CSM 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 elements include:

- **Installations:** CSM provides three distinct installers so that the correct components get installed to the correct places. Installations include:
    - **Server:** Installs the Cherwell Application Server and the support services.
    - **Portal and Browser Apps:** Installs the Browser applications, such as the Customer Portal, Browser Client, APIs, and Auto-Deploy.
    - **Client:** Installs the main Client applications.
- **Connections:** Connections are the means by which the CSM components communicate with each other and/or the database. During a standard installation, there are prompts to create three connections; one for each installation (Server, Portal and Browser Applications, and Client).
- **Demo or Starter database:** CSM provides a Starter database, which contains all the structure needed to get started with CSM (ex: Business Objects, Forms, One-Steps, Security Groups, etc.). CSM also provides a Demo database, which contains structure and sample data.
- **Auto-Deploy:** CSM Auto-Deploy is an installation tool that allows system administrators to automatically push out preconfigured Client installations and connections to client machines.

Installation tools include:

- **Installation Wizards:** The CSM Installation Wizards walk you through the steps to run the Client, Server, and Portal and Browser Application installations. The Installation Wizards are accessed through the Installation Launcher by double-clicking the **CSM Installation.exe** file. Launch each Installation Wizard by clicking the appropriate text (Client, Server, etc.). To move through the wizard, click Next. Many options are set by default to help with decision making.

  When necessary, the Installation Wizards launch the Connection Wizard to help configure or update the connections.

  Note: Run the Server installation first, and then the Portal and Browser Apps installation. Client installations are run last and are typically pushed out to client machines using the Auto-Deploy feature (Auto-Deploy is configured separately to push out preconfigured Client installations and connections).
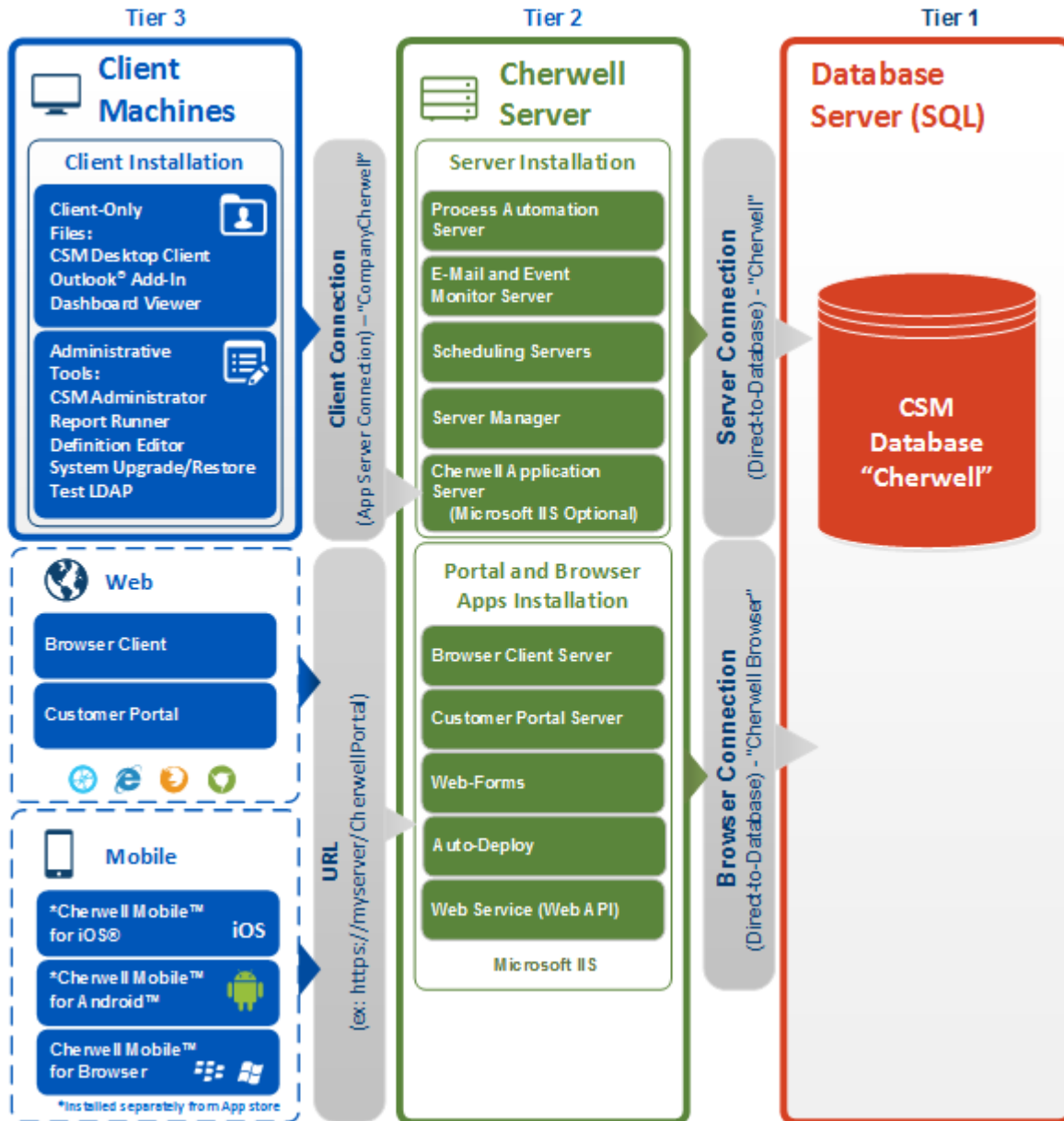
- **Connection Wizard:** Walks through the steps to create the connections between the CSM components.
- **Auto-Deploy Configuration:** Helps configure Auto-Deploy to push out Client installations and connections.
- **Installation Worksheet:** Helps gather the server and account information needed before installing CSM.

Installation steps vary depending on which installers are run (Server, Portal and Browser Apps, and Client), whether it is a new installation or an update, 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 Servers (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 Servers (services), and the Portal and Browser applications.

- **(Tier 3) Client machines:** House 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.

Tier 3

Client Machines

Client Installation

Client-Only Files:
CSM Desktop Client
Outlook® Add-In
Dashboard Viewer

Administrative Tools:
CSM Administrator
Report Runner
Definition Editor
System Upgrade/Restore
Test LDAP

Web

Browser Client

Customer Portal

Mobile

*Cherwell Mobile™ for iOS® iOS

*Cherwell Mobile™ for Android™

Cherwell Mobile™ for Browser

*Installed separately from App store

Client Connection
(App Server Connection) – "CompanyCherwell"

URL
(ex: https://myserver/CherwellPortal)

Tier 2

Cherwell Server

Server Installation

Process Automation Server

E-Mail and Event Monitor Server

Scheduling Servers

Server Manager

Cherwell Application Server
(Microsoft IIS Optional)

Portal and Browser Apps Installation

Browser Client Server

Customer Portal Server

Web-Forms

Auto-Deploy

Web Service (Web API)

Microsoft IIS

Server Connection
(Direct-to-Database) - "Cherwell"

Browser Connection
(Direct-to-Database) - "Cherwell Browser"

Tier 1

Database Server (SQL)

CSM Database "Cherwell"

Note: Be sure to read Before Installing CSM before beginning any installation.

Installations

CSM provides the following installations:

- **Server:** The Server installation should be run first, and installs the Cherwell Application Server and several support services (ex: Automation Process Server, E-mail and Event Monitor, etc.). The Server Manager is also installed, by default.

- **Web Applications:** The Portal and Browser Apps installation installs the various Cherwell Browser applications, such as the Customer Portal and Browser Client. This also installs Auto-Deploy.

- **Client:** The Client installation installs the main Client applications (client-only files) and your choice of 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. For the Client installation to be useful, you must have the Cherwell Application Server installed and configured.

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

The following tables describe in detail 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 (usually using an encrypted TCP connection).
Automation Process Server	The Cherwell Automation Process Server (formerly the Business Process Server) is a CSM service that monitors events and executes background business rules in your system (example: Notifications and escalations). Automation Processes are configured in CSM Administrator.
E-mail and Event Monitor Server	The Cherwell E-mail and Event Monitor Server is a CSM service that automatically monitors e-mail accounts and event streams, and then performs specified actions, such as creating or modifying records based on e-mail content or event details. In addition to connecting to the database server, it also has to be able to talk to the mail server (example: Microsoft Exchange).

Item	Description
Scheduling Server	The Scheduling Server is a CSM service that 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).
Server Manager	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 Servers (services), and restart some managed CSM Web Applications.
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.

Portal and Browser Apps 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.
Auto-Deploy	Cherwell Auto-Deploy is an installation tool that allows system administrators to automatically distribute preconfigured Client 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.

Item	Description
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.
Cherwell Web Service (CWS)/Web API	The Cherwell Web Service (CWS) is an API for communicating with CSM using Simple Object Access Protocol (SOAP) over HTTP. CWS must be running for the Mobile applications to operate, and is also required for a number of other features (RSS feeds, SAML security access, Bomgar® integration, etc.).
Web-Forms	Cherwell Web-Forms™ is a browser-based application that allows Users to enter, view, and edit CSM Business Objects over the web without having to log in (example: Surveys, registration, ordering, etc.). This tool also allows for the remote execution of One-Steps.

Client Installation

Item	Description
Client-Only Applications	CSM Desktop Client, Outlook® Add-in (Installer), Report Runner, and the Dashboard Viewer.
Administrator Applications	CSM Administrator, Definition Editor, System Upgrade/ Restore, and Test LDAP Tool.
Server Applications	See Server installation.
Note: The Browser applications (ex: CSM Browser Client, Customer Portal, CWS, etc.) are installed during the Portal and Browser Apps installation. Cherwell Mobile (Cherwell Mobile for iOS and Cherwell Mobile for Android) is installed via downloadable Mobile Applications.	

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 (ex: Cherwell Application Server) use this type of connection, although the 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 CSM database (Tier 1).

- **App Server connection (3-tier):** An App Server connection is a connection between one or more CSM applications (Ex: CSM Desktop Client) and the Cherwell Application Server. Most commonly, this connection uses TCP, and might or might not be encrypted. 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 first-time 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 Application Server, but includes the Automation Process, E-mail and Event Monitoring, and Scheduling.) 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 Browser apps run inside IIS and the connection needs to work with the IIS security options. During the Portal and Browser Apps 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.

Before Installing CSM

Before installing for the first time:

- Verify that the system meets the system requirements.
- Complete the Installation worksheet.

Installation Worksheet

No.	Installation Item
1.	**Cherwell Server** This is the machine where the Cherwell Application Server and the supporting Servers (services) are installed. The account used to launch the services on this machine is called the Cherwell Server account (aka, 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: *Ex: CherwellServer* Location: *Ex: \\domain\CherwellServer* **Cherwell Server Account Credentials** Username: *Ex: domain\henri* Password: *Ex: Colorado719*

No.	Installation Item
2.	**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 (aka, SQL Login). The Database Login account must have rights to insert, update, and delete rows within tables. If planning to also 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 Servers (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 server, and the service account has rights to the database, and then use Windows Authentication to provide the credentials. This information is needed when creating connections. Server Name: *Ex: CSMDatabaseServer* IP Address: *Ex: 168.212.225.204* **Database Login Account Credentials** Username: *Ex: sa* Password: *Ex: Colorado719*
3.	**Cherwell Application Server** This is the location of the Cherwell Application Server. You can use either HTTP or TCP, although this must match the configuration on the server. We recommend TCP. URL: *EX: tcp://<CHERWELLSERVER>:<Port#>*

No.	Installation Item
4.	**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: *Ex: sa* Password: *Ex: Colorado719*
5.	**License** Organization Name: *Ex: Cherwell Software* Cherwell License Key: *Ex: 3SKPFM-PC9ZM-PD4MK-FPG90-RLUW8*

Port Numbers

The list below lists the default ports that CSM uses.

Connection	Protocol	Port
Client Connection	TCP	8001
Internet	HTTP	80
	HTTPS	443
LDAP	LDAP	389
E-mail	SMTP	25
	SMTP SSL	465
	POP3	110
	POP3 SSL	995
	IMAP4	143
	IMAP4 SSL	993
Microsoft SQL Server	TCP	1433
Redis (optional for load balancing)	TCP	6379
Splunk (optional)	TCP	8089

Steps to Install CSM

The installation steps vary depending on which installations are run (Server, Web Applications, and Client), whether it is a new installation or an upgrade, and whether or not Auto-Deploy is used.

Install the CSM suite for the first time (system administrator).

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

> **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 Cherwell Client and Web Applications.

1. Run the Server installation to install the Server application files.
2. Configure the Server connection (when prompted by the Server installation). This is a direct-to-database (2-tier) connection between the Cherwell Application Server and the CSM database.
3. Run the Portal and Browser Apps installation to install the Browser application files.
4. 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.
5. Configure Auto-Deploy to push out the Client installation and connection to client machines.

   > **Important:** During the Auto-Deploy configuration, the configure the Client connection that are auto-deployed must be configured.

6. License CSM

   > **Note:** After CSM is installed and licensed, log in to CSM Administrator (username = CSDAdmin, password = CSDAdmin) to set up the User and Customer Profiles so that people in the organization can log in to other CSM applications.

Install Client applications to a client machine using Auto-Deploy (Users).

To 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.

Multi-Language Installers

The CSM installer is available in English, German, French, Spanish, and Brazilian Portuguese. Download the CSM installer for your desired language in order to step through the installation process in that language.

Platform code-level support for all five languages is included with each installer, and the assemblies for all languages are added during the Portal and Browser Apps and the Client installations. 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 is enabled by default in the Demo database, but must be enabled in the Starter database. For more information, refer to Enabling Globalization.

Run the Server Installation

Launch the installation on the server in the location to install the Server application files.

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

1. Double-click the **CSM Installation.exe** file.

2. Click Server.

3. Review the introductory text and click Next.

4. Select the I accept the terms in the license agreement radio button and click Next.

5. Provide the Customer information, and click Next.

6. Use the default location/folder in which to install the Server installation files or click Change to browse to another location. We recommend accepting the default installation folder. For details about the default location, refer to Folder Selection Options. Click Next.

7. Select the database components to install, then click Next. For details about the database options, refer to Database Selection Options.

8. Select which CSM Servers (services) to install. We recommend installing all the servers. For details about the server options, refer to Server Selection Options. Click Next.

9. Provide the Cherwell Server account credentials that will be used to launch the CSM Servers (services), then click Next. For details about the Logon Information options, refer to Server Logon Information.

10. Click Install, the page shows an installation progress bar.

11. The next page depends on selections made on the Database Selection page:

    Load the Demo or Starter 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. Click 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.

    The Install Complete page opens.

12. Click Finish.

Configure the Server Connection

Use the Connection Wizard (automatically launched by the Installation Wizard during the Server installation) to configure the Server connection (direct-to-database/2-tier connection between the Cherwell Application Server and the CSM database). Most options are assumed or set by default to help with your decision making (ex: The connection type is assumed to be a direct-to-database connection and the database connection is named Cherwell).

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 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 the Connect to CSM window by clicking the **Add** button.

   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, and then click Next.

   Note: If the Connection Wizard is automatically launched by the Server Installation Wizard, this window does not appear because CSM already knows that it is a direct-to-database/2-tier connection.

3. Select a connection type, then click Next. There are two options for 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).

4. Select where to install the CSM database on the SQL Server machine, then click Next. For more information on selecting a database location, refer to Server Connection Options.

5. Provide a **name** and **owner** for the database, or click Browse to see a list of available databases.

   Note: This database is created as part of the installation process. If unsure of name/owner, leave the defaults ("Cherwell" and "dbo"). The last page of the wizard offers a test for the database connection.

   Click Next.

6. Specify the Database Login account credentials that the system uses to log into the CSM database, then click Next. For more information on the requirements and options for specifying these credentials, refer to Server Connection Options.

7. Specify the **database login 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, then click Next. For more information on the requirements and options for specifying these credentials, refer to Server Connection Options.

   Tip: In most cases, this is the Same as Standard Login.

8. Select connection pooling and security/failover options, then click Next. For more information on these options, refer to Server Connection Options.

9. Accept the **default connection name (Cherwell)**, provide an optional **description** for the Server connection, and then click Next.

   Important: If the default connection name (Cherwell) is not accepted, the CSM Server (service) connections and start the services have to be manually configured.

10. Click Test Connection to verify the connection to the database.

    Tip: If the test fails, an installation can continue.

11. Click 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, click Yes, and then perform the upgrade.

Server Connection Options

Database Location for Server Connection

In the course of configuring your Server connection, you will be required to specify a location for the Database. The following table describes the database location options:

Option	Description	Notes
Database is on this machine	Connect to a local database. Typically, this is only for evaluation systems.	
Specific Server	Connect to a database installed on a named server.	Provide the **database server name**, or select the name of the database server in the drop-down. The drop-down might take a few seconds to populate, and it is possible that the desired server is not listed. 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 for Server Connection

In the course of configuring your server connection, you will be required to specify the Database Login account credentials.

The Database Login account must have rights to insert, update, and delete rows within tables. If planning to also 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 Servers (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 server, and the service account has rights to the database, and then use Windows Authentication to provide the credentials. This information is needed when creating connections.

The following table describes the database login account credentials options:

Option	Description	Notes
Windows Authentication	Click this option to use the stored Windows Authentication (user name and password) for authentication.	
User ID and Password	Click this option to log in using a specific user name and password.	Provide the User ID and password.

Administrative Login Options for Server Connection

In the course of configuring your server connection, you will be required to specify the database login 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.

This account must have rights to create, drop, and alter tables, as well as insert, update, and delete rows within tables. When the CSM Servers (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.

The following table describes the administrative login options:

Option	Description	Notes
Same as Standard Login	Click this option to use the same login options as the system.	
Windows Authentication	Click this option to use the stored Windows credentials (user name and password) for authentication.	
User ID and Password	Click this option to login in using a specific user name and password.	Provide the User ID and password.

Connection Pooling and Advanced Options for Server Connection

In the course of configuring your Server Connection, you will be required to specify a series of connection options. The Connection Options page includes sections for Connection Pooling options and Advanced Settings.

Option	Description	Notes
Use default pooling options	Click this option to use the default pooling options.	This option is appropriate for most systems.
Customize pooling options	Click this option to specify custom pooling options.	This option is only for advanced users. Specify the pool sizes to customize the caching options.
SQL Server is configured as an AlwaysOn group	This option 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 sting.	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.

Option	Description	Notes
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.	

Server Installation Options

Folder Selection Options

In the course of your server installation you will have the option to use the default location/folder in which to install the Server installation files or click Change to browse to another location. The following table describes the default folders:

Option	Description	Notes
Default folder for **32-bit machines**	The default folder for 32-bit machines is: C:\Program Files\Cherwell Service Management	
Default folder for **64-bit machines**	The default folder for 64-bit machines is: C:\Program Files (x86)\Cherwell Service Management	Even though CSM files are installed to the (x86) directory, CSM runs as a 64-bit application on 64-bit machines. The reason CSM installs to the x86 directory is that Windows installers do not easily support installing applications that are both 32-bit and 64-bit. We do not install to C:\Inetpub because IIS sometimes removes files in this directory in certain scenarios.
Change	Choose this option to browse to another location.	We recommend accepting the default installation folder.

Database Selection Options

In the course of your server installation you will be required to 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.	We recommend this option for new Users who would like to evaluate CSM. When Install is clicked, the Connection Wizard opens, prompting Users to configure the database connection.
Cherwell Starter (Empty) Database	Installs the Cherwell Starter database (contains structure but no data).	We recommend this database for Users who are ready to start using CSM in a live environment. This option opens the Connection Wizard, prompting Users 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. Click Install and select a database to update.

Option	Description	Notes
Do not load any data	Skips installing or updating the database.	A database update is typically needed, there might be a prompt to update the database upon first run of the applications.

Server Selection Options

In the course of your server installation you will be required to select the servers (services) to install. We recommend installing all the servers. The Server Manager is installed by default. The following table describes each of the server options:

Option	Description	Notes
Application Server	Select this option to install the Application Server.	You must also choose whether to install the application server as a service or using IIS.
Application Server as a Service	Select this option to install the Application Server as a Windows service on the designated server.	This is the recommended option.
Application Server using IIS	Select this option to install the Application Server as a web application under IIS.	This might be required if firewall policies do not allow opening a new port or to avoid conflicts with IIS when using HTTP as the transport protocol. If the Cherwell Application Server is hosted in IIS, Windows Communication Foundation (HTTP and Non-HTTP Activation) components are also required.
Automation Process Server	Select this option to install the Automation Process Server.	
Scheduling Server	Select this option to install the Scheduling Server.	
E-mail and Event Monitor	Select this option to install the E-mail and Event Monitor service.	

Server Logon Information

In the course of your server installation you will be required to specify a name and password for service configuration. The following table describes each of the logon options:

Option	Description	Notes
Specific account	Provide a User name (should be in the format *DOMAIN\UserAcct*) and Password.	Click Browse to locate domains and accounts on each domain.

Option	Description	Notes
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.
Use Special Account	Select this check box to use a Windows 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 checked.
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 checked.
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 checked.

Run the Web Applications Installation

Launch the installation on the server where you want to install the Portal and Browser applications files.

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. Double-click the **CSM Installation.exe** file.
2. Click Portal and Browser Apps.

   The Portal and Browser Apps Installation Wizard opens.

3. Review the introductory text, and then click Next.
4. 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 click Next.
5. Select which Browser applications to install.

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

   Click Next.

6. Select Auto-Deploy options, then click Next.
7. Use the default location/folder in which to install the Browser installation files or click Change to browse to another location. We recommend accepting the default installation folder. For details about the default location, refer to the folder selection options. Click Next.
8. Click Install.
9. 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. Click Yes and configure it now, or configure it later by clicking **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.

10. Click Finish.

Configure the Browser Connection

Use the Connection Wizard (automatically launched by the Installation Wizard during the Portal and Browser App installation) to configure the Browser connection (direct-to-database/2-tier connection between the Browser applications and the CSM database). Most options are assumed or set by default to assist with decision making (ex: 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 Cherwell Client and 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 clicking 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 there is a prompt 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 click 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. Click Connect directly to a Cherwell database (this is a direct-to-database/2-tier connection), then click 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 click Next. For information on the database location options, refer to Browser Connection Options.

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

    Note: The last page of the wizard offers a test of 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 click Next. For more information on the options and requirements for these credentials, refer to Browser Connection Options.

7. Select connection pooling and security/failover options, then click Next. For more information on these options, refer to Browser Connection Options.

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

   Important: If the default connection name (Cherwell Browser) is not accepted, manually edit configuration files for the Browser applications.

9. Click Test Connection to verify the connection to the database.

   Tip: If the test fails, the installation can continue.

10. Click Finish.

Browser Connection Options

Database Location Options

In the course of configuring your Browser Connection, you will be required to specify the location of the Database server. The following table describes each database location option:

Option	Description	Notes
Database is on this machine	Run a local database.	Typically, this is only for evaluation systems.
Specific Server	Choose a database installed on a named server, and then provide the name of the **named server**, or select the named server in the drop down.	The drop down might take a few seconds to populate, and it is possible that the desired server will not be listed.
IP Address	Choose a database installed on a server referenced by an IP address, and then type the IP address.	

Database Login Account Credentials

In the course of configuring your Browser connection you will be required to specify the Database Login account credentials.

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.

The following table describes the database login account credentials options:

Option	Description	Notes
Windows Authentication	Use the stored Windows credentials (user name and password) for authentication.	
User ID and Password	Log in by providing the User ID and Password.	Recommended for browser connections

SQL Credentials Note: A different connection is used so that the Browser applications can run inside IIS. The connection needs to work with the security options for IIS.

The easiest way to accomplish this is to use SQL credentials to connect to the database (SQL Server must be configured for mixed mode authentication to support the use of SQL credentials). Select the User ID and Password radio button and enter the database account's user ID and password. This account needs to have rights to insert, update, and delete rows in the database.

The reason it is often better (or at least simpler) to use SQL credentials is that the Windows account that would need to be authenticated against SQL Server is the account being 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. Setting up Windows Authentication requires configuration of both IIS and SQL Server and is beyond the scope of this document.

Connection Pooling and Advanced Options

In the course of configuring your Browser Connection, you will be required to specify a series of connection options. The Connection Options page includes sections for Connection Pooling options and Advanced Settings.

Option	Description	Notes
Use default pooling options	Click this option to use the default pooling options.	This option is appropriate for most systems.
Customize pooling options	Click this option to specify custom pooling options.	This option is only for advanced users. Specify the pool sizes to customize the caching options.
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 sting.	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.	

Web Applications Installation Options

Auto-Deploy Options

In the course of running your Web Applications installation, you will be required 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 clicking 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 clicking 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**

Folder Selection

In the course of your Web Applications installation you will have the option to use the default location/folder in which to install the Browser installation files or click Change to browse to another location. The following table describes the default folders:

Option	Description	Notes
Default folder for **32-bit machines**	The default folder for 32-bit machines is: C:\Program Files\Cherwell Browser Applications.	

Option	Description	Notes
Default folder for **64-bit machines**	The default folder for 64-bit machines is: C:\Program Files (x86)\Cherwell Browser Applications	Even though CSM files are installed to the (x86) directory, CSM runs as a 64-bit application on 64-bit machines. The reason CSM installs to the x86 directory is that Windows installers do not easily support installing applications that are both 32-bit and 64-bit. CSM does not install to C:\Inetpub because IIS sometimes removes files in this directory in certain scenarios.
Change	Choose this option to browse to another location.	We recommend accepting the default installation folder.

Run the Client Installation

Launch the installation on the Client machine in the location 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. Double-click the **CSM Installation.exe** file.
2. Click Client.
3. Review the introductory text, and then click 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 click Next.
5. Select who can use CSM on the Client computer, and then click Next.
6. Use the default location/folder in which to install the Client installation files or change the location by clicking **Change**. We recommend accepting the default installation folder. For details about the default location, refer to Default Installation Folders. Click Next.
7. Select which CSM applications to install, and then click Next. For details on the setup types, refer to Client Setup Types.
8. Click Install.
9. When the install is complete, click 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. 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 Cherwell 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 clicking the **Connection** button.

   Manually open the Connection Wizard from the Connect to CSM window by clicking the **Add** button.

   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 click Next.

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

4. Specify where to find the Cherwell Application Server, and then click 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 click Next.

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

6. (Optional) Click 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 (first time install or paused), manually start it using the Server Manager (click Start>All Programs>Cherwell Service Management>Tools>Server Manager, then select the Cherwell Application Sever and click Start Server).

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

7. Click Finish.

CSM creates the Client connection.

Client Connection Options

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.	Use either HTTP or TCP, although this must match the configuration on the server. We recommend TCP (ex: tcp://CherwellServer).
Advanced	Select this link to specify Certificate Validation Mode settings. This option is for advanced CSM 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

Default Installation Folders

In the course of your Client installation you will have the option to use the default location/folder in which to install the Client installation files or click Change to browse to another location. The following table describes the default folders:

Options	Description	Notes
Default folder for **32-bit machines**	The default folder for 32-bit machines is: C:\Program Files\Cherwell Browser Applications	
Default folder for **64-bit machines**	The default folder for 64-bit machines is: C:\Program Files (x86)\Cherwell Browser Applications	Even though CSM files are installed to the (x86) directory, CSM runs as a 64-bit application on 64-bit machines. The reason CSM installs to the x86 directory is that Windows installers do not easily support installing applications that are both 32-bit and 64-bit. We do not install to C:\Inetpub because IIS sometimes removes files in this directory in certain scenarios.
Change	Choose this option to browse to another location.	We recommend accepting the default installation folder.

Client Setup Types

In the course of your Client installation, you will be 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, Definition Editor, System Upgrade/Restore, and Test LDAP)	

Logging in to CSM Applications

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

- CSM Desktop Client or CSM Administrator
- CSM Browser Client
- Cherwell Portal
- Cherwell Mobile™ for Android™
- Cherwell Mobile™ for iOS®
- CSM Definition Editor

To Login 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 login 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

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

The first time a User runs the Desktop Client, he needs download and install Auto-Deploy from the web page. After the initial installation, the User is prompted to install the new version.

To run Auto-Deploy:

1. Type the URL into the Auto-Deploy installation.

2. If you do not have the .NET Framework, click the Microsoft .NET Framework link to install it.

3. To install CSM, click the Cherwell Service Management link.
   The Open/Save download box appears for the download.

4. Run the file.
   Auto-Deploy launches. The Auto-Deploy options vary depending on how the system administrator configured Auto-Deploy.

Configuring Auto-Deploy

To configure Auto-Deploy:

1. Open Auto-Deploy:
   If Cherwell Application Server is installed: click Window Start>All Programs>Cherwell Service Management>Tools>Auto-Deploy Config

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

   > **Note:** If Auto-Deploy is not yet configured, there is a prompt when using the Auto-Deploy Wizard to configure Auto-Deploy.

2. Provide the information in the Auto-Deploy Configuration window:

   > **Important:** For first-time installations, Users must configure the Client connection during this step.

3. Provide the **Client connection**.

   Click the Ellipses button to select an existing Client connection. From the Browse window, click the Add button to create a new connection (for more information about creating a new connection, see the Connection Wizard).

   > **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.

4. Auto Deploy Site: Provide the **URL**.

5. Target Folder: Provide the **directory** on the server where the install files will be stored.

6. Select the applicable Options check boxes:
   Overwrite Client Connection

   Make Connection Be Default

   Require Users to Install Minor Releases

   Connect Without Prompting

   Display Debug Messages

7. Select the applicable Installation Options check boxes:
   Run Installer on Client Without Providing Any Options to User

   Install only the Cherwell Client application

   Install the Cherwell Client and the Administrative Tools

   Allow the User to choose what to install

This option is disabled if the Run Installer on client without providing options to the User check box is selected.

Install for all Users

8. Select the Install Under Specific Account check box.

9. Select an account or Add a new account. For additional information, see Install Accounts.

Note: The installer selects the first account with a domain name that matches the current domain. If there is no match, the installer selects the first account that has no domain specified. There can only be one install account per domain name.

10. Click OK.

Configuring Auto-Deploy Options

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 (ex: http://MyServer/CherwellAuto-Deploy).
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\CherwellAuto-Deploy.
Options	
Overwrite client connection	Overwrites any already-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 would be 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 (ex: 5.0a on top of 5.0) 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.
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.
Install for all Users	Allows Auto-Deploy to run for all Users.

Option	Description
Install under specific accounts	Runs the installer as the specified administrator User for added accounts. The installer selects the first account with a domain name that matches the current domain. If there is no match, the installer selects the first account that has no domain specified. There can only be one install account per domain name.

Install Accounts for Auto-Deploy

Auto-Deploy allows you to add multiple install accounts to the Auto-Deploy configuration. The installer runs through the accounts to find a domain that has installation rights.

To Add or Edit an Install Account for Auto-Deploy

1. Open the Auto-Deploy Configuration window.
2. Select the Install Under Specific Accounts check box.
3. Click Add or select an account and click Edit.
4. Provide the Domain name and User account. The format for the domain name is domain\account (ex: Cherwell/firstname.lastname).
5. Provide the Password for the domain/account.
   You should see the list of added accounts in the Auto-Deploy Configuration window.

   Note: The Validate button only verifies the Domain/Account that the User is currently on.

To Remove an Install Account

Select an install account and click Remove.

Licensing CSM

Licensing controls how many Users can log into CSM. CSM uses a concurrent or floating licensing model. 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.

To help manage licensing, CSM provides the Licensing window (CSM Administrator>Security>Licensing), where Users can:

- License CSM.
- Reserve a license for a particular User to guarantee a login spot.
- Automatically release a license after a specified idle time.

> **Note:** Most options in this window are only be available if there are licenses in place.

License Consumption

License consumption varies depending on the application, who logs in (User or Customer), and which operations each person performs:

- Only the following Cherwell applications require a license: Desktop Client, Browser Client, Cherwell Mobile™ (Cherwell Mobile™ for iOS®, Cherwell Mobile™ for Android™, and Cherwell Mobile™ for Browser), and the Outlook® Add-In. Under special circumstances, the Customer Portal 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 Customer 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 Customer 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™	✔
Cherwell Mobile™ for Browser	✔
Cherwell Portal™	✔ Sometimes (see People)

Item	Consumes License
CSM Administrator	✖
Supporting Applications	
Auto-Deploy	✖
Dashboard Viewer	✖
Definition Editor	✖
Import Utility (legacy)	✖
Outlook® Add-in	✔
Outlook Add-in Installer	✖
Report Runner	✖
System Restore/Upgrade	✖
Test LDAP	✖
Server applications	✖
Server Manager	✖
Cherwell Web-Forms™	✖
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 Portal to view/create/edit their own record (Requestor/record owner)*	✖
Customer logging into the 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 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 can edit another Customer's records without consuming a license (ex: Send an E-mail, Create a Journal, Rating a Record, etc.).	✔ (with exceptions)
* Some Portal Sites and activities require use of a license. CSM prompts the Customer if a license is required.	

Reserve a License

Use the *Reserve License* feature in the Licensing window to ensure that a license is always available for a:

- User: Reserve a license for the system administrator, so that he can always access CSM.
- Department: Reserve two licenses for the IT department so that members of that department can always access CSM.

> **Note:** This option is available only if a Department Holds Property is set on a Department field in the UserInfo Business Object (CSM Administrator>Blueprint>Edit UserInfo Business Object>General Page>Holds drop-down at the bottom of page). It is also recommended that this Field be validated with a list of legal Departments.

To reserve a license:

1. Open the Licensing window (CSM Administrator>Security>Licensing).

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

2. To reserve a license for a particular User:
   a. Click Add user.

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

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

      Tips: Press **Ctrl** to select noncontiguous Users. Press **Shift** to select contiguous Users. Click New User to create a new User Profile easily.

   c. Click OK.

      The User's Profile updates to reflect a reserved license (*Has reserved license* check box is selected).

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

3. To reserve one or more licenses for a particular Department:
   a. Click Add department.

      The Add Department License window opens.

   b. Select the department for whom to reserve a license.

   c. Select the number of licenses to reserve for that department.

   d. Click OK.

4. To free a license, select the User/department, and then click the Remove button.

5. To change the number of reserved licenses for a department, click the department, and then click the Edit button.

6. Click OK.

Automatically Release a License

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

- User inactivity (ex: Walked away with CSM open).
- A CSM Desktop Client crash.

Good to know:

- Configure the system to automatically log out idle Users, thus releasing licenses (CSM Administrator>Security>Edit Security Settings>Desktop Client page>Logout inactive users from Cherwell Client).
- The Browser Client, Customer Portal, and Mobile Clients automatically log out Users/Customers after a period of inactivity based on Browser application settings and IIS configuration.

To Automatically release a license:

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

Troubleshooting CSM Server Install with IIS

Installing IIS as an App Service

Follow these steps if having issues with installing CSM with IIS.

Verify the enabled features:

Note: These features must be enabled for IIS to work.

1. Go to **Windows Server Manager**, click Add roles and features.

   The Add Roles and Features window opens.

2. Click Next until the **Features** page opens.
3. Verify under 3.5: **Http Activation** (a window opens when this is selected asking ot Add feature that are required for HTTP activation. Click Add Features) and **Non-Activation** check boxes are selected. If not, select the check box.
4. Verify under 4.5: **Activation** is selected.
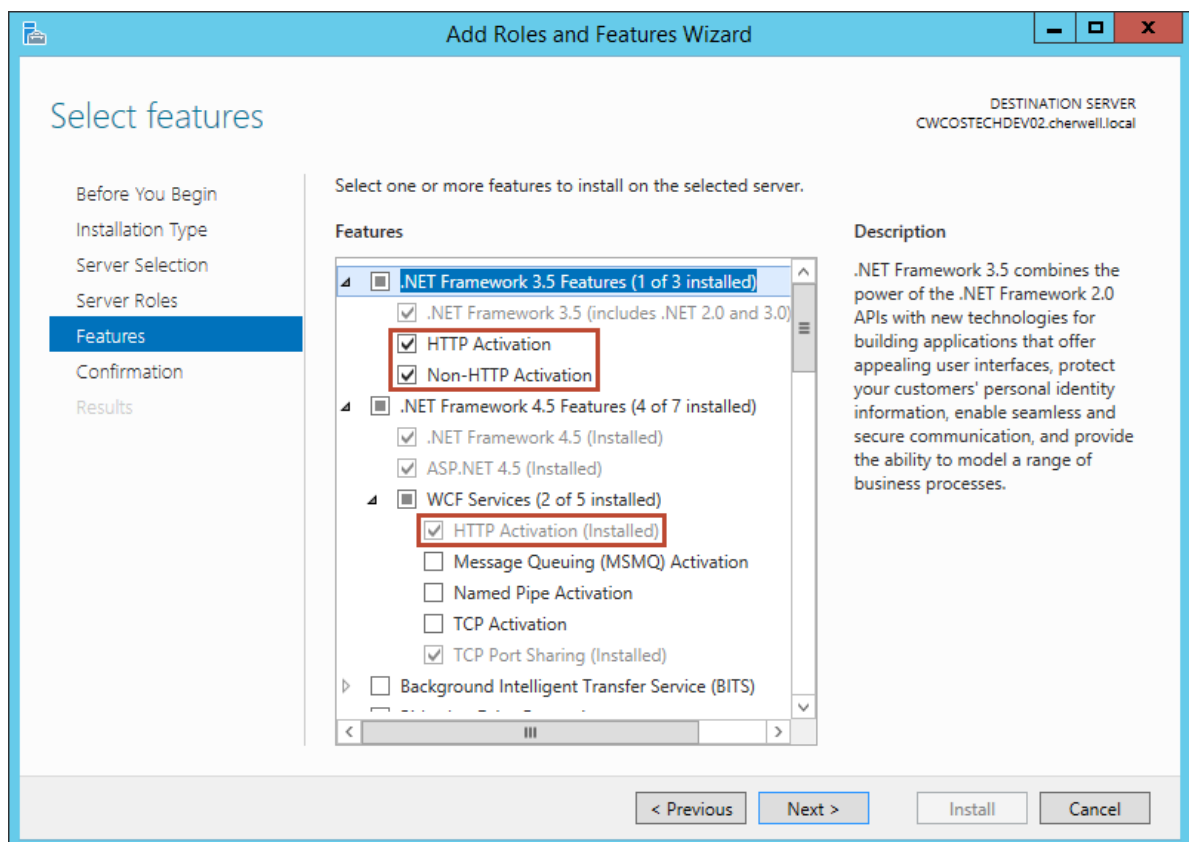
Verify the Server

1. Run the Server Installation.

2. Click the IIS Manager icon ![icon] in the Windows Task bar.
   a. Expand the Connections tree to verify the Cherwell App server is there.
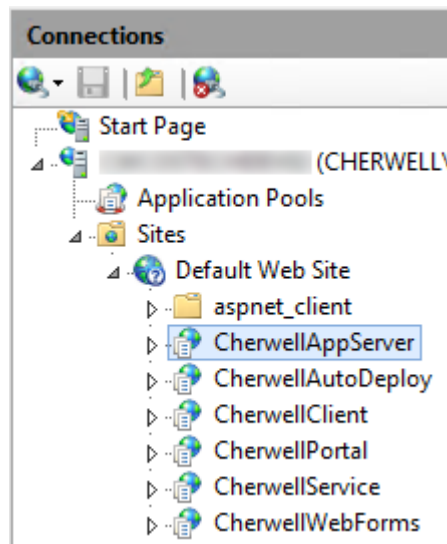
   b. Select Application Pools in the Connections Tree.

   c. Verify Cherwell App Server Identity field is Cherwell App Server or what was used in the Installation Wizard on the Account Selection page.

3. Open the Cherwell Server Manager.
   a. If it is started in IIS, the only available option should be Restart.
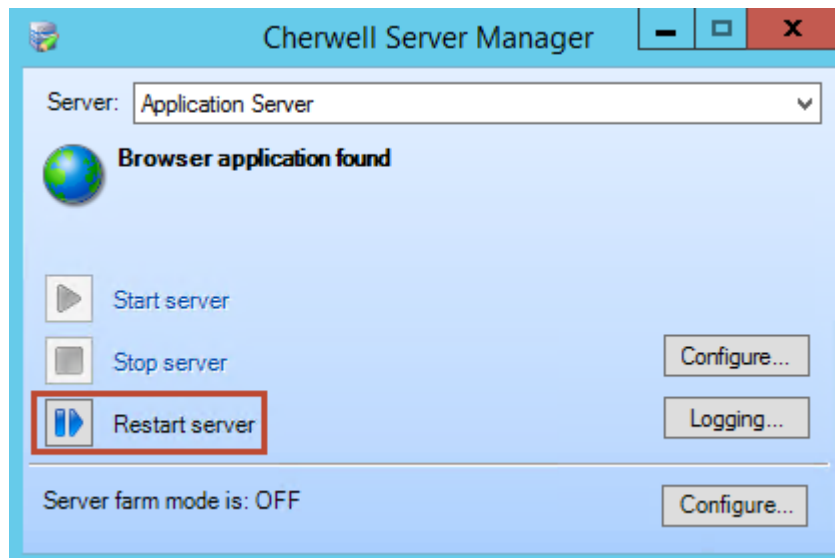
b. Click Configure.

The Server Configuration window opens.
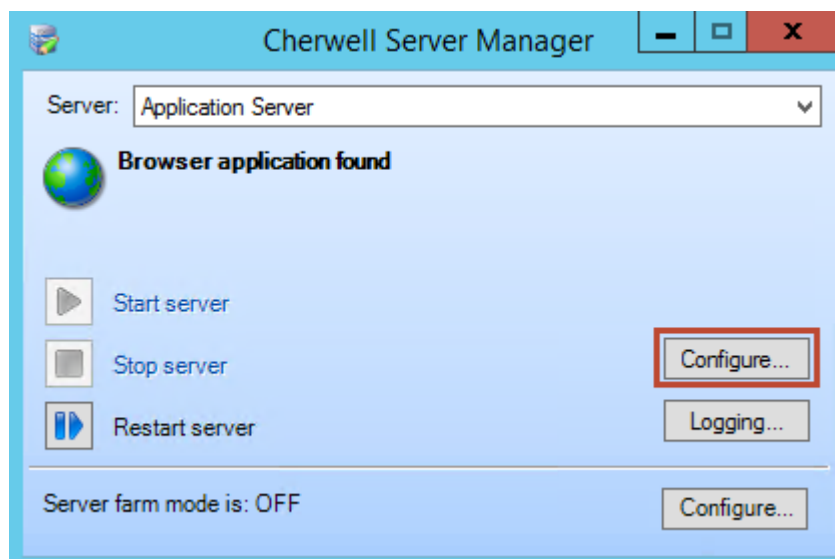
c. Click the ellipsis button.
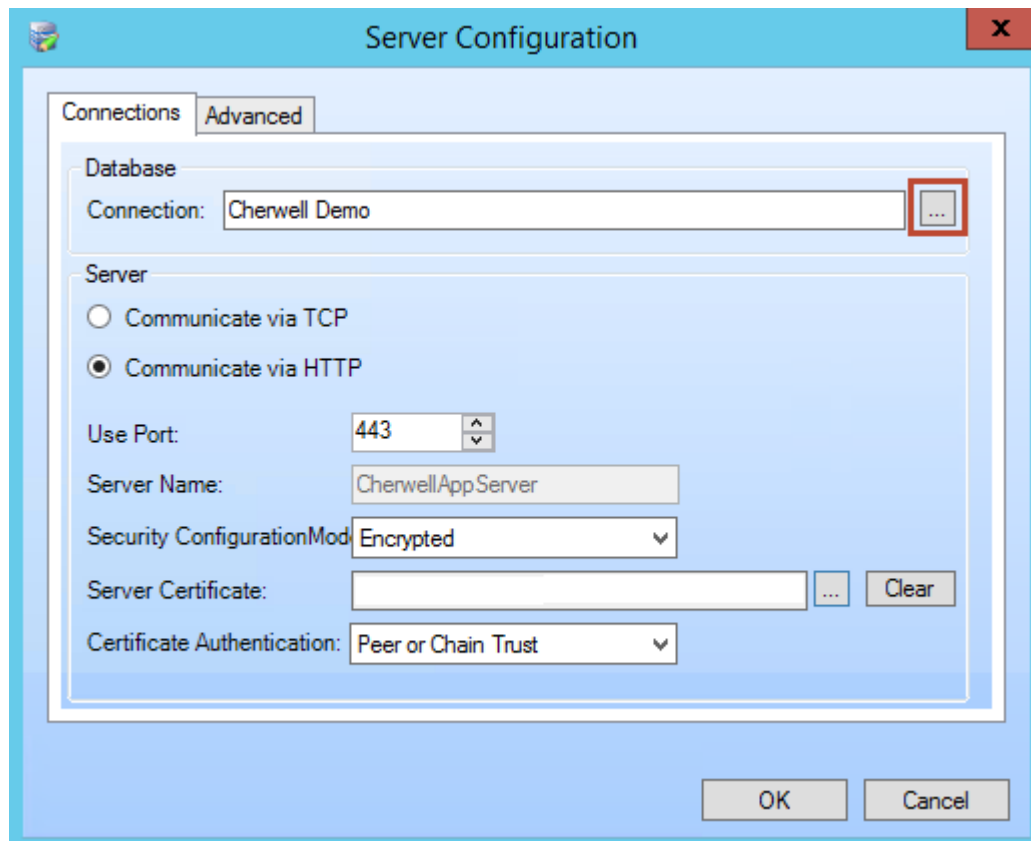
d. Select a **connection** and click Edit.

e. Go through Connection Wizard by clicking **Next**. Do not change any options.

f. At the summary page, click Test Connection.

If the connection fails, the issue is with the Database connection not IIS.
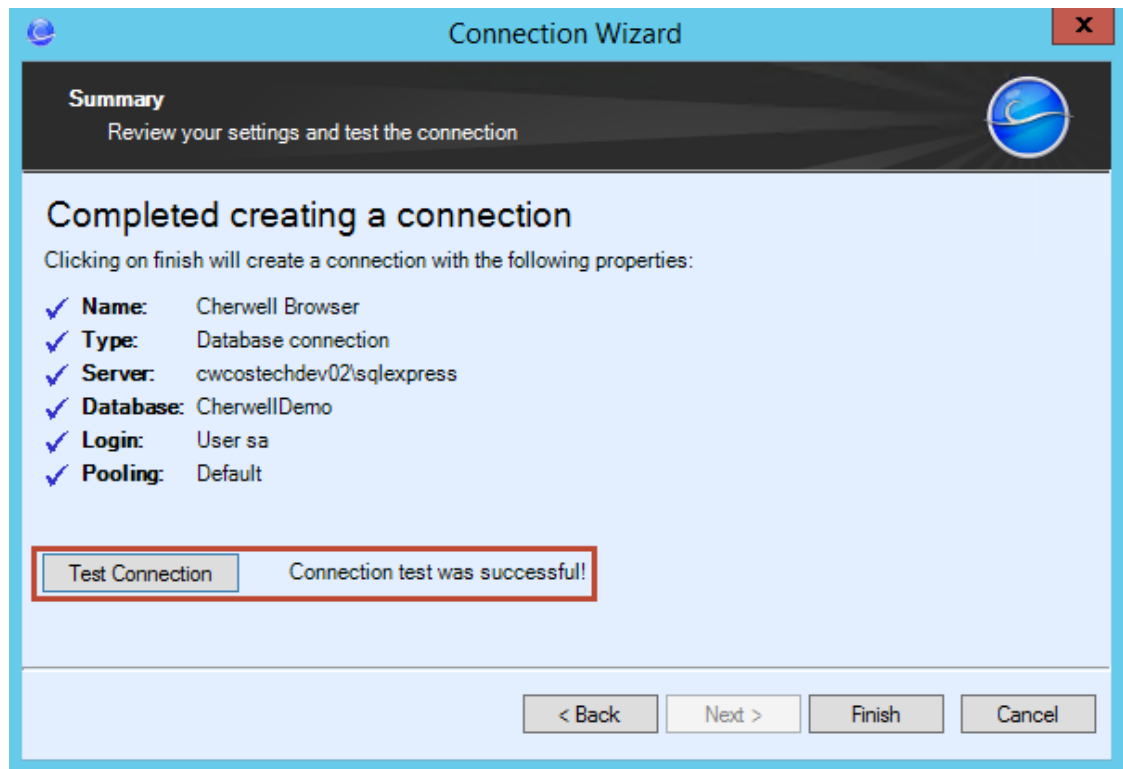
Verify the Server Manager and Connection

1. Go to the Server Manger
   a. Click Configure.

   The Server Configuration window opens.

   b. Verify the **HTTP** or **HTTPS** radio button is selected.

   c. Port: Should be 80 for standard HTTP or 443 for HTTPS.

   d. Security Configuration Mode: If using HTTPS, **Encrypted** should be selected from the drop-down.

   e. Sever Certificate: If this field is not auto-populated, use the ellipsis button to browse and select the certificate.
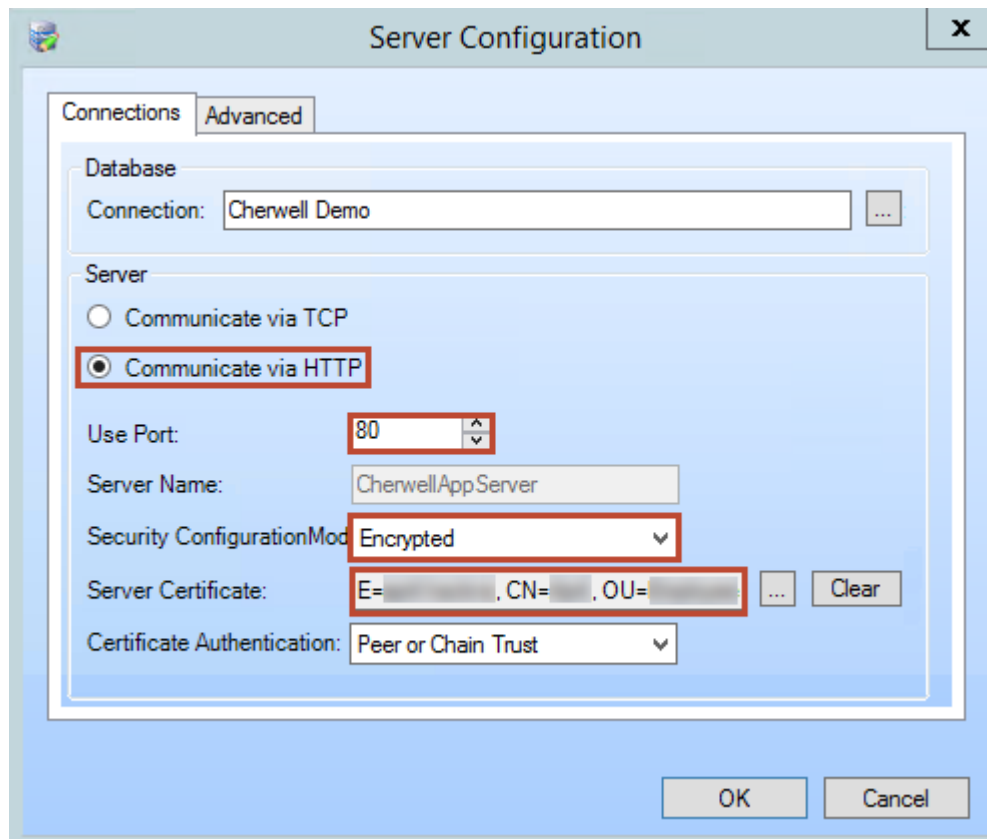
2. Click the ellipsis button to open the Connection window.

3. Click Add.

   The Connection Wizard opens.

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

4. On the pages of the wizard:
   a. Connection Type: Select Cherwell Server.

   b. URL: Provide the **URL** using **http** or **https** and then the server being used. For example, http://cherwell.company.

   c. Provide a **Name** and **Description**.

   d. Click Test connection (see previous screen shot of a successful connection).

Verify Using an URL:

1. Provide the following URL in a browser. For the instance of *Server* provide the server being used. HTTPS or HTTP should be in the URL depending on what was selected during setup.

```
HTTP://Server/CherwellAppServer/Rest.svc
```

A web page should open that shows *Service*.

Installing CSM from the Command Line

During the CSM installation, an advanced User can use a command line to specify where and what features to install, as well as some selected security rights. This procedure is for advanced Users only.

Note: Do not run the Client and Server installations on the same system (the Server install includes the Client install).

Cherwell Client Installation

Options	Definition	Values
ALLUSERS	Install Client application files for all Users or current User.	• 1 = Files are installed for all Users (anyone who uses the computer). (default) • 2 = Files are installed for current User.
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.

The following is an example command line that will install the client applications and the Administrator tools (CSM Administrator, Report Runner, Definition Editor, System Upgrade/Restore, and Test LDAP) for all Users:

```
msiexec /i "Cherwell Client.msi" /qn ALLUSERS=1 INSTALLLEVEL=10
```

Cherwell Web Applications

Note: Installs for ALL USERS by default.

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

CWBROWSWERCLIENT	Install Cherwell Browser Client.	• 1 = Install (default) • 0 = Do not install
CWAUTODEPLOY	Install Auto-Deploy.	• 1 = Install (default) • 0 = Do not install
CWWEBSERVICES	Install the Web Service.	• 1 = Install (default) • 0 = Do not install
CWWEBFORMS	Install Web-Forms.	• 1 = Install • 0 = Do not install (default)
INSTALL_AUTODEPLOY	Select whether or not to update the Auto-Deploy configuration.	• 1 = Update (default) • 2 = Installs the Auto-Deploy feature silently. **Note:** If you install silently, you must manually configure Auto-Deploy to wrap and distribute the most current client installation.
INSTALLDIR	Location/folder in which to install the Browser application files.	[ProgramFilesFolder]Cherwell Browser Applications (default)

The following is an example command line that will install to the default directory, will NOT install the Portal, WILL install the Web-Forms, and WILL update Auto-Deploy:

```
"Cherwell Browser Apps.exe" /s /v"/qn CWPORTAL=0 CWWEBFORMS=1 CWAUTODEPLOY=
1"
```

Cherwell Server

Note: Installs for ALL USERS by default.

Options	Definition	Values

`INSTALLDIR`	Location/folder in which to install the Server installation files.	[ProgramFilesFolder]Cherwell Service Management (default)

Database selection

Note: The Connection Wizard is launched only for 1, 2, or 3.

`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
`USE_LOCALIZED_CONTENT`	Specify whether to install all supported languages with the selected database. This option is only available if you select a demo or starter database.	• 1 = Install • Argument not included (default) = Do not install **Important:** To exclude the additional languages from the installed database, you must leave out this argument or set it to an empty string.

Service Selection Select which CSM Servers (services) to install.

`SERVERSERVICE`	Install the Application Server.	• 1=Install (default) • 0= Do not install
`BUSINESSPROCSERVICE`	Install the Automation Process Server.	• 1 = Install (default) • 0 = Do not install
`SCHEDULINGSERVICE`	Install the Scheduling Server.	• 1 = Install (default) • 0 = Do not install
`EMAILSERVICE`	Install the E-mail and Event Monitoring.	• 1 = Install (default) • 0 = Do not install

Logon Information

`IS_NET_API_LOGON_USERN` `AME`	Cherwell Server account username that will be used to launch the CSM Servers (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. Ex. Cherwell \Henri.Bryce
`IS_NET_API_LOGON_PASSW` `ORD`	Cherwell Server account password that will be used to launch the CSM Servers (services).	Blank (default), but information is required.
`USE_SP_ACCOUNT`	Use special account (Windows account) to launch the CSM Servers (services).	• 1 = True • 0 = False (default)
`CWSPECAILACCOUNT`	Name of special account that will be used to launch the CSM Servers (services).	• LocalSystem (default) • LocalService • NetworkService
`CWAPPSERVERIIS`	Install the Application Server as a web application under IIS.	• 1 = True (default) • 0 = False

Cherwell Service Monitor

Note: Installs for ALL USERS by default.

Available Settings	Definition	Default Values
`INSTALLDIR`	Location/folder in which to install the Service Monitor files.	[programfilesfolder]\Cherwell Service Management (default)
`CW_ISPRODUCTION`	Type of server to be monitored.	• True = Production (default) • False = Non-production

CW_TITLE	Title to be displayed on the Service Monitor web page.	Cherwell Service Monitor (default)
CW_DEFAULTACCESSISREADONLY	Default access to the Service Monitor. This is the default access for Users who are not explicitly given access through the Read/Write Permissions List.	• 1 = Read-only (default) • 0 = Access denied.
The following are set only through the command line. **Note:** View = Read-only access (ex: View service status in the Service Monitor but no edit); Edit = Full read/write access (ex: View service status AND start/stop/restart services in the Service Monitor.		
CW_USERSWHOCANALWAYSEDIT	List of Users who explicitly can edit the Service Monitor (full read/write access).	Blank (default), but information is required. Comma delimited list of Users. Format: DOMAIN\Username if the server is joined by a domain. Ex. Cherwell\Henri.Bryce
CW_USERSWHOCANNEVEREDIT	List of Users who explicitly cannot edit the Service Monitor (access denied).	
CW_ANONYMOUSUSERCANVIEW	Non-authenticated Users can view but not edit (read-only access).	• True • False (default)
CW_ANONYMOUSUSERCANEDIT	Non-authenticated Users can edit the Service Monitor (full read/write access).	• True • False (default)
CW_ADMINISTRATORSCANVIEW	Allow Users in the OS-level Administrator Group to view but not edit the Service Monitor (read-only access).	• True • False (default)
CW_ADMINISTRATORSCANEDIT	Allow Users in the OS-level Administrator Group to edit the Service Monitor (full read/write access).	• True • False (default)

The following is an example command line:

```
"Cherwell Service Monitor.exe" /s /v"/qn CW_USERSWHOCANALWAYSEDIT="user lis
t" CW_DEFAULTACCESSISREADONLY="1""
```

Anything Variable that is passed and has spaces requires the quotes be proceeded by a \. If there are not spaces, this is not required ; however, it will not hurt anything if they are used:

"Cherwell Service Monitor.exe" /s /v"/qn CW_USERSWHOCANALWAYSEDIT=\"user list\" CW_DEFAULTACCESSISREADONLY=\"1\""

Security

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

About Security

Security components include:

- **Security Group:** A Security Group is at the heart of CSM security. A Security Group is a collection of CSM security rights that controls access to CSM functionality and data (Business Objects/fields). Each User/Customer is assigned to only one Security Group. The User/Customer then inherits the security rights of that Security Group, as well as access to the Roles assigned to the Security Group. Examples of Security Groups include Admin, IT service desk manager, and Portal End-User.

- **Role:** A Role is a User/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/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.

- **User:** 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).

- **Team:** 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.

- **Customer:** 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 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).

- **Customer Workgroup:** 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.
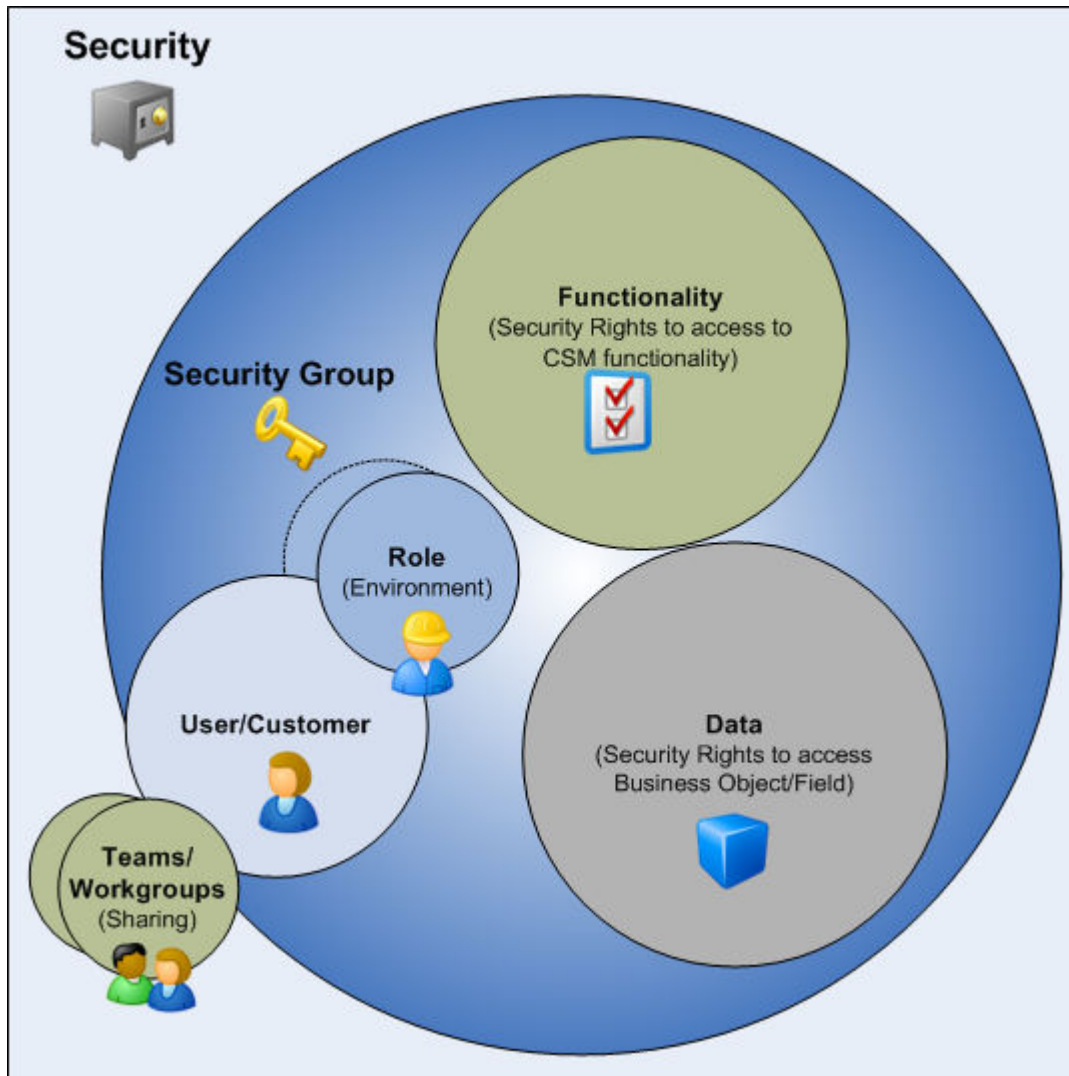
CSM provides an OOTB security design (complete with Security Groups, Roles, Teams/Workgroups, and system security settings). Implement this OOTB design (and just add Users/Customers, assigning them to other OOTB Security Groups, Roles, and Team/Workgroups), edit it, or create a new security design.

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

Security Window

Use the CSM Administrator Security page (CSM Administrator>Security) to:

Action	Description
Edit Users	Opens the User Manager to manage User Profiles.
Edit Security Groups	Opens the Security Group Manager to manage Security Groups.
Edit Roles	Opens the Role Manager to manage Roles.
Edit Teams and Workgroups	Opens the Team and Workgroup Manager to manage Teams and Workgroups.
Edit Security Settings	Opens the Security Settings window to configure general system security settings.
Edit REST API Client Settings	Opens the REST API clients window.
Edit SAML Settings	Opens the SAML Settings window to configure SAML **Note:** For more information about SAML, refer to the SAML documentation.
View Currently Logged-in Users	Opens the Logged-In Users window to view and manage logged-in users.
Lock the System	Opens a window to lock/unlock the system.
Licensing	Opens the Licensing window to manage CSM licensing.
Audit Log	Opens the Audit Log to view login logs.

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>Edit security groups>[Security Group]>[Tab]):

- Rights tab: Use this tab to configure access to functionality; specifically View, Add, Edit, Delete, Allow, Run, and Open rights.
- Business Objects tab: Use this 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/Customer is assigned to one and only one Security Group. The User/Customer then inherits the security rights of that Security Group.

Security Considerations

When designing a security strategy, consider the following:

- **Security rights:** 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 (CSM Administrator>Security>Edit Security Groups>"Security Group">Rights>Security features). For more information, see security rights.

- **Licensing:** 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). For more information, see License Consumption.

- **Users and Customers:** 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.

- **Ownership:** Different record ownership rights can be set to extend/deny access to Users/Customers, managers, departments, Teams/Workgroups, and Team/Workgroup managers. Be sure to consider the implications of Relationships and setting different rights based on ownership. For more information, see Record Ownership.

- **Scope:** 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. For more information, see Scope.

Differences Between Users and Customers

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 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 (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 For more information about licensing, see License Consumption.	Users consume a license when logging in to CSM (Desktop Client or Browser Client).	A Customer logging in to CSM through the 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 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 For more information about security groups, see User and Customer Security Groups.	Assigned to a User Security Group.	Assigned to a Customer Security Group.
Team For more information about Teams, see Teams and Workgroups.	Member of a Team.	Member of a Customer Workgroup.
Ownership For more information about ownership, see Record 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 CSM Browser Client through a browser. For more information about the Browser Client, see Browser Client.	Accesses the CSM Portal through a browser. For more information about the Portal, see Portal Client.

Record Ownership

Record ownership is an important concept in CSM because it affects security and licensing: security because ownership controls who has particular rights to a record and licensing because non-owners typically require a license to edit a record via the 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.

To set record ownership:

1. Open the Business Object Properties window:
   a. 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.

   b. In the Object Manager, click (New Object) in the Object tree, and then click 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 click the Bus Ob Properties button.

      To open the Business Object Editor:

      i. 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, showing the Object Manager in its Main Pane. The Object Manager lists the existing Business Objects.

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

Tip: You can also click the Edit Business Object button [image] on the Blueprint Editor Toolbar to open the Business Object Editor.

2. To activate ownership tracking for a Business Object:

Select the Track owner check box to track Business Object ownership by User.

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.

3. Set the Record Ownership Holds property.

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

4. Set Business Object rights based on ownership: Business Object rights are set at the Business Object level in a Security Group (CSM Administrator>Security>Edit security group>[User/Customer Security Group]>Business Objects tab>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.

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 on the Field's General tab.
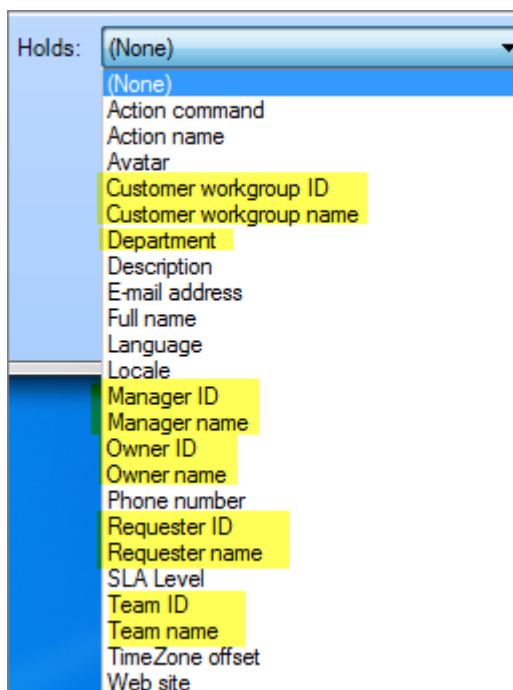
Record Ownership Value Considerations

- 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 OOTB User Profile and Customer Record. For example, we assumed that the record owner manager is the manager

listed on the User Profile (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 our OOTB Starter database but you can manually add them.

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

Record Owner	Description	Holds Value	Example Business Object.Fields
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.

Set a Record Ownership Holds Property

To set a record ownership Holds property:

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. Click Edit business object.

2. Set the property on the Ownership field:
   a. Double-click the icon in front of the Field.

   b. Click the General page.

   c. In the **Holds** drop-down, select a record ownership value.

   d. Click OK.

Set a Record Ownership Holds Property 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. Click Change Request, and then click 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. Click the Field Properties button.

    b. Click the General page:
        i. In the Holds drop-down, select the Customer Workgroup name ownership attribute. This tells CSM that the Workgroup in this Field is a record owner.

    c. Click the Validation/Auto-populate page:
        i. Select the **Other validation types** check box to expand the section.

        ii. Select the **Valid Team or Workgroup** radio button, and then select All customer workgroups. This tells the Field to list all the valid Customer Workgroups.

    d. Define additional Field properties as necessary: Full-Text Search, default values, etc.

    e. Click 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. Click the Field Properties button.

    b. Click the General page:
        i. In the Holds drop-down, select the Customer Workgroup ID ownership attribute. This tells CSM that the Workgroup in this Field is a record owner.

    c. Click the Validation/Auto-populate page:
        i. Select the Auto-populate check box to expand the section.

        ii. In the *Populate when there is a change in table: [ITEM] field* drop-down, select Owned By Workgroup.

        iii. Select the Customer workgroup ID radio button.

      d. Define additional Field properties as necessary: Full-Text Search, default values, etc.

      e. Click 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.

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™ 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-Steps, 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-Steps, 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-Steps, 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

Use Security Groups to implement different levels of security. For example:

- **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 (ex: Business Objects/Fields).
- **File Attachments:** Attachment security rights (ex: 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.

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

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.
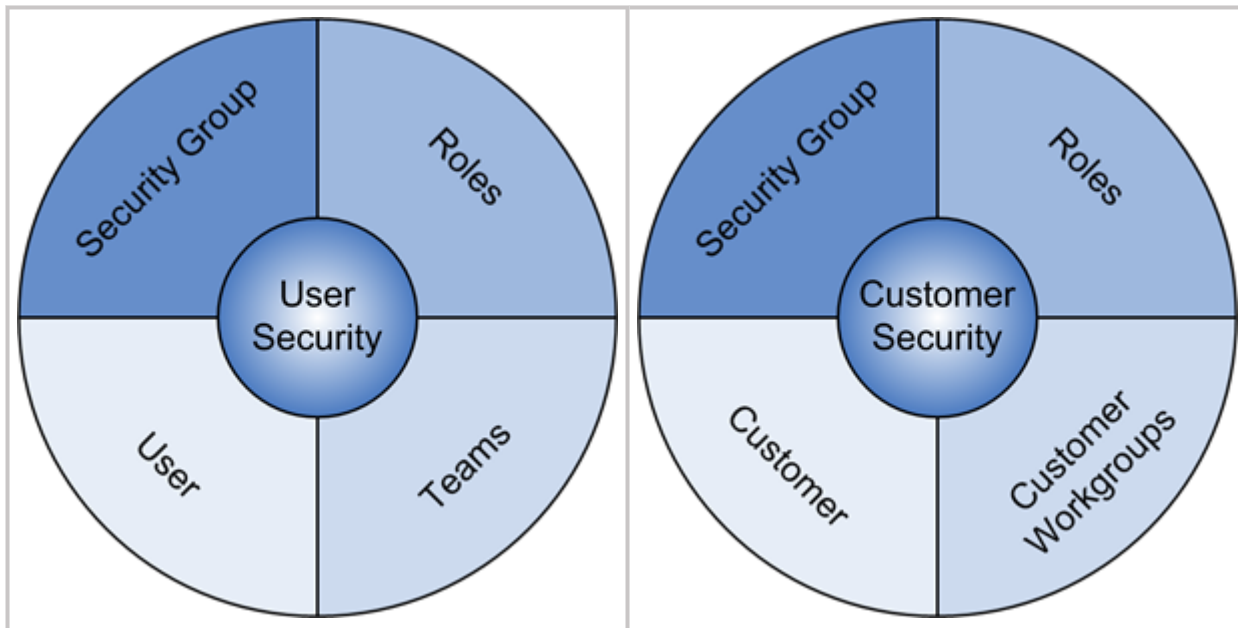
> **Note:** CSM provides several OOTB Security Groups, both User (Admin, IT Service Desk, IT Service Desk Manager) and Customer (Portal Customer and Manager). You can use these OOTB Security Groups as-is, edit them, or create your own using the Security Group Manager.

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 is used for Users/Customers who need to access CSM Browser and Mobile Applications without logging in.

- The Browser and Mobile Clients use the Anonymous Security Group to read basic setup information from the system before the User technically logs in.
- The Portal Client uses the Anonymous Security Group to define permission for Customers accessing Sites that do not require a login.

An Anonymous Security Group is required for the Browser and Mobile Clients to work. Anonymous Security Group should have limited rights. However, it should have rights to run Search Groups and Full-Text Searches. If anonymous access to RSS feeds is allowed, the Security Group should also have access to Business Objects accessible via RSS.

Use the Security Settings window (CSM Administrator>Security>Edit security settings>General page) to enable anonymous access and to tell CSM which Security Group to use for anonymous logins.

Note: The CSM Starter Database provides an OOTB Anonymous Security Group.

Managing Security Groups

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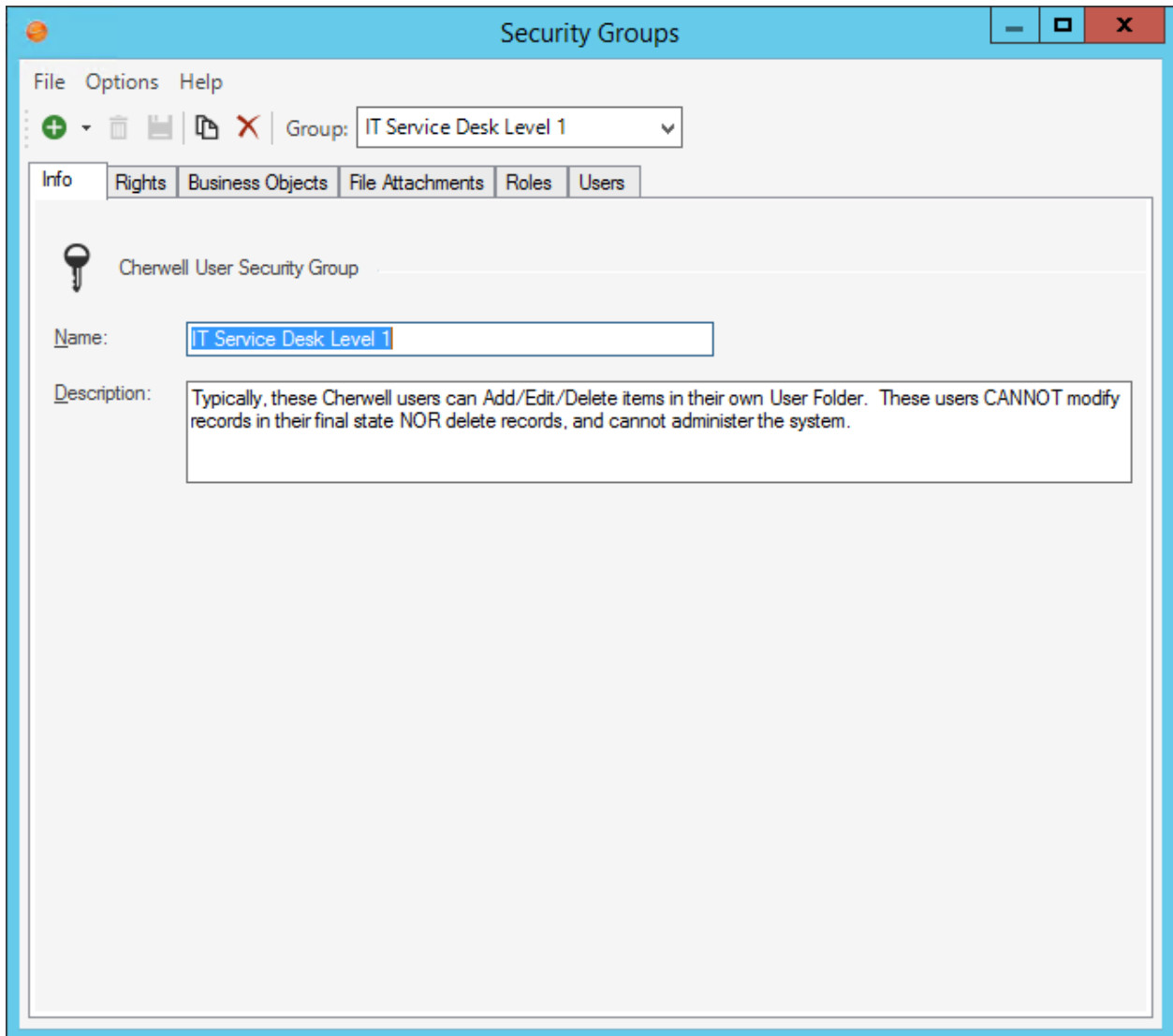
Use the Security Group Manager to:

- 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.

Open the Security Group Manager

To open the Security Group Manager from the CSM Administrator main window, click the Security category, and then click 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

2. Click 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. Click Save .

Define General Information for a Security Group

To Define general information for a Security Group:

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 Info tab.

4. Define the general properties:
   a. Name:

      The name of the new Security Group (this property can be searched in CSM Item Managers).

   b. Description:

      A description of the type of User that belongs to the new Security Group and an explanation of when it should be used (this property can be searched in CSM Item Managers).

5. Click 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 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. In the Group drop-down, select the Security Group for which you want to define rights (example: Admin).
3. Click the Rights tab.
4. Category: Select the CSM functionality category for which you want to set rights (example: Dashboards, Calendars, etc.). Notable categories include:

Option	Description
Default right	Sets default rights for all functionality in a Security Group, use. 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 rights for functionality, those rights override the default. You can override the default at any time by manually setting rights for functionality.
Application rights	Houses basic CSM functionality rights, such as Table Management, Grid/Toolbar/Task Pane personalization, etc.
Security features	Houses security feature rights, such as system settings, Role/Team management, SAML settings, etc.
Sites	Houses Portal Site rights

A list of associated subcategories displays below the category.

5. Subcategory: Select the functionality for which you want to set permissions. 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

> **Note:** Many rights are scope-related (User, Role, Team, Global), meaning they allow/deny access to an item based on an intended audience.

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

7. Click Save .

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

1. Open the Security Group Manager

2. Click the Rights tab.

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

4. Click the Run the administrator tool? security right

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

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, 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.

   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. Please note that 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 the check boxes to allow the Security Group permission to perform the operation. Clear the check box to deny permission. Rights include a combination of the following:
      View: Data/record can be viewed.

      Add: Data/record can be added.

      Edit: Data/record can be modified.

      Delete: Data/record can be deleted.

      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 will be seen by the User. Not only will searches be limited, but Dashboard Widgets will show only included records, as will Reports, and all other features of the system.

Can edit the final state: Data/record can be edited when it is in its defined final state.

Note: This option is only available if the Business Object has a final state, such as Closed. Typically, this Right is limited to managers and system administrators.

Can change the final state to the recall state: Data/record can be changed from its final defined state to a different lifecycle state.

Note: This option is only available if the Business Object has a final state (such as Closed) and a recall state (such as 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 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 to which rights have not been set.

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 the check boxes to allow the Security Group permission to perform the operation. Clear the check box to deny permission. Rights include a 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. Click Save .

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:

- Which Attachment operations the Security Group can perform (ex: 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 (ex: 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 (ex: 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 radio button 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 (ex: pdf), separated by a comma, either by typing directly in the Extensions box, or by clicking the **Choose File Types** button 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 clicking the

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

Tip: To restore the OOTB default file types, click the Restore to Cherwell defaults button .

6. Click Save .

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. 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, select the Security Group for which you want to define rights (ex: Admin).

3. Click the Roles tab.

    A list of assigned Roles (legal Roles) opens.

4. Click the Add button.

    The Add Role to Security Group window opens, listing the available CSM Roles (Roles not already in the Security Group).

5. Click the Role you want to assign to the Security Group or click the **New Role** button to create a Role on-the-fly.

6. Click OK.

7. Designate a default Role by clicking a **Role**, and then clicking 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 logs in using their default Role.

    Note: Click the Remove button to remove a Role from the Security Group.

8. Click Save .

Assign Users to a Security Group

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

Good to know:

- A User is (and must be) assigned to one and only one Security Group at a time. If you reassign an existing User to a Security Group, you will be removing that User from another Security Group.

    Note: The Security Group is stored in the User's Profile; therefore, you can assign a User to a Security Group when you edit a User Profile or when you edit a Security Group (below).

To assign a User to a Security Group:

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 Roles tab.
4. Click the Add button.

    The Add User to Security Group window opens, listing the available Users (Users not already in the Security Group).

5. Click the User you want to assign to the Security Group or click the **New User** button to create a new User Profile.

6. Click OK.

    Note: Click the Move To button to move a User from the Security Group to another Security Group; click the **Import** button to import a User from Windows or AD/LDAP.

7. Click Save .

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.

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/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/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.

