shown below.)
- Use two or more mApp Solutions to develop the functionality and then apply each mApp Solution to the production environment.

To use mApp Solutions for concurrent development:

1. Follow steps 1-6 from the previous section on using Blueprints.
2. Create a mApp Solution based on the approved system configurations included in the Blueprints:
   a. Gatekeeper applies the first Blueprint while referencing the rollout document.
   b. Gatekeeper applies the second Blueprint while referencing the rollout document.
   c. Gatekeeper applies subsequent Blueprints while referencing the rollout document.
   d. Gatekeeper creates a backup of the master development server that includes all of the Blueprints.
   e. Gatekeeper conducts a final review and creates a mApp Solution based on the approved system configurations included in the Blueprints.
3. Conduct testing on the mApp Solution:
   a. Apply the mApp Solution while referencing the rollout document.
   b. Test the mApp Solution while referencing project requirements.
   c. Edit the mApp Solution or create a new mApp Solution based on test results.
   d. Repeat testing (steps *a* through *c*) until the gatekeeper approves the mApp Solution.
   e. Update the rollout document.
4. Release the mApp Solution into the production environment:
   a. Gatekeeper conducts a final review and applies the mApp Solution to the master development database.
   b. Quality assurance engineers complete regression testing.
   c. Publish the mApp Solution to the production environment.

Best Practices for Concurrent Development

Use the following best practices as part of your organization's Software Development Lifecycle (SDLC) to enable multiple designers to work simultaneously on system changes.

Communicate, Communicate, Communicate

Communicate with your team as much as possible. The level of communication needed will vary based on project, but ensure that the following minimum information is shared:

- The Major Business Object and any associated Supporting or Lookup Table Objects that you will work on (example: I'm going to work with Incident and Tasks). Also communicate any associated views or features.
- Features (example: Calendar) you will work on that do not have an associated Business Object.

Communication might include:

- Setting up automatic e-mail notifications (possible in most software).
- Manually sending e-mail or chat messages.

Decide Whether to Use a Blueprint or mApp® Solution

Before beginning the project, decide whether to use a Blueprint or mApp Solution for your system configuration by considering the characteristics and benefits of each.

Blueprints allow you to:

- Use the Blueprint Changes window to view a list of changes included in the Blueprint, remove selected changes from the Blueprint, and compare the version of a change in the Blueprint with the version of the item in the current system.
- Use the Resolve Blueprint Conflicts window to view a list of conflicts between your Blueprint and the current schema. Choose item by item which changes to apply and which to discard.

mApp Solutions allow you to:

- Specify what to import down to the field level of a Business Object.
- Define the specific merge action to take for each item (example: import, overwrite, delete, etc.).
- Rebase (refresh definitions) by looking at the current system's version of each item included in the mApp Solution and bringing the older definition up to parity with the latest definition.

Assign Business Object and Feature Owners

Assign individual Business Objects (including their views and associated features) and features (that do not have an associated Business Object) to different designers as their area of responsibility. For example, one designer is responsible for Incident changes (including the Portal view for Incident) and another designer is responsible for Calendar changes. If multiple designers need to work on the same

Business Object or feature, ensure that the designers are using a check-in/check-out process (refer to the Create a Check-In/Check-Out Process section below).

Create Frequent Backups

Before publishing Blueprints or applying mApp Solutions to the master development database, create a backup .czar file of the system. See Database Export Tool. If the Blueprint or mApp Solution causes significant errors, the database can be restored using the backup file. Also, consider automating frequent backups using the **Backup Database** option in the Scheduler. See Define Action Properties for a Scheduled Item.

Use a Consistent Naming Convention

Ensure that all Blueprints and mApp Solutions follow a consistent naming convention that includes:

- When the Blueprint or mApp Solution was created.
- The primary Business Object.
- The designer's name (example: 2016-12-10-Incident-Johnson.bp or 2016-12-10-Incident-Johnson.mapp).

Store all final Blueprint or mApp Solution files in a common location in a network share. Then, the Blueprints or mApp Solutions can easily be grouped together and applied to the production system in the appropriate order.

Evaluate Security Risks

Consider security risks to both development and production environments throughout the lifecycle of the project. Risks might involve:

- Customer data, including personal or company information.
- Business Object data, including existing active and inactive records.
- Impacted CSM services, such as the Cherwell Application Server,Automation Process Service, etc.
- Impacted external connections, such as SCCM, Outlook, Active Directory, etc.

(Optional) Create a Check-In/Check-Out Process

If more than one designer must work on the same Business Object, create a process similar to the following that allows designers to check out a particular Business Object:

1. Create a master list of all target Business Objects. This can be done using a custom Business Object in CSM, a spreadsheet, or a wiki page.

2. Notify all other designers and update the master list when an item is checked out. The checkout lasts until the changes have been approved by the gatekeeper and applied to the master development database.

3. Create a .czar of the updated master development database. The next time work is done on the item, the designer must use a new .czar.

4. Notify all other designers and update the master list when an item is checked in.

5. Repeat steps two through four until work on the item is complete.

Considerations for Moving from Development to Production

Use the following considerations as a guide for moving changes made in your development environments to your production environment. The application of these considerations may vary depending on your specific strategy.

Database Synchronization

If you are moving changes from development to production by restoring the production environment from a .czar file taken from the development environment, you will need to adjust some configurations to enable integrations with other systems like email and SAML. Before creating the .czar file, adjust the following settings in the development environment to mimic the production environment:

- Set production email account as the default.
- Set the **Current System Production E-mail Sender** stored value.
- Set the Cherwell REST API base URL.
- Adjust browser settings and URLs if needed.
- Set external database connections, if production uses a separate account from development.
- Set CSDAdmin credentials, if you are using an on-premises system.
- Configure the Auto-Deploy Connection to use your production connection.
- If you use Trusted Agent, set the Trusted Agent Hub URL and key for production.

Data Cleanup

Before creating your .czar file, you should remove all test data from the development system, so that it does not get imported into production. Some of the common places you should check for test data include:

- Test ticket records, such as Incidents and Service Requests, Problem Management tickets, Change Requests, and Tasks.
- Supporting records, such as CMDB Configuration CIs, Knowledge Articles, discussion board announcements, vendors, Approvals, Journals, users, customers, and custom Lookup Tables.
- Automation Processes.
- Record ID numbers.

System Maintenance

After cleaning up test data, you should perform system maintenance. First, perform the following data maintenance actions, one at a time, in order:

- **Remove unused user accounts**.

- **Synchronize Team Info Business Objects with team list**.
- **Delete Temporary Data**.
- **Remove orphaned attachments**.

Next, perform the following index management actions, one at a time, in order:

- **Rebuild Business Object indexes**.
- **Rebuild system table indexes**.
- **Shrink SQL event log**.

Note: SaaS customers may need to contact Cherwell Support to perform these actions.

Activate Integrations

Once you have restored the production system with your changes from the development environment, make sure that your integrations are activated as production. The timing of this will vary depending on whether this is your first time using the production system or you are making changes to an existing production system, but some integrations that may need to be activated include:

- Trusted Agent
- Active Directory/LDAP
- User and customer authentication integrations
- Scheduled feeds
- Scheduled CSM Portal credentials
- Current system stored value
- Production Email Monitor
- Custom integrations using web service calls

Final System Checks

Perform these final checks before opening the live production system to your users and customers:

- Check that the Cherwell Service Host is running on the CSM server, and that advanced settings are enabled.
- Check that the CSM Desktop Client, Browser Client, and CSM Portal connections are accessible.
- Check that authentication is working for users and customers.
- Check that inbound and outbound emails are working.
- Check that external database connections are operational.
- Check that the Cherwell REST API URL is operational, if applicable.
- Check that the Scheduling Service is queuing and processing events on time.

- Check that integration events are processing as expected.

Blueprints

A Blueprint is a working copy of changes to your CSM system definitions (Business Objects, Fields, Forms, Grids, etc.) that allows you to make offline changes and then publish them to your live system at a later time.

About Blueprints

Blueprints affect system definitions and are created and managed from within CSM Administrator. Access Blueprints and Blueprint functionality from the CSM Administrator Blueprint page.

Use a Blueprint to:

- **Manage System Objects**: Create, edit, and delete Business Objects, Fields, Forms, Grids, and Relationships.
- **Manage Business Object Data**: Create, edit, and delete data from Supporting Objects and Lookup Objects using the Data Editor.
- **Manage CSM Items at a system level**: Create, edit, and delete various CSM Items (example: Dashboards, Search Groups, etc.) using the CSM Item Managers in a Blueprint. Managing and storing CSM Item definitions at a Blueprint level (and in a Blueprint scope) keeps them extremely secure (only administrators can access them).
- **Access the following Blueprint tools/functionality:**
  - Configure Directory Services integrations: Configure the integration between CSM and various Directory Services (example: Active Directory, LDAP, etc.).
  - Export a Blueprint Schema: A Blueprint Schema is a collection of meta-data that is exported from your system as a single document (.html, .rtf, .txt, or .xml) to textually expose your Business Object definitions and database structure.
  - View the Blueprint Publish Log: A Blueprint Publish Log contains detailed information about Blueprints published to your system.
  - Define global database settings: Global database settings include timeout values, foreign keys, Transaction Log settings, and Form/Grid display settings.

Related concepts

Manage System Objects

Manage Business Object Data

Manage CSM Items

Access Blueprint Tools/Functionality

Related tasks

Review Visual Elements for All Business Objects

Blueprint Workflow

1. Create a Blueprint.

2. Save the Blueprint to the named .bp file (**File>Save As**).

3. Manage your system definitions:
    - System Objects:
        - Business Objects

        - Fields

        - Forms

        - Grids
    - Business Object data
    - CSM Items (example: Dashboards, Saved Searches, etc.)
    - Blueprint tools/functionality

4. Periodically save your changes.

5. Periodically scan the Blueprint for potential errors.

6. View the changes the Blueprint will make to your system definitions.

7. Publish the Blueprint.

> **Tip:** Consider publishing your Blueprint to a test system before publishing to your live system.
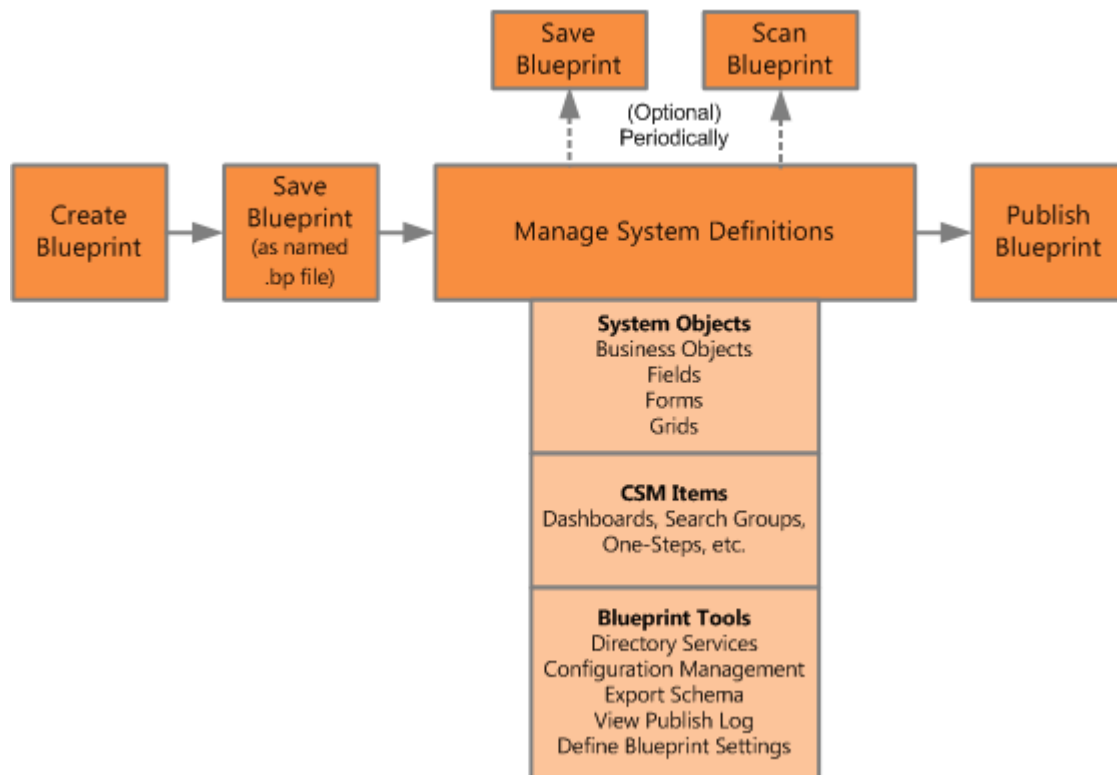
Related concepts

Save a Blueprint

Access Blueprint Tools/Functionality

Scan a Blueprint

View Blueprint Changes

Publish a Blueprint

Related tasks

Create a Blueprint

Managing Blueprints

Blueprints are managed in CSM Administrator using the Blueprint Editor and the Blueprint Tasks pane.

Blueprint Editor

The Blueprint Editor is the built-in interface within CSM Administrator that allows you to manage System Objects, Business Object data, Items, Blueprints, and Blueprint tools/functionality.

When you create and work with Blueprints, the CSM Administrator interface changes to the Blueprint Editor.
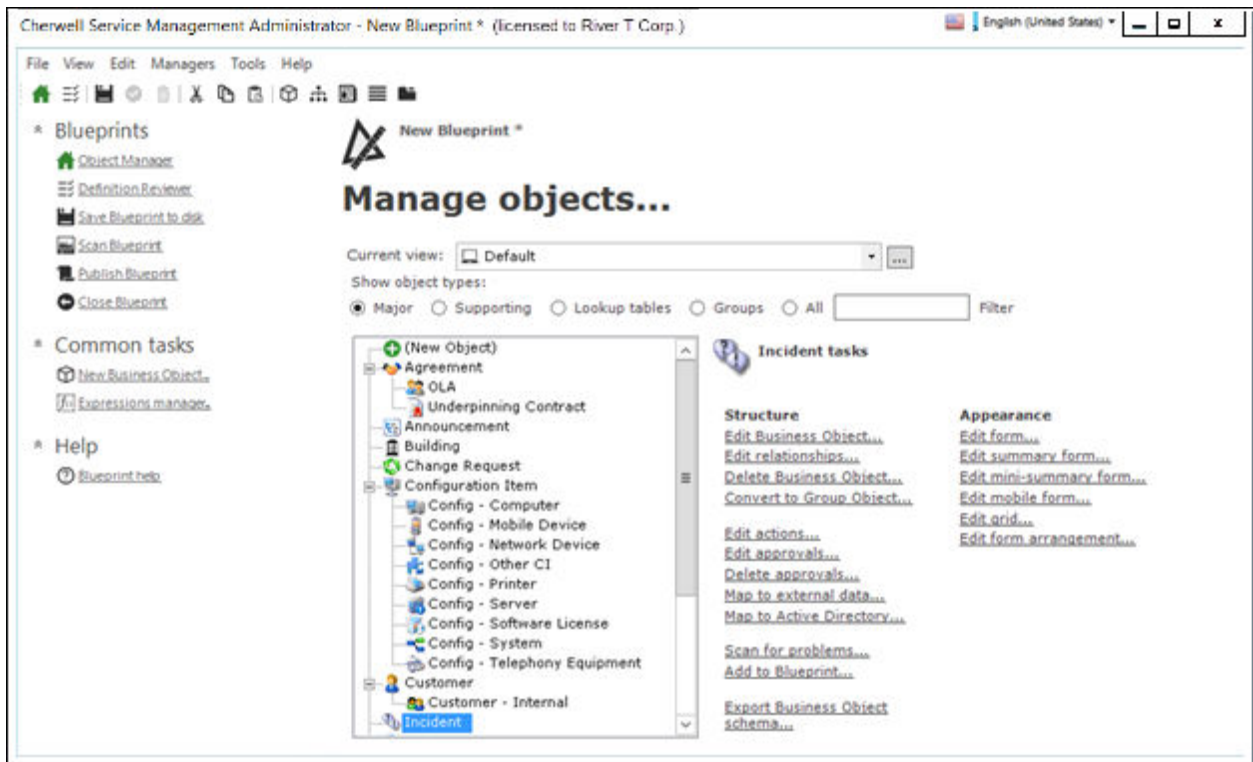
Use the Blueprint Editor to:

- **Manage System Objects**: Create, edit, and delete Business Objects, Fields, Forms, and Grids. System Objects are managed using the Blueprint's powerful Object Manager and Object Editors, which are accessed from the Blueprint Editor main window.

- **Manage Business Object Data**: Create, edit, and delete data from Supporting Objects and Lookup Objects using the Data Editor.

- **Access the Definition Reviewer**: Quickly review and modify Forms, Grids, and Form Arrangements for all Business Objects or for those elements that have changed in the current Blueprint.

- **Manage CSM Items**: Create, edit, and delete Dashboards, Search Groups, etc. at a system level to keep them secure. CSM Items are managed using the various CSM Item Managers.

- **Access the following Blueprint tools/functionality** (click **Tools** from the Blueprint Editor menu bar):

- ◦ Configure Directory Services integrations: Configure the integration between CSM and various Directory Services (example: Active Directory, LDAP, etc.).

- ◦ Export a Blueprint Schema: A Blueprint Schema is a collection of meta-data that is exported from your system as a single document (.html, .rtf, .txt, or .xml) to textually expose your Business Object definitions and database structure.

- ◦ View the Blueprint Publish Log: A Blueprint Publish Log contains detailed information about Blueprints published to your system.

- ◦ Define global database settings: Global database settings include timeout values, foreign keys, Transaction Log settings, and Form/Grid display settings.

- • **Manage Blueprints:** Save, scan, publish, and close Blueprints using the tasks in the Task Pane.

Related concepts

Manage System Objects

Manage Business Object Data

Manage CSM Items

Access Blueprint Tools/Functionality

Related tasks

Review Visual Elements for All Business Objects

Blueprint Editor Menu Bar

Use the Blueprint Editor menu bar to access common Blueprint tasks.

Note: The Blueprint Editor menu bar is dynamic so options vary depending on what is active in the Blueprint Editor main pane. For example, when the Object Manager is active, several additional options are available on the Edit menu; when a grid is active in the Object Manager, the Grid Menu Bar item appears with grid-specific commands; when a form is active in the Object Manager, the Form Menu Bar item appears with form-specific commands; etc.

File Menu

Action	Description
Save Blueprint to disk	Saves changes to the active Blueprint.
Save As	Saves the new or active Blueprint as a named .bp file.
Close Blueprint	Closes the Blueprint, but not CSM Administrator. If the Blueprint is not yet saved to a named .bp file, you are prompted to name and save it. If changes are not yet saved, you are prompted to save them to the active .bp file.
Print Grid	Prints the active grid. Only displayed when a grid is active in the main pane.
Export Grid	Exports the active grid. Only displayed when a grid is active in the main pane.
Scan Blueprint	Scans the active Blueprint for potential errors.
Publish Blueprint	Publishes the active Blueprint to a test or live system.
Blueprint Changes	Opens a window, and then view the items that have been added, changed, or deleted in the active Blueprint.
Exit	Exits CSM Administrator. If you are working in a Blueprint and have unsaved changes, CSM prompts you to save your changes.

View Menu

Selects what to display in the Blueprint Editor main pane.

Action	Description
Object Manager	Opens the Object Manager Home page. For more information about the Object Manager, refer to the Business Object documentation.
Definition Reviewer	Opens the Definition Reviewer. You can then review and modify forms, grids, and Form Arrangements for all Business Objects.

Action	Description
View Business Object	Opens the Business Object Editor. You can then manage the active Business Object.
View Relationship	Opens the Relationship Editor. You can then manage relationships for the active Business Object.
View Form	Opens the Form Editor. You can then manage forms for the active Business Object.
View Grid	Opens the Grid Editor. You can then manage grids for the active Business Object.
View Arrangement	Opens the Form Arrangement Editor. You can then manage the Form Arrangement for the active Business Object.
Find Dependencies	Displays the active Business Object's dependencies.

Edit Menu

Action	Description
Cut	Moves the selected item to the clipboard. You can then paste the item into a new location.
Copy	Copies the selected item to the clipboard. You can then paste the item to a new location.
Paste	Inserts an item from the clipboard to a new location.

Managers Menu

Action	Description
Adaptive Layout Presets	Opens the Adaptive Layout Preset Manager.
Attachment Manager	Opens the Attachment Manager.
Automation Processes	Opens the Automation Process Manager.
Business Hours	Opens the Business Hours Manager.
Calendar Manager	Opens the Calendar Manager.
Counters	Opens the Counter Manager.
Dashboards	Opens the Dashboard Manager, Widget Manager, Metric Manager, or Color Palette Manager.
Database Server Objects	Opens the Database Server Objects Manager.
Document Repositories	Opens Document Repository Manager.
E-mail and Event Monitoring	Opens the E-mail and Event Monitoring Manager.
Expressions	Opens the Expression Manager.
External Connections	Opens the External Connections Manager.

Action	Description
Canonical Definitions	Opens the Canonical Definitions Manager.
Formats	Opens the Stored Format Manager.
Group Maps	Opens the Group Map Manager.
HTML Page Manager	Opens the HTML Page Manager. This allows you to add an HTML page to a Blueprint. To create/edit an internal HTML page, see Manage HTML Pages.
Images	Opens the Image Manager.
Knowledge	Opens Knowledge Mapping Manager, and Knowledge Source Manager.
Language Packs	Opens the Language Pack Manager.
Locked Strings	Opens the Locked Strings Manager.
One-Step Action	Opens the One-Step Action Manager.
Prompts	Opens the Prompts Manager.
Queues	Opens the Queue Manager.
Reports	Opens the Reports Manager.
Scheduled Items	Opens the Scheduled Items Manager.
Searches	Opens the Search Manager.
Site Manager	Opens the Portal Site Manager.
Stored Imports	Opens the Stored Imports Manager.
Stored Values	Opens the Stored Value Manager.
Teams	Opens the Team Manager.
Themes	Opens the Theme Manager.
Twitter Account Manager	Opens the Twitter Account Manager.
Visualizations	Opens the Visualization Manager.
Web Services	Opens the Web Services Manager.
Webhooks	Opens the Webhooks Manager.

Tools Menu

Action	Description
Directory Services	Opens the Directory Services window. You can then configure and manage your Directory Service integrations (example: Active Directory, LDAP, etc.).
Windows Domains	Opens the **Windows Domains** dialog. You can edit your domain connection.

Action	Description
Canonical Mapping Wizard	Opens the Map Canonical Object Wizard. You can use the wizard to map a Canonical object to a Business Object. For more information, see Canonical REST API Mapping Wizard.
Foreign Key Administration	Opens the Foreign Key Administration dialog. You can automatically configure all shared foreign keys in your system. For more information, see Foreign Key Administration.
Export Schema	Exports a Blueprint Schema to a .bp file.
View Publish Log	Displays the Published Blueprint Log.
Options	Opens the Blueprint Options window. You can then define global database settings (example: Timeout values, foreign keys, transaction log, grid and form display settings, etc.).

Localization Menu

Action	Description
Culture Quick Swap (CTRL+Q)	Switch between the preferred culture and the last selected culture.
Preferred Culture (CTRL+D)	Switch to the preferred culture.
Previous Culture (CTRL+L)	Switch to the last culture you selected.

Help Menu

Action	Description
Blueprint Help	Opens the online help.
Report Error	Opens the Report Error window so you can report an error to Cherwell.
About	Opens an **About** window to view version and licensing information for CSM.

Blueprint Editor Toolbar

Use the Blueprint Editor toolbar to quickly access common Blueprint operations.

Note: The Blueprint Editor toolbar is dynamic so options vary depending on what is active in the Blueprint Editor Main Pane (example: When a Business Object is active in the Object Manager, create and delete options are available).

Tip: Many toolbar items are also available from the Blueprint Editor menu bar and the Task Pane.

Button	Action	Description
	Home	Opens the Object Manager Home page in the Editor Main Pane.
	Definition Reviewer	Opens the Definition Reviewer.
	Save	Saves changes in the active window.
	Update	Updates the current item.
	Abandon	Abandons changes to the current item.
	Create New	Creates a new item.
	Delete	Deletes the current selection.
	Cut	Moves the selected item to the clipboard, so you can then paste the item into a new location.
	Copy	Creates a new item whose properties are the same as the copied item. The new item can then be named and customized.
	Paste	Inserts an item from the clipboard to a new location.
	Business Object	Opens the Business Object Editor, where you can manage the active Business Object.
	Relationship	Opens the Relationship Editor, where you can manage Relationships for the active Business Object.
	Form	Opens the Form Editor, where you can manage Forms for the active Business Object.
	Grid	Opens the Grid Editor, where you can manage Grids for the active Business Object.

Button	Action	Description
	Arrangement	Opens the Form Arrangement Editor, where you can manage the Form Arrangement for the active Business Object.

Blueprint Editor Task Pane

Use the Blueprint Editor Task Pane to access Blueprint tasks.

You can access:

- Blueprints: Common tasks for managing Blueprints.
- Common Tasks: Common Blueprint Editor tasks.
- Help: Online documentation.

The Task Pane is located on the left side of the Blueprint Editor.

Behaviors include:

Behavior	Step
• Size the pane	Hover over the gray line on the right side of the pane, and then click-and-drag the **Sizing Handles**.
• Collapse a section	Click the **title banner** of the section.
• Display an item in the Main pane or in a separate window	Click a specific **item**. **Tip:** Hover over an item to display a tooltip.

Open the Blueprint Editor

There are several ways to open the Blueprint Editor:

- In the Common Tasks section of the CSM Administrator Task Pane, select **Create a New Blueprint**.

- In the CSM Administrator main window, select the **Blueprints** category, and then select the **Create a New Blueprint** task or the **Open an Existing Blueprint** task.

  Note: Links to the Publish Log, the Blueprint Consolidation task, and your most recent working Blueprint are also listed here.

Create a Blueprint

Use the Create Blueprint task (accessed from the CSM Administrator main window) to create a new Blueprint file.

To create a Blueprint:

1. Open CSM Administrator.
2. Select **Blueprints > Create a New Blueprint**.
   The Blueprint Editor opens. By default, the Object Manager is displayed in the Blueprint Editor's Main Pane.

   > **Tip:** If any content was applied as part of a Protected mApp™ Solution, you see a shield
   > icon ( ) alongside each item.

3. Select **File > Save As** to save the Blueprint to a named .bp file.
   The name of the open Blueprint is displayed at the top of the CSM Administrator window and at the top of the Blueprint Editor.
4. As you make changes, save the changes to the named .bp file.

   > **Tip:** Periodically scan your Blueprint to find potential errors.

5. When ready, publish the Blueprint to commit the changes.
   Refer to Publish a Blueprint for details about the publication process.

Related concepts
Protected mApp™ Solutions
Protected mApp™ Solution FAQs

Open an Existing Blueprint

Use the Open an Existing Blueprint task (accessed from the CSM Administrator main window) to open an existing Blueprint file.

To open an existing Blueprint:

1. In the CSM Administrator main window, click the **Blueprints** category, and then click the **Open an Existing Blueprint** task.

   Tip: The last saved Blueprint is also listed for your convenience. You can also open the last saved Blueprint by clicking it in the Common Tasks section of the CSM Administrator Task Pane.

2. Select a Blueprint (.bp) file, and then click **Open**.

   The Blueprint opens in the Blueprint Editor. The name of the Blueprint is displayed at the top of the CSM Administrator window and at the top the Blueprint Editor.

Download a Blueprint

Download a Blueprint from the Publish Log to easily revert your system or to apply changes created by another user.

To download a Blueprint:

1. In the CSM Administrator main window, select the **Blueprints** category.
2. Select **View Publish Log** from the Blueprints category. The Blueprint Publish Log opens and displays a list of all Blueprints that have been published to your system.
3. Select a Blueprint, and then select the **Download** button. The File Explorer opens.
4. Select a location on your local machine, and then select **Save**. A copy of the Blueprint is now saved on your local machine.

After downloading a Blueprint, you can open the Blueprint to edit it, or publish the Blueprint to revert your system or apply changes from another user.

Save a Blueprint

You can save a Blueprint to a named .bp file or save changes to the open Blueprint.

To save a Blueprint as a named .bp file:

1. Create a Blueprint.

2. From the Blueprint Editor menu bar, click **File>Save As**.

   Tip: You can also save a Blueprint as a named .bp file by clicking **Save Blueprint to Disk** in the Blueprints section of the Blueprint Editor Task Pane.

3. Provide a **filename** for the Blueprint. Use a naming convention that makes sense to your organization. For example, consider adding a date, time, system name, etc. to the filename to distinguish it.

4. Ensure that the file type is **.bp**.

5. Click **Save**.

   A .bp file is created. The name of the Blueprint is displayed at the top of the CSM Administrator Main window and at the top the Blueprint Editor.

Scan a Blueprint

Use a Blueprint Scan to periodically check your working Blueprint for potential errors. The scan will look for missing items and alert you to any changes you need to make.

Examples of when you will receive warnings:

- You create a Business Object without also creating a Form and/or Grid to display it.
- You delete items that are referenced by other items in CSM (example: An Expression used on a Form).
- A table needs to be rebuilt in the database due to changes in the Business Object.
- You scan a Blueprint that contains Security Group and Role changes that were applied from a mApp Solution.

To scan a Blueprint:

1. Open the Blueprint Editor.
2. From the Blueprint Editor menu bar, click **File>Scan**.

   You can also scan a Blueprint by clicking **Scan Blueprint** in the Blueprints section of the Blueprint Editor Task Pane.

   If the scan is successful, a success window opens.

   If the Blueprint contains changes that require reloading definitions or restarting applications after the Blueprint is published, an alert appears along with the scan results. The alert is triggered if the Blueprint contains changes to significant system definitions, such as Business Objects, Forms, Grids, Form Arrangements, Relationships, Custom Views, One-Step Actions, automated behaviors, Dashboards, and/or Widgets.

   If the scan detects errors, the **Scan Results** window opens and lists errors and warnings.

   You can:

   - Choose to limit the **Display** list to warnings or errors.
   - Click **Show Usage** to open a window that shows how the definition causing an error is used is CSM.
   - Click **Go to Error** to navigate to the error and resolve it (if the error cannot be automatically resolved). For Security Groups and Roles, click this button to compare changes in these definitions.
   - Click **Resolve** to automatically resolve each error or warning separately.
   - Click **Rescan** to rescan the Blueprint.
   - Click **Ignore warnings and continue** to enable the OK button. In this case, when you click OK, the warnings are ignored but the publish continues.

Note: The **Ignore warnings and continue** check box is only available when the display list contains only warnings.

Related concepts

Scan a mApp Solution

Blueprint Scan Errors for Foreign Key Relationships

View Blueprint Changes

Use the Blueprint Changes window in the Blueprint Editor to see which system definitions will be changed by the active Blueprint when it is published.

When you view Blueprint changes, you can:

- Select how to display changes (group by Business Object, Definition Type, or View).
- Search for specific changes in the Blueprint.
- Remove changes from the Blueprint.
- Compare the Blueprint changes with the original system definitions.

The Blueprint Changes window can be opened from the Blueprint Editor menu bar (File>Blueprint Changes).
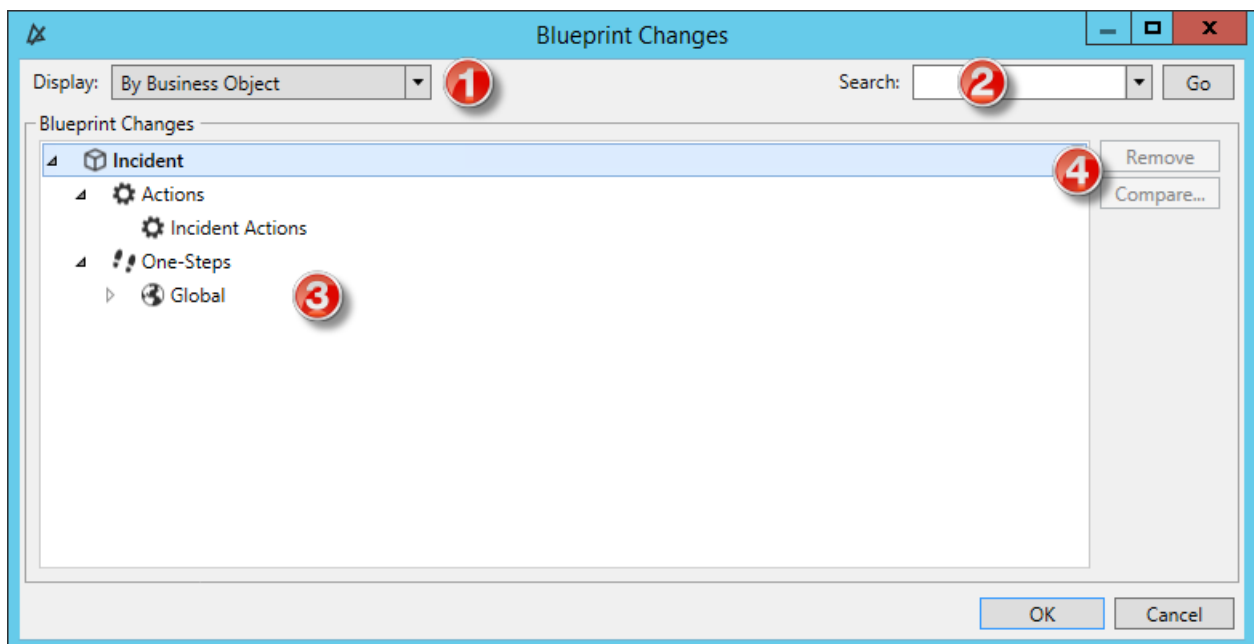
1. Display: Groups changes in the tree by Business Object, Definition, or View.
   - By Business Object: Groups changes by Business Object (example: Incident).
   - By Definition Type: Groups changes by the type of system definition (example: Forms).
   - By View and then Business Object: Groups changes by View (example: Default, Portal Default) and then by Business Object (example: Incident).
   - By View and then Definition Type: Groups changes by View (example: Default, Portal Default) and then by type of system definition (example: Forms).
2. Search: Searches for changes by keyword or phrase.
   a. In the Search Box, provide a **word** or **phrase** to search for. The drop-down displays the most recently used (MRU) searches.

b. Click **Go** to run the search. The items containing the specified word or phrase are displayed within their hierarchical structure.

3. Blueprint Changes tree: Displays changes in a hierarchical tree grouped by the selected display option.
    ◦ Click the **arrow** next to a category (Business Object, Definition Type, or View) to expand it and view its changes. Click the **arrow** again to collapse it.

    Tip: Right-click a **category** or **change** to open a context menu to select options to expand/ collapse the tree, remove changes, or compare definitions.

4. Remove/Compare:
    ◦ Click **Remove** to remove a selected item from the Blueprint (it is not removed from the system).
    ◦ Click **Compare** to compare the Blueprint change with the existing system definition.

    Note: *Remove* and *Compare* are only enabled when you have an individual change selected. You cannot remove or compare changes by selecting display categories (Business Object, Definition Type, or View). You can only compare a change if you edited or updated an existing system definition in the Blueprint; newly added definitions cannot be compared (there is nothing to compare them to).

Review Visual Elements for All Business Objects

The Definition Reviewer provides a quick way to review and modify Forms, Grids, and Form Arrangements for all Business Objects. This is useful for ensuring consistency and usability across visual elements in your system, especially after you apply translations to your system using the Globalization tool set.

You can review and modify:

- All visual elements in a Blueprint or mApp
- Changed visual elements in a Blueprint or mApp

Note: As you modify Forms, Grids, and Form Arrangements in the Definition Reviewer, your changes are saved as you move from definition to definition without having to manually update your Blueprint with changes. This enables you to quickly test and adjust definitions.

To use the Definition Reviewer:

1. Create a Blueprint or mApp.
2. Use one of the following methods to open the Definition Reviewer:
   - From the menu bar, select **View > Definition Reviewer**.
   - Click **Definition Reviewer** in the task pane.
3. From the Definition Reviewer, you can:

Option	Description
1	Select the type of definition to review: Forms, Grids, or Form Arrangements.
2	Select to view all definitions for the selected type or only definitions that have changed in the active Blueprint.
3	Search for a definition of the selected type.
4	Toggle the display of the Business Object name to each visual element.
5	Search for fields used in the selected definition.
6	Toggle the Folders option show definitions in folders or in a list from the root node.
7	Scroll through the definitions list to view Forms, Grids, or Form Arrangements in the editor.

Option	Description
8	Use the editor to modify the Form, Grid, or Form Arrangement as needed. See: ◦ Create/Edit a Form ◦ Create/Edit a Business Object Grid ◦ Create/Edit a Form Arrangement
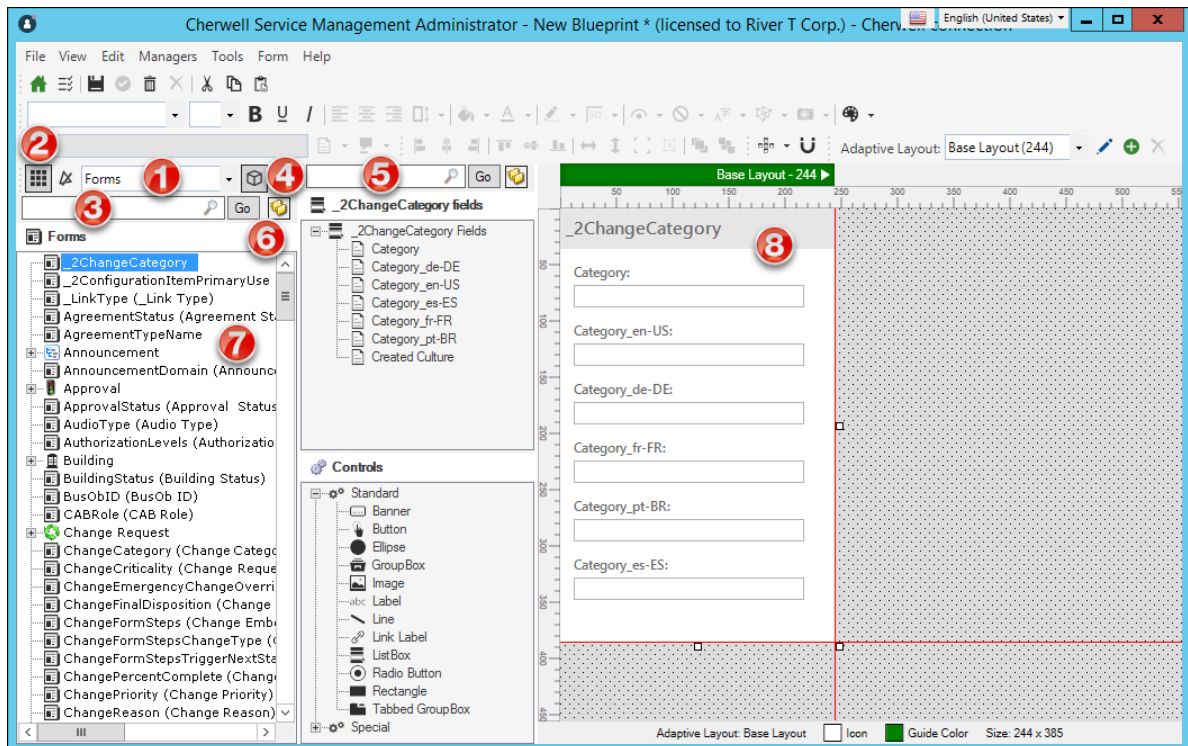
4. Optionally, right-click on a definition in the list to perform these localization tasks:
   ◦ **View Translations**

   See Viewing Translations for Definitions and Form Controls.

   ◦ **Apply Language Pack Bundles**

   See Applying Language Pack Bundles to Definitions or Form Controls.

   ◦ **Delete Translations**

   See Deleting Translations from Definitions.

Publish a Blueprint

Publish a Blueprint to commit definition changes to a test or live system. Before you publish, you are prompted to select before and after publishing operations.

Good to know:

- Publish a Blueprint to a backup test system before publishing to your live system so that you can experiment and verify that everything works.

- If you have transferred protected content from one CSM system to another via Blueprint or a Protected mApp™ Solution, the protected content is transferred in its original format. This means that if it could not be edited or deleted in the original system, then that will be the same in the new system.

- Blueprints *can* be published out of order (that is, if you create Blueprint 1 and Blueprint 2, you can publish Blueprint 2 and then Blueprint 1). However, depending on what you changed, you might get unexpected results.

- A Blueprint contains only those objects that you have modified, so if one administrator works on Incidents and one works on Assets, there will not be any problem. If, however, they both work on Incidents, the changes of the last published Blueprint might overwrite the changes of the previous administrator.

- Use the Cherwell Scheduler to publish the Blueprint after hours when all of the users are out of the system.

- Foreign keys are automatically updated when you publish if the Blueprint contains changes made to foreign key settings for validated fields. The update only occurs for modified foreign key fields and foreign key fields referenced by those fields. For example, foreign keys for the **Sub-Category** field would be updated if changes are made to the **Category** field.

To publish a Blueprint:

1. From the **Blueprint Editor** menu bar, select **File > Publish Blueprint**.

   Tip: You can also publish a Blueprint by selecting **Publish Blueprint** in the **Blueprints** field group of the **Blueprint Editor Task** Pane.

2. Select **Before publishing** operations:

Option	Description
Save Blueprint	Select to save the Blueprint before publishing it. **Note:** If the Blueprint is not yet saved to a named .bp file, you are prompted to name and save it. If changes are not yet saved, you are prompted to save them to the active .bp file.

Option	Description
Create Rollback Blueprint	Select to create a Blueprint rollback file. When published, the changes made by the published Blueprint file are undone.
Scan for errors	Scans the Blueprint for potential errors (for more information, see Scan a Blueprint). The scan looks for missing items and alerts you to any changes you must make.
Stop on Warnings	Select to stop the publishing process when an error is encountered.
Only Scan Enabled Cultures	Select to scan Business Object property values for all cultures that are enabled in your system. For more information, see Manage Cultures.
Only Scan Current Culture	Select to scan Business Object property values for the culture selected in the Culture Selector when you publish a Blueprint.
Scan All Cultures	Select to scan Business Object property values for all cultures available in your system, even disabled cultures, when you publish a Blueprint.
Lock System	(Selected by default) Select to lock the system, preventing users from logging in to CSM Clients while administrative work is being done. **Note:** System administrators can log in to CSM Administrator, but users cannot log in to clients. Users already logged are not automatically logged out of the system.
Pause All Services	(Selected by default) Select to pause all CSM microservices (Automation Process Service, E-mail and Event Monitor, Mail Delivery Service, and Scheduling Service).
Ignore Conflicts	Select to bypass the Blueprint Conflict Resolution feature.

3. Select **Publishing** operations:

Option	Description
Save in the database	(Selected by default) Select to save the Blueprint in the database to which you are connected. We recommend selecting this option to improve system performance when publishing a Blueprint. **Note:** ○ If you choose *not* to save a Blueprint in the database by clearing this check box, the Blueprint *must* be saved and rolled back. Consequently, the **Save Blueprint** and **Create Rollback Blueprint** options in the **Before publishing** field group are automatically selected and disabled. ○ You can only consolidate Blueprints that are saved in the database. When consolidating Blueprints, you must remove any Blueprints that do *not* have the **Save in the database** check box selected.
Publish changes	Select to publish the Blueprint to the database to which you are connected.

4. Select **After publishing** operations:

Option	Description
Rebuild Full-Text Catalog	Select to rebuild the Microsoft SQL Server Full-Text Catalog. If you change Business Objects and fields to include or exclude them in a Full-Text Search, the catalog must be rebuilt for the changes to take effect. **Note:** Include Business Objects and fields in the Full-Text Searches by selecting the **Include in Full-Text Search** check box in the **Business Object Properties** window and the **Field Properties** window. For more information on these windows, see Define Search Results Properties for a Business Object and Define General Properties for a Field, respectively.
Restart Services	Select to restart the CSM microservices you paused before the publish. If you do not select this check box, you must manually restart the Services using the Server Manager. For more information, see About the Server Manager.
Unlock System	Select to unlock the CSM system if you locked before the publish. If you do not select this check box, you must manually unlock the CSM system in CSM Administrator (Security). For more information, see Lock/Unlock the System.
Run a One-Step Action	Select to run a One-Step Action after the publish process is complete. Select a recently used One-Step Action from the drop-down list or select the **Ellipses** button to edit it or to select a different one. When publishing a Blueprint that came from a mApp Solution, the One-Step Action may be pre-populated. **Note:** This option is not available via the CSM Configuration command-line. The Action must be an unassociated One-Step Action (not tied to a particular Business Object).

5. Select **Publish**.

Related concepts

Develop Blueprints Concurrently

Define Publish Blueprint Action Options

Scan a Blueprint

Blueprint Scan Errors for Foreign Key Relationships

Performance Impact of Blueprint Changes

Protected mApp™ Solutions

Performance Impact of Blueprint Changes

Certain changes to Business Objects may cause database tables to be rebuilt during the publish process. This can extend the amount of time it takes to complete the publish process, especially for Business Objects that contain a large number of records. This may impact system performance and cause some Business Objects to be unavailable.

For example, certain changes made to the Journal Business Object may cause a table rebuild, which can prevent users from accessing Journal records in related Business Objects, such as Incidents, during the publish process.

Business Object Changes

Changing the primary key for a Business Object will cause a table to be rebuilt.

Field Changes

The following changes to fields will cause a table to be rebuilt.

Change	Location
Field type	**General** page, **Field Properties** dialog
Text fields only: • **Max allowed** or **Max searchable** options • **Length** setting is decreased	**General** page, **Field Properties** dialog
Number fields only: • **Whole digits** setting decreased • **Decimal digits** decreased	**General** page, **Field Properties** dialog
Field names that are reused in the same publish process. For example, if you rename the **Component** field to **Main Component** and the **Feature** field to **Component**, the table is rebuilt.	**General** page, **Field Properties** dialog

Related concepts

Publish a Blueprint

Scan a Blueprint

Define General Properties for a Field

Define Advanced Properties for a Field

Publish a Rollback Blueprint File to Undo Changes

Rollback Blueprint files serve as a snapshot of CSM prior to changes that are implemented in a newly published Blueprint. After changes are published, you can undo the changes and return the system to its previous state.

Rollback Blueprint files are created before a Blueprint is published, but are only available after a Blueprint has been published.

To remove changes prior to publishing the Blueprint, use the Undo Business Object Changes within a Blueprint feature.

To publish a Rollback Blueprint file and override changes made to your system:

1. In CSM Administrator, select the **Blueprints** category.
2. Select **Open an existing Blueprint**.
3. Navigate to the saved Rollback Blueprint file (example: Desktop/font_changes_rollback.bp).
4. Select **Open**.
   The Rollback Blueprint file opens in the Object Manager.
5. Select **Publish Blueprint**.
   The **Publish Options** window opens.
6. Select the **Ignore Conflicts** check box.
   Select **Publish** in the **Publish Options** window to publish the file.

If changes persist and do not reset when the Rollback Blueprint file is published, reload the system definitions (**CSM Desktop Client > Tools > Reload Definitions**). If reloading the system definitions is unsuccessful, contact your administrator.

Consolidate Blueprints

To simplify the process of applying multiple Blueprints to a system, CSM allows users to combine a series of Blueprints into a single consolidated Blueprint.

You must publish a Blueprint and save it to the database before it appears in the Blueprint Consolidation list. Blueprints are saved to the database by default when they are published.

Note: If you choose not to save the Blueprint to the database, the Blueprint is not available for consolidation in the Blueprint Consolidation list.

When you select a series of Blueprints to consolidate, your selection must include all contiguous Blueprints in the order they were created. You can't leave out any Blueprints in a series, because the changes in the excluded Blueprints might affect subsequent Blueprints. When you select the start and end of the range of Blueprints for consolidation, CSM selects all Blueprints in between.

While most Blueprints can be consolidated, Blueprints that include a Language Pack created from the Globalization section cannot be consolidated. These Blueprints do not have a check box to select in the Blueprint Consolidation list. The simplest approach for consolidation is to apply the Language Pack as one of the last Blueprints. If you need to add a Language Pack in the middle of a series of Blueprints, separately consolidate the range of Blueprints before the Language Pack and the range of Blueprints after the Language Pack. Once the Blueprints are consolidated, you can apply them in order.

Consolidating Blueprints

Create a single Blueprint from a series of Blueprints to simplify the application and save time.

> **Note:** If you edit Blueprint values multiple times, the consolidated Blueprints will not work correctly (**example**: a Blueprint is created and published to update a stored value. The same Blueprint is re-opened to update the same value and published again. If you consolidate those two Blueprints, it will cause "No net changes" errors in the output logs).

To create a Blueprint:

1. Open CSM Administrator.
2. Select **Blueprints** from the Categories list.
   The Blueprints page opens in the main pane.
3. Select **Consolidate Blueprints**.
   The **Blueprint Consolidation** dialog box opens.
4. Select the check box for the Blueprint at the start of the range of Blueprints that will be combined.
5. Shift+Click or Ctrl+Click to select the check box for the Blueprint at the end of the range.
   This will select all check boxes in the range, because only a contiguous set of Blueprints can be consolidated.
6. Select **Save**.
   The Save Consolidated Blueprint window opens.
7. Provide a file name for the consolidated Blueprint.
   Use a naming convention that makes sense to your organization. For example, consider adding a date, time, system name, etc. to the file name to distinguish it.
   A message will indicate that the consolidation was successful.

Close a Blueprint

Use the Close Blueprint option to close the active Blueprint, but not CSM Administrator.

To close a Blueprint, from the Blueprint Editor menu bar, click **File>Close Blueprint**.

Tip: You can also close a Blueprint by clicking **Close Blueprint** in the Blueprints section of the Blueprint Editor Task Pane.

If the Blueprint is not yet saved to a named .bp file, you are prompted to name and save it. If changes are not yet saved, you are prompted to save them to the active .bp file.

View Details of the Last Published Blueprint

Use the View Details of the Last Blueprint Publish task on the Blueprints page to view when and by whom the last Blueprint was published.

Tip: You can also view a detailed Blueprint Publish Log.

To view details of the last published Blueprint in the CSM Administrator Main window, click the **Blueprints** category, and then click the **View Details of the Last Blueprint Publish** task.

Develop Blueprints Concurrently

When you publish a Blueprint, CSM checks your changes against the existing schema and displays a list of conflicts that must be resolved before continuing the publish process.

These conflicts typically arise when another developer has published changes system after you began working on your Blueprint.

The conflicts appear in the **Blueprint Conflict Resolution** window.
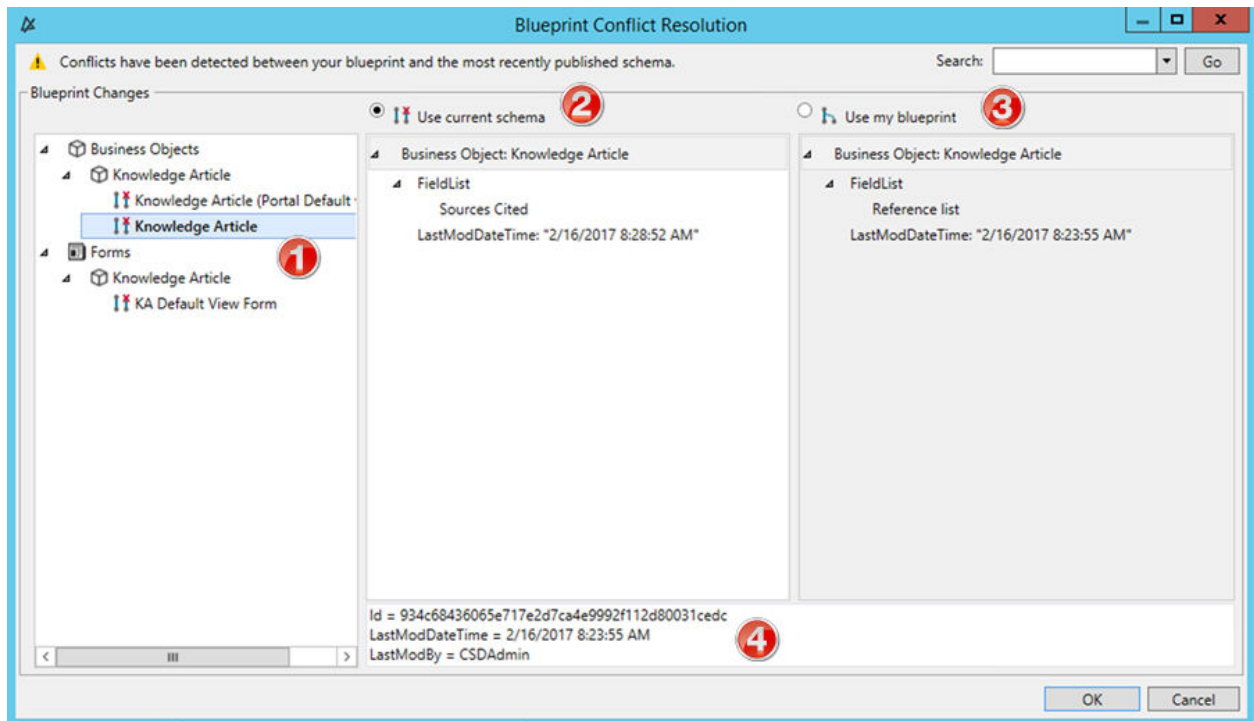
1. The left pane lists conflicts between the most recently-published schema and the Blueprint . Choose item by item which new changes to apply to the schema.

2. Select **Use current schema** to keep the system settings and throw away your changes. This option is selected by default. A disconnect icon ↕✗ denotes you will keep the current schema.

3. Select **Use my blueprint** to publish your Blueprint changes, overwriting the system. The connect icon ↳ denotes items from your Blueprint you intend to publish.

4. Details about the selected item including who last modified it and when.

> **Note:** If another administrator makes a change to the system while you are reviewing the Blueprint Conflict Resolution results, those changes will not be captured in the list of changes. For information on best practices for concurrent development, see Developing in CSM.

You can choose to bypass this feature by selecting **Ignore Conflicts** in the **Publish Options** window.

Using Blueprints

Use Blueprints to manage objects at a system level.

For example, users can:

- **Manage System Objects**: Create, edit, and delete Business Objects, Fields, Forms, and Grids. System Objects are managed using the Blueprint's powerful Object Manager and Object Editors, which are accessed from the Blueprint Editor Main window.

  > **Note:** For more information about managing system objects, refer to the Business Object Documentation.

- **Manage Business Object Data**: Create, edit, and delete data from Supporting Objects and Lookup Tables using the Data Editor.
- **Manage CSM Items**: Create, edit, and delete Dashboards, Search Groups, etc. at a system level to keep them secure. CSM Items are managed using the various CSM Item Managers.
- **Access the following system tools/functionality** (select **Tools** on the Blueprint Editor menu bar):
  ◦ Configure Directory Services.

  ◦ Export a Blueprint Schema.

  ◦ View the Blueprint Publish Log.

  ◦ Define settings for the Blueprint Editor.
- Follow our best practices for system design using concurrent development.

Related concepts
Manage System Objects
Manage Business Object Data
Manage CSM Items
Access Blueprint Tools/Functionality
Related tasks
Review Visual Elements for All Business Objects

Manage System Objects

Use the Object Manager and its various Editors, accessed from within a Blueprint or mApp® Solution, to manage the Business Objects, Forms, Grids, and Fields from a system level.

> **Note:** For more information about managing system objects, refer to the Business Object Documentation.

Manage Business Object Data

Use the Data Editor to manage data in Supporting Business Objects and Lookup Objects.

Note: Because data is edited within a Blueprint, the data in your system is not actually modified until the Blueprint is published.

Data Editor

The Data Editor is the interface within the Blueprint Editor or mApp Solution Editor that allows you to edit data within a Supporting Business Object or Lookup Business Object.

Because data is edited within a Blueprint or a mApp Solution, the data in your system is not actually modified until the Blueprint is published or the mApp Solution is applied.

Use the Data Editor to:

- Add records (rows) with new data.
- Delete existing records.
- Update the data in a record.
- Translate culture-specific values for Lookup Business Objects, if you have localization enabled for the object. See Enable Localization Support for a Lookup Table.
- Clear all data from the table and replace it with new/updated data.

There are several ways to open the Data Editor:

- In the CSM Administrator Main Pane, click the **Settings** category, and then click the **Table Management** task**.**
- In a Blueprint or mApp Solution, select a Supporting Object or Lookup Object (example: Incident Category Lookup Object) from the Object tree in the Object Manager, and then click the **Edit Data** task in the Structure area.
- In the Validation/Auto-Populate page of the Field Properties window, when you select to validate a Field from a table, click the **Edit Table Data** button (activated after selecting a table in the drop-down).
- In a Blueprint or mApp Solution, enable localization for a Lookup Object. Select the option to open the Data Editor so you can translate values. See Configure Localization Support for Lookup Tables.

1. Menu bar: Displays a row of drop-down menus available in the Data Editor.

2. Toolbar: Displays a row of buttons for operations available in the Data Editor.

3. Main Pane: Displays either the list of records in the data table (as a Grid), or the details for the currently selected record (depending on the view you are in). The Action column shows what will be done with the data in each row of the table when the mApp Solution or Blueprint is applied/published.

> **Note:** Select the **Clear all data from destination table** check box to have all existing data in the current system Lookup Object cleared out when the mApp Solution or Blueprint is applied/published. If you want to keep any existing data, you must select the rows with the data you want to keep and click the **Include in mApp** or **Blueprint** button ⬇.

Data Editor Menu Bar

Use the Data Editor menu bar to edit Business Object data.

Note: The Data Editor toolbar is dynamic so available options vary depending on which view you are in (example: When you are viewing the details for a specific record, the cut, copy, and paste options are available) and which tasks you have already performed (example: The option to revert a record to its original values is only available if you have made changes to the record).

File Menu

Action	Description
New	Adds a new row (record) to the table.
Save	Saves changes to the active Blueprint/mApp Solution.
Abandon	Abandons changes to the current item.
Delete	Deletes the current selection.
Include	Includes the selected row (record) in the current Blueprint/mApp Solution (the Action column changes to *Update*).
Restore	Reverts a row (record) back to its original values (the Action column returns to *No Change*).
Print	Prints the current item.
Close	Closes the Manager.

Edit Menu

Action	Description
Undo	Cancels the last operation.
Redo	Repeats the last operation.
Cut	Moves the current selection to the clipboard, so you can then paste it into a new location.
Copy	Creates a new item whose properties are the same as the copied item. The new item can then be named and customized.
Paste	Inserts the cut or copied item from the clipboard.
Refresh	Refreshes the data.

View Menu

Action	Description
Show Results	Displays a set of records meeting a specified criteria.

Action	Description
Show Current Record	Shows the currently selected Record.
First Record	**Go to the first viewed Record.**
Previous Record	Go to the previously viewed Record.
Next Record	Go to the next Record.
Last Record	**Go to the last Record in the list.**

Help

Action	Description
Record Selector Help	Opens the Online Help.

Data Editor Toolbar

Use the Data Editor toolbar to edit Business Object data.

Note: The Data Editor toolbar is dynamic so available options vary depending on which view you are in (example: When you are viewing a specific record, the cut, copy, and paste options are available) and which tasks you have already performed (example: The option to revert a record to its original values is only available if you have made changes to the record).

Tip: Many toolbar items are also available from the Data Editor menu bar.

Button	Action	Description
⊕ New	**Create New**	Creates a new record in the table.
💾	**Save**	Saves changes to the active Blueprint/mApp Solution.
🗑	**Abandon**	Abandons changes to the current item.
✖	**Delete**	Deletes the current selection.
⬇	**Include**	Includes the selected record in the Blueprint/mApp Solution (changes Action column to *Update*).
↩	**Restore**	Reverts an existing record back to its original values (changes Action column back to *No Change*).
✂	**Cut**	Moves the selected item to the clipboard, so you can then paste the item into a new location.
🗐	**Copy**	Creates a new item whose properties are the same as the copied item. The new item can then be named and customized.
📋	**Paste**	Inserts an item from the clipboard to a new location.
✚≡	**Show results**	Displays a set of records meeting a specific criteria.
✚≡	**Show current record**	Displays the currently selected record.
⏮	**Go to first record**	Jumps to the first record in set.
⏪	**Go to previous record**	Jumps to the previous record in set.
⏩	**Go to next record**	Jumps to the next record in set.

Button	Action	Description
▶▶❘	**Go to last record**	Jumps to the last record in the set.

Data Editor Main Pane

Use the Data Editor Main pane to view and select records (rows) in a Lookup table and see how the edits you make will affect each record in your system's Lookup table when the Blueprint is published or a mApp Solution is applied.

When you first access the Data Editor, the Main pane displays a Grid showing a Blueprint/mApp Solution Action column, followed by the lookup table's default Grid.

To view the details of a specific record, click the **Show Current Record** button on the Toolbar.

The Blueprint/mApp Solution Action column shows what will be done to each record in the table when the Blueprint is published (or the mApp Solution is applied):

- No Change: Record will remain unchanged. When you first access the Data Editor, all records are marked as No Change until you edit them.
- Add: A new record was created and will be added to the lookup table.
- Delete: Record will be deleted.
- Update: Existing record will be modified with the values contained in the Blueprint/mApp Solution.

Localization and Lookup Tables

If Localization is enabled for a Lookup Object, the Data Editor includes a column for each culture enabled for your system.

CSM 2022.3 Administration
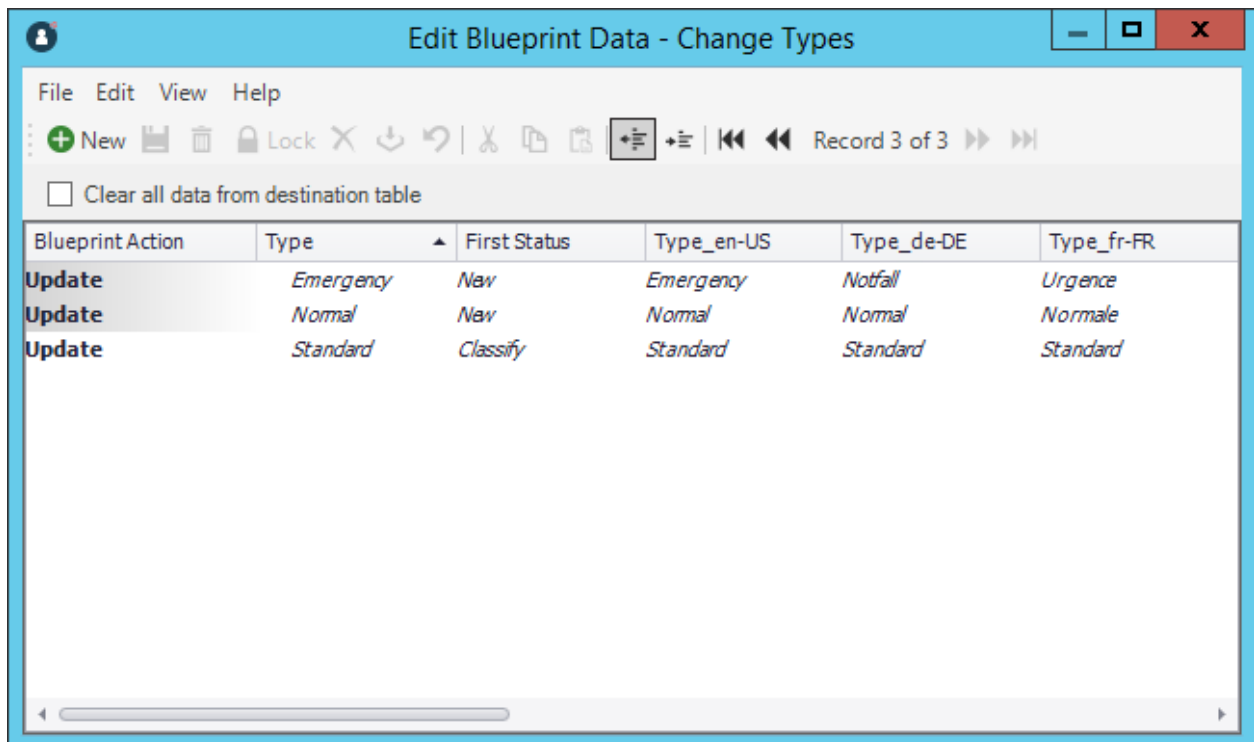
Open the Data Editor

There are several ways to open the Data Editor:

- In the CSM Administrator Main Pane, click the **Settings** category, and then click the **Table Management** task**.**

- In a Blueprint or mApp Solution, select a Supporting Object or Lookup Object (example: Incident Category Lookup Object) from the Object tree in the Object Manager, and then click the **Edit Data** task in the Structure area.

- In the Validation/Auto-Populate page of the Field Properties window, when you select to validate a Field from a table, click the **Edit Table Data** button (activated after selecting a table in the drop-down).

- In a Blueprint or mApp Solution, enable localization for a Lookup Object. Select the option to open the Data Editor so you can translate values. See Configure Localization Support for Lookup Tables.

Manage CSM Items

Manage CSM Items at a system level using the various CSM Item Managers.

Access CSM Item Managers by selecting **Managers** from the Blueprint or mApp Editor menu bar (example: Calendars, Dashboards, and Searches).

When you access CSM Item Managers from within a Blueprint or mApp® Solution, you can view, add, edit, or delete items in the Blueprint or mApp Solution scope. This scope is for items that administrators do not want users to access and manipulate. For more information, see Scope.

Note: For more information about the CSM Items and their Managers, refer to their respective documentation.

Access Blueprint Tools/Functionality

Access Blueprint tools/functionality by selecting **Tools** on the **Blueprint Editor** menu bar.

Use a Blueprint to access the following tools/functionality:

- Define Directory Services: Opens the **Directory Services** window, where you can add, edit, delete, and copy Directory Service definitions.
- Use Trusted Agent Server with Windows Domains
- Export a Blueprint Schema.
- View the Blueprint Publish Log.
- Define Global Database Settings.

Define Directory Services

Use the Directory Service Editor (within the Blueprint Editor) to configure and manage the integration between CSM and a Directory Service.

Using the Editor, you can:

- Add: Create a Directory Service definition that enables and defines the rules for the Directory Service integration.
- Edit: Edits an existing Directory Service integration definition.
- Delete: Deletes a selected Directory Service integration definition.
- Copy: Copies the properties of a selected Directory Service to use a starting point for another Directory Service definition.
- Import: Imports Users from a Directory Service into CSM.

> **Note:** For step-by-step instructions about configuring a Directory Service, refer to the Configuring the Integration with Directory Services.

Use Trusted Agent Server with Windows Domains

When integrating CSM with multiple domains, you can configure single sign-on user authentication by associating a particular Windows Domain with a Trusted Agent Group or Service.

Before you can use Trusted Agent to authenticate Users through a Windows Domain, you must first configure Trusted Agent. For more information, see Configuring Trusted Agent.

Trusted Agent for Windows Domains does not provide pass-through authentication for Windows users. Users must still supply their user name and password in order for their Windows credentials to be validated using the Trusted Agent.

Note: LDAP directory configuration is not required when using Windows.

To enable Windows Domains for Trusted Agent:

1. Verify that CSM is configured for Windows domains:
    - In CSM Administrator, select the **Security** category and then select the **Edit security settings** task. Select each client page (Desktop Client, Browser Client, etc.) and verify that Windows is selected as a login mode.
    - Create or open a Blueprint, and then select **Tools > Windows Domains**. Specify the domain name of the network.
2. On the **Windows Domain Settings** window, select the **Trusted Agents** page.
3. Select the **Use Trusted Agents** check box.

    Note: If you want to disable Trusted Agent for this Windows domain, clear the **Use Trusted Agents** check box.

4. Select one of these group options:
    - **Any Trusted Agent Group**: Select to allow any group to handle requests for this domain.
    - **Trusted Agent Group**: Select a specific group to handle requests for this domain.
5. Select **OK**.

Foreign Key Administration

Foreign key fields shared across Group Members and/or Views must validate from the same table and field to ensure that queries retrieve correct data. You can use the Foreign Key Administrator to automatically configure all shared foreign keys in your system.

If shared foreign key fields are not configured correctly, you receive validation warnings when you edit a foreign key field in a Blueprint or when you run the Foreign Key Configuration Health Check rule.

An example validation warning is:

```
Foreign key field: Agreement.Supplier in view: (Default) requires field: OL
A.Supplier in view: (Default) to be validated from a table
```

Good to Know

- You can use the Foreign Key Configuration Health Check rule to return a list of all shared foreign key fields that are not configured correctly. See About Performance Health Check.
- You can manually configure shared foreign keys in a Blueprint or mApp Solution. See Configuring Shared Foreign Key Fields.
- Standard foreign key rules also apply: shared foreign key fields must be validated from a table and validation must be enforced.
- Constraints for shared foreign key fields can differ between Group Members and Views

To automatically configure share foreign key fields:

1. Create a Blueprint.
2. Open the **Foreign Key Administration** dialog (**Tools > Foreign Key Administration**).
3. Select these options as they apply:

Option	Description
Enforce table validation for all shared foreign key field definitions	Select this check box to automatically configure table validation for all shared foreign key fields in your system. After you publish your Blueprint, the **Validate from table** check box is selected on the **Validation/Auto-populate Page** for all shared foreign keys fields in your system.

Option	Description
Replicate table validation across shared foreign key field definitions	Select this check box to replicate the validation table selection for all foreign key fields that share Views and Groups in the same Business Object. The Foreign Key Administrator attempts to match shared foreign key fields to validation tables based on these rules: ○ If at least one single table match is found for a set of shared foreign key fields, the table is applied to those that do not have a validation table set. For example, if one shared foreign key field in a Group Member has validation set for Table A but a validation table is not specified for the shared foreign key fields in other Group Members, Table A is set as the validation for all Group Members. ○ If two different validation tables are detected for shared foreign key fields in the same Group or View, no change is made. ○ If no validation tables are set for any shared foreign key fields, no change is made.
I have read the following statement...	You are required to acknowledge that you understand the implications of changing table validation on all shared foreign key fields.

4. Select **OK**.

5. Publish the Blueprint.

> **Important:** Verify changes before publishing the Blueprint to a production environment.

Export a Blueprint Schema

Use a Blueprint Schema to quickly and easily scan the characteristics of your Business Objects.

A Blueprint Schema is a collection of meta-data that is exported from your system as a single document (.html, .rtf, .txt, or .xml) to textually expose your Business Object definitions and database structure.

You can export the following meta-data for Major, Supporting, and Lookup Objects:

- Properties
- Lifecycle
- Fields (and Field properties)
- Relationships (and Relationship properties)
- One-Step Actions
- Approvals
- Automation Processes

> **Note:** The Blueprint Schema for the CSM Starter Database is available in the *CSM Starter Database Schema Guide*.

To export a Blueprint Schema:

1. In the CSM Administrator main window, click the **Blueprints** category, and then click the **Create a New Blueprint** task.

   > **Note:** If working on a saved Blueprint, open the existing Blueprint.

   The Blueprint Editor opens.

2. On the Blueprint Editor toolbar, click **Tools>Export Schema**.

3. Select the types of Business Objects to export in the Schema:
   - Major: Select to export Major Business Objects.
   - Supporting: Select to export Supporting Business Objects.
   - Lookup: Select to export Lookup Business Objects.

4. Select the items (meta-data) to export in the Schema:
   - Business Object Properties
   - Business Object Lifecycle
   - Fields
   - Relationships
   - One-Step Actions
   - Approvals

◦ Automation Processes

5. Select **OK**.

6. Provide a **location**, **filename**, and **file type** (.html, .rtf, .txt, or .xml) for the Schema, and then click **Save**.

The selected meta-data is exported to a Schema file. You can then open and view the Blueprint Schema in a viewing tool, such as Microsoft Word.

View the Blueprint Publish Log

Use the Publish Log to view detailed information about Blueprints published to your system.

The log tracks the following details in a Grid:

- A short description of the change the published Blueprint made to the system.
- Type (example: Form) and name (example: Incident) of the system definitions that were changed by the Blueprint.
- User Name of the person who published the Blueprint.
- Dates/times that the Blueprint publish was initiated and completed.
- Scope (example: Global) of the system definition (if applicable), as well as the scope owner (if applicable).
- User-defined name of the Blueprint file (.bp).
- Business Object associated with the definition (if applicable) (Association column).
- The view (example: Portal Default) that the Blueprint change applies to (if applicable).
- The path where the Blueprint file was saved (if applicable).

The Blueprint Publish Log can be opened from the Blueprint Editor menu bar (Tools>View Publish Log).

- Menu bar: Click the **File** menu to perform the following operations:
  - Clear Log: Select this option to clear all entries in the log, or to clear all entries prior to a specified date.
  - Export: Select this option to export the Grid of Publish Log data to a file.
  - Print: Select this option to print the Grid of Publish Log data.
  - Close: Select this option to close the Publish Log window.

    Tip: You can also select Clear Log, Export, and Print from a context menu by right-clicking an item in the Publish Log.

- Toolbar: Select an option from the View drop-down to filter the items in the Publish Log:
  - All Records: Shows everything that was published in a Blueprint.
  - Definition type: Shows all definitions of a particular type (example: Business Object). When you select this option, a Definition drop-down is displayed on the toolbar, and then select a definition type.
  - Only Definition Changes: Shows only the definitions that were changed by the published Blueprint.
  - Particular User: Shows the definitions that were published by a particular User. When this option is selected, a User drop-down is displayed on the toolbar, where you can select a User.
  - View: Shows the definitions that apply to a particular View (example: Default). When this option is selected, a View drop-down is displayed on the toolbar, and then select a View.
- Refresh: Click this button to refresh the data in the Publish Log.

- Download Blueprint: Click this button to download the selected Blueprint.

- Create rollback Blueprint: Select this check box to create a rollback Blueprint when downloading a Blueprint. This allows you to undo a Blueprint's changes.

- Main Pane: Displays the Grid of Publish Log data, filtered by View.

Define Global Database Settings

Global database settings/defaults control how the CSM database looks and behaves by default.

Use the Blueprint Options window in a Blueprint in CSM Administrator to define the following global database settings:

- Global database options (Database Options page): Timeout values and Foreign Keys settings.
- Database Transaction Log settings (Database Transaction Log page): Database Recovery Model and autogrowth settings.
- Configure Grid and Form display settings (Display Options page).

The Blueprint Options window can be opened from the Blueprint Editor menu bar (Tools>Options).

Define Global Database Options

Use the Database Options page in the CSM Administrator Blueprint Options window (accessed from within the Blueprint Editor) to define global general database options.

Options include:

- Database timeout values: How long the database attempts to complete an operation before giving up.
- Foreign Keys: Whether or not to enable/enforce Foreign Keys. Foreign Keys establish and enforce a link between tables in a relational database, and are required by SQL Reporting Services.

To define global database options:

1. Open the Blueprint Editor
2. From the Blueprint Editor menu bar, click **Tools>Options**.
3. Click the **Database Options** page.
4. Define Timeout values for the database:
   a. Database command timeout: Specify the number of seconds to attempt a database command before giving up.
   b. Schema command timeout: Specify the number of seconds to use before timing out on SQL Server DDL (Data Definition Language) commands (used to create and modify database tables in the underlying database).

   > **Note:**
   >
   > Select a **No Limit** check box to indefinitely attempt to complete the operations.
   >
   > Leaving no set limit, however, may have an impact on system performance (for more information, see Worst Queries by CPU). Instead, we recommend increasing the set limit. You must publish the Blueprint for changes to take effect.

5. Enable and define Foreign Key settings:

   > **Note:** You must enable foreign keys in order to use SQL Reporting Services.

   a. Create Foreign Keys for Relationships: Select this check box to enable/create foreign keys.
   b. Not Enforced/Enforced: Select whether or not to enforce foreign keys.

6. Select **OK**.

Define Global Database Transaction Log Settings

Use the Database Transaction Log page in the CSM Administrator Blueprint Options window (accessed from within the Blueprint Editor) to define global Database Transaction Log settings.

Settings include:

- Database Recovery Model: How much data is logged (Simple, Full, or Bulk-logged) in the event that you need to restore your CSM database.
- Autogrowth: Whether or not to enable autogrowth (process for expanding the size of the CSM database when it runs out of space), and then the autogrowth file size increments/thresholds.

Good to know:

- These are all common database tasks, so please consult your database administrator.
- If you are a SaaS User with a 2-tier connection, you must have security rights to access this page and define settings. This page is not available to SaaS Users with 3-tier connections. See Database Options Security Rights.

To define global database settings:

1. Open the Blueprint Editor.
2. From the Blueprint Editor menu bar, click **Tools > Options**.
3. Click the **Database Transaction Log** page.
4. Select a **Database Recovery Model** from the following options:
   - Simple (recommended): Simple backup (minimal logs); can restore full or differential backups only (no point in time).
   - Full: Complete backup (full logs); can restore database to a specific point in time.
   - Bulk-logged: Full backup except that bulk operations are not fully logged.
5. Enable and define autogrowth settings:
   a. **Enable Autogrowth for Transaction Log**: Select this check box to enable autogrowth, allowing the database to expand if it runs out of space. Then, define how the database size will increment, either:
      - In Percent: Select this radio button to allow the database to grow by a percentage of the current size. Then, define the percentage.
      - In Megabytes: Select this radio button to allow the database to grow by a specific size, in megabytes (MB). Then, specify the size.
   b. Specify a **Maximum File Size** for the transaction log, either:
      - Restricted File Growth: Select this radio button to restrict the transaction log to a maximum size (in MB). Then, specify the maximum size.
      - Unrestricted File Growth (recommended): Select this radio button to allow the transaction log to grow until it runs out of space.

> **Note:** This is not stating that the transaction log is a database, but instead that for any given database, you can specify the associated maximum file size for the transaction log.

6. Select **OK**.

Define Global Grid and Form Control Display Settings

Use the Display Options page in the CSM Administrator Blueprint Options window (accessed from within the Blueprint Editor) to define global display settings.

Settings include:

- Form Controls: Default border style for new Form controls.
- Grid Groupings: Enable Grid Groupings and define default display options.

> **Note:** These defaults act like a template because they promote consistency; however, some of the settings can be overridden in the individual Grid and Form definitions.

To define Grid and Form Control display settings:

1. In the CSM Administrator main window, click the **Blueprints** category, and then click the **Create a New Blueprint** task or the **Open an Existing Blueprint** task.

   Tip: Your most recent working Blueprint is also listed here. Click it to open it in the Blueprint Editor.

2. From the Blueprint Editor Menu bar, click **Tools>Options**.

3. Click the **Display Options** page.

4. In the *Border Style for New Controls* drop-down, select a default border style for new Form Controls:

Use Value From Theme	Uses the border format of the Form's default theme.
Create 3D Border	Adds a raised 3D border on new Form Controls.
Create Flat Border	Adds a flat border on new Form Controls.

5. In the Grids area, select default display settings for Grid Grouping:

Default to Allow Grouping on Grids	Shows the Group By box by default on all Grids. **Note:** This default automatically selects the Yes, (Show Grouping) radio button in each system Grid definition; however, it can be overridden.
Default to Showing Grouping on Grids on Tabs	Automatically shows Grid Grouping functionality on Grid Tabs.
Default to Allowing User to Enable Grouping on Grids on Tabs	Allows Users to enable Grid Grouping on Grid Tabs if it is not automatically enabled.

Default to Allowing Users to Remember Grouped Columns Between Sessions	Allows Grid Grouping persistence.

Configuring Blueprints

System Blueprints Security rights are configured in CSM Administrator.

See System Blueprints Security Rights.

mApp Solutions

A mergeable application (mApp) Solution is a bundle of CSM system definitions (Business Objects/Fields, Forms, Grids, Relationships, Actions/One-Step Actions, Saved Searches, etc.), along with merge instructions, that allows definitions to be transferred between databases and functionality to be merged.

Related concepts

Cherwell-provided mApp Solutions

Cherwell Labs mApp Solutions

About mApp Solutions

Use a mApp Solution to share packages of functionality across databases, allowing Users to implement proven functionality into their CSM systems

A number of Cherwell mApp Solutions and third-party integrations have already been created and can be applied to your system using the Apply mApp Wizard.

You can also create your own mApp Solutions. After you create a mApp Solution, you can distribute the file directly to potential Users, or submit it to the Cherwell community. Using the Apply mApp Wizard, system administrators can then apply the mApp Solution to CSM systems based on the items that were included in the mApp Solution.

mApp Solutions are accessed and managed through the mApp Solution Editor, which is similar to the Blueprint Editor, except it has multiple options for adding items to a mApp Solution and defining their behavior. mApp Solutions have their own workflow.
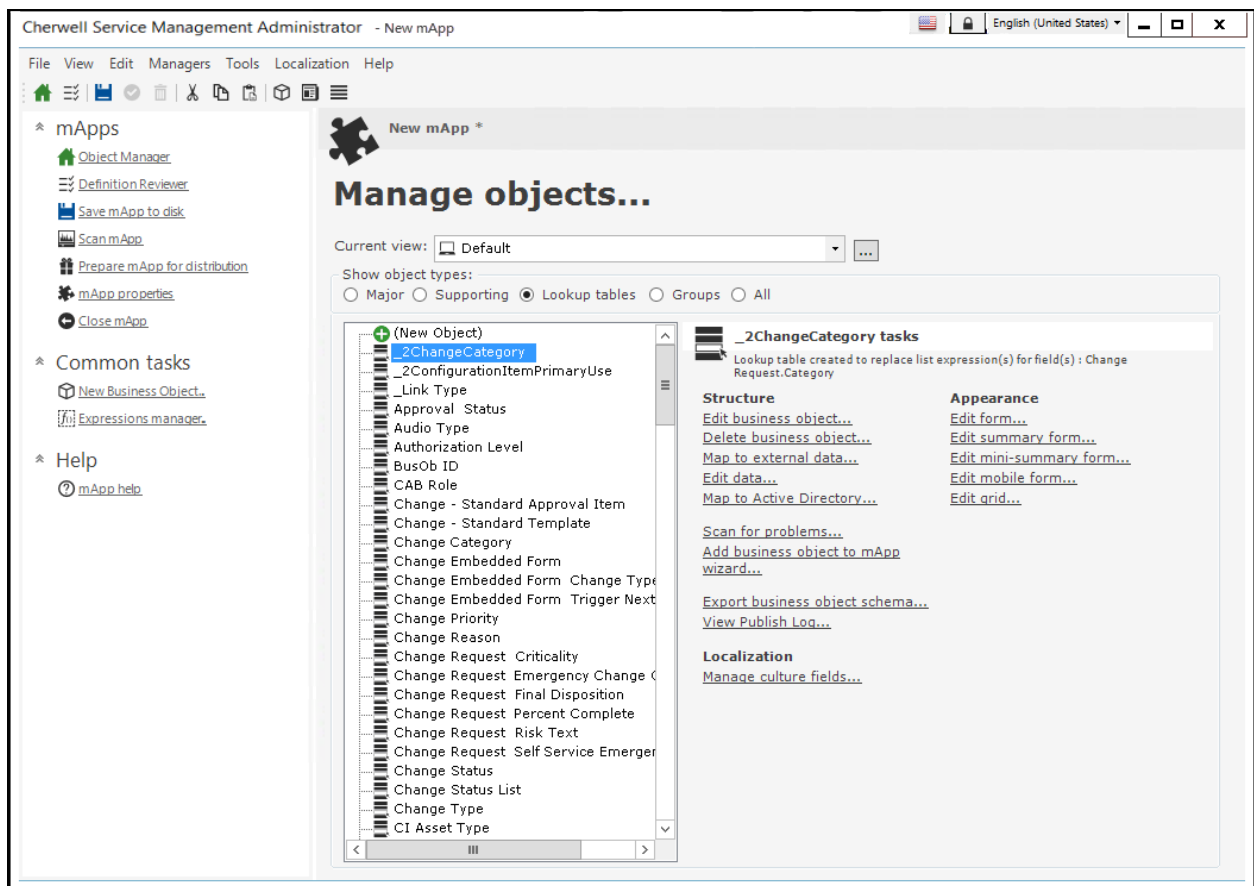
Related concepts
Apply a mApp Solution
Create a mApp Solution

mApp Editor
mApp Solution Workflow

mApp Solution Workflow

1. Create a mApp Solution.

2. Define mApp Solution properties, including any content protection.

3. Save the mApp Solution to a named .mAppBP file (**File > Save As**).

4. Add/edit definitions and items to the mApp Solution:
   - System Objects:
     - Business Objects
     - Fields
     - Relationships
     - Forms
     - Grids
     - Form Arrangements
   - CSM Items (example: Dashboards, Saved Searches, One-Step Actions, etc.)
   - Business Object Data (for Supporting Objects and Lookup Objects)
   - Security Groups and/or Roles.

5. Periodically save your changes.

6. Periodically scan the mApp Solution for potential errors.

7. View the changes the mApp Solution will make to the target system's definitions when the mApp Solution is applied.

   Note: If you have protected the mApp Solution then the existing Business Object fields, relationships etc. can only be merged instead of overwritten.

8. Prepare the mApp Solution for distribution by validating that it is complete and ready for distribution.

   Note: At this point, the mApp Solution must be saved as a .mApp Solution file. This is required in order for it to be applied using the Apply mApp Wizard.

9. Test the mApp Solution in a separate development environment.

10. Distribute the mApp Solution file directly to potential users, or submit it to the mApp Exchange.

11. Apply the mApp Solution to a CSM system using the Apply mApp Wizard.

```
                              ┌──────────┐  ┌──────────┐      ┌──────────┐
                              │   Save   │  │   Scan   │      │   Save   │
                              │   mApp   │  │   mApp   │      │ mApp (as │
                              └──────────┘  └──────────┘      │.mapp file)│
                                     (Optional)               └──────────┘
                                     Periodically
┌────────┐  ┌────────┐  ┌──────────┐  ┌──────────┐  ┌──────────┐  ┌──────────┐  ┌──────────┐  ┌──────────┐
│ Create │  │ Define │  │   Save   │  │   Add    │  │ Prepare  │  │ Test mApp│  │Distribute/│  │  Apply   │
│  mApp  │  │  mApp  │  │ mApp (as │  │Definitions│  │ mApp for │  │in separate│  │ Submit   │  │   mApp   │
│        │  │Properties│ │  named   │  │and Items to│  │Distribution│  │   Dev    │  │   mApp   │  │(using Apply│
│        │  │        │  │.mAppBP file)│ │   mApp   │  │          │  │environment│  │          │  │mApp wizard)│
└────────┘  └────────┘  └──────────┘  └──────────┘  └──────────┘  └──────────┘  └──────────┘  └──────────┘
```

System Objects
(Add Business Object to mApp wizard)

Business Objects
Fields
Relationships
Forms
Grids
Form Arrangements

CSM Items
(mApp button in CSM Item Managers)

Dashboards, Search Groups, One-Steps, etc.

Business Object Data
Edit data for Supporting Object and Lookup Tables

Security
(mApp button in Security Groups and Roles Managers)

Security Groups
Roles

Related concepts

Create a mApp Solution

Apply a mApp Solution

Define mApp Solution Properties

Scan a mApp Solution

Prepare a mApp Solution for Distribution

mApp Solutions Page

Use the CSM Administrator mApp Solutions page to quickly access common mApp Solution operations.

Open the mApp Solutions page by clicking the **mApp Solutions** category in the CSM Administrator main window.

Common operations include:

- View installed mApp Solutions: Opens a window to view a list of mApp Solutions that have already been installed in your system.
- Go to the mApp Exchange: Navigates to the mApp Exchange to submit created mApp Solutions and view mApp Solutions that other Users have submitted.
- Set Designer ID: Allows mApp Solution creators to save a unique developer ID in their current User information. The developer ID is included in history records for all definitions the creator adds to a mApp Solution.
- View mApp Solution History: Scans definitions in the current system and displays history records (if available). The ability to view history records is based on security rights.
- Apply a mApp Solution: Opens the Apply mApp Wizard to walk through the process of applying a mApp Solution to a CSM system.
- Create a New mApp Solution: Creates a new unnamed mApp Solution, and then launches it in the mApp Editor.
- Edit an Existing mApp Solution: Allows you to browse for and open an existing mApp Solution file so that you can edit it in the mApp Editor.

Related concepts
mApp Editor

mApp Solutions Good to Know

Use these tips for helpful information on mApp® Solutions.

- mApp Solutions affect system definitions and are used and managed from within CSM Administrator. Access mApp Solutions and mApp Solutions functionality from the CSM Administrator mApp Solutions page.
- When you include a definition in a mApp Solution, you decide how it will be handled when the mApp Solution is applied to a target system:
  - Import: Imports the definition into the target system.
  - Remove: Removes the definition from the target system.
  - For Reference Only: Includes the definition in the mApp Solution for informational purposes only (the definition is not imported into the target system). You should rarely (if ever) need to do this manually, as the system automatically adds definitions as necessary for reference only. For example, to:
    - Identify the Business Object associated with an item (example: One-Step™ Action) in a mApp Solution so that it can be associated correctly in the target system.
    - Identify a group leader when only some group members are added to a mApp Solution.
    - Identify the view that items belong to. *For Reference Only* allows items to be imported into systems that might not have the same associations, groups, or views available.
- If a definition in a mApp Solution is matched to a definition in a target system, you can select how to import it and what to do with the existing definition:
  - Overwrite: Overwrites the existing definition in the target system.
  - Don't Import: Skips importing the mApp Solution definition into the target system (the existing definition is left unchanged).
  - Merge: Merges the mApp Solution definition with the definition in the target system (you can import/overwrite or skip importing individual areas of the definitions).
- The following definitions can be merged:
  - Business Objects
  - Fields (individual fields and their properties)
  - Relationships (individual relationships and their properties)
  - Form arrangements (individual tabs)
  - Business Object Actions (areas [example: Task Pane] and individual Actions)

  For more information, see Configure Merge Actions for Business Object Definitions.

- Security rights control access to CSM functionality and are configured in the Security Group Manager in CSM Administrator (**Security > Edit Security Groups**). For more information, see Security rights and Configure mApp Solution Security Rights.
- In OOTB content versions 10.0.x, 10.1.x, and 10.2.0, the Related Item Navigation feature is enabled for the Incident and Problem Business Objects. If you have a mApp Solution that was created on a content version earlier than 10.0.0, and it overwrites or merges with Incident or Problem (such as the Managed Service Provider mApp Solution), review the Related Item Navigation within these

Business Objects before you publish the mApp Solution Blueprint. Verify that you need all items within the Related Item Navigation and remove any tabs that are not for reference purposes. Thoroughly test functionality, especially in the CSM Browser Client.

Related concepts

mApp Solutions Page

Create a mApp Solution

mApp Editor

Tips for Creating and Using mApp Solutions

Use the following tips to help you create an effective mApp Solution:

- Have a plan:
  - Gather information (interviews, research, etc.) to get ideas.
  - Create real-world scenarios.
  - Create flowcharts, wireframes, prototypes, etc.
- Check your assumptions:
  - How the mApp Solution will be used.
  - What the target system will look like.
  - What limitations exist (example: You cannot edit an existing Form, but you can create a new Form).
- Keep the following in mind:
  - Check for References to ensure all dependent definitions are included in a mApp Solution.
  - When you include a Business Object in a mApp Solution and select *Merge* as the merge action, only include the Fields that apply to the mApp Solution (delete the Fields you do not want to be imported into a target system). If the Business Object does not exist in the target system, it will be imported in its entirety, without any unnecessary Fields.
  - When you include a Relationship in a mApp Solution, either add the reverse Relationship to the mApp Solution or clear the Reverse Relationship check box (on the General page in the Relationships Properties window).

Following are some tips for applying mApp Solutions:

- Apply a mApp Solution against a test environment before committing it to your live production environment. This allows you to verify that changes are applied without errors and produce the expected results.
- For mApp Solutions that contain Security Groups and Roles, carefully review security changes that may impact the target system after you apply the mApp Solution. Also, remember that you must manually assign Users to Security Groups after you apply a mApp Solution that contains Security Groups.

Protected mApp™ Solutions

Use a Protected mApp Solution to prevent content from being edited or deleted after a Protected mApp Solution is applied.

If a Protected mApp Solution is applied to CSM:

- The list of installed mApp Solutions shows which mApp Solutions are upgradable.

- A shield icon ( ) is shown alongside protected content items. The shield icon may be displayed in Blueprints, Business Object Editors, Item Managers, Relationship Grids, Form Editors, the Form Arrangement Editor or the Grid Editor.

- **Save** is disabled on any Item Manager that has a shield icon ( ) alongside it. You can still make changes to the items in a Manager with a shield icon but you must select **Save As** to create a copy of the contents of the Manager.

- A message is shown, for example, in a Blueprint:
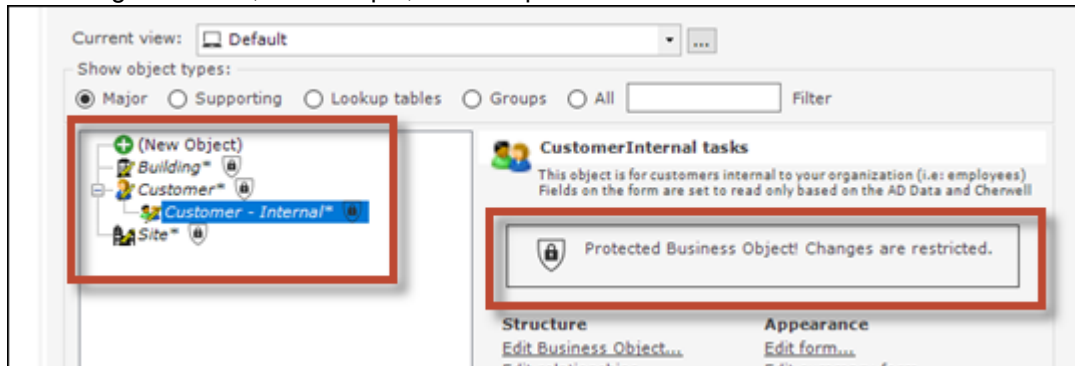
You can also create your own Protected mApp Solutions that can be distributed just like non-upgradable mApp Solutions.

Important: When applying a Protected mApp Solution to your CSM system, the merge actions available to you depend on which items were chosen for protection when the mApp Solution was created. For example, if the mApp Solution was marked as protected when it was created, then the existing fields, relationships etc. can only be merged in the target system instead of being overwritten.

Related concepts

Add a Business Object to a Protected mApp™ Solution

Apply a mApp Solution

Protected mApp™ Solution FAQs

Frequently Asked Questions (FAQs) about Protected mApp Solutions to help you quickly understand how to get the most from this feature.

For help on how a Protected mApp Solution differs from any other mApp Solution, see: Upgradable mApp Solutions.

1. **Why should I protect content by using a Protected mApp Solution?**

   Content protection gives you the ability to lock down your mApp Solution and control customizations to ensure smooth upgrades in the future.

   Content Protection is optional but brings benefits. For example, you can create a Protected mApp Solution on your development system and protect it. This allows you to install it on your test and production systems secure in the fact that no-one can make changes to the Protected mApp Solution.

2. **Can any mApp Solution be protected or just Cherwell mApp Solutions**?

   Protecting a mApp Solution and making it potentially upgradable is part of the mApp Solution authoring process so anyone can do it. You just select a checkbox when you are creating the mApp Solution.

3. **Are all properties of a field protected or can you protect individual properties?**

   Some field properties can be changed. For example, the display name of a field can be changed to suit your requirements and the length of the field can be extended. New indexes can also be added to field properties.

4. **If a form is protected, can I change the form name?**

   No, the form name cannot be changed. This also applies to Business Object names.

5. **How does merging work? For example, what happens to existing fields that are changed?**

   If field A (from the Protected mApp Solution) is merged with field B (in the target system), this results in fields A and B in your system after the merge.

   If field A (from the Protected mApp Solution) is merged with an identical field A (in the target system) from a previous mApp Solution, this results in an *upgraded* field A with the protected properties from the mApp Solution and the customized properties from the target system.

   If field A (from the Protected mApp Solution) and field B (in the target system) have the same field name, the field in your target system will be renamed with an underscore (_) prefix.

    Tip: Automatic renaming of duplicate names with an underscore (_) also applies to Item Managers, forms, relationships and other Business Object Definitions.

6. **When you refer to protecting fields in existing Business Objects, do you mean new fields or can a Protected mApp Solution protect existing fields?**

   Both. New fields added by a Protected mApp Solution are critical to that mApp Solution and will be protected. Existing fields that are merged with new content from the Protected mApp Solution will also be protected after the Protected mApp Solution is applied.

7. **Can we modify relationships after a mApp has been applied?**

   Yes, you can. If the relationship is protected, you cannot modify that relationship but you can replace the relationship. You can make a copy, make the changes, and replace the relationship. You can add all the new relationships that you need; it is the relationships defined in the Protected mApp Solution that are protected.

8. **Can I switch on content protection for an existing mApp Solution?**

   Yes, you can. Open your mApp Solution in the mApp Editor, go to mApp Properties, and select the **Protect mApp content on publishing** check box. Publish your Protected mApp Solution in a Blueprint and then Apply a mApp Solution to your system.

9. **How do I remove the content protection after applying a Protected mApp Solution?**

   Protection cannot be removed from the system itself once installed. However, you can rollback the mApp Solution by publishing a Rollback Blueprint file.

Related concepts

Protected mApp™ Solutions

Add a Business Object to a Protected mApp™ Solution

Managing mApp Solutions

mApp Solutions are managed in CSM Administrator using the mApp Solution Editor.

Use the mApp Solution Editor to:

- Create a mApp Solution.
- Edit an existing mApp Solution.
- Save a mApp Solution.
- Scan a mApp Solution.
- Close a mApp Solution.
- View mApp Solution changes.
- Prepare a mApp Solution for Distribution.

Related concepts
mApp Editor
Open the mApp Editor

mApp Editor

The mApp Editor is the built-in interface within CSM Administrator that allows you to manage mApp®
Solutions and access various tools for adding definitions to mApp Solution.

.

Use themApp Editor to:

- **Add Business Objects to a mApp**: Use the Add Business Object to mApp Wizard to add Business
  Objects and their associated Fields, Relationships, Forms, Grids, and Form Arrangements to a
  mApp Solution.

- **Add CSM Items to a mApp**: Use the mApp Solution options button ✻ in CSM Item Managers (or
  right-click item**>Add to mApp**) to include things like One-Step Actions, Dashboards, Saved
  Searches, etc. in a mApp Solution.

- **Open the Definition Reviewer**: View and modify Forms, Grids, and Form Arrangements for all
  Business Objects or for those that have been modified in the mApp Solution.

- **Edit Business Object Data**: Use the Edit Data task within a mApp Solution to modify (add, edit,
  delete) data for a Supporting Object or Lookup Table.

- **Manage mApp Solutions**: Use the tasks in the Task Pane and/or File menu to:
  ◦ Define mApp Solution properties.
  ◦ Save and close mApp Solutions.
  ◦ View the changes the mApp Solution will make to the target system's definitions (File>mApp
    Solution Changes).
  ◦ Prepare mApp Solutions for distribution.

Related concepts
Open the mApp Editor
Create a mApp Solution
Add a Business Object to a mApp Solution
Add CSM Items to a mApp Solution
Add Security Groups and/or Roles to a mApp Solution
Edit Business Object Data in a mApp Solution

mApp Editor Menu Bar

Use the mApp Editor menu bar to access common mApp tasks.

Note: The mApp Editor menu bar is dynamic so options vary depending on what is active in the mApp Editor Main Pane (ex: When the Object Manager is active, several additional options are available on the Edit menu; when a Grid is active, **Print Grid** and **Export Grid** options are available on the File menu).

File Menu

Action	Description
Save mApp to disk	Saves changes to the active mApp Solution.
Save As	Saves the new or active mApp Solution as a named .mAppBP file.
Close mApp	Closes the mApp Solution, but not CSM Administrator. If the mApp Solution is not yet saved to a named .mAppBP file, you are prompted to name and save it. If changes are not yet saved, you are prompted to save them to the active .mAppBP file.
Scan mApp	Scans the active mApp Solution for potential errors.
Prepare mApp for Distribution	Validates the mApp Solution to ensure it is complete and ready to be distributed to potential users or to the Cherwell community.
mApp Properties	Opens the mApp Solution Properties window to define general mApp Solution properties and Features.
mApp Changes	Opens a window to view the changes that will be made to the target system's definitions.
Print Grid **Note:** Only visible when a Grid is active in the Main pane.	Prints the active Grid.
Export Grid **Note:** Only visible when a Grid is active in the Main pane.	Exports the active Grid.
Exit	Exits CSM Administrator. If you are working in a mApp Solution and have unsaved changes, CSM prompts you to save your changes.

View Menu

Selects what to display in the mApp Editor Main pane.

Action	Description
Object Manager	Opens the Object Manager Home page.
Definition Reviewer	Opens the Definition Reviewer.
Business Object	Opens the Business Object Editor so you can manage the active Business Object.
Relationship	Opens the Relationship Editor so you can manage Relationships for the active Business Object.
Form	Opens the Form Editor so you can manage forms for the active Business Object.
Grid	Opens the Grid Editor so you can manage Grids for the active Business Object.
Arrangement	Opens the Form Arrangement Editor so you can manage the Form Arrangement for the active Business Object.
Find Dependencies	Displays the active Business Object's dependencies.
Scan Results **Note:** Only visible if a mApp Solution scan returns errors that still need to be resolved.	Opens the Scan Results window.

Edit Menu

Action	Description
Cut	Moves the selected item to the clipboard. You can then paste the item into a new location.
Copy	Copies the selected item to the clipboard. You can then paste the item to a new location.
Paste	Inserts an item from the clipboard to a new location.

Managers Menu

Action	Description
Adaptive Layout Presets	Opens the Adaptive Layout Preset Manager.
Attachment Manager	Opens the Attachment Manager.

Action	Description
Automation Processes	Opens the Automation Process Manager.
Business Hours	Opens the Business Hours Manager.
Calendar Manager	Opens the Calendar Manager.
Canonical Definitions	Open the Canonical Definitions Manager.
Counters	Opens the Counter Manager.
Dashboards	Opens the Dashboard Manager, Widget Manager, Metric Manager, or Color Palette Manager.
Database Server Objects	Opens the Database Server Objects Manager.
Document Repositories	Opens Document Repository Manager.
E-mail and Event Monitoring	Opens the E-mail and Event Monitoring Manager.
Expressions	Opens the Expression Manager.
External Connections	Opens the External Connections Manager.
Formats	Opens the Stored Format Manager.
Group Maps	Opens the Group Map Manager.
HTML Page Manager	Opens the HTML Page Manager. This allows you to add an HTML page to a mApp Solution. To create/edit an internal HTML page, see Manage HTML Pages.
Images	Opens the Image Manager.
Knowledge	Opens Knowledge Mapping Manager, and Knowledge Source Manager.
Language Packs	Opens the Language Pack Manager.
Locked Strings	Opens the Locked Strings Manager.
One-Step Action	Opens the One-Step Action Manager.
Prompts	Opens the Prompts Manager.
Queues	Opens the Queue Manager.
Reports	Opens the Reports Manager.
Roles	Opens the Role Manager (available only from the mApp Editor).
Scheduled Items	Opens the Scheduled Items Manager.
Searches	Opens the Search Manager.
Security Groups	Opens the Security Group Manager (available only from the mApp Editor).
Site Manager	Opens the Portal Site Manager.
Stored Imports	Opens the Stored Imports Manager.
Stored Values	Opens the Stored Value Manager.

Action	Description
Teams	Opens the Team Manager.
Themes	Opens the Theme Manager.
Twitter Account Manager	Opens the Twitter Account Manager.
Visualizations	Opens the Visualization Manager.
Web Services	Opens the Web Services Manager.
Webhooks	Opens the Webhooks Manager.

Tools Menu

Action	Description
Directory Services	Opens the Directory Services window to configure and manage the Directory Service integrations (ex: Active Directory, LDAP, etc.).
Export Schema	Exports a mApp Solution Schema to an HTML file.
View Publish Log	Displays the Published Blueprint Log.
Options	Opens the Blueprint Options window, to define global database settings (ex: Timeout values, foreign keys, Transaction Log, Grid and Form display settings, etc.).

Help

Action	Description
mApp Help	Opens the online help.
Report Error	Opens the Report Error window so you can report an error to Cherwell.
About	Opens an About window to view version and licensing information for CSM.

mApp Solution Editor Toolbar

Use the mApp Solution Editor toolbar to quickly access common mApp Solution tasks.

Note: The mApp Solution Editor toolbar is dynamic so options vary depending on what is active in the mApp Solution Editor Main pane (example: When the Object Manager is active, create and delete options are available on the toolbar).

Tip: Many toolbar items are also available from the mApp Solution Editor menu bar and the Task Pane.

Button	Action	Description
🏠	**Home**	Opens the Object Manager Home page in the Editor Main Pane.
☰✓	**Definition Reviewer**	Opens the Definition Reviewer, enabling you to view and modify Forms, Grids, and Form Arrangements for all Business Objects.
💾	**Save**	Saves changes to the active mApp Solution.
✅	**Update**	Updates the current item.
🗑	**Abandon**	Abandons changes to the current item.
➕	**Create New**	Creates a new item.
✕	**Delete**	Deletes the current selection.
✂	**Cut**	Moves the selected item to the clipboard, so you can then paste the item into a new location.
📋	**Copy**	Copies the selected item to the clipboard, so you can then paste the item to a new location.
📋	**Paste**	Inserts an item from the clipboard to a new location.
📦	**Business Object**	Opens the Business Object Editor, where you can manage the active Business Object.
🔗	**Relationship**	Opens the Relationship Editor, where you can manage Relationships for the active Business Object.
🗔	**Form**	Opens the Form Editor, where you can manage Forms for the active Business Object.
☰	**Grid**	Opens the Grid Editor, where you can manage Grids for the active Business Object.

Button	Action	Description
📁	**Arrangement**	Opens the Form Arrangement Editor, where you can manage the Form Arrangement for the active Business Object.

Related concepts

Managing mApp Solutions

Open the mApp Editor

mApp Editor

mApp Editor Menu Bar

mApp Solution Editor Task Pane

mApp Solution Editor Task Pane

Use the mApp Solution Editor Task Pane to access mApp Solution tasks.

You can access:

- mApp Solutions: Tasks for managing mApp Solutions.
- Common Tasks: Common mApp Solution Editor tasks.
- Help: Online documentation.

  Note: Additional options and sections might appear depending on which editor is currently active.

The Task Pane is located on the left side of the mApp Solution Editor.

Behaviors include:

• Expand or collapse the pane	Hover over the line on the right side of the pane, and then click-and-drag the **Sizing Handles** ⊕.
• Collapse a section	Click the title banner of the section.
• Display an item in the Main Pane	Click a specific item. **Tip:** Hover over an item to display a tooltip.

Related concepts
Managing mApp Solutions
Open the mApp Editor
mApp Editor
mApp Editor Menu Bar
mApp Solution Editor Toolbar

Open the mApp Editor

To open the mApp Editor from the CSM Administrator main window, click the **mApps** category, and then click the **Create a New mApp** task or the **Edit an existing mApp** task.

Related concepts

Managing mApp Solutions

mApp Editor

Create a mApp Solution

Use the Create a New mApp Solution task in the CSM Administrator main window to create a mApp Solution.

When you create a mApp Solution, you:

- Define general mApp Solution properties, including name, description, display image, etc. You can also define mApp Solution Features to group subsections of definitions together.
- Add various definitions and items (Business Objects, CSM Items, and Business Object data) to the mApp Solution and specify how they will be merged into the target system.

To create a mApp Solution:

1. In the CSM Administrator main window, click the **mApps** category, and then click the **Create a New mApp** task.

   A mApp Solution is created, and its interface, the mApp Solution Editor, opens. By default, the Object Manager is displayed in the mApp Editor's Main pane. The mApp Solution is unnamed (called New mApp*) until saved to a named mApp Solution Blueprint file (.mAppBP).

2. Define mApp Solution properties.

3. Save the mApp Solution to a named .mAppBP file (**File>Save As**).

4. Add definitions and items to the mApp Solution:
   - Use the Add Business Object to mApp Solution Wizard to walk through the process of adding Business Objects and their associated Fields, Relationships, Forms, Grids, and Form Arrangements.

   - Use the mApp Solution Options button ![icon] (or right-click **item>Add to mApp**) in CSM Item Managers to add CSM Items (example: One-Step Actions, Dashboards, Saved Searches, etc.).

   - Use the Edit Data task within a mApp Solution to manage (add, edit, delete) data in a Supporting Object or Lookup Object (only available if *Show in Table Management* is checked in the Business Object's properties).

   - Use the Security Group Manager and the Role Manager to add predefined Security Groups and/or Roles.

5. Save changes to the named open mApp Solution (click the **Save** button ![icon]). You can also view the changes that will be made to the target system's definitions.

   Tip: Periodically scan your mApp Solution to find potential errors.

   When ready, you can prepare the mApp Solution for distribution, and then distribute the file directly to potential Users, or submit it to the mApp Solution Exchange. System administrators apply the mApp Solution to CSM systems using the Apply mApp Wizard.

Related concepts

Define mApp Solution Properties

Add a Business Object to a mApp Solution

Add CSM Items to a mApp Solution

Add Security Groups and/or Roles to a mApp Solution

Edit Business Object Data in a mApp Solution

Set a Designer ID

Use the Set Designer ID task on the mApp Solutions page in CSM Administrator to save a unique Designer ID to your current user information. Setting a Designer ID uniquely identifies the definitions you add to a mApp Solution and tracks them in history records.

Good to know:

- Setting a Designer ID is optional. If you do not have a Designer ID, no history records are created for definitions you add to a mApp® Solution.
- Each definition can have a maximum of 20 history records. When new history records exceed this limit, the oldest records are deleted.
- Each history record contains the Designer ID, date/time the definition was saved, and the mApp Solution name.
- If a mApp Solution creator modifies or adds a definition that has a most recent history record with the same Designer ID, only the date/time is updated (a new record is not added).

  Note: New Designer IDs cannot be created at this time.

To set a Designer ID in CSM Administrator:

1. In the CSM Administrator main window, select the **mApps** category, and then select the **Set Designer ID** task.

2. Enter your Designer ID.

3. Select **OK**.

Related concepts
About mApp Solutions
Go to the Cherwell Marketplace (formerly the mApp Exchange)

Define mApp Solution Properties

Use the **mApp Solution properties** window, accessed from within the mApp Editor, to define mApp Solution properties.

- General properties:
  - **Name and description:** Specific name and description for the mApp Solution.
  - (Optional) **Image:** Image to represent the mApp Solution.
  - **Created by:** Name of mApp Solution creator (individual or organization).
  - (Optional) **Details URL:** Site that contains detailed information about the mApp Solution.
  - (Optional) **Prevent mApp customizations during install:** Removes the option to ignore parts of a mApp Solution during an upgrade.
  - (Optional) **Protect mApp content on publishing:** Helps to achieve mApp Solution upgradability by preventing editing or deletion of content.
- (Optional) Features: Definitions grouped together into subsections of functionality.

Good to know:

- When system administrators apply a mApp Solution to a CSM system, the general properties are displayed in the Apply mApp Wizard. When users view the mApp Solutions that have been installed in their systems, the general properties are shown in the Installed mApp Solutions window.
- You must define at least the general properties in order for the mApp Solution to be considered ready for distribution.
- If you have Globalization and multiple cultures enabled for your system and translations that impact your mApp Solution have been applied, you must define mApp Solution properties for each culture. For more information, see Applying Cultures to mApps.
- Business Object and CSM Item definitions can be grouped together into Features (subsections of functionality) using mApp Solution conditions. Features can then be applied (or not) as a whole in the Apply mApp Wizard.

To define mApp Solution properties:

1. Open the mApp Editor.
2. From the mApp Editor menu bar, select **File > mApp Properties**.
3. Select the **General Properties** page.
4. Define general properties for the mApp Solution:
   - **Name:** Provide a display name to use for the mApp Solution.
   - **Description:** Provide a description of the mApp Solution. This should be as detailed as possible, as it is displayed in the Apply mApp Wizard.
   - **Image:** Select an image to associate with the mApp Solution.
     - **None:** Select this radio button to not associate an image with the mApp Solution.

- **File:** Select this radio button to use an image for the mApp Solution. Then, select the

  ellipses [ ] to browse to the location of the image file, select the file, and select **Open**.

  - **Created by:** Provide the name of the organization or individual who created the mApp Solution.

  - **Details URL:** If detailed information about the mApp Solution is available on a website,

    provide the URL here. Then, select the ellipses [ ] to navigate to the site and ensure that the URL is correct.

  - **Advanced Options:**
    - **Prevent mApp customizations during install:** As a mApp Solution author, select this check box to remove the **Don't Change** option when a mApp Solution is applied during an upgrade. This means that the mApp Solution is applied in its entirety during an upgrade, lessening the possibility of a mApp Solution failure with customized content.

    - **Protect mApp content on publishing:** Select this check box to protect the contents of your mApp Solution. This helps to achieve upgradability by preventing the editing or deletion of content after the Protected mApp Solution has been applied. If you select this check box, the **Prevent mApp customizations during install** check box is automatically selected.

5. Select the **Features** page.

6. (Optional) Define mApp Solution Features:
   a. Select **Add** to add a new Feature.

   b. Define general properties for the Feature:
      - **Name:** Provide a name for the Feature.

      - **Description:** Provide a description of the Feature. This is the text that explains the Feature to the administrator applying the mApp Solution to his system, so ensure that the description is clear.

      - **This feature is enabled by default:** Select this check box to include the mApp Solution feature by default when the mApp Solution is applied to a CSM system using the Apply mApp Wizard.

   c. Select **OK**.

7. Select the **One-Step** page.

8. (Optional) **Run a One-Step Action**:
   - **One-Step:** Select a recently used One-Step Action from the drop-down list or select the ellipses to edit it or to select a different one.

   - **Description:** Provide a **description** of the One-Step Action. This should be as detailed as possible, as it is displayed in the Apply mApp Wizard and explains what the One-Step Action does. If the One-Step Action already has a description, it is pre-populated.

   Note: This option is not available using the CSM Configuration command-line.

The Action must be an unassociated One-Step Action (not tied to a particular Business Object).

9. Select **OK**.

10. Prepare the mApp Solution for Distribution (**File > Prepare mApp Solution for Distribution**), or save the mApp Solution (**File > Save to mApp Solution to Disk**) to continue making other changes.

Related concepts

mApp Editor

Open the mApp Editor

Apply a mApp Solution

Prepare a mApp Solution for Distribution

Protected mApp™ Solutions

Protected mApp™ Solution FAQs

Add a Business Object to a mApp Solution

The Add Business Object to mApp Solution wizard (accessed from within the mApp Editor) is a specialized tool that adds Business Objects and their associated Fields, Relationships, Forms, Grids, and Form Arrangements to a mApp Solution.

Use the Add Business Object to mApp Solution Wizard to select which Business Object to add to the mApp Solution and define its importance to the mApp Solution. Then, define how the Business Object is imported into the target system when the mApp Solution is applied:

- **Overwrite All:** Overwrites the existing definitions in the target system, or adds them if they are not already there.
- **Overwrite defaults only** (applies to Forms and Grids): Overwrites the existing defaults in the target system.
- **Do not overwrite any:** Leaves the definitions in the target system unchanged (does not overwrite or add the definition).
- **Let me choose:** Allows you to select which items or areas (example: Specific Fields) to merge. Selected items are overwritten if they exist in the target system, and added if they are not. The items you do not select are left unchanged in the target system.

> **Tip:** When you select **Let me choose**, you can select **Uncheck All** to clear everything in the list (example: Clear all Fields) or **Select All** to select everything in the list.

> **Important:** If you apply a mApp Solution containing a newly converted Group Business Object(s), then we strongly recommend that you use overwrite instead of merge options in the Add Business Object to mApp Wizard. If you use merge options with Group Objects, this can result in Blueprint scan errors or unexpected results appearing after the mApp Solution has been applied.

To add a Business Object to a mApp Solution:

1. Open the mApp Editor.
2. Select a Business Object in the Object tree, and then select the **Add Business Object to mApp Wizard** task in the Structure area.
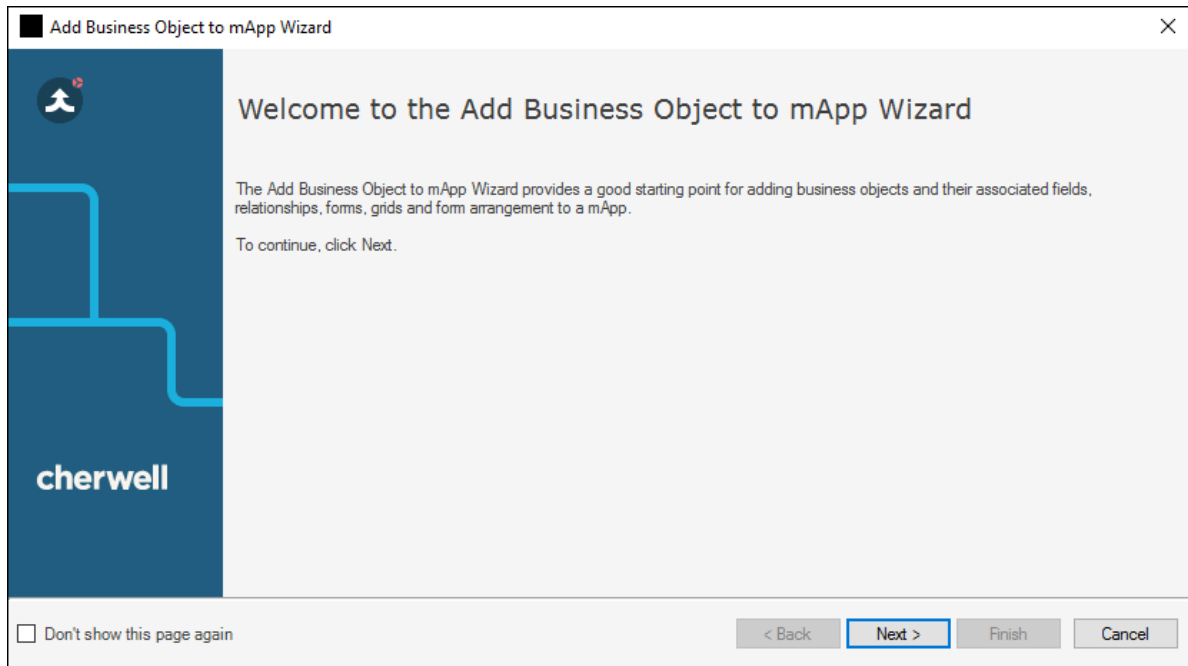
Tip: You can also open the wizard from the Business Object Editor within a mApp Solution, either by selecting **Add to mApp** or the **Add to mApp Wizard** link in the Business Object section of the mApp Solution Editor Task Pane.

3. Select a Business Object to include in the mApp Solution, and then specify its importance to the mApp Solution:

   a. In the drop-down list, select a Business Object. The Business Object you selected in the Object Manager is automatically selected.

      Note: If you add a Group Member, the Group Leader is automatically added to the mApp Solution for reference.

      Tip: The drop-down list displays only Major Business Objects. To display all Business Objects, select the **Show All** check box.

   b. Define the importance of the Business Object to the mApp Solution. This marks the items in the mApp Solution file according to importance so that when a mApp Solution is applied, the most important items are asked about first.

      Note: Because Group Leaders have common items that are shared by all Group Members, Group Objects are always applied first (Group Leader followed by Group Members), regardless of the importance selected here.

      ◦ **High Importance:** Select this radio button if the Business Object is one of the main Business Objects in the mApp Solution.

- ◦ (Default) **Medium Importance:** Select this radio button if the Business Object is a supporting object for the mApp Solution.

- ◦ **Low Importance:** Select this radio button if the Business Object is not critical for the mApp Solution.

> **Tip:** You can select **Finish** on this page or any subsequent pages to accept the default selections for the remaining pages and complete the wizard.

4. Select the Business Object Fields to overwrite in the target system:
   - ◦ (Default) **Overwrite all Fields:** Select this radio button to overwrite all existing Fields in the target system.

   - ◦ **Do not overwrite any Fields:** Select this radio button to make no changes to any of the existing Fields in the target system.

   - ◦ **Let me choose:** Select this radio button to select specific Fields to overwrite.

> **Note:** If you select an option other than **Overwrite all Fields**, the Business Object is added to the mApp Solution as **Merge**. This is because Fields are part of Business Objects, and the Business Object must be set to **Merge** if you do not want all of its Fields to be overwritten. If the Business Object is set to **Overwrite**, all Fields will be overwritten. For more information, see Configure Merge Actions for Business Object Definitions.

5. Select which Relationships to overwrite in the target system:
   - ◦ (Default) **Overwrite all Relationships:** Select this radio button to overwrite all existing Relationships in the target system.

   - ◦ **Do not overwrite any Relationships:** Select this radio button to make no changes to any of the existing Relationships in the target system.

   - ◦ **Let me choose:** Select this radio button to select specific Relationships to overwrite.

6. Select which Business Object Forms to overwrite in the target system:
   - ◦ (Default) **Overwrite default Forms only:** Select this radio button to overwrite the default Forms in the target system. This includes the primary Form for the object, along with the summary and mini-summary Forms.

   - ◦ **Overwrite all Forms:** Select this radio button to overwrite all Forms (default and other) in the target system.

   - ◦ **Do not overwrite any Forms:** Select this radio button to make no changes to any of the Forms in the target system.

   - ◦ **Let me choose:** Select this radio button to select specific Forms to overwrite.

7. Select which Grids to overwrite in the target system:
   - ◦ (Default) **Overwrite Default Grids Only:** Select this radio button to overwrite the default Grid for the Business Object in the target system.

   - ◦ **Overwrite all Grids:** Select this radio button to overwrite all Grids (default and other) in the target system.

- **Do not overwrite any Grids:** Select this radio button to make no changes to any of the Grids in the target system.

- **Let me choose:** Select this radio button to select specific Grids to overwrite.

8. Select whether to overwrite the Form Arrangement (Major Business Objects only):
   - **Overwrite Form Arrangement:** Select this radio button to overwrite the Form Arrangement in the target system.

   - **Do not overwrite Form Arrangement:** Select this radio button to make no changes to the Form Arrangement in the target system.

9. Select which Tabs in the Form Arrangement to overwrite:

   Note: This page is displayed only if you are adding a Major Business Object to the mApp Solution, and if you selected to overwrite the Form Arrangement on the previous page.

   - **Overwrite all Tabs:** Select this radio button to overwrite all Tabs in the target system.

   - **Do not overwrite any Tabs:** Select this radio button to make no changes to the Tabs in the target system.

   - **Let me choose:** Select this radio button to select specific Tabs to overwrite.

      Note: If a Tab is included in a mApp Solution, but the associated Relationship is not added by the mApp Solution and does not already exist in the target system, the Tab will not be displayed in the target system.

10. Define whether to overwrite Approvals:

    Note: This page is displayed only for Major Business Objects that have Approvals defined.

    - **Overwrite Approvals:** Select this radio button to overwrite Approvals in the target system.

    - **Do not overwrite Approvals:** Select this radio button to make no changes to Approvals in the target system.

11. Define whether to overwrite Business Object Action areas:

    Note: This page is displayed only for Major Business Objects that have Actions defined.

    - **Overwrite all Actions:** Select this radio button to overwrite all Business Object Action areas in the target system.

    - **Do not overwrite any Actions:** Select this radio button to make no changes to the Business Object Action areas in the target system.

    - **Let me choose:** Select this radio button to select specific Business Object Action areas to overwrite.

       Note: Actions are categorized by areas (Menu, Task Pane, toolbar, Context Menu, and Automatic Actions). When you select one of the above options from the wizard, you are defining what to do with an entire area. However, you can define separate options

for individual Actions within an area if you use the Business Object Actions window to configure merge actions for Business Object Actions.

12. Review the summary page.

13. Select **Finish**.

The Business Object and its associated Fields, Relationships, Forms, Grids, and Form Arrangements are added to the mApp Solution. When the mApp Solution is applied, these definitions are imported into a target system according to the selections you made.

14. (Optional) Add additional Business Objects or CSM Items to the mApp Solution.

15. (Optional) Select **Options** in the various properties windows of the mApp Solution to configure merge actions for Business Object definitions.

16. Prepare the mApp Solution for Distribution **(File > Prepare mApp Solution for distribution)**, or save the mApp Solution**(File > Save mApp Solution to Disk)** to continue making other changes.

Related concepts
mApp Editor
Open the mApp Editor

Apply a mApp Solution

About Business Objects

Add a Business Object to a Protected mApp™ Solution

The Add Business Object to mApp Solution wizard (accessed from within the mApp Editor) is a specialized tool that adds Business Objects and their associated Fields, Relationships, Forms, Grids, and Form Arrangements to a mApp Solution.

Use the Add Business Object to mApp Solution Wizard to select which Business Object to add to the Protected mApp Solution and define its importance to the Protected mApp Solution.

For a full explanation of the Wizard, see: Add a Business Object to a mApp Solution in conjunction with this help topic.

For help on how a Protected mApp Solution differs from any other mApp Solution , see: Protected mApp™ Solutions.

To add a Business Object to a Protected mApp Solution:

1. Open the mApp Editor.
2. Select a Business Object in the Object tree, and then select the **Add Business Object to mApp Wizard** task in the Structure area.
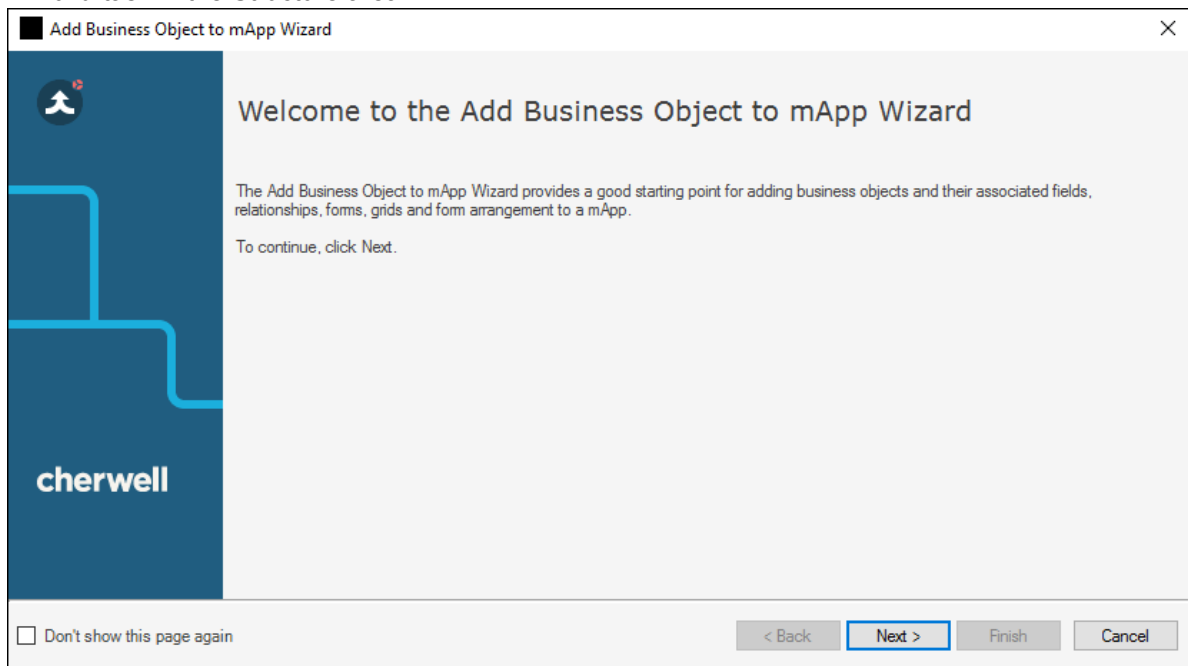
3. Select a Business Object to include in the Protected mApp Solution, and then specify its importance to the mApp Solution:
   a. In the drop-down list, select a Business Object.
   b. Define the importance of the Business Object to the Protected mApp Solution. See: Add a Business Object to a mApp Solution.

4. Select the Business Object Fields to merge in the target system:
   ◦ (Default) **Merge all fields:** Select this radio button to merge fields from the Protected mApp Solution with all existing fields in the target system.

      If field A (from the Protected mApp Solution) is merged with field B (in the target system), this results in fields A and B in your system after the merge.

      If field A (from the Protected mApp Solution) is merged with an identical field A (in the target system) from a previous mApp Solution, this results in an *upgraded* field A with the protected properties from the mApp Solution and the customized properties from the target system.

      If field A (from the Protected mApp Solution) and field B (in the target system) have the same field name, the field in your target system will be renamed with an underscore (_) prefix.

      > **Tip:** Automatic renaming of duplicate names with an underscore (_) also applies to Item Managers, forms, relationships and other Business Object Definitions.

   ◦ **Do not merge any fields:** Select this radio button to make no changes to any of the existing fields in the target system.
   ◦ **Let me choose:** Select this radio button to select specific fields to overwrite.

5. Select which Relationships to merge in the target system:
   ◦ (Default) **Merge all relationships:** Select this radio button to merge relationships from the Protected mApp Solution with all existing relationships in the target system. See point 4 for a description of merging behavior.
   ◦ **Do not merge any relationships:** Select this radio button to make no changes to any of the existing relationships in the target system.
   ◦ **Let me choose:** Select this radio button to select specific relationships to overwrite.

6. Select which Business Object Forms to overwrite in the target system. See: Add a Business Object to a mApp Solution

7. Select which grids to overwrite or merge in the target system:
   ◦ (Default) **Overwrite default grid only:** Select this radio button to overwrite the default grid for the Business Object in the target system.
   ◦ **Merge all grids:** Select this radio button to merge the columns from all grids (default and other) into the target system.
   ◦ **Do not merge any grids:** Select this radio button to make no changes to any of the grids in the target system.
   ◦ **Let me choose:** Select this radio button to select specific grids to overwrite.

8. Select whether to overwrite the form arrangement (Major Business Objects only). See: Add a Business Object to a mApp Solution

9. Select which Form Arrangement Tabs to merge:

   > **Note:** Note: This page is displayed only if you are adding a Major Business Object to the mApp Solution, and if you selected to overwrite the form arrangement on the previous page.

- **Merge all form arrangement tabs:** Select this radio button to merge all Form Arrangement Tabs from the Protected mApp Solution with all existing all Form Arrangement Tabs in the target system.

- **Do not merge any form arrangement tabs:** Select this radio button to make no changes to the tabs in the target system.

- **Let me choose:** Select this radio button to select specific tabs to overwrite.

    Note: If a tab is included in a Protected mApp Solution, but the associated relationship is not added by the Protected mApp Solution and does not already exist in the target system, the tab will not be displayed in the target system.

10. Define whether to overwrite approvals. See: Add a Business Object to a mApp Solution

11. Define whether to merge Business Object Action areas:

    Note: This page is displayed only for Major Business Objects that have Actions defined.

    - **Merge all actions:** Select this radio button to merge all Business Object Action areas from the Protected mApp Solution with all existing all Business Object Action areas in the target system.

    - **Do not merge any actions:** Select this radio button to make no changes to the Business Object Action areas in the target system.

    - **Let me choose:** Select this radio button to select specific Business Object Action areas to overwrite.

        Note: Note: Actions are categorized by areas (menu, task pane, toolbar, context menu, and Automatic Actions). When you select one of the above options from the wizard, you are defining what to do with an entire area. However, you can define separate options for individual Actions within an area if you use the Business Object Actions window to configure merge actions for Business Object Actions.

12. Review the summary page.

13. Select **Finish**.

   The Business Object and its associated fields, relationships, forms, grids, and form arrangements are added to the Protected mApp Solution. When the Protected mApp Solution is applied, these definitions are imported into a target system according to the selections you made.

14. Prepare the Protected mApp Solution for distribution **(File > Prepare mApp Solution for distribution)**, or save the Protected mApp Solution **(File > Save mApp Solution to Disk)** to continue making other changes.

Related concepts

Protected mApp™ Solutions

Protected mApp™ Solution FAQs

Add CSM Items to a mApp Solution

Use the mApp Solution Options button [icon] in CSM Item Managers to include CSM Items (example: Automation Processes, One-Step Actions, Dashboards, Saved Searches, etc.) in a mApp Solution.

Good to know:

- Click the References button to see which definitions throughout CSM are being used by the definitions in a mApp Solution. This allows you to ensure that all necessary definitions are included in the mApp Solution.

  > **Note:** Dashboards are currently the only CSM Items that automatically prompt you to add associated items (Widgets) when you include them in a mApp Solution.

- You can define some additional options when adding Stored Values and external connections to a mApp Solution. For more information, see Add a Stored Value or External Connection to a mApp Solution.

To add a CSM Item to a mApp Solution:

1. Open the mApp Editor.

2. From the menu bar, click **Managers**, and then click a CSM Item Manager.

3. Select an item in the Manager, and then click the **mApp Options** button [icon].

   > **Tip:** You can also **right-click** an item, and then click **Add to mApp** in the context menu. You can then click the **mApp Options** button [icon] to set import options.

4. Select the **Include in mApp Solution** check box.

5. Define options for how to import the item into a target system (Options area):
   - **Import to target system**: Select this radio button to import the item definition into the target system. Then, select a merge action based on whether the definition is already present in the target system.

     If already present: In the drop-down, select a merge action to define how the definition is imported if it already exists in a target system:

       - **Overwrite**: Select this option to have the mApp Solution definition overwrite the existing definition in the target system.
       - **Don't Import**: Select this option to leave the existing definition in the target system unchanged (the mApp Solution definition is not imported into the target system when the mApp Solution is applied).

     If not present: In the drop-down, select a merge action to define whether the definition is imported if it does not currently exist in the target system:

- ◦ **Import**: Select this option to import the mApp Solution definition into the target system if does not already exist.

  - ◦ **Don't Import**: Select this option to skip importing the mApp Solution definition into the target system if it does not already exist (the mApp Solution definition will not be added to the target system).

- ◦ **Remove from Target System**: Select this radio button to have the mApp Solution remove the item definition from the target system when it is applied.

- ◦ **For Reference Only**: Select this radio button to include the item definition in the mApp Solution for reference. When the mApp Solution is applied, the item definition will not be merged into the target system; it exists in the mApp Solution for informational purposes only. You should rarely (if ever) need to do this manually, as the system automatically adds definitions as necessary for reference only.

6. Select the **Import based on Condition** check box to have the mApp Solution import the item definition based on conditions. Then, click the **Ellipses** button to open the mApp Solution Conditions window and configure conditions.

7. Select **OK**.

8. Prepare the mApp Solution for Distribution (File>Prepare mApp for distribution), or save the mApp Solution (File>Save mApp to Disk) to continue making other changes.

Related concepts

Create a mApp Solution

Open the mApp Editor

View Referenced Definitions in a mApp Solution

Configure mApp Solution Conditions

Prepare a mApp Solution for Distribution

Add a Stored Value or External Connection to a mApp Solution

Use the mApp Solution Options button ![icon] in the Stored Value Manager or the External Connection Manager to include Stored Values and/or external connections in a mApp Solution and define how they are imported into a target system when the mApp Solution is applied:

- **Import to target system:** Imports the item definition into the target system. You can select merge actions based on whether the item definition already exists in the target system.
- **Remove from target system:** Removes the item definition from the target system.
- **For Reference Only:** Includes the item definition in the mApp Solution for informational purposes only (it is not merged into the target system when the mApp Solution is applied).
- **Import/remove based on condition:** Imports or removes the item definition based on configured mApp Solution conditions.
- **Prompt for values:** Includes a prompt in the Apply mApp Wizard to allow Users to specify their own values for a Stored Value, or external connection information for an external database.
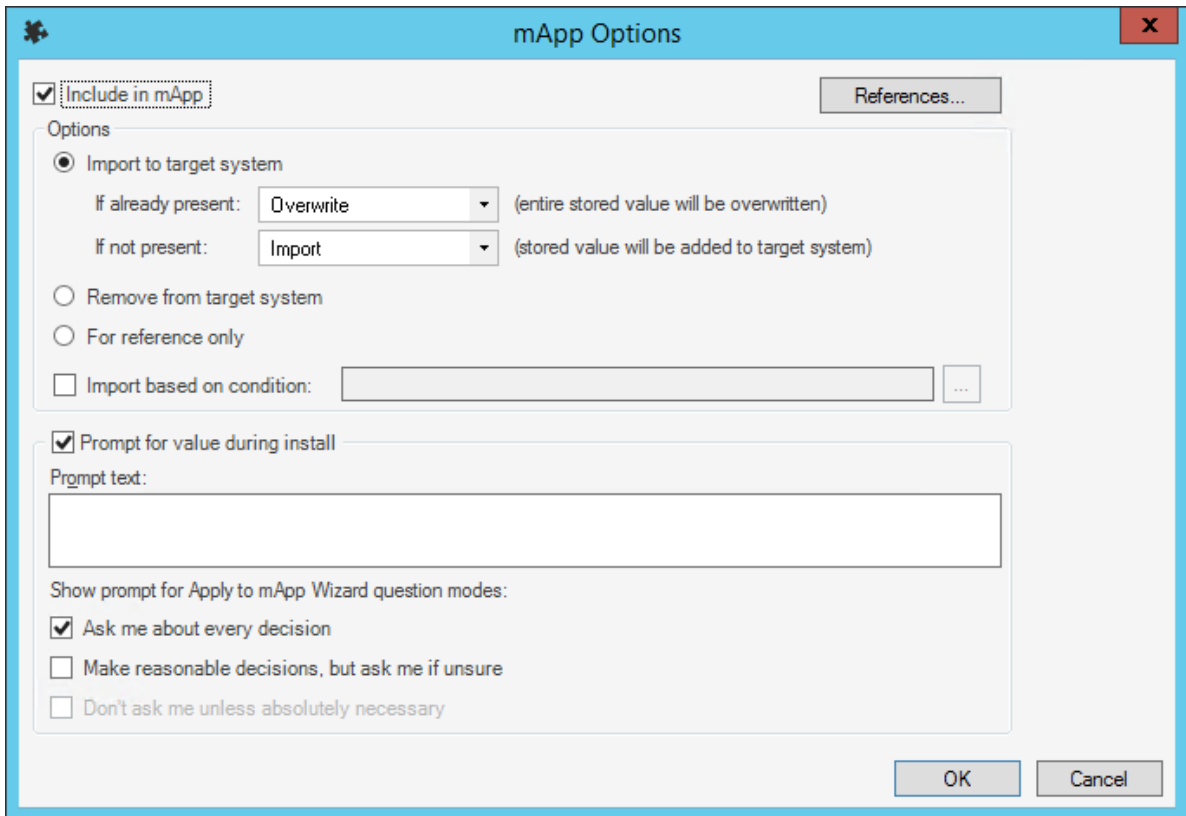
Good to know:

- Click the References button to see which definitions throughout CSM are being used by the definitions in a mApp Solution. This allows you to ensure that all necessary definitions are included in the mApp Solution.
- This procedure assumes that the Stored Values and/or external connections being added to a mApp Solution already exist. For more information about creating Stored Values or external connections, refer to Create a Stored Value or Create an External Connection to an External Database

To add a Stored Value or external connection to a mApp Solution:

1. Open the mApp Editor.
2. Open the Stored Value Manager.
3. Select a **Stored Value** or **external connection**, and then click the **mApp Options** button ![icon] .

   Tip: You can also **right-click** an item, and then click **Add to mApp**.

4. Define general options for the item:
   ◦ Include in mApp Solution: Select this check box to include the item in the mApp Solution.

   ◦ References: Click this button to view which other definitions in the system are being used by the selected item.

5. Define options for how the item will be imported into a target system (Options area):

   Note: These options are only available if *Include in mApp Solution* is selected.

   ◦ Import to target system: Select this radio button to import the item definition into the target system. Then, select a merge action based on whether or not the definition is already present in the target system.

   If already present: In the drop-down, select a merge action to define how the definition is imported if it already exists in a target system:

   ◦ Overwrite: Select this option to have the mApp Solution definition overwrite the existing definition in the target system.

   ◦ Don't Import: Select this option to leave the existing definition in the target system unchanged (the mApp Solution definition is not imported into the target system when the mApp Solution is applied).

If not present: In the drop-down, select a merge action to define whether the definition is imported if it does not currently exist in the target system:

- ◦ Import: Select this option to import the mApp Solution definition into the target system if does not already exist.

- ◦ Don't Import: Select this option to skip importing the mApp Solution definition into the target system if it does not already exist (the mApp Solution definition will not be added to the target system).

- ◦ Remove from Target System: Select this radio button to have the mApp Solution remove the item definition from the target system when it is applied.

- ◦ For Reference Only: Select this radio button to include the item definition in the mApp Solution for reference. When the mApp Solution is applied, the item definition will not be merged into the target system; it exists in the mApp Solution for informational purposes only.

  Note: You should rarely (if ever) need to do this manually, as the system automatically adds definitions as necessary for reference only.

- ◦ Import/remove based on Condition: Select this check box to have the mApp Solution import or remove the item definition based on conditions. Then, click the **Ellipses** button ⬚ to open the mApp Solution Conditions window and configure conditions.

6. Define prompting options:
   - ◦ Prompt for value during install: Select this check box to prompt Users to provide a value for the Stored Value or to edit external connection information when they run the Apply mApp Wizard.

   - ◦ Prompt text: Provide the **text** to display in the Prompt window when it pops up to prompt the User for a value.

   - ◦ Show prompt for Apply mApp Solution Wizard question modes: Select the interaction level(s) at which the prompt is displayed in the Apply mApp Solution Wizard:
     - ◦ Ask me about every decision (default): Select this check box to prompt the User in the Apply mApp Solution Wizard if a high level of interaction is selected (*Ask me about every decision* is selected on the User Interaction page of the Apply mApp Solution Wizard).

     - ◦ Make reasonable decisions, but ask me if unsure: Select this check box to prompt the User in the Apply mApp Solution Wizard if a medium level of interaction is selected (*Make reasonable decisions, but ask me if unsure* is selected on the User Interaction page of the Apply mApp Solution Wizard).

     - ◦ Don't ask me unless absolutely necessary: Select this check box to prompt the User in the Apply mApp Solution Wizard if a low level of interaction is selected (*Don't ask me unless absolutely necessary* is selected on the User Interaction page of the Apply mApp Solution Wizard).

       Note: This option is only available if you also selected to make the prompt available at the medium interaction level (*Make reasonable decisions, but ask me if unsure*).

7. Select **OK**.

8. Prepare the mApp Solution for Distribution (File>Prepare mApp for distribution), or save the mApp Solution (File>Save mApp to Disk) to continue making other changes.

Edit Business Object Data in a mApp Solution

The Data Editor is the interface within the Blueprint Editor or mApp Editor that allows you to edit data within a Supporting Business Object or Lookup Business Object. Use the Data Editor to:

- Add records (rows) with new data.
- Delete existing records.
- Update the data in a record.
- Clear all data from the table and replace it with new/updated data.

There are several ways to open the Data Editor.

To open the Data Editor:

1. The Data Editor can be opened several ways in CSM Administrator:
   - In the CSM Administrator Main Pane, click the **Settings** category, and then click the **Table Management** task**.**
   - In a Blueprint or mApp Solution, select a Supporting Object or Lookup Object (example: Incident Category Lookup Object) from the Object tree in the Object Manager, and then click the **Edit Data** task in the Structure area.
   - In the Validation/Auto-Populate page of the Field Properties window, when you select to validate a Field from a table, click the **Edit Table Data** button (activated after selecting a table in the drop-down).

1. Menu bar: Displays a row of drop-down menus available in the Data Editor.

2. Toolbar: Displays a row of buttons for operations available in the Data Editor.

3. Main Pane: Displays either the list of records in the data table (as a Grid), or the details for the currently selected record (depending on the view you are in). The Action column shows what will be done with the data in each row of the table when the mApp Solution or Blueprint is applied/published.

> **Note:** Select the **Clear all data from destination table** check box to have all existing data in the current system Lookup Object cleared out when the mApp Solution or Blueprint is applied/published. If you want to keep any existing data, you must select the rows with the data you want to keep and click the **Include in mApp** or **Blueprint** button ⬇.

Good to know:

- The objects for which you are editing data are automatically added to the mApp Solution *For Reference Only* if they are not already in the mApp Solution.

- Because data is edited within a Blueprint or a mApp Solution, the data in your system is not actually modified until the Blueprint is published or the mApp Solution is applied.
- Business Object Data is limited to 1,000 records. You will receive a warning if you exceed that limit.

Add Security Groups and/or Roles to a mApp Solution

Use the mApp Solution Options button ![icon] in the Security Group Manager or Role Manager to include pre-defined Security Groups or Roles in a mApp Solution.

You can also define how Security Groups and/or Roles are imported into a target system when the mApp Solution is applied.

Good to Know:

- Security Groups and/or Roles may impact security rights in the target database after the mApp Solution is applied. Be sure to carefully review the merge actions and target items for Security Groups and Roles when you apply the mApp Solution. To ensure that you understand the implications of applying security changes included in the mApp Solution, we strongly advise you to apply the mApp Solution to a test environment and verify the security changes before you commit the mApp Solution to a production environment.
- You cannot modify Security Groups or Roles in a mApp Solution.
- Users assigned to a Security Group are not added to the mApp Solution. You must manually add Users to the Security Group after you apply the mApp Solution to the target system.
- The following attributes are included with Role definitions:
  ◦ Role Name
  ◦ Primary Object
  ◦ Description
  ◦ Culture
  ◦ Role Image

  If you do not choose to include Roles associated with Security Groups when you add Security Groups, you must manually add Roles to Security Groups in the target system.