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

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.
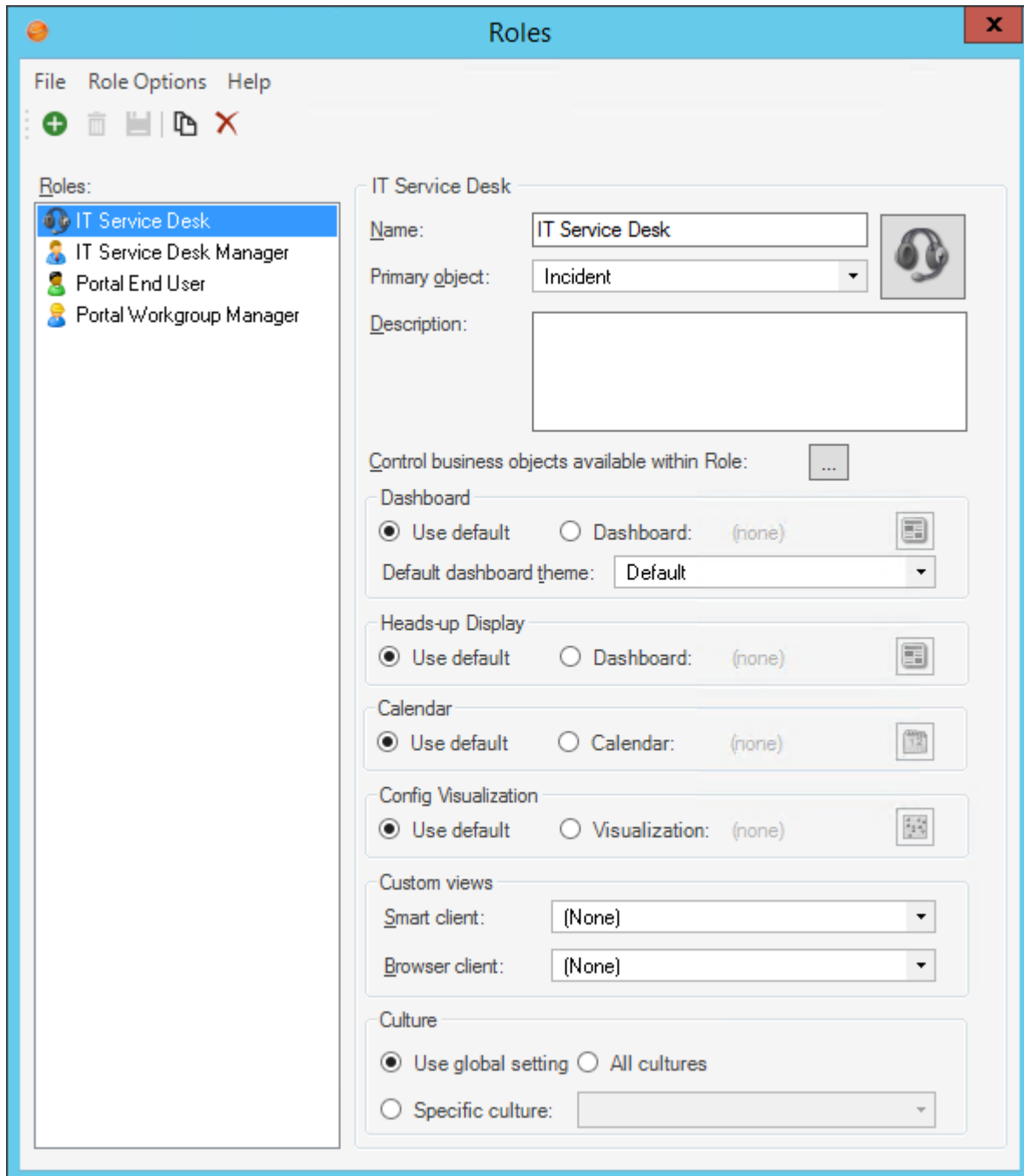
Use the Role Manager to:

- 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. 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 newly added items, searches, etc. (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 (ex: 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 Browser Clients (Portal for Customers and Browser Client for Users).
- Culture: Determines the cultures available for Users assigned to the Role.

  Culture options are only enabled when globalization is enabled for your system. For more information, see Enable Globalization.

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.
- 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.

The Manager lists the existing Roles.

2. Click the Create New button ⊕.

   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:

      Click 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.

   c. Primary Object: Select a **primary Business Object** for the Role.

   d. Description:

      Provide a description to use within CSM (this property can be searched in CSM Item Managers).

   e. Control Business Objects available with this Role: Select the 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 radio button 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).

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

   Note: 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 clicking 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 Browser Clients (Portal for Customers and Browser Client for Users).

   Note: Typically, Customers will have a limited Portal view.

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

7. Click Save .

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.
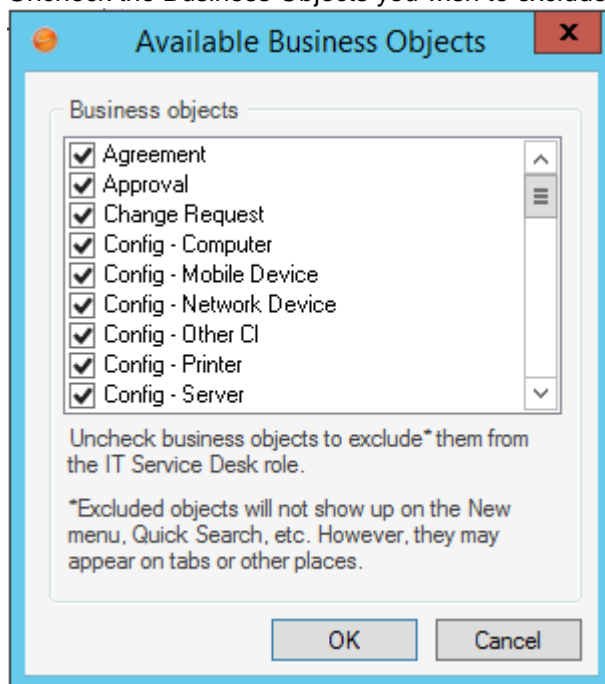
Click OK.

About Teams and Workgroups

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.

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

OOTB Teams and Workgroups

CSM provides several OOTB Teams and Workgroups.

OOTB User Teams:

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

OOTB Customer Workgroups:

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

Use these OOTB 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 a Team/Workgroup.
- Create a Customer Workgroup.
- Create a Team.
- Edit a Team or Workgroup.
- Delete a Team or Workgroup.

Open the Team and Workgroup Manager

To open the Team/Workgroup Manager from the CSM Administrator main window, click the Security category, and then click the Edit Teams and Workgroups task.

View Team Information

The Team Info Business Object creates a lookup table based on the information in Security Teams and Workgroups. Users can access Team Info from:

- A Blueprint Lookup table or Security Teams and Workgroups in CSM Administrator.
- Table Management in the CSM Desktop Client.

> **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. Click Team Info Business Object.
4. Click the Edit data task.

   The Edit Blueprint Data - Team Info objects window opens.

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

> **Note:** For more information on Blueprints and the the Blueprint Editor, see Using Blueprints.

To view Team Info from **Security in CSM Administrator:**

1. Open the Team and Workgroup Manager

To view Team Info in the CSM Desktop Client:

1. Open the Table Management Interface
2. In the Type drop-down, select Team Info.
3. Double-click a **Team Info object** to view the details.

Team Information Synchronization

The information across locations of Team Info is synchronized to keep information current. 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, click the Database category, and then click the System maintenance task.

   The System Maintenance window opens.

2. Select the Synchronize Team Info Business objects with team list check box.

3. Click OK.

Create a Team

Use the Team and Workgroup Manager in CSM Administrator to create a Team or a Customer Workgroup. When you create a Team/Workgroup, you define:

- Info: Name, description, and e-mail information for the Team.
- Members: Users on the Team.

Good to know:

- 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. Click the **User Teams** radio button.

   The Manager lists the existing Teams.

3. Click the Create New button ⊕.

   A [New] Team is added to the list.

4. Define general information for the Team:
   a. Click the Info tab.

   b. Name: Provide a **name** for the Team.

   c. Image:

   Click 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. Description:

   Provide a description to use within CSM (this property can be searched in CSM Item Managers).

5. Define options for determining how e-mails are sent to the Team (when the Team is chosen as an e-mail recipient):
   a. Send to All Members Who Have a Valid E-mail Address: Select this radio button to send e-mails 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 e-mail alias (ex: Admins@mycompany.com) to send e-mails to an already defined e-mail alias. This option is useful if a company has created an e-mail alias (ex: Company Administrators), which mirrors the membership of the Team.

6. Add Users to the Team:

    a. Click the Members tab.

    b. Click the Add button.

        The Add Team Member window opens.

    c. Click one or more Users to add to the Team.

        Tips: Press **CTRL** to select noncontiguous Users. Press **SHIFT** to select contiguous Users. Click New user to create a new User Profile on-the-fly.

    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.

        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. Click OK.

    The User(s) are added to the Team.

7. Click Save 💾.

Add a User to a Team

To add a user to a Team, perform the following steps:

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

   Tip: Click New user... to create a new User Profile on the fly.

5. Click OK.

To designate a 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.

Create a Customer Workgroup

Use the Team and Workgroup Manager to define the following for a Customer Workgroup:

- Info: Name, description, and e-mail information about the Workgroup.
- Members: Customers in the Workgroup.

Good to know:

- 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 **User Teams** radio button.
3. Select the **Customer Workgroup** radio button.

   The Manager lists the existing Workgroups.

4. Click the Create New button 🟢.

   A [New] Workgroup is added to the list.

5. Define general information for the Workgroup:
   a. Click the Info tab.

   b. Name: Provide a **name** for the Workgroup.

   c. Image:

   Click 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. Description:

   Provide a description to use within CSM (this property can be searched in CSM Item Managers).

6. Define options for determining how e-mails are sent to the Workgroup (when the Workgroup is chosen as an e-mail recipient):
   a. Send to All Members Who Have a Valid E-mail Address: Select this radio button to send e-mails to all of the addresses for all Customers in the Workgroup (based on the member list created in the next step).

   b. Send to This Alias: Select this radio button, and then provide the e-mail alias (ex: Admins@mycompany.com) to send e-mails to an already-defined e-mail alias. This option is useful if a company has created an e-mail alias (ex: Company Administrators), which mirrors the membership Workgroup.

7. Add Customers to the Workgroup:
   a. Click the Members tab.

   b. Click the Add button.

      The Contact Manager opens.

   c. Click a **Customer** to add to the Workgroup, and then click OK.

   d. 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.

   e. Click OK.

   The Customer is added to the Workgroup.

8. Click Save ■.

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).

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, contact information, etc.

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

- Account details: Password resets, reserved licenses, etc.
- Assigned Security Group.
- Assigned Teams.

User Profiles are managed (created, viewed, imported, deleted, etc.) as part of Security in CSM Administrator using the User Manager.

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 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.

User Manager

Use the User Manager to complete the following User Profile operations:

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.

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, click the Security category, and then click the Edit Users task.
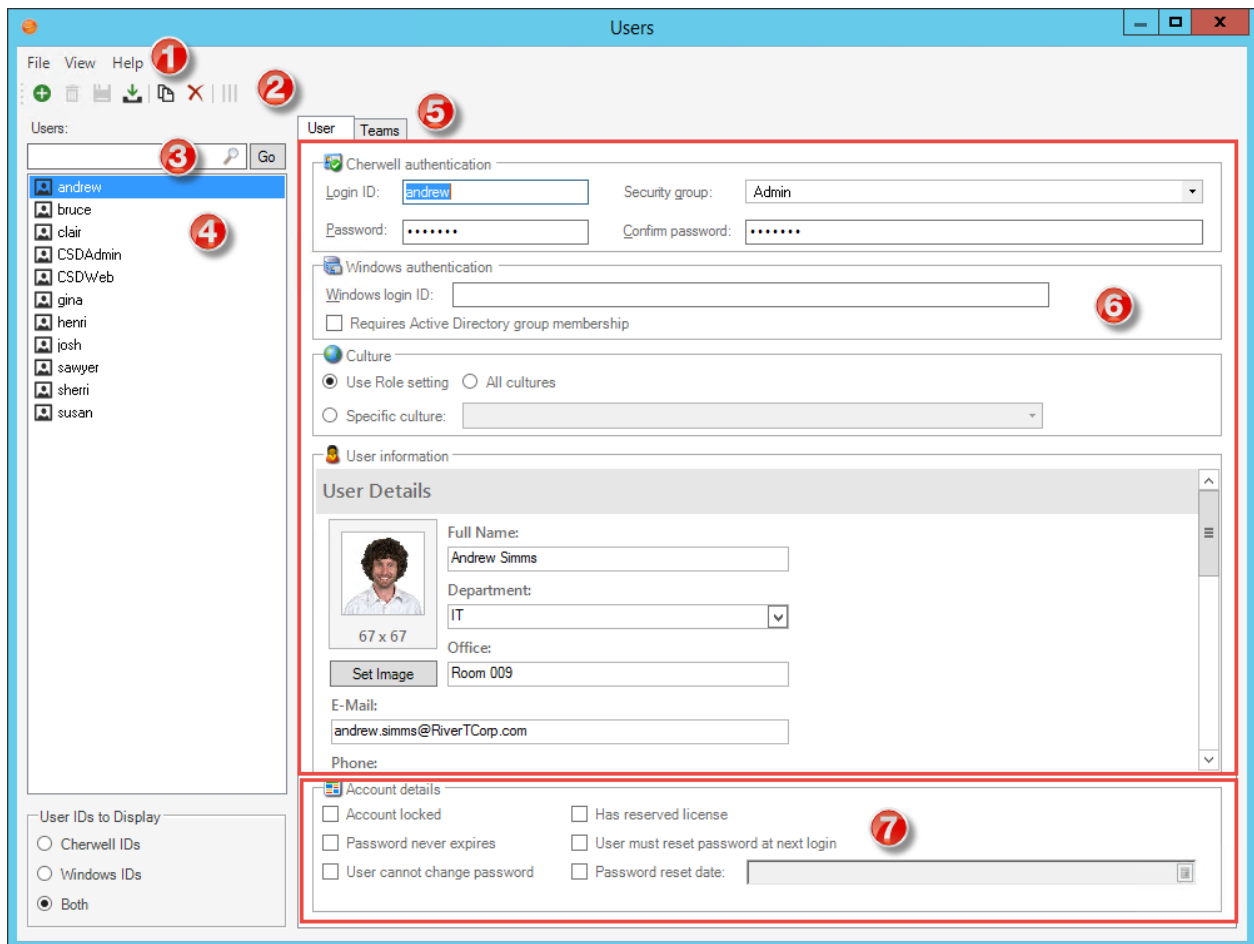
1. Menu bar:

   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, etc.
- Account details: Password resets, reserved licenses, etc.
- Assigned Security Group.
- Assigned Teams.

Good to know:

- To save time, import Users already stored in a Service Directory. Refer to Microsoft Active 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, E-mail, and Manager are highly recommended because some features (record ownership, One-Steps/Actions, Automation Processes, etc.), 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. Click the Create New button ⊕.
   A [New] User is added to the list.
3. Click 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** for the User.

Field	Description
Password	Provide a Cherwell password for the User. Provide the password again to confirm it.
(Optional) Windows authentication	Window login ID: Uses Windows credentials for login (instead of Cherwell credentials). Provide the User's Windows Login ID. See Use Windows Credentials. **Note:** To use this feature, Windows or LDAP must be a supported login mode (CSM Administrator > Security > Edit security settings > 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 > >select the LDAP check box.

Adding User Information

5. Provide personal User Information:

Field	Description
Full name	Provide the User's full name (example: Andrew Simms).

Field	Description
Set Image	Click 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. **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 e-mail address. If e-mail is configured, CSM can send e-mails to this address. Note that Automation Processes and Actions/One-Steps can also use an e-mail address. **Tip:** When testing a system, consider using a test e-mail account to avoid unnecessary e-mails.
Manager	Click the Selector button to open the User Selector window. Then, select another User to be the 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 e-mail address (if defined in the manager's User Profile). If e-mail is configured, CSM can send e-mail to this address. Note that Automation Processes and Actions/One-Steps can also use a User's e-mail address.
Other	Phone numbers, fax number, availability (example: Day shift), scheduled time-off, etc.

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 check box 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 check box to forgo 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 check box to restrict a User from changing his password. If a password reset is required by the system, the system administrator must reset the password.

Field	Description
Has reserved license	Select this check box 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 check box to prompt the Customer to change her password the next time she logs in. This check box will clear itself after the Customer changes her password. **Note:** This restarts any administrator-scheduled password reset. **Tip:** This is an immediate reset. Use this setting if the User forgot his password.
Password Reset Date	Select this check box to prompt a User to change his password on a specific date. Then, click the Date Selector button to select 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. Click the Teams tab.
   b. Click the Add button.
      The Add User to Team window opens.
   c. Select one or more **Teams**.
   d. Click OK.
      The User is added to the Team(s).
   e. To select a default Team, select the Team, and then click the Default Team button.

8. Click Save .

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 (ex: 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 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 Portal login must also have Portal credentials to store:

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

Contact Manager

The Contact Manager is an interface that 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 (ex: ABC, DEF, etc.).
- Find a specific Customer record using filtering and searching options.
- Create, edit, or delete a Customer Record.

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

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.
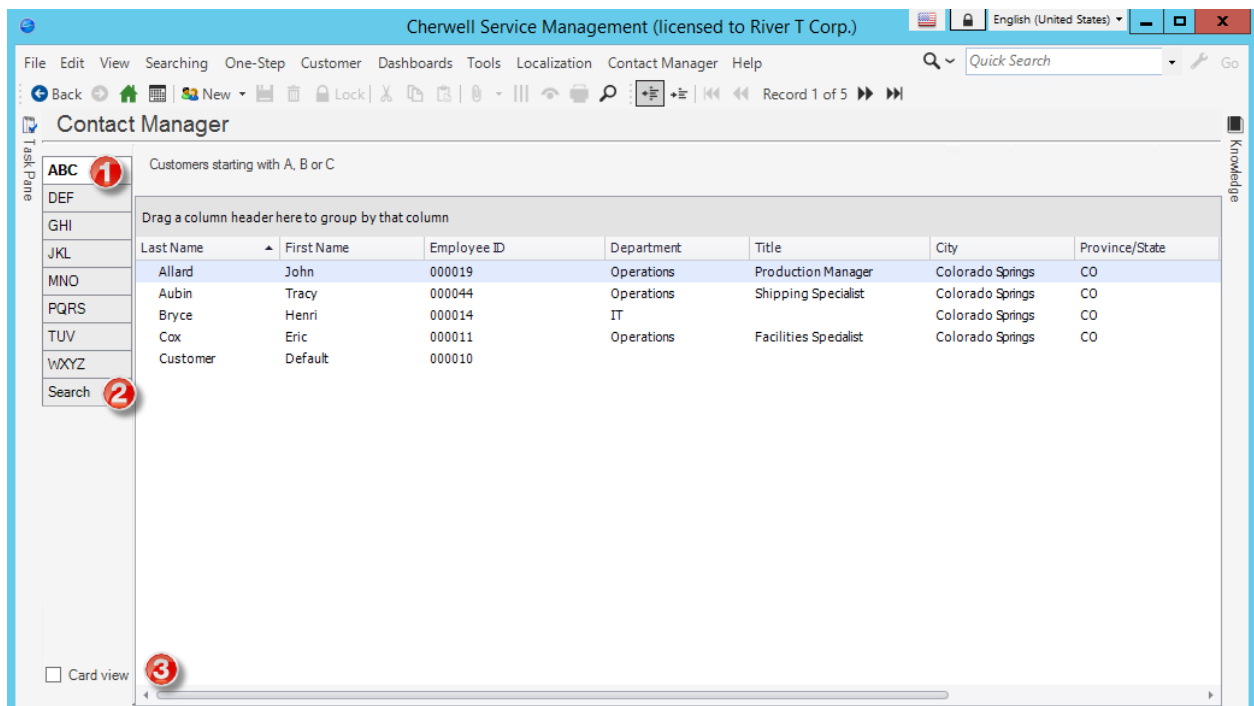
1. Tabs: View Customer records, organized alphabetically by last name on lettered tabs.

2. Search: Shows/hides search and filtering options:

    Search: Search for a specific Customer record (ex: Search any searchable field, such as First Name, Last Name, etc.).

    Changed: Displays a time frame filter to refine your search (ex: 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 by creating and completing a new Employee record in the CSM Desktop Client. The Customer record 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.

Good to know:

- To save time, import Customers already stored in a Service Directory.
- Full Name is the only required Field on a Customer record. Department, Manager, Phone, E-mail, SLA Subscription Level, and Last Survey Date are highly recommended because some features (record ownership, One-Steps/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®.
- The Customer record fields are configurable and are stored in the Customer Record Business Object (called *Customer-Internal* in the default system).
- 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 record:

1. From the CSM Desktop Client toolbar, click the New button and select Customer-Internal.

   A new (empty) Customer record opens.

2. Provide identification information (Personnel Identification section):
   a. Full name: Provide the Customer's **full name** (CSM logically parses the information into the following):

     Pre (ex: Ms.)

     First

     Middle

     Last

     Suffix (ex: Jr.)

   b. Set Image:

      Click 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.

      Tip: A person's image is often called an avatar because it can be a photo or a character representation.

   c. Employee ID: Provide the Customer's **employee identification number**.

     d. Employee Status: Select the Customer's **employment status**.

     e. Network ID: Provide the Customer's **network identification number**.

     f. Department: Select the Customer'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.

     g. Title: Provide the Customer's **job title**.

3. Provide detailed contact information (Personnel Information section):
   a. SAM Account Name: Provide the Customer's **SAM Account Name** (used in conjunction with Active Directory®).

   b. Manager: Select the Customer's **manager** by clicking the **Selector** button to open the User Selector window. Then, select a person to be the manager. Browse, search, or create a new Customer, 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.

   c. Phone: Provide the Customer's **primary phone number**. Note that some CSM Actions/One-Steps can automatically dial this number.

   d. E-mail: Provide the Customer's **e-mail address**. If e-mail is configured, CSM can send e-mails to this address. Note that Automation Processes and Actions/One-Steps can also use an e-mail address.

        Tip: When testing a system, consider using a test e-mail account to avoid unnecessary e-mails.

   e. SLA Subscription Level (Bronze, Gold, Platinum, or Silver). SLA target times use this to determine deadlines.

   f. Last Survey Date: Click the Date Selector button 🗓 to select the date of the Customer's last survey. To avoid too many e-mails being sent, CSM sends only one survey to each Customer every 90 days, and does not send surveys for Password Requests.

   g. Other: Location information, phone numbers, mobile carriers, Network ID, etc.

4. Provide social media information (Social Media Accounts section):
   a. Twitter Handle: Provide the Customer's **Twitter user name**.

   b. Facebook URL: Provide the Customer's **Facebook web address**.

   c. LinkedIn URL: Provide the Customer's **LinkedIn web address**.

   d. Personal E-mail: Provide the Customer's **personal e-mail address**.

5. 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 Portal login credentials (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.

Create Portal Login Credentials (for a Customer)

Before a Customer can access the Portal, you must create Portal login credentials for them. This is necessary for CSM to appropriately identify the Customer, and to make sure that a particular person using the Portal is who they say they are. Customer credentials are configured within the Customer record 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 by making use of the Cherwell Scheduler.

Note: If configured, a Customer can log into the Portal anonymously using CSM's Anonymous Security Group. Anonymous Customers do not require credentials, but they also have very limited rights.

Create Customer credentials:

- On an individual basis (particular Customer).
- For a group of Customers (batch credentials). For a group of Customers, passwords can be generated randomly and e-mailed to each Customer, or can be assigned in other manners, including the use of Active Directory credentials.

Create Portal Login Credentials for an Individual Customer

CSM allows a Customer to log in using assigned Cherwell credentials or using Windows/LDAP credentials.

To create Portal login credentials for an individual Customer:

1. Open the Contact Manager (Customer>Contact Manager).

2. Double-click a **Customer record**.

3. On the menu bar, click Customer>Portal Settings>Current Customer Credentials.

    Tip: You can also press **CTRL+F5** while on a Customer record.

    The Portal Credentials window opens.

4. Define the login credentials for the Customer (either Cherwell Authentication or Windows/LDAP Authentication):
    a. Customer configured to use Cherwell Portal: Select this check box to enable the Customer to log in to the Portal.

    b. Customer group: Select a Customer **Security Group** for the Customer.

    Note: The Security Group controls access to CSM functionality and data. Customers have their own Security Groups in CSM.

    c. Provide Cherwell Credentials:

    Note: If you provide a Windows/LDAP ID, you can omit the Cherwell Login ID and Password.

        i. Login ID: Specify a **Cherwell Login ID** for the Customer (ex: First initial + last name). The value must be unique.

        ii. Password: Provide a **Cherwell password** for the Customer.
            Password: Specify a password.

            Auto-generate a new password for this Customer: Select this check box to have the system randomly generate a password.

    d. (Optional) Windows Login ID: To have CSM attempt to log in the Customer using Windows credentials or LDAP credentials instead of Cherwell credentials, provide the **Customer's Windows Login ID**. For more information, refer to Use Windows credentials in the online help.

    Notes: To use this feature, either Windows or LDAP must be a supported login mode (CSM Administrator>Security>Edit security settings>select the Windows check box). This is intended for situations when you know the Customer (that is, they are employees). If you provide a Windows/LDAP ID, you can omit the Cherwell Login ID and Password.

e. E-mail customer new credential information: Select this check box to e-mail the Customer her credentials. If selected, you can click the **Edit e-mail** button to customize the text that will be sent.

> **Note:** If you randomly generate a password, you should select to e-mail the Customer her credentials; otherwise, there is no way for the Customer to retrieve the password. If selected, you can click the Edit e-mail button to customize the text that will be sent.

5. Define account locking and password reset options (Account details section):
   a. Account locked: Select this check box to lock the Customer's account (preventing them from logging in to the Portal).

   > **Note:** A Customer can be automatically locked out of the system, too, if there are too many failed login attempts (depending on system settings).

   b. Password never expires: Select this check box to forgo 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.

   c. User cannot change password: Select this check box to restrict a Customer from changing their 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 this check box to restrict a Customer 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.

   This is an immediate reset. Use this setting if the Customers forget their passwords.

   e. Password reset date: Select this check box to prompt a Customer to change their password on a specific date. Then, click the Date Selector button to select a reset date.

6. Click OK.

Create Portal Login Credentials for a Batch of Customers

CSM allows a Customer to log in using assigned Cherwell credentials or using Windows/LDAP credentials.

Note: To batch-assign both Cherwell and Windows credentials, you must run the batch process twice, once for standard, and once for Windows credentials.

Tip: Use the CSM Scheduler to assign batch Customer credentials on a scheduled basis. This is commonly used by those who import Customers from LDAP.

To create Portal login credentials for a batch of Customers:

1. Open the Contact Manager (Customer>Contact Manager)

2. Select a group of Customers either by running a Search Group or by using the Search tab in the Contact Manager.

    Tip: The easiest way to assign credentials to all Customers (or all Customers that do not yet have credentials assigned) is to bring up the Contact Manager and switch to the Search tab. Select the Customer type for your Customers (or just select All Customers), leave the Search text blank, and click the Go button (make sure that Changed is set to Any time).

3. Click Customer>\Portal Settings>Batch Customer Credentials.

    The Batch Portal Credentials window opens.

4. Define the login credentials for the Customers (either Cherwell Authentication or Windows/LDAP Authentication):
    a. Field with Login ID: Select the Field to provide the value to use for each Customer's login ID. The value must be unique.

        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 (ex: First letter of First name + Last name).

        Note: For Cherwell 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 will usually be *SAMAccountName*. The value will be combined with a domain to create the full Windows/LDAP User ID.

    b. Customer group: Select a **Security Group** for the Customers.

        Note: The Security Group controls access to CSM functionality and data. Customers have their own Security Group, called *Portal End User* in the Starter Database.

5. Set passwords for Customers. You have several options:

   Randomly generate a password for each Customer: Click this button to have the system randomly generates the password.

   Note: The randomly generated passwords will adhere to the password setting specified in the Cherwell Settings applied in Admin Portal.

   Note: If you select this option, you MUST select to e-mail each Customers their credentials; otherwise there is no way for the Customer to retrieve the password.

   Set password the same for all: Click this button to provide an identical password for everyone in the group.

   Note: Not recommended for secure systems.

   Password is value from Field: Click this button to pull the value from a Field in the Customer Record. This could be something like phone number or office number, or it could be a more complex calculated Field.

   Set login ID Field as Windows/LDAP Login: Click this option to have CSM attempt to log in the Customer using her Windows credentials instead of Cherwell credentials. Then, select options for determining the domain:

   Note: If the Field being used to provide the credentials is fully qualified (in the form of domain \user-id), that identifier will be assumed to be the full Windows ID, and will be used as-is. However, if the Field just contains the User ID, there are several options for how the system should try to determine the domain to use. Note that the first two options are only available if User/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 will try them each in turn until a domain can be determined.

   - 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 to provide a domain name. Then, provide the **domain name**.

     Note: For more information, refer to Use Windows Credentials in the online help.

6. Define account locking and password reset options (Account details section):
   a. Account locked: Select this check box 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 if there have been too many failed login attempts (depending on system settings).

b. Password never expires: Select this check box to forgo 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.

c. User cannot change password: Select this check box to restrict a Customer from changing their 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 this check box to restrict a Customer from changing their password. If a password reset is required by the system, the system administrator must reset the password.

Note: This restarts any system administrator-scheduled password reset.

Tip: This is an immediate reset. Use this setting if the Customer forgot their password.

e. Password reset date: Select this check box to prompt a Customer to change their password on a specific date. Then, click the Date Selector button to select a reset date.

7. Select options for e-mailing Customers their new credentials:
   E-mail customer new credential information: Select this check box to e-mail each Customer their credentials. If selected, you can click the Edit e-mail button to customize the text that will be sent.

   Note: If a password is being auto-generated, you should select to e-mail the Customer their credentials; otherwise, there is no way for the Customer to retrieve the password.

   Skip customers with no e-mail addresses: Select this option to skip assigning credentials to Customers whom do not have known e-mail addresses. E-mail is the only way to retrieve the password.

8. Skip customers who already have login IDs assigned: Select this check box to assign credentials only to new Customers (that is, skip assigning credentials to Customers who already have them).

   Example: To change everyone's credentials at once, clear this check box. If you add new Customers or import new records (Active Directory) in bulk and want to assign credentials to the newly added Customers, select this check box.

9. Click OK.

Use Windows Credentials

If enabled, CSM can use Windows/LDAP Credentials to log in a User/Customer rather than Cherwell credentials.

In order to use Windows credentials, Windows or Active Directory must be enabled for the Client. That is, Windows and/or LDAP must be supported login modes (CSM Administrator>Security>Edit Security Settings>select Windows or LDAP).

Note: In the Desktop Client, Windows credentials are automatically used (if enabled). In Internet Explorer, the Browser Client can automatically retrieve the User's/Customer's Credentials from the system and pass them to the server. In other browsers, Users/Customers might be prompted to provide Windows credentials. The browser validates the credentials before passing them to the server. If a User/Customer has previously provided credentials to the browser, they might not be prompted to provide their credentials.

If a User/Customer is 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.

The User/Customer can provide their Windows (or LDAP) Credentials into the User Name field and their Windows (or LDAP) Credentials into the Password field. When the Login button is selected, CSM confirms that the specified credentials are legal, and then (assuming they are) logs the User/Customer in.

Note: In order for this to work, the User/Customer must specify a fully qualified ID in the format of: **domain\user-id**

CAUTION: Unless the Portal has been configured to use SSL security (HTTPS), the credentials will be passed in clear text from the Browser to the server, and it would be possible for someone monitoring communication to capture credentials going over the wire. For that reason, we strongly suggest users edit web.config files to enforce redirecting HTTP requests to HTTPS for a better, more secure logon experience.

Use the Windows Login for the Portal

Normally, when a Customer wants to access the Portal, they use a URL like this:

http://MyServer/CherwellPortal

Which redirects automatically to the default Portal Site, such as:

http://MyServer/CherwellPortal/IT

The Customer can also go directly to a particular Portal Site:

http://MyServer/CherwellPortal/SomeSite

Depending on the configuration of the Site, the Customer might then be prompted to log in, or might have to click the Login link to be prompted for credentials. However, if the Customer adds a WinLogin clause to the URL:

http://MyServer/CherwellPortal/WinLogin/IT

The system will attempt to automatically log the Customer in using her Windows credentials, and then take the Customer to the Startup page. Note that, if the credentials are not legal, an error message will be displayed.

Note: This is equivalent to going to the Portal, clicking Login, and then clicking Use Windows Login.

Directly Provide Windows/LDAP Credentials

If a User/Customer is not currently logged into their standard Windows system (ex: They are logging in from a mobile device or from 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, but with a little more work.

The User/Customer can provide their Windows (or LDAP) credentials into the User Name field and Windows (or LDAP) credentials into the Password field. When the Login button is clicked, CSM confirms that the specified credentials are legal, and then (assuming they are) logs the User/Customer in.

Note that, in order for this to work, the User/Customer must specify a fully qualified ID in the format of:

domain\user-id

CAUTION: Unless the Portal has been configured to use SSL security (https), the credentials will be passed in clear text from the Browser to the server, and it would be possible for someone monitoring communication to capture credentials going over the wire.

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. Click 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 following information:

Directory Services Information

Account Information: Search and read capability for the Directory Service account is needed.
User Name:
Password:
Domain Name:

Server Information:
Server OS *(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 *(See 1 in the figure)*
Schema Path *(See 2 in the figure)*
Search Start *(See 3 in the figure)*
Custom Filters *(optional; contact the Active Directory/LDAP administrator - see the following Active Directory Users figure)*

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. Click OK.

> **Note:** To unlock the system, repeat the above steps, but select the **Unlock System** check box.

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, click the Security category, and then click the Audit Log task.

   The Audit Log window opens.

2. Users can then:

   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.

   - 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: Click this button to refresh the data in the list.

   Configure: Click 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.

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

To view/manage logged-in Users/Customers:

1. In the CSM Administrator main window, click the Security category, and then click the View Currently Logged-In Users task.

   The Logged-In Users Log window opens. All currently logged-in Users are listed alphabetically by login ID. Customers logged into the Portal will also be listed if they are using licenses. Regular Customers using the Portal (those not logged in) are not shown.

2. Click one or more Users.

3. Click an Action for the User:

   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 product he is currently logged into.

   Lock user out: Logs the User(s) out of the selected module, and then locks him out (i.e., prevents him from logging in again).

   Note: Typically, Users are not immediately logged out; rather, the system waits for a trigger, such as a Create Ne Action or a Search. In any case, Users are permitted to save whatever records they are currently working on. To allow Users back into CSM, you must unlock their accounts on their User Profile (User Info tab).

CSM Administration

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 category>Edit System Settings task) to configure the following system security settings:

- General: Configure the default domain and anonymous login 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. In the CSM Administrator main window, click the Security category, and then click the Edit Security Settings task.

2. Click the General page.

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: Click the Arrow button to have CSM auto-populate the name.

4. Define anonymous login options (required if you want to allow use of the Browser/Portal Clients):
    a. Allow Anonymous Login: Select this check box to allow Browser applications to operate.

    b. Anonymous Security Group: Select the Security Group that should be used by Cherwell web applications before any User/Customer has logged in. Cherwell web applications need to be able to read basic setup from the system before logging in, and this is the Security Group that will be used for such access. Also, for any Portal Sites that do not require login, this is the Security Group that will specify what Customers will be allowed to access before they log in.

    Note: CSM provides an Anonymous Security Group named *Anonymous Browser*.

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. Click OK.

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 radio button 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 (ex: pdf), separated by a comma, either by typing directly in the Extensions box, or by clicking the **Choose File Types** button 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 clicking the **Choose File Types** button to open the Select File Types window.

    Tip: To restore the OOTB default file types, click the Restore to Cherwell defaults button .

5. Click OK.

Configure Login, Authentication, and Inactivity Settings for Each Client

By default, the Browser and Portal Clients use the same settings as the Desktop Client. To specify unique settings for Browser/Portal, clear the *User Same Settings as Desktop Client* check box on their respective pages, and then define the unique settings.

To configure login, authentication, and inactivity settings for the Desktop Client, Browser Client, and Customer Portal:

1. In the CSM Administrator main window, click the Security category, and then click the Edit Security Settings task.

   The Security Settings window opens.

2. Click the Desktop Client page. (To specify unique settings for Browser/Portal, click the respective pages, clear the Use Same Settings as Desktop Client check box on their respective tabs, and then define the unique settings.)

3. Select the login modes you want to allow (Supported Login Modes area):

   Note: 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 (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:
   (Desktop Client only) Display last logged-in User on Login page. If enabled, the User ID will be stored in the registry on the User's computer, which might be considered a security risk.

   (Desktop Client only) Allow Users to have system remember last password (auto-login). If enabled, the password will be 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).

5. Default Domain for Login: Provide a default domain to use when Users log in.

6. Select the Validate credentials via external authentication server check box.

7. Select the Require user to enter credentials: Select this check box to require Users/Customers to provide their credentials each time they log in.

   Note: If this is not selected, and Users/Customers are on the same domain as the Cherwell Authentication Server, then the User's/Customer's current Windows Credentials are used to

determine the person's identity. Otherwise, the User/Customer needs to provide their Windows domain/user ID and password to the login dialog.

8. Authentication server URI: 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. (Desktop Clients only) Select Logout Inactive Users from Cherwell Client.
Specify the Minutes to Wait before logging out an inactive User.

Select the Warning Period check box to warn Users before they are automatically logged out and specify the minutes before the logout to send a warning where Users can select to Stay Logged In or Log out now.

10. Click OK.

Configure Cherwell Mobile Login Settings

Use the Mobile Apps page in the Security Settings window (in CSM Administrator) to configure the following login settings for Cherwell Mobile applications (Cherwell Mobile for iOS, Cherwell Mobile for Android, and Cherwell Mobile for Browser):

- 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. Click 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.
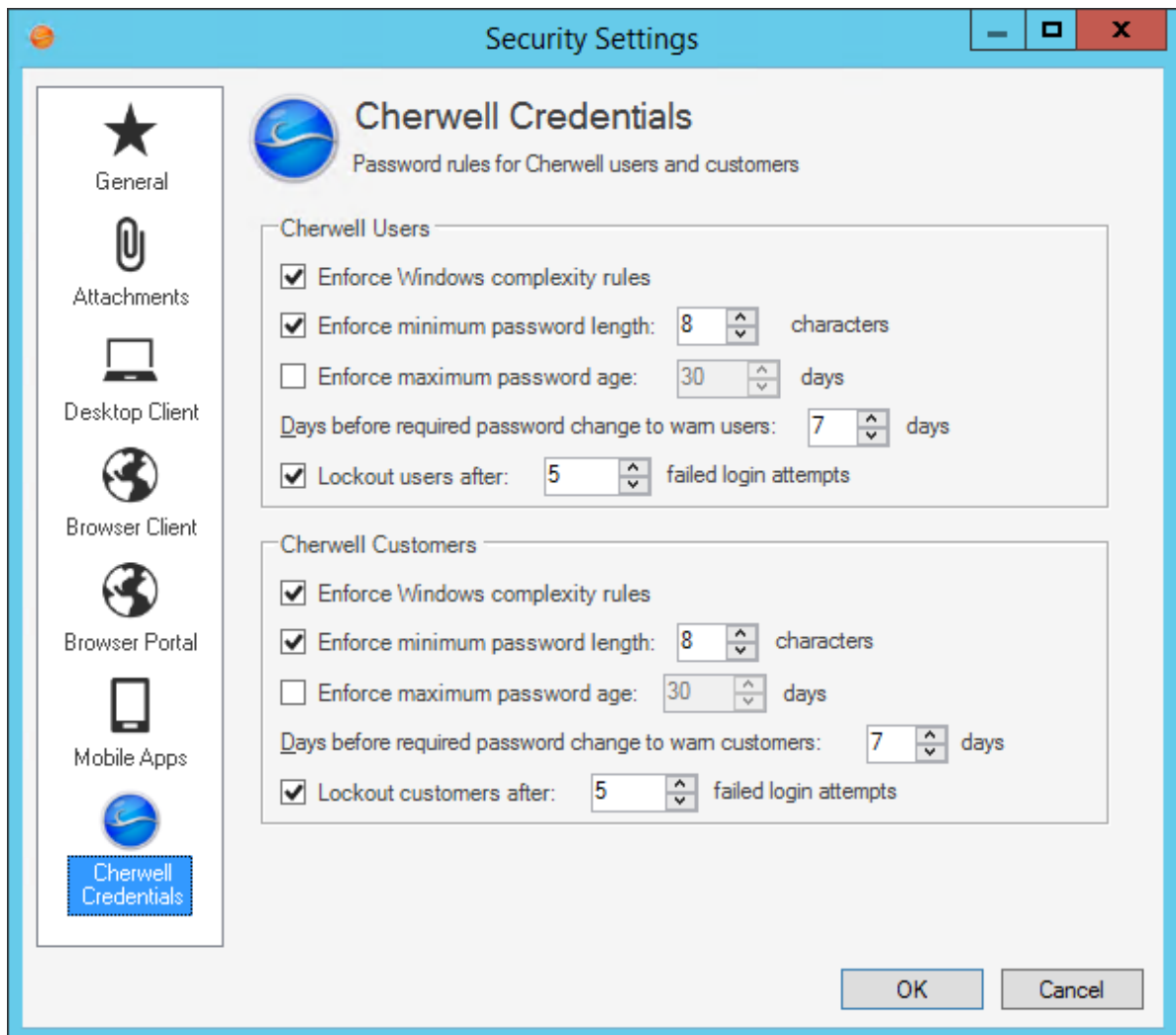
3. Configure enforcement rules for User and Customer credentials:

   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. Click OK.

Security Rights Reference

View detailed information for security rights in each category.

Security rights control access to CSM functionality and are configured in the Security Group Manager in CSM Administrator (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 (CSM Administrator>Security>Edit security groups) 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.

Application Security Rights

Application rights are selected from the Category drop-down on the Rights tab (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

Right	Description (when selected ✔)	Grant To:
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)
Can delete all records in a group?	Allow: Allows selected Users to delete all records in the current Search results group (ex: 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 CSM.	• 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 CSM 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

Automation Process Blueprints Security Rights

Automation Process Blueprints rights are selected from the Category drop-down on the Rights tab (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 (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. **Note:** 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 Business Automation Process Sever (service) using the Pause/Resume Automation Process Server window from within either CSM Administrator or the Server Manager.	• System administrators

Browser and Mobile Device Security Rights

browser and Mobile Device rights are selected from the Category drop-down on the Rights tab (CSM Administrator>Security>Edit Security Groups).

Right	Description (when checked ✔)	Grant To:
Assign login information to groups of Customers (batch)?	Allow: Allows selected Users to create Portal login credentials for a batch of Customers (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-Steps). The default Cherwell Mobile settings (either Global or Role) are initially configured in CSM Administrator. If Users have security rights, they can override her 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 (CSM Desktop Client>Customer>Portal Credentials). • Edit: Create/edit Portal login credentials for Customers (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 (CSM Administrator>Security>Edit Security Groups).

Right	Description (when checked ☑)	Grant To:
Business Hours? Rights are organized by scope: Blueprint, Business Intelligence, Global, Role, Team, and User.	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 (CSM Administrator>Security>Edit Security Groups).

Right	Description (when checked ✅)	Grant To:
Calendars? Rights are organized by scope: Blueprint, Global, Role, Team, and User.	Allows people working with Calendars to: • View: View Calendars. • Add: Create Calendars. • Edit: Edit Calendars. • Delete: Delete Counters.	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 on the Rights tab (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 the Cherwell Web Service (CWS) 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 be logged in by the CWS that processes Bomgar remote support session end notifications. If this privilege is not allowed, the web service will ignore all Bomgar events.	• System administrators • Managers • Users
Chat settings?	Edit: Allows selected Users to edit remote support service settings (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

Right	Description (when checked ✔)	Grant To:
Request chat service information?	Allow: Allows selected Users to access information about the Bomgar 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 (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 (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 (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 (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: Global, Role, Team, and User.	Allows people working with Dashboard Slideshows to: • View: Access Dashboard Slideshows. • Add: Create Dashboard Slideshows. • Edit: Edit Dashboard Slideshows. • Delete: Delete Dashboard Slideshows.	View/Run Only: • Users All rights: • System administrators • Managers • Advanced Users (Level 2 and 3 technicians)

CSM Administration

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 Options rights are selected from the Category drop-down on the Rights tab (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 (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 (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 (CSM Administrator>Security>Edit Security Groups).

Right	Description (when checked ✔)	Grant To:
Default rights?	Allows people 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 looking at the Use default checkbox for each specific 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 (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 (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. **Note:** The emailmonitor.ini file was used prior to CSM version 3.2.	• 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 Server using the pause/resume task in CSM Administrator (E-mail and Event Monitoring>Pause/Resume Monitoring) or from the Server Manager.	• System administrators

E-mail Security Rights

Security rights control access to CSM 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.

Right	Description (when checked ✔)	Grant To:
Can override server and account settings on locked accounts?	Allow: Allows selected Users to override the e-mail account server settings and account information for a global account configured in CSM Administrator (ex: 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 e-mail from the system?	Allow: Allows selected Users to send e-mails from within the system.	• System administrators • Managers • Users
Can add User e-mail accounts?	Allow: Allows selected Users to add and personalize your own e-mail account and settings.	• System administrators • Managers • Advanced Users (Level 2 and 3 technicians)
Can e-mail Teams?	Allow: Allows selected Users to e-mail Teams (ex: IT Service Desk Level 1).	• System administrators • Managers • Users
Can administrate global e-mail settings?	Allow: Allows selected Users to configure global e-mail accounts in CSM Administrator.	• System administrators
Can e-mail Workgroups?	Allow: Allows selected Users to e-mail 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 (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 (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 people 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

Knowledge rights are selected from the Category drop-down on the Rights tab (CSM Administrator>Security>Edit Security Groups).

Right	Description (when selected ☑)	Grant To:
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.	• System administrators • Managers • Advanced Users (Level 2 and 3 technicians) • Users
Import Knowledge?	Allow: Allows selected to import Knowledge using third-party Knowledge bases through the Knowledge Import Wizard.	• System administrators
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: • Users All rights: • System administrators
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: • Users All rights: • System administrators

Manager Security Rights

Manager 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 pin/unpin items from all Users' pinboards?	Allow: Allows you to pin or unpin an item to/from all Users' Pinboards (ex: 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 (ex: 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 (ex: Pinning a One-Step to all Users' Pinboards within the currently logged-in Technician Role so that they can run the same One-Step).	• 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 mApps?	Allow: Allows selected Users to create mApps.	• System administrators
Apply mApps?	Allow: Allows selected Users to apply mApps.	• System administrators
View installed mApps?	Allow: Allows selected Users to view a list of mApps that have already been installed on a CSM system.	• System administrators
View mApps development history?	Allow: Allows selected Users to view available history records for all definitions within a CSM system that were modified by a mApp.	• 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

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 checked ✅)	Grant To:
One-Steps? Rights are organized by scope: Blueprint, Business Intelligence, Global, Role, Site, Team, and User.	Allows people working with One-Steps to: • Run: Run One-Steps. • Add: Create One-Steps. • Edit: Edit One-Steps. • Delete: Delete One-Steps. For the Site scope, the following additional options are available: • Run other Users: Run Site One-Steps (from the One-Step Manager) that were created by other Users. • Add other Sites: Create One-Steps for Sites that belong to other Security Groups. • Edit other Sites: Edit One-Steps for Sites that belong to other Security Groups. • Delete other Sites: Delete One-Steps for Sites that belong to other Security Groups.	View/Run Only: • Users/Customers • Managers All rights: • System administrators
Can edit One-Steps set to explicitly run under any Security Group?	Allow: Allows Users to edit One-Steps, regardless of the Security Group they are configured to run under.	• System administrators
Can edit One-Steps set to explicitly run under this Security Group?	Allow: Allows Users to edit One-Steps if their Security Group is the same as the Security Group the One-Steps are configured to run under.	• System administrators • Managers • Users
Can set One-Steps to run under any Security Group?	Allow: Allows Users who create and edit One-Steps to select any Security Group for One-Steps to run under.	• System administrators

Right	Description (when checked ✓)	Grant To:
Can set One-Steps to run under this Security Group?	Allow: Allows Users who create and edit One-Steps to select only their current Security Group for One-Steps to run under.	• System administrators • Managers • Users
Can a User work with the Web Service One-Step Action?	Allows people working with Web Service One-Step Actions to: • View: Access Web Service One-Step Actions. • Add: Create Web Service One-Step Actions. • Edit: Edit Web Service One-Step Actions. • Delete: Delete Web Service One-Step 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-Steps can access values for fields for which the Security Group doesn't have rights?	Allow: Allows One-Steps to access values for Fields even if the Security Group the One-Step is configured to run under does not have rights to the Field values.	• System administrators
Run One-Steps for groups?	Allow: Allows you to run One-Steps 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 (CSM Administrator>Security>Edit Security Groups).

Right	Description (when checked ☑)	Grant To:
Can edit record locking settings?	Allow: Allows selected Uses 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 (ex: Scheduled imports or reports).	• System administrators
Pause/resume scheduling service?	Allow: Allows selected Users to pause and resume Scheduling Server processing from CSM Administrator, which does not require access to the machine running the service or from the Server Manager. **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.	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 (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

Right	Description (when selected ✔)	Grant To:
Publish log?	Allows people working with Blueprint publish logs to: • View: Access logs in order to publish. • Delete: Deletes previous publish logs.	• System administrators
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

Right	Description (when selected ✔)	Grant To:
Security settings?	Allows people working with Security settings in CSM Administrator to: • View: Access the Security settings. • Edit: Edit the Security settings.	• System administrators
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 (CSM Administrator>Security>Edit 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. ex: When creating Portal menus, Users can define a Create New command that runs a One-Step 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 (ex: 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 (ex: 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

Tools Security Rights

Tools rights are selected from the Category drop-down on the Rights tab (CSM Administrator>Security>Edit Security Groups).

Tools include:

- Definition Editor.
- 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
Run Definition Editor?	Allow: Allows selected Users to run the Definition Editor.	• System administrators

Users Security Rights

Users 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 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 set password reset options?	Allow: Allows selected Users to set password reset options in CSM Administrator.	• System administrators
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
Lock/unlock User Accounts?	Allow: Allows selected Users to lock or unlock User accounts.	• System administrators
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

Right	Description (when checked ☑)	Grant To:
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

Web Services Security Rights

Web Services rights are selected from the Category drop-down on the Rights tab (CSM Administrator>Security>Edit Security Groups).

Right	Description (when checked ✔)	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) from a client machine as opposed to having the server make the call. You can select to have all web service calls forced to the server (CSM Administrator>Edit System Settings>Advanced). **Note:** The global settings for web services must be set to allow calling from a client based on security.	• 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

Concurrent Development

Concurrent development allows multiple designers to 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 mApps.

CSM System Design Using Concurrent Development

Overview

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.

When you use mApps for concurrent development, you have two options:

- Use two or more Blueprints to develop the functionality and then create a mApp to apply the functionality into the production environment.
- Use two or more mApps to develop the functionality and then apply each mApp to the production environment.
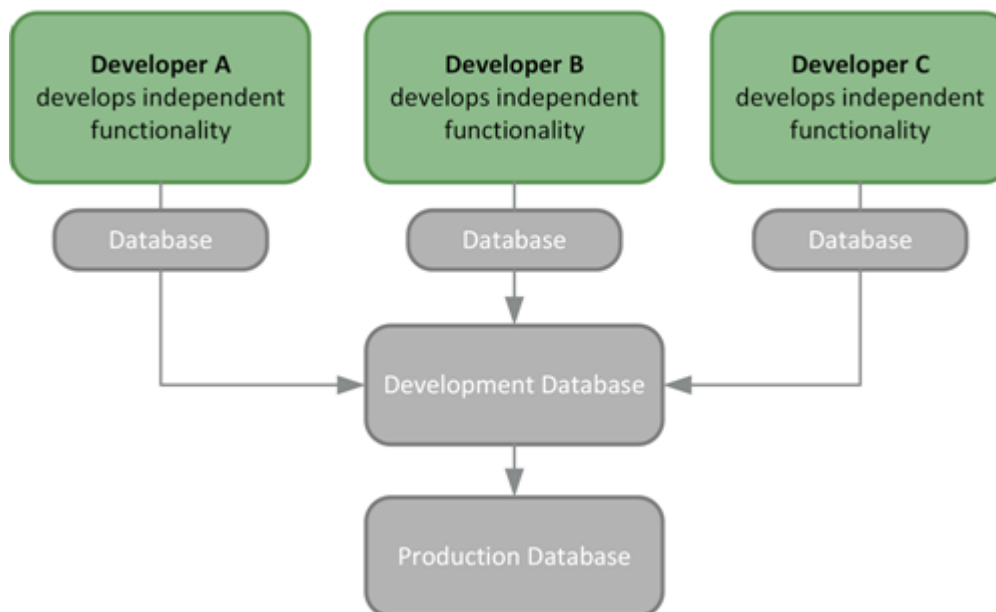
These approaches have several advantages:

- 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 works on Incident Forms, the work of the second designer could overwrite the work of the first designer.

Use the guidelines and best practices in this document enable multiple designers to work simultaneously on system changes.

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 will vary based on project, but ensure that the following information is shared at the very least:

- 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

Before beginning the project, decide whether to use a Blueprint or mApp for your system configuration by considering the characteristics and benefits of each.

Blueprints allow you to:

- Use two or more Blueprints to develop the functionality and then apply each Blueprint to the production environment.
- 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.

mApps allow you to:

- Use one of two options:
    - Use two or more Blueprints to develop the functionality and then create a mApp to apply the functionality to the production environment.
    - Use two or more mApps to develop the functionality and then apply each mApp to the production environment.
- 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.
- 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 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 Multiple Working Databases

Use multiple CSM databases when implementing concurrent development using Blueprints or mApps:

- 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).

Create Frequent Backups

Before publishing Blueprints or applying mApps to the master development database, create a backup .czar file of the system. If the Blueprint or mApp causes significant errors, the database can be restored using the backup file. Also, consider automating frequent backups using the Backup Database option of the Scheduler.

Use a Consistent Naming Convention

Ensure that all Blueprints and mApps follow a consistent naming convention that includes:

- When the Blueprint or mApp 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 files in a common location in a network share. Then, the Blueprints or mApps 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 Application Service, Automation Process Server, 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 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.

CSM Administration

Using Blueprints or mApps for Concurrent Development

Use the following workflows to accommodate multiple designers simultaneously working on system changes using Blueprints or mApps.

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. Project Manager creates a rollout document. The document should be detailed and include the following information at the very least:
   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-Steps, 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.).

   Impacted CSM Services (example: Application Server, Automation Process Server, etc.).

   System configurations that must be done outside the Blueprint. These might include changes to Security, the Scheduler, E-Mail Monitor, etc.

   Test plans, including any user acceptance test requirements.

   A backup and recovery plan.

2. Create a development environment for by restoring the master development server to 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: Application Service, Automation Process Server, etc.) are disabled. If you need to test E-mail Monitor functionality, make sure to configure the test e-mail account.

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.

CSM Administration   273

  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. 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 mApps 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 to apply the functionality into the production environment. (Process shown below.)

- Use two or more mApps to develop the functionality and then apply each mApp to the production environment.

To use mApps for concurrent development:

1. Project Manager creates a rollout document. The document should be detailed and include the following information at the very least:

    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-Steps, 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 mApp adheres to requirements and follows team standards (example: Naming conventions, design guidelines, etc.) before being applied.

    - A product manager who is responsible for the scope and outcome of the project.

    Required external connections (example: SCCM, Outlook, Active Directory, etc.).

    Impacted Services (example: Application Server, Automation Process Server, etc.).

    System configurations that must be done outside the Blueprint. These might include changes to Security, the Scheduler, E-Mail Monitor, etc.

    Test plans, including any user acceptance test requirements.

    A backup and recovery plan.

2. Create a development environment for by restoring the master development server to 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: Application Service, Automation Process Server, etc.) are disabled. If you need to test E-mail Monitor functionality, make sure to configure the test e-mail account.

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. Create a mApp 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 based on the approved system configurations included in the Blueprints.

8. Conduct testing on the mApp:

      a. Apply the mApp while referencing the rollout document.

      b. Test the mApp while referencing project requirements.

      c. Edit the mApp or create a new mApp based on test results.

      d. Repeat testing (steps *a* through *c*) until the gatekeeper approves the mApp.

      e. Update the rollout document.

9. Release the mApp into the production environment:

      a. Gatekeeper conducts a final review and applies the mApp to the master development database.

      b. Quality Assurance Engineers complete regression testing.

      c. Publish the mApp to the production environment.

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

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.

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.

The Blueprint Editor is the interface for Blueprints, which have their own workflow.

Because Blueprints affect system definitions, Blueprints are used and managed from within CSM Administrator. Access Blueprints and Blueprint functionality from the CSM Administrator Blueprint page.

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, Search Groups, 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.
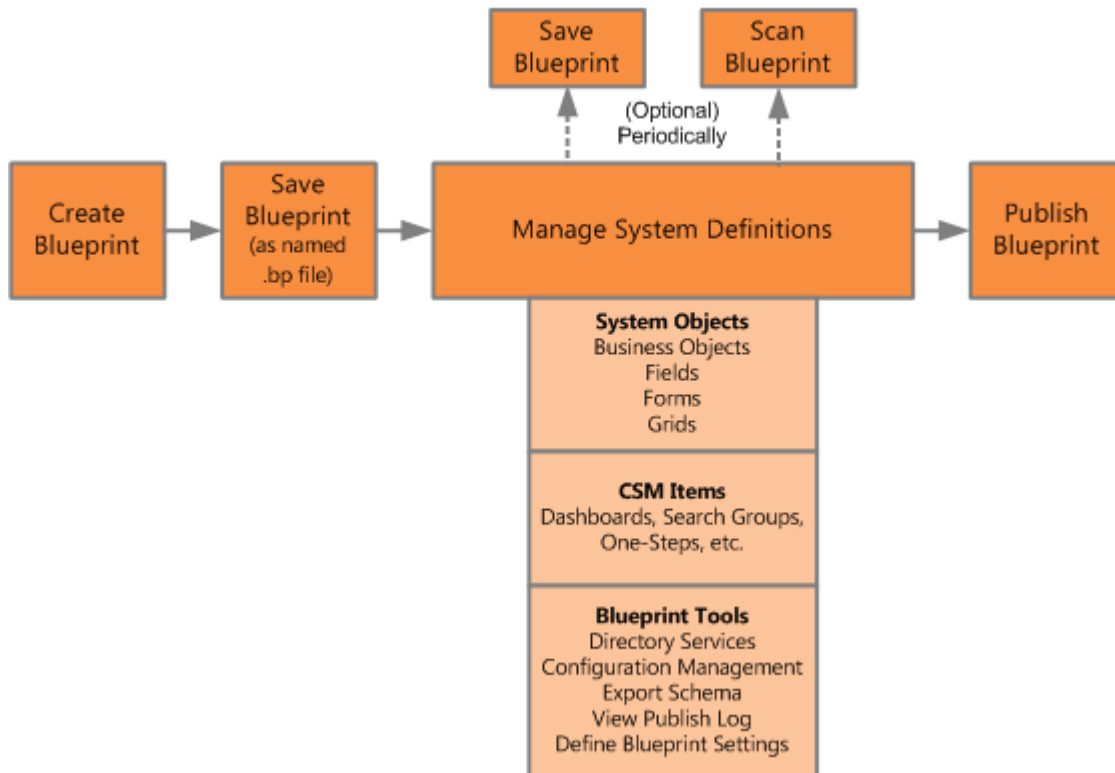
Managing Blueprints

Blueprints are managed in CSM Administrator using the Blueprint Editor. Use the Blueprint Editor to:

- Create a Blueprint.
- Open an existing Blueprint.
- Save a Blueprint.
- Scan a Blueprint (for potential errors).
- View Blueprint changes.
- Publish a Blueprint.
- Close a Blueprint.
- View details of the last published Blueprint.

Blueprint Editor

When creating and working with Blueprints, the CSM Administrator interface changes to the Blueprint Editor.

The Blueprint Editor is the built-in interface within CSM Administrator that allows you to manage System Objects, Business Object data, CSM Items, Blueprints, and Blueprint tools/functionality.
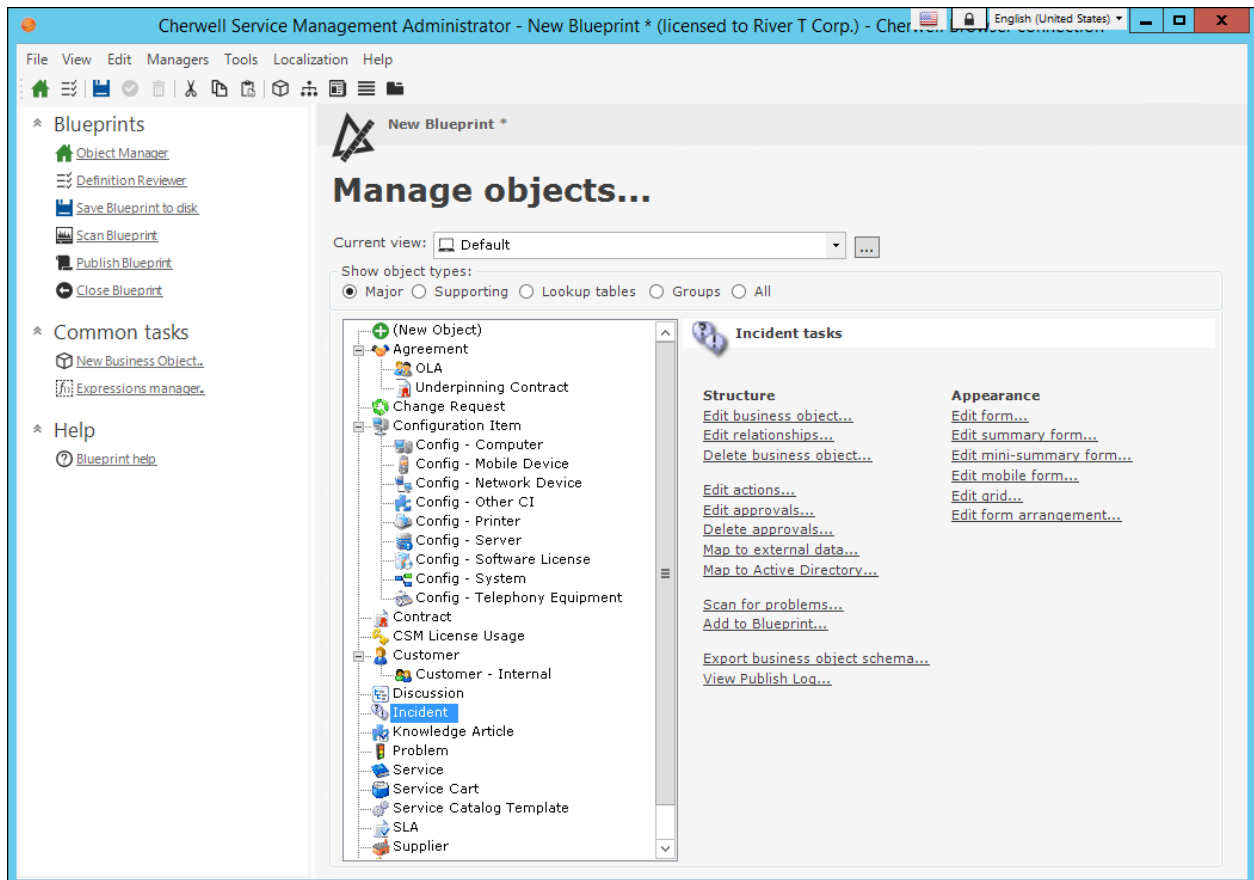
Use the Blueprint Editor to:

- **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.

- **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.

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 **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.
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.
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
Automation Processes	Opens the Automation Process 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.
Expressions	Opens the Expression Manager.
External Connections	Opens the External Connections Manager.
Formats	Opens the Stored Format Manager.

Action	Description
Group Maps	Opens the Group Map Manager.
Images	Opens the Image Manager.
Knowledge	Opens Knowledge Mapping Manager andKnowledge Source Manager.
One-Step	Opens the One-Step Manager.
Searches	Opens the Search Group Manager.
Site Manager	Opens the Portal Site Manager.
Stored Values	Opens the Stored Value Manager.
Teams	Opens the Team Manager.
Themes	Opens the Theme Manager.
Visualizations	Opens the Visualization 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.).
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

The Localization menu is only available if globalization is enabled for your system. For more information, see Enable Globalization.

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+P)	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 Software.
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, specifically:

- 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, click Create a New Blueprint.
- 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.

Create a Blueprint

Follow these steps to create a new Blueprint.

1. Open CSM Administrator.
2. Click Blueprints > Create a New Blueprint.
   The Blueprint Editor opens. By default, the Object Manager is displayed in the Blueprint Editor's Main Pane.
3. Click 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.

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, click the Blueprints category.

2. Click **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 click the Download button. The File Explorer opens.

4. Select a location on your local machine and click Save. A copy of the Blueprint is now saved on your local machine.

After downloading a Blueprint, you can open the Blueprint in order to edit it, or publish the Blueprint to revert your system or apply changes from another user.

Save a Blueprint

There are two save options for a Blueprint:

- Save As: Saves a Blueprint as a named .bp file.
- Save to disk: Saves 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.

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-Steps, 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).

   > 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.

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).
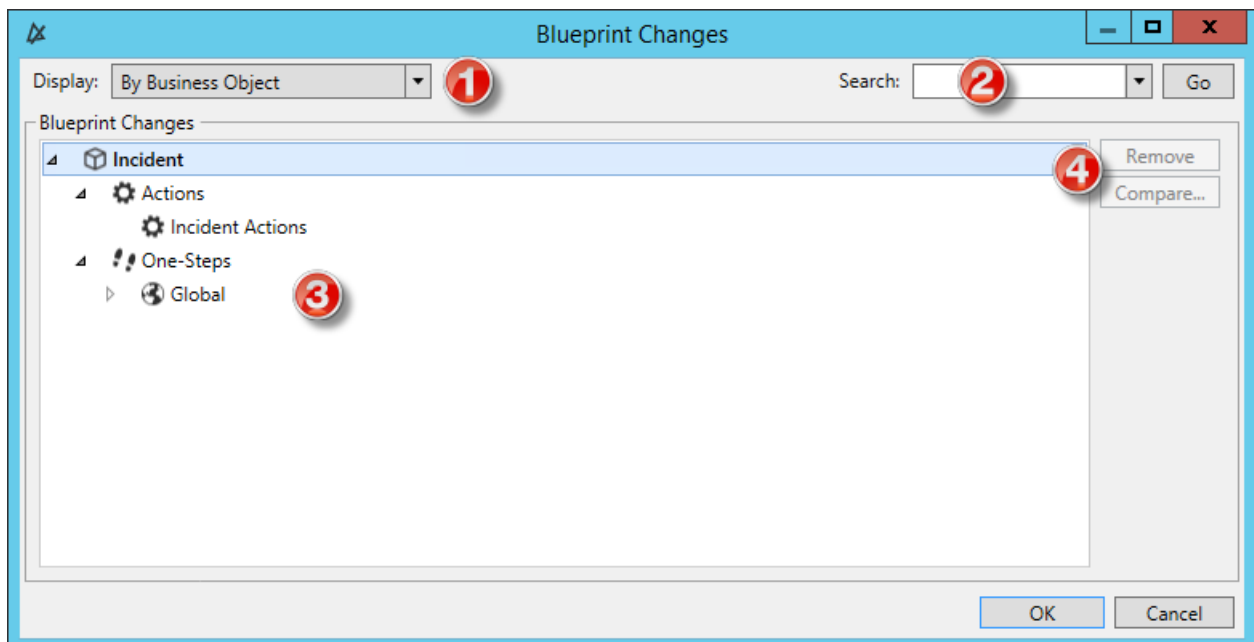
1. Display: Groups changes in the tree by Business Object, Definition, or View.
   By Business Object: Groups changes by Business Object (example: Incident).

   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
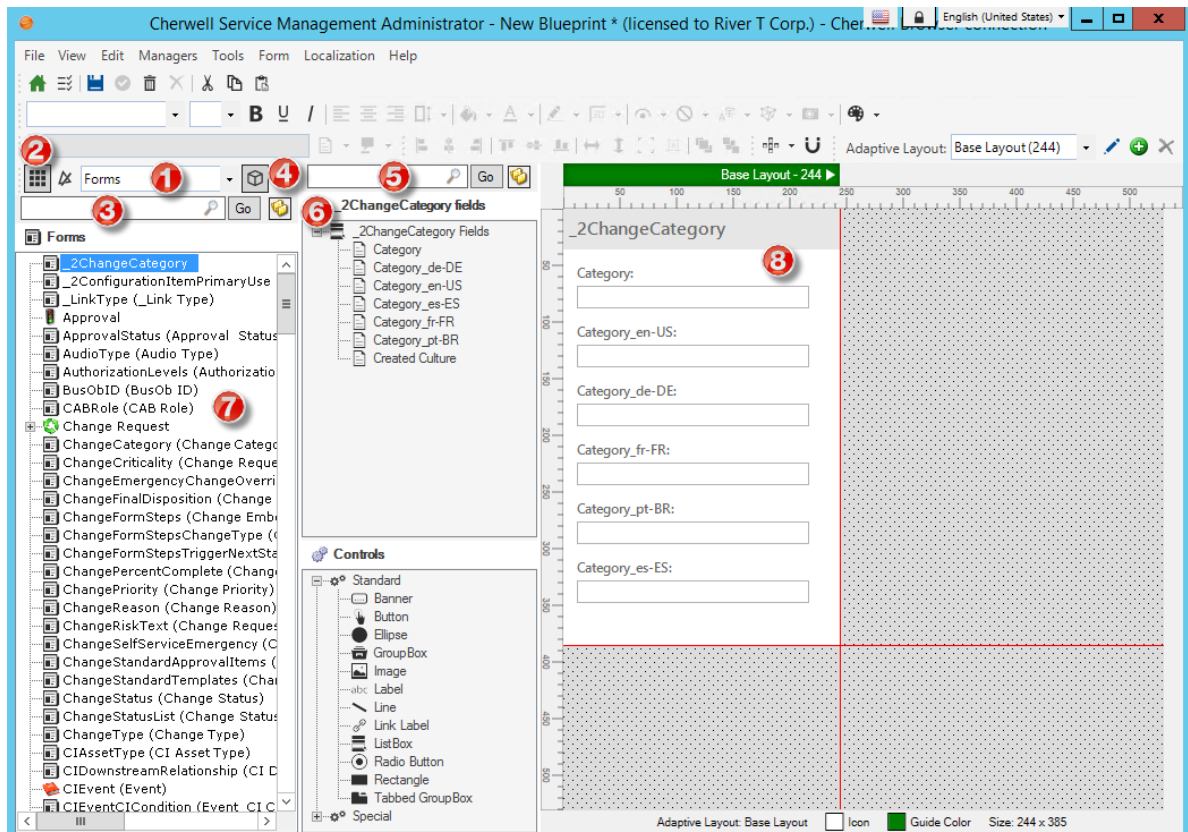
4. Optionally, right-click on a definition in the list to perform these localization tasks:

View Translations

See Viewing Translations for Definitions.

Apply Language Pack Bundles

See Applying Language Pack Bundles to Definitions.

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.
- 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. For more information, refer to the Cherwell Scheduler documentation.

To publish a Blueprint:

1. From the Blueprint Editor menu bar, click File>Publish Blueprint.

   Tip: You can also publish a Blueprint by clicking Publish Blueprint in the Blueprints section of the Blueprint Editor Task Pane.

2. Select before publishing operations:
   a. Save Blueprint: Select this check box 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.

      Create rollback Blueprint: Select this check box to create a Blueprint rollback file that, when published, backs out the changes made by the published Blueprint file.
   b. Scan for errors: Scans the Blueprint for potential errors. The scan will look for missing items and alert you to any changes you need to make.
      Stop on Warnings: Select this check box to stop the publishing process when an error is encountered.
   c. Force Out Users (selected by default): Logs all Users out of the CSM Clients.
   d. Lock System (selected by default): Select this check box to lock the system, preventing Users from logging in to CSM Clients while administrative work is being done.

> **Note:** 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.

    e. Pause All Services (selected by default): Select this check box to pause all CSM Server/Services (example: Application Server, Scheduler Server, etc.).

    f. Ignore Conflicts: Select this check box to bypass the Blueprint Conflict Resolution feature.

3. Select Publishing operations:
    a. Publish changes (selected by default): Publishes the Blueprint to your test or live system.

4. Select after publishing operations:
    a. Rebuild Full-Text Catalog: Select this check box to rebuild the Microsoft SQL Server Full-Text Catalog. If you change Business Objects and Fields to include or not include them in a Full-Text Search, the catalog must be rebuilt in order 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* box in the Business Object Properties window (Search Results page) and the Field Properties window (General page).

    b. Restart Services: Select this check box to restart the CSM Server/Services you paused before the publish. If you do not select this check box, you must manually restart the Services using the Server Manager.

    c. Unlock System: Select this check box to unlock the CSM system you locked before the publish. If you do not select this check box, you must manually unlock the CSM system in CSM Administrator (Security).

    d. Update Validation Foreign Keys: Select this check box to update the values for Fields that store foreign keys. This ensures that selected values are updated for existing records. See Storing Foreign Keys for Validated and Auto-populated Fields.

5. Click Publish.

Publish a Rollback Blueprint File to Undo Changes

Rollback Blueprint files are created before a Blueprint is published. Rollback Blueprint files serve as a snapshot of the CSM system prior to changes that may have been implemented in a newly published Blueprint. After changes have been published (example: changing the system's font style), it is possible to undo the changes and return the system to its previous state.

Rollback Blueprint files are only available once a Blueprint has been published. To remove changes prior to publishing the Blueprint, use theUndo Business Object Changes within a Blueprint feature.

To publish a Rollback Blueprint file and override changes made to your CSM system, follow these steps:

1. In the CSM Administrator Client, select the Blueprints category.
2. Select Open an existing Blueprint.
3. Navigate to the saved Rollback Blueprint file (example: Desktop/font_changes_rollback.bp).

   Note: Rollback Blueprint files are created when a Blueprint is published and saved. If a Blueprint is published and saved, a Rollback Blueprint file is also created.

4. Click Open. The Rollback Blueprint file opens in the CSM Administrator Object Manager.
5. Click Publish Blueprint. The Publish Options window opens.
6. Click Publish in the Publish Options window to publish the file to your live or test system.
   After the Rollback Blueprint file is published to a live or test system, the system returns to its state prior to any implemented changes. (example: the system will have the original font style rather than an updated font style).

   Note: 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 Cherwell Administrator.

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.
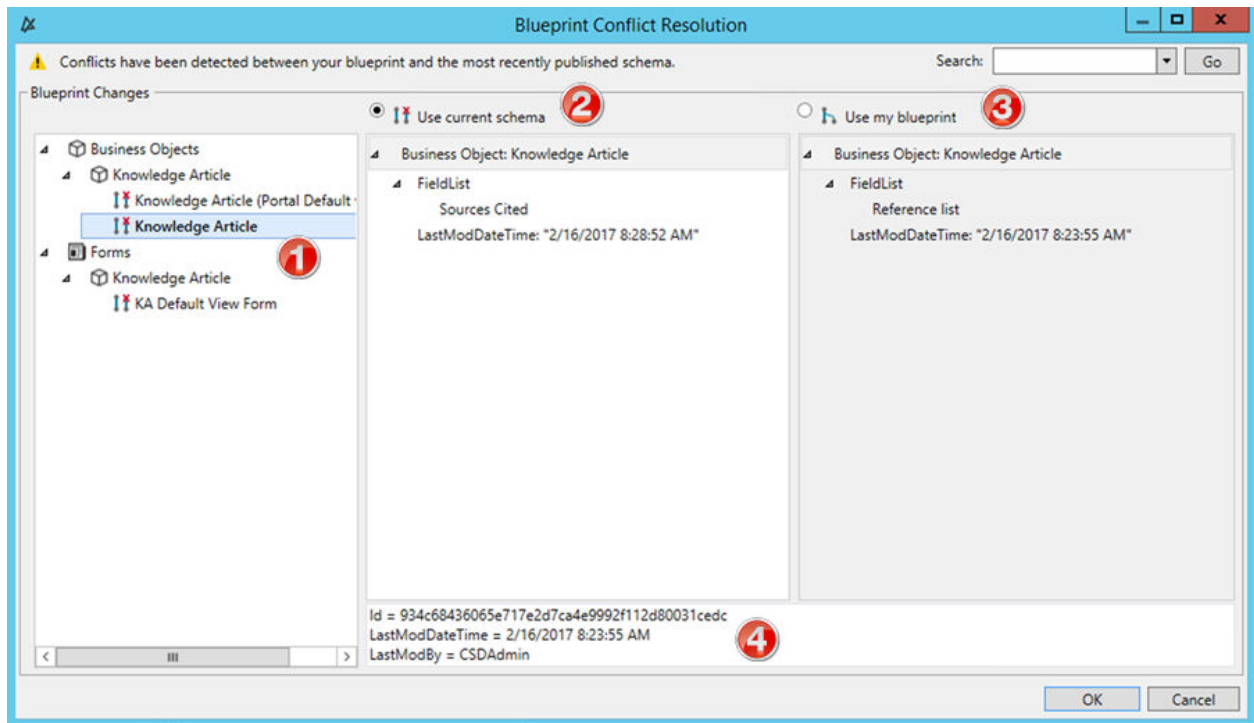
1. The left pane lists conflicts between the most recently-published schema and the Blueprint . Choose item by item which new changes to apply to the schema.

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 CSM concurrent development, see CSM System Design Using Concurrent Development.

You can choose to bypass this feature by selecting Ignore Conflicts in the Publish Options window.

Using Blueprints

When working with Blueprints, 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** (click 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 CSM system design using concurrent development.

Manage System Objects

Use the Object Manager (and its various Editors), accessed from within a Blueprint, to manage the following System Objects:

- Business Objects
- Fields
- Forms
- Grids

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 the following Business Objects:

- Supporting Objects
- 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 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, the data in your system is not actually modified until the Blueprint is published or the mApp 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, 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, 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 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 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.
Abandon	Abandons changes to the current item.
Delete	Deletes the current selection.
Include	Includes the selected row (record) in the current Blueprint/mApp (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.
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.
	Abandon	Abandons changes to the current item.
	Delete	Deletes the current selection.
	Include	Includes the selected record in the Blueprint/mApp (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.

Button	Action	Description
▶▶	**Go to next record**	Jumps to the next record in set.
▶▶▌	**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 mApp is applied.

When you first access the Data Editor, the Main pane displays a Grid showing a Blueprint/mApp 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 Action column shows what will be done to each record in the table when the Blueprint is published (or the mApp 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.

Localization and Lookup Tables

If you have Globalization enabled for your system and Localization is enabled for a Lookup Object, the Data Editor includes a column for each culture enabled for your system.
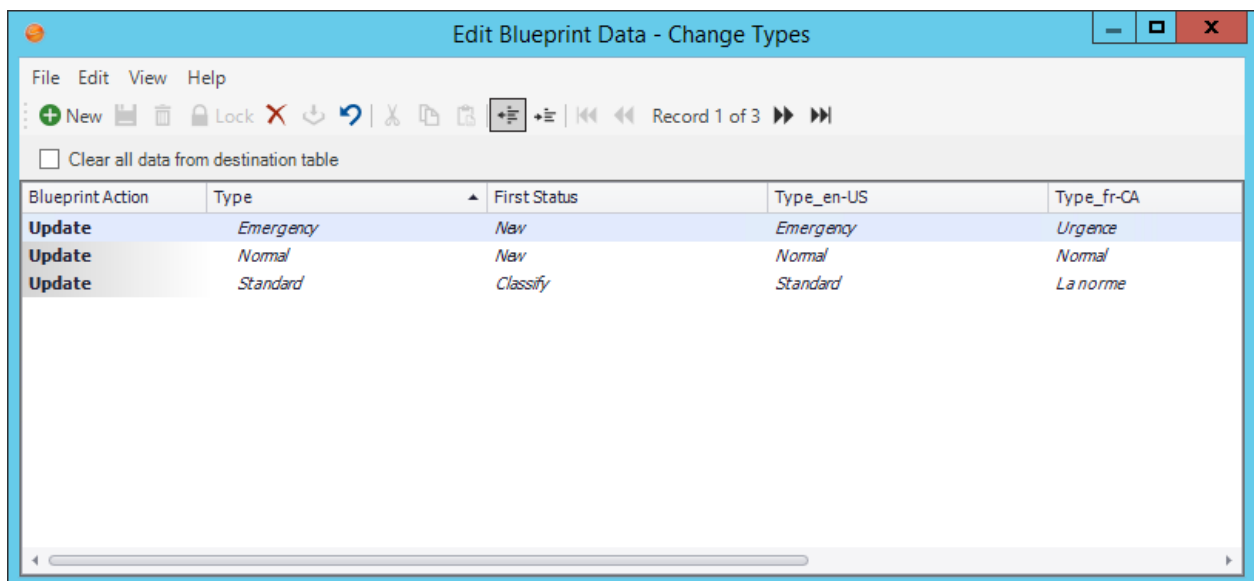
Open the Data Editor

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, 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, 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 (example: Dashboards, Calendars, etc.) at a system level using the various CSM Item Managers, accessed by clicking **Managers** from the Blueprint Editor menu bar. When you access CSM Item Managers from within a Blueprint, you can view, add, edit, or delete items in the Blueprint scope. This scope is for items that administrators do not want Users to access and manipulate.

Note: For more information about the CSM Items and their Managers, refer to their respective documentation.

Access Blueprint Tools/Functionality

Use a Blueprint to access the following Blueprint tools/functionality:

- Configure Directory Services: Opens the Directory Services window, where you can add, edit, delete, and copy Directory Service definitions.
- Export a Schema.
- View the Blueprint Publish Log.
- Define global database settings (Options).