To add a Security Group and/or Role to a mApp Solution:

1. Open the mApp Editor.
2. From the menu bar, click **Managers**, and then click **Security Groups** or **Roles**.
3. Select an item, and then click the **mApp Options** button ![icon].

   > **Tip:** You can also **right-click** a Security Group or Role, and then click **Add to mApp** in the context menu. You can then click the **mApp Options** button ![icon] to set import options.

4. Select the **Include in mApp Solution** check box.
5. If you are adding a Security Group, you are given the option to add Roles associated with the Security Group at the same time. You can:

- Click **Yes** to add associated Roles.

- Click **No** to add the Security Group without its associated Roles.

6. Select the **Import to target system** option to import the Security Group and/or Role into the target system, and then select import options:

   - **If already present**: Select an action to define how the definition is imported if it already exists in a target system:

     - **Overwrite**: Select this option to have the mApp Solution definition overwrite the existing Security Group and/or Roles in the target system.

     - **Don't Import**: Select this option to leave existing Security Group and/or Roles in the target system unchanged.

   - **If not present**: Select an action to define whether the definition is imported if it does not currently exist in the target system:
     - **Import**: Select this option to import the Security Group and/or Roles into the target system if they do not already exist.

     - **Don't Import**: Select this option to skip importing the Security Group and/or Roles into the target system if it they do not already exist..

7. Select the **Import based on Condition** check box to import the Security Group and/or Roles based

   on conditions. Then, click the **Ellipses** button [...] to open the mApp Solution Conditions window and configure conditions.

8. Click **OK**.

9. Prepare the mApp Solution for Distribution (File>Prepare mApp for distribution), or save the mApp Solution (File>Save mApp to Disk) to continue making other changes.

Related concepts

Create a mApp Solution

About Security Groups

About Roles

Configure mApp Solution Conditions

Prepare a mApp Solution for Distribution

Configure mApp Solution Conditions

Use the mApp Conditions window to configure conditions that control which definitions in a mApp Solution are imported into a target system.

When you configure conditions for a mApp Solution definition, you create a list of system definitions or Features (defined in mApp Properties). A mApp Solution definition is only imported into a target system if the definition listed in the condition is imported/overwritten, or if the Feature it belongs to is imported.

You can configure conditions for:

- Business Objects/Fields, Forms, Grids, Relationships, Form Arrangements
- CSM Items (Automation Processes, One-Step Actions, Dashboards, Saved Searches, etc.)
- Security Groups and Roles

Good to know:

- If you add definitions to a mApp Solution using the References window, a condition is automatically set up to only import the definition into a target system if the item using it is also imported (or already exists in the target system).

To configure mApp Solution Conditions:

1. Use one of these methods to open the mApp Conditions window:

   ◦ Select the **Import Based on Condition** check box, and then click the **Ellipses** button [ ] in the following areas:
       ◦ Business Object Properties window

       ◦ Relationship Properties window

       ◦ Field Properties window

       Note: Business Objects and Fields can only have conditions based on Features. Other items can have conditions based on other definitions being imported.

   ◦ Select the **Import Based on Condition** check box, and then click the **Ellipses** button [ ] in the mApp Options window in the following areas:
       ◦ Form Editor

       ◦ Grid Editor

       ◦ Form Arrangement Editor

       ◦ Security Groups and Roles

       ◦ CSM Item Managers
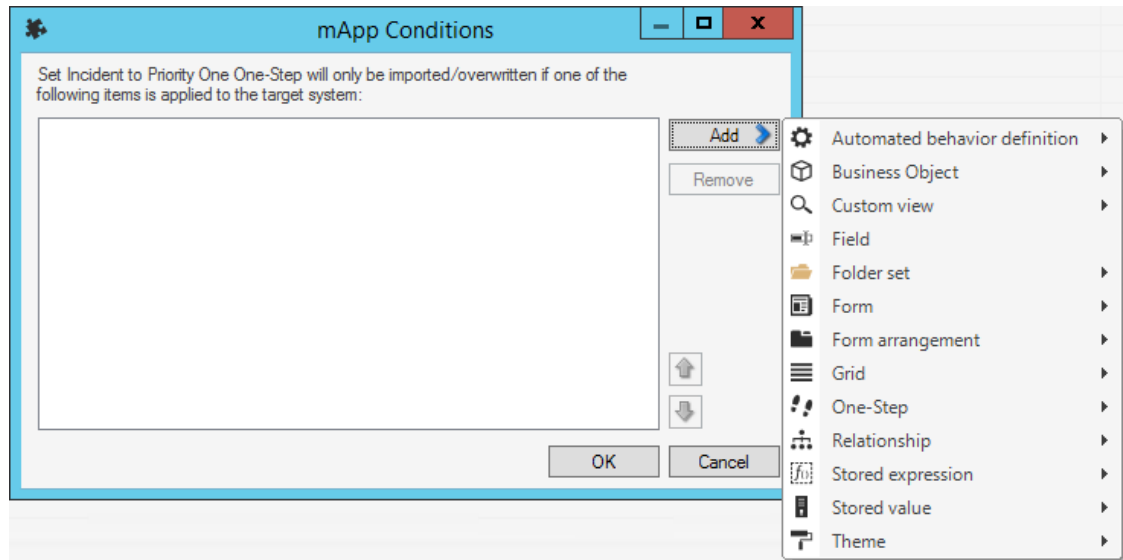
2. Add a definition to the list of conditions:

   a. Click **Add** to open a menu of definitions organized by type (example: Business Object). The list shows all definitions included in the mApp Solution, along with all defined Features (except when adding conditions for Fields and Business Objects, which can only have conditions based on Features).

   b. Hover over a category to open a menu of specific definitions.

   c. Select a definition to add it to the list.

3. Add additional definitions to the list as necessary.

   > **Tip:** Click **Remove** to remove a selected definition from the list. Use the **Up/Down** arrow to change the order of the selected definitions.

4. Select **OK**.

Related concepts
Define mApp Solution Properties

Open an Existing mApp Solution

Use the Edit tasks (accessed from the CSM Administrator main window) to open an existing mApp Solution and edit it.

To open an existing mApp Solution:

1. In the CSM Administrator main window, click the **mApps** category, and then click the **Edit an Existing mApp** task.

   Tip: The last saved mApp Solution is also listed for your convenience. Click it to open it directly in the mApp Editor, and then make edits.

2. Select a .mAppBP file, and then click **Open**.

   The mApp Solution opens in the mApp Editor. The name of the mApp Solution is displayed at the top of the CSM Administrator window and at the top the mApp Editor.

Save a mApp Solution

An open (working) mApp Solution is saved to a .mAppBP file. When the mApp Solution is prepared for distribution, it is saved as a .mApp Solution file (extension required for a mApp Solution to be applied to a target system).

There are two save options for a mApp Solution:

- Save As: Saves a mApp Solution as a named mApp Solution Blueprint (.mApp SolutionBP) file.
- Save to disk: Saves changes to the open mApp Solution (.mAppBP) file.

To save a mApp Solution as a named .mAppBP file:

1. Create a mApp Solution. From the mApp Editor menu bar, click **File>Save As**.

   Tip: You can also save a mApp Solution as a named .mAppBP file by clicking **Save mApp Solution to Disk** in the mApp Solutions section of the mApp Editor Task Pane.

2. Provide a **filename** for the mApp Solution.

   Note: Ensure that the file type is **.mAppBP**.

3. Click **Save**.

   A .mAppBP file is created. The name of the mApp Solution is displayed at the top of the CSM Administrator main window and at the top the mApp Editor.

To save changes to the open mApp Solution:

1. In a mApp Solution, do one of the following:
   - From the mApp Editor menu bar, click **File>Save mApp to Disk**.
   - On the mApp Editor toolbar, click the **Save** button.
   - In the mApp Editor Task Pane, click the **Save mApp to Disk** option.

Scan a mApp Solution

Use a mApp Solution Scan to periodically check your working mApp Solution for potential errors. The scan will look for missing items and alert you to any changes you need to make. Use the Scan Results window to manage any errors and warnings that are found during the scan.

Good to know:

- If you close the Scan Results window without resolving all issues found during the scan, you can return to this window by clicking **View Scan Results** in the mApp Solutions section of the mApp Editor Task Pane. This task is only available while you have issues to resolve; it disappears when you resolve all issues.

- If you resolve errors and warnings that add definitions to a mApp Solution, scan the mApp Solution again to ensure that the newly added definitions do not reference additional definitions that need to be included in the mApp Solution. Depending on the nature of the mApp Solution, some errors or warnings might be acceptable and do not need to be resolved.

To scan a mApp Solution:

1. Open the mApp Editor.

2. From the mApp Editor menu bar, click **File>Scan**.

   Tip: You can also scan a mApp Solution by clicking **Scan mApp Solution** in the mApp Solutions section of the mApp Editor Task Pane.

   If the scan is successful, a success window opens.

   If the mApp Solution contains changes that require reloading definitions or restarting applications after the mApp Solution is applied, an alert appears along with the scan results. The alert is triggered if the mApp Solution contains changes to significant system definitions, such as Business Objects, Forms, Grids, Form Arrangements, Relationships, Custom Views, One-Step Actions, automated behaviors, Dashboards, and/or Widgets.
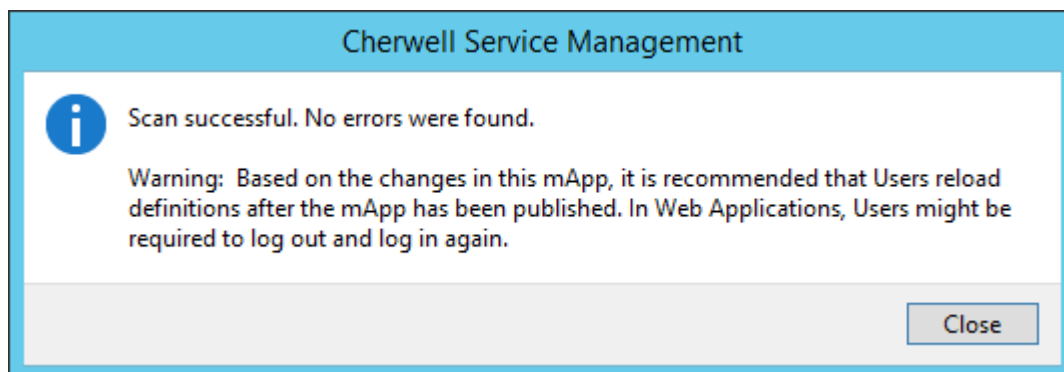
   If the scan detects errors, the mApp Solution Scan Results window opens.
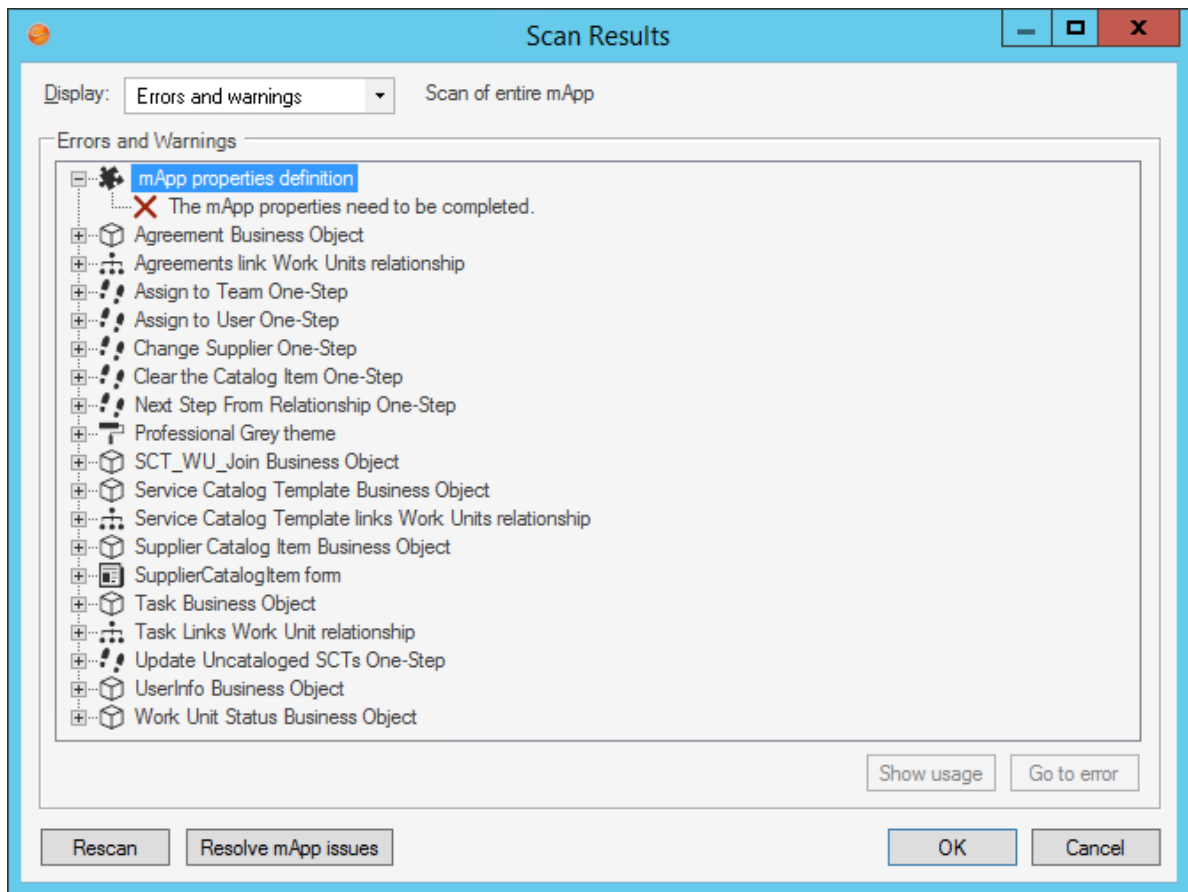
Examples: You will receive errors if you do not define general mApp Solution Properties, or if a definition in the mApp Solution references another definition that is not included in the mApp Solution.

3. Manage errors and warnings:
   - Show Usage: Click this button to open a window that shows how a definition is used in CSM.

   - Go to Error: Click this button to navigate to the error and resolve it (if the error cannot be automatically resolved).

   - Resolve: Click this button to automatically resolve each error or warning separately.

   - Rescan: Click this button to rescan the mApp Solution.

   - Resolve mApp Solution Issues: Click this button to resolve all errors and warnings that can be automatically resolved. If mApp Solution Properties have not been defined, the mApp Solution Properties window will open so that you can complete the properties.

4. Select **OK**.

Related concepts
Open the mApp Editor

Define mApp Solution Properties
Apply a mApp Solution
Scan a Blueprint

Close a mApp Solution

Use the Close mApp Solution option to close the active mApp Solution, but not CSM Administrator.

To close a mApp Solution:

1. From the mApp Editor menu bar, click **File>Close mApp**.

   Tip: You can also close a mApp Solution by clicking **Close mApp Solution** in the mApp Solutions section of the mApp EditorTask Pane.

   If the mApp Solution is not yet saved to a named .mAppBP file, you are prompted to name and save it. If changes are not yet saved, you are prompted to save them to the active .mAppBP file.

View mApp Solution Changes

Use the mApp Solution Changes window opened from the mApp Solution Editor to view the system definitions that will be changed by the active mApp Solution when it is applied to the target system.

The mApp Solution Changes window can be opened from the mApp Editor Menu Bar (**File>mApp Solution Changes**).

When you view mApp Solution changes, you can:

- Select how changes are grouped (by Business Object, Security Groups, Roles, Definition Type, or View).
- Search for specific items in the mApp Solution.
- Remove items from the mApp Solution.
- Compare the mApp Solution definitions with the original system definitions.

The indicators next to each definition show the selected merge actions.

Icon	Merge Action	Description
⚠️	Overwrite	Existing definition will be overwritten (or added if it does not exist).
←	Import if not found	Definition will be imported if it does not already exist in the target system.
✖	Remove	Existing definition will be removed from target system.
⇄	Merge	Definition will be merged into target system (only selected areas will be overwritten).
ⓘ	For Reference Only	Definition is included in mApp Solution for informational purposes only.
No Icon	Don't Import	Definition will not be imported into target system.
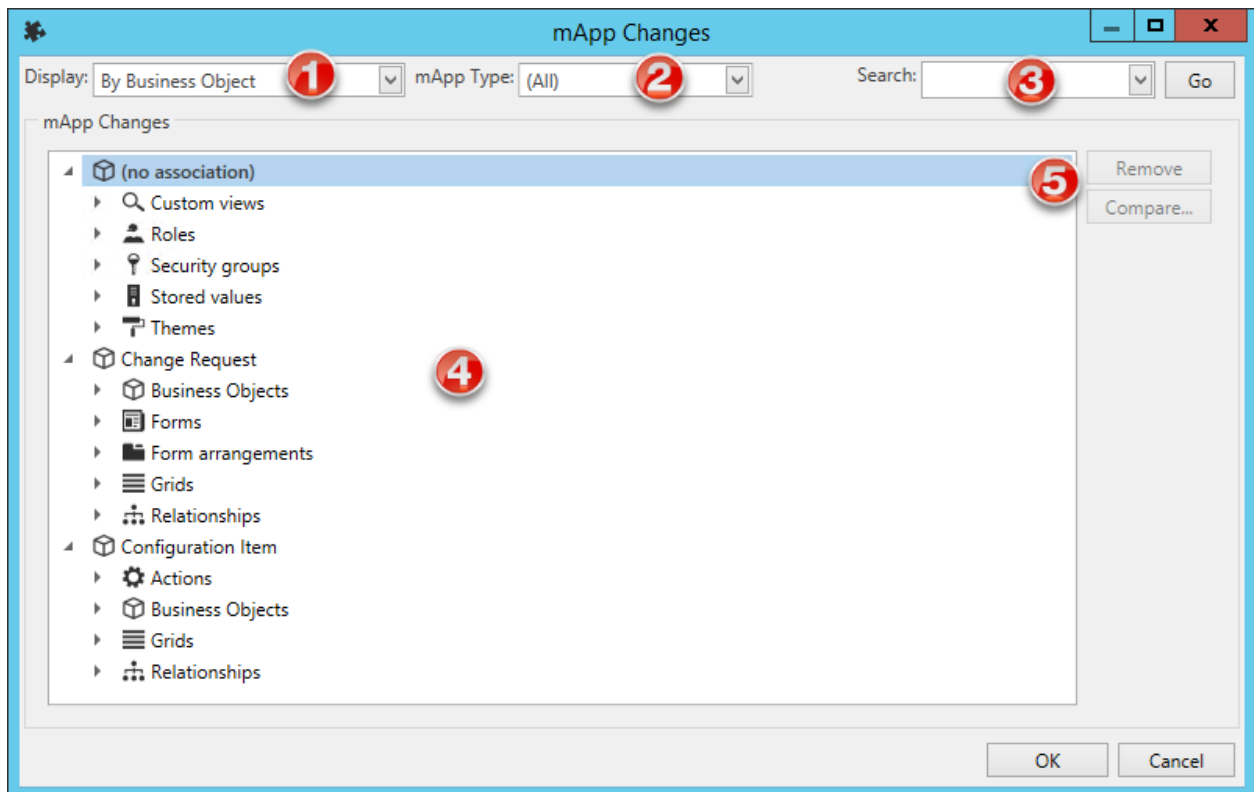
1. Display: Groups items in the tree by Business Object, Security Group, Role, Definition, or View.
   - **By Business Object**: Groups changes by Business Object (example: Incident).
   - By Definition Type: Groups changes by the type of system definition (example: Forms).
   - **By View and then Business Object**: Groups changes by View (example: Default, Portal Default) and then by Business Object (example: Incident).
   - **By View and then Definition Type**: Groups changes by View (example: Default, Portal Default) and then by type of system definition (example: Forms).

2. mApp Solution Type: Filters items in the tree by merge action:
   - **Do Not Overwrite**: Displays items marked *Do Not Overwrite* (definition will remain unchanged in the target system).
   - **For Reference Only**: Displays items marked *For Reference Only* (definition is included in the mApp Solution for informational purposes only).
   - **Import if not found**: Displays items marked *Import* (definition will be imported into the target system if it does not already exist).
   - **Merge by area**: Displays items marked *Merge* (individual areas of the definition have separate merge actions).
   - **Overwrite**: Displays items marked *Overwrite* (definition will be overwritten in the target system).

- ◦ **Remove if found**: Displays items marked *Remove* (definition will be removed from the target system if it already exists).

3. Search: Searches for items by keyword or phrase.
    a. In the **Search** ox, provide a word or phrase to search for. The drop-down displays the most recently used (MRU) searches.

    b. Click **Go** to run the search. The items containing the specified word or phrase are displayed within their hierarchical structure.

4. mApp Solution Changes Tree: Displays items in a hierarchical tree grouped by the selected Display option.
    - ◦ Click the arrow next to a category to expand it and view its items. Click the arrow again to collapse it.

    > **Tip:** Right-click a category or item to open a context menu, and then select options to expand/collapse the tree, remove items, or compare definitions.

5. Remove/Compare:
    - ◦ Click **Remove** to remove a selected item from the mApp Solution (it is not removed from the system).

    - ◦ Click **Compare** to open the mApp Solution Differences window and compare the mApp Solution definition with the existing system definition. This a low-level comparison of the individual properties that make up the definition.

    > **Note:** *Remove* and *Compare* are only enabled when an individual definition is selected. You cannot remove or compare definitions by selecting display categories.
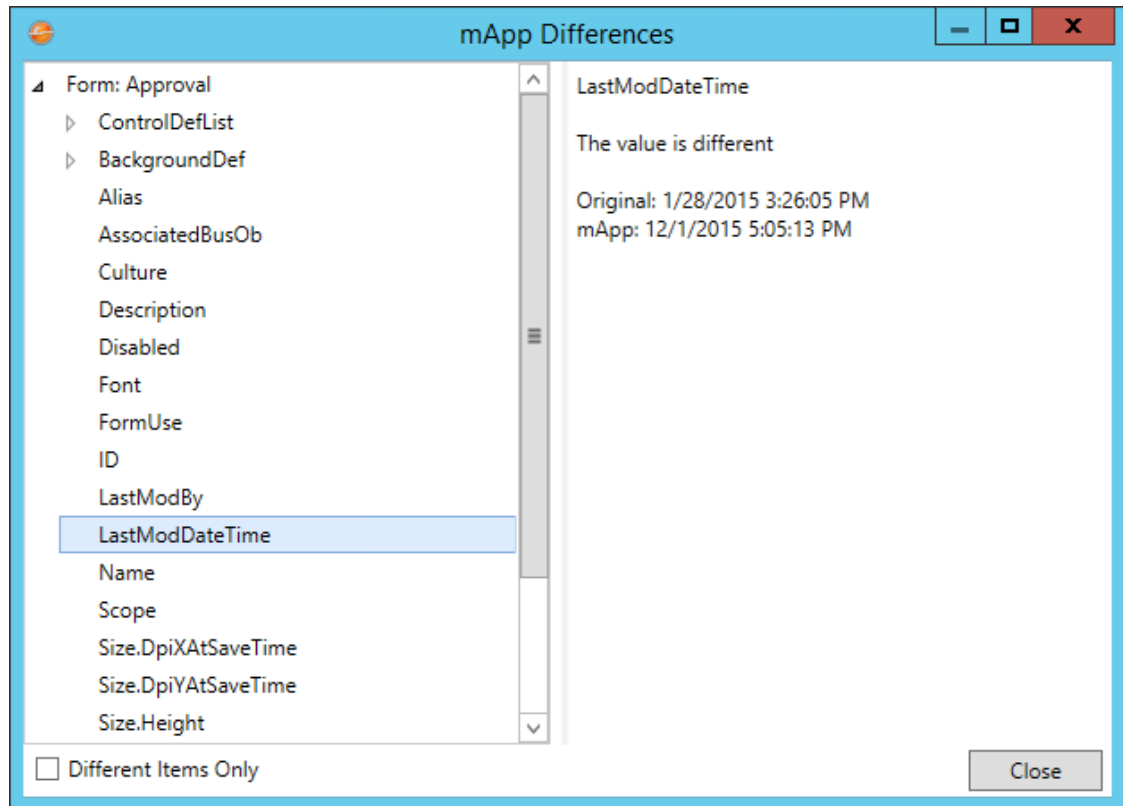
- Select the **Different Items Only** check box to limit the list of existing system definitions to those that the mApp Solution affects.

Rebase mApp Solution Definitions

Use the Rebase mApp Solution Definitions operation to reload mApp Solution definitions from your underlying CSM system.

This allows you to update definitions in a mApp Solution with the latest versions from your system while maintaining the defined merge actions (overwrite, do not overwrite, merge, etc.) for those definitions.

For example, if you create a mApp Solution that includes an Incident Business Object, and then the Business Object is updated in the underlying system (example: Fields are added/deleted), you can update the Business Object definitions in the mApp Solution to reflect those changes.

mApp Solution definitions can be rebased in several ways:

1.
    - (All definitions in a mApp Solution) From the mApp Editor menu bar, click **File>Rebase all mApp definitions**.

    - (Business Object and associated definitions) In the Object Manager in the mApp Editor, click a **Business Object** from the Object tree, and then click the **Rebase mApp Version of Bus Ob, etc.** task in the Structure area.

      Note: The *Rebase mApp Solution Version of Bus Ob, etc.* option is only available if the selected Business Object is included in the mApp Solution.

      The Rebase Business Object window opens. By default, all definitions included in the mApp Solution that are associated with the Business Object are selected. Clear the definitions that you do not want to rebase.

      Tip: Click the **Uncheck All** button to clear all definitions in the window. Click the **Select All** button to select all definitions.

The Rebase Business Object dialog box showing the message: "The Work Unit business object and/or related items are part of the mApp. Choose which ones to rebase from the main system. This will update each selected definition in the mApp to match the version in the main system." with a list of checked items including: Work Unit Business Object, Assign to Team One-Step, Assign to User One-Step, Change Supplier One-Step, Clear the Catalog Item One-Step, Next Step From Relationship One-Step, Update Uncataloged SCTs One-Step, Work Unit Actions automated behavior definition, Work Unit Links Agreement relationship, Work Unit links SCT_WU_Join relationship, Work Unit Links Supplier Catalog Item relationship, Work Unit Links Tasks relationship, Work Unit links to Work Unit Status relationship, Work Unit Links UserInfo relationship, Work Units link Service Catalog Templates relationship, WorkUnit form, WorkUnit form arrangement.

- ◦ (A specific CSM Item definition) In a CSM Item Manager (example: One-Step Action Manager) in the mApp Editor, right-click an **item** (example: One-Step Action) that is included in the mApp Solution, and then select **Rebase in mApp from system**.

Prepare a mApp Solution for Distribution

Prepare a new mApp Solution or a new version of an existing mApp Solution for distribution when you are ready to submit the mApp Solution to the mApp Exchange or distribute it directly to potential users.

When you prepare a version of a mApp Solution for distribution, it is scanned for errors and then saved as a .mApp file so that it can be applied to CSM systems.

Good to Know:

- If the mApp Solution contains translations, you can define mApp Solution properties for each culture. See Applying Cultures to mApps.
- If the mApp Solution contains encrypted Fields, encryption will be disabled and the Fields will be converted to text in the distributable mApp file. If this occurs, you will be notified with a warning message.

To prepare a mApp Solution for distribution:

1. Scan the mApp Solution before preparing it for distribution. This allows you to resolve any issues in the mApp Solution, as well as in the underlying system from which the mApp Solution was created.
2. Open an existing mApp Solution.
3. From the mApp Editor menu bar, click **File>Prepare mApp for distribution**.

   Tip: You can also prepare a mApp Solution for distribution by clicking **Prepare mApp Solution for distribution** in the mApp Solutions section of the mApp Editor Task Pane.

   If there are errors that need to be resolved, the mApp Solution Preparation Scan window opens.
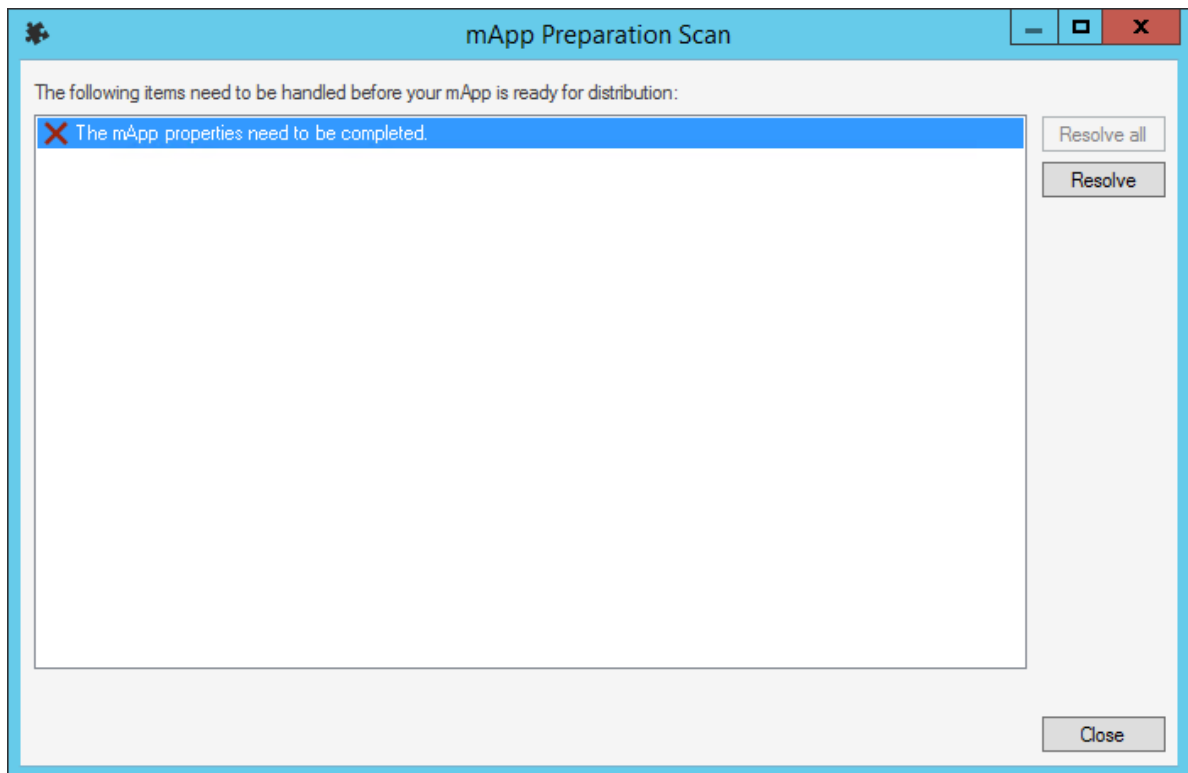
4. Resolve errors:
   - Click **Resolve All** to resolve all items in the list at once.

   - Click **Resolve** to resolve each selected item individually.

After all errors are resolved (or if there are no errors), the Final Preparation for mApp Solution Distribution window opens.

5. Prepare the mApp Solution for distribution:

   a. Enter a version number for the mApp Solution in the New Distribution Version field.

   > **Note:** The mApp Solution version must be in the form of "X.Y" where X is the major version and Y is the minor version. The versions can be any number between 1 and 99.

   b. Define a location for the mApp Solution Blueprint file (.mAppBP). This allows you to save the mAppBP file so you can return to it later and make changes, if necessary. The path where the file was last saved is displayed in the field.
      - Provide the **path** and **filename** where the file will be saved.

      - Click the **Ellipses** button [...] to browse to the location where the file will be saved.

    c. Define a location for the prepared mApp Solution file (.mApp). This is the file that will be submitted to the mApp Exchange or distributed directly to potential users.

        ◦ Provide the **path** and **filename** where the file will be saved.

        ◦ Click the **Ellipses** button to browse to the location where the file will be saved.

        ◦ Create Compressed File: Select this check box to save the distributable mApp Solution file in a compressed binary format. Compressed mApp Solution files (designated with a .mappz extension) cannot be edited.

    d. View additional designers (only appears if the mApp Solution includes definitions that were created or updated by other mApp Solution creators). Each entry includes the mApp Solution creator's personal and/or company name as well as the most recent creation date/time.

6. Select **OK**.

7. Distribute the mApp Solution.

Using mApp Solutions

When working with mApp Solutions, Users can:

- View which mApp Solutions have already been installed in their CSM systems.
- Go to the mApp Exchange to view and download mApp Solutions created by others, or to submit mApp Solutions.
- Apply mApp Solutions to their CSM systems (using the Apply mApp Wizard).

Considerations for Applying mApp Solutions

Before applying a mApp® Solution, read the following recommendations to avoid conflicts or errors on your system.

- As a precaution, back up your database prior to applying a mApp Solution.

- Never apply a mApp Solution to a database that already has an installation of the same mApp Solution, including previous versions. To determine if the mApp Solution has already been applied to your database, review the Items List in the documentation and compare it to your target system to determine if those items are present. If they exist, do not proceed with applying the mApp Solution. Otherwise, you may experience unexpected results.

  > **Note:** If you find yourself in a situation where you must apply a later version of a mApp Solution that has already been applied to your system, there are methods that can be used to accomplish this. See Troubleshooting mApp Solutions

- Apply your mApp Solution against a test system before applying it to your live system.

- If the mApp Solution includes definitions that have history records, a list of additional designers is shown on the introductory page of theApply mApp Wizard. Each entry includes the mApp Solution creator's personal and/or company name as well as the most recent creation date/time.

- The merge actions displayed in the wizard were selected when the mApp Solution was created. If you select a high level of interaction with the wizard (the **Ask me about everything** option), you can change the merge actions. For example, if you do not want to overwrite or change a definition, you can set the merge action to **Don't Change** in the wizard.

- The target objects/items displayed in the wizard are what the wizard detects in the target system as exact (or close) matches to the mApp Solution definitions. An exact match means that the wizard found a target object/item with the same record ID or exactly the same name as the definition in the mApp Solution. If you select a high level of interaction with the wizard (the **Ask me about everything** option), you can change the target objects/items.

- If you select a low level of interaction with the wizard, the wizard assumes you want to use the merge actions selected when the mApp Solution was created and the target objects/items it detects as exact matches in the target system. It only asks for input if an area requires clarification.

- The wizard asks you about objects and items in order of importance (determined by the mApp Solution creator). Business Object Views are always asked about first, followed by Group Objects (Group Leaders, and then Group Members), and then the remaining objects and items in order of importance.

- After you complete the wizard, you can open a Blueprint to preview the changes the mApp Solution will make to your system (recommended) or attempt to directly publish the changes. If you open a Blueprint, you can then scan the Blueprint and view Blueprint changes before publishing it.

- **Important:** If you apply a mApp Solution containing a newly converted Group Business Object(s), then we strongly recommend that you use overwrite instead of merge options in the Add Business Object to mApp Wizard. If you use merge options with Group Objects, this can result in Blueprint scan errors or unexpected results appearing after the mApp Solution has been applied.

Related concepts

Apply a mApp Solution

Scan a Blueprint

View Blueprint Changes

Publish a Blueprint

View Installed mApp Solutions

Use the View Installed mApp Solutions task in the CSM Administrator main window to view a list of mApp Solutions that have been installed in your system. If any Protected mApp™ Solutions have been installed, you see a shield icon ![shield icon] next to them in the list.

The page is searchable.

To view installed mApp Solutions:

1. In the CSM Administrator main window, select the **mApps** category, and then select the **View Installed mApps** task.
2. Select the **name** of the mApp Solution to navigate to a page containing overviews, instructions, and specific contact information. Depending on the item selected, the page might also contain:
   ◦ **Helpful links:** The mApp Exchange, direct access to topics in the CSM web help, etc.
   ◦ **Downloadable files:** mApp Solution files, supporting files, documentation, etc.

Go to the Cherwell Marketplace (formerly the mApp Exchange)

Go to the Cherwell Marketplace to view and download mApp® Solutions created by others or submit mApp Solutions that you created.

Note: In December 2019, the mApp Exchange moved to a new platform and is now called the Cherwell Marketplace. Use the **Go to mApp Marketplace** task or open https://www.cherwell.com/marketplace/ to access the Cherwell Marketplace.

Users must have a Cherwell SSO account to download mApp Solutions or submit their own mApp Solutions on the Cherwell Marketplace. Go to How to Sign Up for a Cherwell SSO Account for more information.

To go to the Cherwell Marketplace:

1. Select the **mApps** category in the **CSM Administrator** main window.
2. Select the **Go to the mApp Marketplace** task.
3. Sign in to the Marketplace to submit or download mApp Solutions.

Note: Go to How to Add or Edit a mApp in Marketplace for information on how to submit a mApp Solution to the Cherwell Marketplace.

View mApp History

Use the View mApp History task on the mApp page in CSM Administrator to view a list of available history records for all definitions within your CSM system that were modified by a mApp Solution.

Good to know:

- Viewing mApp Solution history requires security rights.
- Only definitions with history records are shown. Definitions only have history records if mApp Solution creators used Designer IDs when creating the mApp Solutions that were applied to your system.

To view mApp Solution history, in the CSM Administrator main window, click the mApps category, and then click the View mApp History task.
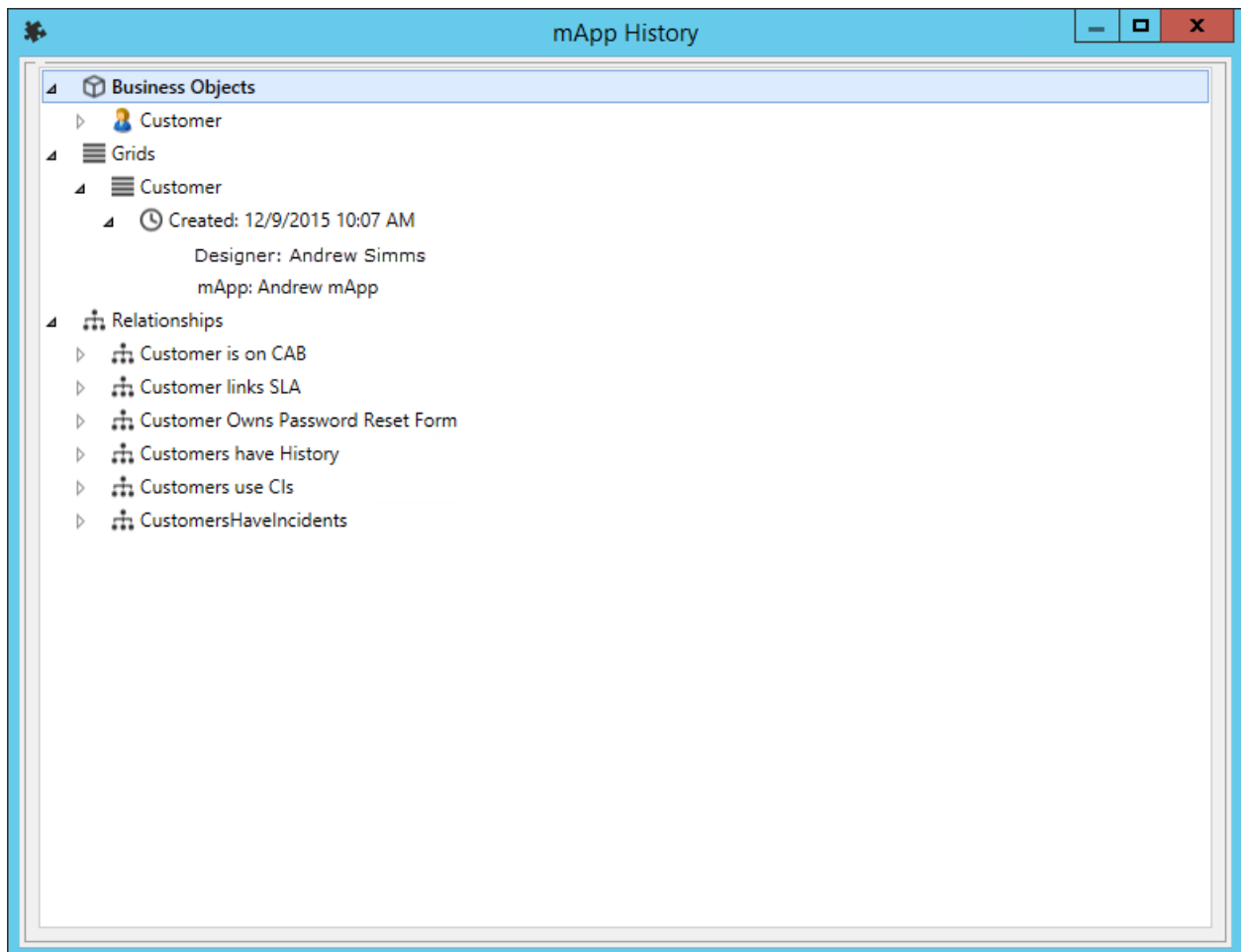
Apply a mApp Solution

The Apply mApp Wizard (accessed from within the mApp Editor) is a specialized tool that walks you through the process of applying a mApp Solution to a CSM system.

Use the Apply mApp Wizard to select how to merge each definition into the target system.

When you apply a mApp Solution, you can define:

- **Interaction Level**: How much you want the wizard to decide automatically.
- **Merge actions**: How you want each Business Object (along with its associated Fields, Relationships, Forms, Grids, and Form Arrangements) and CSM Item (including Security Groups and Roles) to be merged into the target system.
- **Target objects/items**: Which existing items to overwrite in the target system. You can also select to have a new item created for a mApp Solution definition.

Important: If you apply a Protected mApp Solution, you see a message saying `This mApp is protected and can only be modified in limited ways.` Your interaction level is set to **Don't ask me unless absolutely necessary** and other interaction options cannot be selected. For more information, see: Protected mApp™ Solutions.

To apply a mApp Solution to a system:

Note: The following procedure assumes a high level of interaction (*Ask me about everything*). The pages you see in the wizard (and their order) might differ from the following procedure, as they depend on what is included in the mApp Solution, the importance level of each object and item, and the level of User interaction you select.

1. In the CSM Administrator main window, select the **mApps** category, and then select the **Apply a mApp** task.
2. Select a mApp Solution to apply to the target system, and then select **Open**.

   The Apply mApp Wizard opens, displaying the properties defined for the mApp Solution.

   Tip: If available, select the **More Information** link to navigate to a website that contains detailed information about the mApp Solution.

3. Select **Yes** to accept the terms of the license agreement, and then select **Next**.
4. Carefully review the security information that explains that the mApp Solution contains Security Groups and/or Roles that may impact security rights in the target database, and then click **Yes** to accept the terms.
5. On the **Localization** page:

- If you are applying a mApp Solution created in CSM 9.2.0 or later, review the cultures for translations included in the mApp Solution. If Globalization is enabled for your system and you have enabled the cultures listed for the mApp Solution, translated strings are shown to users of the cultures included in the mApp Solution.

- If you are applying a mApp Solution created before CSM 9.2.0, select the target culture for the mApp Solution. You must perform this task even if Globalization is not enabled for your system.

6. Select a level of user Interaction (how automatic the merge process should be):

> **Note:** No matter which interaction level you select, you will have the option to see a summary of all changes before anything is actually modified in the target system.

- **Ask me about every decision**: Allow the wizard ask how you want to apply every object and item that is included in the mApp Solution.

- **Make reasonable decisions, but ask me if you are unsure (default)**: Make the apply mApp Solution process partially automated (you will be asked about any areas that require clarification). If the wizard does not need to ask you anything, you will be directed to the summary page.

- **Don't ask me unless absolutely necessary**: Make the apply mApp Solution process almost fully automated (you will only be asked about areas that absolutely require your interaction, such as Security Groups and Roles). If the wizard does not need to ask you anything, you will be directed to the summary page.

7. Continue through the Wizard and define options for features and definitions included in the mApp Solution.

Define Options for Features

This page only applies if the mApp Solution includes Features. There is a page for each Feature in the mApp Solution.

Select the **Enabled** check box to apply a mApp Solution Feature with all of its associated definitions to the target system. If you clear this check box, the Feature will not be applied to the target system (you will not receive any further prompting about the Feature or any of its associated definitions). If the mApp Solution creator included a Feature by default, this check box is automatically selected.

Define Options for Business Objects

This page only applies if the mApp Solution includes Business Objects. If it includes Group objects, you will be asked about those first (Group Leaders, and then Group Members). If it includes a Group Member without a Group Leader, you will be asked to select or create a Group Leader.

1. Select a merge action and target Business Object:
   - **Select [Business Object Name] Business Object (best match)**: If an exact Business Object match is found in the target system, select this radio button to have the Business Object definition in the mApp Solution imported into this object.

   > **Tip:** Click the information icon to view detailed information about the best match.

- **Select a different existing object**: If an exact match is not found, or to select a different object in the target system, select this radio button to select an existing object to import the mApp Solution object into.
  - **Select from List**: If objects with names similar to the mApp Solution object are found in the target system, they are listed on the page. Select an object in the list.
  - **Select Other Object**: Click this button to open a separate window containing a list of all objects in the target system. Select an object from the list.
- **Create a New Object**: Select this radio button to have the mApp Solution create a new object in the target system.
- **Skip this Object**: Select this radio button to skip importing this object in the target system.

  Note: If you skip the object, related/dependent objects and associated definitions (Relationships, Fields, Forms, etc.) will also be excluded from the import, and the wizard will not ask you about them.

2. Select merge actions for the object's merge areas:
   - **Overwrite**: Overwrites the definition in the target system.
   - **Don't Change**: Leaves the definition in the target system unchanged.

3. Select merge actions and target items for the object's child items (Fields, indexes, and Relationships associated with the object):

   Note: This page does not apply if the mApp Solution is creating a new object, or if the entire Business Object will be overwritten.

   - **Merge Actions**: These are the merge actions the mApp Solution creator defined for each child item in the object. To change the merge action for an item, select an option in the Merge Action column's drop-downs:
     - **Overwrite**: Overwrites the definition in the target system.
     - **Merge**: Merges the Field's properties with the target Field's existing properties.
     - **Don't Change**: Leaves the definition in the target system unchanged.
   - **Target item**: If an exact match is found in the target system, it is listed in this column. To change the target item, select an option in the Target column's drop-downs:
     - **Item with similar name**: If the target system contains items with names similar to the ones in the mApp Solution, they are listed in the drop-down. Select an item in the list.
     - **(Treat as new)**: Select this option to create a new item (must have a unique name).
     - **(More...)**: Select this option to open a separate window containing a list of all items of a particular type (example: Fields) in the Business Object.

       Note: If you select *Treat as new* (for this and any subsequent pages) and do not define a unique name, or if a mApp Solution item is found to have the same name as an item in the target system, the wizard will ask you to resolve naming conflicts.

Define Options for Displayable Items

Select options for displayable items associated with the object (Forms, Grids, Form Arrangement, etc.).

1. Select an option in the Merge Action column's drop-downs:
   - **Overwrite**: Overwrites the definition with the same ID in the target system.

   - **(Treat as new)**: Creates a new item in the target system (must have a unique name).

   - **Don't Change**: Leaves the definition in the target system unchanged.

     Note: For Form Arrangements, you also have the option to Merge the mApp Solution definition with the one in the target system. This means that the Tabs in the mApp Solution Form Arrangement will be merged with the existing Tabs in the target Form Arrangement, allowing you to add Tabs to the existing Form Arrangement without entirely overwriting it. For more information, see Configure Merge Actions for Form Arrangements and Tabs.

2. Select a merge action and target object for removal.

   Note: This page only applies if the mApp Solution is removing a Business Object.

   - **Select [Business Object Name] Business Object (best match)**: If an exact Business Object match is found in the target system, select this radio button to have it removed from the target system.

     Tip: Click the information icon to view detailed information about the best match.

   - **Select a different existing object**: If an exact match is not found, or to use a different object in the target system, select this radio button to select an object to remove from the target system.
     - **Select from List**: If objects with names similar to the mApp Solution object are found in the target system, they are listed on the page. Select an object from the list.
     - **Select Other Object**: Click this button to open a separate window containing a list of all objects in the target system. Select an object from the list.
   - **Skip this Object**: Click this radio button to skip removing this object from the target system.

Define Options for Security Groups and Roles

This page only applies if the mApp Solution includes Security Groups and Roles.

Important: Security Groups and/or Roles may impact security rights in the target database after the mApp Solution is applied. Be sure to carefully review the merge actions and target items for Security Groups and Roles when you apply the mApp Solution. To ensure that you understand the implications of applying security changes included in the mApp Solution, we strongly advise you to apply the mApp Solution to a test environment and verify the security changes before you commit the mApp Solution to a production environment.

Select merge actions and target items for Security Groups and Roles included in the mApp Solution:

- **Merge Action**: To change the merge action for an item, select an option in the Merge Action column's drop-down:
    - ◦ **Overwrite**: Overwrites the Security Group and/or Role in the target system.
    - ◦ **Don't Change**: Leaves the Security Group and/or Role in the target system unchanged.
- **Target item**: If an exact match is found in the target system, it is listed in this column. To change the target item, select an option in the Target Item's column drop-down:
    - ◦ **Item with similar name**: If the target system contains items with names similar to the ones in the mApp Solution, they are listed in the drop-down.
    - ◦ (**Treat as new)**: Select this option to create a new Security Group and/or Role (must have a unique name).
    - ◦ **(More...)**: Select this option to open the CSM Item Manager and select another Security Group and/or Role.

Define Options for CSM Items

Select merge actions and target items for CSM Items included in the mApp Solution.

- **Merge Action**: To change the merge action for an item, select an option in the Merge Action column's drop-down:
    - ◦ **Overwrite**: Overwrites the definition in the target system.
    - ◦ **Don't Change**: Leaves the definition in the target system unchanged.
- **Target item**: If an exact match is found in the target system, it is listed in this column. To change the target item, select an option in the Target Item's column drop-down:
    - ◦ **Item with similar name**: If the target system contains items with names similar to the ones in the mApp Solution, they are listed in the drop-down.
    - ◦ **(Treat as new)**: Select this option to create a new item (must have a unique name).
    - ◦ **(More...)**: Select this option to open the appropriate CSM Item Manager and select another item.

Define Options for One-Step Actions

This page only applies if the mApp Solution includes One-Step Actions.

Select merge actions and target items for the One-Step Actions included in the mApp Solution.

- **Merge Actions**: These are the merge actions the mApp Solution creator defined for each One-Step Action. To change the merge action for a One-Step Action, select an option in the Merge Action column's drop-down:
    - ◦ **Overwrite**: Overwrites the definition in the target system.
    - ◦ **Don't Change**: Leaves the definition in the target system unchanged.
- **Target item**: If an exact match is found in the target system, it is listed in this column. To change the target item, select an option in the Target Item column's drop-down:

- **Item with similar name**: If the target system contains items with names similar to the ones in the mApp Solution, they are listed in the drop-down.

- **(Treat as new)**: Select this option to create a new item (must have a unique name).

- **(More...)**: Select this option to open the One-Step Action Manager and select a different One-Step Action.

Define Options for Miscellaneous Items

Select merge actions and target items for miscellaneous items included in the mApp Solution (example: Dashboards, Stored Searches, Stored Values, external connections, etc.).

1. **Merge Actions**: These are the merge actions the mApp Solution creator defined for each item. To change the merge action for an item, select an option fin the Merge Action column's drop-down:
   - **Overwrite**: Overwrites the definition in the target system.

   - **Don't Change**: Leaves the definition in the target system unchanged.

2. **Target item**: If an exact match is found in the target system, it is listed in this column. To change the target item, select an option in the Target Item column's drop-down:
   - **Item with similar name**: If the target system contains items with names similar to the ones in the mApp Solution, they are listed in the drop-down.

   - **(Treat as new)**: Select this option to create a new item (must have a unique name).

   - **(More...)**: Select this option to open a separate window containing a list of all items of a particular type.

     Note: If this is a CSM Item, the (More...) option will open the appropriate CSM Item Manager.

3. Provide a **value** for the Stored Value.

   Note: This page only applies if the mApp Solution includes Stored Values that prompt Users to provide values. If you do not specify a value, the default value for the Stored Value is used.

4. Click **Edit External Connection** to open the External Connection Wizard and define settings for the external connection.

   Note: This page only applies if the mApp Solution includes external connections that prompt Users to specify their own external connection settings.

Finalize the Wizard

To finalize the Wizard:

1. Review the Summary page, and then click the **Save to File** button to open the Choose Export File window, and then provide a location, file name, and output format (.csv, .html, .htm, .txt, .rtf, .xml) for exporting the summary of mApp Solution definitions that will be applied to the target system.

2. Define final options (what to do after the mApp Solution is applied to the target system):
   - (Recommended) **Open a Blueprint so I can preview the changes**: Select this radio button to open a Blueprint that allows you to see the changes the mApp Solution will make to the target system.

     Important: If you select this option, you will then need to publish the Blueprint to commit the changes to the target system.

◦ **Attempt to publish the changes directly**: Select this radio button to immediately publish the Blueprint of mApp Solution changes directly to the target system without previewing it first.

3. Select **Finish**.

The merge process runs and generates a Blueprint. Depending on the option selected previously, the Blueprint either:

◦ Opens and allows you to view the mApp Solution changes.

◦ Immediately attempts to publish to the target system.

Related concepts

Considerations for Applying mApp Solutions

Protected mApp™ Solutions

About Globalization

Related tasks

Applying Cultures to mApps

Troubleshooting mApp Solutions

Some situations may fall outside the expected setup for mApp® Solutions. Use these steps for those cases.

If you must apply a mApp Solution to your system but already have a previous version of the same mApp Solution applied on your database, you cannot go about applying the mApp Solution like normal. However, there are three approaches you can take to apply the mApp Solution without compromising your data.

⭐ **Important:** For all three approaches, make sure to follow the steps on a development or test system and test thoroughly before moving changes to your production system.

First Approach

1. Make a copy of your existing system in a development or test environment with the existing mApp Solution applied.
2. Apply the new version of the mApp Solution on top of it and scan the Blueprint. You will receive errors.
3. Select each error one by one and determine what needs to be resolved.
4. Resolve each error, one at a time.

Second Approach

1. On a development or test system, restore a Demo.czar, then apply the new mApp Solution.
2. One by one, compare the features of the new mApp Solution against your production system with the existing mApp Solution to see what changed compared to your existing mApp Solution.
3. If there are features in the new mApp Solution that you want but do not have on the existing mApp Solution, add them to a Blueprint or create a new mApp Solution with only those features.
4. On another development or test system with a copy of your production database and your existing mApp Solution, apply your new isolated Blueprint or mApp Solution with only the features you want, and scan it.
5. If you receive errors, determine what errors need to be resolved and resolve them one at a time.

Third Approach

1. On a development or test system, restore a Demo.czar, then apply the new mApp Solution.
2. One by one, compare the features of the new mApp Solution against your production system with the existing mApp Solution to see what changed compared to your existing mApp Solution.
3. If there are features in the new mApp Solution that you want but do not have on the existing mApp Solution, build them from scratch on a separate development or test environment with a copy of your production database, using the demo environment with the new mApp Solution as a reference guide on what to build.

Configuring mApp Solutions

Complete the following procedures to configure mApp Solutions. Configuration procedures are completed in CSM Administrator.

To configure mApp Solutions:

1. Configure mApp Solution security rights: Configure who can access mApp Solution functionality and data.

2. Configure merge actions for system definitions: Configure how definitions are merged into a target system by selecting merge actions from the various properties windows (example: Business Object Properties window, Relationship Properties window, etc.). The properties windows have more detailed mApp Solution options available outside of the Add Business Object to mApp Wizard.

3. View referenced definitions in a mApp Solution: From the various properties windows, view all of the system definitions throughout CSM being used by a selected mApp Solution definition (Business Object, Relationship, Form, Grid, Form Arrangement, and/or CSM Item). Add definitions from the References window to ensure that all necessary definitions are included in a mApp Solution.

4. Configure mApp Solution conditions: Configure conditions that control when definitions are imported into a target system when a mApp Solution is applied.

5. Prepare mApp Solution for distribution: Creates a mApp Solution file that can be distributed or uploaded to the mApp Exchange.

Configure Merge Actions for Business Object Definitions

Merge actions determine how the system definitions in a mApp® Solution are merged into a target system when a mApp Solution is applied.

Use the Add Business Object to Wizard as a convenient method of defining merge actions for Business Objects and their associated Fields, Relationships, Forms, Grids, and Form Arrangements. The definitions added to a mApp Solution using the wizard are imported into a target system when the mApp Solution is applied, and the merge actions you select are applied to the definitions in the target system if they already exist. You can select from the following basic merge actions:

- **Overwrite All:** Overwrites all of the existing definitions of a particular type (example: All Fields) in the target system, or adds them if they are not already there.
- **Do Not Overwrite Any:** Leaves all of the definitions of a particular type (example: All Fields) in the target system unchanged (does not overwrite or add the definitions).
- **Let me choose**: Overwrites the selected definitions of a particular type (example: Only the Fields you select).

However, you have some additional options available when you configure merge actions using the various properties windows (example: **Business Object Properties** window, **Relationship Properties** window, etc.) within the mApp Editor:

- **Import/Don't Import If Not Present:** Imports or does not import the definition into the target system if it does not already exist.
- **Remove:** Removes the definition from the target system.
- **For Reference Only:** Includes the definition in the mApp Solution for informational purposes only (the definition is not imported into the target system).

In addition, when you configure merge actions using the various properties windows, certain definitions that are imported into a target system have *Merge* as an available action. *Merge* means that you can select separate merge actions for individual areas of these system definitions. This is useful if the target system already has a version of the Business Objects included in a mApp Solution and you only want to import/overwrite certain areas. *Merge* is available for the following definitions:

- Business Objects
- Fields
- Relationships
- Form Arrangements
- Form Arrangement Tabs
- Business Object Actions

To configure merge actions for Business Object definitions:

1. Add a Business Object to a mApp Solution using the Add Business Object to mApp Wizard OR Add a Business Object to a Protected mApp Solution using the Add Business Object to mApp Wizard.

2. Configure merge actions for Business Objects.

3. Configure merge actions for Fields.

4. Configure merge actions for Relationships.

5. Configure merge actions for Forms.

6. Configure merge actions for Grids.

7. Configure merge actions for Form Arrangements.

8. Configure merge actions for Business Object Actions.

9. Prepare the mApp Solution for Distribution (**File > Prepare mApp for Distribution**), or save the mApp Solution (**File > Save mApp to Disk**) to continue making other changes.

Important: If you apply a Protected mApp Solution you see different default merge options for Business Objects definitions than when applying any other mApp Solution. For an explanation of merging behavior when using Protected mApp™ Solutions, see Add a Business Object to a Protected mApp™ Solution.

Configure Merge Actions for Business Objects

Set defaults for how the Business Object is merged into the system.

Use the **Business Object Properties** window to configure the following:

- **General properties:** Whether to include the Business Object in the mApp® Solution, and its importance in the mApp Solution.
- Options for merging the Business Object into the target system when the mApp Solution is applied:
    ◦ **Import to target system:** Imports the Business Object definition into the target system. You can select merge actions based on whether the Business Object definition already exists in the target system.
    ◦ **Remove from Target System:** Removes the Business Object definition from the target system.
    ◦ **For Reference Only:** Includes the Business Object definition in the mApp Solution for informational purposes only (it is not merged into the target system when the mApp Solution is applied).
    ◦ **Import based on condition:** Imports or removes the Business Object definition based on configured mApp Solution conditions.
- Merge actions for individual Business Object properties.

    🖊 **Note:** The **Business Object Properties** window is available in the Business Object Editor (accessed from within the Object Manager in the mApp Editor).

Good to know:

- You can only configure separate merge actions for individual Business Object properties and areas if the Business Object is set to **Merge** in the **Business Object Properties** window (**mApps** page). If the Business Object is set to any other option, or if the **Include in mApp Solution** check box is cleared, then you cannot configure separate merge actions for individual properties or areas.
- When a Business Object is included in a mApp Solution using the **Business Object Properties** window, its associated Relationships are not automatically added. Be sure to add all necessary Relationships. Select the References button (on the mApp page in the Business Object Properties window) to view/add the other definitions being used by a Business Object.

To configure merge actions for Business Objects:

1. Add a Business Object to a mApp Solution using the Add Business Object to mApp Wizard.
2. Open the **Business Object Properties** window for the Business Object you just added to the mApp Solution:
    a. In the Object Manager within the mApp Editor, select the **Business Object** in the Object tree, and then select the **Edit Business Object** task in the **Structure** area.

        The Business Object Editor opens.

> **Tip:** You can also select **Business Object** ⬢ on the mApp Editor toolbar to open the Business Object Editor.

    b. Select **Bus Ob Properties**.

3. Select the **mApps** page.

4. Configure mApp Solution properties and merge actions for the Business Object:
   a. Define general mApp Solution properties for the Business Object:
   - **Include in mApp:** Select this check box to include the Business Object in the mApp Solution. Clear this check box to leave the existing definition in the target system unchanged (the Business Object definition is not imported into the target system when the mApp Solution is applied).

     > **Note:** This check box is automatically selected if you added the Business Object using the Add Business Object to mApp Wizard.

   - **Importance:** Select the importance of the Business Object to the mApp Solution.

     > **Note:** Importance is automatically selected based on the option chosen in the Add Business Object to mApp Wizard. However, you can change it here if necessary. Changing the importance impacts the order in which the Apply mApp Wizard asks about Business Objects.

       - **High Importance:** Select this option if the selected Business Object is one of the main Business Objects in the mApp Solution.
       - **Medium Importance:** Select this option if the selected Business Object is a supporting object for the mApp Solution.
       - **Low Importance:** Select this option if the selected Business Object is not critical for the mApp Solution.
   - **References:** Select this button to open the References window and view all of the other definitions being used by the Business Object.
   b. Define options (merge actions) for how the definition will be merged into a target system:

     > **Note:** These options are only available if **Include in mApp** is selected.

   - **Import to target system:** Select this option to import the definition into a target system. Then, select a merge action based on whether or not the definition is already present in the target system:

     If already present: In the drop-down list, select a merge action to define how the definition is imported if it already exists in a target system:

       - **Overwrite:** Select this option to have the mApp Solution definition overwrite the existing definition in the target system.

- **Don't Import:** Select this option to leave the existing definition in the target system unchanged (the mApp Solution definition is not imported into the target system when the mApp Solution is applied).

- **Merge:** Select this option to define separate merge actions for each individual area of a definition.

If not present: In the drop-down list, select a merge action to define whether the definition is imported if it does not currently exist in the target system:

- **Import:** Select this option to import the mApp Solution definition into the target system if does not already exist.

- **Don't Import:** Select this option to skip importing the mApp Solution definition into the target system if it does not already exist (the mApp Solution definition will not be added to the target system).

- **Remove from Target System:** Select this option to remove the definition from a target system.

- **For Reference Only:** Select this option to include the definition in the mApp Solution for informational purposes only (the definition is not imported into the target system when the mApp Solution is applied).

- **Import Based on Condition:** Select this check box to import or remove the definition based on a condition. Select the ellipses to open the **mApp Solution Conditions** window and define mApp Solution conditions.

5. Configure separate merge actions for individual Business Object Property merge areas:
   a. In the **Options** area of the **Business Object Properties** window, select the **Import to Target System** check box.

   b. Select **Merge** as the merge action for the Business Object in the **If Already Present** drop-down list.
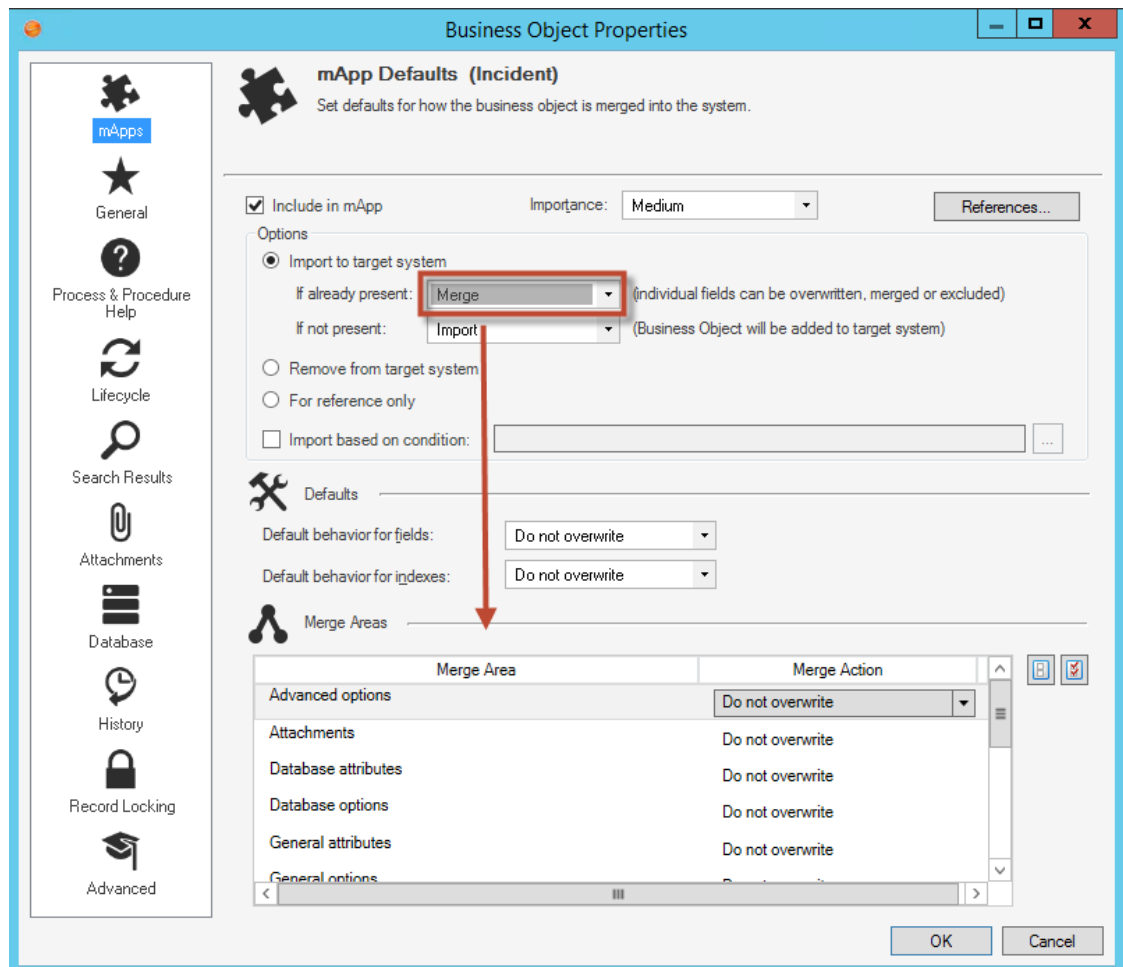
c. Define default behaviors for the Business Object's Fields and indexes. This is how Fields and indexes will be merged unless specified otherwise. In the drop-down lists, select one of the following options:

- **Overwrite:** Select this option to have the Business Object Fields and/or indexes overwritten in the target system when the mApp Solution is applied. You can then go to particular Fields or indexes and exclude the ones you do not want in the mApp Solution.

- **Do Not Overwrite** (Default): Select this option to leave the Business Object Fields and/or indexes unchanged in the target system when the mApp Solution is applied. You can then go to particular Fields or indexes and select which ones to include in the mApp Solution.

  Note: Because Indexes do not have IDs, they will be added to the target system if an exact name match is not found in the system when the mApp Solution is applied.

d. Define individual merge actions for each merge area:

In the Merge Areas Grid: For each merge area, select a merge action in the Merge Action column drop-down lists:

- **Overwrite:** Select this option to have the merge area overwritten in the target system when the mApp Solution is applied.

- **Do Not Overwrite:** Select this option to leave the merge area unchanged in the target system when the mApp Solution is applied.

  Tip: Select **Uncheck All** to set all merge areas to **Do Not Overwrite**. Select **Select All** to set all merge areas to **Overwrite**.

  On the remaining pages of the properties window: Select **mApp** next to each of the merge areas to define merge actions for individual properties:

  i. Define merge actions for general Business Object properties.

  ii. Define merge actions for Business Object process and procedure help.

  iii. Define merge actions for Business Object lifecycle properties.

  iv. Define merge actions for Business Object search results properties.

  v. Define merge actions for Business Object Attachment options.

  vi. Define merge actions for Business Object database options.

  vii. Define merge actions for Business Object history options.

  viii. Define merge actions for Business Object Record Locking settings (only if record locking is enabled for your system).

  ix. Define merge actions for Business Object localization settings.

  x. Define merge actions for Business Object advanced properties.

e. Select **OK**.

  The header in the Business Object Editor shows the selections made in the **Business Object Properties** window. For example, if you select **High Importance** and **Merge**, the appropriate indicators will be displayed in the header:
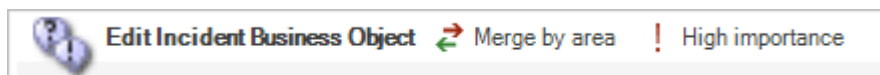
  These indicators are also displayed in the **Task** Section of the Object Manager.

  The mApp Solution Action column in the list of Fields shows the selections made in the Defaults section of the **Business Object Properties** window (**Default Behavior for Fields** drop-down list).

6. Prepare the mApp Solution for Distribution (**File > Prepare mApp for Distribution**), or save the mApp Solution (**File > Save mApp to Disk**) to continue making other changes.

Protected mApp™ Solutions
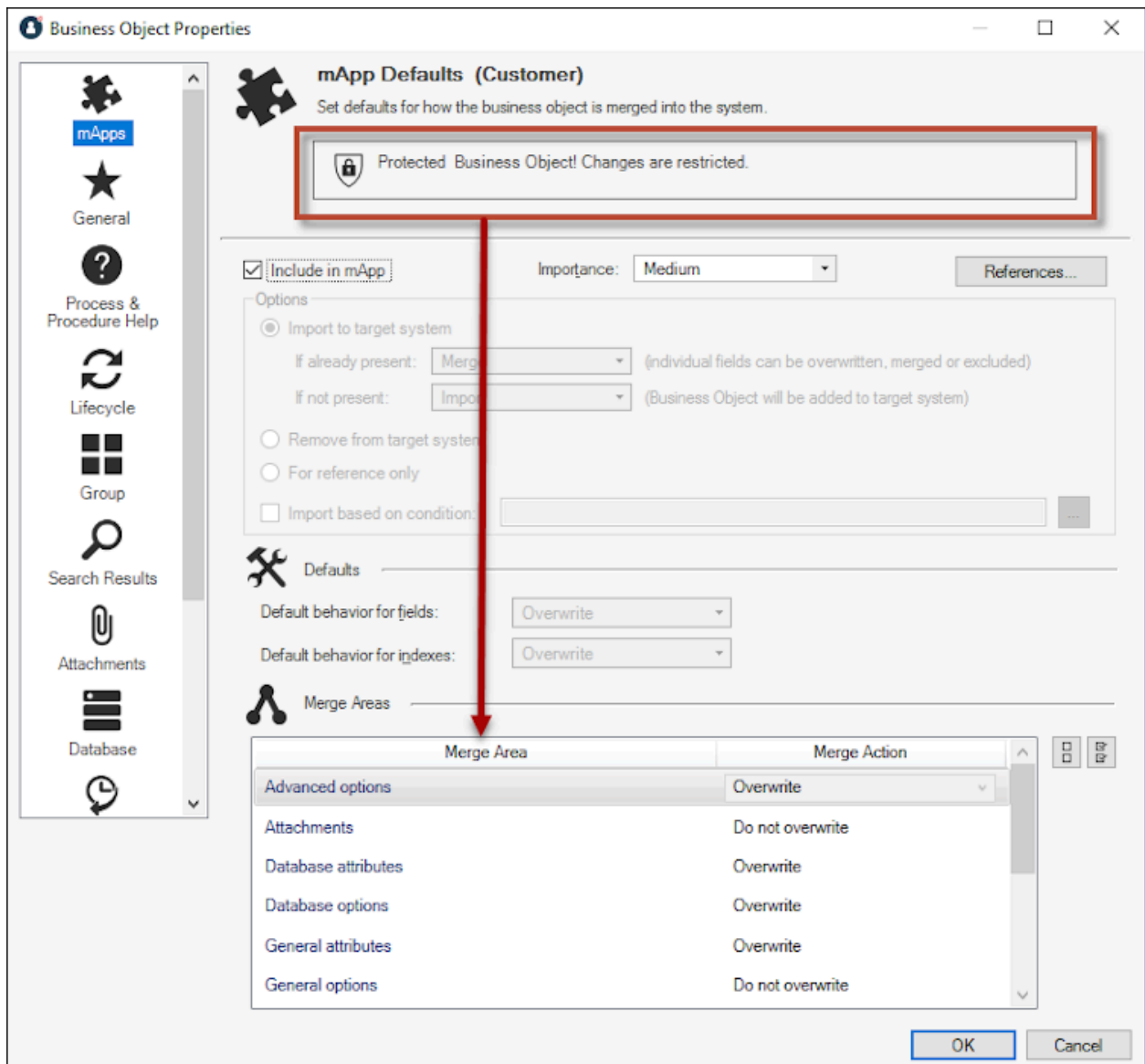
If you configuring merge actions for a Business Object that was previously applied as part of a Protected mApp Solution, the main differences are:

- You see a message saying `Protected Business Object! Changes are restricted.`
- If you select the **Include in mApp** check box, all **Import to target system** options are greyed out and merge actions cannot be changed.

For more information, see: Protected mApp™ Solutions.

Define Merge Actions for General Business Object Properties

Use the **General** page in the **Business Object Properties** window to define overwrite options for the following general properties for a Business Object:

- Name and description.
- General options: Public ID, Business Object type, tracking options, menus and shortcut keys, and various options for defining a Business Object's behavior and where it appears in CSM.

> **Note:** The **Business Object Properties** window is available in the Business Object Editor (accessed from within the Object Manager in the mApp Solution Editor).

Good to know:

- You can only configure separate merge actions for individual Business Object properties and areas if the Business Object is set to **Merge** in the **Business Object Properties** window (mApp Solutions page). If the Business Object is set to any other option, or if the **Include in mApp Solution** check box is cleared, then you cannot configure separate merge actions for individual properties or areas.
- If you are configuring merge actions for a Business Object that was previously applied as part of a Protected mApp Solution, the main differences are:
  - You see a message saying `Protected Business Object! Changes are restricted`.
  - Some fields and options are not available to be changed.
  - See Protected mApp™ Solutions.
- For more information about defining general Business Object properties, refer to Define General Properties for a Business Object.

To define merge actions for general Business Object properties:

1. Add a Business Object to a mApp Solution using the Add Business Object to mApp Solution Wizard.
2. Open the **Business Object Properties** window for the Business Object you just added to the mApp Solution:
   a. In the Object Manager within the mApp Editor, select the **Edit Business Object** task in the Structure area.

   The Business Object Editor opens.

   Tip: You can also select **Business Object** 🔲 on the mApp Editor toolbar to open the Business Object Editor.

   b. Select **Bus Ob Properties**.
3. Set the Business Object to Merge:
   a. Select the **mApps** page, and then select the **Include in mApp** check box.

b. In the Options area, select the **Import to Target System** option.

c. In the **If Already Present** drop-down list, select **Merge** as the merge action for the Business Object.

4. Select the **General** page.

5. Select **mApp** ![icon] next to each property merge area, and then select a merge action:

   For general Business Object information (name and description):

   ◦ **Do Not Overwrite Name and Description:** Select this option to leave the Business Object's name and description unchanged in the target system when the mApp Solution is applied.

   ◦ **Overwrite Name and Description:** Select this option to overwrite the Business Object's name and description in the target system when the mApp Solution is applied.

   For general Business Object options:

   ◦ **Do Not Overwrite General Options:** Select this option to leave the Business Object's general options unchanged in the target system when the mApp Solution is applied.

   ◦ **Overwrite General Options:** Select this option to overwrite the Business Object's general options in the target system when the mApp Solution is applied.

6. Select **OK**.

7. Prepare the mApp Solution for Distribution (**File > Prepare mApp for Distribution**), or save the mApp Solution (**File > Save mApp to Disk**) to continue making other changes.

Define Merge Actions for Business Object Process and Procedure Help Properties

Set merge actions for Business Object Process and Procedure Help Properties.

Use the **Process and Procedure Help** page in the **Business Object Properties** window to define overwrite options for process and procedure help properties of a Business Object.

> 🖉 **Note:** The **Business Object Properties** window is available in the Business Object Editor (accessed from within the Object Manager in the mApp Editor).

Good to know:

- You can only configure separate merge actions for individual Business Object properties and areas if the Business Object is set to **Merge** in the **Business Object Properties** window (mApp® Solution page). If the Business Object is set to any other option, or if the **Include in mApp** check box is cleared, then you cannot configure separate merge actions for individual properties or areas.
- If you do not see the **Process and Procedure Help** page, close the mApp Solution (after saving) and go to **Settings > Edit System Settings**. Select the **Help** page, and then select **Show Process and Terminology Help**. For more information about enabling process and procedure help, refer to Configure Global Help Settings.
- If you are configuring merge actions for a Business Object that was previously applied as part of a Protected mApp Solution, the main differences are:
    - You see a message saying `Protected Business Object! Changes are restricted`.
    - Some fields and options are not available to be changed.
    - See Protected mApp™ Solutions.
- For more information about defining process and procedure help properties for a Business Object, refer to Define Process and Procedure Help Properties for a Business Object.

To define merge actions for Business Object process and procedure help properties:

1. Add a Business Object to a mApp using the Add Business Object to mApp Solution Wizard.

2. Open the **Business Object Properties** window for the Business Object you just added to the mApp Solution:
    a. In the Object Manager within the mApp Editor, select the **Edit Business Object** task in the **Structure** area.

    The Business Object Editor opens.

    Tip: You can also select **Business Object** 📦 on the mApp Editor toolbar to open the Business Object Editor.

      b. Select **Bus Ob Properties**.

3. Set the Business Object to Merge:

    a. Select the **mApps** page, and then select the **Include in mApp** check box.

    b. In the Options area, select the **Import to Target System** option.

       In the **If Already Present** drop-down list, select **Merge** as the merge action for the Business Object.

4. Select the **Process and Procedure Help** page.

5. Select **mApp** ![icon], and then select a merge action:

    ◦ **Do Not Overwrite Process and Procedure Options:** Select this option to leave the Business Object's process and procedure help properties unchanged in the target system when the mApp Solution is applied.

    ◦ **Overwrite Process and Procedure Options:** Select this option to overwrite the Business Object's process and procedure help properties in the target system when the mApp Solution is applied.

6. Select **OK**.

7. Prepare the mApp Solution for Distribution (**File > Prepare mApp for Distribution**), or save the mApp Solution (**File > Save mApp to Disk**) to continue making other changes.

Define Merge Actions for Business Object Lifecycle Properties

Set merge actions for Business Object Lifecycle Properties.

Note for new Business Object lifecycle (CSM 10.2.0 or later)

Important: For CSM 10.2.0 or later versions, use the Business Object Lifecycle Editor to add a lifecycle to a Business Object. See: Open the Lifecycle Editor.

Use the **Lifecycle** page in the **Business Object Properties** window to define overwrite options for the lifecycle properties for a Business Object.

Note: The **Business Object Properties** window is available in the Business Object Editor (accessed from within the Object Manager in the mApp Editor).

Good to know:

- You can only configure separate merge actions for individual Business Object properties and areas if the Business Object is set to **Merge** in the **Business Object Properties** window (**mApp** page). If the Business Object is set to any other option, or if the **Include in mApp** check box is cleared, then you cannot configure separate merge actions for individual properties or areas.
- If you are configuring merge actions for a Business Object that was previously applied as part of a Protected mApp Solution, the main differences are:
  - You see a message saying `Protected Business Object! Changes are restricted`.
  - Some fields and options are not available to be changed.
  - See Protected mApp™ Solutions.
- For more information about defining lifecycle properties for a Business Object, refer to Define Lifecycle Properties for a Business Object.

To define merge actions for Business Object lifecycle properties:

1. Add a Business Object to a mApp using the Add Business Object to mApp Wizard.

2. Open the **Business Object Properties** window for the Business Object you just added to the mApp® Solution:
   a. In the Object Manager within the mApp Editor, select the **Edit Business Object** task in the Structure area.
      The Business Object Editor opens.

      Tip: You can also select **Business Object** ⬡ on the mApp Editor toolbar to open the Business Object Editor.

   b. Select **Bus Ob Properties**.

3. Set the Business Object to Merge:
   a. Select the **mApps** page, and then select the **Include in mApp** check box.

   b. In the **Options** area, select the **Import to Target System** option.

   c. In the **If Already Present** drop-down list, select **Merge** as the merge action for the Business Object.

4. Select the **Lifecycle** page.

5. Select **mApp** [icon], and then select a merge action:
   ◦ **Do Not Overwrite Lifecycle Options:** Select this option to leave the Business Object's lifecycle properties unchanged in the target system when the mApp Solution is applied.

   ◦ **Overwrite Lifecycle Options:** Select this option to overwrite the Business Object's lifecycle properties in the target system when the mApp Solution is applied.

6. Select **OK**.

7. Publish the Blueprint (**File > Publish Blueprint**) to commit the changes, or save the Blueprint (**File > Save Blueprint**) to continue making other changes.

Related concepts

About Business Object Lifecycles

Open the Lifecycle Editor

Define Merge Actions for Business Object Search Results Properties

Set merge actions for Business Object Search Results Properties.

Use the **Search Results** page in the **Business Object Properties** window to define overwrite options for Search Result properties for a Business Object.

✎ **Note:** The **Business Object Properties** window is available in the Business Object Editor (accessed from within the Object Manager in the mApp Editor).

Good to know:

- You can only configure separate merge actions for individual Business Object properties and areas if the Business Object is set to **Merge** in the **Business Object Properties** window (**mApp** page). If the Business Object is set to any other option, or if the **Include in mApp** check box is cleared, then you cannot configure separate merge actions for individual properties or areas.
- If you are configuring merge actions for a Business Object that was previously applied as part of a Protected mApp Solution, the main differences are:
  - You see a message saying `Protected Business Object! Changes are restricted.`
  - Some fields and options are not available to be changed.
  - See Protected mApp™ Solutions.
- For more information about defining Search Results properties for a Business Object, refer to Define Search Results Properties for a Business Object.

To define merge actions for Business Object Search Results properties:

1. Add a Business Object to a mApp using the Add Business Object to mApp Solution Wizard.
2. Open the **Business Object Properties** window for the Business Object you just added to the mApp® Solution:
   a. In the Object Manager within the mApp Editor, select the **Edit Business Object** task in the **Structure** area.

   The Business Object Editor opens.

   Tip: You can also select **Business Object** 🔲 on the mApp Editor toolbar to open the Business Object Editor.

   b. Select **Bus Ob Properties**.
3. Set the Business Object to Merge:
   a. Select the **mApps** page, and then select the **Include in mApp** check box.
   b. In the **Options** area, select the **Import to Target System** option.

      c. In the **If Already Present** drop-down list, select **Merge** as the merge action for the Business Object.

4. Select the **Search Results** page.

5. Select **mApp** , and then select a merge action:

    ◦ **Do Not Overwrite Search Result Options:** Select this option to leave the Business Object's Search Result properties unchanged in the target system when the mApp Solution is applied.

    ◦ **Overwrite Search Result Options:** Select this option to overwrite the Business Object's Search Result properties in the target system when the mApp Solution is applied.

6. Select **OK**.

7. Prepare the mApp Solution for Distribution (**File > Prepare mApp for Distribution**), or save the mApp Solution (**File > Save mApp to Disk**) to continue making other changes.

Define Merge Actions for Business Object Attachment Properties

Set merge actions for Business Object Attachment Properties.

Use the **Attachments** page in the **Business Object Properties** window to define overwrite options for Attachment properties for a Business Object.

> ✎ **Note:** The **Business Object Properties** window is available in the Business Object Editor (accessed from within the Object Manager in the mApp Editor).

Good to know:

- You can only configure separate merge actions for individual Business Object properties and areas if the Business Object is set to **Merge** in the **Business Object Properties** window (**mApp** page). If the Business Object is set to any other option, or if the **Include in mApp** check box is cleared, then you cannot configure separate merge actions for individual properties or areas.
- If you are configuring merge actions for a Business Object that was previously applied as part of a Protected mApp Solution, the main differences are:
    - You see a message saying `Protected Business Object! Changes are restricted`.
    - Some fields and options are not available to be changed.
    - See Protected mApp™ Solutions.
- For more information about defining Attachment properties for a Business Object, refer to Define Attachments Properties for a Business Object.

To define merge actions for Attachment properties:

1. Add a Business Object to a mApp using the Add Business Object to mApp Wizard.

2. Open the **Business Object Properties** window for the Business Object you just added to the mApp® Solution:
    a. In the Object Manager within the mApp Editor, select the **Edit Business Object** task in the Structure area.

    The Business Object Editor opens.

    Tip: You can also select **Business Object** 🔲 on the mApp Editor toolbar to open the Business Object Editor.

    b. Select **Bus Ob Properties**.

3. Set the Business Object to Merge:
    a. Select the **mApps** page, and then select the **Include in mApp** check box.

    b. In the **Options** area, select the **Import to Target System** option.

     c. In the **If Already Present** drop-down list, select **Merge** as the merge action for the Business Object.

4. Select the **Attachments** page.

5. Select **mApp** ![icon], and then select a merge action:
   - **Do Not Overwrite Attachment Options:** Select this option to leave the Business Object's Attachment options unchanged in the target system when the mApp Solution is applied.

   - **Overwrite Attachment Options:** Select this option to overwrite the Business Object's Attachment options in the target system when the mApp Solution is applied.

6. Select **OK**.

7. Prepare the mApp Solution for Distribution (**File > Prepare mApp for Distribution**), or save the mApp Solution (**File > Save mApp to Disk**) to continue making other changes.

Define Merge Actions for Business Object Database Properties

Set merge action for Business Object Database Properties.

Use the **Database** page in the **Business Object Properties** window to define overwrite options for database properties and individual indexes for a Business Object.

> ✏️ **Note:** The **Business Object Properties** window is available in the Business Object Editor (accessed from within the Object Manager in the mApp Editor).

Good to know:

- You can only configure separate merge actions for individual Business Object properties and areas if the Business Object is set to **Merge** in the **Business Object Properties** window (**mApp** page). If the Business Object is set to any other option, or if the **Include in mApp** check box is cleared, then you cannot configure separate merge actions for individual properties or areas.

- If you are configuring merge actions for a Business Object that was previously applied as part of a Protected mApp Solution, the main differences are:
    - You see a message saying `Protected Business Object! Changes are restricted.`
    - Some fields and options are not available to be changed.
    - See Protected mApp™ Solutions.

- For more information about defining database properties for a Business Object, refer to Define Database Properties for a Business Object.

To define merge actions for Business Object database properties:

1. Add a Business Object to a mApp Solution using the Add Business Object to mApp Wizard.

2. Open the **Business Object Properties** window for the Business Object you just added to the mApp® Solution:
    a. In the Object Manager within the mApp Editor, select the **Edit Business Object** task in the **Structure** area.

    The Business Object Editor opens.

    Tip: You can also select **Business Object** 📦 on the mApp Editor toolbar to open the Business Object Editor.

    b. Select **Bus Ob Properties**.

3. Set the Business Object to Merge:
    a. Select the **mApps** page, and then select the **Include in mApp** check box.

    b. In the **Options** area, select the **Import to Target System** option.

    c. In the **If Already Present** drop-down list, select **Merge** as the merge action for the Business Object.

4. Select the **Database** page.

5. Select **mApp** ![icon] next to each property merge area, and then select a merge action:

    For database options:

      ◦ **Do Not Overwrite Database Options:** Select this option to leave the Business Object's database options unchanged in the target system when the mApp Solution is applied.

      ◦ **Overwrite Database Options:** Select this option to overwrite the Business Object's database options in the target system when the mApp Solution is applied.

    For an index:

      ◦ **Do Not Overwrite Index:** Select this option to leave an index unchanged in the target system when the mApp Solution is applied.

   ◦ **Overwrite Index:** Select this option to overwrite an index in the target system when the mApp Solution is applied.

6. Select **OK**.

7. Prepare the mApp Solution for Distribution (**File > Prepare mApp for Distribution**), or save the mApp Solution (**File > Save mApp to Disk**) to continue making other changes.

Define Merge Actions for Business Object History Properties

Set merge actions for Business Object History Properties.

Use the **History** page in the **Business Object Properties** window to define overwrite ootions for history tracking properties for a Business Object.

✏️ **Note:** The **Business Object Properties** window is available in the Business Object Editor (accessed from within the Object Manager in the mApp Editor).

Good to know:

- You can only configure separate merge actions for individual Business Object properties and areas if the Business Object is set to **Merge** in the **Business Object Properties** window (**mApp** page). If the Business Object is set to any other option, or if the **Include in mApp** check box is cleared, then you cannot configure separate merge actions for individual properties or areas.
- If you are configuring merge actions for a Business Object that was previously applied as part of a Protected mApp Solution, the main differences are:
    - You see a message saying `Protected Business Object! Changes are restricted.`
    - Some fields and options are not available to be changed.
    - See Protected mApp™ Solutions.
- For more information about defining history properties for a Business Object, refer to Define History Properties for a Business Object.

To define history properties for a Business Object:

1. Add a Business Object to a mApp Solution using the Add Business Object to mApp Wizard.

2. Open the **Business Object Properties** window for the Business Object you just added to the mApp® Solution:
    a. In the Object Manager within the mApp Editor, select the **Edit Business Object** task in the **Structure** area.

       The Business Object Editor opens.

       Tip: You can also select **Business Object** 📦 on the mApp Editor toolbar to open the Business Object Editor.

    b. Select **Bus Ob Properties**.

3. Set the Business Object to Merge:
    a. Select the **mApps** page, and then select the **Include in mApp** check box.

    b. In the **Options** area, select the **Import to Target System** option.

     c. In the **If Already Present**, select **Merge** as the merge action for the Business Object.

4. Select the **History** page.

5. Select **mApp** ![icon], and then select a merge action:
   - **Do Not Overwrite History Options:** Select this option to leave the Business Object's history properties unchanged in the target system when the mApp Solution is applied.

   - **Overwrite History Options:** Select this option to overwrite the Business Object's history properties in the target system when the mApp Solution is applied.

6. Select **OK**.

7. Prepare the mApp Solution for Distribution (**File > Prepare mApp for Distribution**), or save the mApp Solution (**File > Save mApp to Disk**) to continue making other changes.

Define Merge Actions for Business Object Record Locking Settings

Set merge actions for Business Object Record Locking Settings.

Use the **Record Locking** page in the **Business Object Properties** window to define overwrite options for record locking settings for a Business Object.

> ✏️ **Note:** The **Business Object Properties** window is available in the Business Object Editor (accessed from within the Object Manager in the mApp Solution Editor).

Good to know:

- You can only configure separate merge actions for individual Business Object properties and areas if the Business Object is set to **Merge** in the **Business Object Properties** window (**mApp** page). If the Business Object is set to any other option, or if the **Include in mApp** check box is cleared, then you cannot configure separate merge actions for individual properties or areas.
- For more information about defining Record Locking settings for a Business Object, refer to Define Record Locking Settings for a Business Object.

To define merge actions for Record Locking settings:

1. Add a Business Object to a mApp Solution using the Add Business Object to mApp Wizard.

2. Open the **Business Object Properties** window for the Business Object you just added to the mApp® Solution:
   a. In the Object Manager within the mApp Editor, select the **Edit Business Object** task in the **Structure** area.

      The Business Object Editor opens.

      Tip: You can also select **Business Object** [icon] on the mApp Editor toolbar to open the Business Object Editor.

   b. Select **Bus Ob Properties**.

3. Set the Business Object to Merge:
   a. Select the **mApps** page, and then select the **Include in mApp** check box.

   b. In the **Options** area, select the **Import to Target System** option.

   c. In the **If Already Present** drop-down list, select **Merge** as the merge action for the Business Object.

4. Select the **Record Locking** page.

5. Select **mApp** [icon], and then select a merge action:

- ◦ **Do Not Overwrite Record Locking Options:** Select this option to leave the Business Object's Record Locking settings unchanged in the target system when the mApp Solution is applied.

- ◦ **Overwrite Record Locking Options:** Select this option to overwrite the Business Object's Record Locking settings in the target system when the mApp Solution is applied.

6. Select **OK**.

7. Prepare the mApp Solution for Distribution (**File > Prepare mApp for Distribution**), or save the mApp Solution (**File > Save mApp to Disk**) to continue making other changes.

Define Merge Actions For Business Object Localization Settings

Set merge actions for Business Object Record Localization settings.

Use the **Localization** page in the **Business Object Properties** window to define overwrite options for localization settings for a Business Object.

The **Business Object Properties** window is available in the Business Object Editor (accessed from within the Object Manager in the mApp Editor).

For more information about defining localization settings for a Business Object, refer to Define Localization Properties for a Business Object.

To define merge actions for localization settings:

1. Follow steps 1 — 3 from Configure Merge Actions for Business Objects; refer to Configure Merge Actions for Business Objects.

2. To set the Business Object to Merge, select **Include in mApp**.
   a. In the **Options** area, select the **Import to Target System** option.

   b. In the **If already present** drop-down list, select **Merge**.

   c. Select the **Localization** page

3. Select **mApp** [ ], and then select a merge action:
   ◦ **Do not overwrite localization options**: Select this option to leave the Business Object's localization settings unchanged in the target system when the mApp Solution is applied.

   ◦ **Overwrite localization options**: Select this option to overwrite the Business Object's localization settings in the target system when the mApp Solution is applied.

4. Select **OK**.

5. Prepare the mApp Solution for distribution (**File > Prepare mApp for distribution**), or save the mApp Solution (**File > Save mApp to disk**) to continue making changes. For more information, see Save a mApp Solution.

Related concepts

Business Object Editor

Object Manager

mApp Editor

Add a Business Object to a mApp Solution

Prepare a mApp Solution for Distribution

Define Merge Actions for Advanced Business Object Properties

Set merge actions for Advanced Business Object Properties.

Use the **Advanced** page in the **Business Object Properties** window (accessed from within the mApp Solution Editor) to define overwrite options for the following advanced properties:

- Advanced Options: Whether the Business Object is read-only, cacheable, or has an associated color.
- General Attributes.
- Database Attributes.

> **Note:** The **Business Object Properties** window is available in the Business Object Editor (accessed from within the Object Manager in the mApp Editor).

Good to know:

- You can only configure separate merge actions for individual Business Object properties and areas if the Business Object is set to **Merge** in the **Business Object Properties** window (**mApp** page). If the Business Object is set to any other option, or if the **Include in mApp** check box is cleared, then you cannot configure separate merge actions for individual properties or areas.
- Only advanced Users should define attributes. For more information about attributes, please contact Cherwell Support.
- If you are configuring merge actions for a Business Object that was previously applied as part of a Protected mApp Solution, the main differences are:
  - You see a message saying `Protected Business Object! Changes are restricted`.
  - Some fields and options are not available to be changed.
  - See Protected mApp™ Solutions.
- For more information about defining advanced properties for a Business Object, refer to Define Advanced Properties for a Business Object.

To define merge actions for advanced Business Object properties:

1. Add a Business Object to a mApp Solution using the Add Business Object to mApp Wizard.

2. Open the **Business Object Properties** window for the Business Object you just added to the mApp® Solution:
   a. In the Object Manager within the mApp Editor, select the **Edit Business Object** task in the **Structure** area.

      The Business Object Editor opens.

> **Tip:** You can also select **Business Object** ⬡ on the mApp Editor toolbar to open the Business Object Editor.

      b. Select **Bus Ob Properties**.

3. Set the Business Object to Merge:

      a. Select the **mApps** page, and then select the **Include in mApp** check box.

      b. In the **Options** area, select the **Import to Target System** option.

      c. In the **If Already Present** drop-down list, select **Merge** as the merge action for the Business Object.

4. Select the **Advanced** page.

5. Select **mApp** ✳ next to each property merge area, and then select a merge action:

For advanced options:

- **Do not overwrite advanced options:** Select this option to leave the advanced options unchanged in the target system when the mApp Solution is applied.
- **Overwrite advanced options:** Select this option to overwrite the advanced options in the target system when the mApp Solution is applied.

For general attributes:

- **Do not overwrite general attributes:** Select this option to leave the general attributes unchanged in the target system when the mApp Solution is applied.
- **Overwrite general attributes:** Select this option to overwrite the general attributes in the target system when the mApp Solution is applied.

For database attributes:

- **Do not overwrite database attributes:** Select this option to leave the database attributes unchanged in the target system when the mApp Solution is applied.
- **Overwrite database attributes:** Select this option to overwrite the database attributes in the target system when the mApp Solution is applied.

6. Select **OK**.

7. Prepare the mApp Solution for Distribution (**File > Prepare mApp for Distribution**), or save the mApp Solution (**File > Save mApp to Disk**) to continue making other changes.

Configure Merge Actions for Individual Fields

Use the **mApp Action** context menu in the Business Object Editor within a mApp Solution to configure merge actions for individual Business Object fields. You can also use the **Field Properties** window to configure merge actions for individual fields, as well as for field properties.

Good to know:

- You can only configure separate merge actions for individual Business Object fields and field properties if the Business Object is set to Merge in the **Business Object Properties** window (**mApp** page). If the Business Object is set to any other option, or if **Include in mApp** is cleared, then you cannot configure separate merge actions for individual field properties.

- If you are configuring merge actions for Business Object fields that were previously applied as part of a Protected mApp™ Solution, the main differences are:

  ◦ You see a shield icon [shield icon] next to each content-protected field.

  ◦ If a Business Object field is content-protected, it cannot be deleted. This includes menu, context menu, toolbar, and related buttons.

  ◦ Default fields in a content-protected Business Object cannot be edited in any way but you can add new fields and then edit or delete them.

  ◦ When a Business Object is content-protected, you can increase its field length from the default and decrease it back to the original default length.

  ◦ You can use a content-protected Business Object property field in a Full Text Search by selecting the check box on the **Search Results** page.

  ◦ See Protected mApp™ Solutions.

To configure merge actions for individual Business Object fields:

1. Add a Business Object to a mApp Solution using the Add Business Object to mApp Wizard.

2. In the Object Manager within the mApp Editor, select the **Business Object** from the Object tree, and then select the **Edit Business Object** task in the **Structure** area.

   [pencil icon] **Note:** You can also select **Business Object** [icon] on the mApp Editor toolbar to open the Business Object Editor.

   The Business Object Editor opens, displaying the list of fields with a **mApp Action** column to show which fields you selected to overwrite and which ones you selected not to overwrite (blank in the **mApp Action** column) in the Add Business Object to mApp Wizard. If you set the Business Object to **Merge** in the **Business Object Properties** window, then the selections made in the **Defaults** section (**Default Behavior for Fields** drop-down list) are also reflected in the **mApp Action** column.

Name	Type	Size	mApp Action	Details
RecID	Text	42	⚠ Overwrite	Category=System, Default: NewID()
Incident ID	Text	20	⚠ Overwrite	Full-text, Default: conditional
Created Date Time	Date/Time	Date and Time	⚠ Overwrite	Default: CurrentDateTime()
Created During	Text	30	⚠ Overwrite	Calculated
Created By	Text	50	⚠ Overwrite	Default: CurrentUserDisplayName()
Created By ID	Text	42	⚠ Overwrite	Category=System, Default: CurrentUserRecordID()
Status	Text	30	⚠ Overwrite	Full-text, Default: conditional, Validated from Incident Status.Status
Status Description	Text	100	⚠ Overwrite	Full-text, Category=Status, Auto-filled
Service	Text	50	⚠ Overwrite	Validated from Service.Service Name
Category	Text	30	⚠ Overwrite	Full-text, Validated from Incident Category.Incident Category
Subcategory	Text	30	⚠ Overwrite	Full-text, Validated from Incident SubCategory.Subcategory
SpecificsTypeId	Text	42	⚠ Overwrite	Category=System, Auto-filled
Description	Text	Maximum	⚠ Overwrite	Full-text, Required
Impact	Text	35	⚠ Overwrite	Full-text, Category=Common
Urgency	Text	35	⚠ Overwrite	Full-text, Category=Common
Priority	Text	15	⚠ Overwrite	Conditionally Required

3. Configure separate merge actions for individual fields (using the **mApp Action** context menu):
   a. Select a field, right-click in the **mApp Action** column, and then hover over **mApp Action** to open a context menu.

   Note: The **mApp Action** context menu is only available if the Business Object was set to Merge.

   b. Select a merge action for the field from the context menu:
      - **Make no changes to field:** Select this option to leave the existing definition in the target system unchanged (the mApp Solution definition is not imported into the target system when the mApp Solution is applied).

      - **Import field if not already there:** Select this option to import the field if it does not already exist in the target system. If it already exists, the field is not imported when the mApp Solution is applied.

      - **Overwrite field:** Select this option to have the mApp Solution definition overwrite the existing definition in the target system.

      - **Conditionally merge field properties:** This option is grayed out on the context menu because merging a field requires selecting separate merge actions for individual field property merge areas. This is done using the **Field Properties** window (see step 5).

      - **Remove field from target system:** Select this option to have the field removed from the target system.

      - **Field is reference-only:** Select this option to include the field in the mApp Solution for informational purposes only (the definition is not imported into the target system when the mApp Solution is applied). You should rarely (if ever) need to do this manually, as the system automatically adds definitions as necessary for reference only.

   The selected action shows in the mApp Solution status column (blank if you selected **Make no changes to Field**).

4. Configure separate merge actions for individual fields (using the **Field Properties** window):
   a. Select a field in the Business Object Editor, and then select **Field Properties**.
   b. Select the **mApps** page.
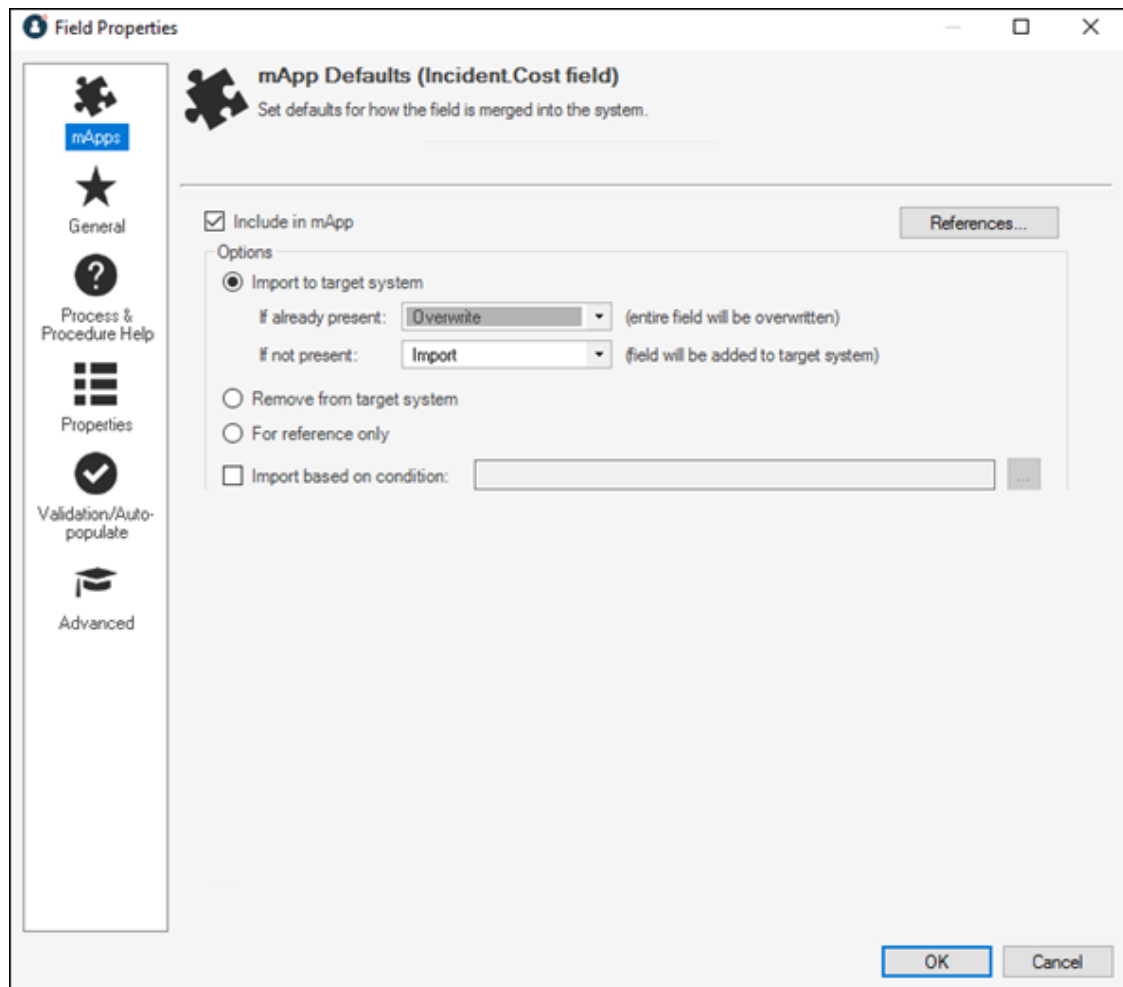
c. Define general mApp Solution properties for the field:
  ◦ **Include in mApp:** Select this check box to include the field in the mApp Solution. Clear this check box to leave the existing definition in the target system unchanged (the field is not imported into the target system when the mApp Solution is applied).

    Note: This check box is automatically selected if some or all of the fields were set to overwrite when the Business Object was added to the mApp Solution (using the Add Business Object to mApp Wizard), or if you selected anything besides **Make no changes to field** in the **mApp Action** context menu.

  ◦ **References:** Select this button to open the References window and view all of the other definitions being used by the field.
d. Define options (merge actions) for how the definition will be merged into a target system:

  Note: These options are only available if **Include in mApp** is selected.

- **Import to target system:** Select this option to import the definition into a target system. Then, select a merge action based on whether or not the definition is already present in the target system:

  If already present: In the drop-down list, select a merge action to define how the definition is imported if it already exists in a target system:

  - **Overwrite:** Select this option to have the mApp Solution definition overwrite the existing definition in the target system.
  - **Don't Import:** Select this option to leave the existing definition in the target system unchanged (the mApp Solution definition is not imported into the target system when the mApp Solution is applied).
  - **Merge:** Select this option to define separate merge actions for each individual area of a definition.

  If not present: In the drop-down list, select a merge action to define whether the definition is imported if it does not currently exist in the target system:

  - **Import:** Select this option to import the mApp Solution definition into the target system if does not already exist.
  - **Don't Import:** Select this option to skip importing the mApp Solution definition into the target system if it does not already exist (the mApp Solution definition will not be added to the target system).

- **Remove from Target System:** Select this option to remove the definition from a target system.

- **For Reference Only:** Select this option to include the definition in the mApp Solution for informational purposes only (the definition is not imported into the target system when the mApp Solution is applied).

- **Import/Remove Based on Condition:** Select this check box to import or remove the definition based on a condition. Then, select the ellipsis [...] to open the **mApp Conditions** window and define mApp Solution conditions.

  Note: The action you selected from the **mApp Action** context menu is automatically selected.

5. Configure separate merge actions for individual field property merge areas:
   a. In the **Options** area of the **Field Properties** window, select **Import to Target System** .

   b. Select **Merge** as the merge action for the field from the **If Already Present** drop-down list.

c. Define individual merge actions for each merge area:

In the Merge Areas Grid: For each merge area, select a merge action in the **Merge Action** column drop-down lists:

- **Overwrite:** Select this option to have the merge area overwritten in the target system when the mApp Solution is applied.

- **Do Not Overwrite:** Select this option to leave the merge area unchanged in the target system when the mApp Solution is applied.

Tip: Select **Uncheck All** to set all merge areas to **Do Not Overwrite**. Select **Select All** to set all merge areas to **Overwrite**.

On the remaining pages of the properties window: Select **mApp** next to each of the merge areas to define merge actions for individual properties:

       i. Define merge actions for General field properties.

      ii. Define merge actions for Field process and procedure help properties.

     iii. Define merge actions for Field behavior properties.

     iv. Define merge actions for Field validation/auto-population properties.

      v. Define merge actions for Field advanced properties.

d. Select **OK**.

The selections you made in the **Options** area are reflected in the Business Object Editor Grid.

6. Prepare the mApp Solution for Distribution (**File > {Prepare mApp for Distribution**), or save the mApp Solution (**File > Save mApp to Disk**) to continue making other changes.

Define Merge Actions for General Field Properties

Use the **General** page in the **Field Properties** window to define whether or not to overwrite the following general property merge areas for a field:

- Name and description.
- Field type (Date/Time, Logical, Number, or Text) and field properties based on type (size, format, decimal places, etc.).

> **Note:** The **Field Properties** window is available in the Business Object Editor (accessed from within the Object Manager in the mApp Editor).

Good to know:

- You can only configure separate merge actions for individual Business Object fields and field properties if the Business Object is set to Merge in the **Business Object Properties** window (**mApp** page). If the Business Object is set to any other option, or if **Include in mApp** is cleared, then you cannot configure separate merge actions for individual field properties.
- For more information about defining general field properties, refer to Define General Properties for a Field.
- If you are configuring merge actions for Business Object fields that were previously applied as part of a Protected mApp™ Solution, the main differences are:
  - You see a shield icon ⊕ next to each content-protected field.
  - If a Business Object field is content-protected, it cannot be deleted. This includes menu, context menu, toolbar, and related buttons.
  - Default fields in a content-protected Business Object cannot be edited in any way but you can add new fields and then edit or delete them.
  - When a Business Object is content-protected, you can increase its field length from the default and decrease it back to the original default length.
  - You can use a content-protected Business Object property field in a Full Text Search by selecting the check box on the **Search Results** page.
  - See Protected mApp™ Solutions.

To define merge actions for general field properties:

1. Add a Business Object to a mApp Solution using the Add Business Object to mApp wizard.
2. Open the **Field Properties** window for a field in the Business Object you just added to the mApp Solution:
   a. In the Object Manager within the mApp Editor, select the **Edit Business Object** task in the **Structure** area.
   The Business Object Editor opens, displaying the list of fields with a **mApp Action** column to show the merge actions selected for the fields in the Add Business Object to mApp wizard (either **Overwrite** or **Do Not Overwrite**. The **mApp Action** column is blank for fields set to **Do Not Overwrite**). If you set the Business Object to **Merge** in the **Business Object Properties**

window (**mApp** page), then the selections made in the **Defaults** section (**Default Behavior for Fields** drop-down list) are also reflected in the **mApp Action** column.

> **Tip:** You can also select **Edit Business Object** [icon] on the mApp Editor toolbar to open the Business Object Editor.

    b. Select a field, and then select the **Field Properties** button.

3. Set the individual field to Merge:
    a. Select the **mApp** page, and then select **Include in mApp**.

    b. In the **Options** area, select **Import to Target System**.

    c. From the **If Already Present** drop-down list, select **Merge** as the merge action for the field.

4. Select the **General** page.

5. Select **mApp** [icon] next to each property merge area to open a drop-down list of merge actions.

6. Select a merge action for general field information (name and description):
   ◦ **Do not overwrite name and description:** Select this option to leave the field's name and description unchanged in the target system when the mApp Solution is applied.

   ◦ **Overwrite name and description:** Select this option to overwrite the field's name and description in the target system when the mApp Solution is applied.

7. Select a merge action for general field properties (merge actions vary based on field type):
   ◦ For all field types:
      ◦ **Overwrite field type:** Select this option to have the field type (Date/Time, Logical, Number, or Text) overwritten in the target system when the mApp Solution is applied.

      ◦ **Overwrite track changes to field:** Select this option to have the field's change tracking options overwritten in the target system when the mApp Solution is applied.

   ◦ For date/time fields, select from the following additional options:
      ◦ **Overwrite date format:** Select this option to have the date format overwritten in the target system when the mApp Solution is applied. This overwrites the general properties for a date/time field (whether it holds date and time, date only, time only, or a timestamp and whether it is adjusted based on timezones).

   ◦ For number fields, select from the following additional options:
      ◦ **Overwrite field Size:**
         ◦ **Do not change size of target field:** Select this option to leave the field size unchanged in the target system when the mApp Solution is applied.

         ◦ **Make target field exactly <n> digits:** Select this option to overwrite the field size in the target system to be the exact size defined for the field in the mApp Solution (the exact number of whole digits and decimal digits specified for the field).

         ◦ **If target field is less than <n> digits, make it <n> digits:** Select this option to overwrite the field size in the target system if it is smaller than the size defined for the field in the mApp Solution (the number of whole digits and decimal digits specified for the field).

      ◦ **Overwrite negative number setting:** Select this option to overwrite the negative number setting in the target system when the mApp Solution is applied. This setting defines whether negative numbers are allowed in the field.

      ◦ **Overwrite currency settings:** Select this option to overwrite the currency settings in the target system when the mApp Solution is applied. These settings define whether the field holds currency values and which currency symbol is used.

   ◦ For text fields (either plain text or rich text), select from the following additional options:
      ◦ **Overwrite plain text/rich text Setting:** Select this option to overwrite the plain text/rich text setting in the target system when the mApp Solution is applied. This setting defines whether the field is plain text (does not contain any special formatting, images, etc.) or rich text (can contain special formatting, images).

      ◦ **Overwrite spell-check setting:** Select this option to overwrite the spell-check setting in the target system when the mApp Solution is applied. This setting defines whether the system checks for spelling errors in the field's content.

- **Overwrite Full-Text Search option:** Select this option to overwrite the Full-Text Search setting in the target system when the mApp Solution is applied. This setting defines whether the field is indexed for Full-Text Search (used by CSM Quick Search and Knowledge Search).
- **Overwrite holds selection:** Select this option to overwrite the field's hold property in the target system when the mApp Solution is applied. The hold property identifies the type of data contained in the field (example: A record ownership "Holds" property on an **Owned By Field** identifies the name in the field as a record owner).
  - For plain text fields, select from the following additional options:
    - **Overwrite field size:**
      - **Do not change size of target field:** Select this option to leave the field size unchanged in the target system when the mApp Solution is applied.
      - **Make target field exactly <defined size>:** Select this option to overwrite the field size in the target system with the field size defined in the mApp Solution. The defined size can be an exact length (the specified number of characters), the maximum allowed size, or the maximum searchable size.
      - **(If an exact length is defined) If target field is less than <n> characters, make it <n> characters:** Select this option to overwrite the field size in the target system if it is smaller than the field length defined in the mApp Solution (the number of characters specified for the field). When the mApp Solution is applied, the target field size is overwritten with the field length defined in the mApp Solution (the exact number of characters).
      - **(If specific length is defined) If target field is less than <n> or max length, make it <n> characters:** Select this option to overwrite the field size in the target system if it is smaller than the defined length or the maximum allowed size for the field. When the mApp Solution is applied, the target field size is overwritten with the field length defined in the mApp Solution (the exact number of characters).
      - **(If max allowed or max searchable is defined) If target field is less than maximum size/maximum searchable size, make it maximum size/maximum searchable size** (whichever is selected for the field in the mApp Solution): Select this option to overwrite the field size in the target system if it is smaller than the maximum allowed size/maximum searchable size for the field. When the mApp Solution is applied, the target field size is overwritten with the field size defined in the mApp Solution (either maximum allowed or maximum searchable).
      - **(If max searchable is defined) If target field is less than maximum searchable size or is maximum size, make it maximum searchable size:** Select this option to overwrite the field size in the target system if it is smaller than the maximum searchable size, or if it is the maximum allowed size for the field. When the mApp Solution is applied, the target field size is overwritten to be the maximum searchable size.
    - **Overwrite multiple line setting:** Select this option to overwrite the multiple line setting in the target system when the mApp Solution is applied. This setting defines whether the field can contain two or more lines of text.
    - **Overwrite format:** Select this option to overwrite the field's format. Plain text fields can have specified formats to enforce how characters and digits are displayed in the field.

◦ For rich text fields, select from the following additional options:

Note: For more information about rich text options, refer to Enable Rich Text on Business Object Fields.

- ◦ **Overwrite rich text field options:**
  - ◦ **Overwrite form image display:** Select this option to overwrite how embedded images are displayed in the field. When the mApp Solution is applied, the form image display setting for the target field is overwritten with the setting selected in the mApp Solution (from the **Form images are displayed as** drop-down list).
  - ◦ **Overwrite zoom image display:** Select this option to overwrite how embedded images are displayed in the rich text zoom window for the field. When the mApp Solution is applied, the zoomed image display setting for the target field is overwritten with the setting selected in the mApp Solution (from the **Zoomed images are displayed as** drop-down list).
  - ◦ **Overwrite image format:** Select this option to overwrite the default for how embedded images are displayed in the field. When the mApp Solution is applied, the image format for the target field is overwritten with the format selected in the mApp Solution (from the **Image format** drop-down list).
  - ◦ **Overwrite maximum size per image setting:** Select this option to overwrite the setting for the maximum size of a single image embedded into the field. When the mApp Solution is applied, the maximum size setting for the target field is overwritten with the format selected in the mApp Solution (whether the global setting is overridden with a different maximum size).
  - ◦ **Overwrite total size for images setting:** Select this option to overwrite the setting for the maximum size of all images embedded into the field. When the mApp Solution is applied, the maximum size setting for the target field is overwritten with the format selected in the mApp Solution (whether the global setting is overridden with a different maximum size).
  - ◦ **Overwrite allow User to override image display mode:** Select this option to overwrite the setting that allows users to override the image display mode for the field. When the mApp Solution is applied, the setting for the target field is overwritten with the selection in the mApp Solution (when **Allow user to override image display mode** is checked).
  - ◦ **Overwrite custom default font setting:** Select this check box to overwrite the custom default font setting for the field. When the mApp Solution is applied, the custom default font for the target field is overwritten with the custom default font defined for the field in the mApp Solution.

8. Select **OK**.

9. Prepare the mApp Solution for Distribution (**File > {Prepare mApp for Distribution**), or save the mApp Solution (**File > Save mApp to Disk**) to continue making other changes.

Define Merge Actions for Field Process and Procedure Help Properties

Use the **Process and Procedure Help** page in the **Field Properties** window to define whether or not to overwrite process and procedure help options.

Note: The **Field Properties** window is available in the Business Object Editor (accessed from within the Object Manager in the mApp Editor).

Good to know:

- You can only configure separate merge actions for individual Business Object fields and field properties if the Business Object is set to Merge in the **Business Object Properties** window (**mApp** page). If the Business Object is set to any other option, or if **Include in mApp** is cleared, then you cannot configure separate merge actions for individual field properties.

- If you do not see the **Process and Procedure Help** page, close the mApp Solution (after saving) and go to **Settings > Edit System Settings**. Select the **Help** page, and then check **Show Process and Terminology Help**. Refer to Configure Global Help Settings for more information.

- For more information about defining process and procedure help properties, refer to Define Process and Procedure Help Properties for a Field.

- If you are configuring merge actions for Business Object fields that were previously applied as part of a Protected mApp™ Solution, the main differences are:

  ◦ You see a shield icon 🛡 next to each content-protected field.

  ◦ If a Business Object field is content-protected, it cannot be deleted. This includes menu, context menu, toolbar, and related buttons.

  ◦ Default fields in a content-protected Business Object cannot be edited in any way but you can add new fields and then edit or delete them.

  ◦ When a Business Object is content-protected, you can increase its field length from the default and decrease it back to the original default length.

  ◦ You can use a content-protected Business Object property field in a Full Text Search by selecting the check box on the **Search Results** page.

  ◦ See Protected mApp™ Solutions.

To define merge actions for field process and procedure help properties:

1. Add a Business Object to a mApp Solution using the Add Business Object to mApp wizard.

2. Open the **Field Properties** window for a field in the Business Object you just added to the mApp Solution:
   a. In the Object Manager within the mApp Editor, select the **Edit Business Object** task in the **Structure** area.

The Business Object Editor opens, displaying the list of fields with a **mApp Action** column to show the merge actions selected for the fields in the Add Business Object to mApp wizard (either **Overwrite** or **Do Not Overwrite**. The **mApp Action** column is blank for fields set to **Do Not Overwrite**). If you set the Business Object to **Merge** in the **Business Object Properties** window (**mApps** page), then the selections made in the **Defaults** section (**Default Behavior for Fields** drop-down list) are also reflected in the **mApp Action** column.

> **Tip:** You can also select **Edit Business Object** on the mApp Editor toolbar to open the Business Object Editor.

    b. Select a field, and then select **Field Properties**.

3. Set the individual field to **Merge**:

    a. Select the **mApp** page, and then select **Include in mApp**.

    b. In the **Options** area, select **Import to Target System**.

    c. From the **If Already Present** drop-down list, select **Merge** as the merge action for the field.

4. Select the **Process and Procedure Help** page.

5. Select mApp Solution ![icon] , and then select a merge action:
   ◦ **Do not overwrite process and procedure options:** Select this option to leave the field's process and procedure help properties unchanged in the target system when the mApp Solution is applied.

   ◦ **Overwrite process and procedure options:** Select this option to overwrite the field's process and procedure help properties in the target system when the mApp Solution is applied.

6. Select **OK**.

7. Prepare the mApp Solution for Distribution (**File > {Prepare mApp for Distribution**), or save the mApp Solution (**File > Save mApp to Disk**) to continue making other changes.

Define Merge Actions for Detailed Field Properties

Use the **Properties** page in the **Field Properties** window to define whether or not to overwrite the following property merge areas:

- Whether the field is required.

- Whether the field is read-only.

- Values: Default and calculated values, as well as values to set before a Business Object is saved.

- Options based on lifecycle state: Behaviors and values based on the Business Object's lifecycle state (only applicable if the Business Object has defined lifecycle states).

> **Important:** For CSM 10.2.0 or later versions, use the Business Object Lifecycle Editor to add a lifecycle to a Business Object. See: Open the Lifecycle Editor.

> **Note:** The Field Properties window is available in the Business Object Editor (accessed from within the Object Manager in the mApp Editor).

Good to know:

- You can only configure separate merge actions for individual Business Object fields and field properties if the Business Object is set to Merge in the Business Object Properties window (mApp Solutions page). If the Business Object is set to any other option, or if *Include in mApp Solution* is cleared, then you cannot configure separate merge actions for individual Field properties.

- For more information about behavior properties, refer to Define Behavior Properties for a Field.

- If you are configuring merge actions for Business Object fields that were previously applied as part of a Protected mApp™ Solution, the main differences are:

  - You see a shield icon next to each content-protected field.

  - If a Business Object field is content-protected, it cannot be deleted. This includes menu, context menu, toolbar, and related buttons.

  - Default fields in a content-protected Business Object cannot be edited in any way but you can add new fields and then edit or delete them.

  - When a Business Object is content-protected, you can increase its field length from the default and decrease it back to the original default length.

  - You can use a content-protected Business Object property field in a Full Text Search by selecting the check box on the **Search Results** page.

  - See Protected mApp™ Solutions.

To define merge actions for field behavior properties:

1. Add a Business Object to a mApp Solution using the Add Business Object to mApp wizard.

2. Open the **Field Properties** window for a field in the Business Object you just added to the mApp Solution:

a. In the Object Manager within the mApp Editor, select the **Edit Business Object** task in the **Structure** area.

   The Business Object Editor opens, displaying the list of fields with a **mApp Action** column to show the merge actions selected for the fields in the Add Business Object to mApp wizard (either **Overwrite** or **Do Not Overwrite**. The **mApp Action** column is blank for fields set to **Do Not Overwrite**). If you set the Business Object to **Merge** in the **Business Object Properties** window (mApp page), then the selections made in the **Defaults** section (**Default Behavior for Fields** drop-down list) are also reflected in the **mApp Action** column.

   Tip: You can also select **Edit Business Object** [icon] on the mApp Editor toolbar to open the Business Object Editor.

b. Select a field, and then select **Field Properties**.

3. Set the individual field to **Merge**:
   a. Select the **mApp** page, and then select I**nclude in mApp**.

   b. In the **Options** area, select **Import to Target System**.

   c. From the **If Already Present** drop-down list, select **Merge** as the merge action for the field.

4. Select the **Properties** page.
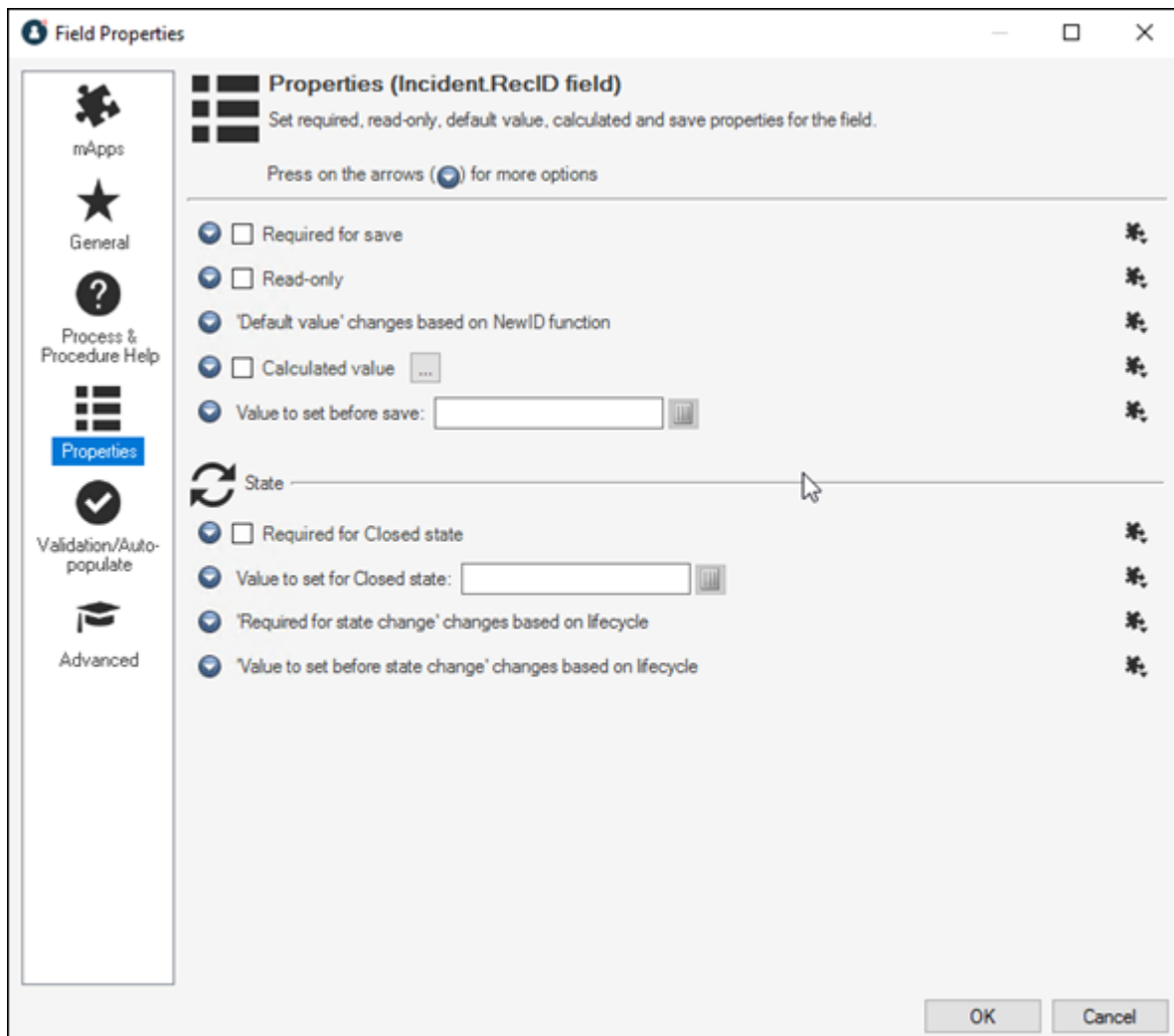
5. Select **mApp** ![mApp icon] next to each property merge area, and then select a merge action:
   ◦ **Do not overwrite the <n> rule:** Select this option to leave the specific property unchanged in the target system when the mApp Solution is applied.

   ◦ **Overwrite the <n> rule**: Select this option to overwrite the specific property in the target system when the mApp Solution is applied.

6. Select **OK**.

7. Prepare the mApp Solution for Distribution (**File > {Prepare mApp for Distribution**), or save the mApp Solution (**File > Save mApp to Disk**) to continue making other changes.

Related concepts

About Business Object Lifecycles

Open the Lifecycle Editor

Define Merge Actions for Field Validation/Auto-Population Properties

Use the **Validation/Auto-Population** page in the **Field Properties** window to define whether or not to overwrite the field's validation and auto-population properties.

> Note: The **Field Properties** window is available in the Business Object Editor (accessed from within the Object Manager in the mApp Editor).

Good to know:

- You can only configure separate merge actions for individual Business Object fields and field properties if the Business Object is set to Merge in the **Business Object Properties** window (**mApp** page). If the Business Object is set to any other option, or if **Include in mApp** is cleared, then you cannot configure separate merge actions for individual field properties.

- For more information about validation/auto-population properties, refer to Define Validation/Auto-Population Properties for a Field.

- If you are configuring merge actions for Business Object fields that were previously applied as part of a Protected mApp™ Solution, the main differences are:
  - You see a shield icon [icon] next to each content-protected field.
  - If a Business Object field is content-protected, it cannot be deleted. This includes menu, context menu, toolbar, and related buttons.
  - Default fields in a content-protected Business Object cannot be edited in any way but you can add new fields and then edit or delete them.
  - When a Business Object is content-protected, you can increase its field length from the default and decrease it back to the original default length.
  - You can use a content-protected Business Object property field in a Full Text Search by selecting the check box on the **Search Results** page.
  - See Protected mApp™ Solutions.

To define merge actions for field validation/auto-population properties:

1. Add a Business Object to a mApp Solution using the Add Business Object to mApp Solution wizard.

2. Open the **Field Properties** window for a field in the Business Object you just added to the mApp Solution:
   a. In the Object Manager within the mApp Editor, select the **Edit Business Object** task in the **Structure** area.
   The Business Object Editor opens, displaying the list of fields with a **mApp Action** column to show the merge actions selected for the fields in the Add Business Object to mApp wizard (either **Overwrite** or **Do Not Overwrite**. The **mApp Action** column is blank for fields set to **Do Not Overwrite**). If you set the Business Object to **Merge** in the **Business Object Properties** window (**mApp** page), then the selections made in the **Defaults** section (**Default Behavior for Fields** drop-down list) are also reflected in the **mApp Action** column.

> **Tip:** You can also select **Edit Business Object** ⬡ on the mApp Editor toolbar to open the Business Object Editor.

    b. Select a field, and then select **Field Properties**.

3. Set the individual field to **Merge**:

    a. Select the **mApp** page, and then select **Include in mApp**.

    b. In the **Options** area, select **Import to Target System**.

4. From the **If Already Present** drop-down list, select **Merge** as the merge action for the field.

5. Select the **Validation/Auto-Populate** page.

6. Select **mApp** ❊ next to each property merge area, and then select a merge action:

For validation properties:

- **Do not overwrite the validation rule:** Select this option to leave the field's validation properties unchanged in the target system when the mApp Solution is applied.
- **Overwrite the validation rule:** Select this option to overwrite the field's validation properties in the target system when the mApp Solution is applied.

For auto-population properties:

- **Do not overwrite the auto-populate rule:** Select this option to leave the field's auto-population properties unchanged in the target system when the mApp Solution is applied.
- **Overwrite the auto-populate rule:** Select this option to overwrite the field's auto-population properties in the target system when the mApp Solution is applied.

7. Select **OK**.

8. Prepare the mApp Solution for Distribution (**File > {Prepare mApp for Distribution**), or save the mApp Solution (**File > Save mApp to Disk**) to continue making other changes.

Define Merge Actions for Field Advanced Properties

Use the **Advanced** page in the **Field Properties** window to define whether or not to overwrite the following merge areas:

- Advanced Options: Whether the Business Object is read-only, cacheable, or has an associated color.
- General Attributes.
- Database Attributes.

> ✏️ **Note:** The **Field Properties** window is available in the Business Object Editor (accessed from within the Object Manager in the mApp Editor).

Good to know:

- You can only configure separate merge actions for individual Business Object Fields and field properties if the Business Object is set to Merge in the **Business Object Properties** window (**mApp** page). If the Business Object is set to any other option, or if **Include in mApp** is cleared, then you cannot configure separate merge actions for individual field properties.
- For more information about defining advanced field properties, refer to Define Advanced Properties for a Field.
- If you are configuring merge actions for Business Object fields that were previously applied as part of a Protected mApp™ Solution, the main differences are:
  - You see a shield icon 🛡 next to each content-protected field.
  - If a Business Object field is content-protected, it cannot be deleted. This includes menu, context menu, toolbar, and related buttons.
  - Default fields in a content-protected Business Object cannot be edited in any way but you can add new fields and then edit or delete them.
  - When a Business Object is content-protected, you can increase its field length from the default and decrease it back to the original default length.
  - You can use a content-protected Business Object property field in a Full Text Search by selecting the check box on the **Search Results** page.
  - See Protected mApp™ Solutions.

To configure merge actions for field advanced properties:

1. Add a Business Object to a mApp Solution using the Add Business Object to mApp wizard.
2. Open the **Field Properties** window for a field in the Business Object you just added to the mApp Solution:
   a. In the Object Manager within the mApp Editor, select the **Edit Business Object** task in the **Structure** area.

The Business Object Editor opens, displaying the list of fields with a **mApp Action** column to show the merge actions selected for the fields in the Add Business Object to mApp wizard (either **Overwrite** or **Do Not Overwrite**. The **mApp Action** column is blank for fields set to **Do Not Overwrite**). If you set the Business Object to **Merge** in the **Business Object Properties** window (**mApp** page), then the selections made in the **Defaults** section (**Default Behavior for Fields** drop-down list) are also reflected in the **mApp Action** column.

> **Tip:** You can also select **Edit Business Object** ⬡ on the mApp Editor toolbar to open the Business Object Editor.

b. Select a field, and then select **Field Properties** .

3. Set the individual field to **Merge**:
   a. Select the **mApp** page, and then select **Include in mApp**.

   b. In the **Options** area, select **Import to Target System**.

   c. From the **If Already Present** drop-down list, select **Merge** as the merge action for the field.

4. Select the **Advanced** page.

5. Select **mApp** [icon] next to each property merge area, and then select a merge action:

For database settings:

- **Do not overwrite database settings:** Select this option to leave the database settings unchanged in the target system when the mApp Solution is applied.

- **Overwrite database settings:** Select this option to overwrite the database settings in the target system when the mApp Solution is applied.

For general attributes:

- **Do not overwrite general attributes:** Select this option to leave the general attributes unchanged in the target system when the mApp Solution is applied.

- **Overwrite general attributes:** Select this option to overwrite the general attributes in the target system when the mApp Solution is applied.

For database attributes:

- **Do not overwrite database attributes:** Select this option to leave the database attributes unchanged in the target system when the mApp Solution is applied.
- **Overwrite database attributes:** Select this option to overwrite the database attributes in the target system when the mApp Solution is applied.

For presentation settings:

- **Do not overwrite presentation settings:** Select this option to leave the presentation settings unchanged in the target system when the mApp Solution is applied.
- **Overwrite presentation settings:** Select this option to overwrite the presentation settings in the target system when the mApp Solution is applied.

For the value splitter:

- **Do not overwrite value splitter:** Select this option to leave the value splitter unchanged in the target system when the mApp Solution is applied.
- **Overwrite value splitter:** Select this option to overwrite the value splitter in the target system when the mApp Solution is applied.

6. Select **OK**.

7. Prepare the mApp Solution for Distribution (**File > {Prepare mApp for Distribution**), or save the mApp Solution (**File > Save mApp to Disk**) to continue making other changes.

Configure Merge Actions for Individual Relationships

Use the **mApp Action** context menu in the Relationship Editor within a mApp Solution to configure separate merge actions for individual relationships. You can also use the **Relationship Properties** window to configure merge actions for individual relationships, as well as for relationship properties.

> **Note:** The **Relationship Properties** window is available in the Relationship Editor (accessed from within the Object Manager in the mApp Editor).

Good to Know:

- If you are configuring merge actions for Business Object relationships that were previously applied as part of a Protected mApp™ Solution, the main differences are:
  - You see a shield icon next to each content-protected relationship.
  - If a Business Object relationship is content-protected, it cannot be deleted.
  - Relationships created during the installation of a Protected mApp Solution cannot be edited or deleted.
  - If you create a new relationship, you can edit and delete it.
  - See Protected mApp™ Solutions.

To configure merge actions for individual relationships:

1. Add a Business Object to a mApp Solution using the Add Business Object to mApp Wizard.

   > **Note:** You can also add relationships to a mApp Solution without also adding the Business Object (except for reference), but this is less common.

2. In the Object Manager within the mApp Editor, select the **Business Object** from the Object tree, and then select the **Edit Relationships** task in the **Structure** area.

   > **Tip:** You can also select **Relationship** in the mApp Editor toolbar to open the Relationship Editor.

   The Relationship Editor opens, displaying the relationships for the Business Object, with a **mApp Action** column to show which relationships you selected to overwrite and which ones you chose not to overwrite (blank in the **mApp Action** column) in the Add Business Object to mApp Wizard.

3. Configure separate merge actions for individual relationships using the **mApp Action** context menu:
   a. Select a relationship, right-click in the **mApp Action** column, and then hover over **mApp Action** to open a context menu.
   b. Select a merge action from the context menu:

- **Make no changes to relationship:** Select this option to leave the existing definition in the target system unchanged (the mApp Solution definition is not imported into the target system when the mApp Solution is applied).

- **Import relationship if not already there:** Select this option to import the relationship if it does not already exist in the target system. If it already exists, the relationship won't be imported when the mApp Solution is applied.

- **Overwrite relationship:** Select this option to have the mApp Solution definition overwrite the existing definition in the target system.

- **Conditionally merge relationship properties:** This option is grayed out on the context menu because merging a relationship requires selecting separate merge actions for individual relationship property merge areas. This is done using the **Relationships Properties** window (see step 5).

- **Remove relationship from target system:** Select this option to have the relationship removed from the target system.

- **Relationship is reference-only:** Select this option to include the relationship in the mApp Solution for informational purposes only (the definition is not imported into the target system when the mApp Solution is applied).

The selected action shows in the mApp Solution status column (blank if you selected **Make no changes to relationship**).

4. Configure separate merge actions for individual relationships using the **Relationship Properties** window):

   a. Select a relationship, and then select **Edit**.

   b. Select the **mApps** page.
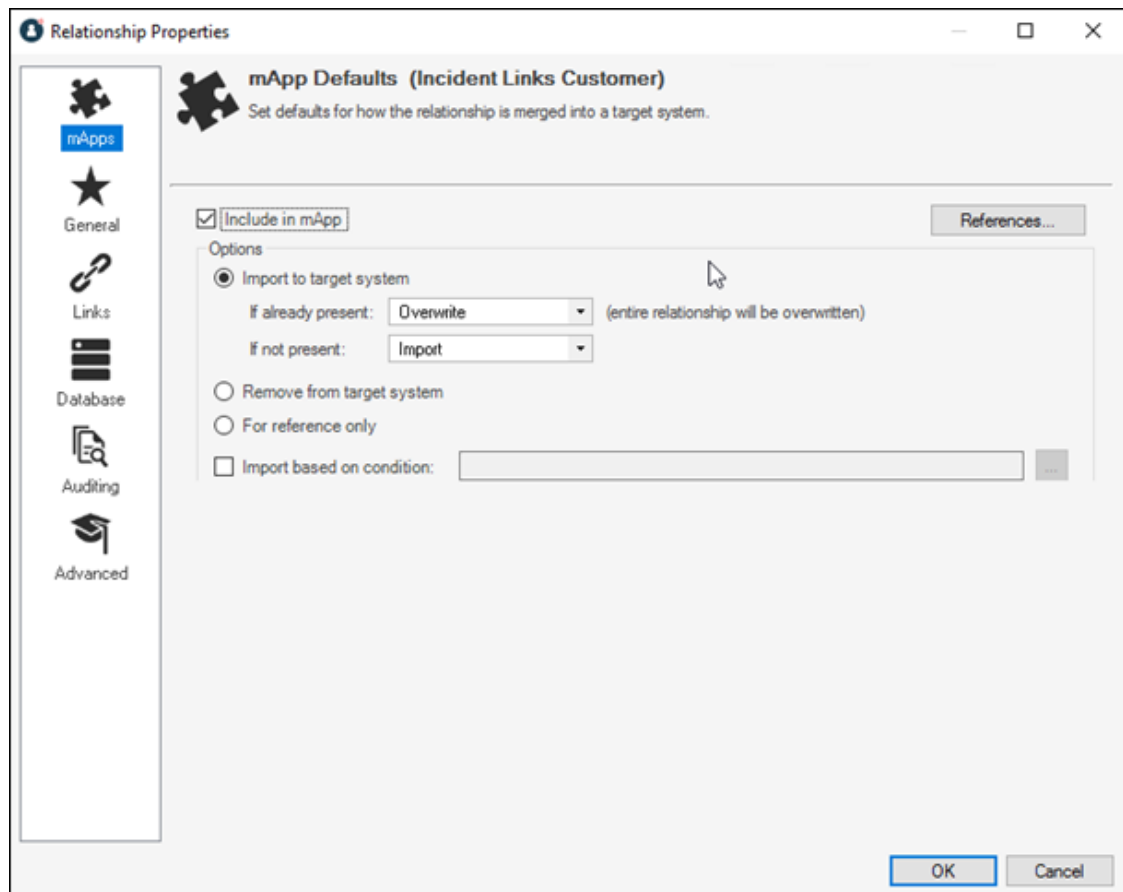
c. Define general mApp Solution properties for the relationship:

  ◦ **Include in mApp:** Select this check box to include the relationship in the mApp Solution. Clear this check box to leave the existing definition in the target system unchanged (the relationship is not imported into the target system when the mApp Solution is applied).

  Note: This check box is automatically selected if you chose to overwrite some or all of the relationships when you added the Business Object to the mApp Solution (using the Add Business Object to mApp Wizard) or if you selected anything besides **Make no changes to relationship** in the **mApp Action** context menu.

  ◦ **References:** Select this button to open the References window and view all of the other definitions being used by the relationship.

d. Define options (merge actions) for how the definition will be merged into a target system:

  Note: These options are only available if **Include in mApp** is selected.

  ◦ **Import to target system:** Select this option button to import the definition into a target system. Then, select a merge action based on whether or not the definition is already present in the target system:

If already present: In the drop-down list, select a merge action to define how the definition is imported if it already exists in a target system:

- **Overwrite:** Select this option to have the mApp Solution definition overwrite the existing definition in the target system.
- **Don't import:** Select this option to leave the existing definition in the target system unchanged (the mApp Solution definition is not imported into the target system when the mApp Solution is applied).
- **Merge:** Select this option to define separate merge actions for each individual area of a definition.

If not present: In the drop-down list, select a merge action to define whether the definition is imported if it does not currently exist in the target system:

- **Import:** Select this option to import the mApp Solution definition into the target system if does not already exist.
- **Don't import:** Select this option to skip importing the mApp Solution definition into the target system if it does not already exist (the mApp Solution definition will not be added to the target system).

- **Remove from target system:** Select this option to remove the definition from a target system.
- **For reference only:** Select this radio button to include the definition in the mApp Solution for informational purposes only (the definition is not imported into the target system when the mApp Solution is applied).
- **Import/remove based on condition:** Select this check box to import or remove the definition based on a condition. Then, select the Ellipsis [ ] to open the **mApp Conditions** window and define mApp Solution conditions.

   Tip: You can also select **mApp Options** ✳ on the mApp Editor toolbar to open the **mApp Options** window for a relationship and define general mApp Solution properties and merge actions for the relationship. The **mApp Options** button shows an indicator based on the merge action you select in the **mApp Solution Options** window or in the Relationship Editor for a particular relationship (example: ✳ for **Overwrite**).

5. Configure separate merge actions for individual relationship property merge areas:
   a. In the **Options** area of the **Relationship Properties** window, select the **Import to Target System** check box.
   b. Select **Merge** as the merge action for the relationship from the **If already present** drop-down list.

c. Define individual merge actions for each merge area:

In the Merge Areas Grid: For each merge area, select a merge action in the **Merge Action** column drop-down lists:

- **Overwrite:** Select this option to have the merge area overwritten in the target system when the mApp Solution is applied.

- **Do not overwrite:** Select this option to leave the merge area unchanged in the target system when the mApp Solution is applied.

Tip: Select **Uncheck All** to set all merge areas to **Do Not Overwrite**. Select **Select All** to set all merge areas to **Overwrite**.

On the remaining pages of the **Properties** window: Select **mApp** next to each of the merge areas to define merge actions for individual properties:

i. Define merge actions for general Relationship properties.

ii. Define merge actions for Relationship link properties.

iii. Define merge actions for Relationship database options.

iv. Define merge actions for Relationship auditing properties.

v. Define merge actions for Relationship advanced properties.

d. Select **OK**.

The Merge Area selections are reflected in the Relationship Editor.

6. Prepare the mApp Solution for Distribution (**File > Prepare mApp for Distribution**), or save the mApp Solution (**File > Save mApp to Disk**) to continue making other changes.

Define Merge Actions for General Relationship Properties

Use the **General** page in the **Relationship Properties** window to define whether or not to overwrite the following property merge areas:

- Name and description.
- Relationship type.
- Relationship cardinality: Whether an object can be related to one or many items.
- Default Group Member: Group member to create by default when the relationship creates a new child object record (only applicable if the child object is a group leader).
- Additional options: Relationship uses, reverse relationships, and full-text searching options.