Access all Blueprint tools/functionality by clicking **Tools** on the Blueprint Editor menu bar.

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.

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. Use a Blueprint Schema to quickly and easily scan the characteristics of your Business Objects.

You can export the following meta-data for Major, Supporting, and Lookup Objects:

- Properties
- Lifecycle
- Fields (and Field properties)
- Relationships (and Relationship properties)
- One-Steps
- 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-Steps

   Approvals

Automation Processes

5. Click 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.

- 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, inlcuding:

- 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 the No Limit check box to indefinitely attempt to complete the operations.

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. Click 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, such as:

- 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.

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 database, either:
      Restricted File Growth: Select this radio button to restrict the database to a maximum size (in MB). Then, specify the maximum size.

      Unrestricted File Growth (**recommended**): Select this radio button to allow the database to grow until it runs out of space.
6. Click OK.

CSM Administration

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 for:

- 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.

CSM Administration   329

Configuring Blueprints

System Blueprints Security rights are configured in CSM Administrator. See System Blueprints Security Rights.

mApps

A Cherwell mergeable application (mApp™) is a bundle of CSM system definitions (Business Objects/ Fields, Forms, Grids, Relationships, Actions/One-Steps, Search Groups, etc.), along with merge instructions, that allows definitions to be transferred between databases and functionality to be merged.

About mApps

▶ **3-Minute Video**: About mApps.

Use a mApp to share packages of functionality across databases, allowing Users to implement proven functionality into their CSM systems. A number of Cherwell mApps 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 mApps. After you create a mApp, 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 to CSM systems based on the items that were included in the mApp.

mApps are accessed and managed through the mApp Editor, which is similar to the Blueprint Editor, except it has multiple options for adding items to a mApp and defining their behavior. mApps have their own workflow.
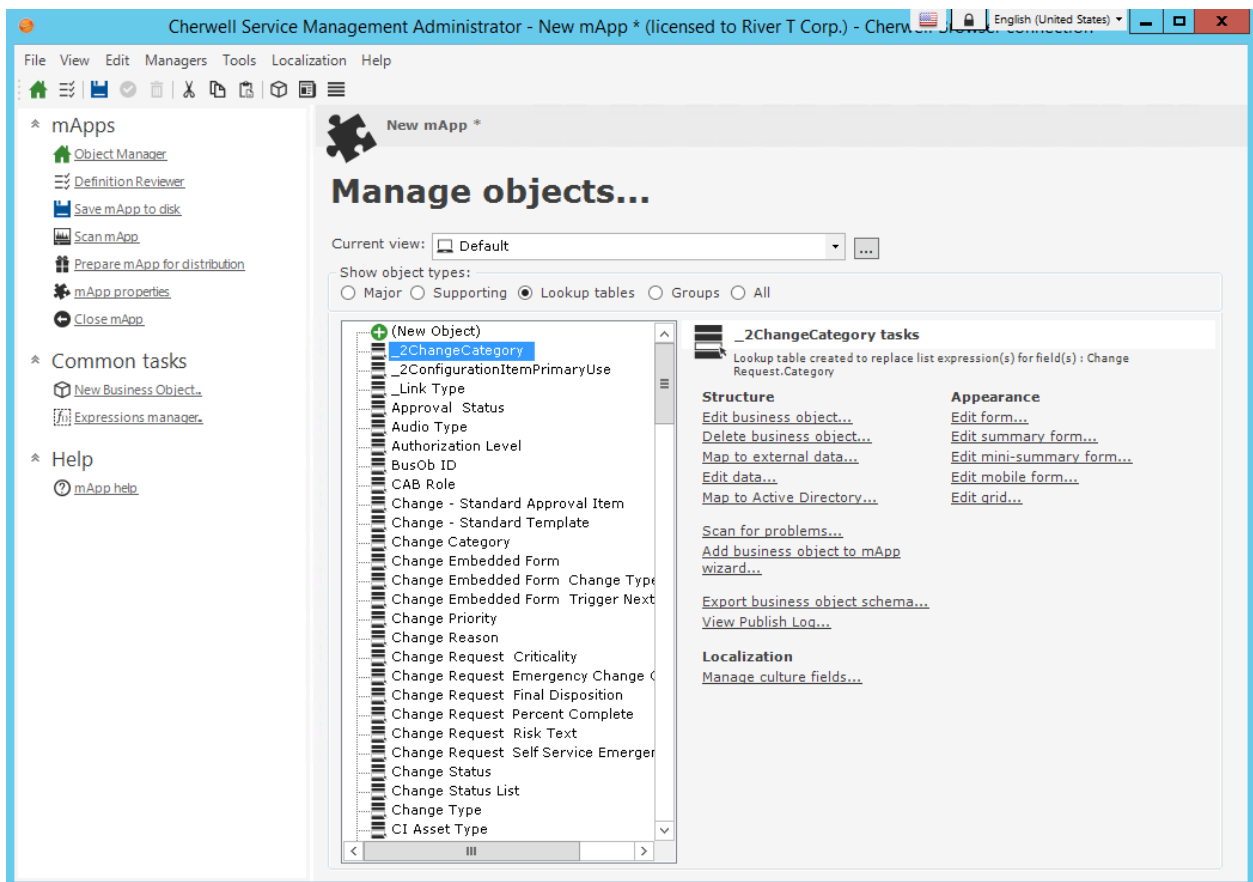
mApp Workflow

1. Create a mApp.

2. Define mApp properties.

3. Save the mApp to a named .mAppBP file (File>Save As).

4. Add/edit definitions and items to the mApp:
   System Objects:
   - Business Objects
   - Fields
   - Relationships
   - Forms
   - Grids
   - Form Arrangements

   CSM Items (example: Dashboards, Search Groups, One-Steps, etc.)

   Business Object Data (for Supporting Objects and Lookup Objects)

5. Periodically save your changes 💾.

6. Periodically scan the mApp for potential errors.

7. View the changes the mApp will make to the target system's definitions when the mApp is applied.

8. Prepare the mApp for distribution by validating that it is complete and ready for distribution.

   Note: At this point, the mApp must be saved as a .mApp file. This is required in order for it to be applied using the Apply mApp Wizard.

9. Distribute the mApp file directly to potential Users, or submit it to the mApp Exchange.

10. Apply the mApp to a CSM system (using the Apply mApp Wizard).
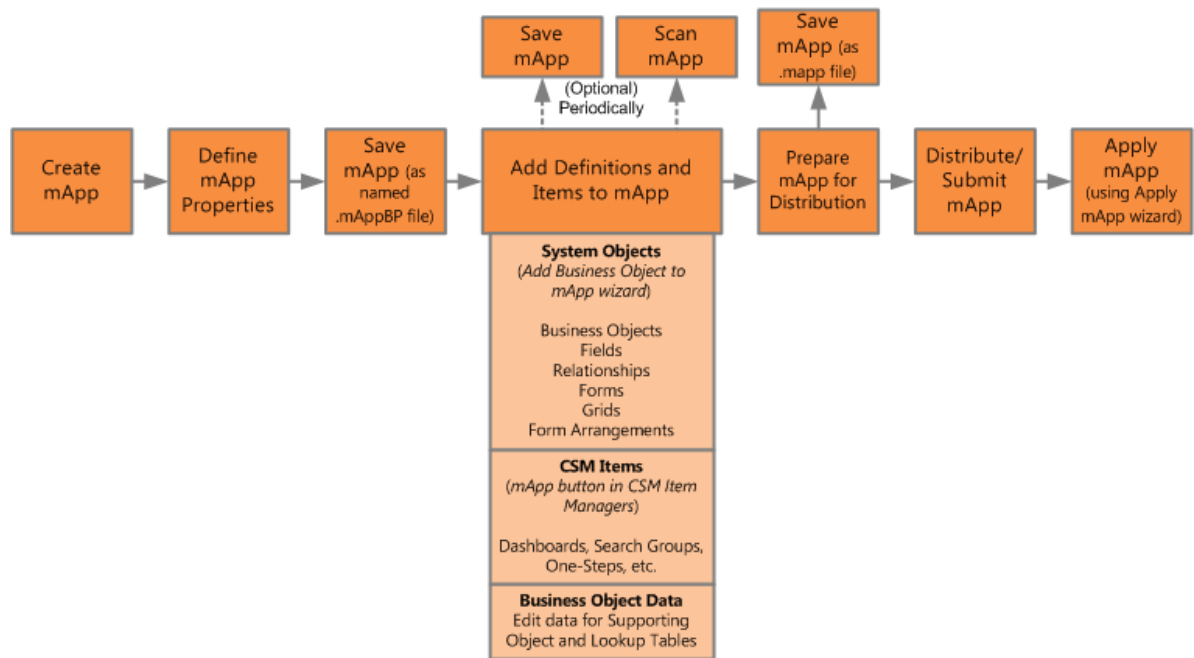
mApps Page

Use the CSM Administrator mApps page to quickly access common mApp operations, including:

- View installed mApps: Opens a window to view a list of mApps that have already been installed in your system.
- Go to the mApp Exchange: Navigates to the mApp Exchange to submit created mApps and view mApps that other Users have submitted.
- Set Designer ID: Allows mApp 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.
- View mApp 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: Opens the Apply mApp Wizard to walk through the process of applying a mApp to a CSM system.
- Create a New mApp: Creates a new unnamed mApp, and then launches it in the mApp Editor.
- Edit an Existing mApp: Allows you to browse for and open an existing mApp file so that you can edit it in the mApp Editor.

Open the mApps page by clicking the **mApps** category in the CSM Administrator main window.

mApps Good to Know

- mApps affect system definitions and are used and managed from within CSM Administrator because they affect system definitions. Access mApps and mApps functionality from the CSM Administrator mApps page.
- When creating and working with mApps, the CSM Administrator interface changes to the mApp Editor, which allows you 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.
    - Add CSM Items to a mApp: Use the mApp Options button 　 in CSM Item Managers (or right-click item>Add to mApp) to include things like One-Steps, Dashboards, Search Groups, etc. in a mApp.
    - Edit Business Object Data: Use the Edit Data task within a mApp to manage (add, edit, or delete) data for a Supporting Object or Lookup Table.
- An open (working) mApp is saved to a .mAppBP file. When the mApp is prepared for distribution, it is saved as a .mApp file (extension required for a mApp to be applied to a target system).
- Use the References window to view referenced definitions (all of the definitions that are dependent on a Business Object or CSM Item included in a mApp).
- Use the mApp Changes window in the mApp Editor to view the changes a mApp will make to a target system's definitions.
- When you include a definition in a mApp, you decide how it will be handled when the mApp 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 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) in a mApp 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.
        - 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 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 definition into the target system (the existing definition is left unchanged).
    - Merge: Merges the mApp 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)

Always consider the following:

- CSM is highly configurable. As a result, a User's system may vary from the Out-of-the-Box content in our documentation.

- Security rights control access to CSM functionality and are configured in the Security Group Manager in CSM Administrator (CSM Administrator>Security>Edit Security Groups). For more information, see Configure mApp Security Rights.

mApp Compatibility

Due to changes made to support Globalization, the following guidelines apply to mApps:

- mApps created using CSM 9.2.0 or later cannot be applied to an earlier version of CSM.
- When you apply a mApp to that was created on a version earlier than CSM 9.2.0, you are prompted to select a target culture for the mApp. You must perform this task even if Globalization is not enabled for your system.

Managing mApps

mApps are managed in CSM Administrator using the mApp Editor. Use the mApp Editor to:

- Create a mApp.
- Edit an existing mApp.
- Save a mApp.
- Scan a mApp.
- Close a mApp.
- View mApp changes.
- Prepare a mApp for Distribution.

mApp Editor

The mApp Editor is the built-in interface within CSM Administrator that allows you to manage mApps and access various tools for adding definitions to mApps.

Use the mApp 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.

- **Add CSM Items to a mApp**: Use the mApp options button ✳ in CSM Item Managers (or **right-click** item**>Add to mApp**) to include things like One-Steps, Dashboards, Search Groups, etc. in a mApp.

- **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.

- **Edit Business Object Data**: Use the Edit Data task within a mApp to modify (add, edit, delete) data for a Supporting Object or Lookup Table.

- **Manage mApps**: Use the tasks in the Task Pane and/or File menu to:
  - Define mApp properties.
  - Save and close mApps.
  - View the changes the mApp will make to the target system's definitions (File>mApp Changes).
  - Prepare mApps for distribution.

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.

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.
Save As	Saves the new or active mApp as a named .mAppBP file.
Close mApp	Closes the mApp, but not CSM Administrator. If the mApp 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 for potential errors.
Prepare mApp for Distribution	Validates the mApp to ensure it is complete and ready to be distributed to potential users or to the Cherwell community.
mApp Properties	Opens the mApp Properties window to define general mApp 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 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 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
Automation Processes	Opens the Automation Process Manager.
Calendar Manager	Opens the Calendar Manager.

Action	Description
Counters	Opens the Counter Manager.
Dashboards	Opens the Dashboard Manager, Widget Manager, Metrics Manager, or Color Palette Manager.
Database Server Objects	Opens the Database Server Objects Manager.
Document Repositories	Opens Document Repository 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.
Images	Opens the Image Manager.
Knowledge	Opens Knowledge Mapping Manager and Knowledge Source Manager.
One-Step	Opens the One-Step Manager.
Searches	Opens the Search Group Manager.
Site Manager	Opens the Portal Site Manager.
Stored Values	Opens the Stored Value Manager.
Teams	Opens the Team Manager.
Themes	Opens the Theme Manager.
Visualizations	Opens the Visualization 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 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.

Action	Description
Report Error	Opens the Report Error window so you can report an error to Cherwell Software.
About	Opens an About window to view version and licensing information for CSM.

mApp Editor Toolbar

Use the mApp Editor toolbar to quickly access common mApp tasks.

Note: The mApp Editor toolbar is dynamic so options vary depending on what is active in the mApp Editor Main pane (ex: 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 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.
	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.

mApp Editor Task Pane

Use the mApp Editor Task Pane to access mApp tasks, specifically:

- mApps: Tasks for managing mApps.
- Common Tasks: Common mApp 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 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.

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.

Create a mApp

▶ **3-Minute Video**: Create a Cherwell mApp.

Use the Create a New mApp task in the CSM Administrator main window to create a mApp. When you create a mApp, you:

- Define general mApp properties, including name, description, display image, etc. You can also define mApp Features to group subsections of definitions together.
- Add various definitions and items (Business Objects, CSM Items, and Business Object data) to the mApp and specify how they will be merged into the target system.

To create a mApp:

1. In the CSM Administrator main window, click the mApps category, and then click the Create a New mApp task.

   A mApp is created, and its interface, the mApp Editor, opens. By default, the Object Manager is displayed in the mApp Editor's Main pane. The mApp is unnamed (called New mApp*) until saved to a named mApp Blueprint file (.mAppBP).

2. Define mApp properties.

3. Save the mApp to a named .mAppBP file (**File>Save As**).

4. Add definitions and items to the mApp:
   Use the *Add Business Object to mApp* Wizard to walk through the process of adding Business Objects and their associated Fields, Relationships, Forms, Grids, and Form Arrangements to a mApp.

   Use the mApp Options button ✳ (or right-click item>Add to mApp) in CSM Item Managers to add CSM Items (ex: One-Steps, Dashboards, Search Groups, etc.) to a mApp.

   Use the Edit Data task within a mApp 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).

5. Save changes to the named open mApp (click the Save button 💾). You can also view the changes that will be made to the target system's definitions.

   Tip: Periodically scan your mApp to find potential errors.

   When ready, you can prepare the mApp for distribution, and then distribute the file directly to potential Users, or submit it to the mApp Exchange. System administrators apply the mApp to CSM systems using the Apply mApp Wizard.

Set a Designer ID
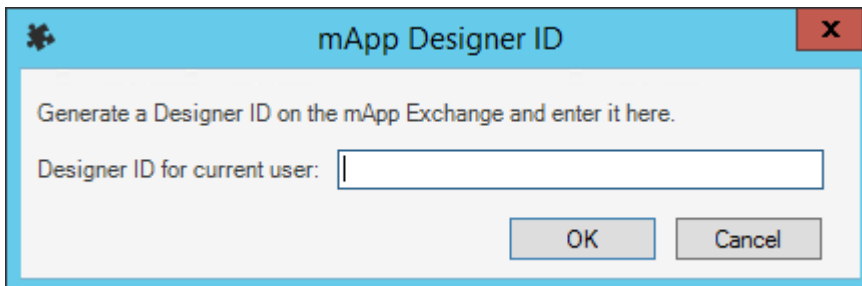
Use the Set Designer ID task on the mApps page in CSM Administrator to save a unique Designer ID to your current User information. Setting a Designer ID uniquely identifies the definitions you add to a mApp and tracks them in history records.

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.
- Designer IDs are generated on the mApp Exchange. Values from sources other than the mApp Exchange are invalid.
- 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 name.
- If a mApp 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).

To set a Designer ID in CSM Administrator:

1. In the CSM Administrator main window, click the mApps category, and then click the Set Designer ID task.

2. Enter your Designer ID (generated on the mApp Exchange).

3. Click OK.

Define mApp Properties

Use the mApp properties window (accessed from within the mApp Editor) to define the following:

- General properties:
    - Name and description: Specific name and description for the mApp.
    - (Optional) Image: Image to represent the mApp.
    - Created by: Name of mApp creator (individual or organization).
    - (Optional) Details URL: Site that contains detailed information about the mApp.
- (Optional) Features: Definitions grouped together into subsections of functionality.

Good to know:

- General properties are displayed in the Apply mApp Wizard when system administrators apply a mApp to a CSM system, and in the Installed mApps window when Users view the mApps that have been installed in their systems.
- You must define at least general properties in order for the mApp to be considered ready for distribution.
- If you have Globalization and multiple cultures enabled for your system and translations that impact your mApp have been applied, you must define mApp properties for each culture. For more information, see Applying Translations to mApps.
- Business Object and CSM Item definitions can be grouped together into Features (subsections of functionality) using mApp conditions. Features can then be applied (or not) as a whole in the Apply mApp Wizard.

To define mApp properties:

1. Open the mApp Editor
2. From the mApp Editor menu bar, click File>mApp Properties.
3. Click the General Properties page.

4. Define general properties for the mApp:

Name: Provide a **display name** to use for the mApp.

Description: Provide a **description** of the mApp. 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.
- None: Select this radio button to not associate an image with the mApp.
- File: Select this radio button to use an image for the mApp. Then, click the Ellipses

    button [...] to browse to the location of the image file, select the file, and click Open.

Created by: Provide the **name** of the organization or individual who created the mApp.

Details URL: If detailed information about the mApp is available on a website, provide the **URL**

here. Then, click the **Ellipses** button [...] to navigate to the site (and ensure the URL is correct).

Allow this mApp to be applied to systems earlier than [CSM version]: Select this check box to allow Users to apply the mApp to CSM systems that are older than the version from which the mApp was created. In the Apply mApp Wizard, Users who apply a mApp created from a CSM system later than their current version are allowed to apply the mApp, but with a warning that all functionality in the mApp might not behave as expected. If this check box is not selected, the Apply mApp Wizard displays a message that Users must upgrade their CSM systems to the same version as the mApp before they can apply it.

Note: When you select this check box for a mApp created in CSM version 5.11 or later, you will receive a warning message that CSM versions below 5.11 do not check for a minimum version before applying a mApp.

5. Click the Features page.
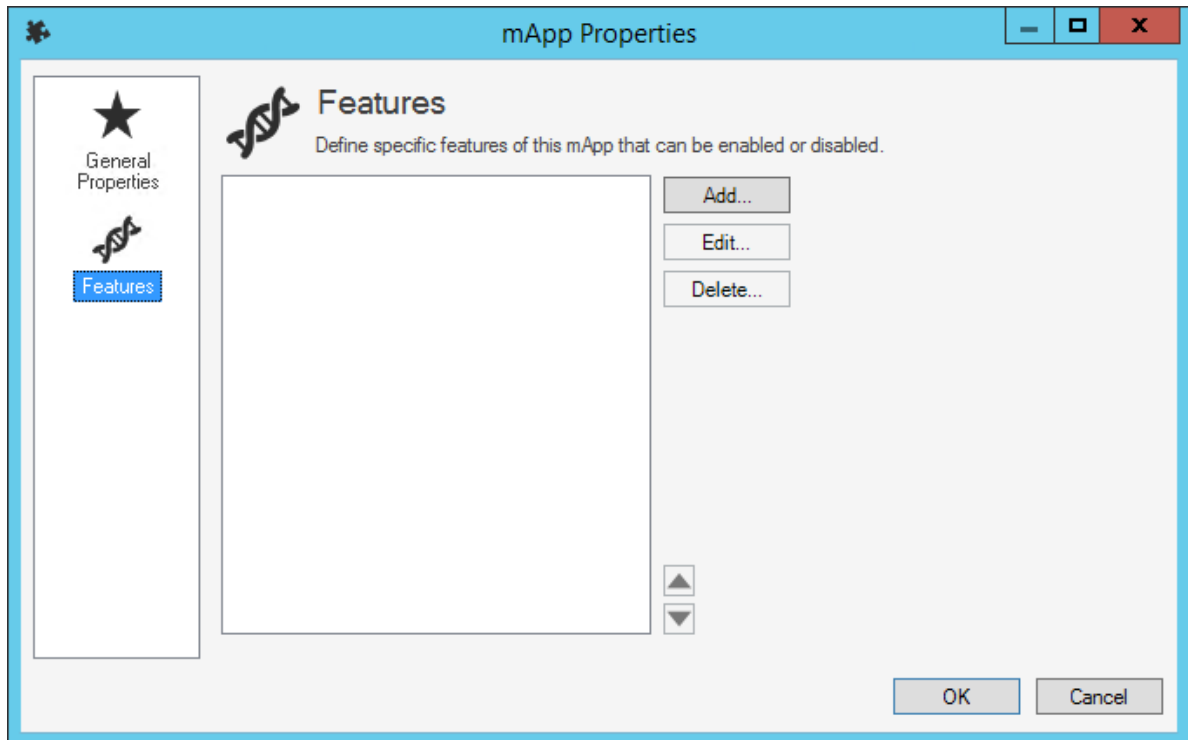
6. (Optional) Define mApp Features:
   a. Click Add to add a new Feature.
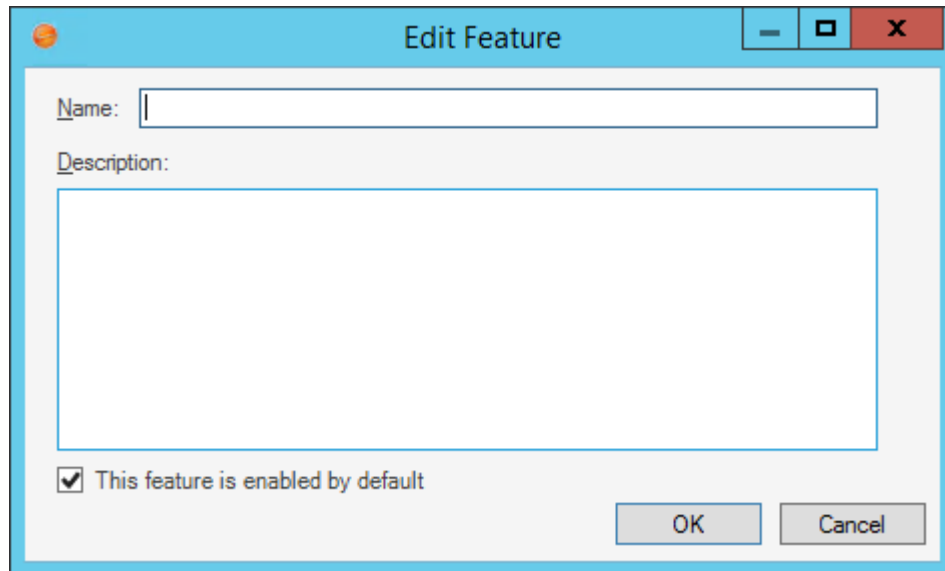
b. Define general properties for the Feature:

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 to his system, so ensure that the description is clear.

This Feature is enabled by default: Select this check box to include the mApp Feature by default when the mApp is applied to a CSM system using the Apply mApp Wizard.

c. Click OK.

7. Click OK.

8. Prepare the mApp for Distribution (File>Prepare mApp for distribution), or save the mApp (File>Save mApp to Disk) to continue making other changes.

Add Business Object to mApp Wizard

The Add Business Object to mApp 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. Use the Add Business Object to mApp Wizard to select which Business Object to add to the mApp and define its importance to the mApp. Then, define how the Business Object will be imported into the target system when the mApp 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 (ex: 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 click the *Uncheck All* button to clear everything in the list (ex: Clear all Fields) or the *Select All* button to select everything in the list.

Add a Business Object to a mApp

The Add Business Object to mApp 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. Use the Add Business Object to mApp Wizard to select which Business Object to add to the mApp and define its importance to the mApp. Then, define how the Business Object will be imported into the target system when the mApp 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 (ex: 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 click the *Uncheck All* button ⊞ to clear everything in the list (ex: Clear all Fields) or the *Select All* button ☑ to select everything in the list.

To add a Business Object to a mApp:

1. Open the mApp Editor
2. Click a **Business Object** in the Object tree, and then click the Add Business Object to mApp Wizard task in the Structure area.
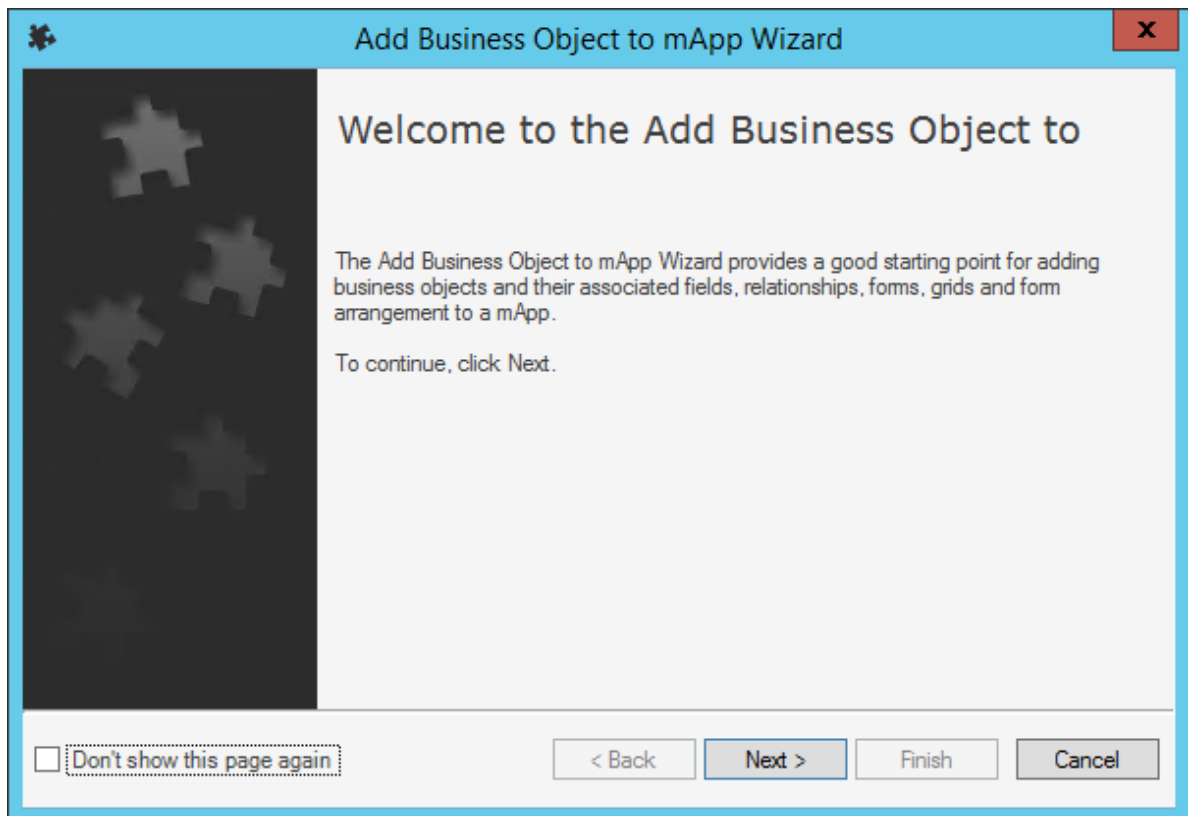
Tip: You can also open the wizard from the Business Object Editor within a mApp, either by clicking the **Add to mApp** button or the **Add to mApp Wizard** link in the Business Object section of the mApp Editor Task Pane.

3. Select a Business Object to include in the mApp, and then specify its importance to the mApp:
   a. In the drop-down, 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 for reference.

      Tip: The drop-down 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. This marks the items in the mApp file according to importance so that when a mApp 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.

(Default) Medium Importance: Select this radio button if the Business Object is a supporting object for the mApp.

Low Importance: Select this radio button if the Business Object is not critical for the mApp.

Tip: You can click 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 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, 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, but the associated Relationship is not added by the mApp 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.
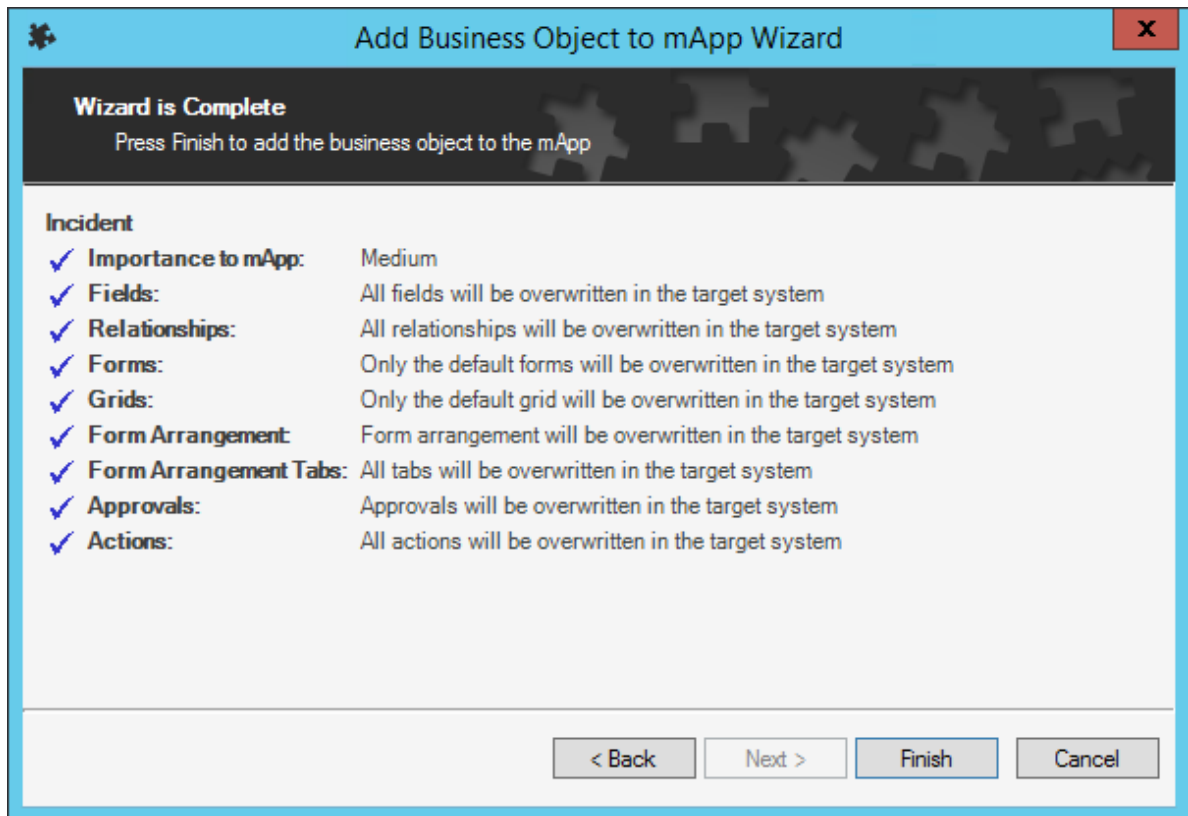
13. Click Finish.

The Business Object and its associated Fields, Relationships, Forms, Grids, and Form Arrangements are added to the mApp. When the mApp is applied, these definitions will be imported into a target system according to the selections you made.

14. (Optional) Add additional Business Objects or CSM Items to the mApp.

15. (Optional) Use the mApp Options button ✷ in the various properties windows to configure merge actions for Business Object definitions.

16. Prepare the mApp for Distribution (File>Prepare mApp for distribution), or save the mApp (File>Save mApp to Disk) to continue making other changes.

Add CSM Items to a mApp

Use the mApp Options button ✹ in CSM Item Managers to include CSM Items (ex: Automation Processes, One-Steps, Dashboards, Search Groups, etc.) in a mApp and define how they are imported into a target system when the mApp 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 for informational purposes only (it is not merged into the target system when the mApp is applied).
- Import/remove based on condition: Imports or removes the item definition based on configured conditions.

Good to know:

- Click the References button to see which definitions throughout CSM are being used by the definitions in a mApp. This allows you to ensure that all necessary definitions are included in the mApp.
- You can define some additional options when adding Stored Values and external connections to a mApp. For more information, see Add a Stored Value or External Connection to a mApp.

To add a CSM Item to a mApp:

1. Open the mApp Editor
2. From the menu bar, click Managers, and then click a CSM Item Manager to open it.
3. Select an item, and then click the mApp Options button ✹ .

    Tip: You can also **right-click** an item, and then click Add to mApp in the context menu.
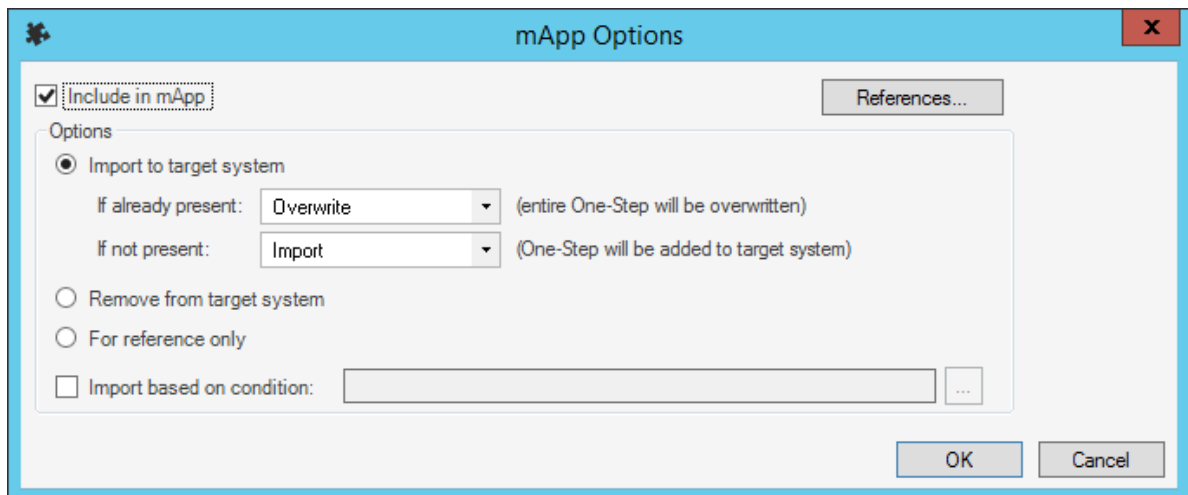
4. Define general options for the item:

Include in mApp: Select this check box to include the item in the mApp.

References: Click this button to view which other definitions in the system are being used by the selected item.

Note: Dashboards are currently the only CSM Items that automatically prompt you to add associated items (Widgets) when you include them in a mApp.

5. Define options for how to import the item into a target system (Options area):

Note: These options are only available if *Include in mApp* 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 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 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 definition is not imported into the target system when the mApp 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 definition into the target system if does not already exist.

- Don't Import: Select this option to skip importing the mApp definition into the target system if it does not already exist (the mApp definition will not be added to the target system).

Remove from Target System: Select this radio button to have the mApp 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 for reference. When the mApp is applied, the item definition will not be merged into the target system; it exists in the mApp 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 import or remove the item definition based on conditions. Then, click the Ellipses button [...] to open the mApp Conditions window and configure conditions.

6. Click OK.

7. Prepare the mApp for Distribution (File>Prepare mApp for distribution), or save the mApp (File>Save mApp to Disk) to continue making other changes.

Add a Stored Value or External Connection to a mApp

Use the mApp Options button ![icon] in the Stored Value Manager or the External Connection Manager to include Stored Values and/or external connections in a mApp and define how they are imported into a target system when the mApp 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 for informational purposes only (it is not merged into the target system when the mApp is applied).
- **Import/remove based on condition:** Imports or removes the item definition based on configured mApp 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. This allows you to ensure that all necessary definitions are included in the mApp.
- This procedure assumes that the Stored Values and/or external connections being added to a mApp 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:

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: Select this check box to include the item in the mApp.
>
> 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* 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 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 definition is not imported into the target system when the mApp 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 definition into the target system if does not already exist.

- Don't Import: Select this option to skip importing the mApp definition into the target system if it does not already exist (the mApp definition will not be added to the target system).

Remove from Target System: Select this radio button to have the mApp 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 for reference. When the mApp is applied, the item definition will not be merged into the target system; it exists in the mApp 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 import or remove the item definition based on conditions. Then, click the Ellipses button to open the mApp 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 Wizard question modes: Select the interaction level(s) at which the prompt is displayed in the Apply mApp Wizard:

- Ask me about every decision (default): Select this check box to prompt the User in the Apply mApp 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 Wizard).

- Make reasonable decisions, but ask me if unsure: Select this check box to prompt the User in the Apply mApp 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 Wizard).

- Don't ask me unless absolutely necessary: Select this check box to prompt the User in the Apply mApp 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 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. Click OK.

8. Prepare the mApp for Distribution (File>Prepare mApp for distribution), or save the mApp (File>Save mApp to Disk) to continue making other changes.

Edit Business Object Data in a mApp

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, select a Supporting Object or Lookup Object (ex: 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 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 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 *For Reference Only* if they are not already in the mApp.

- Because data is edited within a Blueprint or a mApp, the data in your system is not actually modified until the Blueprint is published or the mApp is applied.
- Business Object Data is limited to 1,000 records. You will receive a warning if you exceed that limit.

Open an Existing mApp

Use the Edit tasks (accessed from the CSM Administrator main window) to open an existing mApp and edit it.

To open an existing mApp:

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 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 opens in the mApp Editor. The name of the mApp is displayed at the top of the CSM Administrator window and at the top the mApp Editor.

Save a mApp

There are two save options for a mApp:

- Save As: Saves a mApp as a named mApp Blueprint (.mAppBP) file.
- Save to disk: Saves changes to the open mApp (.mAppBP) file.

Good to know:

- When you prepare the mApp for distribution, you save it as a .mapp file. This extension is required before a mApp can be applied to a system using the Apply mApp Wizard.

To save a mApp as a named .mAppBP file:

1. Create a mApp.From the mApp Editor menu bar, click File>Save As.

   Tip: You can also save a mApp as a named .mAppBP file by clicking **Save mApp to Disk** in the mApps section of the mApp Editor Task Pane.

2. Provide a **filename** for the mApp.

   Note: Ensure that the file type is **.mAppBP**.

3. Click Save.

   A .mAppBP file is created. The name of the mApp 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:

1. In a mApp, 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

Use a mApp Scan to periodically check your working mApp 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 mApps 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, scan the mApp again to ensure that the newly added definitions do not reference additional definitions that need to be included in the mApp. Depending on the nature of the mApp, some errors or warnings might be acceptable and do not need to be resolved.

To scan a mApp:

1. Open the mApp Editor

2. From the mApp Editor menu bar, click File>Scan.

   Tip: You can also scan a mApp by clicking **Scan mApp** in the mApps section of the mApp Editor Task Pane.

   If the scan is successful, a success window opens.

   If the mApp contains changes that require reloading definitions or restarting applications after the mApp is applied, an alert appears along with the scan results. The alert is triggered if the mApp contains changes to significant system definitions, such as Business Objects, Forms, Grids, Form Arrangements, Relationships, Custom Views, One-Steps, automated behaviors, Dashboards, and/or Widgets.
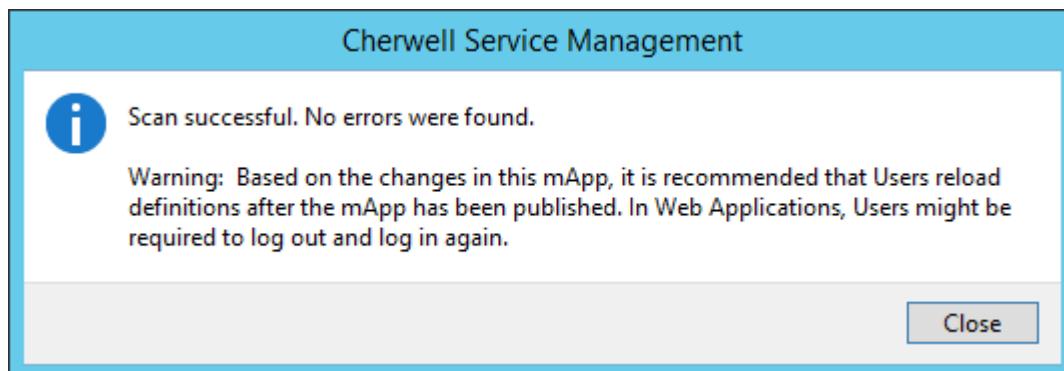
   If the scan detects errors, the mApp Scan Results window opens.
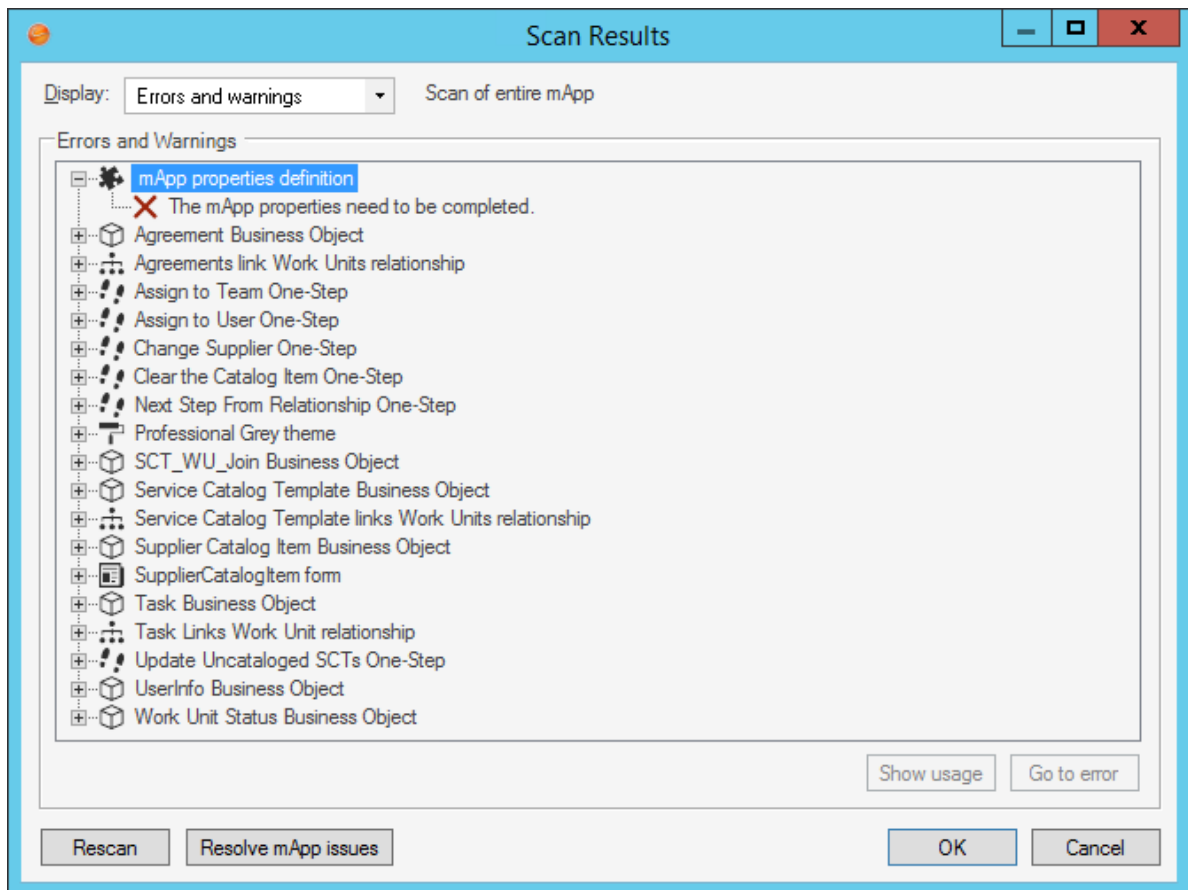
Examples: You will receive errors if you do not define general mApp Properties, or if a definition in the mApp references another definition that is not included in the mApp.

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.

Resolve mApp Issues: Click this button to resolve all errors and warnings that can be automatically resolved. If mApp Properties have not been defined, the mApp Properties window will open so that you can complete the properties.

4. Click OK.

Close a mApp

Use the Close mApp option to close the active mApp, but not CSM Administrator.

To close a mApp:

1. From the mApp Editor menu bar, click File>Close mApp.

   Tip: You can also close a mApp by clicking **Close mApp** in the mApps section of the mApp Editor Task Pane.

   If the mApp 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 Changes

Use the mApp Changes window in the mApp Editor to view the system definitions that will be changed by the active mApp when it is applied to the target system. When you view mApp changes, you can:

- Select how changes are grouped (by Business Object, Definition Type, or View).
- Search for specific items in the mApp.
- Remove items from the mApp.
- Compare the mApp 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 for informational purposes only.
No Icon	Don't Import	Definition will not be imported into target system.

The mApp Changes window can be opened from the mApp Editor Menu Bar (File>mApp Changes).
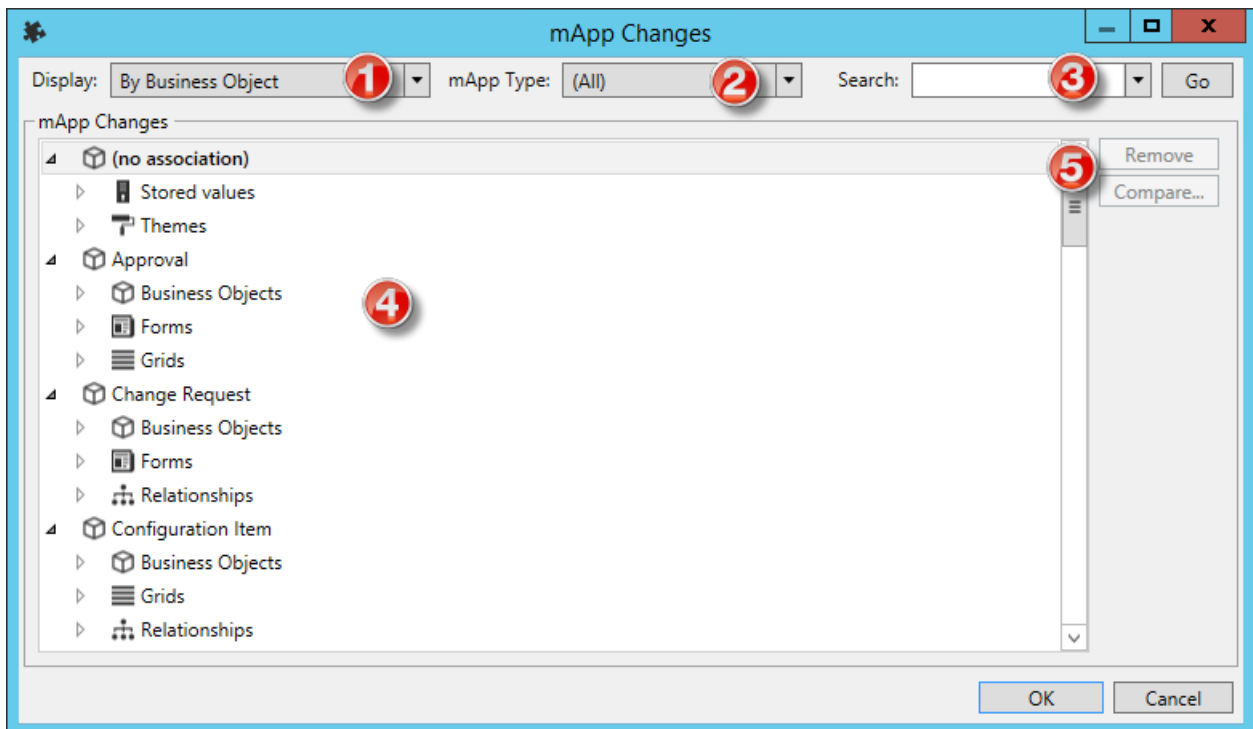
1. Display: Groups items in the tree by Business Object, Definition, or View.

    By Business Object: Groups changes by Business Object (ex: Incident).

    By Definition Type: Groups changes by the type of system definition (ex: Forms).

    By View and then Business Object: Groups changes by View (ex: Default, Portal Default) and then by Business Object (ex: Incident).

    By View and then Definition Type: Groups changes by View (ex: Default, Portal Default) and then by type of system definition (ex: Forms).

2. mApp 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 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 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.

4. mApp Changes Tree: Displays items 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 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 (it is not removed from the system).

Click Compare to open the mApp Differences window and compare the mApp 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 (Business Object, Definition Type, or View).
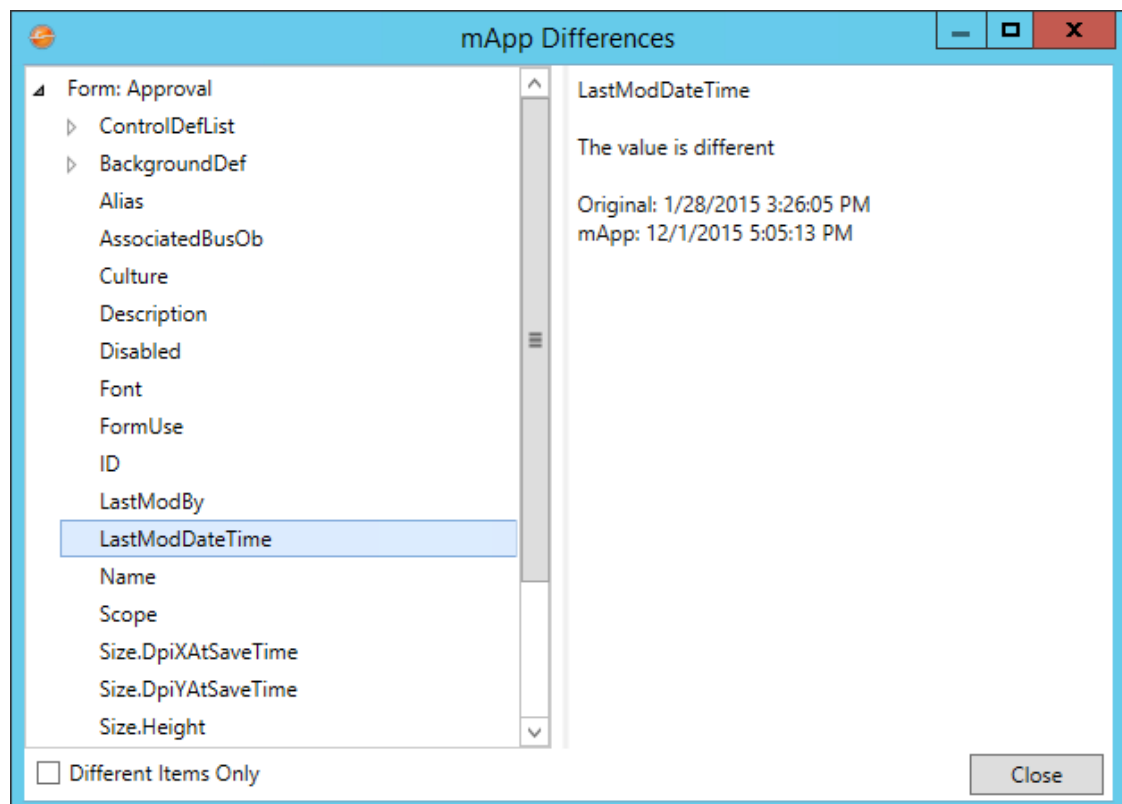
Select the Different Items Only check box to limit the list of existing system definitions to those that the mApp affects.

Rebase mApp Definitions

Use the Rebase mApp Definitions operation to reload mApp definitions from your underlying CSM system. This allows you to update definitions in a mApp 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 that includes an Incident Business Object, and then the Business Object is updated in the underlying system (ex: Fields are added/deleted), you can update the Business Object definitions in the mApp to reflect those changes.

To rebase mApp definitions:

1. mApp definitions can be rebased in several ways:
   (All definitions in a mApp) 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 Version of Bus Ob, etc.* option is only available if the selected Business Object is included in the mApp.

   The Rebase Business Object window opens. By default, all definitions included in the mApp 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.
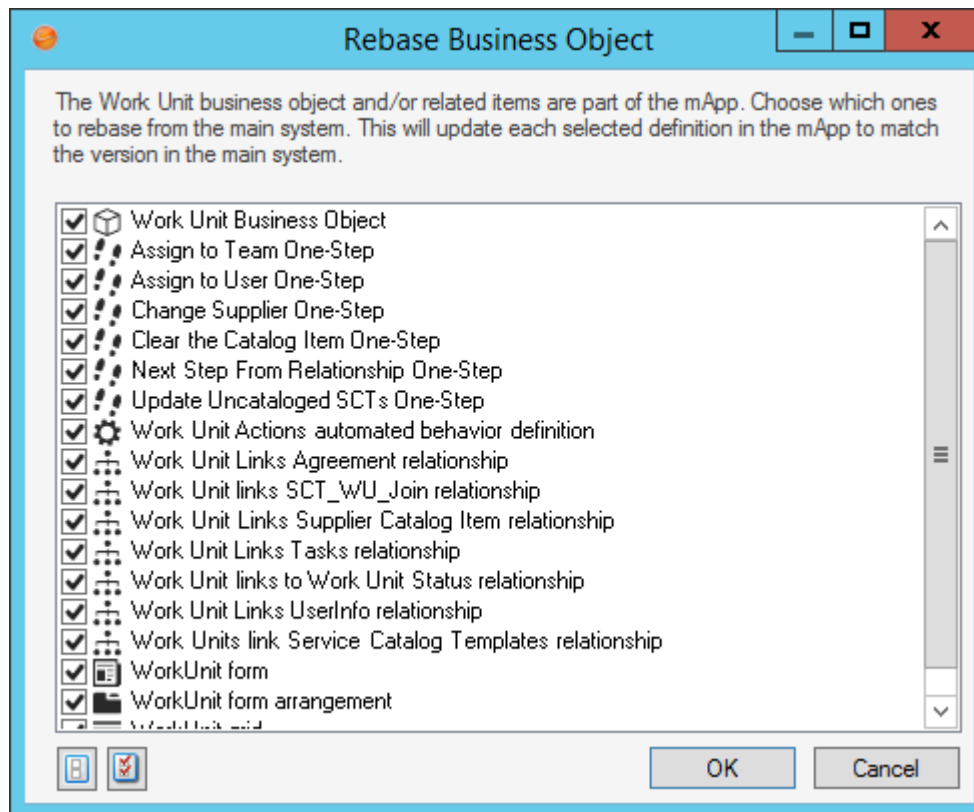
(A specific CSM Item definition) In a CSM Item Manager (ex: One-Step Manager) in the mApp Editor, right-click an **item** (ex: One-Step) that is included in the mApp, and then select Rebase in mApp from system.

Prepare a mApp for Distribution

Prepare a mApp for distribution when you are ready to submit the mApp to the mApp Exchange, or distribute it directly to potential users. When you prepare a mApp 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 contains translations, you must define mApp properties for each culture before you can prepare the mApp for distribution. See Applying Translations to mApps.
- If the mApp 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 for distribution:

1. Scan the mApp before preparing it for distribution. This allows you to resolve any issues in the mApp, as well as in the underlying system from which the mApp was created.

2. Open an existing mApp.

3. From the mApp Editor menu bar, click File>Prepare mApp for distribution.

   Tip: You can also prepare a mApp for distribution by clicking **Prepare mApp for distribution** in the mApps section of the mApp Editor Task Pane.

   If there are errors that need to be resolved, the mApp Preparation Scan window opens.
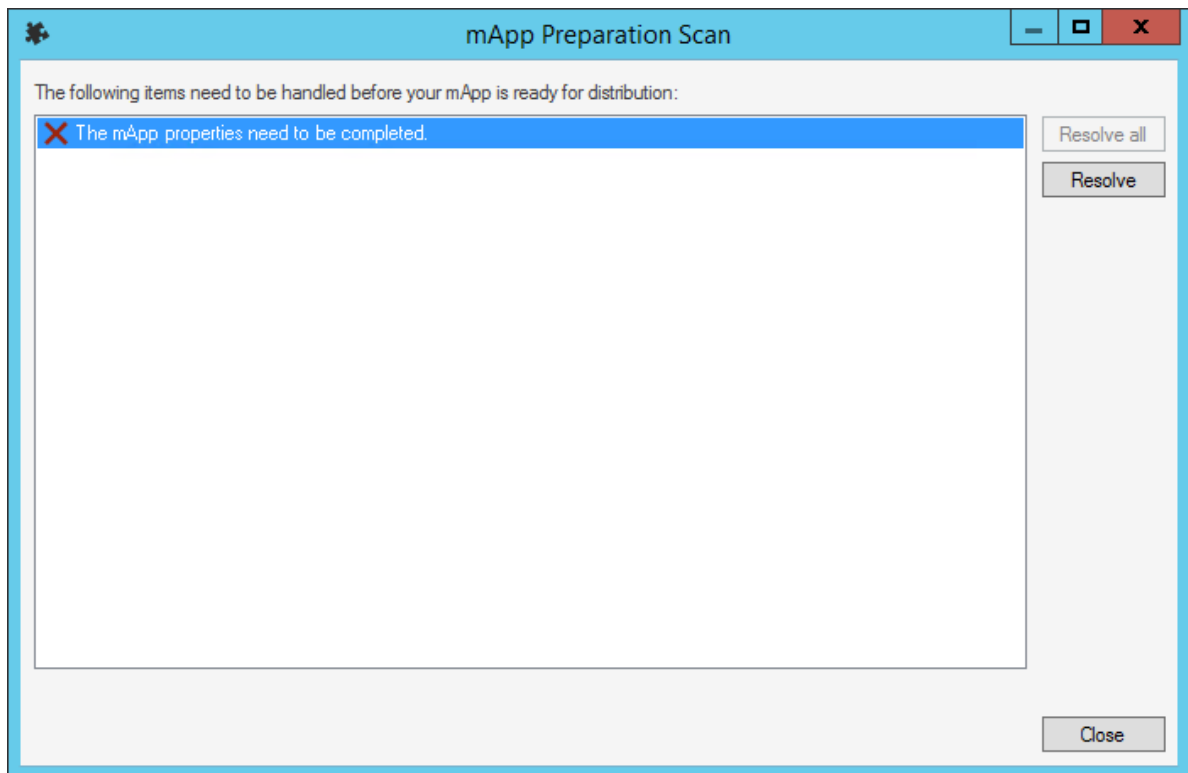
4. Resolve errors:

      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 Distribution window opens.
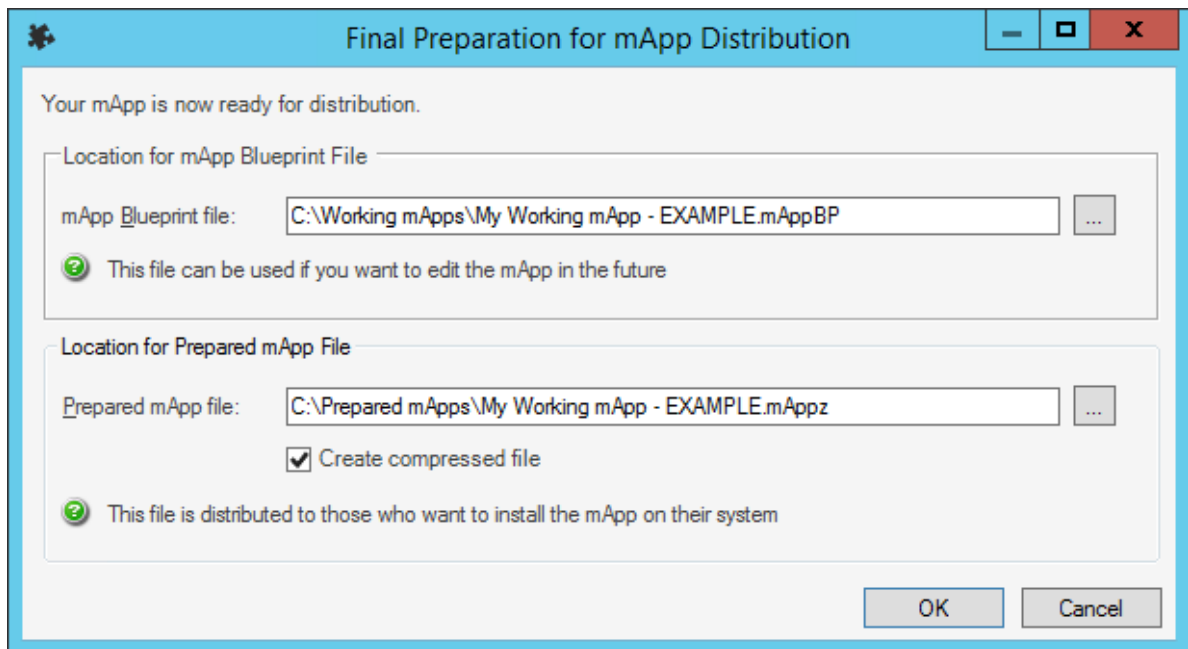
5. Prepare the mApp for distribution:
   a. Define a location for the mApp Blueprint file (.mAppBP). This allows you to save the mAppBP file so you can return to it later and make changes, if necessary. The path where the file was last saved is displayed in the field.

   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.

   b. Define a location for the prepared mApp 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 file in a compressed binary format. Compressed mApp files (designated with a .mappz extension) cannot be edited.

   c. View additional designers (only appears if the mApp includes definitions that were created or updated by other mApp creators). Each entry includes the mApp creator's personal and/or company name as well as the most recent creation date/time.

6. Click OK.

7. Distribute the mApp.

Using mApps

When working with mApps, Users can:

- View which mApps have already been installed in their CSM systems.
- Go to the mApp Exchange to view and download mApps created by others, or to submit mApps.
- Apply mApps to their CSM systems (using the Apply mApp Wizard).

View Installed mApps

Use the View Installed mApps task in the CSM Administrator main window to view a list of mApps that have been installed in your system. The page is searchable.

To view installed mApps:

1. In the CSM Administrator main window, click the mApps category, and then click the View Installed mApps task.

2. Click the name of the mApp 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 webhelp, etc.

   Downloadable files: mApp files, supporting files, documentation, etc.

Go to the mApp Exchange

Use the Go to the mApp Exchange task on the mApps page in CSM Administrator to navigate to the mApp Exchange, and to view and download mApps created by others, or submit mApps that you created. The mApp Exchange is part of the Cherwell Community, and you must be registered User to submit and download mApps.

To go to the mApp Exchange:

1. In the CSM Administrator main window, click the mApps category, and then click the Go to the mApp Exchange task.
2. Sign into the mApp Exchange to upload or download mApps.

View mApp History

Use the View mApp History task on the mApps 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.

Good to know:

- Viewing mApp history requires security rights.
- Only definitions with history records are shown. Definitions only have history records if mApp creators used Designer IDs when creating the mApps that were applied to your system.

To view mApp history in CSM Administrator:

1. In the CSM Administrator main window, click the mApps category, and then click the View mApp History task.
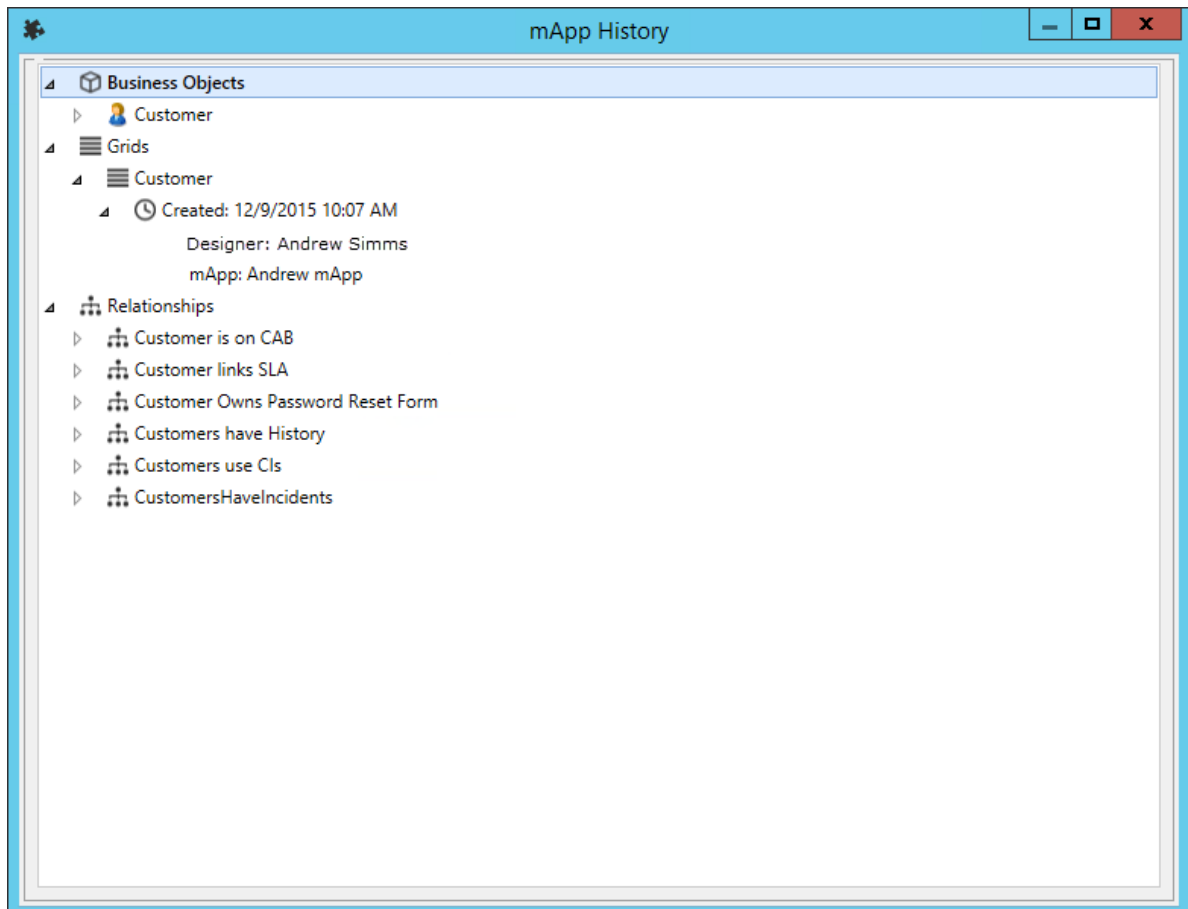
Apply a mApp

The Apply mApp Wizard (accessed from within the mApp Editor) is a specialized tool that walks you through the process of applying a mApp 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, 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 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 definition.

Good to know:

- If the mApp includes definitions that have history records, a list of additional designers is shown on the introductory page of the Apply mApp Wizard. Each entry includes the mApp 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 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 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. 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 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 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 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.
- It is recommended that you first apply a mApp against a test system before applying it to your live 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, the importance level of each object and item, and the level of User interaction you select.

To apply a mApp to a system:

1. In the CSM Administrator main window, click the mApps category, and then click the Apply a mApp task.

2. Select a mApp to apply to the target system, and then click Open.

   The Apply mApp Wizard opens, displaying the properties defined for the mApp.

   Tip: If available, click the More Information link to navigate to a website that contains detailed information about the mApp.
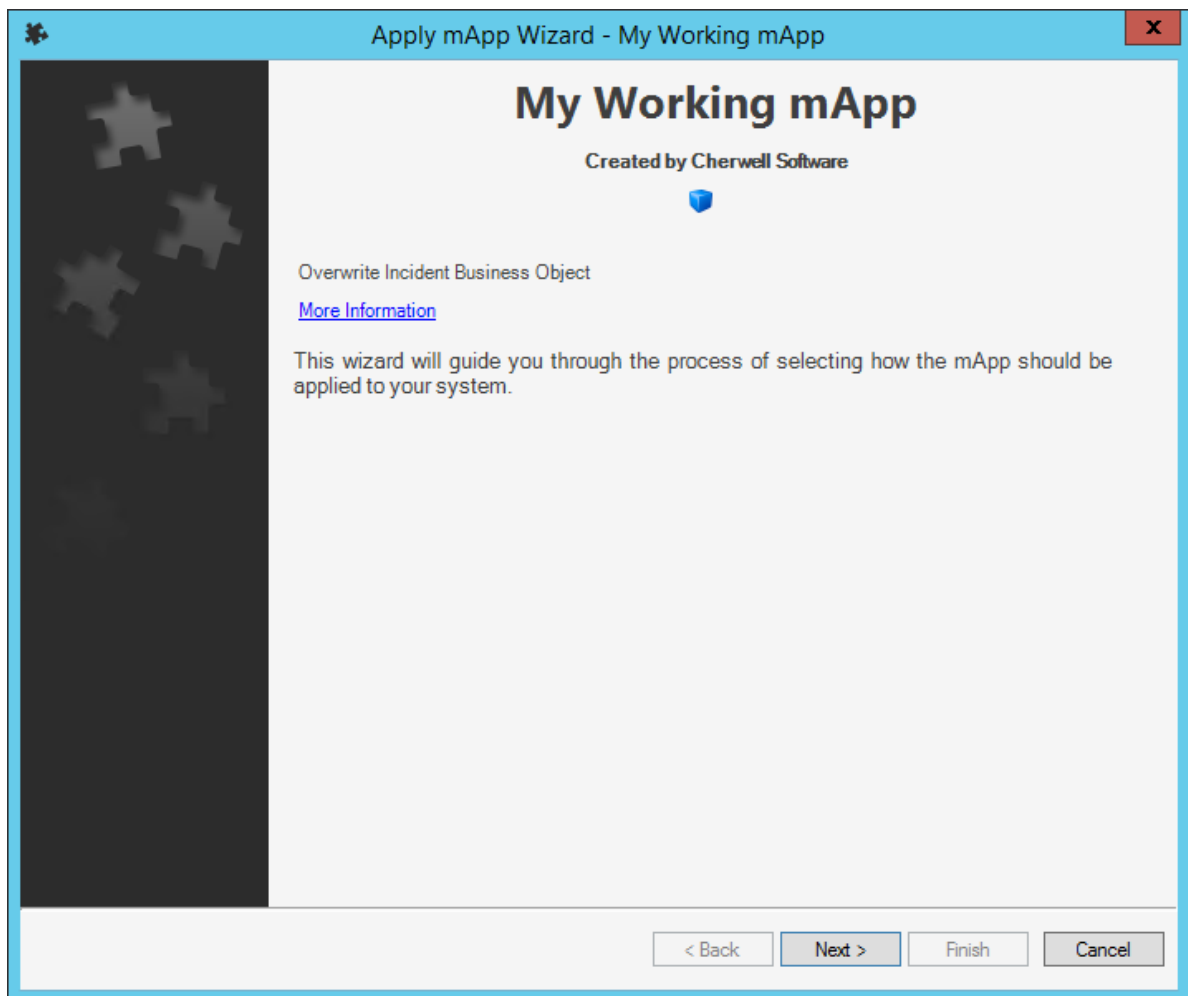
3. Click Yes to accept the terms of the license agreement, and then click Next.

4. On the Localization page:

> If you are applying a mApp created in CSM 9.2.0 or later, review the cultures for translations included in the mApp. If Globalization is enabled for your system and you have enabled the cultures listed for the mApp, translated strings are shown to Users of the cultures included in the mApp.

> If you are applying a mApp created before CSM 9.2.0, select the target culture for the mApp. You must perform this task even if Globalization is not enabled for your system.

For more information, see Applying Translations to mApps.

5. 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: Select this radio button to have the wizard ask how you want to apply every object and item that is included in the mApp.

> Make reasonable decisions, but ask me if you are unsure (default): Select this radio button to make the apply mApp 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: Select this radio button to make the apply mApp process almost fully automated (you will only be asked about areas that absolutely require your interaction). If the wizard does not need to ask you anything, you will be directed to the summary page.

6. Select the Features to apply to the target system:

> **Note:** This page only applies if the mApp includes Features. There is a page for each Feature in the mApp.

> Enabled: Select this check box to apply a mApp 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 creator included a Feature by default, this check box is automatically selected.

7. Select a merge action and target View:

> **Note:** This page only applies if the mApp contains custom Business Object Views, or Business Objects or other definitions that are contained in custom Business Object Views.

> Merge Actions: These are the merge actions the mApp creator defined for each View. To change the merge action for a View, select an option in the Merge Action column's drop-down:
> - Import/Overwrite: Imports/overwrites the View in the target system.
> - Don't Change: Leaves the View in the target system unchanged.

Target View: If the mApp contains a new View, the default option is *Treat as new*. If an exact or close match is found in the target system, it is automatically selected as the target View. To change the target View, select an option in the Target Item's column drop-down:
- Existing View: The existing Views in the target system are listed in the drop-down. Select one to overwrite it with the View in the mApp.
- (Treat as new): Select this option to create a new View (must have a unique name).

8. Select a merge action and target Business Object:

> **Note:** This page only applies if the mApp 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.

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 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 object into.
- Select from List: If objects with names similar to the mApp 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 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.

9. Select merge actions for the object's merge areas: These are the merge actions the mApp creator defined for each mergeable area in the object. To change the merge action for an area, select an option in the Merge Action column's drop-downs:
Overwrite: Overwrites the definition in the target system.

Don't Change: Leaves the definition in the target system unchanged.

10. 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 is creating a new object, or if the entire Business Object will be overwritten.

Merge Actions: These are the merge actions the mApp 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, 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 (ex: 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 item is found to have the same name as an item in the target system, the wizard will ask you to resolve naming conflicts.

11. Select options for displayable items associated with the object (Forms, Grids, Form Arrangement, etc.). These are the merge actions the mApp creator defined for each displayable 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 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 definition with the one in the target system. This means that the Tabs in the mApp 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.

12. Select a merge action and target object for removal.

> **Note:** This page only applies if the mApp 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 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.

13. Select merge actions and target items for CSM Items included in the mApp.
Merge Action: This column shows the merge actions the mApp creator defined for each item. 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, 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.

14. Select merge actions and target items for the One-Steps included in the mApp.

🖊 **Note:** This page only applies if the mApp includes One-Steps.

Merge Actions: These are the merge actions the mApp creator defined for each One-Step. To change the merge action for a One-Step, 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, 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 Manager and select a different One-Step.

15. Select merge actions and target items for miscellaneous items included in the mApp (ex: Dashboards, Stored Searches, Stored Values, external connections, etc.).
Merge Actions: These are the merge actions the mApp 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.

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, 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.

16. Provide a **value** for the Stored Value.

> **Note:** This page only applies if the mApp 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.

17. 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 includes external connections that prompt Users to specify their own external connection settings.

18. Review the Summary page.
    Save to File: Click this 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 definitions that will be applied to the target system.
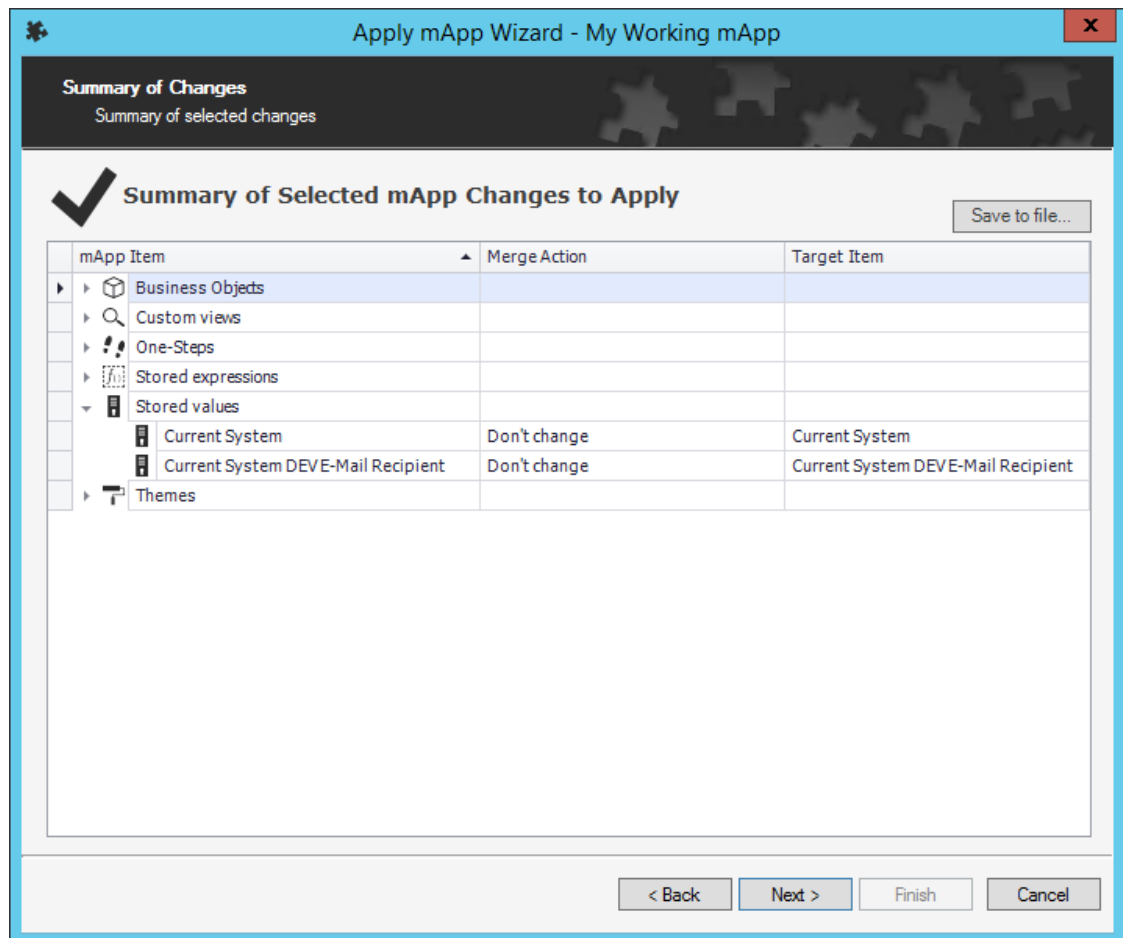
19. Define final options (what to do after the mApp is applied to the target system):
    (Recommended) Open a Blueprint so I can preview the changes: Select this radio button to open a Blueprint that allows you to see the changes the mApp will make to the target system.

    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 changes directly to the target system without previewing it first.

20. Click 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 changes.

    Immediately attempts to publish to the target system.

Tips for Creating and Using mApps

Use the following tips to help you create an effective mApp:

- 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 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.
    - When you include a Business Object in a mApp and select *Merge* as the merge action, only include the Fields that apply to the mApp (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, either add the reverse Relationship to the mApp or clear the Reverse Relationship check box (on the General page in the Relationships Properties window).

Following are some tips for applying mApps:

- Apply a mApp 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.

Configuring mApps

Complete the following procedures to configure mApps. Configuration procedures are completed in CSM Administrator.

To configure mApps:

1. Configure mApp security rights: Configure who can access mApp 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 (ex: Business Object Properties window, Relationship Properties window, etc.). The properties windows have more detailed mApp options available outside of the Add Business Object to mApp Wizard.

3. View referenced definitions in a mApp: From the various properties windows, view all of the system definitions throughout CSM being used by a selected mApp 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.

4. Configure mApp conditions: Configure conditions that control when definitions are imported into a target system when a mApp is applied.

5. Prepare mApp for distribution: Creates a mApp 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 are merged into a target system when a mApp is applied. Use the Add Business Object to mApp 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 using the wizard are imported into a target system when the mApp 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 (ex: 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 (ex: All Fields) in the target system unchanged (does not overwrite or add the definitions).
- Overwrite some (the *Let me choose* option in the wizard): Overwrites the selected definitions of a particular type (ex: Only the Fields you select).

However, you have some additional options available when you configure merge actions using the various properties windows (ex: 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 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 and you only want to import/overwrite certain areas. *Merge* is available for the following definitions:

- Business Objects
- Fields
- Relationships
- Form Arrangements
- Business Object Actions

To configure merge actions for Business Object definitions:

1. Add a Business Object to a mApp 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 for Distribution (File>Prepare mApp for distribution), or save the mApp (File>Save mApp to Disk) to continue making other changes.

Configure Merge Actions for Business Objects

Use the Business Object Properties window to configure the following:

- General properties: Whether to include the Business Object in the mApp, and its importance in the mApp.
- Options for merging the Business Object into the target system when the mApp 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 for informational purposes only (it is not merged into the target system when the mApp is applied).
  - Import/remove based on condition: Imports or removes the Business Object definition based on configured mApp 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* 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 using the Business Object Properties window, its associated Relationships are not automatically added. Be sure to add all necessary Relationships. Click the **References** button (on the mApps 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 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:
   a. In the Object Manager within the mApp Editor, click the Business Object in the Object tree, and then click the Edit Business Object task in the Structure area.

   The Business Object Editor opens.

   Tip: You can also click the Business Object button [image] on the mApp Editor toolbar to open the Business Object Editor.

   b. Click the Bus Ob Properties button.

3. Click the mApps page.

4. Configure mApp properties and merge actions for the Business Object:
   a. Define general mApp properties for the Business Object:

   Include in mApp: Select this check box to include the Business Object in the mApp. 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 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.

   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 radio button if the selected Business Object is one of the main Business Objects in the mApp.

- Medium Importance: Select this radio button if the selected Business Object is a supporting object for the mApp.

- Low Importance: Select this radio button if the selected Business Object is not critical for the mApp.

References: Click 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 radio 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, 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 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 definition is not imported into the target system when the mApp 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, 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 definition into the target system if does not already exist.

- Don't Import: Select this option to skip importing the mApp definition into the target system if it does not already exist (the mApp definition will not be added to the target system).

Remove from Target System: Select this radio button to remove the definition from a target system.

For Reference Only: Select this radio button to include the definition in the mApp for informational purposes only (the definition is not imported into the target system when the mApp is applied).

Import/Remove Based on Condition: Select this check box to import or remove the definition based on a condition. Then, click the Ellipses button [...] to open the mApp Conditions window and define mApp conditions.

5. Configure separate merge actions for individual Business Object Property merge areas:
   a. In the Options area of the Business Object Properties window, click 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).
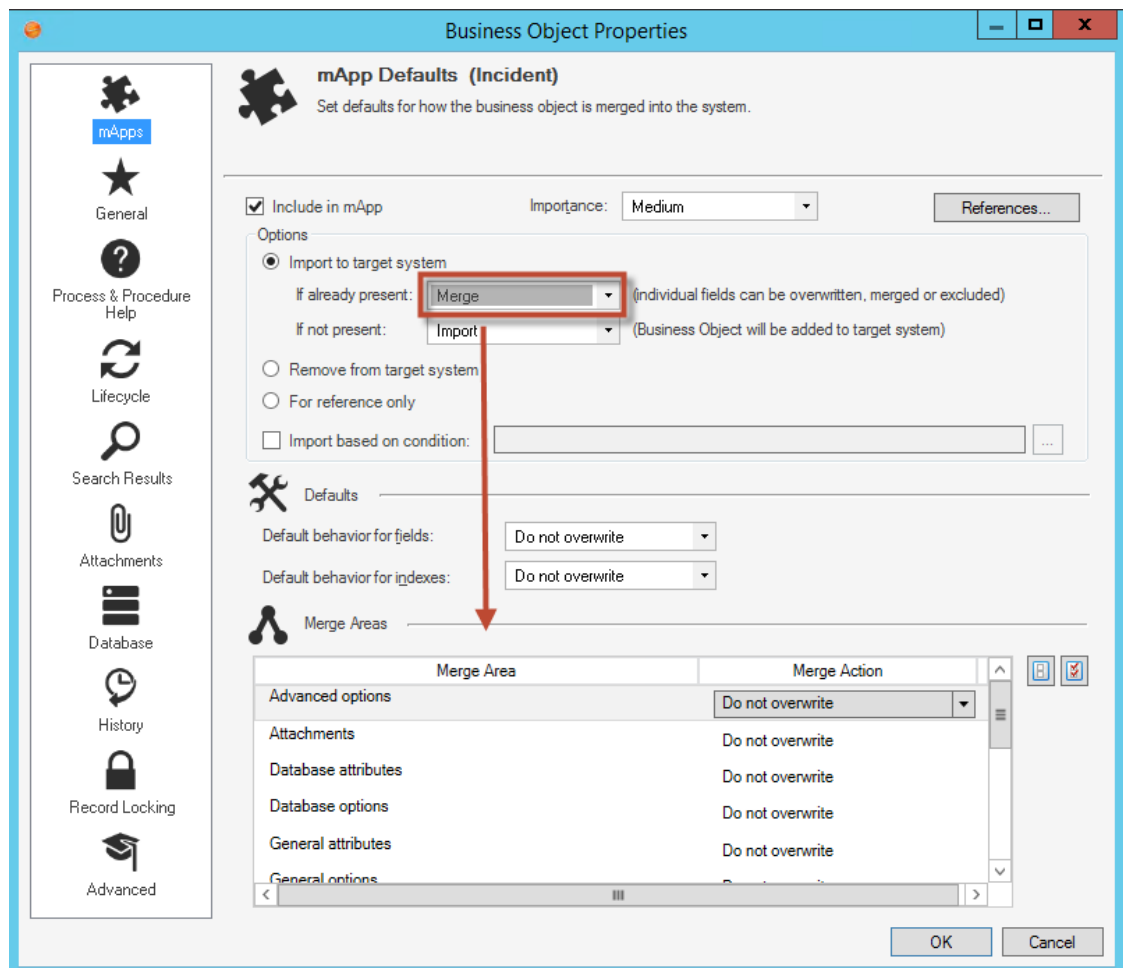
c. Define default behaviors for the Business Object's Fields and indexes. This is how Fields and indexes will be merged unless specified otherwise. In the drop-downs, select one of the following options:

Overwrite: Select this option to have the Business Object Fields and/or indexes overwritten in the target system when the mApp is applied. You can then go to particular Fields or indexes and exclude the ones you do not want in the mApp.

Do Not Overwrite (Default): Select this option to leave the Business Object Fields and/or indexes unchanged in the target system when the mApp is applied. You can then go to particular Fields or indexes and explicitly select which ones to include in the mApp.

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 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-downs:

Overwrite: Select this option to have the merge area overwritten in the target system when the mApp is applied.

Do Not Overwrite: Select this option to leave the merge area unchanged in the target system when the mApp is applied.

Tip: Click the Uncheck All button [image] to set all merge areas to *Do Not Overwrite*. Click the Select All button [image] to set all merge areas to *Overwrite*.

On the remaining pages of the properties window: Click the mApp button [image] 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 advanced properties.

e. Click 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:
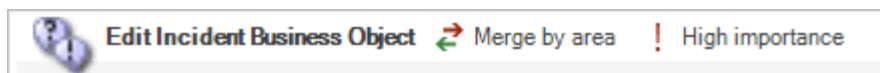
[image]. These indicators are also displayed in the Task Section of the Object Manager.

The mApp 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).

6. Prepare the mApp for Distribution (File>Prepare mApp for distribution), or save the mApp (File>Save mApp to Disk) to continue making other changes.

Define Merge Actions for General Business Object Properties

Use the General page in the Business Object Properties window to define whether or not to overwrite 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 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* check box is cleared, then you cannot configure separate merge actions for individual properties or areas.
- 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 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:
   a. In the Object Manager within the mApp Editor, click the Edit Business Object task in the Structure area.

      The Business Object Editor opens.

      Tip: You can also click the Business Object button ⬡ on the mApp Editor toolbar to open the Business Object Editor.

   b. Click the Bus Ob Properties button.
3. Set the Business Object to *Merge*:
   a. Click the mApps page, and then select the Include in mApp check box.
   b. In the Options area, select the Import to Target System radio button.
   c. In the *If Already Present* drop-down, select Merge as the merge action for the Business Object.
4. Click the General page.

5. Click the mApp button ![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 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 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 is applied.

Overwrite General Options: Select this option to overwrite the Business Object's general options in the target system when the mApp is applied.

6. Click OK.

7. Prepare the mApp for Distribution (File>Prepare mApp for distribution), or save the mApp (File>Save mApp to Disk) to continue making other changes.

Define 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 whether or not to overwrite process and procedure help 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 (mApps 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 (after saving) and go to **Settings>Edit System Settings**. Click 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.

- 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.

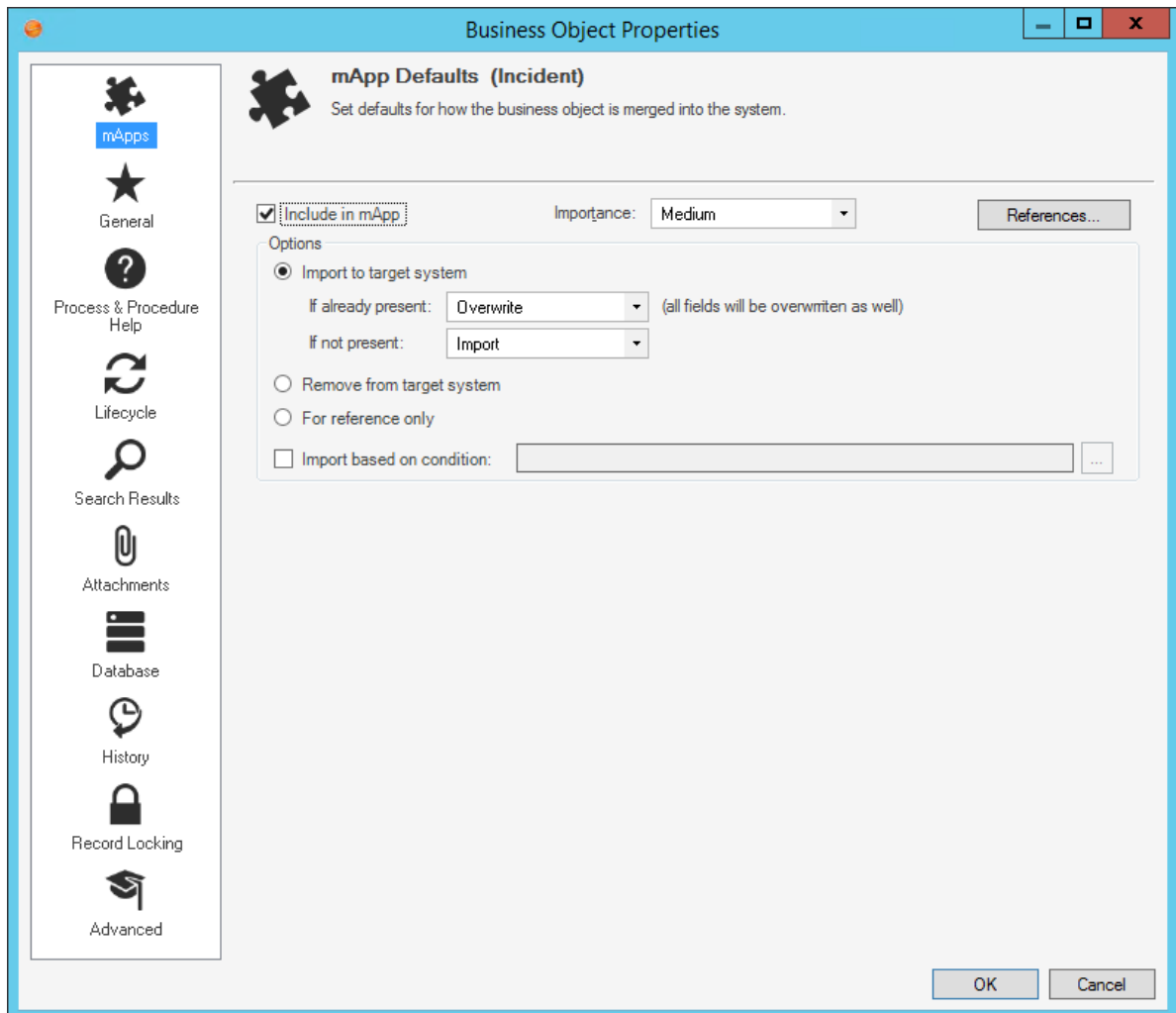To define merge actions for Business Object process and procedure help properties:

1. Add a Business Object to a mApp using the Add Business Object to mApp Wizard.

2. Open the Business Object Properties window for the Business Object you just added to the mApp:
   a. In the Object Manager within the mApp Editor, click the Edit Business Object task in the Structure area.

      The Business Object Editor opens.

      Tip: You can also click the Business Object button ⬡ on the mApp Editor toolbar to open the Business Object Editor.

   b. Click the Bus Ob Properties button.

3. Set the Business Object to *Merge*:
   a. Click the mApps page, and then select the Include in mApp check box.

   b. In the Options area, select the Import to Target System radio button.

      In the *If Already Present* drop-down, select Merge as the merge action for the Business Object.

4. Click the Process and Procedure Help page.
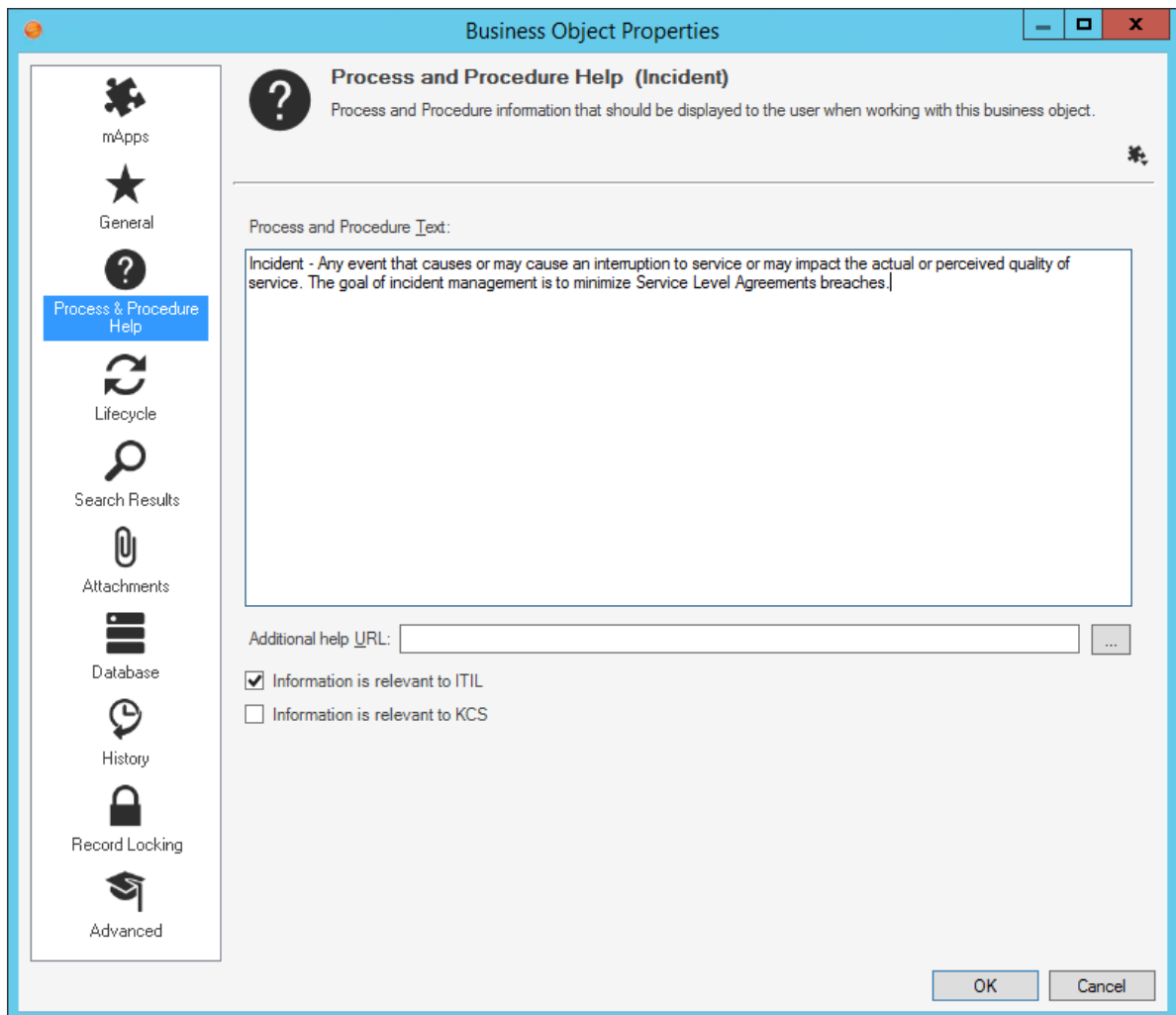
5. Click the mApp button ![mApp icon], and then select a **merge action**:

   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 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 is applied.

6. Click OK.

7. Prepare the mApp for Distribution (File>Prepare mApp for distribution), or save the mApp (File>Save mApp to Disk) to continue making other changes.

Define Merge Actions for Business Object Lifecycle Properties

Use the Lifecycle page in the Business Object Properties window to define whether or not to overwrite 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 (mApps 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 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:
    a. In the Object Manager within the mApp Editor, click the Edit Business Object task in the Structure area.

        The Business Object Editor opens.

        Tip: You can also click the Business Object button [icon] on the mApp Editor toolbar to open the Business Object Editor.

    b. Click the Bus Ob Properties button.

3. Set the Business Object to *Merge*:
    a. Click the mApps page, and then select the Include in mApp check box.

    b. In the Options area, select the Import to Target System radio button.

    c. In the *If Already Present* drop-down, select Merge as the merge action for the Business Object.

4. Click the Lifecycle page.
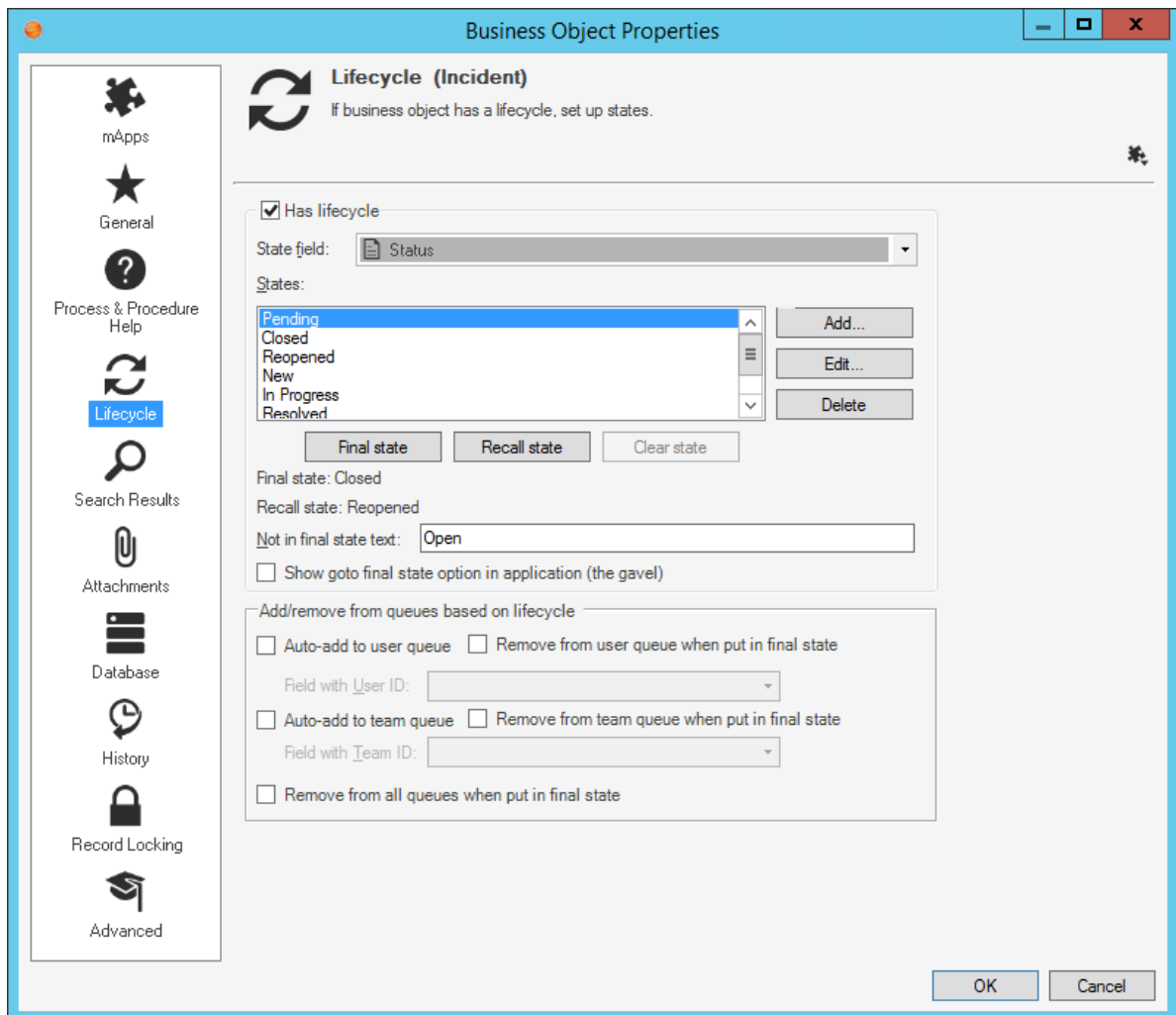
5. Click the mApp button [icon], and then select a **merge action**:

Do Not Overwrite Lifecycle Options: Select this option to leave the Business Object's lifecycle properties unchanged in the target system when the mApp is applied.

Overwrite Lifecycle Options: Select this option to overwrite the Business Object's lifecycle properties in the target system when the mApp is applied.

6. Click OK.

7. Prepare the mApp for Distribution (File>Prepare mApp for distribution), or save the mApp (File>Save mApp to Disk) to continue making other changes.

Define Merge Actions for Business Object Search Results Properties

Use the Search Results page in the Business Object Properties window to define whether or not to overwrite Search Result options 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 (mApps 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 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 Wizard.

2. Open the Business Object Properties window for the Business Object you just added to the mApp:
    a. In the Object Manager within the mApp Editor, click the Edit Business Object task in the Structure area.

       The Business Object Editor opens.

       Tip: You can also click the Business Object button [icon] on the mApp Editor toolbar to open the Business Object Editor.

    b. Click the Bus Ob Properties button.

3. Set the Business Object to *Merge*:
    a. Click the mApps page, and then select the Include in mApp check box.

    b. In the Options area, select the Import to Target System radio button.

    c. In the *If Already Present* drop-down, select Merge as the merge action for the Business Object.

4. Click the Search Results page.

CSM Administration
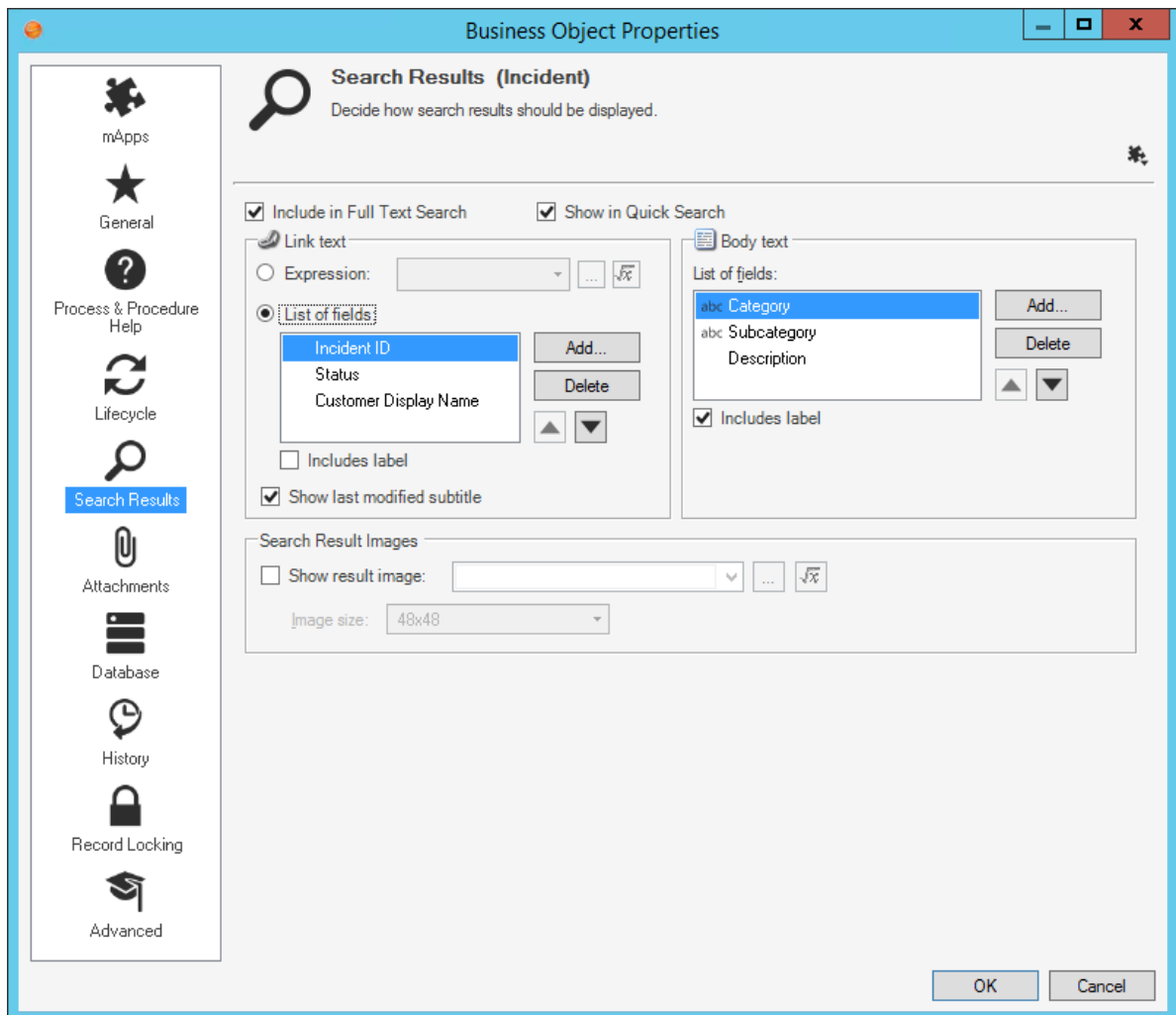
5. Click the mApp button , and then select a **merge action**:

> 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 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 is applied.

6. Click OK.

7. Prepare the mApp for Distribution (File>Prepare mApp for distribution), or save the mApp (File>Save mApp to Disk) to continue making other changes.

Define Merge Actions for Business Object Attachment Properties

Use the Attachments page in the Business Object Properties window to define whether or not to overwrite Attachment options 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 (mApps 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 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:
    a. In the Object Manager within the mApp Editor, click the Edit Business Object task in the Structure area.

    The Business Object Editor opens.

    Tip: You can also click the Business Object button ⬡ on the mApp Editor toolbar to open the Business Object Editor.

    b. Click the Bus Ob Properties button.
3. Set the Business Object to *Merge*:
    a. Click the mApps page, and then select the Include in mApp check box.
    b. In the Options area, select the Import to Target System radio button.
    c. In the *If Already Present* drop-down, select Merge as the merge action for the Business Object.
4. Click the Attachments page.
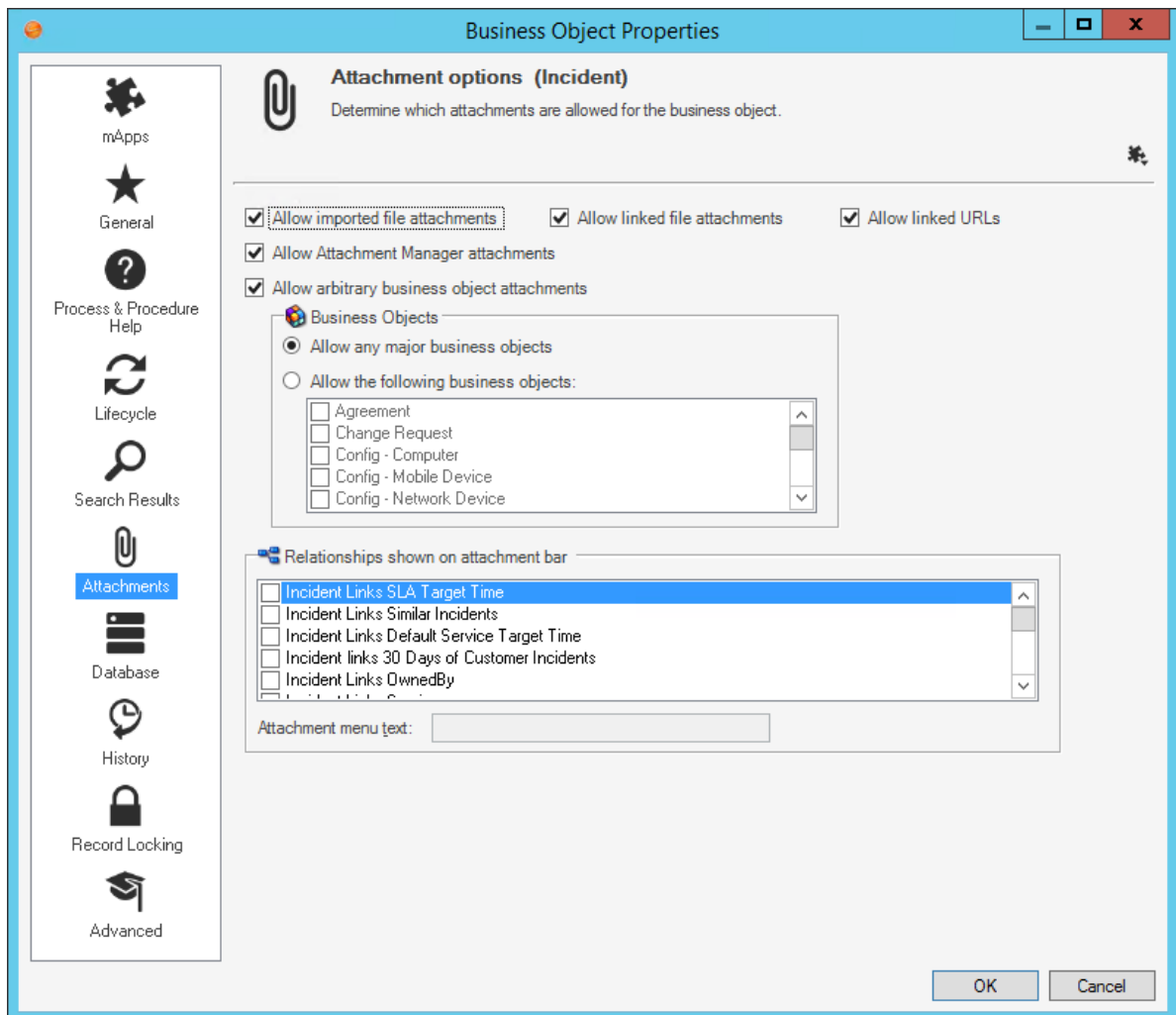
5. Click the mApp button ![icon], and then select a **merge action**:

    Do Not Overwrite Attachment Options: Select this option to leave the Business Object's Attachment options unchanged in the target system when the mApp is applied.

    Overwrite Attachment Options: Select this option to overwrite the Business Object's Attachment options in the target system when the mApp is applied.

6. Click OK.

7. Prepare the mApp for Distribution (File>Prepare mApp for distribution), or save the mApp (File>Save mApp to Disk) to continue making other changes.

Define Merge Actions for Business Object Database Properties

Use the Database page in the Business Object Properties window to define whether or not to overwrite database options 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 (mApps 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 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 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:
   a. In the Object Manager within the mApp Editor, click the Edit Business Object task in the Structure area.

      The Business Object Editor opens.

      Tip: You can also click the Business Object button on the mApp Editor toolbar to open the Business Object Editor.

   b. Click the Bus Ob Properties button.

3. Set the Business Object to *Merge*:
   a. Click the mApps page, and then select the Include in mApp check box.

   b. In the Options area, select the Import to Target System radio button.

   c. In the *If Already Present* drop-down, select Merge as the merge action for the Business Object.

4. Click the Database page.
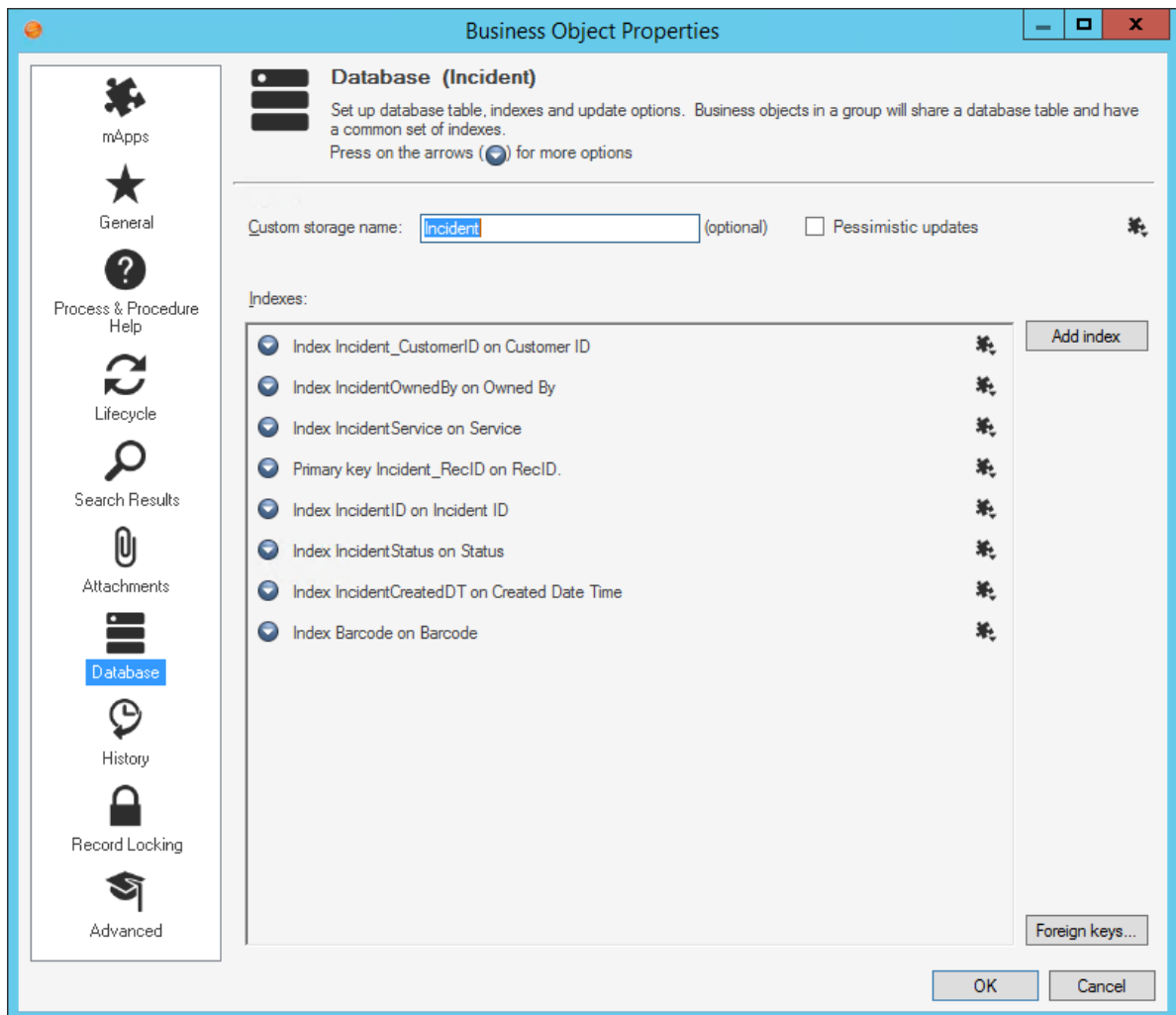
5. Click the mApp button [icon] next to each property merge area, and then select a **merge action**:

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 is applied.

> Overwrite Database Options: Select this option to overwrite the Business Object's database options in the target system when the mApp is applied.

For an index:

> Do Not Overwrite Index: Select this option to leave an index unchanged in the target system when the mApp is applied.

> Overwrite Index: Select this option to overwrite an index in the target system when the mApp is applied.

6. Click OK.

7. Prepare the mApp for Distribution (File>Prepare mApp for distribution), or save the mApp (File>Save mApp to Disk) to continue making other changes.

Define Merge Actions for Business Object History Properties

Use the History page in the Business Object Properties window to define whether or not to overwrite the history tracking options 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 (mApps 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 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 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:
   a. In the Object Manager within the mApp Editor, click the Edit Business Object task in the Structure area.

      The Business Object Editor opens.

      Tip: You can also click the Business Object button [icon] on the mApp Editor toolbar to open the Business Object Editor.

   b. Click the Bus Ob Properties button.

3. Set the Business Object to *Merge*:
   a. Click the mApps page, and then select the Include in mApp check box.

   b. In the Options area, select the Import to Target System radio button.

   c. In the *If Already Present* drop-down, select Merge as the merge action for the Business Object.

4. Click the History page.
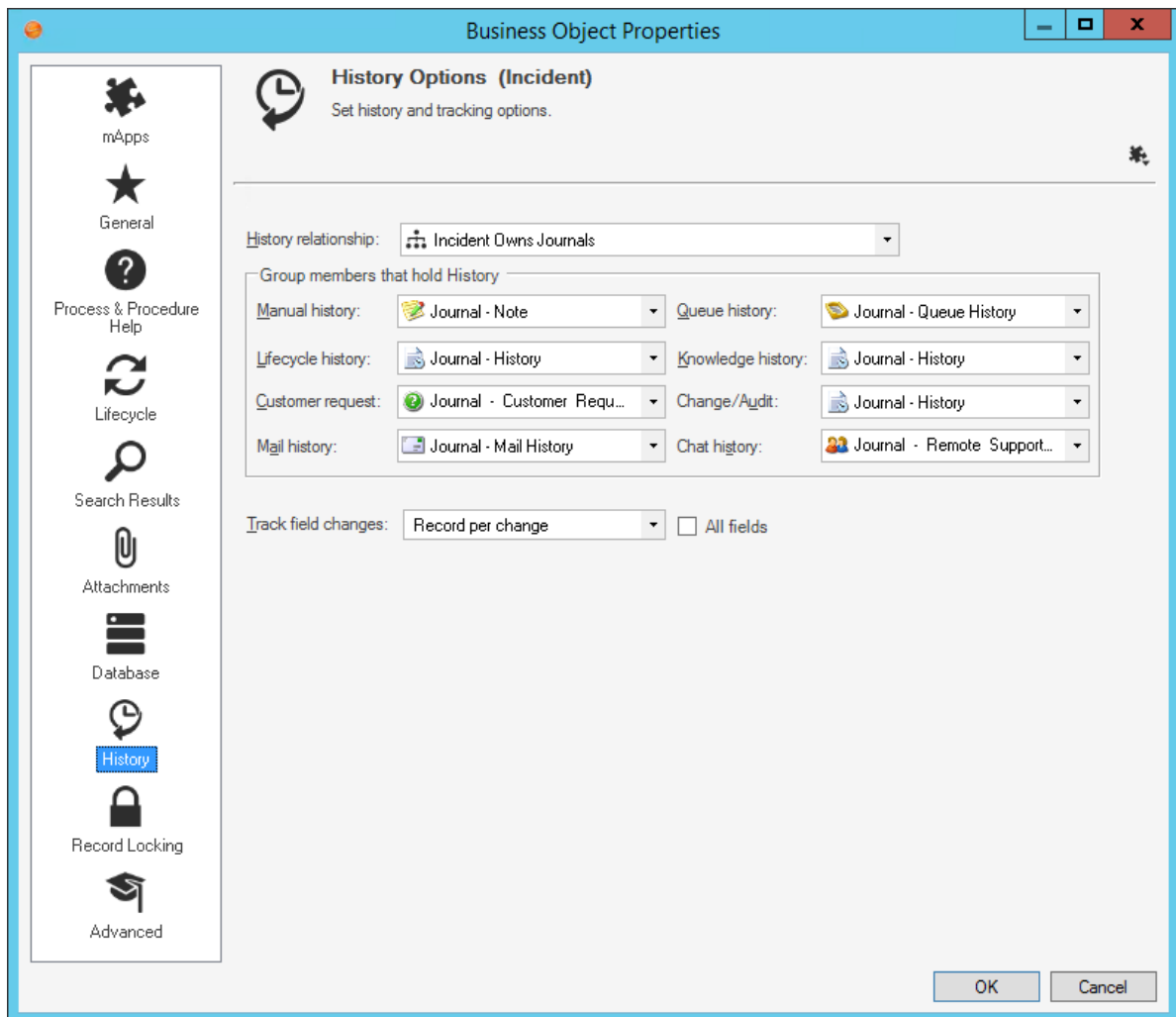
5. Click the mApp button [icon], and then select a **merge action**:

Do Not Overwrite History Options: Select this option to leave the Business Object's history properties unchanged in the target system when the mApp is applied.

Overwrite History Options: Select this option to overwrite the Business Object's history properties in the target system when the mApp is applied.

6. Click OK.

7. Prepare the mApp for Distribution (File>Prepare mApp for distribution), or save the mApp (File>Save mApp to Disk) to continue making other changes.

Define Merge Actions for Business Object Record Locking Settings

Use the Record Locking page in the Business Object Properties window to define whether or not to overwrite 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 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* 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 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:
    a. In the Object Manager within the mApp Editor, click the Edit Business Object task in the Structure area.

       The Business Object Editor opens.

       Tip: You can also click the Business Object button ⬡ on the mApp Editor toolbar to open the Business Object Editor.

    b. Click the Bus Ob Properties button.

3. Set the Business Object to *Merge*:
    a. Click the mApps page, and then select the Include in mApp check box.

    b. In the Options area, select the Import to Target System radio button.

    c. In the *If Already Present* drop-down, select Merge as the merge action for the Business Object.

4. Click the Record Locking page.
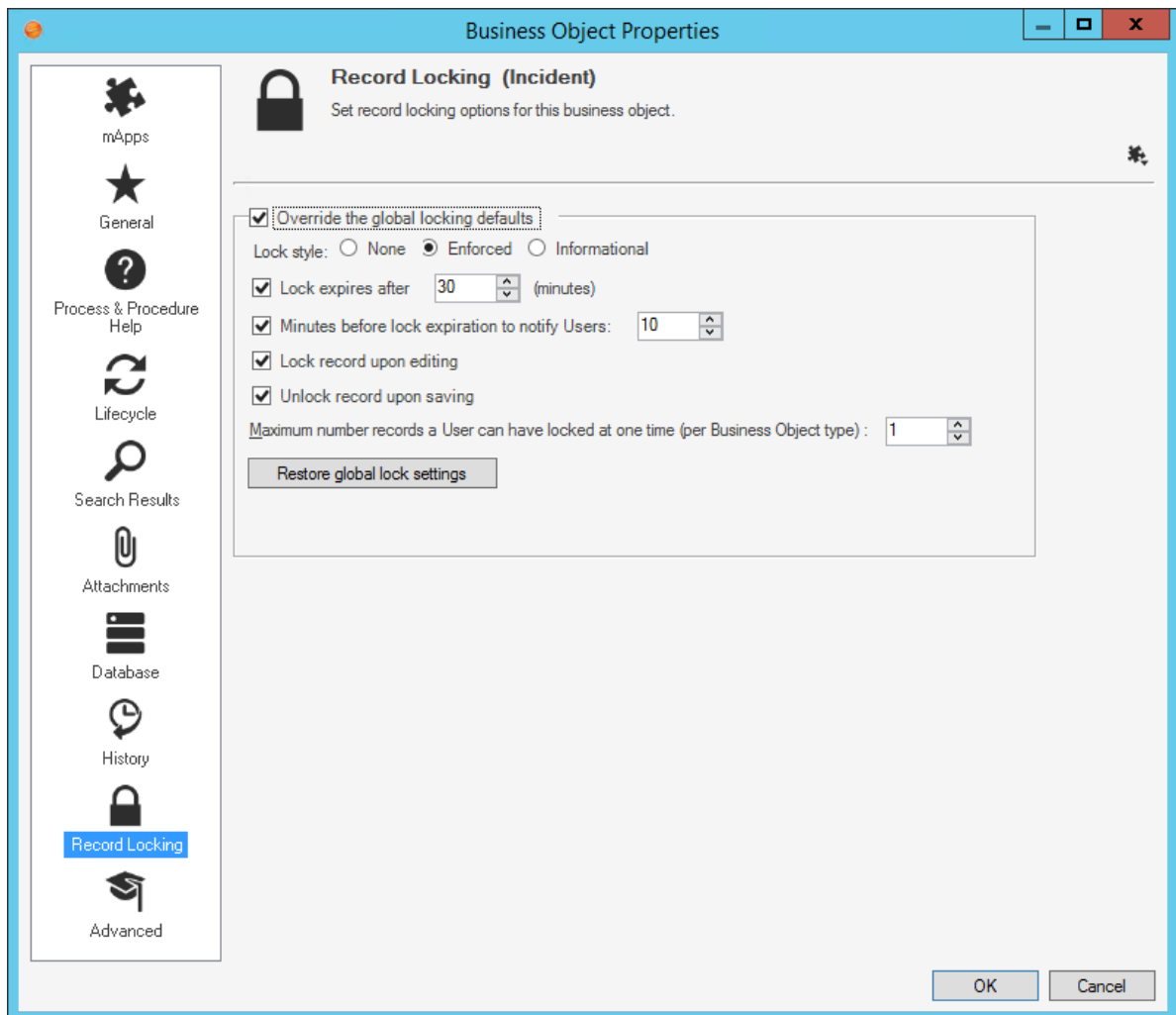
5. Click the mApp button ![icon], and then select a **merge action**:

> 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 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 is applied.

6. Click OK.

7. Prepare the mApp for Distribution (File>Prepare mApp for distribution), or save the mApp (File>Save mApp to Disk) to continue making other changes.

Define Merge Actions for Advanced Business Object Properties

Use the Advanced page in the Business Object Properties window (accessed from within the mApp Editor) to define whether or not to overwrite 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 (mApps 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.
- 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 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:
   a. In the Object Manager within the mApp Editor, click the Edit Business Object task in the Structure area.

      The Business Object Editor opens.

      Tip: You can also click the Business Object button [image] on the mApp Editor toolbar to open the Business Object Editor.

   b. Click the Bus Ob Properties button.
3. Set the Business Object to *Merge*:
   a. Click the mApps page, and then select the Include in mApp check box.
   b. In the Options area, select the Import to Target System radio button.
   c. In the *If Already Present* drop-down, select Merge as the merge action for the Business Object.

4. Click the Advanced page.

5. Click the mApp button ![mApp button] 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 is applied.

Overwrite advanced options: Select this option to overwrite the advanced options in the target system when the mApp 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 is applied.

Overwrite general attributes: Select this option to overwrite the general attributes in the target system when the mApp 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 is applied.

Overwrite database attributes: Select this option to overwrite the database attributes in the target system when the mApp is applied.

6. Click OK.

7. Prepare the mApp for Distribution (File>Prepare mApp for distribution), or save the mApp (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 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 (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 Field properties.

To configure merge actions for individual Business Object Fields:

1. Add a Business Object to a mApp 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 Business Object task in the Structure area.

   Tip: You can also click the Business Object button ⬚ 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) are also reflected in the mApp Action column.

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 definition is not imported into the target system when the mApp 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 will not be imported when the mApp is applied.

    Overwrite Field: Select this option to have the mApp 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 for informational purposes only (the definition is not imported into the target system when the mApp 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 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 click the Field Properties button.

  b. Click the mApps page.
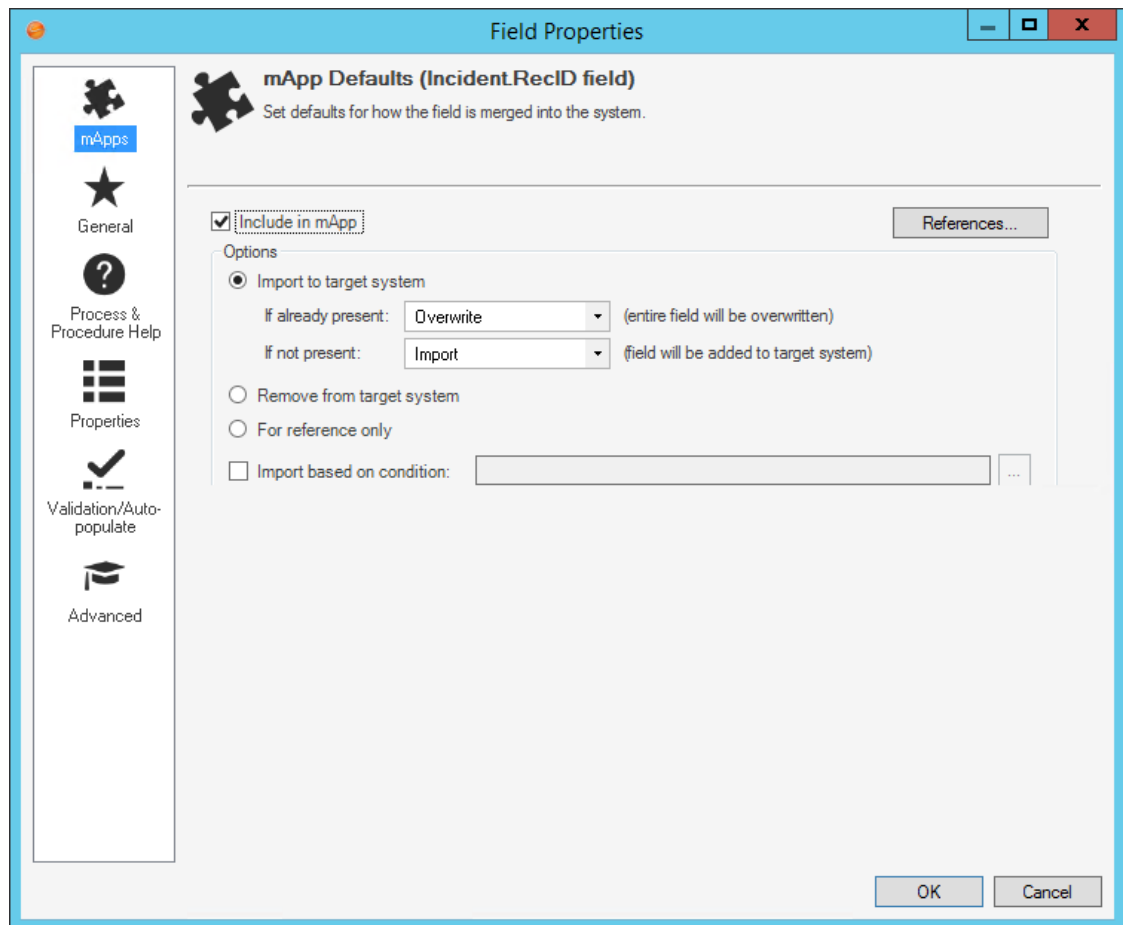
c. Define general mApp properties for the Field:

> Include in mApp: Select this check box to include the Field in the mApp. 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 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 (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: Click 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 radio 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, 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 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 definition is not imported into the target system when the mApp 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, 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 definition into the target system if does not already exist.
- Don't Import: Select this option to skip importing the mApp definition into the target system if it does not already exist (the mApp definition will not be added to the target system).

Remove from Target System: Select this radio button to remove the definition from a target system.

For Reference Only: Select this radio button to include the definition in the mApp for informational purposes only (the definition is not imported into the target system when the mApp is applied).

Import/Remove Based on Condition: Select this check box to import or remove the definition based on a condition. Then, click the Ellipses button to open the mApp Conditions window and define mApp 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, click the Import to Target System radio button.
   b. Select Merge as the merge action for the Field (from the *If Already Present* drop-down).

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-downs:

Overwrite: Select this option to have the merge area overwritten in the target system when the mApp is applied.

Do Not Overwrite: Select this option to leave the merge area unchanged in the target system when the mApp is applied.

Tip: Click the Uncheck All button to set all merge areas to *Do Not Overwrite*. Click the Select All button to set all merge areas to *Overwrite*.

On the remaining pages of the properties window: Click the mApp button 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. Click OK.

The selections you made in the Options area are reflected in the Business Object Editor Grid.

6. Prepare the mApp for Distribution (File>Prepare mApp for distribution), or save the mApp (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 (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 Field properties.
- For more information about defining general Field properties, refer to Define General Properties for a Field.

To define merge actions for general Field properties:

1. Add a Business Object to a mApp 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:
   a. In the Object Manager within the mApp Editor, click 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 menu) are also reflected in the mApp Action column.

      Tip: You can also click the Edit Business Object button ⬡ on the mApp Editor toolbar to open the Business Object Editor.

   b. Click a **Field**, and then click the Field Properties button.
3. Set the individual Field to *Merge*:
   a. Click the mApps page, and then check **Include in mApp**.
   b. In the Options area, click Import to Target System.
   c. From the *If Already Present* drop-down menu, select Merge as the merge action for the Field.
4. Click the General page.

5. Click the mApp button [icon] next to each property merge area to open a drop-down 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 is applied.

   Overwrite Name and Description: Select this option to overwrite the Field's name and description in the target system when the mApp 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 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 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 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 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 (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 (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 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 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 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, etc.).

- Overwrite Spell-Check Setting: Select this option to overwrite the spell-check setting in the target system when the mApp 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 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 is applied. The hold property identifies the type of data contained in the Field (ex: 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 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. 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 (the number of characters specified for the Field). When the mApp is applied, the target Field size will be overwritten with the Field length defined in the mApp (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 is applied, the target Field size will be overwritten with the Field length defined in the mApp (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): 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 is applied, the target Field size will be overwritten with the Field size defined in the mApp (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 is applied, the target Field size will be 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 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 is applied, the form image display setting for the target Field will be overwritten with the setting selected in the mApp (from the *Form Images Are Displayed As* drop-down).

    - 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 is applied, the zoomed image display setting for the target Field will be overwritten with the setting selected in the mApp (from the *Zoomed Images Are Displayed As* drop-down).

    - Overwrite image format: Select this option to overwrite the default for how embedded images are displayed in the Field. When the mApp is applied, the image

format for the target Field will be overwritten with the format selected in the mApp (from the *Image Format* drop-down).

- 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 is applied, the maximum size setting for the target Field will be overwritten with the format selected in the mApp (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 is applied, the maximum size setting for the target Field will be overwritten with the format selected in the mApp (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 is applied, the setting for the target Field will be overwritten with the selection in the mApp (whether *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 is applied, the custom default font for the target Field will be overwritten with the custom default font defined for the Field in the mApp.

8. Click OK.

9. Prepare the mApp for Distribution (File>Prepare mApp for distribution), or save the mApp (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 (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 Field properties.
- If you do not see the Process and Procedure Help page, close the mApp (after saving) and go to **Settings>Edit System Settings**. Click 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.

To define merge actions for Field process and procedure help properties:

1. Add a Business Object to a mApp 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:
   a. In the Object Manager within the mApp Editor, click 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 menu) are also reflected in the mApp Action column.

      Tip: You can also click the Edit Business Object button 🔲 on the mApp Editor toolbar to open the Business Object Editor.

   b. Click a **Field**, and then click the Field Properties button.
3. Set the individual Field to *Merge*:
   a. Click the mApps page, and then check **Include in mApp**.
   b. In the Options area, click Import to Target System.
   c. From the *If Already Present* drop-down menu, select Merge as the merge action for the Field.

4. Click the Process and Procedure Help page.

5. Click the mApp button ![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 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 is applied.

6. Click OK.

7. Prepare the mApp for Distribution (File>Prepare mApp for distribution), or save the mApp (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).

> **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 (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 Field properties.
- For more information about behavior properties, refer to Define Behavior Properties for a Field.

To define merge actions for Field behavior properties:

1. Add a Business Object to a mApp 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:
   a. In the Object Manager within the mApp Editor, click 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 menu) are also reflected in the mApp Action column.

      Tip: You can also click the Edit Business Object button [box icon] on the mApp Editor toolbar to open the Business Object Editor.

   b. Click a **Field**, and then click the Field Properties button.
3. Set the individual Field to *Merge*:
   a. Click the mApps page, and then check **Include in mApp**.
   b. In the Options area, click Import to Target System.
   c. From the *If Already Present* drop-down menu, select Merge as the merge action for the Field.

4. Click the Properties page.

5. Click the mApp button ![mApp button] next to each property merge area, and then select a **merge action**:

   Do Not Overwrite Rule: Select this option to leave the specific property unchanged in the target system when the mApp is applied.

   Overwrite Rule: Select this option to overwrite the specific property in the target system when the mApp is applied.

6. Click OK.

7. Prepare the mApp for Distribution (File>Prepare mApp for distribution), or save the mApp (File>Save mApp to Disk) to continue making other changes.

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 (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 Field properties.
- For more information about validation/auto-population properties, refer to Define Validation/Auto-Population Properties for a Field.

To define merge actions for Field validation/auto-population properties:

1. Add a Business Object to a mApp 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:
   a. In the Object Manager within the mApp Editor, click 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 menu) are also reflected in the mApp Action column.

      Tip: You can also click the Edit Business Object button [icon] on the mApp Editor toolbar to open the Business Object Editor.

   b. Click a **Field**, and then click the Field Properties button.

3. Set the individual Field to *Merge*:
   a. Click the mApps page, and then check **Include in mApp**.

   b. In the Options area, click Import to Target System.

4. From the *If Already Present* drop-down menu, select Merge as the merge action for the Field.

5. Click the Validation/Auto-Populate page.
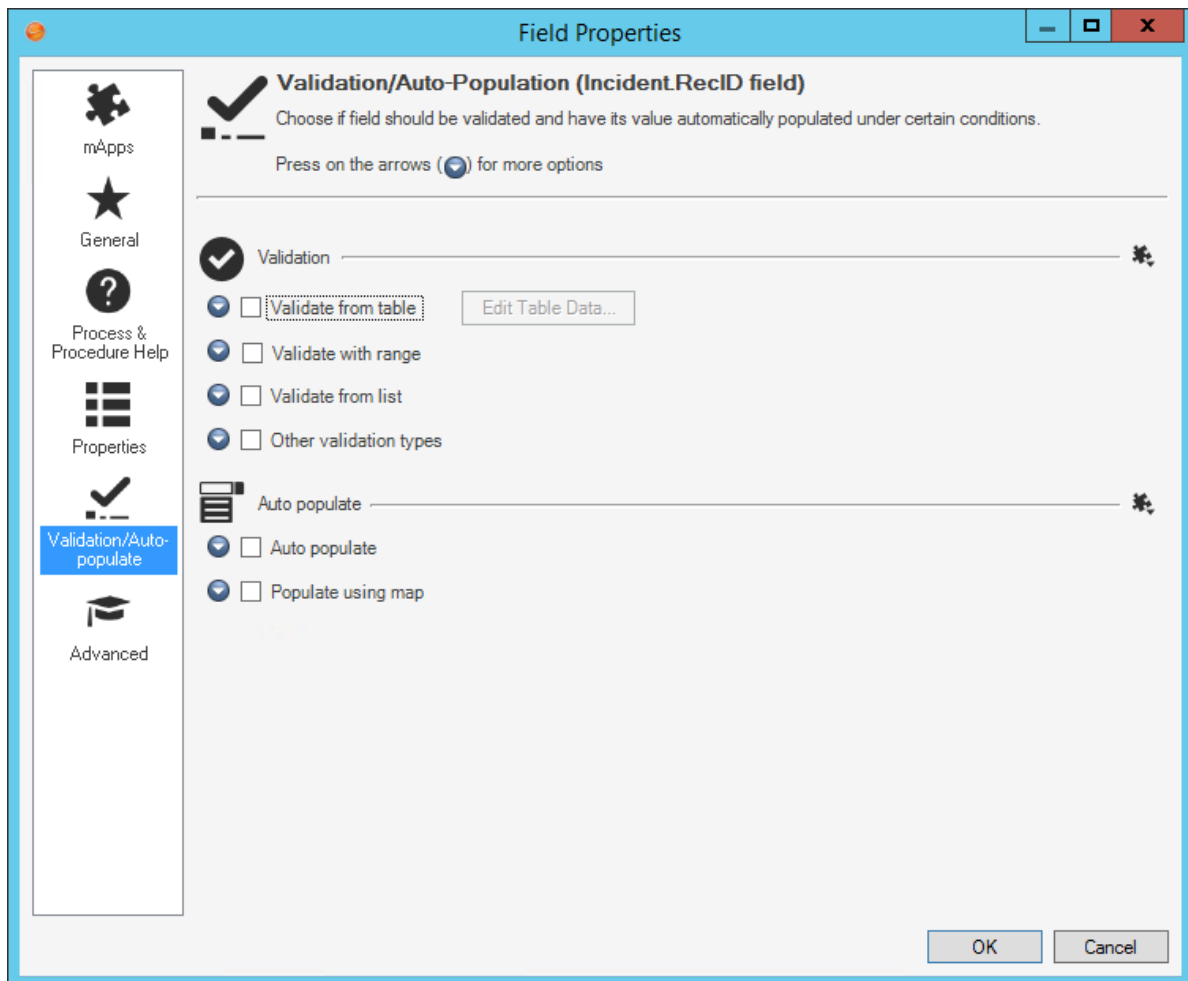
6. Click the mApp button ![mApp] next to each property merge area, and then select a **merge action**:

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 is applied.

Overwrite the Validation Rule: Select this option to overwrite the Field's validation properties in the target system when the mApp 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 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 is applied.

7. Click OK.

8. Prepare the mApp for Distribution (File>Prepare mApp for distribution), or save the mApp (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 (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 Field properties.
- For more information about defining advanced Field properties, refer to Define Advanced Properties for a Field.

To configure merge actions for Field advanced properties:

1. Add a Business Object to a mApp 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:
   a. In the Object Manager within the mApp Editor, click 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 menu) are also reflected in the mApp Action column.

   Tip: You can also click the Edit Business Object button 📦 on the mApp Editor toolbar to open the Business Object Editor.

   b. Click a **Field**, and then click the Field Properties button.
3. Set the individual Field to *Merge*:
   a. Click the mApps page, and then check **Include in mApp**.
   b. In the Options area, click Import to Target System.

c. From the *If Already Present* drop-down menu, select Merge as the merge action for the Field.

4. Click the Advanced page.
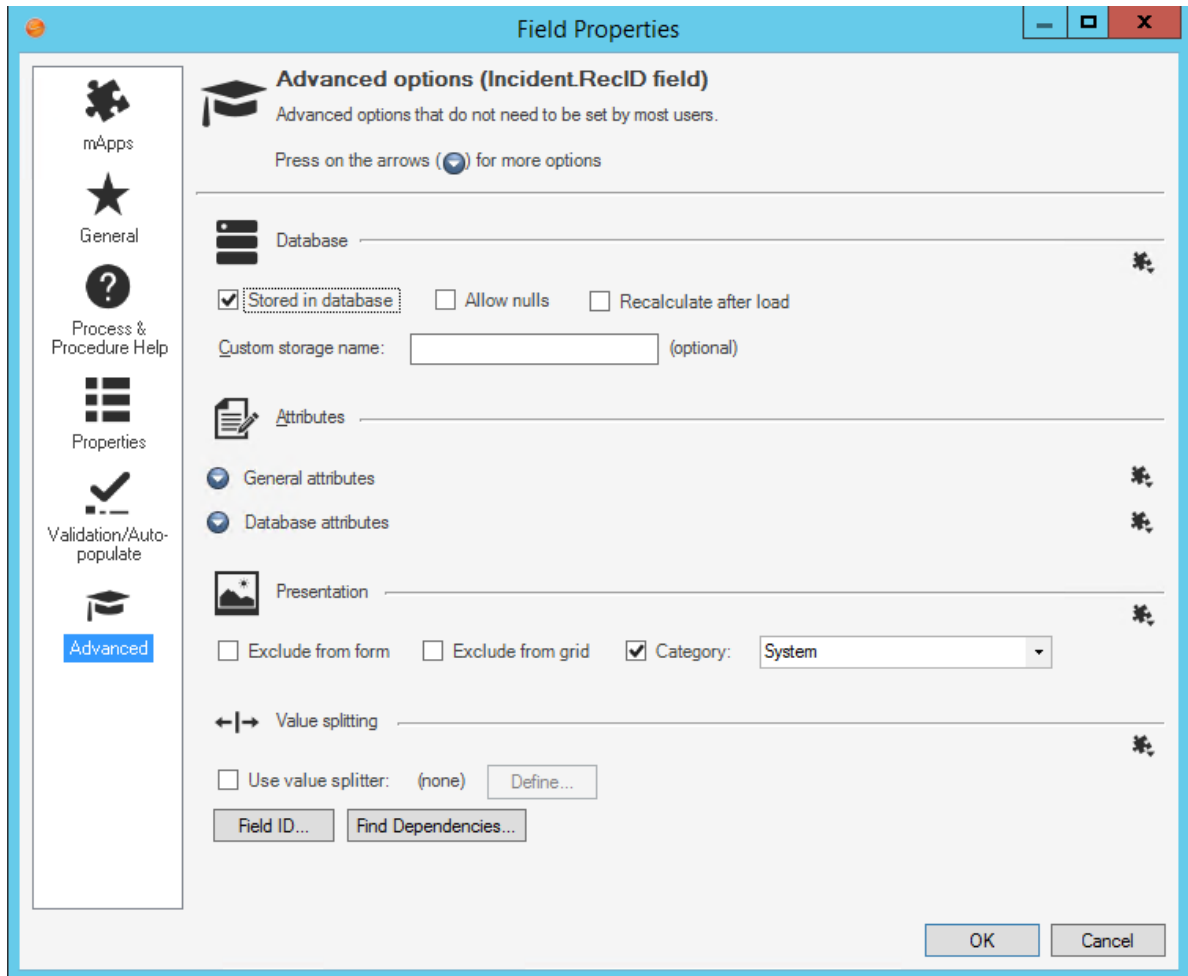
5. Click the mApp button ![mApp button] next to each property merge area, and then select a **merge action**:

For database settings:

Do Not Overwrite Database Settings: Select this option to leave the database settings unchanged in the target system when the mApp is applied.

Overwrite Database Settings: Select this option to overwrite the database settings in the target system when the mApp 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 is applied.

Overwrite General Attributes: Select this option to overwrite the general attributes in the target system when the mApp 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 is applied.

Overwrite Database Attributes: Select this option to overwrite the database attributes in the target system when the mApp 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 is applied.

Overwrite Presentation Settings: Select this option to overwrite the presentation settings in the target system when the mApp 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 is applied.

Overwrite Value Splitter: Select this option to overwrite the value splitter in the target system when the mApp is applied.

6. Click OK.

7. Prepare the mApp for Distribution (File>Prepare mApp for distribution), or save the mApp (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 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).

To configure merge actions for individual Relationships:

1. Add a Business Object to a mApp using the Add Business Object to mApp Wizard.

   > **Note:** You can also add Relationships to a mApp without also adding the Business Object (except for reference), but this is less common.

2. In the Object Manager within the mApp Editor, click the Business Object from the Object tree, and then click the Edit Relationships task in the Structure area.

   Tip: You can also click the Relationship button ⬦ 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 the mApp Action context menu):
   a. Click 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 definition is not imported into the target system when the mApp 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 will not be imported when the mApp is applied.

   > Overwrite Relationship: Select this option to have the mApp 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 for informational purposes only (the definition is not imported into the target system when the mApp is applied).

The selected action shows in the mApp 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. Click a **Relationship**, and then click the Edit button.

   b. Click the mApps page.
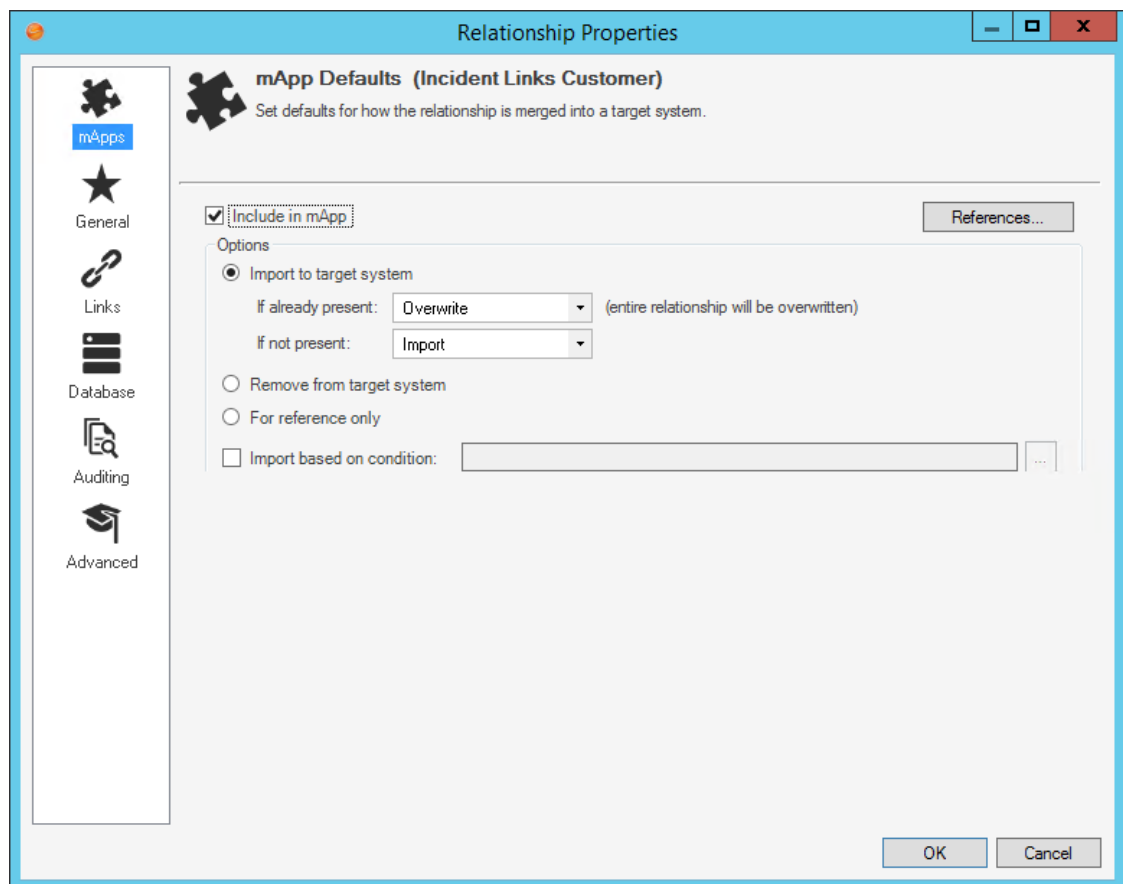
   c. Define general mApp properties for the Relationship:

Include in mApp: Select this check box to include the Relationship in the mApp. 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 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 (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: Click 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 radio 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, 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 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 definition is not imported into the target system when the mApp 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, 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 definition into the target system if does not already exist.

- Don't Import: Select this option to skip importing the mApp definition into the target system if it does not already exist (the mApp definition will not be added to the target system).

Remove from Target System: Select this radio button to remove the definition from a target system.

For Reference Only: Select this radio button to include the definition in the mApp for informational purposes only (the definition is not imported into the target system when the mApp is applied).

Import/Remove Based on Condition: Select this check box to import or remove the definition based on a condition. Then, click the Ellipses button to open the mApp Conditions window and define mApp conditions.

> **Tip:** You can also click the mApp Options button ❋ on the mApp Editor toolbar to open the mApp Options window for a Relationship and define general mApp properties and merge actions for the Relationship. The mApp Options button will show an indicator based on the merge action you select in the mApp Options window or in the Relationship Editor for a particular Relationship (ex: ❋ 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).

   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-downs:

Overwrite: Select this option to have the merge area overwritten in the target system when the mApp is applied.

Do Not Overwrite: Select this option to leave the merge area unchanged in the target system when the mApp is applied.

Tip: Click the Uncheck All button ⊟ to set all merge areas to *Do Not Overwrite*. Click the Select All button ☑ to set all merge areas to *Overwrite*.

On the remaining pages of the properties window: Click the mApp button ✱ 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. Click OK.

The Merge Area selections are reflected in the Relationship Editor.

6. Prepare the mApp for Distribution (File>Prepare mApp for distribution), or save the mApp (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 unchecked, 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.

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, click the Edit Relationships task in the Structure area.

   The Relationship Editor opens.

   Tip: You can also click the Edit Relationship button ⛓ on the mApp Editor Toolbar to open the Relationship Editor.

   b. Click a **Relationship**, and then click the Edit button.
3. Set the Relationship to *Merge*:
   a. Click the mApps page, and then check **Include in mApp**.

   b. In the Options area, click Import to Target System.

      c. From the *If Already Present* drop-down menu, select Merge as the merge action for the Relationship.

4. Click the General page.

5. Click the mApp button ✳ 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 is applied.

        Overwrite Name and Description: Select this option to overwrite the Relationship's name and description in the target system when the mApp 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 is applied.

Overwrite Relationship Type: Select this option to overwrite the Relationship type in the target system when the mApp 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 is applied.

Overwrite Number of Related Items: Select this option to overwrite the number of related items in the target system when the mApp 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 is applied.

Overwrite Default Group Member: Select this option to overwrite the default Group Member in the target system when the mApp 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 is applied.

Overwrite Relationship Use: Select this option to overwrite the Relationship use in the target system when the mApp 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 is applied.

Overwrite Reverse Relationship: Select this option to overwrite the reverse Relationship in the target system when the mApp 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 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 is applied.

6. Click OK.

7. Prepare the mApp for Distribution (File>Prepare mApp for distribution), or save the mApp (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 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 unchecked, 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.

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, click the Edit Relationships task in the Structure area.

       The Relationship Editor opens.

       Tip: You can also click the Edit Relationship button on the mApp Editor Toolbar to open the Relationship Editor.

    b. Click a **Relationship**, and then click the Edit button.
3. Set the Relationship to *Merge*:
    a. Click the mApps page, and then check **Include in mApp**.
    b. In the Options area, click Import to Target System.
    c. From the *If Already Present* drop-down menu, select Merge as the merge action for the Relationship.
4. Click the Links page.
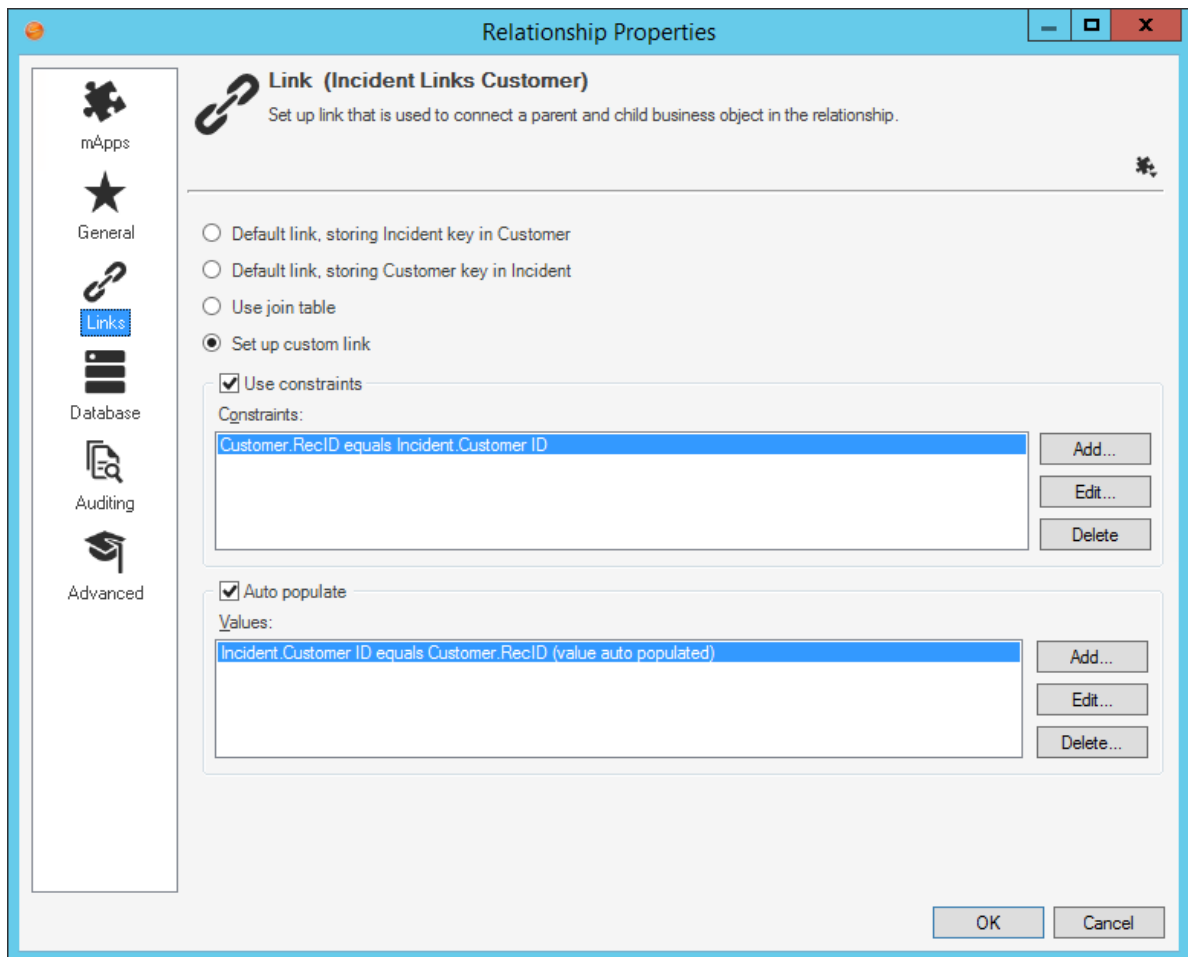
5. Click the mApp button ![icon], and then select a **merge action**:

> Do Not Overwrite Relationship Link Options: Select this option to leave the Relationship's link properties unchanged in the target system when the mApp is applied.

> Overwrite Relationship Link Options: Select this option to overwrite the Relationship's link properties in the target system when the mApp is applied.

6. Click OK.

7. Prepare the mApp for Distribution (File>Prepare mApp for distribution), or save the mApp (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 unchecked, 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.

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, click the Edit Relationships task in the Structure area.

      The Relationship Editor opens.

      Tip: You can also click the Edit Relationship button ⬥ on the mApp Editor Toolbar to open the Relationship Editor.

   b. Click a **Relationship**, and then click the Edit button.

3. Set the Relationship to *Merge*:
   a. Click the mApps page, and then check **Include in mApp**.

   b. In the Options area, click Import to Target System.

   c. From the *If Already Present* drop-down menu, select Merge as the merge action for the Relationship.

4. Click the Database page.
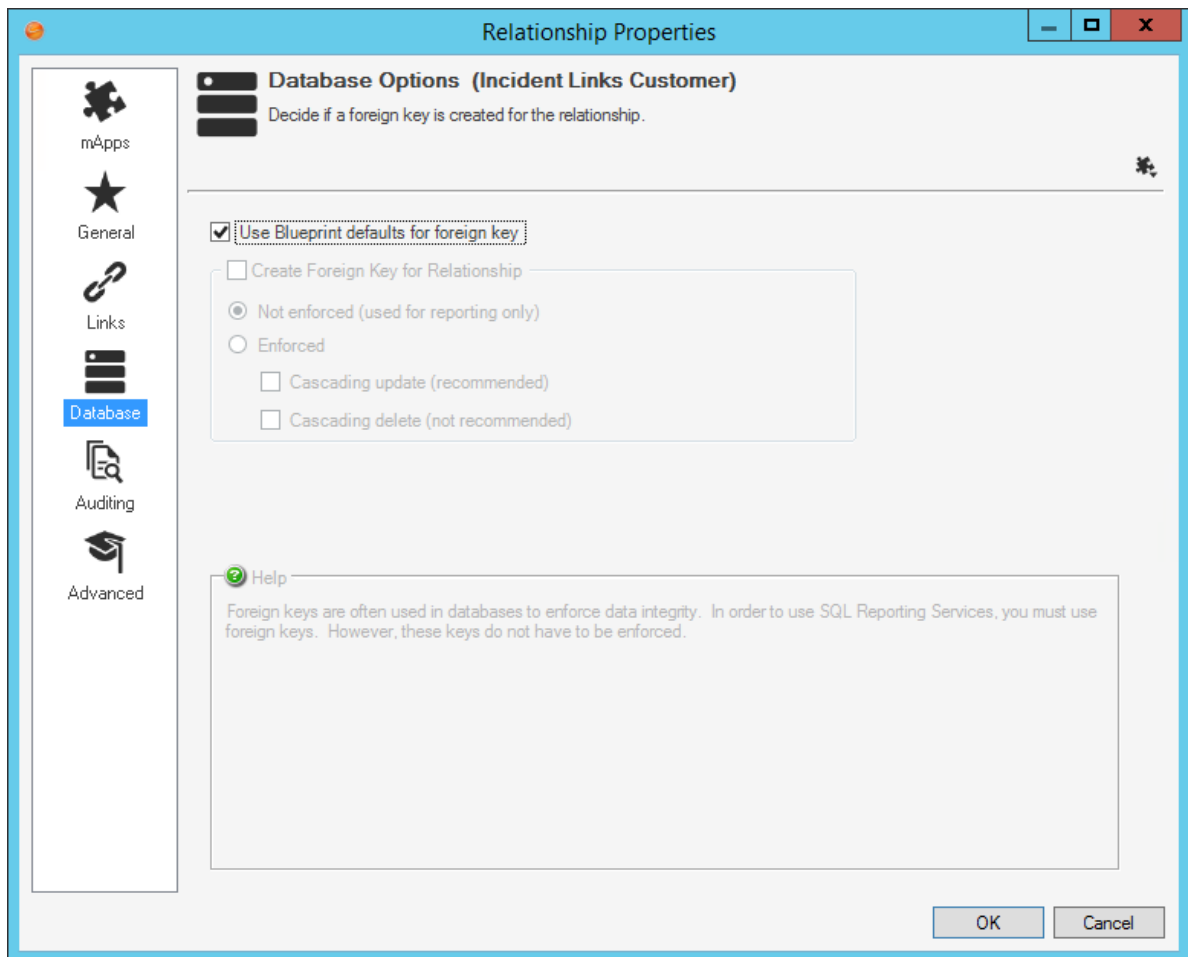
5. Click the mApp button [icon], and then select a **merge action**:

> Do Not Overwrite Database Options: Select this option to leave the Relationship's database properties unchanged in the target system when the mApp is applied.