> **Note:** The **Relationship Properties** window is available in the Relationship Editor (accessed from within the Object Manager in the mApp Editor).

Good to know:

- You can only configure separate merge actions for individual relationships and relationship properties if the Business Object is set to **Merge** in the **Business Object Properties** window (**mApps** page). If the Business Object is set to any other option, or if **Include in mApp** is cleared, then you cannot configure separate merge actions for individual relationship properties.
- For more information about defining general relationship properties, refer to Define General Properties for a Relationship.
- If you are configuring merge actions for Business Object relationships that were previously applied as part of a Protected mApp™ Solution, the main differences are:
  - You see a shield icon 🛡 next to each content-protected relationship.
  - If a Business Object relationship is content-protected, it cannot be deleted.
  - Relationships created during the installation of a Protected mApp Solution cannot be edited or deleted.
  - If you create a new relationship, you can edit and delete it.
  - See Protected mApp™ Solutions.
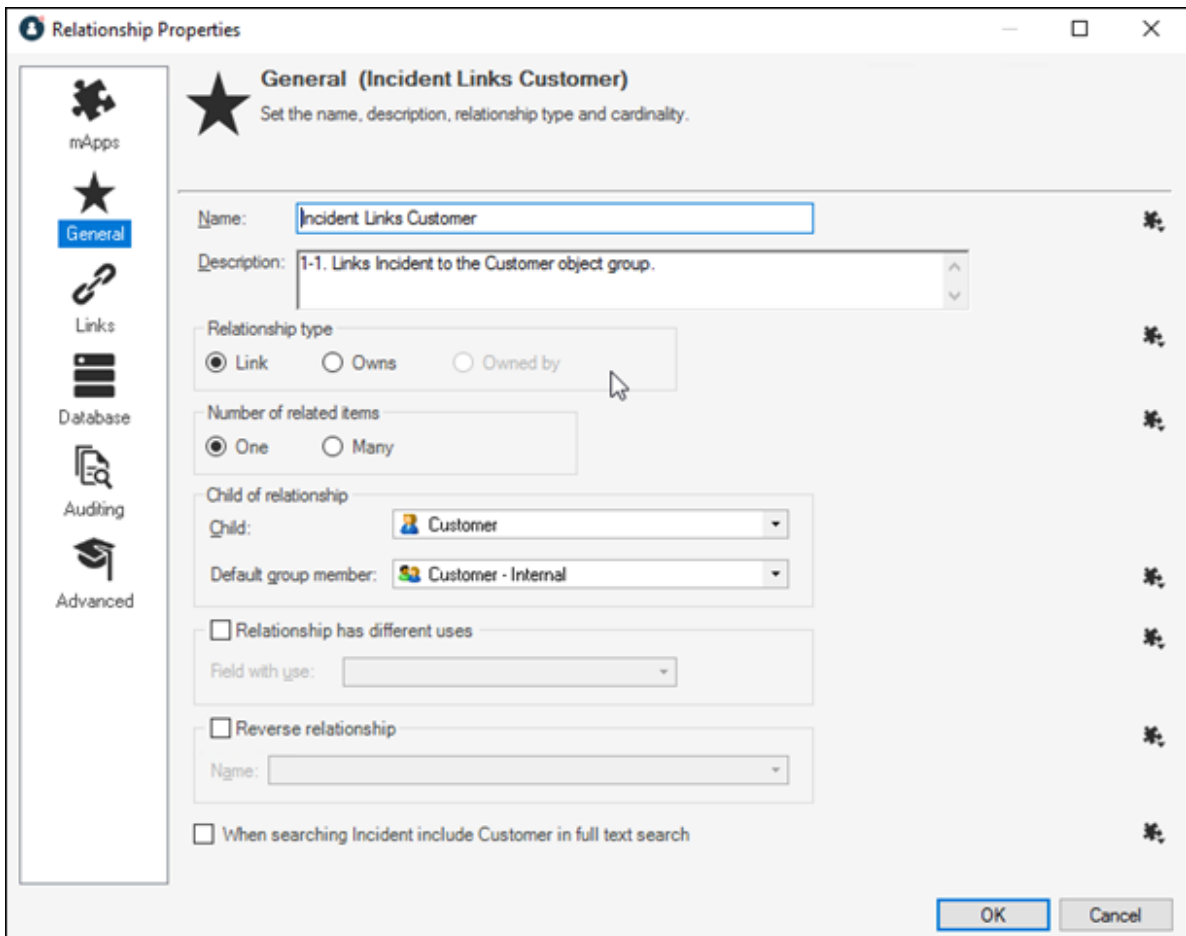
To define merge actions for general relationship properties:

1. Add a Business Object to a mApp using the Add Business Object to mApp wizard.
2. Open the **Relationship Properties** window:
   a. In the Object Manager within the mApp Editor, select the **Edit Relationships** task in the **Structure** area.
   The Relationship Editor opens.

Tip: You can also select **Edit Relationship** ⬡ on the mApp Solution Editor Toolbar to open the Relationship Editor.

   b. Select a relationship, and then select **Edit**.

3. Set the relationship to **Merge**:
   a. Select the **mApps** page, and then select **Include in mApp**.

   b. In the **Options** area, select **Import to Target System**.

   c. From the **If already present** drop-down list, select **Merge** as the merge action for the relationship.

4. Select the **General** page.

5. Select **mApp** ⬡ next to each property merge area, and then select a merge action:

   For general relationship information (name and description):

- **Do not overwrite name and description:** Select this option to leave the relationship's name and description unchanged in the target system when the mApp Solution is applied.
- **Overwrite name and description:** Select this option to overwrite the relationship's name and description in the target system when the mApp Solution is applied.

For relationship type:

- **Do not overwrite relationship type:** Select this option to leave the relationship type unchanged in the target system when the mApp Solution is applied.
- **Overwrite relationship type:** Select this option to overwrite the relationship type in the target system when the mApp Solution is applied.

For the number of related items:

- **Do not overwrite number of related items:** Select this option to leave the number of related items unchanged in the target system when the mApp Solution is applied.
- **Overwrite number of related items:** Select this option to overwrite the number of related items in the target system when the mApp Solution is applied.

For the default Group Member:

- **Do not overwrite default group member:** Select this option to leave the default group member unchanged in the target system when the mApp Solution is applied.
- **Overwrite default group member:** Select this option to overwrite the default group member in the target system when the mApp Solution is applied.

For relationship use:

- **Do not overwrite relationship use:** Select this option to leave the relationship use unchanged in the target system when the mApp Solution is applied.
- **Overwrite relationship use:** Select this option to overwrite the relationship use in the target system when the mApp Solution is applied.

For the reverse relationship:

- **Do not overwrite reverse relationship:** Select this option to leave the reverse relationship unchanged in the target system when the mApp Solution is applied.
- **Overwrite reverse relationship:** Select this option to overwrite the reverse relationship in the target system when the mApp Solution is applied.

For child Full-Text Search:

- **Do not overwrite child full-Text search:** Select this option to leave the child full-text search options unchanged in the target system when the mApp Solution is applied.
- **Overwrite child full-text search:** Select this option to overwrite the child full-text search options in the target system when the mApp Solution is applied.

6. Select **OK**.

7. Prepare the mApp Solution for Distribution (**File > Prepare mApp for Distribution**), or save the mApp Solution (**File > Save mApp to Disk**) to continue making other changes.

Define Merge Actions for Relationship Link Properties

Use the **Links** page in the **Relationship Properties** window (accessed from within the mApp Solution Editor) to define whether or not to overwrite how Business Objects are linked together in a relationship.

🖉 **Note:** The **Relationship Properties** window is available in the Relationship Editor (accessed from within the Object Manager in the mApp Editor).

Good to know:

- You can only configure separate merge actions for individual relationships and relationship properties if the Business Object is set to **Merge** in the **Business Object Properties** window (**mApps** page). If the Business Object is set to any other option, or if **Include in mApp** is cleared, then you cannot configure separate merge actions for individual relationship properties.

- For more information about defining link properties for a relationship, refer to Define Link Properties for a Relationship.

- If you are configuring merge actions for Business Object relationships that were previously applied as part of a Protected mApp™ Solution, the main differences are:
    - You see a shield icon 🛡 next to each content-protected relationship.
    - If a Business Object relationship is content-protected, it cannot be deleted.
    - Relationships created during the installation of a Protected mApp Solution cannot be edited or deleted.
    - If you create a new relationship, you can edit and delete it.
    - See Protected mApp™ Solutions.

To define merge actions for a relationship's link properties:

1. Add a Business Object to a mApp using the Add Business Object to mApp wizard.

2. Open the **Relationship Properties** window:
    a. In the Object Manager within the mApp Editor, select the **Edit Relationships** task in the **Structure** area.
    The Relationship Editor opens.

    🚩 **Tip:** You can also select **Edit Relationship** 📇 on the mApp Editor Toolbar to open the Relationship Editor.

    b. Select a relationship, and then select **Edit**.

3. Set the relationship to **Merge**:
    a. Select the **mApp** page, and then select **Include in mApp**.

    b. In the **Options** area, select **Import to Target System**.

---

      c. From the **If already present** drop-down list, select **Merge** as the merge action for the relationship.

4. Select the **Links** page.

5. Select **mApp** [icon], and then select a merge action:
   ◦ **Do not overwrite relationship link options:** Select this option to leave the relationship's link properties unchanged in the target system when the mApp Solution is applied.

   ◦ **Overwrite relationship link options:** Select this option to overwrite the relationship's link properties in the target system when the mApp Solution is applied.

6. Select **OK**.

7. Prepare the mApp Solution for Distribution (**File > Prepare mApp for Distribution**), or save the mApp Solution (**File > Save mApp to Disk**) to continue making other changes.

Define Merge Actions for Relationship Database Properties

Use the **Database** page in the **Relationship Properties** window to define whether or not to overwrite the relationship's database properties.

🖉 **Note:** The **Relationship Properties** window is available in the Relationship Editor (accessed from within the Object Manager in the mApp Editor).

Good to know:

- You can only configure separate merge actions for individual relationships and relationship properties if the Business Object is set to **Merge** in the **Business Object Properties** window (**mApps** page). If the Business Object is set to any other option, or if **Include in mApp** is cleared, then you cannot configure separate merge actions for individual relationship properties.

- Database properties allow you to create and enable foreign keys for the relationship. Foreign Keys establish and enforce a link between tables in a relational database, and are required by SQL Reporting Services. It is recommended that you do not use foreign keys unless you have a specific need to do so.

- For more information about defining relationship database properties, refer to Define Database Properties for a Relationship.

- If you are configuring merge actions for Business Object relationships that were previously applied as part of a Protected mApp™ Solution, the main differences are:
  - You see a shield icon 🛡️ next to each content-protected relationship.
  - If a Business Object relationship is content-protected, it cannot be deleted.
  - Relationships created during the installation of a Protected mApp Solution cannot be edited or deleted.
  - If you create a new relationship, you can edit and delete it.
  - See Protected mApp™ Solutions.

To define merge actions for relationship database properties:

1. Add a Business Object to a mApp using the Add Business Object to mApp wizard.

2. Open the **Relationship Properties** window:
   a. In the Object Manager within the mApp Editor, select the **Edit Relationships** task in the **Structure** area.
   The Relationship Editor opens.

      🚩 **Tip:** You can also select **Edit Relationship** 🔀 on the mApp Editor Toolbar to open the Relationship Editor.

   b. Select a relationship, and then select **Edit**.

3. Set the relationship to **Merge**:

   a. Select the **mApps** page, and then select **Include in mApp**.

   b. In the **Options** area, select **Import to Target System**.

   c. From the **If already present** drop-down list, select **Merge** as the merge action for the relationship.

4. Select the **Database** page.

5. Select **mApp** ![icon], and then select a merge action:

   ◦ **Do not overwrite database options:** Select this option to leave the relationship's database properties unchanged in the target system when the mApp Solution is applied.

   ◦ **Overwrite database options:** Select this option to overwrite the relationship's database properties in the target system when the mApp Solution is applied.

6. Select **OK**.

7. Prepare the mApp Solution for Distribution (**File > Prepare mApp for Distribution**), or save the mApp Solution (**File > Save mApp to Disk**) to continue making other changes.

Define Merge Actions for Relationship Auditing Properties

Use the **Auditing** page in the **Relationship Properties** window to define whether or not to overwrite how changes to child object records are tracked in the parent object's history records.

Note: The **Relationship Properties** window is available in the Relationship Editor (accessed from within the Object Manager in the mApp Editor).

Good to know:

- You can only configure separate merge actions for individual relationships and relationship properties if the Business Object is set to **Merge** in the **Business Object Properties** window (**mApps** page). If the Business Object is set to any other option, or if **Include in mApp** is unchecked, then you cannot configure separate merge actions for individual relationship properties.

- For more information about defining auditing properties for a relationship, refer to Define Auditing Properties for a Relationship.

- If you are configuring merge actions for Business Object relationships that were previously applied as part of a Protected mApp™ Solution, the main differences are:
  - You see a shield icon ⬚ next to each content-protected relationship.
  - If a Business Object relationship is content-protected, it cannot be deleted.
  - Relationships created during the installation of a Protected mApp Solution cannot be edited or deleted.
  - If you create a new relationship, you can edit and delete it.
  - See Protected mApp™ Solutions.

To define merge actions for relationship auditing properties:

1. Add a Business Object to a mApp Solution using the Add Business Object to mApp wizard.

2. Open the **Relationship Properties** window:
   a. In the Object Manager within the mApp Editor, select the **Edit Relationships** task in the **Structure** area.
   The Relationship Editor opens.

      Tip: You can also select **Edit Relationship** ⬚ on the mApp EditorToolbar to open the Relationship Editor.

   b. Select a relationship, and then select **Edit**.

3. Set the relationship to **Merge**:
   a. Select the **mApps** page, and then select **Include in mApp**.

   b. In the **Options** area, select **Import to Target System**.

      c. From the **If already present** drop-down list, select **Merge** as the merge action for the relationship.

4. Select the **Auditing** page.

5. Select **mApp** ![icon], and then select a merge action:

    ◦ **Do not overwrite audit settings:** Select this option to leave the relationship's auditing properties unchanged in the target system when the mApp Solution is applied.

    ◦ **Overwrite audit settings:** Select this option to overwrite the relationship's auditing properties in the target system when the mApp Solution is applied.

6. Select **OK**.

7. Prepare the mApp Solution for Distribution (**File > Prepare mApp for Distribution**), or save the mApp Solution (**File > Save mApp to Disk**) to continue making other changes.

Define Merge Actions for Relationship Advanced Properties

Use the **Advanced** page in the **Relationship Properties** window to define whether or not to overwrite the following advanced properties for a relationship:

- Advanced Options: Options for deleting child objects when parent objects are deleted, making records in the relationship read-only, reloading the relationship when constraints change, etc.
- Groups: Options for defining group member type when child records are added (only applicable if the child object is a group object).
- General Attributes.
- Database Attributes.

> **Note:** The **Relationship Properties** window is available in the Relationship Editor (accessed from within the Object Manager in the mApp Editor).

Good to know:

- You can only configure separate merge actions for individual relationships and relationship properties if the Business Object is set to **Merge** in the **Business Object Properties** window (**mApps** page). If the Business Object is set to any other option, or if **Include in mApp** is cleared, then you cannot configure separate merge actions for individual relationship properties.
- For more information about defining advanced properties for a relationship, refer to Define Advanced Properties for a Relationship.
- If you are configuring merge actions for Business Object relationships that were previously applied as part of a Protected mApp™ Solution, the main differences are:
  - You see a shield icon [shield icon] next to each content-protected relationship.
  - If a Business Object relationship is content-protected, it cannot be deleted.
  - Relationships created during the installation of a Protected mApp Solution cannot be edited or deleted.
  - If you create a new relationship, you can edit and delete it.
  - See Protected mApp™ Solutions.

To define merge actions for relationship advanced properties:

1. Add a Business Object to a mApp using the Add Business Object to mApp wizard.
2. Open the **Relationship Properties** window:
   a. In the Object Manager within the mApp Editor, select the **Edit Relationships** task in the **Structure** area.
   The Relationship Editor opens.

> **Tip:** You can also select **Edit Relationship** ⚇ on the mApp Editor Toolbar to open the Relationship Editor.

    b. Select a relationship, and then select **Edit**.

3. Set the relationship to **Merge**:
    a. Select the **mApps** page, and then select **Include in mApp**.

    b. In the **Options** area, select **Import to Target System**.

    c. From the **If already present** drop-down list, select **Merge** as the merge action for the relationship.

4. Select the **Advanced** page.

5. Select **mApp** 🧩 next to each property merge area, and then select a merge action:

For advanced options:

- ◦ **Do not overwrite advanced options:** Select this option to leave the advanced options unchanged in the target system when the mApp Solution is applied.
- ◦ **Overwrite advanced options:** Select this option to overwrite the advanced options in the target system when the mApp Solution is applied.

For Group settings:

- ◦ **Do not overwrite group settings:** Select this option to leave the group settings unchanged in the target system when the mApp Solution is applied.
- ◦ **Overwrite group settings:** Select this option to overwrite the group settings in the target system when the mApp Solution is applied.

    Note: These settings are displayed only if the child object in the relationship is a group object.

For general attributes:

- ◦ **Do not overwrite general attributes:** Select this option to leave the general attributes unchanged in the target system when the mApp Solution is applied.
- ◦ **Overwrite general attributes:** Select this option to overwrite the general attributes in the target system when the mApp Solution is applied.

For database attributes:

- ◦ **Do not overwrite database attributes:** Select this option to leave the database attributes unchanged in the target system when the mApp Solution is applied.
- ◦ **Overwrite database attributes:** Select this option to overwrite the database attributes in the target system when the mApp Solution is applied.

6. Select **OK**.

7. Prepare the mApp Solution for Distribution (**File > Prepare mApp for Distribution**), or save the mApp Solution (**File > Save mApp to Disk**) to continue making other changes.

CSM 2022.3 Administration

Configure Merge Actions for Forms

The Add Business Object to mApp Wizard is a convenient way to define merge actions for a Business Object and its associated Forms. However, you can also use the mApp Options window in the Form Editor to configure the following:

- General properties: Whether to include the Form in the mApp Solution.
- Options for importing the Form into the target system when the mApp Solution is applied:
  ◦ Import to target system: Imports the Form into the target system. You can select merge actions based on whether the Form already exists in the target system.
  ◦ Remove from Target System: Removes the Form from the target system.
  ◦ For Reference Only: Includes the Form in the mApp Solution for informational purposes only (it is not merged into the target system when the mApp Solution is applied).
  ◦ Import/remove based on condition: Imports or removes the Form based on configured mApp Solution conditions.
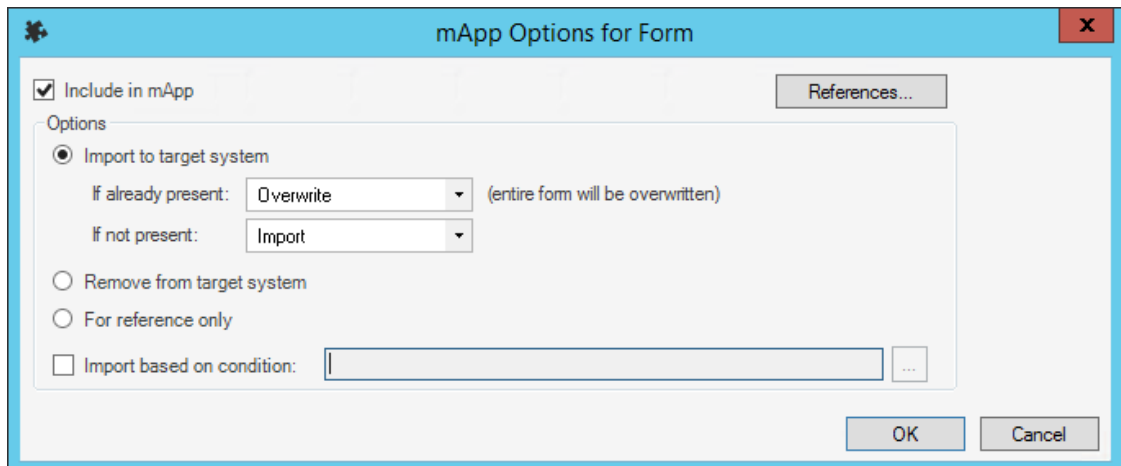
To configure merge actions for Forms:

1. Add a Business Object to a mApp Solution using the Add Business Object to mApp Wizard.
2. In the Object Manager within the mApp Editor, click the **Business Object** from the Object tree, and then click the **Edit Forms** task in the Appearance area.

   The Form Editor opens.

   Tip: You can also click the **Form** button 🖼 in the mApp Editor toolbar to open the Form Editor.

3. Configure merge actions for Forms:
   a. Select a **Form** in the Form drop-down (example: Default Form), and then click the **mApp Options** button 🧩 on the mApp Editortoolbar.

CSM 2022.3 Administration   653

b. Define general mApp Solution properties for the Form:

◦ Include in mApp Solution: Select this check box to include the form in the mApp Solution. Clear this check box to leave the existing definition in the target system unchanged (the Form is not imported into the target system when the mApp Solution is applied).

Note: This check box is automatically selected if some or all of the Forms were set to overwrite when you added the Business Object to the mApp Solution (using the Add Business Object to mApp Wizard).

◦ References: Click this button to open the References window and view all of the other definitions being used by the Form.

c. Define options (merge actions) for how the Form will be merged into a target system:

Note: These options are only available if *Include in mApp Solution* is selected.

◦ Import to target system: Select this radio button to import the form definition into a target system. Then, select a merge action based on whether or not the definition is already present in the target system.

If already present: In the drop-down, select a merge action to define how the definition is imported if it already exists in a target system:

◦ Overwrite: Select this option to have the mApp Solution definition overwrite the existing definition in the target system.

◦ Don't Import: Select this option to leave the existing definition in the target system unchanged (the mApp Solution definition is not imported into the target system when the mApp Solution is applied).

If not present: In the drop-down, select a merge action to define whether the definition is imported if it does not currently exist in the target system:

◦ Import: Select this option to import the mApp Solution definition into the target system if does not already exist.

◦ Don't Import: Select this option to skip importing the mApp Solution definition into the target system if it does not already exist (the mApp Solution definition will not be added to the target system).

◦ Remove from Target System: Select this radio button to remove the form definition from a target system.

◦ For Reference Only: Select this radio button to include the form definition in the mApp Solution for informational purposes only (the definition is not imported into the target system when the mApp Solution is applied).

◦ Import/Remove Based on Condition: Select this check box to import or remove the form definition based on a condition. Then, click the **Ellipses** button to open the mApp Solution Conditions window and define mApp Solution conditions.

d. Select **OK**.

The mApp Solution Options button shows an indicator based on the selected merge action (example: for *Overwrite*).

4. Prepare the mApp Solution for Distribution (File>Prepare mApp for distribution), or save the mApp Solution (File>Save mApp to Disk) to continue making other changes.

Configure Merge Actions for Grids

The Add Business Object to mApp Wizard is the primary method of defining merge actions for a Business Object and its associated Grids. However, you can use the mApp Solution Options window in the Grid Editor to configure the following:

- General properties: Whether to include the Grid in the mApp Solution.

- Options for importing the Grid into the target system when the mApp Solution is applied:
  ◦ Import to target system: Imports the Grid into the target system. You can select merge actions based on whether the Form already exists in the target system.

  ◦ Remove from Target System: Removes the Grid from the target system.

  ◦ For Reference Only: Includes the Grid in the mApp Solution for informational purposes only (it is not merged into the target system when the mApp Solution is applied).

  ◦ Import/remove based on condition: Imports or removes the Grid based on configured conditions.
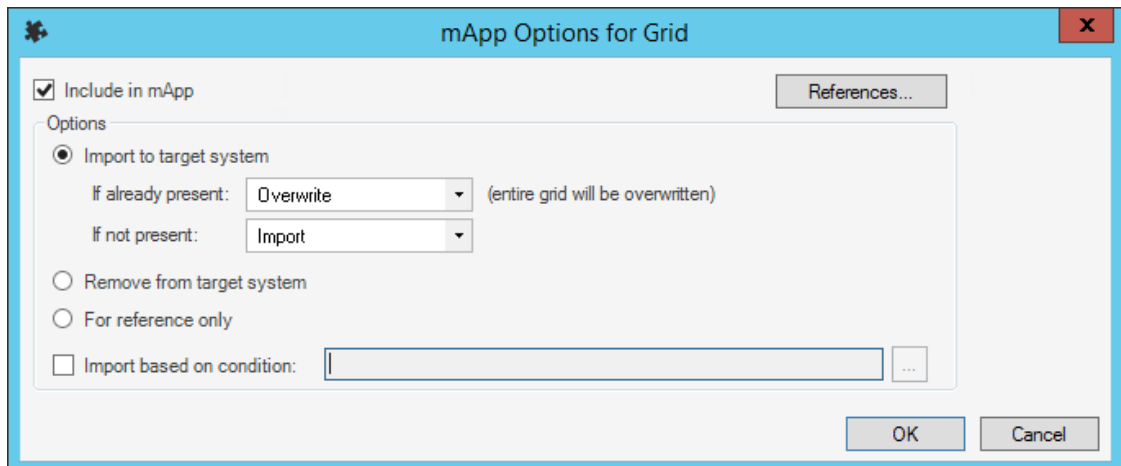
To configure merge actions for Grids:

1. Add a Business Object to a mApp Solution using the Add Business Object to mApp Wizard.

2. In the Object Manager within the mApp Editor, click the **Business Object** from the Object tree, and then click the **Edit Grids** task in the Appearance area.

   The Grid Editor opens.

   Tip: You can also click the **Grid** button [icon] in the mApp Editor toolbar to open the Grid Editor.

3. Configure merge actions for Grids:
   a. Select a **Grid** in the Grid drop-down (example: Default Grid), and then click the **mApp Options** button [icon] on the mApp Editor toolbar.

b. Define general mApp Solution properties for the Grid:

- Include in mApp: Select this check box to include the Grid in the mApp Solution. Clear this check box to leave the existing definition in the target system unchanged (the Grid is not imported into the target system when the mApp Solution is applied).

  Note: This check box is automatically selected if some or all of the Grids were set to overwrite when you added the Business Object to the mApp Solution (using the Add Business Object to mApp Wizard).

- References: Click this button to open the References window and view all of the other definitions being used by the Grid.

c. Define options (merge actions) for how the Grid will be merged into a target system:

Note: These options are only available if *Include in mApp* is selected.

- Import to target system: Select this radio button to import the Grid definition into a target system. Then, select a merge action based on whether or not the definition is already present in the target system:

  If already present: In the drop-down, select a merge action to define how the definition is imported if it already exists in a target system:

  - Overwrite: Select this option to have the mApp Solution definition overwrite the existing definition in the target system.
  - Don't Import: Select this option to leave the existing definition in the target system unchanged (the mApp Solution definition is not imported into the target system when the mApp Solution is applied).

  If not present: In the drop-down, select a merge action to define whether the definition is imported if it does not currently exist in the target system:

  - Import: Select this option to import the mApp Solution definition into the target system if does not already exist.
  - Don't Import: Select this option to skip importing the mApp Solution definition into the target system if it does not already exist (the mApp Solution definition will not be added to the target system).

- Remove from Target System: Select this radio button to remove the Grid definition from a target system.
- For Reference Only: Select this radio button to include the Grid definition in the mApp Solution for informational purposes only (the definition is not imported into the target system when the mApp Solution is applied).
- Import/Remove Based on Condition: Select this check box to import or remove the Grid definition based on a condition. Then, click the **Ellipses** button ⬚ to open the mApp Solution Conditions window and define mApp Solution conditions.

d. Select **OK**.

The mApp Solution Options button shows an indicator based on the selected merge action (example: for *Overwrite*).

4. Prepare the mApp Solution for Distribution (File>Prepare mApp for distribution), or save the mApp Solution (File>Save mApp to Disk) to continue making other changes.

Configure Merge Actions for Form Arrangements and Tabs

The Add Business Object to mApp Wizard is the primary method of defining merge actions for Form Arrangements. However, you can use the mApp Options window in the Form Arrangement Editor to override these selections.

You can also configure separate merge actions for individual tabs in a Form Arrangement using the following tools in the Form Arrangement Editor:

- mApp Action context menu
- Tab Properties window

When you make selections in one tool, they will be reflected in the other tools.

To configure merge actions for Form Arrangements:

1. Add a Business Object to a mApp Solution using the Add Business Object to mApp Wizard.

2. In the Object Manager within the mApp Editor, click the **Business Object** from the Object tree, and then click the **Edit Form Arrangement** task in the Appearance area.

   The Form Arrangement Editor opens.

   Tip: You can also click the **Form Arrangement** button in the mApp Editor toolbar to open the Form Arrangement Editor.

3. Configure merge actions for the Form Arrangement:

   a. Click the **mApp Options** button in the mApp Editor toolbar.
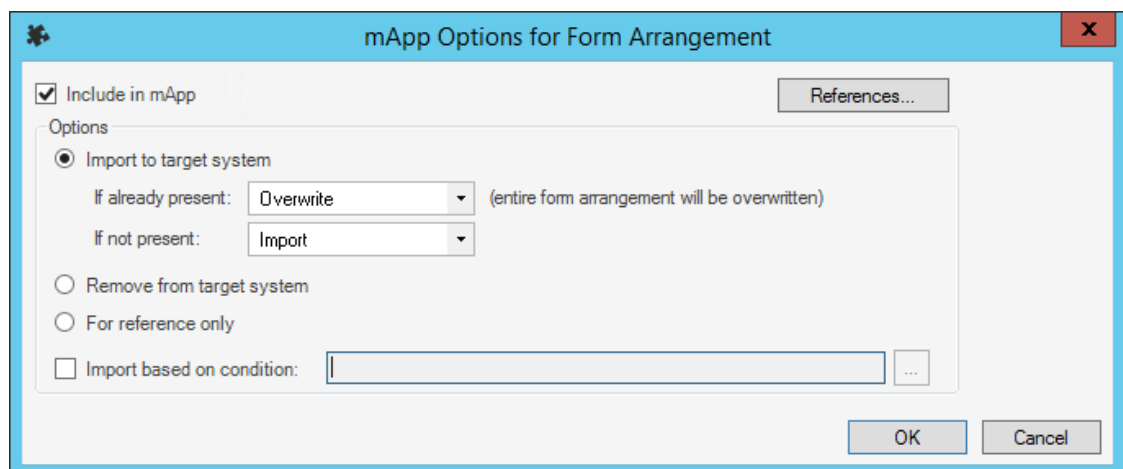
   b. Define general mApp Solution properties for the Form Arrangement:

- ◦ Include in mApp: Select this check box to include the Form Arrangement in the mApp Solution. Clear this check box to leave the existing definition in the target system unchanged (the Form Arrangement is not imported into the target system when the mApp Solution is applied).

  Note: This check box is automatically selected if some or all of the tabs in the Form Arrangement were set to overwrite when you added the Business Object to the mApp Solution (using the Add Business Object to mApp Wizard).

- ◦ References: Select this button to open the References window and view all of the other definitions being used by the Form Arrangement

c. Define options (merge actions) for how the Form Arrangement will be merged into a target system:

Note: These options are only available if *Include in mApp* is checked.

- ◦ Import to target system: Select this radio button to import the Form Arrangement definition into a target system. Then, select a merge action based on whether or not the definition is already present in the target system:

  If already present: In the drop-down, select a merge action to define how the definition is imported if it already exists in a target system:

  - ◦ Overwrite: Select this option to have the mApp Solution definition overwrite the existing definition in the target system.
  - ◦ Don't Import: Select this option to leave the existing definition in the target system unchanged (the mApp Solution definition is not imported into the target system when the mApp Solution is applied).
  - ◦ Merge: Select this option to define separate merge actions for each Tab of a Form Arrangement definition.

  If not present: In the drop-down, select a merge action to define whether the definition is imported if it does not currently exist in the target system:

  - ◦ Import: Select this option to import the mApp Solution definition into the target system if does not already exist.
  - ◦ Don't Import: Select this option to skip importing the mApp Solution definition into the target system if it does not already exist (the mApp Solution definition will not be added to the target system).

- ◦ Remove from Target System: Select this radio button to remove the Form Arrangement definition from a target system.

- ◦ For Reference Only: Select this radio button to include the Form Arrangement definition in the mApp Solution for informational purposes only (the definition is not imported into the target system when the mApp Solution is applied).

     ◦ Import/Remove Based on Condition: Select this check box to import or remove the Form

     Arrangement definition based on a condition. Then, click the **Ellipses** button [___] to open the mApp Conditions window and define mApp Solution conditions.

    d. Select **OK**.

The mApp Options button shows an indicator based on the selected merge action (example: 🧩 for *Overwrite*).

4. Configure separate merge actions for individual tabs in the Form Arrangement (using the mApp Action context menu):
    a. In the mApp Options window for the Form Arrangement, select **Import to Target System**.

    b. Select **Merge** as the merge action for the Form Arrangement (from the *If Already Present* drop-down).

    Each tab shows an indicator based on the merge action for each tab (default is *Overwrite*).

    c. Right-click a tab, and then hover over **mApp Action** to open a context menu.

    d. Select a merge action from the context menu.
      ◦ Make no changes to Tab (Default): Select this option to leave the existing definition in the target system unchanged (the mApp Solution definition is not imported into the target system when the mApp Solution is applied).

      ◦ Import Tab if not already there: Select this option to import the Tab if it does not already exist in the target system. If it already exists, the Tab will not be imported when the mApp Solution is applied.

      ◦ Overwrite Tab: Select this option to have the mApp Solution definition overwrite the existing definition in the target system.

      ◦ Remove Tab from target system: Select this option to have the Tab removed from the target system.

5. Configure separate merge actions for individual tabs in the Form Arrangement (using the Tab Properties window):
    a. Right-click a **tab**, and then click **Properties**.

    b. Click the mApp Solution button 🧩 (on any page), and then select a merge action for the tab:

    Note: The down arrow is only active if the Form Arrangement was set to *Merge* in the mApp Options window.

      ◦ Make no changes to tab (Default): Select this option to leave the existing tab definition (if found) unchanged in the target system (the mApp Solution definition is not imported into the target system when the mApp Solution is applied).

      ◦ Overwrite tab: Select this option to have the tab definition in the mApp Solution overwrite the existing tab definition (if found) in the target system. If the tab definition is not found in the target system, it is added to the system when the mApp Solution is applied.

- ◦ Remove tab if found: Select this option to have the mApp Solution remove the existing tab definition in the target system (if found).

  Note: The merge action selected in the Add Business Object to mApp Wizard for the tab in the Form Arrangement is automatically checked.

  c. Select **OK**.

Each tab shows an indicator based on the action selected in the mApp Solution Action context menu or the Tab Properties window.

6. Prepare the mApp Solution for Distribution (File>Prepare mApp for distribution), or save the mApp Solution (File>Save mApp to Disk) to continue making other changes.

   Note: Even if a tab is set to be added or merged into a target system, it will not be added or merged if the necessary target Relationship does not exist.

Configure Merge Actions for Business Object Actions

Business Object Actions are categorized by areas (Menu, Task Pane, toolbar, Context Menu, and Automatic Actions). When you use the Add Business Object to mApp Wizard to define merge actions for a Business Object and its associated Actions, you are specifying merge actions for entire areas and all Actions within those areas. However, you can use the Business Object Actions window to override these selections. You can also define separate merge actions for individual Actions within a Business Object's Menu, Task Pane, toolbar, and Context Menu.

To configure merge actions for Business Object Actions:

1. Add a Business Object to a mApp Solution using the Add Business Object to mApp Wizard.

2. In the Object Manager within the mApp Editor, click the **Business Object** from the Object tree, and then click the **Edit Actions** task in the Structure area.

3. Click a page (example: Task Pane) to view the Actions for that specific area.
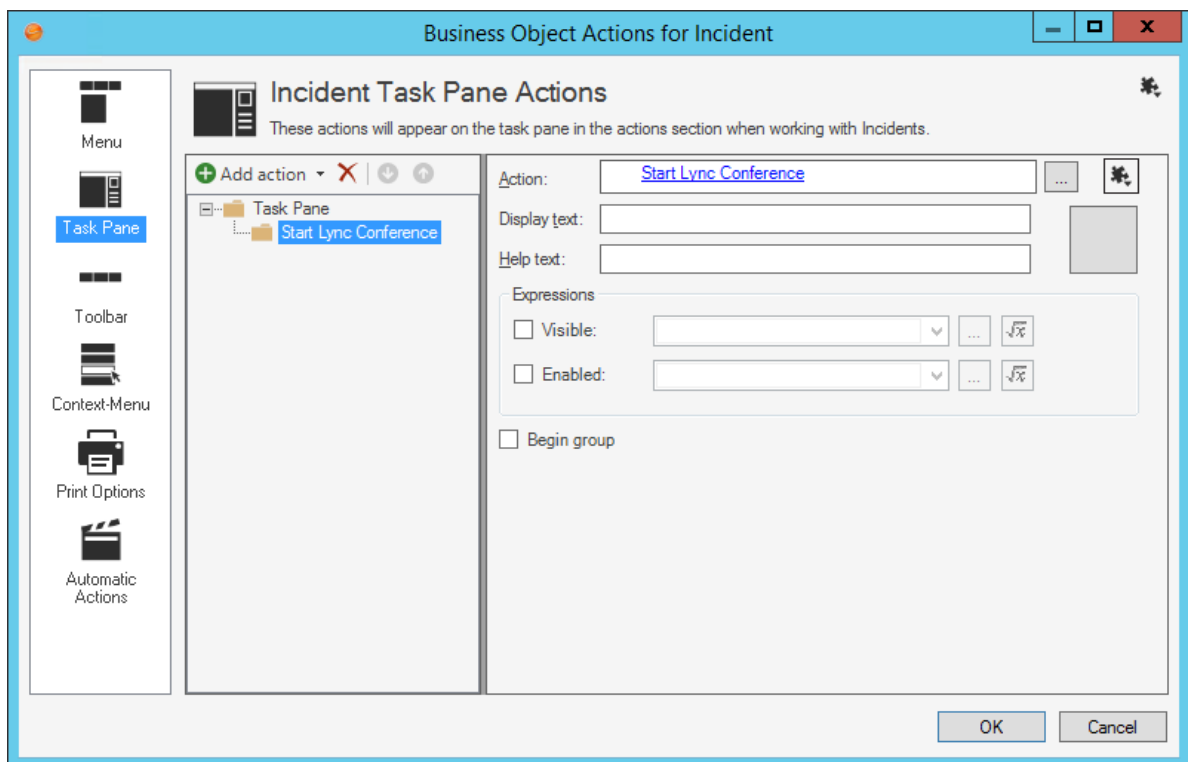
4. Configure separate merge actions for individual Business Object Action areas (the merge action selected will apply to all Business Object Actions within the area:

   a. Click the **mApp** button [icon], and then select a merge action:
      ◦ Clear overwrite option for all Actions: Select this option to set all Actions within an area to *Do Not Overwrite*.

- Set all Actions for overwrite: Select this option to set all Actions within an area to *Overwrite*.

5. Configure separate merge actions for individual Business Object Actions:

   a. Select a specific **Action** within an area, and then click the **mApp** button next to the Action field.

   b. Select a merge action in the drop-down:

   Note: You can only select separate merge actions for Menu, Task Pane, toolbar, Context Menu, and Automatic Actions. Print Actions are handled as a single merge area of a Business Object.

      - Do Not Overwrite Action: Select this option to leave the existing Action definition in the target system unchanged (the mApp Solution definition is not imported into the target system when the mApp Solution is applied).

      - Overwrite Action: Select this option to have the mApp Solution definition overwrite the existing definition in the target system.

      - Conditions: Select this option to open the mApp Conditions window and define conditions for overwriting/adding the Action definition when the mApp Solution is applied.

6. Select **OK**.

7. Prepare the mApp Solution for Distribution (File>Prepare mApp for distribution), or save the mApp Solution (File>Save mApp to Disk) to continue making other changes.

View Referenced Definitions in a mApp Solution

References allow you to see at a glance all of the system definitions throughout CSM being used by a selected mApp Solution definition (Business Object, Relationship, Form, Grid, Form Arrangement, and/or CSM Item). This allows you to ensure that all necessary definitions are included in a mApp Solution.

Good to know:

- If you add a definition to a mApp Solution without also adding all of the other definitions it references, some portions of the object or item might not work in the target system after the mApp Solution is applied.
- You cannot add Business Objects to a mApp Solution from the References window. You must use either the Add Business Object to mApp Wizard or the Business Object Properties window.

Use the References window to:

- View all references associated with a mApp Solution definition.
- View all references that can be automatically added to a mApp Solution.
- Add referenced definitions to a mApp Solution.

The references window can be opened several ways within a mApp Solution by clicking the References button (activated when the **Include in mApp** check box is selected):

- From the mApp page in the Business Object Properties window.
- From the mApp page in the Field Properties window.
- From the mApp page in the Relationship Properties window.
- From the mApp Options window in the Form Editor.
- From the mApp Options window in the Grid Editor.
- From the mApp Options window in the Form Arrangement Editor.
- From the mApp Options window when you add a CSM Item (example: One-Step Action) to a mApp Solution.
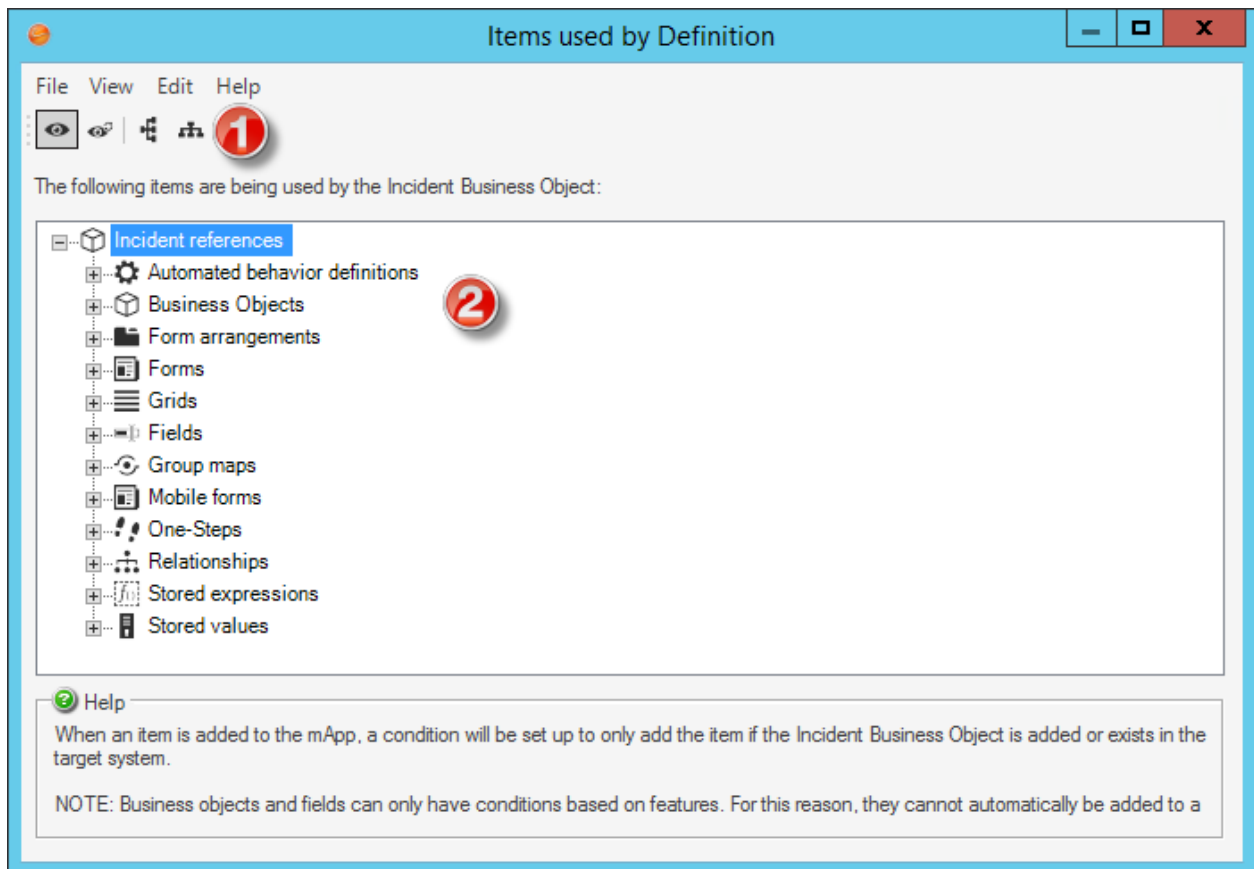
1. Toolbar: Displays a row of drop-down menus available in the References window.
2. Main Pane: Displays dependent definitions grouped in a tree by system definition.

Open the References Window

The references window can be opened several ways within a mApp Solution by clicking the References button (activated when the **Include in mApp** check box is selected):

- From the mApp page in the Business Object Properties window.
- From the mApp page in the Field Properties window.
- From the mApp page in the Relationship Properties window.
- From the mApp Options window in the Form Editor.
- From the mApp Options window in the Grid Editor.
- From the mApp Options window in the Form Arrangement Editor.
- From the mApp Options window when you add a CSM Item (example: One-Step Action) to a mApp Solution.

References Window Toolbar

Use the References window toolbar to view and add definitions that are used by a system definitions included in a mApp Solution. When you add a referenced definition to a mApp Solution, a condition is automatically set to only import the referenced definition into a target system if the definition using it is also imported (or already exists in the target system).

Note: The References window toolbar is dynamic so options vary depending on the type of definition and what is selected in the tree.

References Window Main Pane

Use the References Window Main pane to view referenced definitions, grouped in a tree by the type of system definition (example: Forms). What is shown in the tree depends on where the References window was accessed (example: Clicking the References button from the Relationship Properties window will show a tree of all definitions being used by a particular Relationship). In the References Window Main pane, you can:

- Expand the branches of the tree to drill down into referenced definitions.

- Contract expanded branches back to the main referenced definitions.

- Select an item and add or remove it from a mApp Solution (right-click item or use the buttons on the toolbar).

Automation Processes

Automation Processes allow you to automate behavior by creating rules for the system to follow. For example, you can automate the process for sending a notification to a requester when an Incident is closed.

Automation Processes can automatically complete an Action when a particular event takes place or handle time-sensitive issues, such as notifying a technician when a customer has not been contacted within four hours of creating a request. Automation Processes can also watch for trends, such as taking action when the number of open Incidents exceeds a particular threshold.

Automation Processes operate within the time frame of defined Business Hours.

Types of Automation Processes

There are three types of Automation Processes:

1. Visual Workflow Process: Defines a sequence of time-based and event-based steps that manage a Business Object as it passes through various stages.

2. Threshold-Based Process: Watches a value and performs an Action after a threshold is crossed.

3. Simple Action/Event Process: Runs a One-Step™ Action or action after a specific event occurs.

Automation Process Framework

- **Definitions**
  Automation Processes are created and edited in Blueprints because they rely on Business Object logic to determine when they should run. There are three ways to manage Automation Process definitions in CSM Administrator:

  1. Create or edit an Automation Process Blueprint from the **Automation Processes** pane.

  2. Create or edit a Blueprint.

  3. Create or edit a mApp® Solution.

  Regardless of the method you choose, Automation Processes cannot run until they have been published in a Blueprint or mApp Solution.

- **Processing**
  When conditions are met, Automation Processes are triggered and processed by the Automation Process Service, which is a microservice of the Cherwell Service Host.

  Approvals are also processed by the Automation Process Service.

  You can pause and resume Automation Processes directly in CSM Administrator. See Pause/ Resume Automation Process Processing.

- **Administration**
  Use tools in CSM Administrator to enable, disable, and monitor Automation Processes. See Use Automation Processes.

Related concepts

About the Cherwell Service Host

Performance Considerations for Automation Processes

Related tasks

Create an Automation Process Visual Workflow Process

Create a Threshold-Based Automation Process

Create a Simple Action/Event Automation Process

Manage Automation Processes

CSM provides multiple tools to manage Automation Processes, including the Automation Process Editor and Visual Workflow Process Designer. These tools are available within a Blueprint.

Use the Automation Process Editor to:

- Create a Simple Action/Event Automation Process.
- Create a Threshold-Based Automation Process.
- Create an Automation Process Visual Workflow Process.
- Edit an Automation Process.
- Delete an Automation Process.
- Copy an Automation Process.

Use the Automation Process Visual Workflow Process Designer to:

- Define Visual Workflow Properties
- Define Visual Workflow Events
- Define Visual Workflow Actions

Related concepts
Define Automation Process Visual Workflow Properties
Define Automation Process Visual Workflow Events
Related tasks
Define Automation Process Visual Workflow Actions

Automation Process Manager

Use the Automation Process Manager to complete general CSM Item Manager operations for Automation Processes.

Open the Automation Process Manager from the CSM Administrator menu bar (in a Blueprint or mApp® Solution), by selecting **Managers > Automation Processes**.

Good to know:

- System is the only available scope. Create subfolders underneath this scope to organize items.

- Use the Manager Context (right-click) menu to quickly access menu bar/toolbar options.

- For more information about working in CSM Item Managers, refer to the Item Managers documentation.

Automation Process Editor

Use the Automation Process Editor to define, edit, and delete Automation Processes.

Create and define the following Automation Processes:

- Simple Action/Event Process
- Threshold-Based Process
- Automation Process Visual Workflow Process

The Automation Process Editor displays the list of Automation Processes with the following columns:

- **Automation Process**: The name of the process.
- **Business Object**: The type of Business Object against which the process operates.
- **Type**: The type of process (example: TimeBased).
- **Status**: If the process is enabled or disabled.
- **Priority**: If the process is low, normal, or high execution priority.
- **Trigger**: What sets off the process (example: Creation of a Business Object). If changing a specific field on the Business Object triggers the Automation Process, that field is listed in parentheses.
- **Description**: A description of the process (if entered when the process was set up).

Related tasks
Create a Simple Action/Event Automation Process
Create a Threshold-Based Automation Process
Create an Automation Process Visual Workflow Process

Open the Automation Process Editor

Open the Automation Process Editor from CSM Administrator.

To open the Automation Process Editor from the CSM Administrator main window, select the **Automation Process** category and then select **Create a New Automation Process Blueprint**.

Create a Simple Action/Event Automation Process

Use the **Simple Action/Event Automation Process** window (accessed from within the Automation Process Editor) to create a Simple Action/Event Automation Process.

To create a Simple Action/Event Process:

1. Open the Automation Process Editor.
2. Select the **New** button, and then select **Simple Action/Event Process**.
3. Define general properties: Name, description, Business Object, execution priority, and event.
4. Define record limitations: How to limit records, based on query, field, or expression.
5. Define an action: One-Step™ Action or action to run when the event takes place.

Important: If you are working with Automation Processes after a Protected mApp™ Solution has been applied to your system, note the following:

- If you create or open an Automation Process Blueprint which has a Protected mApp Solution installed, protected processes have shield icons ⊞.
- If you select a content-protected process and right-click, you cannot delete the process.
- If you edit a content-protected Threshold-Based, or Simple/Event Automation Process, you must use **Save As** to create a copy.
- If you view Automation Processes in a Blueprint or by opening an Automation .BP file from CSM Administrator, they cannot be edited in any way.
- See Protected mApp™ Solutions.

Related concepts

Open the Automation Process Editor

Protected mApp™ Solutions

Protected mApp™ Solution FAQs

Define General Properties for a Simple Action/ Event Automation Process
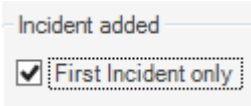
Use the **Simple Action/Event Automation Process** window to define general properties for the process.

To define general properties for a Simple Action/Event Automation Process:

1. Create a Simple Action/Event Automation Process.
2. Define general properties:
    - Provide a display name and brief description.
    - Select the type of Business Object against which the process will operate.
    - Select a priority level, which provides a hint to the Business Process Server as to the importance of the Automation Process. This allows the system to attempt to execute higher priority processes before normal or low priority processes.
    - Select an event to use to activate the Automation Process.

Event Type	Description
<Business Object> Created	The Automation Process starts when a <Business Object> is created.
<Business Object> Changed	**Any Change**: The Automation Process starts if any change is made to the <Business Object>. **Note:** Events that trigger based on any change made to Business Objects can greatly impact system performance. For best results, use the **Field Changed** option rather than the **Any Change** option. **Field Changed**: The Automation Process starts if the selected field is altered. You can choose to define if the Automation Process should operate when any change is made to the field, if the field changes to a value, if the field changes from a value, or if the field changes from one value to another. If you select **Field changes from one value to another**, ensure you complete the **To:** and **From:** fields. Use the **Legal Values** button [III] to choose a value. If you don't complete these fields, the Automation Process doesn't run.
<Business Object> Created or Changed	The Automation Process starts when a <Business Object> is created or changed.

Event Type	Description
<Business Object> Closed	The Automation Process starts when a <Business Object> is closed. You can include this same functionality in lifecycles created using the Business Object Lifecycle Editor by using transition rules and post-transition actions. See About Transitions and Add a Post-Transition Action.
<Business Object> Reopened	The Automation Process starts when a <Business Object> is reopened. You can include this same functionality in lifecycles created using the Business Object Lifecycle Editor by using transition rules and post-transition actions. See About Transitions and Add a Post-Transition Action.

Event Type	Description

Related Child Event	Select the relationship, and then select the type of change that triggers the Automation Process to operate:
	
	○ **<Business Object> Added**
	
	   For relationships that use direct links, events are created when the parent Business Object is saved.
	
	   For relationships that use join tables, events are created when each link is saved.
	
	   For one-to-many relationships, you can select the **First <Business Object> Only** checkbox to trigger the event for only for the first Business Object child created for the relationship.
	
	   Incident added
	   ☑ First Incident only
	
	○ **<Business Object> Record Modified**
	○ **<Business Object> Record Field Change**
	
	   You can define if the Automation Process should operate when any change is made to a specified field, if the field changes to a value, if the field changes from a value, or if the field changes from one value to another.
	
	   Also, the event will only fire if the Business Object is modified while working on the parent. For example, if you edit an Approval in the arrangement below a Change Request, the event fires, but if you edit the Approval by alone it doesn't). If you encounter either scenario, then a direct event associated with an Approval should be created.

Queue Event	○ Queue Event: Select the type of queue event that triggers the Automation Process to operate (**Record added to queue** or **Record removed from queue**). ○ Which Queue: Select the type of queue that should be considered (**Any queue**, **Any user queue**, **Any team queue**, or **Specific queue**).

3. Select **OK**.

Related tasks
Create a Simple Action/Event Automation Process

Define Record Limitations for a Simple Action/ Event Automation Process

Use the **Limit Records** page in the **Simple Action/Event Automation Process** window to define record limitations for the process.

Depending on how you want to limit records, you can choose to limit based on query, field, or an expression.

To define record limitations for a Simple Action/Event Automation Process:

1. Create a Simple Action/Event Automation Process.
2. Select the **Limit Records** page.
   The **Limit Records** section opens below the general properties.
3. Limit records based on Query: Only records for which the query (saved search) condition is true will cause the action to be executed when the event occurs.
   a. Select the **Query** check box.
      The **Query** drop-down list and **ellipsis** button become active.

   b. Select the **ellipsis** button [...] to open the Search Manager, where you can select a saved search or create a new saved search.
4. Limit records based on Field: Only records where the specified value is found in the specified field will cause the action to be executed when the event occurs.
   a. Select the **Field** check box.
      The **Field** and **Value** drop-down lists become active.

   b. From the **Field** drop-down list, select a field.

   c. From the **Value** drop-down list, select a value for the field.
5. Limit records based on an Expression: Only records for which the expression is true will cause the Action to be executed when the event occurs.
   a. Select the **Expression** check box.
      The **Expression** drop-down list, **ellipsis** button, and **Custom Expression** button become active.

   b. Define the Expression:

      ◦ Select an existing expression: Select the **ellipsis** button [...] to open the Expression Manager, and then select an expression.

      ◦ Create a custom expression: Select the **Custom Expression** button [fx], and then define a custom expression.
6. Select **OK**.

Related concepts
About Saved Searches
Create a Saved Search
Expressions
Related tasks

Create a Simple Action/Event Automation Process

Define Actions for a Simple Action/Event Automation Process

Use the **Action** page in the **Simple Action/Event Automation Process** window to define general properties for the process.

When you define actions, you define:

- The One-Step™ Action or Action to run when the event takes place.

🖊 **Note:** If you create a Save One-Step Action that saves child Business Objects before the parent Business Object is saved, those child events will not execute properly. Ensure you clear the **Execute before saving record** check box on the **Save Action** for the child events.

To define general properties for a Simple Action/Event Automation Process:

1. Create a Simple Action/Event Automation Process..
2. Select the **Actions** page.
   The **Actions** section opens below the general properties.
3. Define a One-Step Action to run when the event takes place:
   a. Select the **One-Step Action** option.
      The One-Step Action field and **ellipsis** button become active.

   b. Select the **ellipsis** button ⬚ to open the One-Step Action Manager, and then select an existing One-Step Action or create a new One-Step Action.
4. Define an Action to run when the event takes place:
   a. Select the **Execute Action** option.
      The **Execute Action** field and **Action** button become active.

   b. Select the **Action** button, and then select an available Action in the drop-down list.
5. Select **OK**.

Related concepts
Create/Edit a One-Step Action
Related tasks
Create a Simple Action/Event Automation Process
Related information
Problem: The field [BusinessObject].[Fieldname] must be filled in before the record can be saved

Create a Threshold-Based Automation Process

Use the **Threshold-Based Automation Process** window (accessed from within the Automation Process Editor) to create a Threshold-Based Automation Process. Define when and how an Action is run when a threshold is breached.

To create a Threshold-Based Automation Process:

1. Open the Automation Process Editor.
2. Select **New**, and then select **Threshold-Based Process**.
3. Define general properties:
   - Provide a name and description. You can search these properties in CSM Item Managers.
   - Select the type of Business Object against which this process will operate.
   - Select a priority level, which provides a hint to the Business Process Server as to the importance of the Automation Process. This allows the system to attempt to execute higher priority processes before normal or low priority processes.
4. Define the value that the Automation Process should monitor:
   a. Select the **Value** page.
      The **Value** page opens below the general properties.
   - **Number of Records**: Select this option to monitor the number of records that meet the defined criteria.
   - **Function**: Select this option to apply a mathematical function against a field (example: Average, total) if there is a numeric field on the records being evaluated.
   - **Duration Function**: Select this option to apply a mathematical function against the range of time between two time-based fields (example: Determining the average amount of time that Incidents take to resolve).

   If you select a duration function, you must specify the fields that define the start/end date times and the unit(s) to use (example: Hours, days, months).
5. Define criteria for the records included in the calculation:
   a. Select the **Criteria** page.
      The **Criteria** page opens below the general properties.

   - **Search Criteria**: Select the **ellipsis** [···] to select an existing saved search or select **Search** [🔍] to define a custom query to limit the records considered.
   - **Open Incidents Only**: Select the check box to only include open Incidents in the results.
6. Define one or more thresholds:
   a. Select the **Thresholds** page, and then define threshold properties:
      Use the **Check threshold values every** option to set how often threshold values should be checked. Checking begins when Automation Process is enabled or when an Automation Process Blueprint is published.
   - Define run Actions:

Option	Description
Every time value is checked (if the threshold is crossed):	Select this option to execute the action if the check is completed every hour and the value is above the threshold.
When the threshold is first crossed:	Select this option to execute the Action the first time the value is above the threshold, but not execute the Action again unless the *at least* operator is specified.
Each time a threshold is crossed:	Select this option to execute the Action the first time the value is above the threshold, but not execute the Action again until the value falls below the threshold at least once and then goes above the value again.
At least:	Specify this operator for the rules to be reconsidered. If the option is set to **When the Threshold is First Crossed** and the threshold is crossed, the Action will be executed a single time. If you specify that at least one day must pass between operations, then a day later the Action will be executed again if the threshold is crossed. This option is only available if you select the Automation Process to operate every time a value is checked or each time a threshold is crossed.

- Define thresholds:

Option	Description
Create a threshold	Select **Add** to add a threshold to the list.
Edit a threshold	Use the controls underneath the threshold list to customize the threshold.
Remove a threshold	Select **Remove** to permanently delete a threshold.
Reorder the threshold	Select **Reorder** to organize the threshold list. This option sorts all of the thresholds based on the threshold values, but does not affect the Threshold-Based Automation Process functionality.
Above/Below threshold	Specify whether the threshold should be considered breached when the value exceeds or falls below the threshold value.
Threshold value	Specify the value against which the returned result will be compared.

Option	Description
Action	Select or define a One-Step™ Action to run when the threshold is breached. **Note:** The Action must be an unassociated One-Step Action (not tied to a particular Business Object). This is necessary because there is no single record to operate against, just a single resulting value.

7. Select **Save**.

Important: If you are working with Automation Processes after a Protected mApp™ Solution has been applied to your system, note the following:

- If you create or open an Automation Process Blueprint which has a Protected mApp Solution installed, protected processes have shield icons .
- If you select a content-protected process and right-click, you cannot delete the process.
- If you edit a content-protected Threshold-Based, or Simple/Event Automation Process, you must use **Save As** to create a copy.
- If you view Automation Processes in a Blueprint or by opening an Automation .bp file from CSM Administrator, they cannot be edited in any way.

Related concepts

Open the Automation Process Editor

Protected mApp™ Solutions

Protected mApp™ Solution FAQs

Related tasks

Create an Automation Process Visual Workflow Process

Create an Automation Process Visual Workflow Process

Use the Automation Process Visual Workflow Process Designer (accessed from within the Automation Process Editor) to create a Visual Workflow Automation Process. Define complex workflow Automation Processes with a visual designer.

To create a Visual Workflow Automation Process:

1. Open the Automation Process Visual Workflow Process Designer.
2. Define general properties (such as start event and work hours), events (time and event criteria), and actions (such as Run One-Step™ Action or send email).

> **Important:** If you are working with Automation Processes after a Protected mApp™ Solution has been applied to your system, note the following:
>
> - If you create or open an Automation Process Blueprint which has a Protected mApp Solution installed, protected processes have shield icons 🛡.
> - If you select a content-protected process and right-click, you cannot delete the process.
> - If you edit a content-protected Threshold-Based, or Simple/Event Automation Process, you must use **Save As** to create a copy.
> - If you view Automation Processes in a Blueprint or by opening an Automation .BP file from CSM Administrator, they cannot be edited in any way.
> - See Protected mApp Solutions.

Related concepts
Define Automation Process Visual Workflow Properties
Define Automation Process Visual Workflow Events
Protected mApp™ Solution FAQs
Related tasks
Open the Automation Process Visual Workflow Process Designer

Edit an Automation Process Visual Workflow Process

Use the Automation Process Visual Workflow Process Designer (accessed from within the Automation Process Editor) to edit a Visual Workflow Automation Process.

To edit a Visual Workflow Automation Process:

1. Select **Automation Processes**, then **Create a new Automation Process Blueprint**.
2. Right-click on an Automation Process and select **Edit process**.
   The **Visual Workflow Process Properties** window opens.

3. Select **Save** in the **Visual Workflow Process Properties** window.
   The Automation Process Visual Workflow Process Designer opens.

4. Edit your Automation Process.

Open the Automation Process Visual Workflow Process Designer

Open the Automation Process Visual Workflow Process Designer from CSM Administrator.

To open the Automation Process Visual Workflow Process Designer:

1. Open the Automation Process Editor.
2. Select the **New** button, and then select **Visual Workflow Process**.
   The **Visual Workflow Process Properties** window opens.
3. Define Automation Process properties.
   a. Name and description: Provide a display name and description to use within CSM (search these properties in CSM Item Managers).
   b. Business Object: Select a Business Object to associate with the Automation Process.
   c. Execution Priority: Select a priority level, which provides a hint to the Business Process Server as to the importance of the Automation Process. This allows the system to attempt to execute higher priority processes before normal or low priority processes.
4. Select **OK**.

Related concepts
Open the Automation Process Editor

Define Automation Process Visual Workflow Properties

Use the Visual Workflow Process Designer to define general properties.

General properties are:

- **Start event**: Event that triggers the initiation of the Automation Process.
- **Work hours**: Business hours that will be used by the Automation Process to calculate time.
- **Record limitations**: Limitations of records that should be monitored.
- **Execution limitations**: Limitations as to when and how often the process should run.
- **Abort process**: Criteria used to determine if the process should be aborted.

Related concepts
Automation Process Visual Workflow Process Designer
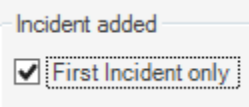
Define the Start Event for an Automation Process Visual Workflow Process

Use the **Start Event** page of the Automation Process Visual Workflow Process Designer to define the event that triggers the initiation of the Visual Workflow Automation Process.

To define the Start Event:

1. Open the Automation Process Visual Workflow Process.
2. Select the **Start Event** page in the left pane of the **Current Step Details** section.
3. Select an event to use to activate the Automation Process.

Event Type	Description
<Business Object> Created	The Automation Process will begin when a <Business Object> is created.
<Business Object> Changed	◦ **Any Change**: The Automation Process will begin if any change is made to the <Business Object>. **Note:** Events that trigger based on any change made to Business Objects can greatly impact system performance. For best results, use the **Field Changed** option rather than the **Any Change** option. ◦ **Field Changed**: The Automation Process will begin if the selected field is altered. You can choose define if the Automation Process should operate when any change is made to the field, if the field changes to a value, if the field changes from a value, or is the field changes from one value to another.
<Business Object> Created or Changed	The Automation Process will begin when a <Business Object> is created or changed.
<Business Object> Closed	The Automation Process will begin when a <Business Object> is closed.
<Business Object> Reopened	The Automation Process will begin when a <Business Object> is reopened.

Event Type	Description
Related Child Event	Select the relationship, and then select the type of change that will trigger the Automation Process to operate: ○ **<Business Object> Added** For relationships that use direct links, events are created when the parent Business Object is saved. For relationships that use join tables, events are created when each link is saved. For one-to-many relationships, you can select the **First <Business Object> Only** check box to trigger the event for only for the first Business Object child created for the relationship. Incident added ☑ First Incident only ○ **<Business Object> Record Modified** ○ **<Business Object> Record Field Change** You can define if the Automation Process should operate when any change is made to a specified field, if the field changes to a value, if the field changes from a value, or if the field changes from one value to another. Also, the event will only fire if the Business Object is modified while working on the parent. For example, if you edit an Approval in the arrangement below a Change Request, the event will fire, but if you edit the Approval alone it will not). If you encounter either scenario, then a direct event associated with an Approval should be created.

Event Type	Description
Queue Event	◦ Queue Event: Select the type of queue event that will trigger the Automation Process to operate (Record Added to Queue or Record Removed from Queue). ◦ Which Queue: Select the type of queue that should be considered (Any Queue, User Queue, Team Queue, or Specific Queue).

4. Select **OK**.

Related tasks

Create an Automation Process Visual Workflow Process

Define Work Hours for an Automation Process Visual Workflow Process

Use the **Work Hours** page of the Automation Process Visual Workflow Process Designer to define the Business Hours that will be used by the Automation Process to calculate passed time.

To define Business Hours for the Automation Process Visual Workflow Process:

1. Open the Automation Process Visual Workflow Process.
2. Select the **Work Hours** page in the left pane of the **Current Step Details** section.
3. Define Work Hours properties. These options affect the Wait for Time, Wait for Event, and Wait for Time or Event options listed under Events. The options affect the time that passes between each step.
   - 24x7: Calculates time passed between steps twenty-four hours a day/seven days a week.
   - Based on SLA: Calculates time passed between steps based on the Business Hours defined in the Service Level Agreement (SLA).
   - Working Hours: Calculates time passed between steps based on the defined Business Hours of your company.

   If you select Working Hours, you must also select specific Business Hours using the drop-down list. To create new Business Hours for the Automation Process, select the **ellipsis** button to access the Business Hours Manager.
4. Select **OK**.

Related tasks
Create an Automation Process Visual Workflow Process

Define Record Limitations for an Automation Process Visual Workflow Process

Use the **Limit Records** page of the Automation Process Visual Workflow Process Designer to limit records that are used by the Automation Process to calculate passed time.

To define limited records:

1. Open the Automation Process Visual Workflow Process.

2. Select the **Limit Records** page in the left pane of the **Current Step Details** section.

3. Limit records based on Query: Only records for which the query (saved search) condition is true will cause the action to be executed when the event occurs.
   a. Select the **Query** check box.
      The **Query** drop-down list and **ellipsis** button become active.
   b. Select the **ellipsis** button to open the Search Manager, where you can select a saved search or create a new saved search.

4. Limit records based on Field: Only records where the specified value is found in the specified field will cause the action to be executed when the event occurs.
   a. Select the **Field** check box.
      The **Field** and **Value** drop-down lists become active.
   b. Select a field and value.

5. Limit records based on an Expression: Only records for which the expression is true will cause the action to be executed when the event occurs.
   a. Select the **Expression** check box.
      The **Expression** drop-down list, **ellipsis** button, and **Custom Expression** button become active.
   b. Define the Expression:
      ◦ Select an existing Expression: Select the **ellipsis** button to open the Expression Manager, and then select an expression.

      ◦ Create a Custom Expression: Select the **Custom Expression** button and define a Custom Expression.

6. Select **OK**.

Related concepts
About Saved Searches
Create a Saved Search
Expressions
Related tasks
Create an Automation Process Visual Workflow Process

Define Execution Limitations for an Automation Process Visual Workflow Process

Use the **Limit Execution** page of the Automation Process Visual Workflow Process Designer to limit execution properties, which control when and how often the Automation Process should run.

To limit execution:

1. Open the Automation Process Visual Workflow Process.
2. Select the **Limit Execution** page in the left pane of the **Current Step Details** section.
3. Define execution properties:
   - Only run once: Select this option to run the process the first time the trigger event or Action occurs.
   - Run any number of times: Select this option to run the process every time the trigger event or Action occurs.
     - Do not start within: Select the check box, and then use the **Up** arrow and **Down** arrow to define the amount of time (number of hours or minutes) that must pass between Automation Process executions.
     - Do not start if process is already running: Select this check box to stop the process from running if the trigger event or Action occurs while the Automation Process is already running.
4. Select **OK**.

Related tasks
Create an Automation Process Visual Workflow Process

Define Abort Process for an Automation Process Visual Workflow Process

Use the **Abort Process** page of the Automation Process Visual Workflow Process Designer to define criteria used to determine when the process should be aborted.

To define the abort process:

1. Open the Automation Process Visual Workflow Process.
2. Select the **Abort Process** page in the left pane of the **Current Step Details** section.
3. In the **Abort Process If** section, select one or more criteria that must be met for the process to abort:
   - **Criteria used to initiate process is no longer valid:** Select the check box to end the process when the criteria defined on the **Start Event** page is no longer true.
   - Query: Select the check box and define the query (search group) to end the process when records for which the query condition is true.
   - **Field/Value:** Select the check box and define the field and value to end the process when the specified value is found in the specified field.
   - **Expression:** Select the check box and select or define an expression to end the process when the specified expression is true.
   - **Incident Closed:** Select the check box to end the process when the Business Object record reaches the final stage of its lifecycle (example: closed). See Example: Create a Lifecycle.
4. In the **Check for Abort** section, select when the process should check for the abort condition(s) to be true:
   - **Before each step starts:** Select this option to check if the abort process criteria is true before each step takes place.
   - **After each step executes:** Select this option to check if the abort process criteria is true after each step takes place.
5. Select **OK**.

Related tasks
Create an Automation Process Visual Workflow Process

Define Automation Process Visual Workflow Events

Use the **Events** section of the Automation Process Visual Workflow Process Designer to define time and event criteria that trigger an Action to take place.

Note: As you drag the icon onto the Designer Board, the locations where the icon can be dropped highlight as the cursor passes over them.

Time and event criteria are:

- Wait for Time: Steps that wait for a defined amount of time before the process continues to the next step.
- Wait for Event: Steps that wait for a defined event before the process continues to the next step.
- Wait for Time or Event: Steps that wait for a defined time or event (whichever occurs first) before the process continues to the next step.

Related tasks

Define a Wait for Time for an Automation Process Visual Workflow Process
Define a Wait for Event for an Automation Process Visual Workflow Process
Define a Wait for Time or Event for an Automation Process Visual Workflow Process

Define a Wait for Time for an Automation Process Visual Workflow Process

Use the **Events** section of the Automation Process Visual Workflow Process Designer to define a wait for time, which includes the steps that wait for a defined amount of time before the process continues to the next step.

To define Automation Process Visual Workflow Process time options:

1. Open the Automation Process Visual Workflow Process Designer.

2. Drag the **Wait for Time** icon onto the Designer Board.
   The **Wait for Time** page opens in the **Current Step Details** section of the designer.

3. Define time criteria for the step:
   - Wait from: Select the amount of time that the Automation Process should wait before watching for the process trigger.
   - How Long: Select how long the step should wait until continuing to the next step.
       - Specific Time: Select the amount of time (number of days, hours, minutes quarters, weeks, years) to use for the calculation. You can also define this option based on a specified time before or after a calendar item.
       - Field Based: Select a Calendar or SLA field to use for the calculation. If you select an SLA field, you also have the option to define the time increment (days, weeks) and/or the specific time before or after another calendar item
       - SLA Based: Select a defined SLA to use for the calculation.

4. Select **OK**.

Related concepts
Automation Process Visual Workflow Process Designer

Define a Wait for Event for an Automation Process Visual Workflow Process
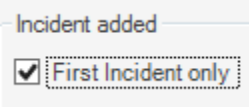
Use the **Events** section of the Automation Process Visual Workflow Process Designer to define a wait for event, which includes the steps that wait for a defined event before the process continues to the next step.

To define Automation Process Visual Workflow Process Event options:

1. Open the Automation Process Visual Workflow Process Designer.

2. Drag the **Wait for Event** icon [icon] onto the Designer Board.
   The **Wait for Event - Event** page opens in the **Current Step Details** section of the designer.

3. From the **Wait from** drop-down list, select the amount of time that the Automation Process should wait before watching for the process trigger.

4. Select an event to use to activate the Automation Process.

Event Type	Description
<Business Object> Created	The Automation Process will begin when a <Business Object> is created.
<Business Object> Changed	◦ **Any Change**: The Automation Process will begin if any change is made to the <Business Object>. **Note:** Events that trigger based on any change made to Business Objects can greatly impact system performance. For best results, use the **Field Changed** option rather than the **Any Change** option. ◦ **Field Changed**: The Automation Process will begin if the selected field is altered. You can choose define if the Automation Process should operate when any change is made to the field, if the field changes to a value, if the field changes from a value, or is the field changes from one value to another.
<Business Object> Created or Changed	The Automation Process will begin when a <Business Object> is created or changed.
<Business Object> Closed	The Automation Process will begin when a <Business Object> is closed.

Event Type	Description
<Business Object> Reopened	The Automation Process will begin when a <Business Object> is reopened.

Event Type	Description
Related Child Event	Select the relationship, and then select the type of change that will trigger the Automation Process to operate: ◦ **<Business Object> Added** For relationships that use direct links, events are created when the parent Business Object is saved. For relationships that use join tables, events are created when each link is saved. For one-to-many relationships, you can select the **First <Business Object> Only** check box to trigger the event for only for the first Business Object child created for the relationship. Incident added ☑ First Incident only ◦ **<Business Object> Record Modified** ◦ **<Business Object> Record Field Change** You can define if the Automation Process should operate when any change is made to a specified field, if the field changes to a value, if the field changes from a value, or if the field changes from one value to another. Also, the event will only fire if the Business Object is modified while working on the parent. For example, if you edit an Approval in the arrangement below a Change Request, the event will fire, but if you edit the Approval by alone it will not). If you encounter either scenario, then a direct event associated with an Approval should be created.

Event Type	Description
Queue Event	◦ Queue Event: Select the type of queue event that will trigger the Automation Process to operate (Record Added to Queue or Record Removed from Queue). ◦ Which Queue: Select the type of queue that should be considered (Any Queue, User Queue, Team Queue, or Specific Queue).

5. Select the **Time Limit** page in the left pane of the **Current Step Details** section to define a time limit for the step:

> **Note:** If you select any option in this section other than **No Time Limit**, the *Wait for Event* step changes to Wait for Time or Event and a new Wait for Time branch displays on the Designer Board.

- ◦ Wait for Time: Step that waits for a defined amount of time before the process continues to the next step:
  - ◦ Wait from: Select the action that triggers the process to begin waiting for the event.
  - ◦ How Long: Select how long the step should wait until continuing to the next step:
    - ◦ Specific Time: Select the amount of time (number of days, hours, minutes quarters, weeks, years) to use for the calculation. You can also define this option based on a specified time before or after a calendar item.
    - ◦ Field Based: Select a Calendar or SLA field to use for the calculation. If you select an SLA field, you also have the option to define the time increment (days, weeks,) and/or the specific time before or after another calendar item
    - ◦ SLA Based: Select a defined SLA to use for the calculation.
    - ◦ No Time Limit. (Default)

6. Select **OK**.

Define a Wait for Time or Event for an Automation Process Visual Workflow Process
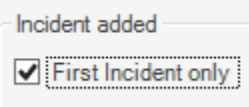
Use the **Events** section of the Automation Process Visual Workflow Process Designer to define a wait for time or event, which includes the steps that wait for a defined time or event (whichever occurs first) before the process continues to the next step.

To define Automation Process Visual Workflow Process Event options:

1. Open the Automation Process Visual Workflow Process Designer.

2. Drag the **Wait for Time or Event** icon onto the Designer Board.
   The **Wait for Event - Event** page opens in the **Current Step Details** section of the designer.

3. From the **Wait from** drop-down list, select the amount of time that the Automation Process should wait before watching for the process trigger.

4. Select an event to use to activate the Automation Process.

Event Type	Description
<Business Object> Created	The Automation Process will begin when a <Business Object> is created.
<Business Object> Changed	◦ **Any Change**: The Automation Process will begin if any change is made to the <Business Object>. **Note:** Events that trigger based on any change made to Business Objects can greatly impact system performance. For best results, use the **Field Changed** option rather than the **Any Change** option. ◦ **Field Changed**: The Automation Process will begin if the selected field is altered. You can choose define if the Automation Process should operate when any change is made to the field, if the field changes to a value, if the field changes from a value, or is the field changes from one value to another.
<Business Object> Created or Changed	The Automation Process will begin when a <Business Object> is created or changed.
<Business Object> Closed	The Automation Process will begin when a <Business Object> is closed.

Event Type	Description
<Business Object> Reopened	The Automation Process will begin when a <Business Object> is reopened.

Event Type	Description
Related Child Event	Select the relationship, and then select the type of change that will trigger the Automation Process to operate: ○ **<Business Object> Added** For relationships that use direct links, events are created when the parent Business Object is saved. For relationships that use join tables, events are created when each link is saved. For one-to-many relationships, you can select the **First <Business Object> Only** check box to trigger the event for only for the first Business Object child created for the relationship. Incident added ☑ First Incident only ○ **<Business Object> Record Modified** ○ **<Business Object> Record Field Change** You can define if the Automation Process should operate when any change is made to a specified field, if the field changes to a value, if the field changes from a value, or if the field changes from one value to another. Also, the event will only fire if the Business Object is modified while working on the parent. For example, if you edit an Approval in the arrangement below a Change Request, the event will fire, but if you edit the Approval by alone it will not). If you encounter either scenario, then a direct event associated with an Approval should be created.

Event Type	Description
Queue Event	◦ Queue Event: Select the type of queue event that will trigger the Automation Process to operate (Record Added to Queue or Record Removed from Queue). ◦ Which Queue: Select the type of queue that should be considered (Any Queue, User Queue, Team Queue, or Specific Queue).

5. Select the **Time Limit** page in the left pane of the **Current Step Details** section to define a time limit for the step.
   If you select any option in this section other than **No Time Limit**, the *Wait for Event* step will change to Wait for Time or Event and a new Wait for Time branch will appear on the Designer Board.
      ◦ Wait for Time: Step that waits for a defined amount of time before the process continues to the next step.
         ◦ Wait from: Select the action that triggers the process to begin waiting for the event.
         ◦ How Long: Select how long the step should wait until continuing to the next step:
            ◦ Specific Time: Select the amount of time (number of days, hours, minutes quarters, weeks, years) to use for the calculation. You can also define this option based on a specified time before or after a calendar item.
            ◦ Field Based: Select a Calendar or SLA field to use for the calculation. If you select an SLA field, you also have the option to define the time increment (days, weeks,) and/or the specific time before or after another calendar item
            ◦ SLA Based: Select a defined SLA to use for the calculation.
            ◦ No Time Limit. (Default)

6. Select **OK**.

Define Automation Process Visual Workflow Actions

Use the **Actions** section of the Automation Process Visual Workflow Process Designer to define one or more Actions, which occur as a result of a time or event trigger.

Good to know:

- If you want more than one Action to take place, drag additional Actions onto the Designer Board and organize them as desired. You can change the behavior of an Action in the Current Step Details pane below the Designer Board. Alternatively, you can double-click the Action to view an associated Manager or editor for the Action (example: One-Step™ Action Manager).

- When you drag a Jump Step onto the Designer Board, the Jump icon displays on steps that allow the Action.

To define Automation Process Visual Workflow Process Actions:

1. Open the Automation Process Visual Workflow Process Designer.
2. Drag one or more Actions to the Designer Board:

Option	Description
Run One-Step Action	Run a One-Step Action when the defined time or event occurs.
Send Email	Send an email when the defined time or event occurs to inform a user that the event has taken place. Edit the email content by selecting the **Send Email** link in the **Execute Action** field.
Tweet	Compose a Tweet to inform users or customers that an event has taken place. Edit the Tweet by selecting the **Send Tweet** link in the **Execute Action** field.
Update Bus Ob	Update a field in a Business Object. Edit the Business Object by selecting the **Update Business Object** link in the **Execute Action** field.
Create Child	Create a child Business Object (example: Journal, Task, Customer Survey). Edit the child Business Object by selecting the **Create Child Business Object** link in the **Execute Action** field.
Queue Action	Add the record to a specific queue.

Option	Description
Jump to Step	Jump to a specific step in the Automation Process. Select the step using the drop-down list.
Jump to End	End the Automation Process if the previous step takes place.

3. Select **OK**.

Related tasks

Open the Automation Process Visual Workflow Process Designer

Automation Process Visual Workflow Process Designer

A Visual Workflow Process defines a sequence of time-based and Event-based steps that manage a Business Object as it passes through various stages. The Visual Workflow Process Designer is a tool that allows you to easily create simple or complex automation processes to help manage workflows in CSM.
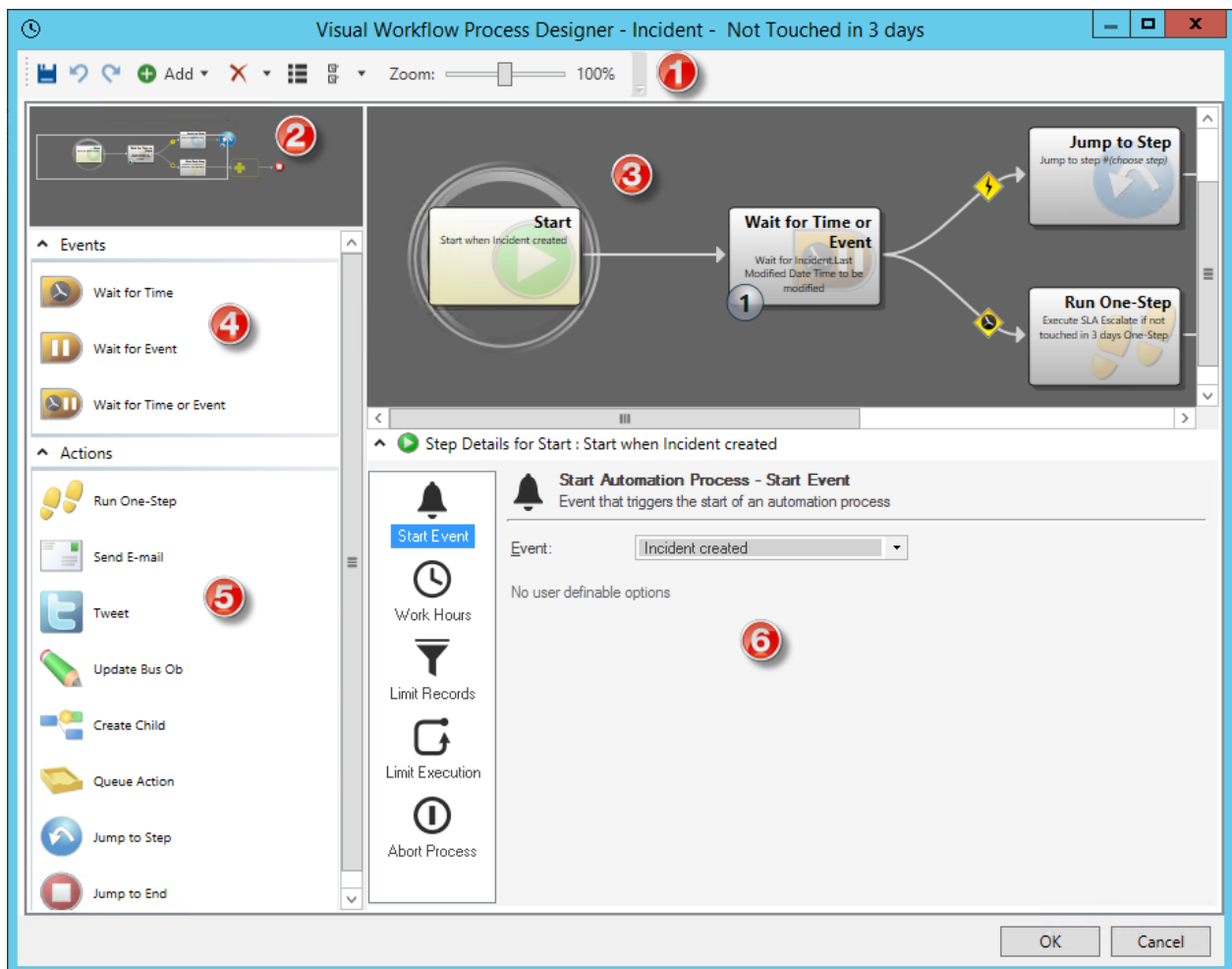
1. Toolbar: Commonly used Visual Workflow Process Designer tasks.

2. Aerial View: View the entire process as you zoom in and out. Also allows you to move the section of the current process on the Designer Board.

3. Designer Board: A visual representation of the process.

4. Events Pane: Time and event options that trigger an Action to occur.

5. Actions Pane: Actions that take place as a result of a time or event trigger.

6. Step Details: Details of the currently selected step in the process.

A new Automation Process Visual Workflow Process Designer Board includes the following elements:
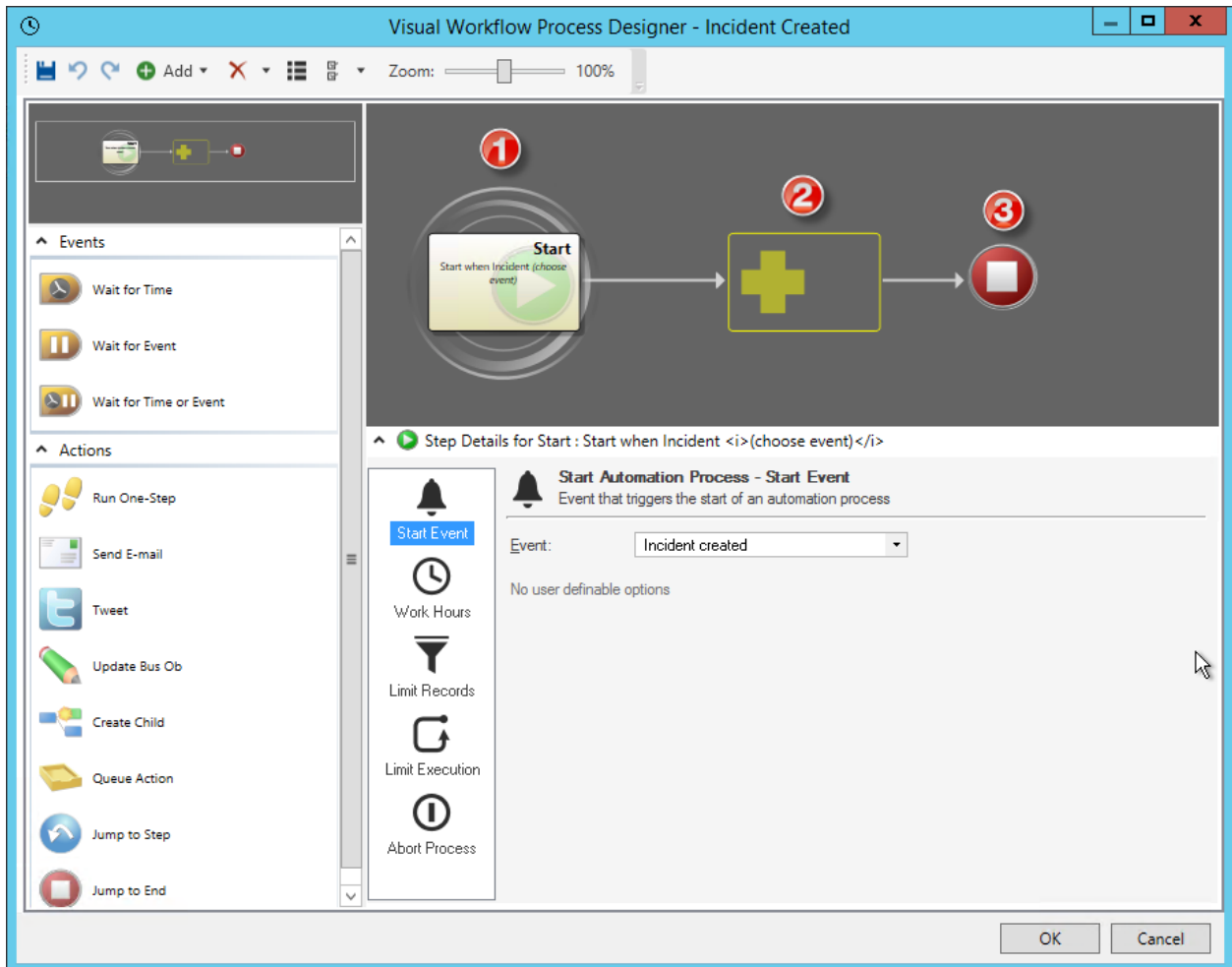
1. Start Graphic: Event or starting point that initiates the process.

   Note: Select the Start Graphic on the Designer Board to define general properties for the process.

2. Placeholder Graphic: Holds the steps (Events and/or Actions) that constitute the process.

3. End Graphic: Indicates the end of the process.

Related concepts

Automation Process Visual Workflow Process Designer Toolbar

Define Automation Process Visual Workflow Events

Related tasks

Define Automation Process Visual Workflow Actions

Automation Process Visual Workflow Process Designer Toolbar

Use the Automation Process Visual Workflow Process Designer toolbar to quickly access common operations.

Button	Action	Description
💾	**Save**	Saves the current process (CTRL+S).
↩	**Undo**	Undoes the last change to the current process (CTRL+Z).
↪	**Redo**	Redoes the last change to the process (CTRL+V).
⊕ Add ▾	**Add a Child Step**	Add a new child (event or action) to the currently selected step.
✗ ▾	**Delete**	Deletes the currently selected step/action, the step/action and children, or the entire diagram.
≣	**Edit Properties for the Process**	Edit Visual Workflow Process Properties, including name, description, Business Object, and execution priority.
▾	**Define Preferences for the Designer/Editor**	Edit Designer/Editor options, including layout, arrow options, size, and animation.
Zoom: ▭ 100%		Increases or decreases the size of the diagram on the Designer Board.

Open an Existing Automation Process Blueprint

Automation Processes are edited within a Blueprint because they rely on Business Object logic.
Blueprints also allow you to set up multiple Automation Processes at one time, then publish them as a set.

To open an existing Automation Process Blueprint:

1. Open CSM Administrator.
2. Select **Automation Processes**.
3. Select **Open an existing Automation Process Blueprint**.
4. Select a Blueprint (.bp) file.
5. Select **OK**.

Important: If you are working with Automation Processes after a Protected mApp™ Solution has been applied to your system, note the following:

- If you create or open an Automation Process Blueprint which has a Protected mApp Solution installed, protected processes have shield icons .
- If you select a content-protected process and right-click, you cannot delete the process.
- If you edit a content-protected Threshold-Based, or Simple/Event Automation Process, you must use **Save As** to create a copy.
- If you view Automation Processes in a Blueprint or by opening an Automation .BP file from CSM Administrator, they cannot be edited in any way.
- See Protected mApp™ Solutions.

Related concepts
Protected mApp™ Solutions
Protected mApp™ Solution FAQs
Related tasks
Create a Simple Action/Event Automation Process

Delete Automation Processes

To optimize performance, delete unused Automation Processes to ensure that events are not triggered and sent to the Automation Process microservice for processing.

Alternatively, you can disable Automation Processes. Events will be triggered, but not processed. See Enable or Disable an Automation Process.

To delete an Automation Process:

1. In CSM Administrator, select the **Automation Processes** task.
2. Select **Create a New Automation Process Blueprint**.
3. Select an Automation Process, right-click, and then select **Delete process**.
   Select **File > Publish Blueprint**.

Use Automation Processes

You can perform several administration tasks for Automation Processes outside of a Blueprint. For example, you can enable and disable one or more Automation Processes and pause and resume Automation Process processing.

Enable or Disable an Automation Process

Use CSM Administrator to enable Automation Processes, which activates processing based on rules and events in the system. When you disable Automation Processes, events are still activated but are not processed by the Automation Process Service.

Alternatively, you can delete unused Automation Processes to ensure that events are not triggered and sent to the Automation Process Service for processing. See Delete Automation Processes.

To change the status of an Automation Process:

1. Select the **Automation Processes** category in CSM Administrator.
2. Select **Individual Automation Process Status**.
3. Select one or more Automation Processes, right-click, and then select a status:
   ◦ Select **Enable** to activate the Automation Process.
   ◦ Select **Disable** to inactivate the Automation Process so it is not processed when events are fired.

Pause/Resume Automation Process Processing

Use the Pause/Resume Processing task to temporarily pause and then resume Automation Process Service processing. This does not stop the Automation Process Service; rather, it suspends the microservice so that, when resumed, the microservice can pick up where it left off.

For example, pause processing to suspend sending out automatic emails; resume processing to continue sending out automatic emails. The ability to pause or resume Automation Processing is controlled by Automation Process Service security rights.

> **Note:** When you pause or resume processing, it could take up to five minutes for the pause or resume operation to take effect. To immediately pause or resume processing, use the Server Manager to disable the Automation Process microservice.

To pause or resume Automation Process Service processing:

1. CSM Administrator main window, select the **Automation Processes** category, and then select the **Pause/Resume Processing** task.
2. Select to pause or resume:
   a. **Pause Automation Process Microservice**: Select the check box to pause processing. You must provide a reason for pausing processing.
   b. **Resume Automation Process Microservice Processing**: Select the check box to resume processing.
3. Select **OK**.

Related concepts
Automation Process Service Security Rights
About the Server Manager

Monitor Automation Process Statistics

Use CSM Administrator to monitor Automation Process statistics such as completed runs (including successes and failures), in-progress runs, and scheduled activities. You can monitor these statistics for individual Automation Processes.

To view Automation Process statistics:

1. CSM Administrator, select **Automation Processes > Individual Automation Process Status**. The **Automation Process Status** window displays the list of Automation Processes with several columns. For the list of columns, see Automation Process Editor.

2. Select an Automation Process, and then select **Process > Statistics** from the toolbar. You can also right-click the Automation Process and select **Statistics**. The **Automation Process Statistics** window displays.

3. Select **OK**.

4. To refresh statistics while viewing the **Automation Process Statistics** window, select **Refresh**.

To clear Automation Processes:

1. From the **Automation Process Statistics** window, select **Clear Process**.

2. Select these options to delete the items:
   ◦ **Clear scheduled activities**: Clears activities that are currently scheduled for the Automation Process.

   ◦ **Clear in-progress items**: Clears activities that are in progress.

   ◦ **Clear completed item history**: Clears statistics for all completed runs for the Automation Process. Use this option only if you do not need the history of completed runs for an Automation Process.

3. Select **OK**.

View Automation Processes for a Single Record

You can view the Automation Processes that have run for a specific record, including detailed status information for each run.

To view Automation Processes for a single record:

1. In the CSM Desktop Client, open a record (example: Incident).
2. From the toolbar, select **Tools > Current Record Automation Processes**.
   A list of Automation Processes that run opens.
   - Select a specific Automation Process, and then select **Details** to view information about the run.
   - Select **Refresh** to update the list with new run records.

> **Tip:** If you are navigating through a set of records, keep the **Automation Processes run against** dialog open to see the Automation Processes that have run for each record.

Configure Automation Processes

Configure security rights for Automation Process Blueprints and the Automation Process Service.

To configure Automation Processes:

1. Configure Automation Process Blueprint security rights: Configure who can access Automation Process Blueprint functionality.
2. Configure the Automation Process Server security rights: Configure who can access Automation Process Service functionality.

Related concepts

Automation Process Blueprints Security Rights
Automation Process Service Security Rights

Automation Process Workflow

Automation Processes are processed and run by the Automation Process Service, which is a microservice of the Cherwell Service Host. Once Automation Process events are logged, they are collected in blocks of 100, and then sent to the Cherwell Message Queue Service (CherwellMQS). Additional workers are added if needed, the events are scheduled, and then they are run.
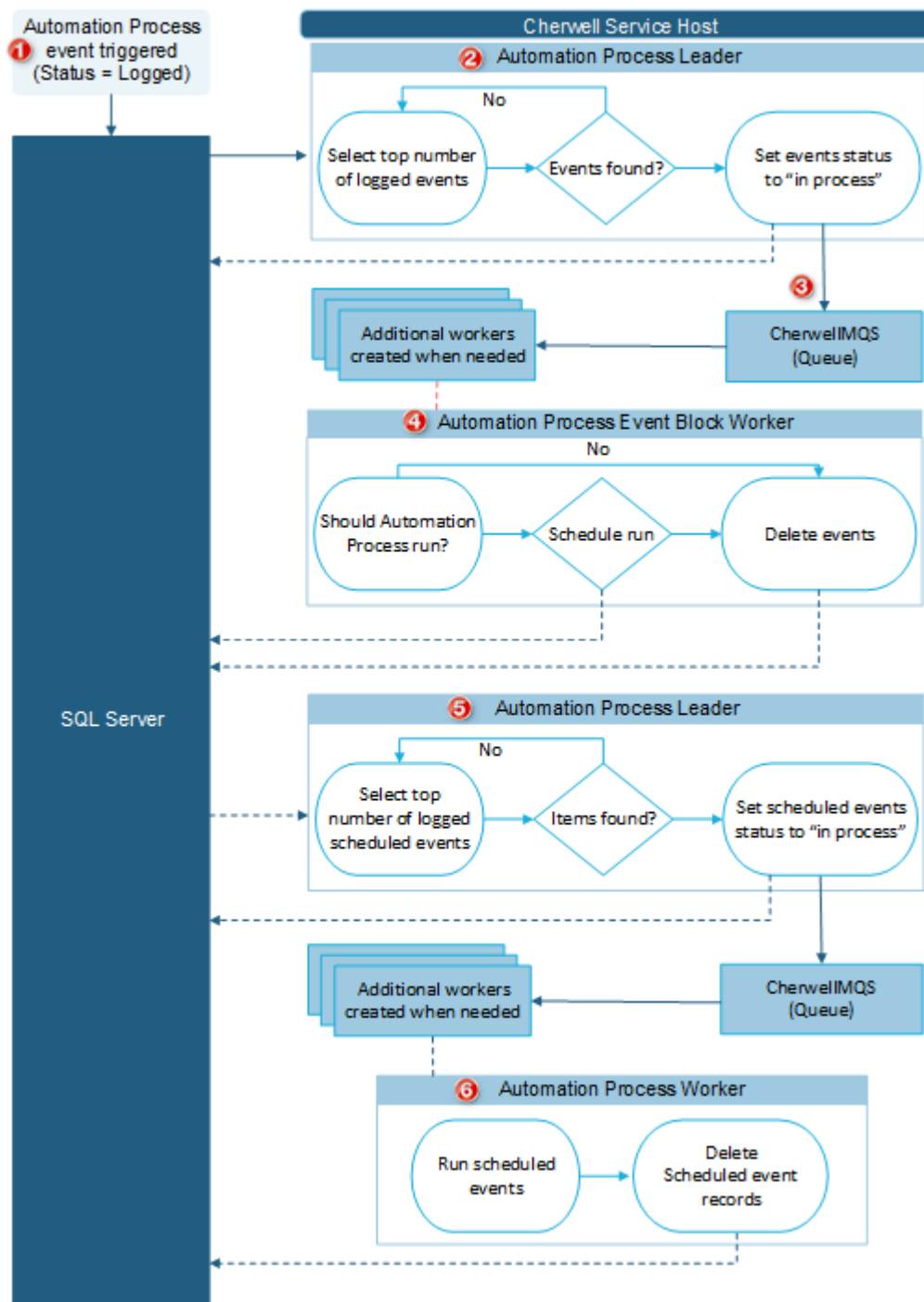
1. Events are triggered and added to the database with a status of "logged."

2. The Automation Process leader continually searches for events with a status of "logged." When events are found, their status is changed to "in process." Events are collected in blocks of 100.

3. Events are published to the queue in blocks of up to 100.

4. The Automation Process Event Block Worker picks up the block message from the queue and evaluates each event to determine if it is valid and should run. For each valid event, a scheduled event record is created with a status of "logged." All processed events are deleted.

5. The Automation Process Leader continually searches for scheduled events with a status of "logged." When scheduled events are found, their status is changed to "in process" and they are published to the queue.

> **Note:** Scheduled events are handled individually and not in blocks.

6. The Automation Process worker picks up messages from the queue and the Automation Process is run. The scheduled event is then deleted.

Related concepts

About the Cherwell Service Host

Performance Considerations for Automation Processes

Performance Considerations for Automation Processes

Because Automation Processes rely on Business Object logic, be sure to optimize configurations that might impact performance. This is especially important in high-load systems that have a large number of concurrent users or a high rate of record creation and updates.

Use these general approaches to configure performance friendly Automation Processes:

- Simpler is better, in terms of performance:
    - Do not reuse common, high-use One-Step™ Actions as the event that triggers Automation Processes or as the Action executed by a large number of Automation Processes.
    - Simplify the Actions performed by each Automation Process.
- Minimize activation by deleting disabled or unnecessary Automation Processes.
- Constrain the number of records evaluated by each Automation Process. For example, when you use a query to limit the number of records to evaluate, configure the query so that it returns the fewest records as possible. If you use a **Related child event** to trigger the Automation Process, use a Relationship that will evaluate the fewest number of records.

Delete Unused Automation Processes

Disabled Automation Processes continue to generate events, but these events are not processed by the Automation Process Service. This can cause performance bottlenecks.

For example:

- An Automation Process fires when the **Status** field on an Incident changes from Open to Closed. The Automation Process is evaluated each time an Incident is saved and an event is sent for processing, which is ignored if the Automation Process is disabled.
- When a disabled Automation Process has an **Execution Priority** of High, events are generated with high priority, which means they are evaluated by the server sooner than lower priority events.
- Scheduled data imports might update thousands of records at one time, which could send a large number of events to the Automation Process Service.

To help resolve bottlenecks, consider deleting rather than disabling Automation Processes that are not needed since disabled Automation Processes continue to produce a load on the system. See Delete Automation Processes.

Avoid "Any Change" Event Types

You can configure Visual Workflow and Simple Action/Event Automation Process types to trigger when any change is made to a specific type of Business Object. In heavy load systems, this can result in a large number of events being triggered that in many cases may not be needed.

Rather than triggering Automation Processes based on any change, use a more restricted condition when possible to avoid triggering unnecessary Automation Processes.

For example, configure "any change" event types to trigger based on changes made to a specific field. For an Automation Process that notifies an owner than an incident has been assigned to someone else, set the **Event Type** to **Field Changed**, and then select the **Assigned to** field.

See Define General Properties for a Simple Action/Event Automation Process and Define the Start Event for an Automation Process Visual Workflow Process.

Use a Calculation to Evaluate Multiple Field Values

If you need to evaluate multiple fields to trigger an Automation Process, consider creating a new field that has a calculated value. You can then configure your Automation Process to trigger on changes to that field.

This reduces the load on the system by evaluating a single field for a specific situation.

For example, if you want an Automation Process to create tasks when either the status of an Incident changes from Pending Approval to New or the source of the Incident was not Portal, create a logical field called **Ready for Tasks** that has a calculated value. Then, set the Automation Process to trigger from the **Ready for Tasks** field.

Simplify One-Step Actions

Design One-Step Actions to be as efficient as possible. For example:

- Avoid unnecessary saves if the same Business Object is updated multiple times.

- Do not configure refreshes that occur when the One-Step Action is run.

- If your One-Step Action is designed to update a Business Object, consider setting the **Update a Business Object** Action for the Automation Process instead of creating an additional One-Step Action.

Additional Information

If you set up a One-Step Action to update a Business Object, consider setting the Update a Business Object Action for the Automation Process instead of creating an additional One-Step Action .

Note: The Update Business Object Action cannot be used instead of refresh commands if the Business Object Association is "None" or if the step is part of a "Step through children" branch of a One-Step Action .

Related concepts
Automation Process Workflow
Related tasks
Define Record Limitations for a Simple Action/Event Automation Process
Define Record Limitations for an Automation Process Visual Workflow Process

Webhooks

Use webhooks to integrate CSM with external tools using HTTP POST methods to send data to a CSM webhook endpoint. A One-Step Action assigned to each endpoint determines how the data is consumed by CSM.

For example, use a webhook to update a CSM Incident with information from a Jira issue based on a defined event in Jira. Once the Jira event is triggered, data is sent to CSM, which fires a One-Step Action to update mapped fields in the Incident.
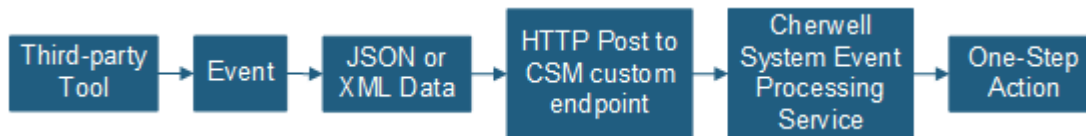
Related concepts

About Webhooks in CSM

Webhooks Process

Configure One-Step Actions for Webhooks

Related tasks

Create a Webhook Endpoint

About Webhooks in CSM

Webhooks process incoming messages triggered by events fired in third-party tools and sent to a CSM endpoint. Incoming data must be valid JSON or XML. You can configure webhook endpoints to use no authentication or basic authentication.

Webhooks Processing

Incoming webhooks are processed by the Cherwell REST API, which:

- Validates that the information passed to it is a valid webhook and that a valid URL is provided.
- Validates that the format type declared in an incoming message header matches the body format. If they do not match, the request is rejected.
- Validates an incoming message does not exceed the webhook limit specified for your system. This limit is set on the **Set REST API URL and Webhook Settings** dialog. The default size limit is 100,000 characters. For more information, see Set the Base URL for the Cherwell REST API.
- Provides a response code to the sender.

For more information, see Webhook Logging.

Parsing JSON or XML Data

Webhooks use JSON and XML Modifiers configured for One-Step Actions to parse, change, and use data between an external tool and CSM. For JSON, incoming data must be either a valid JSON object or array.

Use these methods to convert valid JSON or XML strings into data that CSM can consume:

1. **Use the Update Variables or Stored Values Action**
Use this Action to create a variable that declares a data type of JSON, JSON Array, XML, or XML Collection and holds valid string data of the selected data type. Place the Action at the beginning of a One-Step Action to ensure the variable is available to all Actions through the Token menu. For more information, see Define an Update Variables or Stored Values Action.

2. **Use a Token as a Webhook Value**
Create a webhook body token and add JSON or XML Modifiers to parse data as part of a One-Step Action. When you create the first Modifier, select As JSON or As XML to declare the data type. You can then chain Modifiers below that to parse complex data sent to the webhook. For more information, see Webhook Modifier Examples.

Webhooks Authentication

The type of authentication you set for your webhook endpoint depends on the third-party tool from which events are fired.

For example, Amazon Simple Notification Services (SNS) uses basic authentication for webhooks. Other tools, such as Jira Software, can use no authentication.

Using CSM Webhooks with Amazon Web Services (AWS)

CSM can use Amazon Simple Notification Services (SNS) as a webhook provider.

SNS initiates events by sending an unauthorized request to CSM. The Cherwell REST API sends a 401 response and sets the header to basic authentication. Amazon then resends the message with authentication information. The Amazon URL should include authentication information in this format: https://username:password@webhook_endpoint.

> **Note:** When a webhook is configured for Basic Authentication and uses Amazon SNS as a provider type, certain special characters in the username or password fields must be UTF-8 encoded when the subscription request is performed by Amazon.
> Form example: `https://CSM_User:p%40assword@yourcompany.com/webhookendpoint`
>
> Should be encoded as: `https://CSM%5FUser:p%40ssword@yourcompany.com/webhookendpoint`

You should configure webhook endpoints in CSM before configuring the subscription in Amazon. Endpoints must be in HTTPS format.

When you create a webhook in CSM, select **Amazon SNS** from the **Provider Type** drop-down list on the **General** page of the **Webhook** dialog. For more information, see Create a Webhook Endpoint.

Related concepts
Manage Webhooks
Webhooks Security Rights
Webhook Modifier Examples
Webhook Logging

Webhooks Process

The general process for implementing webhooks is to configure security and applicable CSM services, set the base URL for the Cherwell REST API, configure a webhook endpoint, and use One-Step Actions with Modifiers to map data between an external tool and CSM.

Task	Notes
1. In CSM Administrator, grant webhooks security rights to: • **Users who will manage webhooks** These are typically administrators or developers who will be creating webhooks, mapping data between CSM and the external tool, etc. Grant webhooks managers rights to view, add, edit, and delete webhooks as appropriate. • **Anonymous Browser Security Group** You must grant View rights to this group before POST requests can be sent to webhooks.	See Webhooks Security Rights.
2. Verify that these services are configured and running: • Cherwell Message Queue Service • System Event Processing Service (a microservice of the Cherwell Service Host) • Cherwell Service Host	See: Configure CherwellMQS/RabbitMQ Enable the System Event Processing Service Configure the Cherwell Service Host
3. Verify the base URL for the Cherwell REST API and maximum webhook content length.	See Set the Base URL for the Cherwell REST API.
4. In CSM Administrator, create a webhook endpoint.	See Create a Webhook Endpoint.
5. Create a One-Step Action that includes JSON or XML modifiers on the webhook body token to parse data from an external tool to CSM records.	See Configure One-Step Actions for Webhooks.
6. Create an event in the external tool that will post to CSM, and capture the JSON and XML data that will be sent to CSM.	See the documentation for the external tool.
7. Test the One-Step Action assigned to your webhook using the data captured from the external event.	See Test One-Step Actions Assigned to Webhook Endpoints.
8. Modify data mapping as needed.	See Webhook Modifier Examples.

Related concepts

Configure One-Step Actions for Webhooks

Webhook Modifier Examples

Related tasks

Create a Webhook Endpoint

Enable the System Event Processing Service

The System Event Processing Service is used primarily for webhooks and must be manually enabled before incoming events can be processed. The other services used for webhooks (Cherwell Service Host and Cherwell Message Queue Service) are typically enabled for most CSM systems, but you should verify this.

To enable the System Event Processing Service:

1. Log in to a CSM server instance.
2. Search for or navigate to the Cherwell Server Manager.
3. From the **Server** drop-down list, select Cherwell Service Host.
4. Select the **Configure** button in the top section.
5. Select the **Advanced Settings** button.
6. Select the **System Event Processing Service** check box.
7. Select **OK**.
8. When you are prompted to restart the server, select **Yes**.

Related concepts
Using the Server Manager
About the Cherwell Service Host

Manage Webhooks

Use the Webhooks Manager to add, edit, and delete webhook endpoints.

Related concepts

About Webhooks in CSM

Webhooks Security Rights

Webhook Modifier Examples

Open the Webhooks Manager

The Webhooks Manager is only available in CSM Administrator.

To open the Webhooks Manager:

1. From the main window, select the **Browser and Mobile** category, and then select **Open Webhook Manager**.
2. From a Blueprint or mApp Solution, select **Managers > Webhooks**.

Related concepts
About Webhooks in CSM
Webhooks Process
Configure One-Step Actions for Webhooks
Related tasks
Create a Webhook Endpoint

Create a Webhook Endpoint

Create a webhook endpoint that can receive data from an external tool using HTTP POST methods. Specify a One-Step Action that determines how the data is consumed by CSM. Each webhook can use basic authentication or no authentication.

Good to Know

- Webhooks require that One-Step Actions include Modifiers to map data in the third-party tool to CSM fields. For guidance on configuring One-Step Actions for webhooks, see Configure One-Step Actions for Webhooks. For Modifier examples, see Webhook Modifier Examples.

- The Base URL for the Cherwell REST API must be set before you can create a functional webhook. See Set the Base URL for the Cherwell REST API.

- To ensure that webhooks run for specific cultures, create a webhook endpoint for each culture. This is useful for using the same One-Step Action for several culture-specific webhooks.

- **Important:** If you are working with webhooks after a Protected mApp™ Solution has been applied to your system, note the following:

    ◦ If you create or open a Blueprint which has a Protected mApp Solution installed, protected webhooks have shield icons .

    ◦ If you select a content-protected webhook and right-click, you cannot delete the webhook.

    ◦ If you edit a content-protected webhook, you can change the Authentication Type, add your own username and password for authentication, change the Provider Type, and also change the Endpoint Extension. You cannot delete the associated One-Step Action, Name or Description.

    ◦ See Protected mApp Solutions.

To create a webhook endpoint:

1. Open the Webhooks Manager. See Open the Webhooks Manager.
2. Select a folder in the left pane, and then select **Create**.
3. Provide a name and description.
4. From the **Provider Type** drop-down list, select one of these options:
    ◦ **Amazon SNS**: Select this option to use the Amazon Simple Notification Services (SNS). If you select this option for the webhook and the received request is not from Amazon SNS, the request fails and an error message is added to the Cherwell REST API log. For guidance on using webhooks with Amazon SNS, see Using CSM Webhooks with Amazon Web Services (AWS).
    ◦ **Slack**: Select this option to use Slack. If you select this option for the webhook and the received request is not from Slack, the request fails and an error message is added to the Cherwell REST API log.
    ◦ **Other**: Select this option to use any third-party provider.

5. In the **Endpoint Extension** field, provide text that uniquely identifies the webhook. The extension you provide is combined with the Base URL for the Cherwell REST API to form the full endpoint provided to an external tool.

> **Note:** The endpoint extension cannot be empty or include special characters, including spaces.

6. Copy the Full Endpoint. You will need it to configure the event in an external tool.

7. Select the **Authentication** page, and then select one of these options from the **Authentication Type** drop-down list:
   - **None**
   - **Basic**: Select this option when basic authentication is sent in the header of the HTTP request. Provide a user name and password. The user name does not need to be a CSM account, but the password must comply with CSM password complexity settings. See Configure Cherwell Credential Settings (User/Customer Password Rules).
   - **Slack**: If you select this option, you must enter the Signing Secret that you copied from the Slack App. This is the key used to verify the authenticity of messages coming from Slack.

     This option is only available when the **Provider Type** is Slack.

8. Select the **Action** page, and from the **Run a One-Step** drop-down list, select the One-Step Action that is configured to run for the webhook. You can also select the **Ellipses** to open the **One-Step Manager**, and then select a One-Step Action or create a new one.

9. From the **Culture** drop-down list, select the culture to use when the webhook is run. You can also clear the selected culture.

10. Select the **Test One-Step** button to test data mapping between an external tool and Modifiers added to the selected One-Step Action. For testing instructions, see Test One-Step Actions Assigned to Webhook Endpoints.

11. Select **OK**.

Related concepts

About Webhooks in CSM

Configure One-Step Actions for Webhooks

Webhook Modifier Examples

Related tasks

Test One-Step Actions Assigned to Webhook Endpoints

Related information

JSON Modifiers

XML Modifiers

Configure One-Step Actions for Webhooks

Webhooks can be used with any One-Step Action that support Tokens.

For example, you can:

- Use a Create a New Business Object or Update a Business Object Action to add data from an external tool to CSM records.
- Use a Send an Email Action to send data from an external tool as contents of an email message.
- Use a Write to a File Action to add data from an external tool to a file.
- Use the Decide Between Multiple Cases Action to create an Incident in CSM from Slack.

One-Step Actions used by webhooks must include JSON or XML Modifiers on the webhook body token to parse data from an external tool to CSM records. You must identify the data type and the value to return. In some cases, you must also identify the element.

You can configure One-Step Actions from the One-Step Manager while you are:

- Configuring a webhook endpoint.
- Working in a Blueprint or mApp Solution.
- Working with One-Step Actions in the CSM Desktop Client.

Create a One-Step Action from a Webhook Endpoint

To configure a One-Step Action from a webhook endpoint:

1. Open the **Webhooks Manager**.
2. Create a new webhook endpoint or edit an existing webhook endpoint.
3. Select the ellipses next to the **Run a One-Step** drop-down list.
4. From the **One-Step Manager**, create or edit a One-Step Action.
5. Select the **Start Graphic**.
6. In the Step Details section, select the **Conditions** page.
7. From the **Show custom tokens** drop-down list, select **Webhook**.

Use a Variable to Parse Incoming Data

To ensure that all Actions in a One-Step Action have access to webhook modifiers through the token menu, add an Update Variables and Stored Values Action as the first Action.

To add an Update Variables and Stored Values Action:

1. On the **Designer Board**, add an **Update Variables or Stored Values Action** as the first Action.
2. Provide a name for the Action.
3. Select the **Variable** option, and then provide a name for the variable.

4. From the **Data Type** drop-down list, select one of these options: JSON, JSON Array, XML, or XML Collection.

5. Right-click in the **New Value** box, and then select **Webhook Content > Value**.

6. Double-click **Body**, and then add Modifiers as needed. For guidance on creating Modifiers, see Webhook Modifier Examples.

7. Save the Action.

As you configure other Actions in the One-Step Action, the variable will be available in the **Token** menu.

Use a Webhook Token to Parse Incoming Data

From a One-Step Action that supports tokens, right-click in the content area to open the **Token** menu, and then add the **Webhook Content > Value** token.

For example, to add a webhook token to Business Object Action:

1. Select the **Fields** page.

2. From the **Fields** list, select the Text Field that will store the data from the webhook.

3. From the **Value** options, select **Template**.

4. Right-click in the box, and select **Webhook Content > Body**.

5. Double-click the Body token.

6. Add Modifiers to parse the incoming data. For examples, see Webhook Modifier Examples.

Related concepts
Webhook Modifier Examples
Related tasks
Open the Webhooks Manager
Create a Webhook Endpoint
Related information
Create/Edit a One-Step Action
JSON Modifiers
XML Modifiers

Webhook Modifier Examples

Webhook Modifier examples vary from simple JSON and XML POST messages to complex examples using POST messages from Amazon Simple Notification Service (SNS) and Jira Software.

The examples are intended to provide guidance for using Modifiers to extract JSON or XML data into a format usable for CSM. For guidance on using Modifiers of different types, see JSON Modifiers and XML Modifiers.

Simple JSON POST Request

This example shows how to extract this JSON notes data to a Text Field in a Business Object record:

`"notes": "The customer would like to buy a Silver membership.",`

Post data:

```
{
    "id": "944ff7dfc501391af808764a02ab2fcd4c",
    "firstname": "Jason",
    "lastname": "Taylor Sr.",
    "email": "jason.taylor2@gmail.com",
    "siteid": 46,
    "notes": "The customer would like to buy a Silver membership.",
    "currentdatetime": "07-21-2019",
    "customertypeid": 142
}
```

Modifier sample:

This example requires two Modifiers: one to declare the data type as JSON and another to map the notes data to a Text Field in a Business Object.

Modifier Type	Value, Element, etc.	Notes
As JSON()	N/A	Declares the incoming data as JSON.
JSON Path (value)	notes	Maps the notes data to the selected Text Field.
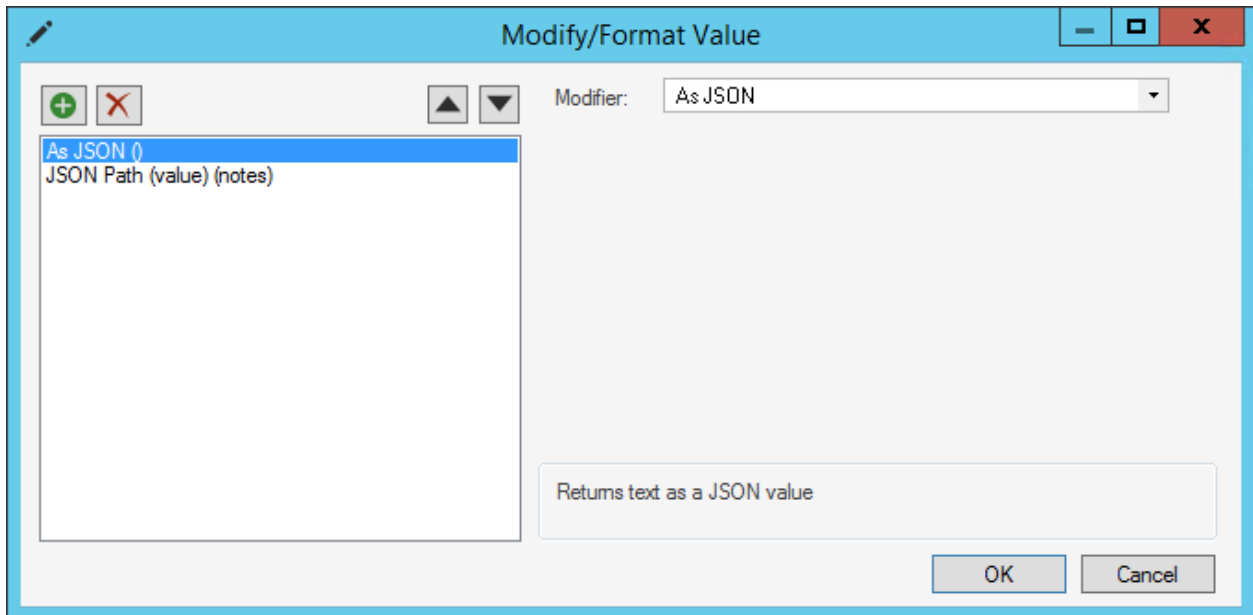
Simple XML POST Request

This example shows how to extract this XML notes data to a Text Field in a Business Object record.

```
<notes>The customer would like to buy a Silver membership.</notes>
```

Post data:

```
<List>
                <item>
                        <id>944ff7dfc501391af808764a02ab2fcd4cd</id>
                        <firstname>Jason</firstname>
                        <lastname>Taylor</lastname>
                        <email>jason.taylor2@gmail.com</email>
                        <siteid>46</siteid>
                        <notes>The customer would like to buy a Silver memb
ership.</notes>
                        <currentdatetime>07-21-2019</currentdatetime>
                        <customertypeid>142</customertypeid>
                </item>
        </List>
```

Modifier sample:

This example requires three Modifiers: one to declare the data type as XML, one to find the item element, and one to map the notes data to a Text Field in a Business Object.

Modifier Type	Value, Element, etc.	Notes
As XML()	N/A	Declares the incoming data as XML.
Find Element	item	Finds the item element in the POST data.
XPath (value) ()	notes	Maps the notes data to the selected Text Field
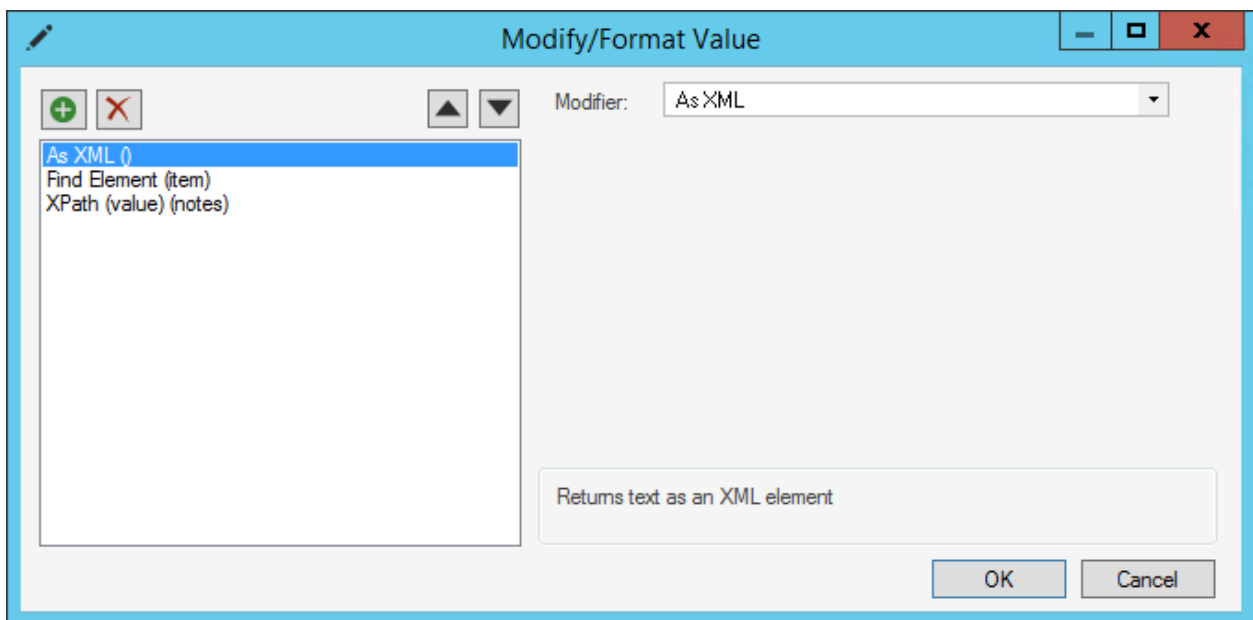
Complex JSON Post Request (Amazon)

This example shows how to extract this JSON notes data to a Text Field in a Business Object record: \"notes\": \"The customer would like to buy a Silver membership.

The sample data is from Amazon Simple Notification Service (SNS).

Post data:

```
{
  "Type" : "Notification",
  "MessageId" : "8db3250a-9ce2-588f-9746-70cde0de2aa0",
  "TopicArn" : "arn:aws:sns:us-west-2:000000000000:New_Customer_Object_AWS_
JSON",
  "Message" : "    {\n          \"id\": \"944ff7dfc501391af808764a02ab2fcd4c\
```

```
",\n       \"firstname\": \"Marie\",\n        \"lastname\": \"Smith\",\
n       \"email\": \"marie.smith@gmail.com\",\n       \"siteid\": 46,\
n       \"notes\": \"The customer would like to buy a Silver membership.\"
,\n       \"currentdatetime\": \"07-21-2019\",\n       \"customertypeid\"
: 142\n    }",
  "Timestamp" : "2019-08-09T13:49:48.167Z",
  "SignatureVersion" : "1",
  "Signature" : "RoPT3rzdzZFptij0j8HpR53dBjeABhAiJ/9+y6YNdsHBWJzFJY0djUQAUr
5zyCujh9qHXXWUgHR07KPhq2YrKoO35nPVoKgIyLzVfGiTacRHpMv9+irc7qBihn+c9eb4cJdsa
RoiS+wRZGdBqnN0w4QXWf/cOnwInIHpkhNpKz2i8xCUQT/yRzUaMRbgGT+wZrtHfhwwhuUEXvli
F+Mp78zxwBGYpNQxyblMneVskroYyaZhjBb6Sl7bOLlF9AvW5riasiUnGlsbxrf9lS7FDE074fR
61bKfNhR0lGYdl4/T0lYceJU+E6tWC5PKKuiqWyArnNaLdJM0tycM7fFSAw==",
  "SigningCertURL" : "https://sns.us-west-2.amazonaws.com/SimpleNotificatio
nService-6aad65c2f9911b05cd53efda11f913f9.pem",
  "UnsubscribeURL" : "https://sns.us-west-2.amazonaws.com/?Action=Unsubscri
be&SubscriptionArn=arn:aws:sns:us-west-2:330538622256:New_Customer_Object_A
WS_JSON:1a7a7e5e-2d54-4723-a9d7-3aec73648792"
}
```

Modifier sample:

This example requires three Modifiers: one to declare the data type as JSON, one to find message object, and one to map the notes data to a Text Field in a Business Object.

Modifier Type	Value, Element, etc.	Notes
As JSON()	N/A	Declares the incoming data as JSON.
Find Object (Message)	item	Finds the item element in the POST data.
JSON Path (value)(notes)	notes	Maps the notes data to the selected Text Field.
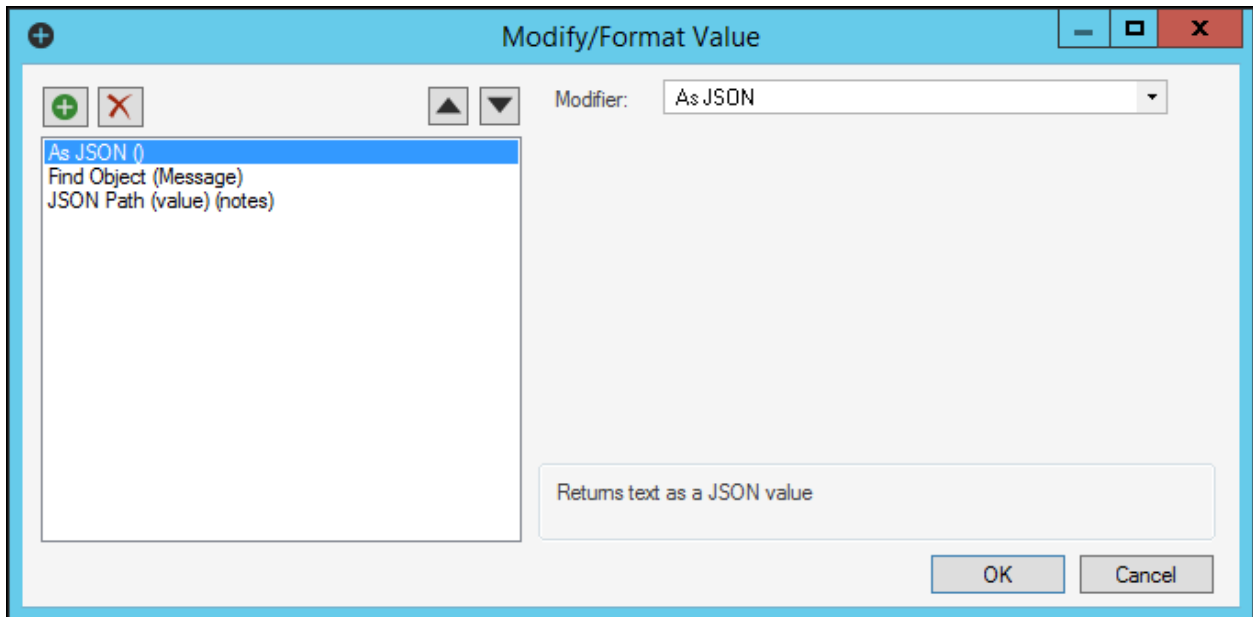
Complex XML POST Request (Amazon)

This example shows how to extract this XML notes data to a Text Field in a Business Object record.

```
<notes>The customer would like to buy a Gold membership.</notes>
```

The sample data is from Amazon Simple Notification Service (SNS).

Post data:

```
{
  "Type" : "Notification",
  "MessageId" : "1582a97c-dd2d-5fd5-abf5-fcbba01b3861",
  "TopicArn" : "arn:aws:sns:us-west-2:330538622256:New_Customer_Object_AWS_
XML",
  "Message" : "\t<List>\n\t\t<item>\n\t\t\t<id>944ff7dfc501391af808764a02ab
2fcd4cd</id>\n\t\t\t<firstname>Jason</firstname>\n\t\t\t<lastname>Taylor</l
astname>\n\t\t\t<email>jason.taylor2@gmail.com</email>\n\t\t\t<siteid>46</s
iteid>\n\t\t\t<notes>The customer would like to buy a Gold membership.</not
es>\n\t\t\t<currentdatetime>07-21-2019</currentdatetime>\n\t\t\t<customerty
peid>142</customertypeid>\n\t\t</item>\n\t</List>",
  "Timestamp" : "2019-08-09T13:53:58.341Z",
  "SignatureVersion" : "1",
  "Signature" : "aSOnIPCzJWj8uC4l5wBhDOoAwOCVEUuqnTIs2axWk0FDJhpLLJiVfnJ571
```

```
GhFQw7j5QQC9fxqyUNl+M8guBfaGv5WylfZqf3nAHYYFauSOoq9kkieVrezNjvtROJGZwkyHxNj
xw0/MPTTgz60IcBrJlwK2/jur5EcFuqvyeqdn6wUowe2u1Sbo+C5E6QORsY9T/2fqTMRtA02uUw
exaIBgBp/xVb+6yXT8AlvwptHoFjV0SCySL1H0SNANuzvFtBQ7r49XRhIjgGWD9B/9RIp8dr9GE
yXtTCe+saN6KLNIynnwb1VJGDt+eMRr3nalsWZ4huwOd7vBuamNotYIB6Wg==",
  "SigningCertURL" : "https://sns.us-west-2.amazonaws.com/SimpleNotificatio
nService-6aad65c2f9911b05cd53efda11f913f9.pem",
  "UnsubscribeURL" : "https://sns.us-west-2.amazonaws.com/?Action=Unsubscri
be&SubscriptionArn=arn:aws:sns:us-west-2:330538622256:New_Customer_Object_A
WS_XML:ebed2bfb-2ec4-4085-934e-c49fc71b79bc"
}
```

Modifier sample:

Because SNS encapsulates all data as JSON, this example requires five Modifiers: one to declare the data type as JSON, one to one to return a value based on the supplied JSON path, one to declare the data inside the JSON as XML, one to find the item element, and one to map the notes data to a Text Field in a Business Object.

Modifier Type	Value, Element, etc.	Notes
As JSON()	N/A	Declares the incoming data as JSON.
JSON Path (value)(message)	message	Returns a value based on the supplied JSON path.
As XML()	N/A	Declares the data inside the JSON as XML.
Find Element (item)	item	Finds the item element in the POST data.
XPath (value)(notes)	notes	Maps the notes data to the selected Text Field.
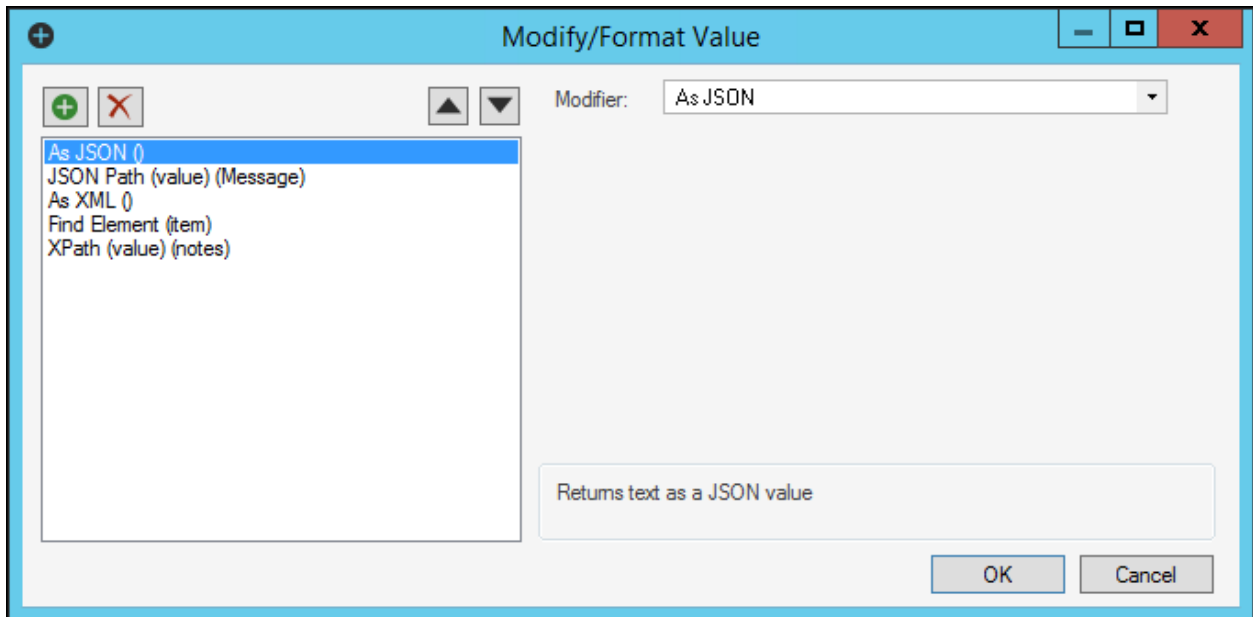
Complex JSON Post Request (Jira Software)

This example shows how to extract this JSON changelog data (shown in bold text below) to a Text Field in a Business Object record.

```
{ "field": "description", "fieldtype": "jira", "fieldId": "description",
"from": null, "fromString": null, "to": null, "toString": "This is the
description field for a new JIRA issue request." },
```

The sample data is from Jira Software.

Post data:

```
{
    "timestamp": 1564693604774,
    "webhookEvent": "jira:issue_created",
    "issue_event_type_name": "issue_created",
    "user": {
        "self": "https://webhookstest.atlassian.net/rest/api/2/user?account
Id=557058%3A57f5e298-87a6-4fc8-87d7-d7ab15be260e",
        "name": "Jill Hanson",
        "key": "jill.hanson",
        "accountId": "557058:57f5e298-87a6-4fc8-87d7-d7ab15be260e",
        "emailAddress": "jill.hanson@example company.com",
        "avatarUrls": {
```

```
            "48x48": "https://avatar-management--avatars.us-west-2.prod.pub
lic.atl-paas.net/557058:57f5e298-87a6-4fc8-87d7-d7ab15be260e/ccb36e82-479b-
4034-950e-6fce17dc2d89/128?size=48&s=48",
            "24x24": "https://avatar-management--avatars.us-west-2.prod.pub
lic.atl-paas.net/557058:57f5e298-87a6-4fc8-87d7-d7ab15be260e/ccb36e82-479b-
4034-950e-6fce17dc2d89/128?size=24&s=24",
            "16x16": "https://avatar-management--avatars.us-west-2.prod.pub
lic.atl-paas.net/557058:57f5e298-87a6-4fc8-87d7-d7ab15be260e/ccb36e82-479b-
4034-950e-6fce17dc2d89/128?size=16&s=16",
            "32x32": "https://avatar-management--avatars.us-west-2.prod.pub
lic.atl-paas.net/557058:57f5e298-87a6-4fc8-87d7-d7ab15be260e/ccb36e82-479b-
4034-950e-6fce17dc2d89/128?size=32&s=32"
        },
        "displayName": "Jill Hanson",
        "active": true,
        "timeZone": "America/Denver",
        "accountType": "atlassian"
    },
    "issue": {
        "id": "10006",
        "self": "https://webhookstest.atlassian.net/rest/api/2/issue/10006"
,
        "key": "TES-7",
        "fields": {
            "statuscategorychangedate": "2019-08-01T15:06:44.856-0600",
            "issuetype": {
                "self": "https://webhookstest.atlassian.net/rest/api/2/issu
etype/10001",
                "id": "10001",
                "description": "Stories track functionality or features exp
ressed as user goals.",
                "iconUrl": "https://webhookstest.atlassian.net/secure/viewa
vatar?size=medium&avatarId=10315&avatarType=issuetype",
                "name": "Story",
```

```
                "subtask": false,
                "avatarId": 10315
            },
            "timespent": null,
            "customfield_10030": null,
            "project": {
                "self": "https://webhookstest.atlassian.net/rest/api/2/proj
ect/10000",
                "id": "10000",
                "key": "TES",
                "name": "JIRA issue summary information",
                "projectTypeKey": "software",
                "simplified": false,
                "avatarUrls": {
                    "48x48": "https://webhookstest.atlassian.net/secure/pro
jectavatar?pid=10000&avatarId=10409",
                    "24x24": "https://webhookstest.atlassian.net/secure/pro
jectavatar?size=small&s=small&pid=10000&avatarId=10409",
                    "16x16": "https://webhookstest.atlassian.net/secure/pro
jectavatar?size=xsmall&s=xsmall&pid=10000&avatarId=10409",
                    "32x32": "https://webhookstest.atlassian.net/secure/pro
jectavatar?size=medium&s=medium&pid=10000&avatarId=10409"
                }
            },
            "fixVersions": "9.7.0",
            "aggregatetimespent": null,
            "resolution": null,
            "customfield_10027": null,
            "resolutiondate": null,
            "workratio": -1,
            "watches": {
                "self": "https://webhookstest.atlassian.net/rest/api/2/issu
e/TES-7/watchers",
                "watchCount": 0,
```

```
            "isWatching": true
        },
        "lastViewed": null,
        "created": "2019-08-01T15:06:44.730-0600",
        "customfield_10020": null,
        "customfield_10021": null,
        "customfield_10022": null,
        "customfield_10023": null,
        "priority": {
            "self": "https://webhookstest.atlassian.net/rest/api/2/prio
rity/3",
            "iconUrl": "https://webhookstest.atlassian.net/images/icons
/priorities/medium.svg",
            "name": "Medium",
            "id": "3"
        },
        "customfield_10024": null,
        "customfield_10025": [],
        "customfield_10026": null,
        "labels": [],
        "customfield_10016": null,
        "customfield_10017": null,
        "customfield_10018": {
            "hasEpicLinkFieldDependency": false,
            "showField": false,
            "nonEditableReason": {
                "reason": "PLUGIN_LICENSE_ERROR",
                "message": "Portfolio for Jira must be licensed for th
e Parent Link to be available."
            }
        },
        "customfield_10019": "0|i0001b:",
        "aggregatetimeoriginalestimate": null,
        "timeestimate": null,
```

```
            "versions": [],
            "issuelinks": [],
            "assignee": null,
            "updated": "2019-08-01T15:06:44.730-0600",
            "status": {
                "self": "https://webhookstest.atlassian.net/rest/api/2/stat
us/10000",
                "description": "",
                "iconUrl": "https://webhookstest.atlassian.net/",
                "name": "Backlog",
                "id": "10000",
                "statusCategory": {
                    "self": "https://webhookstest.atlassian.net/rest/api/2/
statuscategory/2",
                    "id": 2,
                    "key": "new",
                    "colorName": "blue-gray",
                    "name": "New"
                }
            },
            "components": [],
            "timeoriginalestimate": null,
            "description": "test new issue desc",
            "customfield_10010": null,
            "customfield_10014": null,
            "timetracking": {},
            "customfield_10015": null,
            "customfield_10005": null,
            "customfield_10006": null,
            "security": null,
            "customfield_10007": null,
            "customfield_10008": null,
            "attachment": [],
            "aggregatetimeestimate": null,
```

```
            "customfield_10009": null,
            "summary": "my new issue",
            "creator": {
                "self": "https://webhookstest.atlassian.net/rest/api/2/user
?accountId=557058%3A57f5e298-87a6-4fc8-87d7-d7ab15be260e",
                "name": "john.smith",
                "key": "john.smith",
                "accountId": "557058:57f5e298-87a6-4fc8-87d7-d7ab15be260e",
                "emailAddress": "john.smith@example company.com",
                "avatarUrls": {
                    "48x48": "https://avatar-management--avatars.us-west-2.
prod.public.atl-paas.net/557058:57f5e298-87a6-4fc8-87d7-d7ab15be260e/ccb36e
82-479b-4034-950e-6fce17dc2d89/128?size=48&s=48",
                    "24x24": "https://avatar-management--avatars.us-west-2.
prod.public.atl-paas.net/557058:57f5e298-87a6-4fc8-87d7-d7ab15be260e/ccb36e
82-479b-4034-950e-6fce17dc2d89/128?size=24&s=24",
                    "16x16": "https://avatar-management--avatars.us-west-2.
prod.public.atl-paas.net/557058:57f5e298-87a6-4fc8-87d7-d7ab15be260e/ccb36e
82-479b-4034-950e-6fce17dc2d89/128?size=16&s=16",
                    "32x32": "https://avatar-management--avatars.us-west-2.
prod.public.atl-paas.net/557058:57f5e298-87a6-4fc8-87d7-d7ab15be260e/ccb36e
82-479b-4034-950e-6fce17dc2d89/128?size=32&s=32"
                },
                "displayName": "John Smith",
                "active": true,
                "timeZone": "America/Denver",
                "accountType": "atlassian"
            },
            "subtasks": [],
            "reporter": {
                "self": "https://webhookstest.atlassian.net/rest/api/2/user
?accountId=557058%3A57f5e298-87a6-4fc8-87d7-d7ab15be260e",
                "name": "john.smith",
                "key": "john.smith",
```

```
            "accountId": "557058:57f5e298-87a6-4fc8-87d7-d7ab15be260e",
            "emailAddress": "john.smith@example company.com",
            "avatarUrls": {
                "48x48": "https://avatar-management--avatars.us-west-2.
prod.public.atl-paas.net/557058:57f5e298-87a6-4fc8-87d7-d7ab15be260e/ccb36e
82-479b-4034-950e-6fce17dc2d89/128?size=48&s=48",
                "24x24": "https://avatar-management--avatars.us-west-2.
prod.public.atl-paas.net/557058:57f5e298-87a6-4fc8-87d7-d7ab15be260e/ccb36e
82-479b-4034-950e-6fce17dc2d89/128?size=24&s=24",
                "16x16": "https://avatar-management--avatars.us-west-2.
prod.public.atl-paas.net/557058:57f5e298-87a6-4fc8-87d7-d7ab15be260e/ccb36e
82-479b-4034-950e-6fce17dc2d89/128?size=16&s=16",
                "32x32": "https://avatar-management--avatars.us-west-2.
prod.public.atl-paas.net/557058:57f5e298-87a6-4fc8-87d7-d7ab15be260e/ccb36e
82-479b-4034-950e-6fce17dc2d89/128?size=32&s=32"
            },
            "displayName": "John Smith",
            "active": true,
            "timeZone": "America/Denver",
            "accountType": "atlassian"
        },
        "customfield_10000": "{}",
        "aggregateprogress": {
            "progress": 0,
            "total": 0
        },
        "customfield_10001": null,
        "customfield_10002": null,
        "customfield_10003": null,
        "customfield_10004": null,
        "environment": null,
        "duedate": null,
        "progress": {
            "progress": 0,
```

```
            "total": 0
        },
        "votes": {
            "self": "https://webhookstest.atlassian.net/rest/api/2/issu
e/TES-7/votes",
            "votes": 0,
            "hasVoted": false
        }
    }
},
"changelog": {
    "id": "10011",
    "items": [
        {
            "field": "description",
            "fieldtype": "jira",
            "fieldId": "description",
            "from": null,
            "fromString": null,
            "to": null,
            "toString": "This is the description field for a new JIRA i
ssue request."
        },
        {
            "field": "priority",
            "fieldtype": "jira",
            "fieldId": "priority",
            "from": null,
            "fromString": null,
            "to": "3",
            "toString": "Medium"
        },
        {
            "field": "reporter",
```

```
                "fieldtype": "jira",
                "fieldId": "reporter",
                "from": null,
                "fromString": null,
                "to": "john.smith",
                "toString": "John Smith",
                "tmpFromAccountId": null,
                "tmpToAccountId": "557058:57f5e298-87a6-4fc8-87d7-d7ab15be2
60e"
            },
            {
                "field": "Status",
                "fieldtype": "jira",
                "fieldId": "status",
                "from": null,
                "fromString": null,
                "to": "10000",
                "toString": "Backlog"
            },
            {
                "field": "summary",
                "fieldtype": "jira",
                "fieldId": "summary",
                "from": null,
                "fromString": null,
                "to": null,
                "toString": "JIRA issue summary information"
            }
        ]
    }
}
```

Modifier sample:

This example requires five Modifiers: one to declare the data type as JSON, one to find the changelog object, one to find the internal array, one to find the array index, and one to map the toString data to the selected Text Field.

Modifier Type	Value, Element, etc.	Notes
As JSON()	N/A	Declares the incoming data as JSON.
Find Object (changelog)	changelog	Finds the changelog element in the POST data.
Find Array (items)	items	Finds and returns a JSON array for items.
Goto Array Index (0)	0	Returns a new JSON object of the indexed object in the arrary.
Find Object (toString)	toString	Maps the toString data to the selected Text Field.
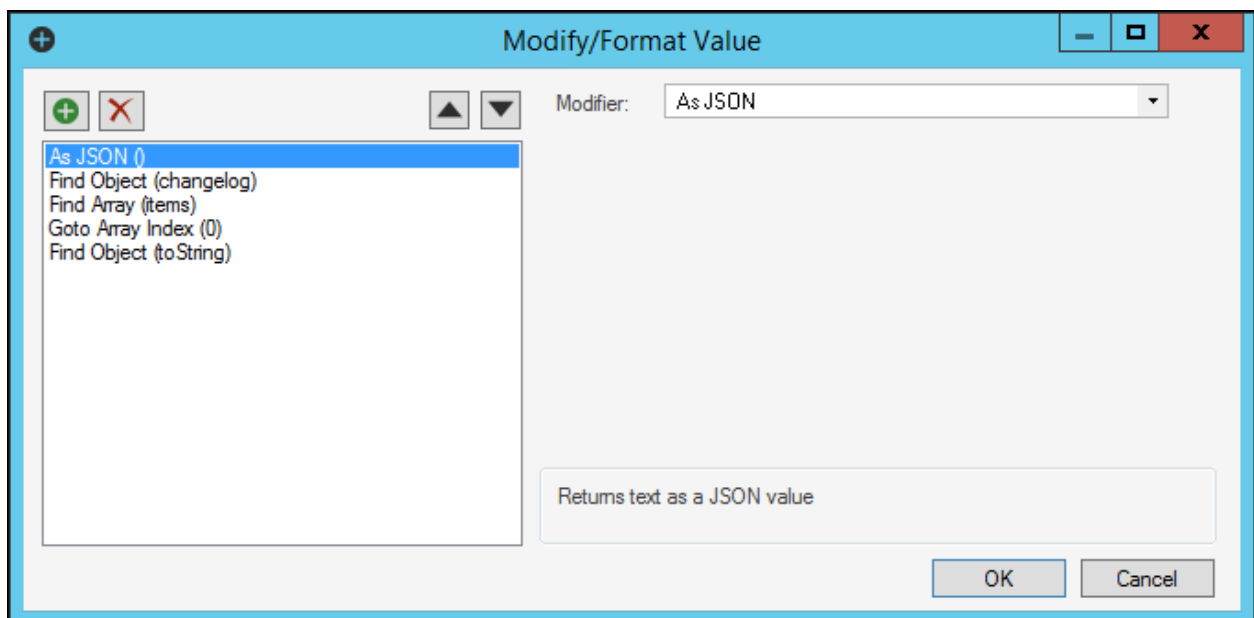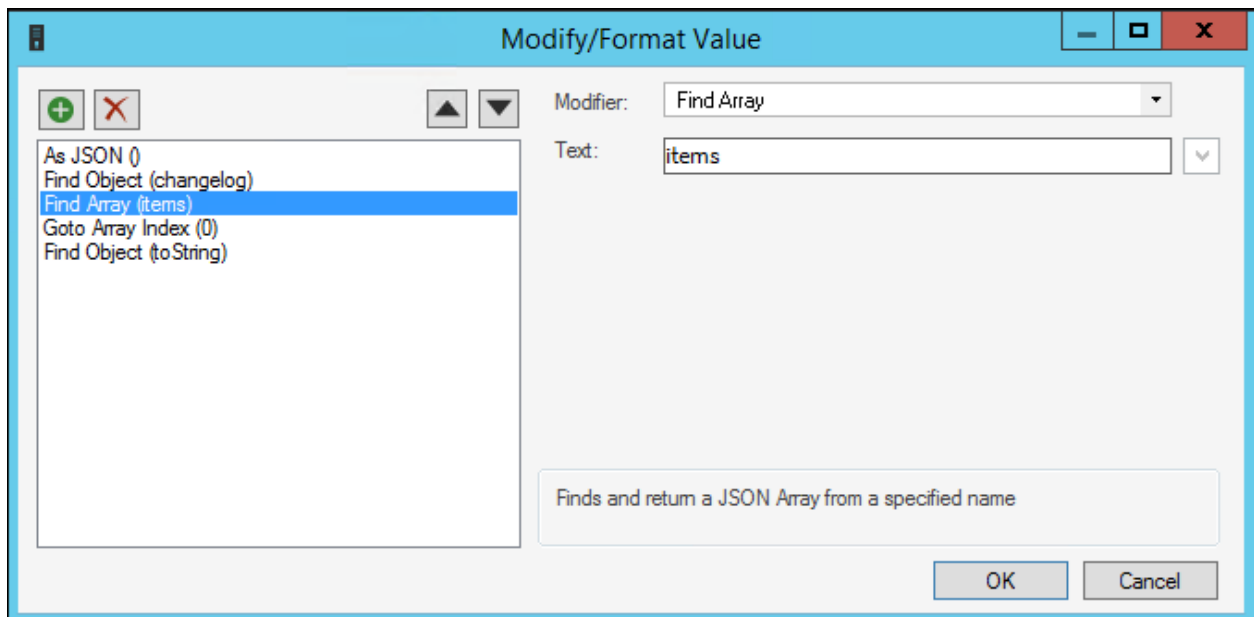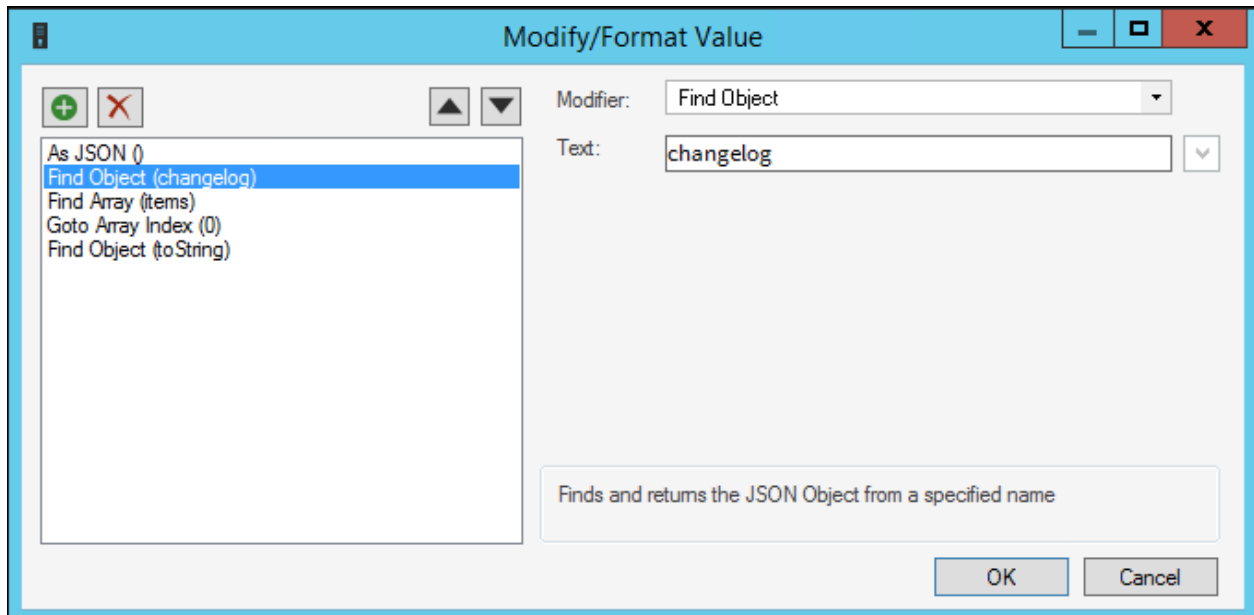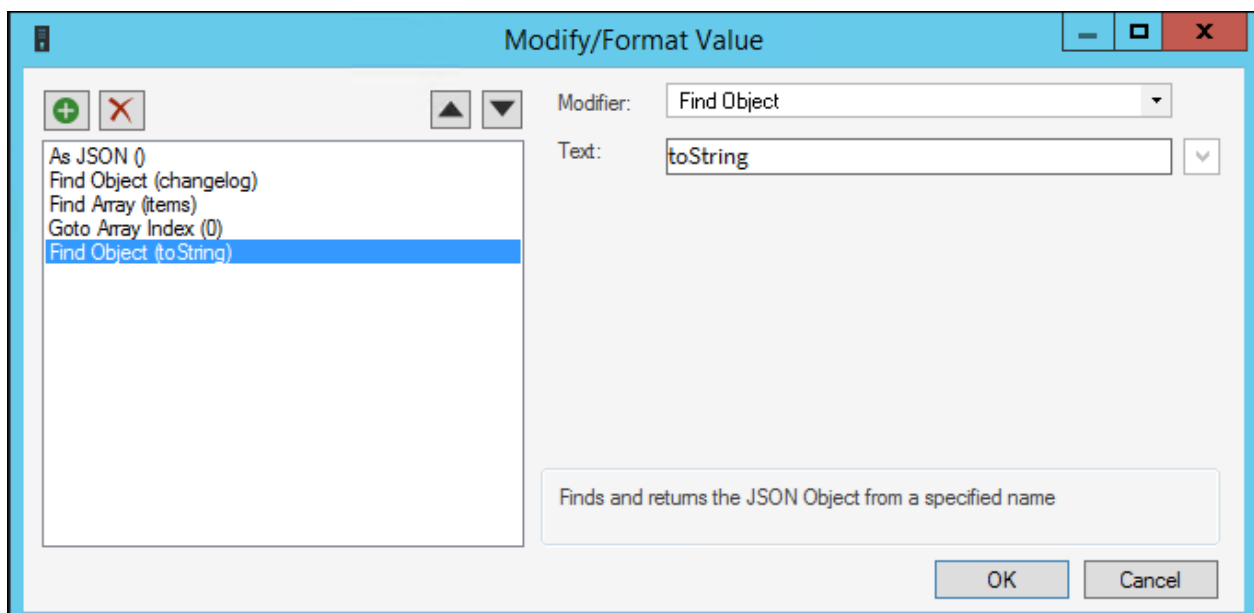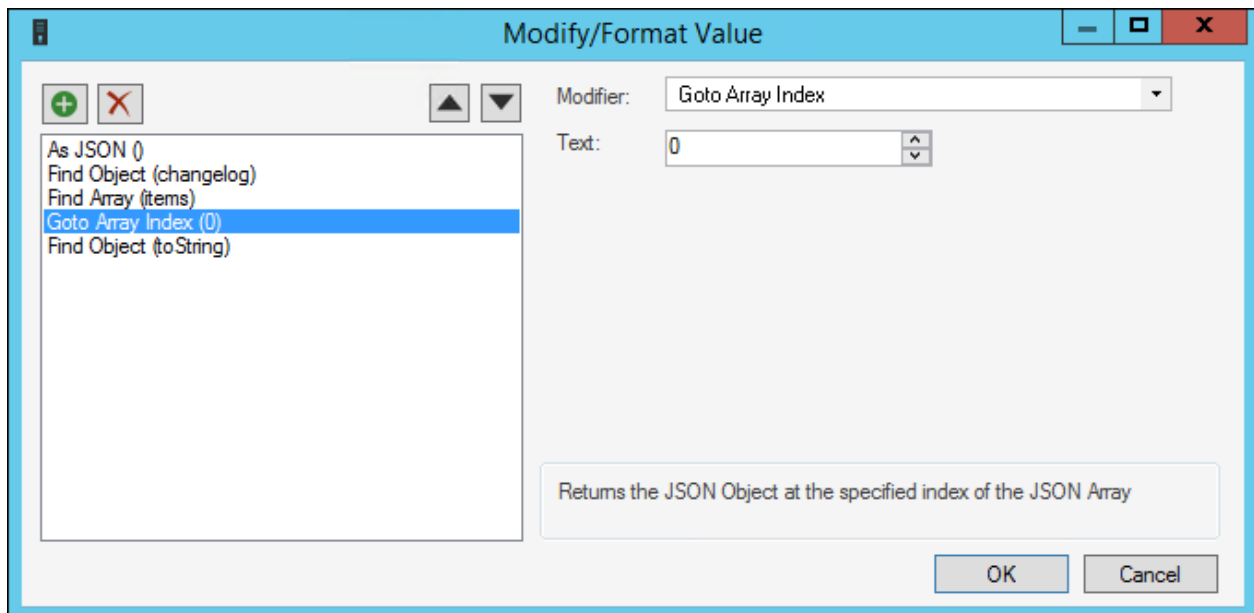
Simple JSON Post Request (Slack)

This example shows how to extract this JSON event and user data to a Text Field in a Business Object record:

```
"event": { "client_msg_id": "db93027c-b354-4bc4-b583-75caeafc5204", "type":
"app_mention", "text": "<@USY1K9YHH> create incident My printer doesn't work",
"user": "USDKMAUSV", "ts": "1580746614.000400", "team": "TSRMJ2UTZ", "blocks":
[ {
```

The sample data is from Slack.

Post data:

```
{
  "token": "6EK61SvTDR1tOLA1gBTm0wU1",
  "team_id": "TSRMJ2UTZ",
  "api_app_id": "AT91HES6Q",
  "event": {
    "client_msg_id": "db93027c-b354-4bc4-b583-75caeafc5204",
    "type": "app_mention",
    "text": "<@USY1K9YHH> create incident My printer doesn't work",
    "user": "USDKMAUSV",
    "ts": "1580746614.000400",
    "team": "TSRMJ2UTZ",
    "blocks": [
      {
        "type": "rich_text",
        "block_id": "SkD",
        "elements": [
          {
            "type": "rich_text_section",
            "elements": [
              {
                "type": "user",
                "user_id": "USY1K9YHH"
              },
              {
                "type": "text",
                "text": " create incident My printer doesn't work"
              }
            ]
```

Modifier sample:

This example requires three Modifiers: one to declare the data type as JSON, one to find the event object, and one to find the user object.

Modifier Type	Value, Element, etc.	Notes
As JSON()	N/A	Declares the incoming data as JSON.
Find Object (event)	item	Finds the item element in the POST data.
Find Object (user)	item	Finds the item element in the POST data.
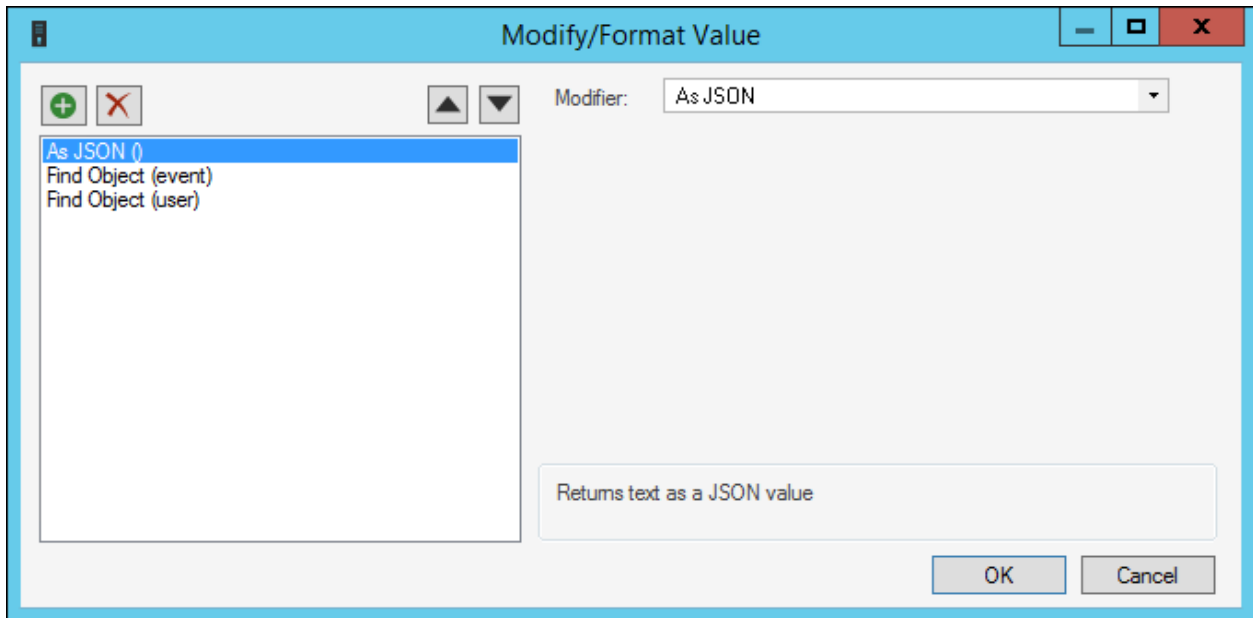
Related concepts

Configure One-Step Actions for Webhooks

About Webhooks in CSM

Related tasks

Test One-Step Actions Assigned to Webhook Endpoints

Related information

JSON Modifiers

XML Modifiers

Test One-Step Actions Assigned to Webhook Endpoints

You can pass JSON or XML sample data to test data mapping between an external tool and Modifiers added to a One-Step Action. This enables you to verify that the One-Step Action is valid before you send events from an external tool.

To test One-Step Actions assigned to webhook endpoints:

1. Open the Webhooks Manager, and then edit the webhook endpoint you want to test.
2. Select the **Run One-Step** button.
3. Paste valid JSON or XML that you expect to be sent from the external tool to the CSM webhook endpoint.
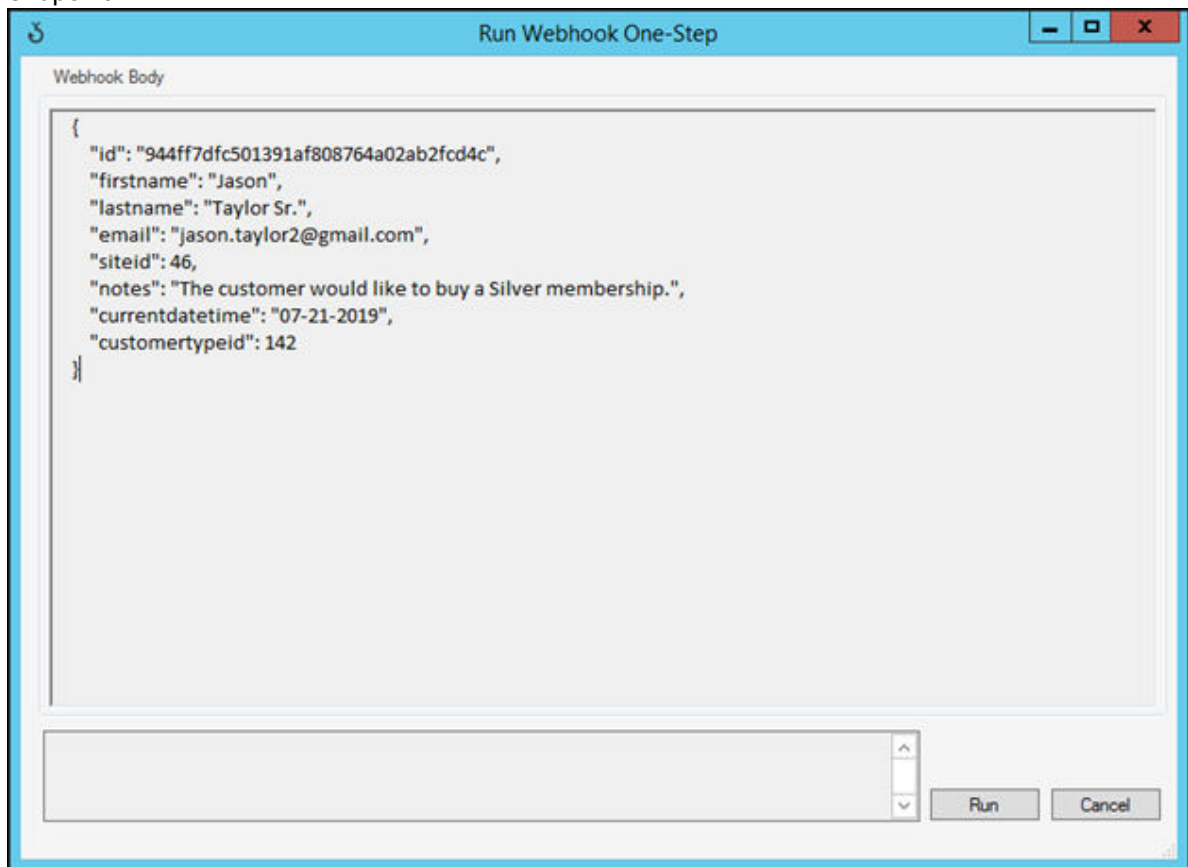
4. Select **Run**.
5. View the results in the bottom of the dialog. If the One-Step Action and Modifiers are not configured correctly, review the messages and adjust the Modifiers in your One-Step Action as needed.

Related concepts

Configure One-Step Actions for Webhooks

Webhook Modifier Examples
Related tasks
Open the Webhooks Manager
Create a Webhook Endpoint
Related information
Create/Edit a One-Step Action

Configure a Slack Workspace for Webhooks

Create and configure a Slack webhook and workspace to integrate CSM with Slack.

After configuring a Slack webhook and workspace, you can use the Slack integration to interact with CSM. Use a bot user token to perform a variety of functions in CSM. Some examples include:

- Create Incidents
- Check the status of Incidents
- Withdraw Incidents

For example, users can create an Incident from a request sent from the Slack workspace. CSM creates the Incident and replies to Slack via the REST API and posts the message with an Incident number. If the customer wants to know the status of an Incident, they can send the request from the Slack workspace. CSM replies to Slack via the REST API and posts the message with the status and priority of the Incident. If the customer no longer needs the Incident, the user can send the Slack request to withdraw the Incident.

Before configuring, you will need to:

1. Verify that you have administrative rights to the Slack workspace.
2. Create a Slack application.
   See https://api.slack.com/start/overview#auth.
3. Copy the Signing Secret. You will add this to CSM.

To configure CSM for the Slack webhooks integration:

1. Verify the Webhooks Security rights.
   ◦ From the **Group** drop-down list, select **Anonymous Browser** and then select the **View** check box.
2. Enable the System Event Processing Service.
3. Create a Slack webhook endpoint. This will include selecting the One-Step™ Action that is configured to run for the webhook.
4. Ensure you have completed all the steps for implementing webhooks. See Webhooks Process.

To configure Slack for the webhooks integration:

1. Add a bot user token.
   See https://api.slack.com/docs/token-types#bot.
2. Set up Event Subscriptions.
   See https://api.slack.com/bot-users#setup-events-api.

   This is where you will need the Full Endpoint URL from Creating a Webhook Endpoint in the section above. The endpoint needs to be publicly accessible.

3. Use the OAuth permission scope to subscribe to Bot Events.
   See https://api.slack.com/events-api#subscriptions.

When you add permissions or scopes, the app will need to be reinstalled to the workspace.

4. Grant the following permissions (scopes) to the bot user token:
   ◦ app_mentions:read
   ◦ chat:write
   ◦ users:read
   ◦ users:read:email

When you change the scopes, the app will need to be reinstalled to the workspace.

5. Copy the Bot User OAuth Access Token. You will add this to CSM.

In CSM Administrator, update the Bot User OAuth Access Token Stored Value with the value you just copied and then publish the Blueprint.

For protection reasons, we recommend storing the Bot User OAuth Access Token Stored Value in the Blueprint scope.

Related concepts
Enable the System Event Processing Service

Webhooks Security Rights
Related tasks
Create a Webhook Endpoint
Related information
Use Slack in the Related Items Pane
Assign a Value to a Stored Value

Webhook Logging

Webhooks log information is stored in different locations, depending on the information captured.

- **Cherwell REST API log**:

  Captures validation information from incoming requests. This includes authentication information, provider type, and Amazon Simple Notification Services (SNS) subscription confirmation.

  For example:
  - Incoming requests that exceed the 100,000 kb size limit are rejected and logged.
  - If an Amazon SNS signature is missing or invalid, requests are rejected and logged.
  - A warning is logged on initial requests from Amazon SNS because they are initially sent as unauthorized. The Cherwell REST API sends a 401 response and sets the header to basic authentication. Amazon then resends the message with authentication information.
  - If a webhook uses the provider type of Amazon SNS and the request is not of that type, the request is rejected and an error is logged.

- **System Event Processing Service log**:

  Captures processing information for requests after they are validated and sent to the queue.

  For example:
  - If the System Event Processing Service is paused, requests are not queued and a 503 error is logged.
  - If the System Event Processing Service is enabled but a webhook endpoint is disabled, requests are not queued and a 404 error is logged.
  - Once the System Event Processing Service is disabled, requests are queued and are processed when the service is enabled. No logging occurs in this case.

Related concepts
About Webhooks in CSM
Configure Logging for a CSM Service, Web Application, and Cherwell REST API
Related tasks
Configure Logging for the Cherwell REST API

Scheduler

The Scheduler is a tool that automatically runs defined actions (called Scheduled Items) on a scheduled basis (example: Back up the database every night at midnight).

Related concepts

Define General Properties for a Scheduled Item

Configure the Cherwell Service Host for a Local Scheduler

About the Scheduler

Schedule items to run on a recurring basis (daily, weekly, monthly, yearly) or one-time only.

The Scheduler operates within the timeframe of defined Business Hours and runs in coordination with the Scheduling Service, which is installed with the CSM Server Installer as a microservice of the Cherwell Service Host.

Access the following actions from the Scheduler:

- **Backup Database**: Exports a selected CSM database to a compressed Cherwell Archive Repository (.czar) file.
- **Database Maintenance**: Performs selected database maintenance operations (example: Rebuilding the full-text catalog, rebuilding indexes, and shrinking SQL logs on a scheduled basis).
- **Import External Data**: Imports data from external databases (example: Active Directory) into CSM.
- **Import from File**: Imports data from comma-separated value (.csv) files into CSM.
- **Import from LDAP**: Imports LDAP records (example: Customer lists) into CSM.
- **One-Step Action**: Runs a selected One-Step™ Action.
- **Portal Credentials**: Creates CSM Portal login credentials for customers.
- **Publish Blueprint**: Publishes Blueprints to your CSM system.
- **Report**: Runs a selected report.
- **Train machine learning**: Runs a configured query to pull data used to train a Machine Learning model.

Good to Know

- Use the **Scheduler** window in CSM Administrator (**Scheduling > Edit Schedule**) to use and manage Scheduled Items.
- Use the **Server Manager** to disable the Scheduling microservice.
- When you view the details of a scheduled item, its properties are read-only.
- To view all scheduled items for a particular day, use the calendar of Scheduled Items.

Backup Database Action:

- We recommend a nightly database backup for your CSM database.
- Schedule database backups for after business hours because backups can take significant time and system resources.
- If a directory does not exist, one will be created on the server where CSM Administrator runs.

Use the Scheduler

Use the Scheduler to schedule, run, and troubleshoot various jobs and actions.

Scheduled Items Window

To open the **Scheduled Items** window from the CSM Administrator main window, select the **Scheduling** category, and then select **Edit Schedule**.

Use the **Scheduled Items** window to:

- View a list of Scheduled Items, filtered by:
    - **Group**: View for a particular Scheduler.

    - **Action**: View by action type.

    - **Status**: View by completion status (Pending, Completed, Not Completed).

- Add, edit, delete, and copy Scheduled Items.

- Refresh Scheduled Items and their statuses. If items are running, use the **Refresh** button to watch the statuses change from Pending, to Running, to Complete.

- Select a Scheduled Item, and then select **Last Run** to see the last time a recurring item was run, its completion status, the duration of its last run, or any errors.

- View errors of a Scheduled Item that were not completed as expected.

- Select **Calendar** to see all the items scheduled for a particular day.

- Select **Test** to test a Scheduled Item to ensure all information is available for the item to run regularly.

Pause/Resume the Scheduling Service

Use the Pause/Resume Scheduler task to temporarily pause and resume the Scheduling Service.

Note: This process affects all enabled Scheduled Items.
Events are generated by the system, even when the Scheduling Service is paused. When the service is resumed, all Scheduled Items are processed.

To pause/resume the Scheduling Service:

1. In the CSM Administrator main window, select the **Scheduling** category, and then select the **Pause/Resume Scheduler** task.
   a. **Pause Scheduling Server**: Select this checkbox to pause the Scheduling Server processing. You must provide a reason for pausing the server to complete the process.
   b. **Resume Scheduling Server**: Select this checkbox to resume Scheduling Server processing.
2. Select **OK**.

View Scheduled Items

View Scheduled Items for details or errors.

You can view Scheduled Items in a few ways:

- View the details of a specific Scheduled Item.
- View a calendar to see all items scheduled for a specific day.
- View errors to see what has interrupted a Scheduled Item's run.

View a Scheduled Item

Use the **Scheduler** window to view the details of a Scheduled Item.

To view a Scheduled Item:

1. In the CSM Administrator main window, select the **Scheduling** category, and then select the **Edit Schedule** task.
2. Select a Scheduled Item, and then select the **View** button.
   You won't see the **View** button if the status is Pending.

View the Calendar of Scheduled Items

Use the Calendar of Scheduled Items to view all items scheduled for a specific day.

To view the Calendar of Scheduled Items:

1. In the CSM Administrator main window, select the **Scheduling** category, and then select the **Edit Schedule** task.
2. Select the **Calendar** button.
3. Select a date in the Calendar to view a list of the items scheduled for that day.
4. (Optional) Select the **Refresh** button to update the status of the Scheduled Items for that particular day.
   By default, the Calendar shows every single occurrence of a recurring item. To view only the next occurrence of a Scheduled Item, select the **Only show next occurrence of recurring items** checkbox.
5. Select **Close**.

View Errors for a Scheduled Item

You can view errors for a Scheduled Item to investigate the cause of the error.

When a Scheduled Item encounters an error, it won't be scheduled again because it's likely in a state where it can't run (example: Shortage of disk space, missing report).

To view the errors for a Scheduled Item:

1. In the CSM Administrator main window, select the **Scheduling** category, and then select the **Edit Schedule** task.
2. Select an item with an Error status, and then select **View Error**.
   The **Scheduled Item Error** window opens to provide details on the error(s) that occurred when the Scheduler attempted to run the Scheduled Item.

Select the **Reset to pending status so item will be scheduled again** checkbox to ensure the Scheduled Item runs after any errors have been resolved.

Configure the Scheduler

In CSM Administrator, configure Scheduler security rights to determine who can access Scheduler functionality.

Manage Scheduled Items

Use the **Scheduled Items Manager** to complete general operations for Scheduled Items.

Open the Scheduled Items Manager

Open the **Scheduled Items Manager** from the Blueprint or mApp Editor menu bar.

To open the Scheduled Items Manager:

- From the Blueprint Editor or mApp Editor menu bar in CSM Administrator, select **Managers > Scheduled Items**.

Create a Scheduled Item

Create a Scheduled Item from the **Scheduler** window or the **Scheduled Items Manager**.

When you create a Scheduled Item you define the following properties:

- **General:** Name and description.
- **Schedule:** Date and time the Scheduled item is scheduled to run.
- **Action:** Action the Scheduled Item runs (example: Backup Database).
- **Error Handling:** Options for handling errors that prevent a Scheduled Item from running.

Define General Properties for a Scheduled Item

Use the **General** page in the **Schedule Item** window to define general properties for a Scheduled Item.

General properties include:

- **Schedule Group:** For only one Schedule Group, leave **Default** selected. If you need multiple schedulers, select the **ellipsis** to create the different schedule groups.
- **Name:** Provide a name.
- **Description:** Provide a description.

Define Schedule Properties for a Scheduled Item

Use the **Schedule** page in the **Schedule Item** window to define the schedule for an item.

Schedule the date and time when an item should run, including:

- **One Time** or **Recurring:** Select the option for the Scheduled Item to run once or multiple times.
- **Scheduled time:** Choose a start date, time, and time zone .

  You can also select the **Scheduling Server Time Zone**.

- **Recurrence:** Choose how often you want the Scheduled Item to run (example: **Daily**, **Weekly**, **Monthly**, or **Every weekday**).
- **Range of recurrence:** Choose a **Start date** and when a recurrence ends for a Scheduled Item (example: **No end date**, **End after 10 occurrences**).

  If you choose **End by** and the item is scheduled to run on the end date, it runs for the last time on this date.

- **Maximum runtime:** Select the maximum number of minutes a Scheduled Item should run.

Define Action Properties for a Scheduled Item

Use the **Action** page in the **Schedule Items** window to define the Actions for the Scheduled Items.

Note: Each Action has its own unique properties. After you select an Action, the page displays the properties that need to be defined for the selected Action.

Define the properties for the selected Action:

- **Backup database:** Exports a selected CSM database to a compressed Cherwell Archive Repository (.czar) file.
- **Database maintenance:** Performs selected database maintenance operations (example: Rebuild the Full-Text catalog, Rebuild Indexes and shrink SQL logs on a scheduled basis).
- **Import external data:** Imports data from external databases (example: Active Directory) into CSM.
- **Import from file:** Imports data from comma separated value (.csv) files into CSM.
- **Import from LDAP:** Imports LDAP records (example: Customer lists) into CSM.
- **One-Step:** Runs a selected One-Step™ Action.
- **Portal Credentials:** Creates CSM Portal login credentials for customers.
- **Publish Blueprint:** Publishes Blueprints to your CSM system.
- **Purge System Table**: Purges email records and attachments from system tables.
- **Train machine learning:** Runs a configured query to pull data used to train a Machine Learning model.

Define Backup Database Action Options

Use the Scheduler's **Backup database** Action to export a selected CSM database to a compressed Cherwell Archive Repository (.czar) file on a scheduled basis.

Define the following settings as they apply, and then select **Save**.

Setting	Description	Notes
Directory	Provide the directory name or select **Browse** to select a directory where database backup files are stored.	The directory must be available on the machine where the Scheduler runs. We recommend a UNC name.
File Name	Provide a file name for the database backup.	
Rollover Files	Define the frequency of database backup files. • **Nightly:** Uses the same file every time the backup runs. • **Weekly:** Appends the day of the week to the backup files for a maximum of seven files. • **Monthly:** Appends the day of the month to the backup files for a maximum of 31 files. • **Yearly:** Appends the month and day to the backup files for a maximum of 365 files (366 for leap years).	If you don't roll over backup files, a new file is created for every database backup. The date is appended to the file name you entered (example: Cherwell20090305_093501.czar). For **Weekly** frequency, if you run a database backup every day of the week, there are seven files (one for each day of the week). If you run a backup every Monday, Wednesday and Friday, there are three files. The action uses these same files every week. For **Monthly** frequency, backup files are made for each day of the month. The action uses these same files every month. For **Yearly** frequency, backup files are made for each day of the year. The action uses these same files every year.
Export type	• **Export a single business object:** Exports a selected Business Object to the database backup file. • **Export entire system:** Exports the entire database to the backup file.	

Setting	Description	Notes
Content	**Export a Single Business Object:** • Select the Business Object from the drop-down list. • **Exclude encrypted fields and protected stored values:** Excludes encrypted fields and protected stored values from the export.	The options available in the **Content** section depend on the selected export type.

	Export entire system:
	
	• **Export all data:** Exports all SQL Server tables (example: Field names and sizes) and data.
	  ◦ **Exclude attachments:** Exports the Attachment table but not the attachment data within the table.
	  ◦ **Exclude automation data (events and scheduled actions, etc.):** Exports the Events and Scheduler tables, but not the data within the tables.
	  ◦ **Exclude emails:** Excludes emails from the export.
	• **Export table structure only:** Exports all SQL Server tables without any data.
	• **Export structure and lookup table data:** Exports SQL Server tables for all Major and Supporting Business Objects, as well as tables, and data for Lookup Objects (validation tables).
	• **Exclude encrypted fields and protected stored values:** Excludes encrypted fields and protected stored values from the export.
		Use **Exclude attachments** and **Exclude automation data** to create a .czar file to troubleshoot problems that are not related to Automation Processes or Scheduled Items.
		
		Use **Export table structure only** to create a .czar file that excludes your confidential company data.
		
		Use **Export structure and lookup table data** to create a .czar that excludes your confidential data but includes values from Lookup tables. Typically, Lookup tables don't contain confidential data, and you can use them to troubleshoot problems with validation and relationships.

Setting	Description	Notes
Logging	**Generate log file for this export (same location as export path):** Generates a log file for the export and uses the same file path as the export.	

Define Database Maintenance Action Options

Use the Scheduler's **Database maintenance** Action to perform selected database maintenance operations on a scheduled basis.

Note: Schedule database maintenance operations for after business hours because it can interrupt performance. For example, when you rebuild the SQL Server Full-Text catalog, it prevents users from doing full-text searches while the catalog is rebuilding.

Define the following settings as they apply, and then select **Save**.

Setting	Description	Notes
Full-text search	**Rebuild full-text search catalog:** Rebuilds the full-text search catalog.	CSM uses full-text search for quick search and knowledge search. If your index gets corrupted, rebuild the search catalog once a week or every night.
Manage indexes	**Rebuild Business Object indexes:** This option allows you to rebuild the indexes of the database tables that represent particular Business Objects. Select the **Select** button to select which Business Objects to reindex.	By default, all Business Objects are selected. Clear Business Objects to exclude them from reindexing. Select **Clear All** to clear all Business Objects. If you have a high volume of data, you may want to run this action monthly.
	Rebuild system table indexes: Rebuilds the indexes of the SQL Server tables associated with CSM system tables. These tables start with "Trebuchet" (the internal code name for the product).	If you have a high volume of data, you may want to run this action monthly.
	Shrink SQL event log: Shrinks the SQL Server event log file.	**Important:** Consult your administrator before you schedule this option. If in doubt, do not use this feature unless you run into problems.
	Pull up SaaS indexes: Pulls up the SaaS indexes.	

Setting	Description	Notes
Data	**Refresh queue status:** Refreshes queue status.	Queue status can unsync if Business Objects that were on queues are deleted. This option ensures that each queue syncs. We recommend you run this action weekly.
	Remove unused user accounts: Remove data associated with deleted user accounts.	When user accounts are deleted from the system, their authorization information may not be removed. This option ensures that the authorization information is in sync with the user list by removing the unused information. We recommend you run this action weekly.
	Synchronize Team Info with team list: Synchronizes the Team Info Lookup table with CSM user and customer team lists.	
	Delete Temporary Data: Deletes temporary data.	
	Remove orphaned attachments: Removes any orphaned attachments.	
	Fix mismatched definition IDs: Fixes any mismatched Def IDs.	

Define Import External Data Action Options

Use the Scheduler's **Import external data** Action to import data from external databases (example: Active Directory) into CSM on a scheduled basis.

When you define an **Import external data** Action, CSM launches the **External Data Import Wizard** to help you setup the import.

> **Note:** You must have a mapped CSM Business Object or an External Business Object to hold the external data that you import.

- Select **Setup** to open the **External Data Import Wizard**, follow the prompts, and then select **Save**.

Define Import from File Action Options

Use the Scheduler's **Import from file** Action to import data from comma separated value (.csv) files into CSM on a scheduled basis.

When you define an **Import from File** Action, CSM launches the **Stored Import Definition Manager** to help you set up the import.

1. Select **Setup** to open the **Stored Import Definition Manager**, and then select an existing CSV Stored Import or create a new one to run.
2. Select **Save**.

Define Import from LDAP Action Options

Use the Scheduler's **Import from LDAP** Action to import LDAP records (example: Customer lists) into CSM on a scheduled basis.

When you define an **Import from LDAP** Action, CSM launches the **Active Directory Import Wizard** to help you set up the import. If you schedule CSM Portal credential updates through the Scheduler, LDAP data must be imported first.

Note: We recommend biweekly LDAP imports.

Select **Setup** to open the **Active Directory Import Wizard**, follow the prompts, then select **Save**.

Define One-Step Action Options

Use the Scheduler's **One-Step** Action to run a One-Step™ Action on a scheduled basis.

For example, run a One-Step Action to send an email indicating that another Scheduled Item is complete (A database backup was successfully completed).

- Select a One-Step Action from the drop-down list or select the **ellipsis** to open the **One-Step Action Manager**.
  - Select an existing One-Step Action or create a new one, and then select **Save**.

Define Portal Credentials Action Options

Use the Scheduler's **Portal Credentials** Action to create CSM Portal login credentials for customers on a scheduled basis.

> **Note:** To import users from LDAP and then create CSM Portal credentials, schedule an **Import from LDAP** Action followed by a **Portal Credentials** Action that executes a few minutes later, ensuring the order of the steps.

Define the following settings as they apply, and then select **Save**.

Setting	Description	Notes
Search group	Select the **ellipsis** to open the **Search Manager**, and then select an existing saved search or create a new one that contains the customers who need CSM Portal credentials (example: Internal Customers).	
Field with Login ID	Select the field from the Customer Business Object that contains the Customers' login IDs.	
Customer group	Select the security group the customers belong to.	This defines the security rights for the Portal Credentials Action. When you select the Portal Workgroup Manager group, it offers greater control than if you select the Portal Customer group.

Setting	Description	Notes
Password	**Randomly generate a password for each customer:** Assigns and emails a random password to each customer.	If a customer doesn't have an email address, they won't get a notification.
	Set password the same for all: Assigns the same password to all customers, and then provides the password to use.	
	Password is value from field: Select a field from the drop-down list. Uses the value from the field as the password.	
	Set Login ID field as Windows/LDAP login: Uses Windows/LDAP login credentials, and then selects an option for determining a domain if the login ID does not include one: • **Attempt to determine domain from LDAP distinguished name:** Finds the customer domain using the stored distinguished name and parsing out the Domain Component (DC). • **Attempt to use domain associated with LDAP customer mapping:** Uses the domain stored in the customer record-mapped LDAP definition. • **Use this domain:** Enter a default domain for the login ID.	You must configure LDAP credentials to use this option.

Setting	Description	Notes
Account details	**Account locked:** Locks the customer's account preventing them from logging in to the CSM Portal.	A customer can also be automatically locked out of the system if there are too many failed login attempts (depending on system settings).
	Password never expires: No password expiration. This overrides any system setting to reset the password.	If you select this option, the **User must reset password at next login** and **Password reset date** options are hidden.
	User cannot change password: Restricts a customer from changing their password.	If a password reset is required by the system, the system administrator must reset it.
	User must reset password at next login attempt: Prompts a customer to change their password the next time they log in.	If a password reset is required by the system, the system administrator must reset it. This restarts any system administrator-scheduled password reset. This is an immediate reset. Use this setting if the customer forgot their password.
	Password reset date: Prompts a customer to change their password on a specific date. Select the **Date Selector** to choose a date.	
	Allow diagnostics: Allows a customer to run the Network Health Check test.	Run the Health Check Tool to get Network Health Check results. See Network Health Check Results.
E-mail	**E-mail customer new credential information:** Emails new credential information to customers. Select **Edit e-mail** to edit the Customer Credentials Email message.	To make this the default email message that is used for all customer emails, select **Make Default**.
	Skip customers with no e-mail address: Skips customers with no email address.	Leave this checkbox cleared if you want an error flagged when a customer doesn't have an email address.
Skip customers who already have login IDs assigned	Includes only new customers.	Leave this checkbox cleared to include all customers. We recommend you select this checkbox so IDs are not reassigned for existing users.

Define Publish Blueprint Action Options

Use the Scheduler's **Publish Blueprint** Action to publish Blueprints to your CSM system on a scheduled basis.

Define the following settings as they apply, and then select **Save**.

Setting	Description
Publish Blueprint	Publishes the Blueprint. Select **Browse** to select the Blueprint file to publish. This directory must be available on the machine where the Scheduler runs. We recommend a UNC name.
Backup Database	Backs up the database before the Blueprint publish. • **Directory:** Provide the directory name, or select **Browse** to select a directory where the database backup file will be stored. • **File name:** Provide the file name to use for the database backup file.
Append date/ time to file name	Appends the current date and time to the file name. This ensures that you don't overwrite previous backups with the same name by adding the most current date/time stamp to the backup file name.

Define Purge System Table Action Options

Use the Scheduler's Purge System Table Action to purge CSM system table email records and attachments on a scheduled basis.

Good to know:

- This Action physically deletes the selected items from the database. Prior to scheduling this Action you should backup any items that you need to retain for future use.
- It is recommended that you schedule this Action to run out of normal business hours as it may take some time to complete, especially for larger purges.
- For on-premise customers that want to reclaim disk space after purging, a DBA will need to run SQL Server's DB shrink command.

To define a Purge System Table Action:

1. In the CSM Administrator main window, select the **Scheduling** category, and then select the **Edit Schedule** task.
2. Add or edit a Scheduled Item that uses a Purge System Table Action, and then select the **Action** page.
3. Provide the following settings as they apply:

Option	Description
Table	**Email:** Select this option to purge email records. Journal - Mail History records recording details about the email will remain, but trying to drill into the actual linked email will result in a "not found" message. **Attachments:** Select this option to purge attachments from the Trebuchet attachment table. ◦ Attachments and their links to the Business Object are removed. ◦ Purging will honor the attachment audit settings for any Business Object; a journal entry will indicate the attachment was removed.
Business Object Selection (attachments only)	Select the Business Objects from which file attachments (and links) will be removed.

Option	Description
Date Filter	**Older Than:** Select this option to purge email or attachments older than the number of Years, Months or Days you specify. **Time Range:** Select this option to purge email or attachments for a date range you specify. Select the calendar buttons to specify the dates.
Estimate	Select to display an estimate of the number of emails or attachments that will be purged.

Define Report Action Options

Use the Scheduler's **Report** Action to run a selected report on a scheduled basis.

When you schedule a Report Action, you select the report to run and define any parameters (example: Date range or priorities). If you create one report with different parameters, you can reuse the report with different values. For example, run a Date Range report at the end of every month, end of every quarter, and end of every year; or, run an Incident report with different priorities or different categories. If a report has parameters, CSM prompts you to set the values that the Scheduler passes to the report when you schedule the report.

To automatically print a report, create a One-Step™ Action that prints the report. Then, use the Scheduler to run the One-Step Action.

Define the following settings as they apply, and then select **Save**.

Setting	Description

Run Report	• **Report:**
	  1. Select a recently used report from the drop-down list or select the **ellipsis** to open the **Report Manager**.
	  2. Select an existing report or create a new one.
	• **Format:** Select a preferred format for the report. Available formats include: .pdf, .bmp, .csv, .emf, .xls, .html, .jpeg, .txt, .png, .rtf, and .tiff.
	• **Output file:** Select **Browse** to choose the location of the output file for the report.
	
	  Note: This file must be creatable on the machine where the Scheduler runs. We recommend you use a UNC name.

Define Train Machine Learning Action Options

Use the Scheduler's **Train machine learning** Action to run a query that pulls verified data to train a Machine Learning model on a scheduled basis.

Define the following settings as they apply, and then select **Save**.

Setting	Description
Machine Learning Training Configuration	1. Select a model from the drop-down list or select the **ellipsis** to open the **Machine Learning Manager**. 2. Select an existing model, or configure a Blueprint to create a new model.
Training Query	Select the **ellipsis** to choose the query that is configured to return verified, accurate training examples. **Note:** A Machine Learning model is only as good as the information used to train it. The sample data returned by this query must provide accurate examples of content that will appear in the field that the model will analyze and the field that the model will predict.
Configuration Details	Displays the fields configured in the Machine Learning Manager and the date and duration of the last time the model was trained.

Define Error Handling Properties for a Scheduled Item

Use the **Error Handling** page in the **Scheduled Item Properties** window to define what to do if a Scheduled Item encounters an error during its scheduled run.

Note: When a Scheduled Item has an error, it's not scheduled again because it's most likely in a state where it can't run (disk space or missing report).

To define error handling properties for a Scheduled Item:

1. Create a Scheduled Item.
2. Select the **Error Handling** page.
3. Define the error handling operations:
   a. **If scheduled item fails run One-Step:** Select this checkbox to run a One-Step™ Action in the event of a Scheduled Item error.
      i. Select a One-Step Action in the drop-down list, or select the **ellipsis** to open the **One-Step Action Manager**.
      ii. Select an existing One-Step Action or create a new one.
   b. **If scheduled item fails, still schedule next run (if recurring):** Select this checkbox to continue a Scheduled Item's original schedule, ensuring that the next run occurs.
4. Select **Save**.

Troubleshoot Scheduled Items

If a Scheduled Item doesn't run as expected, try these troubleshooting procedures.

Check the Scheduled Items Window

1. In CSM Administrator, select the **Scheduling** category, and then select the **Edit Schedule** task.
2. Select the **Calendar** button.
3. The **Calendar Of Scheduled Items** window opens.
4. Select the day that the item should have run.
5. Look to see if the Scheduled Item is listed:
   - If it's listed, check the status. If the status has an error, select the row. The error message displays at the top of the screen. Only the first 250 characters of an error message are stored. If the message is longer than 250 characters, go to the Windows Event Viewer (**Windows™ Start menu > Adminstrative Tools > Event Viewer**) to see the complete error message.
   - If the Scheduled Item isn't listed and the item is recurring, select the date that the item should have run last. Verify that the status on that day was complete and the Scheduled Item didn't have an error.

Verify the Scheduling Service is not Paused

1. In CSM Administrator, select the **Scheduling** category, and then select the **Pause/Resume Scheduler** task.
2. Verify that there's not a pause.
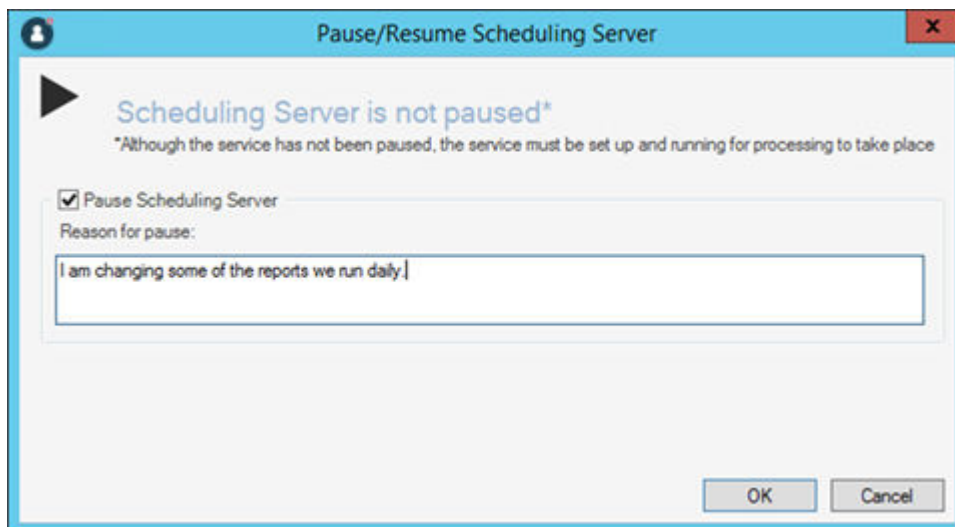
Verify the Cherwell Service Host and Cherwell Message Queue Service Are Running

1. Log in to the machine where the Scheduling Service is installed.

2. Verify Cherwell Service Host configuration.
   ◦ From the Cherwell Server Manager, select **Cherwell Service Host > Configure**. Ensure that the **Connection** value is set as expected.

   ◦ Validate that the Cherwell user ID and password are correct and that the test connection completes successfully.

   ◦ Under **Advanced Settings**, ensure that the **Cherwell Service Host** processes show the **Scheduling Service** is selected and that the **Scheduling Group** is set to the expected value as defined by the Scheduled Item (Normally, this is **(Default)** unless otherwise specified in the Scheduled Item).

3. Verify the Message Queue configuration.
   ◦ From the Cherwell Server Manager, select **Message Queue > Configure**. Ensure that the **Queue Connection** settings are configured correctly per your installation.

4. In the Windows™ Start menu, go to **Control Panel > Administrative Tools > Services**.

5. Locate the Cherwell Service Host and CherwellMQS, and then verify that the **Status** column shows Started.
   ◦ Restart the services if they are stopped.

   ◦ Check the Windows Event Viewer for logging information.
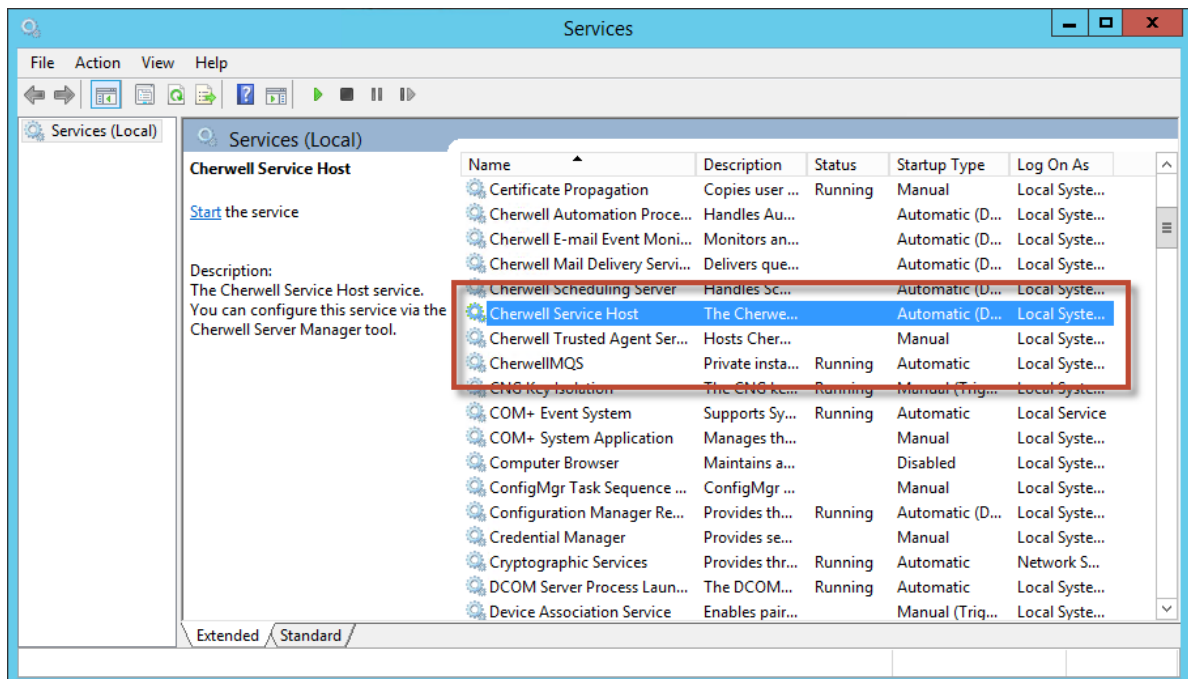
Verify SQL Server Database (Advanced Users Only)

Advanced users that are comfortable executing SQL queries can run queries to see the items that are scheduled and their statuses.

One Time Scheduled Items Status

For items that execute one time, use this query and replace [My Scheduled Item] with the name of the Scheduled Item you're looking for:

select DefName**,** ExecutionType**,** NextDT**,** Status**,** ErrorMsg **from** TrebuchetScheduler **where** DefName **= 'My Scheduled Item'**

and ExecutionType **= 'OneTime' order by** NextDT

Recurring Scheduled Items Status

For items that are recurring use this query and replace [My Scheduled Item] with the name of the Scheduled Item you're looking for:

select DefName**,** ExecutionType**,** NextDT**,** Status**,** ErrorMsg **from** TrebuchetScheduler **where** DefName **= 'My Scheduled Item'**

and (ExecutionType **= 'Recurring') and (**Instance **>** 0**) order by** NextDT

Data and Database Tools

A variety of tools are provided to help you configure and manage your CSM database. Tools for importing data into CSM are also provided.

About CSM Data and Databases

CSM ships with preconfigured starter databases. One includes a blank framework of Business Objects, grids, forms, and other CSM items. A second starter database can also be installed that provides sample data to populate the framework of CSM items with.

Data and Database Overview

CSM works with several different types of databases such as:

- **CSM Database:** This is a database that stores data and all of the CSM definition-based objects, such as Business Objects and expressions. The CSM database can connect to external databases, mail servers, and integrations to third-party databases such as Active Directory. A CSM database can have multiple connections, and you can create several databases within their CSM instance.

- **Exchange Mail Server:** CSM uses POP, IMAP, or Exchange for email and event monitoring.

- **External Database:** An external database is a third-party database that integrates with CSM by importing or linking data. CSM can connect to SQL Server and Object Linking and Embedding (OLE) Databases. You can create multiple connections to external databases as well as assign a Scheduler to the data imports.

- **Integrations:** CSM can connect with third-party Integrations such as Cherwell Asset Management and Active Directory.

🖉 **Note:** Multiple file groups in databases are not supported in CSM. CSM only uses the primary file group for backing up and restoring the database.

External Data and Database Overview

CSM can connect to an external database so that data can be imported or linked with CSM or viewed/updated in the external database. The integration between CSM and the external system is done at the database level. To qualify for integration, the database must be a SQL Server or have an OLE DB driver. Most of the major databases (Oracle, DB2, Access, etc.) have OLE DB drivers. However, consult database vendors to acquire an OLE DB driver or to determine if the server is 32-bit or 64-bit because different drivers are required. CSM can also import existing Comma Separated Values (csv) data.

Imported and linked data are both accessed by a created external connection:

- External data is initially imported into the CSM database. Automatic re-imports can be scheduled to automatically update and overwrite outdated data. From that point forward, the records can diverge, although data can be re-imported (entirely replacing existing data or appending/updating changed data) if desired. Re-imports can be run manually or they can be regularly scheduled using the Scheduler. A Last Modified Time/Date field in a Business Object assists in tracking the most recently imported external data. Additionally, it facilitates viewing or updating that data in CSM.

- When linking to external data, the external data is viewed and updated in CSM, but it continues to reside in the external database. A special External Business Object monitors the external data and facilitates viewing/updating that data in CSM.
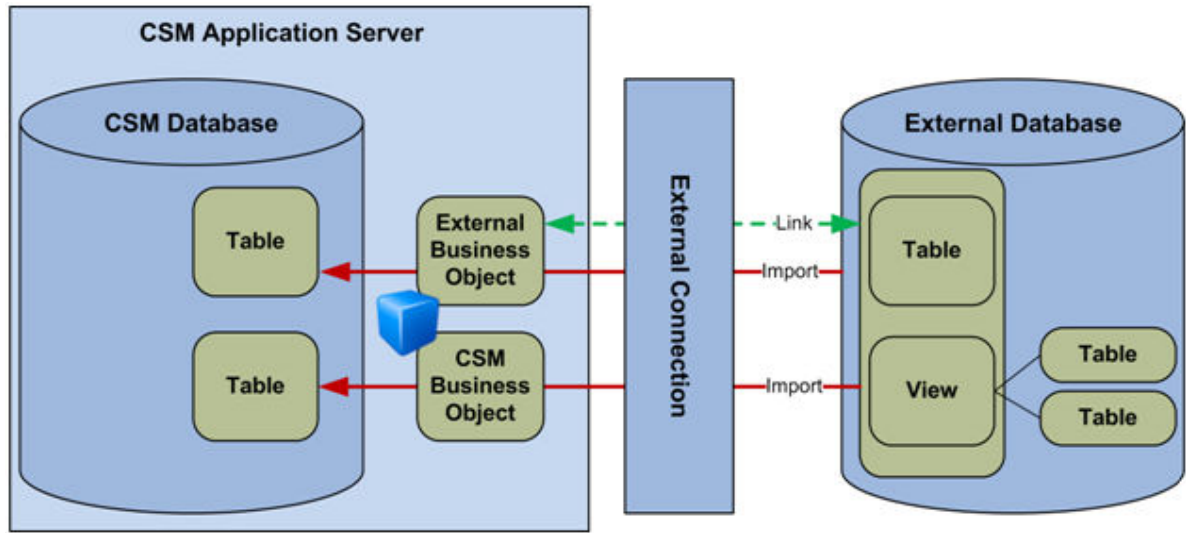
Database Server Objects Overview

Database Server Objects allow you to connect stored procedures, triggers, user functions, and replication scripts objects to CSM so that they can be dropped and recreated as necessary when CSM Blueprints are published to the database. Database Server Objects are important because Business Object tables cannot be dropped when there is a Database Server Object referencing the table. After CSM is connected to a Database Server Object, it can manage drops/recreates as needed during publishing operations. If the native system is exported to a .czar file, when the .czar file is re-imported, then the Database Server Objects are automatically created in the new database.

To import Database Server Objects:

- Use the Database Server Objects Import option if the CSM database already contains stored procedures, SQL Server connections, or triggers.
- Add objects through a preferred SQL tool and then import the objects into CSM.

Table Views Overview

Many external databases are normalized, meaning their data is spread across many tables. Before CSM can share data in a normalized external database, create one or more database views to collect, combine, and filter the information that is shared (importing/linking). To make mapping fields easier, first compare the fields in the external database view with the fields in the CSM Business Objects, then set the fields in the view to match the names. For more information, see Create CSM Database Views.

Database Tools

CSM provides tools and wizards to help manage data and databases. Tools are accessed in several ways: launched automatically when performing a task, accessed from within CSM Administrator, and accessed as stand-alone tools from the CSM Tools folder.

Database Tools and Wizards in CSM Administrator

- **Connection Wizard:** Provides the steps to configure the connections between the CSM applications and the CSM Database. The steps vary depending on the type of connection, either direct-to-database (2-tier) or Application Server (3-tier).

- **External Connection Wizard:** Walks through the steps to create a saved connection to an External Database (called an External Connection). CSM also provides the External Connection Manager to help manage (create, edit, and delete) the External Connections. In the CSM Administrator main window, create a New Blueprint. From the Menu bar, click **Managers>External Connections**.

- **External Data Wizard:** Provides the steps to either map an existing CSM Business Object to an External Database, or create an External Business Object to link/import external data.

- **External Data Import Wizard:** Provides the steps to import external data from an External Database into a mapped CSM Business Object or an External Business Object. In the CSM Administrator main window, click the **Database** category, and then the **Import external data** task.

- **Import Data Wizard:** Provides the steps to run a one-time import of .csv data into a CSM Business Object. In CSM Administrator, click the **Database** category, and then either Run a one-off data import (.csv files) or Stored Import Definition Manager (.csv files).

- **Stored Import Definition Manager:** Helps manage (create, edit, and delete) stored .csv imports.

- **Scheduler:** Use the Scheduler to manage automated data imports.

- **Import Utility:** Imports .csv files into the CSM Database.

Stand-alone Database Tools

- **System Restore Tool**: Allows a system administrator to import the CSM Database for the first time or reload the CSM Database from an archive file (.czar file).

- **System Upgrade Tool**: Allows a system administrator to upgrade a CSM Database to a new version. When installing a new version of CSM and running Cherwell Administrator, it prompts an upgrade to the database and automatically runs this tool.

- **Import Utility:** Imports .csv files into the CSM Database.

System Restore Tool

The System Restore tool is a standalone database tool that allows a system administrator to import the CSM database for the first time or reload the CSM database from an archive file (.czar file).

Use the System Restore tool to:

- Copy the database over multiple environments (testing, staging, and development).
- Provide copies of database for a support team.
- Back up and restore the data if moving the database from one server to another.
- Back up the data and restore the database in another environment.
- Enable multi-byte support for a database.

Warning: After restoring a database, replaced data is no longer accessible.

To restore a database:

1. Open the System Restore tool (**Start > All Programs > Cherwell Service Management > Tools > System Restore**.

    Note: On Windows 7, right-click and select **Run as Administrator**.

2. Select the database file (.czar) to import (restore):
    a. Select **Browse** and navigate to a .czar file.
    b. Select the file and select **Open**. The .czar path and name appear in the **Import file** field. The .czar details (Date/Time exported, Mode, and version) appear below the file.

3. Select where to restore the .czar file, either:
    ◦ **Existing connection**: Enables the .czar file to overwrite an existing database. Select the ellipsis to select the database (connection) to overwrite, and then select **Import**.
    ◦ **New database**: Enables the .czar file to create a new database connection. Select the ellipsis to open the Connection Wizard to create a new database connection.

    When the restore is complete, the database connection is available when CSM opens.

4. Unicode support: Enables support for multi-byte characters in your database. See Configure CSM for Multi-Byte Language Support.

5. Select the environment type:
    a. **Development**: The database file is being used to configure functionality.
    b. **Production**: The database file meets all requirements, has been tested, and is ready for business use.
    c. **Test**: The database file is being used for testing purposes.

    Note: The environment type provides visibility into the environment you are working with while managing your system. Once this value is selected, it displays in the client login windows, window titles for the CSM Desktop Client and CSM Administrator (when configured), the **Health Check Results** window, and the **Company Information** drop-down

list in the CSM Browser Client and CSM Portal. You can leverage these values in your configurations using their associated System Functions.

6. Provide the base URL of the Cherwell REST API in the format https://host.domain/CherwellAPI/api/.

> **Note:** If you skip this step, you can still install CSM, but an error that says that the application is not configured to communicate with the Cherwell REST API server will display when you attempt to log in.

When the restore is complete, the database connection is available when CSM opens.

Related concepts

Cherwell REST API Command-Line Options

Set the Base URL for the Cherwell REST API

System Upgrade Tool

The System Upgrade tool allows a system administrator to upgrade a CSM database to a new version. This program usually runs automatically when a new version of CSM is loaded.

There are some systematic windows that might populate as the system runs the update. You are not required to do anything when these windows open.

The System Upgrade tool (accessed from the Cherwell Service Management installation directory) should only be used if the database was not upgraded as part of an application upgrade or an installation.

Note: Only users with appropriate permissions can use the System Upgrade tool.

To upgrade a database:

1. Open the System Restore tool (**Start > All Programs > Cherwell Service Management > Tools > System Upgrade**).

   The **Connect to Service Management - System Upgrade** window opens.

2. Select the database to upgrade.

3. Select **OK**.

   The **System Upgrade** window opens to verify the upgrade.

4. Select **OK**.

   The **System Upgrade** login window opens.

5. Provide the user ID and password.

6. Select **OK**.

Import Utility

Use the Import Utility option in CSM Administrator to import .csv files into the CSM Database.

To use the Import Utility:

1. Go to **Start > All programs > Cherwell Service Management > Tools > Import Utility**.
2. Select the connection to import the data to.

   The Import Utility login window opens.

3. Provide the **User ID** and **Password** for the Import Utility.

   The Cherwell Import Utility window opens.

4. Select **OK**.

   The Cherwell Import Utility window opens.

5. Import from:
   a. Select the **Ellipses**.

   b. Select the file, and then select **Open**.

6. Import to:
   a. From the drop-down list, select the **Business Object**.

     Note: To delete the existing data, select the **Delete existing data from Business Object before import** check box.

7. Advanced:
   a. In the Unique fields, provide column names that make up the unique database key.

     Note: Select the check box to **Try to save object even if one or more fields cannot be set**.

8. Select **Import**.

     Note: If there are unequal fields, a warning window opens. Select **Yes**.

Database Export Tool

Use the Export Data option in CSM Administrator to export a selected CSM database to a compressed Cherwell Archive Repository (.czar) file.

You can export:

- A single Business Object.
- An entire system (full backup).
- A log file to capture the details of the database export.

To export a single Business Object:

1. In CSM Administrator, select the **Database** category, and then select the **Export data** task.

   The **Export Data** window opens.

2. Select the **Export Single Business Object** option.

   The window changes to select a single Business Object.

3. Select the **Business Object** to export.

4. Select the **Exclude encrypted fields and protected stored values** check box to exclude encrypted fields from the export. We recommend excluding encrypted fields and protected stored values you will provide the data to the CSM support team.

5. (Optional) Select the **Logging** check box to generate and export a log file (.log) that captures the details of the export. This file is named the same and exported to the same location as the .czar file.

6. In the **Save To** field, provide a name for the .czar file (example: Incident_Nov2014), and then specify a location. Provide a location or select the ellipsis to navigate to a location.

7. Select **OK**.

To export a system:

1. Follow step 1 above.

2. Select the **Export Entire System** check box.

3. Select the content to export:
   - **Export All Data**: Exports all SQL Server tables (example: Field names and sizes) and data. Use this option to create a full backup .czar of an entire CSM system, and then select to exclude the following so the file is smaller:
     - **Exclude Attachments**: Exports the Attachment table but not the attachment data within the table. Use this option to create a .czar file to troubleshoot problems that are not related to file attachments.

     - **Exclude automation data**: Exports the Events and Scheduler tables, but not the data within the tables. Use this option to create a .czar file to troubleshoot problems that are not related to Automation Processes or scheduled items.

- **Exclude encrypted fields and protected stored values**: Exports field data, but not encrypted fields or protected stored values. Use this option to exclude sensitive data from a .czar file.

  Note: A.czar file will never contain decrypted data, even if encrypted fields are exported. If data is provided to support, we recommend excluding encrypted fields from database exports. Encryption keys are not included in any database exports; we recommend exporting keys from the Server Manager and storing them in a secure location. See Configure Encryption Keys for a Server or Web Application.

- **Exclude emails**: Select to exclude email messages.
- **Export Table Structure Only**: Exports all SQL Server tables without any data. Use this option to create a .czar file that excludes confidential company data.
- **Export Structure and Lookup Table Data**: Exports SQL Server tables for all Major and Supporting Business Objects, as well as tables and data for Lookup Objects (validation tables). Use this to create a .czar file that excludes confidential data but includes values from Lookup Tables (typically, Lookup Tables do not contain confidential data and can be used to troubleshoot problems with validation and relationships).

4. Follow steps 5 - 7 above.

Perform Database System Maintenance

System Maintenance is a database option that helps users maintain their database within CSM. The **System Maintenance** window has a series of check box options separated into sections: Full-Text Search, Manage Indexes, and Data.

Note: Some index management tasks are only available for on-premises installations of CSM.

To perform database System Maintenance:

1. In CSM Administrator, select **Database** task, and then select **System Maintenance**.
2. Select one or all check boxes to run maintenance options.
3. Select **OK**.

Full-Text Search

The **Full-Text Search** section has the option to **Rebuild full-text search catalog**. An ALTER statement drops the full-text index on each searchable Business Object, adds the index back, and then runs a final ALTER FULLTEXT CATALOG Trebuchet REBUILD command.

SQL 2012 and later has built-in logic that performs the rebuild.

Note: This option is only available for on-premises installations of CSM.

Manage Indexes

The **Manage indexes** section has all of the options for running maintenance on the various indexes in the database. The type of indexes include:

Rebuild Business Object Indexes: Runs a SQL statement for selected tables. For example using the Task table:

```
DBCC DBREINDEX('[dbo].[Task]')
```

Rebuild system table indexes: Runs a SQL statement for all of the Cherwell system tables (i.e. TrebuchetTable). For example, using TrebuchetAttach:

```
DBCC DBREINDEX('[dbo].[TrebuchetAttach]')
```

Shrink SQL event log: Runs a SQL statement to shrink the event log for the Cherwell Database. For example using a database named C50:

```
DBCC SHRINKFILE(C50_log,3)
```

Pull up SaaS indexes: Allows Cherwell to pull manually added indexes into the content for hosted customers. This ensures that indexes added to improve performance become part of the content, ensuring completeness for czar backups and other content operations.

Data

The **Data** section has options for running maintenance on the data in the database. These options include:

Refresh queue status: Deletes orphaned records in the TrebuchetQueues system table. This table holds the list of records and queues that the records are on. Running this system maintenance option removes any TrebuchetQueues records that reference a non-existent Business Object record.

Remove unused user accounts: Deletes orphaned records in the TrebuchetAuth system table. This table holds the credentials for users and customers. Running this system maintenance option removes any TrebuchetAuth records that reference non-existent UserInfo or customer records.

Synchronize Team Info Business Objects with team list: Synchronizes the Team Info Lookup table with the CSM user and customer team list.

Delete Temporary Data: The TrebuchetAttach table is used for the temporary storage of various items. For example, if you import a list of customers from a CSV file, the CSV file is stored in this table while it is being processed by the One-Step™ Action. If you write an email, and add an attachment but choose not to import the attachment, the attachment gets uploaded to the TrebuchetAttach table and marked as temporary with a flag. You send your email and then the attachment is removed from the table automatically after 24 hours.

If you use this system maintenance option, it forces the deletion of items older than 24 hours that are not in the middle of being processed. It deletes records stored in the TrebuchetAttach table where the AttachFlags column is marked as "Temporary" or "TemporaryGeneralBlogStorage". As an administrator, you cannot see what is in this table, but rest assured, only data that is no longer needed by CSM is removed when you use this system maintenance option.

Remove orphaned attachments: Attachments can be orphaned (or left behind) when, for example, a Business Object is deleted and the attachment is left with a shortcut that is no longer associated with a Business Object. These orphaned attachments are stored in the TrebuchetAttach table and cannot be viewed because they are not associated with a record or document repository. This system maintenance option removes these orphaned Business Object attachments from the database.

Fix mismatched definition IDs: Fixes incorrect values in the DefID columns in the TrebuchetDefs table to match what is serialized into DefDetails columns. A backup record is saved with the old ID under the DefName.

Configuring Database Security Rights

Configuration procedures are completed in CSM Administrator.

To configure database security rights:

1. Configure database options and Database Server Objects security rights: Configure who can access database functionality.

2. Configure External Data Options security rights: Configure who can access external data functionality.

Configuring a Database Server Object

Licensing Note: Database Server Objects cannot be configured within CSM if the User environment is run in a SaaS or CSM-hosted environment.

1. In CSM Administrator, create a Blueprint.
2. Select **Managers > Database Server Objects**.

   🖉 **Note:** This option is not available for SAAS systems or non-licensed evaluation systems.

   The Database Server Object Manager opens.

3. Select **Create New** ⊕ to open the **Database Server Object** window.

General Page

1. Specify a **Name**.
2. Select a **Server Object** type in the drop-down list.
3. Select a **Dependent Business Object** in the drop-down list.
4. Select the **Show all** check box to display all possible Business Objects in the drop-down list.
5. Specify the SQL script in the text box to create the replication script.
6. Choose the object to import and select **OK**.
7. Select the **Check Syntax** button to validate that the SQL script is correct.
8. Select **Save**.

SQL to Create Object Page

1. Specify a SQL script or click **Import** to import a script.
2. Select **Check Syntax** to validate the SQL script.
3. Select **Save**.

SQL to Drop Object Page

1. Specify a SQL drop script.
2. Select a **Drop and Recreate Behavior** radio button.

Option	Description
Table Dropped	Drops and recreates the server object whenever the table for the Business Object is dropped and recreated.

Option	Description
Table Changed	Drops and recreates the server object whenever the CMS Business Object table is changed.
Only When Function Changes	Creates an object in the CMS database when the Blueprint is published. Use this option to keep stored procedures, triggers, etc. with the CSM database when it is moved.

3. Select **Save**.

Configuring SQL Server

SQL Server can be optimized for your CSM system. For example, you can customize the default stoplist to improve search performance and ensure more meaningful search results. This optimization is typically performed by a database administrator who has knowledge of CSM database structures and tables.

SQL Drop Object Page

On the Drop page, provide the SQL that Cherwell executes to drop the database server object. The SQL to Drop Object page allows entry of a SQL script to drop the object and allows three options for the drop/recreate behavior.

Customizing Stopwords and Stoplists in SQL Server

CSM uses a default stoplist that ignores words like "the" or "an" when Users perform full-text searches. This improves search performance and ensures more meaningful search results.

To learn more about stopwords and stoplists in SQL Server, refer to SQL Server Stopwords and Stoplists.

You can create a custom stoplist that contains stopwords specific to your company's needs. The custom stoplist overrides the default stoplist provided with CSM. (Hosted customers: Contact Cherwell Support for information about custom stoplists.)

Follow this process to implement custom stoplists in SQL Server:

1. Create the custom stoplist.
2. Bind the full-text catalog to a custom stoplist.

> **Note:** The use of SQL scripts is an advanced task typically performed by database administrators. The examples provided in this topic are intended to provide guidance for creating SQL scripts for your system only. Cherwell Software is not liable for changes made to your CSM system with SQL scripts.

3. Creating a Custom Stoplist

Use a SQL script similar to the following example to create a custom stoplist.

Important: Your custom stoplist must be named CherwellStopList.

The following example SQL script:

- Creates a stoplist called CherwellStopList.
- Adds the stopword "search" to the stoplist.
- Removes the stopword "will" from the stoplist.

```
USE <DBName>
GO
CREATE FULLTEXT STOPLIST [CherwellStopList]
FROM SYSTEM STOPLIST;
ALTER FULLTEXT STOPLIST CherwellStopList ADD 'search' LANGUAGE 'English';
```

```
ALTER FULLTEXT STOPLIST CherwellStopList DROP '
will' LANGUAGE 'English';
```

Binding the Full-text Catalog to a Custom Stoplist

Use a SQL script similar to the following example to bind the full-text catalog to your custom stoplist. This process must only be run once; CSM will automatically bind to new and updated tables after the script is run once.

Important: For large databases, this process could take a significant amount of time and may impact search results during the rebuild.

The following example SQL script:

- Creates and populates a temporary table that lists all tables using full-text search.
- Alters each table to use the custom stoplist.

```
Use <DBName>
go
--Create Temp Table for list of tables utilizing Full Text Search
Create table #FullTextTables(
TableName varchar(500))
--Populate the Temp Table
Insert into #FullTextTables
select t.name as TableName
from sys.fulltext_indexes i,  sys.tables t
where i.object_id = t.object_id
--Perform Loop to alter each table to use a different StopList
Declare @TableName varchar(500)
select Top 1 @TableName = TableName from #FullTextTables order by TableName
While @TableName is not null
                        begin
                        exec ('ALTER FULLTEXT INDEX ON '+@TableName+'  Set
StopList CherwellStopList')
                        set @TableName = (Select min(TableName) from #FullT
extTables where TableName > @TableName)
                        end
```

--Rebuild the FullText Catalog to repopulate the Full Text Catalog with the new Stoplist

```
ALTER FULLTEXT CATALOG [Trebuchet] REBUILD
```

Using Databases with CSM

CSM has the ability to connect with an External Database and integrate with third-party software using one of the connection wizards or integrations. CSM works with the CSM Database, Exchange Mail Server, External Database, and Integrations.
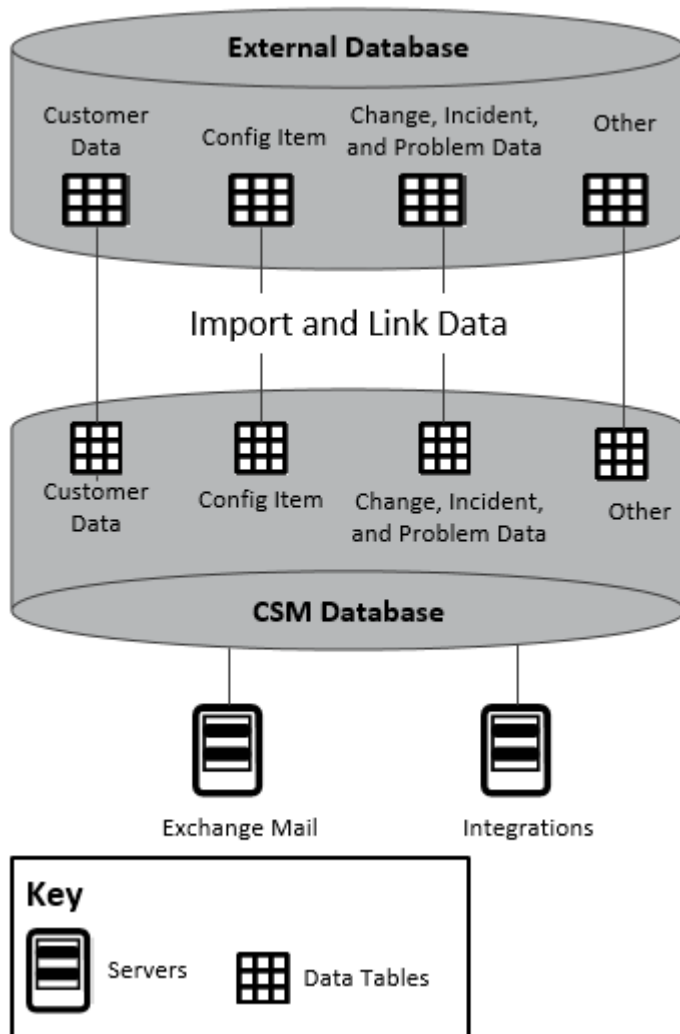
Demo and Starter Databases

CSM provides two databases:

- Starter database: Contains all the structure (example: Business Objects, Forms, One-Step Actions, Security Groups, etc.) needed to start using CSM in a live environment. The Starter database option does not include sample data.

- Demo database: Contains structure (example: Business Objects, Forms, One-Step Actions, Security Groups, etc.) and sample data (example: Sample Incidents, Requests, Problems, Users,

Customers, etc.) for new Users who want to demo CSM. Demo content can be cleared to begin using the system.

If installing the Starter database:

1. Create User Profiles before anyone can log into CSM.
2. Create Customer Profiles before anyone can log into the Customer Portal.

Tip: Use **CSDAdmin** (User ID and Password) to initially log in.

Database Categories Options

Use the CSM Administrator Database page (CSM Administrator>Database) to perform several data and database operations:

- **Export Data:** Opens the Export Data window to export a database (or parts of it) to a compressed file (.czar).

- **Run a One-Off Data Import (.csv files):** Opens the Import Data Wizard that walks Users through the steps to run a one-time import of CSV data into a CSM Business Object.

- **Stored Import Definition Manager (.csv files):** Opens the Stored Import Definition Manager that helps manage (create, edit, delete, etc.) Stored Imports (saved imports that can be used over and over again). For more information, see Use the Stored Import Definition Manager for .CSV Files.

- **Import External Data:** Opens the External Data Import Wizard that walks Users through the steps to import external data from an External Database into a mapped CSM Business Object.

- **Import Active Directory Data into Business Object**: Opens the Active Directory Import Wizard that walks Users through the process to import contacts from Active Directory into a CSM Business Object.

- **Import Knowledge**: Opens the Import Knowledge Wizard that walks Users through the steps to import canned Knowledge from KnowledgeBroker, Inc®.

  Note: For more information about Importing Knowledge, see Knowledge.

- **System Maintenance:** Opens the System Maintenance window to perform database system maintenance (Full-Text Searches, indexes, and some Queue/User accounts).

External Connection Manager

Use the External Connection Manager to complete general CSM Item Manager operations for External Connections.

To open the External Connection Manager:

In the Blueprint or mApp Editor menu bar, select **Managers > External Connections**. For more information, see Blueprint Editor Menu Bar or mApp Editor Menu Bar.

Stored Import Definition Manager

Use the Stored Import Definition Manager to complete general CSM Item Manager operations for stored .csv imports.

Open the Stored Import Definition Manager

Open the Stored Import Definition Manager from CSM Administrator.

To open the Stored Import Definition Manager:

- In CSM Administrator, select **Database > Stored Import Definition Manager (.csv files)**.
- In the Blueprint or mApp Editor menu bar, select **Managers > Stored Imports**.

Create CSM Database Views

Database views combine data from different database tables. In CSM, Views allow Users to view or import data using external connections.
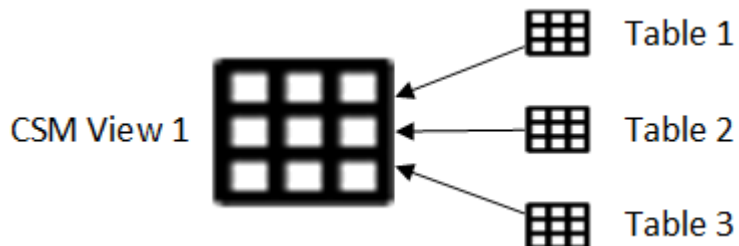
To create a CSM Database view:

1. In CSM Administrator, create a Blueprint.

2. Select **Managers > Database Server Objects**.

   🖉 **Note:** This option is not available for SAAS systems or non-licensed evaluation systems.

   The Database Server Object Manager opens.

3. Select **Create New** ➕.

   The **Database Server Object** window opens.

4. On the **General** page:
   a. Specify a **Name**.

   b. Select **View** in the **Server Object** drop-down list.

   c. Select the **Business Object** in the **Dependent Business Object** in the drop-down list.

   d. Select **Save**.

5. Select the **SQL to Create Object** tab.
   a. Specify a SQL script or select **Import** to import a script.

   b. Select **Check Syntax** to validate the SQL script.

   c. Select **Save**.

6. Select the **SQL Drop Object** tab.
   a. Specify a SQL drop script.

   b. Select the **Drop and Recreate Behavior** radio button.
      i. **Table Dropped:** Drops and recreates the server object whenever the table for the Business Object is dropped and recreated.

      ii. **Table Changed:** Drops and recreates the server object whenever the Business Object table is changed.

     iii. **Only When Function Changes:** Creates an object in the database when the Blueprint is published. Use this option to keep view with the CSM database when it is moved.

     iv. Select **Save**.

7. Publish the Blueprint.

Clear CSM Records

Clear test records from your system so they do not interfere with your metrics during production. For example, you can clear Demo content from a database.

Complete the following procedure for any Business Object.

To clear Business Object records:

1. Open the CSM Desktop Client.

2. Run a **Quick Search** for the Business Object:
   a. In the CSM Desktop Client Task Pane, select the down arrow on the **Search** button.

   b. Select a **Business Object** to search (example: Incident).

   > **Tip:** Make sure that you are not limiting the search by either the date or open records only.

   c. Select the **Go** button to run the search.

   The test record(s) display in the Main Pane.

3. Select **File** and select **Delete All**.

   A window opens verifying that you want to delete all of the records from the group.

4. Select **Yes**.

   The records are cleared from the system.

Import Data from External Databases

Import data into CSM by creating connections to an external database. Map a Business Object to the external connection, and then import data into the Business Object.

CSM and all Business Objects can be mapped to several external databases at one time.

To define the following external connections, open CSM Administrator, create or open a Blueprint, select **Managers > External Connections**, and select the **Add** button to open the **External Connection Wizard**:

- Data Source
- Provider
- Location of the database server
- Name/location of the database
- Login options (credentials)
- Owner/schema
- Pooling options

About Imported Data and Linked Data

You can choose to use an external database connection to import or link to CSM Business Object data. There are pros and cons to each approach.

Considerations for Linked Data

Pros:

- CSM always shows the external database's most recent data (that is, databases are in sync).
- CSM Users can directly update data in the external database if you enabled updates for the External Business Object.

Cons:

- The option to link new Business Objects to an external database is not available for Cherwell SaaS customers.
- You cannot modify an existing Business Object to configure external database connections.
- CSM's underlying SQL queries cannot cross the CSM/external database boundary.
  - **Example 1:** Create a One-Step Action to use a Linked External Business Object, but that One-Step Action cannot use a CSM Business Object. Likewise, create a One-Step Action to use a CSM Business Object, but that One-Step Action cannot use a Linked External Business Object.
  - **Example 2:** Create a Search to use a Linked External Business Object, but that Search cannot use a CSM Business Object. Likewise, create a Search to use a CSM Business Object, but that Search cannot use a Linked External Business Object.
- There is potential for reduced performance when retrieving data from an external database. If the external database goes offline, there can be a significant delay while CSM attempts to connect before timing out.
- Unless done carefully, updates from CSM could possibly violate business rules of the external database.
- When data is changed outside of CSM, CSM Automation Processes are not initiated. If the data is changed within CSM, then the business logic is executed.

Considerations for Imported Data

Pros:

- You can import external data into new and existing Business Objects.
- The data is available for every single feature in CSM. The data is not limited by the CSM boundary or system boundary mentioned above.
- Use additional CSM fields to augment the imported data.
- Full-Text Search can be used for searching.

- The imported Table/View can become part of a CSM Group (example: It could be a Configuration Item Group member).

Cons:

- The data is only as current as the last import. However, use the Cherwell Scheduler to import the data at regular intervals.
- If data is deleted from the external database, it still exists in CSM.

Map an Existing Business Object to External Data

Use an existing Business Object to establish external connections and import external data directly into both the Business Object and CSM. The imported data can be edited within CSM or updated via Automation Processes.

An existing Business Object cannot link to external data. To link external data to a Business Object and manipulate the data from the external source, refer to Create an External Business Object to Link to External Data.

To establish an external connection to a Business Object and import external data:

1. In the CSM Administrator main window, click the **Blueprints** category, and then click **Create a New Blueprint** or open an existing Blueprint.

   The Blueprint Editor opens, showing the Object Manager in its Main Pane. The Object Manager lists the existing Business Objects.

2. Select an existing Business Object (example: Incident).

3. Click the **Map to external data** task. Or select **New Object**, and then **New external business object** task. The External Data Wizard opens.

4. Select **Next**.

   The Import vs. Linked page opens.

   > **Note:** The Link to Data option is available only when creating a new Business Object. Connecting to an existing Business Object must be performed with an import.

5. Click the **Import Data** radio button.

6. Select **Next**.

   The Data Source page opens.

7. Click the ellipses button. The **External Connection** manager opens. Select an existing External Database or click the **New** button to create a new External Connection.

8. Select **Next**.

   The External Table to Map page opens, listing the available tables the selected External Database.

9. Select a **table** to import.

10. Select **Next**.

    The Fields to Map page opens.

11. Map fields from the selected table to a field in the new External Business Object:

a. Click the **Add** button.

   The Map Field from External Table manager opens, listing the available fields based on the selected External Database and External Table.

b. Select an external field (example: Created By).

c. Select an existing Cherwell Service Management field to map the external field to or create a new field (example: Last Modified).

d. Select **OK**.

e. Repeat mapping process for all desired fields.

12. Select **Next**.

   The Unique Key and Timestamp Fields page opens. Values in the Unique Key and Timestamp drop-downs are based on the fields that were mapped in Step 11.

13. Choose a Unique Key and Timestamp field:
   a. Field that Holds Unique Key drop-down: Displays the external field chosen from the previous page. This field becomes the unique key, which is used during imports to ensure records in the field are updated if they already exist in Cherwell Service Management.

   b. Last Modified Date/Time drop-down: Select a value from the drop-down to dictate when to update the unique key field. If selecting a Last Modified Date/Time value, it is recommended to add SQL indexes to these fields after configuring the External Data Import (**Business Object Editor > Business Object Properites > Databases > Add Index button > Select Last Modified Date/Time values**). Doing so ensures optimal import performance.

14. Select **Next**.

   The Summary page opens and displays details established during the setup process.

15. Select **Finish**.

   The Business Object's Properties window opens, showing current and editable Business Object properties. An external data page displays External Connection details established in the External Data Wizard.

16. Click **OK** to close the Properties window.

17. (Optional for Supporting Objects) If needed, create a Relationship between the newly created Supporting Objects and the Major Object they support.

18. Publish the Blueprint (File>Publish Blueprint) to commit the changes, or save the Blueprint (File>Save Blueprint) to continue making other changes.

Map a Business Object to Multiple External Connections

Multiple external connections can be mapped to the same Business Object. Doing so allows users to import data into the Business Object from both external connection sources.

You can map a Business Object to multiple external connections through the Business Object Properties page. You can also create and configure external connections via the External Connections Manager.

Create Multiple External Connections with the External Connection Wizard

To map a Business Object to multiple external connections:

1. In the CSM Administrator main window, select the **Blueprints** category and select **Create a New Blueprint** or **Open an Existing Blueprint**.

2. Select a **Business Object** that has already been mapped to one or more instances of external data (example: another user has mapped the Problem Business Object to two external databases).

3. Select **Map to External Data**. The External Data Wizard opens.

4. Select **Next**.

5. Select **Import Data**. The Linking Data feature is disabled; multiple database connections can only be established when importing data directly into CSM. Linking Data is also only available when mapping External Data to a new Business Object.

6. Select **Next**.

7. From the **Data Source** page, select the **Ellipses** button to open the External Connection Manager.

8. Select an additional external connection from the Data Source menu (example: Employee_Info_1 and Employee_Info_2).

9. Select **Next**.

10. Select the **External Table to Map** page, select a table name from the external database to map the Business Object to (example: EmployeeName).

11. Select **Next**.

12. In the **Fields to Map** page, select **Add**. The Map Field from External Table picker opens.

13. Select **Existing Field** or **Create a New Field** to determine what Business Object field the imported data is added to.

14. Select **OK** to close the Map Field from External Table picker.

15. Repeat for all desired fields.

16. Select **Next**.

17. From the **Unique Key and Timestamp Fields** page, select a **Unique Key Field**. CSM uses the Unique Key and the Last Modified field to determine whether or not data needs to be updated during imports.

18. (Optional) Select a **Last Modified** value (example: ActualEndDate). CSM uses the Last Modified field to determine if the Unique Key data needs updating. Leaving this field blank means CSM

always updates previously imported data from the selected database. If selecting a Last Modified Date/Time value, it is recommended to add SQL indexes to these fields after configuring the External Data Import (**Business Object Editor > Business Object Properites > Databases > Add Index button > Select Last Modified Date/Time values**). Doing so ensures optimal import performance.

19. Select **Next**. The **Summary** page opens.

20. Select **Finish**. The **Business Object Properties** page opens, view and edit external connections mapped to the selected Business Object if desired.

Edit External Connections from the Business Object Properties Page

A Business Object's external connections can be edited through the **Business Object Properties** page. You can also create new external connections for a Business Object that has already been mapped to external connections.

To map a Business Object to multiple external connections:

1. Select a Business Object from the Blueprint Object Manager. The Business Object must be an existing Business Object that is already mapped to external data.

2. Select **Edit Business Object**. The **Edit Business Object** page opens.

3. Select the **Business Object Properties button**. The **Business Object Properties** page opens.

4. Select the **External Data** category. If this category is not visible, then the Business Object has not been mapped to external data. To map a Business Object to external data, see Map an Existing Business Object to Import External Data. After selecting the External Data category, the External Data summary page opens, detailing the external connections that have been mapped to the selected Business Object.

5. Select an external connection from the **Mapped External Connections** menu. Summary information displays in the External Data summary page.
   From the summary page, you can:

   ◦ Select **Add** to create an additional external connection.

   ◦ Remove the mapping to external connections from the Business Object.

   ◦ Add, edit, or remove mapped fields.

   ◦ Update the field that holds the book unique ID.

   ◦ Update the field that holds the last modified date/time.

   ◦ Edit the number of records to import at a time. The default batch size is 1,000, which should be appropriate in most cases. Importing large batches may cause load balancer timeouts, so if you are experiencing either of these problems, try lowering the number of records imported at a time. The minimum batch size is 1 and there is no upper limit.

   Note: This setting only applies if you are using a 3-tier connection.

6. After editing the external connections, select **OK** to close the **Business Object Properties** page.

7. Save or publish the Blueprint.

Related concepts

[Link External Data to a New External Business Object](#)

[Map an Existing Business Object to External Data](#)

Create an External Connection to an API

Use the External Connection Wizard to create and manage External Connections. External Connections can be created with the following types of APIs that provide access to a range of data sources:

- MySQL or SQL Server

- Oracle

- ODBC: Used for many sources, including file formats like Excel files, Access databases, .txt files, and more.

  🖉 **Note:** The ODBC Providers list might vary depending on the drivers installed.

- OLE DB: This is the newer version of ODBC and is used for both relational and non-relational databases (SQL, Oracle, Excel, raw files, etc.)

Create an External Connection to a MySQL or SQL Server Database

Create a connection to an external MySQL or SQL Server database. Then, you can map a Business Object to the connection, and import data into the Business Object.

MySQL Connector 6.9.4 must be installed to create, edit, or use MySQL external connections. The MySQL Connector can be downloaded from https://downloads.mysql.com/archives/c-net/.

An external connection connects CSM to an external database. These steps are specifically for an external connection between CSM and a SQL Database.
To create an External Connection to a MySQL or SQL Server Database:

1. Open or create a Blueprint.
2. Select **Managers > External Connections** to open the External Connections Manager.
3. Select **Create New** to open the External Connection Wizard.
4. Select **Next**.
5. On the **Login options** page, select the **Use Trusted Agents** check box if you use the Trusted Agents feature and you want to control how the system logs in to the external data source.
6. Select one of these options, and then select **Next**.
    ◦ **Any Trusted Agent Group**: Select to allow any group to handle requests for this external connection.
    ◦ **Trusted Agent Group**: Select a specific group to handle requests for this external connection.
7. On the **Data Source** page, select **MySQL** or **SQL Server**, and then select **Next**.

   > **Note:** The option to select MySQL is available only if the MySQL Connector 6.9.4 is installed.

8. On the **Database Location** page, select the location of the SQL Database:
    ◦ **Located on this machine**: Select this option if running a local database. Typically, this is only for evaluation systems.
    ◦ **Specific Server**: Select this option to select a database installed on a named server, and then select the specific server in the drop-down list.

      > **Note:** If the connection is to a named instance of SQL (a non-default instance of SQL), select the option and then specify the instance in the **Specific Server** value using the format: DatabaseServer\InstanceName.

    ◦ **IP Address**: Select this option to select a database installed on a server referenced by an IP address, and then provide the database server IP address.
9. Select **Next**.
10. On the **Select Database** page, select **Browse**.
    The **Login to server** window opens.
11. Select a login radio button to use either:

- **Windows authentication**: Use the stored Windows credentials (user name and password) for authentication.
- **User ID and Password**: Provide the server User ID and Password.

12. Select **OK**. The system runs for a few minutes and the **Choose a Value** window opens.

13. Select a database, select **OK**, and then select **Next**.

14. On the **Login Options** page, if the database requires login information, select the **Login Required** check box and either:
    - **Windows Authentication**: Uses the stored Windows credentials (user name and password) for authentication.
    - **User ID and Password**Provide a user ID and password.

    > **Note:** The account must have select rights for each table that is imported or linked to CSM. If CSM is allowed to update data in the database, this account must also have insert and update rights.

15. Select **Next**.

16. On the **Database Owner or Schema** page, select an option from the drop-down list or provide a database owner or schema. This field should be pre-populated.

    > **Note:** Not all databases have this concept. If implemented and CSM is able to read the available owners, then they are listed in the drop-down list. If not, provide the owner name. If unsure, provide the default dbo.

17. On the **Pooling Options** page, select a Connection Pooling option for the database:
    - Select the **Use default pooling options** radio button.
    - Select the **Customize the pooling options** radio button, and then provide the minimum and maximum pool size.

        > **Note:**
        >
        > To improve performance, set the maximum pool size to three times the number of concurrent CSM licenses that are used in your organization. You may need to adjust this value, depending on usage of your system.

    The **Connection name** page opens.

18. On the **Connection name** page, provide a name and description (optional) of the database connection, and then select **Next**.
    The **Connection String** page opens, showing the connection string that is used to connect to the database. Modify the connection string, if needed. Many examples of connection strings can be found at www.connectionstrings.com.

19. Select **Test Connection** to verify the connection to the server/database. Text appears next to the button confirming the connection is successful.

20. Select **Finish**. A connection now exists to the SQL Server database.

21. Publish the Blueprint (**File > Publish Blueprint**) to commit the changes, or save the Blueprint (**File > Save Blueprint**) to continue making other changes.

Related concepts
Publish a Blueprint
Save a Blueprint
Related tasks
Create a Blueprint
Import External Data Using Trusted Agent

Create an External Connection to Oracle

Create a connection to an external Oracle Server database. Then, you can map a Business Object to the connection, and import data into the Business Object.

An external connection connects CSM to an external database. The steps below are specifically for an External Connection between CSM and an Oracle Database.
To create an external connection to an Oracle Server Database:

1. Open or create a Blueprint.
2. Select **Managers > External Connections** to open the External Connections Manager.
3. Select **Create New** to open the External Connection Wizard.
4. On the **Login options** page, select the **Use Trusted Agents** check box if you use the Trusted Agents feature and you want to control how the system logs in to the external data source.
5. Select one of these options, and then select **Next**.
   - **Any Trusted Agent Group**: Select to allow any group to handle requests for this external connection.
   - **Trusted Agent Group**: Select a specific group to handle requests for this external connection.
6. On the **Data Source** page, select **Oracle**.
7. On the **Select Net Service Name** page, provide the full string containing the service name.

   ```
   (DESCRIPTION=(ADDRESS=(protocol_address_information))(CONNECT_DATA=(SE
   RVICE_NAME=service_name)))
   ```

8. On the **Login Options** page, if the database requires login information, select the **Login Required** check box and either:
   - **Windows Authentication**: Uses the stored Windows credentials (user name and password) for authentication.

     Note: When Cherwell Services use this connection, the account under which the Cherwell Application Service is running is the account whose credentials are used to connect to the database.

   - **User ID and Password**: Provide a user ID and password.

     Note: The account must have select rights for each table that is imported or linked to CSM. If CSM is allowed to update data in the database, this account must also have insert and update rights.

9. Select **Next**.
10. On the **Database Owner or Schema** page:
    a. Select an option from the drop-down list or provide a database owner or schema. This field should be pre-populated. Not all databases have this concept. If implemented and CSM is able to read the available owners, then they are listed in the drop-down list. If not, provide the owner name. If unsure, provide the default dbo.

b. Select **Next**.

11. On the **Pooling Options** page, select a Connection Pooling option for the database, and select **Next**:
    - Select the **Use default pooling options** radio button.
    - Select the **Customize the pooling options** radio button, and then provide the minimum and maximum pool size.

        Note:

        To improve performance, set the maximum pool size to three times the number of concurrent CSM licenses that are used in your organization. You may need to adjust this value, depending on usage of your system.

12. On the **Connection name** page, provide a name and description (optional) of the database connection, and then select **Next**.
    The **Connection String** page opens, displaying the connection string that is used to connect to the database. Modify the connection string, if needed. Many examples of connection strings can be found at www.connectionstrings.com.

13. Select **Test Connection** to verify the connection to the server/database. Text appears next to the button confirming the connection is successful.

14. Select **Finish**. A connection now exists to the Oracle database.

15. Publish the Blueprint (**File > Publish Blueprint**) to commit the changes, or save the Blueprint (**File > Save Blueprint**) to continue making other changes.

Related concepts
Publish a Blueprint
Save a Blueprint
Related tasks
Create a Blueprint
Import External Data Using Trusted Agent

Create an External Connection to an OLE DB

Create a connection to connect CSM through OLE DB to an Oracle Database. OLE Database is a standard that allows CSM to connect to a variety of databases in a common format.

The steps below are specifically for an external connection between CSM and an OLE Database to SQL. **To create an external connection to an OLE Server Database:**

1. Open or create a Blueprint.
2. Select **Managers > External Connections** to open the External Connections Manager.
3. Select **Create New**.
   The External Connection Wizard opens.
4. Select **Next** to open the **Data Source** page.
5. On the **Login options** page, select the **Use Trusted Agents** check box if you use the Trusted Agents feature and want to control how the system logs in to the external data source.
6. Select one of the following options, and then select **Next**.
   - **Any Trusted Agent Group**: Select to allow any group to handle requests for this external connection.
   - **Trusted Agent Group**: Select a specific group to handle requests for this external connection.
7. On the **Data Source** page, select **OLE DB**, and then select **Next**.
8. On the **OLE DB Provider** page, select an OLE DB Provider, and then select **Next**.

   Note: If you are using Oracle as the provider, there are some differences in the wizard. Drivers are available from Oracle: www.oracle.com/database/technologies/instant-client.html. Consult Oracle Support if you need assistance locating this driver. There are also OLE Database drivers from third-party vendors that can be used.

9. On the **Database Location** page, select one the following database locations of the connecting database, and select **Next**.
   - **Located on this Machine**: Select this option if running a local database. Typically, this is only for evaluation systems.
   - **Specific Server**: Select this option to select a database installed on a named server, and then select the named server.
   - **IP Address**: Select this option to select a database installed on a server referenced by an IP address, and then provide the IP address.
   - **Data Comes from file**: Select this option if the driver connects directly to a file rather than to a database server. If selected, the **Database** field is replaced with a **File** field.

     Note: This radio button is only shown when CSM does not detect if the provider connects to a database or a file.

10. On the **Select Database** page, provide the name of the database/file to which to connect, or select **Browse** to see a list of available databases/files.
11. On the **Login to server** window, select to use either Windows authentication or the ID and password of the server.

The system runs for a few minutes, and then the **Choose a Value** window opens.

12. Select a database, then select **Next**.

13. On the **Login Options** page, if the database requires login information, select the **Login Required** check box and either:
    ◦ **Windows Authentication**: Uses the stored Windows credentials (user name and password) for authentication.
    ◦ **User ID and Password**: Provide a user ID and password.

    > **Note:** The account must have select rights for each table that is imported or linked to CSM. If CSM is allowed to update data in the database, this account must also have insert and update rights.

14. Select **Next**.

15. On the **Database Owner or Schema** page, select an option from the drop-down list or provide a database owner or schema. This field should be pre-populated. Select **Next**.

16. On the **Pooling Options** page, select either **Use OLE DB connection pooling** or **No pooling**.

17. On the **Connection name** page, provide a name and description (optional) of the database connection, and then select **Next**.
    The **Connection String** page opens, displaying the connection string that is used to connect to the database. Modify the connection string, if needed. Many examples of connection strings can be found at www.connectionstrings.com.

18. Select **Test Connection** to verify the connection to the server/database. Text appears next to the button confirming the connection is successful.

19. Select **Finish**. A connection now exists to the External OLE Database database.

20. Publish the Blueprint (**File > Publish Blueprint**) to commit the changes, or save the Blueprint (**File > Save Blueprint**) to continue making other changes.

Related concepts
Publish a Blueprint
Save a Blueprint
Related tasks
Create a Blueprint
Import External Data Using Trusted Agent
Create an External Connection to Oracle

Create an External Connection to ODBC

An External Connection connects CSM to an External Database. The steps below are specifically for an External Connection between CSM and an ODBC.

ODBC Requirements:

- The ODBC provider must show as available on the current machine.
- The Desktop Client must be installed.
- For Oracle: Client must have Oracle 11 or 12 on the Application Server and it must be configured.

To create an External Connection to an ODBC Server Database:

1. Open or create a Blueprint.
2. Select **Managers > External Connections** to open the External Connections Manager.
3. Click **Create New**.

   The External Connection Wizard opens.

4. On the **Login options** page:
   - Select the **Use Trusted Agents** check box if you use the Trusted Agents feature and you want to control how the system logs in to the external data source.
   - Select one of these options:
     - **Any Trusted Agent Group**: Select to allow any group to handle requests for this External Connection.
     - **Trusted Agent Group**: Select a specific group to handle requests for this External Connection.
   - Click **Next**.

   For more information, refer to Import External Data Using Trusted Agent.

5. On the **Data Source** page:
   a. Select **ODBC**.

   b. Select **Next**.

6. On the **ODBC Provider** page:
   a. Select an **ODBC Provider**.

      Note: The ODBC Providers list might vary depending on the drivers installed. If using Oracle as the provider, there are some differences in the Wizard. For more information, see Create an External Connection to Oracle.

   b. Select **Next**.

7. On the Database Location page:

       a. Select the **Database Location** of the connecting database:
- **Located on this Machine:** Select this option if running a local database. Typically, this is only for evaluation systems.
- **Specific Server:** Select this option to select a database installed on a named server, and then select the named server.
- **IP Address:** Select this option to select a database installed on a server referenced by an IP address, and then provide the IP address.

       b. Select **Next**.

8. On the **Select a Database** page:
- Provide the **Name** of the database/file to which to connect, or click **Browse** to see a list of available databases/files.
- Click **Browse**.

       The Login to server window opens.

       a. Select a **login** radio button to use either:
- Windows authentication
- User ID and Password: Provide the server User ID and Password.

       b. Select **OK**.

       The system runs for a few minutes and the Choose a Value window opens.

       c. Click a **database**.

       d. Select **OK**.

9. Select **Next**.

10. On the **Login Options** page:
       a. If the database requires login information, select the **Login Required** check box and either:
- Windows Authentication: Uses the stored Windows credentials (user name and password) for authentication.

       Note: When Cherwell Services use this connection, the account under which the Cherwell Application Service is running is the account whose credentials are used to connect to the database.

- User ID and Password: Provide a **User ID** and **Password**.

       Note: The account must have select rights for each table that is imported or linked to CSM. If CSM is allowed to update data in the database, this account must also have insert and update rights..

       b. Select **Next**.

11. On the **Database Owner or Schema** page:
    a. Click an option from the drop-down or provide a **Database owner or schema**. This field should be pre-populated.

> **Note:** Not all databases have this concept. If implemented, and CSM is able to read the available owners, they are listed in the drop down. If not, provide the owner name. If unsure, provide the **dbo** default.

    b. Select **Next**.

12. On the **Connection Name** page:
    a. Provide a **Name** for the database connection.

    b. (Optional) Provide a **Description** for the database connection.

    c. Select **Next**.

    The Connection String page opens, showing the connection string that is used to connect to the database. Modify the connection string, if needed. Many examples of connection strings can be found at www.connectionstrings.com.

13. Click **Test Connection** to verify that the connection to the server/database.

    Text appears next to the button confirming the connection is successful.

> **Note:** If the test connection is not successful, contact a DBA for help.

14. Select **Finish**.

    There is now a connection to the External ODBC Database.

15. Publish the Blueprint (File>Publish Blueprint) to commit the changes, or save the Blueprint (File>Save Blueprint) to continue making other changes.

Link External Data to a New External Business Object

Linking Business Objects to external data allows for real-time updates between an external database and CSM. If updates of the external data are permitted, the Business Object can be configured to enforce the appropriate rules. A Business Object can only be linked to one external data connection.

To link external data to a new External Business Object:

1. In the CSM Administrator main window, click the **Blueprints** category, and then click the Create a New Blueprint task.

   The Blueprint Editor opens, showing the Object Manager in its Main Pane. The Object Manager lists the existing Business Objects.

2. Click **New Object** from the Object Manager, then select the **New External Business Object** task.

   The External Data Wizard opens.

3. Select **Next**.

   The Import vs. Linked page opens.

4. Click the **Link to data** radio button.

5. Select **Next**.

   The Data Source page opens.

6. Click the ellipses button. The **External Connection** manager opens. Select an existing External Database or click the **New** button to create a new External Connection.

7. Select **Next**.

   The External Table to Map page opens, listing the Tables and/or Views from the External Database.

8. Click to select the **Table** or **View** to link to.

9. Select **Next**.

   The Business Object Type page opens.

10. Select the **type** of External Business Object to create: Major Business Object, Supporting Business Object, or Lookup.

11. Click **Next**.

    The Cherwell Group page opens.

12. Select a radio button to assign the External Business Object to a Group.

13. Select **Next**.

    The Fields to Map page opens.

14. Map fields from the selected table to a field in the new External Business Object:
    a. Click the**Add** button.

       The Map Field from External Table manager opens, listing the available fields.

    b. Select an external field (example: Created By).

    c. Select an existing Cherwell Service Management field to map the external field to or create a new field.

    d. Click **OK**.

    e. Repeat mapping process for all desired fields.

15. Select **Next**.

    The Unique Key and Timestamp Fields page opens. The screen shots show example fields.

16. Designate a Unique Key and Timestamp field:
    ◦ **Field that Holds Unique Key:** Select the **field from the View that is deemed as the unique identifier** (example: MachineID or ComputerID).

       Note: There must be a unique ID field for CSM to use the External Table/View. If the Table/View does not have a Unique Key, add one.

    ◦ **Last Modified Date/Time:** Select the **field** from the Table/View that is deemed as the last modified date/time field (example: LastScanDate or date_modified).

17. Select **Next**.

    The Read-Only or Updatable page opens.

18. Select the radio button to establish whether the data should be read-only or if it can be updated in CSM.

19. Select **Next**.

    The Search Options page opens.

20. Define searching options for the External Business Objects (only available for linked external data):
    a. Use SQL Server Full-Text Search: Select this check box to enable Full-Text Search.

       SQL Server Note: If the External Database is SQL Server, select the **SQL Server Full-Text Search** check box to have CSM send full-text queries to the External Database when searches are done. In order to use Full-Text Search, it must be configured in the External Database. Refer to SQL Server documentation for details on how to set up Full-Text Search.

     b. Fields to search: Click **Add** to select the fields that should show when searches are conducted inside CSM (example: Quick Search).

     c. Select the Search type:

       ◦ **Exact match:** The search string must exactly match a word or phrase in order for the record to be found. For those familiar with SQL, use the SQL clause:

        where (field = 'value')

       ◦ **Starts with:** This finds records containing words or phrases that start with the search string. This is the recommended selection. For those familiar with SQL, use the SQL clause:

        where (field LIKE 'value%')

       ◦ **Contains:** This returns records that contain the search string. This is slower than the other two options. If the database table contains millions of records, then do not use this option. For those familiar with SQL, use the SQL clause:

        where (field LIKE '%value%')

21. Select **Next**.

    The Name and Description page opens.

22. Provide a **Name** for the External Business Object.

23. (Optional) Type a **Description** for the External Business Object.

24. Select **Next**.

    The Summary page opens. The information varies depending on selections throughout the wizard.

25. Select **Finish**.

    The Business Object's Properties window opens, displaying current (and editable) properties, including a:

    ◦ **External Data page:** View/edit the field mappings, unique ID, and last modified date/time fields.

    ◦ **External Search page:** View/edit external search options (if defined).

    ◦ **Search Results page:** Displays the Full-Text Search and quick search (if defined).

    ◦ **Database page:** Read-only because the Table/View actually resides in another database.

26. Click **OK** to close the Properties window. Create Forms and Grids for the External Business Object just as a new CSM Business Object.

    Create Forms and Grids for the External Business Object just as a new CSM Business Object. (Optional for Supporting Objects) If needed, create a Relationship between the newly created Supporting Objects and the Major Object they support.

27. Publish the Blueprint (File>Publish Blueprint) to commit the changes, or save the Blueprint (File>Save Blueprint) to continue making other changes.

Import External Data into a New External Business Object

Create a new Business Object to import external data into.

When importing external data, data is imported into the Cherwell Service Management system and edited there. Linking external data allows for the data to be manipulated within the external source.

To import external data to a new External Business Object:

1. In the CSM Administrator main window, select the **Blueprints** category, and then select **Create a New Blueprint** or open an existing Blueprint.

   The Blueprint Editor opens, showing the Object Manager in its Main Pane. The Object Manager lists the existing Business Objects.

2. Select **New Object** from the Blueprint Object Manager, and then select the **New external Business Object** task. The External Data Wizard opens.

3. Select **Next**.

   The **Import vs. Linked** page opens.

4. Select the **Import data** option.

5. Select **Next**.

   The **Data Source** page opens.

6. Select **Ellipses**. The **External Connection** manager opens. Select an existing External Database or select **New** to create a new External Connection.

7. Select **Next**.

   The **External Table to Map** page opens, listing the Tables and/or Views from an External Database.

8. Select the **Table** or **View** to import.

9. Select **Next**.

   The **Business Object Type** page opens if creating a new object. If using an existing object, go to the **Map to Fields** page.

10. Select the Type of Business Object to create: Major, Supporting, or Lookup.

11. Select **Next**.

    The **Part of Cherwell Group** Group page opens.

12. Define Group information options for the External Business Object:

- Not a Member of a Group: Select this option if the Business Object is not part of a Group.

- Group Leader: Select this option to make the Business Object a Group Leader.

- Member of: Select this option if the Business Object is going to be part of an existing Group. Select the Group from the enabled drop-down list.

13. Select **Next**.

    The **Fields to Map** page opens.

14. Map fields from the Table/View to a Field in the new External Business Object:
    - To map all available Table/View Fields at once, select **Map all fields**. The Wizard automatically creates a new Field for each external Table/View Field and populates the mapping list.

    - To map one Field at a time, select **Add**.

      The **Map Field from External Table** window opens, listing the available Table/View fields.

        - Select the **external field** to map to.
        - Select **Create new field** and type a name for the new field.

        - Select **OK**.

15. Select **Next**.

    The **Unique Key and Timestamp Fields** page opens.

16. Designate a Unique Key and Timestamp Field:
    a. Field that Holds Unique Key: Select the Field from the View that is considered the unique identifier (example: MachineID or ComputerID).

    b. Last Modified Date/Time: Select the Field from the Table/View that is considered the last modified date/time Field (example: LastScanDate or date_modified).

17. Select **Next**.

    The **Read-Only or Updatable** page opens.

18. Select the **Data is read-only** or **Allow data to be updated** option.

19. Select **Next**.

    The **Name and Description** page opens.

20. Provide the Name and Description for the Business Object.

21. Select **Next**.

    The **Summary** page opens. The information varies depending on selections throughout the wizard.

22. Select **Finish**.

The **Business Object's Properties** window opens, showing current (and editable) properties, including a new external data page where the Field mappings, unique ID, and last modified date/time Fields can be viewed/edited.

23. Select **OK** to close the **Properties** window.

24. Create Forms and Grids for the External Business Object just as for a new CSM Business Object.

25. (Optional for Supporting Objects) If needed, create a Relationship between the newly created Supporting Objects and the Major Object they support.

26. Publish the Blueprint (File>Publish Blueprint) to commit the changes, or save the Blueprint (File>Save Blueprint) to continue making other changes.

Import External Data into an Existing Business Object

Use the External Data Import Wizard to import data from an external database into an external Business Object. External data can only be imported into External Business Objects, which is a Business Object that has already been mapped to an external connection..

To import external data into an existing external Business Object:

1. In the CSM Administrator window, click the **Database** category.

2. Click the **Import External Data** task. The External Data Import Wizard opens.

3. Select **Next**.

   The Select Business Object page opens. Only Business Objects that have already been mapped to an external connection appear.

4. Select a **Business Object**.

5. Select **Next**.

   The Existing Records page opens.

6. Select whether to delete or update existing records within CSM:
   - Delete All Existing Data: Select this radio button to delete all the records from the Table/View before importing new data.

     Warning: If records were linked to CSM records and then deleted in the External Database, those links will no longer work. Deleting records from CSM before re-importing them might break some, or all, of the existing Relationships to that record.

   - Update Existing Records: Select this radio button to import new data and refreshes any existing records with changed data. Existing records are updated based on the chosen Unique Key field.

7. (Optional) Select the **Only import records changed since** check box to shorten the import time based on a selected date. Click the **Date Selector** button to select a date.

8. Select **Next**.

   The Choose Filter page opens.

9. Select data to import:
   - **All records:** Select this radio button to import all external data.

   - **Use filter:** Select this radio button to filter the imported data based on a defined query. When the User Filter radio button is selected, the Saved Search option enables. Click the **Ellipses** button to open the Search Manager, and then select an existing Saved Search (saved Search Query) or create a Saved Search. Saved Searches can be used over and over in numerous places.

> **Note:** Typically, data in a View is already filtered.

10. Select **Finish**.

    The data is imported and then shows in the CMDB (CSM>Tools>CMDB). If the CSM Scheduler is used, the import starts at the scheduled time.

Share Data with an External Database

Consider creating Views in your external database to connect to your CSM database.

To share data with an external database:

1. (Optional) If connecting to a normalized database, create Views of the data that connect to each other.

    Note: For more information about creating and testing Views of the external database, consult a DBA.

2. In CSM Administrator, create an external connection to an external database.
3. Designate a CSM Business Object to accept the external data. There are three options:
    ◦ Map an existing CSM Business Object to external data, and then import the external data. (No link option is available for existing CSM Business Objects.)
    ◦ Create an External Business Object to import the external data, and then import the external data.
    ◦ Create an External Business Object to link to the external data.

Import Data From .csv Files

If you do not need to import real-time record or user data into your CSM system, you can import Business Object or user data from .csv (comma delimited) files as needed or create a Stored Import Definition that can be used repeatedly.

For example, you can create an Excel spreadsheet to import user data. Add a column for each field you want to import data to. A spreadsheet that has columns named Title, First Name, Last Name, Email address, Company and Job Title can be mapped for similar fields in CSM.

	A	B	C	D	E	
1	Title	First Name	Last Name	Email address	Company	Job Title
2	Mr	Mark	Jones	mark_jones@r	Rada Inc.	VP, Director, Process Excellence
3	Ms	Leann	Johnson	ljohnson@wav	The Waving	Information Technology Manager

When you save the spreadsheet as a .csv file, the data is saved as:

- Mr,Mark,Jones,mark_jones@rada.com,"Rada Inc.","VP, Director, Process Excellence"

- Ms,Leann,Johnson,ljohnson@wavings.edu,The Wavings Institute,Information Technology

.CSV Reference

- The .csv file must have a column name specified in the first row.

- Data that contains commas or quotes should have double-quotes around the value. A double quote is included by being doubled. For example: "The ""very"" important data" imports very with one set of double quotes.

- To include carriage returns, place the text \R\N into the string. To actually include the text "\R," double the slash: \\R. Most of these things are automatically done by programs that support exporting in a .csv format.

- Each row can have its values imported into a Business Object and/or related Business Objects. For example, if each row of the .csv file contains an Incident and its Customer, Journal, and Specifics data, then the import can create an Incident Record and use its Relationships to create associated Customer, Journal, and Specifics Records. Be aware that each row can create only one instance of a record for each Relationship. For example, it cannot create two Journals from the same data row unless using two different Relationships.

Related concepts
Stored Import Definition Manager
Related tasks
Import Business Object Data with .csv Files
Importing Users with .csv Files

Import Business Object Data with .csv Files

You can import Business Object record data from a .csv (comma delimited) file. You can do this one time or create a Stored Import Definition that can be used repeatedly.

Related concepts
Import Data From .csv Files
Stored Import Definition Manager
Related tasks
Importing Users with .csv Files

Run a One-time Import of Business Object Data

Use a one-off import to quickly add Business Object data to your system. For example, to import data from a legacy Service Management tool, you can export that data to a .csv file, and then run a one-time import.

To run a one-off data import:

1. In the CSM Administrator, select the **Database** category.
2. Select the **Stored Import Definition Manager (CSV files)** task.
3. Select **New** to open the **Import Data Wizard**, and then select **Next**.
4. From the **Primary Business Object** drop-down list, select Business Object to import the .csv file data into.
5. Optionally, select a timeout to specify the number of seconds the system should wait before the import operation times out. This option is only available for 3-tier database connections.
6. Select **Next**.
7. Select a **Column in File** (example: Description) to map it to a Business Object Field, and then select an action:

Option	Description
Do not import this column	Select this option to prevent data from this column from being imported
Import into field	Select this option, and then select a Business Object field to import the column data into.

    Repeat these steps for all columns.
8. Select **Next**.
9. Optionally, select**Add** to add more data to Business Object fields, and then select a field from the **Field to Populate** list.

Option	Description
Expression	Select this option, and then select the Expression.
Concatenate Columns from File	Select this option, and select **Add** to choose a column from the file to concatenate data in the columns based on the specified separator characters.
Separator characters	Choose the character to separate column data during the import process.

10. Select **Next**.
11. Define options to take when duplicate data is detected.

Option	Description
Duplicate Records in Import File	Select the **Ignore Duplicate Entries** checkbox to ignore duplicate entries in the .csv file. Select **Add** to select which columns to ignore when duplicate entries are found.
Records in Database that Match Import File	Select one of these options: ◦ Select the **Import all records - No duplicate check** radio button to import all data from the .csv file, even if data matches existing records in the database. ◦ Select the **Ignore/skip duplicate records** radio button to skip records that exist in the .csv file and the database. ◦ Select the **Update duplicate records** radio button to update the database with information from the .csv file. **Important:** Selecting the **Ignore/ skip duplicate records** radio button or the **Update duplicate records** radio buttons requires column names to be specified (Add>Select column names for the Import Data Wizard to ignore or update)

12. Select **Next**.

13. Optionally, use the **Delete Existing Data** page to define these options:

Option	Description
Delete existing data from the business object before import	Select this check box to replace current data with new data from the .csv file.
Do not delete data if import file is empty	Select this checkbox to prevent Business Object data from being deleted but not repopulated. (example: the .csv file has blank columns, so the original Business Object data is still needed).

14. Select **Next**.

15. Optionally, select the **Test Import** button. After the test runs, warnings appear for any duplicate entries.

16. Select **Import**.

Related concepts

Import Data From .csv Files

Related tasks

Run Repeated Imports of Business Object Data

Importing Users with .csv Files

Run Repeated Imports of Business Object Data

Use the Stored Import Definition Manager to create a stored and named .csv import definition so that a specific .csv file can be imported more than once. When a Stored Import is created, you are prompted to complete the Import Data Wizard, and then name and save the import definition.

To run a stored import:

1. In the CSM Administrator window, select the **Database** category, and then select the **Stored Import Definition Manager (CSV Files)** task.
   The Stored Import Definition Manager opens, listing existing Stored Imports.

2. Select **Create New**.
   The **Import Data Wizard** opens.

3. Follow the steps to run a One-Off Data Import.

4. Provide a name for the Stored Import when prompted.

5. Choose one of these options to use the Stored Import Definition:
   - Select **Run** in the Stored Import Definition Manager window to run the import.
   - Schedule an import using the Scheduler. For more information, see Define Import from File Action Options.

Related concepts

Import Data From .csv Files

Stored Import Definition Manager

Related tasks

Run a One-time Import of Business Object Data

Importing Users with .csv Files

Importing Users with .csv Files

You can import user data from a .csv (comma delimited) file. You can choose to include LDAP authentication data in your .csv file. For best results, create a Stored Import Definition that can be used repeatedly.

To import users with internal authentication settings:

1. In the CSM Administrator, select the **Database** category.
2. Select the **Stored Import Definition Manager (CSV files)** task.
3. Select **New** to open the **Import Data Wizard**, and then select **Next**.
4. Navigate to a .csv file that contains user data.
5. from the **Primary Business Object** drop-down list, select the Business Object that stores internal user information. In most cases, this is the UserInfo Business Object.
6. Optionally, select a timeout to specify the number of seconds the system should wait before the import operation times out. This option is only available for 3-tier database connections.
7. Select **Next**.
8. On the **Set Special User Authentication Column** page of the **Import Data Wizard**, select the **Column** button for each column shown, and then select the matching data column in the .csv file.

   > **Note:** At least one Login ID column and the Rec ID, Security Group, Default Security Group, and Default Team fields are required.

9. Optionally, select the **Include LDAP Authentication** checkbox if your .csv file contains LDAP user information and LDAP is configured for your system.
10. Select **Next**.
11. If you are importing LDAP user information, you must add LDAP information to the import.

Option	Description
Users Name Starts With	Select the Column button, and then choose the .csv column that matches the start of each user name.
LDAP Directory Service	Select the LDAP connection to use for the data import.
LDAP Key Field	Select a field from the User Business object to serve as the LDAP key.
Default Domain	Provide you LDAP domain name or IP address.
Use Default Domain	Select this option to use the specified LDAP domain if another is not detected from the .csv file.

Option	Description
Always Use Default Domain	Select this option to use the specified LDAP default domain.

12. Select **Next**.
13. Select a **Column in File** (example:Email) to map it to a User field, and then select an action:

Option	Description
Do not import this column	Select this option to prevent data from this column from being imported
Import into field	Select this option, and then select a Business Object field to import the column data into.

Repeat these steps for all columns.

14. Optionally, select**Add** to add more data to Business Object fields, and then select a field from the **Field to Populate** list.

Option	Description
Expression	Select this option, and then select the Expression.
Concatenate Columns from File	Select this option, and select **Add** to choose a column from the file to concatenate data in the columns based on the specified separator characters.
Separator characters	Choose the character to separate column data during the import process.

15. Select **Next**.
16. Define options to take when duplicate data is detected.

Option	Description
Duplicate Records in Import File	Select the **Ignore Duplicate Entries** checkbox to ignore duplicate entries in the .csv file. Select **Add** to select which columns to ignore when duplicate entries are found.

Option	Description
Records in Database that Match Import File	Select one of these options: ◦ Select the **Import all records - No duplicate check** radio button to import all data from the .csv file, even if data matches existing records in the database. ◦ Select the **Ignore/skip duplicate records** radio button to skip records that exist in the .csv file and the database. ◦ Select the **Update duplicate records** radio button to update the database with information from the .csv file. **Important:** Selecting the **Ignore/skip duplicate records** radio button or the **Update duplicate records** radio buttons requires column names to be specified (Add>Select column names for the Import Data Wizard to ignore or update)

17. Choose one of these options to use the Stored Import Definition:
    ◦ Select **Run** in the Stored Import Definition Manager window to run the import.
    ◦ Schedule an import using the Scheduler. For more information, see Define Import from File Action Options.

18. Optionally, select the **Test Import** button. After the test runs, warnings appear for any duplicate entries.

Related concepts

Import Data From .csv Files

Stored Import Definition Manager

Related tasks

Import Business Object Data with .csv Files

Troubleshooting Data and Databases

General Troubleshooting

- For any problems or issues in importing, linking, or connecting to databases through CSM, contact a database administrator or Cherwell Support.

- When updating to a new software version, choose to update the existing database to the most recent database version. Updating a CSM database installs any new and required internal system definitions.

- Import data should be maintained in CSM and linked to transient or reference data that can be maintained outside CSM. There are pros and cons of both imported and linked data.

- Only users with correct permissions can use the database tools. If a user cannot see database tools, verify that the user has administrator security rights.

- When Cherwell Services use a Windows Authentication connection, the account under which the Cherwell Application Service is running is the account whose credentials are used to connect to the database. The account must have select rights for each table that is importing or linking to CSM. If intending to allow CSM to update data in the database, then this account must also have insert and update rights.

OLE Database Connection Troubleshooting

Drivers should be available from a database vendor. Consult a database provider for assistance locating this driver. There are also OLE database drivers from third-party vendors that can be used. Although ODBC Drivers is an option in this list, it is not compatible with the .NET OLE database mechanism, which is used by CSM for communication with external data sources.

SQL Database Connection Troubleshooting

If connecting to a named instance of a SQL (a non-default instance of SQL), then provide the instance in the Specific Server value using the format: DatabaseServer\InstanceName.

External Business Object and External Data Connection Troubleshooting

- External data can only be imported into External Business Objects, ensure your selected Business Object is an External Business Object.

- A combination of imported and linked data can be used, but not within the same Business Object. The option to Link Data is disabled when applicable: if data has already been imported into the Business Object or an External Connection is being created.

- The Link to Data option is available only when creating a new Business Object; connecting to an existing Business Object must be performed with an import.

- Use an existing Business Object to share external data. To use an existing Business Object, map an Existing CSM External Business Object to Import External Data, and then import the external data (linking from an existing Business Object is not allowed).

- SQL Server: In order to use SQL Full-Text Search, it must be configured in the external database. Refer to SQL Server documentation for details on how to set up Full-Text Search.

- If External data is not importing at the selected time (example: when the selected Unique Key field was Last Modified) ensure SQL indexes have been assigned to the selected fields. Assign SQL indexes in CSM Administrator and the Business Object Editor (**Business Object Editor > Business Object Properites > Databases > Add Index button > Select Last Modified Date/ Time values**).

- Some advanced data types may not import into CSM and are not supported (example: Int data types).

CSV Data Troubleshooting

- Commas are the only accepted separators.

- CSV data can only be imported, it cannot link to CSV data.

- Before importing CSV data, prepare the data so the column names are specified in the first row.

- Save an Excel Spreadsheet as a .csv file by selecting **File>Save As** and choosing the .csv file format from the **Save As Type** box.

Email Configuration

CSM supports sending and receiving email in several different formats (POP3/SMTP, IMAP/SMTP, and Microsoft® Exchange).

A variety of tools are provided to help you configure and manage email.

Configuring Email Accounts

You can perform procedures for configuring email accounts in CSM Administrator and the CSM Desktop Client.

Complete the following procedures to configure email accounts.

To configure email accounts:

1. Configure e-mail security rights.

2. Configure global e-mail accounts: Global email accounts are configured in CSM Administrator. If a user has security rights, they define personal e-mail settings in the CSM Desktop Client to customize the account and use it to send emails. Make the account unavailable to users and set it up solely as a monitored account (using the Email and Event Monitor).

3. Define default email history attachment options: Define which records to have emails attached to (as Journal - Mail History Records). The email history attachment options selected here are set as defaults, but users can override them using the email history attachment options in the Email Message window in the Desktop Client.

   > **Note:** The Business Objects might also need to be configured to receive email history (see Define Default Email History Attachment Options) or to allow users to email customers from a Business Object Record. For emails to be sent to the current customer on a particular Business Object (example: Incident), the Business Object must have a Customer Relationship (example: Incident links Customer) with the CustomerInfo general attribute. This relationship exists on most Major Business Objects in the system, but should be added to any new objects created. If a user tries to send an email to a customer, and CSM cannot find a relationship with this attribute, it returns a *Customer e-mail address was not found* error message. For more information about relationships, see the Relationships documentation.

4. Configure personal email accounts in the Desktop Client: Customize a global email account or configure a personal account for special circumstances such as sending email from home or an off-site location.

Configure a Global Email Account

When configuring an email account, you can add or delete an account, edit or copy an existing account, designate a default account for sending emails from within CSM, and find dependencies.

Use the **Accounts** page in the **E-mail Options** window to set up global email accounts.

To configure a global email account:

1. In the CSM Administrator main window, select the **E-mail and Event Monitoring** category, and then select **E-mail Accounts and Settings**.
2. Select the **Accounts** page on the **E-mail Options** window.
3. Configure an email account:
   a. Select **Add** to select the type of email account to set up (POP, IMAP, or Exchange).
   b. Select **Edit** to edit the settings for an existing account.
   c. Select **Delete** to delete an existing account.

   > **Note:** Users might have security rights to customize global email account settings, so there are several options when deleting an email account. See Delete a Global Email Account for more information.

   d. Select **Copy** to copy the settings from an existing account, then edit the settings as necessary.
4. Configure the account:
   a. Define Global POP or IMAP Account Settings
   b. Define Global Microsoft Exchange Account Settings
5. Select **Spell Check E-mail** to have CSM spell check emails as a message is typed (misspelled words are underlined with red lines).
6. Select **Make Default Account** to make the selected account the default account for sending emails. This account is used for emails sent from the Browser Client.
7. Select **Find Dependencies** to show other CSM Items using the selected email account (example: An Email and Event Monitor).

Define Global POP or IMAP Account Settings

You can configure a POP or IMAP account to send and receive email through CSM. As a prerequisite, gather the required information before starting the configuration process.

Setting up a POP or IMAP account requires:

- A name for the email account.
- Incoming (POP or IMAP) and outgoing (SMTP) email server information, including the:
  - Location of the mail server.
  - Security protocol.
  - Account credentials.
- Options for adding Conversation IDs to outgoing messages.

  A Conversation ID is a unique, alphanumeric identifier that correlates an email message with a particular conversation so that it can be associated with a CSM Record. CSM inserts Conversation IDs into emails to identify if a particular email is a reply to a previous message that was associated with a specific Business Object record.

  A Conversation ID looks similar to the following: {CMI: ABCD1234}, where ABCD is an identifier for the particular CSM system (set this value in the History Attachment Options for a global email account), and the numeric indicator is the specific Conversation ID. The number is automatically incremented for each message.

- From Addresses that are allowed for sending emails from CSM.

  Note: The padlock button in each of the sections determines if users can override administrative settings when they personalize a global email account by defining their own personal email settings. By default, server settings are locked and credentials are unlocked so that Users can enter their own user names and passwords. Select the **padlock** buttons to change the defaults.

To set up a POP or IMAP account:

Note: The options for a POP or IMAP account are the same. The ports are different and are listed in step 6c.

1. In the CSM Administrator main window, select the **E-mail and Event Monitoring** category, and then select the **Edit E-mail Accounts and Settings** task.
2. Select the **Accounts** page on the **E-mail Options** window opens.
3. Select **Add**, and then select **POP account** or **IMAP account**.

Tip: Users can also edit or copy an existing account. Select **Edit** to modify the settings for an existing email account. Select **Copy** to copy the settings for an existing email account, then modify them as necessary.

4. The **Incoming Server** page should be open as the default.

5. Define general incoming server (POP or IMAP) settings:
   a. Name: Provide a name for the account.

   Tip: When defining a test account, use names such as MyDevAccount or DevTestAccount. This naming convention allows users to quickly identify test accounts in the system.

   b. **Make Account Available to Users**: Select this check box to allow users to send emails from within CSM using this account. If the account is only used by the E-mail and Event Monitor to scan incoming emails, leave the check box cleared so that users never see the account.
   c. To use Google Authentication for G Suite accounts, select the **Use Credentials-Based Authentication** check box.

   Note: You can use credentials-based authentication on the incoming server, the outgoing server, or both.

6. Define incoming mail server (POP or IMAP) information:
   a. **Incoming Mail Server**: Provide the name of the POP or IMAP server.
   b. **Security**: Select a security protocol in the drop-down list:
      ◦ **Auto**: Select this option to have CSM select the best method to use. It selects the most secure method available in order to prevent transmission of unencrypted User IDs and passwords, if possible.
      ◦ **Basic**: Select this option to have User IDs and passwords passed as plain text.
      ◦ **SSL**: Select this option to use SSL encryption (a Server Certificate is required).
      ◦ **SSL with No Authentication (IMAP only)**: Select this option to use SSL encryption only (no Server Certificate is required).
      ◦ **TLS (IMAP only)**: Select this option to use the TLS protocol.

      Note: The mail server must support the selected security mode.

   c. **Custom Port**: Select this check box to enter a port for the POP or IMAP server that is different than the default.

      Note: For POP servers, the default port is 110 (the SSL port is 995). For IMAP servers, the default port is 143 (the SSL port is 993).

7. Enter account information:
   a. **User Name**: Provide the user name for the email account.

b. **Password**: Provide the password for the email account. This field is deactivated if you use credentials-based authentication.

> **Note:** Leave the user name and password blank to allow Users to provide their own credentials. Also, ensure the padlock button is unlocked 🔓. If it is locked, click it and select **Users Can Change Credentials**. If all Users will use the same credentials, or if this account will be used by an automated process like the E-mail and Event Monitor, provide credentials here.

c. **Credentials**: Select the Google credential you want to use. You can also configure a new set of credentials in the E-mail Credentials Manager.

d. **Mailbox (IMAP only)**: Select the mailbox (example: Inbox) from the drop-down list where the incoming mail should be stored.

8. Select the **Outgoing Server** page.

9. Define outgoing mail server (SMTP) information:
   a. **Outgoing Mail Server (SMTP)**: Provide the name of the SMTP server.

   b. **Security**: Select a security protocol in the drop-down list:
      ◦ **Auto**: Select this option to have CSM select the best method to use. It selects the most secure method available in order to prevent transmission of unencrypted User IDs and passwords, if possible.

      ◦ **Basic**: Select this option to have User IDs and passwords passed as plain text.

      ◦ **SSL**: Select this option to use SSL encryption (a Server Certificate is required).

      ◦ **TLS**: Select this option to use the TLS protocol.

      > **Note:** The mail server must support the selected security mode.

   c. **Custom Port**: Select this check box to enter a port for the SMTP server that is different than the default (default port is 25, SSL port is 465).

10. Specify account information:
    a. **Requires Authentication**: Select this check box if the SMTP server requires authentication and select one of the following options:
       ◦ **Use Same Settings as My Incoming Server**: Select this radio button if the user name and password for the SMTP server are the same as the incoming server. If you use credentials for the incoming server

       ◦ **Log on Using**: Select this radio button to specify a user name and password that is different from the incoming server settings and provide the user name and password. If you want to use credentials, choose a certificate or private key.

       > **Note:** To allow Users to enter their own credentials, leave the user name and password blank and ensure that the padlock button is unlocked 🔓. If it is locked, click it and select **Users Can Change Credentials**.

11. Define conversation ID options:

a. **Add Conversation IDs to Outgoing Messages**: Select this check box to include Conversation IDs in outgoing emails.

> **Note:** When a Conversation ID is found within an email message, CSM can immediately find the record (example: Incident) associated with the various emails. If Conversation IDs are not used, then it can still identify records, but it has to use less reliable techniques, such as comparing the details of the subject line.

b. Specify where in the email to include the Conversation ID, either:
   ◦ **Add to Subject Line**: Select this radio button to include the Conversation ID in the subject line of outgoing emails.
   ◦ **Add to Body**: Select this radio button to include the Conversation ID in the body of outgoing emails.

   > **Note:** Do not delete Conversation IDs from email messages. Doing so makes it harder for CSM to associate customer replies with the correct record.

12. Select the **Test Account** button to ensure that emails can be sent from within CSM using this account.

    A test email is sent to the current user.

    > **Note:** All required Incoming and Outgoing Server information must be completed before testing the account.

13. **Optional**: Select the **From Settings** page and specify the addresses and settings associated with outbound emails.

14. **Optional**: Select the **Trusted Agents** page and define how Trusted Agents should be used with this account.

Related concepts
Default Port Numbers
Related tasks
Configure Email Credentials for Google

Define Global Microsoft Exchange Account Settings

You can configure a Microsoft Exchange account to send and receive email through CSM. As a prerequisite, gather the required information before starting the configuration process.

Setting up a Microsoft Exchange account requires:

- A name for the email account.
- Exchange Server information.
- Account credentials.
- Options for adding Conversation IDs to outgoing messages.

  A Conversation ID is a unique, alphanumeric identifier that correlates an email message with a particular conversation so that it can be associated with a CSM Record. CSM inserts Conversation IDs into emails to identify if a particular email is a reply to a previous message that was associated with a specific Business Object record. A Conversation ID looks similar to the following: {CMI: ABCD1234}, where ABCD is an identifier for the particular CSM system (set this value in the History Attachment Options for a global email account), and the numeric indicator is the specific Conversation ID. The number is automatically incremented for each message.

- From Addresses that are allowed for sending emails from CSM.

  Note: The padlock button in each of the sections determines if users can override administrative settings when they customize a global email account by defining their own personal email settings. By default, server settings are locked and credentials are unlocked so that users can enter their own usernames and passwords. Select the padlock buttons to change the defaults.

To configure a global Microsoft Exchange account:

1. In the CSM Administrator main window, select the **E-mail and Event Monitoring** category, and then select the **E-mail Accounts and Settings** task.

   The **E-mail Options** dialog opens.

2. Select the **Accounts** page.
3. Select **Add**.
4. Select **Exchange**.

   Tip: Users can also edit or copy an existing account. Select **Edit** to modify the settings for an existing email account. Select **Copy** to copy the settings for an existing email account, and then modify them as necessary.

   The **E-mail Options** dialog for an Exchange account opens.

5. Select the **Exchange Settings** page.

6. Define general account information:
    a. **Name**: Provide a name for the Exchange account.

    b. **Make Account Available to Users**: Select this check box to allow users to send emails from CSM using this account. If the account is only used by the Email and Event Monitor to scan incoming emails, leave the check box cleared so users never see the account.

7. Select an authentication type. CSM supports Basic Authentication, credentials-based (Modern Auth), and Microsoft Graph.

    Note: Microsoft will begin disabling basic authentication in October 2022. Microsoft is also no longer providing feature updates to Exchange Web Services (EWS), which is used for Credential-based authentication. We recommend customers use Microsoft Graph for CSM authentication.