> Overwrite Database Options: Select this option to overwrite the Relationship's database properties in the target system when the mApp is applied.

6. Click OK.

7. Prepare the mApp for Distribution (File>Prepare mApp for distribution), or save the mApp (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.

To define merge actions for Relationship auditing 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, click the Edit Relationships task in the Structure area.

      The Relationship Editor opens.

      Tip: You can also click the Edit Relationship button ⊹ on the mApp Editor Toolbar to open the Relationship Editor.

   b. Click a **Relationship**, and then click the Edit button.
3. Set the Relationship to *Merge*:
   a. Click the mApps page, and then check **Include in mApp**.
   b. In the Options area, click Import to Target System.
   c. From the *If Already Present* drop-down menu, select Merge as the merge action for the Relationship.
4. Click the Auditing page.
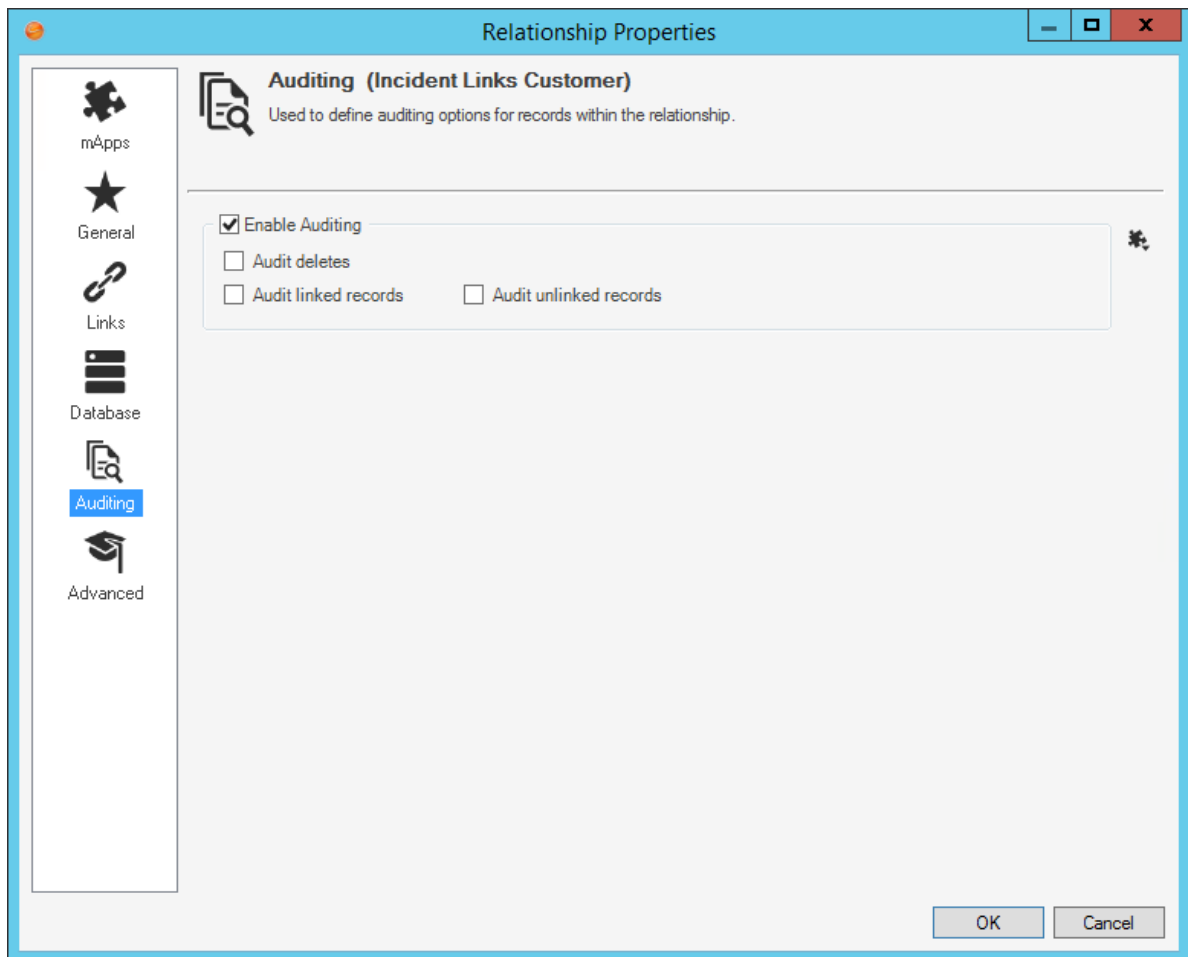
5. Click the mApp button , and then select a **merge action**:

> Do Not Overwrite Audit Settings: Select this option to leave the Relationship's auditing properties unchanged in the target system when the mApp is applied.

> Overwrite Audit Settings: Select this option to overwrite the Relationship's auditing properties in the target system when the mApp is applied.

6. Click OK.

7. Prepare the mApp for Distribution (File>Prepare mApp for distribution), or save the mApp (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 unchecked, 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.

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, click the Edit Relationships task in the Structure area.

    The Relationship Editor opens.

    Tip: You can also click the Edit Relationship button ⬚ on the mApp Editor Toolbar to open the Relationship Editor.

    b. Click a **Relationship**, and then click the Edit button.
3. Set the Relationship to *Merge*:
    a. Click the mApps page, and then check **Include in mApp**.
    b. In the Options area, click Import to Target System.
    c. From the *If Already Present* drop-down menu, select Merge as the merge action for the Relationship.

4. Click the Advanced page.

5. Click the mApp button [icon] 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 is applied.

Overwrite Advanced Options: Select this option to overwrite the advanced options in the target system when the mApp 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 is applied.

Overwrite Group Settings: Select this option to overwrite the group settings in the target system when the mApp 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 is applied.

Overwrite General Attributes: Select this option to overwrite the general attributes in the target system when the mApp 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 is applied.

Overwrite Database Attributes: Select this option to overwrite the database attributes in the target system when the mApp is applied.

6. Click OK.

7. Prepare the mApp for Distribution (File>Prepare mApp for distribution), or save the mApp (File>Save mApp to Disk) to continue making other changes.

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.
- Options for importing the Form into the target system when the mApp 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 for informational purposes only (it is not merged into the target system when the mApp is applied).
  - Import/remove based on condition: Imports or removes the Form based on configured mApp conditions.

To configure merge actions for Forms:

1. Add a Business Object to a mApp 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 ![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 (ex: Default Form), and then click the mApp Options button ![mApp Options button] on the mApp Editor toolbar.

b. Define general mApp properties for the Form:

Include in mApp: Select this check box to include the form in the mApp. 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 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 (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* 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 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 definition is not imported into the target system when the mApp 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 definition into the target system if does not already exist.
- Don't Import: Select this option to skip importing the mApp definition into the target system if it does not already exist (the mApp 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 for informational purposes only (the definition is not imported into the target system when the mApp 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 Conditions window and define mApp conditions.

d. Click OK.

The mApp Options button shows an indicator based on the selected merge action (ex: for *Overwrite*).

4. Prepare the mApp for Distribution (File>Prepare mApp for distribution), or save the mApp (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 Options window in the Grid Editor to configure the following:

- General properties: Whether to include the Grid in the mApp.
- Options for importing the Grid into the target system when the mApp 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 for informational purposes only (it is not merged into the target system when the mApp is applied).
    - Import/remove based on condition: Imports or removes the Grid based on configured conditions.
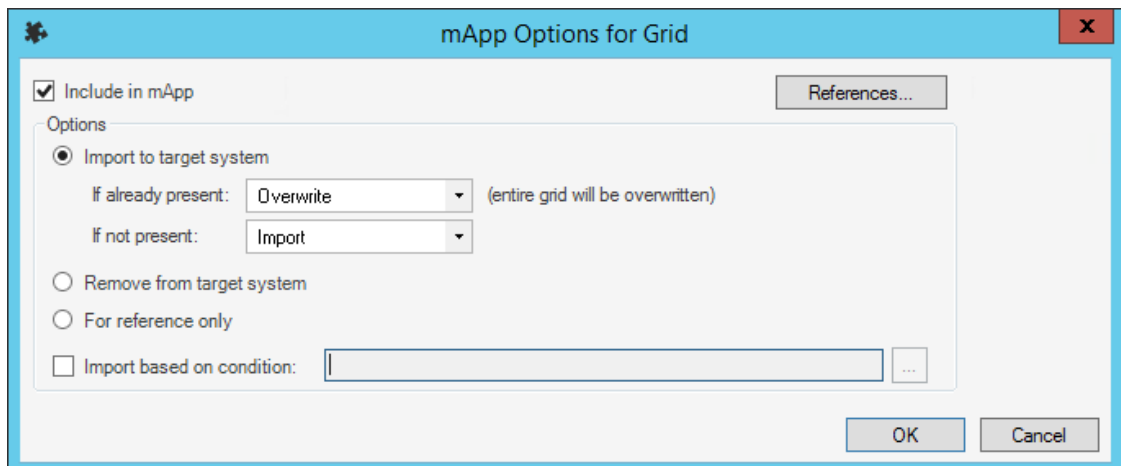
To configure merge actions for Grids:

1. Add a Business Object to a mApp 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 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 (ex: Default Grid), and then click the mApp Options button on the mApp Editor toolbar.

b. Define general mApp properties for the Grid:

Include in mApp: Select this check box to include the Grid in the mApp. 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 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 (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 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 definition is not imported into the target system when the mApp 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 definition into the target system if does not already exist.
- Don't Import: Select this option to skip importing the mApp definition into the target system if it does not already exist (the mApp 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 for informational purposes only (the definition is not imported into the target system when the mApp 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 Conditions window and define mApp conditions.

d. Click OK.

The mApp Options button shows an indicator based on the selected merge action (ex: for *Overwrite*).

4. Prepare the mApp for Distribution (File>Prepare mApp for distribution), or save the mApp (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 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 [icon] 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 [icon] in the mApp Editor toolbar.
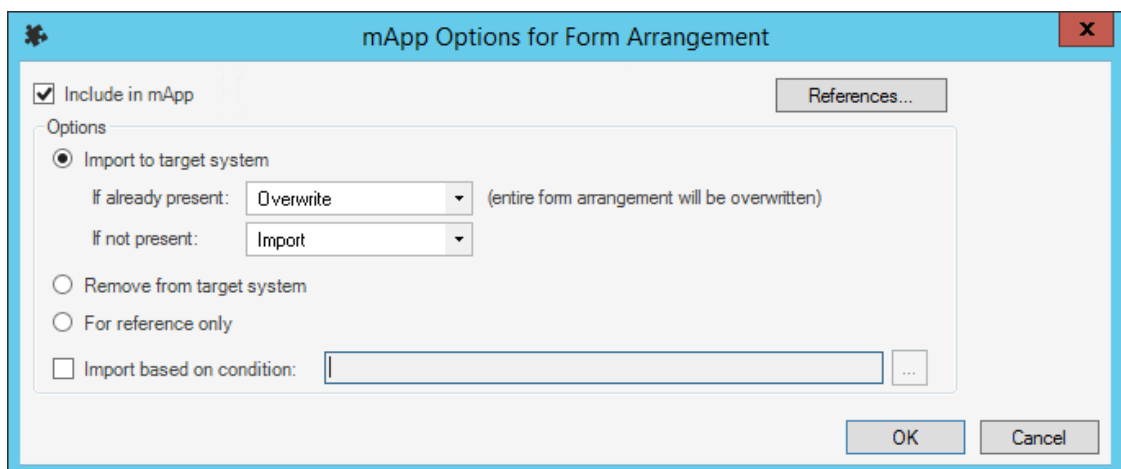
   b. Define general mApp properties for the Form Arrangement:

Include in mApp: Select this check box to include the Form Arrangement in the mApp. 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 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 (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 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 definition is not imported into the target system when the mApp 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 definition into the target system if does not already exist.
- Don't Import: Select this option to skip importing the mApp definition into the target system if it does not already exist (the mApp 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 for informational purposes only (the definition is not imported into the target system when the mApp 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 conditions.

    d. Click OK.

The mApp Options button shows an indicator based on the selected merge action (ex: 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 definition is not imported into the target system when the mApp 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 is applied.

        Overwrite Tab: Select this option to have the mApp 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 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 definition is not imported into the target system when the mApp is applied).

        Overwrite tab: Select this option to have the tab definition in the mApp 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 is applied.

        Remove tab if found: Select this option to have the mApp 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. Click OK.

Each tab shows an indicator based on the action selected in the mApp Action context menu or the Tab Properties window.

6. Prepare the mApp for Distribution (File>Prepare mApp for distribution), or save the mApp (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.
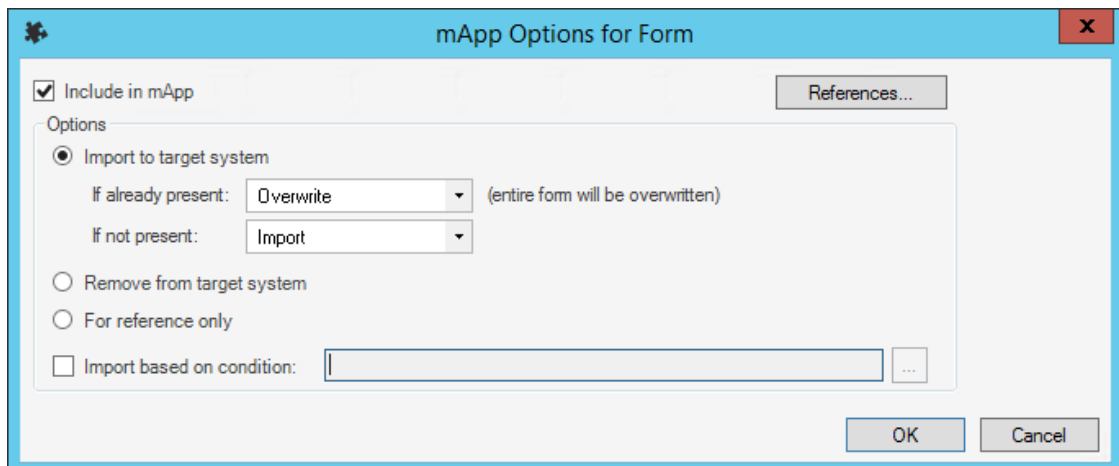
To configure merge actions for Business Object Actions:

1. Add a Business Object to a mApp 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 (ex: Task Pane) to view the Actions for that specific area.
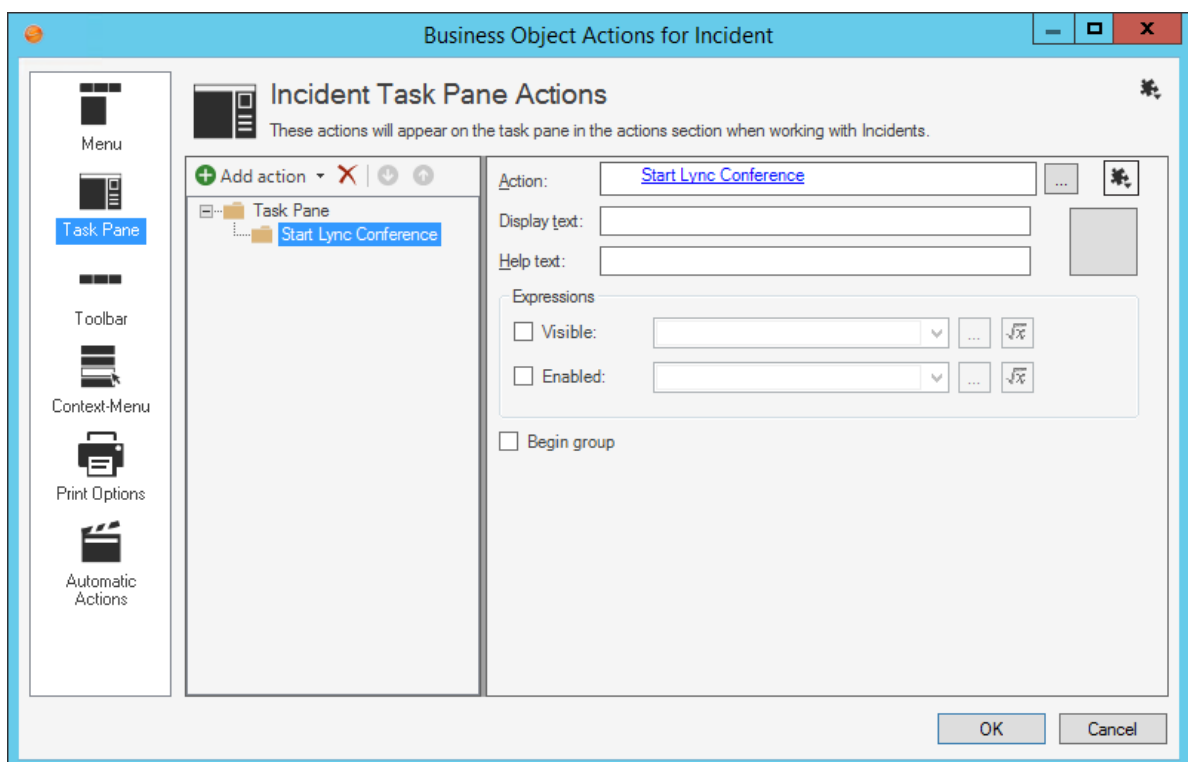
4. Configure separate merge actions for individual Business Object Action areas (the merge action selected will apply to all Business Object Actions within the area:
   a. Click the mApp button [icon], and then select a merge action:

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 ![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 definition is not imported into the target system when the mApp is applied).

   Overwrite Action: Select this option to have the mApp 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 is applied.

6. Click OK.

7. Prepare the mApp for Distribution (File>Prepare mApp for distribution), or save the mApp (File>Save mApp to Disk) to continue making other changes.

View Referenced Definitions in a mApp

References allow you to see at a glance all of the system definitions throughout CSM being used by a selected mApp 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.

Good to know:

- If you add a definition to a mApp 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 is applied.
- You cannot add Business Objects to a mApp 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 definition.
- View all references that can be automatically added to a mApp.
- Add referenced definitions to a mApp.

The references window can be opened several ways within a mApp by clicking the References button (activated when the **Include in mApp** check box is selected):

- From the mApps page in the Business Object Properties window.
- From the mApps page in the Field Properties window.
- From the mApps 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 (ex: One-Step) to a mApp.
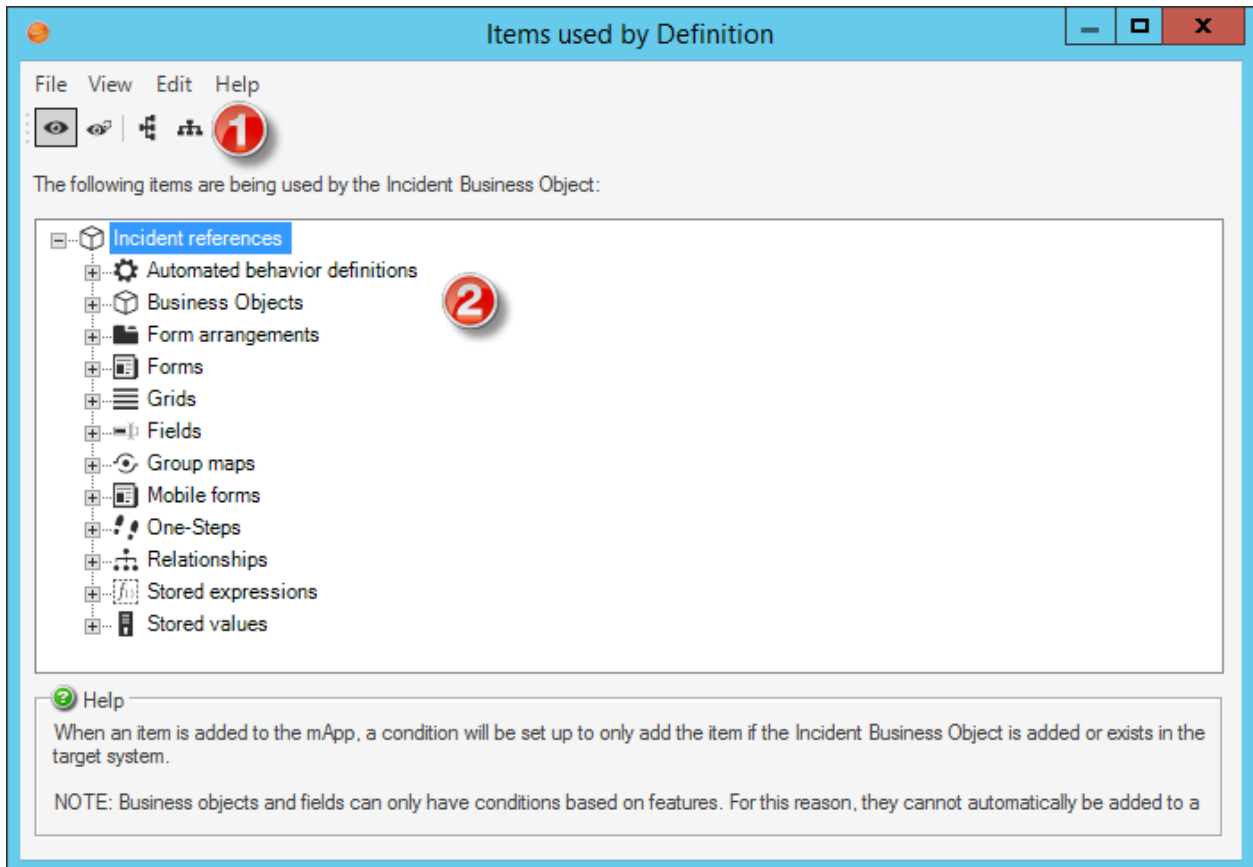
1. **Toolbar**: Displays a row of drop-down menus available in the References window.
2. **Main Pane**: Displays dependent definitions grouped in a tree by system definition.

Open the References Window

The references window can be opened several ways within a mApp by clicking the References button (activated when the **Include in mApp** check box is selected):

- From the mApps page in the Business Object Properties window.
- From the mApps page in the Field Properties window.
- From the mApps 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 (ex: One-Step) to a mApp.

References Window Toolbar

Use the References window toolbar to view and add definitions that are used by a system definitions included in a mApp. When you add a referenced definition to a mApp, 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 (ex: Forms). What is shown in the tree depends on where the References window was accessed (ex: 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 (right-click item or use the buttons on the toolbar).

Configure mApp Conditions

Use the mApp Conditions window to configure conditions that control which definitions in a mApp are imported into a target system. When you configure conditions for a mApp definition, you create a list of system definitions or Features (defined in mApp Properties). A mApp 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, and CSM Items.

Good to know:

- If you add definitions to a mApp 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 Conditions:

1. 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 mApps Options window in the following areas:
    - Form Editor

    - Grid Editor

    - Form Arrangement Editor

    - CSM Item Managers
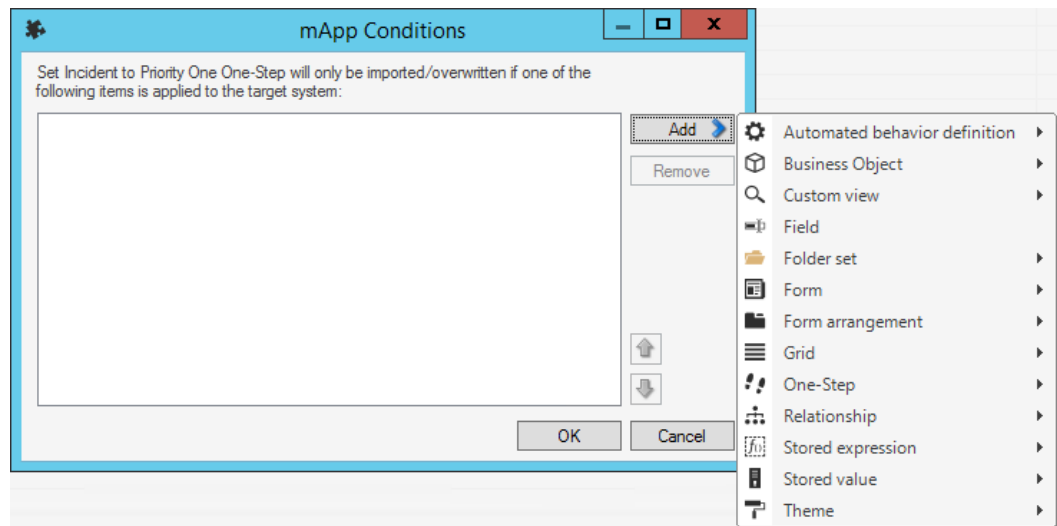
2. Add a definition to the list of conditions:

   a. Click Add to open a menu of definitions organized by type (ex: Business Object). The list shows all definitions included in the mApp, 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** arrows [▼] [▲] to change the order of the selected definitions.

4. Click OK.

Automation Processes

Automation Processes allow CSM Users to automate behavior by creating rules for the system to follow.

About Automation Processes

Automation Processes could include either automatically completing an Action when a particular event takes place (example: When an Incident is closed, send a notification to the Customer), or handling time-sensitive issues (example: If the Customer has not been contacted within four hours, automatically remind the Technician). Automation Processes can also watch for trends (example: If the number of open Incidents exceeds a particular threshold, then automatically act). Automation Processes operate within the timeframe of defined Business Hours.
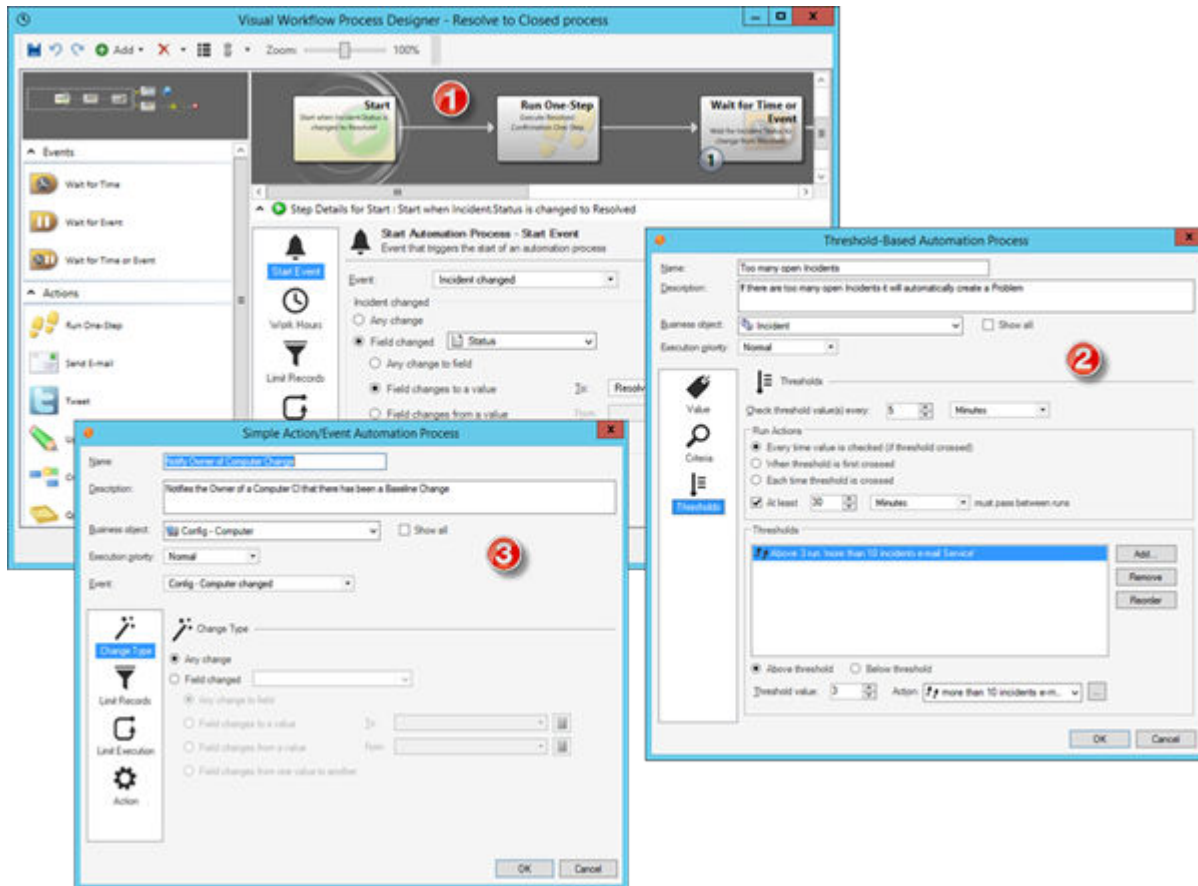
There are three types of Automation Processes:

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 or Action after a specific event occurs.

CSM provides multiple tools to manage Automation Processes, including the Automation Process Editor and Visual Workflow Process Designer.

CSM provides several OOTB Automation Processes designed to help automate common service desk operations. Use these OOTB Automation processes as-is, edit them, or create your own using the Automation Process Manager and Automation Process Editor.

Automation Processes Good to Know

- There are three types of Automation Processes in CSM, including:
  - 🔔 Simple-Action Automation Process
  - ⊩ Threshold-Based Automation Process
  - 🕐 Automation Process Visual Workflow Process

- CSM provides several OOTB Automation Processes designed to help automate common service desk operations. Use these OOTB Automation processes as-is, edit them, or create your own using the Automation Process Manager and Automation Process Editor.

- Use the Automation Processes page in CSM Administrator (CSM Administrator>Automation Processes) to quickly access common Automation Process operations.

- CSM provides two tools that can be used to manage Automation Processes. Use the Automation Process Editor to work with Automation Processes (create, edit, delete, etc.) outside of a Blueprint (typical use). Use the Automation Process Manager to work with Automation Processes (create, edit, delete, etc.) within a Blueprint (required when adding an Automation Process to a mApp).

Always consider the following:

- Security rights control access to CSM functionality and are configured in the Security Group Manager in CSM Administrator (CSM Administrator>Security>Edit Security Groups). For detailed information, see Configure Automation Process Blueprint Security Rights and Configure Automation Process Service Security Rights.

Using Automation Processes

OOTB Automation Processes

CSM provides numerous OOTB Automation Processes, which are organized and defined based on Business Objects:

- Incident
- Problem
- CMDB
- Change
- Knowledge Article
- Task
- Customer Internal
- Event
- Password Reset

CSM Administration

Customer - Internal Automation Processes

CSM provides the following OOTB Customer - Internal Automation Process:

Name	Description
Last Logon 90 Days Ago - Customer Internal	Waits 90 days after the Customer - Internal Last Logon date and time change, then runs the Disable User Account One-Step (changes the status of a User Account to Disabled).

CSM Administration   491

Event Automation Processes

CSM provides the following Event Automation Process:

Name	Description
Update CI Status to Down	When an Event Record is created, the process initiates the Update CI Status One-Step, which Updates the CI status to Down.

Password Reset Form Automation Processes

CSM provides the following Password Reset Automation Process:

Name	Description
Self Service Password Reset	When a new Self-Service Password Reset Form is created, the process determines whether the password should be reset and then takes the appropriate actions.

Open an Existing Automation Process Blueprint

Automation Processes are edited within a Blueprint in order to allow the system administrator to set up multiple rules that take place at the appropriate time. Use the Open an Existing Automation Process Blueprint task to import a previously-created Blueprint (.bp) from your computer files.

To open an existing Automation Process Blueprint:

1. Open CSM Administrator.

2. Click Automation Processes.

3. Click Open an existing Automation Process Blueprint.

   A window opens displaying your computer files.

4. Select a **Blueprint file (.bp)**.

5. Click OK.

   The Automation Process Blueprint opens.

Enable or Disable an Automation Process

By default, all Automation Processes are disabled in CSM. Use CSM Administrator to enable Automation Processes, which activates the processes and initiates them at the appropriate time.

> **Note:** Automation Process e-mails use the Current System Stored Value. The processes will send e-mails to the test receiver account (ex: ServiceDeskTESTReceiver@company.com) until you migrate to a production environment.

While many default processes are available for your use, we recommend the following at a minimum:

- **Incident Confirmation E-mail on Create:** (Association: Incident) When an Incident is created, the process initiates the Incident Confirmation One-Step, which sends the Customer an e-mail to confirm their record and provide the Record ID number.

- **Incident - Not Touched in 3 Days:** (Association: Incident) Waits for the Last Modified Date Time Field to update. If the Field is not updated for three days, the process initiates the SLA Escalate if Not Touched in 3 Days One-Step that sends an e-mail to the Incident owner with a reminder to follow up with the Customer.

- **Resolve to Closed:** (Association: Incident) Waits for three days after the status of an Incident is changed to Resolved. If the status does not change from Resolved, it marks the status as Closed.

The following CSM icons indicate the type of Automation Process:

Icon	Action
🔔	Simple Action/Event Automation Process
▐▤	Threshold-Based Automation Process
🕐	Visual Workflow Automation Process

Use the Individual Automation Process Status task (CSM Administrator) to either enable or disable Automation Processes:

- Enabled Automation Process: Active in the system and operate at the scheduled time.

- Disabled Automation Processes: Inactive in the system, so they do not operate when events are fired.

The Automation Process Status window (CSM Administrator>Automation Processes>Individual Automation Process Status) uses the following icons to indicate status:

Icon	Action
▶	The Automation Process is enabled (active).

Icon	Action
⊙	The Automation Process is disabled (inactive).

To change the status of an Automation Process:

1. Click the Automation Processes category in CSM Administrator.
2. Click Individual Automation Process Status.

   The Automation Process Status window opens.
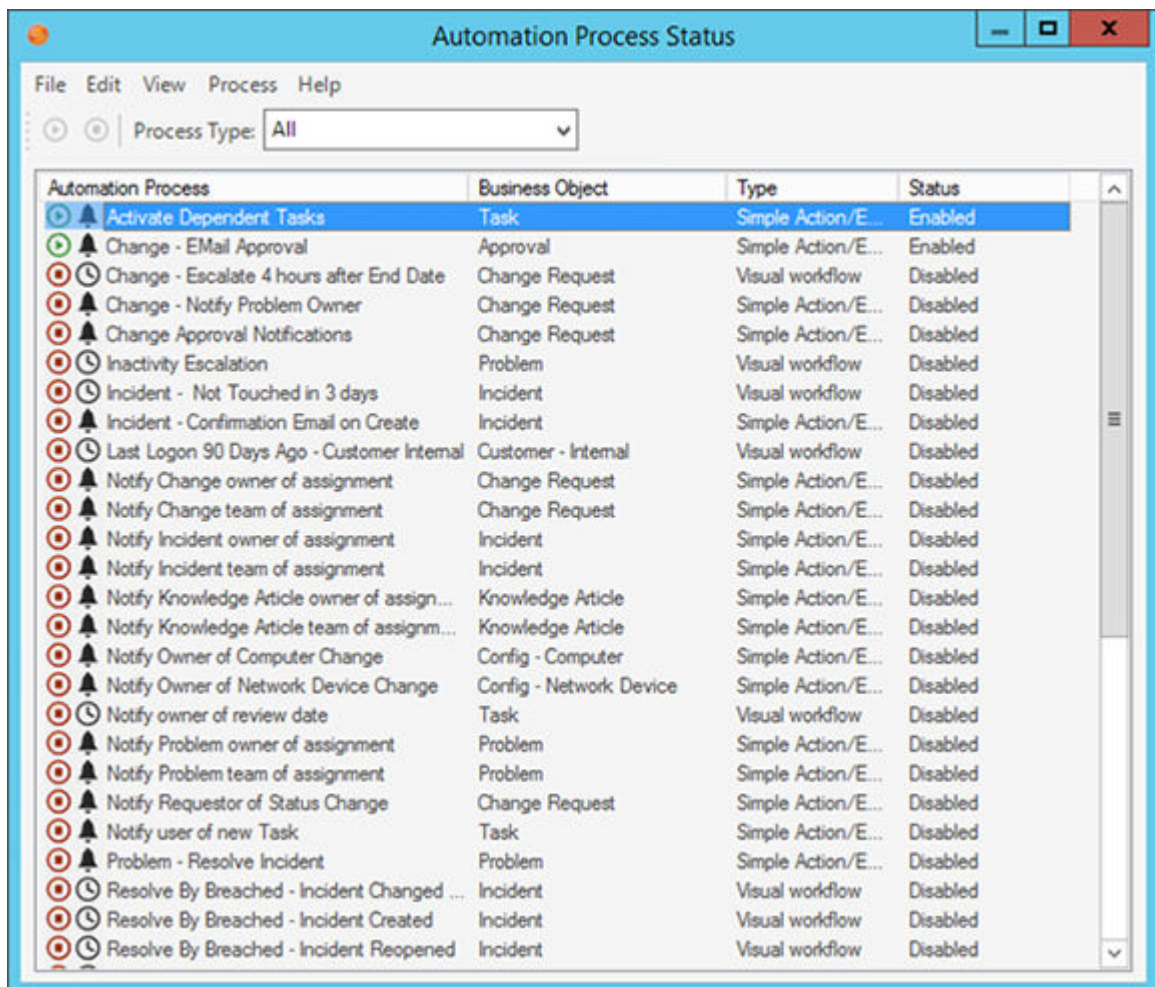
3. Select the Automation Process that you want to change.
4. Select a status:

   Click the Enable button ⊙ on the toolbar to enable the Automation Process.

Tip: You can also click Process on the menu bar and select Enable, or right-click an **Automation Process** and select Enable.

Click the Disable button on the toolbar to disable the Automation Process.

The Automation Process reflects the selected status in the Grid.

5. Close the Automation Process Status window.

Note: Your changes are saved automatically.

Pause/Resume Automation Process Server Processing

Use the Pause/Resume Processing task (CSM Administrator>Automation Processes) to temporarily pause, and then resume Automation Process Server processing. This does not stop the Automation Process Server (service); rather, it suspends the server so that, when resumed, the server can pick up where it left off. For example, pause processing to suspend sending out automatic e-mails; resume processing to continue sending out automatic e-mails. The ability to pause or resume Automation Server processing is controlled by Automation Process Service security rights.

Good to know:

- 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 or Service Monitor to stop the server itself.

To pause or resume Automation Process Server processing:

1. In the CSM Administrator main window, click the Automation Processes category, and then click the Pause/Resume Processing task.

2. Select to pause or resume:
    a. Pause Automation Process Server: Select the check box to pause processing. You must provide a reason for pausing processing.

    b. Resume Automation Process Server Processing: Select the check box to resume processing.

3. Click OK.

Monitor Automation Process Statistics

You can monitor these statistics for individual Automation Processes:

- Completed runs, including successes and failures
- In-progress runs
- Scheduled activities

To view Automation Process statistics:

1. Click the Automation Processes category in CSM Administrator.
2. Click Individual Automation Process Status.
3. Select an Automation Process, and then click Process>Statistics.

To clear Automation Processes:

1. From the **Automation Process Statistics** window, select Clear Process.
2. Select these options to delete these items:
   Clear scheduled activities: Clear activities that are currently scheduled for the Automation Process.

   Clear in-progress items: Clear activities that are in progress.

   Clear completed item history: Clear 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.

   CAUTION: Once you click OK, the selected items are deleted.

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, such as an Incident.
2. Select Tools>Current Record Automation Processes.
   A list of Automation Processes that than run opens.
3. You can:
   > Select a specific Automation Process, and then click Details to view information about the run.

   > Click 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.

Managing Automation Processes

CSM provides multiple tools to manage Automation Processes, including the Automation Process Editor and Visual Workflow Process Designer.

- Automation Process Editor
- Open the Automation Process Editor

Good to know:

- CSM provides two tools that can be used to manage Automation Processes. Use the Automation Process Editor to work with Automation Processes (create, edit, delete, etc.) outside of a Blueprint (typical use). Use the Automation Process Manager to work with Automation Processes (create, edit, delete, etc.) within a Blueprint (required when adding an Automation Process to a mApp).

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

Automation Process Editor

Use the Automation Process Editor to define Automation Processes, including:

- Simple Action/Event Process
- Threshold-Based Process
- Automation Process Visual Workflow Process

Note: Automation Processes are edited using Blueprints. This allows for a number of changes to be made together, but only applied to the system when you are ready.

Open the Automation Process Editor

To open the Automation Process Editor from the CSM Administrator main window, click the Automation Process category and then click 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. Click 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 or Action to run when the event takes place.

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:
   Name:

   Provide a display name.

   Description:

   Provide a brief description.

   Business Object:

   Select the type of Business Object against which the process will operate.
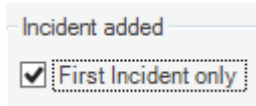
   Execution Priority:

   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.

   Event:
   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>. • Field Changed: The Automation Process will begin if the selected Field is altered. **Note:** You have the option 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 is the Field changes from one value to another.

Event Type	Description
<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.
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. • **<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).

3. Click OK.

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.

To define record limitations for a Simple Action/Event Automation Process:

1. Create a Simple Action/Event Automation Process.

2. Click 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 (Search Group) condition is true will cause the Action to be executed when the Event occurs.
   a. Select the Query check box.

      The Query drop-down and Ellipses button become active.

   b. Click the **Ellipses** button [ ] to open the Search Group Manager, where you can select an existing Search Group or create a new Search Group.

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 drop-down and Value drop-down become active.

   b. From the Field drop-down, select a **Field**.

   c. From the Value drop-down, 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, Ellipses button, and Custom Expression button become active.

   b. Define the Expression:

      Select an existing Expression: Click the Ellipses button [ ] to open the Expression Manager, and then select an **Expression**.

   c. Create a Custom Expression: Click the Custom Expression button [ ] and define a Custom Expression.

6. Click OK.

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:

- One-Step: One-Step to run when the event takes place.
- Action: Action to run when the event takes place.

To define general properties for a Simple Action/Event Automation Process:

1. Create a Simple Action/Event Automation Process.
2. Click the Actions page.

    The Actions section opens below the general properties.

3. Define a One-Step to run when the event takes place:
    a. Select the **One-Step** radio button.

        The One-Step Field and Ellipses button become active.

    b. Click the **Ellipses** button [...] to open the One-Step Manager, and then select an existing One-Step or create a new One-Step.

4. Define an Action to run when the event takes place:
    a. Select the Execute Action radio button.

        The Execute Action Field and Action button become active.

    b. Click the **Action** button, and then select an available **Action** in the drop-down:
        Send an E-Mail

        Send Tweet

        Update a Business Object

        Create a Child Business Object

5. Click OK.

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. When you define the Automation Process, you define:

- **General properties:** Name, description, Business Object, and execution priority.
- **Value:** A value that the Automation Process should monitor.
- **Criteria:** Search criteria for the value included in the calculation.
- **Threshold:** 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. Click the New button, and then select Threshold-Based Process.
3. Define general properties:
   Name:

   Provide a display name to use within CSM (this property can be searched in CSM Item Managers).

   Description:

   Provide a description to use within CSM (this property can be searched in CSM Item Managers).

   Business Object:

   Select the type of Business Object against which this process will operate.

   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. Define the value that the Automation Process should monitor:
   a. Click the Value page.

      The Value page opens below the general properties.

   b. Define value properties:
      Number of Records:

      Select this **radio button** to monitor the number of records that meet the defined criteria.

      Function:

Select this **radio button** to apply a mathematical function against a Field (ex: Average, total, etc.) if there is a numeric Field on the records being evaluated.

Duration Function:

Select this **radio button** to apply a mathematical function against the range of time between two time-based Fields (ex: Determining the average amount of time that Incidents take to resolve).

Note: If you select a duration function, you must specify the Fields that define the start/end date times and the unit(s) to use (ex: hours, days, months, etc.).

5. Define criteria for the records included in the calculation:
   a. Click the Criteria page.

   The Criteria page opens below the general properties.

   b. Define criteria properties:
      Search Criteria:

      Click the Ellipses button [ ] to select an existing Search Group or click the Search

      button [Q] to define a Custom Query to limit the records considered.

      Date Range:

      Click the Range drop-down to select a date range or click the New button to create a new date range to use to limit records for consideration.

      Open Incidents Only:

      Select the check box to only include open Incidents in the results.

6. Define one or more thresholds.
   a. Click the Thresholds page.

   b. Define threshold properties:
      i. 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.

      ii. Define run Actions:
          Every time value is checked (if the threshold is crossed):

          Select this **radio button** 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 **radio button** 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 **radio button** 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 the "at least" 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.

Note: 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.

iii. Define thresholds:
Create a threshold:

Click the Add button to add a threshold to the list.

Edit a threshold:

Use the **controls underneath the threshold list** to customize the threshold.

Remove a threshold:

Click the Remove button to permanently delete a threshold.

Reorder the thresholds:

Click the Reorder button 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.

Action:

Select or define a **One-Step** to run when the threshold is breached.

Note: The Action must be an unassociated One-Step (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. Click OK.

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.
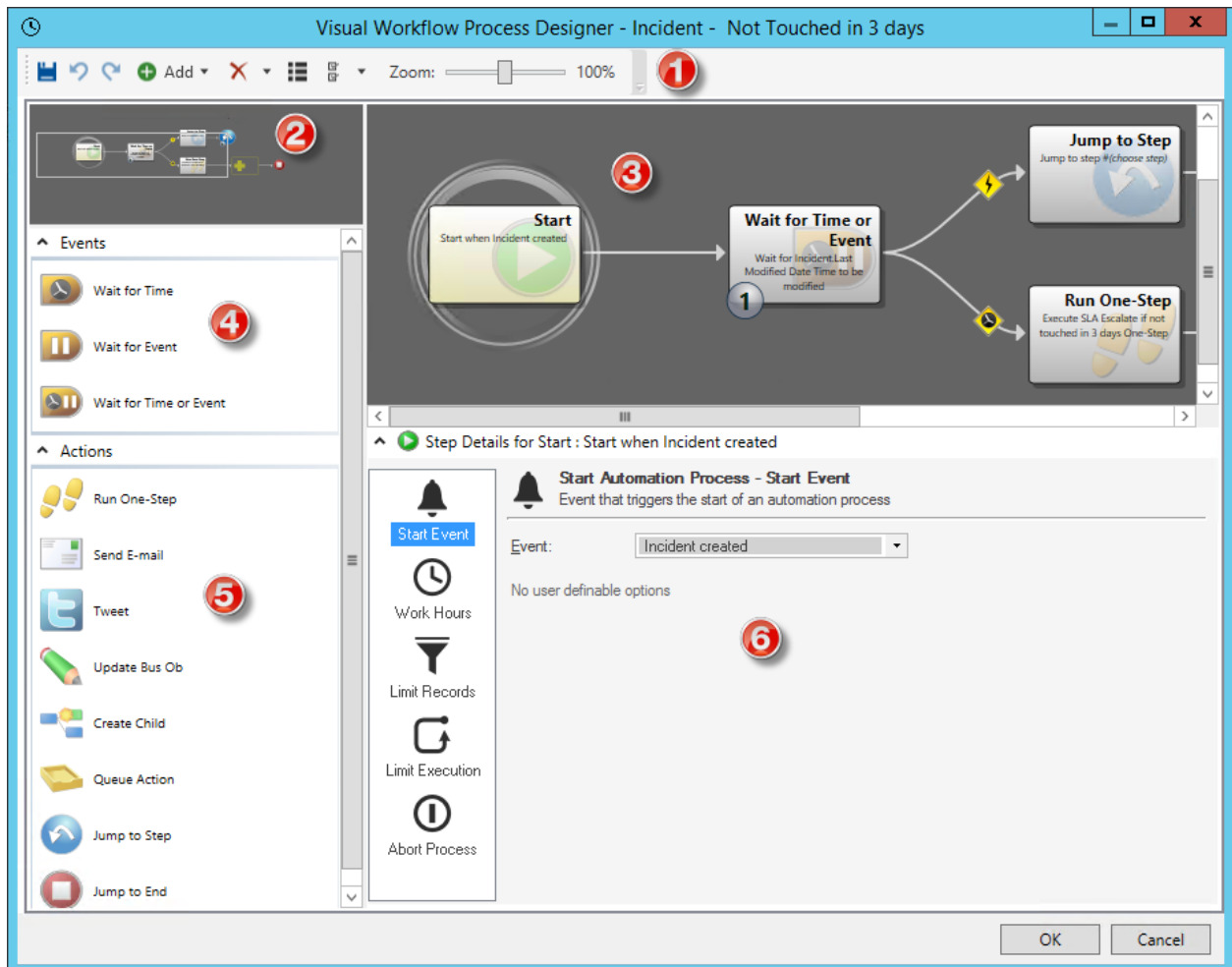
1. Toolbar:

   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:
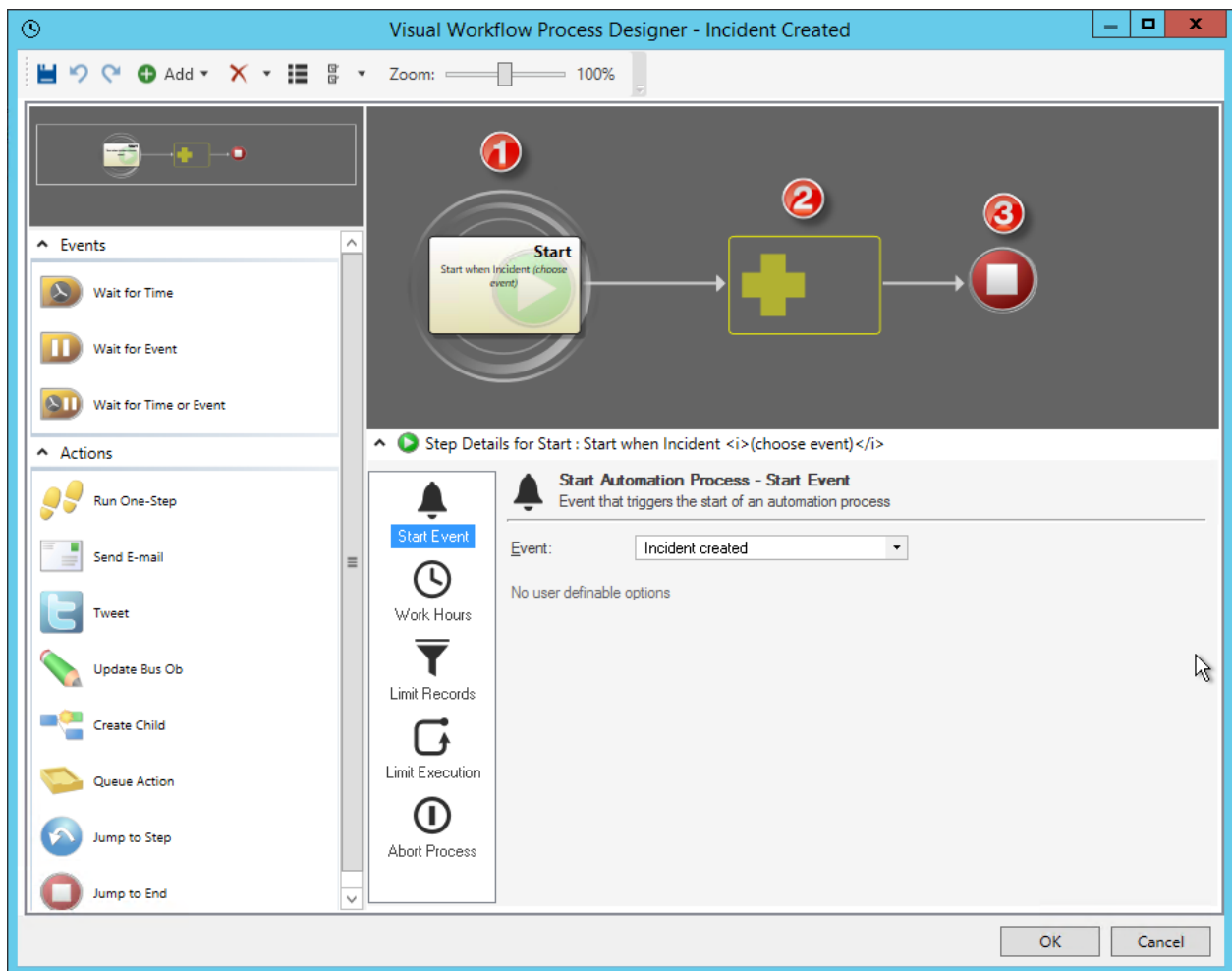
1. Start Graphic:

   Event or starting point that initiates the process.

   Tip: Click 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.

Open the Automation Process Visual Workflow Process Designer

To open the Automation Process Visual Workflow Process Designer:

1. Open the Automation Process Editor.

2. Click the New button, and then select Visual Workflow Process.

   The Visual Workflow Process Properties window opens.

3. Define Automation Process properties.
   a. Name:

      Provide a display name to use within CSM (this property can be searched in CSM Item Managers).

   b. Description:

      Provide a description to use within CSM (this property can be searched in CSM Item Managers).

   c. Business Object:

      Select a **Business Object** to associate with the Automation Process.

   d. 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. Click OK.

Automation Process Visual Workflow Process Designer Toolbar

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 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.
		Increases or decreases the size of the diagram on the Designer Board.

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.

To create a Visual Workflow Automation Process:

1. Open the Automation Process Visual Workflow Process Designer.
2. Define general properties: Start event, work hours, record limitations, execution limitations, and the abort process.
3. Define events: Amount of time before the Automation Process continues to the next step and/or the event that triggers the Automation Process to move to the next step.
4. Define actions: Actions that occur as a result of a time or event trigger (ex: Run One-Step, send E-mail, etc.).

Define Automation Process Visual Workflow Properties

Use the Current Step Details section of the Visual Workflow Process Designer to define general properties. When you define general properties, you define:

- **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.

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. Click the Start Event page in the left pane of the Current Step Details section.
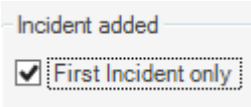
   The Start Automation Process - Start Event page opens.
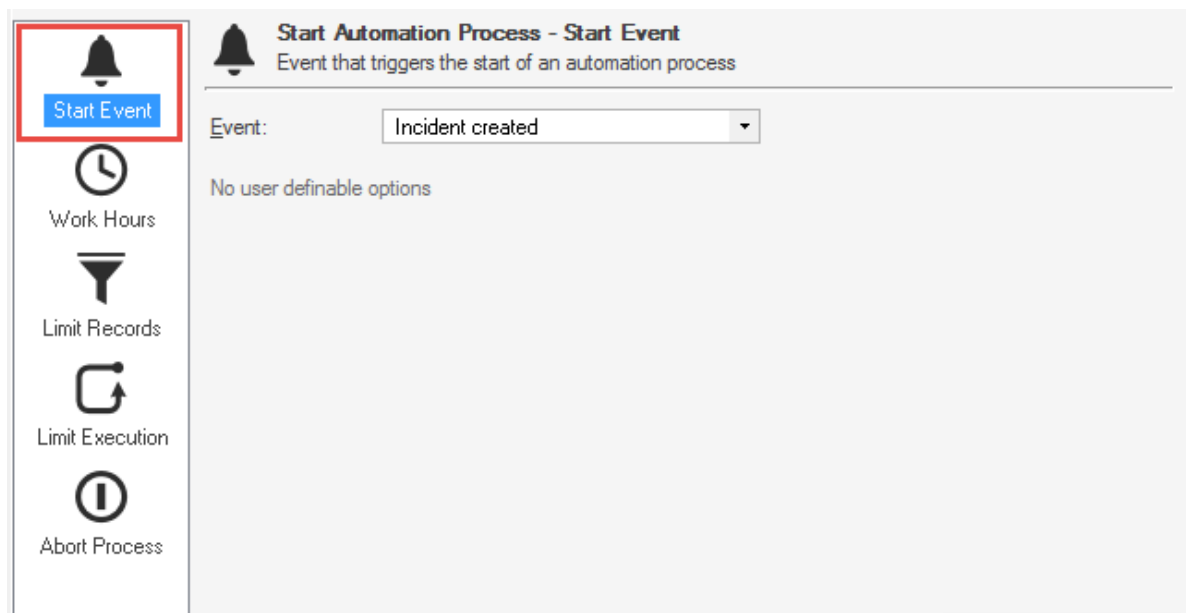
3. Select an event to use to activate the Automation Process.

Event Type	Description
<Business Object> Created	The Automation Process will begin when a <Business Object> is created.

Event Type	Description
<Business Object> Changed	Any Change: The Automation Process will begin if any change is made to the <Business Object>. Field Changed: The Automation Process will begin if the selected Field is altered. **Note:**You have the option 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 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. **<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.
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. Click OK.

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. Click the Work Hours page in the left pane of the Current Step Details section.

   The Start Automation Process - Work Hours page opens.

3. Define Work Hours properties.

   Note: 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.

Note: If you select Working Hours, you must also select specific **Business Hours** using the drop-down. To create new Business Hours for the Automation Process, select the Ellipses button to access the Business Hours Manager.

4. Click OK.

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. Click the Limit Records page in the left pane of the Current Step Details section.

   The Start Automation Process - Limit Records page opens.

3. Limit records based on Query: Only records for which the Query (Search Group) condition is true will cause the Action to be executed when the Event occurs.
   a. Select the Query check box.

      The Query drop-down and Ellipses button become active.

   b. Click the **Ellipses** button [...] to open the Search Group Manager, where you can select an existing Search Group or create a new Search Group.

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 drop-down and Value drop-down become active.

   b. From the Field drop-down, select a **Field**.

      c. From the Value drop-down, 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, Ellipses button, and Custom Expression button become active.

       b. Define the Expression:

           Select an existing Expression: Click the Ellipses button to open the Expression Manager, and then select an **Expression**.

       c. Create a Custom Expression: Click the Custom Expression button and define a Custom Expression.

6. Click OK.

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. Click the Limit Execution page in the left pane of the Current Step Details section.

   The Start Automation Process - Limit Execution page opens.
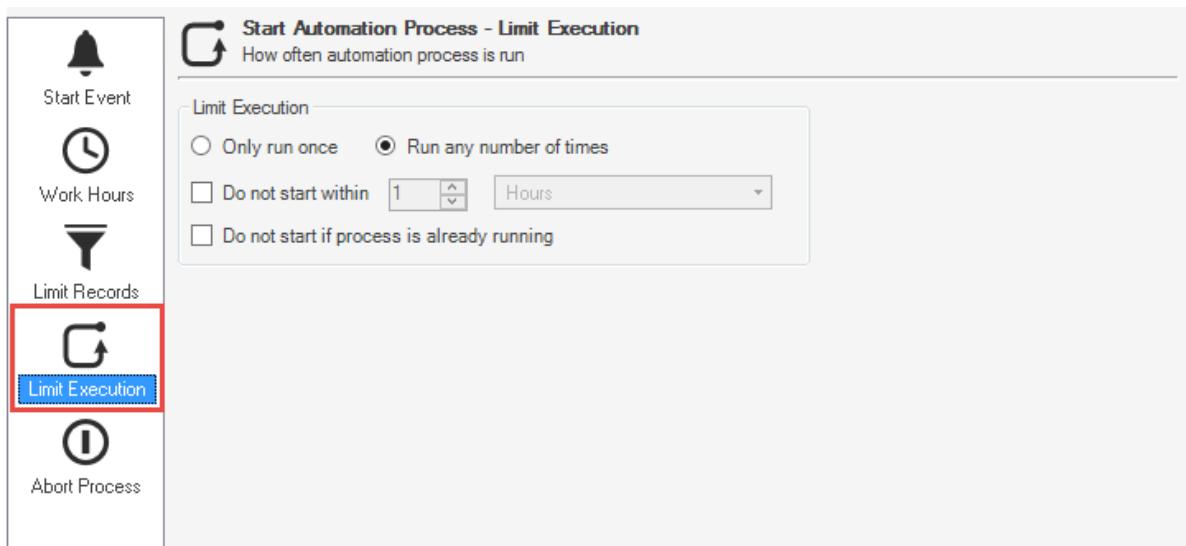
3. Define execution properties:

   Only run once: Select the radio button to run the process the first time the trigger event or Action occurs.

   Run any number of times: Select the radio button 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 the check box to stop the process from running if the trigger event or Action occurs while the Automation Process is already running.

4. Click OK.

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. Click the Abort Process page in the left pane of the Current Step Details section.

   The Start Automation Process - Abort Process page opens.

3. Define when the process should be aborted:
   a. 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 Incident is closed.

   b. 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 the radio button to check if the abort process criteria is true before each step takes place.

After each step executes: Select the radio button to check if the abort process criteria is true after each step takes place.

4. Click OK.

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. When you define time and event criteria, you define:

- 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.

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.

Good to know:

- As you drag the icon onto the Designer Board, the locations where the icon can be dropped highlight as the cursor passes over them.

To define Automation Process Visual Workflow Process time options:

1. Open the Automation Process Visual Workflow Process Designer.

2. Click-and-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, etc.) and/or the specific time before or after another another Calendar item

    - SLA Based: Select a defined SLA to use for the calculation.

4. Click OK.

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.

Good to know:

- As you drag the icon onto the Designer Board, the locations where the icon can be dropped highlight as the cursor passes over them.

To define Automation Process Visual Workflow Process Event options:

1. Open the Automation Process Visual Workflow Process Designer.
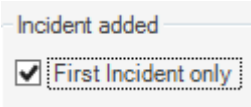
2. Click-and-drag the **Wait for Event icon** onto the Designer Board.

   The Wait for Event - Event page opens in the Current Step Details section of the designer.

3. From the **Wait from** 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\>. Field Changed: The Automation Process will begin if the selected Field is altered. **Note:** You have the option 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 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. **\<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.
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. Click 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, etc.) and/or the specific time before or after another another Calendar item

    - SLA Based: Select a defined SLA to use for the calculation.

    - No Time Limit. (Default)

6. Click 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.

Good to know: As you drag the icon onto the Designer Board, the locations where the icon can be dropped highlight as the cursor passes over them.
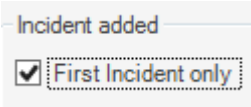
To define Automation Process Visual Workflow Process Event options:

1. Open the Automation Process Visual Workflow Process Designer.

2. Click-and-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** 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> Changed	Any Change: The Automation Process will begin if any change is made to the <Business Object>. Field Changed: The Automation Process will begin if the selected Field is altered. **Note:** You have the option 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 is the Field changes from one value to another.
<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. **<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.
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. Click 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 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, etc.) and/or the specific time before or after another another Calendar item

    - SLA Based: Select a defined SLA to use for the calculation.

    - No Time Limit. (Default)

6. Click 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 (ex: One-Step Manager).

- When you click-and-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. Click-and-drag one or more **Actions** to the Designer Board:

Run One-Step: Run an One-Step when the defined time or event occurs.

Send E-mail: Send an e-mail when the defined time or event occurs to inform a User that the event has taken place. Edit the e-mail content by clicking the Send E-mail 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 clicking the Send Tweet link in the Execute Action field.

Update Bus Ob: Update a Field in a Business Object. Edit the Business Object by clicking the Update Business Object link in the Execute Action field.

Create Child: Create a Child Business Object (ex: Journal, Task, Customer Survey). Edit the Child Business Object by clicking the Create Child Business Object link in the Execute Action field.

Queue Action: Add the Record to a specific Queue.

Jump to Step: Jump to a specific step in the Automation Process. Select the step using the drop-down.

Jump to End: End the Automation Process if the previous step takes place.

3. Click OK.

Configuring Automation Processes

Complete the following procedures to configure Automation Processes. Configuration procedures are completed in CSM Administrator.

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 Server functionality.

Advanced Automation Processes

Information on the following topics is intended for advanced Users (2nd Level Support, 3rd Level Support) and system administrators:

- Automation Process Manager
- Open the Automation Process Editor

Good to know:

- CSM provides two tools that can be used to manage Automation Processes. Use the Automation Process Editor to work with Automation Processes (create, edit, delete, etc.) outside of a Blueprint (typical use). Use the Automation Process Manager to work with Automation Processes (create, edit, delete, etc.) within a Blueprint (required when adding an Automation Process to a mApp).

Use the Automation Process Manager to:

- View/Run an Automation Process.
- 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.
- Search for an Automation Process.
- Organize Automation Process.
- Copy an Automation Process.
- Import/export an Automation Process.
- Find Automation Process dependencies.

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), by clicking **Managers>Automation Processes**.
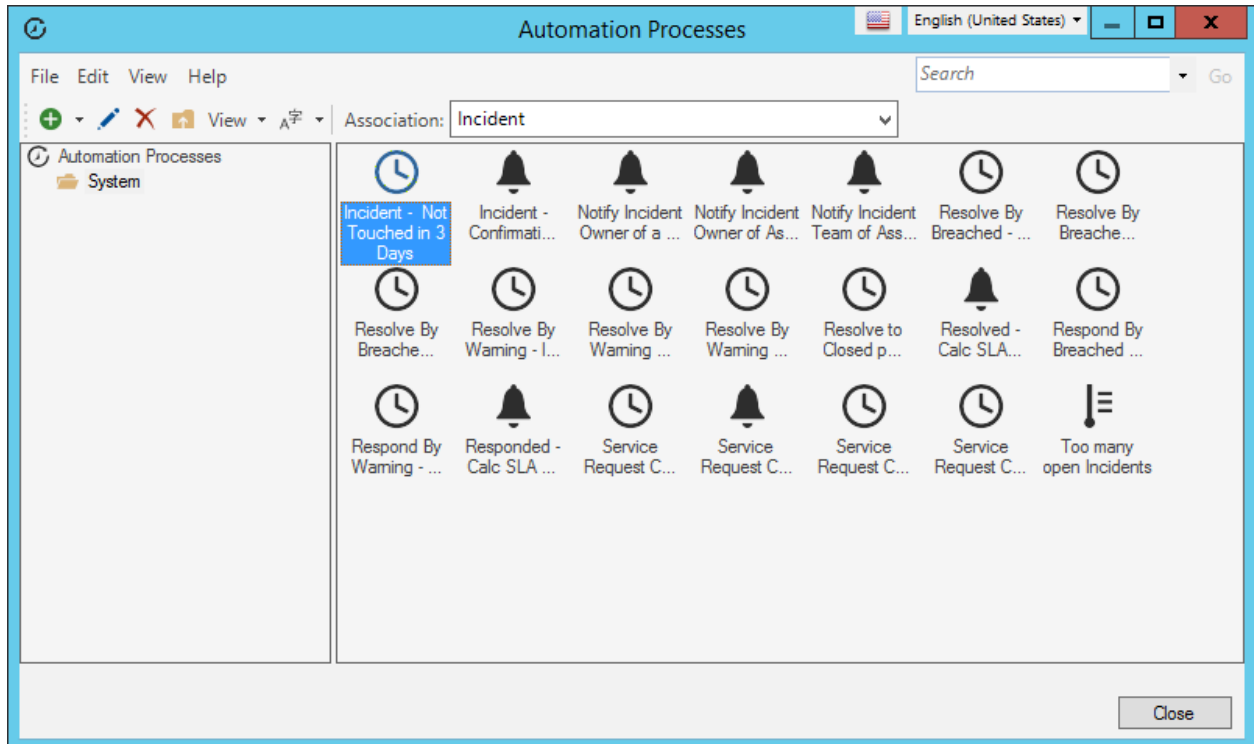
Good to know:

- 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.

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).

About the Scheduler

The following actions are available 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**: Runs a selected One-Step.
- **Portal Credentials**: Creates Portal login credentials for Customers.
- **Publish Blueprint**: Publishes Blueprints to your CSM system.
- **Report**: Runs a selected Report.
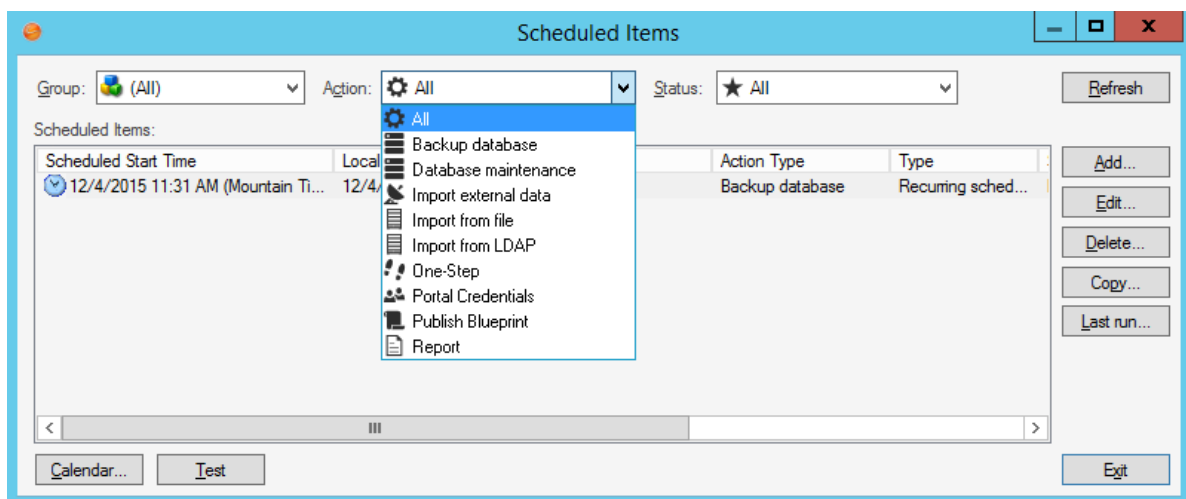
Items can be scheduled to run on a recurring basis (daily, weekly, monthly, yearly) or one-time only. The Scheduler operates within the timeframe of defined Business Hours and can be accessed through CSM Administrator.

The Scheduler runs in coordination with the Scheduling Server (service), which is installed with the CSM Server Installer.

Scheduler Good to Know

- Use the Scheduler window in CSM Administrator (CSM Administrator>Scheduling>Edit Schedule) to use and manage Scheduled Items.
- The Scheduler runs in coordination with the Scheduling Server (service), which is installed with the CSM Server Installer.
- Start, Stop, or Restart the Scheduling Server using the Server Manager or Service Monitor.
- 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

- A nightly database backup is recommended 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 Cherwell Service Management Administrator runs.

Using the Scheduler

When using the Scheduler, Users can:

- Pause/resume the Scheduling Server.
- View Scheduled Items.

Opening the Scheduler Window

To open the Scheduler window from the CSM Administrator main window, click the Scheduling category, and then click the Edit Schedule task.

Scheduler Window

Use the Scheduler window to:

- **View** a list of Scheduled Items, filtered by:
  - Group: View Scheduled Items for a particular Scheduler.
  - Action: View Scheduled Items by Action type.
  - Status: View Scheduled Items by completion status (Pending, Completed, Not Completed).
- **Add, edit, delete, and copy** Scheduled Items.
- **Refresh** Scheduled Items and their statuses. If items are running, the Refresh button can be used to watch the statues change from pending, to running, to complete.
- View the **Last Run** of a Scheduled Item to see the last time a recurring item was run, its completion status, or any errors.
- **View error**(s) of a Scheduled Item that was not completed as expected.
- View the **Calendar of Scheduled Items** to see all of the items scheduled for a particular day.
- **Test** a Scheduled Item to ensure all information is available for the item to run regularly
.
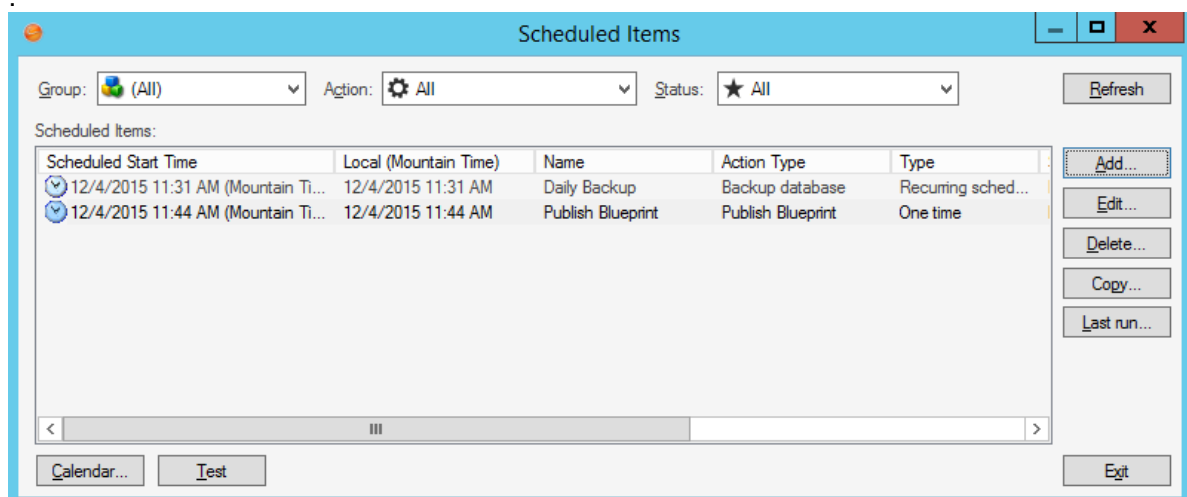
Pause/Resume the Scheduling Server

Use the Pause/Resume Scheduler task (CSM Administrator) to temporarily pause and resume the Scheduling Server (service).

Notes: Completing this process affects all enabled Scheduled Items. Also, even while the Scheduling Server is paused, Events will be generated by the system. When the service is resumed, all Scheduled Items are processed.
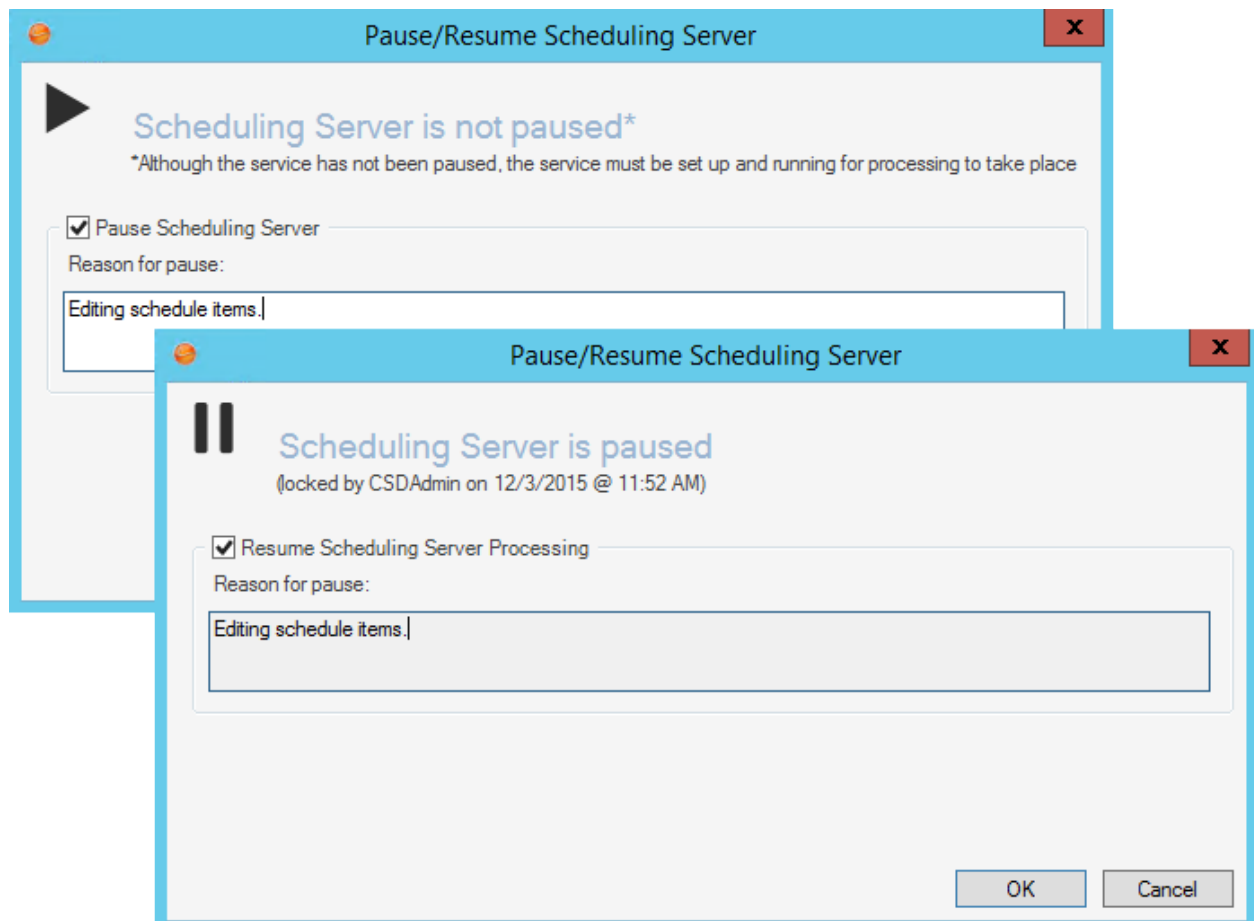
To pause/resume the Scheduling Server:

1. In the CSM Administrator main window, click the Scheduling category, and then click the Pause/Resume Scheduler task.

2. Pause or resume the Scheduling Server:
   a. Pause Scheduling Server: Select this check box to pause the Scheduling Server processing. You must provide a reason for pausing the server in order to complete the process.

b. Resume Scheduling Server: Select this check box to resume Scheduling Server processing.

3. Click OK.

View Scheduled Items

You can view Scheduled Items in a few ways:

- View the details of a specific Scheduled Item.
- View a Calendar of Scheduled Items to see all items scheduled for a specific day.
- View Errors of a Scheduled Item 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, click the Scheduling category, and then click the Edit Schedule task.

   The Scheduler window opens.
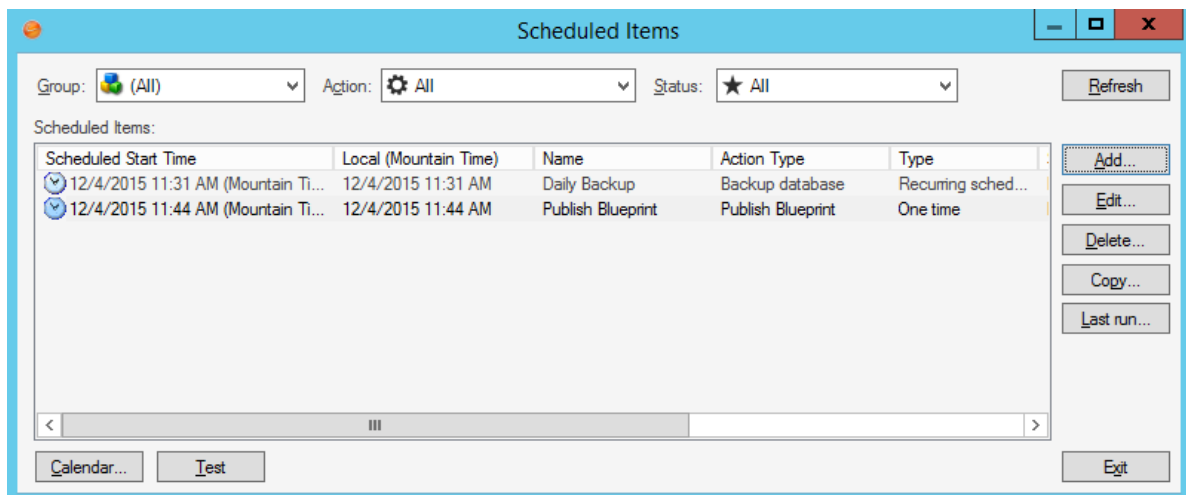
2. Select a **Scheduled Item**, and then click the View button.

   The Scheduled Item Properties window opens.

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, click the Scheduling category, and then click the Edit Schedule task.

   The Scheduler window opens.
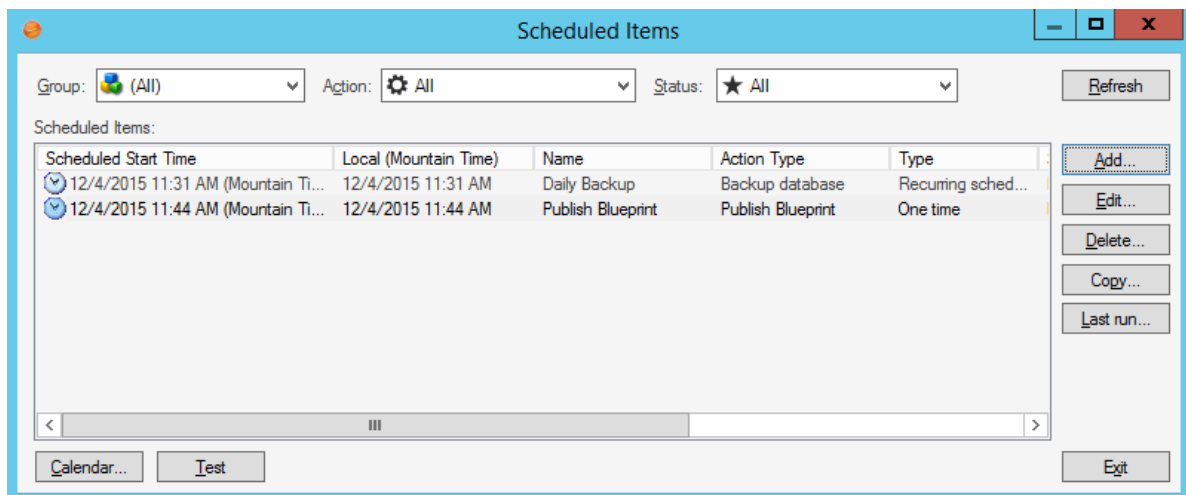
2. Click the Calendar button.