8. Define Exchange server information. The fields available depend on the authentication type you choose:
    ◦ **Basic**:
        ◦ **Exchange Domain**: Provide the name of the Exchange Domain.

        ◦ **Server (Client Access)**: Provide the name of the Exchange Client Access server. Client Access is the web service used by CSM to connect with Exchange.

        ◦ **Use SSL Connection**: Select this check box to use SSL encryption for sending and receiving emails.

        ◦ **Allow Invalid Server Certificate**: Select this check box to allow emails to be sent and received even when the digital certificate is invalid.

            Warning: This option is not recommended, as it can pose a security risk to the Exchange email system.

        ◦ Enter Account Information:

            Note: This must be a full Microsoft Exchange user account (it must be licensed). Non-user accounts, such as shared mailboxes or resource mailboxes are not supported.

            ◦ **User**: Provide the email address for the Exchange account. If you are using Office 365 Modern Authentication credentials, this address can be one of the user email addresses set up in Azure, or it can be the Azure administrative address.

            ◦ **Password**: Provide the password for the Exchange account. This field is disabled if you use credentials-based authentication.

                Note: Leave the user name and password blank to allow users to enter their own credentials. Also, ensure that the padlock button is unlocked. If it is locked, select the image and select **Users Can Change Credentials**. If all users use the same credentials, or if this account is used by an

automated process like the Email and Event Monitor, provide credentials here.

- ◦ **Credential-Based (Modern Auth)**:
  - ◦ **User**: Provide the email address for the Exchange account. If you are using Office 365 Modern Authentication credentials, this address can be one of the user email addresses set up in Azure, or it can be the Azure administrative address.
  - ◦ **Credentials**: Select the ellipsis to access the **E-mail Credentials Manager**, and then select the Office 365 credentials you wish to use. You may also configure a new set of credentials in the **E-mail Credentials Manager**.
- ◦ **Microsoft Graph** (see Configure an Azure App Using Microsoft API for information on registering an app using Microsoft Graph):
  - ◦ **Client ID** and **Tenant ID**: Copy these IDs from the Azure portal.
  - ◦ **User**: Provide the email address for the Exchange account.
  - ◦ **Password**: Provide the password for the Exchange account.

9. Define Conversation ID options:
   a. **Add Cherwell conversation IDs to outgoing messages**: Select this check box to include Conversation IDs in outgoing emails. Implementing Conversation IDs increases reliability when attempting to locate emails discussing specific Records.

   b. Specify where in the email to include the Conversation ID, either:
      - ◦ **Add to Subject Line**: Select this radio button to include the Conversation ID in the subject line of outgoing emails.
      - ◦ **Add to Body**: Select this radio button to include Conversation ID in the body of outgoing emails.

10. Select the **Test Account** button to ensure emails can be sent from within CSM using this account.

    A test email is sent to the current user. All required Exchange server information must be filled in before the account to be tested. Testing the account only confirms that the account was successfully linked to CSM. It does not confirm that the account is compatible with the email monitor.

11. Select the **From Settings** page and specify the addresses and settings associated with outbound emails.

12. Select the **Trusted Agents** page and define how Trusted Agents should be used with this account.

Related tasks
Configure Email Credentials for Office 365 Accounts

Configure an Azure App Using Microsoft API

Configure an App in Azure Active Directory, then link the App to CSM.

For more information on Microsoft Graph API use in Azure Active Directory, see https://docs.microsoft.com/en-us/azure/active-directory-b2c/microsoft-graph-get-started?tabs=app-reg-ga.

To set up an Azure App for use with Microsoft Graph authentication:

1. Go to Azure Active Directory on the Azure Portal. You must be an administrator in the Azure account.
2. Add a new App registration.
   a. In the **Supported account types** section, select **Accounts in this organizational directory only**.
   b. Create the registration.
3. In the newly registered App, edit the authentication options.
   a. Select **Add a platform > Mobile and desktop application**.
   b. In the Redirect URLs section, select **https://login.microsoftonline.com/common/oauth2/nativeclient**, then select the **Copy to clipboard** icon.
   c. In the **Advanced settings** section, enable public client flows.
4. Edit the API permissions options.
   a. Select **Add a permission**, then select **Microsoft Graph**.
   b. Select **Delegated permissions**.
   c. Enter `mail` in the search function under **Select permissions**. When the search results appear, choose **Mail**.
   d. Expand the Mail options and select **Mail.Read**, **Mail.ReadWrite**, and **Mail.Send**.
   e. Select **Enterprise applications** at the bottom of the **Configured permissions** section.
   f. Select **Users and groups** from the left menu.
   g. Select **Add user/group**, then add the Cherwell admin user account.
   h. Grant admin consent to the Cherwell admin user.
5. Note the Application (client) ID and Directory (tenant) ID of the App you created. Find those IDs in the **Overview** page of the App under **Essentials**. You will use those when you set up MS Graph authentication in CSM Administrator.

Define Default From Settings for a Global Email Account

A system administrator might want to control which email addresses can be used to send email from within CSM. Use the **From Settings** page to define allowed From addresses for a configured email account.

To define from settings:

1. In the CSM Administrator main window, select **E-mail and Event Monitoring > E-mail Accounts and Settings**.

   The **E-mail Options** window opens.

2. Select the **Accounts** page.

3. Select a configured email account, and select **Edit**.

   The **E-mail Options** window for the account opens.

4. Select the **From Settings** page.

5. Define general account information:
   a. **Name**: Provide a name for the account.

   b. **Make Account Available to Users**: Select this check box to allow users to send emails from CSM using this account. If the account is only used by the Email and Event Monitor Service to scan incoming emails, leave the check box cleared so that users never see the account.

6. Define which From addresses are allowed (select any or all of the following options):
   ◦ **Allow User's E-mail Address**: Select this check box to allow the user's email address as a From address.

   ◦ **Allow Arbitrary FROM addresses**: Select this check box to allow any valid email address as a From address. We do not recommend this option since it can be used for spam and to impersonate other users, and because most mail servers reject emails with unexpected From addresses.

7. Provide a list of legal From addresses (example: servicedesk@mycompany.com, sales@mycompany.com, support@mycompany.com).

   Note: The email server needs to be configured to allow these From addresses from the account.

   ◦ **Add**: Select to add a new email address as a Legal From address.

   ◦ **Edit**: Select to edit an existing From address.

   ◦ **Remove**: Select to remove an email address from the list.

Tip: If all emails sent from a global email account in CSM should have the same From address, add that address to the list of Legal From addresses and clear the **Allow User's E-mail Address** and **Allow Arbitrary FROM addresses** check boxes.

- If there is a list of Legal From addresses, select one as the default From address (select the **Make Default Address** button) that is automatically used for all emails sent from the account.

8. Select where to send emails from, either:
   - **Client**: Select this radio button to have emails sent from the user's client machine. Emails sent from the CSM Browser Client or CSM Portal using this setting still utilize the Cherwell Message Queue Service.

   - **Server**: Select this radio button to have emails sent from the server. Sending email from a server puts an additional load on the server and should be used if only the server has access to the mail server for security reasons, or if there are CSM users outside of the corporate firewall/network. If only a few users need to send email from the server, create a separate account for those users.

     Note: If you use Trusted Agents with the email account, the email source will automatically be set to **Server**.

Delete a Global Email Account

You can remove a global email account that is no longer needed. When deleting an account, keep in mind that this might be an active account with defined personal email settings for some users.

To delete a global email account:

1. In CSM Administrator, select **E-mail and Event Monitoring > Edit E-mail Accounts and Settings**. The **E-mail Options** window opens.
2. Select the **Accounts** page.
3. Select the email account to delete.
4. Select the **Delete** button.
   The **Update or Delete Dependent Accounts** window opens.
5. Select whether to preserve or delete user customizations on the account:
   - **Keep User Accounts**: Select this radio button to have the global settings copied into each user account based on this account, so it continues to function as before. Users are able to edit any portion of the account (even the items that were locked previously).
   - **Delete Any User Customizations for the Account**: Select this radio button to delete the global account and all user customizations at the same time. Users are no longer able to use the account to send email from within CSM.
6. Select **OK**, and then select **OK** again.

Related concepts
Configure User Email Settings

Define Default Email History Attachment Options

Using Journal - Mail History Records, you can define default settings for attaching email history to records.

Note: For emails to be attached to a Business Object as a Journal - Mail History Record, the Business Object must have a History Relationship. For emails to be attached to the customer associated with a particular Business Object (example: Incident), the Business Object must have a Customer Relationship (example: Incident links Customer) with the CustomerInfo general attribute. This Relationship exists on most Major Business Objects in the default system, but should be added to any new objects created. For more information about Relationships, see the Relationships documentation.

Use the **History** page in the **E-mail Options** window to define email history options, such as:

- What types of records emails should be attached to, either:
    - The current Business Object.
    - Customers identified from the email or Business Object.

        Note: The email history attachment options selected here are set as defaults, but users can override them using the email history attachment options in the E-mail Message window.

- A Conversation ID prefix that is used when Conversation IDs are embedded in emails. The option to embed Conversation IDs into outgoing messages is available in the account settings for the POP, IMAP, or Microsoft Exchange account.

    A Conversation ID is a unique, alphanumeric identifier that correlates an email message with a particular conversation so that it can be associated with a CSM Record. CSM inserts Conversation IDs into emails to identify if a particular email is a reply to a previous message that was associated with a specific Business Object record. A Conversation ID looks similar to the following: {CMI: ABCD1234}, where ABCD is an identifier for the particular CSM system (set this value in the History Attachment Options for a global email account), and the numeric indicator is the specific Conversation ID. The number is automatically incremented for each message.

To define default email history attachment options:

1. In the CSM Administrator main window, select the **E-mail and Event Monitoring** category, and then select the **E-mail Accounts and Settings** task.

    The **E-mail Options** window opens.

2. Select the **History** page.

3. Define Default E-mail History Attachment Options: Specify which records get a Journal - Mail History Record when an email is sent.

◦ Current Record: Select this check box to attach emails to the Business Object record the user currently has in focus or has selected in a list of records (example: An Incident Record in a search results list).

◦ Current Record's Customer: Select this check box to attach emails to the customer associated with the current record.

◦ Recipients in To Line: Select this check box to attach emails to the records of customers that CSM can identify from email addresses in the To line.

◦ Recipients in Cc Line: Select this check box to attach emails to the records of customers that CSM can identify from email addresses in the Cc line.

◦ Recipients in Bcc Line: Select this check box to attach emails to the records of customers that CSM can identify from email addresses in the Bcc line.

Note: This option only applies to outgoing email.

◦ Parents of recipients (example: Organization that contact works for): Select this check box to attach emails to the parent records of recipients. For example, if an email recipient is a contact that works for a particular organization, the email can be attached to the Company Record as well as the Customer Record.

4. Define remaining email history attachment options:
   a. Import file attachments automatically when sending email: Select this check box if file attachments sent out in emails should, by default, be imported and attached as part of history. This will also import attachments from all system-generated emails (triggered by One-Step™ Actions, Automation Processes, etc.)

   b. Message Conversation ID Prefix: Provide a prefix for Conversation IDs that are embedded in the subject or body of emails sent from within CSM.

   Note: The prefix should be unique for the system or organization and should be between two and eight characters. If a value is not specified, a random value is created, but can be updated at any time to something relevant to the organization. In the message, the Conversation ID looks similar to the following: {CMI: ABCD1234}, where ABCD is the specified prefix, and the numeric indicator is the specific Conversation ID. The prefix is especially important for sending emails among multiple companies that use CSM (example: If contacting Cherwell Support).

   Tip: Select the **Information** button to view this same information.

5. Select **OK**.

Managing Email Credentials

Use the E-mail Credentials Manager to hold authentication credentials.

Set up Email Credentials in CSM Administrator. When working in the Desktop Client, you can select which credentials to use with an email account, but you can't set up new credentials or edit existing ones.

CSM currently supports Modern Authentication for Microsoft Office 365 accounts and Google Authentication (OAuth 2.0) for G Suite IMAP and POP accounts.

Configure Email Credentials

Set up email credentials using the Email Credentials Manager in CSM Administrator.

Note: You can only configure email credentials if you have the **Can administer email credentials** security permission.

CSM uses server-side authentication to manage email primarily through the Automation Process service and the Email and Event Monitor. Office 365 and G Suite do not offer account restrictions for this flow, but CSM keeps credential-based email accounts secure through encrypted access tokens stored on CSM servers. In addition, email credentials can only be created and modified in CSM Administrator by a user with the Can administer email credentials security right. For Office 365, you must grant the Azure App full access to Exchange Web Services (EWS). See Daemon app that calls web APIs - app registration. For G Suite, you must enable domain-wide delegation. See Control G Suite API access with domain-wide delegation.

We also recommend these CSM settings to secure credential-based email accounts:

- When defining the default From settings for an email account, ensure messages are sent from the server, rather than the client machine. Ensure the **Allow arbitrary FROM addresses** check box is cleared.

- When defining email security rights, ensure the **Can specify arbitrary FROM addresses even if not allowed for Users?** security right is disabled.

To set up email credentials:

1. Open the **Email Credentials Manager**.
2. Select the **New** button, or edit an existing set of credentials.
3. In the **General** page, provide a **Name** and **Description**.
4. Choose a **Credential Type**.
   - Office 365
   - Google Authentication

   Depending on the credential type you choose, a corresponding page appears in the page section.
5. Select the page for your chosen credential type.
   - Office 365
   - Google Authentication
6. To convert existing password-based email accounts to use credentials:
   a. Edit the email account you want to update.
   b. Select the **Use Credentials-Based Authentication** check box.
   c. In the **Account Information** section, select the appropriate credentials in the **Credentials** menu.

Related concepts

Modern Authentication and Google Authentication FAQs

Email Security Rights

Related tasks

Configure Email Credentials for Office 365 Accounts
Configure Email Credentials for Google

Configure Email Credentials for Office 365 Accounts

Use the information in your Azure account to complete the fields in this form.

Before you set up Office 365 credentials in CSM, you must have a registered App in Azure. For information on creating and registering Apps, see https://docs.microsoft.com/en-us/azure/active-directory/develop/scenario-daemon-app-registration and https://portal.azure.com/#blade/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/RegisteredApps.

The App must have full access to Exchange Web Services (EWS). In the App, select **API Permissions > Add a Permission** and select **Exchange**. Select **APIs my organization uses**. In the search prompt, enter `Office`. When **Office 365 Exchange Online** appears, select it. Select **App Permissions**, then select **full_access_as_app**. In the **Configured Permissions** section, select the **Grant admin consent for <your server>** button.

To set up credentials in CSM for Office 365:

1. Enter the **Client ID** and **Tenant ID**.
2. You can use a Secret or Certificate. Your Azure account may have both set up, but you only need one for CSM.
     ◦ **Use Secret**: enter the Secret.
     ◦ **Use Certificate**: import the Certificate's .pfx file.
3. Select **Test** to ensure sending and receiving emails using the credentials works correctly. If either part of the test failed, you will see an error message to help you diagnose the problem. You can find more information on generic errors in the log files (see the Application Server log for 3-tier connections and the CSM Client log for 2-tier connections).
4. You can edit the default values for **URL**, **Scope**, and **Country**, but we strongly recommend leaving the default values in place.

Related concepts
Modern Authentication and Google Authentication FAQs

Configure Email Credentials for Google

Use the information in your G Suite account to complete the fields in this form.

Prior to setting up Google Authentication in CSM, you must have the following set up in G Suite:

- A project on the Google Cloud platform.

- Access to the Gmail API enabled.

- A service account that will authenticate CSM with G Suite.

- Domain-wide delegation enabled in G Suite. To do this, add the client ID of the service account, then grant access to supported Google APIs. For more information, see Control G Suite API access with domain-wide delegation.

    🖊 **Note:** We suggest adding a single scope (`https://mail.google.com`) that grants all rights to the email account.

- Either the Google secret JSON file or the certificate .p12 file.

To set up credentials for Google Authentication:

1. Enter the **Service Account E-mail**.
2. You can use a Private Key or Certificate. Your G Suite account may have both set up, but you only need one for CSM.
    - **Use Private Key**: Enter the Google Secret in the **Private Key** field. When copying the Secret from the JSON file you downloaded from G Suite, you don't have to edit out the line break characters. CSM will remove them for you.
    - **Use Certificate**: Import the Certificate's .p12 file.
3. Select **Test** to ensure sending and receiving emails using the credentials works correctly. If either part of the test failed, you will see an error message to help you diagnose the problem.
    You can find more information on generic errors in the log files (see the Application Server log for 3-tier connections and the CSM Client log for 2-tier connections).
4. (Optional): You can edit the default values for **URL** and **Scope**, but we strongly recommend leaving the default values in place.

Related concepts
Modern Authentication and Google Authentication FAQs

Modern Authentication and Google Authentication FAQs

Find information about securing credentials-based email accounts and answers to frequently-asked questions about Modern Authentication and OAuth 2.0.

Currently, provider limitations require you set the following permissions for CSM email credentials to function:

- **Enable Domain Wide Delegation** in G Suite. The G Suite service account is not a member of your G Suite domain, unlike other user accounts. You must grant it explicit permission to access user accounts by enabling domain-wide delegation. See Control G Suite API access with domain-wide delegation.
- **Full access as app** in Office 365 Exchange Web Services (EWS). You must grant the Azure app full access to the EWS API. This API does not allow selection of more granular permissions like mail.read or mail.write. See Daemon app that calls web APIs - app registration.

CSM uses server-side authentication to manage email primarily through the Automation Process service and the Email and Event Monitor. Office 365 and G Suite do not offer account restrictions for this flow, so we use a service account for G Suite and an Azure app with application permissions for Office 365. Neither provider allows us to configure access to specific accounts.

CSM keeps credential-based email accounts secure through encrypted access tokens stored on CSM servers.

Refer to Configure Email Credentials to see our recommended settings for securing credentials-based email accounts.

Can I use Modern Authentication or OAuth 2.0 with my CSM implementation?

Versions of CSM older than CSM 10.1 do not support credential-based email account management. For more information on upgrading CSM, refer to Upgrade CSM.

For more information on Microsoft's plans to deprecate Basic Authentication, see https://techcommunity.microsoft.com/t5/exchange-team-blog/basic-authentication-and-exchange-online-april-2020-update/ba-p/1275508. For more information on Google's plans to deprecate less secure app (LSA) access, see https://gsuiteupdates.googleblog.com/2020/03/less-secure-app-turn-off-suspended.html.

What's the difference between Modern Authentication and OAuth 2.0?

Microsoft 365 Exchange Online utilizes Modern Authentication, which is a combination of authentication and authorization methods between a client and a server, as well as additional security measures that rely on access policies. Its authentication method is a mix between multi-factor authentication, smart card authentication, and client certificate-based. Its authorization method is an implementation of OAuth and the access policies are Mobile Application Management (MAM) and Azure Active Directory (Azure AD) Conditional Access.

Google utilizes the OAuth 2.0 protocol for both authentication and authorization.

Can I convert existing email accounts that use passwords to use credentials?

Yes. After you set up credentials in CSM Administrator, manually update the password-based email accounts to use credentials.

Modern Authentication

How do I create an Azure app?

When Modern Authentication is enabled, background applications (example: Automation Processes and the Email and Event Monitor) will need to use credentials from an Azure app. A user that has access to this application will be able to read and send emails.

1. Log into Azure AD and register an app https://portal.azure.com/#blade/Microsoft_AAD_IAM/ ActiveDirectoryMenuBlade/RegisteredApps.

2. Follow the steps in this link to create an app. https://docs.microsoft.com/en-us/azure/active-directory/develop/scenario-daemon-app-registration. A callback URI is not required.

3. The App must have full access to Exchange Web Services (EWS). In the App, select **API Permissions > Add a Permission** and select **APIs my organization uses**.

4. In the search prompt, enter `Office`. When **Office 365 Exchange Online** appears, select it.

5. Select **App Permissions**, then select **full_access_as_app**. In the Configured Permissions section, select the **Grant admin consent for <your server>** button.

   > 🖉 **Note:** For information on restricting access based on policy groups, see https://forums.ivanti.com/s/article/Restricting-Access-to-a-Modern-Authentication-Application.

6. Once the app is created, retrieve the app id, tenant id, and client secret. These will be used to configure the Cherwell email account.

7. You can now add the secret/certificate information. Navigate to https://portal.azure.com/#blade/ Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/RegisteredApps

8. Navigate to **Certificates & Secrets** to upload a certificate or add a secret.

Google Authentication

How do I set up a service account on the Google platform?

1. Create a new project on the Google Cloud Platform (see https://console.developers.google.com/).

2. Enable access to the Gmail API.

3. Create a service account that will authenticate Cherwell with G Suite.

4. Download the JSON/ PFX file that contains the credentials for the account.

5. Enable G Suite domain wide delegation. To do this, add the client ID of the service account, then grant access to supported Google APIs.

How do I configure G Suite with the service account?

1. In the G Suite account, select **Security > Advanced Settings**.

2. Select **App Access Control**.

3. Select **Manage Domain Wide Delegation**.

4. Select **Add New**.

5. Paste the unique ID from service account creation in the **Client ID** field.

6. Add `https://mail.google.com` to the **Scopes** field.

7. Select **Authorize**.

Implementing Email Accounts

To get started with email, you can implement the CSM default email system by completing a worksheet, configuring test and production accounts, and configuring a global test email account.

To implement the default email system:

1. Complete the email worksheet.

2. Configure test and production accounts.

3. Configure a CSM global email account for testing.
   a. Define account settings. Account options include:
      ◦ POP or IMAP.

      ◦ Microsoft Exchange.

   b. Define default From Address for the global account.

   c. Define default email history attachment options.

4. Configure a CSM global email accounts.
   a. Define account settings. Account options include:
      ◦ POP or IMAP.

      ◦ Microsoft Exchange.

   b. Define default From Address for the global account.

   c. Define default email history attachment options.

   > **Note:** Alternatively, configure these settings using the Getting Started Page in CSM Administrator (**Help > Go to Getting Started Page**.

5. Implement email notifications.

6. Configure the production email account.

Email Worksheet

Organize email information such as user credentials, account information, and server location into a worksheet for easy reference during the configuration process.

Before configuring CSM email, users must create three email accounts using their own email service:

- Test Receiver Account: Create a test email account to receive test messages from CSM (example: ServiceDeskTESTReceiver@company.com).
- Test Sender Account: Create a test email account to send messages via CSM (example: ServiceDeskTESTSender@company.com).
- Production Account: Create a production email account to send messages via CSM (example: support@company.com).

Depending on the type of email service being used, complete one of the following worksheets to organize the email information.

POP or IMAP Account

Email Item	Test Account (Sender) Information		Production Account Information
Account Name			
	Example: MyDevAccount		*Example: MyProductionAccount*
Account Username			
	Example: ServiceDeskTESTSender		*Example: Support*
Account Password			
	Example: Colorado719		*Example: Colorado719*
Incoming (POP or IMAP) Server Location			
	Example: pop.PrimaryDomain or imap.PrimaryDomain		*Example: pop.PrimaryDomain or imap.PrimaryDomain*
Incoming (POP or IMAP) Server Security Protocol			
	Example: Auto, Basic, SSL, TLS		*Example: Auto, Basic, SSL, TLS*
Outgoing (SMTP Server Security Protocol			
	Example: smtp.PrimaryDomain		*Example: smtp.PrimaryDomain*

Exchange Account

Email Item	Test Account (Sender) Information		Production Account Information

Account Name		
	Example. MyDevAccount	*Example. MyProductionAccount*
Account Username		
	Example. ServiceDeskTESTSender	*Example. Support*
Account Password		
	Example: Colorado719	*Example: Colorado719*
Exchange Domain		
	Example: mycompany.com	*Example: mycompany.com*
Server (Client Access)		
	Example: exchange.mycompany.com	*Example: exchange.mycompany.com*

Configure Test and Production Accounts

CSM provides a Stored Value, named Current System, that holds either a Development or Production value. This Stored Value allows users to easily transition their accounts from testing to production.

By default, the Stored Value is set to Development and controls the status of the other Current System Stored Values related to email, including:

- Current System DEV E-mail Recipient: Holds the test receiver email account (example: ServiceDeskTESTReceiver@company.com).
- Current System DEV E-mail Sender: Holds the test sender email account (example: ServiceDeskTESTSender@company.com).
- Current System Production E-mail Sender: Holds the production email account (example: support@company.com).

To configure test and production email accounts:

1. In the CSM Administrator main window, select the **Settings** category, and then select the **Open Stored Values Manager** task.

   The Stored Value Manager opens, listing the existing Stored Values.

2. In the Manager tree, select the **Global** folder.

   A list of globally available items opens in the main pane.

3. Right-click the **Current System DEV E-mail Recipient** Stored Value and select **Edit**.

4. In the **Value** field, provide the test recipient account address (example: ServiceDeskTESTReceiver@company.com).

5. Select **OK**.

6. Right-click the **Current System DEV E-mail Sender** Stored Value and select **Edit**.

7. In the Value field, provide the test email account address (example: ServiceDeskTESTSender@company.com).

8. Select **OK**.

9. Right-click the **Current System Production E-mail Sender** Stored Value and select **Edit**.

10. In the **Value** field, provide the production account (example: support@company.com).

Stored Value	x

Name: Current System Production E-Mail Sender

Description: E-Mail account used as sender during Production. This account is also the account used by the E-mail Event Monitor for incoming e-mails.|

Type: Text ▾
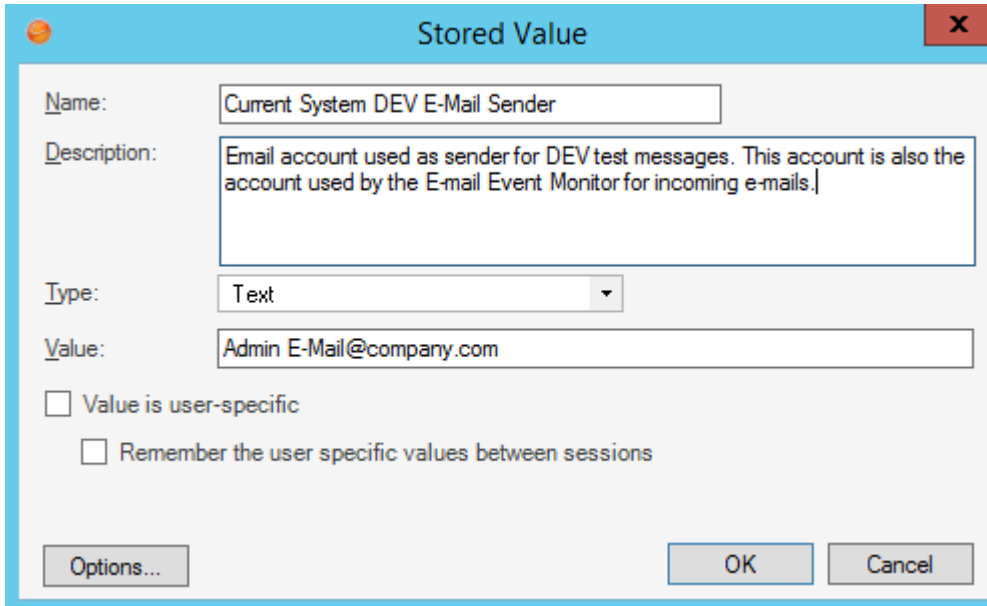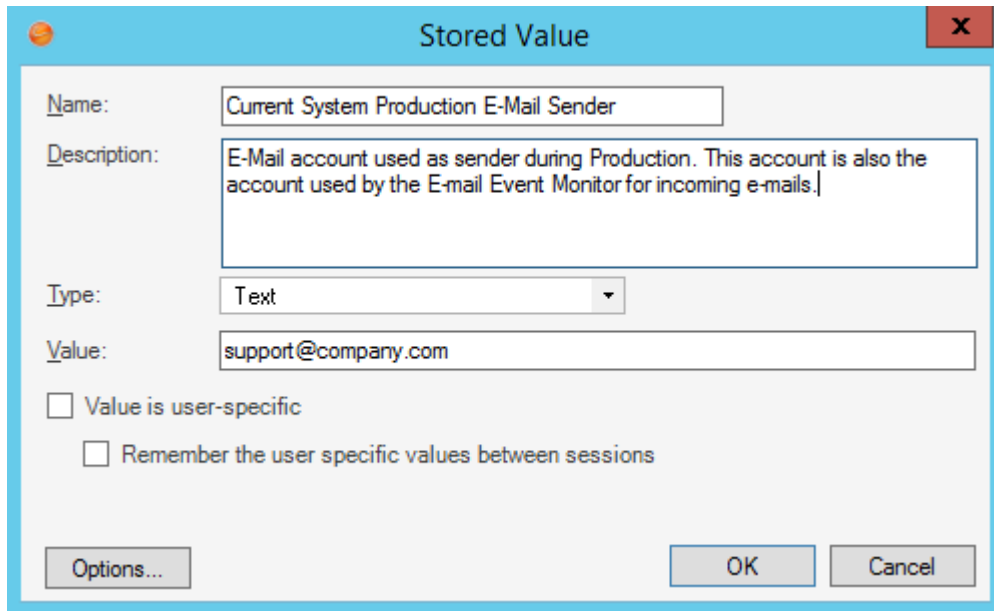
Value: support@company.com

☐ Value is user-specific

   ☐ Remember the user specific values between sessions

Options...   OK   Cancel

Configure Global Email Accounts

As a prerequisite for creating test and production email accounts for users, configure a global email account within CSM Administrator.

You can configure two separate CSM email accounts:

- Test account: Use this account while developing and testing the system. It is monitored by the Email Monitor during development and used as the sender account for automated test emails.

  Note: Use test sender account (ServiceDeskTESTSender@company.com) information on the Email Worksheet.

- Production account: Transition to this account after development. It is monitored by the Email Monitor during production and used as the sender account for all automated emails.

  Note: Use production account (example: support@company.com) information on the Email Worksheet.

1. In the CSM Administrator main window, select the **E-mail and Event Monitoring** category, and then select the **E-mail Accounts and Settings** task.
   The **E-mail Options** window opens.
2. Select the **Accounts** page.
3. Select the **Add** button to select the type of email account to set up (POP, IMAP, or Exchange).
4. Configure the account:
   a. Define global settings for a POP or IMAP account
   b. Define global settings for a Microsoft Exchange Account
5. Select the **Spell Check E-mail** check box to have CSM spell check emails as messages are typed.
6. Select the **Make Default Account** button to make the selected account the default account for sending emails.
7. Select **OK**.

Implement Email Notifications

Use the Current System Stored Values to determine email senders and recipients for email notifications. This is especially useful when email templates are created, and ensures that email notifications are sent to a test account (rather than to actual customers) when the system is in a testing environment.

When ready to transition to Production, change the Current System Stored Values to Production to have email notifications sent to Customers.

Note: Email Actions in default Incident One-Step Actions use templates with the Current System Stored Values. Use these as a starting point, edit them, or create your own.

To implement email notifications (example: In One-Step Actions, Automation Processes, etc.):

1. From a One-Step Action or Automation Process, create a new Send Email action.
2. Configure test and production account Stored Values.
3. In the **E-mail Message** window, use the System State E-mail Expression for the From Address field:
   a. Right-click in the **From** field to open the Token Selector and expand **Expressions**.

   b. Select **Browse** to open the Expression Manager.

   c. In the Manager tree, select the **Global** folder.

   d. Select **System State E-mail**.

   This Expression states that if the Current System Stored Value is set to Production, then the Current System Production Email Sender Stored Value is used as the sender's address. If the Current System Stored Value is set to DEV, then the Current System DEV Email Sender Stored Value is used as the sender's address.

4. In the **E-mail Message** window, define a Custom Expression for the To Address field using the test and production account Stored Values:

    a. Right-click in the **To** field to open the Dynamic Value Selector and expand **Expressions**.

    b. Select **New Custom Expression** to create a new case Expression.

    This Expression uses the Customer's email address (from the email address field on the current record) as the default recipient address unless the Current System Stored Value is set to DEV. If the Current System Stored Value is set to DEV, then the Current System DEV E-mail Recipient Stored Value is used as the recipient's address.

Configure the Production Email Account

When ready to transition the email system to production, change the Current System Stored Values from Development (default) to Production to activate all user and customer emails. Once changed, emails are no longer sent to users and customers during development.

To set the Current System Stored Value to production:
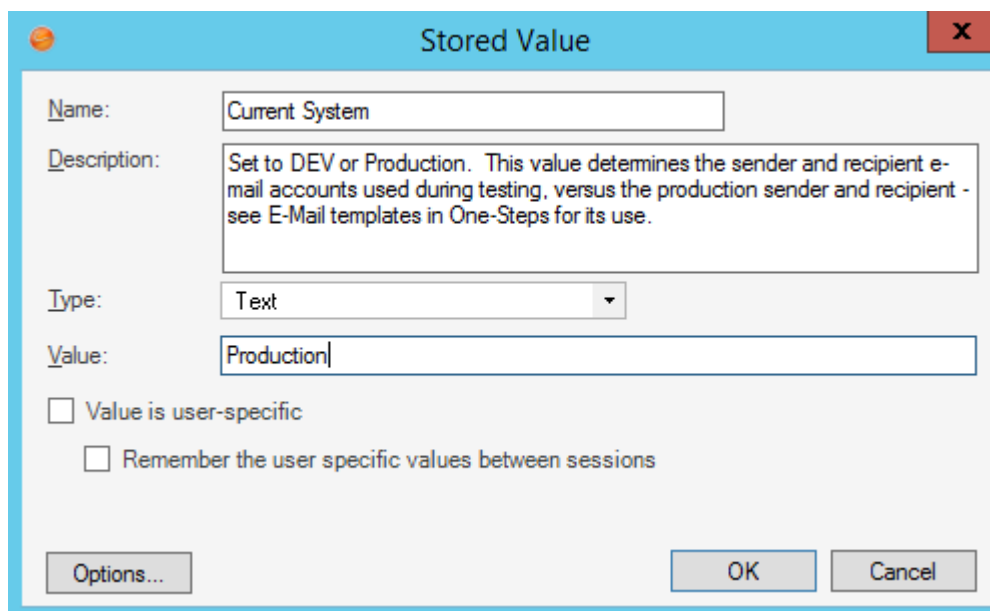
1. In the CSM Administrator main window, select the **Settings** category, and then select the **Open Stored Values Manager** task.

   The Stored Value Manager opens, listing the existing Stored Values.

2. In the Manager tree, select the **Global** folder.

   A list of globally available items opens in the main pane.

3. Right-click the **Current System** Stored Value and select **Edit**.

4. Delete **DEV** from the **Value** field.

5. In the Value field, type `Production`.

Configure Outlook Integration

Configure CSM to integrate with Microsoft Outlook and interact with Business Object records directly from Outlook.

Configuring CSM Outlook Integration Configurations in CSM Administrator

Use CSM Administrator to configure CSM to integrate with Microsoft Outlook and interact with CSM Business Object Records directly from the Outlook interface.

To configure an Outlook Integration Configuration:

1. Configure Outlook Integration security rights: Determine who can set or override defaults, run the Add-In from Outlook, and add, edit, or delete Outlook Integration Configurations.

2. Create an Outlook Integration Configuration in CSM Administrator: Use the Configure Outlook Integration window (accessed from the Outlook Integration Manager) to create an Outlook Integration Configuration and define:

   a. General settings for the Outlook Integration Configuration: Name, description, auto-link options, and Conversation ID options.

      A Conversation ID is a unique, alphanumeric identifier that correlates an email message with a particular conversation so that it can be associated with a CSM Record. CSM inserts Conversation IDs into emails to identify if a particular email is a reply to a previous message that was associated with a specific Business Object record. A Conversation ID looks similar to the following: {CMI: ABCD1234}, where ABCD is an identifier for the particular CSM system (set this value in the History Attachment Options for a global e-mail account), and the numeric indicator is the specific Conversation ID. The number is automatically incremented for each message.

   b. Customer Identification settings for the Outlook Integration Configuration.

   c. Which Business Objects can be linked to Outlook emails.

3. Configure Outlook Integration Configuration Defaults: Define which Roles can view and use which Outlook Integration Configurations.

Outlook Integration Manager

Use the Outlook Integration Manager to complete general CSM Item Manager operations for Outlook Integration Configurations.

You can use the Outlook Integration Manager to disable an Outlook Integration. The disable icon 🚫 indicates that an Outlook Integration is disabled. Enable/disable Outlook Integrations either by right-clicking the item or by selecting **Disabled** from the **Edit** menu.

1. Manager Tree:

   Displays items in a hierarchical tree, organized by scope, and subfolder if applicable. Also lists any searches run during the session.

2. Main Pane:

   Displays items by view (icon, list, or details [grid]) and lists search results when a search is run.
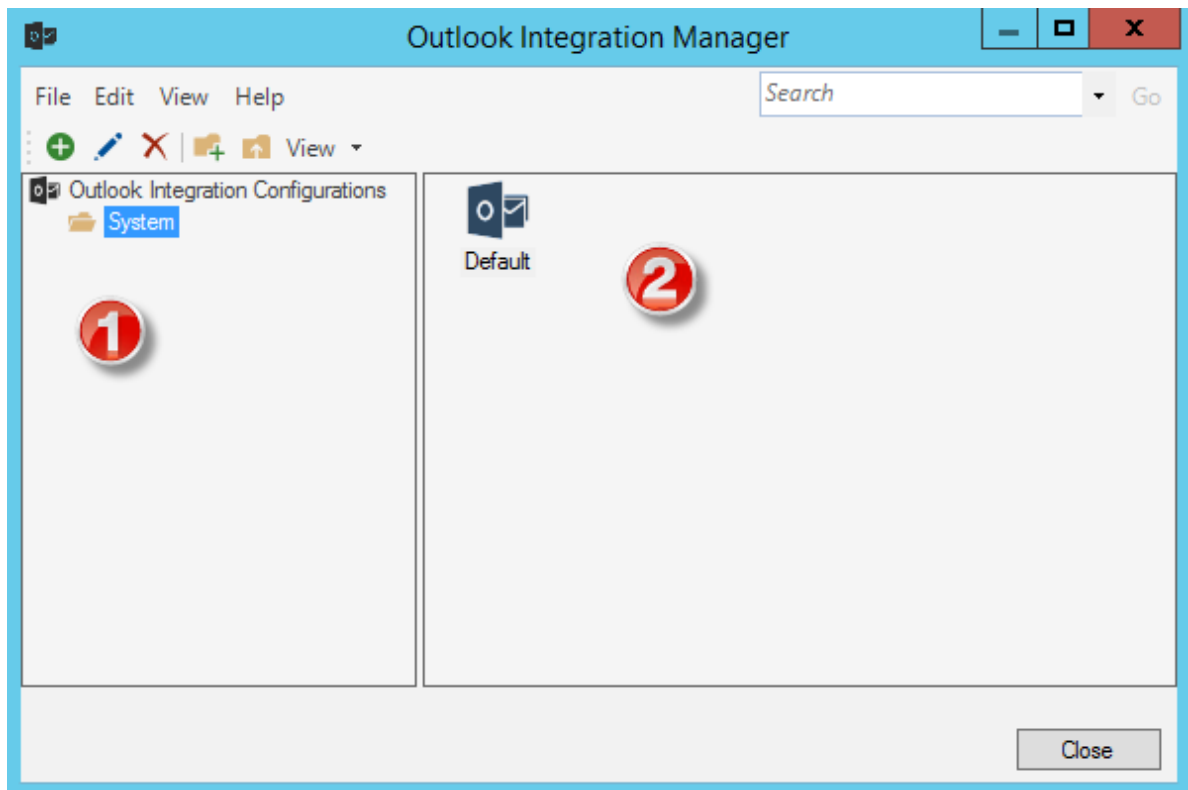
General Settings Options for an Outlook Integration

Define general settings such as name, description, user override and exclude rules, and Conversation ID options for Outlook Integrations.

Use the **General** page in the **Configure Outlook Integration** window (accessed from the Outlook Integration Manager) to define general settings.

To define general settings for an Outlook Integration Configuration:

Name	Provide a display name (this property can be searched in CSM Item Managers).
Description	Provide a description (this property can be searched in CSM Item Managers).
Auto-Link Options	Enable auto-linking for incoming Outlook emails, and then define exclusion rules, embedded property rules, and override options.
Default to Auto-Linking Incoming E-mail	Select this check box to automatically associate incoming emails from a monitored folder with a Business Object Record (a Journal - Mail History Record is created). **Note:** An email message is auto-linked only if CSM can identify a Customer from the email, and then associate the Customer with a specific Business Object Record. Otherwise, messages must be manually linked to Customers and Business Objects.
Clear Embedded properties from Messages before Sending	Select this check box to have embedded properties removed from emails sent from Outlook. **Note:** The Cherwell Outlook Add-In adds a single embedded property to outgoing messages to enable recipients who also use the Add-In to see when an email is already linked to a Business Object Record. Although this is just one small property, Exchange Servers can only handle a limited number of unique embedded properties, and might reject incoming emails that contain new, unmapped properties. This limitation is sometimes encountered on Exchange 2007 and earlier (less likely on Exchange 2010 and later), but rarely warrants removing the Add-In's embedded properties from outgoing emails. Leave this box cleared so that other email recipients who use the Add-In can see link information. The ability to see this information makes it less likely that the same message will be linked multiple times. **Tip:** Select the **Information** button to view this same information.
Allow Users to Override Auto-Link Settings	Select this check box to allow users to override the default auto-link settings when configuring the Outlook Integration in Microsoft Outlook.
Exclude	Select this button to define Skip Item Rules for determining which incoming messages are discarded based on defined criteria (example: skip emails from automated systems).

Define Conversation ID Options	Define whether to have Conversation IDs added to outgoing emails. A Conversation ID is a unique, alphanumeric identifier that correlates an email message with a particular conversation so that it can be associated with a CSM Record. CSM inserts Conversation IDs into emails to identify if a particular email is a reply to a previous message that was associated with a specific Business Object record. A Conversation ID looks similar to the following: {CMI: ABCD1234}, where ABCD is an identifier for the particular CSM system (set this value in in the History Attachment Options for a global email account), and the numeric indicator is the specific Conversation ID. The number is automatically incremented for each message.
Conversation IDs Options	Select this check box to include Conversation IDs in outgoing emails. **Note:** When a Conversation ID is found within an email message, CSM can immediately find the record (example: Incident) associated with the various emails. If Conversation IDs are not used, then it can still identify records, but it has to use less reliable techniques, such as comparing the details of the subject line.
Add to Subject Line	Select this radio button to include the Conversation ID in the subject line of incoming emails.
Add to Body	Select this radio button to include the Conversation ID in the body of incoming emails. **Note:** Do not delete Conversation IDs from email messages. Doing so makes it harder for CSM to associate customer replies with the correct record.

Define Skip Item Rules for an Outlook Integration Configuration

Skip Item Rules are defined criteria that determine which emails from a monitored account are discarded (and not processed). For example, anything identified by a spam filter can be thrown out automatically.

Also, specify recipient addresses so that items such as global company announcements can be ignored (and Incidents are not created from them). The discarded emails are not automatically linked to Business Objects.

Note: Users can define Skip Item Rules for an Email Monitor.

To define Skip Item Rules:

Word/phrase	Provide the text to search for incoming emails.
Appears In	Select which part of incoming emails you want CSM to search for the specified word/phrase (example: Subject).
Anywhere	Select this radio button to have CSM search anywhere in the Appears In location for the specified word/phrase.
Begins with	Select this radio button to have CSM search the beginning of the Appears In location for the specified word/phrase.
Ends with	Select this radio button to have CSM search the end of the Appears In location for the specified word/phrase.

Define Customer Identification Options for an Outlook Integration

Use the **Identify Customer** page in the **Configure Outlook Integration** window (accessed from the Outlook Integration Manager) to define options for identifying customers and associating them with the appropriate Customer and Business Object Records.

Note: The options for identifying customers are ordered hierarchically. If more than one option is selected, CSM attempts to identify customers by the first option selected, then by the second, etc. For example, if **Find Customers by E-mail Address** and **Custom** is selected, CSM attempts to find the customer by email address first; if it cannot identify a customer using that method, it attempts to identify the customer based on the Custom settings.

To define Customer Identification options:

Find Customers by E-mail Address	Look up the sender's email address in the email field of the appropriate Customer Object, and then specify which field CSM should search in Customer objects. This is useful if emails are received from a particular company but do not necessarily know who at the company will be sending the emails (example: If an email comes in from Bob@Example.com, the system searches the Business Object and Field for Example.com).
	• **Use Default E-mail Address Fields**: Select this radio button to have CSM look in the Customer Object (and its associated children) in the field that is marked as the email field. **Tip:** This is almost always the most appropriate option.
	• **Search All Contact Manager Objects**: Select this check box to have CSM search email fields in all objects in the Contact Manager. **Note:** It is possible to include other objects in addition to the Customer Object in the Contact Manager (example: External data). If Customers are kept in an External Business Object or other custom object, then check this option to include it in the search.
	• **Custom Business Object or Field**: Select this radio button to have CSM always search a particular Business Object and look in a particular field to identify Customers, and then select the Business Object and Field in the drop-down lists.
	Note: This is an advanced option for use when email addresses are stored in a non-standard object for specialized use (example: A server list that sends alerts). If these are not requirements, use the Customer - Internal Business Object default.

Find Customers by Domain	Look up the sender's domain in a specified Business Object and Field (select the **Business Object** and **Field** in the drop-down lists). **Note:** In order for this to work, the selected Business Object must be configured to have an appropriate field containing the domain. Create a field and either require it to be manually filled or use an Expression to determine the domain from the already-entered email address (which can be done easily using a Text After Modifier).
Custom	Look up Customers by searching for a value in a Business Object that are specified. This is useful if Customers need to be identified using information other than an email address. This option uses information other than the sender's e-mail address (ex: Subject) to identify Customers. In the drop-down, select what and where CSM should search: • Value to Find: Select the area of the email (example: Subject) to search. • Business Object: Select the type of Business Object to search. • Field: Select the field to search in the Business Object.
Default Customer to Use	Select a default Customer from the Contact Manager (select the **Ellipses** button). CSM uses the default customer with which to associate Business Objects if the customer cannot be identified using the other methods. This option designates a default customer if CSM cannot identify a customer using the other methods. This is useful to automatically link emails from unknown addresses to a particular place for later review.

Related concepts

Outlook Integration Manager

Define Which Business Objects can be Linked to Outlook Emails

Use the **Objects** page in the **Configure Outlook Integration** window (access from the Outlook Integration Manager) to define which Business Objects can be linked to Outlook emails.

To define which Business Objects can be linked to Outlook emails:

Add	Select a type of Business Object to add to the list (ex: Incident)
Edit	Edit the settings for the highlighted type of Business Object
Remove	Remove the selected Business Object type and associated settings.
Up/Down Arrows	Change the order of the Business Objects.
If Adding or Editing:	This is only applicable when adding or editing a Business Object. • General: Defines basic properties for the Business Object. • Update Behavior: Defines behaviors when updating a Business Object Record from an Outlook email. • Create Behavior: Defines behaviors when creating a new Business Object Record from an Outlook email. • Available Actions: Adds One-Step Action Actions that can be executed on the linked Business Object Record.

Related concepts
Outlook Integration Manager

Define General Options for Business Objects Linked to Emails

Define basic properties for Business Objects that are linked to Outlook emails. These properties determine which Business Object Records the Cherwell Outlook Add-In lists as potential link items.

Define potential link items to show for the identified customer. For example, if an Outlook Integration Configuration identifies a customer (based on the Customer Identification settings), but cannot find a definitive Business Object to link to, it suggests potential link items that the user can select from.

To define general properties for Business Objects linked to emails:

Related Items	Lists the most recent records based on a specified Relationship (example: Incidents associated with the identified Customer).
Main <Business Object> Only	Lists only the identified Customer as a link item. **Note:** This option is only applicable if the Business Object selected on the Objects page is a Customer Object (example: Customer - Internal). In this case, using a Relationship does not make sense because the linkable object is the Customer Record itself (rather than a Business Object related to the Customer Record).
If Customer is not part of the Customer bus-ob group, automatically determine potential link items	Lists related Business Object Records for an identified customer who is not part of the CSM Customer Business Object Group (example: an external Customer Business Object). In this case, the system searches all of the Relationships for that object until it finds one whose child type is the same as the Business Object specified on the Objects page.
Allow Creation of new <Business Objects (ex: Incidents)> from Outlook	Allows Business Objects to be created directly from the Outlook Add-In. If this option is cleared, the **Create Behavior** page disappears.
Display New Record before Saving	Shows new Business Object Records created from the Outlook Add-In before being saved in CSM. This gives the user a chance to tweak records and potentially fill in required information that could not be determined automatically.

Define Update or Create Behaviors for Business Objects Linked to Emails

Use the **Update Record Behavior** page and the **New Record Behavior** page to define behaviors for updating or creating Business Object Records from Outlook emails.

To define update or create behaviors for Business Objects linked to emails:

Attach Outlook e-mail to to Business Object (example: Incident)	Attaches incoming emails to linked Business Objects as Journal - Mail History Records.
Import Attachments as Part of E-mail	Imports email attachments along with incoming emails. **Options**: Select this button to define rules for excluding attachments based on size or type of file.
Attach E-mail Attachments to <Business Object (for example, Incident)>	Attaches email attachments to Business Object Records (not just to the internal copy of the email). **Note:** If this option is selected, email attachments are stored in Business Object Records as Attachments. For more information, refer to the Attachments documentation.
Preserve Inline Images within E-mail Body	Preserves images within the body of incoming emails with the text of the email. **Note:** The target Field must be configured to store Rich Text for this to work correctly.
Attach Inline Images to <Business Object (for example, Incident)>	Attaches images within the body of incoming emails to the selected Business Object.

Attach Outlook E-mail to Customers	Attaches incoming emails to Customer Records as Journal - Mail History Records. Select the **Options** button to define which Customer Records to attach emails to: • **Attach to Customer (From address):** Attach emails to Customer Records that are identified from the addresses in the From line. • **Attach to Customers in CC Line:** Attach emails to Customer Records that are identified from email addresses in the CC line. • **Attach to Parents of Customers (for example, company that contact works for):** Attach emails to Parent Records of Customer Records (for example, if an email sender is a contact that works for a particular company, the email can be attached to the Company Record as well as the Customer Record). **Note:** This capability, along with the ability to attach to a particular Business Object, can mean that an incoming email is attached to a specific Incident, the Customer who sent the email, other Customers who were also CC'd on the message, and even to the company for whom the Customer works. This powerful feature means that the communication history about a particular record, or all communication from a particular Customer or company, can be seen (although, of course, there is the potential for significant overhead).
Store E-mail as Plain Text	Discards Rich Text formatting contained in incoming emails and store them in Journal - Mail History Record as plain text. Do this to reduce the amount of space used by messages.
Actions	

Add	Sselect **Actions** from a list. The following Actions are available: • Create New <Business Object (for example, Incident)> (only available on the Create Behavior page): Creates a new Business Object Record (of the type selected in the Objects page of the Configure Outlook Integration window) based on information from incoming Outlook emails. Specify which Fields are populated, and the values of those Fields. • Update <Business Object (for example, Incident)>: Updates a Business Object Record (of the type selected in the Objects page of the Configure Outlook Integration window) with information from incoming Outlook emails. Specify which Fields are updated and the values of those Fields. **Note:** There must be a create Action (either a direct Action to create a new Business Object Record or a One-Step Action that contains the same functionality) when specifying Create Behavior. For an update, however, there is no need to specify an Update Behavior. Without custom update Actions, a Journal - Mail History Record can still be associated with the Business Object Record, which is frequently all that is needed. • Add to a Queue: Determines which CSM Queue the Business Object Record (of the type selected in the Objects page of the Configure Outlook Integration window) is added to (for example, New Request Queue) after it is created or updated. Select the ellipses button to open the Queue Manager and select a Queue. • Run a One-Step Action: Runs a One-Step Action related to the Business Object Record (of the type selected in the Objects page of the Configure Outlook Integration window). Select the ellipses button to select an existing One-Step Action or create a new one.
Edit	Edit the highlighted Action.
Copy	Create a copy of the selected Action.
Delete	Delete the selected Action
Up/Down Arrows	Change the order of the selected Actions

Define Available Actions for Business Objects Linked to Emails

In addition to creating and updating records, you can arbitrarily make other functionality available to execute against a linked record. For example, you can configure an Action to add a new Task to the record (as a reminder to follow up), or to assign the record.

Actions can do anything allowed by One-Step Actions. These Actions are shown as a drop-down list in the Cherwell Outlook Add-In.

Add, delete, or reorder Actions available for the linked Business Object (specified in the Objects page of the Configure Outlook Integration window). The Actions specified here show up on the Actions drop-down list within the Cherwell Outlook Add-In.

To define available actions for Business Objects linked to emails:

Add	Select a type of Action in the drop-down list. • **Add One-Step Action Action:** Adds One-Step Actions to the Actions drop-down list in the Outlook Add-In to execute them directly from Outlook. Select the **Ellipses** button to open the Action Manager and select a different One-Step Action. **Note:** When this option is selected, the One-Step Action Manager opens, and select an existing One-Step Action or create a new one. • **Add Folder:** Adds a folder to the Actions drop-down menu in the Outlook Add-In to organize Actions.
Delete	Removes the currently selected Action.
Up/Down Arrows	Moves Actions up or down in the list (this is how they appear on the drop-down list within the Outlook Add-In).
New Action General Options	• **Action:** Shows the name of the Action as it is recognized by CSM (example: the name of the Dashboard). **Tip:** Select the **Ellipses** button to open the Action Manager and select a different Action. • **Display text:** Provides the text to display on the Action in the menu. • **Image button:** Opens the Image Manager, and then select an image to represent the Action on the menu. Select an existing image or import a new image.

Define Expressions for showing and enabling Actions	
Visible	Shows/hides the Action based on an Expression, and then define the Expression using one of the following options: • **Stored Expression:** Select the Ellipses button to open the Expression Manager, and then select an existing stored Expression or create a new stored Expression. Stored Expressions can be reused in numerous places in CSM. • Custom Expression: Select the Custom Expression button to open the Custom Expression Builder, and then create a custom Expression specifically for this scenario.
Enabled	Enables/disables the Action based on an Expression, and then define the Expression using one of the following options: • **Stored Expression:** Select the Ellipses button to open the Expression Manager, and then select an existing stored Expression or create a new stored Expression. Stored Expressions can be reused in numerous places in CSM. • **Custom Expression:** Select the Custom Expression button to open the Custom Expression Builder, and then create a custom Expression specifically for this scenario.
Begin Group	Shows a horizontal line before the menu item, separating it from other Actions.

Configure Outlook Integration Defaults

Outlook Integration Defaults define who sees what in the Outlook Integration (which roles can see which Outlook Integrations). Specify default integration configurations for each role.

To configure the Outlook integration defaults:

1. In the CSM Administrator main window, select the **E-mail and Event Monitoring** category, and then select the **Outlook Integration Defaults** task.

   The **Outlook Integration Defaults** window opens.

2. Define the Default Integration Configuration for each role:

   Note: For more information about roles, refer to the Security documentation on Roles.

   a. In the **Default by Role** area, select a role (example: IT Service Desk).

   b. In the **Default Integration** area, select a Default Integration Configuration in the drop-down list.

   c. Repeat this until a Default Integration Configuration is assigned to each role.

   Note: When an Outlook user configures the Cherwell Outlook Add-In, the default configuration specified here is the one to which she is initially assigned. Depending on Outlook Integration security rights, the user might also be allowed to select a different Integration Configuration.

3. Select **Close**.

Configuring the Cherwell Outlook Add-In in Microsoft Outlook

View, edit, and create CSM Business Object Records directly from Microsoft Outlook using the Cherwell Outlook Add-In.

To install the Cherwell Outlook Add-in:

1. From Cherwell Service Management in the Start menu, select I**nstall or Uninstall Cherwell Outlook Add-In**.

2. Select the **Install** button.

3. After the installation is complete, restart Outlook.

   A Cherwell Group appears in the Home tab on the Microsoft Outlook ribbon.

   > **Note:** Uninstall the Cherwell Outlook Add-In using the Cherwell Outlook Installer Wizard. The Add-In can be disabled without uninstalling it (**Microsoft Outlook > File tab > Manage Add-Ins**.

4. Configure the Cherwell Outlook Add-in to connect to the CSM database, link emails to CSM Business Objects, and monitor specified folders.

Configure the Cherwell Outlook Add-In

Configure the Cherwell Outlook Add-In after it has been installed in Microsoft Outlook. Configuration tasks include connecting to the CSM database, providing login credentials, setting up auto-linking for incoming emails, and more.

To configure the Cherwell Outlook Add-In:

1. Select **Not Connected** from the Cherwell Group in the Outlook ribbon.

   If the Add-In has never been used before, a window opens stating that the connection is not configured.

   > **Note:** If the Cherwell Outlook Add-In has been used before, the button may show Connected. In this case, select **Connected**. A window opens with CSM connection and login information, and the ability to edit the configuration.

2. Select **Configure**.
3. Check the **Enable Cherwell Integration** check box to enable the Cherwell Outlook Add-In.
4. Select **Configure** to select a CSM connection to use.
5. Specify connection and login information for the CSM connection that the Cherwell Outlook Add-In will use:
   a. Select the ellipses button and select the appropriate CSM database connection.

      Note: If there is only one connection, then select this connection.

   b. Provide the login credentials.
      ◦ Windows Authentication: The Cherwell Outlook Add-In uses Windows authentication to connect to CSM.

         > **Note:** In order to use Windows Credentials, Windows or LDAP must be enabled in CSM Administrator (that is, Windows and/or LDAP must be supported login modes (**Security > Edit Security Settings > Windows or LDAP**.

      ◦ User ID and Password: The Cherwell Outlook Add-In uses CSM credentials to connect to CSM, and then provide the User ID and password.
   c. Select **Test** to verify that the Outlook Add-In can connect to CSM.

      The name of the CSM connection now appears in the Cherwell Options window next to the Connection button.

6. Define the remaining options for the Cherwell Outlook Add-In:
   a. **Outlook Configuration:** Select the appropriate Outlook Integration Configuration that was configured in CSM Administrator.

      Note: A default Outlook Integration Configuration might have been automatically set. Depending on the security rights, select a configuration other than the default.

b. **Auto-Link Incoming E-mails:** Automatically associates incoming e-mails from a monitored folder with a Business Object Record (a Journal - Mail History Record is created).

> **Note:** This option is only available if Users are allowed to override auto-link settings, configured in CSM Administrator (General settings for OutlookIntegration Configurations). It only enables processing of e-mails as they arrive in a monitored folder. If currently existing e-mails should be processed and automatically linked, select the Rescan Items options in Outlook's explorer UI.

c. **Auto-Link Outgoing Reply/Forward:** Automatically associates outgoing replies or forwards of linked e-mails with the same Business Object Record to which the original e-mail is linked.

d. **Always Default to Non-Final Only Candidates:** The Cherwell Outlook Add-In always lists only non-closed Business Object Records as potential link items.

e. **Folders to Monitor:** Click the **Ellipses** button, select the folders to monitor (example: Inbox), and then select **OK**.

The Cherwell Group in the Outlook ribbon (Home tab) shows connected. Users can begin using the Cherwell Outlook Add-In.

About the Email and Event Monitor

The Email and Event Monitor Service is a CSM service that automatically monitors email accounts and event streams, and then performs specified actions, such as creating or modifying records based on email content or event details.

The Email and Event Monitor Service is a microservice of the Cherwell Service Host. In addition to connecting to the database server, it can communicate with the mail server (example: Microsoft Exchange). See Cherwell Service Host.

The Email and Event Monitor performs the following functions:

- Email monitoring: Email monitoring is a function performed by a CSM Email Monitor to scan an email account's incoming mail and automatically perform actions based on specified conditions (example: Update an Incident record with email content if an existing record can be found).

To use email monitoring, there must be at least one email account configured in CSM. The Email Monitor processes incoming emails from a monitored account and performs actions, such as attaching emails to Business Object records as Journal - Mail History records, creating or updating records with the contents of incoming emails, and executing One-Step Actions against newly updated or created Business Object records. See Configuring Email Accounts.

Restrictions on who can access Email and Event Monitor functionality and data can be put in place using security rights. See E-mail and Event Monitor Security Rights.

An Email Monitor is used to watch one particular email account. Create as many individual monitors as required, but do not create multiple monitors that point to the same email account unless only one is enabled. Otherwise, the behavior of the Email Monitor is ambiguous. A monitor's behavior is defined by a series of Monitor Items (consisting of conditions and actions) that are configured as needed so that emails are processed according to business needs. See Create an Email Monitor.

CSM provides a demo Email Monitor (complete with defined Monitor Items). Implement this demo design for testing, and then create a production design using the Email and Event Monitoring Manager. See Demo Email Monitor.

Email Monitor Good to Know

Note the following behaviors and recommendations about using email and the Email and Event Monitoring Service.

- Manage and create multiple monitors using the Email and Event Monitoring Manager. See Create an Email Monitor.

- Each Monitor's behavior is configured using a series of Monitor Items, which include conditions and actions that define how emails are processed.

- Email accounts cannot be added or modified when you are managing Monitors in a Blueprint or a mApp Solution. You can only select existing email accounts. If the email account is not found when the Blueprint or mApp Solution is published, the email account is removed and must be reconfigured on the target system.

- When pausing or resuming processing, it can take up to five minutes for the pause or resume operation to take effect. To immediately pause or resume processing, use the Server Manager to disable the Email and Event Monitor microservice. Also, even while the Email and Event Monitor microservice is disabled, monitored email accounts continue to receive emails, but those emails are not processed. When the microservice is resumed, all Email and Event Monitors resume processing emails.

- System is the only available scope. Create subfolders underneath this scope to organize items.

- Defining options is not required for identifying an existing record. For example, if the Monitor Item is set up to create a new Incident from an email, it does not need to find an existing record. However, if one of the conditions for the Monitor Item is to find an existing record, then define how the system finds the record.

- The options for identifying records are ordered hierarchically. If more than one option is selected CSM attempts to identify records by the first option selected, then by the second, etc. until it finds an existing record.

- Hosted customers are strongly recommended to restart the Service Host as soon as possible after any credential changes on email accounts. If this is not done, the Auth Token may expire after a period of time causing the Service Host to stop. The time period at which this may occur is dependent on the configuration of the server. Worker leaders in the Email Monitor continue to process emails, but do not pick up any changes in the Definitions until any of the following are true:
  - There are no more emails to process within a given time, causing the worker leader to unload the worker and clear up old messages. When a new email comes in, it will load a new worker and pick up modified Definitions.
  - There is a Service Host error, or the Service Host is manually stopped, causing the new Definitions to be picked up.
  - The Auth Token expires, causing the Service Host Email Monitor to stop processing emails until it is restarted.

Implementing Email Monitoring

When implementing email monitoring, use the demo CSM email monitor as a starting point to implement and test email monitoring. When ready to transition to production, configure the Email and Event Monitor account, and then create an Email Monitor.

To implement email monitoring:

1. Define general settings for the demo Email Monitor. See Define General Options for an Email Monitor.

   > **Tip:** These settings can also be accessed from the **Getting Started** page in CSM Administrator (**Help > Go to Getting Started Page**).

2. Test the demo Email Monitor. See Send a test email through the E-mail Monitor.

3. Once you are satisfied with your settings in the demo Email Monitor, create a new Email Monitor for production using those settings, and configure it with your production email account. See Create an Email Monitor.

   > **Note:** We recommend not to simply configure the demo Email Monitor with the production account. You should create a new Email Monitor using the settings you tested.

4. Disable the demo Email Monitor. See Disable a Monitor.

Demo CSM Email Monitor

CSM provides a demo Email Monitor that includes several defined Monitor Items. Start with this Monitor when testing the CSM email system. Later, create a new Email Monitor to meet organizational needs.

All demo Monitor Items scan incoming emails for an existing customer (using the Email Field of the Customer - Internal Business Object). If an existing Customer is not found, the Monitor uses the default Customer Record as a placeholder.

The following is a summary of the demo Email Monitor Items:

- **Skip Certain Items**: Skip Item Rules are defined criteria that determine which emails from a monitored account are discarded (and not processed). For example, anything identified by a spam filter can be thrown out automatically. Also, specify recipient addresses so that items such as global company announcements can be ignored (and Incidents are not created from them). Skip Certain Items is always the first in the list of Monitor Items, and it cannot be deleted.

- **Reopen Incident**: The Reopen Incident Monitor Item scans incoming emails for a Conversation ID associated with an existing Incident Record. If an existing record is found, the Monitor searches the Subject line of the email for the phrase *Reopen*. If the Subject line matches, the Monitor executes an Action that reopens the Incident.

- **Change Approved**: The Change Approved Monitor Item scans incoming emails for a Conversation ID associated with an existing Approval Record. If an existing record is found, the Monitor searches the Subject line of the email for the phrase *Change Request Approved*. If the Subject line matches, the Monitor executes an Action that changes the Approval status of the Change Record to *Approved*.

- **Change Denied**: The Change Denied item scans incoming emails for a Conversation ID associated with an existing Approval Record. If an existing record is found, the Monitor searches the Subject line of the email for the phrase *Change Request Denied*. If the Subject line matches, the Monitor executes an Action that changes the Approval status to *Denied.*

- **Change Abstained**: The Change Abstained item scans incoming emails for a Conversation ID associated with an existing Approval Record. If an existing record is found, the Monitor searches the Subject line of the email for the phrase *Change Request Abstained*. If the Subject line matches, the Monitor executes an Action that changes the Approval status to *Abstained*.

- **Update Existing Incident**: The Update Existing Incident item scans incoming emails for a Conversation ID associated with an existing Incident Record. If an existing record is found, the Monitor attaches the email to the Incident (including any email attachments).

- **Default**: The Default Monitor Item consists of actions that a Monitor performs if no other conditions are true. Default is always the last item in the list of Monitor Items, and it cannot be deleted. It is configured the same way as a new Monitor Item, except that it has no Conditions page. Its built-in condition is that none of the actions for the other Monitor Items were executed because their conditions were not met. By default, this Monitor Item creates a new Incident from the email.

Send a Test Email through the Email Monitor

Test the demo Email Monitor to ensure that email accounts and Email and Event Monitor settings work properly.

For more information on the demo Email Monitor, see Demo Email Monitor. To test the demo Email Monitor:

1. Send a basic email to a test CSM account.
    a. Access the sending account (example: ServiceDeskTEST@company.com) via an email service.
    b. Create a new email.
    c. Provide the email address monitored by the demo Email Monitor in the **To:** line of the email.
    d. Type `Test` in the subject line.
    e. Type `Test` in the body of the email.
    f. Send the email.
        The email is automatically sent to the Email Monitor to be scanned for properties that match the defined Monitor Items. Since the email does not contain any Monitor Item properties in the demo Email Monitor, the Email Monitor initiates the default Monitor Item, which creates an Incident in CSM.
2. Open the Incident created by the email.
    a. Open the CSM Desktop Client.
    b. Select **Searching > All Incidents**.
        A list of Incidents opens in the main pane.
    c. Select the **Created Date Time** column header to view the most recently created record first.
    d. Double-click the incident to open the record in the main pane.

    Note: If the email is not immediately visible in the list of Incidents, wait a few moments for the Email Monitor to recognize the account changes and scan the account. If Incident is still not visible, make sure the appropriate default Email Monitor settings are selected.

Recommendations for Implementing Email Monitoring in CSM

When implementing Email Monitoring in CSM, follow this guide for recommendations of how to avoid common mistakes and troubleshoot common issues.

Keep in mind the following tips when implementing Email Monitors:

- Avoid having multiple customer records in CSM with the same name. Duplicate records may cause errors if an email comes in from an email address matching one of the duplicates.

- Avoid special characters in attachment names on incoming emails if possible. Special characters in email attachment names are likely to cause errors.

- Avoid allowing non-numeric characters in Incident IDs. Email Monitors may have difficulty finding Incident IDs in incoming emails when they contain letters or special characters.

- Avoid sending emails from the same email address as the recipient address. By default, emails with matching to and from addresses will be skipped. This setting can be disabled in a blueprint; however, doing so may result in a send loop. See Define General Options for an Email Monitor.

- Ensure that the monitor items for your Email Monitors are arranged in the order in which you want them to process emails. Monitor items being out of order can cause new emails to be read by the Email and Event Monitor Service, but appear not to be processed. For more information on how to adjust the order of your monitor items, see Define Monitor Items for an E-mail Monitor.

- Ensure that your email accounts' credentials are correct. Incorrect credentials will often cause the error message: "The request failed with HTTP status 401: Unauthorized." For more information on how to adjust account credentials, see Configure a Global Email Account. If you continue to see that error after correcting account credentials, please refer to the Ivanti Community for more potential solutions.

- If automated emails are common in your organization, consider including rules that skip emails in which the subject contains phrases that identify emails as automated in order to prevent infinite loops. See Configure Skip Item Rules for an Email Monitor.

- Refer to the DevExpress list of supported and unsupported HTML tags (see https://docs.devexpress.com/WPF/9136/controls-and-libraries/rich-text-editor/html-import-and-export/html-support-limitations?utm_source=SupportCenter&utm_medium=mail&utm_campaign=docs-feedback&utm_content=T987950__;) for information on appropriate tagging.

  For example, if the Email Monitor is processing a message to create a Business Object, and the message contains the following:

```
<input type="text"
value="Some text">
```

  The value

```
"Some text"
```

is stripped out and does not appear in the description because `input` is not a supported HTML tag.

Managing Email and Event Monitoring

Email and Event Monitors are managed using the Email and Event Monitoring Manager. You can create, edit, disable, delete, or pin an email monitor.

CSM currently only supports email monitoring, so the only items in the Manager are Email Monitors.

E-mail and Event Monitoring Manager

Use the Email and Event Monitoring Manager to complete general CSM Item Manager operations for Email Monitors. The small disabled icon 🛑 indicates that a Monitor is disabled. Enable/disable Monitors either by right-clicking on the item or by selecting **Disabled** from the **Edit** menu.
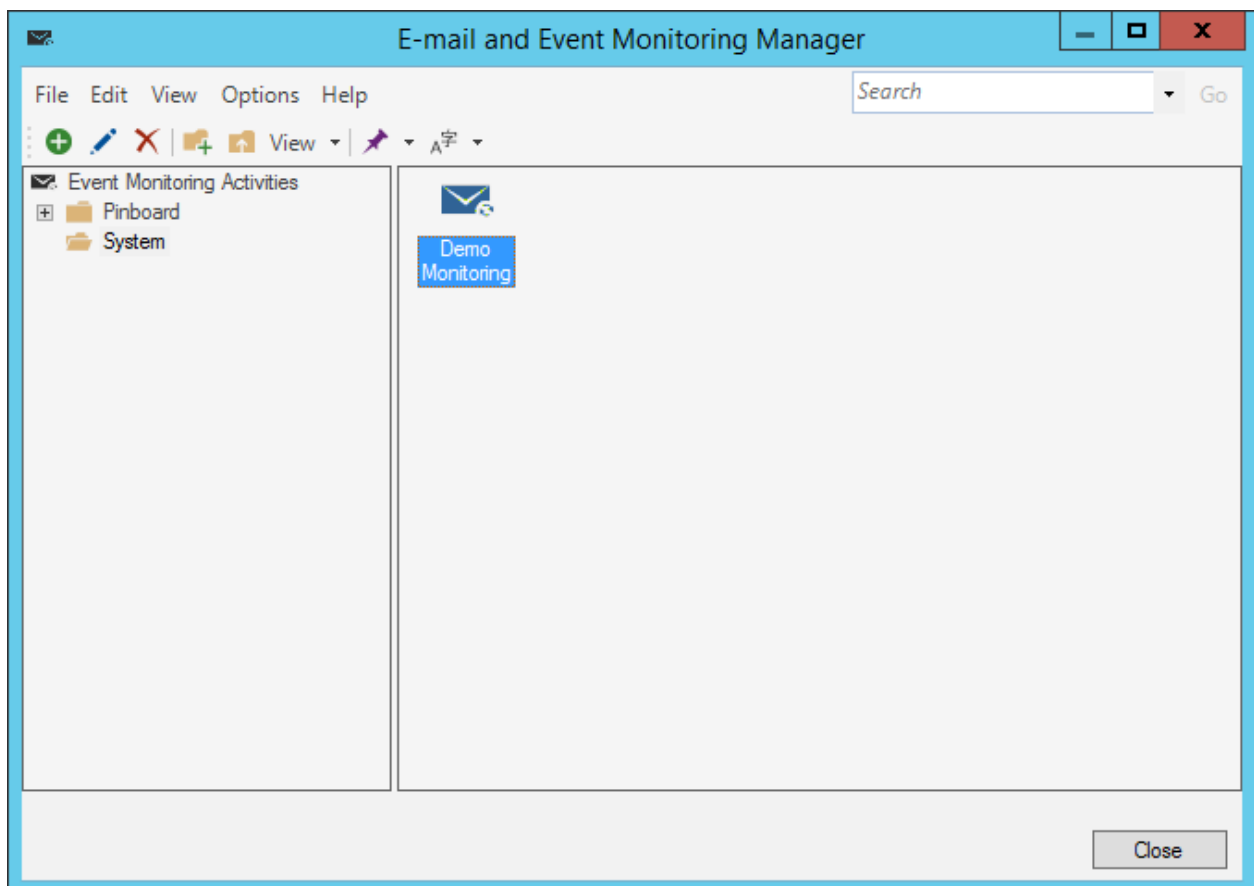
Open the Email and Event Manager

The Email and Event Monitoring Manager is located in CSM Administrator in the **Managers** menu.

To open the Email and Event Monitoring Manager:

- In the CSM Administrator main window, select **E-mail and Event Monitoring > E-mail and Event Monitoring Manager**.
- In the Blueprint or mApp Editor menu bar, in CSM Administrator, select **Managers > E-mail and Event Monitoring**.

Create an Email Monitor

Use the Email and Event Monitoring Manager to create Email Monitors to meet the specific needs of a company.

Create as many individual Monitors as required, but do not define multiple Monitors that monitor the same email account unless all but one is disabled; otherwise, the behavior of the Email Monitor is ambiguous.

To create a Monitor:

1. Open the Email and Event Manager. See Open the E-mail and Event Manager.
2. Select a subfolder (if needed).
3. Select the **Create New** button ⊕.
4. Define general options for the Email Monitor (**General** page):

    📝 **Note:** To use email monitoring, there must be at least one email account set up.

5. Define identity customer options to associate with incoming emails (**Customer Identification** page).
6. Define conditions and associated actions for a Monitor (**Monitors** page).

Define General Options for an Email Monitor

Define general options for the Email Monitor, including name, description, culture, monitor email account, account settings, and more.

Use the **General page in the E-mail Event Monitor** window (accessed from the Email and Event Monitoring Manager) to define the general settings for the Monitor.

To define general settings for an Email Event Monitor:

Option	Description
Name	Provide a name (this property can be searched in CSM Item Managers).
Description	Provide a name (this property can be searched in CSM Item Managers).
Culture	Select the culture used by the E-mail Monitor. If your system uses multiple cultures, you must create an Email Monitor for each culture. For more information, see Managing the E-mail Monitor for Multiple Cultures. **Note:** This option applies to CSM Globalization features. If only one culture is used in your system, you can ignore this setting.

Option	Description
Monitor E-mail Account	Select an email account to monitor. • Select the account drop-down list to select an existing global email account to monitor. • Select the ellipses button to open the **E-mail Accounts** window and select an existing account or configure a new one if needed. **Note:** This option is not available when you create an Email Event Monitor from a Blueprint or a mApp Solution. You can only select existing email accounts. If the email account is not found when the Blueprint or mApp Solution is published, the email account is removed and must be reconfigured on the target system. • Select the **Do not download linked images** check box to automatically discard images that are attached to an incoming email with a URL. Use this option if your server restricts outbound internet requests. Clearing this check box if your server restricts outbound internet requests causes the Email Monitor to timeout. • Select the **Allow matching to/from address (warning: may create send loop)** check box to allow processing of emails with matching to and from addresses. This option is only enabled when opened from within a Blueprint. • **Note:** If a monitored email address is not included in the **To:** field, the Email and Event Monitor Service processes emails using addresses in the **CC:** field. Email addresses in the **BCC:** field are not visible in Journal entries. To include the email address in the Journal entry, add it to the the **To:** or **CC:** field.

Option	Description
Define Account-Specific Settings This only applies if an IMAP or Microsoft Exchange account is selected as the monitored account. POP accounts do not have options for handling processed messages; they are always deleted.	Select options for how to handle processed emails and emails that cannot be processed due to an error. • **Delete:** Deletes emails after they are processed, or if an error occurs during processing. • **Mark as read:** Marks emails as read after they are processed, or if an error occurs during processing. **Note:** If this option is selected, emails are left in the monitored folder. Periodically clear the monitored folder to prevent performance issues. • **Move to folder:** Moves emails to a specified folder after they are processed, or if an error occurs during processing. Select a folder in the drop-down list.

Related tasks
Configure a Global Email Account

Customer Identification Options for an Email Monitor

Use the **Identify Customer page in the E-mail Event Monitor** window (accessed from the Email and Event Monitoring Manager) to define options for identifying Customers and associating them with the appropriate Customer and Business Object Records.

Note: The options for identifying customers are ordered hierarchically. If more than one option is selected, CSM attempts to identify customers by the first option selected, then by the second, etc. For example, if **Find Customers by E-mail Address** and **Custom** is selected, CSM attempts to find the customer by email address first; if it cannot identify a customer using that method, it attempts to identify the customer based on the Custom settings.

To define Customer Identification options:

Option	Description
Find Customers by E-mail Address	Look up the sender's email address in the email field of the appropriate Customer Object, and then specify which field CSM should search in Customer objects. • **Use Default E-mail Address Fields**: Select this radio button to have CSM look in the Customer Object (and its associated children) in the field that is marked as the email field. This is almost always the most appropriate option. **Search All Contact Manager Objects**: Select this check box to have CSM search email fields in all objects in the Contact Manager. **Note:** It is possible to include other objects in addition to the Customer Object in the Contact Manager (example: External data). If Customers are kept in an External Business Object or other custom object, then check this option to include it in the search. • **Custom Business Object or Field**: Select this radio button to have CSM always search a particular Business Object and look in a particular field to identify Customers, and then select the Business Object and Field in the drop-down lists. **Note:** This is an advanced option for use when email addresses are stored in a non-standard object for specialized use (example: A server list that sends alerts). If these are not requirements, use the Customer - Internal Business Object default.

Option	Description
Find Customers by Domain	Look up the sender's domain in a specified Business Object and Field (select the Business Object and Field in the drop-down lists). **Note:** The selected Business Object must be configured to have an appropriate field containing the domain. Create a field and either require it to be manually filled or use an Expression to determine the domain from the already-entered email address (which can be done easily using a Text After Modifier).
Custom	Use information other than the sender's email address (example: Subject) to identify Customers. In the drop-down list, select what and where CSM should search: • **Value to Find**: Select the area of the email (example: Subject) to search. • **Business Object**: Select the type of Business Object to search. • **Field**: Select the field to search in the Business Object.
Default Customer to Use	Select a default customer from the Contact Manager (select the ellipses button). CSM uses the default customer with which to associate Business Objects if the customer cannot be identified using the other methods.

Define Monitor Items for an E-mail Monitor

Define conditions and actions such as adding, deleting, editing, and copying monitor items to tell a Monitor how to process incoming emails.

Use the **Monitors** page to define Email Monitor Items.

To define Monitor Items for an Email Monitor:

Option	Description
Add	Adds a new monitor item.
Edit	Edits an existing monitor item.
Delete	Deletes an existing monitor item.
Copy	Copy the settings for an existing Monitor Item, and then edit the settings as necessary.
Up/Down Arrows	Select to change the order of the selected items. The order of the items in the list is important. The system steps through the list of conditions and actions in order, until it finds one where the condition is true, and then it executes the associated actions. The system does not evaluate any other conditions and actions once it finds one to execute. **Note:** The order of Skip Certain Items (always appears first) and Default (always appears last) cannot be deleted or rearranged.

Configure Email Monitor Behaviors

Monitor items, with their associated conditions and actions, are at the heart of Email Monitors. Monitor items determine how a Monitor behaves.

When it finds a condition that is true, it executes the defined actions. Use the Monitors page in the **E-mail and Event Monitor** window (accessed from the Email and Event Monitoring Manager) to:

- Add new Monitor Items.
- Edit existing Monitor Items.
- Delete existing Monitor Items.
- Copy an existing Monitor Item, and then edit the settings as necessary.
- Change the order of the Monitor Items (use the up/down arrow buttons).

The Monitors page lists two items by default:

- Skip certain items: Configure rules for eliminating emails that the Monitor should not process. See Configure Skip Item Rules for an Email Monitor.
- Default actions: Configure actions to execute if no other conditions in the list are found to be true. See Configure Default Actions for an Email Monitor.

Skip certain items is always at the top of the list, and Default is always at the bottom. Add new items between them. See Configure New Monitor Items. When adding a new item, define:

1. General settings for the Monitor Item: Name, description, and type of Business Object to associate with incoming emails. See Define General Settings for E-mail Monitor Items.
2. How to identify existing records: Methods that CSM uses to identify existing records to associate with incoming emails. See Define Identify Existing CSM Records Options.
3. Conditions for the Monitor: The conditions that must be met before the associated actions are executed. See Define Monitor Item Condition Options.
4. Actions for the Monitor: The actions to execute if specified conditions are true. See Define Monitor Item Action Options.

   Note: The order of the items in the list is important. The system steps through the list of Monitor Items in order, until it finds one where the condition is true, and then it executes the associated actions. The system does not evaluate any other Monitor Items once it finds one to execute.

Configure Skip Item Rules for an Email Monitor

Skip Item Rules are defined criteria that determine which emails from a monitored account are discarded (and not processed). For example, anything identified by a spam filter can be thrown out automatically.

Also, specify recipient addresses so that items such as global company announcements can be ignored (and Incidents are not created from them).

Skip Certain Items is always the first in the list of Monitor Items, and it cannot be deleted. If any of the Skip Item Rules is true (example: If the text "[SPAM]" is found in the subject), then the email message is not processed further through the list of Monitor Items. The email message itself is processed according the account-specific settings for the monitored email account (see the general settings for an Email Monitor).

Note: Define Skip Item Rules for an Outlook Integration Configuration.

To define Skip Item Rules:

1. Open the E-mail and Event Monitor.

2. Select the **Create New** button ⊕ .

   The Email Event Monitor window opens.

3. On the **Monitors** page, select **Skip Certain Items...**, and then select **Edit**.

   The **Skip Item Rules** window opens.

4. Add new, delete existing, or reorder Skip Item Rules.

5. Define criteria for the Skip Item Rules (when adding a new item):

Word/phrase	Provide the text to search for incoming emails.
Appears In	Select which part of incoming emails you want CSM to search for the specified word/phrase (example: Subject).
Anywhere	Select this radio button to have CSM search anywhere in the Appears In location for the specified word/phrase.
Begins with	Select this radio button to have CSM search the beginning of the Appears In location for the specified word/phrase.
Ends with	Select this radio button to have CSM search the end of the Appears In location for the specified word/phrase.

Configure Default Actions for an Email Monitor

The Default Monitor Item consists of actions that a Monitor performs if no other conditions are true. Default is always the last item in the list of Monitor Items, and it cannot be deleted.

The Default Monitor Item is configured the same way as a new Monitor Item, except that it has no Conditions page. Its built-in condition is that none of the actions for the other Monitor Items were executed because their conditions were not met. By default, this Monitor Item creates a new Incident from the email.

Note: If an Email Monitor should handle all incoming messages the same way, have Default as the only item (aside from Skip Item Rules) in the list of Monitor Items, and then the same list of actions are performed against every email (that passes the Skip Item Rules) received in the monitored account.

To configure the Default Monitor Item:

1. Open the E-mail and Event Monitor.
2. On the **Monitors** page, select **Default**, and then select **Edit**.
3. Define general properties for the Default item (**General** page).

   Note: The name for the Default item (Default) cannot be edited.

4. Define how to identify existing records (**ID Existing Record** page).
5. Define actions for the Default item.

Configure New Monitor Items

Use the Monitors page in the **Email Event Monitor** window (accessed from the Email and Event Monitoring Manager) to add or edit Monitor Items.

To configure Email Monitor Items:

1. Open the Email and Event Monitor. See Open the Email and Event Manager.

2. Select the **Create New** button ⊕.

3. On the **Monitors** page, select a monitor and select **Add** or **Edit**.

4. Define general options: Name, description, and type of Business Object to associate with incoming emails.

5. Define identify existing record options: Methods that CSM uses to identify existing records to associate with incoming emails.

6. Define conditions options: The conditions that must be met before the associated actions are executed.

7. Define actions options: The actions to execute if specified conditions are true.

Define General Settings for E-mail Monitor Items

Use the **General** page to define basic properties such as name, description, and Business Object for a Monitor Item.

Name	Provide a name (this property can be searched in CSM Item Managers).
Description	Provide a name (this property can be searched in CSM Item Managers).
Business Object	Select a **Business Object** to associate with the Monitor. Only one type of Business Object can be selected. The drop-down list displays only Major Business Objects. Show All: Shows all Business Objects.

Define Identify Existing CSM Records Options

Use the **ID Existing Record** page to define how the system should find existing records and associate them with incoming emails.

To define how to identify existing CSM records:

Attempt to find existing record	Select this check box before selecting any options for identifying existing records
Look for Cherwell Service Management conversation ID	CSM identifies an existing record from the Conversation ID in an email message. **Note:** This is the simplest and most reliable way of finding an existing record, but it only works if an incoming email is a reply to a CSM email. When an email is sent out from CSM, a Conversation ID can be embedded in either the message body or the subject. If the message is not a reply to a CSM message, or if the user deleted the Conversation ID, then this option does not work.
Try to match based on subject	CSM identifies an existing record based on the subject line of an email message. • Ignore Short Subjects: CSM ignores subject lines that are less than 10 characters. **Note:** For this option to work correctly, the original email must be attached to an Incident. **Note:** This option is not as reliable as using Conversation IDs. People often use similar subjects for different issues (example: have problem). Checking Ignore Short Subjects increases the reliability, as subjects with only one or two words are less likely to be unique.
Search subject for ID	CSM identifies an existing record from a Record ID in the subject of an email message. This is useful receiving messages from automated systems, or if email senders use a template that always includes the Record ID in the subject.
Look for number	CSM searches an email subject for the first whole number.
Number at end of subject	CSM searches for a number as the last item in an email subject

After term	CSM searches for a Record ID that appears after a particular term. Provide the term (example: Incident) and select either: • End of Line: Searches everything in the subject, starting from the specified term until the end of the subject. • Next Word/Number: Searches only the word or number after the specified term.
Between	CSM searches for a Record ID between two specified terms, and then provide the terms.
Search body for ID	CSM identifies an existing record from a Record ID in the body of an email message.
After term	CSM searches for a Record ID that appears after a particular term. Provide the term (example: Incident) and select either: • End of Line: Searches everything in the subject, starting from the specified term until the end of the message body. • Next Word/Number: Searches only the word or number after the specified term.
Between	CSM searches for a Record ID between two specified terms, and then provide the terms.
Ignore Closed records	Excludes closed records from the search for an existing record. **Note:** This option refers to the final state or stage of the Business Object chosen in the general settings and varies depending on the object (example: the final state for an Incident is Closed, for a Knowledge Article is Retired, and for a Change Request is Completed). If a Business Object does not have a final state (example: Approval), or final stage, then this option is not available.

Define Monitor Item Condition Options

Use the **Conditions** page to control the conditions that determine whether the associated actions are executed. The actions are executed only if all of the options selected on this page are true.

To define Monitor Item conditions:

Define the conditions that determine if the associated actions are executed.

Existing record found	Select this check box to have associated actions executed if an existing record is found (using the options selected on the ID Existing Record page).
Expression	Applies an Expression against an existing record that CSM finds. • Stored Expression: Select the ellipses button to open the Expression Manager, and then select an existing stored Expression or create a new stored Expression. Stored Expressions can be reused in numerous places in CSM. • Custom Expression: Select the **Custom Expression** button to open the Custom Expression Builder, and then create a custom Expression specifically for this scenario. **Note:** If this option is selected, actions are executed only if an existing record is found and the Expression is true.
Customer found	Associates actions are executed if a customer is identified (using the options selected on the Identify Customer page in the **E-mail Event Monitor** window). **Note:** If a default customer is specified, that counts as having found a customer.

	Select these check boxes to have associated actions executed if the specified fields and values are found.
Field/ Operator/ Value	• Field drop-down list: Select a part of the email message (example: Subject and Body Combined) to search. **Note:** Some field options seem similar, but produce different results when searching for matched values. For example, if you select the **From** field, validation is performed against a concatenation of the user's name and email address (e.g. "(Henri Bryce) henri.bryce@address.com"). If you want the validation to run against a name or email address only, choose **From (just name)** or **From (just address)**. • Operator drop-down list: Select an operator. 　◦ Equals: Finds email items where value in field equals value in right-most drop-down list. 　◦ Not equal: Finds email items where value in field does not equal value in right-most drop-down list. 　◦ Like: Finds email items where the value matches the value and its wildcard in the right-most drop-down list. For example, Jo% will find Joe, John, etc. 　　**Note:** Use % or * as the wildcard character. For example, enter John% to find all email items that start with "John." Do not use the wildcard character at the beginning of the string if it can be avoided (i.e., %SON), because the underlying database query will be very slow. 　◦ Not like: Finds all email items that do not match a value and its wildcard. 　◦ Empty: Finds all email items where the field value is empty. 　◦ Not empty: Finds all email items where the field value is not empty. 　◦ Greater than: Finds all email items where the value is greater than the value in the right-most drop-down box. 　◦ Greater or equal: Finds all email items where the value is greater than or equal to the value in the right-most drop-down box. 　◦ Less than: Finds all email items where the value is less than the value in the right-most drop-down box. 　◦ Less or equal: Finds all email items where the value is less than or equal to the value in the right-most drop-down box. 　◦ Contains: Does a SQL Server Full-Text search to find email items that contain the text in the right-most drop-down box. 　◦ Does not contain: Finds email items that do not contain the text in the right-most drop-down box. 　◦ Begins with: Finds email items that begin with the value in the right-most drop-down box. 　◦ Ends with: Finds email items that end with the value in the right-most drop-down box. 　◦ Is: Finds email items where the value in the field is an exact match to the value in the right-most drop-down box. • Value: Provide a keyword or phrase, select a date/time, etc. **Note:** The operators and values vary depending on the fields chosen. For

Define Monitor Item Action Options

Use the **Actions** page to define the actions that are executed when the specified conditions are met. The actions are executed only if all of the conditions are true.

Note: The actions defined on this page are executed in the order they appear. If one action fails, the remaining actions are not executed. However, the Monitor might still consider the email to have been handled successfully. Success is determined in the following manner: If there is at least one Create a new Business Object or Update a Business Object Action, and the first (primary) one succeeds, then the actions are considered to have succeeded. If the Email and Event Monitor is configured for logging in the Server Manager, then view these errors in the specified log. If there are no Create/Update Actions, then all of the actions must succeed for the execution to be considered successful.

To define Monitor Item Actions:

Specific Actions	
Attach e-mail to [Business Object (example: Incident)]	Attaches incoming emails to Business Objects as Journal - Mail History Records.

Import attachments as part of e-mail	Imports email attachments along with incoming emails. Options: Select this button to define rules for attachments. **Note:** File Attachment rights control the Attachment operations that can be performed in CSM. • All Attachments/Files: Select this radio button to include all Attachments/files from the selected Business Object/directory. • First: Select this radio button to include the first defined number of Attachments/files from the selected Business Object/directory. Then, provide a number or use the up/down arrows to increase/decrease the number. • Last: Select this radio button to include the last defined number of Attachments/files from the selected Business Object/directory. Then, provide a number or use the up/down arrows to increase/decrease the number. **Note:** If *First* or *Last* is selected, Attachments/files are sorted in alphabetical order if they are from a directory, and by the order of appearance on the Business Object's Attachment Bar if they are from a Business Object. • Include Attachment/File: Select this check box to include Attachments/files based on file masks (include Attachments/files that contain certain characters, words, file extensions, etc.). Then, specify the file masks, using semicolons to separate each mask. • Exclude Attachment/File: Select this check box to include Attachments/files based on file masks (include Attachments/files that contain certain characters, words, file extensions, etc.). Then, specify the file masks, using semicolons to separate each mask. • Minimum Size: Select this check box to include Attachments/files that are of a minimum defined size. Then, provide a number or use the up/down arrows to increase/decrease the number. In the drop-down list, select kilobyte or megabyte. • Maximum Size: Select this check box to include Attachments/files that are of a maximum defined size. Then, provide a number or use the up/down arrows to increase/decrease the number. In the drop-down, select kilobyte or megabyte.
Attach e-mail attachments to [Business Object (example: Incident)]	Attaches email attachments to Business Object Records (not just to the internal copy of the e-mail). **Note:** If this option is selected, email attachments are stored in Business Object Records as Attachments. For additional information, refer to the Attachments.

Preserve inline images within e-mail body	Preserves images within the body of incoming emails with the text of the email. **Note:** The target Field must be configured to store Rich Text for this to work correctly.
Attach inline images to [Business Object (example: Incident)]	Attaches images within the body of incoming emails to the selected Business Object.
Attach e-mail to Customers	Attaches incoming emails to Customer Records as Journal - Mail History Records. Select the **Options** button to define which Customer Records to attach emails to: • **Attach to Customer (From Address)**: Select this check box to attach emails to Customer Records that are identified from the addresses in the From line. • **Attach to Customers in Cc Line**: Select this check box to attach emails to Customer Records that are identified from email addresses in the CC line. • **Attach to Parents of Customers** (example: company that contact works for): Select this check box to attach emails to Parent Records of Customer Records (example: If an email sender is a contact that works for a particular company, the email can be attached to the Company Record as well as the Customer Record). **Note:** This capability, along with the ability to attach to a particular Business Object, can mean that an incoming email is attached to a specific Incident, the Customer who sent the email, other Customers who were also CC'd on the message, and even to the company for whom the Customer works. This powerful feature means that the communication history about a particular record can be seen or all communication from a particular Customer or company (although, of course, there is the potential for significant overhead).
Store e-mail as plain text	Discards Rich Text formatting contained in incoming emails and stores them in the Journal - Mail History Record as plain text. Do this to reduce the amount of space used by messages.
Define Custom Actions	

Add	Select to select actions from a list. The following actions are available: • Create New [Business Object (example: Incident)]: Creates a new Business Object Record (of the type selected in the General page of the Event Monitor Condition and Action window) based on information from incoming e-mails. Specify which Fields are populated with email contents and the values of those Fields. To retrieve data from within an email message, insert the appropriate Email Contents item (example: body) into the Template section of the Field to populate (Selector button>E-mail Contents, or right-click>E-mail Contents), and then right-click the Token and select Modifiers. Use Modifiers such as Text After and Text Between to extract the text wanted from the email message. If no options are selected any options for identifying an existing record and an existing Business Object is not updating, it is typical (though not required) for the first action to be Create New [Business Object (example: Incident)]. Otherwise, no record is created for other actions to run against. • Update [Business Object (example: Incident)]: Updates a Business Object Record (of the type selected in the General page of the Event Monitor Condition and Action window) with information from incoming emails. Specify which Fields are updated and the values of those Fields. Defining custom actions is not needed to have an email attached to a Business Object Record as a Journal - Mail History Record. Selecting the Attach email to [Business Object (example: Incident)] check box is sufficient and frequently all that is needed. • Add to a Queue: Determines which CSM Queue the Business Object Record (of the type selected in the General page of the Event Monitor Condition and Action window) is added to (example: New Request Queue) after it is created or updated. Select the ellipses button to open the Queue Manager and select a Queue. • Run a One-Step Action: Runs a One-Step Action related to the Business Object Record (of the type selected in the General page of the Event Monitor Condition and Action window). Select the ellipses button to select an existing One-Step Action or create a new one. If a One-Step Action is created or edited from here, that One-Step Action has access to email-specific data, such as the email address of the sender, the subject line, etc. If the One-Step Action is created elsewhere and needs to reference One-Step Action Tokens, set Show Custom Tokens to Email on the Conditions page of the One-Step Action.
Edit	Edit the highlighted section.
Copy	Create a copy of the selected action.
Delete	Delete the selected action.
Up/Down Arrows	Change the order of the selected actions.

Note: To exclude all email attachments from the database, you must clear all these options:

- Import attachments as part of email
- Attach email attachments to Incident
- Attach inline images to Incident

Disable a Monitor

Disable a Monitor if it has a problem or if there is a need to apply special handling for certain situations (such as emergencies). For example, define an emergency Monitor and disable it until needed. When enabling an emergency Monitor, disable the regular Monitors.

Use the Email and Event Monitoring Manager to disable specific Monitors.

Good to know:

- Disabling a specific Monitor only disables a specific Monitor that is selected. It is not the same as pausing the Email and Event Monitor Service, which affects all enabled Monitors.
- When an Email Monitor is disabled, the monitored email account continues to receive emails. However, those emails are not processed according to the rules in the disabled Monitor.

To disable an Email Monitor:

1. Open the E-mail and Event Monitor.
2. Select the **Monitor** to disable.
3. Select **Edit > Disabled** (or right-click and select **Disabled**).

   The selected Monitor is disabled, and a disable icon appears on the item in the Email and Event Monitoring Manager.

Pause/Resume Email and Event Monitor Service Processing

Use the Pause/Resume Monitoring task in CSM Administrator to temporarily pause, and then resume Email and Event Monitor Service processing.

Pausing the service does not stop the Email and Event Monitor Service; rather, it suspends the service so that, when resumed, the service can pick up where it left off. Pause processing to suspend processing emails from monitored accounts, or resume processing to continue processing emails, starting with emails that are received from that point forward. The ability to pause or resume monitor processing is controlled by Email and Event Monitor security rights.

To pause or resume Email and Event Monitor Service processing:

1. In the CSM Administrator main window, select the **E-mail and Event Monitoring** category, and then select the **Pause/Resume Processing** task.
2. Select to pause or resume:
   a. **Pause E-mail and Event Monitor Server**: Select this check box to pause processing. Provide a reason for pausing processing.
   b. **Resume E-mail and Event Monitoring Server Processing**: Select this check box to resume processing.
3. Select **OK**.

Configure a SMTP Relay Server Connection for Microsoft Outlook

Use the Server Manager to create a Simple Mail Transfer Protocol (SMTP) Connection to avoid possible Automation Process Service overload. If numerous e-mails are automatically sent from associated Outlook accounts, a SMTP Relay Server allows outgoing e-mails to be distributed between multiple server queues. Doing so prevents possible server overload by transferring e-mails from the Automation Process Service to the SMTP Relay Server.

A SMTP Relay Server Connection requires a Web Server (IIS) Connection. During SMTP installation, users are prompted to install or upgrade the IIS Connection if needed. For more information about configuring mail Relay Connections, visit Microsoft's website.

To create a SMTP Relay Server Connection:

1. Install the SMTP Server Role:
   a. Open the Server Manager: Click **Start > Run > Server Manager > OK**.

   b. Click the **Manage** drop-down.

   c. Click **Add Roles and Features**. The Add Roles and Features Wizard opens.

   d. Click the **Next** button on the Before You Begin section.

   e. Select the **Installation Type** radio button (example: Role-based or feature-based installation).

   f. Click **Next**.

   g. Select a **location** for the Roles to be installed (example: Select a server from the server pool).

   h. Select the **name** of the **location** from the Server Pool field (example: SERVERNAME05).
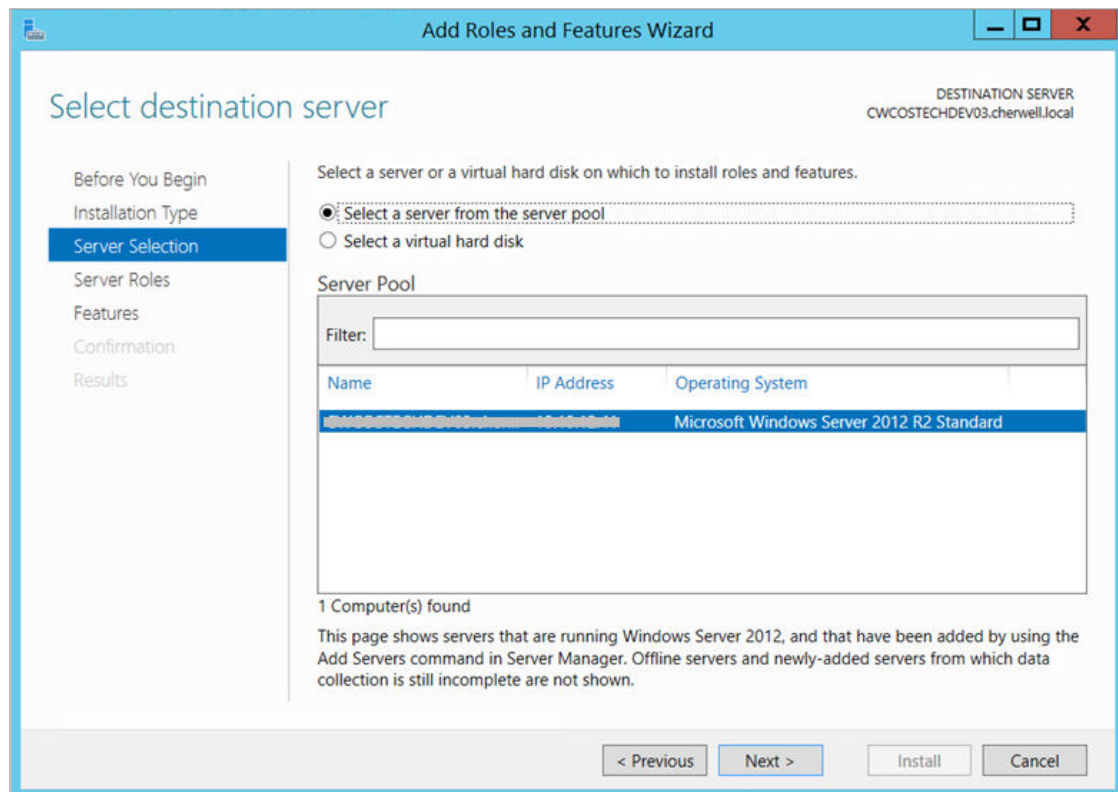
i. Click **Next**.

j. Server Roles:
   i. Click **Next** to accept the default Role selections or customize the selections based on your organization's needs.

k. Features Section:
   i. Select the **SMTP Server** radio button. An informational pop-up displays and specifies features of the SMTP server.

   ii. Select **Add Features** to accept these features.

l. Click **Next**.

> ⭐ **Important:** Depending on your server version, you may be prompted to install additional required features for the SMTP Server Connection before installation can occur. Click **Add Features** on the notification window to also install the required components.

m. Review the summary of changes and click **Install**.

n. Click **Close** after the installation is finished.

2. Configure the SMTP Server:
   a. Open the Internet Information Services: **Start > Internet Information Services (IIS) Manager**.

   b. Ensure an SMTP Virtual Server connection is populated the left-hand navigation pane.

c. If the SMTP Server Connection is missing, right-click on the **computer name**. If the SMTP Server Connection already exists, move to Step M.

d. Select **New > Virtual Server**. The New SMTP Virtual Server Wizard opens.

e. Provide a unique name for the server.

f. Click **Next**.

g. Select an **IP Address** from the drop-down.

h. Click **Next**.

i. Select a **Home Directory** from the drop-down.

j. Click **Next**.

k. Provide a **Default Domain** name for the virtual server.

l. Click **Finish**. The new SMTP Virtual Server name now populates the left-hand navigation pane.

m. Right-click on the **SMTP Server Connection name** and select **Properties** to customize the Server Connection to fit your organization's needs.

> **Important:** Virtual Server settings are extremely important if your Relay Server is connected to the Internet. Security breaches can occur from spam and malware being sent via an open-Relay Server. We recommend careful customization and working alongside your organization's Security Team to ensure the Virtual Server Connection is Security Compliant.

n. Customize the following Properties:
   i. **General Tab**: Provide a **Connection time-out limit** (example: 10 minutes).

   ii. **Access Tab**: Control forms of **Authentication** accepted by the server and establish **IP Address** or **Internet domain** access rights.

   iii. **Messages Tab**: Provide data for e-mail messaging limits or accept the default settings.

   iv. **Security Tab**: Click **Add** to establish which Window's user accounts are allowed to access the server.

Add a SMTP Relay Server Connection to CSM

After establishing an SMTP Relay Server Connection, use CSM Administrator to configure CSM so that it directs emails to the Server connection.

To configure CSM for the SMTP Relay Server Connection:

1. In CSM Administrator, select the **Email and Event Monitoring** category.
2. Select **Edit -mail accounts and settings**. The **Email Options Manager** opens.
3. Select **Add > IMAP Account**.
4. Provide a **Name** for the IMAP account.
5. Provide a **Name** for the Incoming mail server.
6. Select the **Outgoing Server** section.
7. Provide the **Name of the Virtual Server** in the Outgoing mail server field.

   > **Note:** It is recommended to use the name of your Virtual Server rather than an IP Address due to the fact that IP Addresses could change. However, both can be used in the Outgoing mail server field.

8. Select the **From Addresses** section.
9. Select the **Allow user's email address** radio button.
10. Select the **Allow arbitrary FROM adresses** radio button.
11. Select **Add** to provide a FROM address. A Legal Return Request pop-up displays.
12. Provide an email address in the **Email Address** field.
13. Select **OK**.
14. Select **Test Account** to ensure the provided email address complies with the Server Relay.
15. Select **OK** to save the changes and close the IMAP Account Manager.
16. Select **OK**.

Once the SMTP Relay Server Connection has been established and added to your CSM Administrator content, emails sent through CSM Administrator are automatically sent via the Relay Server Connection. To send an email from the CSM Desktop Client, select **File > Send Email** to open and send a new email message.

System Analyzer

The System Analyzer is a tool that allows you to track behind-the-scene operations in a live environment directly from the CSM Desktop Client. Open the System Analyzer in the CSM Desktop Client (**Help > System Analyzer**).

Related concepts

System Analyzer Message Categories

Best Practices for Performance

Guidance for System Reliability and Stability

Related tasks

Define System Analyzer Messages

About the System Analyzer

Use the System Analyzer to track operations, including messages related to Business Objects and load timing, table validation and load timing, execution of One-Step™ Actions, system exceptions and errors, and technical logging information.

You can track all messages or define breakpoints to pause the application when a specific message is found. The System Analyzer allows you to step through operations individually to see what is happening behind-the-scenes.

Security rights control access to CSM functionality and are configured in the Security Group Manager in CSM Administrator (**Security > Edit Security Groups**). System Analyzer security rights are grouped with Tools security rights. For more information, see Security rights and Configure Tools Security Rights.

Related concepts
System Analyzer Message Categories
Best Practices for Performance
Guidance for System Reliability and Stability
Related tasks
Define System Analyzer Messages

System Analyzer Window

The **System Analyzer** window opens independent of the CSM Desktop Client (**Help > System Analyzer**).

Use the window to:

- Start/stop the System Analyzer.
- Run/pause the System Analyzer.
- Manage message categories.
- Define latency.
- Define breakpoints.
- View fields and values in the active Business Object.
- Export message data.
- Clear messages from the window.

In the main pane, view operation information:

- **Timestamp**: Date and time that the System Analyzer intercepted the operation.
- **Category**: Category of the message (examples: Business Object, table validation)
- **Type**: Type of definition (examples: relationship, field)
- **Name**: Name of the definition (examples: Incident Links Similar Incidents, Incident.ServiceID.)
- **Message**: Description (details) of the operation.

Related concepts
About the System Analyzer
System Analyzer Message Categories
Related tasks
Define System Analyzer Messages

System Analyzer Message Categories

The System Analyzer uses categories to classify the messages listed in the main pane, which makes it easy for you to filter the information.

Good to Know:

- Before you run the System Analyzer, define the message categories that you want to track.
- The following message categories are selected by default: Business Object, BusOb Load Timing, Error, One-Step™ Action, Table Validation Timing, Token Expression Error, and Web Service Call. Messages are not selected by default if they generate a large number of messages or are only applicable for 2-tier or 3-tier systems.

The System Analyzer uses the following categories:

Category	Description	Example
Action Block	Logs Execution Begin, Execution End, Value Input (parameters), and Value Output (parameters).	
Adaptive Layout	Logs when Business Object forms are resized.	
App Service call	Tracks calls that have been made from the CSM Desktop Client to the Application Server. This type of message is only applicable if you are running a 3-tier system. Logging this type of message might cause unexpected results (example: Pausing on a remote call might cause timeout errors).	
Business Object	Tracks Business Objects, including fields and relationships. Use these messages to find issues related to field changes.	(Incident.Location) value set to "Colorado Springs."
BusOb Load Timing	Tracks the amount of time that Business Object operations require to load. Use these messages to track messages related to loading Business Objects and their relationships. It can also be used to improve efficiency by eliminating or grouping operations.	(Customer - Internal) Retrieved Business Object: Tracy E. Aubin, Time: 0.0320019.
Error	Tracks various system exceptions and errors.	
Foreign Key	Logs values set for foreign key fields.	
Foreign Key Potential Issue	Logs when an expected foreign key does not display.	
Modify Value	Tracks changes to modifier values.	
One-Step	Tracks the execution of One-Step Actions.	(Select User) About to execute step Select User.

Category	Description	Example
Other	Tracks all other miscellaneous messages. These messages are often dependent on the type of system (2-tier or 3-tier) you are running.	
Query (2-tier only)	Tracks the execution of queries. This type of message is only applicable if you are running a 2-tier system.	
Session	Tracks session information.	
Table Validation	Tracks field validation values, which might read from the local cache or cause queries to the database.	Querying for a Lookup value in data cache for Incident Type.Incident Type: Valid value found.
Table Validation Timing	Tracks the amount of time that table validation operations require. Use these messages to improve performance by either changing the behavior or marking tables as cacheable.	Retrieved single row for Service.Service Name table validation request: 0.052003.
Token Expression Error	Tracks token expressions. Token expressions are used for building text and number expressions, which replace tokens and evaluate the results. These expressions are also used to build text (example: Incident.Category). While this is allowed, it can cause performance issues (particularly on forms with multiple token expressions). A check box in the Expression Editor indicates whether or not the expression is calculated. If the token expression error message opens in the System Analyzer, it might indicate that this check box should be cleared.	Non-valid token Expression evaluation for Field Incident.Matching Text. Value: Printing.
Web Service Call	Tracks details related to calls made by the web service One-Step Action.	

Related concepts
Best Practices for Performance
Guidance for System Reliability and Stability
Related tasks
Define System Analyzer Messages

Use the System Analyzer

Use the System Analyzer in the CSM Desktop Client to stop and start the analyzer, view a read-only list of fields and values in an active Business Object, and export message data. You can also define messages, latency, and breakpoints.

Related concepts

Configuring the System Analyzer

Best Practices for Performance

Guidance for System Reliability and Stability

Open the System Analyzer

To open the System Analyzer from the CSM Desktop Client menu bar, select **Help > System Analyzer**.

Related concepts
Use the System Analyzer
Configuring the System Analyzer

Run the System Analyzer

Use the **System Analyzer** window to run the System Analyzer. By default, message tracking begins immediately. The System Analyzer only runs when the **System Analyzer** window is open.

Good to Know:

- You can stop tracking messages at any time by selecting the **Stop** button.
- If the System Analyzer is stopped, select the **Start** button to begin tracking messages.
- Clear messages from the **System Analyzer** window at any time by selecting the **Clear** button.

To run the System Analyzer:

1. Open the System Analyzer from the CSM Desktop Client (**Help > System Analyzer**).
2. Optionally, configure the System Analyzer:
   ◦ Define which messages to track.
   ◦ Define latency.
   ◦ Define breakpoints.
3. In the CSM Desktop Client, reproduce the issue that you want to test. For example, open an Incident.
   A list of messages appear in the System Analyzer main pane.
4. Optionally, navigate breakpoints using the System Analyzer toolbar:
   ◦ Select the **Pause** button to temporarily stop processing operations.
   ◦ If paused, select the **Next Message** button to step to the next operation.
   ◦ If paused, select the **Run** button to run the System Analyzer until the next breakpoint.
5. Optionally, double-click a message in the **System Analyzer** window to view details (example: Category, type, name, ID, and message).

Related tasks
Define System Analyzer Messages
Define System Analyzer Breakpoints

View Business Object Fields

Use the **Current Object Values** window to view a read-only list of fields and values in an active Business Object directly from the **System Analyzer** window, rather than modifying forms to show all fields or using One-Step™ Action prompts to show relevant data while troubleshooting.

Good to know:

- A Business Object record (example: Incident) must be open to view fields and values.

- All fields are read-only. Security rights control which fields you can view.

- To enable the ability to copy a value to the clipboard, select a value in the **Value** column, and then double-click the value or press **F2**.

To view Business Object fields and values:

1. With an active Business Object record open in the CSM main window, open the System Analyzer (**Help > System Analyzer**).
2. Select the **Business Object Field Values** button.
   The **Current Object Values** window opens.
3. Optionally, define how field values are displayed.
   - Select the **Show/Hide Fields** button to show or hide fields that do not have values.
   - Select the **Sort Fields** button to sort fields in folders based on type (example: SLA, Status, Time Tracking, etc.).
   - Select the **Relationships** button to specify whether or not all Business Object relationships should be loaded.

     Note: If you do not select this option, only the relationships with data that has been loaded will display in the **Current Object Values** tree. If you select this option, the **Current Object Values** tree will execute a query against all relationships and cause records to be loaded, even if the relationships have not yet been referenced. Selecting this option might cause additional loading time, and can potentially alter expected behaviors because it affects the order in which operations occur. After this option is selected, clearing it will not affect the current record, since the relationship data will already be displayed. However, it will affect the data displayed for the next record that you view.

4. Select **Close**.

Related tasks
Run the System Analyzer
Define System Analyzer Messages
Define System Analyzer Breakpoints

Export System Analyzer Data

Use the **Export System Analyzer Messages** window (accessed from within the **System Analyzer** window) to export data to share information across systems.

Data can be exported to .csv and .xlsx file formats.

Use the **Up** and **Down** arrows to organize the data in the pane. Data displays in this order in the exported file.

To export System Analyzer data:

1. Open the System Analyzer from the CSM Desktop Client menu bar (**Help > System Analyzer**).
2. Select the **Export Messages** button.
   The **Export System Analyzer Messages** window opens.
3. Select the **Browse** button, and then navigate to a file location for the data.
4. Use the **Right** and **Left** arrows to select the columns you want to export. Items in the **Selected Columns** pane are exported.

   Note: All columns are selected by default.

5. Select **OK**.

The data is exported to the defined file location.

Related tasks
Run the System Analyzer

Configuring the System Analyzer

Configure how to track System Analyzer messages, define latency simulation, and set breakpoints to help you analyze messages more easily.

Related tasks
Run the System Analyzer

Define System Analyzer Messages

Use the **Analyzer Messages** dialog box (accessed within the **System Analyzer** window) to define which messages to track.

Good to Know:

- Only the following message categories are not selected by default: App Service call (3-tier only), Other, and Query. Messages are not selected by default if they generate a large number of messages or are only applicable for 2-tier or 3-tier systems.

- Select the **Clear** button to clear all options and select the **Select** button to select all standard options.

To define which System Analyzer messages to track:

1. Open the System Analyzer in the CSM Desktop Client (**Help > System Analyzer**).

2. Select the **Messages** button ⊞.
   The **Analyzer Messages** window opens.

3. Define message categories by selecting or clearing the corresponding check boxes:
   - Action Block
   - Adaptive Layout
   - App Service call (3-tier only)
   - Business Object
   - BusOb Load Timing
   - Error
   - Foreign Key
   - Foreign Key Potential Issue
   - Modify Value
   - One-Step
   - Other
   - Query (2-tier only)
   - Session
   - Table Validation
   - Table Validation Timing
   - Token Expression Error
   - Web Service Call

Related concepts

System Analyzer Message Categories

Best Practices for Performance

Guidance for System Reliability and Stability

Define System Analyzer Latency

Use the **System Analyzer Options** dialog box (accessed within the **System Analyzer** window) to define the amount of network latency that you want to simulate.

Good to know:

- Define latency to capture accurate timing data related to CSM operations to understand how latency will affect system performance. This option is helpful as you locally develop a system that will be deployed to clients that are geographically remote from the server.
- Use networking tools (example: Tracert or Ping) to determine the actual latency between the client and server before defining the simulated latency in the System Analyzer.
- When the **System Analyzer** window is closed, simulated latency is disabled, but not cleared. When the System Analyzer is reopened, the defined latency is enabled until you clear the **Add Network Latency** check box in the **System Analyzer Options** dialog box.

To define System Analyzer latency:

1. Open the System Analyzer in the CSM Desktop Client (**Help > System Analyzer**).

2. Select the **Options** button [wrench icon].
   The **System Analyzer Options** dialog box opens.

3. Select the **Add Network Latency** check box.

4. Select the **Up** or **Down** buttons to define latency in 50 millisecond increments.

5. Select **OK**.

The defined latency displays in the **System Analyzer** window.
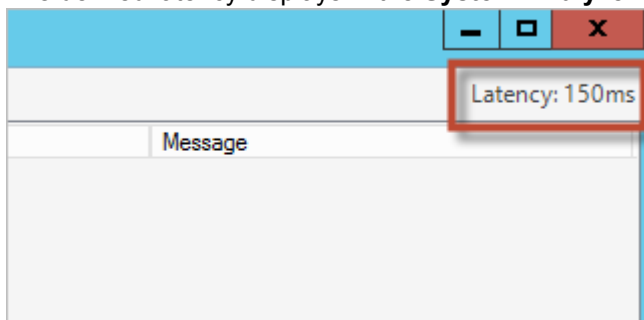
Related tasks
Run the System Analyzer
Define System Analyzer Messages
Define System Analyzer Breakpoints

Define System Analyzer Breakpoints

Use the **Breakpoints** dialog box (accessed within the **System Analyzer** window) to define breakpoints, which pause messages when a specific operation is found.

Good to know:

- Messaging will not pause for breakpoints unless the System Analyzer is open and running.
- During the pause, you can examine the data to determine if the application is functioning as expected, and then step operation by operation to see what is happening behind-the-scenes.
- Delete all breakpoints from the list by selecting the **Delete** button.
- Clear all breakpoints by selecting the **Clear** button.
- Select all breakpoints by selecting the **Select** button.
- If a breakpoint is cleared, the System Analyzer will not stop when the breakpoint is encountered during a process. This allows you to save commonly used breakpoints in the **Breakpoints** dialog for later use.

To define a System Analyzer breakpoint:

1. Open the System Analyzer in the CSM Desktop Client (**Help > System Analyzer**).
2. Select the **Breakpoints** button.
   The **Breakpoints** dialog box opens.
3. Select **Add**.
   The **Edit Breakpoint** dialog box opens.
4. Define the breakpoint.
   a. From the **Category** drop-down list, select a category (example: Business Object). To search all categories for the breakpoint, select **(Any)**.
   b. In the **Look for** box, specify text (example: Name, ID, or any other text) to serve as the breakpoint (example: ServiceID).
   c. Select **OK**.
5. Select **OK**.

Related tasks
Run the System Analyzer
Define System Analyzer Messages
Define System Analyzer Latency

Performance

Cherwell® Service Management is architected to meet the demands of global, distributed organizations that handle a high volume of transactions. To ensure ongoing responsiveness and stability over high-demand workloads, the Cherwell Performance Team conducts regular testing using environments configured to ensure comparative results across multiple versions of CSM.

Test results for specific versions of CSM may be available on request.

In addition to Cherwell-conducted peformance testing, CSM provides tools that enable you to to view, analyze, and optimize performance.

Performance best practices are also provided to help you review your system and analyze specific performance issues.

Related concepts
Best Practices for Performance
About Performance Health Check
Creating Indexes

Best Practices for Performance

For best results, periodically review performance best practices to analyze and troubleshoot performance issues.

Advice on performance is also available for the following specific areas:

- Business Objects (see Business Object Performance).
- Automation Processes (see Performance Considerations for Automation Processes).
- Cherwell REST API (see Cherwell REST API Performance).
- Relationships (see Relationships and Performance).
- Form Arrangement tabs (see Define General Tab Properties for a Form Arrangement).
- Widgets (see Add a Widget to a Dashboard (General)).

Determine the Affected Location

Investigate if the entire system or a specific area of the system is perceived as slow. Specific areas might include:

- CSM Desktop Client
- CSM Administrator (example: Blueprint publishing)
- CSM Browser Client
- CSM Portal
- Certain Business Objects (example: Incident, Change Request)
- Dashboard content
- One-Step™ Actions
- Internal databases (example: CMDB)
- External databases (example: Active Directory, SCCM)
- External tables

In addition, determine if the slowness is perceived in one of the following environments:

- Geographic location: Offices in other cities, states, or countries.
- Remote employees: Employees who are connecting via wireless, using a VPN, or working from home.
- Hosted or on-premises: Installation method of the affected environment.

Evaluate the Installation Configuration

Ideally, Cherwell server components should run on a dedicated machine. However, some customers may co-locate CSM with other applications or utilities. In this case, you must consider these additional applications or utilities when assessing performance.

Investigate the installation configuration of the affected environment, which affects how you analyze performance and who implements the recommendations. After connecting to the environment (either via the hosted server or via a remote session), consider the following:

- Load balancing.
- Available memory.
- Available disk space.
- Subscription numbers.
- Number of processors.
- Other installed applications.
- Separate installed applications.
- Distribution of servers (on one machine or several).
- Available Central Processing Units (CPUs).

Note: If you are using a virtual machine, ensure that all memory and CPUs are dedicated.

Note: For information on minimum and recommended server configurations based on the number/ type of CSM Clients, see Scaling CSM.

CSM uses a dedicated message queue system to allow horizontal and vertical scaling for one or more server components. Scaling CSM enables the system to use a network of machines to distribute work, providing more resources to alleviate barriers and improve availability. For more information, see:

- About the Cherwell Service Host
- Scaling the Cherwell Service Host

Assess Resource Consumption

Determine how resources such as available memory and the number of processors are being used. If the performance issue is acute, restarting a Server might provide a resolution. If the issue is chronic, resources might need to be increased or expanded.

SaaS customers must contact Cherwell Support for resource requests.

Investigate the Network Environment

If you determine that there are sufficient resources, consider the network environment, including the network path between users and the server. Pings, TraceRoutes, and Packet evaluations can help identify the existence of an issue and diagnose complications with remote locations. After investigation, if you suspect that a network issue is affecting performance, consider searching for common indicators (example: All affected users are using wireless or accessing the VPN).

Run the System Analyzer to Evaluate Business Object Structure

You can use the System Analyzer to determine which aspects of the Business Object structure are impacting performance. For example, determine if Business Object relationships are loading in a way that impacts performance. For more information, see About the System Analyzer.

Evaluate Automation Processes

Automation Processes provide great power, but if they are not optimized for best performance, they can cause heavy loads on the Automation Process Service. See Performance Considerations for Automation Processes for guidance.

Assess Memory and CPU Usage

Investigate your server memory and CPU usage to determine if either factor is affecting performance. Access this information by right-clicking the Windows Task Bar, selecting **Start Task Manager**, and selecting the **Performance** tab. When you have the data, consider the following:

- Memory usage should not consistently rise above 80%. Consider that even though system memory is in the normal range, a server (example: Automation Process Server) might be running higher than expected.
- CPU usage should not consistently rise above 80%. Consider that CPU does not necessarily negatively impact performance, so consider other potential issues, as well.

Common issues that impact memory and CPU include:

- Setting logging to both Splunk and a file.
- Running a Report that uses all Application Server resources.
- Using an Automation Process continuously, which causes the Automation Process Service to use additional resources.

If you notice memory spikes when loading an SLA record, specifically, the configuration of the SLA Business Object could be causing the issue. The Breached Incidents and Open Incident alert bars in the Quick Info Tile use an aggregate expression with a Count function to determine the number of records for each category; this can cause the system to reference a large number of records, which can result in a memory leak and issues with the Application Server.

To resolve this issue, remove the aggregate expressions from the Form. If you do not want to remove the expression, consider adding an attribute with the name RecalculateSetDirty to the field; this identifies the record as saved after the expression on the field is run. You can use this solution for any fields that contain an aggregate expression with a Count Function.

Implement Database Maintenance Actions

Define database maintenance Actions using the Scheduler to perform selected database maintenance operations on a scheduled basis (for more information, see Define Database Maintenance Action Options). Using these Actions, you can:

- **Rebuild Full-Text Search catalog**: Rebuild the Full-Text Search catalog when the database maintenance Action is run. CSM uses Full-Text Search for Quick Search and Knowledge Search. If you have problems with your index getting corrupted, you might want to rebuild the search catalog once a week or every night.

- **Rebuild Business Object indexes**: Rebuild Business Object indexes when the database maintenance action is run. This option allows you to rebuild the indexes of the database tables that represent particular Business Objects. Then, select the **Select** button to select which Business Objects to re-index.

  Note: By default, all Business Objects are selected. Clear Business Objects to exclude them from reindexing, or select **Clear All** to clear all Business Objects, and then select the ones you want to re-index. If you have a high volume of data, you might want to rebuild your table indexes monthly.

- **Rebuild system table indexes**: Rebuild the indexes of the SQL Server tables associated with CSM system tables when the database maintenance action is run. These tables start with "Trebuchet" (the internal code name for the product). If you have a high volume of data, you might want to rebuild your table indexes monthly.

- **Shrink SQL event log**: Shrink the SQL Server event log file when the database maintenance action is run.

  Note: Consult with your Administrator before scheduling this option. If in doubt, do not use this feature unless you run into problems.

- **Refresh Queue status**: Refresh Queue status when the database maintenance action is run. Queue status can get out of sync if Business Objects that were on Queues are deleted. This option ensures that each Queue is synchronized. We recommend scheduling this weekly.

- **Remove unused user accounts**: Remove data associated with deleted user accounts when the database maintenance action is run. When user accounts are deleted from the system, their authorization information might not be removed. This option ensures that the authorization information is in sync with the user list by removing the unused information. We recommend scheduling this weekly.

- **Synchronize Team Info with team list**: Synchronizes the Team Info Lookup table with CSM user and customer team list.

- **Run SQL Traces**: Run traces on your SQL using a tool such as SQL Server Management Studio. This helps you to identify problematic or slow SQL queries that may be causing poor application performance. For more information on using SQL profilers to run SQL traces, see Microsoft documentation: https://docs.microsoft.com/en-us/sql/tools/sql-server-profiler/sql-server-profiler?view=sql-server-ver15

  Tip: If you have a lookup table including between 50-100 rows with values that will not change (example: statuses such as open, closed, and so on), we recommend that you mark those Business Objects as cacheable. The system stores these records in memory and will not fetch them from the database. If you modify these values, however, you should restart the system.

Mitigate Database Growth

Use the E-mail Monitor, Blueprint Publish Log, and Automation Process Log to reduce database growth. When emails are imported into your system, large attachments can contribute to increased database size. To keep database growth caused by email attachments under control, you can prevent attachments being imported and control their size by using the E-mail Monitor Actions.

You can define the following settings for each monitor:

- **Attach email to [Business Object (example: Incident)]**: Attaches incoming emails to Business Objects as Journal - Mail History Records.
- **Import attachments as part of email**: Imports email attachments into the database along with incoming emails and allows you to define Attachment settings such as type and size.
- **Attach email attachments to [Business Object (example: Incident)]**: Attaches email attachments to Business Object Record's Attachment bar (not just to the internal copy of the email).
- **Preserve inline images within email body**: Preserves images within the body of incoming emails with the text of the email.
- **Attach inline images to [Business Object (example: Incident)]**: Attaches images within the body of incoming emails to the selected Business Object.
- **Attach email to Customers**: Attaches incoming emails to Customer Records as Journal - Mail History Records.

🖉 **Note:** For more information, see Define Monitor Item Action Options.

Using the Blueprint Publish Log (for more information, see View the Blueprint Publish Log), you can reduce the size of the TrebuchetPublishLogs system table, which holds historical publishing data. Before clearing the data, ensure that you have the information you need. Clear the log using CSM Administrator by selecting **File > Clear** in the **Publish Log** window.

Using the Automation Process Publish Log (for more information, see Monitor Automation Process Statistics), you can reduce the size of the TrebuchetProcesses system table, which holds historical publishing data. Clear the log using CSM Administrator by selecting **File > Clear All Processes > Clear Completed Item History** in the **Automation Process Statistics** window.

Investigate Browser Configurations

If the Browser Client loads more than a few seconds slower than the Desktop Client, determine if any system configurations are impacting performance. Consider the following when investigating the issue:

- Server memory and CPU usage can cause performance issues with the Browser Client. For more information, review the standards in Assess Memory and CPU Usage.
- Calendars can cause performance issues due to the amount of data that refreshes each time a Calendar is opened.
- Automatic Actions can cause issues because the Save Actions are executed before the Save occurs. Prevent this from happening by creating an expression for the Actions to run if a condition is

true/false and clearing the **Execute Before Saving a Record** check box; this allows the system to only save the record if necessary.

General Server Maintenance

Investigate your server memory usage to determine if Portal performance is being affected as a result. Access this information by right-clicking the Windows Task Bar, selecting **Start Task Manager**, and selecting the **Processes** tab. Then, you can restart the process or server using the IIS Manager.

When you restart the process or server, the memory use will temporarily decrease, but will continue to increase afterwards; this might happen because the Application Pool in IIS does not have permissions to write to the directory and instead of displaying an error, the log messages consume memory. If this happens, you have several options:

- Using the **Portal Logging Options** window (for more information, see Configure Encryption Keys for a CSM Server or Web Application) and the **Browser Logging Options** window in the Cherwell Server Manager, change the file path.

- Using the Application Pool Identity window in the IIS Manager, change the Identity for the Application Pool.

- Enable file permissions for the Application Pool so it can write log files to your chosen location. For more information, see Securing IIS.

Related concepts

About Performance Health Check

Run the Health Check Tool

Interpreting Health Check Results

About Performance Health Check

The Health Check Tool helps system administrators monitor and optimize system configurations that impact performance.

For example, use the tool to:

- Find inefficient queries.

- Find and fix mismatched Def IDs.

- See which Business Objects can be set as cachable.

- Send Health Check results to Cherwell Support for analysis on request.

- Discover missing indexes for Business Object database tables that contain a large number of records.
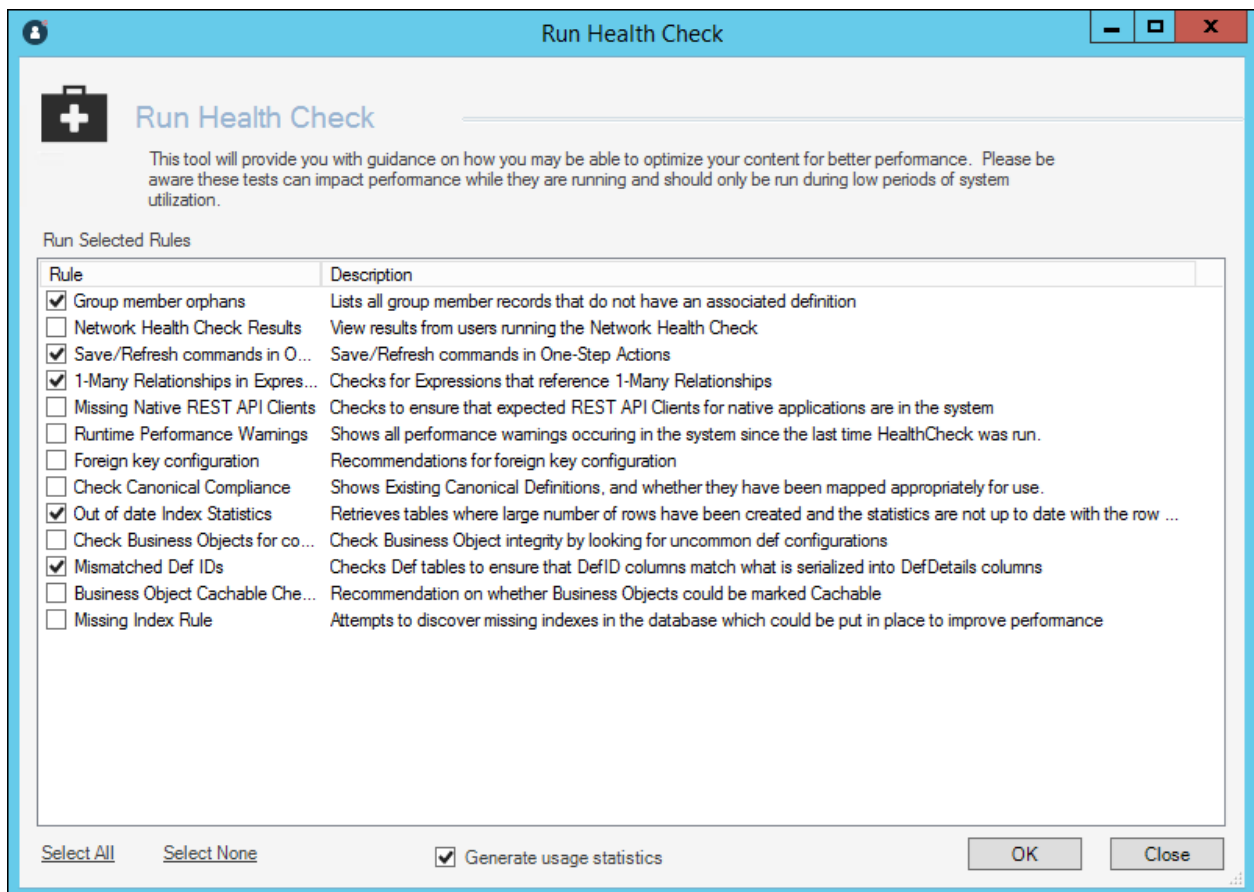
There are three levels of Health Check tests:

- **Basic:** Provides information about your CSM system (runtime at the time the Health Check is performed, foreign key, Def ID mismatch) and the Health Check plug-in. Basic results are included every time you run the Health Check.

- **Rule-based:** Provides information for the rules you select when you run the Health Check.

- **Usage Statistics:** Provides system and database information not related to the rules you select when you run the Health Check. Examples include expensive database queries, wait statistics, and table sizes.

Run rule-based or usage tests alone or as a set.

Related concepts
Run the Health Check Tool
Interpreting Health Check Results
Related tasks
System Information

Run the Health Check Tool

Run the Health Check Tool to monitor and optimize system configurations that impact performance. You can select which tests to run, and then save the results to a file.

Hosted and on-premises customers can run the Health Check Tool. Cherwell hosted servers run a standard SQL configuration so hosted customers can disregard some Health Check Tool results.

In all cases, suggestions made for adding or dropping indexes should be made in CSM Administrator rather than directly in the database. This prevents the next Blueprint publish from removing the index changes.

Before Running the Health Check Tool

We recommend:

- SQL Server should run for a minimum of three business days before using the Health Check Tool.
- If changes are made, again let the server run for a minimum of the business days before using the Health Check Tool.
- On-premises customers should check these SQL Server settings prior to running the Health Check Tool:
    - ServerMaxMemory
    - OptimizeAdhoc

    If you are using a dedicated server (not a shared cluster) to host the database, Cherwell recommends you set OptimizeAdHoc to true. If an on-premises database has OptimizeAdHoc set to False and is not using a shared cluster, this setting should be changed accordingly.

Run the Health Check Tool

To run the Health Check Tool:

1. From the CSM Administrator main window, select the **Performance** category.
2. Select **Run Health Check**.
3. Choose which tests to run:
    - In the **Run Selected Rules** pane, select the rules to check various areas of your system. The list of rules available to you may vary depending on the version of CSM and the Health Check plug-in that you have installed.
    - Select the **Generate Usage Statistics** check box to check system and database information.

        Note: Some rules and usage statistics require `View server state` privilege for the database login account. In SQL Server Management Studio, this privilege is located on the **Securables** tab of the **Login Properties** dialog box.

    - Select the **Select None** link to generate CSM system and the Health Check plug-in information only.

4. Select **OK**.

    The Health Check results open in a separate window.

5. Select the relevant option:
    ◦ **Save to File**: Save the results to an HTML file.

    ◦ **Submit**: Send the results to Cherwell Support on request.

    ◦ **Create Blueprint**: Create and save a new Blueprint to add recommended missing indexes and remove duplicate indexes based on the Health Check results. This option provides greater convenience and accuracy than adding and removing indexes manually. Blueprints created from Health Check results only include missing and duplicate indexes; they will not address other recommendations from the Health Check.

    Note: If you select the **Create Blueprint** option be aware that missing indexes are only created if the TotalCost metric has a value of 10 million or greater.

Related concepts

Interpreting Health Check Results

Health Check Command-Line Options

Related tasks

System Information

Business Object Attribute Checks

Interpreting Health Check Results

After running the Health Check Tool, you can optimize system configurations based on the results of the basic checks, rules reports and usage statistics.

Basic checks:

- System Information
- Business Object Unique Attribute Checks
- Plugin Manager Rules

Interpreting Rules reports:

- Group Member Orphans
- Network Health Check
- Save/Refresh Commands in One-Step Actions
- 1-to-Many Relationships in Expressions
- Missing Native REST API Clients
- Runtime Performance Warnings
- Foreign Key Configuration
- Check Canonical Compliance
- Out of Date Index Statistics
- Check Business Objects for Consistency
- Mismatched Def IDs
- Business Object Cachable Check
- Missing Index Rule

Interpreting Usage Statistics:

- Check Database
- Worst Queries by Average Reads
- Worst Queries by CPU
- SQL Wait Statistics
- Table Size Statistics
- Index Usage Statistics

Note: Open your report in a browser.

Related tasks
System Information

System Information

Run the Health Check Tool and select the **Select None** check box or any rule. This rule gives you a high-level overview of your system.

Good to Know

- You may be asked to provide some of this information if you contact Cherwell Support.

1. Select the **Select None** check box or any of the rules when you Run the Health Check Tool. You see the System Information results as part of the basic checks in the report.

System Information
Retrieves information about the current runtime of the Cherwell System

Results Date:	2020-01-14T16:25:03.1411074+00:00
Version:	10.0.0.0
License:	Cherwell Internal Test License 100U - 25
Current User:	CSDAdmin
Connection:	2Tier- Cherwell Browser
System Environment:	Development

2. **Connection** shows you the type of connection (2 tier/3 tier) used to run the test.

   Note: If the connection is 3-tier, the Cherwell Application Server version is shown and it should match the CSM version shown above.

3. Check that the **System Environment** value is **Production**.

Related tasks
Define Advanced Properties for a Business Object
Business Object Attribute Checks
Plugin Manager Rules
Runtime Performance Warnings

Business Object Attribute Checks

Run the Health Check Tool and select the **Select None** check box or any rule. This rule checks that specific attributes are applied to a unique Business Object in the system.

Good to Know

These are the attributes that are checked:

- CustomerBusinessObject
- DefaultPrimaryBusinessObject
- ConfigurationItemBusinessObject
- JournalBusinessObject

1. Select the **Select None** check box or any of the rules when you Run the Health Check Tool. You see the results in the report.

Business Object Unique Attribute Checks
Check for Unique Attribute that are used by multiple Business Objects

(No Data)
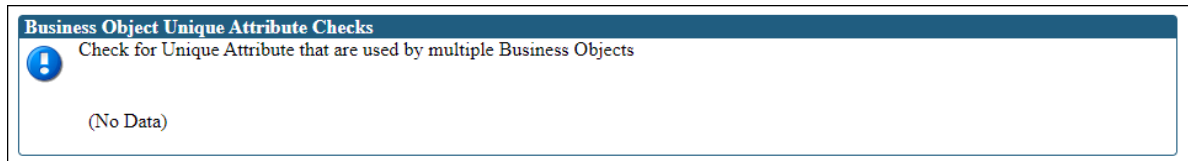
2. If you get results in this report, you need to remove the duplicate attribute from the affected Business Object to make sure that they are unique. For example, you cannot have two Business Objects with an attribute called CustomerBusinessObject.

Related tasks
Plugin Manager Rules
Runtime Performance Warnings
Foreign Key Configuration

Plugin Manager Rules

Run the Health Check Tool and select the **Select None** check box or any rule. This rule indicates the version of the Health Checker being used to run all the performance checks.

1. Select the **Select None** check box or any of the rules when you Run the Health Check Tool. You see the Plugin Manager results as part of the basic checks in the report.

2. You may be asked to provide these details if you contact the Cherwell Support.

Related tasks
Runtime Performance Warnings
Foreign Key Configuration
Check Canonical Compliance

Group Member Orphans

Run the Health Check Tool and select the **Group member orphans** rule. This rule scans for group member records that do not have an associated definition.

Group member orphans are records whose definitions have been deleted but whose associated rows have not been deleted because they are members of a group. This rule returns a list of all group member orphans so that you can clean them up.

Related concepts

Run the Health Check Tool

About Performance Health Check

Network Health Check Results

Run the Health Check Tool and select the **Network Health Check Results** rule. This rule performs a built in speed test so a technician can check for network issues between their client and the server.

Good to Know

- If you run this tool from CSM Administrator, the report displays the results from the last 30 days of all users running the Network Health Check. This allows administrators to view results from everyone and compare network performance from different locations.

- Users must have the *Allow diagnostics* right to run the test.

- Users with the correct permissions to run the test will see the *Network Health Check* option under the **Tools** menu in the CSM Desktop Client and CSM Browser Client.

> **Note:** Users must be logged in with a 3-tier connection or the menu options are not displayed.

To see information about the Network Health Check:

- Select the **Network Health Check Results** check box when you run the Health Check Tool. This displays the report with a time for each test file size, a minimum time, a maximum time, the average amount of time, and standard deviation.

Related concepts

Run the Health Check Tool

User Manager

SaaS One-Step Action Check

Run the Health Check Tool and select the **SaaS One-Step Action Check** rule. This rule looks for One-Step Actions and tokens that may need to use a Trusted Agent in a hosted environment.

SaaS customers must use a Trusted Agent for all of the following Actions when they will run on a server. This includes the Browser Client, CSM Portal, Cherwell REST API, Automation Processes, and the Scheduler running in a two-tier configuration.

- Print
- Run a Program
- Run a Report
- Write to a File
- Transfer Attachments
- Excel Merge

Important: One-Step Actions listed in the results will not run until you configure them to use a Trusted Agent.

This rule is only available on systems using a SaaS license.

To see One-Step Actions that must use a Trusted Agent:

1. Select the **SaaS One-Step Action Check** rule when you Run the Health Check Tool.
2. Use the information returned in the report to locate and configure One-Step Actions and tokens to use a Trusted Agent:

For example, for this results entry:
Token: Product Name, Business Object: Incident, Folder: Buttons and Link Labels, Type: One-Step Action - Create Mobile CI

Follow these steps:

1. Open the **One-Step Manager**, and then search for *Create Mobile CI*.
2. Edit the One-Step Action.
3. Select each One-Step Sub-Action until you see a warning message that indicates the Action must use a Trusted Agent.
4. Select the **Trusted Agent** page.
5. Select the **Use Trusted Agents** check box and a specific Trusted Agent Group, if applicable.
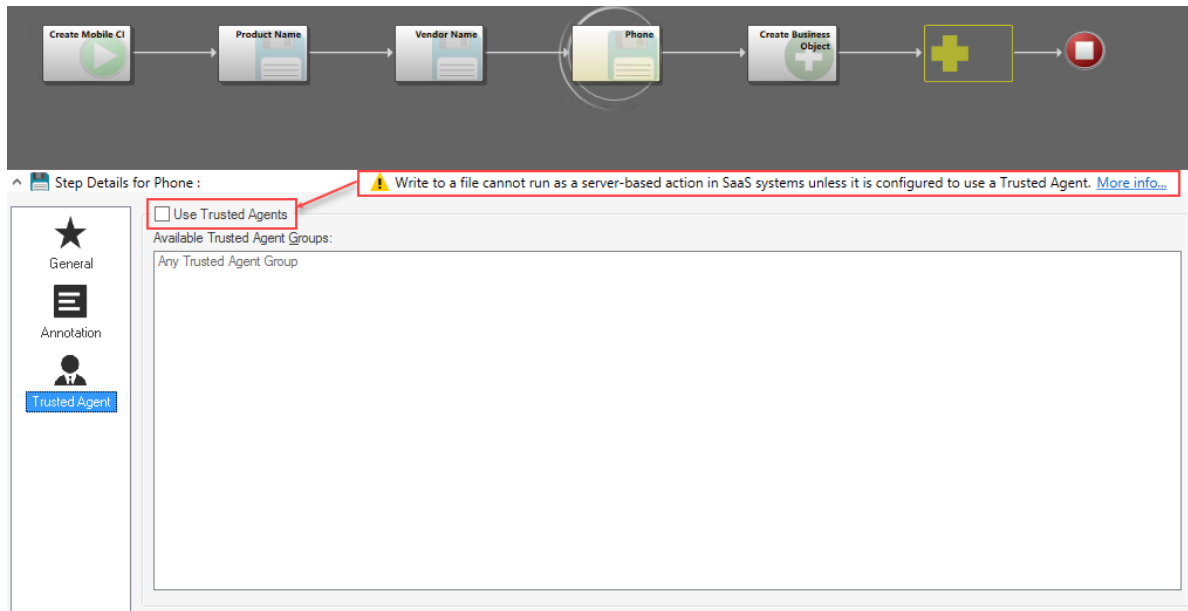
6. Verify that other Sub-Actions in the One-Step Action are configured correctly.