   The Calendar of Scheduled Items opens.
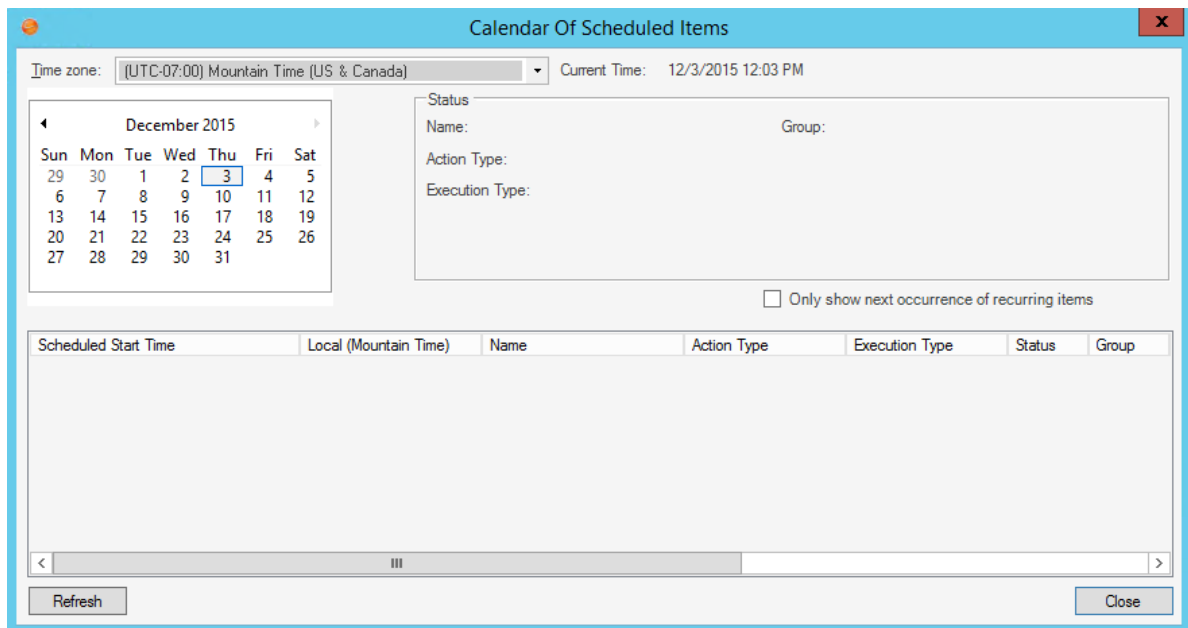
3. Click a **date** in the Calendar to view a list of the items scheduled for that day.

4. (Optional) Click the Refresh button to update the status of the Scheduled Items for that particular day.

   Note: 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 check box.

5. Click Close to close the window.

View Errors of a Scheduled Item

When a Scheduled Item encounters an error, it will not be scheduled again because it is likely in a state where it cannot run (ex: Shortage of disk space, missing Report, etc.). You can view errors of a Scheduled Item to investigate the cause of the error.

To view the errors of a Scheduled Item:

1. In the CSM Administrator main window, click the Scheduling category, and then click the Edit Schedule task.

   The Scheduler window opens.
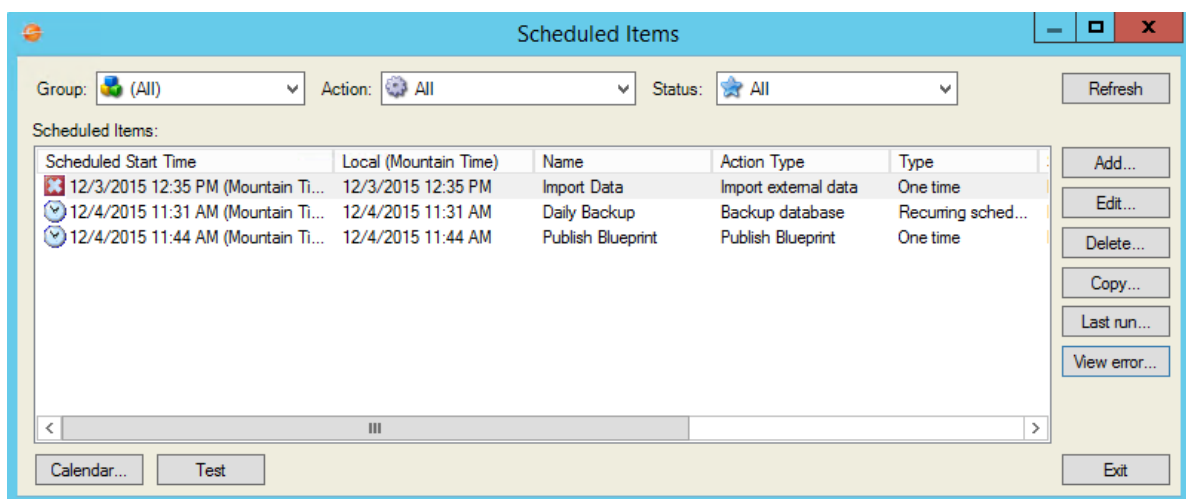
2. Select an item with an **Error** status and click View Error.
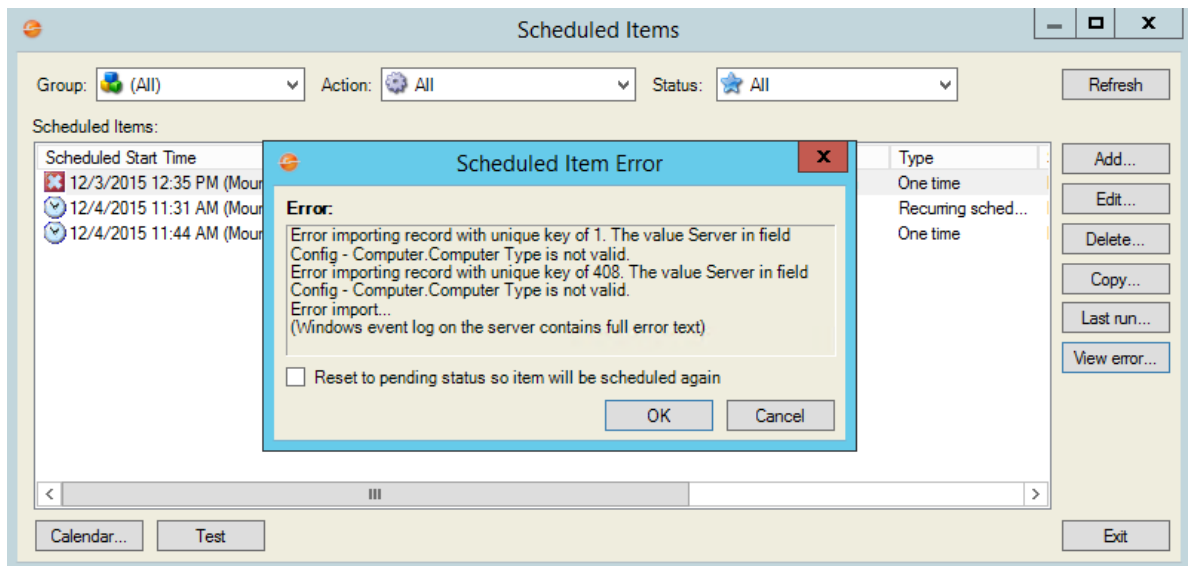
The Scheduled Item Error window opens to provide details on the error(s) that occurred when the Scheduler attempted to run the Scheduled Item.

Note: If a Scheduled Item has an error, it will not be scheduled to run again. Select the Reset to pending status so item will be scheduled again check box to ensure that the Scheduled Item will run after any errors have been resolved.

Create a Scheduled Item

Use the Schedule Item Properties window (accessed from within the Scheduler window in CSM Administrator) to create a Scheduled Item. When you create a Scheduled Item you define the following properties:

- **General**: Name and description.
- **Schedule**: Date/time the Scheduled item is scheduled to run.
- **Action**: Action the Scheduled Item runs (ex: Backup Database).
- **Error Handling**: Options for handling errors that prevent a Scheduled Item from running.

To create a Scheduled Item:

1. In the CSM Administrator main window, click the Scheduling category, and then click the Edit Schedule task.
2. Click the Add button.

   The Schedule Item Properties window opens.

3. Define Scheduled Item properties:
   a. Define general properties for a Scheduled Item.

   b. Define schedule properties for a Scheduled Item.

   c. Define action properties for a Scheduled Item.

   d. Define error handling properties for a Scheduled Item.

4. Click OK.

Define General Properties for a Scheduled Item

Use the General page in the Scheduled Item Properties window to define general properties for a Scheduled Item.

To define General properties for a Scheduled Item:

Schedule Group	If only one Schedule Group is used, leave **Default** selected. If multiple schedulers are needed, click the Ellipses button to create the different schedule groups.
Name	Provide a name for the Scheduled Item.
Description	Provide a description for the Scheduled Item.

Define Schedule Properties for a Scheduled Item

Use the Schedule page in the Scheduled Item Properties window to define the schedule for an item, inclduing:

- **One Time or Recurring**: Whether a Scheduled Item will run once or multiple times.
- **Scheduled time**: Start date and time for the Scheduled Item.
- **Recurrence**: Daily, Weekly, or Monthly.
- **Range of Recurrence**: Number or date range for a Scheduled Item's recurrence.

> **Note:** The Scheduled Item Properties window is accessed from within the Scheduler window in CSM Administrator.

To define Scheduling properties for a Scheduled Item:

One time: Select this radio button to schedule the item to run one time. .

Start Time	Specify the time using the arrow buttons or providing the time (ex: 12:30 AM).
Time Zone	Use the drop down to specify a time zone or specify to have the schedule item run on the same time zone as the schedule server. **Note:** The Time Zone feature should only be used with a three-tier connection. A two-tier connection causes undesired results.

Recurring: Select this radio button to schedule the item to run on a recurring basis.

Schedule Time	
Start time	Specify the time using the arrow buttons or providing the time (ex: 12:30 AM).
Time zone	Use the drop down to specify a time zone or specify to have the schedule item run on the same time zone as the schedule server. **Note:** The Time Zone feature should only be used with a three-tier connection. A two-tier connection causes undesired results.
Recurrence	Select how often to run the Scheduled Item.
Hourly	Run the Scheduled Item every X number of hours (ex: Every 24 hours).
Daily	Run the Scheduled Item every X number of days (ex: Every 7 days) or every weekday.
Weekly	Run the Scheduled Item every X number of weeks on specific days (ex: Monday, Wednesday, and Friday).
Monthly	Run the Scheduled Item on a specific day of the month (ex: Day 1 of every month) or on a specified week/day of the month (ex: First Monday of every 1 month).
Yearly	Run the Scheduled Item on a specific date (ex: Every January 1) or on a specific day of the year (ex: First Monday of June).

Range of recurrence:	Schedule the amount of time to run a recurring Schedule Item.
No end date	The recurrence continues indefinitely.
End after	The recurrence ends after a defined number of occurrences. Specify the **number** of occurrences.
End by	The recurrences end by a certain date. Then, specify an **end date**. **Note**: If the item is scheduled to run on then end date, it will run for the last time on this date.

Define Action Properties for a Scheduled Item

Use the Action page in the Scheduled Items Properties 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.

Note: The Scheduled Item Properties window is accessed from within the Scheduler window in CSM Administrator.

To define Action properties for a Scheduled Item:

1. In the CSM Administrator main window, click the Scheduling category, and then click the Edit Schedule task.
2. Click the Add button.

   The Schedule Item Properties window opens.

3. Click the Action page.
4. Select an **Action**,
5. Define the properties for the selected Action:
   Backup Database Options: Exports a selected CSM database to a compressed Cherwell Archive Repository (.czar) file.

   Database Maintenance Options: Performs selected database maintenance operations (ex: Rebuilding the Full-Text catalog, Rebuilding Indexes and shrinking SQL logs on a scheduled basis

   Import External Data Options: Imports data from external databases (ex: Active Directory) into CSM.

   Import from File Options: Imports data from comma separated value (.csv) files into CSM.

   Import from LDAP Options: Imports LDAP records (ex: Customer lists) into CSM.

   One-Step Options: Runs a selected One-Step.

   Portal Credentials Options: Creates Portal login credentials for Customers.

   Publish Blueprint Options: Publishes Blueprints to your CSM system.

   Report Options: Runs a selected Report.
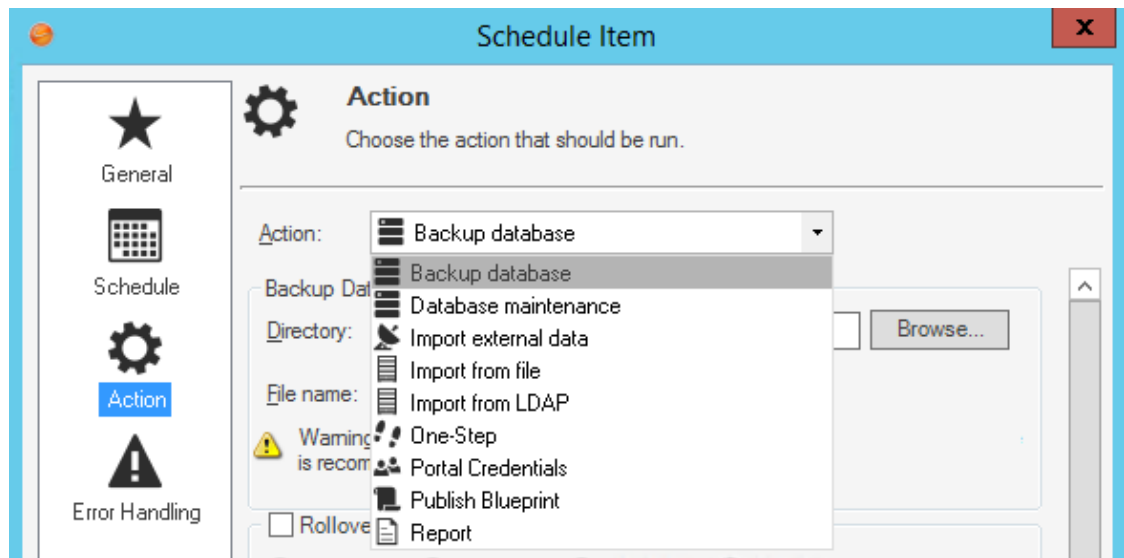
Define Backup Database Action Options

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.

To Define a Backup Database Action:

1. In the CSM Administrator main window, click the Scheduling category, and then click the Edit Schedule task.

2. Provide the following settings as they apply:

Option	Description
Directory	Provide the directory name or click the Browse button to select a directory for where database backup files will be stored. **Note:** The directory must be available on the machine where the Scheduler runs. A UNC name is recommended.
File Name	Provide a file name for the database backup.
Rollover Files	Define the frequency of database backup files. **Note:** If you do not roll over backup files, a new file will be created for every database backup. The date will be appended to the File Name you entered (ex: Cherwell20090305_093501.czar). **Nightly**: Uses the same file every time the backup is run. **Weekly**: Appends the day of the week to the backup files (Sun, Mon, Tue, Wed, Thu, Fri, Sat). This means there will be a maximum of seven files. For example, if you run a database backup every day of the week, you will have seven files (one for each day of the week). If you run a backup every Monday, Wednesday and Friday, you will have three files. These same files are used every week. **Monthly**: Appends the day of the month appended to the backup files (ex: 01-31). This means there will be a maximum of 31 files. The same files are used every month. **Yearly**: Appends the month and day to the backup files (ex: Jun28). This means there will be a maximum of 365 files used (366 for leap years). The same files are used every year.

Option	Description
Export Type	Export a single Business Object: Select this check box to export a selected Business Object to the database backup file when the database backup is run. Export entire system: Select this check box to export your entire database to the backup file when the database backup is run.
Content	The options available in this section depend on the selected export type. Export a Single Business Object: Select the Business Object drop-down Export Entire System: **Export all data:** Exports all SQL Server tables (ex: Field names and sizes) and data. **Tip:** Use this option to create a .czar file to troubleshoot problems that are not related to Automation Processes or Scheduled Items. **Export table structure only:** Exports all SQL Server tables without any data. **Tip:** Use this option to create a .czar file that excludes your confidential company data. **Export structure and lookup table data:** Exports SQL Server tables for all Major and Supporting Objects, as well as tables AND data for Lookup Objects (validation tables). **Tip:** Use this to create a .czar that excludes your confidential data but includes values from Lookup tables (because typically, Lookup tables do not contain confidential data and can be used to troubleshoot problems with validation and relationships). **Exclude attachments:** Exports the Attachment table but not the Attachment data within the table. **Tip:** Use this option to create a .czar file to troubleshoot problems that are not related to Automation Processes or Scheduled Items. **Exclude automation data:** Exports the Events and Scheduler tables, but not the data within the tables. **Tip:** Use this option to create a .czar file to troubleshoot problems that are not related to Automation Processes or Scheduled Items.

Define Import from LDAP Action Options

Use the Scheduler's *Import from LDAP Action* to import LDAP records (ex: Customer lists) into CSM on a scheduled basis. When you schedule an Import from LDAP Action, CSM launches the Active Directory Import Wizard to help you define the import. If you are also scheduling Portal Credential updates through the Scheduler, LDAP data must be imported first.

Note: Biweekly LDAP imports are recommended.

Note: To schedule an LDAP import, see Integrating CSM with Microsoft Active Directory for more information.

To define an Import from LDAP Action:

Click the Setup button to be taken to the Active Directory Import Wizard. For more information, see Import Active Directory into Business Objects for Map the Customer Object to a Directory Service.

Define Database Maintenance Action Options

Use the Scheduler's *Database Maintenance Action* to perform selected database maintenance operations on a scheduled basis. When you schedule a Database Maintenance Action, you define which database maintenance operations to perform:

- Full-Text Search maintenance: Rebuilding Full-Text Search catalog.

- Index maintenance: Rebuilding Indexes and shrinking SQL logs. Database maintenance requires re-indexing database tables.

- Queue and User account maintenance: Refreshing Queue status and removing unused User accounts.

> **Note:** Schedule your database maintenance operations for after business hours because it can interrupt performance. For example, rebuilding the SQL Server Full-Text catalog will prevent Users from doing Full-Text searches while the catalog is rebuilding. For more information about database maintenance, refer to Perform Database System Maintenance.

To define a Database Maintenance Action:

Full-text Search	**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.
Manage Indexes	**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, click the Select button to select which Business Objects to re-index. **Note**: By default, all Business Objects are selected. Uncheck Business Objects to exclude them from reindexing, or select Clear All to uncheck 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. **IMPORTANT**: Consult with your Administrator before scheduling this option. If in doubt, do not use this feature unless you run into problems.

Data	**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.

Define Import External Data Action Options

Use the Scheduler's *Import External Data Action* to import data from external databases (ex: Active Directory) into CSM on a scheduled basis. When you define an Import External Database Action, CSM launches the External Data Import Wizard to help you define the import.

Note: You must have either a mapped CSM Business Object or an External Business Object to hold the external data that is imported.

To define an Import External Data Action:

Click the Setup button to open the External Data Import Wizard. For more information, see Import External Data into a Business Object.
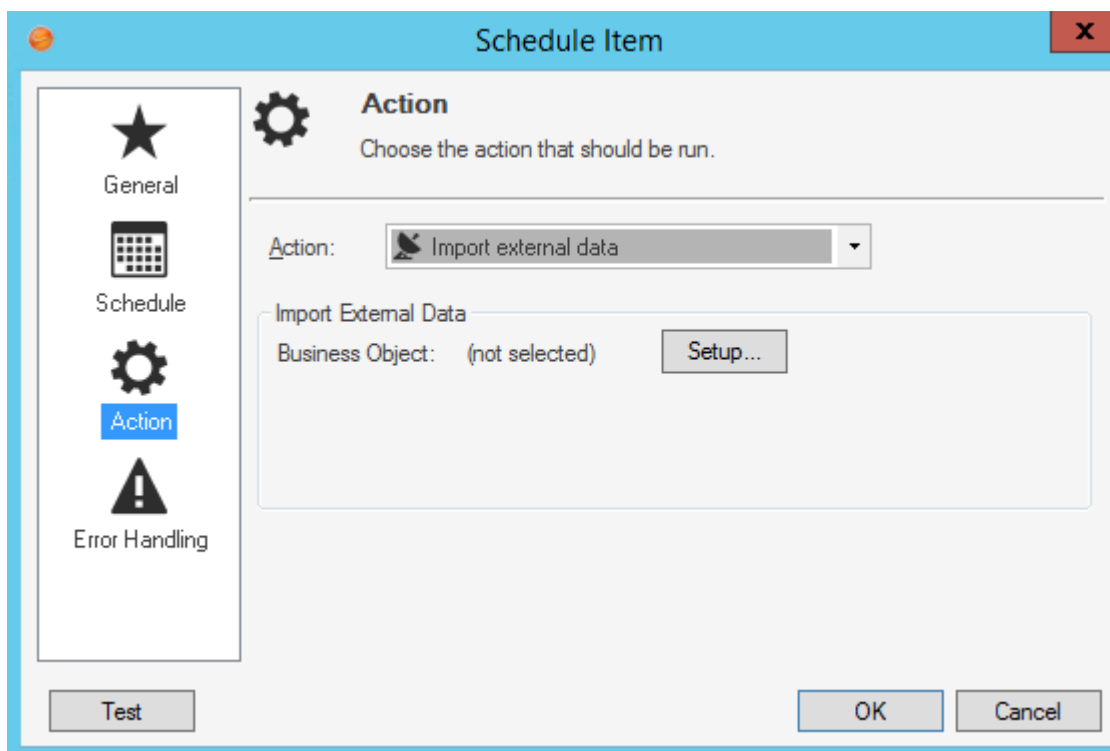
Define Portal Credentials Action Options

Use the Scheduler's *Portal Credentials Action* to create Portal login credentials for Customers on a scheduled basis.

Note: To import Users from LDAP and then create 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.For more information about Portal Credentials, refer to Create Portal Login Credentials.

To define a Portal Credentials Action:

Search group	Click the Ellipses button to open the Search Group Manager, and then select an existing **Search Group** or create a new one that contains the Customers who need Portal credentials (ex: Internal Customers).
Field with Login ID	In the drop-down, select the field from the Customer Business Object that contains the Customers' login IDs.
Customer group	In the drop-down, select the **Security Group** the Customers belong to. This defines the security rights for the Portal Credential action. Selecting the Portal Workgroup Manager Group offers greater control than selecting the Portal Customer Group.
Password	Randomly generate a password for each customer: Select this radio button to assign and e-mail a random password to each Customer. If a Customer does not have an e-mail address, she will not be notified. Set password the same for all: Select this radio button to assign the same password to all Customers, and then provide the password to use. Password is value from field: Select this radio button to use the value from a field as the password, and then select the field in the drop-down. Set Login ID field as Windows/LDAP login: Select this radio button to use Windows/LDAP login credentials, and then select an option for determining a domain if the login ID does not include one: • **Attempt to determine domain from LDAP distinguished name:** Find the Customer domain using the stored Distinguished Name and parsing out the Domain Component (DC). • **Attempt to use domain associated with LDAP customer mapping:** Use the domain stored in the Customer record-mapped LDAP definition. • **Use this domain:** Enter a default domain for the Login ID. **Note**: LDAP credentials must be configured to use this option. For more information about configuring LDAP, see Enabling Authentication for Users or Enabling Authentication for Customers.

Account details	**Account locked:** Select this check box to lock the Customer's account (preventing them from logging in to the Portal). **Note:** A Customer can be automatically locked out of the system, too, if there are too many failed login attempts (depending on system settings). **Password never expires:** Forgo 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:** Restrict a Customer from changing their password. If a password reset is required by the system, the system administrator must reset the password. **User must reset password at next login attempt:** Restrict a Customer 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. **Tip:** This is an immediate reset. Use this setting if the Customer forgot her password. **Password reset date:** Prompts a Customer to change their password on a specific date. Click the Date Selector button to select a reset date.
E-mail	**E-mail customer new credential information:** E-mail new credential information to Customers, and then click Edit E-mail to edit the Customer Credentials E-mail message. **Tip:** To make this the default e-mail message that is used for all Customer e-mails, click Make Default. **Skip customers with no e-mail address:** Skip Customers with no e-mail address (e-mails will not be sent to them). Leave this check box unchecked if you want an error to be flagged when a Customer does not have an e-mail address.
Skip customers who already have login IDs assigned	Include only new Customers. Leave it cleared to include all Customers. It is recommended to Select this check box so IDs are not reassigned for existing users.

Schedule Item

Action

Choose the action that should be run.

General

Schedule

Action

Error Handling

Action: 👥 Portal Credentials ▾

Search group: Internal Customers   [...]

Field with Login ID: First name ▾

Customer group: Portal Workgroup Manager ▾

🔒 Password

○ Randomly generate a password for each customer

◉ Set password the same for all: [　　　　　　　]

○ Password is value from field: [　　　　　　　▾]

○ Set Login ID field as Windows/LDAP login

    If Login ID does not include a domain

     ☐ Attempt to determine domain from LDAP distinguished name

     ☐ Attempt to use domain associated with LDAP customer mapping

     ☐ Use this domain: [　　　　　　　]

Account details

☐ Account locked

☐ Password never expires   ☐ User must reset password at next login

☐ User cannot change password   ☐ Password reset date: [　　　　　　　]

✉ E-mail

☐ E-mail customer new credential information   [Edit e-mail...]

☐ Skip customers with no e-mail address

☐ Skip customers who already have login IDs assigned

[Test]   [OK]   [Cancel]

Define Publish Blueprint Action Options

Use the Scheduler's *Publish Blueprint Action* to publish Blueprints to your CSM system on a scheduled basis. When you schedule a Blueprint Publish Action, you define:

- Which Blueprint to publish.
- Whether or not to back up your database before the publish.

For more information about Blueprints, refer to the Blueprints documentation.

To define a Blueprint Publish Action:

Publish Blueprint	Use the Browse button to locate the Blueprint to publish. This directory must be available on the machine where the Scheduler runs. A UNC name is recommended.
Backup Database	Backup the database before the Blueprint publish.
Directory	Directory: Provide the directory name, or click the Browse button to select a directory where the database backup file will be stored.
File Name	File Name: Provide the file name to use for the database backup file.
Append date/time to file name	Append the current date and time to the file name. This ensures that you do not overwrite previous backups with the same name by adding the most current date/time stamp to the backup file name
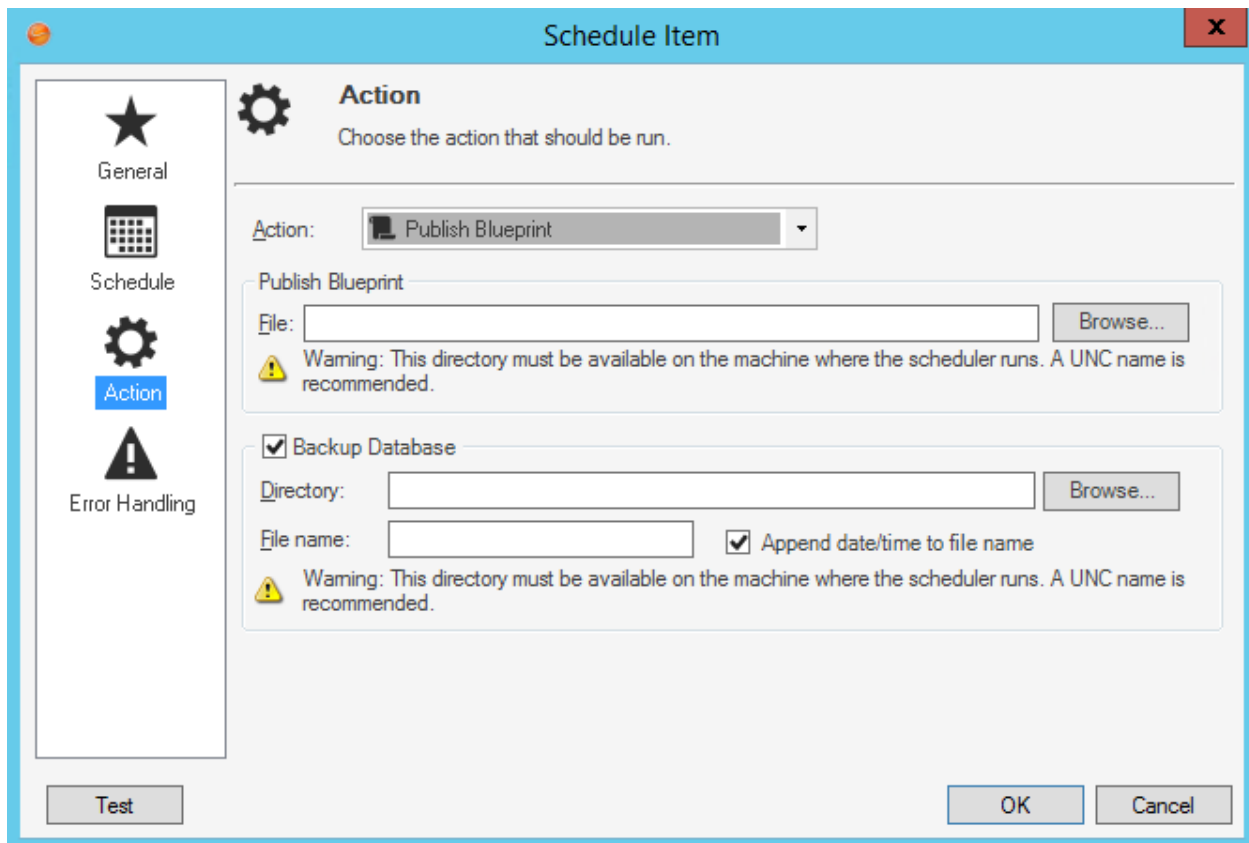
Define Import from File Action Options

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 schedule an Import from File Action, CSM launches the Stored Import Definition Manager to select an existing CSV Stored Import or create a new CSV Stored Import to run.

For more information about CSV files, see Managing CSV Data.

Define One-Step Action

Use the Scheduler's *One-Step Action* to run a One-Step on a scheduled basis. For example, run a One-Step to send an e-mail indicating that another Scheduled Item is complete (ex: Database backup was successfully completed, Report was run, etc). Select the One-step to run when scheduling a One-Step Action. For more information about One-Steps, see the One-Steps documentation.

To define a One-Step Action:

Run One-Step: Select the One-Step from the drop down or click the Ellipses button to open the One-Step Manager, and select an existing One-Step or create a new One-Step.
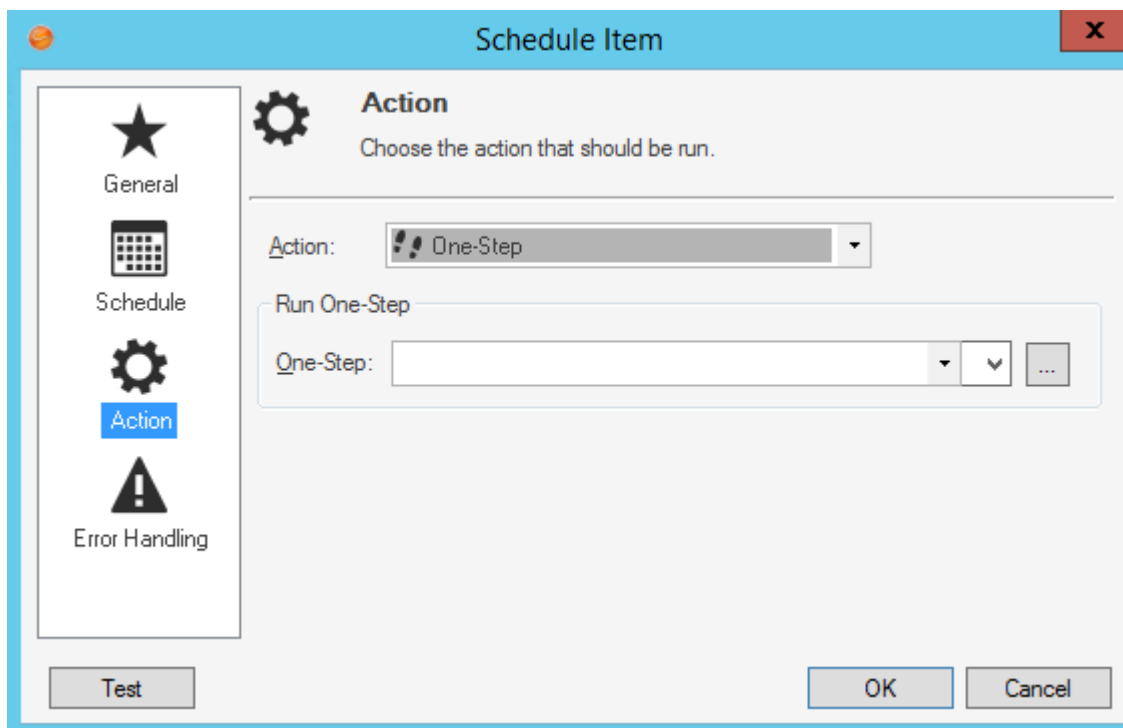
Define Report Action Options

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 (ex: Date range, priorities, etc.). Consider creating one Report with different parameters (ex: Prompts) so that 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, you are prompted to set the values that the Scheduler will pass to the Report when you schedule the Report.

To automatically print a Report, create a One-Step that prints the Report. Then use the Scheduler to run the One-Step.

For more information about Reports, see the Reporting documentation.

To define a Report Action:

Report	Select a most recently used (MRU) Report. Click the Ellipses button to open the Report Manager, and then select an existing Report or create a new Report.
Format	Preferred format for the Report. Available formats include: .pdf, .bmp, .csv, .emf, .xls, .html, .jpeg, .txt, .png, .rtf, and .tiff
Output file	Where to output the Report file: Click the Browse button to locate the Output file for the Report. **Note:** This file must be creatable on the machine where the Scheduler runs. We recommend using a UNC name.
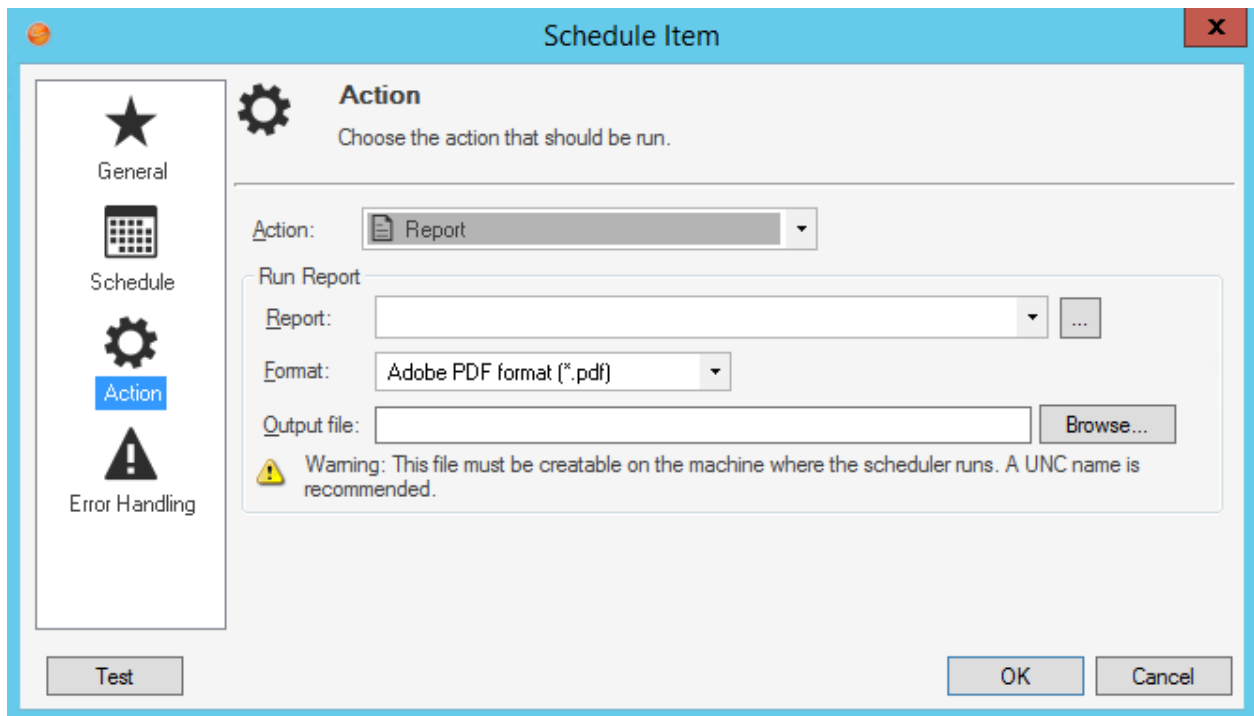
Define Error Handling Properties for a Scheduled Item

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. The Scheduled Item Properties window is accessed from within the Scheduler window in CSM Administrator. From the window:

- Run a One-Step (ex: Run a Report in the event of an error).
- Still schedule next run.

Note: When a Scheduled Item has an error, it will not be scheduled again because it is probably in a state where it cannot run (disk space, missing report, etc.).

To define Error Handling Properties for a Scheduled Item:

1. In the CSM Administrator main window, click the Scheduling category, and then click the Edit Schedule task.

2. Click the Add button.

   The Schedule Item Properties window opens.

3. Click the Error Handling page.

4. Define the error handling operations:

    a. If scheduled items fails run One-Step: Select this check box to run a One-Step in the event of a Scheduled Item error. Select a **One-Step** in the drop-down, or click the Ellipses button to open the One-Step Manager, and then select an existing One-Step or create a new One-Step.

    b. If scheduled item fails, still schedule next run (if recurring): Select this check box to continue a Scheduled Item's original schedule, ensuring that the next run occurs.

5. Click OK.

Configuring the Scheduler

To configure the Scheduler in CSM Administrator, configure Scheduler security rights to determine who can access Scheduler functionality.

Troubleshooting Scheduled Items

If a Scheduled Item does not run as expected, try the following troubleshooting procedures.

Check the Scheduled Items Window

1. In CSM Administrator, click the Scheduling category, and then click the Edit Schedule task.
2. Click the Calendar button.
3. The Calendar Of Scheduled Items window opens.
4. Click the day that the item should have run.
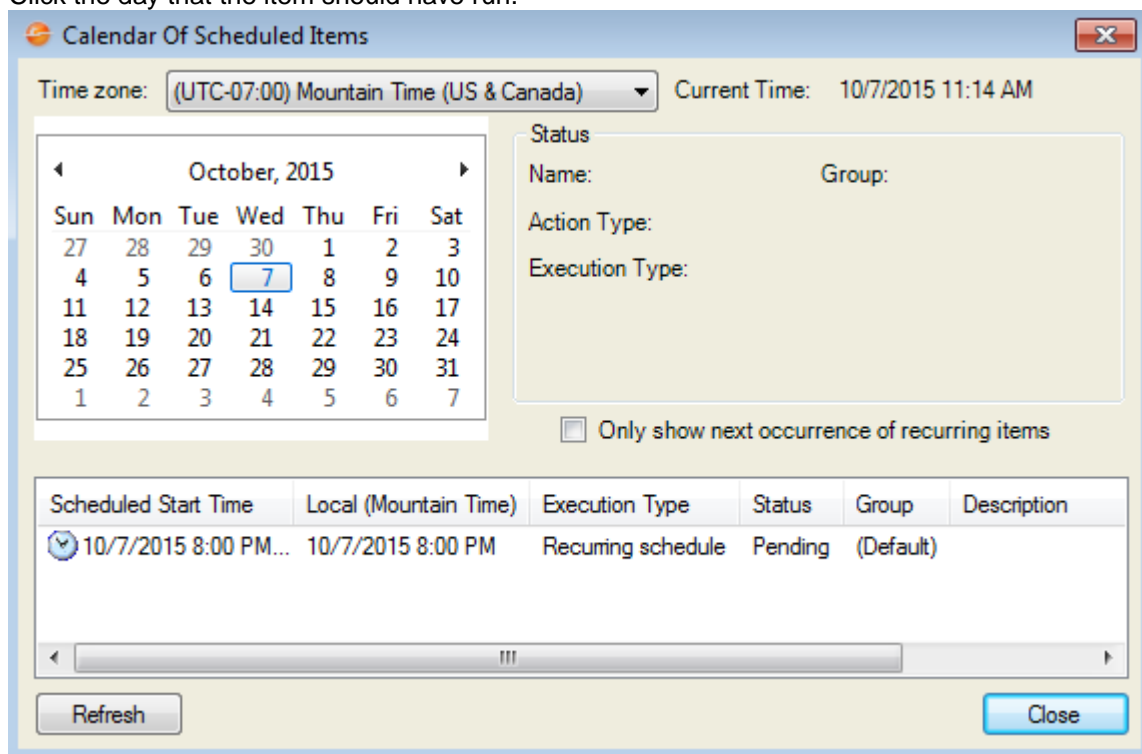
5. Look to see if the Scheduled Item is listed:
   If listed: Check its status. If the status has an error, click the row. The error message shows at the top of the screen. Only the first 250 characters of an error message is stored. If the message is longer than 250 characters, go to the Windows Event Viewer to see the complete error message.

   Note: Go to the machine where the Scheduling Service is installed. From the Windows Start menu select Control Panel, double click on Administrative Tools, and then double-click on Event Viewer.

If the Scheduled Item is not listed and the item is recurring: Go to the date that the item should have run last. Verify that the status on that day was complete and the Scheduled Item did not have an error.

Verify the Scheduling Server is not Paused

1. In CSM Administrator, click the Scheduling category, and then click the Pause/Resume Scheduler task.

2. Verify that there is not a pause. In the example, Henri the User paused the server to change some reports.
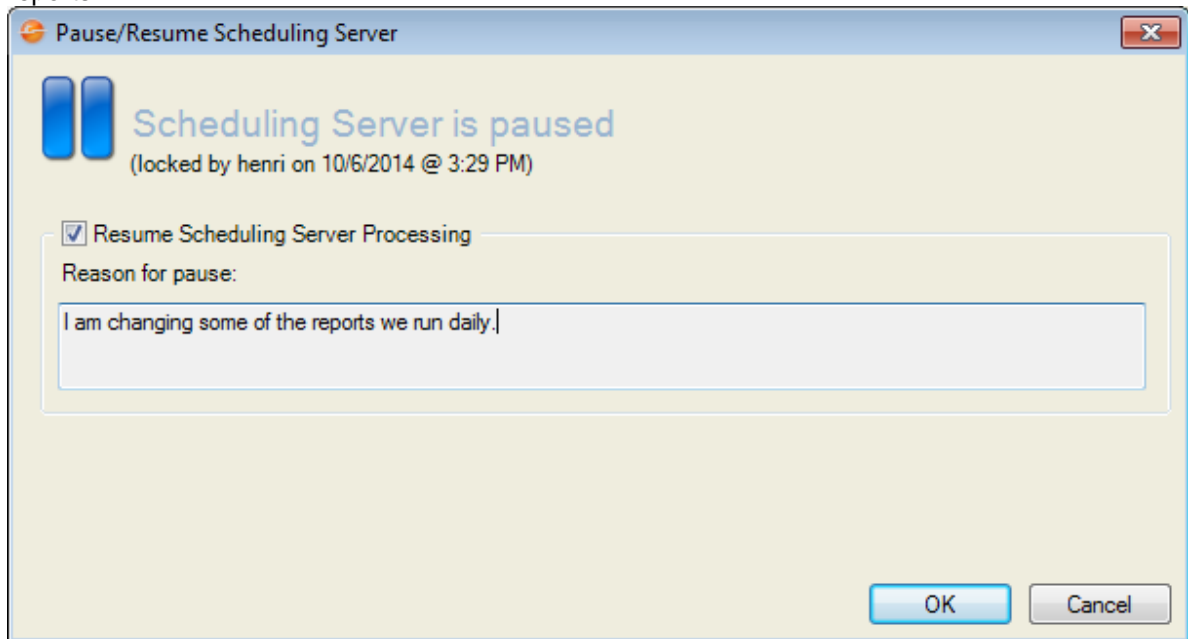
Verify the Scheduling Service is Running

1. Login to the machine where the Scheduling Service is installed.

2. From the Windows Start menu, go to **Control Panel>Administrative Tools>Services**.
   The Services window opens.

3. Verify that the Status column shows Started. If the service has stopped running, check the Windows Event Viewer (Administrative Tools>Event Viewer).
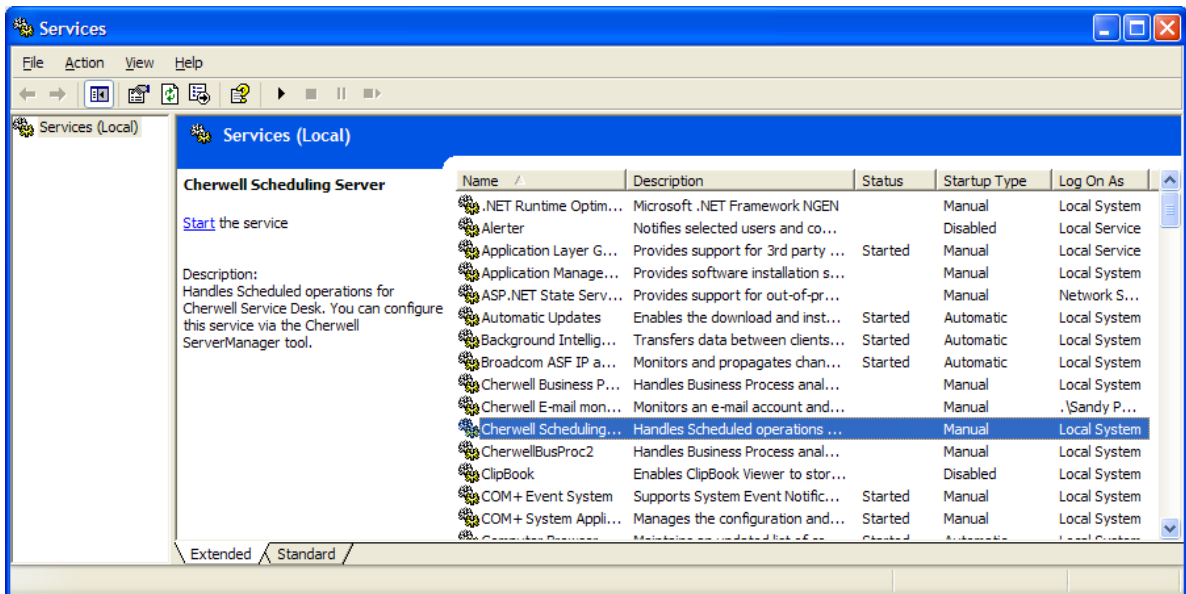
Verify SQL Server Database (Advanced Users Only)

For advanced Users who are comfortable executing SQL queries, run the following queries to see what items are scheduled and their statuses.

One Time Scheduled Items Status

For items that execute One Time use this query, replace [My Scheduled Item] with the name of the Scheduled Item you are 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, replace [My Scheduled Item] with the name of the Scheduled Item you are 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/Database Tools

CSM is a definition-driven system, with definitions stored in the CSM database. A variety of tools are provided to help you connect to and manage your CSM database.

External Data and Databases

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.

Note: Consult a database vendor to acquire an OLE DB driver. First determine if the server is 32-bit or 64-bit because different drivers are required.

Note: CSM can also import Comma Separated Values (csv) data. The .csv data cannot be updated, it can only be deleted and new data imported, or new data imported on top of the existing data.

When connecting to an External Database, decide:

- Whether to import or link to the external data.
- Which external data to import or link (ex. An entire Table or a View).
- Where to put the external data in CSM (ex. A new External Business Object or existing CSM Business Object).

Imported and linked data are both accessed by a created External Connection:

- When importing external data into CSM, it is imported into the Cherwell Database. 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 CSM Scheduler. A Business Object keeps track of the external data and facilitates viewing/updating that data in CSM.
- When linking to external data, the external data is viewed (and sometimes 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.
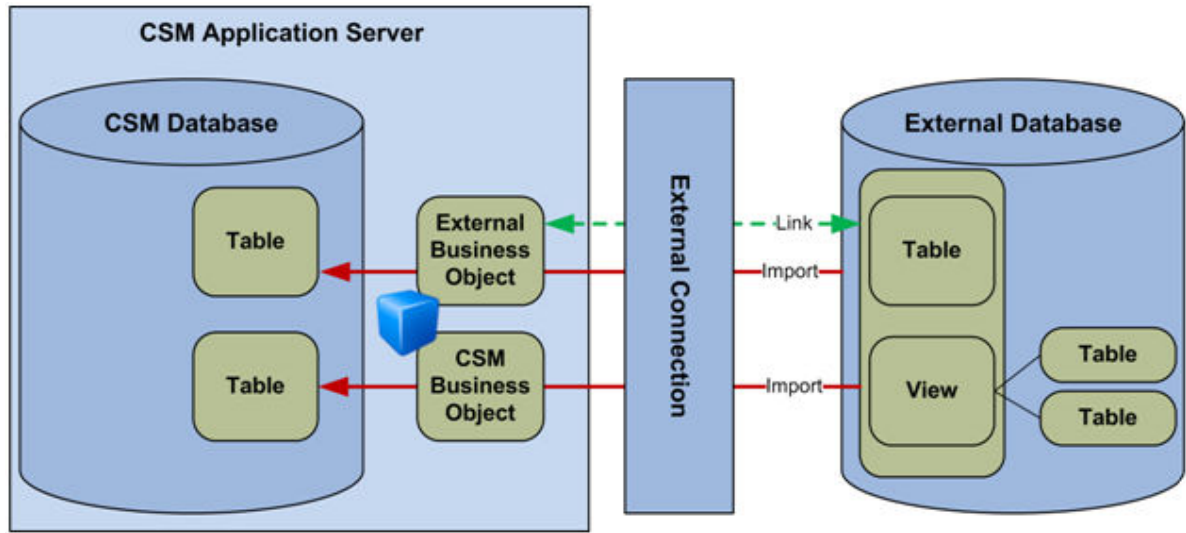
Table Views

\
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).

> **Tip:** 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.

> **Note:** For more information, see Create CSM Database Views .

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.
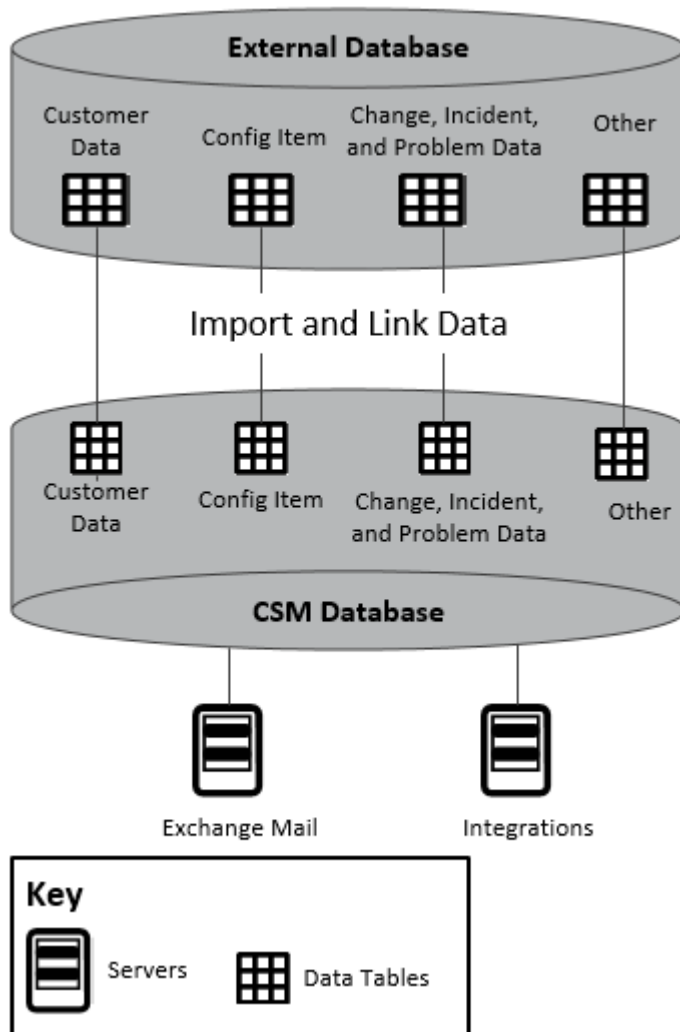
Demo and Starter Databases

CSM provides two databases:

- Starter database: Contains all the structure (ex: Business Objects, Forms, One-Steps, 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 (ex: Business Objects, Forms, One-Steps, Security Groups, etc.) and sample data (ex: 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.

    Note: See Upgrading for information about Upgrading a CSM 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:

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. From the Menu bar, click Managers>External Connections.
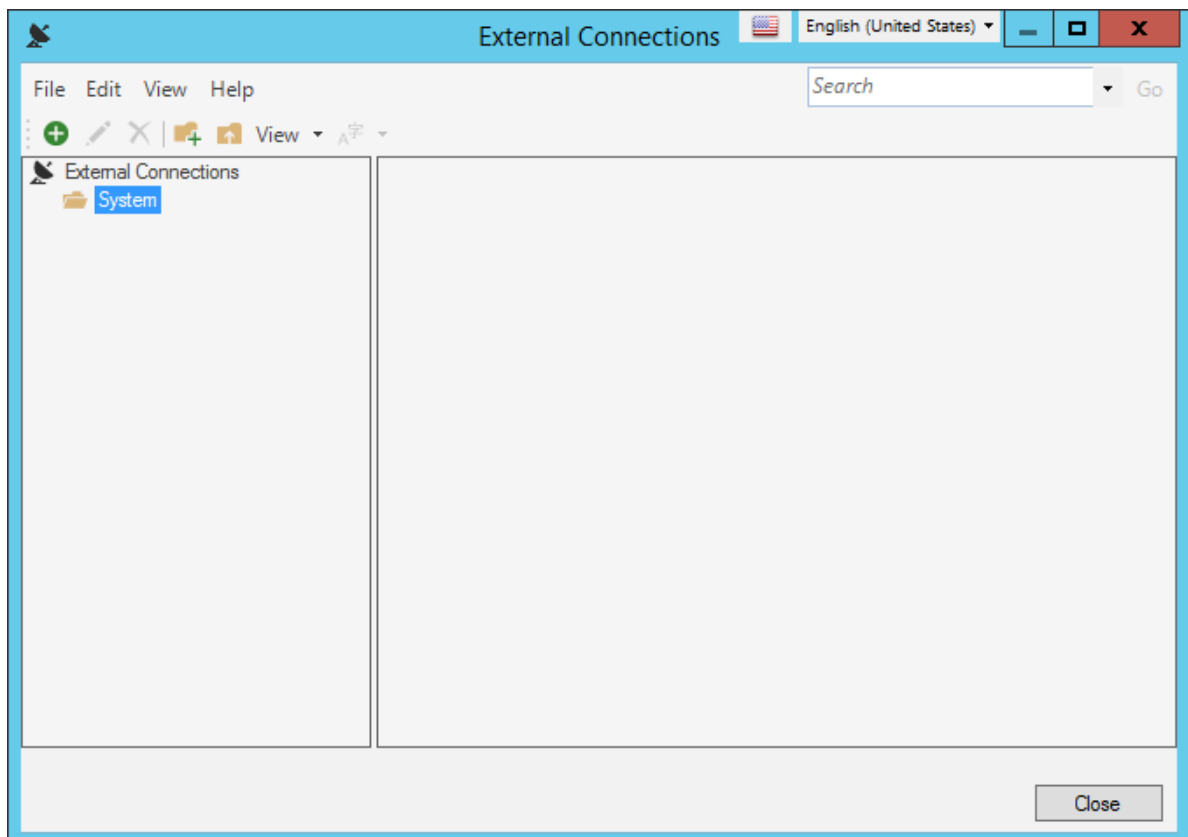
Stored Import Definition Manager

Use the Stored Import Definition Manager to complete general CSM Item Manager operations for stored .csv imports. The interface of the Stored Import Definition Manager has a:

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. Manager tree:

   Displays items in a hierarchical tree, organized by scope, and subfolder if applicable. Also lists any Searches run during the session.

5. Main Pane:

   Displays items by View (Icon, List, or Details (Grid) and lists search results when a Search is run.

To open the Stored Import Definition Manager:

1. In the Cherwell Administrator window, click on the Database category, and then the click Stored Import Definition Manager (.csv files) task.
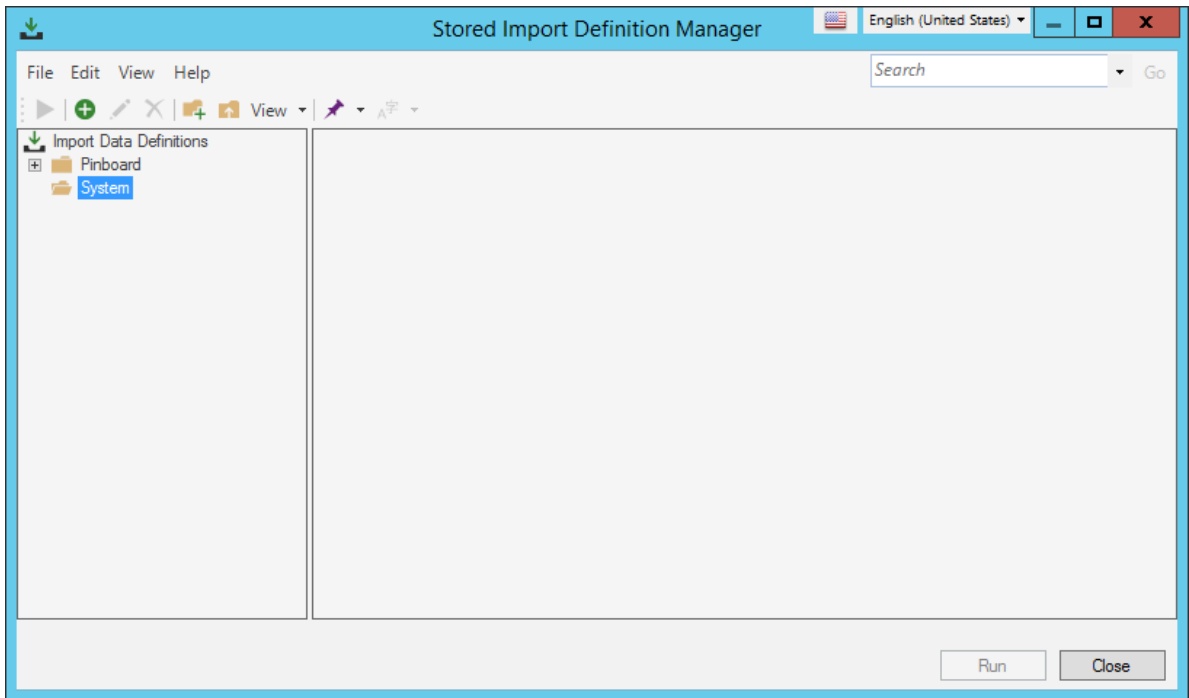
Database Tools and Wizards

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.

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.

  Note: When installing a new version of CSM and running Cherwell Administrator, it prompts an upgrade to the database and automatically runs this tool.

- **Definition Editor:** Allows Users to clear demo content from a database and search through definitions and make changes that cannot be made in the application.

  CAUTION: This is a powerful tool and should only be used if working with the Cherwell Support Team to accomplish advanced troubleshooting or configuration objectives. Please contact the Cherwell Professional Consulting Services team at support@cherwell.com for advanced configurations.

- **Import Utility:** Imports .csv files into the CSM Database.

System Restore Tool

The System Restore tool is a stand-alone 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 (accessed from the Cherwell Service Monitor Tools folder) 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.

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. Click Browse and navigate to a .czar file.

   b. Select the file and click 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. Click the Ellipses button to select the database (connection) to overwrite, and then click Import.

New database: Enables the .czar file to create a new database connection. Click the Ellipses button to open the Connection Wizard to create a new database connection.

Unicode support: Provides Unicode support for data.

When the restore is complete, the database connection is available when CSM opens.

System Upgrade Tool

The System Upgrade tool is a stand-alone database tool that 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. The User is not required to do anything when these windows open.

The System Upgrade tool (accessed from the Cherwell Service Monitor Tools folder) should only be used if the database was not upgraded as part of an application upgrade or an install.

> **Note:** Only Users with permissions, for example an Administrator User, 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).

   > **Note:** On Windows 7, right-click and select Run as Administrator.

   The Connect to Cherwell Service Management- System Upgrade window opens.

2. Click to select the database to upgrade.

3. Click OK.

   The System Upgrade window opens to verify the upgrade.

4. Click OK.

   The Cherwell System Upgrade login window opens.

5. Provide the **User ID** and **Password**.

6. Click OK.

Definition Editor

The Definition Editor is a stand-alone tool for advanced Users that allows Users to clear demo content from a database and search through definitions and make changes that cannot be made in the application.

CAUTION: This is a powerful tool and should only be used if working with the Cherwell Support Team to accomplish advanced troubleshooting or configuration objectives. Please contact the Cherwell Professional Consulting Services team at support@cherwell.com for advanced configurations.

Clear Demo Content from a Database

CSM comes with demo data so that Users can utilize the system in a non-live environment. When the system is ready to go live, clear out the demo data before importing real data. If Users do not want to clear out all of the data, they can clear records from individual Business Objects.

Note: During the install of the client applications, the Client and Administration tools check box must be selected on the Installation Type page. For more information, see Run the Client Installation.

To clear Demo content from a database:

1. Open the Definition Editor (Start>All Programs>Cherwell Service Management>Tools>Definition Editor).

   Note: On Windows 7, right-click and select Run as Administrator.

   The Connect to Cherwell Service Management - Definition Editor window opens.

   CAUTION: This is a powerful tool and should only be used if working with the Cherwell Support Team to accomplish advanced troubleshooting or configuration objectives. Please contact the Cherwell Professional Consulting Services team at support@cherwell.com for advanced configurations.

2. Select a database.
   a. Click the All Users tab (view database connections available to All Users) or the **User** tab (view the User database connections only available to the User).
   b. Click a **database connection**. To create a new database connection, click Add to launch the Connection Wizard. To modify an existing database connection, click the database connection, and then click Edit. To delete an existing database connection, click the database connection, and then click Delete.
3. Select the Automatically use connection without asking box to automatically use this database connection each time CSM is launched. The prompt to select a connection does not show again.
4. Click OK.
   The Cherwell Definition Editor login page opens.
5. Provide the login credentials.

Option	Description
User ID	Provide the **User ID** (this could be domain name/network or just user name)

Option	Description
Password	Provide the **network password**. Passwords are case-sensitive. **Tip:** By default, there is a User ID called CSDAdmin with a password of CSDAdmin in the Demo and Starter Databases.

6. Click OK.

   The Trebuchet Definition Editor window opens.

7. Click System in the Menu bar, and then select Clear Demo Content.
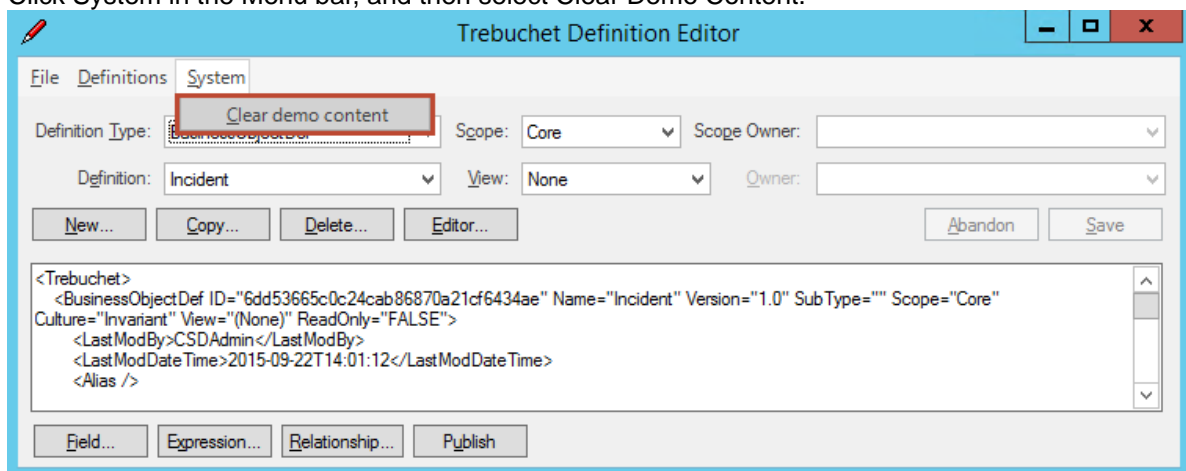
8. Click Yes to clear the demo content.
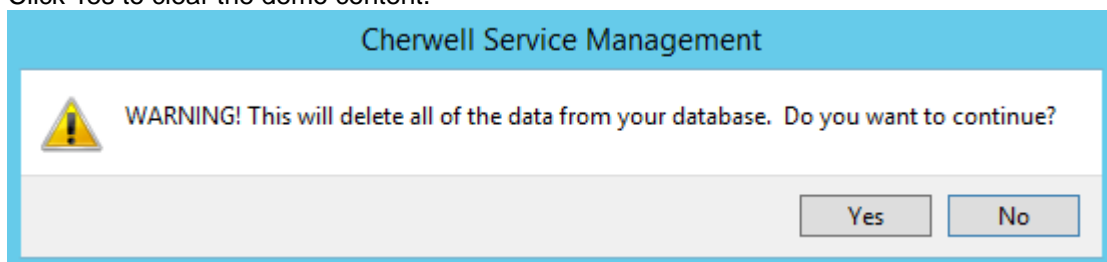
Clear CSM Records

Clear test records from your system so they do not interfere with your metrics during production.

Complete the following procedure for each of the following Business Objects:

- Configuration Items (CIs)
- Incident/Service Request
- Problem
- Change Request
- Knowledge Article

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, click the down arrow on the **Search** button

   .

   b. Select a **Business Object** to search (ex: Incident).

      Tip: Make sure that you are not limiting the search by either the date or open records only.

   c. Click the Go button to run the search.

      The test record(s) display in the Main Pane.

3. Click File and select **Delete All**.

   A window opens verifying that you want to delete all of the records from the group.

4. Click Yes.

   The records are cleared from the system.

Import Utility

The Import Utility is a legacy stand-alone utility used to import .csv files into the CSM Database. Perform the same functionality using the by Managing CSV Data in the CSM Administrator.

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. Click OK.

    The Cherwell Import Utility window opens.

5. Import from:
    a. Click the Ellipses button [...].
    b. Select the file, and then click Open.

6. Import to:
    a. In the drop-down, 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. Click Import.

> **Note:** If there are unequal fields, a warning window opens. Click Yes.

Export a Database

Use the Export Data option in CSM Administrator to export a selected CSM Database to a compressed Cherwell Archive Repository (.czar) file. Export a/an:

- Single Business Object.
- Entire system (full backup).
- Log file to capture the details of the database export.

When exporting an entire system, define what to export:

- **All Data:** Exports all SQL Server tables (ex: Field names and sizes) and data. Use this option to create a full backup .czar of an entire CSM system.

  When using this option, select to exclude the following data so that the .czar file size is smaller:

    - 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.
    - 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.
    - Encrypted fields: Exports Field data, but not encrypted Fields. Use this option to exclude sensitive data from a .czar file. Note that 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.
- **Table Structure Only:** Exports all SQL Server tables without any data. Use this option to create a .czar file that excludes confidential company data.
- **Table Structure and Lookup Tables:** Exports SQL Server tables for all Major and Supporting 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 (because typically, Lookup tables do not contain confidential data and can be used to troubleshoot problems with validation and Relationships).

To export a single Business Object:

1. In the CSM Administrator window, click the Database category, and then click the Export Data task.

   The Export Data window opens.

2. Click 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 check box to exclude encrypted Fields from the export. We recommend excluding encrypted Fields if data is provided to support.

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 (Ex: Incident_Nov2014), and then specify a location. Provide a location or click the Ellipses button [...] to navigate to a location.

7. Click OK.

To export a system:

1. In the CSM Administrator window, click the Database category, and then click the Export Data task.

   The **Export Data** window opens.

2. Select the Export Entire System check box.

3. Select the Content to export:

    Export All Data: Select this check box to export all tables and data, and then select to exclude the following so the file is smaller:

    - **Exclude Attachments:** Select this check box to exclude Attachments.

    - **Exclude automation data:** Select this check box to exclude automation data.

    - **Exclude encrypted fields**: Select this check box to exclude encrypted Fields.

    Export Table Structure Only: Select this check box to export tables but no data.

    Export Structure and Lookup Table Data: Select this check box to export Major and Supporting Business Object tables, as well as Lookup tables and Lookup table data.

4. (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.

5. In the Save To field, provide a **name** for the .czar file (Ex: Backup_Nov2014), and then specify a location. Provide a location or click the Ellipses button ⌷ to navigate to a location.

6. Click OK.

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 by categories: Full-Text Search, Manage Indexes, and Data.

To perform database System Maintenance:

1. In the CSM Administrator window, click the Database category, and then click the System Maintenance task.

2. Select one or all check boxes to run maintenance requests.

3. Click OK.
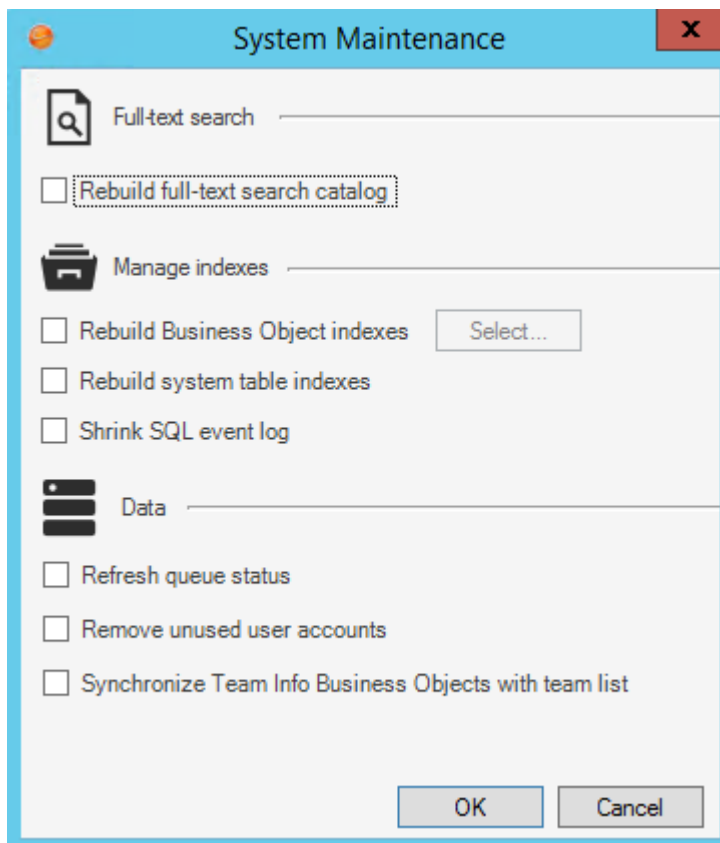
Full-Text Search

The Full-Text Search category has the option to Rebuild Full-Text Search catalog. The Rebuild Full-Text Search catalog executes various SQL Server stored procedures to rebuild the SQL Server Full-Text. For example:

```
exec sp_fulltext_column @tabname=N'dbo.Incident',@colname=N'IncidentID',@ac
tion=N'add',@type_colname=NULL
```

Note: For SQL 2012 and above there is logic behind the scenes that performs the rebuild.

Manage Indexes

The Manage Indexes category has all of the options so that Users can run 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)
```

Data

The Data category has the options so that Users can run maintenance on the data in the database. The Data 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-existing 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 a non-existing UserInfo or Customer records.

Synchronize Team Info with team list: Synchronizes the Team Info Lookup table with CSM User and Customer Team list.

Managing External Connections

Before CSM can share data with an External Database, create an External Connection to the External Database. An External Connection is a named connection between CSM and an External Database that passes the External Database's location and access information to CSM. The connection defines the:

- Data Source
- Provider
- Location of the database server
- Name/location of the database
- Login options (credentials)
- Owner/schema
- Pooling options

To help manage (create, edit, and delete) External Connections, CSM provides the External Connection Manager and the External Connection Wizard.

Note: The connection is made from the Cherwell Application Server to the External Database. The connection should be configured to work from that location and, if applicable, use the account of the Cherwell Application Server.

Share Data with an External Database

Perform the steps below in CSM Administrator to share data with an External 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. 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.

Create an External Connection to an External Database

Use the External Connection Wizard to create (and manage) an External Connection. 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

An External Connection connects CSM to an External Database. The steps below are specifically for an External Connection between CSM and a SQL Database.

Requirements for SQL Server and MySQL Connections:

- MySQL Server must be installed.
- User rights must be granted.
- Know the location and name of the server.

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. Click Create New ⊕.

   The External Connection Wizard opens.
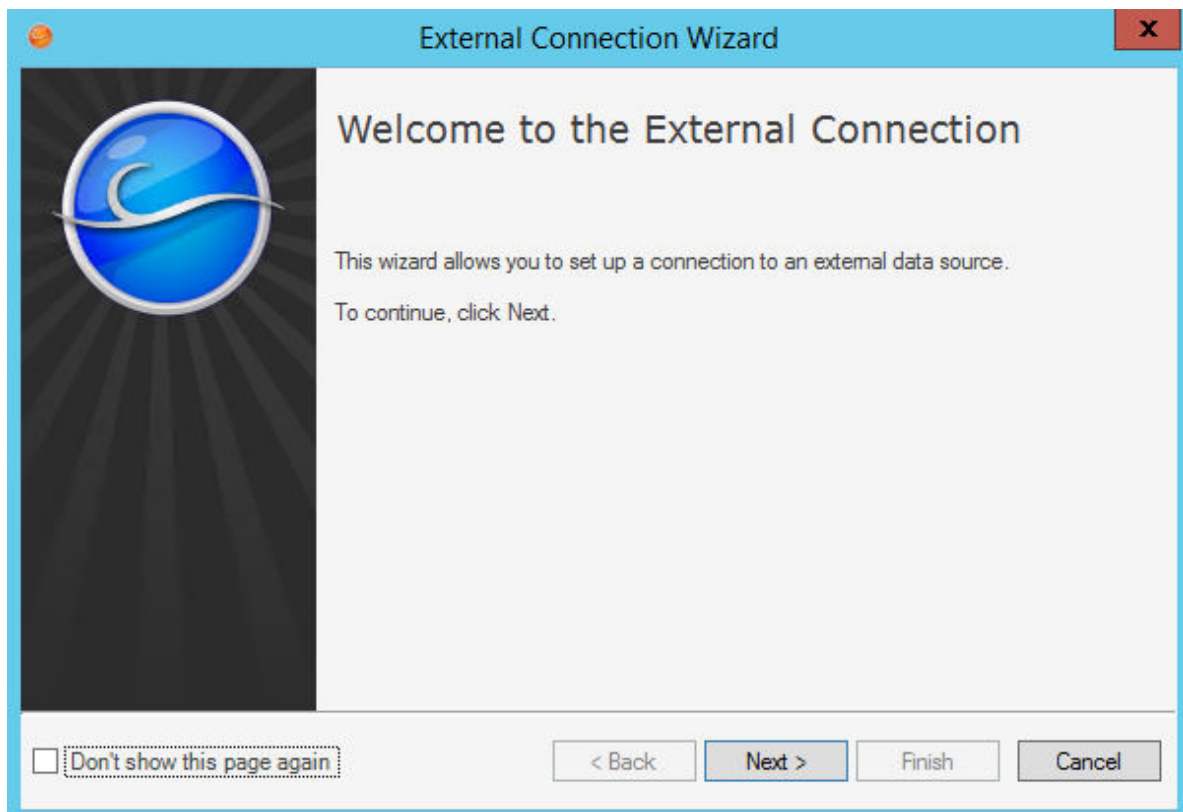
4. Click Next.

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.

   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 Agents.

6. On the Data Source page:
   a. Click MySQL or **SQL Server**.

   b. Click Next.

7. On the Database Location page, 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 click the Specific server in the drop-down.

   Note: If the connection is to a named instance of a SQL (a non-default instance of SQL), 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**.

8. Click Next.

9. On the Select Database page, click Browse.

   The Login to server window opens.
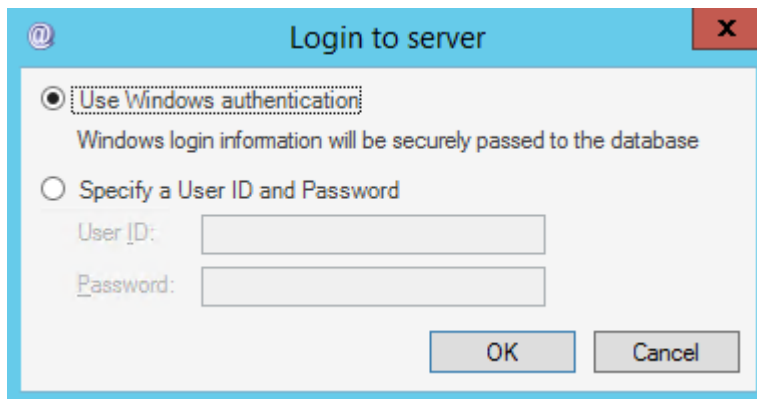
10. Select a **login** radio button to use either:

   Windows authentication: Use the stored Windows credentials (user name and password) for authentication.

   User ID and Password: Provide the server User ID and Password.

11. Click OK.

   The system runs for a few minutes and the Choose a Value window opens.
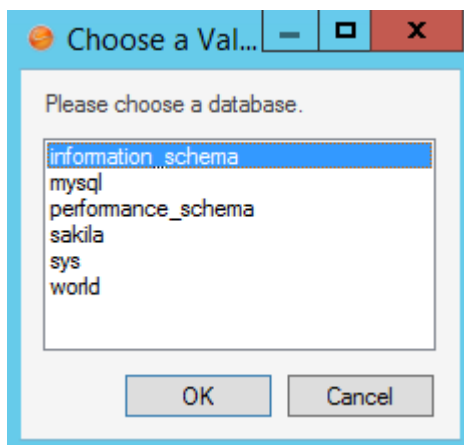
12. Choose a Value:
   a. Click a **database**.

   b. Click OK.

   c. Click Next on the wizard page.

13. On the Login Options page, provide the Login Options:
   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. Click Next.

14. On the Database Owner or Schema page, 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, then they are listed in the drop-down. If not, provide the owner name. If unsure, provide the default dbo.

15. On the Pooling Options page, select a Connection Pooling option for the database:
     Select the Use default pooling options radio button.

Note: The defaults are usually acceptable for most scenarios; however, setting the pool sizes customizes the caching options.

Select the Customize the pooling options radio button, and then provide the minimum and maximum pool size.
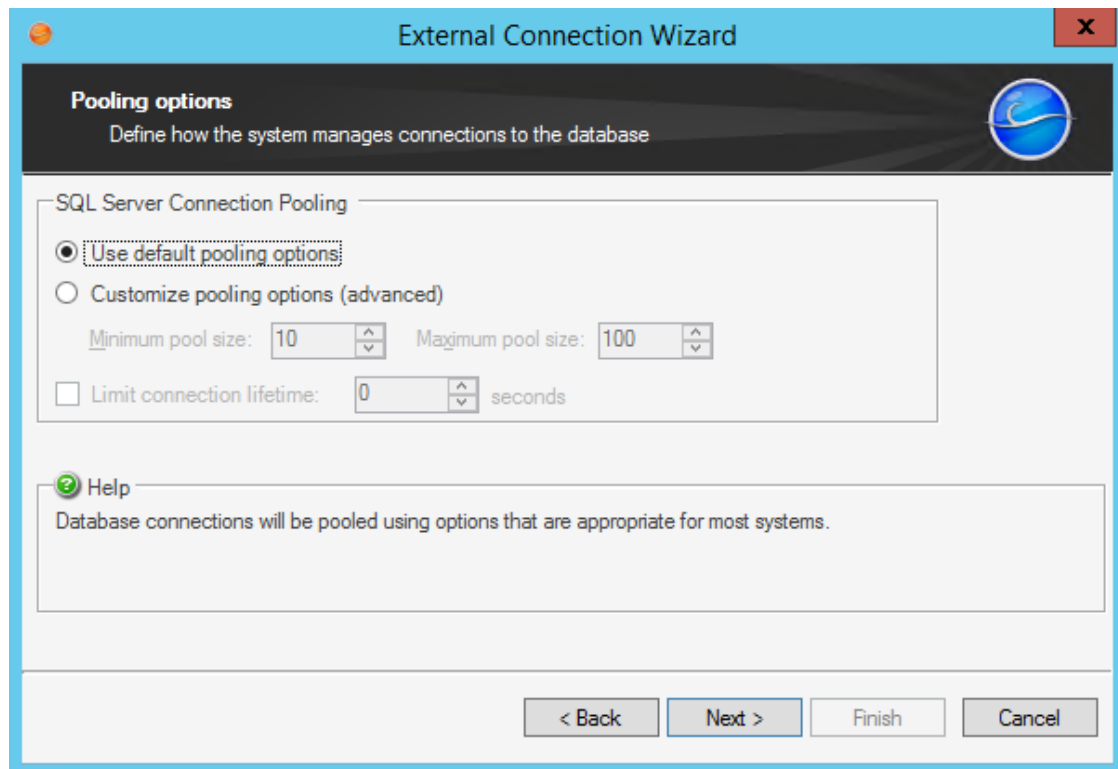
Click Next.

The Connection name page opens.

16. On the Connection name page:
     a. Provide a Namefor the database connection.

     b. (Optional) Provide a Description for the database connection.

     c. Click 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.

17. Click Test Connection to verify 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 Cherwell Administrator for help.
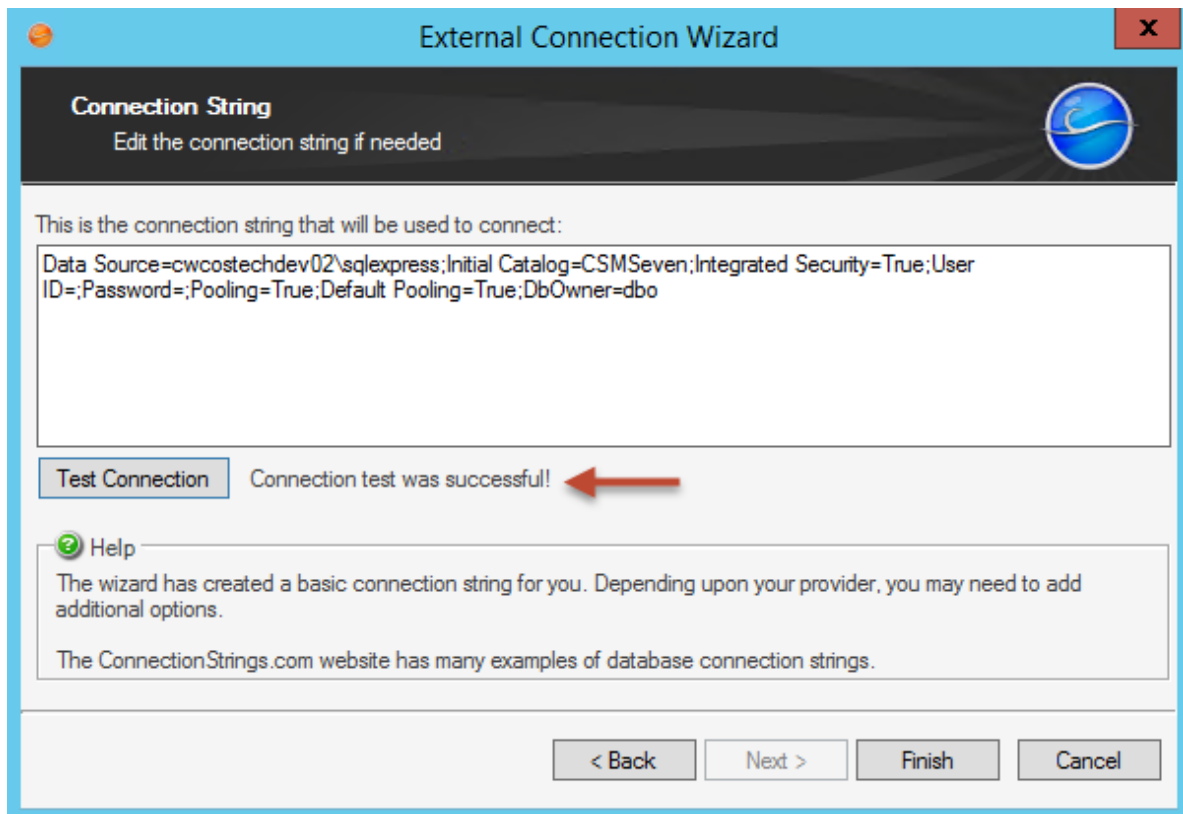
18. Click Finish.

    There is now a connection to the SQL Server database.

19. Publish the Blueprint (File>Publish Blueprint) to commit the changes, or save the Blueprint (File>Save Blueprint) to continue making other changes.

Create an External Connection to Oracle

An External Connection connects CSM to an External Database. The steps below are specifically for an External Connection between CSM and an Oracle Database.

In order to create an Oracle connection, the Oracle client must be installed and configured.

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. 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 Agents.

5. On the Data Source page, select Oracle.

6. On the Select Net Service Name page, provide the **full string** containing the service name. For example:

```
(DESCRIPTION=(ADDRESS=(protocol_address_information))(CONNECT_DATA=(SE
RVICE_NAME=service_name)))
```


7. 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. Click Next.

8. 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. Click Next.

9. opens.

10. On the Pooling Options page:
    a. Select the Use default pooling options radio button.

        Note: The defaults are usually acceptable for most scenarios; however, setting the pool sizes customizes the caching options).

    b. Select the Customize the pooling options radio button, and then provide the minimum and maximum pool size.

    c. Click Next.

11. On the Connection name page:
    a. Provide a **Name** for the database connection.

    b. (Optional) Provide a **Description** for the database connection.

    c. Click 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.

12. 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.

13. Click Finish.

    There is now a connection to the External Oracle Database.

14. Publish the Blueprint (File>Publish Blueprint) to commit the changes, or save the Blueprint (File>Save Blueprint) to continue making other changes.

Create an External Connection to an OLE DB

Creating an External Connection with connects CSM through OLE DB to an Oracle Database. The steps below are specifically for an External Connection between CSM and an OLE Database to SQL.

> **Note:** OLE Database is a standard that allows CSM to connect to a variety of databases in a common format.

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. Click the Create New button ⊕.

   The External Connection Wizard opens.
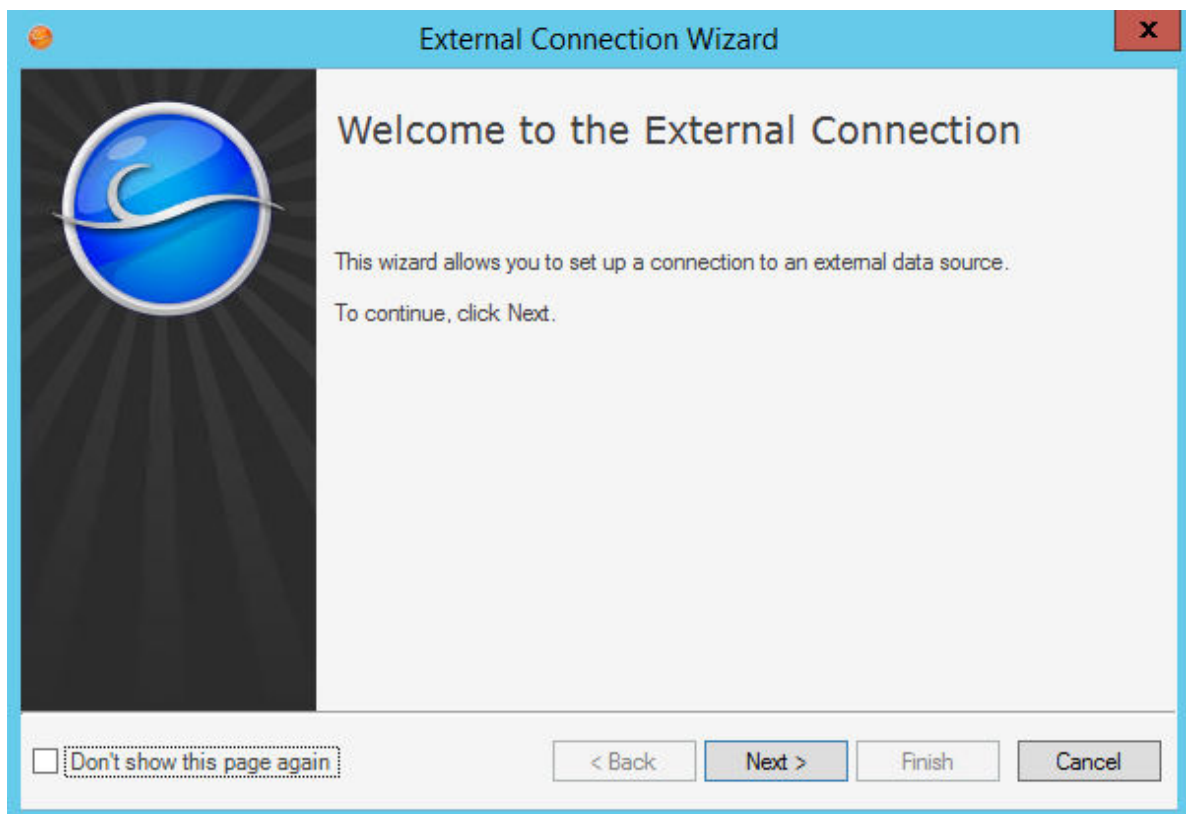
4. Click Next.

   The Database Source page opens.

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.

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 Agents.

6. On the Data Source page:
   a. Select OLE DB.

   b. Click Next.
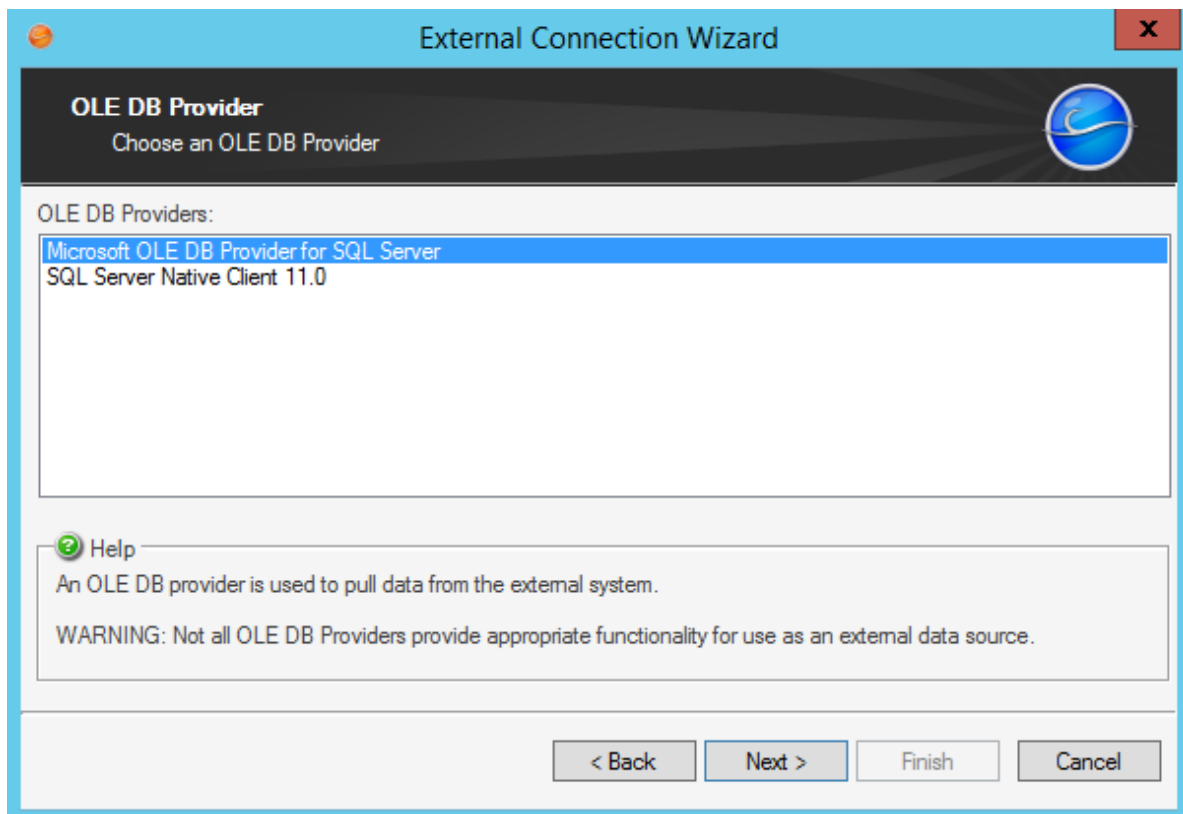
7. On the OLE DB Provider page:
   a. Select an **OLE DB Provider**.

> **Note:** If you are using Oracle as the provider, there are some differences in the Wizard. For more information, see Create an External Connection to Oracle.

> **Note:** Drivers should be available from a database vendor. Consult the database vendor for assistance locating this driver. There are also OLE Database drivers from third-party vendors that can be used.

    b. Click Next.

8. 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.

        Data Comes from file: Select this option if the driver connects directly to a file rather than to a database server.

        Note: This radio button is only shown when CSM does not detect if the provider connects to a database or a file.

    b. Click Next.

> **Note:** If Data comes from a file is selected on the Database Location page, the Database field is replaced with a File field.

9. On the Select 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.

10. On the Login to server window, select to use either:

    Windows authentication

    User ID and Password: Provide the server User ID and Password.
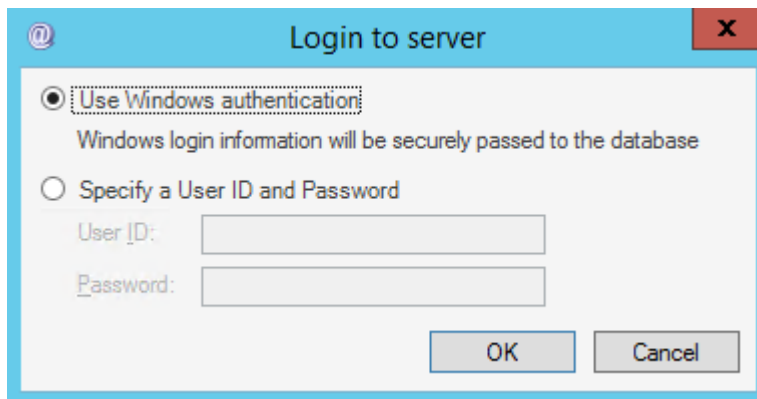
11. The system runs for a few minutes, and then the Choose a Value window opens.
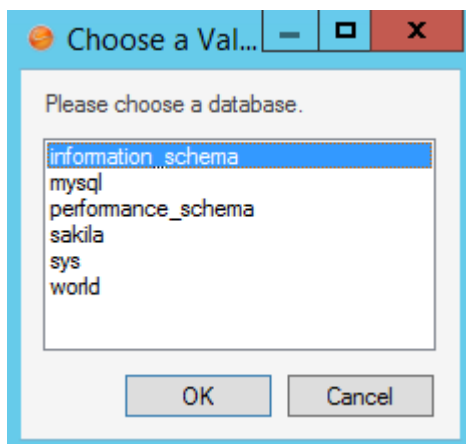
12. Click a **database**.

13. Click Next.

14. 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. Click OK.

15. 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. Click Next.

16. On the Pooling Options page, select either:
          Use OLE DB connection pooling.

          No pooling.

17. On the Connection name page:
       a. Provide a **Name** for the database connection.

       b. (Optional) Provide a **Description** for the database connection.

       c. Click 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.

18. 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.

19. Click Finish.

       There is now a connection to the External OLE Database.

20. Publish the Blueprint (File>Publish Blueprint) to commit the changes, or save the Blueprint (File>Save Blueprint) to continue making other changes.

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 Agents.

5. On the Data Source page:
   a. Select ODBC.

   b. Click Next.
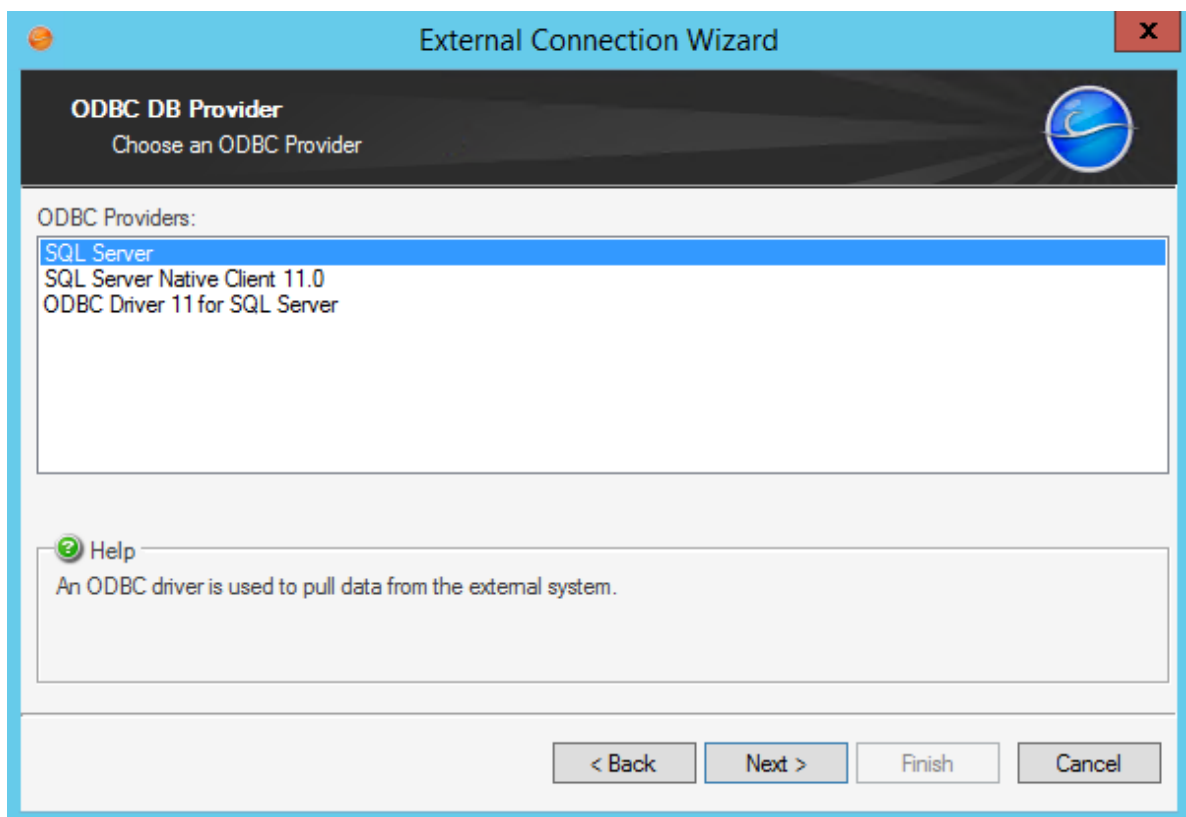
6. On the ODBC Provider page:
   a. Select an **ODBC Provider**.

> **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. Click 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. Click 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.
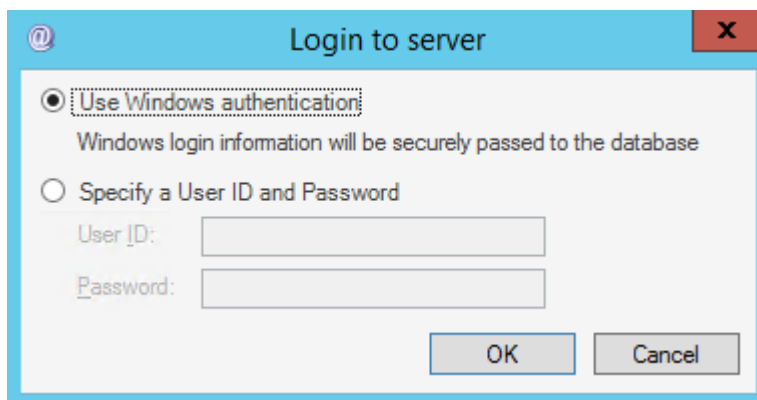
    a. Select a **login** radio button to use either:
      Windows authentication

      User ID and Password: Provide the server User ID and Password.

    b. Click OK.

    The system runs for a few minutes and the Choose a Value window opens.
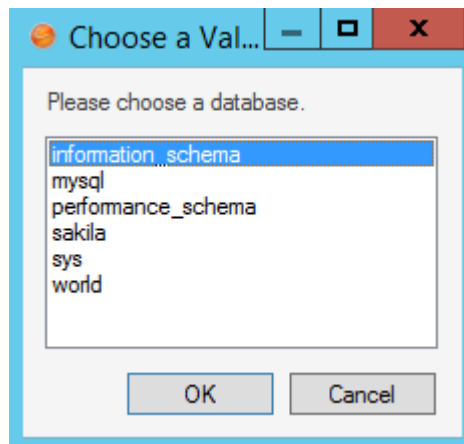
    c. Click a **database**.

    d. Click OK.

9. Click 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. Click 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. Click 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. Click 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. Click 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.

Using External Business Objects with External Data

An External Business Object is a Business Object that shares data with an External Database, either by:

- Importing external data: Facilitates the importing of the external data into CSM.
- Linking to external data: Keeps track of the external data and facilitates viewing the external data in CSM. If updates of the external data are permitted, the Business Object can be configured to enforce the appropriate rules.

The External Business Object definition notifies CSM what the external data is, where that external data is stored, and what rules to apply to that external data.

External data must have a designated place to be stored either by:

- Mapping an existing CSM Business Object to external data, and then importing the external data. No link option is available for existing CSM Business Objects.
- Creating an new External Business Object to import the external data, and then importing the external data.
- Creating an External Business Object (an use it like any other CSM Business Object) to link to the external data. There are a few limitations that might be encountered when the underlying database queries between the CSM Database and the External Database. The advantage of an External Connection is that a User can use the data within CSM without realizing it comes from another database.

> **Note:** A combination of imported and linked data is not possible within the same Business Object.

Map an Existing Business Object to Import External Data

Use an existing Business Object to import external data directly into the Business Object. An existing Business Object cannot link to external data, a new External Business Object must be created. For more information, see Create an External Business Object to Link to External Data.

To import external data:

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, showing the Object Manager in its Main Pane. The Object Manager lists the existing Business Objects.

2. Select an existing Business Object, and then click Map to external data task. Or select New Object, and then **New external business object** task.

    The External Data Wizard opens.

3. Click 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.

4. Click Import Data.

5. Click Next.

    The Data Source page opens.

6. Select the External Connection that was created to connect to the External Database.

7. Click Next.

    The External Table to Map page opens, listing the Tables and/or Views from an External Database.

8. Click the Table or **View** to import.

> **Note:** If the Table/View is not listed, check the login account and database owner/schema to ensure it has rights to view the data.

9. Click Next.

   The Fields to Map page opens.

10. Map fields from the Table/View to a field in the new External Business Object:

    Tip: To remove a field: Click to select a **field**, and then click the Remove button. To edit a field's mapping: Click to select field, and then click the Edit button.

    a. click Add.

       The Map Field from External Table window opens, listing the available Table/View fields.

    b. Click to select the external field to map to.

    c. Click Create new field and type a **name** for the new field.

    d. Click OK.

11. Click Next.

   The Unique Key and Timestamp Fields page opens. Example fields are used in the screen shots.
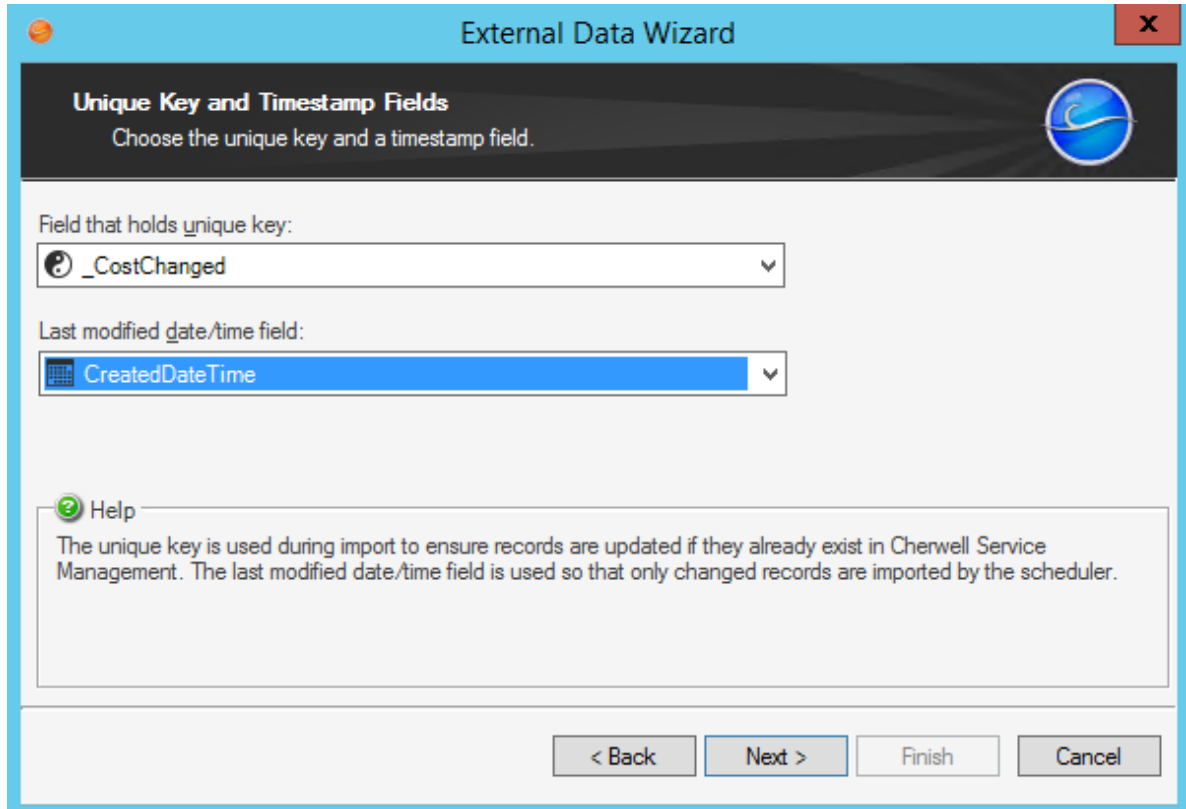
12. Designate a Unique Key and Timestamp field:
   a. Field that Holds Unique Key: Select the field from the View that is deemed as the unique identifier (ex: MachineID or ComputerID).

      Note: A unique ID field for CSM must be used in the external Table/View. If the Table/View does not have a Unique Key, add one.

   b. Last Modified Date/Time: Select the field from the Table/View that is deemed as the last modified date/time field (ex: LastScanDate or date_modified).

      Note: This field is used to import only changed records.

13. Click Next.

   The Summary page opens. The information varies depending on selections throughout the wizard.
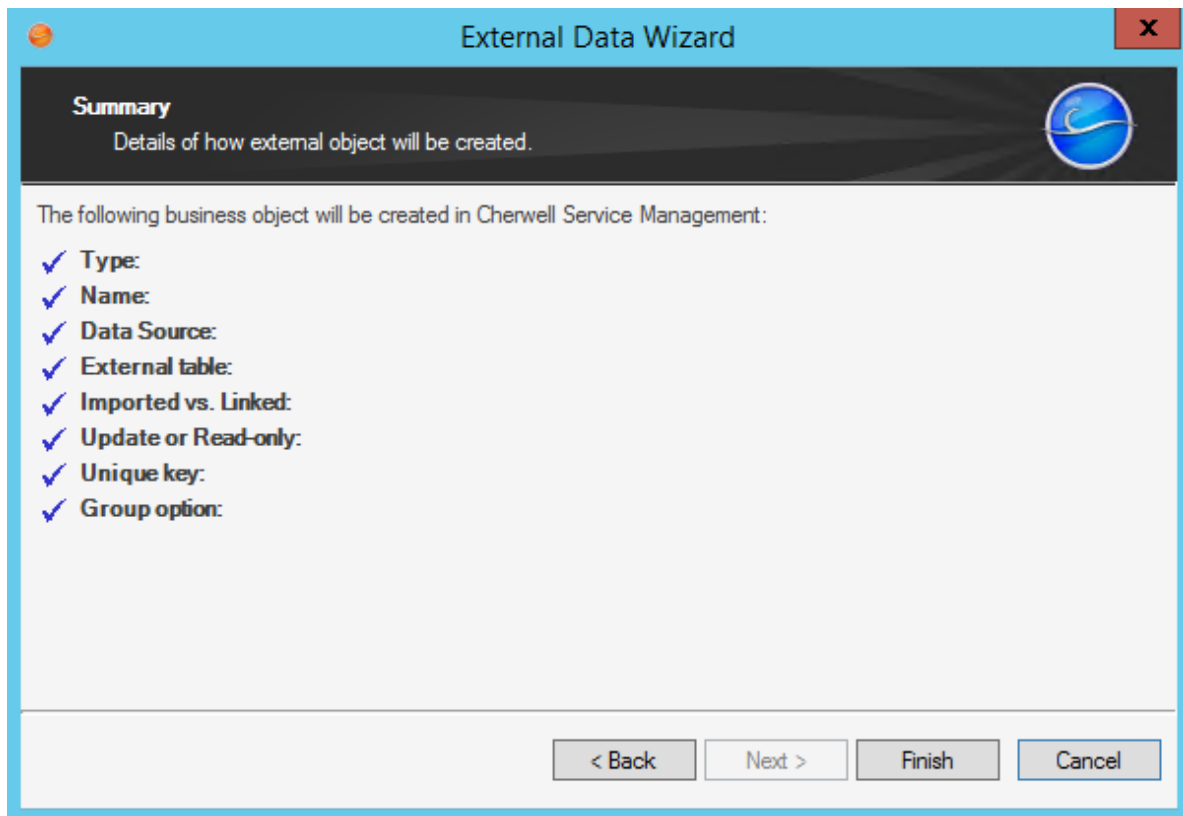
14. Click Finish.

    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.

15. Click OK to close the Properties window.

16. (Optional for Supporting Objects) If needed, create a Relationship between the newly created Supporting Objects and the Major Object they support.

17. Publish the Blueprint (File>Publish Blueprint) to commit the changes, or save the Blueprint (File>Save Blueprint) to continue making other changes.

Create a New Business Object to Import External Data

Use an existing Business Object to import external data directly into the Business Object. An existing Business Object cannot link to external data, a new External Business Object must be created. For more information, see Create an External Business Object to Link to External Data.

To import external data:

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, showing the Object Manager in its Main Pane. The Object Manager lists the existing Business Objects.

2. Select New Object, and then **New external business object** task.

   The External Data Wizard opens.

3. Click 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.

4. Click Import Data.

5. Click Next.

   The Data Source page opens.

6. Select the External Connection that was created to connect to the External Database.

7. Click Next.

   The External Table to Map page opens, listing the Tables and/or Views from an External Database.

8. Click the Table or **View** to import.

   > **Note:** If the Table/View is not listed, check the login account and database owner/schema to ensure it has rights to view the data.

9. Click 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 External Business Object to create, either:

>   **Major Business Object:** A Major Business Object is a stand-alone Business Object that represents a major component of a business. It can exist by itself and have child objects that are part of its composition (using Relationships). Examples include Incident, Problem, Change, Knowledge Article, Customer, Configuration Item, and Service.
>
>   **Supporting Business Object:** A Supporting Business Object is a Business Object that exists solely to complement, or support, a Major Object. Examples include Task, Journal, and Approval.
>
>   **Lookup Business Object:** A Lookup Business Object is a Business Object that supplies valid values to other Business Objects. More precisely, it stores values for Fields that require constrained selections. For example, the Incident Cause Lookup Object holds values such as Hardware Malfunction, Outage, Permissions, etc.

11. Click Next.

    The Part of Cherwell Group page opens.

12. Define Group information options for the External Business Object:

> **Note:** A Group Business Object is a set of Business Objects that share common Fields. For example, the Configuration Item Group has Group Members named Computer, Printer, and Telephony Equipment. A Group Leader (ex: Configuration Item) is the Business Object that is the root of a Group. It stores common Fields that all Group Members share. All Group Members are descended from the Group Leader.

Not a Member of a Group: Select this option to 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.

13. Click Next.

The Fields to Map page opens.
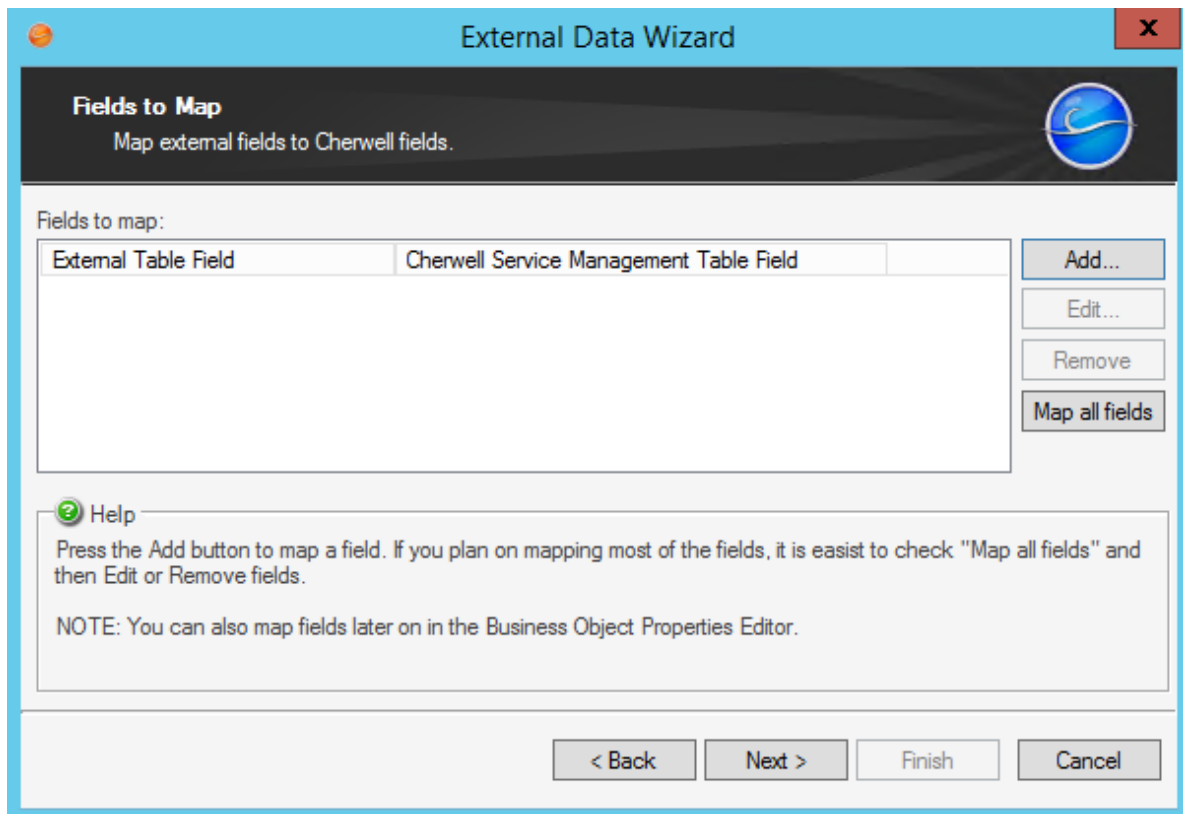
14. Map fields from the Table/View to a field in the new External Business Object:

    To map all available Table/View Fields at once, click Map all fields. The Wizard automatically creates a new field for each external Table/View Field and populates the mapping list.

    Tip: To remove a field: Click to select a **field**, and then click the Remove button. To edit a field's mapping: Click to select field, and then click the Edit button.

    To map one field at a time, click Add.

    The Map Field from External Table window opens, listing the available Table/View fields.

    a. Click to select the external field to map to.

    b. Click Create new field and type a **name** for the new field.

    c. Click OK.

15. Click Next.

    The Unique Key and Timestamp Fields page opens. Example fields are used in the screen shots.
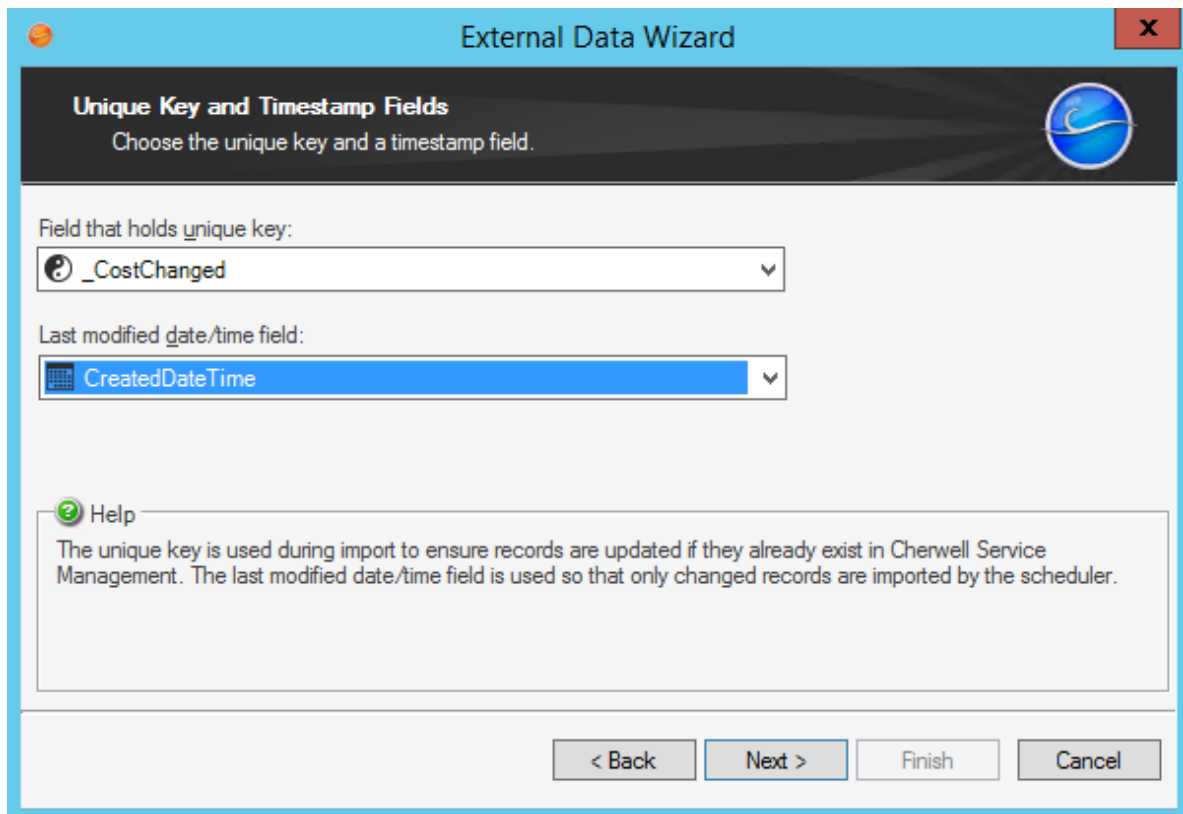
16. Designate a Unique Key and Timestamp field:
    a. Field that Holds Unique Key: Select the field from the View that is deemed as the unique identifier (ex: MachineID or ComputerID).

       Note: A unique ID field for CSM must be used in the external Table/View. If the Table/View does not have a Unique Key, add one.

    b. Last Modified Date/Time: Select the field from the Table/View that is deemed as the last modified date/time field (ex: LastScanDate or date_modified).

       Note: This field is used to import only changed records.

17. Click Next.

    The Read-Only or Updatable page opens.

18. Select Data is read-only or **Allow data to be updated** radio button.

19. Click Next.

    The Name and Description page opens.

20. Provide the **Name** and **Description** for the Business Object.

21. Click Next.

The Summary page opens. The information varies depending on selections throughout the wizard.
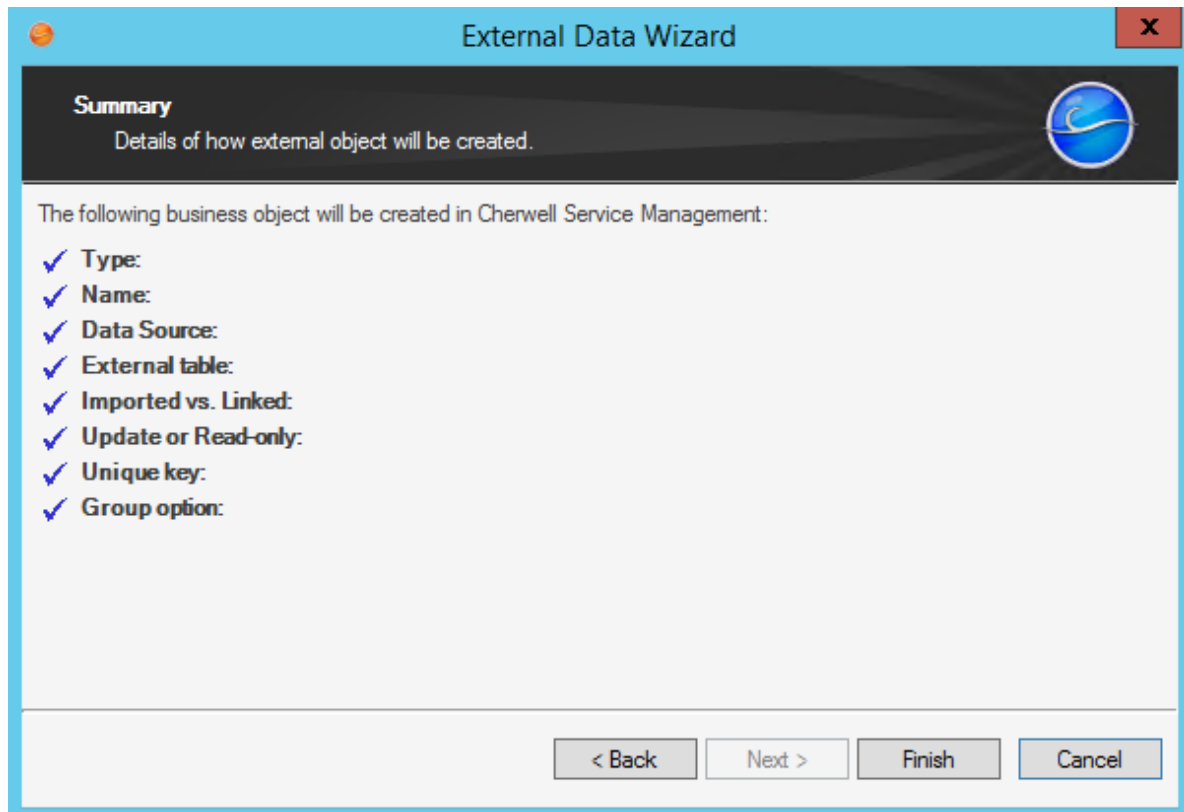
22. Click Finish.

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. Click 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.

Create an External Business Object to Link to External Data

Create a new Business Object to import or link external data. When a new Business Object is created, either import or link external data. If using an existing Business Object, only import data. For more information, see Map an Existing External Business Object to Import External Data.

To create a new Business Object and link or import data:

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, showing the Object Manager in its Main Pane. The Object Manager lists the existing Business Objects.

2. Click (New Object), and then click New External Business Object.

   The External Data Wizard opens.
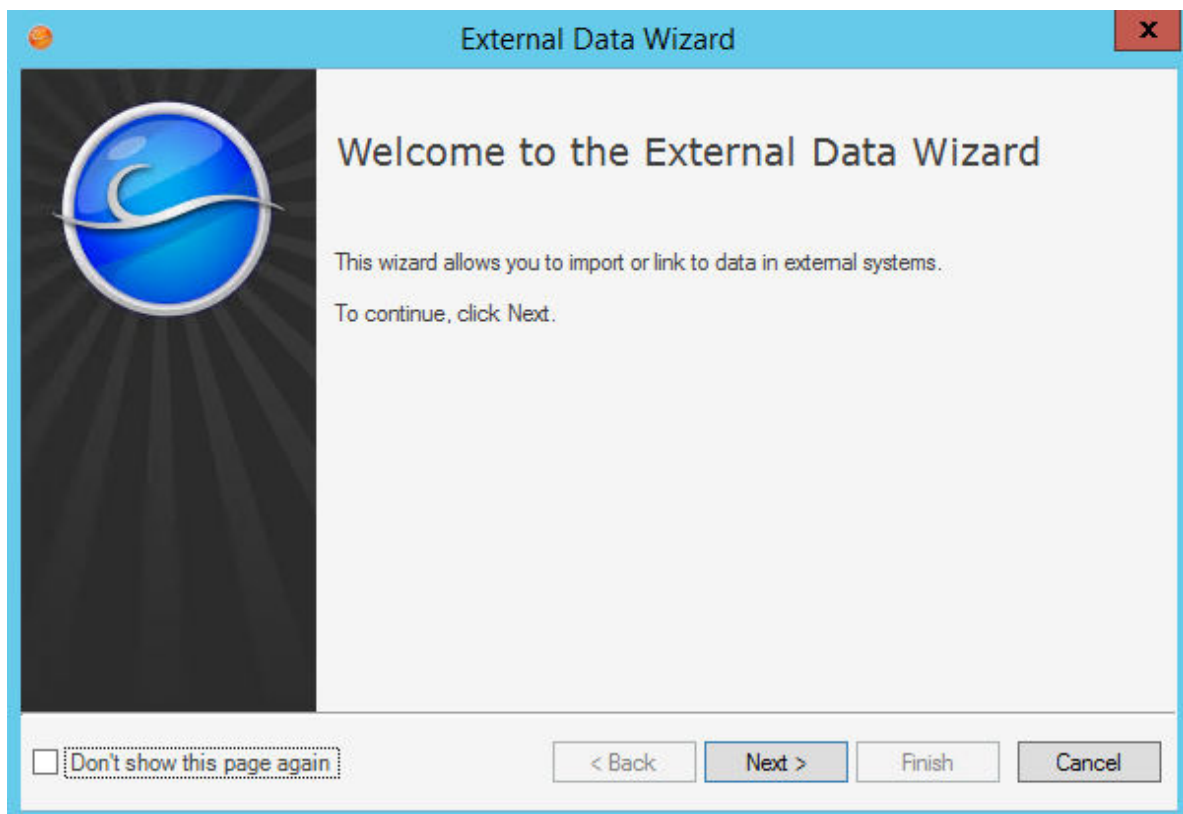
3. Click Next.

    The Import vs. Linked page opens.

4. Click Link to data.

5. Click Next.

    The Data Source page opens.

6. Select the External Connection that was created to connect to the External Database.

7. Click 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.

    Note: If the Table/View is not listed, check the login account and database owner/schema to ensure it has rights to see the data.

9. Click Next.

    The Business Object Type page opens.

10. Select the Type of External Business Object to create, either:

> **Major Business Object:** A Major Business Object is a stand-alone Business Object that represents a major component of a business. It can exist by itself and have child objects that are part of its composition (using Relationships). Examples include Incident, Problem, Change, Knowledge Article, Customer, Configuration Item, and Service.

> **Supporting Business Object:** A Supporting Business Object is a Business Object that exists solely to complement, or support, a Major Object. Examples include Task, Journal, and Approval.

> **Lookup Business Object:** A Lookup Business Object is a Business Object that supplies valid values to other Business Objects. More precisely, it stores values for Fields that require constrained selections. For example, the Incident Cause Lookup Object holds values such as Hardware Malfunction, Outage, Permissions, etc.

11. Click Next.

The Fields to Map page opens.

12. Map fields from the Table/View to a field in the new External Business Object:
To map all available Table/View fields at once, click Map all fields. The Wizard automatically creates a new Field for each External Table/View field and populates the mapping list.

Tip: To remove a field: Click to select a field, and then click the Remove button. To edit a field's mapping: Click to select a field, and then click the Edit button.

To map one field at a time, click to select individual fields, and then click Add.

The Map Field from External Table window opens, listing the available Table/View fields.
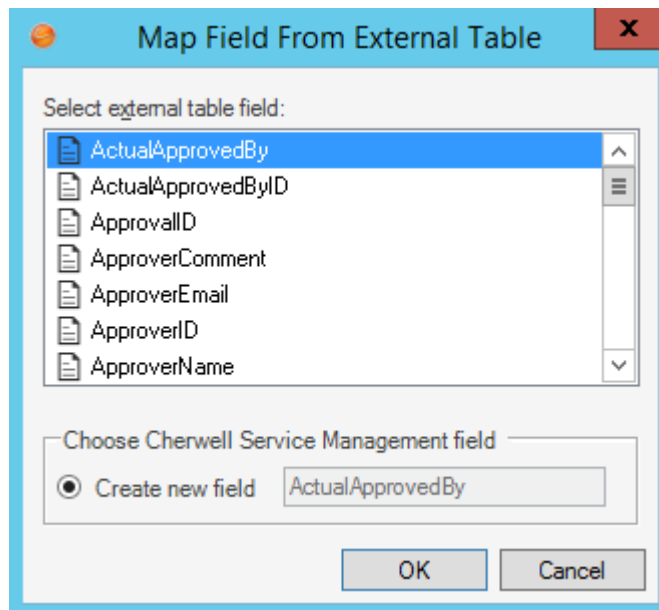
a. Click to select the external field to map.

b. Select Create new field and type a **name** for the new field.

c. Click OK.

13. Click Next.

The Unique Key and Timestamp Fields page opens. The screen shots show example fields.
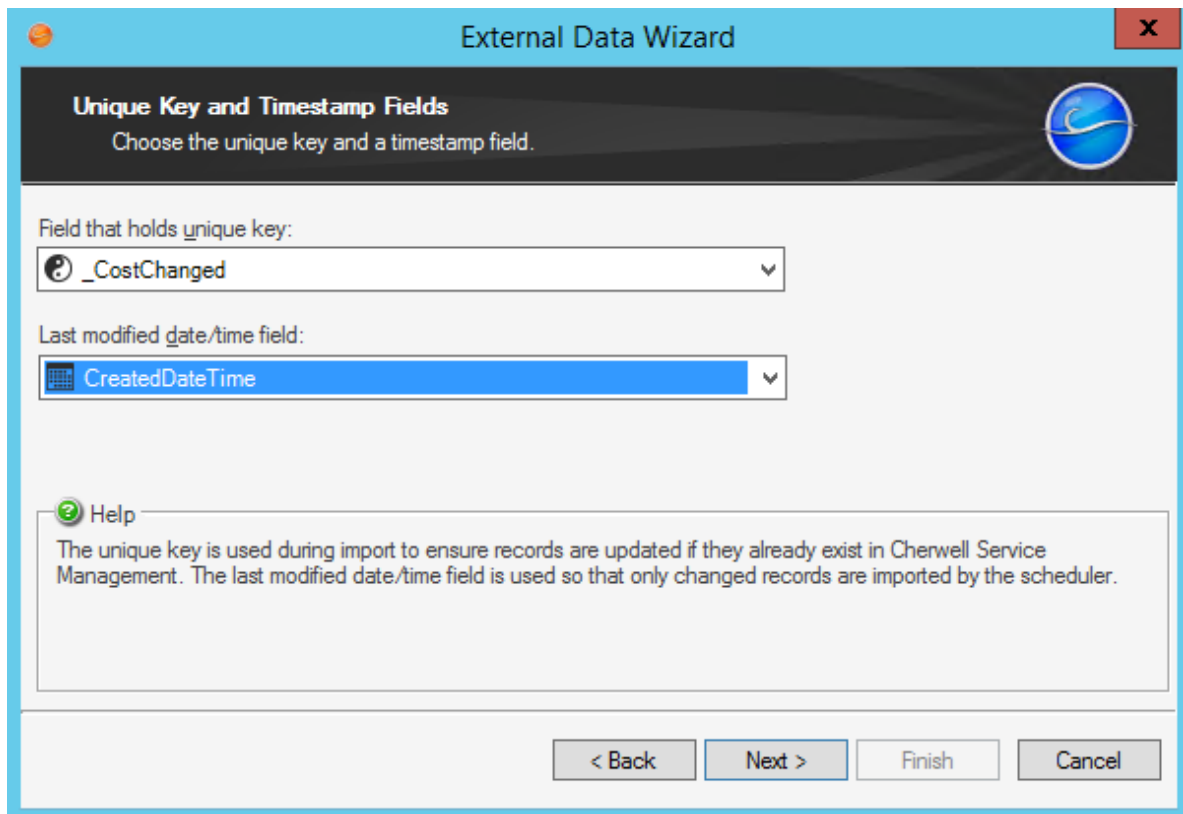
14. Designate a Unique Key and Timestamp field:

> **Field that Holds Unique Key:** Select the field from the View that is deemed as the unique identifier (ex: 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 (ex: LastScanDate or date_modified).

> **Note:** This field is used to import only changed records.

15. Click Next.

> The Read-Only or Updatable page opens.
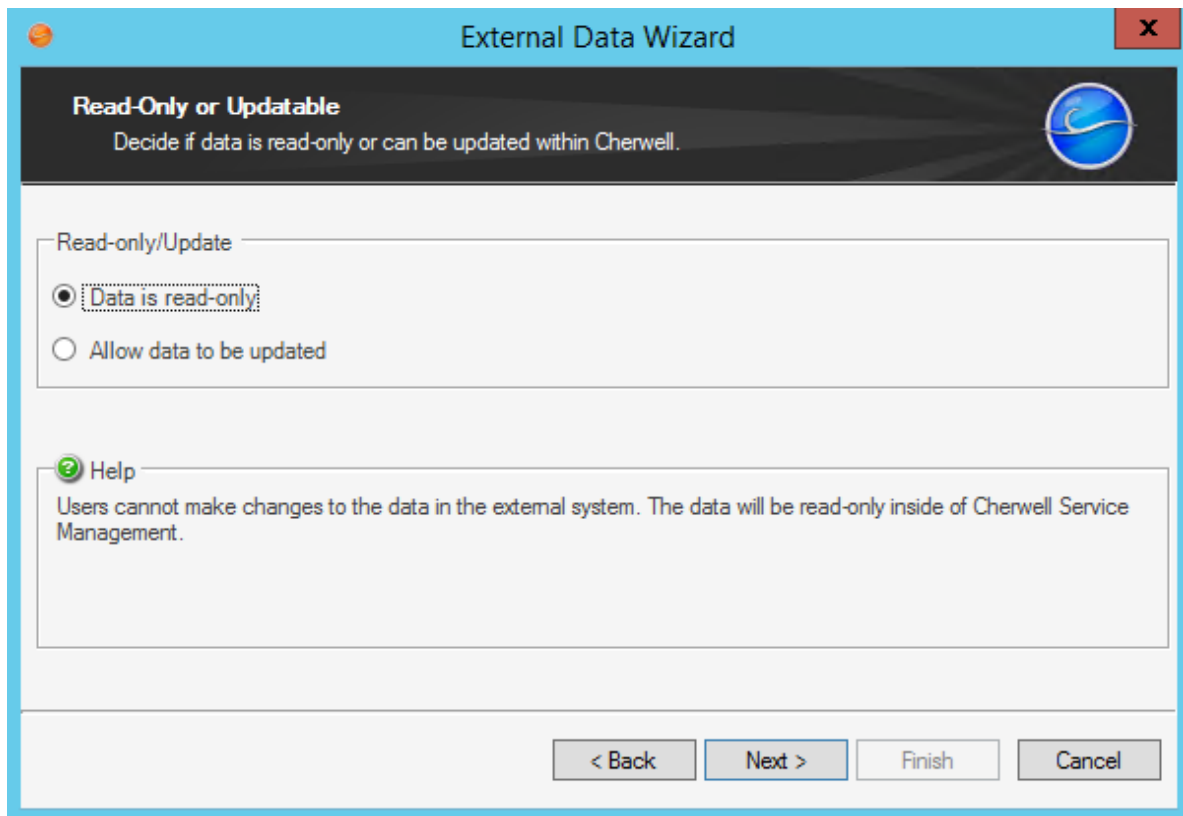
16. Select the radio button to determine if the data should be read-only or if it can be updated in CSM.

> **Note:** Unless linking to a very simple flat database, usually this integration should not be updatable. This CSM connection does not have any knowledge of the application rules for the receiving end of the updates.

> **Note:** The database login account that was used to set up the External Connection to the External Database must have rights to insert and update this Table/View. Be aware that Views cannot be updated in some databases.

17. Click Next.

    The Search Options page opens.

18. Define searching options for the External Business Objects:

    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 (ex: Quick Search).

    Tip: DBAs might want to set up a database index for these fields in the order specified so that searching is faster.

    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%')

19. Click Next.

    The Name and Description page opens.

20. Provide a **Name** for the External Business Object.

    Note: The internal name is always the name of the Table or View from the External Database. By default, the display name is the same. If the Table/View name matches an existing CSM Business Object, alter the name to ensure the name is unique. If the name is not altered, external data cannot be imported to the Business Object.

21. (Optional) Type a **Description** for the External Business Object.

22. Click Next.

    The Summary page opens. The information varies depending on selections throughout the wizard.
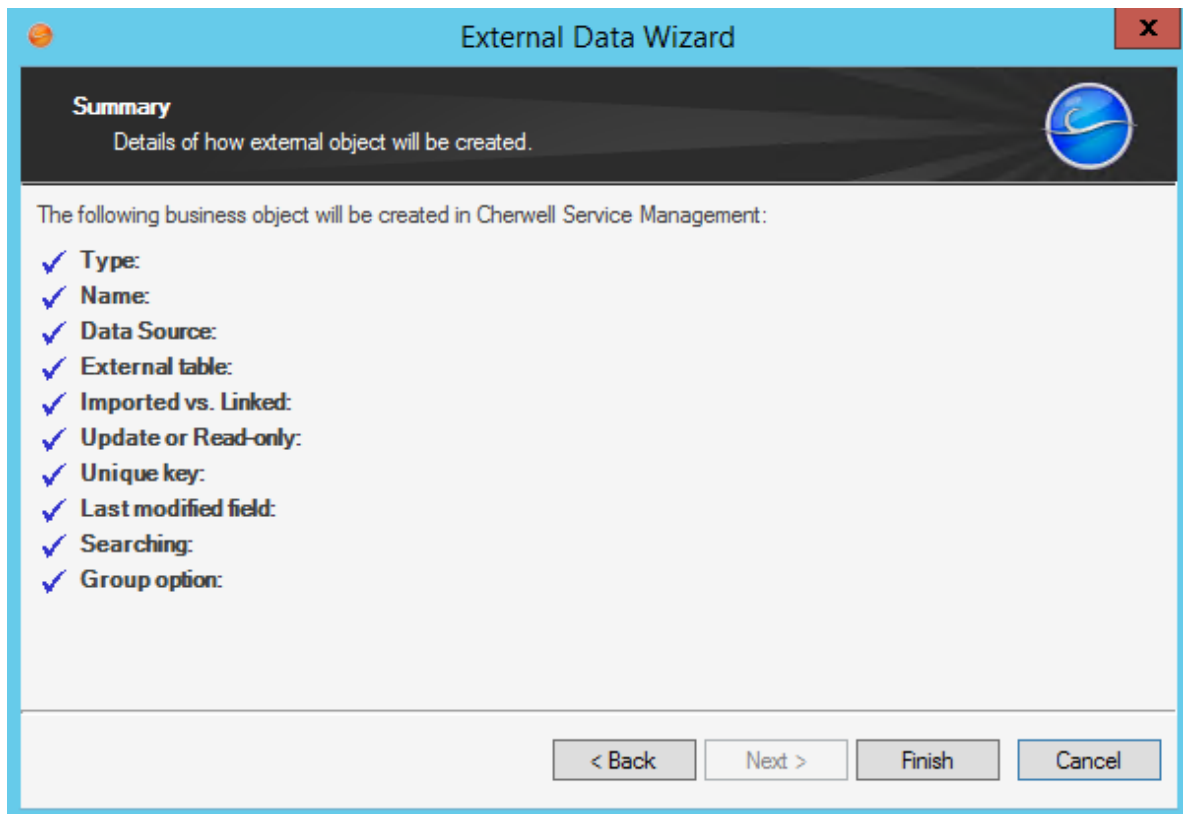
23. Click Finish.

    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.

24. Click OK to close the Properties window.

25. Create Forms and Grids for the External Business Object just as a new CSM Business Object.

26. (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 an External Business Object

Use the External Data Import Wizard to import data from an External Database into an External Business Object.

🖊 **Note:** Create an External Business Object that imports data before importing external data.

To import external data into an External Business Object:

1. In the CSM Administrator window, click the Database category, and then click the Import external data task.

   The External Data Import Wizard opens.
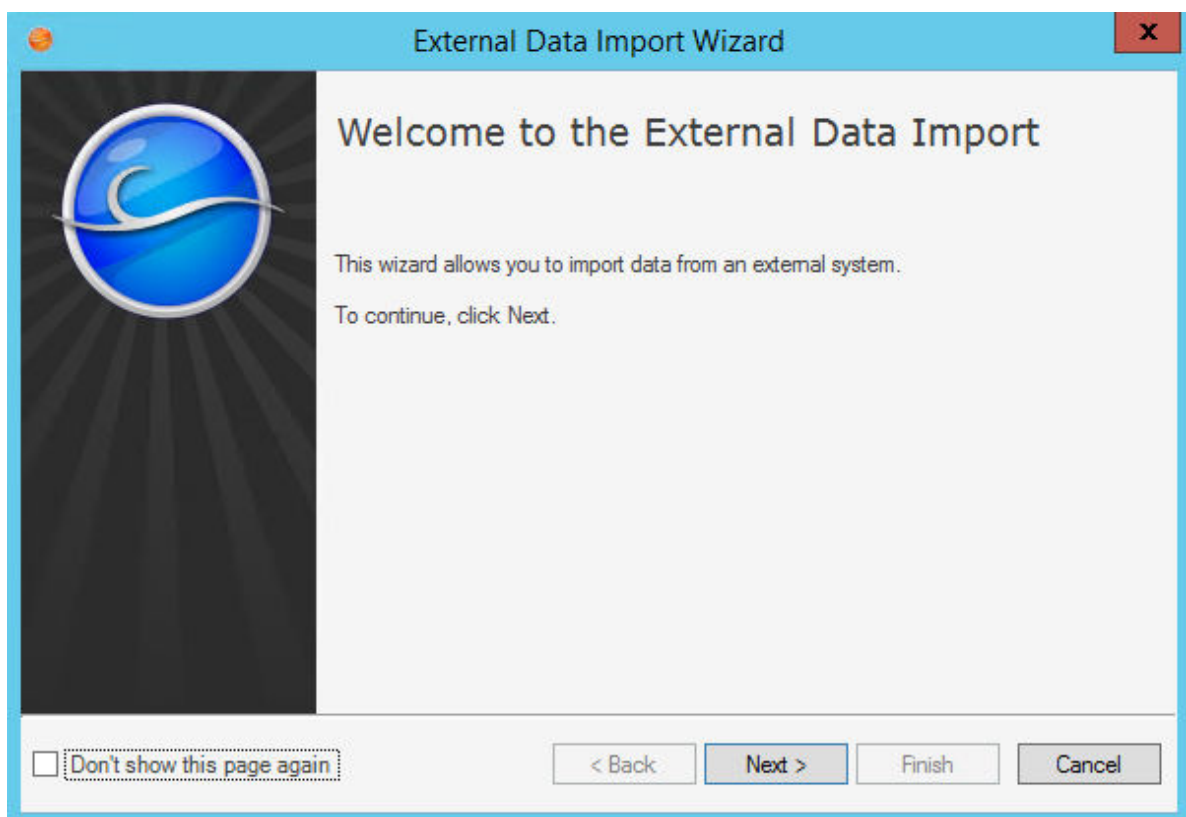
2. Click Next.

   The Select Business Object page opens.

Note: Only Business Objects that are eligible to import external data are listed (for example, either External Business Objects or existing CSM Business Objects with mapped data).

3. Select the Business Object mapped to the external data.

4. Click Next.

   The Existing Records page opens.
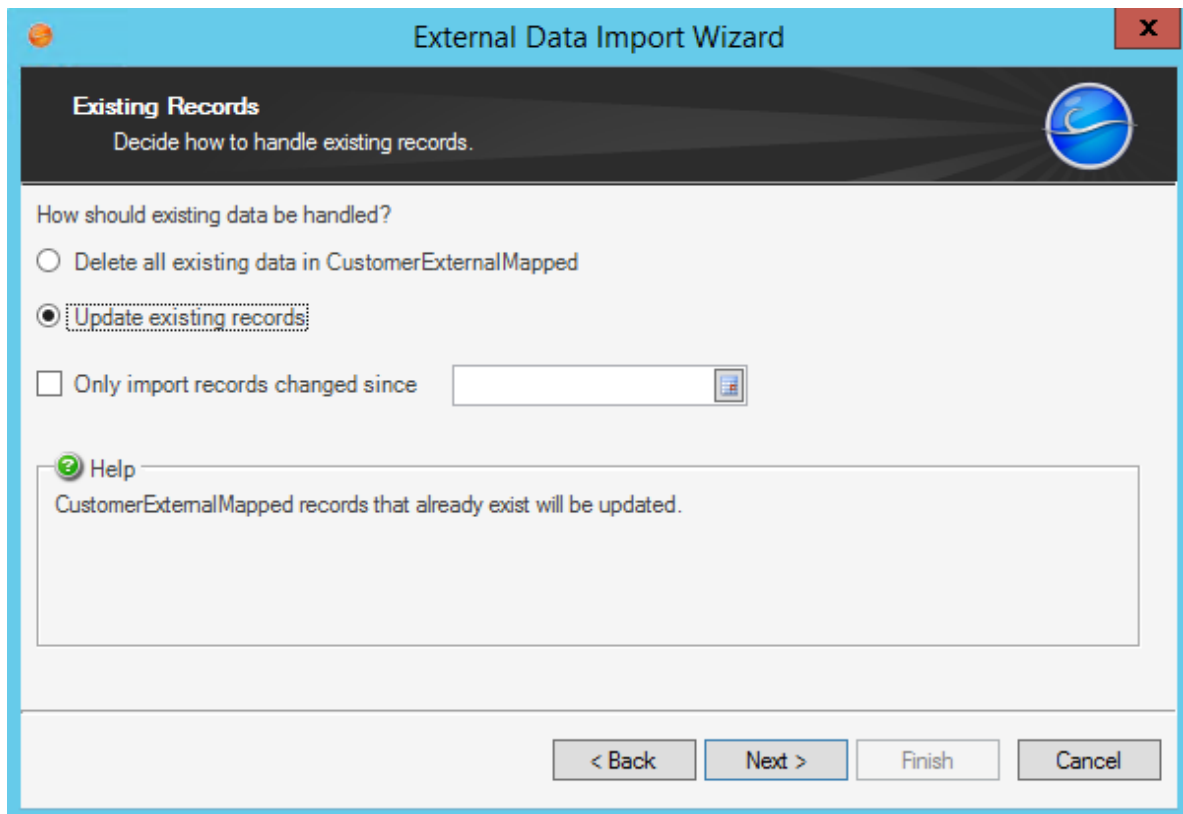
5. Select whether to delete or update existing records within CSM:

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.

Note: Existing records are updated based on the matching Unique Key field.

6. (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.

Tip: Typically, imports are quick enough that this option is not necessary, especially if imports are scheduled for non-peak work hours.

7. Click Next.

The Choose Filter page opens.
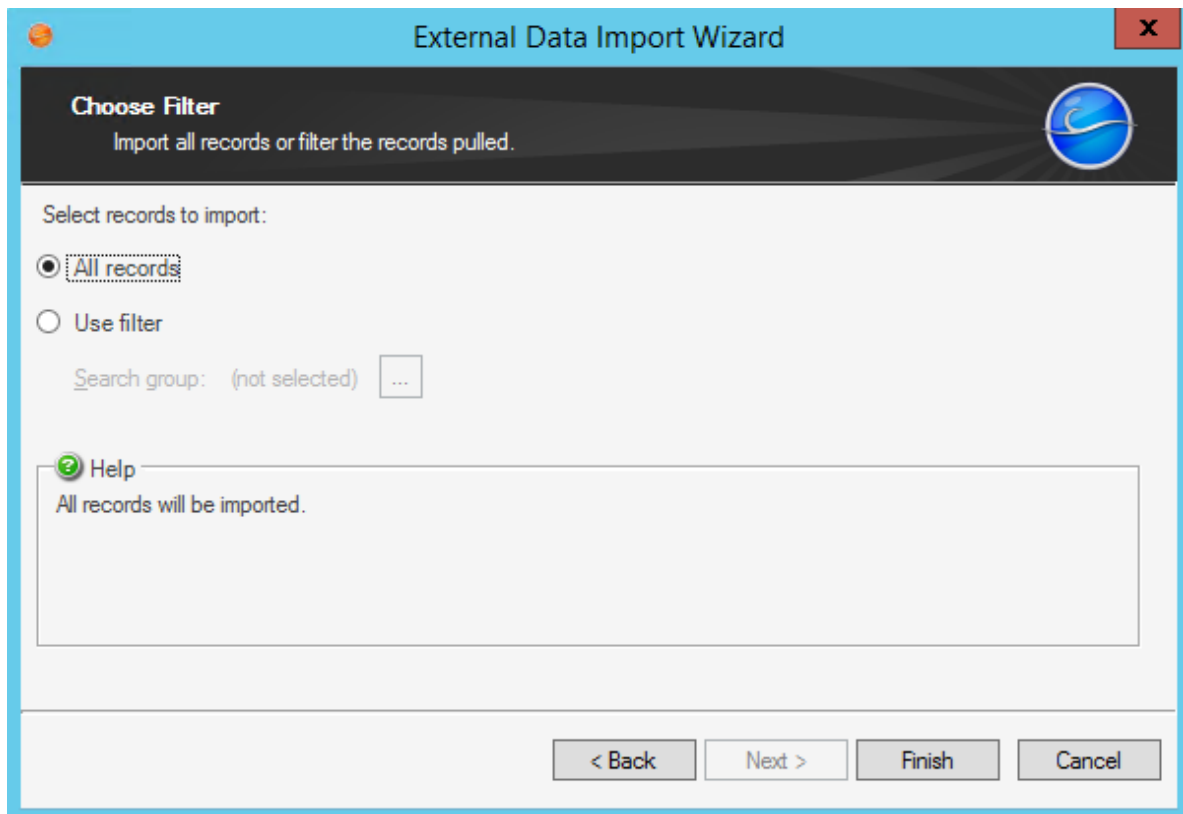
8. Select the data to import:

All records: Select this radio button to import all the external data.

Use filter: Select this radio button to filter the data to import based on a defined query (Search Group). When the User Filter radio button is selected, the Search Group option enables. Click the Ellipses button [...] to open the Search Group Manager, and then select an existing Search Group (saved Search Query) or create a Search Group. Saved Searches can be used over and over in numerous places.

Note: Typically, data in a View is already filtered.

9. Click 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.

Managing CSV Data

CSM can import data from .csv (comma delimited) files into an existing CSM Business Object or into the CSM database.

To create a .csv file:

1. Create an Excel spreadsheet populated with desired data (example: RecID information or employee e-mail addresses).

   ✏️ **Note:** Commas are the only accepted separators when importing.

   An example Excel spreadsheet:

	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

2. Save the Excel spreadsheet as a .csv file (File > Save As > Save As Type dropdown > Select .csv comma delimited > Click Save).

3. Use the .csv file to import users, import Business Object data, or import data on a scheduled basis with the Scheduler.

.CSV Reference

- In order to be imported, the .csv file must have a column name specified in the first row. Also, any 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.
  - Example:
    Mr,Mark,Jones,mark_jones@rada.com,"Rada Inc.","VP, Director, Process Excellence"
  - Example:
    Ms,Leann,Johnson,ljohnson@wavings.edu,The Wavings Institute,Information Technology
- 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.

Import Data with CSV Files

Use the Database category in the CSM Administrator to import data with .CSV files.

Run a One-Off Data Import

To run a one-off data import:

1. In the CSM Administrator window, click the Database category.

2. Select the Run a one-off data import (CSV files) task. The Import Data Wizard opens.

3. Click Next.

4. Click the Browse button to navigate to the desired .csv file.

5. Select a Primary business object to import the .csv file data into from the drop down.

6. (Optional) If configured for 3-tier database connections, enter a **timeout value** to specify the number of seconds the system should wait until the import operation times out.

7. Click Next.

8. Define how columns in the .csv file are mapped to fields:
   a. Select a column name (example: Address).

   b. Select an **Action to take**:
      i. Click the Do not import this column radio button.

      ii. Click the Import into field drop down to select a Business Object field to import the column data into.

   c. Repeat Steps A and B for all .csv column data.

9. Click Next.

10. (Optional) Click the Add button to add additional data to Business Object fields. The Populate Field manager opens.

11. (Optional) Select a **field to populate** from the drop down.

12. (Optional) Choose data to populate the field with:
    a. Click the **Expression** radio button and

    b. Select an Expression.

    c. Click the Concatenate Columns from File radio button.

    d. Click Add to select a Business Object field (example: E-Mail).

    e. Select a Separator character radio button (example: Space).

13. (Optional) Click OK. The Populate Field manager closes.

14. Click Next.

15. Define what action the Import Data Wizard should take if duplicate .csv entries are detected:
    a. Duplicate Records in the .csv file:
       i. Select the **Ignore Duplicate Entries** checkbox if you want the Import Data Wizard to ignore duplicate entries in the .csv file.

ii. Click the Add button.

iii. Select column names for the Import Data Wizard to ignore (example: the RecID column may have duplicates and the duplicates should not be imported).

b. Records in Database that Match Import File:

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)

16. Click Next.

17. (Optional) From the **Delete Existing Data** page, define whether existing data should be replaced with the newly imported data:

    a. (Optional): Select the Delete existing data from the business object before import check box to replace current data with new data from the .csv file.

    b. (Optional): If the Delete existing data from the business object before import check box is selected, the Do not delete data if import file is empty check box is enabled. 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).

18. Click Next.

19. (Optional) Select the Test Import button. After the test runs, warnings appear for any duplicate entries.

20. Click Import. The Import Data Wizard closes.

Run a Stored Import

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, the User is prompted to complete the Import Data Wizard, and then name and save the import definition.

To run a stored import:

1.

    a. In the CSM Administrator window, click the Database category, and then click the Stored Import Definition Manager (CSV Files) task.
    The Stored Import Definition Manager opens, listing existing Stored Imports.

    b. Click the Create New button ⊕.
    The Import Data Wizard opens.

    c. Follow the steps to run a One-Off Data Import, except provide a name for the Stored Import when prompted.

Import Users with CSV Files

Import internal User data to CSM through CSV files and the Import Data Wizard. User data can update existing User Records or can be used to create new User Records.

Importing Internal Users

1. In the CSM Administrator window, click the Database category.

2. Select the Stored Import Definition Manager (CSV files) task.

3. Click the New button. The Import Data Wizard opens.

4. Click Next.

5. Navigate to the desired .csv file.

6. Select UserInfo from the Primary Business Object drop-down menu.

7. (Optional) If configured for 3-tier database connections, enter a **timeout value** to specify the number of seconds the system should wait until the import operation times out.

8. Click Next.

9. In the **Set Special User Authentication Column** page of the Import Data Wizard, define user information details by clicking the Column buttons. Then, select the information that matches your .csv file (example: In the User Login ID Column field, select Windows Login ID from the Choose Value window. The Import Data Wizard matches User Login ID's with the Windows Login information in the .csv file).

   > **Note:** The UserInfo Rec ID, User Login ID, Security Group, Default Security Group, and Default Team fields are required. Selections are customizable as long as the .csv content matches the selections made.

10. Click Next.

11. (Optional) The **Map Import File Columns to Fields** page displays a list of columns from the .csv file and a list of fields that information is being mapped to. Select a row to customize how it is imported.
    a. Select the Do not import this column radio button to remove that column from the User Import.

    b. Select the Import into field radio button and choose a new field value from the drop-down menu if desired.

12. Click Next after reviewing the column mapping and making desired customizations.

13. Review additional values if any are provided. (Optional): Repeat Step 11 for the any additional values displayed.

14. Click Next.

15. Define what action the Import Data Wizard should take if duplicate .csv entries are detected:
    a. Duplicate Records in the .csv file:
       i. Select the **Ignore Duplicate Entries** checkbox if you want the Import Data Wizard to ignore duplicate entries in the .csv file.

b. Records in Database that Match Import File:

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.

Note: No unique key selection is required when importing user data. Instead, the unique keys used to check for duplicates match the RecID or Login ID column fields in the .csv file.

16. Click **Next**.

17. Provide a **name** for the import.

18. Click **Next**.

19. (Optional) Select the Test Import button.

20. Click Finish. The Import Data Wizard closes.

21. Click Run in the Stored Import Definition Manager window to run the import.

Importing Internal Users with LDAP Authentication:

1. In the CSM Administrator window, click the Database category.

2. Select the Stored Import Definition Manager (CSV files) task.

3. Click the New button. The Import Data Wizard opens.

4. Click Next.

5. Navigate to the desired .csv file.

Note: The .csv file should contain user LDAP authentication information.

6. Select UserInfo from the Primary Business Object drop-down menu.

7. Click Next.

8. In the **Set Special User Authentication Column** page of the Import Data Wizard, select the Include LDAP Authentication checkbox.

9. Define user information details by clicking the Column button. Then, select the information that matches your .csv file (example: In the Default Security Group field, select Admin from the Choose Value window. The Import Data Wizard matches user's Default Security Group with the provided Security information in the .csv file).

Note: The Security Group, Windows Login, Default Security Group, and Default Team fields are required. Selections are customizable as long as the .csv content matches the selections made.

10. Click Next.

11. Set special user LDAP authentication:
    a. Select the Column button to choose the **LDAP Username Starts With** column from the .csv import file.

    b. Select a **LDAP Directory Service** from the drop-down menu to specify the LDAP connection for the data import.

    c. Select a **Business Object Field** from the User Business object to serve as the LDAP key.

    d. Provide an LDAP domain in the Default Domain field.

    e. (Optional) Select the **Use Default Domain** radio button to use the specified LDAP domain if another is not detected from the .csv file or select the **Always Use Default Domain** radio button to always use the specified LDAP domain.

12. (Optional) The **Map Import File Columns to Fields** page displays a list of columns from the .csv file and a list of fields that information is mapped to. Select a row to customize how it is imported.
    a. Select the Do not import this column radio button to remove that column from the User Import.

    b. Select the Import into field radio button and choose a new field value from the drop-down menu if desired.

13. Review additional values if any are provided. (Optional): Repeat Step 10 for the any additional values displayed.

14. Define what action the Import Data Wizard should take if duplicate .csv entries are detected:
    a. **Skip duplicate entries:** Select this option from the drop-down menu if you want the Import Data Wizard to ignore any duplicates. Only Rec ID and/or UserId can be used to pinpoint duplicates for LDAP User Import.

15. Click **Next**.

16. Provide a **name** for the import.

17. (Optional) Select the Test Import button. After the test runs, warnings appear for any duplicate entries.

18. Click Finish. The Import Data Wizard closes.

19. Click Run in the Stored Import Definition Manager window to run the import.

Import Business Object Data with CSV Files

Import Business Object data into existing Business Objects with CSV files and the Import Data Wizard.

1. In the CSM Administrator window, click the Database category.

2. Select the Stored Import Definition Manager (CSV files) task.

3. Click the New button. The Import Data Wizard opens.

4. Click Next.

5. Click the Browse button to navigate to the desired .csv file.

6. Select a Business Object from the Primary Business Object drop-down menu.

7. (Optional) If configured for 3-tier database connections, enter a **timeout value** to specify the number of seconds the system should wait until the import operation times out.

8. Click Next.

9. (Optional) The **Map Import File Columns to Fields** page displays a list of columns from the .csv file and a list of fields that information is mapped to. Select a row to customize how it is imported.
   a. Select the Do not import this column radio button to remove that column from the User Import.

   b. Select the Import into field radio button and choose a new field value from the drop-down menu if desired.

10. Click Next after reviewing the column mapping and making desired customizations.

11. Review additional values if any are provided. (Optional): Repeat Step 10 for the any additional values displayed.

12. Define what action the Import Data Wizard should take if duplicate .csv entries are detected:
    a. Duplicate Records in the .csv file:
       i. Select the **Ignore Duplicate Entries** checkbox if you want the Import Data Wizard to ignore duplicate entries in the .csv file.

       ii. Click the Add button.

       iii. Select column names for the Import Data Wizard to ignore (example: the RecID column may have duplicates and the duplicates should not be imported).

    b. Records in Database that Match Import File:
       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)

13. Click Next.

14. From the **Delete Existing Data** page, define whether existing data should be replaced with the newly imported data:
    a. (Optional): Select the Delete existing data from the business object before import check box to replace current data with new data from the .csv file.

    b. (Optional): If the Delete existing data from the business object before import check box is selected, the Do not delete data if import file is empty check box is enabled. 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).

15. Click Next.

16. Provide a **name** for the import.

17. Click **Next**.

18. (Optional) Select the Test Import button. After the test runs, warnings appear for any duplicate entries.

19. Click Finish. The Import Data Wizard closes.

20. Click Run in the Stored Import Definition Manager window to run the import.

Configuring Database Security Rights

Use the following procedures to configure databases. Configuration procedures are completed in CSM Administrator.

To configure databases:

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.

About Data and Databases

To help beginning to use CSM, the application ships with a preconfigured Starter Database. The starter database contains all of the structure needed to use CSM (example: Business Objects, Grids, Forms, One-Steps, Search Groups, Security Groups, etc.), but there is no actual data (example: Incidents, Problems, People, etc.). For Users who want to simulate using CSM with data, CSM also provides a Demo database, complete with sample data (example: Incidents, Service Requests, People, etc.). When CSM is installed, the database is installed, and then a connection to the database is created.

> **Note:** One database can have multiple connections and having several databases is possible (example: Production/Test).

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 several databases and data in servers:

- **CSM Database:** The CSM Database is a database that stores data and all of the CSM definition-based objects, for example Business Objects, One-Steps, Expressions, etc. The CSM Database connects to External Databases, E-mail Exchange Servers, and integrations to third-party databases (ex. LDAP and Active Directory).
- **Exchange Mail Server:** CSM uses POP, IMAP, or Exchange for e-mail and event monitoring and integrates with Microsoft Outlook.
- **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.
- **Integrations:** Integration in CSM is the process of connecting CSM with a third-party applications so that the two systems can function together.

CSM has additional database tools to assist with managing a database after a connection is established and data is imported or linked. The database tools are found under Programs along with the Cherwell Management System. The database tools allow system administrators to restore the data in the database and upgrade the database to the most recent version. The final step in creating database connections is to configure database security settings to create groups that grant rights permissions to the database.

Imported/Linked Data Pros and Cons

Consider the following when deciding whether to import or link to data from an External Database.

Linked Data Pros/Cons

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 the External Business Object is marked as updatable.
Cons:
• CSM's underlying SQL queries cannot cross the CSM/External Database boundary. **Example 1:** Create a One-Step to use a Linked External Business Object, but that One-Step cannot use a CSM Business Object. Likewise, create a One-Step to use a CSM Business Object, but that One-Step 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. Imported Data Pros/Cons
Pros:
• 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 shows in CSM.

SQL Server Configuration

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.

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 th
e new Stoplist
                        ALTER FULLTEXT CATALOG [Trebuchet] REBUILD
```

Troubleshooting Data and Database

- For any problems or issues in importing, linking, or connecting to databases through CSM, contact a DBA 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, required internal system definitions.