7. Save and publish your changes.

Related tasks
Configure One-Step Actions for Trusted Agent
Update a Business Object with Content from a File

Save/Refresh Commands in One-Step Actions

Run the Health Check Tool and select the **Save/Refresh commands in One-Step Actions** rule. This rule retrieves a list of all One-Step Actions and Action Blocks in the system that contain save and/or refresh actions.

1. Entries in the report for this rule contain the following information:
   - The Business Object with which the One-Step Action or Action Block is associated.
   - The folder in which the One-Step Action or Action Block is located.
   - The One-Step Action or Action Block's type, name, and scope.
   - How many save and refresh commands are present.
2. While save and refresh commands are sometimes necessary, excessive use of them can cause performance issues. If any of the commands reported by this rule are unnecessary, you may be able to improve performance by removing them from the relevant One-Step Action or Action Block using a Blueprint.

1-Many Relationships in Expressions Rule

Run the Health Check Tool, and then select the **1-Many Relationships in Expressions** rule. This rule detects expressions that use one-to-many relationships, which may cause performance issues because only the first record in a relationship is evaluated by an expression, even if thousands of records are returned.

Use this information to find and assess the need for expressions that use one-to-many relationships. For example, you may want to replace these expressions with those that use one-to-one relationships. Other configurations may also meet your needs, such as using a constant value rather than an expression.

Note that aggregate expressions are not included in the Health Check rule because in this case, using one-to-many relationships is valid.

The rule returns the following information for each expression used in a one-to-many relationship:

- **Owner**: Indicates the Business Object that contains returned expressions. Example: Change Request.
- **ParentDefType**: Indicates the type of definition used by each expression. For example, BusinessProcessDef indicates an expression is used by an Automation Process definition.
- **ParentDefName**: Indicates the name of the parent definition using the expressions. Example: Change - Notify Problem Owner.
- **Relationship**: Indicates the relationship that uses an expression. Example: Change Request Links Problems.
- **Path**: Provides guidance on how to find an expression that needs review.

  Example: `BusinessProcessDef (Change - Notify Problem Owner)\Expression (Left) [Problem.ChangeRequestID (Change Request Links Problem)]`

To find the expression in the example, create an Automation Process Blueprint, and then edit the **Change - Notify Problem Owner** Automation Process.

To fix the potential performance issue for the example, consider creating a one-to-one relationship that links Change Request to Problem.

Related concepts
Relationships and Performance
Expressions
Run the Health Check Tool
Interpreting Health Check Results

Missing Native Rest API Clients

Run the Health Check Tool and select the **Missing Native REST API Clients** rule. This rule looks for missing REST API clients that should have been created when a native application, such as a CSM Portal, is added to CSM.

Good to Know

- By selecting **Browser and Mobile > Site Manager** in the CSM Administrator, you can set up custom login options for a CSM Portal. If your custom login options are not displayed on the Portal as expected, you should run this Health Check rule.

To see information about Missing REST API clients:

1. Select the **Missing Native REST API Clients** rule when you run the Health Check Tool (for more information, see Run the Health Check Tool).
   The Missing Client results are displayed in the report.

2. If you get any results in this report, select **Repair**.
   All missing native client entries are fixed for you.

3. To verify the report is now empty, re-run the Health Check again with this rule.

Related tasks
Runtime Performance Warnings
Foreign Key Configuration
Check Canonical Compliance

Runtime Performance Warnings

Run the Health Check Tool and select the **Runtime Performance Warnings** rule. This rule collates any performance messages which are logged at runtime as warnings.

Good to Know:

- Any warnings that occurred in the past week are shown when the Health Check tool is run with this rule.

- When the report finishes, the warning records are cleared from the database.

- Two performance issues are reported:
    - Reports which retrieve rich text fields.

    - Business Object relationships that retrieve over 1,000 rows.

1. Select the **Runtime Performance Warnings** rule when you Run the Health Check Tool.
   You see any warnings from the past week in the report.

2. If you see warnings for reports which retrieve Rich text fields, this can affect performance. To remove Rich Text fields from a report, clear the Retrieve Rich Text Fields check box.

3. If you see warnings for a Business Object relationship that retrieves more than 1,000 rows, scroll down to read the guidance. You can change the relationship to load only the keys and/or add constraints to the relationship to retrieve less values. For example, instead of a relationship retrieving all of a customer's Incidents, the relationship could retrieve just the last 30 days of incidents. For more information, see: Define Advanced Properties for a Relationship.

Related tasks
Foreign Key Configuration
Check Canonical Compliance
Out of Date Index Statistics

Foreign Key Configuration

Run the Health Check Tool and select the **Foreign Key Configuration** rule. This rule looks at all Business Object fields in the system which are flagged to use Foreign Keys and validates that those fields are configured correctly for use with foreign keys.

Good to Know

- For Fields, a foreign key stores Field values in validated Lookup Tables as record IDs rather than text.

- A foreign key relationship correctly links values in a Lookup Table to the validated Field.

To see information about foreign key fields:

1. Select the **Foreign Key Configuration** rule when you Run the Health Check Tool.
   You see the field validation results in the report.

2. If you get results in the report, define new foreign key relationships.

Note: There are examples for defining foreign key relationships if you need some help. You can also store foreign keys for fields that are validated from Lookup tables and that enforce validation. This ensures that changes to Lookup table values are updated in existing records because record IDs are used rather than text values.

Related concepts

Defining Foreign Key Relationships

Example: Defining a Foreign Key Relationship for Asset Status Field

Storing Foreign Keys for Validated and Auto-populated Fields
Related tasks
Check Canonical Compliance
Out of Date Index Statistics

Check Canonical Compliance

Run the Health Check Tool and select the **Check Canonical Compliance** rule. This rule looks at any canonical definitions and checks whether they have been mapped correctly for use.

Good to Know

- About the Cherwell Canonical REST API

- Canonical REST API Mapping Wizard

- **Important:** To ensure standardization, canonical definitions are supplied and managed by Cherwell. You can access canonical definitions in the Canonical Definitions Manager, but we strongly advise against creating, editing, or deleting canonical definitions as you may inadvertently impact your system's integration capabilities.

To see information about canonical compliance:

1. Select the **Canonical Compliance** rule when you Run the Health Check Tool.
   You see the compliance results in the report.

   Check Canonical Compliance
   Shows Existing Canonical Definitions, and whether they have been mapped appropriately for use.
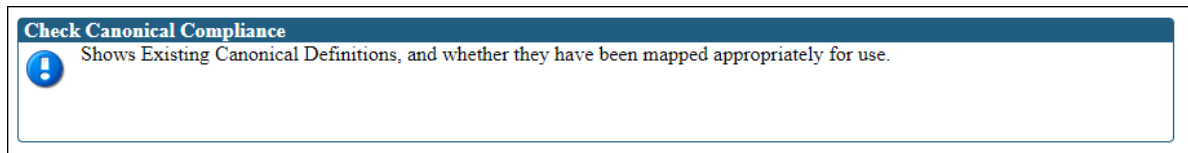
2. If you get results in the report, see Interpreting the Results of a Canonical Compliance Health Check for a list of common errors and descriptions of what to do next.

Related concepts
About the Cherwell Canonical REST API
Interpreting the Results of a Canonical Compliance Health Check
Related tasks
Canonical REST API Mapping Wizard
Out of Date Index Statistics
Check Business Objects For Consistency

Out of Date Index Statistics

Run the Health Check Tool and select the **Out of Date Index Statistics** rule. This rule retrieves tables where a large number of rows have been created and the statistics are not up to date with the row count.

Good to Know

- If you have a hosted system, a nightly job is run to update the statistics, so you should generally never see information in this section unless you run the Health Check just prior to the job running.
- If your system is on-premises, we recommend that you ask your DBA to run this command to update these statistics: **exec sp_updatestats**.

To see information about Out of Date Index Statistics:

1. See the above **Good to Know** point about timing of this report.
2. Select the **Out of Date Index Statistics** check box when you Run the Health Check Tool. You see the Out of Date Index Statistics in the report.

Related tasks
Check Business Objects For Consistency
Mismatched Def IDs Check
Business Objects Cachable Check

Check Business Objects For Consistency

Run the Health Check Tool and select the **Check Business Objects for Consistency** rule. This rule checks if there are duplicate fields in the system by storage name or field ID.

1. Select the **Check Business Objects for Consistency** rule when you Run the Health Check Tool. You see the results in this report.
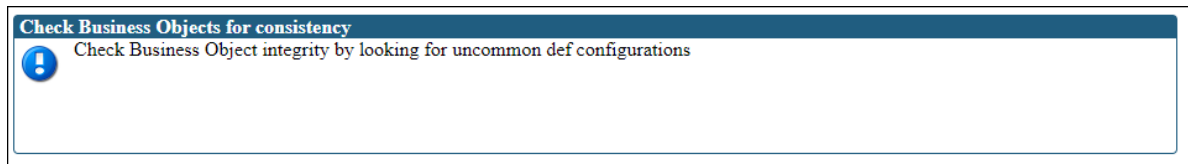
2. If this report shows duplicate fields in the system, fix them yourself or ask your DBA for help.

Related tasks
Mismatched Def IDs Check
Business Objects Cachable Check
Missing Index Rule

Mismatched Def IDs Check

Run the Health Check Tool and select the **Mismatched Def IDs Check** rule. This rule checks definition tables to determine whether DefID columns match the information that is serialized into DefDetails columns.

1. Select the **Mismatched Def IDs Check** rule when you Run the Health Check Tool.
   You see the results of using this rule in the report.

   Mismatched Def IDs
   Checks Def tables to ensure that DefID columns match what is serialized into DefDetails columns

   (No Data)
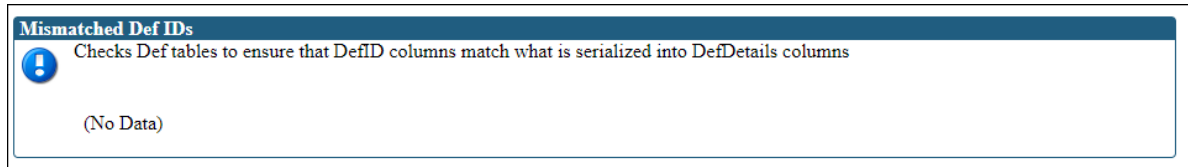
2. If you get any entries in this report, you can check the reason codes for the entries in the Reason column. The meanings of the reason codes are as follows:
   ◦ 1: MismatchedIDs
   ◦ 2: DuplicateNames

   If there are entries in the report, you can select Repair, located in the top right of the report, to fix the mismatched definition IDs.

3. You can also Perform Database System Maintenance to fix the mismatched definition IDs.

Related tasks
Business Objects Cachable Check
Missing Index Rule
Check Database

Business Objects Cachable Check

Run the Health Check Tool and select the **Business Objects Cachable Check** rule. This rule looks at all the Business Objects that are not flagged as cachable and then checks the row count in each table.

Good to Know

- Data which doesn't change very often can be cached to improve system performance. One method is to cache Business Objects when used as a validation table. For more information, see Define Advanced Properties for a Business Object.

- These tables are often Lookup tables that don't change much in terms of their content. Consequently, these could be marked as cachable so the values are stored in memory and the application doesn't query the database for those table values.

- The cache is periodically updated when the App Server is restarted.

1. Select the **Business Objects Cachable Check** Rule when you run the Health Check Tool (for more information, see Run the Health Check Tool).
   You see the results of using this rule in the report.

2. Check each of the listed Business Objects. If the row count is small, the system recommends that you switch on the cachable flag. For more information, see Define Advanced Properties for a Business Object

Related tasks
Missing Index Rule
Check Database
Worst Queries by Average Reads

Missing Index Rule

Run the Health Check Tool and select the Missing Index rule. This rule looks for missing indexes.

Good to Know

- For more guidance on creating indexes, see Creating Indexes.

To see information about Missing Indexes:

1. Select the Missing Index Rule when you Run the Health Check Tool.
   You see the Missing Index results in the report.

2. Identify any tables with a high **TotalCost** and high **IndexSeeks**. Also look for values which are an order of magnitude higher than the rest of the values; these tables are good candidates to add indexes. In the example shown above, this would be the first two rows.

3. Identify any tables that have values in **EqualityUsage** or **InequalityUsage**. The indexes recommended by those rows could also be good candidates. In the example above that would be the fourth and fifth rows; with one index you also aggregate the cost of both rows.

4. Indexes need to be added using a Blueprint. Add the index to the table and field identified and include the fields identified in the **IncludeColumns** section.

   Note: Adding the recommended Include columns can help speed up the query by covering the query. However, the more Include columns are added, especially when they are key columns, the longer it can take to keep the indexes up to date.

5. The columns in the EqualityUsage indicate columns being used in queries with equality predicates ("Select * from employee where id = 2") and the InequalityUsage column displays columns being used in queries using inequality predicates, for example, "Select * from employee where id > 2").

Related concepts
Worst Queries by CPU
Related tasks
Check Database
Worst Queries by Average Reads

Check Database

Run the Health Check Tool and select **Generate Usage Statistics**. Check Database runs a high-level check of the database without inspecting tables.

✏️ **Note:** Multiple file groups are not supported in CSM. If you database uses multiple file groups or transaction logs, this check will fail.

To run a health check on the database:

1. Select the **Generate Usage Statistics** check box when you .
   The Check Database report opens.

2. Verify the database name to ensure that the correct database is being checked.
3. Check that **ServerCollation** and **DatabaseCollation** match. They should be case insensitive as indicated by **CI** in the collation name, for example SQL_Latin1_General_CP1_**CI**_AS.
4. Check that **RecoveryModel** is FULL.
5. Check that **ServerMaxMemory** is 1GB less than the total available system memory.
6. If you are using a dedicated server for CSM then **OptimizeAdHoc** should be set to true.
7. Check that **Version** contains one of the supported SQL versions and has x64 in it.

8. Check that the Database Files section has two entries.
    ◦ The **is_percent_growth** column should be false.

    ◦ In general, and for small databases, we recommend that growth not be more than 10% of the **Size** column. For example, if the Size is 1000 MB, the growth should ideally not be more than 100 Mb. For production databases, the minimum recommended value for the Growth column is 50 MB.

Related concepts

Worst Queries by CPU

Related tasks

Worst Queries by Average Reads

SQL Wait Statistics

Worst Queries by Average Reads

Run the Health Check Tool and select **Generate Usage Statistics**. Worst Queries by Average Reads retrieves the most expensive queries on the system as determined by the average reads per execution.

To see information about the worst queries:

1. Select the **Generate Usage Statistics** check box when you Run the Health Check Tool.
   You see the Worst Queries by Average Reads in the report.

2. Focus on the queries with the highest **execution_count** and the highest **MaxReads** (10th column to the right). Then look at the queries and compare them to the Missing Indexes section.

   Note: A query being at the top of the list doesn't necessarily mean it is a bad query.

Related concepts
Worst Queries by CPU
Related tasks
SQL Wait Statistics
Table Size Statistics

Worst Queries by CPU

Run the Health Check Tool and select **Generate Usage Statistics**. Worst Queries by CPU retrieves the most expensive queries as determined by total CPU usage. This statistic is similar to Worst Queries by Average Reads but is based on total CPU time for a query, rather than the number of reads executed.

Note:

System performance of the Worst Queries by CPU usage check may be affected by global database options. For more information, see Define Global Database Options.

Specifically, the **Database Timeout Values** may have no set limits. Selecting a **No limit** check box can result in performance issues and is not recommended. Instead, we recommend increasing the set limit.

To see information about the worst queries:

1. Select the **Generate Usage Statistics** check box when you Run the Health Check Tool.

   You see the Worst Queries by CPU in the report.

2. Focus on the queries with the highest **TotalCPUTime** and the highest **execution_count**.

   Note: You may have expensive queries that reference system tables, such as TrebuchetCounters. It is not possible to add indexes to system tables so these can be ignored.

Related tasks
SQL Wait Statistics
Table Size Statistics
Index Usage Statistics

SQL Wait Statistics

Run the Health Check Tool and select **Generate Usage Statistics**. Retrieves SQL Wait Statistics which can be used to identify performance issues with the CSM SQL server.

🖉 **Note:** High wait times indicate that an investigation may be needed. Inform your DBA that there are possible issues with the SQL server.

Select the **Generate Usage Statistics** check box when you Run the Health Check Tool.
You see the SQL Wait Statistics in the report.

SQL Wait Statistics

ℹ Retrieves the SQL Wait statistics, which can be useful in identifying performance issues with the server.

Top 20 Waits by Wait Time (seconds):

wait_type	wait_time_s	pct	running_pct	pct_of_uptime
QDS_CLEANUP_STALE_QUERIES_TASK_MAIN_LOOP_SLEEP	2,382,610.18	25.00	25.00	100.00
HADR_FILESTREAM_IOMGR_IOCOMPLETION	2,382,595.63	25.00	50.00	100.00
QDS_PERSIST_TASK_MAIN_LOOP_SLEEP	2,382,589.24	25.00	74.99	100.00
FT_IFTSHC_MUTEX	2,381,032.77	24.98	99.97	99.93

Related concepts
Configuring the Performance Health Check Tool
Related tasks
Table Size Statistics
Index Usage Statistics

Table Size Statistics

Run the Health Check Tool and generate usage statistics. Table Size Statistics retrieves the row count and size statistics for all tables.

To see information about table sizes:

1. Select the **Generate Usage Statistics** check box when you run the Health Check Tool (for more information, see Run the Health Check Tool).
   You see the Table Size Statistics in the report.

Table Size Statistics
Retrieves the row count and size statistics for all tables in the database server

Top 20 Tables by Row Count:

TableName	indexName	Rows	TotalPages	UsedPages	DataPages	TotalSpaceMB	UsedSpaceMB	DataSpaceMB
Journal	PK_Journal	16793632	3657812	3657253	3286532	28576	28572	25676
EndpointService	PK_EndpointService	2995820	260324	256432	251851	2033	2003	1967
Specifics	PK_Specifics	1974868	155464	155240	153517	1214	1212	1199
Incident	Incident_RecID	1348512	1204207	1178324	859846	9407	9205	6717
ConfigurationItem	PK_ConfigurationItem	1207566	149105	148835	147635	1164	1162	1153
ENPOINTNETWORK	PK_ENPOINTNETWORK	960066	54797	53310	52739	428	416	412
ScheduledAction	PK_ScheduledAction	950286	78091	77287	76617	610	603	598
OS	PK_OS	802483	47150	47092	46714	368	367	364
BASEBOARD	PK_BASEBOARD	802268	29261	29230	28982	228	228	226
BIOS	PK_BIOS	802194	27646	27612	27373	215	215	213
RaidController	PK_RaidController	802166	26238	26213	25987	204	204	203
Software	PK_Software	624627	52181	47966	47016	407	374	367

2. Use this information to identify tables that could be cleaned up by your DBA. For example, a table could be truncated to improve performance.

> **Note:** Pay special attention when the TotalSpaceMB is much larger than the DataSpaceMB for a row. This could be an indication that the number or configuration of indexes on that table isn't ideal. Below is a very clear example:

Top 20 Tables by Row Count:

TableName	indexName	Rows	TotalPages	UsedPages	DataPages	TotalSpaceMB	UsedSpaceMB	DataSpaceMB
Journal	PK_Journal	5198276	76829398	76752321	1764656	600229	599627	13786
AssignmentHistory	PK_AssignmentTracking	542641	41901	41762	40800	327	326	318

Related concepts
Configuring the Performance Health Check Tool
Creating Indexes
Related tasks
Index Usage Statistics

Index Usage Statistics

Run the Health Check Tool and select **Generate Usage Statistics**. Index Usage Statistics retrieves index usage statistics from the SQL server.

To see information about index usage:

1. Select the **Generate Usage Statistics** check box when you Run the Health Check Tool.
   You see the Index Usage Statistics in the report.

Index Usage Statistics

Gathers the index usage statics from the database server

Top 10 Index Usages by User Updates:

Database_name	Table_Name	Schema_name	Index_name	Type_Desc	user_seeks	user_scans	user_lookups	user_updates
SampleCompanyTest	Journal	dbo	PK_Journal	CLUSTERED	942694	123	350274	561049
SampleCompanyTest	Journal	dbo	History_HistoryType	NONCLUSTERED	0	0	0	444548
SampleCompanyTest	Journal	dbo	Journal_ParentRecordID	NONCLUSTERED	315481	0	0	444548
SampleCompanyTest	Journal	dbo	Journal_ParentTypeID	NONCLUSTERED	107	0	0	444548
SampleCompanyTest	Journal	dbo	JournalComment_CommentID	NONCLUSTERED	0	0	0	444548
SampleCompanyTest	Journal	dbo	JournalIdx0	NONCLUSTERED	34685	0	0	444548
SampleCompanyTest	Journal	dbo	JournalNote_JournalTypeName	NONCLUSTERED	0	2	0	444548
SampleCompanyTest	Incident	dbo	Incident_RecID	CLUSTERED	1607887	664	31465	383125
SampleCompanyTest	Incident	dbo	Incident_IncidentType	NONCLUSTERED	0	1	0	278836
SampleCompanyTest	Incident	dbo	IncidentStatus	NONCLUSTERED	0	572	0	278836
SampleCompanyTest	Incident	dbo	LandingPageCounts	NONCLUSTERED	0	182	0	278830

Top 10 Index Usages by User Seeks:

Database_name	Table_Name	Schema_name	Index_name	Type_Desc	user_seeks	user_scans	user_lookups	user_updates
SampleCompanyTest	ResponseUnits	dbo	PK_ResponseUnits	CLUSTERED	10422657	10777	0	0
SampleCompanyTest	IncidentPhaseStatus	dbo	PK_IncidentPhaseStatus	CLUSTERED	7995820	194221	0	0
SampleCompanyTest	IncidentType	dbo	PK_IncidentType	CLUSTERED	4721885	28411	0	0
SampleCompanyTest	UserInfo	dbo	PK_UserInfo	CLUSTERED	2198732	427	20	63
SampleCompanyTest	Service	dbo	PK_ServiceCatalog	CLUSTERED	2130524	32574	0	53
SampleCompanyTest	SLAStatus	dbo	PK_SLAStatus	CLUSTERED	1914846	42612	0	0
SampleCompanyTest	Incident	dbo	Incident_RecID	CLUSTERED	1607887	664	31465	383125
SampleCompanyTest	IncidentCategory	dbo	PK_IncidentCategory	CLUSTERED	1172840	28456	0	102
SampleCompanyTest	IncidentSubCategory	dbo	PK_IncidentSubCategory	CLUSTERED	1171972	27903	0	337
SampleCompanyTest	SLATargetTime	dbo	PriorityLevel	NONCLUSTERED	1149047	40	0	0
SampleCompanyTest	IncidentStatus	dbo	PK_IncidentStatus	CLUSTERED	1144477	27489	0	0

2. Check for indexes with a high value for **user_updates** and very low or zero values for **users_seeks** and **user_scans**. This means that this index is not being used much, and you can get this index dropped from the system to improve performance.

3. Overall ideally you should see more seeks than scans. A high value for **user_scans** compared to **user_seeks** could justify the addition of an index to that table. Check the worst queries by reads or CPU results to find out if a query is being run on the same table.

Related concepts
Configuring the Performance Health Check Tool
Creating Indexes
Related tasks
Log Viewer Utility

Configuring the Performance Health Check Tool

Health Check Security rights are configured in CSM Administrator. See Tools Security Rights.

Related concepts

Tools Security Rights

Creating Indexes

Best Practices for Performance

Related tasks

Log Viewer Utility

Creating Indexes

After running the Health Check Tool, you may need to add new indexes to some tables or make changes to those you already have.

The recommendations in this topic are specific to that situation. For general instructions on how to add indexes, see Define Database Properties for a Business Object.

Combining Multiple Rows

To combine multiple rows in an index:

Identify any tables that have values in **EqualityUsage** or **InequalityUsage**. The indexes recommended by those rows could be good candidates for adding an index. In the example above that would be the fourth and fifth rows; with one index you also aggregate the cost of both rows.

About Key Columns and Include Columns

The columns in the EqualityUsage indicate columns being used in queries with equality predicates ("Select * from employee where id = 2") and the InequalityUsage column displays columns being used in queries using inequality predicates, for example, "Select * from employee where id > 2").

An Index key column is the column used in the index, and used by the optimizer to decide if the index is applicable. It is also used by the execution engine to fulfill the WHERE part of the query. It is used for the SELECT part of the query if the column is needed.

An Included column is added to the index, not used by the optimizer or execution engine in finding the rows or joining tables. It can only be used by the SELECT part of the query to return the data.

What Not to Do

Adding the recommended Include columns can help speed up the query by covering the query. However, the more Include columns are added, especially when they are key columns, the longer it can take to keep the indexes up to date.

> **Note:**
> An index must be updated every time a relevant record's data is changed. When users access a record, the **Last Modified date/time** is highly likely to be updated.

Consequently, if a record is likely to be frequently modified, we recommend that you avoid adding indexes on the **Last Modified date/time** field.

Instead, consider adding indexes on the **Created date/time** field.

Log Viewer Utility

Use the Log Viewer utility to review CSM logs, even if you do not have access to the server on which CSM or its services are installed.

Use the Log Viewer utility to view logs for the:

- Cherwell® Application Server
- Trusted Agent Server (only available for on-premise installations)
- Cherwell Service Host
- CSM Browser Client
- CSM Portal
- Cherwell REST API

You must select **Log to File** in your logging configuration in the Cherwell Server Manager. If you are a SaaS customer, contact Cherwell Support to configure file logging. See Configure Logging for a CSM Service, Web Application, and Cherwell REST API.

> **Note:** To avoid system performance issues, the Log Viewer only retrieves the most recent 10,000 lines (up to 512kb of data) from the latest log file. The Log Viewer does not combine the beginning of a new log file with the end of a previous log file if the new log file has fewer than 10,000 lines in it.

To use the Log Viewer:

1. In CSM Administrator, select the **Performance** category.
2. Select **Log Viewer**.
   The **Log Viewer** window opens.
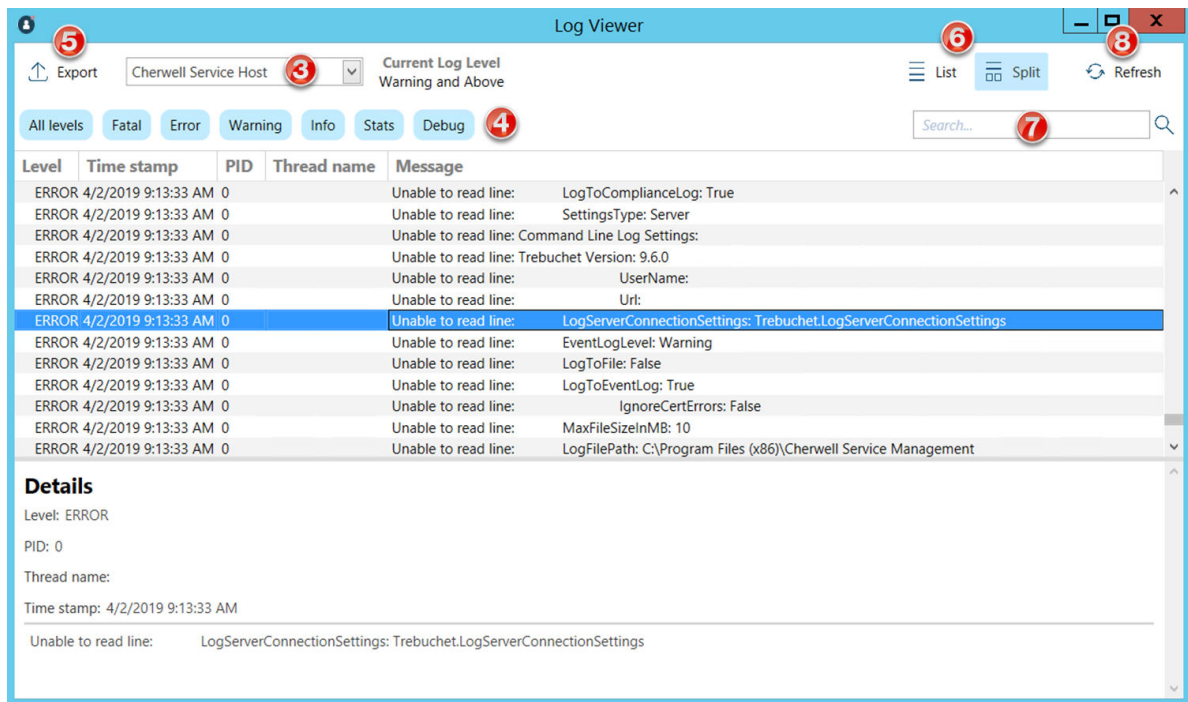
3. Use the drop-down list to choose the logs you want to view.

4. Select the log level you want to view.

5. Select **Export** to generate a .txt of the log results.

6. Choose **List** or **Split** to control your view. Choosing **Split** gives you a detail pane for the log record you select.

7. Use the search box to search the log records.

> **Note:** Search results are shown as highlighted matching terms in the viewer, rather than a filtered list of matching records.

8. Select **Refresh** to update log information.

9. If you are not seeing entries in the Log Viewer as expected, perform the following steps. If you are a SaaS customer, contact Cherwell Support to perform these steps for you.

10. In Windows Explorer, right-click the folder where the log file is located (this is the folder you created when setting up file logging).

11. Select **Properties**.

12. Select the **Security** tab.

13. Select **Edit**.

14. For all users and groups, select **Allow** on Full control.

15. Reset Internet Information Services (IIS).

Related concepts

Server Tools

Server Tools include the Server Manager and command-line options.

CSM provides the following server tools:

- The Server Manager is a stand-alone tool that allows system administrators to efficiently monitor, manage (start, stop, or restart), and configure (database connections, login authentication, logging, etc.) the CSM services, and restart some managed CSM Web Applications.

- Command-line options are available for the CSM Client, CSM Configuration, Administrative, and System Restore.

Related concepts

CSM Services

About the Server Manager

About the Cherwell Service Host

Other Command-Line Options

CSM Services

CSM services are Microsoft Windows® services dedicated to particular tasks. These services run in the background while monitoring for, and accepting, requests from CSM clients.

The available CSM services are:

- **Cherwell Application Server**: Runs programs and handles application operations between users and their databases. The Application Server is the middle tier of the Cherwell three-tier application. Client applications connect to the Application Server via a three-tier connection.
- **Cherwell Service Host**: Serves as a container host and allows you to configure the following microservices, which use queues to distribute workload:
  - **Automation Process Service**: Monitors events and executes background business rules in your system (example: Notifications and escalations). Automation Processes are configured in CSM Administrator.
  - **Email and Event Monitor Service**: Manages processing for emails sent to CSM.
  - **Mail Delivery Service**: Manages processing for emails sent from CSM.
  - **Scheduling Service**: Executes actions or activities, such as imports and reports, on a time-based recurring basis. Predefined actions are scheduled in CSM Administrator and run by the service (example: A system backup can be scheduled to occur at a set time every night).
  - **System Event Processing Service**: Processes incoming messages triggered by events fired in third-party tools and sent to a CSM webhooks endpoint. The System Event Processing Service is used primarily for webhooks and must be manually enabled before incoming events can be processed.
- **Server Farm**: Provides a framework that consists of a load balancer, multiple web servers, SQL Server, and Redis.
- **Trusted Agent Server**: Allows connections to CSM servers using firewall-friendly protocols; the Trusted Agents perform operations on behalf of CSM servers.

About the Server Manager

The Server Manager is a standalone tool that allows system administrators to efficiently monitor, manage, and configure the CSM services. You can also restart some managed CSM Web Applications.

Use the Server Manager to:

- Monitor the status (running or stopped) of CSM services and Web Applications.
- Start, stop, and restart CSM Servers.
- Restart CSM Web Applications.
- Configure CSM Services: CSM Services are configured by default during installation. If settings need to be changed, use the Server Manager. For example, you can change the protocol used to communicate with the Cherwell Application Server, a connection to the database, or a method of logging Server events.
- Configure the Trusted Agents Server.
- Configure Encryption Keys for CSM services or Web Applications.
- Configure logging for CSM services or Web Applications.
- Configure Overwatch settings.

Add comments or helpful information to the Server Manager. For example, add a note to inform other system administrators of upcoming maintenance.

The Server Manager is automatically installed on the same machine where CSM Servers are installed.

Related concepts
Configure the Application Server
Configure the Cherwell Service Host
Configure Logging for a CSM Service, Web Application, and Cherwell REST API

Using the Server Manager

The Cherwell Server Manager is installed on each CSM server instance. It enables administrators to configure and manage all CSM servers, including the Application Server, the Cherwell Service Host, the Auto Update Service, and CSM Web Applications.

To open the Server Manager:

1. Log in to the a CSM server instance.
2. Search for or navigate to the Cherwell Server Manager.

Start/Stop/Restart a CSM Server, or Restart a Web Application from the Server Manager

Use the Server Manager to stop, start, or restart CSM services and CSM Web Applications.

Instructions for On-Premises Customers

On-premises customers can start, stop, or restart the following CSM services with the Server Manager:

- Cherwell Application Server
- Cherwell Service Host.
- Trusted Agent Server (if installed and configured)

   Note: If using Trusted Agent for security or email operations, restart the Trusted Agent Server first.

- Auto Update Service (if installed).

Use the Server Manager to restart (recycle the application pools for) the following CSM Web Applications:

- CSM Browser Client
- CSM Portal
- Cherwell Web API

To start/stop/restart a CSM service or restart a web application:

1. In the Windows™ Start menu, select **Cherwell Service Management >Server Manager**.

   Note: If the Server Manager application does not appear in the above location it may be located under the **Cherwell Service Management >Tools** menu or there may be a shortcut on your desktop.

2. From the **Server** drop-down list, select a CSM service or web application.
3. Select an operation:
   - To force a refresh of the service status, double-click the **Server Status** icon.
   - To start a selected CSM service or web application, select the **Start Server** button.
   - To stop a selected CSM service or web application, select the **Stop Server** button.
   - To restart a selected CSM service or web application, select the **Restart Server** button.

Instructions for SaaS Customers

Although SaaS customers cannot access the Server Manager directly, they can start/stop/restart a CSM service or restart a web application from the Cherwell Self-Service portal:

1. Log into https://support.cherwell.com.

2. Select **Browse All Services**.

3. Select **Environment Assistance**.

4. Select **Service Restart**.

5. Complete and submit the **Service Restart Request** form. The restart will begin immediately and cannot be canceled after submission.

Any user authorized to submit support incidents through the Cherwell Self-Service Portal can make these service restart requests. Authorized users can stop/start/restart the following services from the Cherwell Self-Service Portal:

- All CSM Web Applications
- Cherwell API Service
- Cherwell Application Server
- Automation Process Service
- Email and Event Monitor Service
- Mail Delivery Service
- CSM Portal
- System Event Processing Service
- CSM Browser Client

Configure the Application Server

Use the Server Manager to configure the 3-tier Cherwell Application Server connection so that connections can be maintained between the CSM Applications and the Database.

Important: TCP connections are a legacy configuration and are only available for systems upgraded from a version earlier than CSM 9.5.0. For new installations of CSM 9.5.0 and later, only HTTP connections are supported.

To configure the 3-tier Application Server connection:

1. Select **Start > All Programs > Cherwell Service Management > Tools > Server Manager**.
2. Select **Application Server** from the Server field drop-down.
3. Select the **Configure** button.
4. Select the **Ellipses** button to select the connection the server should use to connect to the CSM database.
5. Select a connection or select **Add** to configure a new connection.
6. Select **OK**.
7. Select a Server communication method:
   a. **Communicate via HTTP:** The Communicate via HTTP radio button is selected by default and uses HyperText Transfer Protocol (HTTP) to communicate with the Application Server. It is recommended to use HTTP as the Server communication method.
   b. **Communicate via TCP:** Select this radio button to use Transmission Control Protocol (TCP) to communicate with the Application Server.
8. Set a **Use Port** value based on the selected communication method:
   a. **Communicate via HTTP:** Select the default Use Port value of 80.
   b. **Communicate via TCP:** Select the default Use Port value of 8001.

   Note: Use Port values are configurable based on unassigned ports as well as selected Encryption settings. Provide a custom Use Port value if desired.

9. (Optional): Edit the **Server Name**. The Server Name field is disabled by default on newer CSM instances.
10. (Optional): Select **Encrypted** from the **Security Mode** drop-down to sign and encrypt communications using the specified server certificate. The encryption is at the transport level using SSL/TLS. By default, the communications between the Client applications and the Application Server are not encrypted or signed.
11. (Optional): Select the **Encryption Server Certificate**.
12. (Optional): Select a **Certificate Authentication** option to determine how the Server Certificate should be authenticated.
13. Select the **Advanced** tab to view default settings.

Do not change the Advanced Server Configuration settings without consulting Cherwell Support.

14. Select **OK**.

Application Server Reference

Application Server Advanced Settings Tab Reference:

Item	Description
Maximum TCP Connections	Maximum number of client connections the server keeps pooled. **Note:** A client might maintain a connection that is not actively being used for a service request.
Maximum Concurrent Calls	Maximum number of service requests the server handles concurrently. Service requests above this amount fail.
Maximum Concurrent Instances	Maximum number of concurrent service instances. This value is used for testing purposes.
Maximum Concurrent Sessions	Maximum number of concurrent sessions allowed to the server. **Note:** A client may have more than one session at a time. Trying to create sessions above this amount result in an error.
Allowed Connection Backlog	Number of connections above the maximum that can be backlogged before the server returns an error.
Maximum Buffer Pool Size	Maximum memory, in bytes, the server uses for buffering messages. Decreasing this amount can reduce the memory usage of the server but could cause a performance degradation on each service call.
Maximum Message Size	Maximum size of a message, in bytes, the server or client consumes. Messages over this size are not be processed and result in an error. **Note:** The message header is included in this size.
Maximum Message Depth	Maximum depth the client or server accepts when parsing an XML message. Depth refers to the nesting of XML elements in a message.
Maximum Message Table Count	The message table contains the unique names of all elements and attributes in a message as it is consumed on the client or server. If this value is exceeded, an error message is generated. Reports with large datasets could require this setting to be increased.
Maximum Content Length	Maximum number of characters allowed in XML element content.
Maximum Array Length	Maximum allowed size of a message being received by the client or server.
Enable Message Compression	When selected, compresses message traffic between the client and application server.

Item	Description
Enable Service Performance Counters	When selected, allows the entire service behavior to be measured, which can then be used to diagnose performance. These can be found under the performance object when viewing with Performance Monitor (Perfmon.exe).
Enable Rest for HTTP	When selected, the Application Server communicates with REST and gzip rather than SOAP and Cherwell compression. Select this option to use less bandwidth, ensure that communication is more discoverable by standard security tools, and enhance debugging capabilities with external tools, such as Fiddler.
Restore Default Value	When selected, restores all limits and options to their default values.

Related concepts

Using the Server Manager

Configure the Server Connection

Default Port Numbers

Configure the Auto Update Service

Use the Server Manager to configure the Auto Update Service, which automatically checks for newer versions of the Trusted Agent Server.

You can choose to install the Auto Update Service when installing the Trusted Agent Server.

To configure the Auto Update Service:

1. Select **Start > All Programs > Cherwell Service Management > Tools > Server Manager**.
2. Select **Auto Update Service** from the **Server** drop-down menu.
3. Select the **Configure** button.
4. Select the **Ellipses** button to select the connection the server should use to connect to the CSM database.
5. Provide connection to the CSM database:

Option	Description
Connection	Use the **ellipsis** button to browse and locate the database to connect to.
Login to Cherwell	Chose one of these options: ◦ **Windows authentication**: Use the Windows credentials for the account that is used to run the Trusted Agent Service. ◦ **User ID and Password**: Provide a CSM user ID and password. This is usually an administrative account with broad system access, but don't use the CSDAdmin default account. Provide a blank password to allow the specified user to log in without a password. This only works if the user does not have a password. This is not recommended.
Test	Select to verify login information.

6. Select **Advanced Settings** to change the update check interval (default value is 300 seconds), download folder, and application folder.

Configure Encryption Keys for a CSM Server or Web Application

Use the Server Manager to configure encryption keys for CSM Servers or Web Applications. Encryption keys protect sensitive data contained in Business Object Fields (example: Financial data, SSNs, etc.). When configuring encryption keys, you can:

- Add keys, or modify the display name of existing keys.
- Import and export keys using password-protected Cherwell Key Files (.ckf) to move them across systems.
- Configure compliance logging to the Splunk Server to log decryption attempts (whether or not they are successful).

Good to know:

- The ability to configure encryption keys depends on your security rights.
- Encryption keys are managed on a per-server basis; all servers within a server farm require the same encryption keys.
- Encryption keys are protected using Windows Data Protection API (DPAPI) and are stored in a restricted area of the Windows file system (the Windows Keystore). The keys cannot be accessed directly; they can only be managed using the Encryption Key Management interface in the Server Manager.
- Compliance logging to a Splunk server is handled separately from event logging for a Server or web application. For more information on integrating Splunk and CSM, see Splunk Integration (Splunk Integration, http://docs.splunk.com/Documentation). The Splunk integration is included in hosted environments by default. Compliance logging is optional.
- Internal CSM auditing is enforced. CSM uses Journal-History records to track encryption/decryption attempts for encrypted fields in Business Object records.
- References to encryption keys (identifiers and display names) are stored in the CSM database in a table separate from the Business Objects to which they belong; however, the actual encryption keys are not stored in the database. We recommend exporting keys to a password-protected Cherwell Key File (.ckf) and storing them in a secure location as backup. As a best practice, store .ckf and .czar files in separate locations.

To configure encryption keys for a CSM Server or Web Application:

1. Select **Start > All Programs > Cherwell Service Management > Tools > Server Manager**.
2. From the Server drop-down, select a **Server** or **Web application**.
3. Click the **Configure** button next to Encryption keys.
4. Select a database connection and enter your login credentials.

   Note: This can only be done on a two-tier connection and is intended to be performed directly on the server running CSM.

The Encryption Key Management window opens.

5. Add an encryption key:
   a. Click the **Add** button.

   b. In the Prompt window, enter a **name** for the key. This is a display name only; the actual key is stored in the Windows Keystore.

   > **Tip:** To edit the display name of an encryption key, select the key, and then click the **Edit** button.

   c. Select **OK**.

   A caution message opens, giving you the option to export encryption keys.

   d. Click **Yes** to export keys to a password-protected .ckf file.

   > **Note:** You can choose not to export keys. However, we recommend exporting and storing them in a secure location. Encryption keys are not stored in the database, and therefore are not exported in .czar files.

   e. If exporting keys, specify a **folder location** and **name** for the .ckf file.

   f. Click **Save**.

   Before the file is saved, you are prompted to enter a password to protect the file.

6. (Optional) Configure compliance logging:
   a. Select the **Compliance Logging** check box.

   b. Click the **Configure** button.

   The Splunk Server Settings window opens.

   c. Define the following settings:
      ◦ **Server URL**: Provide the URL of the Splunk Server (example: https://splunkserver:8089).

      ◦ **User Name**: Provide the user name for the Splunk Server acount.

      ◦ **Password**: Provide the password of the individual with an account on the Splunk Server.

      ◦ **Ignore Certificate Errors**: Select this check box to ignore certificate errors that might be generated by Splunk using self-signed certificates to encrypt data. Select this check box only if you trust your connection with the server.

   d. Select **Test** to test the connection to the Splunk Server.

   e. Select **OK**.

7. Close the Encryption Key Management Window.

8. Configure encryption keys for another server or web application, as necessary.

Configure Logging for a CSM Service, Web Application, and Cherwell REST API

Use the Cherwell® Server Manager to configure logging for CSM services, CSM Web Applications, and the Cherwell REST API. Logging records significant events and errors, and is used for troubleshooting.

Logging can be configured to go to an event log, a file locations, or a Splunk server. For more information about integrating Splunk and CSM, see Splunk Integration and http://docs.splunk.com/Documentation.

You can configure separate logging for:

- Cherwell Application Server

    Note: The Cherwell Trusted Agent Service logs messages through the Cherwell Application Server and will follow the Cherwell Application Server's log settings. See Trusted Agent Logging.

- Cherwell REST API
- Cherwell Service Host and its microservices (Automation Process Service, Email and Event Monitor Service, Mail Delivery Service, Scheduling Service, and System Event Processing Service)
- CSM Web Applications

Use these guidelines to configure logging:

- Consider logging debug messages (debug and above) to a file or to Splunk, and not to an event log. CSM logs numerous debug messages, so a log would be slow and might require more resources. When logging is enabled for the Cherwell Application Server, the logging settings will also apply to the System Upgrade and System Restore Utilities.
- Logging may need to be enabled for multiple services. For example, if you use CSM Desktop Client with a 3-tier connection using Trusted Agents, enable logging for the Cherwell Application Server and the Trusted Agent Service.
- Best practice is to separate each server or application to point to its own logging file.
- If you log to a file for the CSM Web Applications, the log file must be stored in a location accessible to the account that IIS uses to run the CSM sites. This is typically the ApplicationPoolIdentity, also referred to as the IUSR account. To prevent security issues, do not configure the IIS Application Pool to use the LocalSystem account.
- You can use the Log Viewer utility to view logs in CSM Administrator, but you must save logs to files.
- Logging can be enabled for each instance of the Desktop Client. For more information, refer to Configure User General Settings.

To configure logging:

1. Select **Start > All Programs > Cherwell Service Management > Tools > Server Manager**.
2. Select a service from the **Server** drop-down list.

> **Note:** If you select the Cherwell Service Host, logging is enabled for all microservices. To configure logging for specific microservices, select **Cherwell Service Host**, select **Logging**, and then select the microservice from the **Services** list.

3. Select **Logging**.

   The **Logging Options** window for the selected service opens.

4. Define logging options for the selected service. See Logging Options.

5. Select **OK**.

Related concepts
Blueprint Editor Menu Bar
Logging Options
About the Server Manager
Related tasks
Log Viewer Utility

Configure Logging to a Splunk Server

Use the Server Manager to configure event logging for selected CSM services to a Splunk Server. Event logging records significant events and errors, and is used for troubleshooting.

Splunk is a third-party tool that identifies data patterns, provides metrics, diagnoses problems, and provides intelligence for business operations. CSM integrates with Splunk so that CSM event log data can be indexed and made easily searchable. Download and install Splunk onto a server and configure it for logging events.

To configure logging to a Splunk server:

1. Select **Start > All Programs > Cherwell Service Management > Tools > Server Manager**.
2. Select a service from the **Server** drop-down list.

   > **Note:** If you select the Cherwell Service Host, logging is enabled for all microservices. To configure logging for specific microservices, select Cherwell Service Host, then click the **Logging** button and select the microservice from the **Services** list.

3. Click the **Logging** button.

   The Logging Options window for the selected Server opens.

4. Select the **Log to Splunk** check box.
5. Select a log level:
   - **Debug and above**: Very verbose messages. This level is space and resource intensive.

     > **Note:** For best results, log debug messages (Debug and above) to a file or to Splunk, and NOT to an event log. CSM logs numerous debug messages, so a log would be slow and might require more resources.

   - **Stats and above**: Detailed messages that track performance.
   - **Info and above**: Informational messages that can be used to diagnose a problem.
   - **Warning and above**: Warning messages that occurred.
   - **Error and above**: Errors that were encountered.
   - **Fatal only**: Errors that caused the service or process to stop.
6. Click **OK**.
7. In the Log Server area, click the **Configure** button.
8. Define the following settings:
   - **Server URL**: Provide the URL of the Splunk Server (example: https://splunkserver:8089).
   - **User Name**: Provide the user name for the Splunk Server acount.
   - **Password**: Provide the password of the individual with an account on the Splunk Server.

◦ **Ignore Certificate Errors**: Select this check box to ignore certificate errors that might be generated by Splunk using self-signed certificates to encrypt data. Select this check box only if you trust your connection with the server.

9. Select **Test** to test the connection to the Splunk Server.

10. Select **OK**.

Related concepts

Configure Logging for a CSM Service, Web Application, and Cherwell REST API

Logging Options

Logging Options

Logging options apply to most CSM logs, such as the Cherwell® Service Host, Cherwell Application Server, and the Cherwell REST API. Users can create custom logs from the CSM Desktop Client, as well. For each CSM log, you can choose to log to the event log, to a file, or to Splunk.

From the **Logging Options** window, select one of the following log locations:

- Select **Log to event log** to log CSM events to the Windows Event Viewer. Then, the log level:
  - **Debug and above**: Very verbose messages. This level is space and resource intensive.

    Note: For best results, log debug messages (Debug and above) to a file or to Splunk, and NOT to an event log. CSM logs numerous debug messages, so a log would be slow and might require more resources.

  - **Stats and above**: Detailed messages that track performance.
  - **Info and above**: Informational messages that can be used to diagnose a problem.
  - **Warning and above**: Warning messages that occurred.
  - **Error and above**: Errors that were encountered.
  - **Fatal only**: Errors that caused the service or process to stop.

    Note: In the Windows Event Viewer, CSM events are visible under **Applications and Services Logs > CSM - Cherwell Service Management**.

- Select **Log to file** to write the logs to a specific location and file for the selected service. Then, set your file limits.
  - **Log Level**: Select a log level.
  - **File Name**: Select the ellipses button to select a location and file name for the log file. When you configure log files:
    - For the Browser Client and CSM Portal, the logging path is automatically modified using the application name. For example, if the user chooses the file path c:/logs/logs.log, the system will use c:/logs/*{application name}*/logs.log.
    - For the Cherwell Service Host, specify a file location and name.
    - For the Cherwell Service Host microservices, you only need to specify a file location. A log file is automatically created for each microservice leader and worker.
    - For the Cherwell Web API (Cherwell REST API), which is required for CSM authentication, the recommended setting is to log warnings and above to the Windows Event Viewer and debug and above to a specified file location.
  - By default, the file size is set to 10 MB, but can be changed by entering a new value in the **File Size Limit** field.
  - **File Count Limit**: Rolling event logs are used, so that when the maximum file size is reached for a log file, a new file is created. By default, the number of files is set to 20 (but can be changed), after which the oldest log file is overwritten by continued logging.
- Select **Log to Splunk** to write the logs to a Splunk server, and then configure Splunk logging.

Related concepts

Configure Logging for a CSM Service, Web Application, and Cherwell REST API

Configure Logging to a Splunk Server

Configure User General Settings

Define a Write to Log Action

Configure Logging for the Cherwell REST API

If issues occur when working with CSM features that rely on the Cherwell REST API (example: Authentication, Saved Searches, and webhooks), you can configure event logging in the Cherwell Server Manager to log warnings and errors that are associated with REST API.

The base URL for the Cherwell REST API is required for CSM authentication. If the base URL is not configured properly through the Cherwell Server Manager or the Command-Line Configure utility, users will get an error when logging in to CSM.

Configure event logging for warnings and errors that are associated with the REST API:

1. To open the Cherwell Server Manager, select **Start > All Programs > Cherwell Service Management > Tools > Server Manager**.

2. In the **Server** field, select **Cherwell Web API**.

3. Select **Logging**.

4. Select your logging location and level of log messages. The recommended setting is to log warnings and above to the Window Event Viewer and debug and above to a specified file location. See Logging Options for more information.

5. Select **OK**.

6. Select **Restart server** to apply the changes.

Related concepts
Logging Options
Set the Base URL for the Cherwell REST API
Cherwell REST API Command-Line Options

About Overwatch

Cherwell Overwatch provides a centralized place to manage CSM settings.

Overwatch is a Windows service included when you install the Cherwell Server. You can continue to use Cherwell Server Manager to update CSM Services, but those updates will now be stored in Overwatch. Settings managed in web.config files in previous versions of CSM are now made in Overwatch.

In addition to handling settings changes made through the Cherwell Server Manager, you can access Overwatch via Command-Line Configuration to control other settings, like web.config settings, which are not available in Server Manager. You will find this especially useful if your on-premise implementation uses Redis and multiple front-end services, as Overwatch is now the single place to update settings for all servers.

Configure Overwatch itself via the Cherwell Server Manager. If you want to connect to Overwatch running on a different server, provide the info there. When you update them, restart all services. Restart IIS from an Administrator prompt to ensure services are recycled correctly.

Configure Overwatch Settings

Use the Server Manager to configure Overwatch settings. You should only need to change the default settings if you are not running Overwatch on the same server as your Cherwell installation.

To configure Overwatch settings:

1. Select **Start > All Programs > Cherwell Service Management > Tools > Server Manager**.
2. Select the **Configure** button next to **Overwatch Configuration**.
3. Edit the settings if your Overwatch instance is at a different location than your Cherwell Server installation.

Option	Description
Overwatch URL	Location of the Overwatch instance. Default is http://localhost:5000
Environment Key	This key is used by the CSM service to attempt to connect to an instance of Overwatch.
Registration Key	This key is used by Overwatch to allow CSM applications access to settings.
REST API URL	Defaults to the same base URL for the API used by the rest of CSM.

4. Restart IIS from an Administrator prompt to ensure services are recycled correctly.

About the Cherwell Service Host

The Cherwell Service Host serves as a container for these microservices: Automation Processes, Email and Event Monitoring, Email Delivery, Scheduling, and System Event Processing.

The microservices use the Cherwell Message Queue Service, which is a centralized queue that enables workload distribution. The microservices can be configured to allow for both local and remote installations of the Cherwell Service Host to process the queue, providing increased throughput.

Each piece of work sent to the Cherwell Message Queue Service is considered a message. For example, email messages sent from CSM are delivered to Cherwell Message Queue Service; the Mail Delivery Service consumes the messages from the queue and sends them.

Each microservice has:

- A leader that monitors the CSM database and identifies work that needs to be done. That work is then queued.
- Multiple workers that pull work off the queue and then complete that work.

Monitor the number of workers and workload on the RabbitMQ management interface to help determine when you need to scale the Service Host or manually multiply the number of workers.

Good to Know:

- You can set the database connection for the Cherwell Service Host in the Cherwell Server Manager.
- You can monitor, stop, and start the Cherwell Service Host from Cherwell Server Manager or the Command Line Configure utility.
- No actual user or email data will be stored in queue channels with the Cherwell Message Queue Service. The service only uses IDs used to complete processes.

Related concepts
Automation Processes
About the Scheduler
About the Email and Event Monitor
Configure the Cherwell Service Host
Monitor Queues from the RabbitMQ Management Interface

Configure the Cherwell Service Host

The Cherwell Service Host, its five microservices, and Cherwell Message Queue Service are automatically installed with the Server Installation, but you can choose which microservices to enable as you install. You can later enable or disable microservices and configure connection settings in the Cherwell Server Manager.

The Cherwell Service Host manages these microservices:

- Automation Process Service
- Email and Event Monitor Service
- Mail Delivery Service
- Scheduling Service
- System Event Processing Service

The microservices process and add work messages to queues, which are managed by the Cherwell Message Queue Service. Each microservice has a single queue, but you can distribute microservices across multiple servers to enable horizontal scaling.

Use the Server Manager to configure these Service Host settings:

- Configure connection and login settings.
- Enable or disable microservices.
- Configure logging for the Cherwell Service Host and microservices.
- Configure Message Queue connection settings.

Good to know:

- You must configure and start the Cherwell Service Host after you install or upgrade CSM.
- A 2-tier connection is required for the Cherwell Service Host, unless you are using it to run a local Scheduling Service (and no other microservices) on a separate network. Then, a 3-tier connection is required. For information, see Configure the Cherwell Service Host for a Local Scheduler.
- Use the Configuration Command Line Utility to configure the settings above and to additional settings, such as setting the maximum number of workers per virtual processor.

Configuring Service Host Connection and Login Settings

The Service Host can be installed on a single server or on multiple servers, depending on the needs for your environment. Use connection and login settings to ensure that each instance of the Service Host uses the same database connection.

To configure connection and login settings:

1. Select **Start > All Programs > Cherwell Service Management > Tools > Server Manager**.
2. From the **Server** list, select **Cherwell Service Host**.

3. Select the **Configure** button.

4. Select the connection the Service Host should use to connect to the CSM database.
   If the name of the correct database connection is not displayed, select the **ellipsis** button to open the **Connection** window and select an existing connection or configure a new connection.

5. Select the method the Service Host will use to log in to CSM.

Option	Description
Windows Authentication	Uses the account associated with the Windows credentials used by the Windows server. Windows must be a supported login mode (In CSM Administrator, go to **Security > Security Settings**, select the **Desktop Client, Browser Client,** or **Browser Portal**, and in the Supported login modes section, select **Windows**).
User ID and Password	Uses CSM login credentials. Provide the username and password. This is usually an administrative account with broad system access, but don't use the CSDAdmin default account.
Blank Password	Allows a user to log in without a password. This only works if the specified account does not have a password assigned. This is not recommended.
Execute Using Default Role of This User	Runs the Service Host using the properties of the view associated with the role that the login account is configured to use. When this setting is not selected, this CSM Server uses a system default role. However, control the behavior of field properties in a view, based on the role of the logged in user, by making this selection. In other words, based on a custom view for the role of the person logging in (example: IT Manager), the behavior of the fields for a Business Object can be different when a record is created or modified.

6. Select **Test** to confirm that the login/connection works.

Enabling or Disabling Service Host Microservices

During the CSM installation or upgrade process, the Cherwell Service Host is configured and you choose which microservices to enable by default.

This might be useful for distributing the microservices across multiple services. For example, if your system processes a large number of email messages on a regular basis, consider moving the Mail Delivery Service to its own server. In this case, you would enable the Mail Delivery Service, but disable all other services.

1. Select **Start > All Programs > Cherwell Service Management > Tools > Server Manager**.

2. From the **Server** field drop-down menu, select **Cherwell Service Host**.

3. Select the **Configure** button.

4. Select the **Advanced Settings** button.

5. Select the check box for each microservice to enable it; clear the check box to disable it:
   ◦ Automation Process Service

   ◦ Email and Event Monitor Service

   ◦ Mail Delivery Service

   ◦ Scheduling Service

   ◦ System Event Processing Service

> **Note:** You can choose to run all Scheduled Items on the machine or select a Scheduling Group to run a specific set of Scheduled Items. If you choose to run multiple Scheduling Groups, you must distribute the work across multiple machines.

Configuring Logging for the Service Host and Microservices

You configure separate logging for the Cherwell Service Host and its microservices. For each microservice, separate log files for leaders and workers are created.

Event and file logging apply to the machine on which logging is configured in the Server Manager. See Configure Logging for a CSM Service, Web Application, and Cherwell REST API.

To aggregate logs across distributed machines, use Splunk.

Related concepts

Configure Logging for a CSM Service, Web Application, and Cherwell REST API

Service Host Command-Line Options

Connect Multiple Cherwell Service Hosts to a Single CherwellMQS

Configure CherwellMQS/RabbitMQ

Configure the Cherwell Service Host for a Local Scheduler

For SaaS customers, it is possible to configure the Cherwell Service Host to run the Scheduling Service on your local network. Configuration steps include creating a new Schedule Group and then associating that Group with the Cherwell Service Host. These steps can also be used in on-premises systems to run the Scheduling Service on a separate network from your main CSM installation.

Most environments have the Scheduling Service on the same network as the other CSM services. However, in some cases you may want to set up a second Scheduler on a separate network. A common use case for such a configuration in SaaS environments is setting up a schedule to run a report and save a PDF of the report on your local network. Another use case is setting up a schedule to import a locally generated file into CSM. For example, you might want to create a schedule that runs a PowerShell script on your local network, save the output as a .csv file, and then import that .csv file into CSM. In this case, the script can access resources on your local network that are not available to the CSM server. This type of configuration is less common in on-premises environments, but if your organization utilizes multiple networks, you may find it useful for similar reasons.

Requirement for 3-Tier Client Connection With Locally Installed RabbitMQ

Running a local Scheduler in a SaaS environment requires a 3-tier connection between the Cherwell Service Host and your SaaS connection (or your main CSM server in on-premises installations).

Also, to use the Scheduling Service in your local network, you must also configure the Cherwell Message Queue Service (RabbitMQ) so that it can communicate with the Cherwell Service Host on your local network. The Cherwell Service Host does not use the RabbitMQ that is installed on the CSM server that is hosted by Cherwell.

Create the Schedule Group

Schedule Groups allow you to set up schedules for a specific Cherwell Service Host.

> **Note:** The default Schedule Group (**[Default]**) is designed for running Scheduled Items in a SaaS environment only.

To create the Schedule Group:

1. Open CSM Administrator, and select **Scheduling > Edit Schedule**.
2. In the **Scheduled Items** window, select **Add**.
3. Beside the **Schedule group** field, select the ellipses button to create a new group for Schedule Items that you want to run locally (example: `MyLocalServer`).
4. Save your changes.

Configure the Cherwell Service Host

After you create the Schedule Group to run Scheduled Items in your local environment, you must enable the Scheduling Service in the Cherwell Service Host and configure it to point to the new Schedule Group.

To configure the Cherwell Service Host:

1. Open the Cherwell Service Host (**Start > All Programs > Cherwell Service Management > Tools > Server Manager**).

2. In the **Cherwell Server Manager** window, in the **Server** field, select **Cherwell Service Host**, and then select **Configure**.

3. In the **Cherwell Service Host** window, select **Advanced Settings**.

4. Select **Scheduling Service**, and then select the Schedule Group that you created earlier to run on your local network (example: `MyLocalServer`).

5. Make sure that the Automation Process Service, Mail Delivery Service, and Email and Event Monitor Service are disabled, as they can cause problems by taking over from the main Cherwell Service Host.

6. Select **OK** to save your changes.

7. In the **Cherwell Server Manager** window, select **Configure** on the Message Queue line.

8. Configure the Cherwell Message Queue Service to connect to your local RabbitMQ instance.

9. Select **Save** to save your changes.

Now, the Cherwell Service Host will run only the Scheduled Items that are configured for your local Schedule Group.

Related concepts

Configure CherwellMQS/RabbitMQ

Configure the Cherwell Service Host

About the Scheduler

Related information

Configure the Client Connection

Configure CherwellMQS/RabbitMQ

The Cherwell Message Queue Service (CherwellMQS) is required for queuing. CherwellMQS requires minimal configuration.

The RabbitMQ User ID and password are set to admin/admin during installation. It is highly recommended that you change this password after installation and update the RabbitMQ credentials in CSM. When you change the RabbitMQ credentials, you must also update the credentials in CSM.

The RabbitMQ credentials are set using the RabbitMQ Management Interface and the credentials are configured in CSM using the Command-Line Configuration option or the Message Queue configuration in the Server Manager. The following procedures describe credential configuration using the CLC option.

> **Note:** Both Cherwell Service Host and the Application server use message queuing and must be recycled if any CherwellMQS details change.

Disable Queuing

- Use the Cherwell Server Manager to stop the Cherwell Service Host.
- Use the Windows Services Manager to stop the CherwellMQS.

Change Administrator Credentials in RabbitMQ

1. In a browser, enter the RabbitMQ Management Interface URL:
   http://localhost:15672

2. Log in with the RabbitMQ credentials.

3. On the **Admin** tab, select **admin** from the Name column of the Users table.

4. In the Update this user section of the User page, enter the new password in the **Password** field and in the **Confirm** field.

5. Click **Update user**.

> **Note:** Because you are changing the password for the user you are logged in as, you will see an error message with the message, "Login failed." To make additional changes in the RabbitMQ Management Interface, log out and log back in.

6. Close the RabbitMQ Management Interface.

Update RabbitMQ Credentials in CSM

1. Stop Cherwell Service Host and Cherwell Message Queue Service.

2. On the primary Message Queue Service host machine, open a Command window from the Cherwell Service Management folder.

3. Run the following command:

```
Trebuchet.CommandLineConfigure.exe -messagequeue -connectionuserid=[NEW USER ID] -connectionpassword:[NEW PASSWORD]
```

4. Restart the Cherwell Service Host and the Application server.

Related concepts

About the Cherwell Service Host

Configure the Cherwell Service Host

Connect Multiple Cherwell Service Hosts to a Single CherwellMQS

Advanced Configurations for the Cherwell Service Host

Only one Cherwell Message Queue Service (CherwellMQS) node is permitted per CSM environment. Configure complex systems with Cherwell Service Host by adding multiple service host instances, connecting distributed Cherwell Service Host instances to a primary CherwellMQS instance, or connecting distributed Cherwell Service Host instances to a RabbitMQ cluster.

During the Server Installation, CherwellMQS is automatically installed. By default, Cherwell Service Host is connected to the CherwellMQS instance on the machine on which it was installed. If you use multiple instances of the Cherwell Service Host, you must connect those distributed instances to a primary CherwellMQS or connect all RabbitMQ instances into a cluster and leave Cherwell Service Host connected to the CherwellMQS instance on the machine on which it was installed.

Adding Multiple Service Host Instances

Add multiple instances of the Cherwell Service Host and distribute microservices across multiple machines to distribute the queuing workload. Use the Server Installer to add the Service Host and selected microservices to additional machines.

To add Service Host instances:

1. Verify that your main instance of the Cherwell Message Queue Service and Cherwell Service Host are configured correctly and running. See Configure the Cherwell Service Host.

2. Launch the CSM Server installer, and select normal installation options until you come to the Database Selection page.

3. Select the **Don't load any data** option. Select **Next**.

4. On the Server Selection page, select one or more of these microservices:
   - Automation Process Service
   - Scheduling Service
   - Email and Event Monitor Service
   - Mail Delivery Service
   - System Event Processing Service

   🖉   **Note:** You can clear the **Application Server** check box.
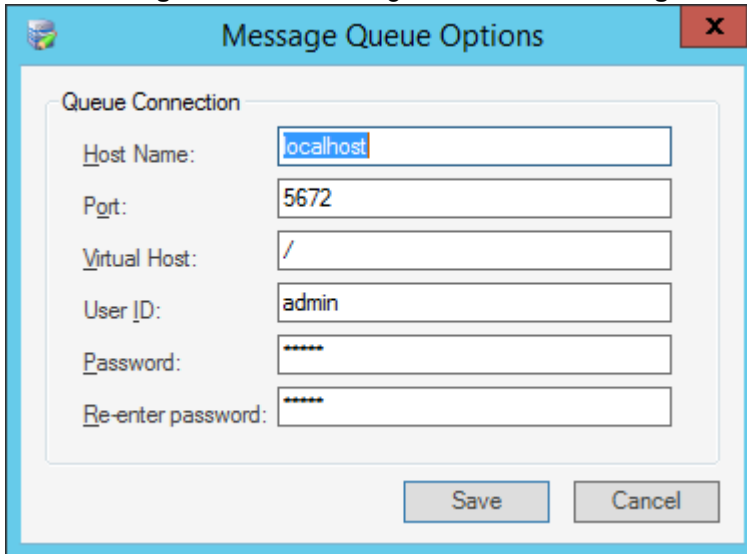
5. Click **Next**.

6. On the Logon Information page, select a user account that has privileges to run and modify services on the machine.

7. Click **Next**, and then finish the installer.

Connect Multiple Cherwell Service Hosts to a Single CherwellMQS

Though a RabbitMQ node is installed along with Server Installation, you can choose to point to an existing node of RabbitMQ. If you have multiple Service Hosts, you can configure them to point to the same RabbitMQ node, or you can set up RabbitMQ clustering and direct the Service Hosts to the cluster.

To connect multiple Cherwell Service Host instances to CherwellMQS:

1. On the machines that have distributed instances of Cherwell Service Host, open the Cherwell Service Manager.

2. Select **Configure** next to Message Queue. The **Message Queue Options** dialog box opens.

3. In the **Host Name** field, change "localhost" to the server name or IP address of the primary CherwellMQS instance.

4. Change the User ID and password to match the credentials for the primary instance of CherwellMQS.

    Note: You should change the default CherwellMQS password as part of your initial configuration of CSM. See Configure CherwellMQS/RabbitMQ.

5. Select **Save**.

6. Repeat for each distributed instance of CherwellMQS.

Connect Multiple Cherwell Service Hosts to a RabbitMQ Cluster

Cherwell Service Hosts cannot point to multiple RabbitMQ nodes. However, each machine with Cherwell Service Host installed also has CherwellMQS installed. If each instance of CherwellMQS is part of a single RabbitMQ cluster, the Service Host can remain connected to its local version of CherwellMQS.

RabbitMQ clustering is configured outside of CSM and guidance is not provided by Cherwell Support. See https://www.rabbitmq.com/clustering.html for information about RabbitMQ clustering.

Monitor Queues from the RabbitMQ Management Interface

RabbitMQ, which is the message-oriented middleware used by Cherwell Message Queue Service (CherwellMQS), offers a management interface for on-premises installations that displays data related to queues and connections.

Use the data that RabbitMQ provides to make informed decisions about scaling CSM microservices. Helpful data includes a list of machines with CSM installed connecting to RabbitMQ, the number of workers, the number of pending messages, and the number of queued messages.

> **Note:** Access to the RabbitMQ Management Interface is only available for on-premises installations of CSM.

Opening the RabbitMQ Management Interface

Use a standard web browser to access the RabbitMQ management interface.

The default location of the management interface is http://localhost:15672. The default login ID and password are admin/admin. To change these default settings, refer to the RabbitMQ documentation.

> **Note:** The CherwellMQS settings must match RabbitMQ. If you update the username or password for RabbitMQ, as is advised, you must update the CherwellMQS settings to match. See Configure CherwellMQS/RabbitMQ.

RabbitMQ Connections

The Connections tab of the RabbitMQ management interface provides data to help monitor connections.

Identifying Connections

The Connections tab on the RabbitMQ management interface displays the following information when Cherwell® Service Host is started:

Information	Description
Machine Name	The name of the server hosting CSM. If CSM is horizontally scaled, it will display multiple machine names.
Process ID	Windows assigned value. This information is also in Task Manager on the "Details" tab for a specific CSM process that is running.
AppDomain ID	Internal to .NET. There will be a different integer value for each CSM service that is running under Cherwell Service Host.
Trebuchet object name	Either display the Exchange name or the Queue name, depending on the nature of the queuing.

RabbitMQ Queues

The RabbitMQ management interface provides data to help monitor queues.

Monitoring Queues

The Queues tab on the RabbitMQ management interface displays the following information when Cherwell Service Host is started:

Information	Description
Name	The name of the queue is a reflection of the service it supports.
Consumers	Each queue must have at least one consumer when it is initially set up.
Messages	Messages are the number of messages currently being held by the queue.

Queue Naming Conventions

Queues names are created using the following pattern:

```
[Code Namespace].messages.[Queue Name].[Partition Key].[ServiceHostIdentifier]
```

The last three components are described in the following table:

Component	Description
Queue Name	Lists what type of items are in the queue and is used to discern how to interpret metrics that deal with the number of items in the queue.
Partition Key	Primarily used for scenarios where multiple CSM instances share a single RabbitMQ instance. For on-premises environments, the partition key should be constant, but may get changed on upgrade of CSM.
Service Host Identifier	Allows you to determine machine-specific queues where applicable. Not all queue names are scoped per machine.

Consider this queue name as an example:

Trebuchet.Plugin.core.services.messages.Starttaskmessage. 909e287f-a1fa-4f53-be17-194a0a061770.15424

This queue name has the following components:

- Queue name: Starttaskmessage
- Partition Key: 909e287f-a1fa-4f53-be17-194a0a061770
- Host identifier: 15424

Queue names can indicate information about their ready and unacknowledged (unacked) message volumes. In the following table, some of these elements are described. Large queues refer to the total number of items in the queue:

Queue Name Element	Description
Sendmailrequest	Large queues are representative of items pending retrieval from the database for transmission.
Automatedprocessmsg	Large queues are representative of items which are pending processing for AP (Automated Processing) Events. **Note:** Each message does not usually correlate to a single Business Object as a message can signal to process multiple records.
Schedulemsg	Large queues are representative of items that are pending processing by the scheduler. Each message includes items that are due to be run but not items that have not reached time to execute.
Starttaskmessage	A request to create a new worker for scaling. The number of messages waiting should always be small (less than 20% of the maximum number of workers).
Stoptaskmessage	A request to remove a worker. This occurs when the Cherwell Service Host is scaling down workers after high activity. The number of messages waiting should always be small (less than 20% of the maximum number of workers).
Restarttaskmessage	Each worker sends a heartbeat periodically. A process monitors workers, and if the worker has a critical error, the worker will be restarted. This message is used to queue a worker to be shutdown. **Note:** Any messages indicate critical failures for the service host and should be investigated.
Emaildeliverymessage	Large queues are representative of items pending transmission.
Heartbeatmessage	Each worker generates periodic messages to alert the Cherwell Service Host that the worker is responsive and report metrics. Large message counts could indicate a failure in the Cherwell Service Host monitoring. (This should be very close to 0.)

Note: Select an item on the RabbitMQ management interface to drill down and investigate a specific queue.

Exchange Types

Queues names are created and managed by CherwellMQS. They are based on the type of exchange the queue is bound to. CSM uses two types of exchanges:

- Direct: Delivers a message to a single queue based on the message routing key.
- Fanout: Delivers messages to multiple unique queues bound to the exchange. In a Fanout exchange, the routing key is ignored.

The name for a queue that is bound to a Direct exchange is a combination of the name of the message, the tenant's partition key, and depending on the behavior of the message, the instance ID. The name for a queue that is bound to a Fanout exchange includes the message handler's target name to create multiple queues to handle multiple messages per instance.

> **Note:** Since queue names created automatically by CherwellMQS with specific meaning, Users should not attempt to edit or rename queues.

Analyzing Messages

The Overview tab on the RabbitMQ management interface displays data that helps determine the health of the queue over time. Monitor trends of published messages, consumed messages, and queued messages. Pay attention to the following graphs in the Overview tab:

- Queued messages: This graph displays the number of messages queued over time. If there is a growth rate, then the queue will fall behind and eventually overflow.
- Message rates: This graph displays the most basic and telling metric in the queuing system. If the number of messages being Published is greater then the number of Consumer acknowledged (acked) messages, then the system is getting more work requests then it can handle. In this case, steps must be taken to prevent a failure

Analyzing Queuing Data

Decisions you make regarding scaling CSM services or multiplying the number of workers available on any single Cherwell Service Host machine depend on a number of factors. Each organization has unique needs, and you must consider the needs of your organization to determine the best scaling options.

For example, you may see short-terms spikes in the amount of queued work based on business demands or on your organization's business hours. Or, you may notice one CSM microservice is continually filling the queue when it is enabled on a machine where other microservices are enabled.

When to scale or distribute microservices:

Consider adding another machine instance of the Cherwell Service Host in these cases:

- The numbers of consumers, pending messages, or messages queued grows or remains even over a period of time.
- The CPU of the Cherwell Service Host machine consistently hits or exceeds unacceptable ranges.

Use the Server Installer to add the Cherwell Service Host to additional machines. See Advanced Configurations for the Cherwell Service Host.

When to multiply the number of workers on a Cherwell Service Host machine:

Consider multiplying the number of workers on a single machine in these cases:

- The numbers of consumers, pending messages, or messages queued grows or remains even over a period of time.
- The CPU of the Cherwell Service Host machine is not fully used.

Use the Configuration Command-Line Utility to increase the number of workers per virtual processor on each Cherwell Service Host machine. See CherwellMQS Command Line Options.

CherwellMQS Metrics

Identify the metrics on the RabbitMQ management interface that help monitor queues and connections.

Use the following RabbitMQ metrics, which can be found in the management interface, to monitor queue health:

Metrics	Descriptions
Disk space used	Ideal is less than 50 mb per node. On the machine where RabbitMQ is installed, an important metric to track is the amount of disk space used. This metric reflects how many messages each RabbitMQ node is using to store messages that are queued or in process. See https://www.rabbitmq.com/disk-alarms.html.
Memory used	Ideal is less than 20 percent of the entire machine. Once RabbitMQ exceeds a default threshold of 40%, RabbitMQ will start to block all connections that are publishing messages. See https://www.rabbitmq.com/memory-use.html.
Connection performance	All traffic flows through a TCP connection. Monitoring the connection will help you understand the traffic for the application, see how the network is used, and determine if there are connectivity issues. See https://www.rabbitmq.com/reliability.html.
Data rates	This includes throughput and performance. Queues receive, push, and store messages. After a message is routed through an exchange, it is placed in a queue. A queue is the final destination within RabbitMQ before the message is passed to an application.
Queue depth	Number of the messages in the queue.
Messages unacknowledged	Number of messages a queue has delivered without receiving an acknowledgement from a consumer.
Messages ready	Number of messages available to be consumed.
Message rates	Number of messages that move in and out of a queue per second. This is highly variable from tenant to tenant, depending on the type of work being done and how long each piece of work takes. A complicated Automated Process will result in a lower message rate. Monitor this section to see messages pass from the Ready state to the Unacked state. If there are messages in the Ready state, then there should be an equal number of messages in the Unacked column as Consumers for that queue. With enough time on a given tenant, a pattern starts to emerge.
Number of consumers	Number of workers that are registered to do work from that queue. Each service is designed to scale within the bounds of its settings. If there is a lower, or higher then expected number of consumers, it could mean there is a failure of some type in Cherwell Service Host.
Consumer utilization	Time that a queue's consumer could take on new messages. It is a number between 0 and 1, or NA if a queue does not have any consumers. If the utilization is less then 1 (100%) then a consumer is not able to take a message. This can be an indication of network congestion.

Troubleshooting Queues in CherwellMQS

It is important to know how to interpret CherwellMQS through the RabbitMQ management interface.

When a Queue Appears Stuck

Sometimes, a worker is unable to process a request, so an item will sit as unacknowledged (unacked) and appear to be stuck. For a scheduled job, deleting the queue may mean that job and subsequent jobs won't run until the next scheduled time. Similarly, deleting Automation Process (AP) events that are queued and unacked could keep them from being processed, and removing mail delivery queues could keep items that are in an unacked state from being sent. All queues with a Cherwell Service Host identifier can be cleanly deleted if needed.

Use the Get Messages section to check messages in the queue and remove a troublesome message without deleting the whole queue. In normal cases, you will see unacked messages in the queue and the system will not be processing the messages. The number of unacked messages stays the same while the Ready count increases. There are two options in the Get Messages section in the **ACK Mode** drop-down list that allow you to perform these actions:

- Nack message requeue true: An ultimately non-destructive action that reads the message and adds it back into the queue in the same position.
- Automatic ack: A destructive action that acknowledges the message from the queue and then does not requeue the message.

To identify a stuck item in a queue:

1. In a browser, enter the RabbitMQ Management Interface URL:
   http://localhost:15672

2. Log in with the RabbitMQ credentials.

3. On the **Queues** tab, select the queue with the stuck message.

4. Expand the **Get Messages** section.

5. Select **Nack message requeue true** in the **ACK Mode** list.

6. Select **Get Message(s)**.

7. Review the message and note the ID.

8. Restart the Cherwell Service Host.

9. Refresh the queue.

10. On the Get Messages section, select **Nack message requeue true** in the **ACK Mode** list again.

11. Select **Get Messages**.

12. Review the message, and if the ID is the same, then that message is stuck.

To remove a single item in a queue:

1. Pause the E-mail and Event Monitor Service or if there are Automation Process tasks associated with the queue, pause the Automation Process server.

2. In a browser, enter the RabbitMQ Management Interface URL:
   http://localhost:15672

3. Log in with the RabbitMQ credentials.

4. On the **Queues** tab, select the queue with the stuck message.

5. Expand the **Get Messages** section.

6. Select **Automatic ack** in the **ACK Mode** list.
   Leave the **Messages** field number at 1. If multiple messages need to be removed, you can increase this number, but proceed with caution. This is an ultimately destructive action and cannot be undone.

7. Select **Get Message(s)** to remove the item.

8. Resume the E-mail and Event Monitor Service and the Automation Process server if they were paused in the first step.

Increase the Speed of Automation Processing Events

The quantity and processing time of an AP event directly correlates to how much work the event generates in the system. Disabling events will not prevent the leader from working to filter out each of those items. To maximize performance, you should have only the number of events you need. Broad functionality like **Change on Any Field** can also have a negative impact on performance, because these items require more effort than may be needed.

Decrease Processing Time

There are two settings that can have a large impact on processing time. These are found in the C:\ProgramData\Trebuchet\Trebuchet.settings file:

HostMaxWorkers: Default is 21. This number is calculated by the default HostMaxWorkers limit per server (5) multiplied by the number of services (4) plus 1.

Note: Allocating high numbers to the HostMaxWorkers setting can negatively impact workers and other processes on the server where Cherwell® Service Host is running.

MaxWorkers: This is the maximum number of workers that can be created for each service. While the total number of workers between services exceeds what is created by the VPMultiplier, the total count of workers will be limited by the VPMultiplier in a first come first serve fashion.

Monitor AP Events Processing

For AP Events, the following SQL Queries can provide some context:

```
--The longest running AP by BusObType for today
Declare @Now DateTime;
Declare @Earlier DateTime;
--Select up to now.
Select @Now = GetDate();


--Get from midnight today
Select @Earlier = DATEFROMPARTS(DatePart(yyyy, @Now) , DatePart(M, @Now), DatePart(D, @Now))


Select td.DefName,
        Cast(FORMAT(DatePart(HOUR, ttp.Duration), 'D2') as VarChar(20)) + ':'
        + Cast(FORMAT(DatePart(MINUTE, ttp.Duration), 'D2') as VarChar(20)) + ':'
+ Cast(FORMAT(DatePart(SECOND, ttp.Duration), 'D2') as VarChar(20)) As ElapsedTime,
        ttp.RecCount
from TrebuchetDefs td WITH(NOLOCK)
INNER JOIN (SELECT BusObTypeID, Duration=(MAX([CompletedDateTime]-[StartedDateTime])), count(RecId) as recCount
        FROM [dbo].[TrebuchetProcesses] with (NOLOCK)
        where startedDateTime >= @Earlier AND completedDateTime <= @Now
        group by [BusObTypeID]
        )  as ttp ON td.DefId = ttp.BusObTypeID



--Count of AP Events pending processing by the leader, high numbers are pro
```

```
blematic.
SELECT COUNT(RecId) FROM TrebuchetEvents WITH(NOLOCK) WHERE EventStatus = '
Logged'
```

Command-Line Configuration (CLC) Options

Use Configuration command-line options to automatically run instructions or commands that configure and manage CSM after it is installed using the CSM installation package or silent installation command-line options. For example, CSM Configuration command-line options can publish a Blueprint and create a Blueprint from a mApp file.

Use a command window to run Trebuchet.CommandLineConfigure.exe, which is usually found in the directory C:\Program Files\Cherwell Service Management.

Arguments can either be prefixed with a forward slash or with a dash, so /? and -? are equivalent.

> **Note:** In the following examples, square brackets (example: [Common]) denote placeholder variables for customer data. Replace these variables, including the brackets, with your own values.

Create a Blueprint File From a mApp File

Option	Description
/mapp	This option allows for the creation of a Blueprint file from a mApp file.
/mappfilepath	This is the file path to a mApp file (*.mapp or *.mappz).
/mappoutputpath	This is the file path to store a Blueprint file (*.bp) created from a mApp file (*.mapp or *.mappz).
/mapplegalaccept	This is a flag for accepting legal terms. The default is False. The options are: True or False. False prevents the Blueprint from being created.
/mappsecurityinformationaccept	This is the flag for accepting the security message that explains that a mApp Solution contains Security Groups and/or Roles that may impact security rights in the target database. The options are: True or False. False prevents the Blueprint from being created.
/connection	This is the common connection name (Example: Demo).
/connectionuserid	This is the user ID for a connection. Typically, this is the CSM user ID for the requested server.
/connectionpassword	This is the password for a connection. Typically, this is the CSM User password for the requested server.

Example:

```
Trebuchet.CommandLineConfigure.exe /mapp /mapplegalaccept=true
        /mappfilepath="C:\..." /mappoutputpath="C:\..." /connection="[Com
mon]Cherwell
```

```
Browser" /connectionuserid=user ID/connectionpassword=password
```

Publish an Existing Blueprint File

Option	Description
/publish	This option publishes an existing Blueprint file.
/blueprint	This is the file path to a Blueprint (*.bp) for restore. It requires a user ID and password.
/[createrollback]	This is a flag for saving a Blueprint rollback file. The default is True. The options are: True or False.
/[scanblueprint]	This is a flag for scanning a Blueprint prior to publishing. The default is True. The options are: True or False.
/[ignoreconflicts]	This is a flag for ignoring Blueprint conflicts while publishing. The default is True. The options are: True or False.
/[restartservices]	This is a flag for restarting services after publishing. The default is True. The options are: True or False.
/[unlocksystem]	This is a flag for unlocking the system after publishing. The default is True. The options are: True or False.
/[updateforeignkeys]	This is a flag for updating foreign keys while publishing. The default is False. The options are: True or False.
/[stoponwarning]	This is a flag to stop publishing on a warning during "/[scanblueprint]". The default is False. The options are: True or False.
/[scanenabledculturesonly]	This is a flag to scan Business Object property values for enabled cultures only. When False is passed, all cultures are scanned.
/[rebuildfulltext]	This is a flag for rebuilding the full text catalog while publishing. The default is False. The options are: True or False.
/connection	This is the common connection name (Example: Demo).
/connectionuserid	This is the user ID for a connection. Typically, this is the CSM user ID for the requested server.
/connectionpassword	This is the password for a connection. Typically, this is the CSM User password for the requested server.

Example:

```
Trebuchet.CommandLineConfigure.exe /publish
        /blueprint="C:\..." /connection="[Common]Cherwell Browser"
        /connectionuserid=user ID/connectionpassword=password
```

Restore a .czar File

Option	Description
/restoreczar	This option restores a .czar file.
/restoreczarfile	This is the file path to a .czar file for restore. This requires a user ID and password.
/restoreenv	This is the CSM installation environment. The options are: Development, Test, or Production.
/[restoreunicode]	Restore the .czar as Unicode? The options are: True or False.
/[restoreplatformczarfilepath]	This is the file path to the .czar file containing platform strings.
/[ignoreplatformczarversioncheck]	Option to skip version checks when loading a .czar file that contains platform strings. The options are: True or False.

Test Connection

Option	Description
/testconnection	This option tests a connection by name.

Trusted Agents Server

Option	Description
/trustedagenthost	This option sets up the Trusted Agents Server.
/[trustedagenthostuninstall]	This uninstalls the Trusted Agents Server.
/[trustedagenthostinstallaccount]	This is the account the service will log on as. The options are: LocalService, LocalSystem, or NetworkService.
/[trustedagenthostinstalluserid]	This is the user ID the service will log on as. The value type is String.
/[trustedagenthostinstallpassword]	This is the password the service will log on with. The value type is String.
/[trustedagenthostinstallautostart]	This option sets the service to auto start during installation. The options are: True or False.
/[trustedagenthoststart]	This option starts the Trusted Agents Server.
/[trustedagenthoststop]	This option stops the Trusted Agents Server.
/[trustedagenthostdisplayname]	This option sets the display name. The value type is String.
/[trustedagenthosthuburl]	This is the URL of the Trusted Agent Hub to connect to. HTTPS is recommended.

Option	Description
/[trustedagenthosthubsharedkey]	This is the shared key for the Trusted Agent Hub.
/[trustedagenthostpingfrequency]	This is the hub ping frequency. The value is in seconds.
/[trustedagenthostlogeventloglevel]	This is the setting for the Trusted Agent logging event log level. The value type is String.
/[trustedagenthostlogfileloglevel]	This is the setting for the Trusted Agent logging file log level. The value type is String.
/[trustedagenthostlogfilepath]	This is the setting for the Trusted Agent logging file path. The value type is String.
/[trustedagenthostlogserverloglevel]	This is the setting for the Trusted Agent logging server log level. The value type is String.
/[trustedagenthostlogtoevent]	This is the setting for the Trusted Agent logging to event log. The options are: True or False.
/[trustedagenthostlogtofile]	This is the setting for the Trusted Agent logging to file. The options are: True or False.
/[trustedagenthostlogtoserver]	This is the setting for the Trusted Agent logging to log server. The options are: True or False.
/[trustedagenthostlogmaxfilesizeinmb]	This is the setting for the Trusted Agent logging max file size in MB. The value type is Integer.
/[trustedagenthostlogmaxfilesbeforerollover]	This is the setting for the Trusted Agent logging max files before rollover. The value type is Integer.

Trusted Agents Hub

Option	Description
/trustedagenthub	This option allows configuration of the Trusted Agents Hub.
/[trustedagenthubenable]	This enables or disables the use of Trusted Agents. The options are: True or False.
/[trustedagenthuburl]	This is the URL that should be used for Trusted Agent communication. HTTPS is recommended.
/[trustedagenthubsharedkey]	This is the value to use as the shared key for Trusted Agent communication.
/[trustedagenthubgeneratesharedkey]	This option generates a new cryptographically secure key for the Trusted Agent shared key. **Note:** Only one option can be used: Provide the value for a shared key or generate a shared key.
/[trustedagenthuboperationtimeout]	This is the operation timeout for Trusted Agents. The value is in seconds.

Option	Description
/[trustedagenthubregistrationtimeout]	This is the registration timeout for Trusted Agents. The value is in seconds.

Upgrade Database

Option	Description
/upgrade	This option upgrades the database, if needed.

Application Server Command-Line Options

Use the Command-Line Configuration (CLC) /appserver major command to access all sub-commands to configure, start, stop, and uninstall the Application Server.

/appserver

Example:

```
/appserver /connection="[Common]Cherwell Browser" /connectionPort:8001 /con
nectionhostingmode:AppServer /connectionProtocol:$env:Protocol_AppServer
```

> 🖊 **Note:** In the following examples, square brackets (example: [Common]) denote placeholder variables for customer data. Replace these variables, including the brackets, with your own values.

Sub-command	Description
/connection	Name of the CSM connection. **Accepted values**: string **Required**: Yes
/connectionservername	The server name for the specified connection. **Accepted values**: string
/connectionport	The port to host the Application Server connection. **Accepted values**: {0 - 65535} **Default**: 80
/appservercertificatesubject	The display name of the certificate subject. This is not used for searches. **Accepted values**: string Examples: CN=myhost.cherwell.com, OU=NA, O=NA, L=Colorado Springs, S=CO, C=US.
/appservercertificatethumbprint	Certificate thumbprint used to look up certificates in the store configured by option /appservercertstorename. **Accepted values**: string Example: 99C732FBDD70D798AE2AB23D862835D144C658F4

Sub-command	Description
/appservercertificatevalidationmode	Certificate validation mode to pass to auto-clients. **Accepted values**: {server | chain | peer | trust | peerorchain} **Default**: peerorchain
/appservercertstorelocation	The location on the machine with the X.509 certificate store. **Accepted values**: {currentuser | localmachine} **Default**: currentuser
/appservercertstorename	The name of the certificate store that the /appservercertstorelocation option is configured to use. **Accepted values**: {addressbook | authroot | certificateauthority | disallowed | my | root | trustedpeople | trustedpublisher} **Default**: my
/appserverlogtoevent	If true, log to the event log. **Accepted values**: {true | false} **Default**: True
/appserverlogeventloglevel	The minimum level at which logs will be sent to the event log. **Accepted values**: {fatal | error | warning | info | stats | debug} **Default**: warning
/appserverlogtofile	If true, log to the log file. **Accepted values**: {true | false} **Default**: False
/appserverlogfileloglevel	The minimum level at which logs will be sent to the log file. **Accepted values**: {fatal | error | warning | info | stats | debug} **Default**: warning
/appserverlogfilepath	The path to the log file. **Accepted values**: string **Default**: Path to the directory that contains CSM executables.

Sub-command	Description
/appserverlogmaxfilesbeforerollover	Maximum number of log files before files roll over. **Accepted values**: integer **Default**: 20
/appserverlogmaxfilesizeinmb	Maximum log file size in MB. **Accepted values**: integer **Default**: 10
/appserverlogtoserver	If true, Service Host will log to the log server (Splunk). **Accepted values**: {true | false} **Default**: False
/appserverlogserverloglevel	The minimum log level at which logs will be sent to the log server (Splunk). **Accepted values**: {fatal | error | warning | info | stats | debug} **Default**: warning
/appserverrecoverylocation	Overrides the patch to the Application Server recovery file. **Accepted values**: string
/appserversecuritymode	Application Server security mode for encryption. Normal equals none. **Accepted values**: {normal | signed |encrypted | server} **Default**: normal
/appserveruserest	If true, the Application Server will attempt to bind WCF calls to REST. **Accepted values**: {true | false} **Default**: False

/appserverinstall

Use the /appserverinstall sub-command to install the Application Server.

Example:

```
/appserver /appserverinstall /connection="[Common]Cherwell Browser" /appser
verinstalluserid="domain\userloginID" /appserverinstallpassword="password"
```

Sub-command	Description
/appserverinstalluserid	The Windows domain account the service will use to log in. Format: domain\useraccount. **Accepted values**: string **Required**: Yes
/appserverinstallpassword	Password for the Windows domain account. **Accepted values**: string **Required**: Yes
/appserverinstallautostart	If true, the service starts automatically during installation. **Accepted values**: {true | false} **Default**: False

/appserverstart

Use the /appserverstart sub-command to start the Application Server. There are no options for this sub-command.

Example:

```
/appserver /appserverstart
```

/appserverstop

Use the /appserverstop sub-command to stop the Application Server. There are no options for this sub-command.

Example:

```
/appserver /appserverstop
```

/appserveruninstall

Use the /appserveruninstall sub-command to uninstall the Application Server. There are no options for this sub-command.

Example:

```
/appserver /appserveruninstall
```

Related concepts

Configure the Application Server

Configure Logging for a CSM Service, Web Application, and Cherwell REST API Connections

Installing CSM from the Command Line

Auto-Deploy Command-Line Options

Use the Command-Line Configuration (CLC) /autodeploy and autodeployfromsettings major commands to create an Auto-Deploy package that automatically distributes preconfigured Desktop Client and CSM Administrator installations and connections.

Arguments passed through the /autodeploy are saved to the C:\ProgramData\Trebuchet\trebuchet.settings file. You can then use /autodeployfromsettings to create the Auto-Deploy package from those settings.

🖉 **Note:** In the following examples, square brackets (example: [Common]) denote placeholder variables for customer data. Replace these variables, including the brackets, with your own values.

/autodeploy

Example with minimally required commands:

```
Trebuchet.CommandLineConfigure.exe /autodeploy /adconnectionname="[Common]3
TierConnectionName" /adtargetfolder="C:\Program Files\Cherwell Browser Appl
ications\CherwellAutoDeploy" /adsite="https://YourAutoDeploymentSite/Cherwe
llAutoDeploy/"
```

Example with installation options:

```
Trebuchet.CommandLineConfigure.exe /autodeploy /adoverwrite=True /admakedef
ault=True /adnoprompt=True /adminorrelease=False /ReqMinorReleases=False /a
dtargetfolder="C:\Program Files\Cherwell Browser Applications\CherwellAutoD
eploy" /adsite=https://YourAutoDeploymentSite/CherwellAutoDeploy/ /adnouser
options=False /adinstalloptions=UserChoice /adinstallaccounts=[{\"Domain\":
\"cherwell\",\"Username\":\"john\",\"Password\":\"12345},{\"Domain\":\"cher
well\",\"Username\":\"john2\",\"Password\":\"12345\"}]
```

Sub-command	Description
/adconnectionname	The Client connection that is pushed out to all clients during installation. This must be an Application Server connection (3-tier connection). **Accepted values**: string **Required**: Yes

Sub-command	Description
/adtargetfolder	The directory on the server where the install files are stored. This should be the directory where Auto-Deploy is installed (the physical directory that is pointed to by the Auto-Deploy site). If defaults were selected during the installation, this should be ..\Cherwell Browser Applications\Cherwell Auto-Deploy. **Accepted values**: string **Required**: Yes
/adsite	The URL of the website housing the Auto-Deploy installation. If the defaults are selected during the installation, the URL is https://*YourAutoDeploymentSite*/CherwellAutoDeploy. **Accepted values**: string **Required**: Yes
/admsifilepath	The full path to the CSM installer .msi file. The system will attempt to locate the file, but if it has been moved from its default location (\ProgramData\cherwell service management), you must provide the location. **Accepted values**: string
/admakedefault	If true, uses the installation connection as the default Auto-Deploy connection for users. **Accepted values**: {true | false} **Default**: True
/adnoprompt	If true, automatically connects to the installation connection without prompting users. **Accepted values**: {true | false} **Default**: False
/adminnorelease	If true, users are required to install minor releases even if the current version is compatible with the CSM server. **Accepted values**: {true | false} **Default**: False
/addebug	If true, a series of message boxes is shown during deployment to assist with troubleshooting. **Accepted values**: {true | false} **Default**: False

Sub-command	Description
/adoverwrite	If true, the installer will overwrite existing connections with the same name. **Accepted values**: {true | false} **Default**: True
/adnouseroptions	If true, users are not prompted with options during installation. **Accepted values**: {true | false} **Default**: True
/adinstalloptions	Indicates the type of installation created. If /adnouseroptions is true, then either ClientOnly, or Complete must be selected. **Accepted Values**: {ClientOnly | Complete | UserChoice} **Default**: UserChoice
/adinstallallusers	If true, all users can run the installation. If false, then installation accounts must be defined. **Accepted values**: {true | false} **Default**: True
/adinstallaccounts	If set, the installer runs as one of the specified administrative users that matches the domain on the target machine (or does not specify domain) rather than as the current user. **Accepted value**s: JSON string. Example: `[{\"Domain\":\"cherwell\",\"Username\":\"john\",\"Password\":\"12345},{\"Domain\":\"cherwell\",\"Username\":\"john2\",\"Password\":\"12345\"}]` **Default**: Installation accounts not used.

Related concepts

Configuring Auto-Deploy

Configure Auto-Deploy Options

Using Auto-Deploy

Auto Update Command-Line Options

Use the Command-Line Configuration (CLC) /autoupdateservice and /update major commands to install the Auto Update Service and check for Trusted Agent Server updates.

> ✏️ **Note:** In the following examples, square brackets (example: [Common]) denote placeholder variables for customer data. Replace these variables, including the brackets, with your own values.

/autoupdateservice

Use the /autoupdateservice major command to access all minor commands for the Auto Update Service subcommands, and configuration.

/autoupdateserviceinstall

Use this minor command is to install the Auto Update Service.

Sub-command	Description
/installuserid	User ID the service will log on as. Optional as long as /trustedagenthostinstallaccount has a valid value. **Accepted values**: string **Required**: Depends
/installpassword	Password that the service will log on with. Optional as long as /trustedagenthostinstallaccount has a valid value. **Accepted values**: string **Required**: Depends
/installaccount	Account the service will log on as. **Accepted values**: {LocalService|LocalSystem|NetworkService} **Default value**: LocalSystem **Required**: Depends; optional as long as /trustedagenthostinstalluserid and /trustedagenthostinstallpassword have valid values
/installautostart	Set the service to autostart during installation. **Accepted values**: {true | false}

/autoupdateserviceuninstall

Use this minor command to uninstall the Auto Update Service windows service.

/start

Use this minor command to start the Auto Update Service.

/stop

Use this minor command to stop the Auto Update Service.

/update

Use /update major command to load the latest version of the Trusted Agent server into Overwatch.

Sub-command	Description
/downloadendpoint	Format: {scheme}//{path}/{apptype}/{version} Endpoint indicating the update to be performed. • Scheme indicates the protocol scheme (such as http: or https:). • Path indicates the source of the update files (use "Overwatch"). • AppType indicates the type of update to perform (use "TrustedAgent"). • Version indicates the version of this update in the form: xx.xx.xx.xx. **Accepted values**: string **Required**: Yes
/downloadfile	The. zip file containing the files that the Auto Update Service will copy to the application (Trusted Agents) folder. **Note:** The size limit for the .zip file is 200,000 MB. **Accepted values**: string **Required**: Yes

CSM 2022.3 Administration

CherwellMQS Command Line Options

Use Command-Line Configuration (CLC) commands to configure Cherwell Message Queue Service.

/messagequeue

Use the /messagequeue major command to access sub-commands to configure CherwellMQS.

Sub-command	Description
/connectionport	The port to contact on the server. **Accepted values**: Any integer **Default**: 5672
/connectionservername	The host name or IP where the RabbitMQ broker is installed. **Default**: localhost
/connectionuserid	User ID for the connection. **Accepted values**: Any string **Default**: "admin"
/connectionpassword	Password for the connection. **Accepted values**: Any string **Warning:** Don't use "&" in the password because the CLC doesn't recognize the character and will only use the part of the password before the "&" (example: If the password is "Cherwell&Ivanti", the CLC will only use "Cherwell" as the password).
/connectionvirtualhost	Virtual host to use on the RabbitMQ server. The administrator must setup the virtual host within RabbitMQ. **Accepted values**: Any string or "/" **Default**: "/", which is RabbitMQ's default virtual host

/cmqs

Use the /cmqs major command to access sub-commands to configure CherwellMQS.

/cmqsstart

Use the /cmqsstart sub-command to start CherwellMQS. This command is typically run after performing management actions that require CherwellMQS to be restarted.

CSM 2022.3 Administration

1079

Example:

```
/cmqsstart
```

/cmqsstop

Use the /cmqsstop sub-command to stop CherwellMQS.

Example:

```
/cmqsstop
```

Command-Line Configure Logging Options

Use the /commandlineconfigure major command to configure logging for the Command-Line Configure (CLC) utility. Use sub-commands to configure log location and maximum log file sizes.

/commandlineconfigure

Example:

```
/commandlineconfigure /commandlineconfigurelogtoevent=true /commandlineconf
igurelogeventloglevel=debug
```

Sub-command	Description
/commandlineconfigurelogtoserver	If true, Command Line Configure will log to the log server. **Accepted values**: {true | false}
/commandlineconfigurelogserverloglevel	The minimum level at which logs will be sent to the log server. **Accepted values**: {fatal | error | warning | info | stats | debug}
/commandlineconfigurelogtoevent	If true, Command Line Configure will log to the event log. **Accepted values**: {true | false}
/commandlineconfigurelogeventloglevel	The minimum level at which logs will be sent to the event log. **Accepted values**: {fatal | error | warning | info | stats | debug}
/commandlineconfigurelogtofile	If true, Command Line Configure will log to the file system log. **Accepted values**: {true | false}
/commandlineconfigurelogfileloglevel	The minimum level at which logs will be sent to the file system log. **Accepted values**: {fatal | error | warning | info | stats | debug}
/commandlineconfigurelogfilepath	The path to the file system logs. **Accepted values**: string

Sub-command	Description
/commandlineconfigurelogmaxfilesizeinmb	Maximum log file size in MB. **Accepted values**: integer
/commandlineconfigurelogmaxfilesbeforerollover	Maximum number of log files before files roll over. **Accepted values**: integer

Related concepts

Configure Logging for a CSM Service, Web Application, and Cherwell REST API

Connection Creation Command-Line Options

Use the Command-Line Configuration (CLC) /create2tier and /create3tier major commands to access all sub-commands to create or update two-tier or three-tier connections to the CSM database.

/create2tier

Example:

```
/create2tier /connection=2TierConnection /sqlconnectionstring="Data Source=
$env:dbServer,1433;Initial Catalog=$env:dbName;DbOwner=dbo;User ID=$env:dbA
dminUser;Password=$env:dbAdminPass;Default Pooling=True;Packet Size=4096" /
sqlconnectionuserid=$env:dbAppUser /sqlconnectionpassword=$env:dbAppPass
```

Sub-command	Description
/connection	Name of the CSM connection. **Accepted values**: string **Required**: Yes
/sqlconnectionstring	The SQL Server administration connection string. **Accepted values**: string **Example**: Data Source=*ServerName*,1433:Initial Catalog=*DatabaseName*;DbOwner=dbo;User ID=*SQLAdminUserId*;Password=*SQLAdminPassword*;Default Pooling=True;Packet Size=4096 **Required**: Yes
/sqlconnectionuserid	The SQL Server user ID. **Accepted values**: string **Required**: Yes
/sqlconnectionpassword	The password for the SQL Server user ID. **Accepted values**: string **Required**: Yes

/create3tier

Example:

```
/create3tier /connection=3TierConnection /url=Https://127.0.0.1:8001 /appse
rverhostiis=true
```

Sub-command	Description
/connection	Name of the CSM connection. **Accepted values**: string **Required**: Yes
/url	The URL to the remote machine. **Accepted values**: string **Required**: Yes
/appserverhostiis	If true, the Application Server is hosted in Internet Information Services (IIS). **Accepted values**: {true | false}

Related concepts
Configure the Server Connection
Configure the Client Connection
Related tasks
Configure the Browser Connection

Environment Command-Line Options

Use the Command-Line Configuration (CLC) /environment commands to get or set the installation environment partition key or type.

Note: In the following examples, square brackets (example: [Common]) denote placeholder variables for customer data. Replace these variables, including the brackets, with your own values.

/environment

Example:

```
/environment /envvalue="Test" /connection="[Common]Cherwell Browser" /connectionuserid=CSDAdmin /connectionpassword=CSDAdmin
```

Note: These commands only work on 2-tier connections.

Sub-command	Description
/connection	Name of the CSM connection. **Accepted values**: string **Required**: Yes
/connectionuserid	The CSM user ID for the requested server. **Accepted values**: string
/connectionpassword	The CSM password for the requested server. **Accepted values**: string
/envvalue	The CSM installation environment. **Accepted values**: {Development | Test | Production}
/envpartitionkey	The CSM installation partition key. **Accepted values**: string

Related concepts

Connections

Export Settings Command-Line Options

Cherwell uses the Command-Line Configuration (CLC) /exportsettings major command to export file system settings and import them into Overwatch.

There are more than two dozen settings objects in Overwatch that are populated from the following files:

- Trebuchet.settings
- ComplianceLogServer.settings
- ServerFarm.xml
- WebAPI web.config
- Browser Client web.config
- Portal web.config

By default, this command looks up the location of these files based on the installation paths of the CSM applications. However, the settings files in the previous list each have a command parameter that can specify a file location override.

/exportsettings

Example:

```
/exportsettings /trebuchetsettingspath="C:\Backups\trebuchet.settings" /compliancelogserverpath="C:\Backups\ComplianceLogServer.settings" /serverfarmpath="C:\Backups\ServerFarm.xml" /browserconfigpath="C:\Backups\BrowserClient\Web.config" /portalconfigpath="C:\Backups\Portal\Web.config" /webapiconfigpath="C:\Backups\WebApi\Web.config"
```

Sub-command	Description
/connection	The name of the CSM connection. **Accepted values**: string **Required**: No
/connectionuserid	The CSM user ID for the requested server. **Accepted values**: string **Required**: No

Sub-command	Description
/connectionpassword	The CSM password for the requested server. **Accepted values**: string **Required**: No
/trebuchetsettingspath	The path to the Trebuchet.settings file. **Accepted values**: string **Required**: No **Default location**: C:\ProgramData\Trebuchet\trebuchet.settings
/compliancelogserverpath	The path to the ComplianceLogServer.settings file. **Accepted values**: string **Required**: No **Default location**: C:\ProgramData\Trebuchet\ComplianceLogServer.settings"
/serverfarmpath	The path to the ServerFarm.xml file. **Accepted values**: string **Required**: No **Default location**: C:\ProgramData\Trebuchet\ServerFarm.xml
/browserconfigpath	The path to the CSM Browser client web.config file. **Accepted values**: string **Required**: No **Default location**: C:\Program Files\Cherwell Browser Applications\BrowserClient\Web.config
/portalconfigpath	The path to the Portal web.config file. **Accepted values**: string **Required**: No **Default location**: C:\Program Files\Cherwell Browser Applications\Portal\Web.config
/webapiconfigpath	The path to the Cherwell API web.config file. **Accepted values**: string **Required**: No **Default location**: C:\Program Files\Cherwell Browser Applications\CherwellAPI\Web.config

Export System Command-Line Options

Use the Command-Line Configuration (CLC) /exportsystem major command to export CSM to a .czar or .car file.

✏️ **Note:** In the following examples, square brackets (example: [Common]) denote placeholder variables for customer data. Replace these variables, including the brackets, with your own values.

/exportsystem

Example:

```
/exportsystem /connection="[Common]Cherwell Browser" /connectionuserid=CSDA
dmin /connectionpassword=CSDAdmin /filename=C:\temp\system.czar /format=Cza
r /mode=EntireSystemAndData
```

Sub-command	Description
/connection	The name of the CSM connection. **Accepted values**: string **Required**: Yes
/connectionuserid	The CSM User ID for the requested server. **Accepted values**: string **Required**: Yes
/connectionpassword	The CSM password for the requested server. **Accepted values**: string **Required**: Yes
/filename	The full path and filename to export the system to. The path must exist. **Accepted values**: {filepath} **Required**: Yes
/format	File format for the exported system. **Accepted values**: {czar | car} **Default Value**: czar

Sub-command	Description
/mode	What is to be exported. **Accepted values**: {EntireSystemAndData | EntireSystemStructureOnly | EntireSystemAndLookupData} **Default Value**: EntireSystemAndData
/flags	Different options for the export. Multiple flags can be separated by a comma or pipe. **Accepted values**: {ExcludeAttachments | GenerateLog | ExcludeBusinessProcessData | ExcludeEncryptedFields | ExcludeEmails}

License Command-Line Options

Use the Command-Line Configure (CLC) /license commands to add or update a CSM license key.

/license

Sub-command	Description
/connection	Name of the CSM connection. **Accepted values**: string **Required**: Yes
/connectionuserid	The CSM user ID for the requested server. **Accepted values**: string **Required**: Yes
/connectionpassword	The CSM password for the requested server. **Accepted values**: string **Required**: Yes
/licensekey	A company's license key. For upgrading, this is the only required parameter. **Accepted values**: string **Required**: Yes
/licensename	The name of the company that owns the license. This parameter is required for installation but not upgrade. **Accepted values**: string **Required**: Yes

Related concepts
Connections
Add a License Key

Overwatch Command-Line Options

Use the Command-Line Configuration utility to install, start, and stop Overwatch, and to control CSM Portal and CSM Browser Client settings.

> **Note:** In the following examples, square brackets (example: [Common]) denote placeholder variables for customer data. Replace these variables, including the brackets, with your own values.

/overwatch

Example with minimally required commands:

```
/overwatch /overwatchinstall /servicepath="C:\Program Files\Cherwell Servic
e Management\Overwatch\Trebuchet.Overwatch.exe"
```

Example with installation options:

/overwatchinstall

Use this minor command to install Overwatch.

Sub-command	Description
/installuserid	User ID the service uses to log on. **Accepted values**: string **Required**: No
/installpassword	Password the service uses to log on. **Accepted values**: string **Required**: No
/installaccount	Account the service uses to log on. **Accepted values**: {LocalService|LocalSystem|NetworkService} **Default value**: LocalSystem **Required**: No
/installautostart	Sets the service to autostart during installation. **Accepted values**: {true | false}

Sub-command	Description
/servicepath	Overrides the location of the windows service executable. **Accepted values**: string

/overwatchstart

Use this minor command to start Overwatch.

/overwatchstop

Use this minor command to stop Overwatch.

/overwatchuninstall

Use this minor command to uninstall Overwatch.

/updateportalsettings

This major command will update CSM Portal settings in Overwatch. If Overwatch can't be reached, this command will not work as expected.

/updatebrowserclientsettings

Examples:

```
/updateportalsettings /trebuchetdatasource=[Common]CherwellTest /testmode=t
rue /tabcontentheight=250 /disablecertificatevalidation=true /allowunsafela
bels=true /inlinebrowserdisplayextensions=.pdf,.xml /lookupalwaysenabled=tr
ue /queryrequestlimit=60 /usecdn=true /usehttpcompression=true /loadallfile
sindividually=true /enablesessionserialization=true /alwaysloadkeys=true /u
iinteractiontimeoutinseconds=120 /allowscriptsinreports=true /disableanchor
ing=true /disablesplitters=true /uselegacycompleteresponse=true /signalrcon
nectiontimeoutinseconds=200 /signalrdisconnecttimeoutinseconds=250 /signalr
keepaliveinseconds=300 /scanditlicensekey=da06e9dc-f4fb-4dba-954c-5b0ab614f
f9b /redirecthttptohttps=true /enableinsecuredeeplinks=true /autosizelabels
=true /authlogfile=mylog.txt /defaultauthmode=SamlLogin
```

This major command will update Browser Client settings in Overwatch. If Overwatch can't be reached, this command will not work as expected.

Examples:

```
/updatebrowserclientsettings /trebuchetdatasource=[Common]CherwellTest /tes
tmode=true /tabcontentheight=250 /disablecertificatevalidation=true /allowu
nsafelabels=true /inlinebrowserdisplayextensions=.pdf,.xml /lookupalwaysena
bled=true /queryrequestlimit=60 /usecdn=true /usehttpcompression=true /load
allfilesindividually=true /enablesessionserialization=true /alwaysloadkeys=
true /uiinteractiontimeoutinseconds=120 /allowscriptsinreports=true /disabl
eanchoring=true /disablesplitters=true /uselegacycompleteresponse=true /sig
nalrconnectiontimeoutinseconds=200 /signalrdisconnecttimeoutinseconds=250 /
signalrkeepaliveinseconds=300 /scanditlicensekey=da06e9dc-f4fb-4dba-954c-5b
0ab614ff9b /redirecthttptohttps=true /enableinsecuredeeplinks=true /autosiz
elabels=true /authlogfile=mylog.txt /defaultauthmode=SamlLogin
```

Use the following sub-commands with both /updateportalsettings and /updatebrowserclientsetting.

Sub-command	Description
/trebuchetdatasource	The name of the CSM connection (example: [Common]Cherwell Browser) to be used by the Browser Client. **Accepted values**: string
/testmode	If true, various test options are set for things like default menus. **Accepted values**: {true | false}
/tabcontentheight	The height, in pixels, of the tab content area. **Accepted values**: integer
/disablecertificatevalidation	If true, disables certificate validation when performing internal resource requests (such as to allow self-signed certificates). This can be used in a test environment to avoid errors that may arise when using SSL connections for SAML. Do NOT set this value to true in a production environment. **Accepted values**: {true | false}
/allowunsafelabels	If true, HTML and scripts can be embedded in labels to be executed in the browser (not recommended). **Accepted values**: {true | false}
/inlinebrowserdisplayextensions	Comma-separated list of file extensions whose corresponding downloadable files will have the HTTP response content-disposition header with a value of "inline". **Accepted values**:.pdf,.xml

Sub-command	Description
/lookupalwaysenabled	If true, the Lookup button is enabled when editing a Business Object. By default, it is enabled only on controls that support lookups. If the logic associated with the availability of a lookup button is extremely complex, it may not enable. **Accepted values**: {true | false}
/queryrequestlimit	Number of rows to return per query. **Accepted values**: integer
/usecdn	If true, third-party *.js components (example: jquery.min.js, jquery-ui.min.js, kendo.all.min.js) are served by third-party CDNs (example: //ajax.googleapis.com , //kendo.cdn.telerik.com) and not by our site. **Accepted values**: {true | false}
/usehttpcompression	If true, HTTP compression is enabled from the server to the client. **Accepted values**: {true | false}
/loadallfilesindividually	If true, all third-party *.js components (example: jquery.min.js, jquery-ui, kendo.all.min.js) are forced to be served by CSM. **Accepted values**: {true | false}
/enablesessionserialization	Only used when NOT in web-farm mode. If true, session serialization is turned on. **Accepted values**: {true | false}
/alwaysloadkeys	If true, a Business Object relationship is forced to use keys when loading data. **Accepted values**: {true | false}
/uiinteractiontimeoutinseconds	The timeout in seconds that CSM waits for a user interface interaction request to complete. **Accepted values**: integer
/allowscriptsinreports	If true, the DevExpress.XtraReports.Security.ScriptPermissionManager.GlobalInstance is initialized using the ExecutionMode.Unrestricted mode. **Accepted values**: {true | false}
/disableanchoring	If true, disables control anchoring. **Accepted values**: {true | false}
/disablesplitters	If true, disables rendering of splitters. **Accepted values**: {true | false}

Sub-command	Description
/uselegacycompleteresponse	Use the pre-10.0 mechanism for ending the request. Note that this bypasses a lot of configurations in IIS. **Accepted values**: {true | false}
/signalrconnectiontimeoutinseconds	Maximum amount of time in seconds for long polling connections to wait for a response. When this connection time expires, a timeout command is triggered and the client is forced to reconnect. Default is -1, indicating you shouldn't override SignalR's default settings. **Accepted values**: integer
/signalrdisconnecttimeoutinseconds	Maximum time in seconds after a transport connection is lost before raising the disconnected event to terminate the SignalR connection. Defaults to -1, indicating SignalR's default settings should not be overridden. **Accepted values**: integer
/signalrkeepaliveinseconds	For transports other than long polling, this value represents how often to send a keepalive packet. This value must be no more than 1/3 of the SignalRDisconnectTimeoutSec value. Defaults to -1, indicating SignalR's default settings should not be overridden. **Accepted values**: integer
/scanditlicensekey	Scandit Barcode Scanning license key **Accepted values**: string
/redirecthttptohttps	If true and the incoming request is an HTTP request, it redirects to HTTPS. **Accepted values**: {true | false}
/enableinsecuredeeplinks	If true, enables the ability to pass the username and password on the URL to all deep links. We do not recommend non-secure deep links. We recommend internal authorization with a user that has the absolute minimum permissions to perform the action (example: Creating a new Business Object), giving the appearance of an anonymous form. **Accepted values**: {true | false}
/autosizelabels	If true, labels dynamically autosizes. False is not recommended. **Accepted values**: {true | false}
/authlogfile	Authentication information log file name. **Accepted values**: string
/defaultauthmode	Sets the default login mode. **Accepted values**: {WinLogon|WinLogin|CherwellLogin|SamlLogin}

Cherwell REST API Command-Line Options

Use the Command-Line Configure (CLC) /restapiurl commands to get or set the Cherwell® REST API base URL. The base URL for the REST API is required for various CSM features, including authentication, Saved Searches, and webhooks.

You can also set the base URL for the Cherwell REST API in Cherwell Server Manager. See Set the Base URL for the Cherwell REST API.

Always use HTTPS instead of HTTP for security purposes.

> **Note:** In the following examples, square brackets (example: [Common]) denote placeholder variables for customer data. Replace these variables, including the brackets, with your own values.

/restapiurl

Example: Set the API URL:

```
/restapiurl /baseurl=https://host.domain/CherwellAPI/api/ /connection="[Com
mon]Cherwell Browser" /connectionuserid=CSDAdmin /connectionpassword=CSDAdm
in
```

Example: Get the API URL

```
/restapiurl /connection="[Common]Cherwell Browser" /connectionuserid=CSDAdm
in /connectionpassword=CSDAdmin
Output: https://host.domain/CherwellAPI/api/
```

Sub-command	Description
/baseurl	**Retrieve the Current URL** To retrieve the current base URL of the REST API, omit this value to write the current URL to the console. **Set the URL** The base URL of the REST API must be in the following format: https://host.domain/CherwellAPI/api/. **Accepted values**: string
/connection	The name of the CSM connection. **Accepted values**: string

Sub-command	Description
/connectionuserid	The CSM user ID for the requested server. **Accepted values**: string
/connectionpassword	The CSM password for the requested server. **Accepted values**: string

Related concepts
Set the Base URL for the Cherwell REST API
Related tasks
Configure Logging for the Cherwell REST API

Server Farm Command-Line Options

Use the Command-Line Configure (CLC) /serverfarm major command to access all sub-commands to manage Cherwell Server Farms using the Command-Line Configure (CLC) utility.

Note: In the following examples, square brackets (example: [Common]) denote placeholder variables for customer data. Replace these variables, including the brackets, with your own values.

/serverfarm

Example:

```
/serverfarm -serverfarmenable=true -serverfarmredislist=127.0.0.1:6379 -ser
verfarmredispassword="12345"
```

Sub-command	Description
/[serverfarmenable]	Enable or disable Server Farms. **Accepted values**: {true | false}
/[serverfarmredislist]	Specifies a comma-delimited list of Redis servers to add for Server Farms (Example: server1:6379,server2:6379). This option overwrites the existing list. **Accepted values**: string
/[serverfarmredispassword]	Specifies the Redis password. **Accepted values**: string
/[serverfarmredistimeout]	Specifies the Redis connection time-out period, in seconds. **Accepted values**: integer
/[serverfarmredissynctimeout]	Specifies the Redis sync time-out for server farms. The value is in seconds. **Accepted values**: integer

Related concepts
Scaling the CSM Web Applications
Cherwell Server Farms Q&A

Service Host Command-Line Options

Use the Command-Line Configure (CLC) /servicehost major command to access all sub-commands for the Cherwell Service Host and its microservices: Automation Processes, E-mail and Event Monitor, Mail Delivery, Scheduling, and System Event Processing. Use sub-commands to configure, start, stop, and uninstall the Service Host.

Note: In the following examples, square brackets (example: [Common]) denote placeholder variables for customer data. Replace these variables, including the brackets, with your own values.

/servicehost

Note: To configure options for multiple leaders at a time, use the /servicehost /configureleaders subcommand.

Example:

```
/servicehost -servicehostapleaderpause=false -connection="[Common]Cherwell
" -connectionuserid=CSDAdmin -connectionpassword=CSDAdmin
```

Sub-command	Description
/servicehostlogtologserver	If true, Service Host will log to the log server (Splunk). **Accepted values**: {true | false}
/servicehostlogserverloglevel	The minimum log level at which logs will be sent to the log server (Splunk). **Accepted values**: {fatal | error | warning | info | stats | debug}
/servicehostlogtoeventlog	If true, Service Host will log to the event log. **Accepted values**: {true | false}
/servicehostlogeventloglevel	The minimum log level at which logs will be sent to the event log. **Accepted values**: {fatal | error | warning | info | stats | debug}
/servicehostlogtofile	If true, Service Host will log to the file system log. **Accepted values**: {true | false}

Sub-command	Description
/servicehostlogfileloglevel	The minimum log level at which logs will be sent to the file system log. **Accepted values**: {fatal | error | warning | info | stats | debug}
/servicehostlogfilepath	The path to the file system logs. **Accepted values**: string
/servicehostlogmaxfilesizeinmb	Maximum log file size in MB. **Accepted values**: integer
/servicehostlogmaxfilesbeforerollover	Maximum number of log files before files roll over. **Accepted values**: integer
/servicehostuserid	Service Host User ID setting. **Accepted values**: string
/servicehostpassword	Service Host password setting. **Accepted values**: string
/servicehostconnection	Service Host connection setting. **Accepted values**: string
/servicehostusewindowslogin	If true, Service Host will use a Windows login. **Accepted values**: {true | false}
/servicehostusedefaultroleofuser	If true, Service Host will use the default role of the User. **Accepted values**: {true | false}
/servicehostmaxworkers	The number used to determine the maximum number of workers. For example, if you specify four and the machine has 4 virtual processors, then you will have a maximum of 16 workers. **Accepted values**: {true | false} **Default:** 21
/servicehostapleaderenable	If true, the Automation Process Service Leader is enabled. **Accepted values**: {true | false} **Default**: True

Sub-command	Description
/servicehostapleadermaxworkers	The maximum number of workers for the Automation Process Service. **Accepted values**: integer **Default**: 5
/servicehostapleaderheartbeatinterval	The AAutomation Process Service heartbeat interval in seconds. **Accepted values**: integer **Default**: 30
/servicehostapleaderwaittime	The amount of wait time in seconds for the Automation Process Service Leader to check the system for work. **Accepted values**: integer **Default**: 15
/servicehostapleaderblockstoprocess	The number of blocks of work for an Automation Process Service leader to process per interval. **Accepted values**: integer **Default**: 100
/servicehostapleaderscheduleditemspullcount	The number of items for the Automation Process Service to pull per block. **Accepted values**: integer **Default**: 100
/servicehostapleaderpause	If true, Automation Process Service is paused. **Accepted values**: {true | false} **Default**: False
/servicehostedleaderenable	If true, the Mail Delivery Service Leader is enabled. **Accepted values**: {true | false} **Default**: True
/servicehostedleadermaxworkers	The maximum number of workers for the Mail Delivery Service. **Accepted values**: integer **Default**: 5
/servicehostedleaderheartbeatinterval	The Mail Delivery Service heartbeat interval in seconds. **Accepted values**: integer **Default**: 30

Sub-command	Description
/servicehostedleaderwaittime	The amount of wait time in seconds for the Mail Delivery Service Leader to check the system for work. **Accepted values**: integer **Default**: 15
/servicehostedleaderpause	If true, the Mail Delivery Service is paused. **Accepted values**: {true | false} **Default**: False
/servicehosteeleaderenable	If true, the Email and Event Monitor Service Leader is enabled. **Accepted values**: {true | false} **Default**: True
/servicehosteeleadermaxworkers	The maximum number of workers for the Email and Event Monitor Service. **Accepted values**: integer **Default**: 5
/servicehosteeleaderheartbeatinterval	The Email and Event Monitor Service heartbeat interval in seconds. **Accepted values**: integer **Default**: 30
/servicehosteeleaderwaittime	The amount of wait time in seconds for the Email and Event Monitor Service Leader to check the system for work. **Accepted values**: integer **Default**: 15
/servicehosteeleaderemailitemspullcount	The number of items for theEmail and Event Monitor Service to process per pull. **Accepted values**: integer **Default**: 100
/servicehosteeleaderpause	If true, the Email and Event Monitor Service is paused. **Accepted values**: {true | false} **Default**: False
/servicehostssleaderenable	If true, the Scheduling Service Leader is enabled. **Accepted values**: {true | false} **Default**: True

Sub-command	Description
/servicehostssleadergroup	The group that this Scheduling Service will work on exclusively. **Accepted values**: string
/servicehostssleadermaxworkers	The maximum number of workers for Scheduling Service. **Accepted values**: integer **Default**: 5
/servicehostssleaderheartbeatinterval	The Scheduling Service heartbeat interval in seconds. **Accepted values**: integer **Default**: 30
/servicehostssleaderwaittime	The amount of wait time in seconds for the Scheduling Service Leader to check the system for work. **Accepted values**: integer **Default**: 15
/servicehostssleaderpause	If true, the Scheduling Service is paused. **Accepted values**: {true | false} **Default**: True
/servicehostwhleaderenable	If true, the System Event Processing Service Leader is enabled. **Accepted values**: {true | false} **Default**: True
/servicehostwhleadermaxworkers	The maximum number of workers for System Event Processing Service. **Accepted values**: integer **Default**: 5
/servicehostwhleaderheartbeatinterval	The System Event Processing Service heartbeat interval in seconds. **Accepted values**: integer **Default**: 30
/servicehostwhleaderwaittime	The amount of wait time in seconds for the System Event Processing Service Leader to check the system for work. **Accepted values**: integer **Default**: 15

Sub-command	Description
/servicehostwhleaderpause	If true, the System Event Processing Service is paused. **Accepted values**: {true | false} **Default**: True

/configureleaders

The purpose of this command is to configure service and logging settings for all the Service Host microservices: Automation Processes, E-mail Delivery, E-mail and Event Monitor, Scheduling, and Webhooks.

The **/leaders** option specifies which leaders all provided configuration options apply to. If a configuration option is not provided, that setting is ignored for all specified leaders.

Example:

```
# Disable Email Delivery and Email and Event Monitoring
/servicehost /configureleaders /leaders=emaildeliver,emailevent /leaderenab
le=false


# Enable file logging for all leaders
/servicehost /configureleaders /leaders=all /logtofile=true /fileloglevel=d
ebug


# Set Automated Process Scheduled items pull count and Email and Event item
s pull count to 50
# Note: Even with /leaders=all, the leader-specific option only aplies to a
pplicable leaders
/servicehost /configureleaders /leaders=all /itempullcount=50


# Set the number of blocks of work for an automated process leader to proce
ss per interval to 600
/servicehost /configureleaders /leader=automatedprocess /leaderblockstoproc
ess=600
```

Option	Description
/leaders	Determines which leaders to configure. "All" configures all leaders. Multiple leaders can be separated by comma or pipe "|". **Required**: True **Accepted values**: [All|AutomatedProcess|EmailDelivery|EmailEvent|Schedule|Webhook]
/logtologserver	Determines whether leaders will write logs to the log server. **Accepted values**: [True | False] **Default**: False
/logserverloglevel	The minimum log level at which logs will be sent to the log server. **Accepted values**: [Fatal | Error | Warning | Info | Stats | Debug] **Default**: Debug
/logtoeventlog	Determines whether leaders will log to the log server. **Accepted values**: [True | False] **Default**: True
/logeventloglevel	The minimum log level at which logs will be sent to the event log. **Accepted values**: [Fatal | Error | Warning | Info | Stats | Debug] **Default**: Warning
/logtofile	Determines whether leaders will log to the file system log. **Accepted values**: [True | False] **Default**: True
/logfileloglevel	The minimum log level at which logs will be sent to the file system log. **Accepted values**: [Fatal | Error | Warning | Info | Stats | Debug] **Default**: Debug
/logfilepath	The path to the file system logs. **Accepted values**: [String] **Default**: C:/Logs/csm_log.txt
/logmaxfilesizeinmb	The maximum log file size in MB. **Accepted values**: [Integer] **Default**: 10

Option	Description
/logmaxfilesbeforerollover	The maximum number of log filess before files roll over. **Accepted values**: [Integer] **Default**: 20
/logtosumologic	Determines whether the leaders will log to Sumo Logic. **Accepted values**: [True | False] **Default**: False
/sumologicloglevel	The minimum log level at which logs will be sent to Sumo Logic. **Accepted values**: [Fatal | Error | Warning | Info | Stats | Debug] **Default**: Warning
/leaderenable	Determines whether the leaders are enabled. **Accepted values**: [bool] **Default**: True
/leadermaxworkers	The maximimum number of workers for leaders. **Accepted values**: [Integer] **Default**: 5
/leaderheartbeatinterval	The leader's heartbeat interval in seconds. **Accepted values**: [Integer] **Default**: 30
/leaderwaittime	The amount of time in seconds for the leaders to wait before checking the system for work. **Accepted values**: [Integer] **Default**: 15
/leaderitemspullcount	The number of items for the leaders to pull per block. This applies to Automated Process and E-mail and Event Monitoring. **Accepted values**: [Integer] **Default**: 100
/leaderblockstoprocess	The number of blocks of work for a leader to process per interval. This applies to Automated Process. **Accepted values**: [Integer] **Default**: 100

Option	Description
/leadergroup	The group that the leaders will work on exclusively. This applies to Schedule. **Accepted values**: [String]

/servicehostinstall

Use the /servicehostinstall sub-command to install the Cherwell Service Host Windows service.

Example:

```
/servicehost /servicehostinstall /servicehostinstallaccount=LocalService
```

Example:

```
/servicehost /servicehostinstall /servicehostinstalluserid=Bob /servicehost
installpassword=1234 /servicehostinstallaccount=NetworkService
```

Option	Description
/servicehostinstalluserid	User ID the service will log on as. Optional as long as /servicehostinstallaccount has a valid value. **Accepted values**: string
/servicehostinstallpassword	Password that the service will log on with. Optional as long as /servicehostinstallaccount has a valid value. **Accepted values**: string
/servicehostinstallaccount	Account the service will log on as. Optional as long as /servicehostinstalluserid and /servicehostinstallpassword have valid values. If no /servicehostinstallaccount or /servicehostinstalluserid or /servicehostinstallpassword values are provided, then LocalService is used. **Accepted values**: [LocalService | LocalSystem | NetworkService] **Default**: LocalSystem
/servicehostinstallautostart	Set the service to auto start during installation. **Accepted values**: {true | false} **Default**: False

/servicehoststart

Use the /servicehoststart sub-command to start the Cherwell Service Host Windows service. There are no options for this sub-command.

Example:

```
/servicehost /servicehoststart
```

/servicehoststop

Use the /servicehoststop sub-command to stop the Cherwell Service Host Windows service. There are no options for this sub-command.

Example:

```
/servicehost /servicehoststop
```

/servicehostuninstall

Use the /servicehostuninstall sub-command to uninstall the Cherwell Service Host Windows service. There are no options for this sub-command.

Example:

```
/servicehost /servicehostuninstall
```

Related concepts

About the Cherwell Service Host

Configure the Cherwell Service Host

Configure Logging for a CSM Service, Web Application, and Cherwell REST API

Installing CSM from the Command Line

Trusted Agent Host Command-Line Options

Use the Command-Line Configure (CLC) /trustedagenthost major command to access all sub-commands for the Trusted Agent Host and host configuration.

/trustedagenthost

Examples:

```
/trustedagenthost /trustedagenthostpingfrequency=60 /trustedagenthosthubsha
redkey=supersecretkey
```

Sub-command	Description
/trustedagenthostlogtologserver	If true, Trusted Agent Host will log to the log server. **Accepted values**: {true | false}
/trustedagenthostlogserverloglevel	The minimum log level at which logs will be sent to the log server. **Accepted values**: {fatal | error | warning | info | stats | debug}
/trustedagenthostlogtoeventlog	If true, Trusted Agent Host will log to the event log. **Accepted values**: {true | false}
/trustedagenthostlogeventloglevel	The minimum log level at which logs will be sent to the event log. **Accepted values**: {fatal | error | warning | info | stats | debug}
/trustedagenthostlogtofile	If true, Trusted Agent Host will log to the file system log. **Accepted values**: {true | false}
/trustedagenthostlogfileloglevel	The minimum log level at which logs will be sent to the file system log. **Accepted values**: {fatal | error | warning | info | stats | debug}
/trustedagenthostlogfilepath	The path to the file system logs. **Accepted values**: string
/trustedagenthostlogmaxfilesizeinmb	The maximum log file size in MB. **Accepted values**: integer

Sub-command	Description
/trustedagenthostlogmaxfilesbeforerollover	The maximum number of log files before files roll over. **Accepted values**: integer
/trustedagenthostdisplayname	Overrides the display name of Trusted Agent Host. **Accepted values**: string
/trustedagenthosthuburl	The URL that is used for Trusted Agent communication. HTTPS is recommended. **Accepted values**: {url}
/trustedagenthosthubsharedkey	The shared key that is used for Trusted Agent communication. **Accepted values**: string
/trustedagenthostpingfrequency	The hub ping frequency in seconds. The default value is 30 seconds. **Accepted values**: integer

/trustedagenthostinstall

Use the /trustagenthostinstall sub-command to install the Trusted Agent Host Service.

Examples:

```
/trustedagenthost /trustedagenthostinstall /trustedagenthostinstallaccount=
LocalService
```

```
/trustedagenthost /trustedagenthostinstall /trustedagenthostinstalluserid=B
ob /trustedagenthostinstallpassword=1234 /trustedagenthostinstallaccount=Ne
tworkService
```

Sub-command	Description
/trustedagenthostinstallaccount	The account used by the service. This sub-command is optional if /trustedagenthostinstalluserid and /trustedagenthostinstallpassword have valid values. **Note:** If no values for the /trustedagenthostinstallaccount sub-command or /trustedagenthostinstalluserid or /trustedagenthostinstallpassword sub-commands are provided, then LocalSystem is used. **Accepted values**: {LocalService|LocalSystem|NetworkService}
/trustedagenthostinstallautostart	Sets the service to auto-start during installation. The default value is false. **Accepted values**: {true | false}
/trustedagenthostinstallpassword	The password used by the service to log on. This sub-command is optional if /trustedagenthostinstallaccount has a valid value. **Accepted values**: string
/trustedagenthostinstalluserid	The user ID used by the service to log on. This sub-command is optional if /trustedagenthostinstallaccount has a valid value. **Accepted values**: string

/trustedagenthoststart

Use the /trustedagenthoststart sub-command to start the Trusted Agent Host Windows service. There are no options for this sub-command.

Example:

```
/trustedagenthost /trustedagenthoststart
```

/trustedagenthoststop

Use the /trustedagenthoststop sub-command to stop the Trusted Agent Host Windows service. There are no options for this sub-command.

Example:

```
/trustedagenthost /trustedagenthoststop
```

/trustedagenthostuninstall

Use the /trustedagenthostuninstall sub-command to uninstall the Trusted Agent Host Windows service. There are no options for this sub-command.

Example:

```
/trustedagenthost /trustedagenthostuninstall
```

/trustedagenthub

Use the /trustedagenthub sub-command to configure the settings for the Trusted Agent hub.

Examples:

```
/trustedagenthub /trustedagenthubenable=true
```

```
/trustedagenthub /trustedagenthubenable=true /trustedagenthuboperationtimeo
ut=60 /trustedagenthubregistrationtimeout=360
```

Sub-command	Description
/trustedagenthubenable	Enable or disable the use of Trusted Agents. The default value is false. **Accepted values**: {true | false}
/trustedagenthuburl	The URL that is used for Trusted Agent communications. HTTPS is recommended. **Accepted values**: {url}
/trustedagenthubsharedkey	Value to use as the shared key for Trusted Agent communications. **Accepted values**: string
/trustedagenthubgeneratesharedkey	Generates a new cryptographically secure key for the Trusted Agent shared key. This key is then used as the value for /trustedagenthubsharedkey.
/trustedagenthuboperationtimeout	The operation timeout for Trusted Agents in seconds. The default value is 30 seconds. **Accepted values**: integer

Sub-command	Description
/trustedagenthubregistrationtimeout	The registration timeout for Trusted Agents in seconds. The default value is 180 seconds. **Accepted values**: integer

Related concepts

Trusted Agent

Configuring Trusted Agent

Trusted Agent Logging

Related tasks

Install the Trusted Agent Server

Health Check Command-Line Options

Use the Command-Line Configure (CLC) /healthcheck commands to run the Health Check tool via Command-Line Configuration (CLC) and monitor and optimize system configurations that impact performance.

You can run the /healthcheck commands in the following modes:

- **Full** (default): Runs selected rules, shows a summary on the console, and produces an HTML report to the specified file. If no file is specified, a default HealthCheck.html report is saved to the documents folder of the currently logged in CSM user.

- **Silent**: Produces no report. A default warning level of Low is used. However, you can optionally set a higher warning level (such as, Urgent). If no warnings are found, a result of 0 (success) is returned. If the Health Check finds warnings, a value of 1 (failure) is returned.

> **Note:**
> - If you require a report, do not use silent mode. Silent mode ignores /reportfilesavepath or /reportfilename parameters.
>
> - The /warninglevel parameter only works in silent mode. It provides a failure measure for silent mode, specifically.

When running the /healthcheck commands, you can optionally run all Health Check rules, or run a specified set of rules. You can optionally run multiple lines in a single call.

/healthcheck

Example: Run the Health Check tool with all rules and provide a default report

The following example runs a Health Check against a Cherwell database, based on the provided connection information. On completion, a default report called HealthCheck.html is saved to the Documents folder of the currently logged in CSM user (the default save location). No rules are specified; consequently all rules available in the system are run.

```
/healthcheck /connection="[Common]Cherwell Browser" /connectionuserid="CSDA
dmin" /connectionpassword="CSDAdmin"
```

Example: Run the Health Check tool with specific rules and provide a unique report

The following example runs a Health Check against a Cherwell database, based on the provided connection information. On completion, a report called HealthCheckReport.html is saved to the specified C:/dev folder. The example runs generic rules (as CSM Administrator does) and the specified Mismatched Def IDs and Missing Index Rule rules.

```
/healthcheck /connection="[Common]Cherwell Browser" /connectionuserid="CSDA
dmin" /connectionpassword="CSDAdmin" /reportfilename="HealthCheckReport" /r
eportfilesavepath="C:/dev" /rules="mismatcheddefids, missingindexrule"
```

Example: Run the Health Check in silent mode with a warning level of Urgent

The following example runs a Health Check in silent mode (No report is produced). No rules are specified, consequently all rules available in the system are run. If no issues with the specified warning level of Urgent or higher are found, a result of 0 (success) is returned. If one or more issues with the specified warning level of Urgent or higher are found, a result of 1 (failure) is returned.

```
/healthcheck /connection="[Common]Cherwell Browser" /connectionuserid="CSDA
dmin" /connectionpassword="CSDAdmin" /silent="true" /warninglevel="urgent"
```

Sub-command	Description
/connection	The name of the CSM connection. **Accepted values**: string
/connectionuserid	The CSM user ID for the requested server. **Accepted values**: string
/connectionpassword	The CSM user password with which to log in. **Accepted values**: string

Sub-command	Description
/rules	Specifies the rules for each run of the Health Check tool. Enter a comma delimited list (example: "rule 1, rule2, etc."). If you provide no rules, or if /rules is not specified, *all* rules available in the system are run. The available rules are: • missingnativerestapiclients (Missing Native REST API Clients) • runtimeperformancewarnings (Runtime Performance Warnings) • foreignkeyconfiguration (Foreign key configuration) • checkcanonicalcompliance (Check Canonical Compliance) • outofdateindexstatistics (Out of date Index Statistics) • checkbusinessobjectsforconsistency (Check Business Objects for consistency) • mismatcheddefids (Mismatched Def IDs) • businessobjectcachablecheck (Business Object Cachable Check) • missingindexrule (Missing Index Rule) **Note:** You can enter rules using any case. Spaces are ignored. For example, you can specify the mismatcheddefids rule as "Mismatched Def IDs".
/silent	Used with /warninglevel below. Runs the Health Check tool in silent mode. No report file is created. The run returns either 0 for success, or 1 for failure.

Sub-command	Description
/warninglevel	Used with /silent above. Specifies the warning level for each run of the Health Check tool in silent mode. The silent Health Check is run for the specified warning level and all levels *higher* than it (excluding Error which only applies under certain circumstances). For example, if you specify a warning level of Medium and the Health Check finds no medium impact but an Urgent warning is found, a result of 1 (failure) is still returned. If you do not provide a warning level, a default level of Low is used. The available warning levels (listed from low to high) are: • **Low**: Low impact on system health. Some low priority recommendations to consider. • **Medium**: Some impact on system health. Some medium priority recommendations to consider. • **Urgent**: Major impact on system health. Some urgent priority recommendations to consider. • **Error**: Only used when a Health Check rule is run *before* publishing a Blueprint. Impact is major enough to recommend *not* publishing the Blueprint. **Default**: Low
/reportfilesavepath	Specifies the location to which the Health Check report is saved. If you do not provide a save location, a default location of the Documents folder for the logged in CSM user is used. **Default**: Documents folder for the logged in CSM user
/reportfilename	Specifies the file name for the Health Check report. If you do not provide a file name, a default file name of HealthCheck.html is used. **Default**: HealthCheck **Warning:** Do not include the file extension in the specified file name. For example, enter `health_report_1`. Do *not* enter `health_report_1.html`.

/healthcheckblueprint

Example: Convert the Health Check results into a Blueprint

The following example shows the filepath to the Health_Check_Results.html input file containing results to convert into a Blueprint. Also shown is the filepath to where the export file for the resulting Blueprint is created.

```
/healthcheckblueprint /connection="[Common]Cherwell Browser" /connectionuse
rid="CSDAdmin" /connectionpassword="CSDAdmin" /inputpath="C:/Users/Username
/Desktop/Health_Check_Results.html" /exportpath="C:/Users/Username/Desktop"
```

Sub-command	Description
/connection	The name of the CSM connection. **Accepted values**: string
/connectionuserid	The CSM user ID for the requested server. **Accepted values**: string
/connectionpassword	The CSM user password with which to log in. **Accepted values**: string
/inputpath	The filepath to the .html input file containing Health Check results to convert into a Blueprint.
/exportpath	The filepath to the location in which the resulting Blueprint is created. **Note:** This must be a valid filepath that does not already exist.

Related concepts
About Performance Health Check

Other Command-Line Options

You can launch CSM from a command line to automatically execute instructions. For example, a third-party tool might launch the CSM application to take a user to a specific Incident record. An administrator can automatically execute a system backup. CSM supports a number of command-line options for making these tasks possible.

A command also allows a hyperlink to be created in an email that, when clicked, launches the CSM application and executes an instruction. For this to work, CSM must be installed on the machine.

In both cases (command-line or hyperlink) if CSM is already running, the command is still executed, without relaunching the application or requiring the user to log in again. CSM executes the command in a separate console window and will not interfere with any CSM windows/applications running.

Good to Know:

- Arguments can either be prefixed with a forward slash or with a dash, so /? and -? are equivalent.
- In the provided examples, square brackets (example: [Common]) denote placeholder variables for customer data. Replace these variables, including the brackets, with your own values.

Client Command-Line Options

Use the CSM client command-line options to automatically execute instructions or commands. Client command-line options can launch programs more quickly and use fewer system resources.

To use the CSM client command-line options, execute the CSM Desktop Client with arguments. The client application to run is called Trebuchet.App.exe, which is found in the Cherwell Service Management installation directory.

General Settings

Option	Description
/?	Provides help text for the supported command-line options.
/c	This is the connection to use. To use a connection that is available to all users of the machine, add the prefix [Common]. To use a connection that is associated with the current user, add the prefix [User]. When using the interactive dialog, [Common] connections are on the **All Users** tab, while [User] connections are on the tab named for the current user.
/u	This is the user ID to use. This only works when CSM authentication is enabled and is not supported with other authentication types (Windows or LDAP).
/p	This is the password to use. This only works when CSM authentication is enabled and is not supported with other authentication types (Windows or LDAP). **Note:** Putting a password into a shortcut is a potential security issue, since other users can edit the properties of the shortcut and read the password.
/l or /r	This is the culture override. Example language culture pairs are: de-DE (German), fr-FR (French), and pt-BR (Portuguese). Use /l to set the culture for content strings; use /r to set the culture for platform strings. For more information, see String Types.

The format for connection is:

```
Trebuchet.App.exe /c "[Common]connection name"
```

The format for user ID and password is:

```
Trebuchet.App.exe /u user ID/p password
```

The format for culture is:

```
Trebuchet.App.exe /l language-culture pair /r language-culture pair
```

Logging Authentication Information

Option	Description
/la logfile	This option specifies the path and file name where authentication information should be logged. This must also be enabled in Security Settings.

Command Execution

Option	Description
/n	This option specifies to use a new window (default).
/g [name] [id]	This is the Goto record: Name = name of Business Object; ID = ID of record. This command takes the system to a particular record, identified by its internal record ID. This is a special value used to uniquely identify records (Example: 939cd1f313b3b6866ef7d043faa258398c765d444a). Obtain this value by running a One-Step Action that populates or writes to a field or a file, the value in the RecID field. An exception to this is the Incident Business Object. For historical reasons, (although there is a RecID field in Incident) Incident actually uses its IncidentID as a RecID. Other custom objects might also use different fields for the record ID. If using a tool to launch CSM and bring up a record, sometimes the RecID comes from a query or other mechanism.
/gp [name] [public id]	This is the Goto record by public ID: Name = name of the Business Object; Public ID = Public ID of record. The Public ID of a Business Object is the ID by which it is normally identified by users. For an Incident, this would be the Incident ID; for a Change, it would be the Change ID (Example: Change 12345). The Public ID does not need to be a number. For example, the Public ID for a customer is the customer's full name.
/gs [name] [Saved Search]	This is the Goto Saved Search: Name = name of the Business Object; Saved Search = Name of Saved Search. This option launches a named global search and displays the results. Use the following format for the Saved Search to launch non-global searches: Scope;Scope-Owner;SavedSearch. The scope can be any supported scope – Global, Team, Persona (the internal name for role), user, etc. The scope-owner must be the internal ID of the owner. **Note:** This is a 42-character ID that identifies the team, the user, or the role. For this reason, this functionality is designed to be used in very specialized circumstances.
/s [name] [search text]	This executes a text search: Name = name of the Business Object; Search text = text to find. This option allows searching for arbitrary text in the specified type of record. This is the equivalent of typing search text into the quick search box in the main application. **Note:** The Business Object must have full-text searching enabled, and the text needs to be URL encoded.
/NP	This executes a new process. Normally, when launching the CSM Desktop Client (with or without any additional command-line arguments) the system checks if it is already running. If it is, a new window of the existing process is launched. This means the program launches more quickly and uses less system resources. If the application is already running, arguments related to connection, user ID, and password are ignored. By using /NP, the application does not try to find an existing instance and always launches a new one. **Note:** If the CSM Desktop Client is run from two different directories, it always creates a new instance.

The format for Goto record is:

```
Trebuchet.App.exe /g [name] [id]
```

The format for Goto record by public ID is:

```
Trebuchet.App.exe /gp [name] [public id]
```

The format for Goto Saved Search is:

```
Trebuchet.App.exe /gs [name] [Saved Search]
```

The format for search for text is:

```
Trebuchet.App.exe /s [name] [search text]
```

Administrative Command-Line Options

Use the Administrative command-line to launch CSM Administrator and automatically execute instructions or commands. Administrative command-line options can launch programs more quickly, use less system resources, and perform tasks more efficiently.

To use the Administrative command-line options, execute CSM Administrator with arguments. The administrative application to run is called Trebuchet.Admin.exe, which is found in the Cherwell Service Management installation directory.

General Settings

Option	Description
/?	Provides help text for the supported command-line options.
/c	This is the connection to use. To use a connection that is available to all users of the machine, add the prefix [Common]. To use a connection that is associated with the current user, add the prefix [User]. When using the interactive dialog, [Common] connections are on the **All Users** tab, while [User] connections are on the tab named for the current user.
/u	This is the user ID to use. This only works when CSM authentication is enabled and is not supported with other authentication types (Windows or LDAP).
/p	This is the password to use. This only works when CSM authentication is enabled and is not supported with other authentication types (Windows or LDAP). **Note:** Putting a password into a shortcut is a potential security issue, since other users can edit the properties of the shortcut and read the password.
/l or /r	This is the culture override. Example language culture pairs are: de-DE (German), fr-FR (French), and pt-BR (Portuguese). Use /l to set the culture for content strings; use /r to set the culture for platform strings. For more information, see String Types.

The format for connection is:

```
Trebuchet.Admin.exe /c "[Common]connection name"
```

The format for User ID and password is:

```
Trebuchet.Admin.exe /u User ID/p password
```

The format for culture is:

```
Trebuchet.Admin.exe /l language-culture pair /r language-culture pair
```

System Backup

Option	Description
/b [path and file]	This is the path and file name that the back up should go to. If the extension is a .car, then the backup is an uncompressed archive. If the extension is a .czar, or not included, the backup is compressed in a .czar file format.

Option	Description
/r [rollover option]	These are the rollover options. To have the file name automatically have date/time information be appended, use this optional argument. If used with /b, it causes the date/time information to be appended to the file name. The options are: • Unmodified: No value is appended. • Current: The current date and time is appended. • Nightly: The current date is appended. • Weekly: The day of the week is appended. • Monthly: The day of the month is appended. • Yearly: The month and day of the month is appended.
/c	This is the connection to use. To use a connection that is available to all users of the machine, add the prefix [Common]. To use a connection that is associated with the current user, add the prefix [User]. When using the interactive dialog, [Common] connections are on the **All Users** tab, while [User] connections are on the tab named for the current user.
/u	This is the User ID to use. This only works when CSM authentication is enabled and is not supported with other authentication types (Windows or LDAP).
/p	This is the password to use. This only works when CSM authentication is enabled and is not supported with other authentication types (Windows or LDAP). **Note:** Putting a password into a shortcut is a potential security issue, since other users can edit the properties of the shortcut and read the password.

You can use administrative command-line options to do backups outside of the CSM Scheduler. For example, you want to use different scheduler or would like the backup to be done on a system that is not running the CSM Scheduler. This is common when installed in a SaaS environment.

The format for backing up CSM is:

```
Trebuchet.Admin.exe /c "C:\..." /u User ID/p password /b [path and file] /r
["rollover option"]
```

The connection, user ID, and password work the same as for any other application.

Logging Authentication Information

Option	Description
/la logfile	This specifies the path and file name where authentication information should be logged. This must also be enabled in Security Settings.

System Maintenance

Option	Description
/db	This is a comma-delimited list of which database maintenance operations to run. The options are: • RebuildSystemTableIndexes: Rebuilds indexes of all system database tables. • RebuildFullTextCatalog: Rebuilds the Full-Text Search catalog. • RebuildAllBusObIndexes: Rebuilds indexes of all business object tables. • RefreshQueueStatus: Updates the queue status data. • ShrinkDatabaseLog: Reduces the size of the database log. • RemoveUnusedAuthRecords: Removes obsolete authorization data.

The format for system maintenance is:

```
Trebuchet.Admin.exe /c "[Common]connection name" /u User ID/p password /db
delimited-list-of-options
```

As an example, to rebuild the full text catalog and refresh queue status, execute the following command (all on one line):

```
Trebuchet.Admin.exe /c "[Common]Cherwell Browser" /u Henri /p password /db
RebuildFullTextCatalog,RefreshQueueStatus
```

System Restore Command-Line Options

Use System Restore command-line options to automatically execute instructions or commands. A system administrator can use the System Restore command-line options to import the CSM database for the first time or reload the CSM database from an archive file (.czar file).

To use the System Restore command-line options, execute CSM Administrator with arguments. The System Restore application to run is called SystemRestore.exe, which is found in the Cherwell Service Management installation directory.

General Settings

Option	Description
/?	Provides help text for the supported command-line options.
/s or /i	This option specifies to run from the installer.
/w	This option specifies to run for web applications.
/a	This option specifies to run automatically.
/pc	This specifies a privileged connection.
/z	This is the .czar file location.
/c	This is the connection to use. To use a connection that is available to all users of the machine, add the prefix [Common]. To use a connection that is associated with the current user, add the prefix [User]. When using the interactive dialog, [Common] connections are on the **All Users** tab, while [User] connections are on the tab named for the current user.
/u	This is the user ID to use. This only works when CSM authentication is enabled and is not supported with other authentication types (Windows or LDAP).
/p	This is the password to use. This only works when CSM authentication is enabled and is not supported with other authentication types (Windows or LDAP). **Note:** Putting a password into a shortcut is a potential security issue, since other users can edit the properties of the shortcut and read the password.
/pe	This is the encrypted password to use.
/ps	This is the platform definition file location.
/unicode	This option enables Unicode support.

Example of a System Restore command-line flag:

```
/c "[Common]Cherwell Browser" /u henri /p mypassword /z "C:\Cherwell/
CherwellDemo.czar" /a
```

Platform Resource Manager Command-Line Options

Use the Platform Resource Manager command-line utility to export and import CSM platform string satellite assemblies. Assemblies are exported as .dll files, which can be imported into software localization tools.

Review and modify strings in the localization tool, and then export them as a satellite assembly that can be reimported into CSM using the Platform Resource Manager command-line utility.

The Platform Resource Utility is run from the command window by calling Trebuchet.Platform.Resource.Manager.exe. This utility is located in the Cherwell Service Management installation directory.

Prerequisites

To exports assemblies, you must install the .Net SDK developer tools on the machine that runs the Platform Resource Manager command-line utility. You can download and install the relevant tools from https://developer.microsoft.com/en-us/windows/downloads/sdk-archive.

Export and Import Options

Option	Description
/devex	Use to convert to a .tsv file DevExpress assemblies from English to the specified culture. The DevExpress binaries must be available in the specified folder. (Use /rexp to export the DevExpress assemblies.) Example: `/devex "C:\temp\filelocation\de-de" "de-de"`
/rexp	Use to export and create the binary resource files in the specified location for the target language specified. The target language parameter must match a value in the CSM database. Example: `/rexp "C:\temp\filelocation" "de-de"`

Option	Description
/ri	Use to import resource assemblies. Optional parameters: Assemblies folder location; language/culture pair. Example: `/ri "C:\temp\filelocation\de-de" "de-de"` When invoked with no parameters from the folder than contains assemblies, the assemblies are scanned for resources and imported as en.
/tools	Optional. Use with /rexp to provide the location of the Microsoft Windows SDK utility (AL.exe). Example: `/tools "C:\Programs\toollocation\al.exe"` If not used, the application will try to determine the location, if possible.

Optional Connection Options

You can specify optional connection options from the command line. If you do not, you are prompted to select a connection and login information when you run an export or import command.

Option	Description
/c	This is the connection to use. To use a connection that is available to all users of the machine, add the prefix [Common]. To use a connection that is associated with the current user, add the prefix [User]. When using the interactive dialog, [Common] connections are on the **All Users** tab, while [User] connections are on the tab named for the current user.
/u	This is the user ID to use. This only works when CSM authentication is enabled and is not supported with other authentication types (Windows or LDAP).
/p	This is the password to use. This only works when CSM authentication is enabled and is not supported with other authentication types (Windows or LDAP). **Note:** Putting a password into a shortcut is a potential security issue, since other users can edit the properties of the shortcut and read the password.

Scaling CSM

There are two ways to scale CSM. One is to horizontally scale high-impact services, such as the Automation Process and the Email and Event Monitor. The other is to implement a server farm to load balance the CSM web applications.

In most cases, CSM will perform well without additional scaling. If you see performance spikes over time, you may choose to scale the Cherwell Service Host, the CSM web applications, or both. You can also try increasing the RAM and CPU on the CSM server before using one of the more advanced methods.

The scaling method you use depends on these factors:

- **Scale the Cherwell Service Host only.**

  If you use a lot of automation, such as Automation Processes and One-Step Actions, consider scaling the Cherwell Service Host. See Scaling the Cherwell Service Host .

- **Scale the web applications only.**

  If you have a large number of people using the system at the same time, consider scaling the web applications. See Scaling the CSM Web Applications.

- **Scale the Cherwell Service Host and the web applications.**

  If you use a lot of automation and you have a large number of people using the system at the same time, you can scale the Cherwell Service Host and the web applications.

Related concepts
Scaling the CSM Web Applications
Scaling Scenarios
Recommended Cherwell Service Host Scaling Configurations
Related information
Scaling the Cherwell Service Host

Scaling the Cherwell Service Host

Cherwell® Service Management (CSM) uses a dedicated message queue system to allow horizontal and vertical scaling for one or more server components. Scaling CSM enables the system to use a network of machines to distribute work, providing more resources to alleviate barriers and improve availability.

Common Terms and Definitions

See the following common terms and definitions that are related to horizontal and vertical scaling deployments.

- Horizontal Scale — The process of adding more machines to a pool of resources.
- Vertical Scale — The process of adding more resources (CPU, RAM) to a single machine.
- Queue — The message destination and repository where messages are stored until they are delivered to a CSM Service.
- Scaled Services — Services include Automation Process Service, Email and Event Monitor Service, Mail Delivery Service, and Scheduling Service.
- Enqueue — To add a unit of work or data to the queue to await processing.
- Dequeue — To remove a unit of work or data from the queue to begin processing.

Configuration Rules and Considerations

The number of configurations for CSM is widely varied, but these constant rules must be followed for a successful configuration.

- At least one of each of the scaled services must be enabled.
- If a scheduled group item makes use of a resource that only exists on a single node, then the system must be configured to only run scheduled group items of that group on that specific node.
- Cherwell Service Host comes preconfigured to vertically scale all services equally. This configuration may not work in all installations and can be adjusted, allowing the services to scale vertically to different levels.
- To ensure the correct actions are taken, consider the current utilization of a node before changing the scale of that node,

Related concepts
About the Cherwell Service Host
Recommended Cherwell Service Host Scaling Configurations
Scaling the CSM Web Applications

Recommended Cherwell Service Host Scaling Configurations

Cherwell recommends the following deployments and configurations to horizontally scale the various components of CSM.

The configurations described below do not apply to hosted environments that use the Cherwell Service Host to run a local Scheduler. See Configure the Cherwell Service Host for a Local Scheduler.

🖉 **Note:** Cherwell recommends no more than 21 workers per Service Host process.

Single-Node Configuration

In this typical CSM server installation, all Cherwell components are on a single machine and do not require horizontal scaling considerations. However, individual services scale vertically automatically. By default, each of the scaled services vertically scale when more work is enqueued then can be dequeued with the current resources.
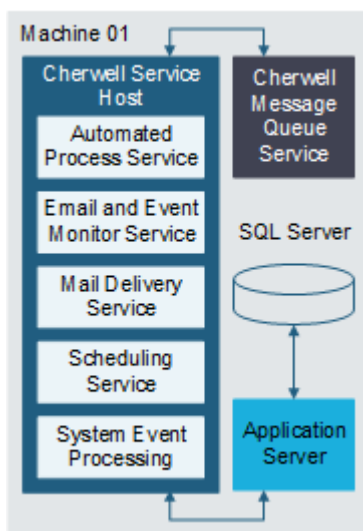
To set up a single-node configuration, the Cherwell Service Host component is installed on a new machine. After the installation is complete, Cherwell Service Host is configured to communicate with the Application Server and the Cherwell Message Queue Service.

Full-Node Scaling Configuration

When the original installation can no longer handle the rate of work enqueued by CSM, and the original node can no longer vertically scale, then you should scale the system horizontally. The most straightforward way to horizontally scale CSM is to create a new full node.
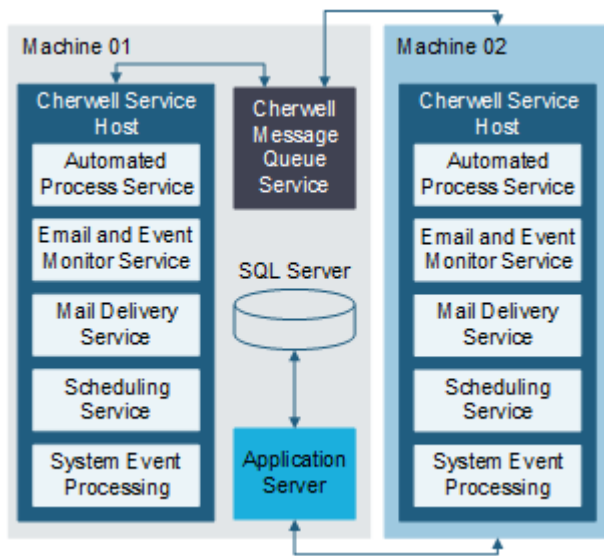
In this configuration, the Cherwell Service Host component is installed on a new machine. After the installation is complete, Cherwell Service Host is configured to communicate with the Application Server and the Cherwell Message Queue Service from the first node.

Single-Service Separate Node Partial Scaling Configuration

Individual components of the CSM infrastructure may become overwhelmed as a company's domain-specific business logic is implemented. In these cases, the CSM installation can be a single service at a time to help accommodate the workload.
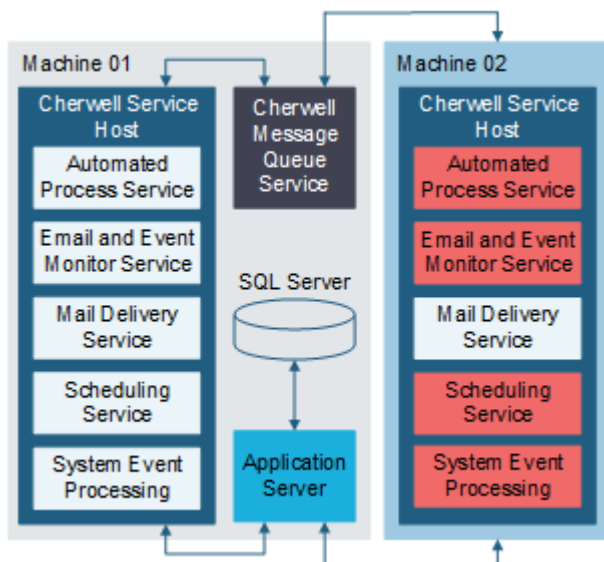
In this scenario, the original installation is no longer able to keep up with the mail delivery workload and must scale. To accommodate a large amount of mail that needs to be delivered, a new instance of Cherwell Service Host is installed on a new server. The server is configured to communicate with the

Application Server and the Cherwell Message Queue Service that is installed on the first node. Cherwell Service Host manages all services except for Mail Delivery Service, which is disabled.

Single-Service Separate Node Full Scale Configuration

In more advanced scenarios, CSM is scalable on any combination of services that are active on any number of nodes. While the options of scaled services are almost endless, a few rules must be maintained. One example configuration of CSM at scale is a single service per node.
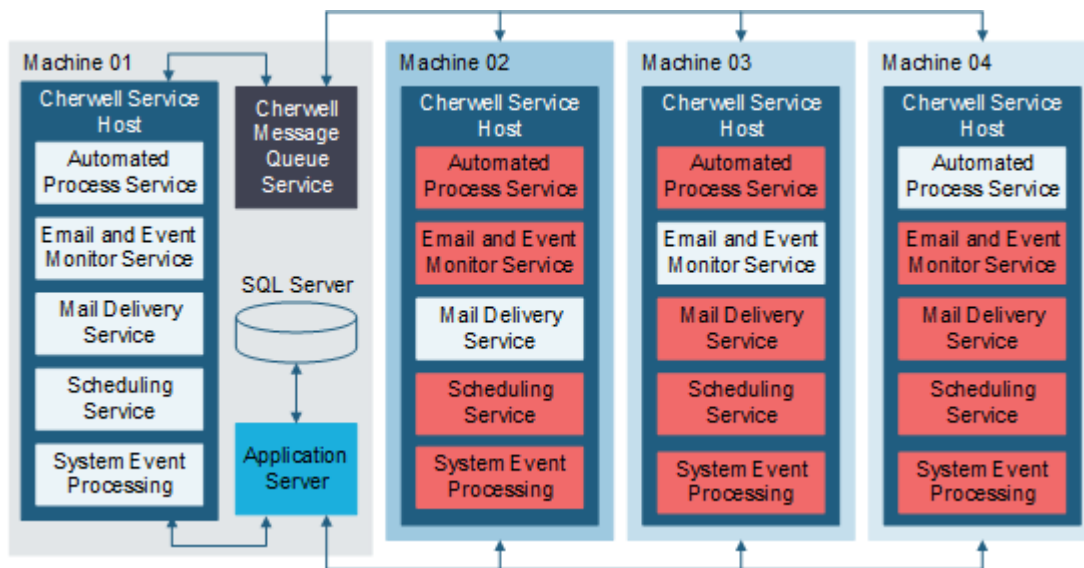
In this configuration, the Cherwell Service Host component is installed on three new machines. After the installation is complete on each of the machines, Cherwell Service Host is configured to communicate with the Application Server and the Cherwell Message Queue Service from the first node. With communications configuration complete, each of the four Cherwell Service Host systems are configured to enable only a single service, one on each box.

Related concepts
Scaling the CSM Web Applications

Scaling Scenarios
Related information
Scaling the Cherwell Service Host

Scaling the CSM Web Applications

A Cherwell server farm enables you to scale CSM web applications less expensively and without the constraints of a single server. A server farm allows high volumes of users to utilize several medium (4-core or higher) servers. A server farm typically consists of multiple CSM servers connecting to multiple Redis servers.

There is near-linear growth using Cherwell server farms. The more servers added to the farm, the more users CSM web applications can support. For example, assuming identical hardware is used, if users are consuming 100 percent of CPU on a single server, create a farm with three servers to support more users. If two servers support 100 users, then three servers can support 150 users.

There are two main reasons to implement a Cherwell server farm:

- **To scale the number of users.**

  You can add more hardware and grow horizontally to satisfy the demands of the population. In a single-server scenario, you would have to add hardware to a single server, but there's a limit to the amount of hardware you can implement in a single machine. The more you grow a single server, the more expensive it gets. Use a Cherwell server farm to add low-cost commodity boxes to the farm without having to exponentially pay more.

- **To provide redundancy.**

  A Cherwell server farm eliminates a single point of failure because if one server fails or is taken down for maintenance, CSM can still be used by its users.

Server Farm Components

Some scaling can typically be done in a single-server scenario just by adding CPUs and memory to the one machine. Such a proposition usually costs more than increasing the number of commodity servers in a Cherwell server farm.
Server farms can be configured differently from business to business, but all server farms should have similar components set up in the same way.

A server farm will contain the following components at a minimum:

- **Load Balancer** (not provided by Cherwell): Takes a certain load of users and balances them out across different servers. The load balancer is set up between the company firewall and the web service servers. The load balancer directs traffic to the server with the most availability, or one of the other distribution methods.

- **Web Servers**: Deliver information and process users' requests. All servers must be configured the same way. Be sure all servers have the same hardware configuration and point to the same SQL and Redis. There are two types of servers:
    ◦ A physical server (box)

    ◦ A virtual server, which is a software server, installed on a physical server; or a virtual machine installed on a hypervisor (bare-metal OS installed on a physical host).

- **Databases** (not provided by Cherwell): The SQL Server and Redis Server hold the content of a CSM system.

Single CSM Server Setup

Database Server   CSM Server   Firewall

Server Farm Setup

Database Server   Redis   CSM Servers   Load Balancer   Firewall
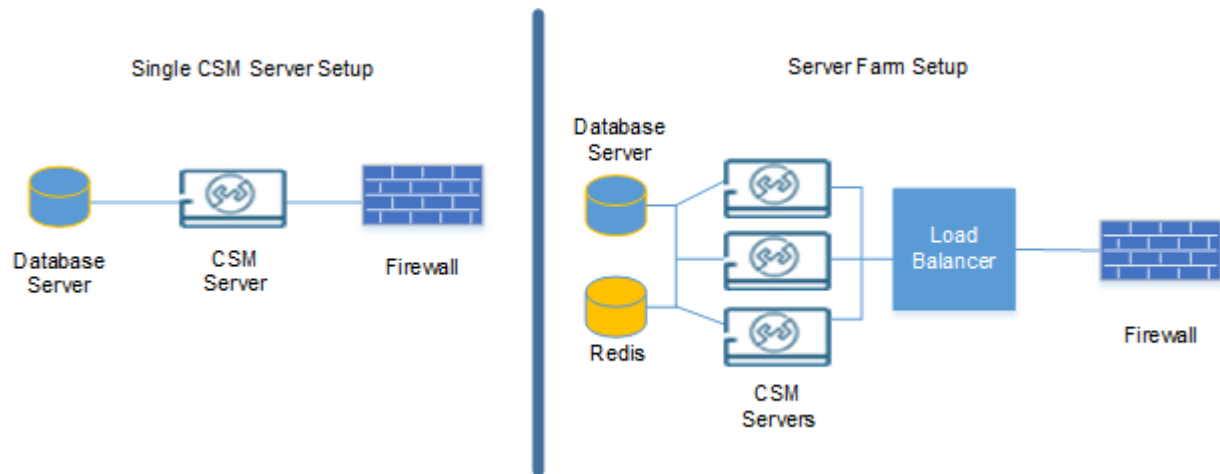
Related concepts

Scaling Scenarios

Purpose of Redis

Using a Load Balancer with CSM

Implementing a Cherwell Server Farm

Related information

Scaling the Cherwell Service Host

Purpose of Redis

Redis is an in-memory data structure store and is used as a database, cache, and message broker. Redis functions as an in-memory cache for Cherwell server farms.

By connecting every web server to the same Redis, the applications can share state and collaborate. When a server performs an operation, it saves the state of the current user or application to Redis. In a scenario where a user is bounced from one server to the another, each server can pick up from where the previous server left off by retrieving the latest state from Redis.

For a Cherwell Application Server, the cost of synchronizing with Redis is minimal because the Application Server exchanges a limited amount of information with Redis. For a Cherwell web server, Internet Information Services (IIS) holds state for each user in form of session, and it can reach the size of a few MB (3-5 MB is the typical size). For every web request going from the Cherwell web application to the server, there is an exchange of session state twice with Redis:

- When the request starts, to retrieve session from Redis.
- When the request ends, to save session to Redis.

For more information and support, refer to Redis.Io.

Related concepts

Scaling the CSM Web Applications

Using a Load Balancer with CSM

Advanced Redis Information

Using a Load Balancer with CSM

A Cherwell server farm enables you to add load-balancing capabilities using your existing firewall between the CSM server and the web.

In a single-server scenario, all traffic that comes in for CSM is directed to the same server. In a Cherwell server farm, users are redirected to different machines.

The Cherwell Application Server and the web server can be load balanced. These servers can run in a load-balanced mode where servers on different machines can coordinate as a single unit by communicating with a central-state storage. CSM uses Redis as a central-state storage technology. For more information, see Purpose of Redis.

Three load-balanced servers should be deployed to match the performance of a single standalone server. This is due to the overhead associated with the Cherwell Server Farm topology. The UI in a load-balanced environment can appear slightly slower because of session state serialization and Redis traffic.

The following example shows how a load balancer can be configured to handle requests.
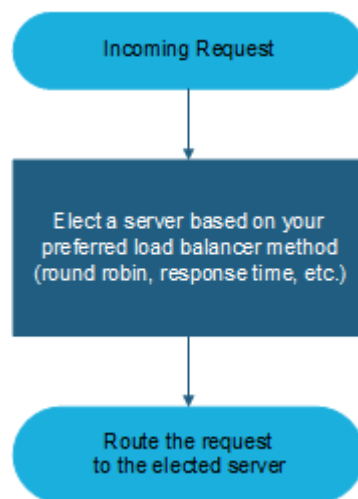
Related concepts
Scaling the CSM Web Applications
Purpose of Redis
Implementing a Cherwell Server Farm
Related information
Scaling the Cherwell Service Host

Scaling Scenarios

Server farms are flexible enough to handle various configurations. The simplest setup is to use multiple CSM servers to handle the user load and a single server to handle the service load. Or, you can distribute services across multiple servers and enable a cluster for the Cherwell Message Queue Service.

The example scenarios assume each machine in the Cherwell server farm is a commodity box.

Minimal Server Farm

The following example shows the most common scaling scenario and the easiest to configure. The Cherwell Application Server and CSM web servers share machines, and a single instance of the Cherwell Service Host is configured.
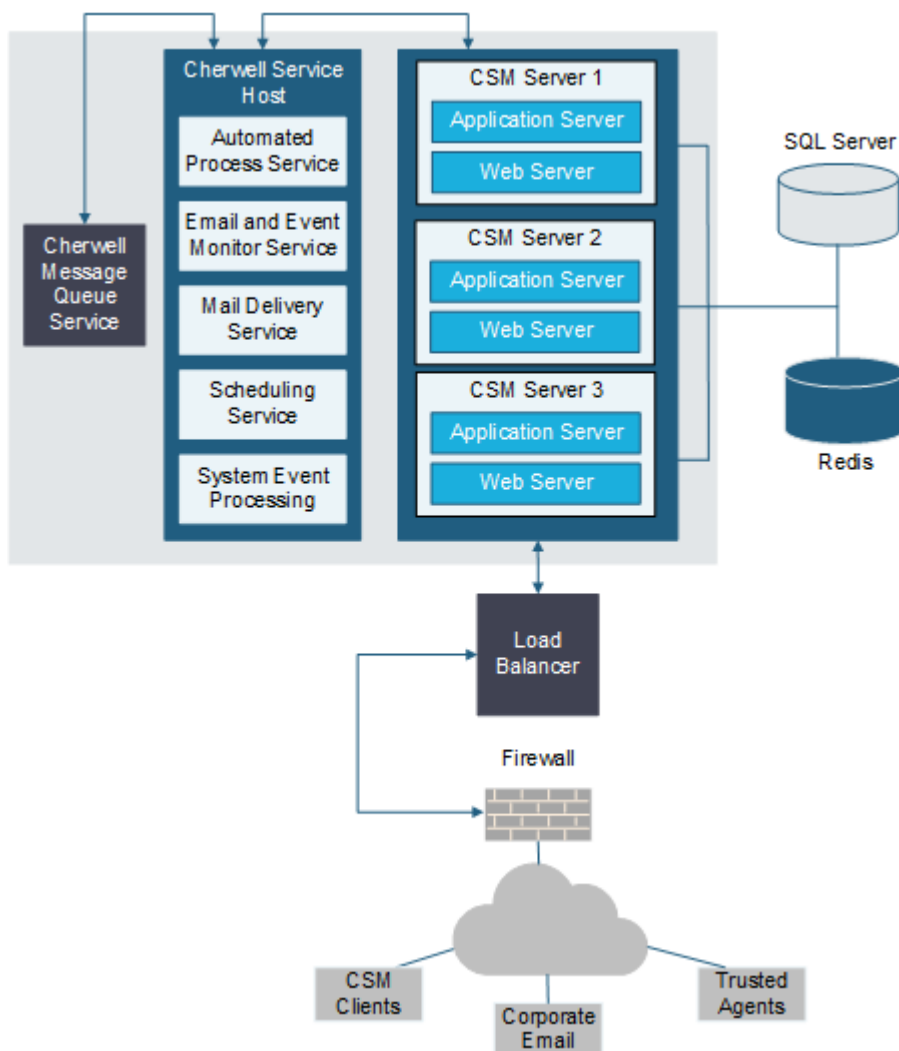
Distributed Services

The following example shows how to scale by creating a cluster for the Cherwell Message Queue Service and distributing the load for individual services across the cluster. You can choose to run the Cherwell Service Host on the same machines as a CSM server or on different machines.
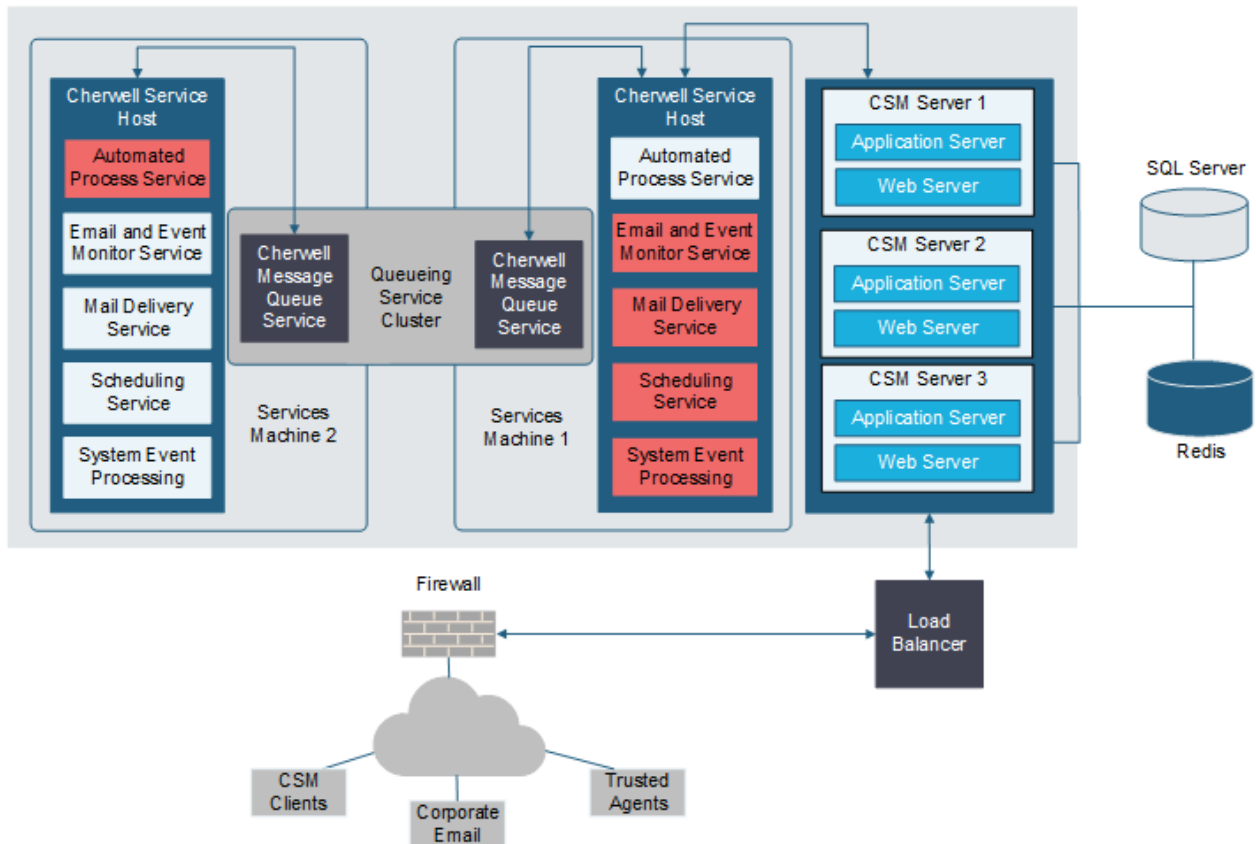
For guidance on configuring a Cherwell Message Queue Service/RabbitMQ cluster, see Configuring a Cluster for Cherwell Message Queue Service.

Related concepts

Scaling the CSM Web Applications

Recommended Cherwell Service Host Scaling Configurations

Related information

Scaling the Cherwell Service Host

Server Farm Resource Recommendations

No two Cherwell server farms are identical because of the user load they are under, the CSM content and configuration, and how the product is used. Our recommendations assume that your network, load balancer, and SQL Server infrastructure are inherently scalable to the size needed.

CSM Requirements

When promoting from a single server to a Cherwell server farm model, remember that a Cherwell server farm incurs overhead that lowers the number of concurrent users serviced by a single machine. Three load-balanced servers is the standard recommendation to handle the same user load with high-availability.

When designing the configuration for the Cherwell server farm, use these guidelines for CSM components.

- **Hardware**:
  Use the same hardware across servers for easier management and performance predictability. Be careful when using virtual machines. If all virtual machines are on the same physical hardware and the server goes down, the web farm stops working.

  If CSM is installed on a single server using a big server approach (8 core, 32 GB and up) and not commodity hardware (4 core, 16 GB), determine if the same hardware configuration should be kept for each server or if there is a cost saving opportunity by moving to commodity hardware when moving to a Cherwell server farm. If you decide to move to less expensive hardware, there is no exact equation for how many servers are needed, but keep the following in mind: load-balanced servers are typically CPU heavy, so the CPU is the first and most important factor in the multiplier.

- We recommend no more than 12 active nodes, but increase the size of each node once you exceed 10 nodes. For example, increase each node from eight cores instead of four. For optimal performance, do not exceed 36 cores on each node.

- **CPU**:
  One CPU core per 50 concurrent users; minimum of two to start.

  This ratio may be higher or lower, depending on the content in the system and how that content is used.

- **Memory**:
  50 MB of memory per session for the Cherwell Application Server and web server machines.

- **Storage**:
  500 MB of storage per license per year.

- **Configuration**:
  The Windows IIS features HTTP Activations and Non-HTTP Activations must be installed. See Configure IIS for CSM.

  Machine keys must be generated in IIS on one CSM server and copied to IIS on all CSM servers in the Cherwell server farm. See Configuring Server Farms in IIS.

Redis Guidelines

CSM is compatible with Redis Labs Enterprise Cluster (RLEC). Use RLEC to configure Redis environments. See the System Requirements for supported versions.

You can run Redis in a single-server or clustered environment. Redis Cluster provides the ability to:

- Automatically shard (split) your dataset among multiple nodes.
- Continue operations when a subset of the nodes are experiencing failures or are unable to communicate with the rest of the cluster.

Guidelines for a Master/Replica Setup

- Use a single-server Redis scenario for systems with up to 1,300 users.
- A machine or virtual machine should be dedicated to Redis.
- The dedicated machine should have exactly two CPUs: one is used by the system and is mostly idle; the other CPU is used by Redis. Allocating three CPUs does not hurt Redis, but the third CPU will never be used.

Guidelines for a Redis Cluster Setup

- The threshold for determining when you need a Redis Cluster is between 1,300 and 1,800 concurrent users.
- To gauge how much memory you will need per user, divide the total memory needed by the clusters. For example, if you need a total 12 GB of RAM for Redis, use three 4 GB Redis clusters.
- Redix 5.x or later is required for using Redis Cluster with CSM.
- To learn more, see the Redis Cluster documentation.

Guidelines for All Redis Configurations:

- **CPU**:
  CPU speed is not a crucial factor. The Redis server CPU remains dormant most of the time and it takes a lot of traffic to increase the CPU to a heavy load. By the time the CPU is getting fatigued, the network connection might already be the bottleneck.

- **Memory:**
  10 MB of memory usage per technician/Browser Client user session and 5 MB for each CSM Portal user session. For example: 1,000 concurrent Browser Client users x 10 MB/user = 10 GB of RAM per server.

  Redis is used as a centralized in-memory database. Everything stored in Redis is kept in RAM. There should be enough RAM to serve concurrent users. Dedicate 10 MB of memory per session for Redis Servers; 2 CPU cores per server.

  When Redis is hosted on a virtual machine, it is critical that memory is never oversubscribed.

- **Miscellaneous**:

For high availability, you need a minimum of two Redis processes and three sentinel processes. The sentinel processes to not need to run on their own server; they can run with Redis or on the web servers used by CSM.

Sticky sessions or other methods of load balancing where Redis is not deployed are not supported.

See these sections for additional guidance:

- Redis Sizing Guidelines
- Redis Configuration

Load Balancer Requirements

Non-load-balanced CSM web servers are memory intensive, but load-balanced servers free up memory as soon as a request is ended.

- You can use most load balancers and load balancing methods with CSM.
- Cherwell does not recommend using IIS ARR for a load balancer in a production environment.

Microsoft SQL Server Guidelines

The database server size (CPU and memory) primarily depends on CSM content configuration and use. Server size does not scale directly with the number of concurrent users unless they are doing almost exactly the same work.

Network Guidelines

- **Traffic between each web server and Redis**: Redis must be deployed in a high-speed, low-latency, directly connected environment. This is typically a 10 GbE network (dedicated is best), but this number is highly dependent on your content. Each page on the browser might turn into multiple web requests, depending on the page content.
  In general, if server farms are deployed, the network interface to the Redis server can require very high bandwidth. If possible, utilize dedicated network connections for Redis traffic to and from server farm servers.
- **Traffic between the CSM web applications and the web server**: This is highly dependent on your content and outside the scope of this document. Bottlenecks are related to the volume of traffic between the Cherwell web servers.
  Network traffic between browser and server is not affected by a server farm configuration, and therefore is not considered in this document, but evaluate if the network is prepared to support the traffic.

Tested Redis Configurations

CSM has been tested with Redis in the following environments:

- Windows with a single instance.
- Linux master/replica with sentinel.

- Windows master/replica with a sentinel.
  When configuring a cluster environment in Cherwell Server Managers, users only need to provide one IP for the cluster. In master/replica environment, add the IPs of the master and all replicas in the Connect to field when configuring.

- Redis Labs Enterprise Cluster.
  When configuring a RedisLab Enterprise Cluster environment in Cherwell Server Managers, users only need to provide one IP for RLEC. In master/replica environment, add the IPs of the master and all replicas in the Connect to field when configuring.

Related concepts

Scaling the CSM Web Applications

Web Applications Installation Options

Server Installation Options

Scaling Scenarios

Implementing a Cherwell Server Farm

Several implementation steps are required on your network and in CSM.

Some key points:

- Ensure the CSM configuration is the same across servers.
- A server farm can only be used when the Cherwell Application Server is hosted in IIS. HTTPS and REST are required for the Application Server.
- Performance can be slightly impacted when a server farm is enabled because it adds overhead to the individual servers participating in the farm.

For additional requirements, see Server Farm Resource Recommendations.

Single-server Setup Steps for Testing

Before you implement a server farm, first set up a single-server farm for testing and sizing purposes. The single-server configuration ensures that Redis is configured correctly and measures how much memory the Redis Servers need. Once you confirm that the single-server farm is configured correctly, you can add additional servers.

To set up a single-server farm:

1. Prepare a supported version of Redis Server or Redis Labs Enterprise Cluster (RLEC). See the System Requirements and the Redis documentation.
2. Install the Cherwell Application Server and CSM Web Server on a single machine.
3. In the Cherwell Server Manager, enable server farm features and connect to Redis. For more information, see Configure Server Farms in Cherwell Server Manager.
4. Do not set up a load balancer. At this point you have a single server that behaves as if it is part of a farm. Open the CSM Portal and Browser Client to see the data being stored in Redis.

Production Configuration Steps

Implementation Task	Task Location
1. Verify that your organization has a load balancer.	Your network.
2. Prepare a supported version of Redis Server or Redis Labs Enterprise Cluster (RLEC). See the System Requirements and the Redis documentation.	Your network.
3. Configure a Cherwell server farm for one CSM server in the farm. See Configure Server Farms in Cherwell Server Manager.	Cherwell Server Manager on a CSM server.
4. Configure server farms in Internet Information Systems (IIS). See Configuring Server Farms in IIS.	IIS for all CSM servers in a Cherwell server farm

Implementation Task	Task Location
5. Configure HTTP headers. See Configuring HTTP Headers for Load Balancers, Web Application Firewalls, and Reverse Proxies.	Load balancers, firewalls, and reverse proxies.

Related concepts

Scaling the CSM Web Applications

Scaling Scenarios

Related tasks

Configure Server Farms in Cherwell Server Manager
Configuring Server Farms in IIS
Configuring a Cluster for Cherwell Message Queue Service

Configure Server Farms in Cherwell Server Manager

There are several ways to configure a server farm. Changes you make in Cherwell Server Manager will be saved in Overwatch, which will propagate the updates to all the servers in your server farm.

To configure a Cherwell server farm:

1. On a CSM server, select **Start > All Programs > Cherwell Service Management > Tools > Server Manager**.
2. Select the **Configure** button located next to the **Server farm mode** label.
   A window opens warning you to stop the server farm before changing settings.
3. Select **Yes**.
4. Select the **Enable server farm mode** check box.
5. Define **New Redis Server** options:
   - In the **Host** box, provide the IP address for the Redis server.
   - Use the up and down arrows to select the **Port**.
   - Select**Add**.

   The IP address and Port appear in the **Connect to** list. Repeat this step to add all Redis servers.
6. Provide the password for the Redis server. If there are multiple servers in a master/replica configuration, ensure all servers share the same password.
7. Use the **Connection Timeout** setting to specify the number of seconds the system will wait for a connect operation to complete before returning a timeout message. On startup, the system evaluates the list of connections in the order they appear in the **Connect to** list, and then attempts to connect to the first available master. The **Connection Timeout** setting determines how long the system will wait for each Redis endpoint to connect before returning a timeout.
8. Use the **Sync Timeout** setting to specify the number of seconds the system will wait for a Synchronous operation to complete before returning a timeout.
   If you have a master/replica with sentinel configuration and a replica becomes a master, the **Sync Timeout** setting determines how many seconds will elapse before your application switches to the new master.
9. Select **OK**.

Related concepts
Implementing a Cherwell Server Farm
Scaling the CSM Web Applications
Scaling Scenarios
Related tasks
Configuring Server Farms in IIS
Configuring a Cluster for Cherwell Message Queue Service

Configuring Server Farms in IIS

You must create and apply a machine key that is applied to Internet Information Services (IIS) for all CSM servers in a Cherwell server farm. The key you apply must be identical across all CSM servers.

To generate machine keys:

1. Choose one server to create validation and encryption machine keys that can be added to IIS on all other instances of CSM.
2. Open IIS on the server.
3. Determine at which level the keys should be generated:
   ◦ If IIS hosts only CSM sites on all servers included in the server farm, you can create your keys for the IIS instance by selecting the top-level server name.
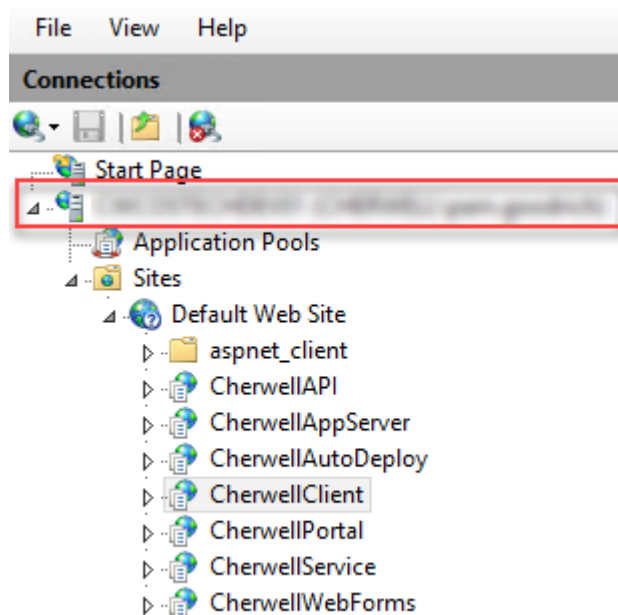
   ◦ If other sites are hosted on any of the servers in the server farm, generate keys at a CSM site level, such as CherwellClient.
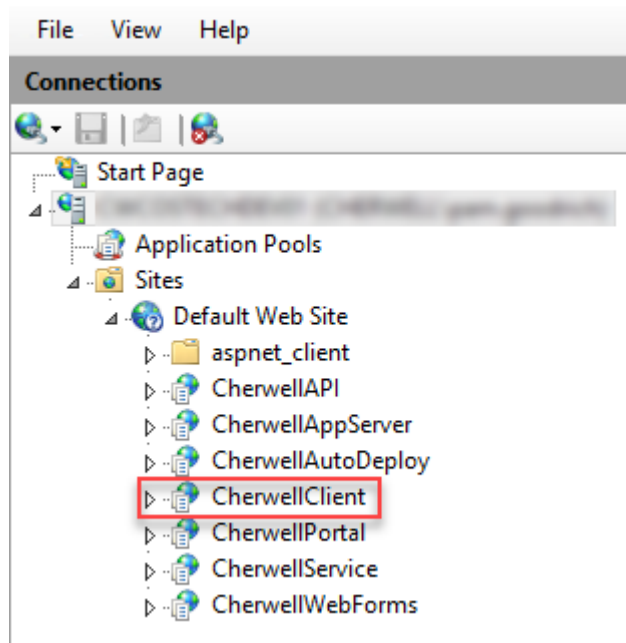
- ◦ Select the level, and then double-click the **Machine Key** icon.
4. Choose a validation method (example: AES).
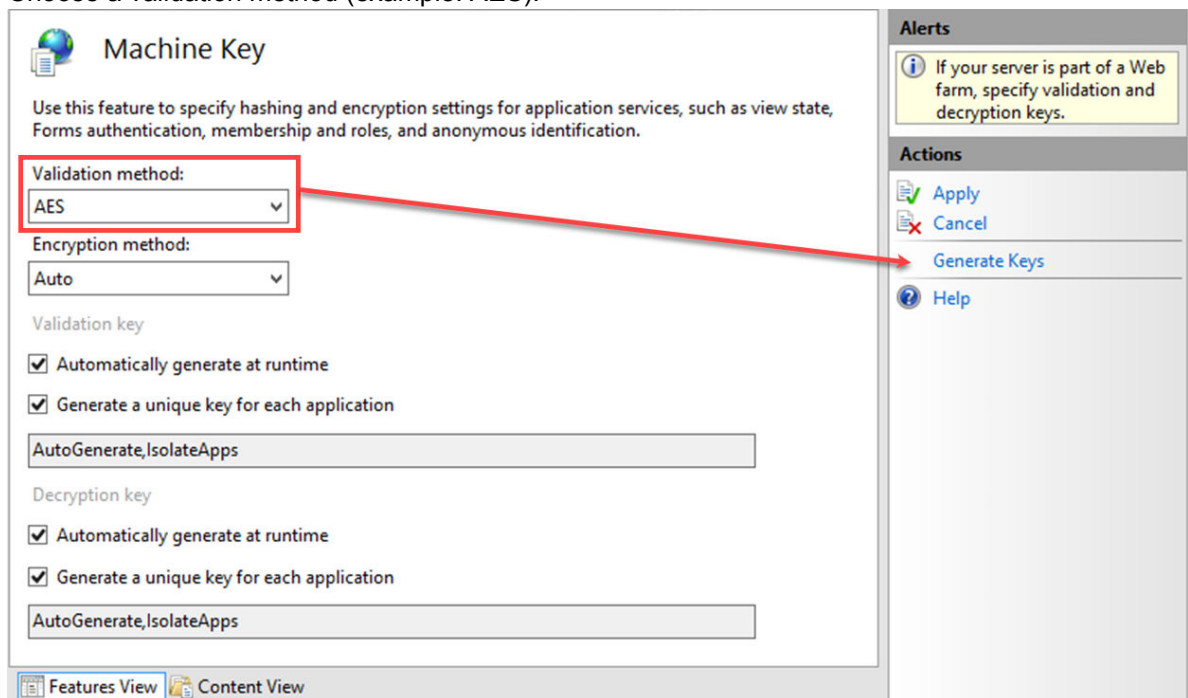
5. Select the **Generate Keys** link located in the Actions area.

6. Copy the Validation Key and Decryption Key to an external location for easy access.

7. Select **Apply**.

8. If you generated keys at the site level, such as CherwellClient, apply the saved keys to all other Cherwell sites on this IIS instance.

9. Restart IIS.

You must apply the machine keys generated in the previous section to IIS on all CSM servers in your server farm. The keys must be the same.

The keys should be applied at the same level: server or site.

IIS or the Application Pool must be restarted on each server after you apply machine keys.

Related concepts
Scaling the CSM Web Applications
Related tasks
Configure Server Farms in Cherwell Server Manager

Configuring a Cluster for Cherwell Message Queue Service

Use a RabbitMQ cluster to handle large service loads for a Cherwell server farm. This scenario should only be used for systems where the impact on CSM services, such as the Automation Process Service, is heavy on an ongoing basis.

For more information about using a cluster with the Cherwell Message Queue Service, see Scaling Scenarios.

For guidance on using clusters with RabbitMQ, which powers the Cherwell Message Queue Service, see the RabbitMQ Clustering Guide.

To configure a cluster for the Cherwell Message Queue Service:

1. Run the CSM server installer on each machine that will host an instance of the Cherwell Message Queue Service.
2. Verify that each instance can be contacted by a host name rather than an IP address.
3. Select one Cherwell Message Queue Service instance that will serve as the main node that others will connect to.
4. Run the rabbitmqctl.bat cluster_status command to verify that each node resolves to the correct hostname. If they do not, uninstall the Cherwell Server, including RabbitMQ and Erlang, rename the machine, and then reinstall.
5. On the server that you chose as the main node, copy the erlang.cookie.file located here: C:\windows\system32\config\systemprofile and possibly C:\Users\Administrator.
6. Paste the erlang.cookie.file file to the same two locations on the other cluster nodes, and then restart the Cherwell Message Queue Service on each machine.
7. Reset the RabbitMQ node on each instance so it can join the cluster.
   a. On each server, navigate to the RabbitMQ installation folder, which is typically C:\Program Files\Cherwell Service Management\CMQS\rabbitmq_server-3.7.14\sbin).
   b. Open a command prompt, and run:
      - rabbitmqctl.bat stop_app
      - rabbitmqctl.bat reset
      - rabbitmqctl.bat join_cluster <master rabbit node>
      - Rabbitmqctl.bat start_app
8. Open the RabbitMQ management interface and verify the nodes are available in the cluster. See Monitor Queues from the RabbitMQ Management Interface.

To remove a node from a cluster, run .\rabbitmqctl -n rabbit@MAIN-NODE-NAME forget_cluster_node rabbit@NODE-NAME.

Related concepts

Scaling the CSM Web Applications

Scaling Scenarios

Recommended Cherwell Service Host Scaling Configurations

Configuring HTTP Headers for Load Balancers, Web Application Firewalls, and Reverse Proxies

Certain functionality in the CSM Browser Client, CSM Portal, and Cherwell REST API requires knowledge of a user's fully qualified domain name (FQDN).

In the initial request, this information is provided by the "Host:" header, but web application firewalls (WAFs), load balancers, and reverse proxies typically overwrite the value of this header as they pass the request through to the web server that will ultimately service the request (upstream server).

CSM looks for two groups of headers to determine the original connection's host (FQDN) and protocol/ scheme (HTTP vs. HTTPS) respectively. These follow current web standards, some of which are set by default on some of the more common WAFs and load balancers.

Connection's Host

- X-Forwarded-Host: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Forwarded-Host
- Host: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Host

Connection's Protocol/Scheme

- Forwarded: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Forwarded (note that CSM only evaluates the "proto=" part of this header's value, if present)
- X-Forwarded-Proto: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Forwarded-Proto

If multiple headers are present, CSM will look for the first one present, starting at the top of the lists above (that is, "X-Forwarded-Host" takes precedence over "Host").

Alternate option: Some WAFs, load balancers, and reverse proxies allow system administrators to configure the value used for the "Host:" header sent to the upstream server. This can work, but is not recommended.

> **Note:** We include reference to reverse proxies due to certain similarities to WAFs and load balancers. However, we recommend using a load balancer for server farms and an optional WAF; a reverse proxy is not required by CSM and is typically unnecessary and discouraged. Forward proxies are not supported.

Related concepts
Scaling the CSM Web Applications

Advanced Redis Information

Redis is a fast, in-memory, caching mechanism that allows Cherwell to quickly exchange data between servers.

Cherwell stores temporary, volatile data into Redis so that each server can pick up where other servers have left off. Redis runs very well on commodity hardware and does not need any hard-drive space because it stores everything in-memory. Redis is an open source database that can run both on Windows and Linux. Download it here.

> **Note:** In earlier versions of Redis, master/slave terminology was used. In later versions of Redis, slave was changed to replica. This documentation uses master/replica terminology for all Redis versions.

Redis is used to share two types of data:

- **User session data:** Describes the state of the current logged in User. There is an entry in Redis for each of the active sessions on the web. No sensitive data (password or encrypted fields) are stored in Redis. Session data is only stored transiently as Users go from one request to another. All session information is deleted on session expiration, and all information is deleted if Redis is turned off.
- **Common application data needed for the application server to work:** Application data is stored in Redis for the entire time that the application is running.

Redis Labs Enterprise Cluster

CSM is compatible with Redis Labs Enterprise Cluster (RLEC), the enterprise offering that allows you to simplify your Redis management. In a RLEC environment, many implementation details are simplified. For example, RLEC eliminates the need to manually edit configuration files, manually set up a master/replica environment, or determine how many sentinels you need.

While the documentation in this section is primarily intended written for users who do not use RLEC, it is beneficial for you to understand the underlying technology and the options described in our documentation so you can make decisions appropriate to your specific environment.

If you are using RLEC, we recommend you become familiar with the concepts expressed in the documentation, as they apply in both scenarios. For the few places where RLEC deserves specific considerations, you will see RLEC notes accompanying the documentation.

Related concepts
Scaling the CSM Web Applications
Purpose of Redis
Using a Load Balancer with CSM

Redis Sizing Guidelines

Redis stores two types of data: application state and user state.

Application state typically can take up a few MB and is not a factor when making sizing considerations. Session state grows linearly with the number of concurrent users in your system. Since Redis stores session data for the duration of active sessions, if you have session duration set to 90 minutes, at any given point in time, Redis stores session for any user with activity in the last 90 minutes.

As a best practice, calculate how much Redis memory you need by figuring out the maximum number of users in any time window equivalent to a session duration, and then multiply it by 10 MB. That covers in the majority of the cases. If this proves to be insufficient, proceed with the process below in order to measure actual memory consumption

The size needed for each system can vary depending on your content and the particular page and activity users are performing. Measure your own specific load to estimate the sizing numbers. Use the measurements below to calculate what kind of Redis memory your Cherwell server farm requires, and, if necessary, increase the memory of your server.

To measure sizing numbers:

1. For the purposes of sizing Redis, set up a farm with a single server.
2. Load into the system 10 users, and then measure the load in Redis.
3. Load into the system 20 users, and then measure the load in Redis.
4. Load into the system 100 users, and then measure the load in Redis.

With the data points, compute the average Redis load per user expressed in KB. Multiply that number by the peak (or total) number of users.

Retrieving the Size of Redis Memory

When Redis is installed, you can open a client window and send Redis commands. One of those commands is INFO, which shows the current memory size occupied by the Redis database. The sample output of the command shows the peak usage of Redis. This is the number needed to calculate how much memory each user needs.

```
lru_clock:1854465
used_cpu_sys:59.86
used_cpu_user:73.02
used_cpu_sys_children:0.15
used_cpu_user_children:0.11
connected_clients:1
connected_slaves:0
client_longest_output_list:0
client_biggest_input_buf:0
blocked_clients:0
used_memory:1329424
used_memory_human:1.27M
used_memory_rss:2285568
used_memory_peak:1595680
used_memory_peak_human:1.52M
mem_fragmentation_ratio:1.72
mem_allocator:libc
loading:0
aof_enabled:0
changes_since_last_save:0
bgsave_in_progress:0
last_save_time:1360719404
bgrewriteaof_in_progress:0
total_connections_received:221
total_commands_processed:29926
expired_keys:2
evicted_keys:0
```

Related concepts

Advanced Redis Information

Purpose of Redis

Using a Load Balancer with CSM

Redis Configuration

Redis can be configured in multiple ways. Cherwell recommendations are based on testing results for working optimally with a general configuration of CSM.

This section offers suggestions on how to setup an ideal CSM environment, including high availability considerations that add resiliency to a Redis database.

Settings

Redis is a simple application that requires an executable to be present and running on a given machine. On the startup.exe, Redis reads a flat .config file that contains a number of value pairs to establish the different available settings. Some settings will be specific to your environment, but others directly impact CSM.

Common Settings

All Redis instances should be configured to NOT save any data to disk by commenting out the SAVE directive in the default config file. Commenting is done by adding a # in front of it. Use the password directive in the default file to set the password so communication with Redis only happens with processes that know the password.

Optional Settings

Depending on the environment, if you want to provide high availability, you need to configure sentinels, masters, and replicas. If the Redis memory demand exceeds what is provided on a single server, configure Redis with clustering. Using a cluster configuration provides three main benefits:

- Shares large memory cache across many servers.
- Provides high availability.
- Distributes the CPU load across multiple CPUs (Redis is a single CPU process).

For more information on Redis clusters, refer to the Redis Cluster Specification.

> **Note:** Clustering is only supported when CSM is using specific versions of Redis. See the System Requirements for details.

Connections

Run Redis in standalone, master/replica, or cluster mode. Ideally, the minimum configuration is master/replica with sentinels.

Sentinels

A sentinel is a component of Redis that keeps an eye on both the master and the replica. It identifies when the master goes down and immediately promotes the replica as the master. Ideally the minimal configuration has two sentinels, one for master and one for replica. When the sentinel switches the master, CSM switches as well if both are listed in Connect to field on the Server Manager.

For more information on Redis sentinels, refer to Redis Sentinel Documentation.

Master/Replica

This configuration is only required if operating Redis as a high availability service. If an organization wants to horizontally scale Cherwell services, only one Redis server is required.

A master/replica connection has one copy of the master data kept in a replica. The replica and master both must be configured via the Server Manager, including both IPs and both ports with the same password. If there is a cluster of Redis, add the IP of the cluster in Host field on the Server Manager. If master and replica copy each other, one is always master and one is replica. If the master goes down, the replica does not know unless there is a sentinel. If the master goes down, it becomes the replica when it comes up again. CSM does not need to know who is master and who is replica, just the nodes for Redis in the chain.

For more information, see the Redis Replication documentation.

Backup vs. Replica

Redis, by default, is setup to backup information to disk every second, but it causes slowdowns. When Redis is installed, the configuration file has a save directive with parameters. Turn off the save to disk by deleting the directive or commenting it out. Use a master/replica configuration to provide backup functionality. There are some points to remember:

- If all of Redis goes down and the customer does not have the save to disk feature, then everyone will be logged off and can log on again when it comes up.

- If all of Redis goes down and the customer does not have save to disk feature, then there is no way to predict how the server farm will behave because it fails and IIS shut down. This is why the save directive is not recommended.

Related concepts

Advanced Redis Information

Purpose of Redis

Using a Load Balancer with CSM

Redis Q&A

Question: What if my Redis Server goes down? Is that a single point of failure?

Answer: Yes. Fortunately, you can set up Redis with high availability, see Redis Configuration.

Question: How often does Redis fail?

Answer: Cherwell tests have not experienced an unstable Redis. Failures are usually due to hardware problems, with the following exceptions:

- If enough memory is not allocated to the Redis process. When Redis starts requesting more memory than the system can allocate, it fails.
- If too much memory is pre-allocated to Redis, and the OS does not have any memory left for itself.

Question: How many sentinels should I install, and where?

Answer: A common approach is to install a sentinel for each Redis Server running. For example, if there are one master and two replicas, then have three sentinels.

Question: How does a sentinel work?

Answer: A sentinel pings the master server at regular intervals, and if it does not receive an answer within a certain amount of time (configurable in the settings), it evaluates the possibility of promoting a replica to master. A single sentinel does not necessarily have the authority to switch a master to a replica, because there might be other sentinels that disagree with it. For the master to actually be swapped with a replica, a minimum number of sentinels (configurable) called quorum, need to agree that the master is down. That means that based on your particular setup, you might have to change the default quorum number, as well as the master timeout interval.

Question: Can Redis Servers be deployed in multiple geographic locations?

Answer: No, all Redis Servers should be together on the same LAN as the application servers in the Cherwell server farm due to latency sensitivity.

Question: What is the minimum line speed and latency required for Redis?

Answer: At least 1 GbE with latencies below 3 milliseconds between the Redis Servers and the application servers. Today's Enterprise networks are usually 10 GbE or better, which is more desirable.

Related concepts

Advanced Redis Information
Purpose of Redis
Using a Load Balancer with CSM

Cherwell Server Farms Q&A

Question: Could I take one physical box, divide it into two virtual machines, and install CSM services on them as two different participants of the server farm?

Answer: Yes, but we do not recommend it. One of the purposes of the farm is to eliminate having a single point of failure. If the hardware below the two virtual machines fails, the entire farm goes down, making the purpose of the farm useless. Having the two virtual machines reside on different hardware is a better option.

Question: Can I mix and match server types on a single box?

Answer: Yes. You would have to make some performance and high availability considerations to determine which servers can reside together.

Question: How do I know if I have to separate my servers onto multiple machines with a dedicated machine, or if I can share a machine across multiple Cherwell servers?

Answer: Depending on the size of the machine and the performance load, you might find that a shared machine is not enough.

Question: How many servers in a Cherwell server farm should be deployed to match the performance of a single standalone server, and why?

Answer: Three load-balanced servers should be deployed to match the performance of a single standalone server in the event that one of them fails. This is because of the overhead associated with the Cherwell server farm topology. CSM clients in the load-balanced environment can appear slightly slower because of session state serialization and Redis traffic.

Question: What are the bandwidth and latency requirements for the Cherwell server farm?

Answer: Network interfaces should provide high bandwidth and very low latency. For example, 10GbE interconnects to high capacity hardware-switched aggregators that provide near 100 percent wireline throughput bi-directionally with no backplane over-subscription and nanosecond latency performance.

Process Servers

Question: Can CSM services (Automation Processes, E-mail and Event Monitoring, Mail Delivery, and Scheduling) be load-balanced?

Answer: CSM services use a centralized queue to enable the distribution of workload. For more information, see Scaling the Cherwell Service Host .

Question: Can these non-load-balanced services be set up for high availability?

Answer: Yes, using Windows Server Fail-over Clustering with the Generic Service or VM Clustering.

SQL Server

Question: What type of cluster model does Cherwell recommend for SQL Server?

Answer: Always-On Availability Groups.

Question: What is the formula for determining the total amount of disk storage needed?

Answer: A starting best practice is to allocate 600 MB of storage per licensed user per year. If routinely saving large attachments to records, this formula should be doubled.

Question: When using SANs to store SQL data, are there any special considerations?

Answer: Yes. Differentiate networks between SAN traffic and other traffic, such as communications between applications servers, SQL, and Redis. Storage for SQL data should be on different spindles than other data.

Question: Does SQL Server have to be set up on a dedicated, physical machine?

Answer: We highly recommend that SQL Server run on dedicated hardware or on virtual machines with dedicated CPU cores, memory, and dedicated physical storage. It was Microsoft's position to say "never run SQL Server on a virtual machine". SQL is optimized in how it accesses memory and deals with the file system. Microsoft has backed away from this firm stance, although it still recommends running SQL on physical, dedicated machines. If SQL is run on a virtual machine, memory and CPUs CANNOT be oversubscribed. It is still recommended that SQL hit physical disks (or NAS) and not a virtual file system. Dedicated is best. If you give SQL 'X' amount of memory and another process on that machine suddenly takes the memory away, it drastically affects SQL's performance.

Question: Does SQL Server need to be set up on the same LAN as the application and process servers?

Answer: Not required, but highly recommended. High throughput and low latency is the goal for best performance.

Question: Should SQL Server files be distributed across separate disks?

Answer: Yes. For example, separate data, logs, temp, and database files.

Load Balancer

Question: Can software-based load balancers be used for Cherwell's server farm solution?

Answer: Yes, as long as they are set up properly. IIS ARR is an example of a software load balancer solution, although we do not recommend it. To use it, ensure that all of its response-caching features are disabled.

Question: What are the key performance indicators of a load balancer?

Answer: Maximum throughput, SSL throughput, SSL transaction per second (TPS) based on key size - typically 2048 - HTTP requests per second.

Question: For health monitoring, which application may be monitored to indicate server online state?

Answer: /CherwellService application pool is a good candidate for this; others can be used.

Related concepts
Scaling the CSM Web Applications
Scaling Scenarios
Implementing a Cherwell Server Farm

Trusted Agent

Trusted Agent offers cross-network access between CSM servers and other private resources, such as LDAP directories, mail servers, and relational databases. An enabled Trusted Agent connects to CSM servers using firewall friendly protocols. The CSM servers then call the Trusted Agent to perform operations on their behalf.

For example, Trusted Agent:

- Provides CSM SaaS customers secure access between resources on their private network and the Cherwell data center.
- Enables secure access to private resources across networks in your organization.
- Enables secure access between a Cherwell partner's CSM network and private resources on your network.

The following diagram provides an example of one possible Trusted Agent configuration. While other deployment architectures are possible, this diagram provides a simple visual representation of the relationship between the components.
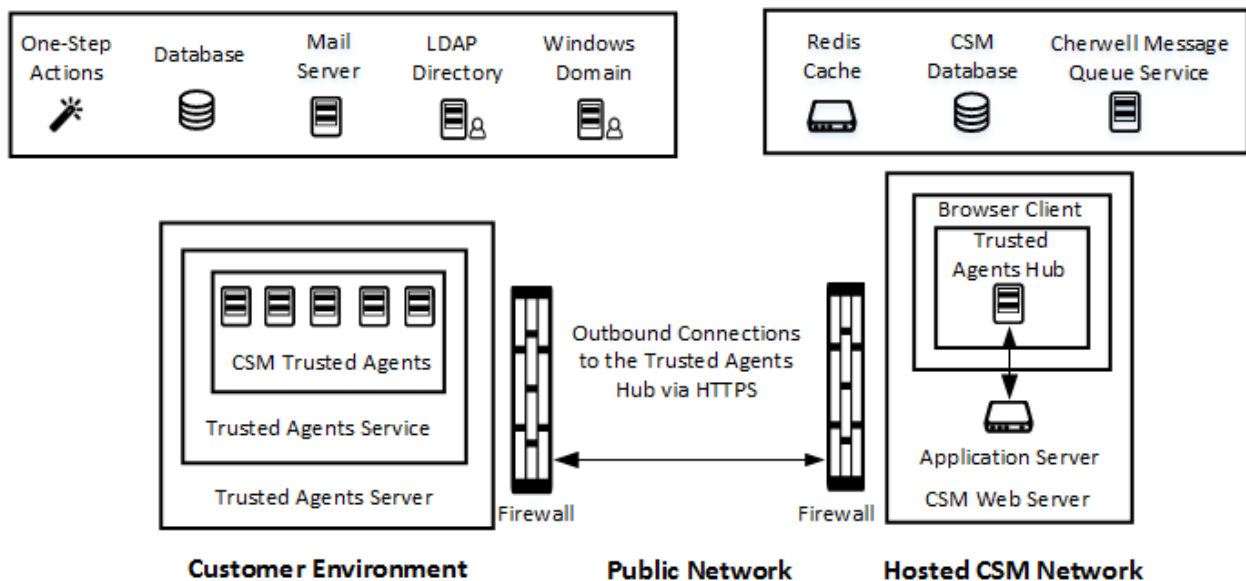
Features That Can Use Trusted Agent

Trusted Agent supports integration with several different kinds of private resources. The table below summarizes these supported types of resources and the CSM operations that can be performed with each. You can create service groups to control which private resources use Trusted Agent and to route requests to each service group. For more information, see Trusted Agent.

Private Resource Type	CSM Operations
Email	All email operations within CSM.
LDAP Directory	LDAP Authentication. LDAP-mapped user import. LDAP-mapped Business Object import.
One-Step Actions	The following Action types: • Print • Run a Program • Run a Report • Write to a File • Transfer Attachments • Call a Web Service • Excel Merge
External databases (relational database)	Bulk import of mapped Business Objects. **Note:** Linked data imports are not supported at this time.
Windows Domain	Windows Authentication.

Related concepts

Configuring Trusted Agent

Configuring Trusted Agent Features

Trusted Agent Logging

Troubleshoot Trusted Agent

Trusted Agent Components

Understanding the components that participate in Trusted Agent scenarios is key to a successful cross-network implementation.

Component	Definition
Private CSM Network	The network in which CSM servers are running. For SaaS customers, this is the Cherwell data center. This network is separate from the network in which one or more private resources reside, so Trusted Agent is required to communicate with those private resources.
Private Customer Network	A network that contains one or more private resources, such as an LDAP directory and/or a relational database, that need to be accessed by CSM but which are separated from CSM by one or more network security boundaries.
Private Resource	A server, service, or data source that is not directly accessible to CSM servers because of one or more network security boundaries. A typical scenario is to have one or more private resources within a private customer network while CSM is hosted outside of the customer network.
Redis Cache	A Redis database used to enable scale-out of Trusted Agent Hubs.
Trusted Agent	A software component that acts as a proxy for communication between a Trusted Agent Hub and one or more private resources of a given type. Each Trusted Agent can handle communication with one type of private resource, but it can handle communication with more than one instance of that private resource type. For example, a Trusted Agent for external data can connect to any number of databases as long as those databases are accessible to the Trusted Agent. Similarly, a Trusted Agent for LDAP can connect to any number of LDAP directories as long as those directories are accessible to the Trusted Agent. Each Trusted Agent is hosted within a Trusted Agent Service.
Trusted Agent Hub	A CSM software component that runs within a CSM Browser Client web application and acts as the central point of communication for all Trusted Agent interactions. Trusted Agents connect to a Trusted Agent Hub at startup, and CSM servers communicate to Trusted Agents by sending requests to the Trusted Agent Hub, which selects the Trusted Agent to receive each request. Trusted Agent Hubs may be scaled out using Redis just as CSM Browser Client can be scaled out. For SaaS customers, the Trusted Agent Hub is hosted in the Cherwell data center.
Trusted Agent Service Group	A configurable set of Trusted Agent Services that can be created in CSM Administrator and selected when configuring Trusted Agent usage for CSM features. Trusted Agent Groups are used to route requests to only specific Trusted Agent Services. If no groups are configured, all Trusted Agent Services are assumed to be capable of performing all Trusted Agent operations.

Component	Definition
Trusted Agent Server	The physical or virtual machine that hosts a Trusted Agent Service and is collocated on a private network with the private resources that should be accessible to CSM servers. A Trusted Agent Server can host only one Trusted Agent Service, but multiple Trusted Agent Servers can be used to support request routing and fault tolerance. For SaaS customers, the Trusted Agent Server is hosted in the servers in the customer's domain.
Trusted Agent Service	A Windows service that hosts Trusted Agents. Each Trusted Agent Service hosts one Trusted Agent for each feature supported by CSM, for a total of five: external databases, LDAP authentication, Windows Domains, email, and One-Step Actions.

Related concepts

Trusted Agent Server Technical Architecture

Configuring Trusted Agent

Related tasks

Using Trusted Agent Server with LDAP

Use Trusted Agent Server with Windows Domains

Import External Data Using Trusted Agent

Using Trusted Agent with Email

Configuring Trusted Agent

Trusted Agent configuration requires steps on two networks and potentially multiple servers.

Good to Know:

- You need separate Trusted Agent Hubs and shared keys for each CSM environment (development, test, and production, for example).
- Each Trusted Agent Server makes one connection to each LDAP or Active Directory server. If you have multiple domains, you must install a Trusted Agent Server on each domain, but each server can connect to the same Trusted Agent Hub for its environment.
- For server and operating system requirements, refer to the CSM System Requirements.
- When you upgrade CSM, you must also upgrade all Trusted Agent Servers.

Process for SaaS Customers

To facilitate communications between CSM and your private resources, Cherwell configures the Trusted Agent Hub on Cherwell servers. You install and configure one or more Trusted Agent Servers on your network.

Configuration Task	Task Location
1. Request a Trusted Agent Hub from Cherwell.	Cherwell data center.
2. Install the Trusted Agent Server. See Trusted Agent.	A server on the same network as your private resource.
3. Configure the Trusted Agent Server. See Trusted Agent.	The same server where you installed the Trusted Agent Server on the same network as your private resource.
4. Grant Security rights to control access to Trusted Agent configuration options in CSM Administrator. See Tools Security Rights.	From CSM Administrator.

Configuration Task	Task Location
5. Connect to the Trusted Agent Hub from CSM Administrator. This step is required if you intend to use features that require configuration in CSM Administrator. These features include: • Importing external data using Trusted Agent • Scaling Trusted Agent for request routing • Importing Directory Service data Into Business Objects • Using email • Executing One-Step Actions on a remote network See Trusted Agent.	From CSM Administrator.
6. Create Trusted Agent Service groups. This step is required if you want to route requests to only specific Trusted Agent Services. See Trusted Agent.	From CSM Administrator.

Process for On-premises Customers

On-premises customers configure all Trusted Agent components.

Configuration Task	Task Location
1. Enable the Trusted Agent Hub. See Trusted Agent.	On the server that runs the CSM Browser Client web application. If you are using server farms, this task must be performed on each server.
2. Install the Trusted Agent Server. See Trusted Agent.	A server on the same network as your private resource.
3. Configure the Trusted Agent Server. See Trusted Agent.	The same server where you installed the Trusted Agent Server on the same network as your private resource.
4. Grant Security rights to control access to Trusted Agent configuration options in CSM Administrator. See Tools Security Rights.	From CSM Administrator.

Configuration Task	Task Location
5. Connect to the Trusted Agent Hub from CSM Administrator. This step is required if you intend to use features that require configuration in CSM Administrator. These features include: • Importing external data using Trusted Agent • Scaling Trusted Agent for request routing • Importing Directory Service data Into Business Objects • Using email • Executing One-Step Actions on a remote network See Trusted Agent.	From CSM Administrator.
6. Create Trusted Agent Service groups. This step is required if you want to route requests to only specific Trusted Agent Services. See Trusted Agent.	FromCSM Administrator.

Related concepts
Tools Security Rights
Related tasks
Install the Trusted Agent Server
Configure the Trusted Agent Hub in the Server Manager
Configure the Trusted Agent Server
Connect to the Trusted Agent Hub from CSM Administrator
Configure Trusted Agent Service Groups

Configure the Trusted Agent Hub in the Server Manager

The Trusted Agent Hub is configured in the Cherwell Server Manager on the same machine running the CSM Browser Client. If you are using a server farm, you must install the Trusted Agent Hub on each server.

Cherwell performs this task for SaaS customers.

To configure the Trusted Agent Hub:

1. On the machine running the CSM Browser Client, go to **Start>All Programs>Cherwell Service Management>Tools>Server Manager** to open the Cherwell Server Manager.
2. Select the **Configure** button next to **Trusted Agents usage**.
3. On the **Trusted Agent Hub Configuration** dialog, select the **Enable Trusted Agents** check box.
4. In the **Hub URL** box, provide the address that is used to connect to the Hub from other Cherwell servers and services. This is typically the same URL that is used to access the CSM Browser Client (https://server name/CherwellClient).
5. In the **Shared Key** box, provide the key that will be used in each Trusted Agent Server configuration. This key is used to ensure that only properly configured Trusted Agent are permitted to connect to the Hub. Each CSM system should have a unique Shared Key.
6. Select **Generate Key** to generate a secure shared key. You can create your own Shared Key, but the key generation tool provides a simple way to generate a unique key.
7. Select **Test** to verify connection information.
8. Set timeout settings:

Option	Description
Agent Operation Timeout	Specify the amount of time the Trusted Agent Hub waits for an operation to complete, send data back, or how long an operation takes to send a progress update before timing out. The default setting is 30 seconds. **Note:** Use -1 to disable timeouts.

Option	Description
Agent Registration Timeout	Specify the amount of time the Trusted Agent Hub waits for a ping from the Trusted Agent before it assumes the Trusted Agent is down. The default setting is 180 seconds. **Note:** This setting should never be lower than the **Hub Ping Frequency** set for each Trusted Agent Server. The default for the Hub Ping Frequency is 20 seconds.

9. Select **OK**.
10. Restart all Cherwell services and Internet Information Services (IIS).

Related concepts
Configuring Trusted Agent
Using the Server Manager
Related tasks
Install the Trusted Agent Server
Configure the Trusted Agent Server
Connect to the Trusted Agent Hub from CSM Administrator
Configure Trusted Agent Service Groups

Install the Trusted Agent Server

The Trusted Agent Server is installed on the same network as the private resource to which it connects. For example, if you want to use Trusted Agent for LDAP authentication, install the Trusted Agent Server on the same network as your directory service.

Good to Know:

- This task applies to on-premises and SaaS customers.
- The Trusted Agent Server can be installed on the same server as the Cherwell Service Host. For example, you can use the same server to host the Trusted Agent Server and the Scheduling microservice provided by the Cherwell Service Host.

To install the Trusted Agent Server:

1. Open the Cherwell Installer.
2. In the Trusted Agent section, select **Install**.
   The **Cherwell Trusted Agent Server Setup** window opens.
3. Select **Install**.
   The **Trusted Agents Server Setup Wizard** opens.

   > **Note:** You can also install the Trusted Agent Server from the **Cherwell Disk Image** folder. Open the **Utilities** folder and double-click the **Cherwell Trusted Agents Server.exe** file.

4. Select **Next**.
5. Select **I accept the terms in the license agreement**.
6. Select a custom installation location or select **Next** to use the default location.
7. Select **Install**.
   The Cherwell Configuration Manager launches.
8. In the Cherwell Configuration Manager, select the **Start** button. On the **Enable Trusted Agent Auto Update** screen, **Enable Auto Update** is enabled by default. If you don't want the autoupdater service to check for new versions of the Trusted Agent server, clear the checkbox. Use the Server Manager to configure the Auto Update Service.
9. Select **Finish**.

Related concepts
Configuring Trusted Agent
Related tasks
Configure the Trusted Agent Server
Configure the Trusted Agent Hub in the Server Manager
Connect to the Trusted Agent Hub from CSM Administrator
Configure Trusted Agent Service Groups

Configure the Trusted Agent Server

Configure the Trusted Agent Server to connect to the Trusted Agent Hub. The Trusted Agent Server is installed on a same machine in the same network as your private resources.

This task applies to on-premises and SaaS customers.

To configure the Trusted Agent Server:

1. Go to the installation directory to run the Trebuchet.ServerConfigTool.exe. The default path from the install is: C:\Program Files\Cherwell\Cherwell Trusted Agent Server.
2. Double-click **Trebuchet.ServerConfigtool.exe** to open the Server Manager.
3. Select **Trusted Agent Server** from the **Server** drop-down list, and then select **Configure**.
4. Provide a display name for the server. This will display in CSM Administrator.
5. Provide Hub connection settings:

Option	Description
Hub URL	Provide the URL. This is the address that should be used to connect to the Hub from other Cherwell servers and services. **Note:** Secure transport (HTTPS) should be used for all Hub communications in production environments.
Shared Key	Provide the Shared Key. This must be the same Shared Key that is used in the Trusted Agent Hub configuration. Cherwell provides this key to SaaS customers.
Test	Select to verify that the Hub URL and shared key are valid.

6. Provide connection to the CSM database:

Option	Description
Connection	Use the **ellipsis** button to browse and locate the database to connect to.

Option	Description
Login to Cherwell	Chose one of these options: ◦ **Windows authentication**: Use the Windows credentials for the account that is used to run the Trusted Agent Service. ◦ **User ID and Password**: Provide a CSM user ID and password. This is usually an administrative account with broad system access, but don't use the CSDAdmin default account. Provide a blank password to allow the specified user to log in without a password. This only works if the user does not have a password. This is not recommended.
Test	Select to verify login information.

7. Enter the **Hub Ping Frequency** in seconds, to send a ping to the Hub. If a ping is not received by the Hub within the Agent Registration timeout period, then the Agent's registration with the Hub is considered expired. No further requests are sent to the Agent until the next registration request or ping is received from the Agent. The **Hub Ping Frequency** should always be lower than the Agent Registration period set for the Trusted Agent Hub. The Hub default is 180 seconds.

> **Note:** Use -1 to disable pings sent to the Hub (not recommended).

8. Select **OK**.

9. Restart the Trusted Agent Server.

Related concepts
Configuring Trusted Agent
Related tasks
Install the Trusted Agent Server
Configure the Trusted Agent Hub in the Server Manager
Connect to the Trusted Agent Hub from CSM Administrator
Configure Trusted Agent Service Groups

Connect to the Trusted Agent Hub from CSM Administrator

Once you connect to the Trusted Agent Hub from CSM Administrator, return here to easily access your Hub URL and shared key.

Trusted Agent must be configured before you can connect to the Trusted Agent Hub from CSM Administrator.

This task applies to on-premises and SaaS customers.

To connect to the Trusted Agent Hub:

1. In CSM Administrator, select the **Trusted Agents** category, and then the **Edit Trusted Agents Hub Settings** task.
2. On the **Trusted Agents Hub Settings** dialog, provide:
   ◦ The URL for your Trusted Agent Hub.
   ◦ The Shared Key used by the Trusted Agent Server and the Trusted Agent Hub.
3. Select **Test** to verify that you can connect to the Trusted Agent Hub.

Related concepts
Configuring Trusted Agent
Related tasks
Install the Trusted Agent Server
Configure the Trusted Agent Server
Configure the Trusted Agent Hub in the Server Manager
Configure Trusted Agent Service Groups

Configure Trusted Agent Service Groups

Trusted Agent service groups are used to route requests to specific Trusted Agent Services. If no groups are configured, all Trusted Agent Services are assumed to be capable of performing all Trusted Agent operations.

Trusted Agent service groups are created in CSM Administrator and selected when you configure Trusted Agent for external data sources, LDAP directories, Windows Domains, One-Step Actions, and email operations.

You can view status and last ping time information for each Trusted Agent Service and Trusted Agent Service Group.

To configure the Trusted Agent service groups, you must configure Trusted Agent and connect to the Trusted Agent Hub from CSM Administrator.

To add Trusted Agent service groups:

1. In CSM Administrator, select the **Trusted Agents** category, and then the **Edit Trusted Agents service groups** task.
   The **Trusted Agents** dialog opens. If Trusted Agent is correctly configured and running, all Trusted Agent Services appear under the **All Agent Services** node.
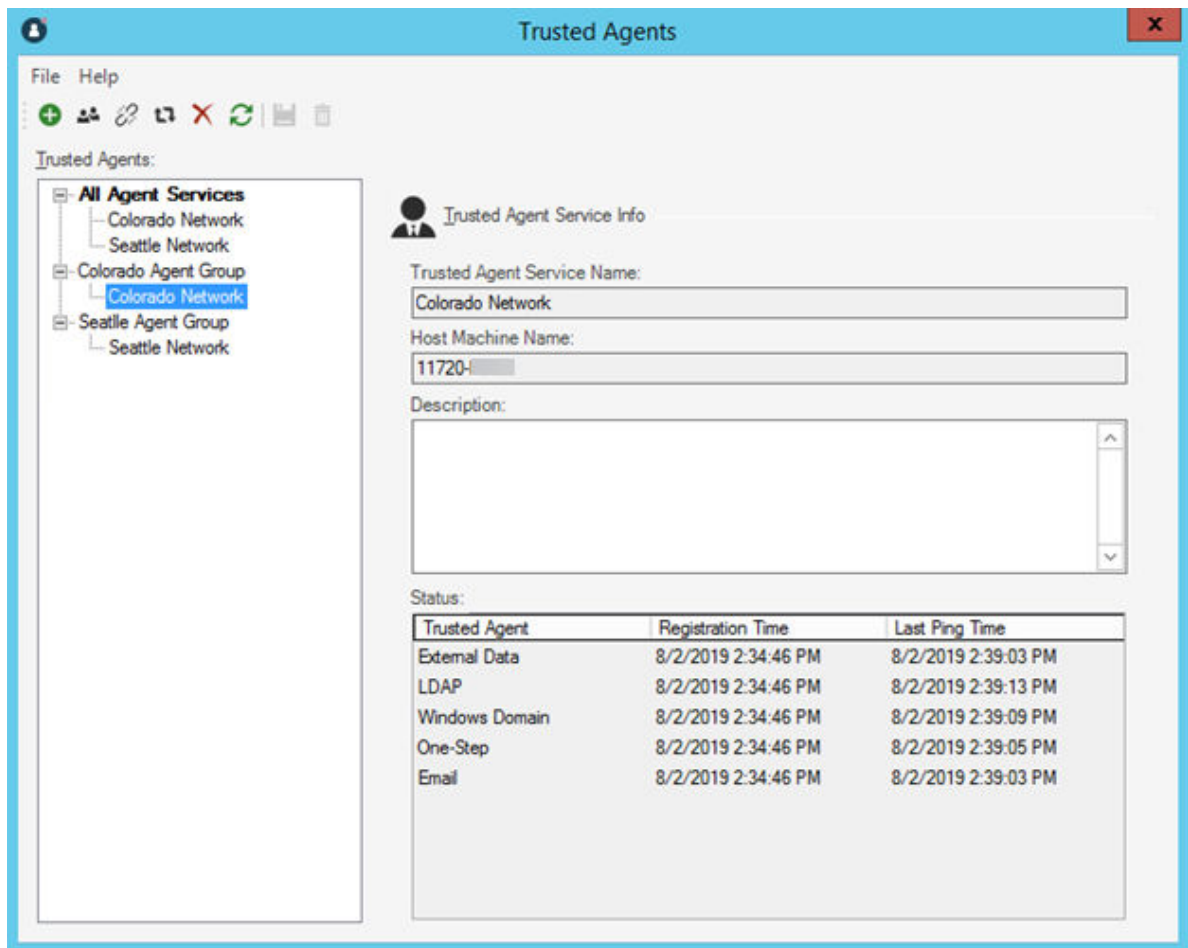
Note: Trusted Agent Services are shown when they are successfully connected to the Trusted Agent Hub. If no Trusted Agent Services are present in this dialog, connect your services to the Trusted Agent Hub first, and then use this dialog to configure your services and groups.

2. Select the **Create** icon.

3. In the **Trusted Agent Group Info** section, provide a Name and Description for the service group.

4. Select **Save**.

5. Repeat the steps to add all of the service groups you need.
   The newly created groups appears in the tree.

6. Select a service group, and then select the **Add trusted agent service to group** 📇 icon.

7. Select a Trusted Agent Service to assign to the service group.

8. Select **OK**.

9. Assign a Trusted Agent Service to each service group.

Related concepts

Configuring Trusted Agent

Related tasks

Install the Trusted Agent Server

Configure the Trusted Agent Server

Configure the Trusted Agent Hub in the Server Manager

Connect to the Trusted Agent Hub from CSM Administrator

Configuring Trusted Agent Features

Trusted Agent can be used for LDAP connections, validation through Windows domains, importing external data, One-Step Actions, and email operations.

Related tasks
Using Trusted Agent Server with LDAP
Import External Data Using Trusted Agent
Using Trusted Agent with Email

Using Trusted Agent Server with LDAP

Use your LDAP connection with Trusted Agent to authenticate users, import Directory Services users, and import Directory Service data into Business Objects.

Before enabling LDAP for Trusted Agent, you must first configure Trusted Agent. For more information, see Trusted Agent.

To enable LDAP for Trusted Agent:

1. Verify that CSM is configured for LDAP:
   - In CSM Administrator, select the **Security** category and then select the **Edit Security Settings** task. Select each client page (Desktop Client, Browser Client, etc.) and verify that LDAP is selected as a login mode.
   - Create or open a Blueprint, and then select **Tools>Directory Services**. Edit an LDAP connection, and then verify that the **Map LDAP Object** settings are applied.
2. On the **Map LDAP Object** dialog, select the **Trusted Agents** page.
3. Select the **Use Trusted Agents** check box.

   Note: If you want to disable Trusted Agent for a specific LDAP connection, clear the **Use Trusted Agents** check box.

4. Select one of these group options:
   - **Any Trusted Agent Group**: Select to allow any group to handle requests for this LDAP Connection.
   - **Trusted Agent Group**: Select a specific group to handle requests for this LDAP connection.
5. Select the **General** tab.
6. Optionally, select the **Client-side LDAP (for SaaS)** check box.

   Note: This setting is not required for Trusted Agent, but it may complement its use by reducing round trips between CSM Administrator and LDAP directories for activities initiated within CSM Administrator using an Application Server and 3-tier connection. This setting does not impact LDAP interactions that are initiated by Cherwell services that use a direct-to-database and 2-tier connection.

7. Select **OK**.

Related concepts
Configuring Trusted Agent
Import Directory Service Users
Import LDAP Data into Business Objects
Configuring CSM Directory Services Settings
Related tasks
Install the Trusted Agent Server

Use Trusted Agent Server with Windows Domains

When integrating CSM with multiple domains, you can configure single sign-on user authentication by associating a particular Windows Domain with a Trusted Agent Group or Service.

Before you can use Trusted Agent to authenticate Users through a Windows Domain, you must first configure Trusted Agent. For more information, see Configuring Trusted Agent.

Trusted Agent for Windows Domains does not provide pass-through authentication for Windows users. Users must still supply their user name and password in order for their Windows credentials to be validated using the Trusted Agent.

> **Note:** LDAP directory configuration is not required when using Windows.

To enable Windows Domains for Trusted Agent:

1. Verify that CSM is configured for Windows domains:
   - In CSM Administrator, select the **Security** category and then select the **Edit security settings** task. Select each client page (Desktop Client, Browser Client, etc.) and verify that Windows is selected as a login mode.
   - Create or open a Blueprint, and then select **Tools > Windows Domains**. Specify the domain name of the network.
2. On the **Windows Domain Settings** window, select the **Trusted Agents** page.
3. Select the **Use Trusted Agents** check box.

   > **Note:** If you want to disable Trusted Agent for this Windows domain, clear the **Use Trusted Agents** check box.

4. Select one of these group options:
   - **Any Trusted Agent Group**: Select to allow any group to handle requests for this domain.
   - **Trusted Agent Group**: Select a specific group to handle requests for this domain.
5. Select **OK**.

Import External Data Using Trusted Agent

Use Trusted Agent to import external data into existing Business Objects.

To import external data using Trusted Agent, first configure Trusted Agent. For more information, see Configuring Trusted Agent.

Trusted Agent is compatible with any connections available in CSM. You can import data using Trusted Agent, but you cannot link data or import realtime or bidirectional data.

To import external data using Trusted Agent:

1. Open or create a Blueprint.
2. Select an existing Business Object, or create a new Business Object.
3. Go to **Manager > External Connections**.
4. Select **Create New**.
5. Select **Next** on the **Welcome** page.
6. Select **Use Trusted Agent**, and then select one of these options:
     ◦ **Any Trusted Agent Group**: Select to allow any group to handle requests for this External Connection.
     ◦ **Trusted Agent Group**: Select a specific group to handle requests for this External Connection.
7. Continue through the External Connection Wizard.
8. Map to a Business Object or create a new external Business Object.

     Note: If you are using a new Business Object and you select **Link to data** on the **Import vs Linked** page, an error appears on the **Data Source** page because you can only import data using Trusted Agent.

9. Select the **Database** category, and then select the **Import Data** task.
10. Complete the steps in the External Data Import Wizard.

Related concepts
Configuring Trusted Agent
Create an External Connection to an API
Map an Existing Business Object to External Data
Import External Data into an Existing Business Object

Using Trusted Agent with Email

Use Trusted Agent to process CSM emails from a server on a remote network.

To use Trusted Agent with email, you must first configure Trusted Agent. For more information, see Configuring Trusted Agent.

Note: Using Trusted Agent with email will increase e-mail processing time.

To configure an email account to use Trusted Agent:

1. In CSM Administrator, select the **Email and Event Monitoring** category.
2. Select the **Edit email accounts and settings** task.
3. Select the email account you wish to configure, and then select the **Edit** button.
4. On the **Email Options** dialog, select the **Trusted Agents** page.
5. Select the **Use Trusted Agents** checkbox, then select a Trusted Agent Group, or select **Any Trusted Agent Group** to allow any group to handle email requests.

   Note: When using Trusted Agent, outgoing email messages will always be sent from the Server, not the Client. This setting (viewable in the **From Settings** page) will be changed automatically.

Related concepts
Configuring Trusted Agent
Related tasks
Configure Global Email Accounts

Configure One-Step Actions for Trusted Agent

One-Step™ Actions can be configured to run using Trusted Agent. This enables you to run specific Actions, such as Print and Write to a File, on remote servers and distributed systems.

You can use Trusted Agent with these Actions:

- Print
- Run a Program
- Run a Report
- Write to a File
- Transfer Attachments
- Call a Web Service
- Excel Merge

With the exception of Call a Web Service, SaaS customers must use a Trusted Agent for all of these Actions when One-Step Actions will run on a server. This includes the Browser Client, CSM Portal, Cherwell REST API, Automation Processes, and the Scheduler running in a two-tier configuration. You can use a Health Check rule to locate and configure One-Step Actions for a Trusted Agent as needed. See SaaS One-Step Action Check.

> **Important:** One-Step Actions listed in the Health Check results will not run until you configure them for Trusted Agents.

You can configure a Trusted Agent for one or more of the supported Actions within a single One-Step Action. Depending on your needs, you can assign a different Trusted Agent service group to each Action.

To use Trusted Agent with One-Step™ Actions:

- Trusted Agent must be configured for your system. For more information, see Configuring Trusted Agent.
- Optionally, define Trusted Agent Service Groups so you can execute One-Step Actions on specific Trusted Agent Services.
- You must have security rights to configure One-Step Actions to run on a Trusted Agent. If you do not have these rights, you can view Trusted Agent configuration settings, but you cannot change them.

To configure a One-Step Action to run on a Trusted Agent:

1. From the **One-Step Editor Designer Board**, select an Action that supports Trusted Agent.
2. Select the **Trusted Agent** page.
3. Select the **Run on Trusted Agent** check box.
4. Select one of these Trusted Agent service group options:
   - **Any Trusted Agent Group**: Uses the next available Trusted Agent to execute the Action.
   - **Specific Trusted Agent Group**: Uses a specific Trusted Agent service group to use for the Action.

5. Review General properties for the One-Step Action to ensure they are valid for the selected Trusted Agent service group. For example, for a Print Action, verify that the printer you select is valid for the Trusted Agent service group.

Related concepts

Configuring Trusted Agent

Define a Write to a File Action

Define a Run a Program Action

Define a Run a Report Action

Define a Call a Web Service Action

Related information

One-Step Security Rights

Define a Print Action

Scaling Out the Trusted Agent Service

While a single Trusted Agent Service can be used to provide access to one or more private resources in a single private network, additional Trusted Agent Services may be used for fault tolerance and request routing.

Related concepts

Scaling Trusted Agent for Fault Tolerance

Scaling Trusted Agent for Request Routing

Related tasks

Configuring Trusted Agent for Request Routing

Scaling Trusted Agent for Fault Tolerance

More than one Trusted Agent Service can be provisioned within a single private network to allow for increased redundancy of communication with private resources. If one Trusted Agent Service goes down or is otherwise unavailable, additional Trusted Agent Services can facilitate communications with the same private resources.

The Trusted Agent Hub will distribute work among registered Trusted Agents based on a simple selection algorithm that considers the last ping time for each Trusted Agent. As a result, work will not necessarily be load balanced between the Trusted Agents but will be distributed between them depending on the timing of requests and the timing of pings received from each agent.

To enable scale-out of Trusted Agent on a single private network, install and configure more than one Trusted Agent Service on that private network, and then configure each to use the same Trusted Agent Hub URL and Shared Key. No further configuration is required.

While there is no enforced limit on the number of Trusted Agent Servers that can be provisioned and connected to a single Hub, you might experience performance and maintenance issues with large numbers of Trusted Agent Servers. Therefore, no more than 20 Trusted Agent Servers are recommended. Since each Trusted Agent Server hosts five Trusted Agents (one for each feature that uses Trusted Agent), this recommendation allows for 100 Trusted Agents.
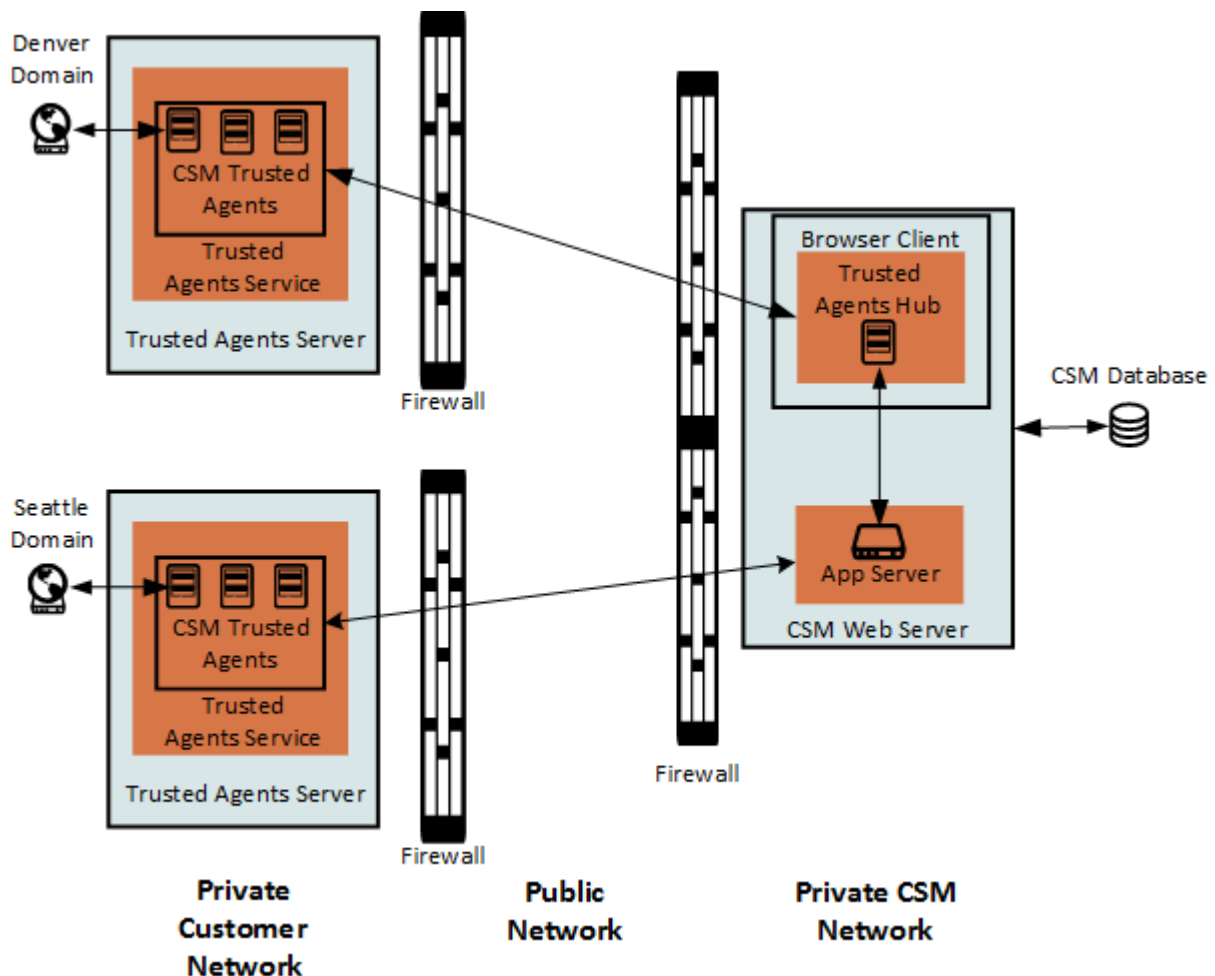
Related tasks
Install the Trusted Agent Server
Configure the Trusted Agent Hub in the Server Manager

Scaling Trusted Agent for Request Routing

Use Trusted Agent Groups to allow request routing to specific groups of Trusted Agent Services, whether in the same or different private networks.

If private resources reside in multiple private networks, Trusted Agent Services may be provisioned in each of those private networks to allow communication with those private resources. Trusted Agent Groups may be used to route requests to the appropriate Trusted Agent Services in each private network.

For example, consider a sample distributed network that contains more than one Active Directory (AD) domain, such as a "Denver" domain and a "Seattle" domain. While these domains may have an Active Directory trust between them, authentication requests may be more efficient if "Denver" domain requests are routed to Denver Active Directory domain controllers and "Seattle" authentication requests are routed to "Seattle" Active Directory domain controllers. Routing of requests in this way can be accomplished using Trusted Agent Service scale-out.

Related tasks
Install the Trusted Agent Server

Configure the Trusted Agent Hub in the Server Manager
Configuring Trusted Agent for Request Routing

CSM 2022.3 Administration

Configuring Trusted Agent for Request Routing

Before you configure request routing, you must:

1. Configure Trusted Agent.
2. Trusted Agent.
3. Configure Trusted Agent service groups.

To configure the Trusted Agent Service scale-out for request routing:

1. Configure service groups as described in Trusted Agent.
2. Create a new Blueprint.
3. Choose one of the following:
   - For LDAP, go to **Tools>Directory Services**, and then edit your LDAP connection.
   - For Windows domains, go to **Tools>Windows Domains**, and then edit your domain connection.
4. Verify the **Trusted Agents** page is configured to have authentication requests properly routed.

5. Select the **Trusted Agents** page.
   Verify that the requests are routed to the correct Trusted Agent group. For example, Colorado domain requests can be routed to the Colorado Trusted Agent group by selecting that group when configuring the Colorado LDAP settings.
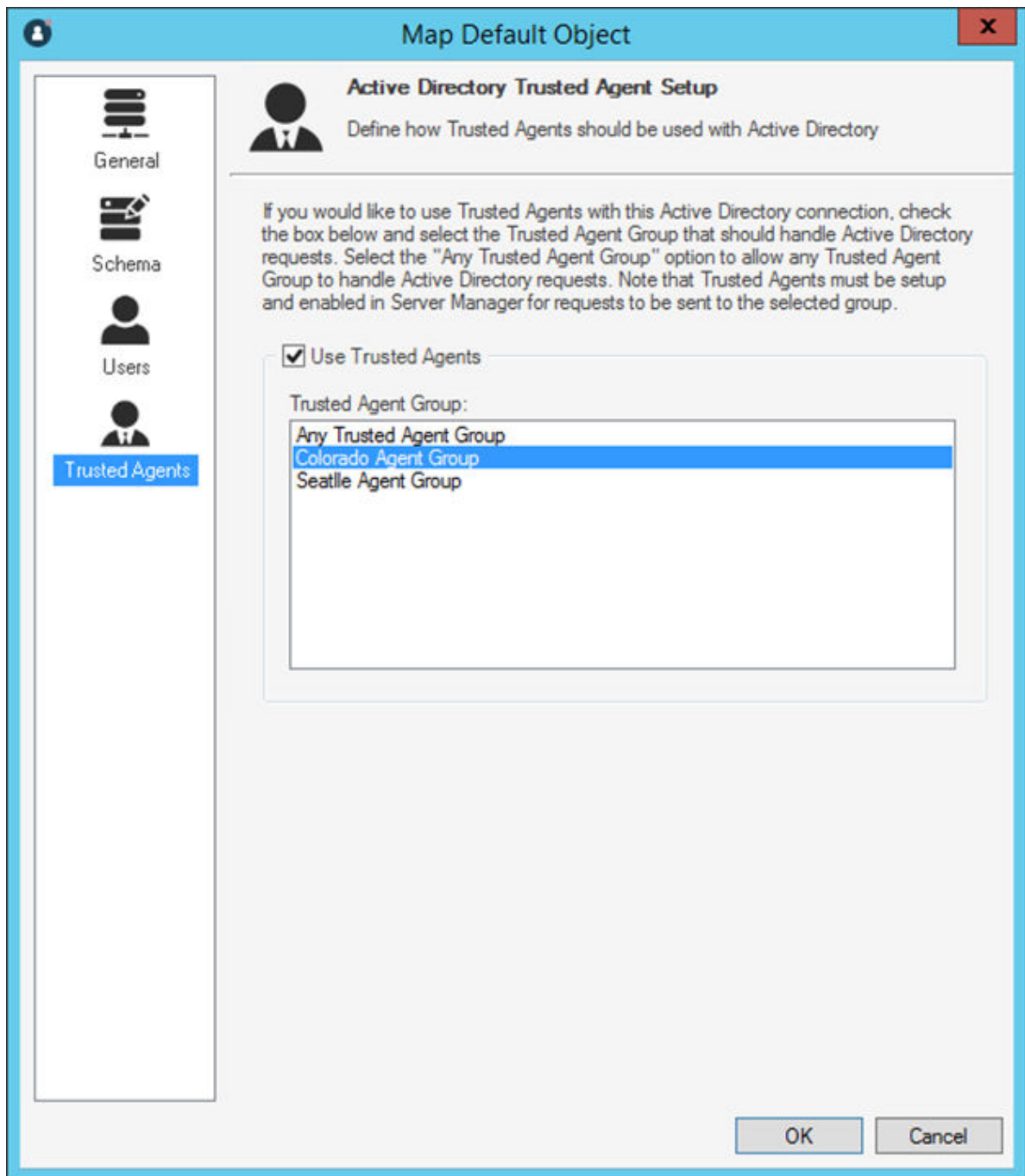
Related concepts
Scaling Trusted Agent for Request Routing
Related tasks
Install the Trusted Agent Server
Configure the Trusted Agent Hub in the Server Manager

Trusted Agent Server Technical Architecture

Each Trusted Agent establishes its own connections to the Trusted Agent Hub and to the private resources it accesses. Trusted Agent may also communicate with the Cherwell Application Server for some operations, including bulk data import.

Related concepts

Communication Between Trusted Agent and Private Resources

Communication Between Trusted Agent and the Trusted Agent Hub

Communication Used for Bulk External Data Imports

Trusted Agent Network Communication

Communication Between Trusted Agent and Private Resources

The connections between Trusted Agent and the private resources they access are typically short-lived and utilize the communication protocols appropriate for the target private resource type.

For example, when a Trusted Agent receives a request from a Trusted Agent Hub to verify an LDAP user account, that request includes LDAP directory connection information configured in CSM Administrator. The Trusted Agent uses this connection information to open a direct LDAP connection to the LDAP directory and issues LDAP queries to verify the User account. When completed, the Trusted Agent disconnects from the LDAP directory and returns the result of the user verification operation to the Trusted Agent Hub for delivery to the requesting CSM service or application.

The connection between a Trusted Agent and a private resource should typically occur over a private local network to reduce latency. Additionally, just as you would with other direct connections to secure resources, consideration should be given to using secure LDAP and encrypted database communications to protect the flow of sensitive information between these two components on the private network.

Note: The way in which Trusted Agent connects to and interacts with private resources is exactly the same as how CSM would directly connect to and utilize those resources if no network security boundaries were in place. That is, the same resource access logic is used for both scenarios. Trusted Agent simply provides a mechanism to relay those requests across network security boundaries. As a result, it may be helpful to configure an LDAP connection or an External Database connection in CSM Administrator without using Trusted Agent first, when possible. Then, when the connection is working properly, you can update the connection settings to indicate that Trusted Agent should be used.

Related concepts

Trusted Agent Server Technical Architecture

Communication Between Trusted Agent and the Trusted Agent Hub

Communication Used for Bulk External Data Imports

Trusted Agent Network Communication

Communication Between Trusted Agent and the Trusted Agent Hub

Unlike connections to private resources, the connection between a Trusted Agent and a Trusted Agent Hub is established when the Trusted Agent is started and is maintained until the Trusted Agent is stopped, the Trusted Agent Hub is no longer available, or there is a loss of network connectivity between the two.

In either of the latter two cases, the Trusted Agent will continue to try to reconnect to the Trusted Agent Hub until the Trusted Agent is stopped.

This long-lived and resilient connection is established to ensure a Trusted Agent Hub can send requests to the Trusted Agent as needed. Since the Trusted Agent resides inside a private network that is different than the network of the Trusted Agent Hub, a Trusted Agent Hub would not be able to initiate an inbound connection request to a Trusted Agent without opening the private network in a way that is typically undesirable.

As a result, a Trusted Agent establishes an *outbound* connection from within the private network to the Trusted Agent Hub using web-standard and firewall friendly protocols. The outbound connection request is made to either port 443 or port 80 of the CSM Browser Client, which hosts the Trusted Agent Hub. The port number is dependent on the protocol specified for the Trusted Agent Hub URL when the Trusted Agent Service is configured in Cherwell Server Manager.

> **Note:** Production environments should always use HTTPS (TLS/SSL) for the connection between the Trusted Agent and the Trusted Agent Hub to protect sensitive authentication information and business object data.

Trusted Agent uses a technology called SignalR to establish a persistent, bi-directional connection with a Trusted Agent Hub. SignalR is an open source technology from Microsoft which facilitates use of several transports for real-time messaging between a client (Trusted Agent) and a server (Trusted Agent Hub). A SignalR connection starts as HTTP(S) and then may be promoted to a WebSocket connection if it is available. Otherwise, other another transport is used.

The following summary describes the transports SignalR may use to establish bi-directional communication between a Trusted Agent and a Trusted Agent Hub:

- WebSocket: an HTML5 protocol for an efficient and persistent two-way connection between client and server
- Server Sent Events, also known as EventSource: an HTML5 standard describing how servers can initiate data transmissions to clients after a client connection has been established
- Forever Frame: a technique in which a hidden IFrame makes a request to an endpoint on the server that does not complete. The server then continually sends script to the client which is immediately executed, providing a one-way real-time connection from server to client
- Ajax long polling: a technique in which the client polls the server with a request that stays open until the server responds, at which point the connection closes and a new connection is requested immediately

More information about SignalR is available from Microsoft at the following site:

Introduction to SignalR

Related concepts

Trusted Agent Server Technical Architecture

Communication Between Trusted Agent and the Trusted Agent Hub

Communication Used for Bulk External Data Imports

Trusted Agent Network Communication

Communication Used for Bulk External Data Imports

When you use Trusted Agent to perform a bulk external data import, a Trusted Agent establishes a connection to the Cherwell Application Server similar to how CSM Administrator or the CSM Desktop Client establish a 3-tier connection to the Cherwell Application Server.

The settings for this Cherwell Application Server connection are configured using the **Trusted Agent Server Settings** dialog box in Cherwell Server Manager.

The connection from the Trusted Agent to the Cherwell Application Server is used to send data from an external database to CSM for mapping and importing as CSM Business Objects.

During the import, progress information is sent back to the CSM Administrator regarding the different phases of the import operation. You can let the operation run to completion or cancel the operation. If you cancel the operation, a request is sent along the path described above to allow each step in the operation to cancel its processing.

The following table describes an example request flow for Business Object imports using a Trusted Agent.

Steps	Actions
1	Using CSM Administrator with a 3-tier connection to a Cherwell Application Server, create an External Connection that uses Trusted Agent, maps data from the External Connection to a CSM Business Object, and initiates an import of external data into that Business Object.
2	The Cherwell Application Server recognizes that the External Connection is configured to use Trusted Agent and that Trusted Agent is enabled in Cherwell Server Manager. The Cherwell Application Server sends a request to the Trusted Agent Hub to import external data through a Trusted Agent.
3	The Trusted Agent Hub attempts to find an active Trusted Agent that is configured to handle external data import requests (for example, a Trusted Agent for External Data). If the External Connection indicates that only agents in a specific Trusted Agent Group should be used to process the request, the Trusted Agent Hub further restricts the selection process to only include Trusted Agents in that group. When a Trusted Agent is selected, the Trusted Agent Hub sends a request to that agent to import the specified external data.
4	The Trusted Agent receives the import request and uses the provided External Connection settings to open a connection to the specified database. The Trusted Agent then constructs a query to obtain the required data from the database and executes the query to obtain a data reader with the results.
5	The Trusted Agent then opens a connection to the Cherwell Application Server using the settings defined in Server Manager and begins to stream the data obtained from the external database to the Application Server.
6	The Cherwell Application Server receives the stream of data from the external database, maps each record from the data stream to a new or existing Business Object based on the settings specified for the import, and saves the Business Object to the CSM Database.
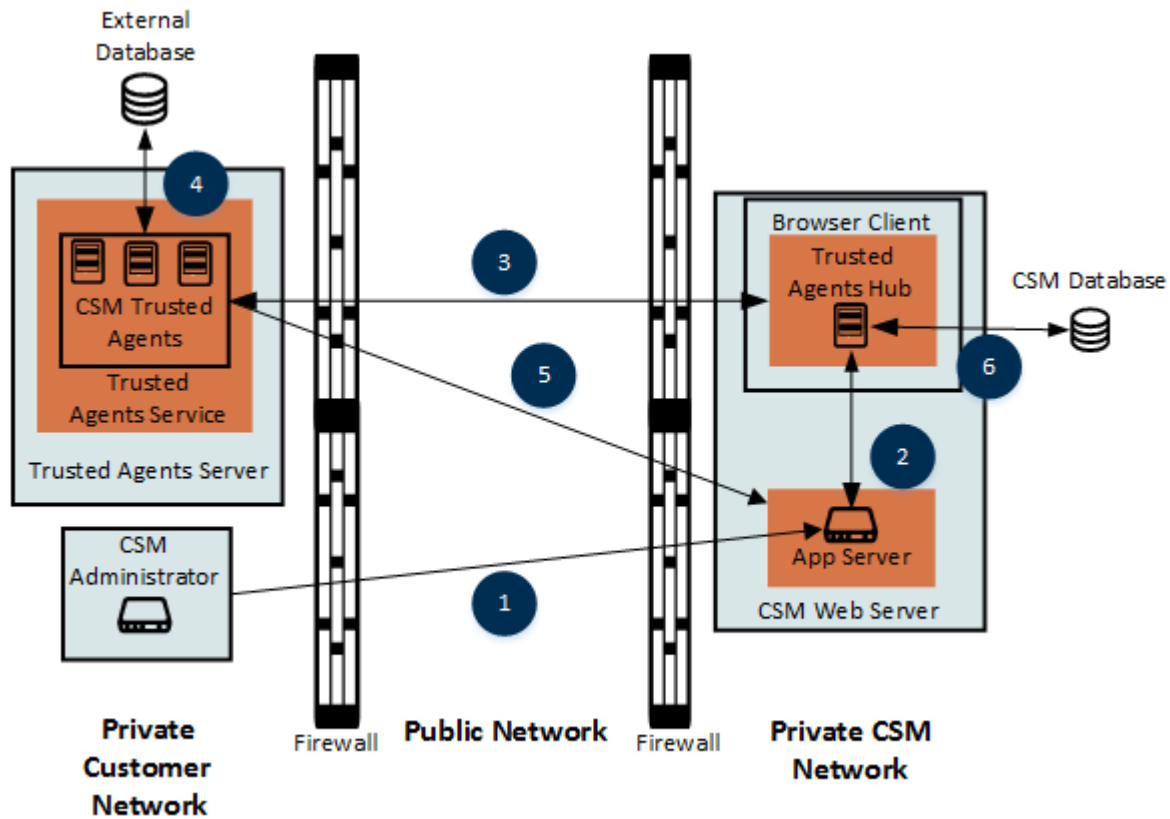
Related concepts
Trusted Agent Server Technical Architecture
Communication Between Trusted Agent and Private Resources
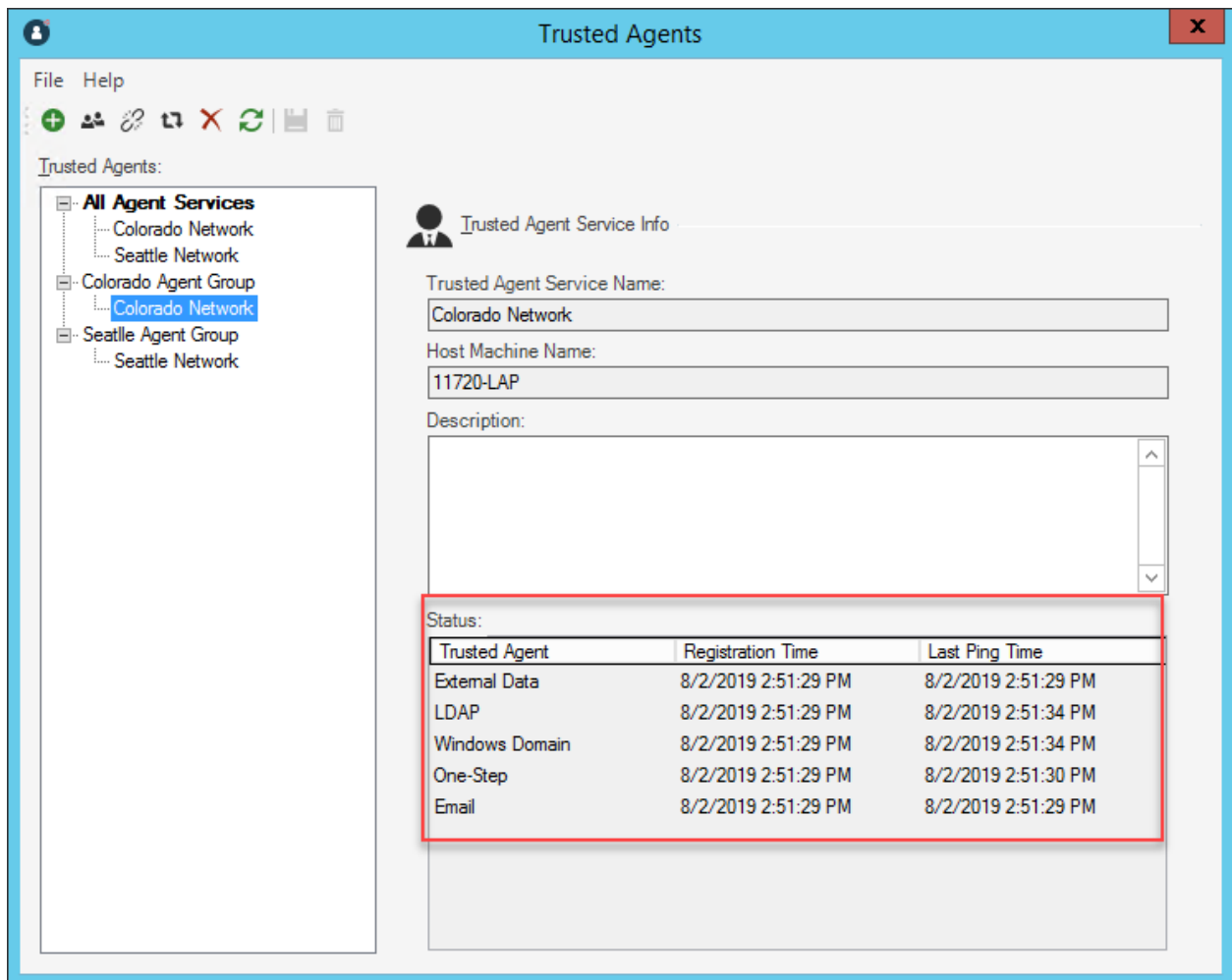Communication Between Trusted Agent and the Trusted Agent Hub
Trusted Agent Network Communication

Trusted Agent Network Communication

When started, each Trusted Agent registers itself with the Trusted Agent Hub and begins to send "ping" requests to the Trusted Agent Hub regularly to confirm to the Trusted Agent Hub that the Trusted Agent is still present and available to receive requests.

Each Trusted Agent's initial registration request and subsequent pings are logged in both the Trusted Agent Service log and the Trusted Agent Hub log if Debug level logging is enabled.

Additionally, CSM Administrator provides Trusted Agent registration and last ping time information for each Trusted Agent Service and Trusted Agent Service Group.

Related concepts

Trusted Agent Server Technical Architecture

Communication Between Trusted Agent and Private Resources

Communication Between Trusted Agent and the Trusted Agent Hub

Communication Used for Bulk External Data Imports

Trusted Agent Logging

Extensive and detailed logging is available for Trusted Agent connectivity and operations, including activities that occur on CSM servers, Trusted Agent Hubs, and Trusted Agents.

Logging can be configured to go to the Windows event log, files, or to a Splunk server. For best results, log debug messages to a file or to Splunk rather than to the Windows Event Log because CSM generates many messages when debug logging is enabled.

The logging information collected is determined by the service/server with logging enabled.

Detailed logging information for:	Then enable logging for:	Location
Trusted Agent Hub	Browser Client When using file logging: • SaaS customers can view the Hub logs by selecting **Browser Client** in the Log Viewer in CSM Administrator. For more information, see Log Viewer Utility. • The log file must be writable by the IIS application pool in which the Browser Client is running. • Do not place the log file within the physical path for the Browser Client. Changing the files in this directory, or subdirectory, can cause the application pool to recycle every time the log file is updated, resulting in Users being logged out unexpectedly.	Cherwell Server Manager on the Trusted Agent Hub. Cherwell performs this task for SaaS customers.

Detailed logging information for:	Then enable logging for:	Location
Trusted Agent	Trusted Agent Server, Cherwell Application Server	Cherwell Server Manager on each Trusted Agent server and on the main CSM server. The Trusted Agent Service logs messages through the Cherwell Application Server on the main CSM server, in addition to logging on its own server. Detailed logging is available on the Trusted Agent server when enabled. Warning and Above logging for the Trusted Agent Service is also available on the main CSM server if logging is enabled for the main Cherwell Application Server at the Warning and Above level or higher. **Note:** When logging is enabled on the Trusted Agent server, it can take up to 60 seconds for messages to be seen and delivered to the Cherwell Application Server. This information applies to both on-premises and SaaS customers.
Initiation of Trusted Agent operations from CSM servers	Application Server or Cherwell Service Host	Cherwell Server Manager.
Manual Active Directory or external data imports from CSM Administrator.	Client-side logging.	Logging configured in the CSM Desktop Client applies to CSM Administrator. For more information, see Configure User General Settings

Set log levels for selected log types:

Log to	Option description

Event log	Log level:
	
	• **Debug and above**: Very verbose messages. This level is space and resource intensive.
	
	    Note: For best results, log debug messages (Debug and above) to a file or to Splunk, and NOT to an event log. CSM logs numerous debug messages, so a log would be slow and might require more resources.
	
	• **Stats and above**: Detailed messages that track performance.
	• **Info and above**: Informational messages that can be used to diagnose a problem.
	• **Warning and above**: Warning messages that occurred.
	• **Error and above**: Errors that were encountered.
	• **Fatal only**: Errors that caused the service or process to stop.
	
	    Note: To see email success and failure messages, choose **Info and above** or **Debug and above**.

File	• **Log Level**: Select an event classification as described above (example: Debug and above, Info and above, etc.) • **File Name**: Select the **Ellipses** button to select a location for the log file. • **File Size Limit**: By default, the file size is set to 10 MB, but can be changed by entering a new value in the field. • **File Count Limit**: Rolling event logs are used, so that when the maximum file size is reached for a log file, a new file is created. By default, the number of files is set to 20 (but can be changed), after which the oldest log file is overwritten by continued logging.
Splunk	Writes the logs to a Splunk server. You must configure Spunk logging for logging to Splunk.

Related concepts
Using the Server Manager
Related tasks
Log to Splunk

Troubleshoot Trusted Agent

Before you call support for assistance, review troubleshooting tips and verify that your system adheres to the recommendations.

If Trusted Agent operations are failing but the cause is unknown or more information is needed, detailed logging can provide more information about the cause of the failure. Refer to Trusted Agent Logging for more information.

Related concepts

Verify that a Trusted Agent Hub is Operational

Verify Trusted Agent Connections to the Trusted Agent Hub

Verify LDAP Authentication Outside of Trusted Agent

Verify Clients Are Using a 3-Tier Connection

Verify the Maximum Message Size Setting for the Cherwell Server Manager

Verify Trusted Agent Hub Timeout Settings

Find Your Trusted Agent Hub URL and Shared Key

Each Trusted Agent Server must use the same Hub URL and shared key set in the Trusted Agent Hub. There are various ways to find your Hub URL and shared key.

Use one of these options to find your shared key:

- Cherwell provides the shared key to SaaS customers when a Trusted Agent Hub is provisioned. Locate the communication from Cherwell to find the Hub URL and shared key.

- If Trusted Agent is already configured and you need the key to configure an additional Trusted Agent Service, open CSM Administrator, and then select the **Trusted Agents** category. Select the **Edit Trusted Agents Hub Settings** task to see the Hub URL and the shared key for your system.

- On-premises customers can find the shared key in the Trusted Agent Hub on the server that hosts the CSM Browser Client. For more information, see Trusted Agent.

Verify that a Trusted Agent Hub is Operational

When enabled and operational, a Trusted Agent Hub responds with a message at a relative `URL:/SignalR/Hubs.` If you do not receive this file when you access this URL, the Trusted Agent Hub is not operational.

For example, if your CSM Browser Client is accessible at this URL:

`https://www.example.com/CherwellClient`

The Trusted Agent Hub uses this URL:

`https://www.example.com/CherwellClient/SignalR/Hubs`

This URL responds with a message similar to this example:

```
/*!
 * ASP.NET SignalR Javascript Library v2.2.2
 * http://signalr.net
 *
 * Copyright (c) .NET Foundation. All rights reserved.
 * Licensed under the Apache License, Version 2.0
 *
 */
```

To fix this issue:

- Verify that Trusted Agent is enabled in the Cherwell Server Manager.

    🖉 **Note:** For SaaS customers, Cherwell Support must perform this step.

- Restart Internet Information Services (IIS) or the CSM Browser Client web application.

Related concepts
Troubleshoot Trusted Agent
Verify Trusted Agent Connections to the Trusted Agent Hub
Verify LDAP Authentication Outside of Trusted Agent
Verify Clients Are Using a 3-Tier Connection
Verify the Maximum Message Size Setting for the Cherwell Server Manager
Verify Trusted Agent Hub Timeout Settings

Verify Trusted Agent Connections to the Trusted Agent Hub

When a Trusted Agent fails to connect to a Trusted Agent Hub, you should verify connection settings and shared keys between the Trusted Agent Service and Trusted Agent Hub.

For example, you should verify:

- The Trusted Agent Hub is enabled and operational. See Trusted Agent.
- You can connect to the CSM Browser Client from the machine that is hosting the Trusted Agent Service. If you cannot, the network connection between the Trusted Agent and Trusted Agent Hub may be experiencing a problem.
- A firewall is not preventing outbound communication from a Trusted Agent to the Trusted Agent Hub on port 443 (if using HTTPS) or port 80 (if not using HTTPS). (HTTPS should be used for all production Trusted Agent deployments.)
- The URL specified for the Trusted Agent Hub is valid and points to theCSM Browser Client web application. See Trusted Agent.
- The shared key specified for the Trusted Agent Service in Cherwell Server Manager on the Trusted Agent Server exactly matches the shared key for the Trusted Agent Hub using Cherwell Server Manager on the CSM web server. See Trusted Agent.
- Enable Debug level logging on the Trusted Agent Service to determine more information about the cause of the problem. See Trusted Agent

Related concepts

Troubleshoot Trusted Agent

Verify that a Trusted Agent Hub is Operational

Verify LDAP Authentication Outside of Trusted Agent

Verify Clients Are Using a 3-Tier Connection

Verify the Maximum Message Size Setting for the Cherwell Server Manager

Verify Trusted Agent Hub Timeout Settings

Verify LDAP Authentication Outside of Trusted Agent

Trusted Agent relays authentication requests from CSM servers using the same LDAP configuration settings that are specified in CSM Administrator. The most common cause of LDAP authentication problems is LDAP misconfiguration due to the number and variety of LDAP directory types and settings.

If LDAP authentication is not working through Trusted Agent, verify the LDAP settings by running CSM Administrator on the same network as the LDAP directory. Enable "Client-side LDAP" so that LDAP queries are executed directly by CSM Administrator rather than sending them to the Cherwell Application Server for execution. If the LDAP settings work correctly when on the same network as the LDAP directory, enable Trusted Agent usage.

See Trusted Agent.

Related concepts

Troubleshoot Trusted Agent

Verify Trusted Agent Connections to the Trusted Agent Hub

Verify Clients Are Using a 3-Tier Connection

Verify the Maximum Message Size Setting for the Cherwell Server Manager

Verify Trusted Agent Hub Timeout Settings

Verify Clients Are Using a 3-Tier Connection

Authentication requests that originate on a CSM client, such as CSM Administrator, are only sent through a Trusted Agent if the CSM client has a 3-tier connection to a Cherwell Application Server and the request is processed by the Cherwell Application Server.

Other reasons why authentication requests may not be sent through a Trusted Agent include:

- Trusted Agent is not enabled on CSM servers using Cherwell Server Manager. See Configure the Trusted Agent Server.
- There is no Trusted Agent available to process the request. This situation is noted in a Debug log by the Trusted Agent Hub. See Trusted Agent Logging.

Related concepts

Troubleshoot Trusted Agent

Verify Trusted Agent Connections to the Trusted Agent Hub

Verify LDAP Authentication Outside of Trusted Agent

Verify Clients Are Using a 3-Tier Connection

Verify the Maximum Message Size Setting for the Cherwell Server Manager

Verify Trusted Agent Hub Timeout Settings

Verify the Maximum Message Size Setting for the Cherwell Server Manager

If you attempt to import a large number of records from an external database through a Trusted Agent, you may receive a CommunicationException error.

An example error is:

```
System.ServiceModel.CommunicationException: The maximum message size quota for
incoming messages (50000000) has been exceeded. To increase the quota, use the
MaxReceivedMessageSize property on the appropriate binding element.
```

To solve this problem:

1. Open the Cherwell Server Manager (**Start > All Programs > Cherwell Service Management > ToolsServer Manager**.
2. Select the Application Server, and then select **Configure**.
3. Select the **Advanced** page.
4. Increase the **Maximum Message Size**. The maximum value is 2147483647.

Related concepts

Troubleshoot Trusted Agent

Verify that a Trusted Agent Hub is Operational

Verify Trusted Agent Connections to the Trusted Agent Hub

Verify LDAP Authentication Outside of Trusted Agent

Verify Clients Are Using a 3-Tier Connection

Verify Trusted Agent Hub Timeout Settings

Verify Trusted Agent Hub Timeout Settings

If the Trusted Agent Server is not processing as expected, verify timeout settings for the Trusted Agent Hub against the Hub Ping Frequency setting for the Trusted Agent Server. Restarting services may also solve the issue.

For example, the Trusted Agent Server may time out when attempting to process email messages with large attachments. This would trigger a communication error message in the Trusted Agent log file.

Possible solutions:

- Verify that the **Agent Registration Timeout** setting on the Trusted Agent Hub is greater than the **Hub Ping Frequency** setting for the Trusted Agent Server. For more information, see Trusted Agent and Trusted Agent.

    Note: SaaS customers must contact Cherwell Support to determine if the Agent Registration Timeout period for the Trusted Agent Hub has changed from the default of 180 seconds.

- Restart the Trusted Agent Server.
- Restart the Trusted Agent Server and CSM service used by the feature that is not working as expected, in that order. For example, if the Trusted Agent Server is not processing email, restart the Trusted Agent Server, and then restart the Cherwell Service Host.

Related concepts

Troubleshoot Trusted Agent

Verify that a Trusted Agent Hub is Operational

Verify Trusted Agent Connections to the Trusted Agent Hub

Verify LDAP Authentication Outside of Trusted Agent

Verify Clients Are Using a 3-Tier Connection

Verify the Maximum Message Size Setting for the Cherwell Server Manager

Verify Trusted Agent Hub Timeout Settings

Verify Access to Remote Files, Printers, and Network Resources

Resources using Trusted Agent must be in a network location that is accessible by the Trusted Agent. In addition, the Trusted Agent must run as a domain user on the external network so it can access domain resources such as printers and network resources.

For example, if you used Trusted Agent to run a One-Step Action that writes to a file on a remote network, the Trusted Agent must have permissions to write to files on the remote network location. In addition, users running the One-Step Action must have permissions to access and write to the file location you specify.

Globalization

You can use Globalization tools to translate text, referred to as "strings," into one or more languages. This ensures that Users can use a single CSM installation to view the same data in multiple languages.

You can translate strings for:

- Content definitions for all Business Objects or for specific Business Objects and their associations.
- Portal definitions, such as User-defined menus, toolbars, headers and footers.
- Lookup Table data.
- System platform strings.
- System Portal strings.

Related concepts

Globalization Terms and Concepts

Globalization Workflows

Globalization Best Practices

About Globalization

CSM provides several methods for translating your system into multiple languages.

Use Globalization features to:

- **Perform Bulk Updates**

  Export a Language Pack, and then send the Language Pack to a translator. After strings in the Language Pack are translated, you can import the file back into your system.

- **Perform Updates in the Language Pack Editor**

  Use the Language Pack Editor to translate a small number of strings or modify existing translations.

- **Use Machine Translation**

  Apply machine translations to a Language Pack. Currently, the Google Cloud Translator is supported.

- **Perform On-the-Fly Updates**

  Translate strings as you manage CSM features, such as forms, One-Step Actions, and expressions. This method is recommended for maintaining an existing translation.

Related concepts
Globalization Workflows
Globalization Terms and Concepts
Globalization Best Practices

Globalization Terms and Concepts

Globalization Terms

- **Culture**
  Culture is used to assign a language and locale pair to Users. For example, the culture "en-US" assigns the English language and the U.S. locale to Users. Cultures can be set globally and assigned to Roles and to individual Users.

  - **Base Cultures**
    Refers to the strings provided for these languages and cultures:

    - English (United States) (en-US)

    - German (Germany) (de-DE)

    - French (France) (fr-FR)

    - Portuguese (Brazil) (pt-BR)

    - Spanish (Spain) (es-ES)

  - **Primary Culture**
    The primary culture, also referred to as the installed culture, is the culture used by the majority of a CSM system. In most cases, the culture is based on the culture selected when you upgrade CSM from a version earlier than 9.2.0.

  - **Preferred Culture**
    Refers to the first preferred fallback culture that is shown to Users when a translation is unavailable in their selected culture. The preferred culture is always the first enabled culture listed on the **Manage Cultures** page of the **Globalization Management** window.

  - **Source Culture**
    Refers to the culture that is a starting point for a Language Pack. The source culture provides a set of strings for a particular culture that you can translate.

  - **Target Culture**
    Refers to the culture for which you will translate strings. For example, your source culture might be English and your target culture might be Danish (Denmark). In this case, you will translate English strings to Danish.

- **Definition**
  A definition is a system entity that makes up a CSM content object, such as a Business Object, form, grid, relationship, or saved search.

  Each definition contains a set of strings that can be modified. These strings may be used in one or many definitions.

- **Language Pack**
  A Language Pack is a set of strings that enable support for specific languages and locales. Each Language Pack has a set of strings in a source language; these strings are translated to a target language.

- **Language Pack Bundle**
  A Language Pack Bundle is a set of Language Packs based on existing languages in your system when you create a Language Pack.

String Types

Each CSM system includes the following types of strings that can be translated.

String Type	Description
Content	Strings for Business Objects, forms, dashboards, expressions, One-Step Actions, etc. This includes OOTB content and customer-created content.
Lookup Table Data	Strings for Fields values for Lookup Tables can be translated after you enable localization for each table and Fields within those tables.
Portal Content	Portal-based strings for User-defined header and footer, menus, toolbars, and more.
Platform	Typically client-based strings, such as those for menu items, toolbars, dialogs, form controls, and tooltips. You cannot change the Platform strings for the languages provided by CSM. You can, however, use one of the five base CSM languages as the starting point for a Language Pack that includes platform strings.
Portal Platform	Portal-based resource strings for toolbars, menus, errors, and more.

To translate various string types, select the scope when you create a Language Pack.

Fallback Mechanism

The order of cultures on the **Manage Cultures** page determines which language is shown to Users if there is not a translation available for the culture they are using.

🖉 **Note:** The fallback mechanism applies to all strings, except those in Lookup Tables.

The first culture in the list is known as the "preferred" culture. This is the culture that pertains to most Users in your system. Below that, the order of enabled languages determines what is shown to Users if a translation is not available for their culture.

In the example below, Users with the Spanish (Peru) culture set will see strings in Spanish. If a string is not available for that language, it will be shown in English, and then French if an English version is not available.

Enabled	Culture	Code
☑	English (United States)	en-US
☑	French (Canada)	fr-CA
☑	Spanish (Peru)	es-PE

Globalization Workflows

Workflow for Translating Strings

Follow this general process to translate strings.

Task	Notes
1. Populate your system with cultures.	See Manage Cultures.
2. Define security by assigning cultures to Roles or to Users.	See Configure Security for Cultures.
3. Create Language Packs.	See Create a Language Pack.
4. Translate strings.	Use one of these approaches: • **Perform Bulk Updates** Export a Language Pack, and then send the Language Pack to a translator. After strings in the Language Pack are translated, you can import the file back into your system. • **Perform Updates in the Language Pack Editor** Use the Language Pack Editor to translate a small number of strings or modify existing translations. • **Use Machine Translation** Apply machine translations to a Language Pack. Currently, the Google Cloud Translator is supported. • **Perform On-the-Fly Updates** Translate strings as you manage CSM features, such as forms, One-Step Actions, and expressions. This method is recommended for maintaining an existing translation.
5. Apply Language Packs to your system. When you apply Language Packs, a Blueprint is created.	See Apply a Language Pack.
6. From the Blueprint created when you apply a Language Pack, use the Definition Reviewer to review the impact of your translations on Forms, Grids, and Form Arrangements. You can modify these visual elements as you review them in the Definition Reviewer.	See Review Visual Elements for All Business Objects.
7. Publish the Blueprint that contains the Language Pack.	See Publish a Blueprint.
8. Verify that your Portal strings have been translated and add the Language Selector to each Portal Site.	See Translating Strings for Portal Sites.

Task	Notes
9. Enable cultures so that translations are visible to Users.	See Enable and Disable Cultures.

Workflow for Distributing Language Packs

You can distribute translated strings to various target systems by adding Language Packs to a Blueprint or mApp Solution. After the Blueprint or mApp Solution is published, apply the included Language Packs to your target system.

Follow this general process to distribute Language Packs:

Task	Notes
1. Create Language Packs.	See Create a Language Pack.
2. Translate strings using one of the approaches listed in the table above.	
3. Create a Blueprint or mApp Solution.	See Create a Blueprint or Create a mApp Solution.
4. Add the Language Pack to the Blueprint or mApp Solution.	From the Blueprint or mApp Solution, select **Managers > Language Pack Manager**, and then select the Language Pack. Then, right-click and select **Add to Blueprint** or **Add to mApp**.
5. Publish the Blueprint or apply the mApp Solution to a target system.	See Publish a Blueprint or Apply a mApp Solution.
6. Apply the Language Pack.	See Apply a Language Pack.

Globalization Good to Know

Excluded Strings

Most text strings can be translated. The following list contains examples of strings that are excluded from Language Packs or that should not be translated:

- Team and Workgroup names
- File paths
- Email addresses
- Date formats
- True/false values, unless they appear in a sentence string
- The word "System," unless it appears in a sentence string
- [Font] strings
- Strings that start with "BO:" and "DefType:"

You can create custom lists of locked strings to prevent them from being translated. See Managing Locked Strings.

mApps Compatibility

Due to changes made to support Globalization, the following guidelines apply to mApp Solutions:

- mApp Solutions created using CSM 9.2.0 or later cannot be applied to an earlier version of CSM.
- When you apply a mApp Solution to that was created on a version earlier than CSM 9.2.0, you are prompted to and must select a target culture for the mApp Solution.

Globalization and Cherwell Mobile

Globalization support is currently not available for Cherwelll Mobile for iOS or Cherwell Mobile for Android.

Date, Time, Number, and Currency Formats

Date, time, number, and currency formats are determined by the user's operating system's region setting for all CSM Windows-based clients and for the Microsoft Edge browser. For other web browsers, date, time, number, and currency formats are determined by the browser's language settings; the top language set for a browser is used for these formats.

Disabling Localization on Localized Fields

You may see unexpected values for fields that have been localized if you disable localization support for the fields. (This task is performed on the Localization page of the **Business Object Properties** dialog. See Define Localization Properties for a Business Object) If this occurs, you can manually edit values in the Data Editor to reflect values for your installed culture.

Configuring Globalization

Before you can translate platform and content strings, you must first add cultures, configure machine translation, and manage security rights.

Manage Cultures

Use the **Manage Cultures** page of the **Globalization Management** dialog to manage the cultures for your system.

You can:

- **Add cultures**

  You must do this before you can enable the culture so that translations are visible to users.

- **Enable and disable cultures**

  This enables you to control which translations are visible to users for each culture.

- **Reorder cultures to specify "fall-back" languages**

  Culture order determines the "fall-back" languages that are visible to users if a translation is not available for their selected culture.

- **Delete cultures**

  Delete cultures that are no longer needed.

Add Cultures

When you add a culture, definitions for that culture are added to a Blueprint that you can publish immediately or save and publish later.

> **Note:** Newly created culture-specific fields are automatically populated with data from the primary culture. This prevents the culture-specific fields from having null values.

To add a culture:

1. In the CSM Administrator main window, select the **Globalization** category, and then select **Globalization Settings**.
2. Select the **Manage Cultures** page.
3. Select the Plus sign to the right of the drop-down menu.
   The **Add Culture** dialog opens, and the **Cultures** menu contains cultures you can add to your system.
4. Select the culture to add to your system.
5. Select **OK**.

> **Note:** The Blueprint that contains new definitions based on the added culture opens. Once you publish the Blueprint, the newly added culture is shown on the **Manage Cultures** page. You must enable the culture before it is available in the culture selector.

Enable and Disable Cultures

Cultures are available in the culture selector after you enable them. Disabled cultures are not available in the culture selector.

To enable a culture, select the **Enabled** check box.

To disable a culture, clear the **Enabled** check box.

Reorder Cultures to Specify "Fall-back" Languages

Use the arrows to reorder the priority in which enabled cultures are shown to users if a translation is unavailable for their culture. For more information, see Fallback Mechanism.

Delete Cultures

When you delete a culture, associated definitions are deleted from Business Objects, grids, and forms. A Blueprint is created so you can verify your changes before you publish them to your system.

> **Warning:** Do not delete the German (de-DE) culture. CSM uses this culture as a baseline because it often has larger strings than other cultures, which helps to ensure new cultures don't have overlapping controls when platform resources are translated. If the German culture is removed, it has no "fall-back," so it will take empty values for size and position. This could result in hidden or tiny controls and labels.

> **Warning:** When a culture is deleted, data associated with culture-specific fields is also deleted and cannot be recovered once you publish the Blueprint.

The primary culture, also referred to as the installed culture, cannot be deleted or removed from the list of cultures.

To delete a culture:

1. In the CSM Administrator main window, select the **Globalization** category, and then select **Globalization Settings**.
2. Select the **Manage Cultures** page.
3. Select a culture in the list, and then select the **Delete** icon.

The Blueprint with deleted definitions opens. Once you publish the Blueprint, deleted definitions are removed from your system and the deleted culture is no longer shown on the **Manage Cultures** page.

Configure Machine Translators

You can use machine translators to more quickly add translations to strings in a Language Pack. You can then use the Language Pack Editor to review and modify strings.

Google Translate can be used to power translations in CSM. For more information, refer to https://translate.google.com.

✎ **Note:** You must create your own Google Cloud Translator account and add your API key to enable machine translations for CSM.

To configure a machine translator:

1. In the CSM Administrator main window, select the **Globalization** category, and then select **Globalization Settings**.
2. Select the **Translators** page.
3. Select **Google**, and then click **Configure**.
4. Apply the following settings to the **Google Translation** dialog.

Setting	Description
Enable Google Translator	Select this check box to enable the Google Cloud Translator for your system.
Application Name	Provide the Application Name you used when set up your Google Cloud Translator account.
Google Key	Add the API key for your instance of Google Cloud Translator.
Error Tolerance Level	Select an error tolerance level to use for machine translations. The tolerance level determines the number of attempts made to translate strings when errors occur. Errors can occur because of complex strings or rules in your machine translation API. A lower tolerance level increases the number of translation attempts and the amount of time needed to translate strings. In most cases, a higher tolerance level produces acceptable results; however, machine translations should always be reviewed in the Language Pack Editor.
Verify	Click this button to verify your settings. If you receive an error, verify that you specified the correct application name and Google key.

5. Click **OK**.

Configure Localization Support for Lookup Tables

Before you can translate values for Fields in Lookup Tables, you must enable localization support for each Lookup Table.

To enable localization support for Lookup Tables:

1. Verify that you have multiple cultures enabled for your system.
2. Review the information about current culture Fields and specific culture Fields. See About Globalization and Lookup Tables.
3. Enable localization support for Lookup Tables.
4. Use the Data Editor to translate values for culture-specific Fields.
5. Publish your Blueprint.
6. Optionally, set and update foreign key values to ensure that Lookup Table values is updated in existing records in your system.
7. Verify security settings for Lookup Tables. See Configure the Default Domain, Anonymous Login, and Lookup Table Security Settings.

Related concepts

Manage Cultures

Storing Foreign Keys for Validated and Auto-populated Fields

Related tasks

Enable Localization Support for a Lookup Table

Translating Values for Culture-Specific Fields

About Globalization and Lookup Tables

When you enable localization support for a Lookup Table, you can determine which Text Fields within that object can show translated values to Users as they select, search for, and validate Field values based on their current culture or from other enabled languages in your system.

A separate copy of each Field is added to the Lookup Table for each enabled culture in the system.

Tip: Consider storing foreign keys for Fields in your Lookup Table. This ensures that Users are presented with the translated values in the correct language and lets you backfill translated values in existing records. For more information, see Storing Foreign Keys for Validated and Auto-populated Fields.

Fields in Lookup Tables with localization enabled are referred to as:

- **Current Culture Fields**

  A current culture Field is used when localization is enabled for a specific Field. For example, if you enable localization for the Priority and Urgency Fields for the Change Priority Lookup Object, these are considered the current culture Fields. The value of the current culture Field is based on the User's currently selected culture.

- **Specific Culture Fields**

  A specific culture Field refers to the Field added to a Lookup Object for each culture enabled for your system. For example, if you enable localization for the Priority and Urgency Fields, a copy of each field is added for each culture you have enabled in your system. Users can use specific culture Fields to validate values from languages other than their current culture.

Specific culture Fields are identified by their language and locale pair.

Name	Type	Size	Details
▶▶ 📄 RecID	Text	42	Default: NewID()
📄 Change Priority ID	Text	10	
📄 Priority	Text	10	Current culture
📄 Impact	Text	35	
📄 Urgency	Text	35	Validated from CI Status.Status, Current culture
📄 Matrix Order	Text	5	Current culture
📄 Created Culture	Text	20	Default: CurrentCulture()
📄 Priority_en-US	Text	10	Specific Culture=en-US
📄 Priority_fr-CA	Text	10	Specific Culture=fr-CA
📄 Urgency_en-US	Text	35	Specific Culture=en-US
📄 Urgency_fr-CA	Text	35	Specific Culture=fr-CA
📄 Matrix Order_en-US	Text	5	Specific Culture=en-US
📄 Matrix Order_fr-CA	Text	5	Specific Culture=fr-CA
➕			

You can also view information about the current culture and specific culture Fields on the **Advanced** page in the **Field Properties** window. See Define Advanced Properties for a Field.

Enable Localization Support for a Lookup Table

You must enable localization support for Lookup Tables before you can translate Field values for the table.

To enable localization support for a Lookup Table:

1. Create a Blueprint.
2. In the Object Manager, select the Lookup Table for which you want to enable localization features.
3. Select **Edit Business Object**.
4. Click **Bus Ob Properties**.
5. Select the **Localization** page.
6. Select the **Supports Localization** check box.
7. Select the Fields for which you will translate values.

   Note: To enable localization support for a Field in a Group Member, enable localization for the Group Leader, and then select the Fields to translate.

8. Click **OK**.
   The **Manage Culture-specific Fields** dialog opens.
9. Select options to determine how values are managed for the languages enabled for your system.

Option	Description
Copy the neutral-culture field values to specific culture Fields	Select this check box to copy existing values into Fields for the selected culture.
Select the culture that the neutral-culture field value is currently in	Select a culture that you know has existing values for the fields you want to translate. Typically, this is the installed culture for your system.
Overwrite existing culture-specific Field values	Select this check box to overwrite existing culture-specific values with values from the selected culture.
Copy the neutral-culture value to all culture-specific Fields	Select this check box to copy the neutral-culture value to all culture-specific Fields. This adds a value for all enabled cultures. **Tip:** For best results, select this option because it gives you a starting point for translations.
Open the Data Editor	Select this check box to open the Data Editor after values are copied.
Add culture-specific values to the default Form and Grid	Select this check box to add culture-specific values to the Default Form and Grid.

Option	Description
Purge orphaned culture-specific Fields	Select this check box to remove culture-specific Fields that exist in your system but are not used. For example, you may have Fields from a culture no longer used in your system, so you can remove these orphans.

10. Click **OK**.
    A message opens, indicating the results of the copy.
11. Close the message.

You can now:

- Use the Data Editor to translate values for culture-specific Fields. You can do this before you publish the Blueprint.

- Publish the Blueprint, and then create a Language Pack that includes the Lookup Table and use the Language Pack Editor to translate values for culture-specific Fields. Refer to Create a Language Pack.

- Manage culture Fields from the Object Manager. From the Object Manager, select the Lookup Table, and then click the **Manage Culture Fields** link.
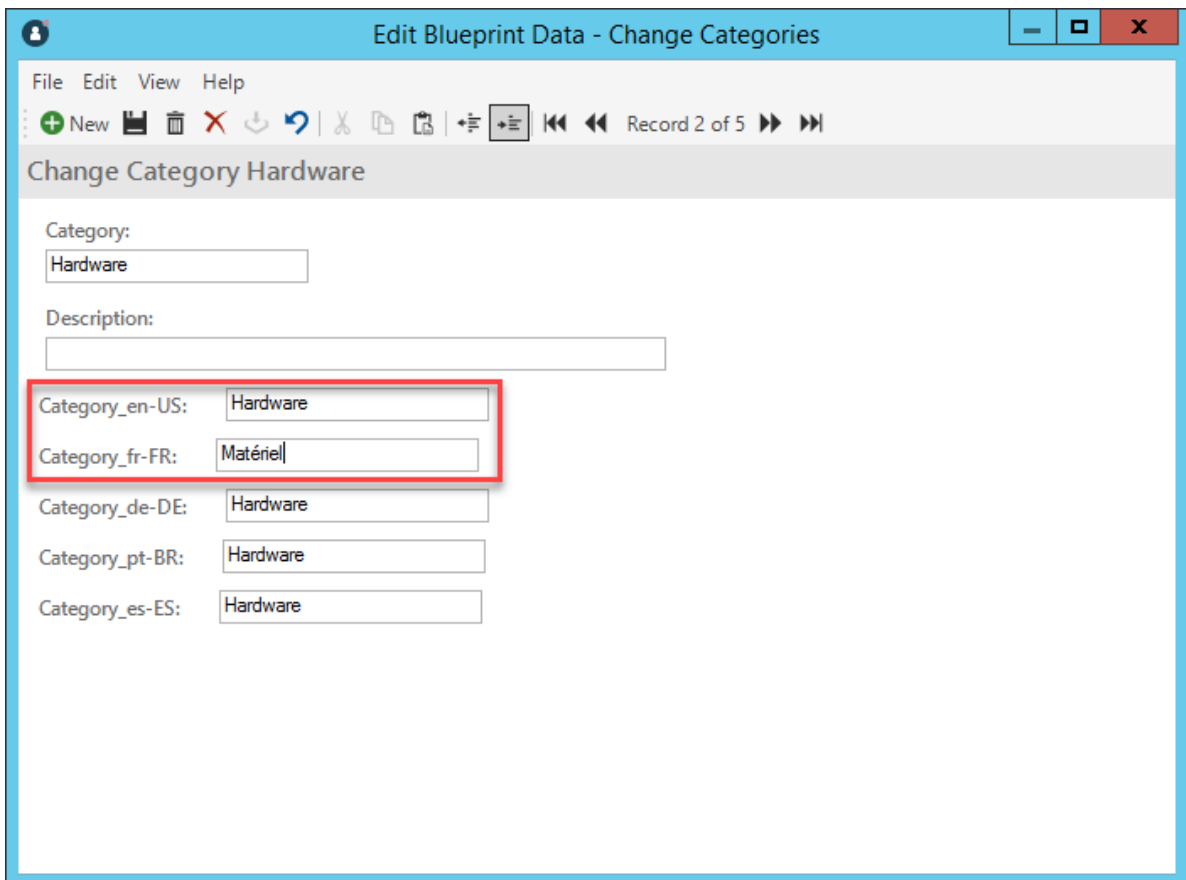
Translating Values for Culture-Specific Fields

Use the Data Editor to modify values for culture-specific Fields.

The Data Editor opens automatically after you enable localization support for a Lookup Table if you selected the **Open the Data Editor** check box on the **Manage Culture Specific Fields** dialog. You can also follow the steps in Open the Data Editor.

To translate culture-specific Field values:

1. Configure a Lookup Table for localization.
2. Open the Data Editor.
3. Double-click a row in the Data Editor.
4. Translate the values for each language as needed.

5. Publish the Blueprint.

Configure Security for Cultures

You can control the cultures that are available to Users by enabling culture settings globally, for Roles, or for individual Users.

Specifically, you can give Users access to:

- **All Cultures**

  Enables Users to choose any enabled culture as they work with CSM.

- **Preferred Culture**

  Presents the preferred fall-back culture listed at the top of the listed on the **Manage Cultures** page.

- **Specific Culture**

  Presents a single, specific culture to Users. For example, if your system is translated into Italian, you can specify that only Italian is used globally (for all Users), for Users assigned to specific Roles, or to individual Users. This also removes the culture selector from all clients, except the CSM Portal.

Culture Hierarchy

The following hierarchy determines which culture is presented to Users:

- User settings override Role settings
- Role settings override Global settings
- Global settings override Preferred culture

Related concepts
Hide the Culture Selector
Related tasks
Set Global Cultures
Set Cultures for Roles
Set Cultures for Users

Set Global Cultures

The cultures you set globally are applied to all users and roles, unless you explicitly override the global settings for specific users and roles.

By default, the preferred culture is used.

To set cultures at a global level:

1. In the CSM Administrator main window, select the **Settings** category, and then select the **Edit System Settings** task.
2. Select the **Globalization** page.
3. Select one of these options:
   ◦ **Use preferred culture**:

   Select this option to use the preferred fall-back culture that is shown to users when a translation is unavailable in their selected culture. The preferred culture is always the first enabled culture listed on the **Manage Cultures** page.

   ◦ **All cultures**

   Select this option to enable users to choose any enabled culture as they work with CSM.

   ◦ **Specific culture**

   Select this option to designate a single enabled culture for your system, and then select the culture from the drop-down list. This option removes culture selector for all users in all clients, except the CSM Portal.

4. Select **OK**.

Related concepts
Configure Security for Cultures
Hide the Culture Selector
Related tasks
Set Cultures for Roles
Set Cultures for Users

Set Cultures for Roles

You can specify cultures for specific Roles to override culture settings made at the global level.

By default, the global setting is used.

To set cultures at the Role level:

1. In the CSM Administrator main window, click the **Security** category, and then click the **Edit Roles** task.
2. In the Culture section, select one of these options:
   - **Use global culture**:

     Select this option to use the global culture setting.

   - **All cultures**

     Select this option to enable Users assigned to the Role to choose any enabled culture as they work with CSM.

   - **Specific culture**

     Select this option to designate a single enabled culture for Users assigned to the Role, and then select the culture from the drop-down list. This option removes culture selector for Users assigned to the Role.

3. Click **OK**.

Related concepts
Configure Security for Cultures
Hide the Culture Selector
Related tasks
Set Global Cultures
Set Cultures for Users

Set Cultures for Users

You can specify cultures for specific Users to override culture settings made at the global and Role level.

By default, the role setting is used.

To set cultures at the User level:

1. In the CSM Administrator main window, click the **Security** category, and then click the **Edit Users** task.
2. In the Culture section, select one of these options:
   - **Use Role setting**:

     Select this option to use the culture set for the User's Role.

   - **All cultures**

     Select this option to enable Users to choose any enabled culture as they work with CSM.

   - **Specific culture**

     Select this option to designate a single enabled culture for the User, and then select the culture from the drop-down list. This option removes culture selector for the User in all clients, except the CSM Portal.

3. Save your changes.

Related concepts
Configure Security for Cultures
Hide the Culture Selector
Related tasks
Set Global Cultures
Set Cultures for Roles

Hide the Culture Selector

Select a specific culture at the global level, for a user, or for a role to hide the culture selector from the CSM Desktop Client and CSM Browser Client. You can hide the culture selector for each CSM Portal Site.

Note: In the CSM Desktop Client, CSM Browser Client, and CSM Portal, only enabled cultures appear. In the CSM Administrator, all cultures in the system are available.

Hide the Culture Selector for All Users

Set a specific culture globally to hide the culture selector from the CSM Desktop Client and CSM Browser Client for all users. Once you specify a global culture, that culture is used for all Users, unless you override the global setting at the User or Role level.

To hide the culture selector for all Users:

1. In the CSM Administrator main window, select the **Settings** category, and then click the **Edit System Settings** task.

2. Select the **Globalization** page.

3. Select the **Specific culture** option, and then select the language that CSM display for all Users.

Hide the Culture Selector for Roles or Users

Set a specific culture for Roles or Users to hide the culture selector from the CSM Desktop Client and CSM Browser Client.

To hide the culture selector for Roles or Users:

1. In the CSM Administrator main window, select the **Security** category, and then click the **Edit User** or **Edit Roles** task.

2. Select a User or Role.

3. In the Culture area, select the **Specific culture** option, and then select the language that CSM display for the User or Role.

Hide the Culture Selector from the Portal

You can hide the culture selector from each Portal Site.

To hide the culture selector:

1. In CSM Administrator, select **Site Manager** to open your CSM Portal site in the Site Editor.

2. Select **Edit**. The **Site Properties** page opens.

3. Select the **Localization** page.

4. Clear the **Show Language Selector on Application Bar** check box.

Related concepts

Switching Cultures
Related tasks
Set Global Cultures
Set Cultures for Roles
Set Cultures for Users

Configure CSM for Multi-Byte Language Support

CSM is configured to support single-byte languages by default. You can, however, use the System Restore tool to enable multi-byte languages, such as Chinese and Japanese, for your CSM database.

Note: Right-to-left languages, such as Arabic, are not supported at this time.

To enable multi-byte support for your CSM database:

1. Use the Export Data tool to export your existing database to a .czar file, selecting these options:
   ◦ **Export Entire System**
   ◦ **Export All Data**
   ◦ **Exclude Attachments**
   ◦ **Exclude Automation Data**
   ◦ **Exclude Encrypted Fields**
2. Use the System Restore Tool to reload the exported .czar file, selecting the **Use Unicode Data Types** check box as part of the restore process.
3. In the CSM Administrator main window, select the **Globalization** category, and then select **Globalization Settings**.
4. Select the **Show Multi-byte Languages** check box.

   Note: If the check box is disabled, you must first enable support for multi-byte languages in your database.

After you enable multi-byte language support for your system, cultures that use multi-byte languages can be enabled on the **Manage Cultures** page.

Related concepts
Database Export Tool
Manage Cultures
Related tasks
System Restore Tool

Change the Installed Culture

When CSM is upgraded from a version earlier than CSM 9.2.0, you are prompted to select a primary culture, which is also referred to as the installed culture. You can change the installed culture in CSM Administrator, but you should understand the impact of doing so first.

Good to Know

- This feature is intended for customers who upgraded CSM from a version earlier than 9.2.0 who may have chosen the incorrect installed culture during the upgrade process. You should not need to change your installed culture if you initially installed CSM 9.3.0 or later.

- Be sure to back up your database before changing the installed culture. Publishing a Blueprint that changes the installed culture of your system is irreversible. Restoring a database backup is the only recovery method.

- The installed culture does not impact formatting of your system; it only determines the basis of your installation.

- If you want to hide or disable cultures from your system, the recommended methods are:
  - Disabling cultures. See Enable and Disable Cultures.
  - Hiding the culture selector globally or for specific Roles or Users. See Hide the Culture Selector.

Changing the Installed Culture

To change the installed culture:

1. Back up your CSM database.

2. In the CSM Administrator main window, select the **Globalization** category, and then select **Globalization Settings**.

3. On the **General** page, select **Change**.

4. On the **Change Installed Culture** dialog, select the installed culture you want to change your system to.

5. Select these options:

Option	Description
Overwrite existing [new installed culture] values with values from [old installed culture]	Select this check box to overwrite the target installed culture with strings from the original installed culture. You should only perform this action if you want to permanently replace strings in the selected installed culture with those in the current installed culture. Only content strings are impacted by this action; platform strings not changed.

Option	Description
Purge [old installed culture] completely from the system	Select this option to permanently delete content strings for the original installed culture from your system. Culture-specific fields are also removed from localized Business Objects, Forms, and Grids, causing data to be deleted.
I have read the following statement...	You are required to acknowledge that you understand the implications of changing the installed culture.

6. Click **OK**.

A Blueprint with the replaced installed culture and overwritten values is created. This process may take several minutes.

Applying the Installed Culture Changes

Important: Cherwell highly recommends publishing the Blueprint in a test environment before publishing it to a production environment.

You can save or publish the Blueprint created when you change the installed culture. It may take several minutes to publish the Blueprint.

After the Blueprint is published, all CSM clients should be restarted.

Managing Globalization

You can manage string translations through Language Packs or as you work with content elements in your system.

For example:

1. Use Language Packs translate strings for a specific scope, such as a Business Object, a set of Business Objects, or Cherwell platform strings.
2. Translate strings as you work with elements, such as field names or form elements.

Managing Language Packs

Manage Language Packs through the Language Pack Settings dialog in the Globalization category in CSM Administrator or through a Blueprint or mApp Solution, depending on how you intend to distribute the Language Pack.

For example:

- If you are managing translated strings for a single CSM system, use the Language Pack Settings dialog box.
- If you intend to distribute translated strings with a mApp Solution or a Blueprint, use the Language Pack Manager.

Language Pack Settings Dialog

Use the **Language Pack Settings** dialog to:

- Create Language Packs.
- Edit strings in a Language Packs.
- Apply a Language Pack bundle to your system.
- Export a Language Pack to a tab-delimited (.tsv) file.
- Import Language Packs after strings have been translated in an exported Language Pack.
- Merge two Language Packs with the same culture pair.
- View Language Pack bundle properties.
- Delete a Language Pack.

To open the **Language Pack Settings** dialog from the CSM Administrator Main Window, select the **Globalization** category, and then select **Manage Language Packs**.

You can sort and filter the list of Language Packs on the **Language Pack Settings** dialog by:

- Name
- Source
- Target
- Scope
- Description
- Created By
- Created Date
- Last Modified By
- Last Modified Date

To sort the list, click a column header.

To filter the list, select the Filter icon on the right side of the column header, and then select the values to filter the list as needed. For example, you can filter the list of Language Packs by scope, such as those that only include platform strings.

Language Pack Manager

Use the Language Pack Manager to:

- Add a Language Pack to a Blueprint or mApp Solution.
- Create a Language Pack.
- Edit a Language Pack.

To open the **Language Pack Manager** from a Blueprint or mApp Solution, select **Managers > Language Packs**.

Create a Language Pack

Use the **Create Language Pack Wizard** to create a Language Pack based on a source culture and scope, such as content strings for a specific Business Object or system platform strings.

You can then use the Language Pack Editor to translate strings in a Language Pack or you can export the Language Pack and send it to a vendor for translation. After strings are translated, you can apply translated strings in a Language Pack bundle to a Blueprint that you can publish immediately or save and publish later.

Run the Create a Language Pack Wizard

To run the Create Language Pack Wizard:

1. Use one of these methods to open the wizard from CSM Administrator :
   - In the Main Window, select the **Globalization** category, and then select **Manage Language Packs**. On the **Manage Language Packs** page, select **Create**.
   - From a Blueprint or mApp Solution, select **Managers > Language Packs**, and then select the **Create** icon.

     Note: To create a Language Pack that will be a part of a consolidated Blueprint, create the Language Pack from a Blueprint. Language Packs created from the Globalization category in the Main Window cannot be consolidated with other Blueprints.

2. Select **Next** on the **Language Pack Wizard Welcome** page.
3. Select a target culture. This represents the language and locale you want to translate to. Example: Select French (Canada) to translate source strings to Canadian French.
4. Select **Next**.

Select the Language Pack Scope

Identify the scope for your Language Pack.

You can choose one of three options:

- **Content Strings**
  Choose one or more of the following options:

  - **Definitions**
    Select a Business Object scope:

Option	Description
All	Strings for all Business Object definitions.
Specific Business Objects	Strings associated with Business Objects selected on the **Identify Specific Business Objects** page.

Option	Description
Blueprint Content	Strings for new or modified Business Object definitions only. This option is only available when you create a Language Pack from a Blueprint or a mApp® Solution that contains new or modified definitions.

- **Portal Content Strings**
  Extract strings for User-defined labels.

- **Lookup Table Data**
  Extract strings for Field values in Lookup Tables.

> **Note:** You must configure Lookup Tables for localization before you can create a Language Pack that includes Lookup Table data. See Enable Localization Support for a Lookup Table.

- **Platform Strings**
  Choose one or both of the following options:

  - **System Platform Strings**
    Extract strings for application controls, dialogs, etc. for all CSM clients, except for the CSM Portal.

  - **Portal Platform Strings**
    Extract strings for CSM Portal resources, such as error messages, toolbar definitions, menus, etc.

- **None**
  Create an empty Language Pack. Empty Language Packs are useful for merging multiple Language Packs with the same target language. For more information, see Use Small Scopes for Language Packs.

Limit the Scope to Specific Business Objects

If you chose to create the Language Pack with specific Business Objects, the **Identify Specific Business Objects** page opens.

Select the Business Objects and Views to include in your Language Pack. You can choose from:

- Major
- Supporting
- Lookup
- Group Leader
- Group Member

Tip: Use the options at the top of the list to filter Business Objects by type. You can also select the **Type** column to sort the list.

Select the Source Culture for Platform Strings

If you chose to create the Language Pack with platform strings, select the source culture or base language from which strings will be translated.

Initially, you can choose one of the following base languages as your source:

- English (en)
- German (de)
- French (fr)
- Portuguese (pt)
- Spanish (es)

After you have translated platform strings in at least one Language Pack, you can select the source culture for that Language Pack. For example, if you translate platform strings into Italian (Italy) (it-IT), you can use that as your source culture for new Language Packs.

Add Lookup Table Strings

If you chose to include Lookup Tables in your Language Pack, the **Identify Specific Lookup Tables** page opens.

Select the Lookup Tables to apply translations to, and then select **Next**.

Adding Portal Site Strings

If you chose to include CSM Portal content strings in your Language Pack, the **Identify Specific Sites** page opens.

Select the Sites to apply translations to.

Define Language Pack Properties

Finalize the Language Pack by defining these properties:

- On the **Order the Source Cultures** page, use the arrows to order the selected source cultures to determine the fall-back mechanism for strings that don't exist in a particular language. For more information, refer to Fallback Mechanism.
- On the **Define Properties** page, provide a name and description for your Language Pack.

On the **Summary** page, review the options you selected.

Select **Back** to change your options; select **Finish** to complete the wizard.

Related tasks
Export a Language Pack

Import a Language Pack
Apply a Language Pack

Edit a Language Pack

Use the Language Pack Editor to translate and manage strings in a Language Pack.

Each Language Pack contains a row for each string for the scope chosen when the Language Pack was created.
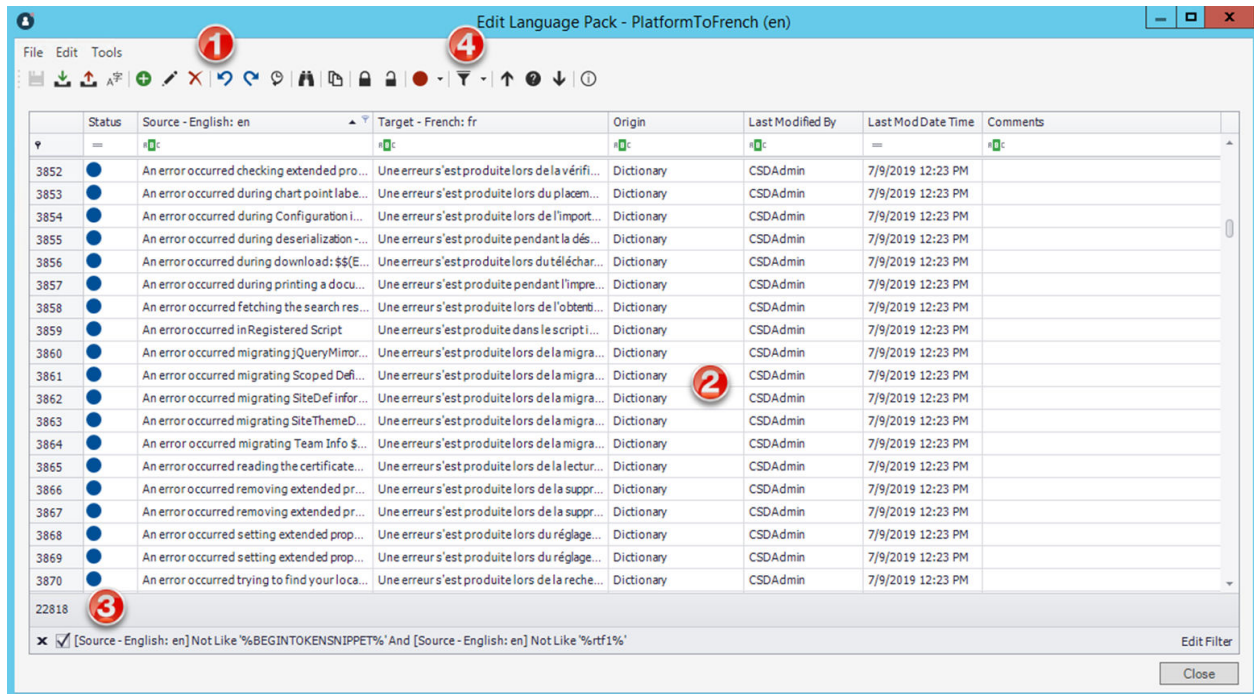
1. Language Pack toolbar

2. Language Pack Grid

3. Language Pack row count

4. Filter options

The Language Pack Toolbar

Icon	Action	Notes
💾	Save changes you make to the Language Pack.	
⬇	Update the Language Pack with strings from new definitions.	See Refreshing a Language Pack.
⬆	Export the Language Pack to a .tsv file.	See Export a Language Pack.

Icon	Action	Notes
	Select a machine translator and translation options for the Language Pack.	See Using Machine Translation.
	Add a row to your Language Pack.	This feature is useful if you want to pre-translate strings in the Language Pack and apply them to your system as part of the Language Pack.
	Open an Item Details page for a specific string. You can then add or modify the target value and comments.	See Editing a String Row.
	Delete selected rows from the Language Pack.	When you delete a row, translations are not applied for the target culture. You can only delete unlocked rows. **Tip:** If you delete a row and later want to restore it, you can update the strings from the definition. See Refreshing a Language Pack.
	Undo the last change in the Editor.	
	Redo the last change in the Editor.	
	View the history of changes to strings for the current editing session.	See Working with String Change History.
	Find source and target strings and replace target strings.	See Finding and Replacing Strings.
	Copy the source value for selected strings to the target value.	
	Lock selected rows so they cannot be edited or deleted.	
	Unlock selected rows so they can be edited or deleted.	
	Set the status for selected string rows.	See Setting Status for Strings.

Icon	Action	Notes
▼ ‧	Apply a pre-defined filter to the Editor. Choices are: • Hide locked items • Hide items not containing whole words • Hide items containing Expression Tokens and Rich Text strings • Show only items containing Token Expressions • Show only items containing Rich Text strings Select **Clear Filter** to remove the filter applied to the strings list.	To create a custom filter, see Creating a Custom Filter for the Language Pack Editor.
↑	Select the previous row.	
❓	Toggle between the row view and the detailed view.	
↓	Select the next row.	
ⓘ	View statistics for the Language Pack.	See Viewing Language Pack Statistics

Opening the Language Pack Editor

To open the Language Pack Editor:

1. Do one of the following:
   - In the CSM Administrator main window, select the **Globalization** category, and then select **Manage Language Packs**.
   - From a Blueprint or mApp Solution, select **Managers > Language Packs**.
2. Select a Language Pack bundle, then select a Language Pack from the context menu.
3. Select **Edit**.

Editing a String Row

You can edit each string row directly in the Language Pack Grid by providing target values and comments.

You can also edit string rows on the **Item Details** page, which provides more detail about each row.

To open the Item Details page:

1. Open the Language Pack Editor.
2. Select a string row, and then click **Edit**.
3. The **Item Details** page opens. From here, you can:
   - View status information for the string. See Setting Status for Strings.
   - See who validated a string and when.
   - See who locked a string and when.
   - See the source value and change the target value, if the string is unlocked.
   - Provide comments for a string.
4. Click **Update** to apply your changes.

Translating Plain Text Associated with Tokens

Use the Language Pack Editor to translate or move plain text in strings that contain Tokens.

Tokens are dynamic values that are handled by the system, so the Tokens themselves do not need to be translated. Text associated with a Token can be translated and its location in the string can be changed, however.

Note: You can translate text before or after the Token, but not in both locations. When text is added before and after a token, the translation is not applied.

To translate text associated with Tokens in a Language Pack:

1. Open the Language Pack Editor.
2. From the toolbar, select the Filter icon, and then click **Show only items containing Token Expressions**.
3. Double-click a row in the Editor.
   Tokens are shown as disabled text in the Source Value box. Translatable text is showed as editable text.
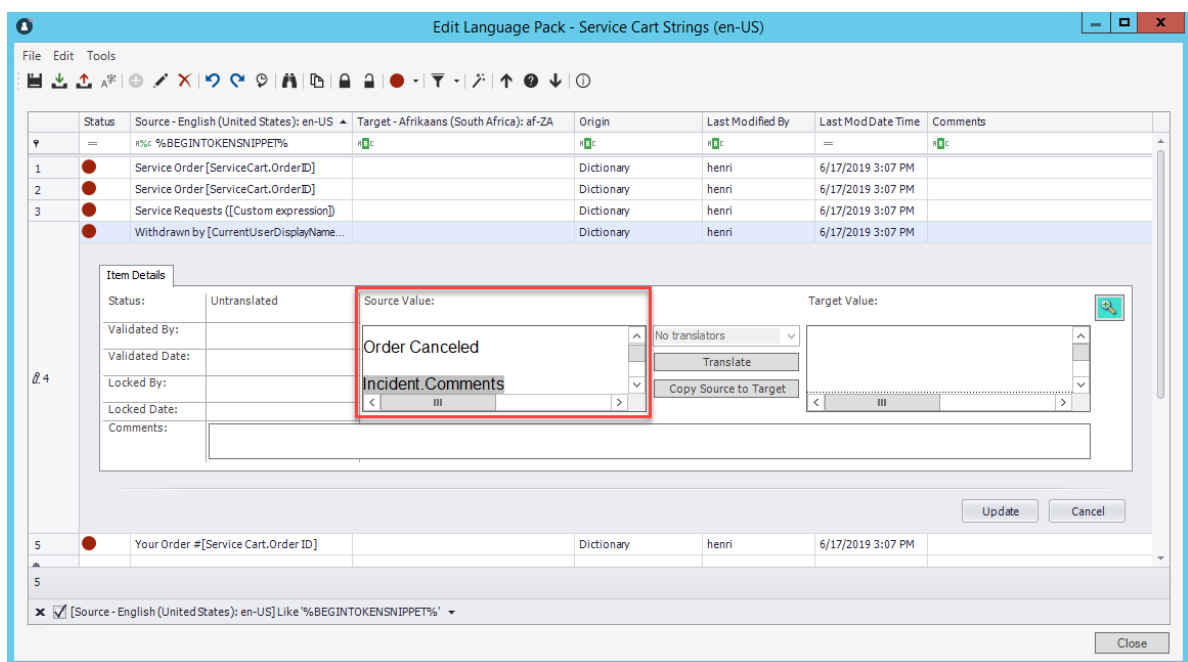
4. Click **Copy Source to Target**, and then translate the editable portion of the string.
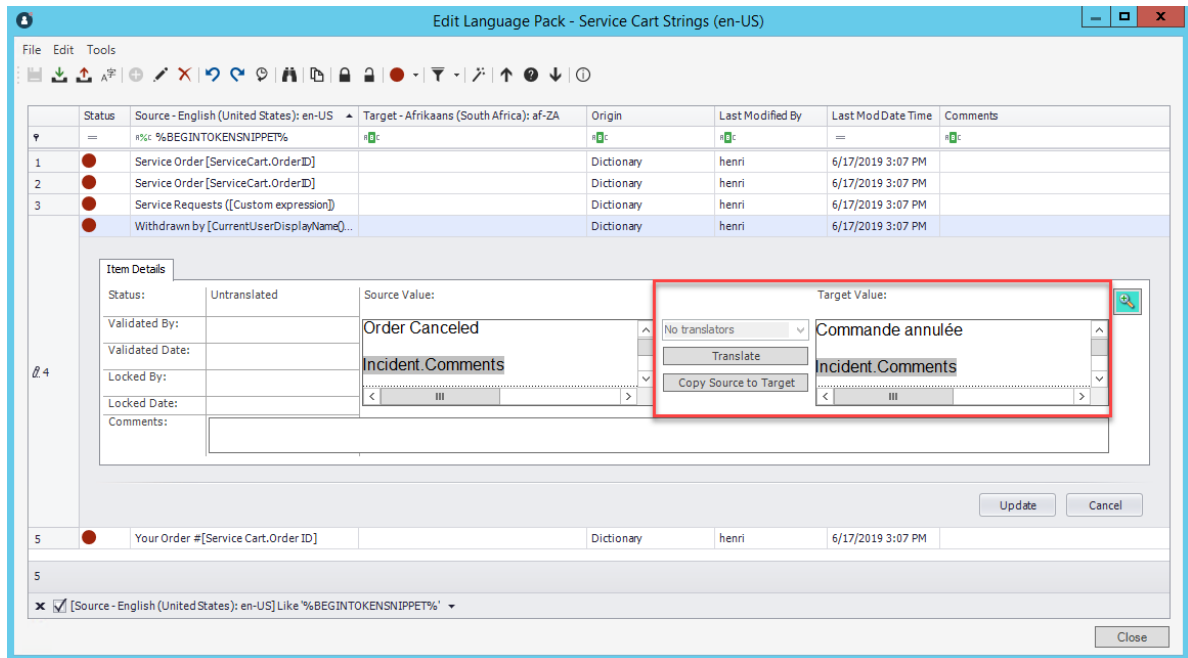
5. Click **Copy Source to Target**, and then click the Expand icon (![Expand icon]).

6. Translate and move plain text in the string as needed, and then click **OK**.

7. Click **Update**.

Translating Rich Text Strings

Use the Language Pack Editor to translate or format Rich Text strings.

Strings that use Rich Text formatting can be translated as long as the formatting elements are left intact.

1. Open the Language Pack Editor.
2. From the toolbar, select the Filter icon, and then click **Show only items containing rich text strings**.
3. Double-click a row in the Editor.
   Depending on the string, the Source Value box shows text, formatting, and Tokens. Tokens should not be modified or deleted.

4. Click **Copy Source to Target**, and then click the Expand icon ( ).
   The Rich Text Editor opens.
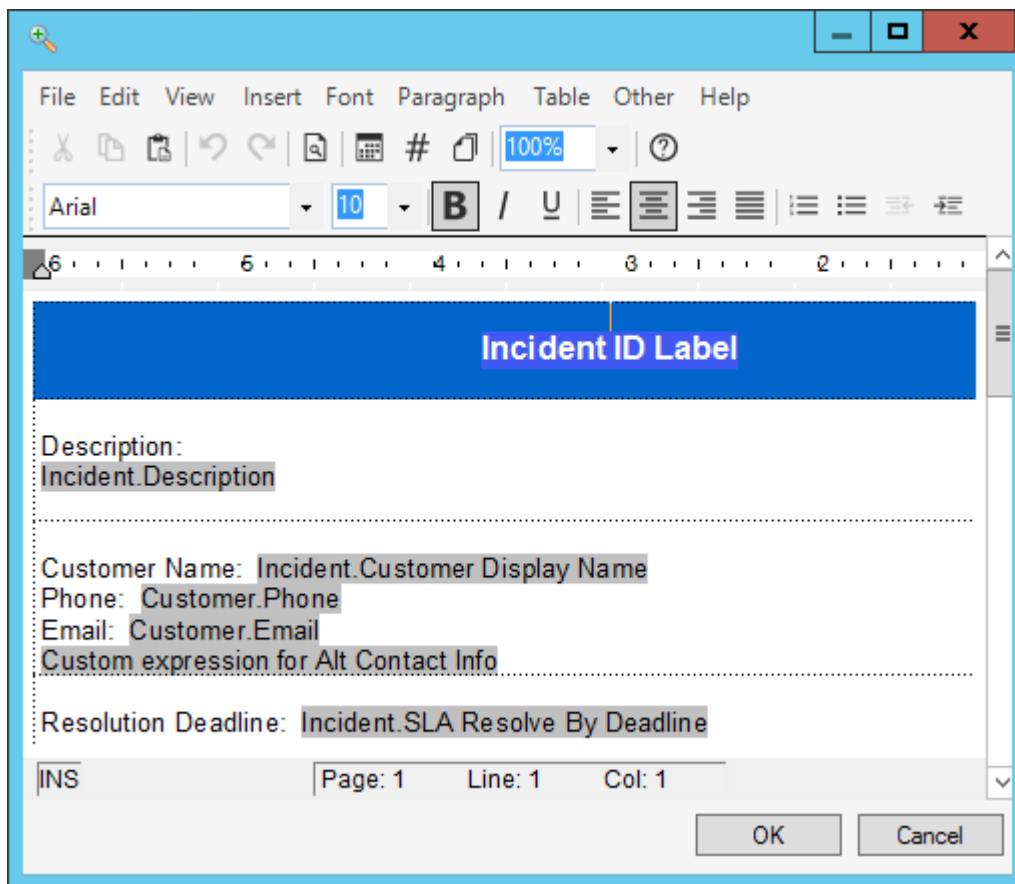
5. Use the Editor to translate and format editable text, and then click **OK**.
6. Click **Update**.

Setting Status for Strings

As you translate strings, you may want to apply a status to each string to help manage the effort, especially if multiple Users participate in translations.

To apply a status to strings:

1. Open the Language Pack Editor.
2. Select one or more strings in the Grid.
3. From the toolbar, select one of these status values:

Icon	Status
●	**Untranslated** Set by default for new items in a Language Pack.
●	**Translated** Translation is complete, but not reviewed or validated. When you add a value to the Target column, this status is set automatically.
●	**For Review** Translation is ready for review.
●	**Validated** Translation is complete and has been validated.
●	**Validated-preferred** If you have duplicate strings in the target language, set one string to this status to ensure the translation is always used for the string.

Refreshing a Language Pack

You can update the strings that have been added or changed since the Language Pack was created. This enables you to easily manage translations over time as your content changes or as you upgrade CSM.

Examples:

- If you add new Fields to a Business Object included in a Language Pack with a content scope, use the refresh feature to add strings for that field.
- If you upgrade to a new version of CSM, use the refresh feature to update platform strings that were added or modified.

To update strings in a Language Pack:

1. Open the Language Pack Editor.

2. Select the Update Language Pack icon ( ).
   The **Update Language Pack** dialog opens.

3. Select one of the following options:
   - **Add and Update Existing Items**

      Select this option to update your Language Pack with new strings for the Language Pack scope and with strings that have been updated in your target language since the Language Pack was created.

      - **Include Updating Items with a Translated Status**

         Select this option to overwrite strings that have a status of "translated" with the strings stored in the definition.

      - **Include Updating Items with a Validated or Validated Preferred Status**

         Select this option to overwrite strings that have a status of "validated" or "validated-preferred" with the string stored in the definition.

      Note: Translated strings are never replaced by empty strings.

   - **Only Add New Items**

      Select this option to only update your Language Pack with new strings for the Language Pack scope.

A pop-up window opens and shows the results of the update.

Using Machine Translation

You can use a configured machine translator to translate stings in a Language Pack. You can choose to translate a set of strings or all strings in a Language Pack.

> **Note:** To quickly translate selected strings in the Language Pack Editor, use the Quick Translation feature. See Using Machine Translation.

1. Verify that you have a machine translator configured for your system. See Configure Machine Translators.
2. Open the Language Pack Editor.
3. If you want to translate a set of strings, select them in the Grid.
4. Click the **Translator** icon (A字).
   The **Translate Language Pack** dialog opens.
5. Select the following options:

Option	Description
Translator	Select the translator configured for your system.
Translate All	Select this option to translate all of the strings in the Language Pack.
Translate Selected Items	Select this option to translate the strings you selected before you opened the **Translate Language Pack** dialog.
Only translate items that have not been translated	Select this option to use the machine translator for strings with an "untranslated" status or strings with empty target rows.
Do not translate locked items	Select this option to have the machine translator skip locked items.
Maximum number of words per string	Select this option to limit the machine translation to strings under a specified character size. This enables you to use machine translation for short strings. You can then manually translate strings with a larger number of characters.

6. Click **OK**.
   Strings in the Target column are translated based on selections made in the **Translate Language Pack** dialog.

Using Quick Translation

Use the Quick Translation feature to quickly translate selected strings in the Language Pack Editor. Quick translation uses the options defined in the **Translate Language Pack** dialog.

To use Quick Translation:

1. Verify that you have a machine translator configured for your system. See Configure Machine Translators.

2. Open the Language Pack Editor.

3. In the Language Pack Editor, select strings you want to translate.

4. Right click, and then select **Quick Translation Selected Items With**, and then select your configured machine translator.
   The selected items are translated into the language defined for the Language Pack.

Working with String Change History

You can view the history of changes to strings for the current editing session. All changes are shown, except those made by machine translators.

You can also use the **Change History** dialog to:

- Undo and redo changes made in the current editing session.
- Revert selected strings to their original state.
- Go to a selected item in the Language Pack Editor strings list.

To open the Change History dialog:

1. Open the Language Pack Editor.
2. Modify strings in the strings list, and then save your changes.
3. Click the **Change History** icon (⊙).
   The **Change History** dialog opens and shows the index number for each change, each source string, and each change made during the current editing session.

   Tip: Move the Change History dialog to a position where you can easily see changes you made to strings in the Language Pack Editor Grid.

4. Use the following options to manage changes:

Option	Description
Go to Selected Row	Click this icon to open the selected string row in the Language Pack Editor Grid.
Revert Changes	Click this icon to revert all changes made to a string past the point where the string is selected in the changes list. This enables you to selectively revert changes to a string without losing all changes.
Undo Last Change	Click this icon to revert the last change made to a selected string.

Option	Description
Redo Change	Click this icon to redo a change for a selected string.

5. Click **OK**.

Finding and Replacing Strings

You can search for strings in a Language Pack and replace strings in the target language as needed.

To find and replace strings in a Language Pack:

1. Open the Language Pack Editor.

2. Click the **Find** icon ( ).
   The **Find and Replace** dialog opens.

   > **Note:** To find and replace strings, your cursor must be placed in a Target row when you click the **Find** icon.

3. Use the following options to find and replace strings:

Option	Description
Find What	Provide the text you want to find.
Replace and Replace With	If you select the **Target** segment option, you can select the **Replace** check box and specify replacement text.
Segment	Choose to search for **Source** or **Target** strings.
Only Whole Words	Select this check box to limit the search to whole words only.
Match Case	Select this check box to limit the search to words that match the case of the text you want to find.
Find Previous	Click this button to find text that occurs before the string selected in the Language Pack Grid.
Find Next	Click this button to find the next occurrence of the text.
Replace	Click this button to replace the next occurrence of the text.
Replace All	Click this button to replace all occurrences of the text.

Viewing Language Pack Statistics

You can view the following information about strings in a Language Pack:

- Number of rows
- Source word count
- Number of untranslated strings

To view Language Pack Statistics:

1. Open the Language Pack Editor.
2. Click the **Strings Statistics** icon (ⓘ).
3. Review statistics for the current view based on the applied filter and for the entire Language Pack.

Creating a Custom Filter for the Language Pack Editor

You can create a custom filter to help limit the strings list in the Grid to a manageable set. You can use the Filter Editor to add a condition expression, or you can use the filter icon above each visible column to modify the existing filter.
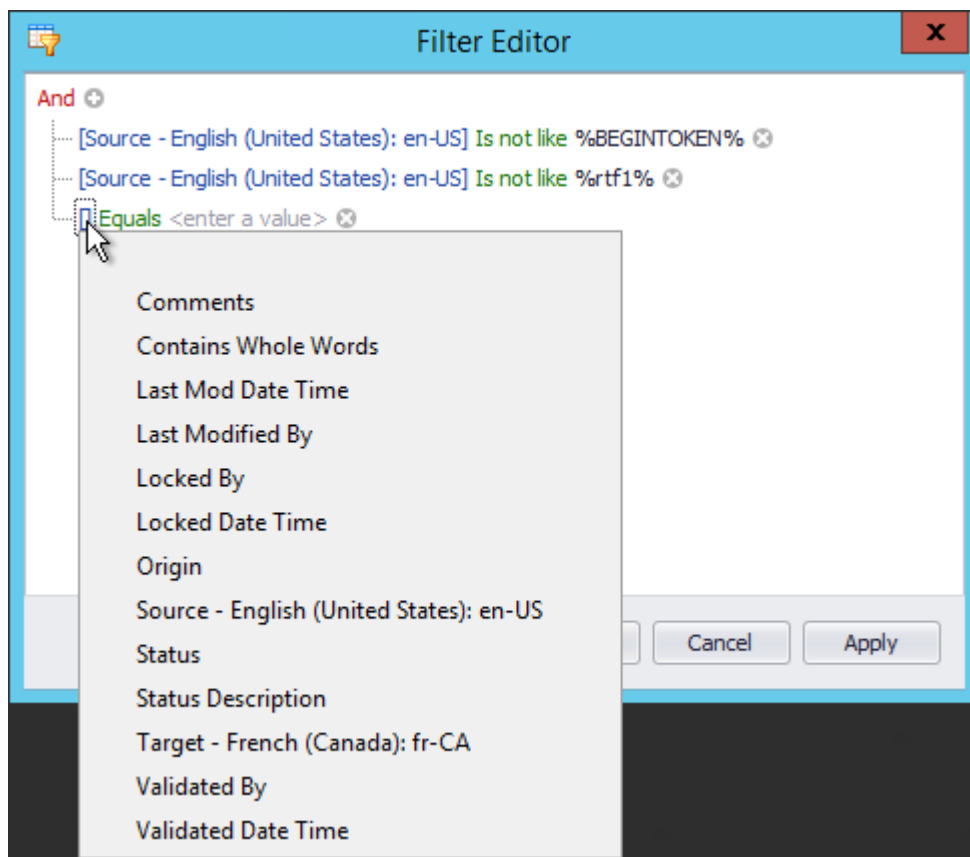
Use the Filter Editor

To create a custom filter using the Filter Editor:

1. Open the Language Pack Editor.
2. Click **Edit Filter** in the bottom right corner of the Editor.

   The **Filter Editor** opens with the filter set from the Filter option ( ) on the toolbar.
3. Click **And** to add, change, or remove operators, conditions and groups.
4. Click the **Plus** sign to add a condition and value.

5. Add as many conditions as needed to filter the strings to the list you need.
6. Click **Apply**.

Use the Filter Icons

To customize a filter using Filter icons:

1. Hover over a column header in the Language Pack Editor, and then click the Filter icon.

2. Choose an appropriate filter based on the type of data in the column. For example, for the Source column, select the Text Filters tab, then set the filter to show source values that end with "ing."
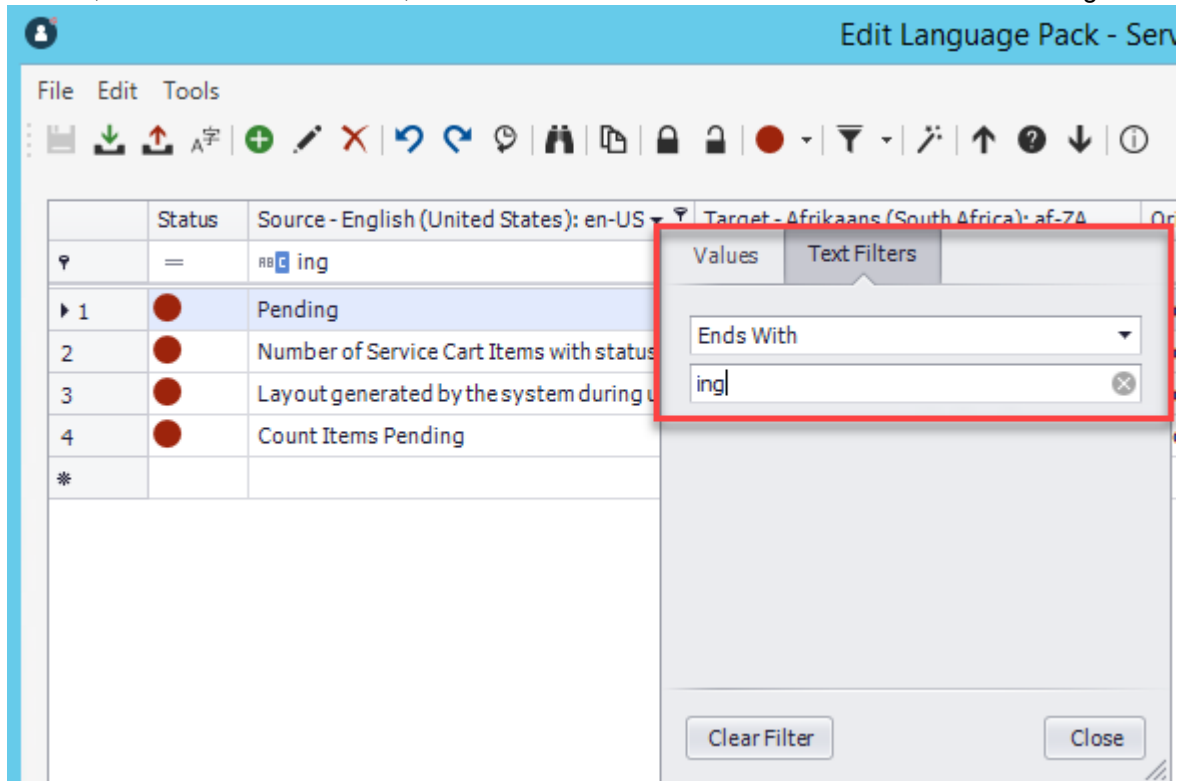
Changes are cumulative; each change you make using filter icons is added to the **Edit Filter** dialog.

Apply a Language Pack

Use the **Apply a Language Pack** wizard to apply translated strings in a Language Pack bundle to a Blueprint that you can publish immediately or save and publish later. The Blueprint only includes definitions modified by the Language Pack.

Once a Blueprint containing a Language Pack bundle is published, Users will see strings in the language associated with the Language Pack bundle based on their selected culture and their security settings. For more information, see Configure Security for Cultures.

To apply a Language Pack bundle:

1. Use one of these methods to open the wizard from CSM Administrator:
   - In the Main Window, select the **Globalization** category, and then select **Manage Language Packs**.
   - From a Blueprint or mApp Solution, select **Managers > Language Packs**.

   > **Note:** You can also apply a Language Pack to any definition or one or more Form controls. See Applying Language Pack Bundles to Definitions or Form Controls.

2. Select a Language Pack bundle, and then select **Apply**.
   The **Apply Language Pack** wizard opens.
3. Select **Next**.
   The **Identify Scope** page opens and the scopes applied to the Language Pack when it was created are selected by default.
4. (Optional) Change the scope if you want to apply translations to identical strings in your Language Pack to a different scope. See Select a Language Pack Scope.
5. Select **Next**.
   If you chose to apply the Language Pack bundle to specific Business Objects, the **Identify Specific Business Objects** page opens and the Business Objects chosen for the Language Pack when it was created are selected by default.
6. (Optional) Select additional Business Objects and Views if you want to apply translations to identical strings in different Business Objects and Views.
7. Select **Next**.
   If you chose to apply the Language Pack bundle to Lookup Tables, the **Identify Specific Lookup Tables** page opens and the Lookup Tables applied to the Language Pack when it was created are selected by default.
8. Select the Lookup Tables to apply translations to.
9. Select **Next**.
   If you chose to apply the Language Pack bundle to Portal content strings, the **Identify Portal Sites** page opens and the Sites applied to the Language Pack when it was created are selected by default.
10. (Optional) Select different Sites to apply translations to.
11. Select **Next**.
    The **Select Strings to Update** page opens.
12. Choose one of these options:

◦ **Update All Strings**

Select this option to update and overwrite all strings in the system, including strings you may have already translated.

◦ **Only Update Strings Without Translations**

Select this option to only update strings that do not have translations applied.

Note: If you are applying a Language Pack with a Lookup Table scope and you copied neutral-culture values to culture-specific Fields, select the Update All Strings option to ensure that translated values are correctly applied.

The **Locked Strings File** page opens.

13. If you have created locked strings lists that prevent the translation of strings, you can select a one or more lists or no locked string lists.

14. Select **Next**.

15. On the **Summary** page:
    ◦ Review selections you made with the wizard.
    ◦ Select the **Log Change** check box to view or save a list of translation changes that will be made once you publish the Blueprint that contains the Language Pack. See Log Translation Changes in a Language Pack.

16. Select **Back** to change your options; select **Finish** to complete the wizard.

A Blueprint that contains the applied Language Pack opens. You can publish the Blueprint or save it and publish it at a later date.

Related concepts

Create a Language Pack

Using Language Packs to Translate Portal Strings

Managing Locked Strings

Publish a Blueprint

Related tasks

Configure Localization Support for Lookup Tables

Log Translation Changes in a Language Pack

You can view and save translation changes for a Language Pack. The log contains changes to Lookup tables, definitions, Portal strings, and platform strings. This enables you to understand the impact of your translations once you publish a Blueprint that contains the Language Pack.

You can choose to log changes from the **Summary** page of the Apply Language Pack Wizard or from individual definitions or Form Controls.

If you select the Log Changes check box when you apply a Language Pack, the log opens in a separate window. Click **Save to File** to save the log file.

Related concepts
Publish a Blueprint
Related tasks
Apply a Language Pack
Applying Language Pack Bundles to Definitions or Form Controls

Export a Language Pack

To ease large translations, translation reviews, and translations completed by an external vendor, you can export a Language Pack to a tab-delimited (.tsv) file.

Vendors can either import the .tsv file into their translation tool or convert the file to a format supported by their translation tool.

Note: Tokens and Rich Text strings are included in the exported file but should always be translated in the Language Pack Editor. For more information, see Translating Plain Text Associated with Tokens and Translating Rich Text Strings.

To export a Language Pack:

1. In the CSM Administrator main window, select the **Globalization** category, and then select **Manage Language Packs**.
2. Select a Language Pack bundle, and then click **Export**.
   The **Export Language Pack** dialog opens.
3. Select the following file options as they apply:

Option	Description
Include Header Row	Select this check box to include a header in the exported file. If you do not include metadata, the header includes the source value and the target value.
Include Metadata	Select this check box to include metadata, such as origin, validation, and lock data, in the exported file. Headers for metadata are included if you select the **Include Header Row** check box.

4. Select one the following export options:

Option	Description
All strings	Select this option to export all strings in the Language Pack.
Translated strings	Select this option to export only translated strings included in the Language Pack.
Untranslated strings	Select this option to export only untranslated strings included in the Language Pack.
Strings marked for review	Select this option to export only strings that need to be reviewed.

5. Click **OK**.
6. Provide a file name and location for the exported Language Pack.

7. Click **Save**.

Once the exported file has been translated, you can import the Language Pack back into CSM. See Import a Language Pack.

Related concepts
Guidelines for Translating .tsv Files
Related tasks
Import a Language Pack

Guidelines for Translating .tsv Files

Strings files are exported in tab-delimited (.tsv) format. You must follow specific guidelines for modifying these files to successfully import translations into CSM.

- Each string is exported in this format:

  ```
  (untranslated text) tab (translated text) tab EOL
  ```

  Add translations to the "(translated text)" portion of each string only. Do not modify other portions of the string.

- If you do not use a translation tool to translate the strings file, use Microsoft Excel to help you adhere to the tab-delimited format.

- The .tsv file must be encoded as UTF-8. For steps on viewing and setting the encoding, refer to your editor's documentation.

- Do not modify the first line of the exported file.

- Tokens are exported in this format:

  ```
  $$(TOKEN NAME)$$
  ```

  Do not modify text between dollar signs.

- Rich Text strings are included in the exported file but should always be translated in the Language Pack Editor.

Related tasks
Export a Language Pack
Import a Language Pack

Import a Language Pack

You can import a Language Pack that is in a tab-delimited (.tsv) file. For best results, the .tsv file should originate as a Language Pack that you exported from CSM and then modified.

To import a Language Pack:

1. In the CSM Administrator main window, select the **Globalization** category, and then select **Manage Language Packs**.
2. Select **Import**.
   The **Import Language Pack** dialog opens.
3. Select the ellipsis to navigate to the file you want to import.
4. Select the **Source Culture** for the Language Pack you are importing.
5. Select the **Target Culture** for the Language Pack you are importing.
6. Provide a name and description for the Language Pack.
7. Optionally, select the **Merge with existing Language Pack** check box. When you select **OK**, the **Merge Language Pack** wizard opens after the import is complete.
   See Merge Language Packs.

Merge Language Packs

You can merge two Language Packs that have the same language and culture pair. This enables you to focus translation efforts on specific areas, and then consolidate translations into a single Language Pack.

To merge two Language Packs:

1. In the CSM Administrator main window, select the **Globalization** category, and then select **Manage Language Packs**.

2. Select a Language Pack bundle, and then click **Merge**.
   The **Merge Language Pack** wizard opens.

3. Click **Next**.
   The **Identify Language Pack** page opens.

4. Select the Language Pack to merge into.

5. Click **Next**.
   The **Identify Merge Options** page opens.

6. Select an option to handle duplicate values from the source language:
   ◦ Select which Language Pack to take target values from.

   ◦ Select the **Allow me to choose with targets to keep** to control how duplicate or conflicting values are handled during the merge.

7. Optionally, select the **Delete the Language Pack that is being merged from** check box. This deletes the Language Pack when the wizard is complete.

8. Click **Next**.

9. If you selected the **Allow me to choose with targets to keep** option on the previous page, the **Handle Duplicate Source Values** page opens if the following types of duplicate values are found.

Language Pack #1	Language Pack #2	Merge Result
Source value of "AAA" and target value of "BBB"	Source value of "AAA" and target value of "CCC"	Duplicate list to choose from; choose either "BBB" or "CCC"
Multiple source values of "AAA" and multiple different target values.	No duplicates.	Duplicate list populated with source "AAA" and a choice of all target values; choose none or multiple values.

> **Note:** Empty target values are automatically merged with a source value if one exists in either Language Pack. If not, the blank values are retained for the source and target values.

10. Click **Next**.

11. On the **Summary** page, review the options you selected.

12. Select **Back** to change your options; select **Finish** to complete the wizard.

View Language Pack Properties

You can view the properties for each Language Pack bundle, including target culture, source culture, and scope.

To view Language Pack bundle properties:

1. In the CSM Administrator main window, select the **Globalization** category, and then select **Manage Language Packs**.
2. Select a Language Pack bundle, and then click the **Properties** button.

Managing Locked Strings

You can prevent strings from being translated by locking them. You can then exclude the locked strings when you apply a Language Pack.

For example, you may want to lock your company or product name so that it is not inadvertently translated and applied to your CSM system.

Good to Know

- Certain strings are automatically locked by the system or should not be translated in any system. See the list in Globalization Good to Know.

- For best practices, see Best Practices For Locking Strings from Translation.

- You can create a locked strings list from a Blueprint or mApp Solution. Locked strings lists can only be applied to a Language Pack once a Blueprint has been published or a mApp Solution applied.

- You can lock text strings or use regular expressions to lock strings.

- String lists are case sensitive.

Process for Locking Strings

1. Create a Blueprint or a mApp Solution.
2. Select **Managers > Locked Strings** to open the Locked Strings Manager.
3. Select **Create** to open the Locked Strings List Editor.
4. Provide a name and description for the locked strings list.
5. Select **Add**, and then select one of these string types:
   - **String:** Locks exact strings you specify.
   - **RegEx:** Locks strings based on the regular expression. For example, `Service Catalog| Service Catalogs` locks "Service Catalog" and "Service Catalogs".
6. Select **OK**.
7. Add all strings that you want locked.
8. Select **Save**.
9. Publish the Blueprint or apply the mApp Solution.
10. Apply a Language Pack.
11. Select a locked strings list to prevent matching target strings in the Language Pack from being translated.

Merging Locked Strings Lists

1. Create a Blueprint or a mApp Solution.
2. Select **Managers > Locked Strings** to open the Locked Strings Manager.

3. Select the locked strings you want to merge.

4. Right click, and then select **Merge**.

The lists are merged into a single list.

Related concepts

Create a mApp Solution

Publish a Blueprint

Apply a mApp Solution

Related tasks

Create a Blueprint

Apply a Language Pack

Translating Content Strings On the Fly

When globalization and multiple cultures are enabled for your system, you can translate content strings on the fly as you work with elements. This is useful for maintaining a translated system or for adjusting translations after you apply a Language Pack.

You can translate text strings for Business Object elements, such as Fields and Grids, as you work with Blueprints and mApps in CSM Administrator.

You can also apply Language Packs directly to Form controls. See Applying Language Pack Bundles to Definitions or Form Controls.

Strings for certain elements, such as Stored Queries and Expressions, can be also be translated in the Desktop Client.

To translate content as you work with elements:

1. Use the culture selector to switch to a different culture.
2. Edit elements and translate or modify text strings as needed.
3. Save your changes.
4. Switch to additional cultures and translate the element as needed.

> **Note:** If you have applied translated Language Packs to your system, you may see translated text strings for some elements. You can keep the translations or modify them as needed. If you delete translations, Users will see text for the preferred culture, which serves as a fall-back culture.

Remember to update strings from definitions if you edit a Language Pack that was created before you made on-the-fly changes.

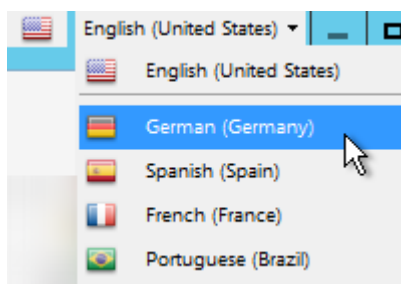# Example: Translating E-mail Templates on the Fly

To translate E-mail Templates on the fly:

1. Open the One-Step Editor.
2. Create or edit a One-Step Action that uses a Send an E-mail Action.
3. Edit the Send an E-mail Action, and then add text for the language selected in the culture selector.
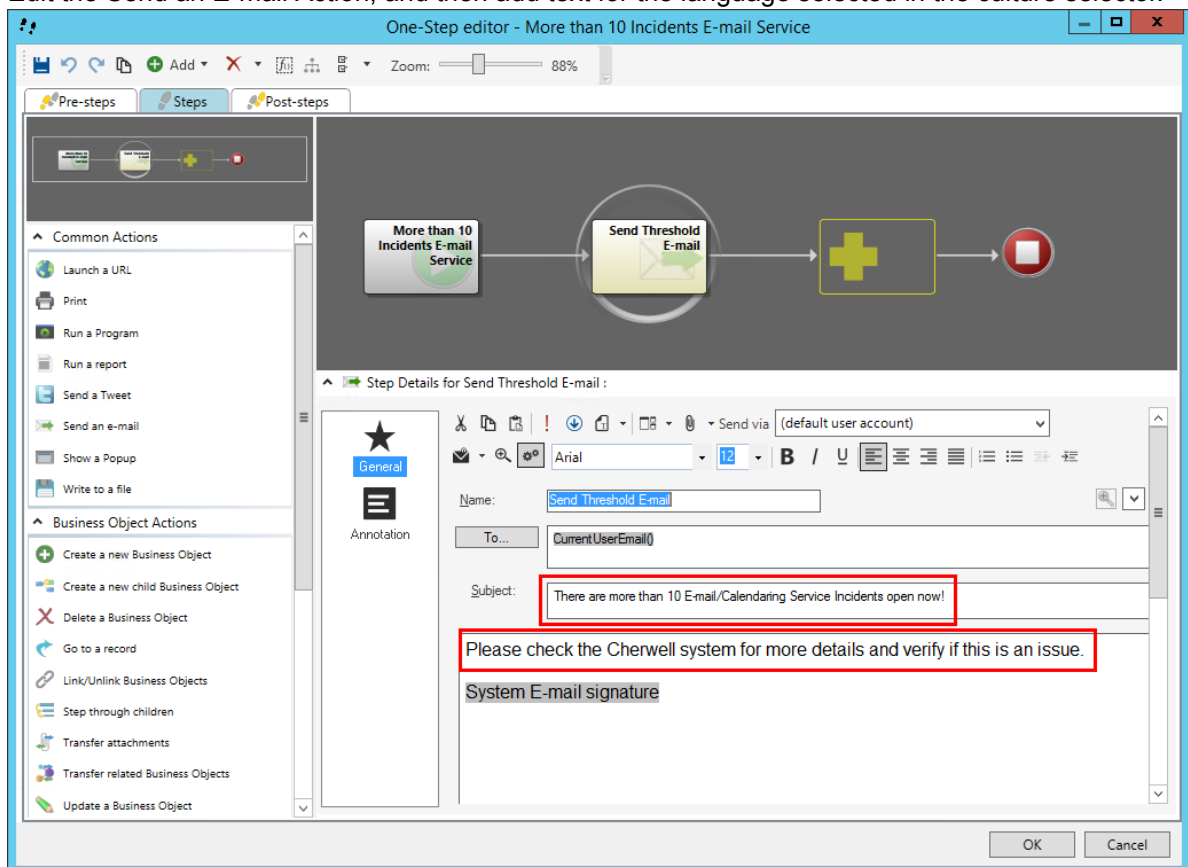
4. Click **OK**.
5. Use the culture selector to switch languages.

6. Edit the One-Step Action and the Send an E-mail Action.

7. Translate text strings for the language you selected in the culture selector.

8. Click **OK**.

9. Repeat as needed for additional cultures.

Related concepts

Open the One-Step Editor

Define a Send an E-mail Action

Example: Translating Expressions on the Fly

The logic for an Expression applies to all cultures, but you can manually translate Expression values for multiple cultures.

To translate Expressions on the fly:

1. Open the Expression Manager.
2. Create or edit an Expression. For this example, create an Expression, and select Case from the **Editor** drop-down.
3. Provide values for the language selected in the culture selector.

4. Click **OK**.

5. Use the culture selector to switch languages.

6. Edit the Expression.
7. Provide values for the language you selected in the culture selector.

8. Click **OK**.

9. Repeat as needed for additional cultures.

Related concepts

Open the Expression Manager

Managing Translations for Individual Definitions

You can perform several localization tasks related to individual definitions from a Blueprint or a mApp Solutionin CSM Administrator.

- **View Translations**

  See Viewing Translations for Definitions and Form Controls.

- **Apply Language Pack Bundles**

  See Applying Language Pack Bundles to Definitions or Form Controls.

- **Delete Translations**

  See Deleting Translations from Definitions.

From a Blueprint, you can also restrict definitions from being localized. See Restricting Translations for Definitions and Removing Translation Restrictions from Definitions.

Viewing Translations for Definitions and Form Controls

You can view translated strings and property information for individual definitions from a Blueprint or a mApp Solution.

You can:

- Use the Item Managers to view translations for definitions, such as One-Step Actions, Stored Values, and Expressions.
- Use the Definition Reviewer to view translations for Forms, Grids, and Form Arrangements.
- Use the Form Editor to view translations for Form control text.

To view translations for a definition:

1. In CSM Administrator, create a Blueprint or mApp Solution.
2. Do one of the following:
   - Select an Item from the **Manager** menu, and then select an item, such as a Stored Value.
   - Open the Definition Reviewer, and then select an item in the definition list.
   - From the Form Editor, select a Form control.
3. Use one of these methods to open the **Translations** dialog:
   - Right-click and select **Localization > View Translations**.
   - Select the Localization icon on the toolbar, and then select **View Translations** (Item Managers and Form Editor only).
4. View the following string definition information for each enabled culture:

Column	Description
Culture	Indicates the string's culture.
Property	Indicates the string's definition property.
Definition Type	Indicates the string's definition type.
Definition Name	Indicates the name of the definition for each string.
Value	Indicates the value for each string. Translations are shown for each culture.

5. Click **OK**.

Related concepts
Managing Controls on Translated Forms
Form Editor
Related tasks
Review Visual Elements for All Business Objects

Restricting Translations for Definitions

You can control which Items can be translated. This enables you to ensure that certain definitions, such as Stored Values, remain in a specific language for all Users.

This option is available when Globalization is not enabled so you can ensure that certain strings are not translated if definitions are shared across systems that may or may not be translated. This option also helps you prepare for translation by enabling you to specify invariant values that you want ignored during a translation effort. For example, you may want to ensure that all organizations in your company are shown in English.
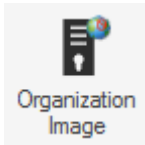
To prevent a definition from being translated:

1. In CSM Administrator, create a Blueprint.
2. Select an Item from the **Managers** menu. For example, select **Managers > Stored Values**.
3. Select an Item, and then you can:
   - Right-click and select **Localization > Do not allow the item to be localized**.
   - Select the Localization icon on the toolbar, and then select **Do not allow the item to be localized**.

   The **Select the Invariant Culture** dialog opens, with all applicable cultures listed.
4. Select the culture that contains values you want shown for the definition for all cultures. This invariant culture is also referred to as a "constant" culture because the values cannot be translated and will therefore not change based on a User's selected culture.
5. Click **OK**.

Definitions that cannot be translated include a Localization stamp in the upper right corner.


Organization Image

Removing Translation Restrictions from Definitions

You can remove translation restrictions from definitions that have restrictions defined, but you must select a culture whose value can be copied to all cultures. The invariant value typically comes from the culture that was selected when the restriction was placed on the definition. (See Restricting Translations for Definitions.)

To remove translation restrictions from a definition:

1. In CSM Administrator, create a Blueprint or mApp Solution.
2. Select an Item from the **Managers** menu. For example, select **Managers > Stored Values**.
3. Select a definition that has a Localization stamp in the upper right corner. This indicates that translations are restricted for the definition.
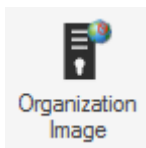
4. You can then:
   ◦ Right-click and select **Localization > Allow item to be localized**.
   ◦ Select the Localization icon on the toolbar, and then select **All item to be localized**.

   The **Select the Invariant Culture** dialog opens, with all applicable cultures listed.
5. Select the culture from which to apply an invariant value. This copies the invariant value from the selected culture to all cultures.
6. Click **OK**.

You can now apply Language Packs to translate the definition values.

Applying Language Pack Bundles to Definitions or Form Controls

You can apply one or more Language Pack bundles directly to one or more definitions or Form controls.

Translations will be applied to strings contained in the definition or control, but not to strings referenced by the definition or control. To see which strings will be translated, you can view the strings before applying translations.

You can:

- Use the Item Managers to apply Language Pack bundles to definitions, such as One-Step Actions, Stored Values, and Expressions.
- Use the Definition Reviewer to apply Language Pack bundles to Forms, Grids, and Form Arrangements.
- Use the Form Editor to apply Language Pack bundles to one or more Form controls.

To apply Language Packs to definitions:

1. In CSM Administrator, create a Blueprint or mApp Solution.
2. Do one of the following:
    ◦ Select an Item from the **Manager** menu, and then select an item, such as a Stored Value.
    ◦ Open the Definition Reviewer, and then select an item in the definition list.
    ◦ Open a form, and then select one or more form controls.
3. Use one of these methods to open the **Select Language Pack Bundles** dialog.
    ◦ Right-click and select **Localization > Apply Language Pack Bundles**.
    ◦ Select the Localization icon on the toolbar, and then select **Apply Language Pack** (Item Managers and the Form Editor only).

    Tip: You can apply Language Pack Bundles to multiple definitions from an Item Manager.

    The **Select Language Pack Bundles** dialog opens.
4. Select the Language Pack Bundles to apply to target culture of the selected definitions. You can choose one or more Language Pack Bundle.
5. Select the **Log Change** check box to view or save a list of translation changes that will be made once you publish the Blueprint that contains the Language Pack. See Log Translation Changes in a Language Pack.
6. Click **OK**.

Related concepts
Managing Controls on Translated Forms
Log Translation Changes in a Language Pack
Related tasks
Viewing Translations for Definitions and Form Controls
Review Visual Elements for All Business Objects

Deleting Translations from Definitions

You can delete translations for a selected definition. Translations contained in the definition are deleted, but translations for referenced strings are not deleted. To see which strings will be deleted, you can view the strings in each definition.

You can:

- Use the Item Managers to delete translations for definitions, such as One-Step Actions, Stored Values, and Expressions.
- Use the Definition Reviewer to delete translations for Forms, Grids, and Form Arrangements.

Note: You cannot delete strings for the preferred culture.

To delete translations for definitions:

1. In CSM Administrator, create a Blueprint or mApp Solution.
2. Do one of the following:
   ◦ Select an Item from the **Manager** menu, and then select an item, such as a Stored Value.
   ◦ Open the Definition Reviewer, and then select an item in the definition list.
   ◦ Open a form, and then select one or more form controls.
3. Use one of these methods to open the **Select Translations to Remove** dialog:
   ◦ Right-click and select **Localization > Delete Translations**.
   ◦ Select the Localization icon on the toolbar, and then select **Delete Translations** (Item Managers only).

   The **Select Translations to Remove** dialog opens.
4. Select the culture than contains the translation for the definition.
5. Click **OK**.

Managing Controls on Translated Forms

You can modify the size and location of Form controls for each Adaptive Layout for each Form.

This enables you to use a single Form for all cultures by adjusting the Form for Users of various cultures.

For example, the English text for a Form control may be shorter than the German text for the same control. You can expand the size of the control for German without impacting the size of the control for English.

Modifying Forms for Multiple Cultures

To modify Forms for multiple cultures:

1. In CSM Administrator, create a Blueprint.
2. Create or edit a Form.
3. Use the culture selector to switch to the culture you want to modify for the Form.
   The Form should appear the same for all cultures, except you may have translated strings if you previously translated and applied strings.
4. Modify a control on the Form. For example, move a control or resize it.

The changes you make apply only to the culture where you made the change. To apply changes to multiple cultures, see the following section.

Applying Form Values to Multiple Cultures

To apply Form control size and location settings to multiple cultures:

1. Select a control on a Form.
2. Right-click on the control, and then select **Localization Options > Copy Between Cultures**.
3. You can then:
   - Copy values from one culture to the culture you are currently viewing.
   - Copy values from the current culture to one or more other cultures.
   - Select **Copy size**, **Copy position**, or both.
   - Click **Apply**.

The size and position values for the control are copied to the selected cultures.

Setting Tab Order for Multiple Cultures

You can set tab order, also known as tab stops, for each culture for a single Form. Use the culture selector to select a culture, and then follow the steps in Set Tab Order on a Form.

Related concepts

Form Editor

Create/Edit a Form

Switching Cultures

Related tasks

Applying Language Pack Bundles to Definitions or Form Controls

Optimizing Content for Localization

The Content Optimization Tool assesses your content and makes recommendation for changes to help prepare your content for translation, particularly strings used for Lookup Tables. You can choose to keep the recommended changes or make your own changes based on the tool's assessment.

Before You Get Started

CAUTION: The Content Optimization Tool can potentially make significant changes, including schema changes, to your system. Before you proceed, read this entire topic and follow the steps and guidance provided.

About the Content Optimization Tool

The tool can:

- Convert Validation Lists to Lookup Tables
- Consolidate Lookup Tables
- Upgrade Existing Validated Fields
- Localize Text Fields

Guidelines for Optimizing Content

Follow these guidelines to optimize your content:

1. Always use the Content Optimization Tool in a test environment before you run the tool on your production system.

2. Carefully review each tab and each selected item before you finalize your changes.

3. Always save a log file when you use the tool. This will help you troubleshoot issues you find after you run the tool.
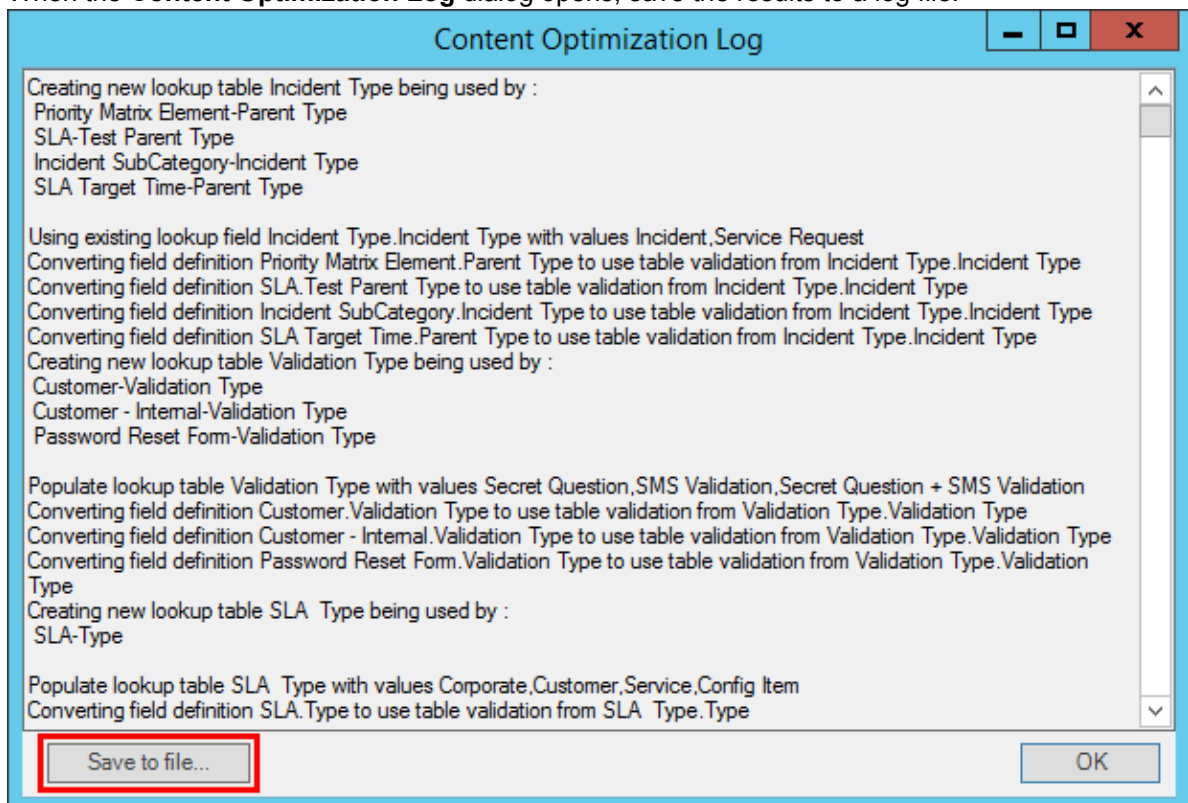
Running the Content Optimization Tool

Important: Read the information in Optimizing Content for Localization before you use the Content Optimization Tool.

To run the Content Optimization Tool:

1. In the CSM Administrator main window, select the **Globalization** category, and then select **Content Optimization Tool**.

2. Select each page tab in the tool and carefully review the recommendations. For guidance, see:
   - Converting Validation Lists to Lookup Tables
   - Consolidating Lookup Tables
   - Upgrade Existing Validated Fields
   - Localize Text Fields

3. Modify recommended selections as needed.

4. Click **OK**.

5. When the **Content Optimization Log** dialog opens, save the results to a log file.

6. Save the results as a Blueprint.

7. Publish the Blueprint.

Important: Do not publish the Blueprint on a production environment until you publish and review the results in a test environment.

Converting Validation Lists to Lookup Tables

The Content Optimization Tool finds all Fields that validate from a list. You can choose to convert these lists to a newly created Lookup Tables or to an existing Lookup Table that has the same values.

Important: Read the information in Optimizing Content for Localization before you use the Content Optimization Tool.

Tip: Using Lookup Tables to validate Fields is best practice for a localized system. For more information, see Globalization Best Practices.

To convert validation lists to Lookup Tables:

1. Run the Content Optimization Tool.
2. Select the **Convert List Expressions** tab.
3. Review the recommended selections and the information in these columns:

Column	Description
Lookup Table	Shows the new Lookup Table that will be created or the existing Lookup Table that will be used to store values.
For Fields	Shows the Fields that will be converted.
Current Validated Fields	If an existing Lookup Table is found, shows the Fields that will be converted to use that object.
Values	Shows the discovered list values.

4. Select or clear these check boxes as they apply:
    ◦ **Convert**

    Converts the Fields listed in the **For Fields** column into a new Lookup Table (shown in the **Lookup Table** column), and adds Fields to the new table to store converted values.

    ◦ **Localize**

    Enables localization support for the new Lookup Table and the newly created Field in the object.

5. Select the **Consolidate Lookup Tables** tab to review options.

Tip: You can also choose to convert all items in the list, convert nothing, localize all, or localize nothing.

Consolidating Lookup Tables

The Content Optimization Tool detects duplicate values across multiple Lookup Table Fields and gives you the option of consolidating them into a single Lookup Table.

For example, if multiple Lookup Tables contain values of "Active," "New," and "Retired," the Content Optimization Tool selects one Lookup Table to store the values and converts the remaining tables to use that Lookup Table.

Important: Read the information in Optimizing Content for Localization before you use the Content Optimization Tool.

To consolidate Lookup Tables:

1. Run the Content Optimization Tool.
2. Select the **Consolidate Lookup Tables** tab.
3. Review the recommended selections and the information in these columns:

Column	Description
Lookup Fields	Shows the Lookup Table and Field that duplicate values will be converted to use.
Lookups	Shows the Lookup Tables and Fields that will be converted.
Values	Shows the duplicate values in the specified Lookup Tables.

4. Select the **Consolidate** check box for each set of duplicate values you want to convert.
5. Select the **Consolidate Lookup Tables** tab to review options.

Upgrade Existing Validated Fields

The Content Optimization Tool can enable foreign key support for validated Fields and apply localization support to Lookup Tables and validation Fields in those objects.

The tool will also increase the size of Fields as needed when localization is enabled for those Fields.

Important: Read the information in Optimizing Content for Localization before you use the Content Optimization Tool.

To upgrade existing validated Fields:

1. Run the Content Optimization Tool.
2. Select the **Upgrade Existing Validated Fields** tab.
3. Review the recommended selections and the information in these columns:

Column	Description
Validated Field	Shows Fields that validate from a Lookup Table.
Validation Business Object	Shows the Business Object that contains the validated Field.
Validation Field	Shows the Fields that are used to validate Fields in the first column.

4. Select or clear these check boxes as they apply:
   - **Foreign Key**

     Enables foreign key support for selected validated Fields.

   - **Localize Validation Business Object**

     Enables localization support for selected Business Objects that contain validation Fields.

   - **Localize Validation Field**

     Enables localization support for selected validation Fields and increases each Field's size as needed.

5. Select the **Localize Fields** tab to review options.

Tip: You can also choose to upgrade all items in the list or upgrade nothing.

Localize Text Fields

The Content Optimization Tool can enable localization support for Text Fields that are not used for validation.

Important: Read the information in Optimizing Content for Localization before you use the Content Optimization Tool.

To enable localization support for Text Fields:

1. Run the Content Optimization Tool.
2. Select the **Localize Fields** tab.
3. Select the **Localize** check box for the Fields for which you want to enable localization support.

   Tip: The text before the period indicates the table name; the text after the period indicates the Field name.

4. Click **OK**.

Translating Strings for Portal Sites

Portal Sites can be easily translated into other languages. Use Language Packs to translate strings for Portal Sites; to translate the Service Catalog, use Language Packs and manually translate records in specific Lookup Tables.

Related concepts

Create a Language Pack

Build and Manage a Portal

Related tasks

Apply a Language Pack

Define Localization Properties for a Site

Using Language Packs to Translate Portal Strings

Use Language Packs to translate strings for Portal Sites. Once you apply translated Language Packs for enabled cultures, you can override startup actions, login actions, and custom Search Widgets for each language.

There are two types of Portal strings:

- **Content**: User-defined labels.
- **Platform**: System resource strings for error messages, toolbar definitions, menus, etc.

To fully translate Portal Sites, you must create at least two Language Packs for each culture: one for content strings and one for platform strings. The content Language Pack can include translations for multiple Sites.

To translate content for CSM Portal Sites:

1. Verify that you have Portal Sites created and configured.
2. Verify that cultures used by your Portal Sites are enabled for your system. If cultures are not enabled, the languages will not be shown in the language selector.
3. Verify security settings for cultures.
4. Create two Language Packs with these scopes for each culture:
    ◦ Portal Content Strings
    ◦ Portal Platform Strings
5. Translate the strings for each Language Pack using the Language Pack Editor or an external vendor.
6. Apply both Language Packs.
7. Verify that the **Show Language Selector on application bar** check box is selected for each translated Portal Site. See Define Localization Properties for a Site.
8. Override the startup action, login action, and custom Search Widget for each Site translation, as needed. See Override Site Options for Each Language.

Related concepts
Create a Language Pack
Configure Security for Cultures
Related tasks
Apply a Language Pack
Define Localization Properties for a Site

Translating Service Catalog Strings

Service Catalog strings presented to Users in the CSM Portal may come from multiple sources, so the process for translating strings involves multiple steps.

The following figure shows the types of strings in the OOTB Service Catalog. The steps explain where strings originate and how to translate them.
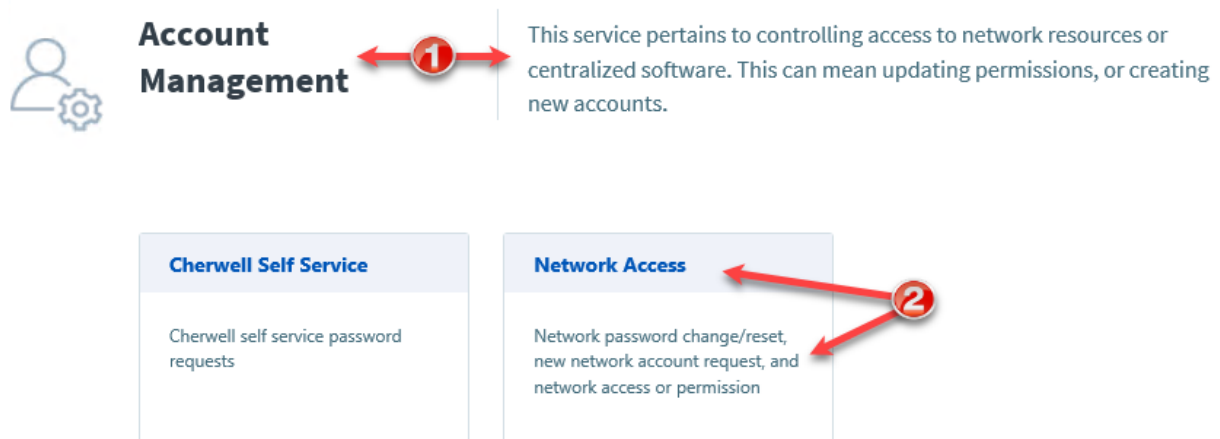
1. Translating the Service Name and Description

The Service Name and Description labels are populated from records in the Service Business Objects.

To translate Service name and description labels:

1. From the CSM Desktop Client or CSM Browser Client, use the culture selector to switch to the culture you want to translate labels to.
   Example: Switch to German.

2. Use a Search feature to locate a Service record.
   Example: From the Quick Search Pane, select the Service Business Object from the drop-down list, and then search for *Account Management*.

3. Open the record, and then manually translate values for the Name and Description Fields.

4. Repeat for each culture.

2. Translating the Service Category Name and Description

The Service category and subcategory name and description labels are populated from values in the Incident Category and Incident SubCategory Lookup Tables.

To translate Service category and subcategory name and description labels:

1. In CSM Administrator, create a Blueprint.

2. Enable localization support for the Incident Category and Incident SubCategory tables.

3. Publish the Blueprint.

4. Create a Language Pack that includes these options:
   ◦ Scope: Lookup Table Data

   ◦ Lookup Objects: Incident Category and Incident SubCategory.

5. Translate the Language Pack.

6. Apply the Language Pack.

7. Repeat for each culture.

Related concepts

Supplied Service Catalog and Cards with Search Styling

About the Service Catalog

Switching Cultures

Related tasks

Configure Localization Support for Lookup Tables
Enable Localization Support for a Lookup Table

Managing the E-mail Monitor for Multiple Cultures

You can use E-mail Monitors with multiple cultures to create or modify records based on specific languages. For best results, use a culture-specific email account for each E-mail Monitor.

To use E-mail Monitors with multiple cultures:

1. Create an E-mail Monitor for each culture that is enabled for your system.
2. Select the applicable culture for each E-mail Monitor.
3. Select a culture-specific email account for each E-mail Monitor.

4. Select the **Monitors** page, and then verify or modify rules to accommodate translations in your system. For example, verify that strings for One-Step Actions that run based on the rule have been translated.

Configuring Record Translation

Configure record translation to translate Fields in Business Object Records using a translation Web Service, such as the Google Translate API. For example, enable a technician to translate a localized Incident description to English. Leveraging a translation Web Service allows the translation to take place directly in CSM so that translated text is stored in the Business Object Record.

For this procedure, some experience with designing Forms and One-Step Actions is highly recommended. Work with your system administrator if your CSM experience is limited.
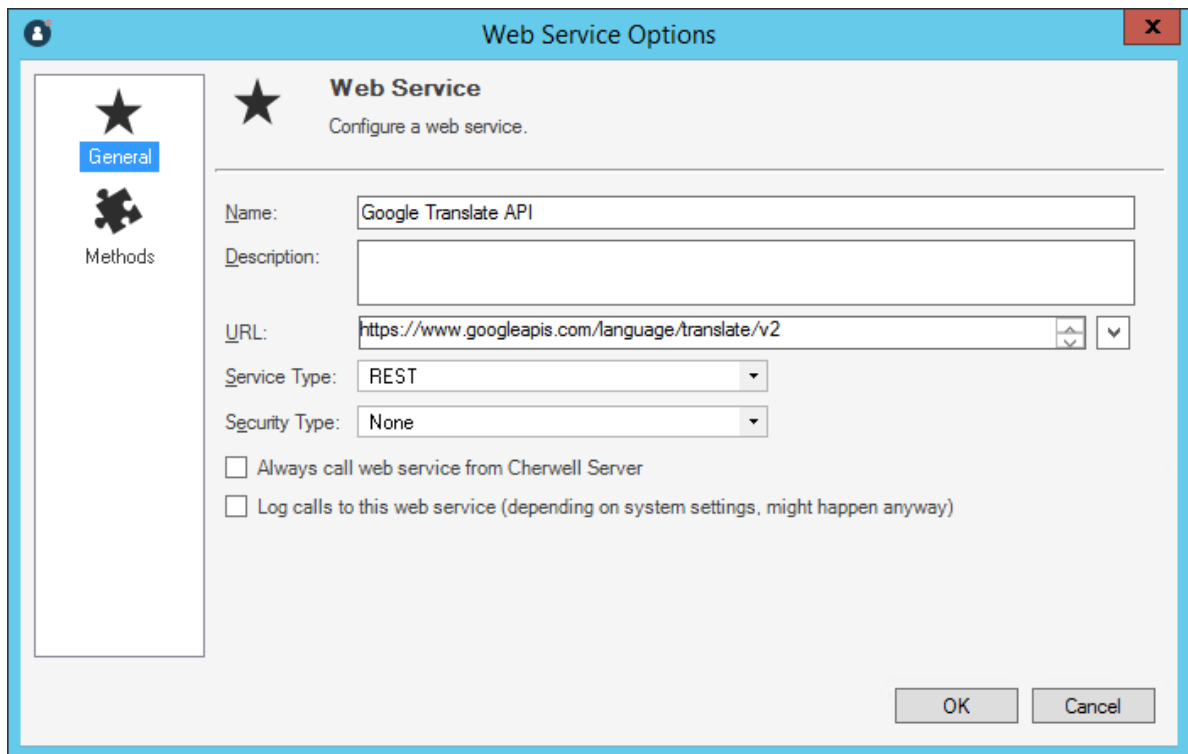
Follow this general process to configure record translation:

Task	Notes
1. Configure the translation Web Service.	See below.
2. Configure the Business Object Form with Fields for translation.	See below.
3. Configure the One-Step Action to perform the translation.	See Configure a Translation One-Step Action.

Configure the Translation Web Service

To configure the translation web service:

1. Verify that you have an API key for your selected translation service.
2. In CSM Administrator, create a new Blueprint.
3. Open the Web Services Manager, and select the Create New button ⊕.
4. Define the General properties for the Web Service. For more information about defining General properties and Methods for a Web Service, see Set Up a Web Service.

5. Define a translation Method for the Web Service.

6. Save and publish the Blueprint.
   The translation Web Service is now available in the system.

Configure the Form and Fields for Translation

To configure the Business Object Form with Fields for translation:

1. In CSM Administrator, create a new Blueprint.

2. From the list of Business Objects, select the Business Object to be configured for translation. For example, select Incident.

3. Select **Edit Business Object.**
   The Business Object Editor opens.

4. Create or edit Fields for the translation inputs and outputs. For example, navigate to the Business Object Editor for Incident and create a text Field called Translated Description to display the translated text on an Incident Form.

5. Return to the Object Manager and select **Edit form.**
   The Form Editor opens. Edit the Form to facilitate translation. For example, add the Translated Description Field next to the Description Field.

6. Create a One-Step Action to perform the translation in the Business Object Record. Refer to Configure a Translation One-Step Action.

7. Save and publish the Blueprint.

Configure a Translation One-Step Action

Verify that your translation Web Service is set up in the Web Services Manager and that you have an API key for the service.

1. Open the One-Step Manager, and verify that the association is set to the Business Object to be configured for translation. For example, select **Association>Incident**.

2. Click **Create New**.

3. Add a **Call a Web Service** Action to the Designer Board.

4. With the Call a Web Service Action selected, in the General properties, click the ellipses button next to **Service**.
The Web Services Manager opens. Select your translation Web Service and then click **OK**.

5. Check the box next to **Store result as: Call a web service result**.
This stores the translated text as a variable.

6. In the Method properties, set the parameter values.
For example, if using the Google Translate API, set the following parameters:

Parameter	Value
q (Endpoint Parameter)	The Field that contains the text to be translated, such as **Incident.Description**
target (Endpoint Parameter)	The target language for the translation, such as **en** for English
key (Endpoint Parameter)	The API key

7. Add an **Update Business Object** Action to the Designer Board.

8. In the General properties, check the box to **save Business Object after action**.
The Business Object Record will be saved each time the One-Step Action is run.

9. In the Fields properties, select the Field that contains the translated text and choose **Template** from the available options. Right-click in the white space and select **Variables>Call a web service**

result. For example, expand Incident and set the Translated Description Field.
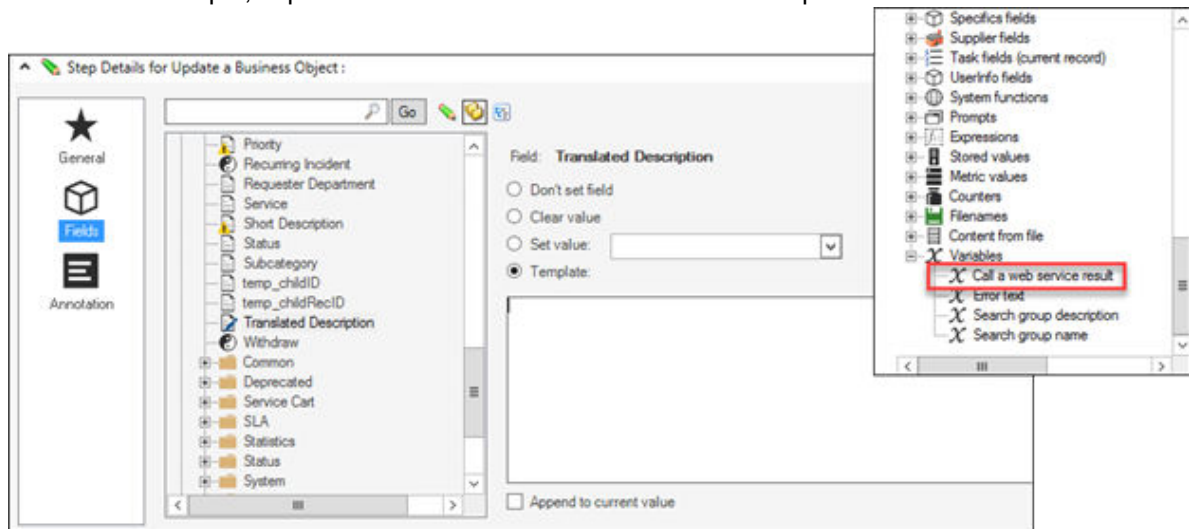
The Field is now set to the variable that contains the translated text.

10. Optional: Right-click**call a Web Service result** and select **Modifiers** to modify the value of the variable. For example, if using the Google Translate API, the JSON response includes other information in addition to the translated text. Modify the value so that only the translated text is displayed in the Field.
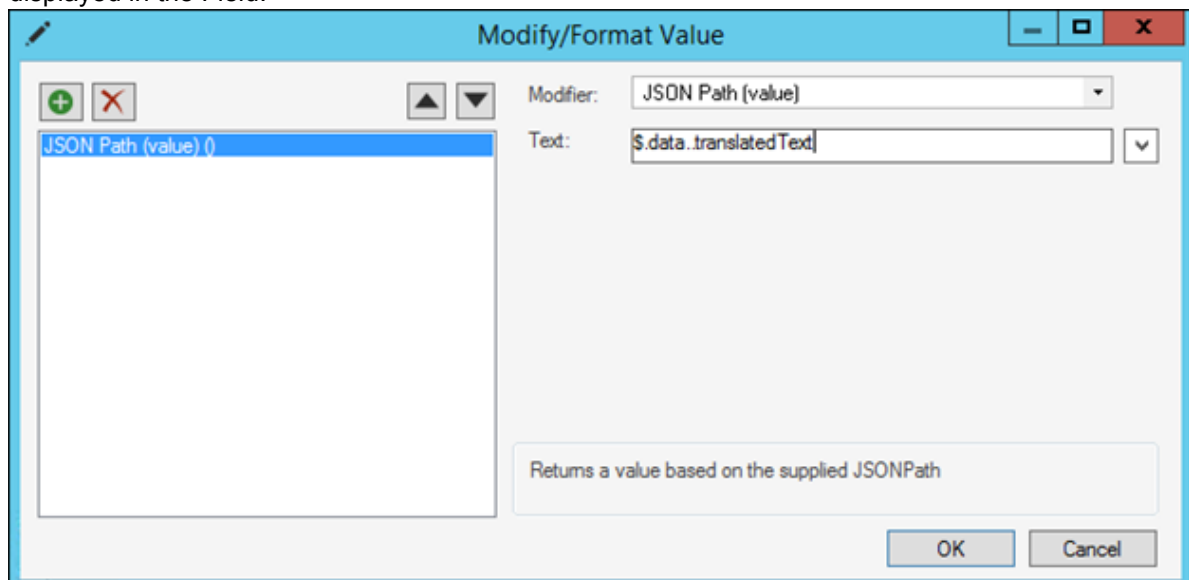
11. Optional: Define an automatic action so that the translation One-Step Action is executed automatically when the Business Object is saved. See Define Automatic Actions for a Business Object

Applying Cultures to mApps

You can apply cultures to mApp Solutions if multiple cultures are enabled and you have applied Language Packs that include translations for the enabled cultures.

The enabled cultures are included with the mApp® Solution, along with translations for definitions included in the mApp Solution.

To apply cultures to a mApp Solution:

1. Create a mApp Solution.

2. Define mApp Solution properties for the culture currently selected in CSM Administrator.

3. Use the culture selector to change to each culture enabled for your system, and then define mApp Solution properties for each culture.
   If you do not define mApp Solution properties for each enabled culture, properties for the default culture are applied.

4. Prepare a mApp Solution for distribution and verify that mApp Solution properties have been defined for all cultures included in the mApp Solution.

5. Apply the mApp Solution. The cultures and translations included in the mApp Solution will be listed on the **Localization** page of the Apply mApp Wizard.

For more information on modifying multi-language mApp Solutions, see the Applying a mApp to a Globalized System free Video Learning Library course.

Related concepts

Create a mApp Solution

Define mApp Solution Properties

Prepare a mApp Solution for Distribution

Apply a mApp Solution

Using Globalization with CSM Features

Users with rights to access multiple cultures can use the culture selector to switch languages as they work with CSM.

Switching Cultures

When multiple cultures are enabled, users with multi-language security settings can switch cultures to change the display language for each CSM client.

The culture selector is available in the:

- CSM Desktop Client
- CSM Browser Client
- CSM Portal
- CSM Administrator
- CSM Dashboard Viewer
- CSM Report Runner (Report Manager only)

In the CSM Desktop Client and CSM Administrator, the culture selector is available in the Item Managers, such as the Dashboard Manager and One-Step Manager.

The initial culture selection is determined by:

1. The culture last selected by the user.
2. The culture set for a specific user in CSM Administrator.
3. The culture set for specific role in CSM Administrator.
4. The Global culture set for CSM in CSM Administrator.
5. The language setting for the user's operating system for all CSM Windows-based clients and for the Microsoft Edge browser. For other web browsers, the browser's language settings; the top language set for a browser is used.
6. The CSM primary culture.

Using the Culture Selector in the Web Applications

In the CSM Browser Client, select Languages, and then select your preferred language.
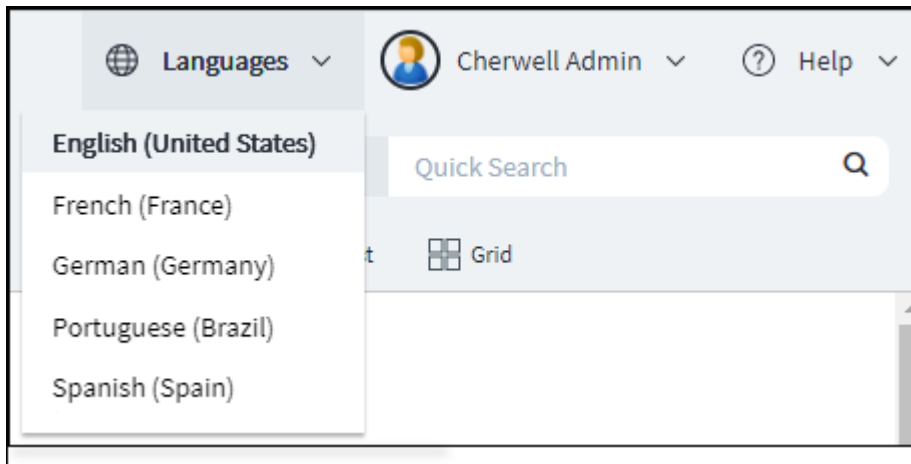
In the CSM Portal, select the language/culture on the toolbar, and then select your preference language.
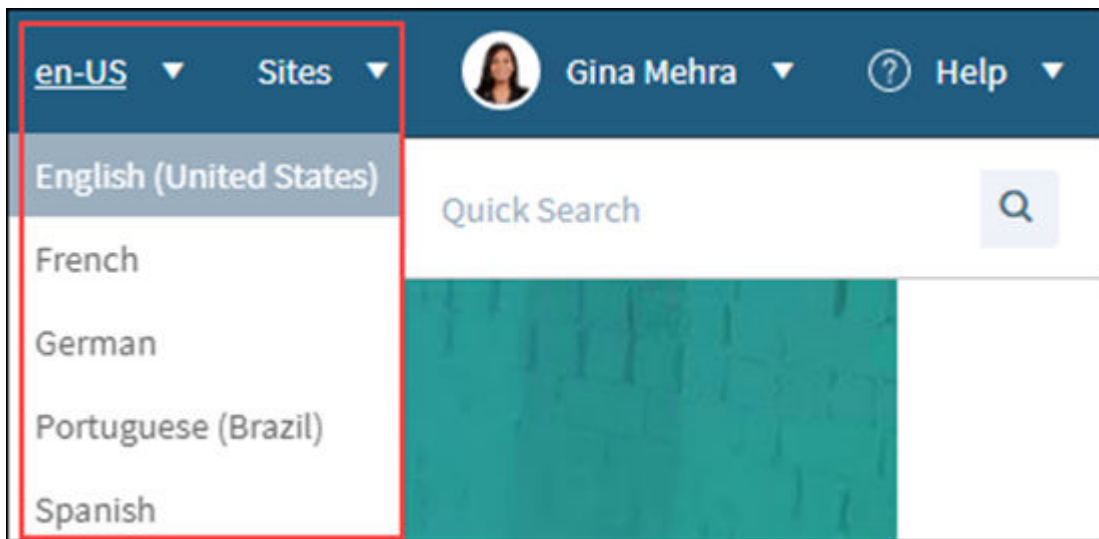
Multi-tab browsing support in the Browser Client allows you to open tabs in multiple languages and work in the tabs within the same session. In the CSM Portal, multi-tab browsing means you can have multiple tabs of the same language open. If you have multiple tabs open and select a new culture, all tabs refresh to display the newly chosen culture.

Using the Culture Selector in the Windows Clients

In most CSM Windows clients, such as CSM Desktop Client and CSM Administrator, you can select your preferred language and quickly toggle between two languages.

Note: In the CSM Desktop Client, only enabled cultures appear. In the CSM Administrator, all cultures in the system are available.

1. Select the language/culture on the toolbar, and then select your preferred language.

2. Select the first flag icon to switch to the preferred culture for your system.

3. Select the second flag icon to switch to the previously used culture. This is always a different culture than the preferred culture.

Using the Culture Selector in Blueprints

You can change cultures as you manage Blueprints so you can manually translate definitions as you work. Only content strings change when you switch cultures in a Blueprint, unless you close the Blueprint. In this case, CSM Administrator uses the last-selected culture from the Blueprint.

Related concepts

Manage Cultures

Multi-Tab Browsing Support

Hide the Culture Selector

Using Reports with Multiple Cultures

Reports are not managed by Language Packs, so you must create a copy of a Report for each culture you have enabled in your system. This enables you to translate column headers and labels in the Report for each culture.

🖉 **Note:** The culture selector does not impact how a Report appears when it is run. Users run a unique Report for each translation.

See Translating a Report.

In addition, you are prompted to select a culture for each Report when you run or edit an existing report if its culture has not been defined.

Selecting a Report Culture

The first time you run or edit each existing Report in the CSM Desktop Client, you may be prompted that the Report does not have an associated culture. The installed culture is detected, however, and you are asked if you want to use that culture.

If you:

- Click **Yes**, the Report's culture is set.
- Click **No**, the **Report Properties** dialog opens. Select the culture you want to use for the Report.

You can use the Report Properties dialog to change the culture assigned to a particular Report at any time.

Translating a Report

Report elements, such as labels and headers, must be translated in each Report assigned to a specific culture. You do not need to do this for every Report, but you may want to translate Reports that are pertinent to Users of a specific culture.

To translate a Report:

1. Open the Report Manager.

2. Copy and paste the Report you want to translate.

3. Rename the Report.

4. Right-click on the Report, and then select **Edit Report Properties**.

5. Select a new culture for the Report, and then click **OK**.

6. Right-click on the Report, and then click **Design Report**.

7. Use the Report Designer to translate visual elements, such as labels and headers.

Related concepts
Open the Report Manager
Designing Reports
Related tasks
Editing Report Properties

Setting a Culture for Running One-Step Actions

You can choose a specific culture to use when a One-Step Action is run. This is particularly useful for ensuring that email messages sent by a One-Step Action are translated into a specific language.

If you do not select a specific culture, the One-Step Action runs in the culture of the User who runs the One-Step Action.

To set a culture for a One-Step Action:

1. Open the One-Step Manager.

2. Create or edit a One-Step Action.

3. Click the **Start Graphic** on the Designer Board to edit One-Step Action general properties and conditions.

4. On the General page, select the **Use a specific culture when executing the One-Step** check box.

5. Click the arrow, and then select a specific culture. Options include:
   ◦ Select a culture from the list of enabled cultures.

   ◦ Select a custom culture code stored in a Business Object Field. For example, you can create a Culture Field in the UserInfo table so the One-Step Action is run using the culture set for the User running the One-Step Action.

Related concepts

Open the One-Step Action Manager

Create/Edit a One-Step Action

Define General Properties for a One-Step Action

Using Online Help with Multiple Cultures

CSM provides extensive online help in English and German. Limited online help is also available for French, Spanish, and Brazilian Portuguese.

When Users access online help from within CSM, the selected culture determines which language for which help is opened in the Documentation Portal. For example, if you select German (Germany) as the culture, German help is shown.

If online help content is not available for a selected culture, Users are shown English content.

Related concepts
Switching Cultures

Globalization Keyboard Shortcuts

Culture Selector Shortcut Keys (CSM Desktop Client)

Use the following keyboard shortcuts to use the culture selector in the CSM Desktop Client .

Key	Action
CTRL+Q	Switch between the preferred culture and the last selected culture.
CTRL+D	Switch to the preferred culture.
CTRL+L	Switch to the last culture you selected.

Language Pack Editor Navigation Shortcut Keys

Use the following keyboard shortcuts to navigate string rows in the Language Pack Editor.

Key	Action
CTRL+UP	Select the previous row.
CTRL+ENTER	Toggle between the row view and the detailed view.
CTRL+DOWN	Select the next row.

Globalization Best Practices

Globalization is a powerful yet complex feature. Following best practices as you plan and implement multiple languages will help ensure your success.

Consider Impact of Translations

If you intend to globalize your system at some point, always design your customizations with translation in mind. Some translations may require Form adjustments, for example. See Managing Controls on Translated Forms.

Add One Culture at a Time

For best results, enable one culture and translate strings for that culture before enabling additional cultures.

Use Lookup Tables for Field Validation

Values for Fields that validate from lists cannot be localized. Use Lookup Tables to ensure that validated values are available to users in all languages.

Benefits include:

- You can apply foreign key support to the validated Fields. See Storing Foreign Keys for Validated and Auto-populated Fields.
- You can backfill translated values in existing records.

Use the Content Optimization Tool to easily convert validation lists to Lookup Tables.

Manage Language Packs Within Blueprints

Create and apply Language Packs through Blueprints or mApp Solutions to manage translations for new or modified definitions. This enables you to maintain translations as your system changes and to manage smaller Language Packs than those created outside of Blueprints or mApp Solutions.

Use Small Scopes for Language Packs

While you can create a Language Pack that contains a large set of strings for multiple scopes, you may find it easier to manage multiple Language Packs that have a smaller scope for each target language.

Benefits include:

- You can manage translations, particularly reviews, in small batches. This is especially useful if multiple people are performing these tasks.
- You can apply small Language Packs more quickly than large Language Packs.
- You can use Language Pack naming techniques to manage the various types of strings that need to be translated.

You can apply Language Packs separately as they are ready, or you can create a Language Pack with an empty scope, and then merge completed Language Packs into it. You can then apply the merged Language Pack at one time.

Create Language Packs that Contain Only Tokens or Rich Text

You may find it useful to translate certain items as a single Language Pack. For example, you may want to create a Language Pack for the Incident scope that contains only Tokens.

To do so:

1. Create a Language Pack.

2. Open the Language Pack in the Language Pack Editor.

3. Verify that the **Hide items containing Expression Tokens and Rich Text Strings** check box is selected.

4. Select all of the visible strings, and then delete them.

5. Change the filter to **Show only items containing Rich Text strings**.

6. Select all of the visible strings, and then delete them.

Your Language Pack now only contains Tokens. You can use the **Show only items containing Token Expressions** filter to view and modify these strings following the guidance in Translating Plain Text Associated with Tokens.

Best Practices For Locking Strings from Translation

You can prevent strings from being translated by locking them. You can then exclude the **locked strings lists** when you apply a Language Pack. This can be important during different stages of your localization strategy, including the first time you localize your system and also during system maintenance and upgrades.

- **First Time Localizing Your System**: When first localizing your system, you might exclude certain strings from being translated. Users can create one or more lists that can be selected when applying a language pack as part of the LP wizard. For example, you can create individual lists for each language, category of strings, child company of an MSP (Managed Service Provider), etc. Locked strings lists can be modified and updated at any time.

- **System Maintenance or Upgrades**: Once the system has been localized, translations for certain strings might need to be changed based on context or preference (personal or stylistic preference). Since Language Packs do not contain duplicate entries, only one possible translation is contained in the Language Pack. This can result in existing, customized, context-based strings being overwritten. To preserve these existing translations, locked strings lists can be used to prevent overwriting when a new Language Pack is applied for updating (localizing newly added content) or maintaining your system.

Best practices for strings to include in locked strings list:

- **Team Names:** Team names (such as "Customer Service" and "Accounting") might be used in other contexts in the application (example: Service Category within an organization). Also, Expressions and Stored Searches can reference Team Names and can break if Team Names are translated.

- **Company and Product Names**: You may want to lock Company and/or Product names so they are not inadvertently translated and applied to your system.

- **Polysemantic Words**: Words with different meanings based on context/part of speech can be difficult to translate (examples: order, record, open, site, state). These words can be used as a noun or verb or assume completely different meanings based on context.

For general guidelines on creating and managing Locked String lists, see Managing Locked Strings

For specific categories of strings that could cause issues when being translated, see Globalization Good to Know.

Troubleshooting Globalization

Learn about potential issues might occur with Globalization features and how to rectify these issues. If you have an issue that is not listed, contact Cherwell Support for assistance.

Problem: Culture Selector Is Not Visible

Troubleshoot problems that prevent Users from seeing the culture selector in any CSM client, so they are not able to switch languages.

If this problem occurs, try the following solutions.

Solution: Verify that Cultures Are Enabled

1. In the CSM Administrator Main Window, select the **Globalization** category, and then select **Globalization Settings**.
2. Select the **Manage Cultures** page.
3. Verify that at least one culture is enabled.

   Note: Only enabled cultures are visible to Users.

Solution: Verify Culture Security Settings

1. Read about how to apply security settings for different cultures.
2. Verify that security is correctly enabled:
   ◦ Globally
   ◦ For Roles
   ◦ For Users

Solution: Reload Definitions in the CSM Desktop Client

1. Open the Desktop Client.
2. Select **Help>Reload Definitions**.

Solution: Clear Browser Cache

If Users cannot see the culture selector in the CSM Browser Client or CSM Portal, suggest that they clear their browser cache.

Solution: Restart IIS

If Users cannot see the culture selector in the CSM Browser Client or CSM Portal and clearing the browser cache did not solve the problem, restart Internet Information Services (IIS).

Problem: Solving Blueprint Conflicts in Globalized Systems

Troubleshoot issues that cause conflicts when you publish Blueprints in a globalized system.

Conflict errors typically occur because many Globalization features make schema changes. Depending on the order in which some features are enabled, you may receive conflicts when you publish a Blueprint.

If this problem occurs, try the following solution.

Solution: Overwrite Blueprint with Your Changes

To resolve conflicts, select the **Use my Blueprint** option on the **Blueprint Conflict Resolution** dialog. For more information, see Develop Blueprints Concurrently .

Problem: Multiple Legal Value Messages Appear in the Log File

Troubleshoot issues that cause "multiple legal values" messages to appear in log files.

You may see messages in the System Analyzer or the Application Server log that state:

Multiple legal values were detected for the field [field name].

The error indicates that duplicate values exist for a Lookup Table Field, so Users may see unexpected results in Searches, etc.

If this problem occurs, try the following solutions.

Solution: Remove Duplicate Values for a Lookup Table Field

Use the Data Editor to remove duplicate values from the Lookup Table Field specified in the log message. Repeat this task for all languages.

Solution: Change Field Properties

1. In CSM Administrator, create a Blueprint.
2. Edit the Lookup Table that contains the Field referenced in the log file.
3. Select the Field referenced in the log file, and then click **Edit**.
   Select the Validation/Auto-populate page of the Field Properties dialog.
4. In the Validation area, select the **On Conflict Use First Match** check box.

Related concepts

Data Editor
Define Validation/Auto-Population Properties for a Field

Problem: Errors Occur When Large Language Packs Are Applied

Troubleshoot errors that occur when you apply a Language Pack that contains a large number of strings.

You may receive "System.OutOfMemoryException" errors when you apply a Language Pack with a large number of strings.

If this problem occurs, try the following solution.

Solution: Increase Database Connection Timeout Values

1. In CSM Administrator, create a Blueprint.
2. From the Blueprint Editor menu bar, select **Tools>Options**.
3. Increase the number of seconds set for the **Database command timeout** option or select the **No Limit** check box.
4. Save your changes and publish the Blueprint.

Administrative Resources

There are various methods for linking to CSM items from within CSM clients, from email messages, and in other applications. In some cases, you need an internal record ID, or RecID, to correctly construct URLs.

Linking Directly to CSM Objects

You can provide links (also known as deep linking) to CSM objects, such as records and Saved Searches. This is useful for adding links to email messages sent to users or to records on remote systems.

Hyperlinks always open a new window in CSM. Users may be prompted for connection information and their user ID and password.

Parameter Key

Parameters are in italics and should be replaced with the values noted in the following table. Parameter values that contain spaces must be URL-encoded.

Parameter	Replacement Value
ServerName	The server name or IP address for the Browser Client or CSM Portal.
BusinessObjectID	The internal ID for the Business Object type, such as Incident. A typical internal ID might look like: 6dd53665c0c24cab86870a21cf6434ae
BusinessObjectName or rectype	The common name for a Business Object type. A typical name might be: incident
RecID or RecordID	This internal ID, or Record ID, uniquely identifies Business Object records (also referred to as Object.RedID). For most types of records, this string looks similar to: 939cd1f313b3b6866ef7d043faa258398c765d444a To find internal IDs, refer to Finding Internal Record IDs.
PublicID	The Business Object Public ID is normally identifiable by users. For example, the Public ID for an Incident would be an Incident ID. The Public ID does not need to be a number. For example, the Public ID for a customer is the customer's full name, which needs to be URL-encoded. A typical record ID might look like: 102259
Scope	The name or internal ID of an items' Scope (Global, Team, etc.).
ScopeOwner	The internal ID of the Scope Owner. For example, if *Team* is the Scope, then *1st Level Support* might be a Scope Owner. For best results, use the internal ID for Scope Owner. For more information, refer to Finding Internal Record IDs.

Go to Record Links

- **Go to Record by Record ID: Desktop Client**
  - **URL Command**
    CherwellClient://commands/goto?rectype=*BusinessObjectName*&recid=*Record ID*

  - **Example:**
    CherwellClient://commands/goto?
    rectype=*incident*&recid=*93d6067b6f6e1a17a2364744bc984bdb2715f624fa*

- **Go to Record by Record ID: Browser Client**
  - **URL Command**
    https://*ServerName*/CherwellClient/Access/*BusinessObjectID*/*Record ID*

  - **Example:**
    https://*ServerName*/CherwellClient/Access/*incident/*
    93d6067b6f6e1a17a2364744bc984bdb2715f624fa

- **Go to Record by Record ID: CSM Portal**
  - **URL Command**
    https://*ServerName*/CherwellPortal/*SiteName*/*BusinessObjectID*/*Record ID*

  - **Example:**
    https://*ServerName*/CherwellPortal/IT/*incident/*
    93d6067b6f6e1a17a2364744bc984bdb2715f624fa

- **Go to Record by Public ID: Desktop Client**
  - **URL Command**
    CherwellClient://*BusinessObjectName*/*PublicID*

  - **Example:**
    CherwellClient://commands/goto?rectype=incident&PublicID=123456

- **Go to Record by Public ID: Browser Client**
  - **URL Command**
    https://*ServerName*/CherwellClient/Access/*BusinessObjectName*/*PublicID*

  - **Example:**
    https://*ServerName*/CherwellClient/Access/*incident*/*123456*

- **Go to Record by Public ID: CSM Portal**
  - **URL Command**
    https://*ServerName*/CherwellPortal/*SiteName*/*BusinessObjectName*/*PublicID*

  - **Example:**
    https://*ServerName*/CherwellPortal/IT/*incident*/*123456*

- **Go to Record in Edit Mode: Browser Client**
  - **URL Command**
    https://*ServerName*/CherwellClient/Access/Command/Queries.GoToRecord?
    BusObID=*BusinessObjectName*&PublicID=*PublicID*&EditMode=*True*

  - **Example:**
    https://*ServerName*/CherwellClient/Access/Command/Queries.GoToRecord?
    BusObID=*incident*&PublicID=*123456*&EditMode=*True*

- **Go to Record in Edit Mode: CSM Portal**
  - ◦ **URL Command**
    https://*ServerName*/CherwellPortal/*SiteName*/Command/Queries.GoToRecord?
    BusObID=*BusinessObjectName*&PublicID=*PublicID*&EditMode=*True*

  - ◦ **Example:**
    https://*ServerName*/CherwellPortal/IT/Command/Queries.GoToRecord?
    BusObID=*incident*&PublicID=*123456*&EditMode=*True*

Create Record Links

- **Create Record by Business Object Name: Browser Client**
  - ◦ **URL Command**
    https://*ServerName*/CherwellClient/Access/New/*BusinessObjectName*

  - ◦ **Example:**
    https://*ServerName*/CherwellClient/Access/New/*incident*

- **Create Record by Business Object Name: CSM Portal**
  - ◦ **URL Command**
    https://*ServerName*/CherwellPortal/*SiteName*/New/*BusinessObjectName*

  - ◦ **Example:**
    https://*ServerName*/CherwellPortal/IT/New/*incident*

- **Create Record for a Specific Locale: CSM Portal**
  The following example shows the URL for creating an incident in the CSM Portal for a French locale.

  > **Important:** This does not work if a User's preferred culture is set to a different culture than specified in the URL.

  - ◦ **URL Command**
    https://*ServerName*/CherwellPortal/*SiteName*/New/*BusinessObjectName*?Locale=*locale*

  - ◦ **Example:**
    https://*ServerName*/CherwellPortal/IT/New/*Incident*?Locale=*fr-FR*

Search Links

- **Go to a Saved Search: Desktop Client**
  To run Saved Searches from other Scopes, change the ScopeName and ScopeOwner parameters. Example: the Scope is *Team* and the ScopeOwner is the internal ID for *1st Level Support*.

  > **Note:** For best results, always use the internal ID for the Scope Owner. For more information, refer to Finding Internal Record IDs.

  - ◦ **URL Command**
    CherwellClient://commands/goto?rectype=*recordType*&group=*Search%20Group%20Name*

  - ◦ **Example:**
    CherwellClient://commands/goto?rectype=*incident*&group=*All%20Incidents*

- **Go to a Saved Search: Browser Client**
  To run Saved Searches from other Scopes, change the ScopeName and ScopeOwner parameters.
  Example: the Scope is *Team* and the ScopeOwner is the internal ID for *1st Level Support*.

  > **Note:** For best results, always use the internal ID for the Scope Owner. For more information, refer to Finding Internal Record IDs.

  ◦ **URL Command**
  https://*ServerName*/CherwellClient/Access/Command/Queries.SearchByID?
  Scope=*Global*&ScopeOwner=*(None)*&Owner=*BusinessObjectID*&Name=*Saved%20Search%20Name*

  ◦ **Example:**
  http://localhost/CherwellClient/Access/Command/Queries.SearchByID?
  Scope=*Global*&ScopeOwner=*(None)*&Owner=incident&Name=*All%20Incidents*

- **Go to a Saved Search: CSM Portal**
  To run Saved Search from other Scopes, change the ScopeName and ScopeOwner parameters.
  Example: the Scope is *Team* and the ScopeOwner is the internal ID for *1st Level Support*.

  > **Note:** For best results, always use the internal ID for the Scope Owner. For more information, refer to Finding Internal Record IDs.

  ◦ **URL Command**
  https://*ServerName*/CherwellPortal/*SiteName*/Command/Queries.SearchByID?
  Scope=*Global*&ScopeOwner=*(None)*&Owner=*BusinessObjectID*&Name=Saved%20Search%20Name

  ◦ **Example:**
  https://*ServerName*/CherwellPortal/IT/Command/Queries.SearchByID?
  Scope=*Global*&ScopeOwner=*(None)*&Owner=*incident*&Name=All%20Incidents

- **Search for Text Format: Desktop Client**
  This option allows searching for arbitrary text in the specified type of record. This is the equivalent of typing search text into the quick search box in the main application.

  > **Note:** The *recordType* must be a Business Object that has Full-Text Searching enabled, and the searchText must be URL encoded.

  ◦ **URL Command**
  CherwellClient://commands/search?rectype=*recordType*&search=*searchText*

  ◦ **Example:**
  CherwellClient://commands/search?rectype=*incident*&search=*Printer%20%problem*

Dashboard Links

- **Open a Dashboard by Name: Browser Client**
  ◦ **URL Command**
  https://*ServerName*/CherwellClient/Access/Dashboard/*Dashboard%20Name*

  ◦ **Example:**
  https://*ServerName*/CherwellClient/Access/Dashboard/*CMDB%20Assets*

- **Open a Dashboard by Name: CSM Portal**
  - ◦ **URL Command**
    https://*ServerName*/CherwellPortal/*SiteName*/Dashboard/*Dashboard%20Name*

  - ◦ **Example:**
    https://*ServerName*/CherwellPortal/IT/Dashboard/*CMDB%20Assets*

- **Open a Dashboard by ID: Browser Client**
  - ◦ **URL Command**
    https://*ServerName*/CherwellClient/Access/Dashboard/by-id/*Dashboard%20ID*

  - ◦ **Example:**
    https://*ServerName*/CherwellClient/Access/Dashboard/by-id/
    93c6d34533492283691b0b4531802a4e6552e8baf5

- **Open a Dashboard by ID: CSM Portal**
  - ◦ **URL Command**
    https://*ServerName*/CherwellPortal/*SiteName*/Dashboard/by-id/*Dashboard%20ID*

  - ◦ **Example:**
    https://*ServerName*/CherwellPortal/IT/Dashboard/by-id/
    93c6d34533492283691b0b4531802a4e6552e8baf5

Calendar Links

- **Go to a Calendar: Browser Client**
  - ◦ **URL Command**
    https://*ServerName*/CherwellClient/Access/Calendar/*CalendarName*

  - ◦ **Example:**
    https://*ServerName*/CherwellClient/Access/Calendar/*Change%20Calendar*

- **Go to a Calendar: CSM Portal**
  - ◦ **URL Command**
    https://*ServerName*/CherwellPortal/*SiteName*/Calendar/*CalendarName*

  - ◦ **Example:**
    https://*ServerName*/CherwellPortal/IT/Calendar/*IT%20Calendar*

Miscellaneous Links

- **Specify Login Method: Browser Client and CSM Portal**
  - ◦ **URL Command**
    https://*ServerName*/*ClientName*/*LoginMethod*

  - ◦ **Example:**
    https://*ServerName*/CherwellClient/CherwellLogin

  > **Note:** Acceptable values are: `WinLogin` for Windows credentials, `SamlLogin` for SAML, and `CherwellLogin` for internal credentials.

- **Run a One-Step Action**

- **URL Command**
  https://*ServerName*/CherwellPortal/*SiteName*/One-Step/*OneStepName*

- **Example:**

  https://*ServerName*/CherwellPortal/IT/One-Step/*Create%20Task*

- **Alternate Format:**
  https://*ServerName*/CherwellPortal/*SiteName*/One-Step/*OneStepName*/*BusObName*/
  BusObRecIDorPublicID

  Warning: The following format will be deprecated soon; we suggest you use one of the methods listed above:
  https://*ServerName*/CherwellPortal/*SiteName*/command/OneStep.LaunchOneStep/
  OneStepName

  Note: Linking to One-Step Actions works best when users are logged into CSM.

- **Run a Report by ID: Browser Client**
  - **URL Command**
    https://*ServerName*/CherwellClient/Access/Report/by-id/*ReportID*

  - **Example:**
    https://*ServerName*/CherwellClient/Access/Report/by-id/
    939015c2ff09e43342f1094612a5cfc84de38baa37

- **Go to an HTML Page: CSM Portal**
  - **URL Command**
    https://*ServerName*/CherwellPortal/*SiteName*/Page/*PageName*

  - **Example:**
    https://*ServerName*/CherwellPortal/IT/Page/*IT%20Home*

Friendly Links and URL Encoding in CSM

Use an expression in the email options or a One-Step™ Action to provide links to send inside of CSM.

The display text of the link is the same as the content of the link. If you send links from One-Step Actions, the display text is different than the actual link. This works for launching CSM and links to other web sites or files.

Insert a Custom Text Expression into a One-Step Action

To create a link with a different display text in a CSM email message or One-Step Action and then change the expression to Text:

1. Right-click in the body of the message, and select **Expressions > New customer Expression**.
2. In the **Editor** drop-down list, select **Text**.

You must use one of these formats for the text:

- `[LINK friendly-text|URL]`
- `[LINK]friendly-text;URL`

The word LINK in square brackets tells CSM to treat this as a link, the friendly text is what's displayed as the link text, and the URL after the | (pipe) character or semicolon is the actual hyperlink.

The new line is caused by wrapping because there are no line breaks in the expression. When the user gets this email, the link looks similar to: Go to Incident 10928. When the user selects the link, they're taken to the record.

URL Encoding

The following rules apply to URL encoding:

- Values must be URL encoded to pass field values that might contain unsupported characters.
- Links can't include spaces or certain punctuation characters.
- You can use a token, such as IncidentID, but if you use search text, it may cause issues.

You can URL encode the URLs to convert certain characters to an allowed format. For example, spaces are converted into the sequence %20.

To perform URL encoding:

1. Right-click in the inserted field of the One-Step Action.
2. In the **Modifier** drop-down list, select **URL Encode**.
3. Select **OK**.

Finding Internal Record IDs

Each CSM object has an internal ID, also referred to as a RecID. Typically, you do not need to know the internal ID, but this information is helpful for certain features. For example, internal IDs are useful for constructing URLs so users can link directly to CSM objects.

Use these tips for finding Internal IDs for CSM objects:

- Export an object, such as a saved search or dashboard. You can then open the .ced file in a text editor to retrieve internal IDs for elements such as scope and scope owner. See Import/Export a CSM Item.
- Find the Internal IDs for Business Objects, fields, and relationships in CSM Administrator.
- Use an appropriate Cherwell REST API operation to find the RecID for an object. For example, use `getbusinessobjectsummaries` to find RecIDs for Business Objects and fields. For more information, refer to About Cherwell REST APIs.

Finding Record IDs for Field Values

To simplify the process of finding record IDs for field values, add the RecID field to the grid for the Business Object that contains the foreign key field. Users can then see the record ID in Table Management.

You may first need to change presentation properties for the RecID field to allow it to be added to grids. See Define Advanced Properties for a Field.

Guidance for System Reliability and Stability

Read Cherwell guidance for optimizing your CSM system for best performance and stability.

Performance

- **Best Practices**
  For best results, periodically review performance best practices to analyze and troubleshoot performance issues. See Best Practices for Performance.

- **Business Objects**
  Learn how to prevent long load times for Business Object records. See Business Object Performance.

- **Relationships**
  Relationships provide a powerful way to pull record data together in meaningful ways. Learn how to ensure your relationships meet the needs of your users without impacting performance. See Relationships and Performance.

- **Automation Processes**
  Because Automation Processes rely on Business Object logic, be sure to optimize configurations that might impact performance. This is especially important in high-load systems that have a large number of concurrent users or a high rate of record creation and updates. See Performance Considerations for Automation Processes.

  Also, learn about how Automation Processes are queued and run. See Automation Process Workflow.

- **Cherwell REST API**
  Learn how to resolve poor performance with the Cherwell REST API. Examples of poor performance might be API calls, such as the first call made to CSM, taking longer than expected to complete. See Cherwell REST API Performance.

Optimization

- **Content Standards**
  Learn about the standards Cherwell uses for developing CSM content elements, such as Business Objects, forms, fields, and more. Consistently applying these standards to content you create and modify will help minimize issues associated with inconsistent content items. See Content Standards Overview.

- **Email Monitoring**
  Learn how to avoid common mistakes and troubleshoot issues that may occur with the Email and Event Monitor Service. See Recommendations for Implementing Email Monitoring in CSM.

- **Recommended Timeout Settings**
  Learn about the recommended timeout settings in CSM and its supporting services. Recommendations are intended to optimize system performance. See Suggested Timeout Settings for CSM.

- **Approval and Denial Rules**

Learn about the set process used to determine whether an approval or a denial can be actioned. Detailed examples are provided for a variety of approval and denial scenarios. See Approval and Denial Threshold Rules.

- **Blueprint Publishing**
Certain changes to Business Objects may cause database tables to be rebuilt during the publish process. This can extend the amount of time it takes to complete the publish process, especially for Business Objects that contain a large number of records. This may impact system performance and cause some Business Objects to be unavailable. See Performance Impact of Blueprint Changes.

- **Integration Options**
Learn the pros and cons of various integration options that enable you to import, export, or link information between two systems. There are also options for performing actions that are triggered by an external tool or by CSM. See CSM Integration Options.

Security

- **Platform Security Certification**
Application and environment testing are performed regularly to ensure security hardening for CSM. See CSM Core Platform Security.

- **Authentication Methods**
Learn about the four methods for authenticating users: internal, LDAP/Active Directory, Security Assertion Markup Language (SAML), and Windows authentication. See Authentication Methods.

- **Enable HTTP Strict Transport Security (HSTS)**
On-premise customers can learn how to enable HSTS to inform a browser that it should contact CSM web applications only through HTTPS connections and should automatically convert all attempts to access applications using HTTP to HTTPS requests instead.

Be aware that the process is different depending on which version of Internet Information Services (IIS) you use. See Enable HTTP Strict Transport Security (HSTS).

- **Email Credentials FAQ**
Find information about securing credentials-based email accounts and answers to frequently-asked questions about Modern Authentication and OAuth 2.0. See Modern Authentication and Google Authentication FAQs.

- **Encrypt Sensitive Data**
Learn how to encrypt sensitive data using two CSM features:
  - Encryption modifiers store private information, such as API keys, user names, or passwords in CSM. This is useful for integrating CSM with other systems (Examples: Amazon, Microsoft Teams) that require credentials and other sensitive information to be stored in the CSM database. See Encryption Modifiers.

  - Field-level encryption enables you to safely gather sensitive information from forms. See About Encrypted Fields.

Diagnostics

- **Run the Performance Health Check Tool**

Learn how to monitor and optimize system configurations that impact performance. For example, use the tool to find inefficient queries and find and fix mismatched Def IDs. See About Performance Health Check.

- **Network Health Check**
Validate network speed and connectivity, so a technician can check for network issues between their client and the server. See Network Health Check Results.

- **Interpret Health Check Results**
After running the Health Check Tool, you can optimize system configurations based on the results of the basic checks, rules reports, and usage statistics. See Interpreting Health Check Results.

- **View Queue Service Logs**
Use the data that RabbitMQ provides to make informed decisions about scaling CSM microservices. Helpful data includes a list of machines with CSM installed connecting to RabbitMQ, the number of workers, the number of pending messages, and the number of queued messages. See Monitor Queues from the RabbitMQ Management Interface.

- **Troubleshoot Queues in CherwellMQS**
Find information and steps for identifying and removing "stuck" items in a queue, increasing the speed of Automation Processing events, and decreasing event processing time. See Troubleshooting Queues in CherwellMQS.

Configuration

- **Considerations to Move from Development to Production**
See guidelines to synchronize databases between a development or test system and production, remove test data, and perform system maintenance. Also, learn about activating integrations on production and see a final system checklist. See Considerations for Moving from Development to Production.

- **Configure the Cherwell Service Host for a Local Scheduler**
Most environments have the Scheduling Service on the same network as the other CSM services. However, in some cases you may want to set up a second Scheduler on a separate network. Follow these steps to configure this setup: Configure the Cherwell Service Host for a Local Scheduler.

- **Scale CSM**
Guidance and recommendations for scaling CSM have been simplified and improved. Learn how, why, and when to scale the Cherwell Service Host, the CSM web applications, or both. See Scaling CSM.

In addition, see specific hardware, CPU, memory, and storage recommendations for using CSM with a load balancer through server farms. Redis guidelines are included. See Server Farm Resource Recommendations.

- **MSP Deployment and Configuration Options**
Learn how to configure CSM for simple access deployment or by using segregated tenants. The choices depend on the level of access and customization required by the tenants weighed against the cost of configuring and maintaining the system. See MSP Deployment and Configuration Options.

Machine Learning

Machine learning allows you to train a classification model that analyzes the content of a field and makes a prediction about a different field. The machine learning model can autopopulate the prediction or a score that measures the confidence in the prediction.

About Machine Learning

Accurate predictions from machine learning models require a large amount of reliable data for training.

During training, a machine learning model identifies connections within the data. The model then uses those connections to predict the output value based on the input that it receives. Considering this, the model can only be only as good as the information used to train it.

Improving Accuracy

To get accurate predictions, you must verify that the data used to train the model is correct. The examples you use to train a model teach the system what correct relationships between the input field and the field being predicted look like.

The amount of verified data is just as important as quality when training a model. To guarantee that an appropriate quantity of data continues to be available, base your model on fields that are used often and are consistently accurate.

Prediction models require a diverse data set. The data set used for training should include examples of each classification available. The training data should be verified as correct and representative of common uses for the fields. A model is trained using 80 percent of the training data set. The remaining 20 percent of the data is used for testing to verify the model. If all of the data used to train the model is identical, you get an error and the model is not trained.

Scoring Confidence

The CSM machine learning model calculates a confidence score for each prediction it makes. This score indicates the likelihood that the classification it predicts is correct. When a prediction is made, each possible classification is given a score. These scores are decimals whose sum is 1.0. The machine learning model provides the classification with the highest confidence score as the predicted value, and the decimal is displayed as the conficence score.

Some algorithms can produce a confidence score higher than 1.0. This is caused by the way numbers are rounded for calculations. This happens only in especially small or repetitive data sets. For better results, use large amounts of varied data.

Manage Machine Learning

Use the Machine Learning Manager to manage Machine Learning scenarios and settings.

To create a machine learning model:

1. Open CSM Administrator.
2. Select **Create a new Blueprint** from the **Common Tasks** list.
   The **New Blueprint** page opens in the main pane.
3. Select **Managers > Machine Learning**.
   The **Machine Learning Manager** opens.

From the Machine Learning Manager, you can configure a new Machine Learning model. You can also adjust default values for prediction categories and timeout.

1. In the Machine Learning Manager, select **Machine Learning > Settings**.
   The **Machine Learning Settings** window opens.
2. Adjust the values as needed:
   - **Maximum Prediction Categories**: Defaults to 250; provide a value between 2 and 500.
   - **Prediction Timeout**: Defaults to 5 seconds; provide a value between 1 and 60.

Related tasks
Configure a Machine Learning Model

Train a Machine Learning Model

Configure CSM to run a scheduled task that trains a machine learning model. This model analyzes an input field and generate a prediction.

Task	Notes
1. Configure a machine learning model	Create a machine learning model using the machine learning Manager. This will determine the field that the model will analyze and the field that will be predicted. See Configure a Machine Learning Model.
2. Create a query to provide example data	Use the Search Manager to configure a machine learning query that returns example content for the input field and the prediction field. To create a model that makes quality predictions that are both precise and accurate, the sample data returned by this query must provide a large amount of verified data. See Searching .
3. Schedule the training	Create a Schedule Item that will use the machine learning search to pull the appropriate data. The Action **Train Machine Learning** uses that data to train the machine learning model. When the Schedule Item runs, it processes the data returned by the stored search using the algorithm to train the model. This training can be set as a recurring event. As new data is saved to CSM, it is used to retrain the model, and the quality of the predictions can improve. See Scheduler.
4. Create an expression	Create a machine learning Prediction Expression to autopopulate the prediction and confidence score fields. See Expressions.
5. Configure the fields	Configure a Business Object to include the input field and the prediction field specified in the machine learning model. The confidence score for a prediction can be displayed in a form as well. See Define Auto-population Properties for a Field.

Configure a Machine Learning Model

Determine the fields that should be used for input and prediction in the machine learning model.

To create a machine learning model:

1. Open CSM Administrator.
2. Select **Create a new Blueprint** from the **Common Tasks** list.
    The **New Blueprint** page opens in the main pane.
3. Select **Managers > Machine Learning**.
    The **Machine Learning Manager** opens.
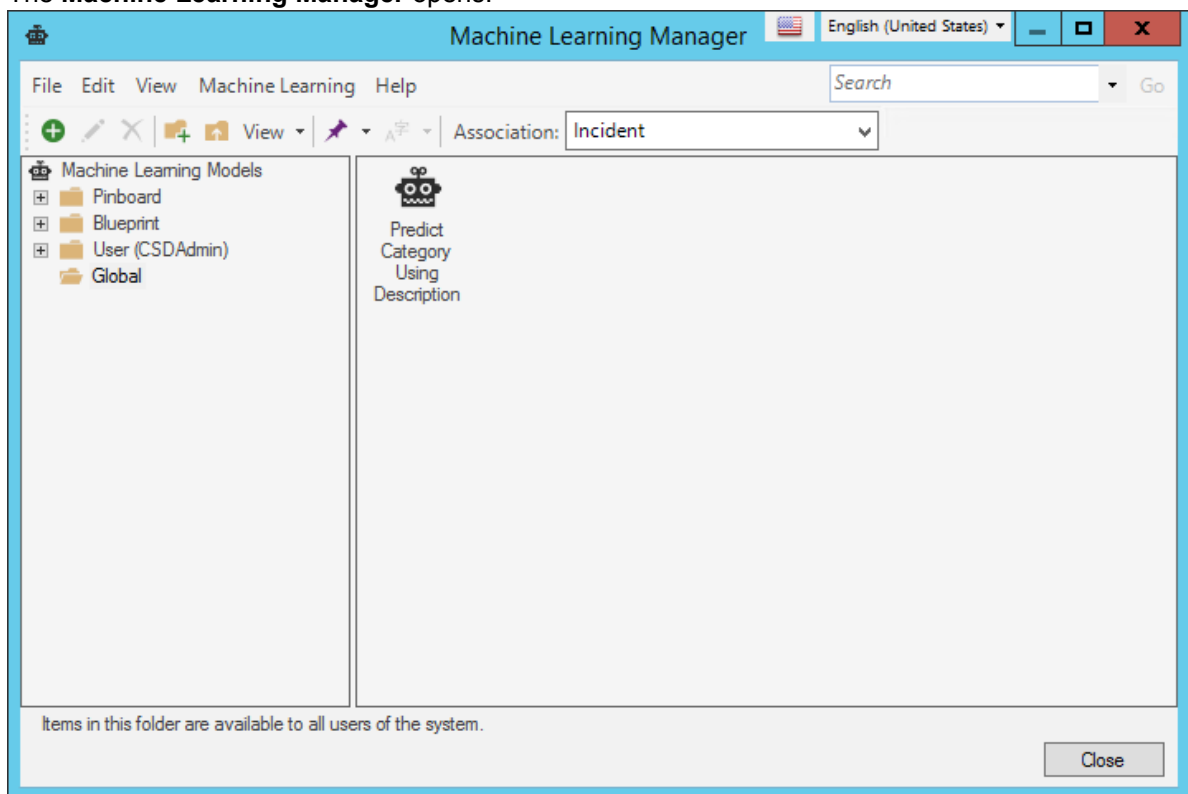
4. Select the Business Object that will use the classification model from the **Association** drop-down list.
5. Right-click in the Machine Learning Model pane and select **New**.
    The **Machine Learning Model Properties** dialog box opens.
6. Complete the fields for the machine learning model.

Field	Description
Name	The title of the machine learning model.
Description	A description of the machine learning model.

Field	Description
Filed used for input	Field to be used as input for the classification model. The field options in the drop-down list are restricted to the selected Business Object.
Field to be predicted	Field that will display the predictions based on the classification model. The field options in the drop-down list are restricted to items in lookup tables. The model will autopopulate this field when content is entered in the input field. **Note:** By default, the record limit on lookup tables used for predictions is 250 records. You can increase the record limit to a maximum of 500 (in the Machine Learning Manager, select **Machine Learning > Settings**).

7. Close the Machine Learning Manager.

Related tasks
Manage Machine Learning