- Typically, import data should be maintained in CSM and link to transient or reference data that can be maintained outside CSM; however, there are pros and cons of both imported and linked data.

- Only Users with permissions, for example an Administrator User, can use the Database tools.

- 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.

For OLE Database Connections

- 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.

For SQL Database Connections

- 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 Objects

- Create an External Business Object that imports data before you can import external data.

- Use a combination of imported and linked data but not within the same Business Object.

- 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.

CSV Data

- 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.

About Database Server Objects

Database Server Objects allow the User 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 CSM 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.

> **Note:** The core implementation of CSM does not require the use of Database Server Objects (stored procedures, triggers, User functions, and replication scripts), but some companies choose to use them.

To import Database Server Objects:

- If the CSM database already contains stored procedures, triggers, etc. that were created outside of the Database Server Objects manager in CSM (ex. created through SQL Server Management Studio, etc.), then import them into CSM using the Database Server Objects Import option.
- If the objects do not exist, either add objects to CSM through the user interface or use a preferred SQL tool and import the objects into CSM.

General Page

The General page is where the name for the Database Server Object is provided and the options for its type and association are selected. If the Server Object depends on a CSM Business Object, then select the relying object in the drop-down. This ensures that the trigger, stored procedure, etc. is dropped and recreated whenever the corresponding Business Object is dropped and recreated. If the Server Object depends on multiple CSM objects (ex: a view that combines multiple tables), then you can select (Multiple) in the drop-down. The multiple option allows you the option to select multiple tables.

Create Object Page

The Create Object page is where the SQL script is used to create the trigger, stored proc, etc. that will be run by Cherwell to create the appropriate Database Server Object. You can either enter the script directly, or click the Import button to import an existing object from the database so that Cherwell manages it.

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.

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. Click 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. Click the Create New button ⊕ to open the Database Server Object window.

General Page

1. Specify a **Name**.
2. Select a **Server Object** type in the drop-down.
3. Select a **Dependent Business Object** in the drop-down.
4. Select the Show all check box to display all possible Business Objects in the drop-down.
5. Specify the SQL script in the text box to create the replication script.
6. Choose the object to import and click OK.
7. Click the Check Syntax button to validate that the SQL script is correct.
8. Click OK.
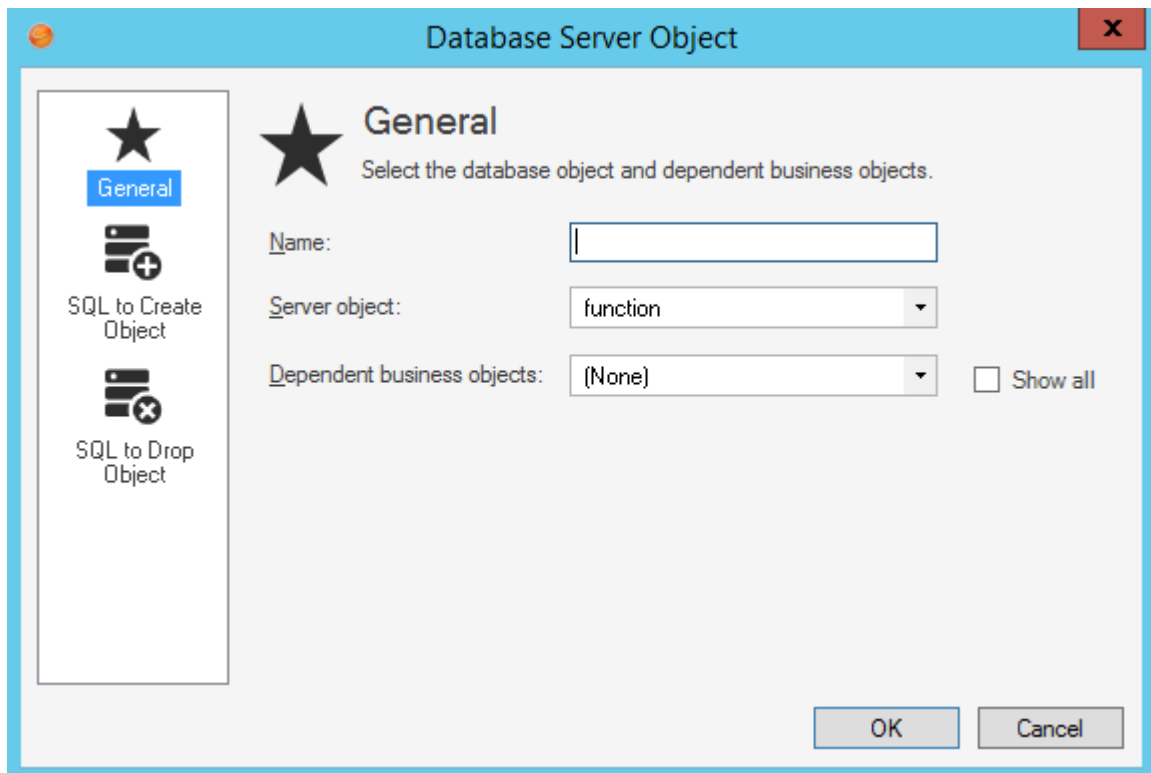
SQL to Create Object Page

1. Specify a SQL script or click Import to import a script.
2. Click Check Syntax to validate the SQL script.
3. Click OK.
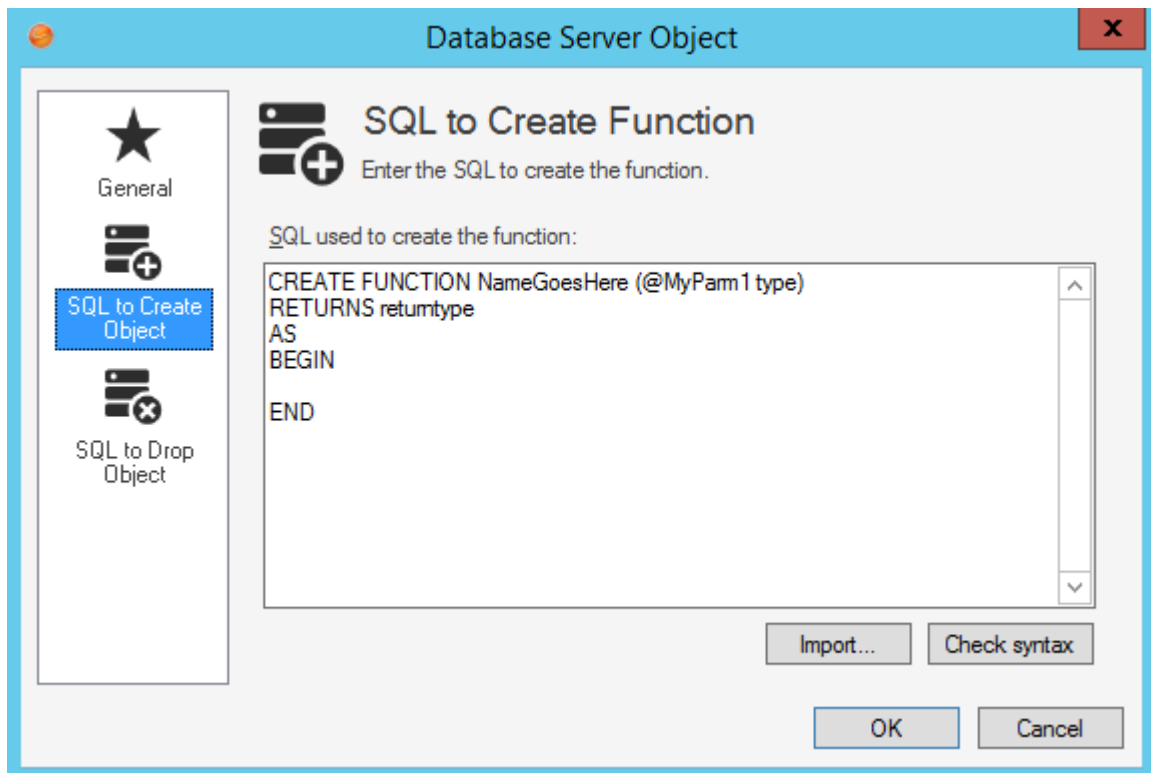
SQL to Drop Object Page

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.
Table Changed	Drops and recreates the server object whenever the CMS Business Object table is changed.
Only When Stored Procedure 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. Click OK.
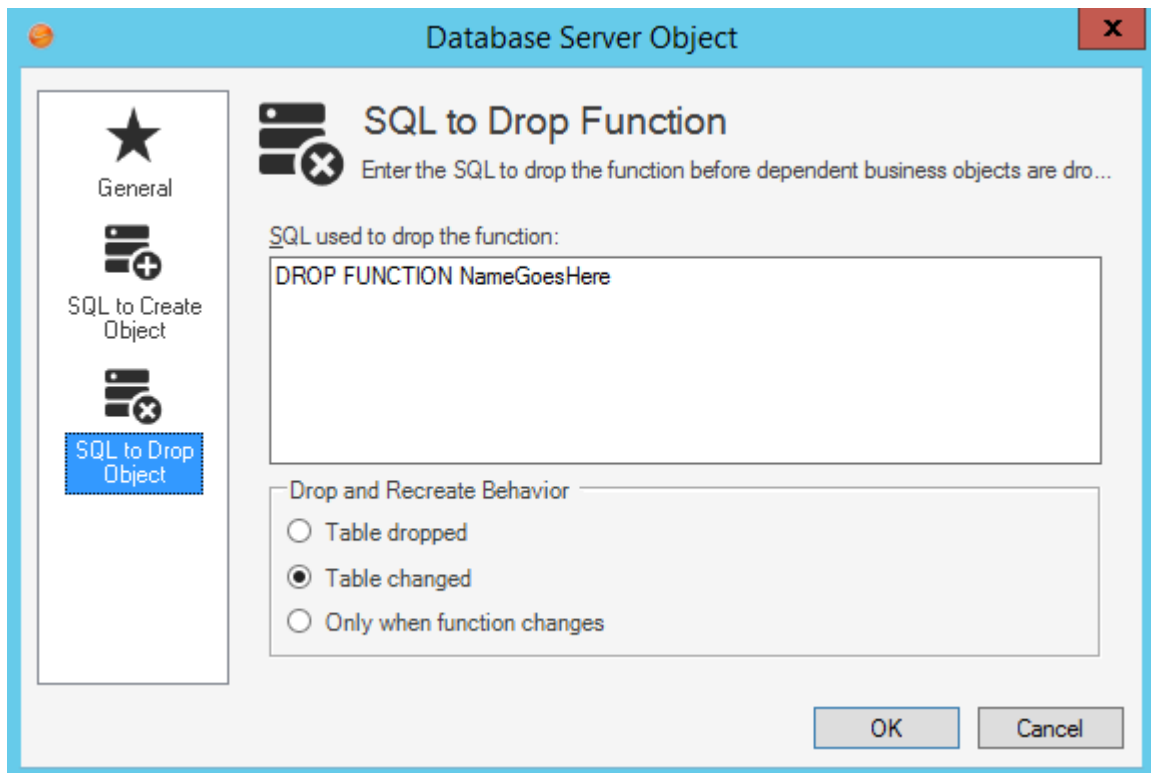
Database Server Objects Good to Know

- Choosing one of these Database Server Object types only sets up the default template for the object. Cherwell does not in any way manage or check the details of these scripts for legality (although you can confirm with SQL that the script is legal at the time you create it). For example, if you reference CSM Fields, and then later remove the referenced Fields, Cherwell does not know about the error, although the script will likely fail to be created (which will generate an error).

- You should use Database Server Object even if the server object does not depend on a Cherwell Business Object. Doing so ensures that the objects are sent and received with Cherwell when it is exported and re-imported into another database. Or, you can publish a Blueprint to a test system, and then later publish it to your live system. By having the server objects in the Blueprint, they will automatically be added to the database when the Cherwell Blueprint is published.

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.
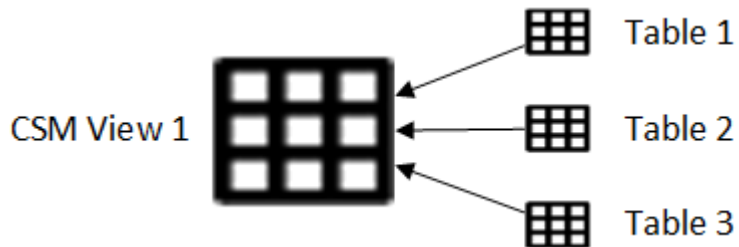
To create a CSM Database view:

1. In CSM Administrator, create a Blueprint.

2. Click 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. Click the Create New button ⊕.

   The Database Server Object window opens.

4. On the General page:
   a. Specify a **Name**.

   b. Select View in the **Server Object** drop-down

   c. Select the Business Object in the **Dependent Business Object** in the drop-down.

   d. Click OK.
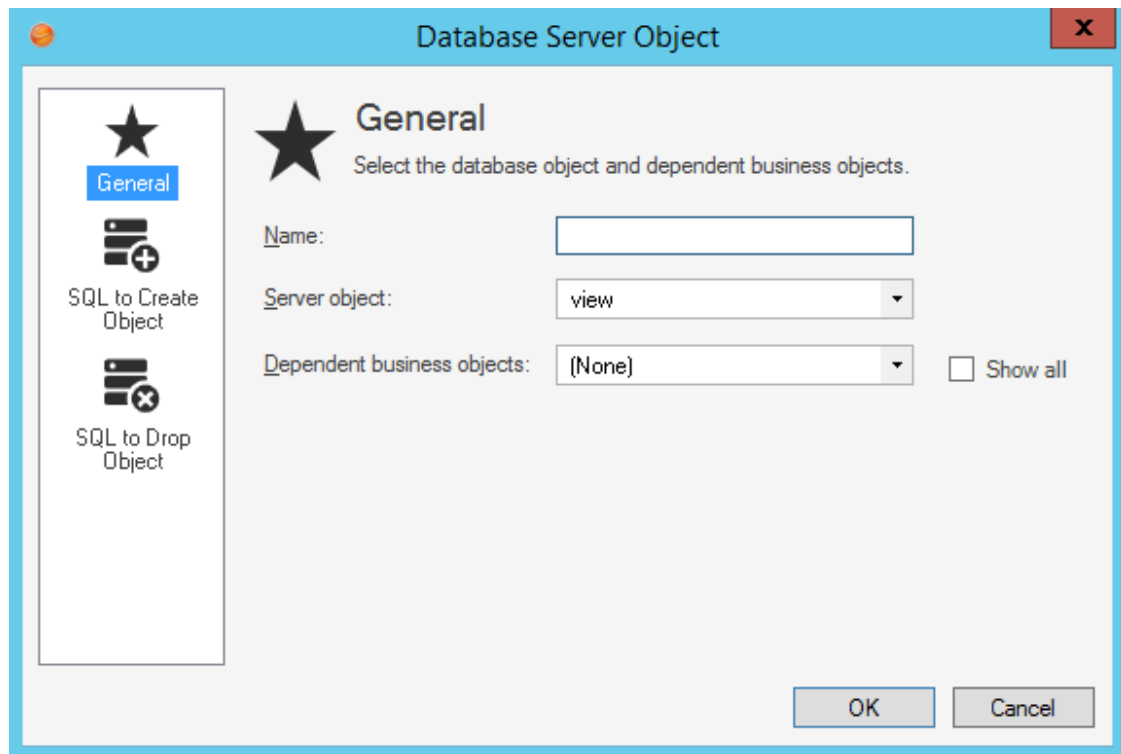
5. Click the SQL to Create Object tab.

    a. Specify a SQL script or click Import to import a script.

    b. Click Check Syntax to validate the SQL script.

    c. Click OK.
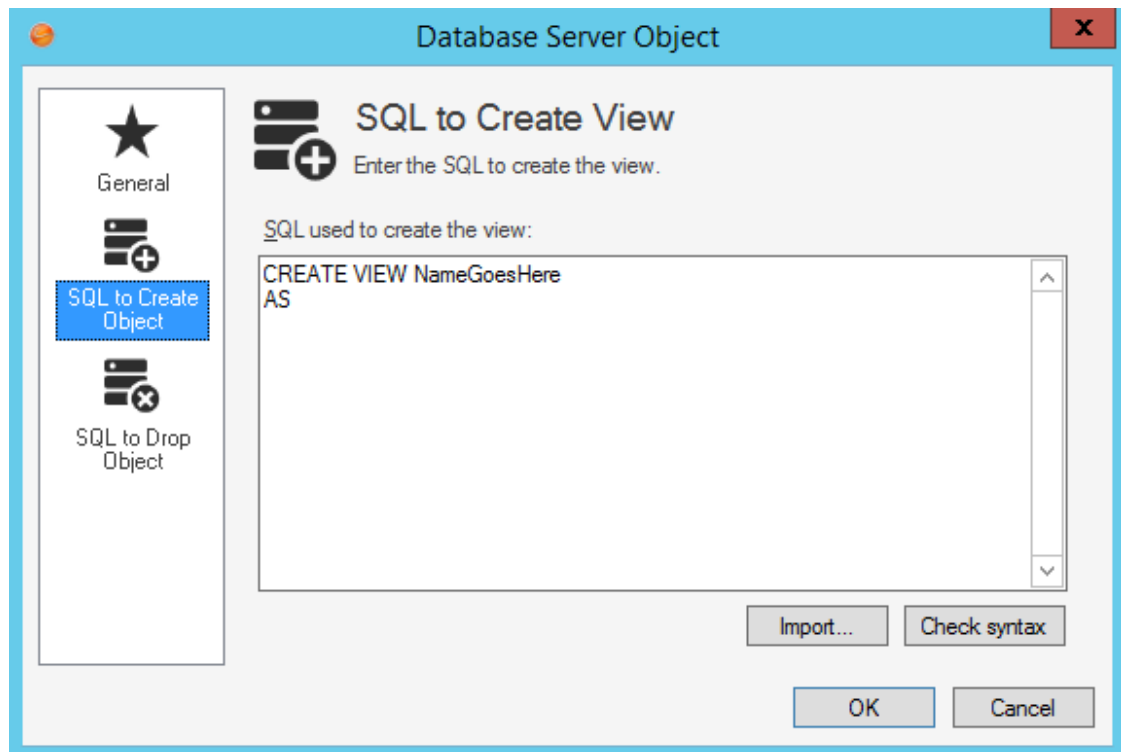
6. Click the SQL Drop Object tab.
   a. Specify a SQL drop script.

   b. Select a **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 CMS Business Object table is changed.

      iii. Only When View Changes: Creates an object in the CMS database when the Blueprint is published. Use this option to keep view with the CSM database when it is moved.

      iv. Click OK.

7. Publish the Blueprint.

Database Server Object

SQL to Drop View

Enter the SQL to drop the view before dependent business objects are dropp...

★
General

SQL to Create
Object

SQL to Drop
Object

SQL used to drop the view:

DROP VIEW NameGoesHere

Drop and Recreate Behavior

○ Table dropped
◉ Table changed
○ Only when view changes

OK   Cancel
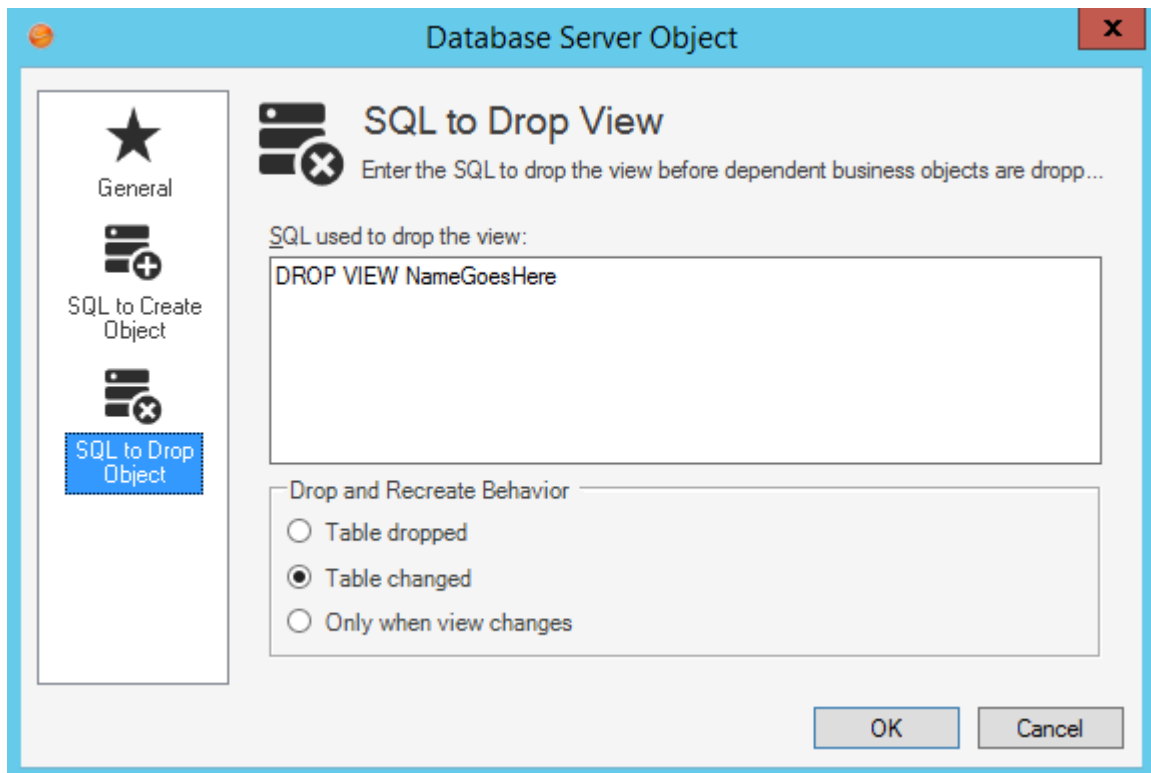
Directory Services

A directory service is a network service that stores, organizes and provides access to descriptive, attribute-based information in a directory. Information that is stored includes Users, groups, and devices.

About Directory Services

Many vendors provide implementations. On the General Options page of the Map an Object window, the Directory Service drop-down shows a complete list of available vendors. The vendor list is comprised of the following:

- 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 here, but the information is the same for any type of directory service. 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. Click the Add button to see all of the directory service fields that were not mapped and add any additional fields. There is no maximum fields allowed. Click the Delete button to remove any fields that are not necessary.

IMPORTANT: 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:** This shows the name of the CSM User Business Object that holds the LDAP data.
- **LDAP Object:** This is 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 e-mail attribute, etc. To setup additional filters, click 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

Complete the following procedures to configure the integration between CSM and a Directory Service. Most configuration procedures are completed in CSM Administrator.

> **Note:** CSM provides an OOTB Directory Service with example settings selected. Use the Directory Services Worksheet to have the necessary values specific to an organization ready for configuration.

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 is only available for LDAP connections.

Using a directory service with CSM consists of both configuring Users and Customers as shown in the figure.

Configuring Users and Customers

Configure Directory Services Settings
(User attributes are mapped to the
UserInfo object)

Users

Map Directory Service Groups to CSM
Security Groups

↓

Enable Authentication

Mapped Groups:
Accounts are created
at login.

Not Mapped Groups:
Import Users
through the User
Manager.

Customers

Map the CSM Customer object

↓

Enable Authentication

↓

Import Directory Service Data into a
Customer Business Object

↓

Batch Portal Credentials

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, click the Blueprints category, and then click the **Create a New Blueprint** task.

2. In the menu bar, click Tools>Directory Services (Active Directory, LDAP).

   The Directory Services (Active Directory, LDAP, etc.) window opens.

3. Click Add to set up a new Directory Service.

   The Map LDAP Object window opens.

4. In the Directory Service drop-down, select Active Directory.

   The window name changes to the Directory Service selected.

5. On the Map Object window, complete these tasks:
   - Define General properties.
   - Define Schema properties.
   - Define Users properties.
   - Define Groups properties. (This page is available if the Allow LDAP Users check boxes are selected on the Users page.)
   - Define Trusted Agents properties.

Define General Properties

The General page in the Map Object window in a Blueprint includes options for general information, Security, Configuration, and Searching settings, as well as a series of check boxes for mapping options.

To define General properties:

1. Open the Map Active Directory Object Window.
2. Click 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: Provide a name for the service.
- Directory Service: This is the type of directory service.
- Domain: This is the domain name of the network.
- Server: This is the host name of the LDAP directory server.

> **Note:** If you are using 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: This is 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: This is 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: Click the Question Mark to see the list of valid formats. Ask an LDAP administrator which format is being used at a specific organization.

  - Search Password: This is 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 click the Locate button. Before doing this, go to the Security section on the General properties page and verify the encryption type, User ID, and Password is 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 are:
  - 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 are:

- 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 assists to increase the speed of searching by grouping search results into pages set by the Max page size limit. The time limit is set to have the server stop 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. Click the Test Paged Search button to see if the feature is supported.

Miscellaneous Options

- Allow Business Objects to be mapped to objects: Select this check box to map CSM Business Objects to Active Directory Objects.

- Allow Business Objects to be imported from data: Select this check box to import Active Directory data into CSM.

- Client-Side LDAP (for SaaS): Select this check box to allow data to be shared from CSM to LDAP without going through SaaS. Do not select this check box unless specifically directed.

Define 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. Click the Schema page.
3. Select the Save schema first time it is read in check box.
4. Define 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	This is 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). Click the Add button to add attributes. Select an **Attribute**, and then click Delete to un-associate the attribute. Use the arrows to order the attributes.

Define Users Properties

The directory service Users page (in the Map 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 Active Directory Object Window.
2. Click 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, go to CSM **Administrator>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	This is used to 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. Click the Test button to verify the directory specified is correct.
Additional Filters When Pulling Active Directory Data:	Click Add to open a window to add additional criteria that are applied to LDAP objects when an import is done.

Define 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, best practice is to click 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 there is a security setting that is preventing it from being shown.

To define the LDAP Groups:

1. Open the Map Active Directory Object Window
2. Click 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. Click 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, best practice is to select the *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 how to run the wizard, refer to User Mapping Wizard.
Name of Active Directory User Class	This is used to 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. LDAP searches can be slow, it is best to pick the LDAP directory that contains all groups and enter that path. Click the Test button to confirm the directory is correct.
Test	Click Add to open a window to add additional criteria that are applied to LDAP objects when an import is done.

Define Trusted Agents Properties

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.
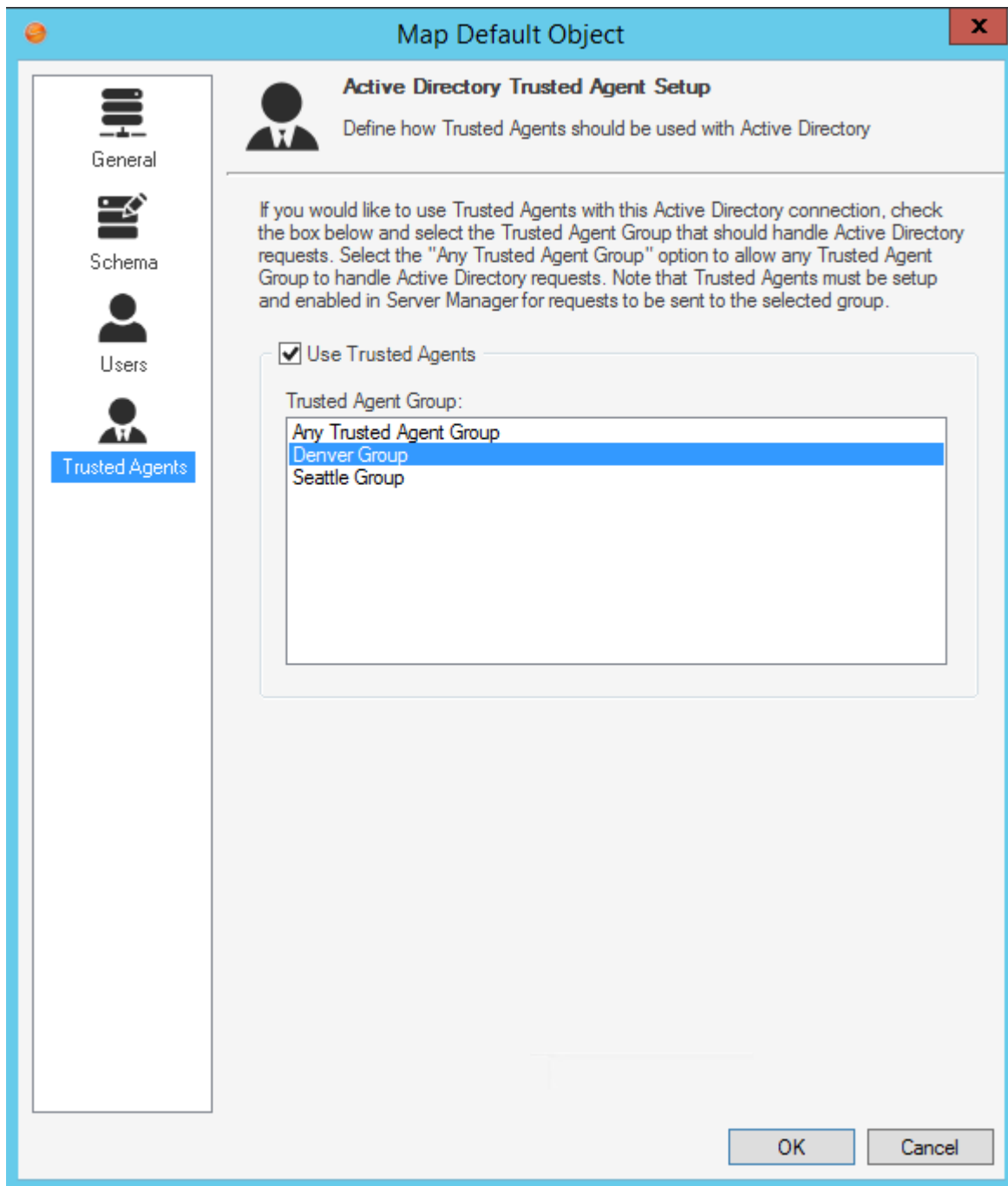
To define Trusted Agents properties:

1. Open the Map LDAP Object Window.
2. Click the Trusted Agents page.
3. Select the Use Trusted Agents check box.

4. Select one of these options:

Any Trusted Agent Group: Select to allow any group to handle requests for this Active Directory connection.

Trusted Agent Group: Select 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, then the account is created when Users login to Cherwell using their Active Directory/LDAP credentials.

   If Groups are not mapped, or the Users are entered manually, then accounts are imported using the User Manager in CSM Desktop Client.

Map Active Directory Groups to CSM Security Groups

When a User logs into CSM, the assigned security rights are based upon the CSM Security Group. When the User is a Directory Services User, the security rights only are assigned in an Active Directory Group. For this reason, 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 Directory Services Groups to CSM Security Groups:

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

   The Security Groups window opens.

2. Select the Users tab on the **Security Groups** window (the directory service must be configured in the database).

3. Click **Order groups**. If no groups are shown in the Groups section, click Add.

   The Associate LDAP Groups window opens.

4. Provide a group or set of characters in the *Starts with* text field, and then click Search.

   The available groups appear.

5. Select the groups that should be associated with this CSM Security Group and click 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 click on the Groups page to verify the Search Start settings.

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 into 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 the Security Groups window (CSM Administrator>Security>Edit Security Groups>Users tab), click Order groups.

   The Order LDAP Groups window opens.

2. Click the up or **down** 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. Click OK.

Enabling LDAP Authentication for Users

Regardless of the type of directory service being used, the selections for this setting all refer to LDAP in the UI. Before a directory service can work with CSM, LDAP must be enabled as a supported login mode in CSM Security Settings.

Note: For versions 8.3 later, LDAP authentication does not fallback 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 CSM Administrator main window, click the Security category, and then click the Edit Security Settings task.

   The Security Settings window opens.

2. Click the Desktop Client page.

3. Under Supported login modes, select the LDAP check box.

4. Click 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 set up, importing Users is not necessary, as Users are added to the system when they login.

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. Open the User Manager (CSM Administrator > Security > Edit Users).

2. In the toolbar, click the **Import Users** button ⬇ .

   The Import Users window opens.

3. Select the Directory Service Users radio button and provide the following User information:
   LDAP Directory Service: Select the created LDAP Blueprint in the drop-down.

   Starts With: Leave blank or provide a few characters to narrow the search, and then click 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 drop-down.

   Tip: If the LDAP Users are not shown, go to the Map LDAP Object window. Click the Users page to verify the Search Start setting.

   LDAP Key Field: Select the Key Field for the LDAP import in the drop-down.

4. Click 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 CSM Administrator main window, click the Create a Blueprint.
2. On the Object Manager, verify the **Major** radio button is selected.
3. Select Customer Internal.

   Note: This process can also be done on the User-Info Lookup table Object for Users.

4. Click the Edit Business Object task.

   The Edit Customer Internal Business Object Group member page opens.

5. Click on Bus Ob Properties button.
6. Click the Active Directory page.
7. Click Add.

   The Map Active Directory Field window opens.

8. Under User Attributes, select the Active Directory attribute that holds the image. The default attribute is thumbnailPhoto.
9. Click Add.
10. Select the Attribute for the image in the Map Active Directory Field window.
11. Click the Existing field radio button, and select Avatar.

12. Click OK.
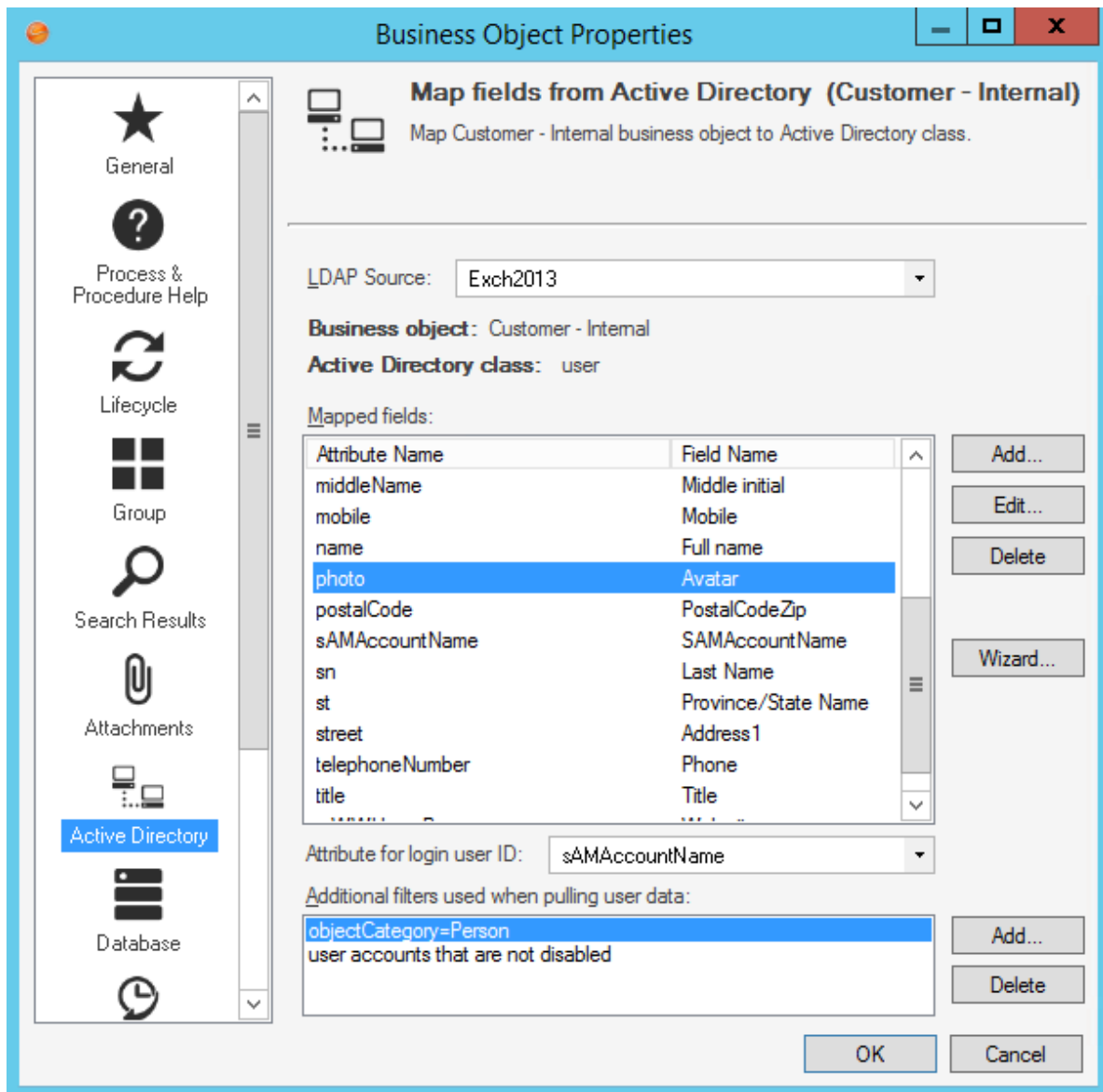
13. Click Object Manager in the Blueprints task pane.

14. Click the Lookup tables radio button.

15. Select UserInfo.

16. Click the Edit Business Object task.

17. Click the Bus Ob Properties button.

18. Click the Active Directory page.

19. Click Add.

The Map Active Directory Field window opens.

20. Under User Attributes, select the Active Directory attribute that holds the image.

21. Click the Existing field radio button, and select Avatar.

22. Click 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, Customers need to be mapped 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 the Customer-Internal Business Object. Under Structure, click Map to Active Directory to open the LDAP Mapping Wizard.

3. Click Next.

4. Select the LDAP directory service to use for the mapping, and then click Next.

5. (This step is only shown if mapping a New Object) Select if the new LDAP Business Object is part of a group:

   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 it is selected, the drop-down enables. Select an item.

   Group Members: Click 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 selected in the Blueprint.

   b. Directory Service object: Scroll down and select User.

   c. Reload Schema button: Click the Reload Schema button to reload the Active Directory objects. There is a warning 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, click the Add button.

   Note: IMPORTANT: 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 a User re-import is done.
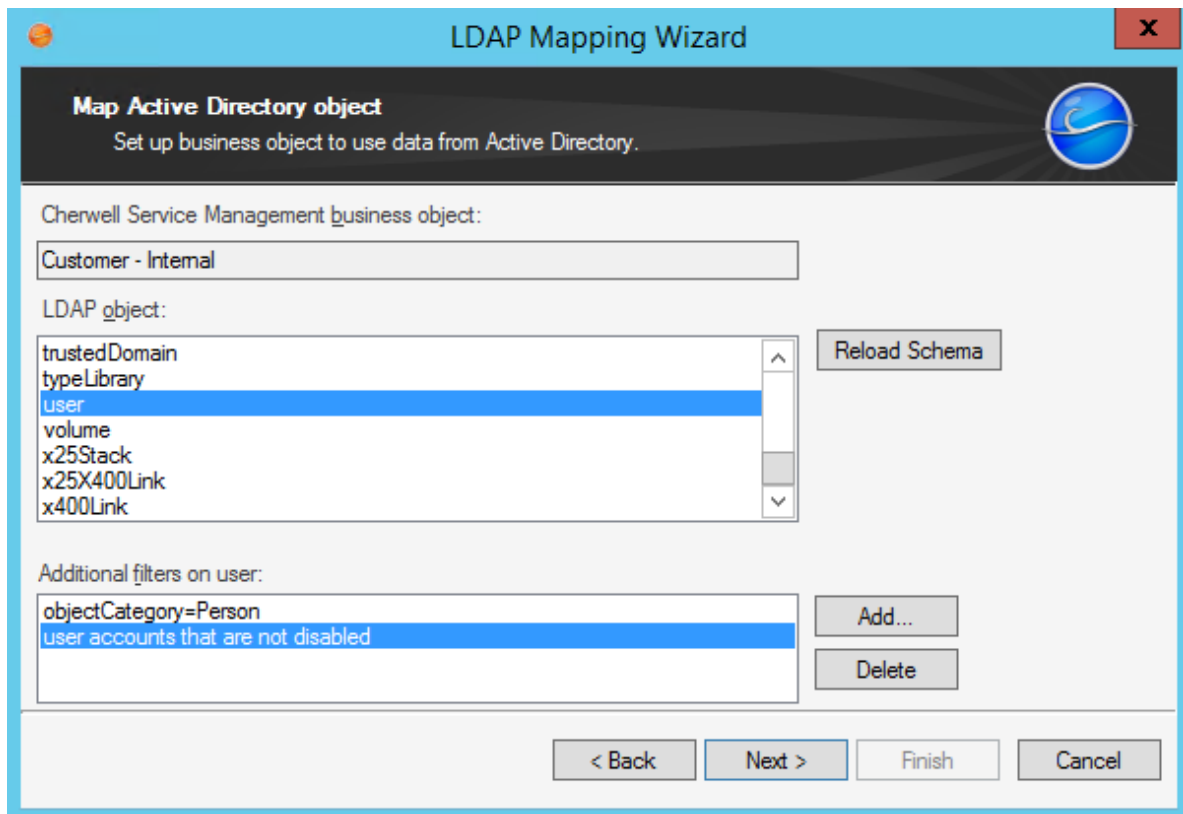
7. Click Next.

8. Click Add to add fields to map on the Map fields to LDAP attributes page to open the Map LDAP Field window.

9. Click to select the User Attribute.

10. Select either:

    New field: Creates a new field. Select an option in the Data Type drop-down and provide the size.

    Existing field: Select this radio button, and then select an already existing field in the drop-down.

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.
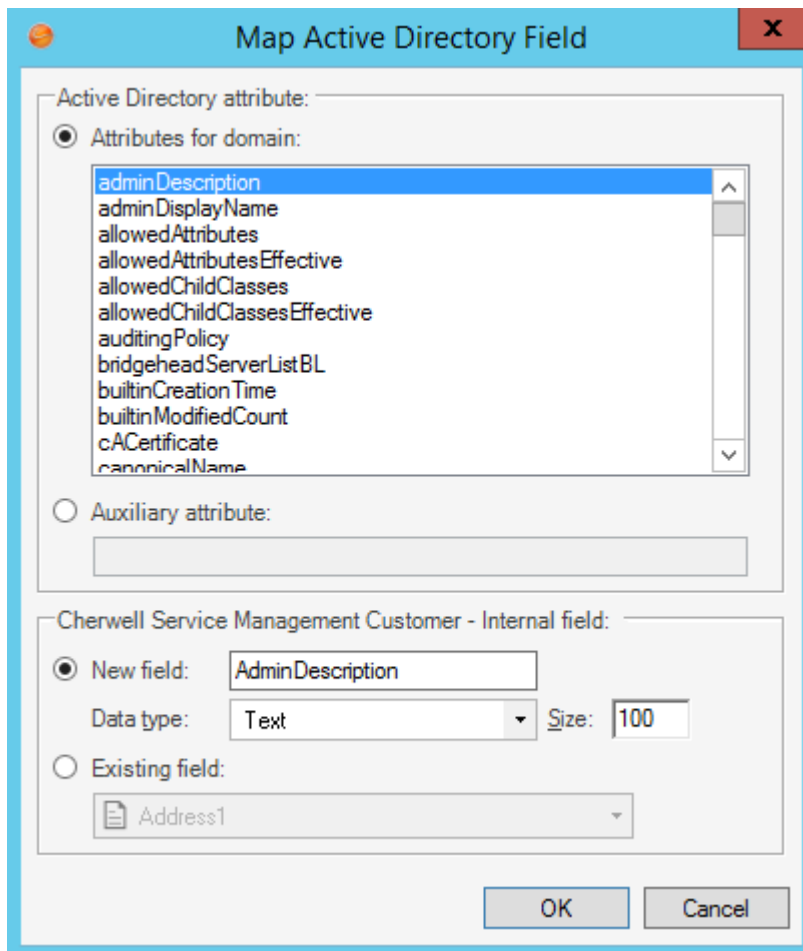
12. Click Finish.

    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.

Enabling Authentication for Customers

Regardless of the type of directory service being used, the selections for this setting all refer to LDAP in the UI. Before a directory service can work with CSM, the CSM Security Settings must be set to enable.

To enable authentication:

1. In CSM Administrator main window, click the Security category, and then click Edit Security Settings task.
2. Click the Browser Portal tab.
3. Verify the **Use Same Settings as Desktop Client** check box is selected.
4. Under the Supported login modes, verify the **Internal** and **LDAP** check boxes are selected.

> **Note:** If the LDAP check box is clear, select it.

Import Directory Service Data into Business Objects

The LDAP Import Wizard assists with importing LDAP data. Before importing data, create a Business Object to import the data into, and then complete importing Customers using the Customer-Internal Business Object. The CSM Scheduler can be used to import LDAP data at scheduled times. For more information, see Create a Scheduled Item.

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 CSM Administrator main window, click the Database category, and then the **Import from Active Directory** task (or other directory service) to open the Import Wizard.

2. Click Next.
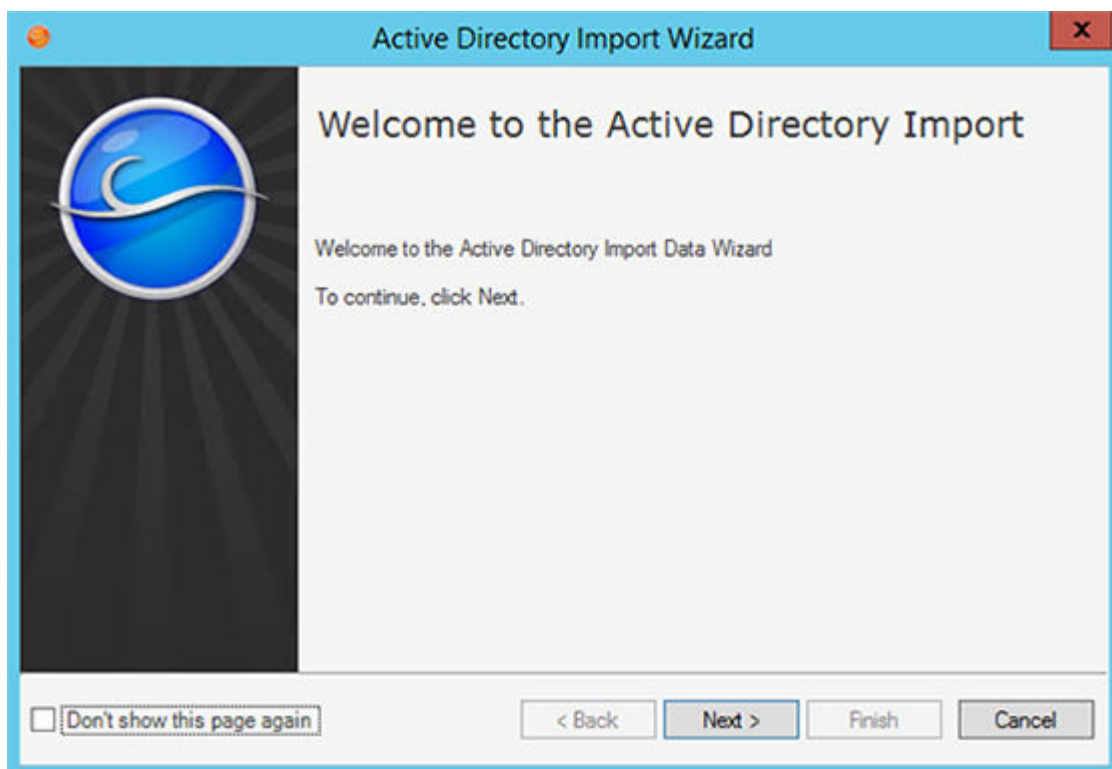
3. Select the Directory Service that was configured to Import Active Directory Users/Customers in the Customer - Internal Business Object.

4. Click Next.

5. On the Select Business Object page, click to select the Business Object that is mapped to Active Directory, and then click Next to continue.
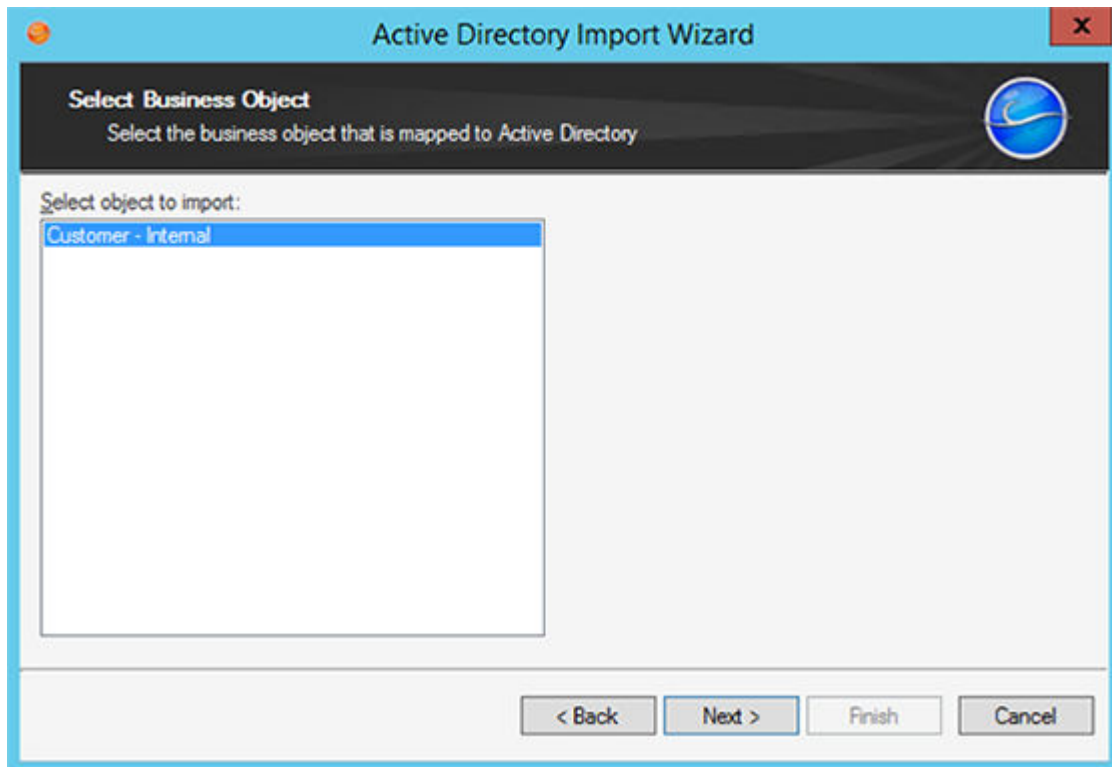
6. Select the option to either import all items or select particular ones.

    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. If any existing items should be refreshed select the **Do not update existing items** check box.

    If CSM data should not be overwritten when LDAP field is empty, select the Do not overwrite CSM Service Management field when the LDAP field is empty check box.

a. If the *Import all* radio button 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.

Click the Add button to set up additional filters or **Delete** to delete filters.
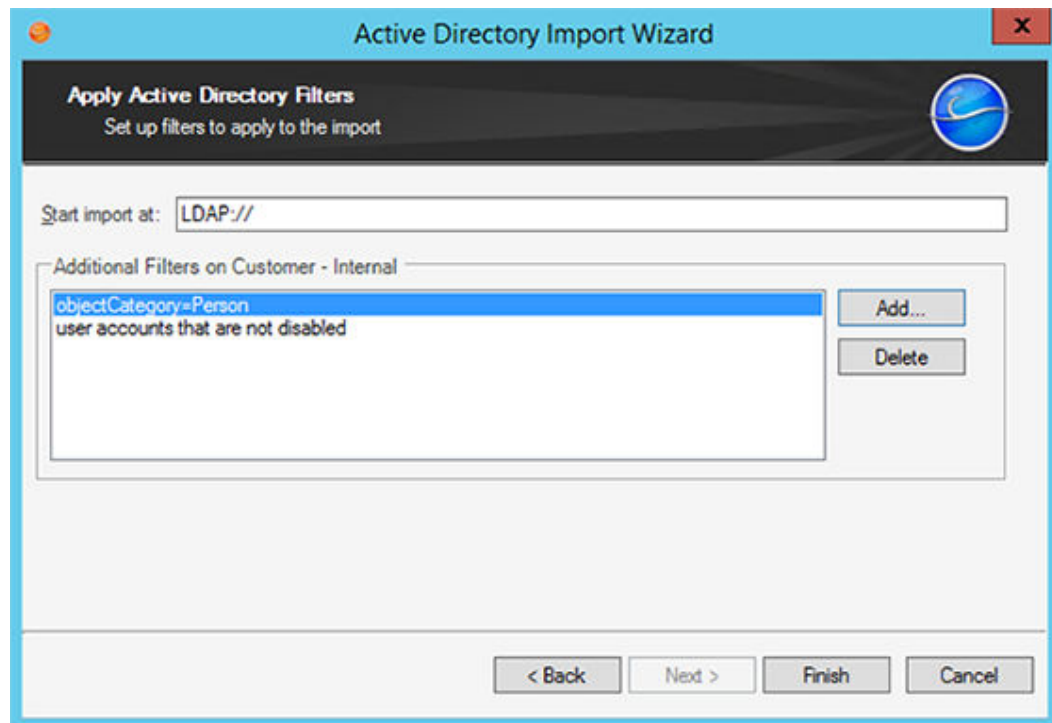
b. If the *Choose items to import* radio button is chosen, the Select Active Directory Data page opens. To view items, either leave the *Starts with* text field empty or enter a few characters in order to narrow the search.

 i. Click Search.

 ii. Click to select **Customer-Internal** items.

7. Click Finish to complete the import.

> **Tip:** Use the Scheduler (CSM Administrator>Scheduling>Edit Schedule) to import Customer data consistently at a defined date and time.
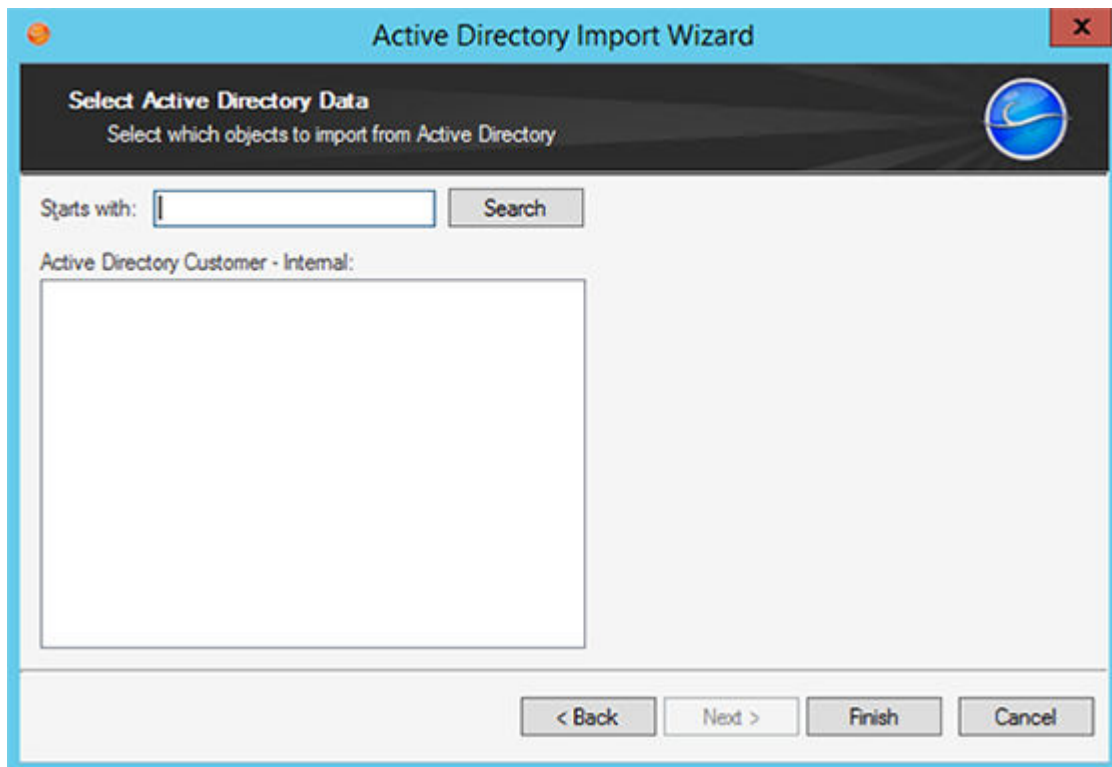
Batch Updating Customer Credentials for a Directory Service

After using the Import Wizard, use the Contact Manager in the CSM Desktop Client to view, edit, and manually batch update Customer credentials. This 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, select Security>Edit Security Settings, and select the either **Windows** or **LDAP** check boxes 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, select the Business Object that is mapped and has the imported data.
3. Click the Go button. This shows all of the Users imported from the directory service.
4. On the Menu bar, click Customer>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 the User ID Field. This is usually SAMAccountName (depending on the directory service).
   b. Customer Group: Select the Security Group to assign Users 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 this check box 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 due because of too many failed login attempts (depending on system settings).
   b. Password never expires: Select this check box to forgo 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.

      c. User cannot change password: Select this check box to restrict a Customer from changing their 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 this check box to restrict a Customer from changing the password. If a password reset is required by the system, the system administrator must reset the password.

          Note: This restarts any system administrator-scheduled password reset.

          Tip: This is an immediate reset. Use this setting if the Customer forgot the password.

      e. Password reset date: Select this check box to prompt a Customer to change the password on a specific date. Click the Date Selector button to select a reset date.

8. Select E-mail options:
      a. Select the E-mail customer new credential information check box so that Customers receive an e-mail with their User ID/password for credentials.

      b. Select the Skip customers with no e-mail addresses check box. This option is used when using Cherwell Internal Authentication. LDAP, Windows Authentication, and domain credentials do not require an e-mail.

9. Skip the customers who already have login IDs assigned: Select this check box to assign credentials only to *new* Customers (that is, skip assigning credentials to Customers whom already have them).

10. Click OK to generate the IDs.

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.
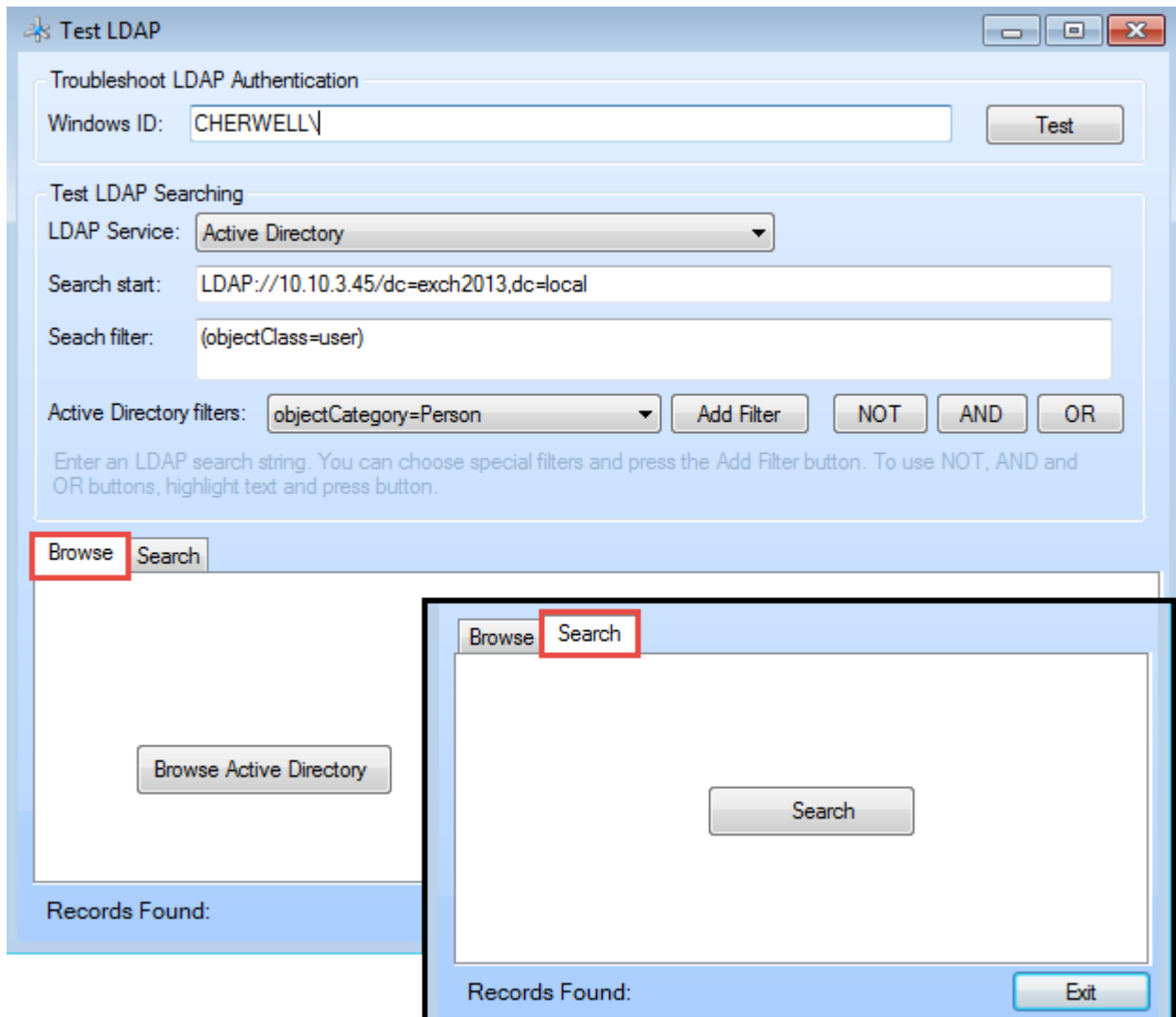
To use the Test LDAP tool:

1. Go to **Start>All Programs>Cherwell Service Management>Tools>Test LDAP**.

   The Connect to Cherwell Service Management window opens.

2. Select a connection and click OK.

The Test LDAP login window opens.
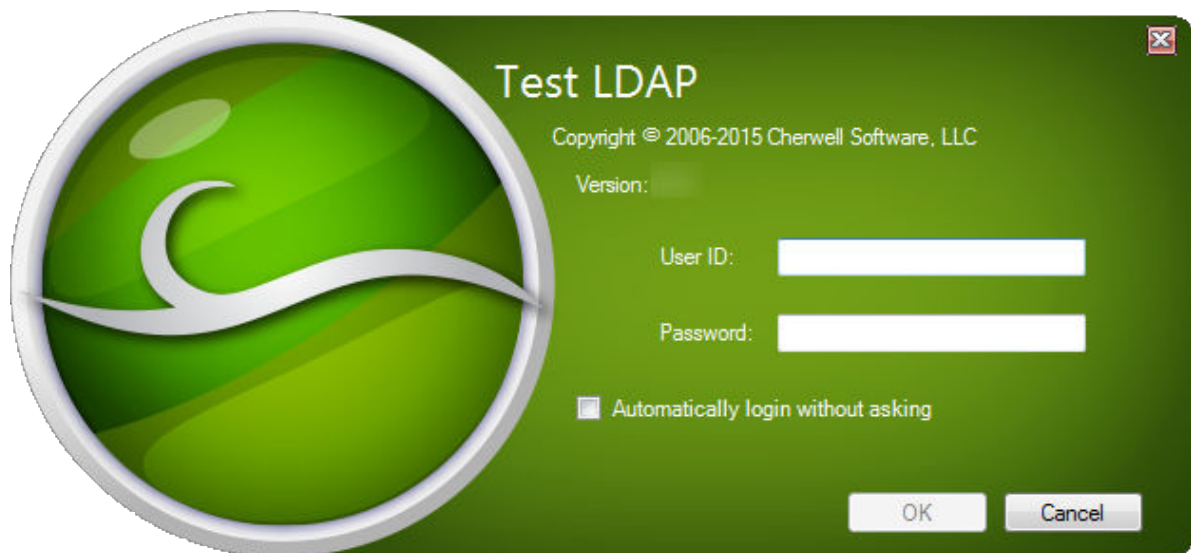
3. Provide the **User ID** and **Password**.

4. Click OK.

   The Test LDAP window opens.

5. Troubleshoot LDAP Authentication:
   Windows ID: Searches LDAP for the account in field and auto-populates with the account of the person logged into 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. Click the Browse or **Search** tab, then click:
   Browse: This runs a directory service browser and shows the different containers in a tree. Click a container to view the objects in the container.

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, e-mail addresses, etc. 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.

For more information, see Microsoft Active Directory Integration.

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. For more information, see to Lightweight Directory Access Protocol (LDAP) Integration.

Troubleshooting Directory Services

- 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 using 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.

E-mail Configuration

CSM supports sending and receiving e-mail in several different formats (POP3/SMTP, IMAP/SMTP, and Microsoft® Exchange). A variety of tools are provided to help you configure and manage e-mail.

Configuring E-mail Accounts

Complete the following procedures to configure e-mail accounts. Configuration procedures are completed in CSM Administrator and the CSM Desktop Client.

To configure e-mail accounts:

1. Configure e-mail security rights.

2. Configure global e-mail accounts: Global e-mail 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 e-mails. Make the account unavailable to Users and set it up solely as a monitored account (using the E-mail and Event Monitor).

3. Define default e-mail history attachment options: Define which records to have e-mails attached to (as Journal - Mail History Records). The e-mail history attachment options selected here are set as defaults, but Users can override them using the e-mail history attachment options in the E-mail Message window in the CSM Desktop Client.

    Note: The Business Objects might also need to be configured to receive e-mail history (see Define Default E-mail History Attachment Options) or to allow Users to e-mail Customers from a Business Object Record. For e-mails 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 OOTB system, but should be added to any new objects created. If a User tries to send an e-mail 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 e-mail accounts in the CSM Desktop Client: Customize a global e-mail account or configure a personal account for special circumstances such as sending e-mail from home or an off-site location.

Configure a Global E-mail Account

▶**3-Minute Video**: Configuring Global E-mail Accounts.

Use the Accounts page in the E-mail Options window to set up global e-mail accounts. From here Users can:

- Add an account.
- Edit or copy an existing account.
- Delete an account.
- Designate an account as the default account for sending e-mails from within CSM.
- Find dependencies.

To configure a global e-mail account:

1. In CSM Administrator main window, select the E-mail and Event Monitoring category, and then select **E-mail Accounts and Settings**.
2. Click the Accounts page on the E-mail Options window.
3. Configure an e-mail account:
   Add button: Click to select the type of e-mail account to set up (POP, IMAP, or Exchange).

   Edit button: Click to edit the settings for an existing account.

   Delete button: Click to delete an existing account.

   Note: Users might have security rights to customize global e-mail account settings, so there are several options when deleting an e-mail account. See Delete a Global E-mail Account for more information.

   Copy: Click to copy the settings from an existing account, then edit the settings as necessary.
4. Configure the account:
   a. Define settings for a global POP or IMAP account.
   b. Define settings for a global Microsoft Exchange account.
5. Spell Check E-mail: Select this check box to have CSM spell check e-mails as a message is typed (misspelled words are underlined with red lines).
6. Make Default Account: Click this button to make the selected account the default account for sending e-mails.
7. Find Dependencies: Click this button to show other CSM Items using the selected e-mail account (ex: An E-mail and Event Monitor).

Define Global POP or IMAP Account Settings

Setting up a POP or IMAP account requires:

- A name for the e-mail account.
- Incoming (POP or IMAP) and outgoing (SMTP) e-mail 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 e-mail message with a particular conversation so that it can be associated with a CSM Record. CSM inserts Conversation IDs into e-mails to identify if a particular e-mail 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.

- From Addresses that are allowed for sending e-mails from CSM.

> **Note:** The padlock button in each of the sections determines if Users can override administrative settings when they personalize a global e-mail account by defining their own personal e-mail settings. By default, server settings are locked and credentials are unlocked so that Users can enter their own user names and passwords. Click 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 click the Edit E-mail Accounts and Settings task.
2. Click the Accounts page on the E-mail Options window opens.
3. Click Add, and then select POP account or **IMAP account**.

> **Tip:** Users can also edit or copy an existing account. Click Edit to modify the settings for an existing e-mail account. Click Copy to copy the settings for an existing e-mail 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 e-mails from within CSM using this account. If the account is only used by the E-mail and Event Monitor to scan incoming e-mails, leave the check box cleared so that Users never see the account.

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:

          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 e-mail account.

      b. Password: Provide the **password** for the e-mail account.

      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. Mailbox (IMAP only): Select the mailbox (ex: Inbox) from the drop-down where the incoming mail should be stored.

8. Click 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:

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.

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.

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 e-mails.

Note: When a Conversation ID is found within an e-mail message, CSM can immediately find the record (ex: Incident) associated with the various e-mails. 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 e-mail 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 e-mails.

Add to Body: Select this radio button to include the Conversation ID in the body of outgoing e-mails.

Note: Do not delete Conversation IDs from e-mail messages. Doing so makes it harder for CSM to associate Customer replies with the correct record.

12. Click the Test Account button to ensure that e-mails can be sent from within CSM using this account.

A test e-mail is sent to the current User.

Note: All required Incoming and Outgoing Server information must be completed before testing the account.

13. **Optional**: Click the From Settings page and specify the addresses and settings associated with outbound e-mails.

14. **Optional**: Click the Trusted Agents page and define how Trusted Agents should be used with this account.

Define Global Microsoft Exchange Account Settings

Setting up a Microsoft Exchange account requires:

- A name for the e-mail 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 e-mail message with a particular conversation so that it can be associated with a CSM Record. CSM inserts Conversation IDs into e-mails to identify if a particular e-mail 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.

- From Addresses that are allowed for sending e-mails from CSM.

  Note: The padlock button in each of the sections determines if Users can override administrative settings when they customize a global e-mail account by defining their own personal e-mail settings. By default, server settings are locked and credentials are unlocked so that Users can enter their own usernames and passwords. Click the padlock buttons to change the defaults.

To configure a global Microsoft Exchange account:

1. In the CSM Administrator main window, click the E-mail and Event Monitoring category, and then click the E-mail Accounts and Settings task.

   The E-mail Options window opens.

2. Click the Accounts page.

3. Click Add.

4. Select Exchange.

   Tip: Users can also edit or copy an existing account. Click Edit to modify the settings for an existing e-mail account. Click Copy to copy the settings for an existing e-mail account, and then modify them as necessary.

   The E-mail Options window for an Exchange account opens.

5. Click the Exchange Server 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 e-mails from CSM using this account. If the account is only used by the E-mail and Event Monitor to scan incoming e-mails, leave the check box cleared so Users never see the account.

7. Define Exchange server Info:

      a. Exchange Domain: Provide the **name** of the Exchange domain.

      b. 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.

      c. Use SSL Connection: Select this check box to use SSL encryption for sending and receiving e-mails.

      d. Allow Invalid Server Certificate: Select this check box to allow e-mails 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 e-mail system.

8. Enter Account Information:

      a. User: Provide the **e-mail address** for the Exchange account.

      b. Password: Provide the **password** for the Exchange account.

      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, click 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 E-mail and Event Monitor, provide credentials here.

9. Define Conversation ID options:

      a. Add Conversation IDs to Outgoing Messages: Select this check box to include Conversation IDs in outgoing e-mails. Implementing Conversation IDs increases reliability when attempting to locate e-mails discussing specific Records.

      b. Specify where in the e-mail 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 e-mails.

         Add to Body: Select this radio button to include Conversation ID in the body of outgoing e-mails.

10. Click the Test Account button to ensure e-mails can be sent from within CSM using this account.

    A test e-mail 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 e-mail monitor.

11. **Optional**: Click the From Settings page and specify the addresses and settings associated with outbound e-mails.

12. **Optional**: Click the Trusted Agents page and define how Trusted Agents should be used with this account.

Define Default From Settings for a Global E-mail Account

A system administrator might want to control which e-mail addresses can be used to send e-mail from within CSM. Use the From Settings page to define allowed From Addresses for a POP, IMAP, or Microsoft Exchange account.

> **Note:** Many mail servers do not allow a From Address that does not match the account. In that case, limit the From Address to prevent mail from being rejected.

To define From settings:

1. In the CSM Administrator main window, click the E-mail and Event Monitoring category, and then click the E-mail Accounts and Settings task.

   The E-mail Options window opens.

2. Click the Accounts page.
3. Select a **POP account**, **IMAP account**, or **Exchange account** that is configured.

   The E-mail Options window for a POP, IMAP, or Microsoft Exchange account opens.

4. Click 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 e-mails from CSM using this account. If the account is only used by the E-mail and Event Monitor to scan incoming e-mails, leave the check box cleared so that Users never see the account.

   Note: If the general account information is defined in the settings for POP or IMAP accounts, or for Microsoft Exchange accounts, then it shows up here.

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 e-mail address as a From Address.

   Allow Arbitrary From Addresses: Select this check box to allow any valid e-mail address as a From Address.

   Note: This option is not recommended since this can be used for spam and to impersonate other Users. Also, most mail servers reject e-mails with unexpected From Addresses.

7. Provide a list of Legal From Addresses (example: servicedesk@mycompany.com, sales@mycompany.com, support@mycompany.com).

Note: The e-mail server needs to be configured to allow these From Addresses from the account.

Add: Click to add a new e-mail address as a Legal From Address.

Edit: Click to edit an existing From Address.

Remove: Click to remove an e-mail address from the list.

Note: If there is a list of Legal From Addresses, select one as the default From Address (click the Make Default Address button) that is automatically used for all e-mails sent from the account.

Tip: If all e-mails sent from a global e-mail 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.

8. Select where to send e-mails from, either:

Client: Select this radio button to have e-mails sent from the User's client machine.

Server: Select this radio button to have e-mails sent from the server.

Note: Sending e-mail 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 e-mail from the server, create a separate account for those Users.

Note: If you use Trusted Agents with the e-mail account, the e-mail source will automatically be set to Server.

Delete a Global E-mail Account

Use the Delete button in the E-mail Options window to remove a global e-mail account that is no longer needed. When deleting an account, keep in mind that Users might be using this account and might have defined personal e-mail settings for the account.

To delete a global e-mail account:

1. In CSM Administrator, click E-mail and Event Monitoring>Edit E-mail Accounts and Settings.

   The E-mail Options window opens.

2. Click the Accounts page.

3. Select the e-mail account to delete.

4. Click 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 e-mail from within CSM.

   Click OK.

6. Click OK.

Define Default E-mail History Attachment Options

In the default system, e-mails are set up to be attached to records using Journal - Mail History Records.

Note: For e-mails to be attached to a Business Object as a Journal - Mail History Record, the Business Object must have a History Relationship. For e-mails to be attached to the Customer associated with a particular Business Object (ex: Incident), the Business Object must have a Customer Relationship (ex: 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 e-mail history options, such as:

- What types of records e-mails should be attached to, either:
  - The current Business Object.
  - Customers identified from the e-mail or Business Object.

    Note: The e-mail history attachment options selected here are set as defaults, but Users can override them using the e-mail history attachment options in the E-mail Message window.

- A Conversation ID prefix that is used when Conversation IDs are embedded in e-mails. 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 e-mail message with a particular conversation so that it can be associated with a CSM Record. CSM inserts Conversation IDs into e-mails to identify if a particular e-mail 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.

To define default e-mail 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. Click the History page.

3. Define Default E-mail History Attachment Options: Specify which records get a Journal - Mail History Record when an e-mail is sent.

Current Record: Select this check box to attach e-mails to the Business Object record the User currently has in focus or has selected in a list of records (ex: An Incident Record in a search results list).

Current Record's Customer: Select this check box to attach e-mails to the Customer associated with the current record.

Recipients in To Line: Select this check box to attach e-mails to the records of Customers that CSM can identify from e-mail addresses in the To line.

Recipients in Cc Line: Select this check box to attach e-mails to the records of Customers that CSM can identify from e-mail addresses in the Cc line.

Recipients in Bcc Line: Select this check box to attach e-mails to the records of Customers that CSM can identify from e-mail addresses in the Bcc line.

Note: This option only applies to outgoing e-mail.

Parents of recipients (ex: Organization that contact works for): Select this check box to attach e-mails to the parent records of recipients. For example, if an e-mail recipient is a contact that works for a particular organization, the e-mail can be attached to the Company Record as well as the Customer Record.

4. Define remaining e-mail history attachment options:
   a. Import file attachments automatically when sending e-mail: Select this check box if file attachments sent out in e-mails should, by default, be imported and attached as part of history. This will also import attachments from all system-generated e-mails (triggered by One-Steps, Automation Processes, etc.)

   b. Message Conversation ID Prefix: Provide a prefix for Conversation IDs that are embedded in the subject or body of e-mails 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 e-mails among multiple companies that use CSM (ex: If contacting Cherwell Support).

   Tip: Click the Information button to view this same information.

5. Click OK.

Implementing E-mail Accounts

CSM provides a default e-mail system to get Users started. To implement the default e-mail system:

1. Complete the e-mail worksheet.
2. Configure test and production accounts.
3. Configure a CSM global e-mail account for testing.

   Note: This is the test account monitored by the OOTB E-mail and Event Monitor.

   a. Define account settings. Account options include:
      - POP or IMAP.
      - Microsoft Exchange.
   b. Define default From Address for the Global account.
   c. Define default e-mail history attachment options.

4. Configure a CSM global e-mail accounts.

   Note: This account is monitored by the OOTB E-mail and Event Monitor during production.

   a. Define account settings. Account options include:
      - POP or IMAP.
      - Microsoft Exchange.
   b. Define default From Address for the Global account.
   c. Define default e-mail history attachment options.

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

5. Implement E-mail notifications.
6. Configure the production e-mail account.

E-mail Worksheet

Before configuring CSM E-mail, Users must create three e-mail accounts using their own e-mail service:

- Test Receiver Account: Create a test e-mail account to receive test messages from CSM (ex: ServiceDeskTESTReceiver@company.com).
- Test Sender Account: Create a test e-mail account to send messages via CSM (ex: ServiceDeskTESTSender@company.com).
- Production Account: Create a production e-mail account to send messages via CSM (ex: support@company.com).

Depending on the type of e-mail service being used, complete one of the following worksheets to organize the e-mail information.

POP or IMAP Account

E-mail Item	Test Account (Sender) Information		Production Account Information
Account Name			
	Ex: MyDevAccount		*Ex: MyProductionAccount*
Account Username			
	Ex: ServiceDeskTESTSender		*Ex: Support*
Account Password			
	Ex: Colorado719		*Ex: Colorado719*
Incoming (POP or IMAP) Server Location			
	Ex: pop.PrimaryDomain or imap.PrimaryDomain		*Ex: pop.PrimaryDomain or imap.PrimaryDomain*
Incoming (POP or IMAP) Server Security Protocol			
	Ex: Auto, Basic, SSL, TLS		*Ex: Auto, Basic, SSL, TLS*
Outgoing (SMTP Server Security Protocol			
	Ex: smtp.PrimaryDomain		*Ex: smtp.PrimaryDomain*

Exchange Account

E-mail Item	Test Account (Sender) Information		Production Account Information
Account Name			

	Ex. MyDevAccount		*Ex. MyProductionAccount*	
Account Username				
	Ex. ServiceDeskTESTSender		*Ex. Support*	
Account Password				
	Ex. Colorado719		*Ex. Colorado719*	
Exchange Domain				
	Ex: mycompany.com		*Ex: mycompany.com*	
Server (Client Access)				
	Ex: exchange.mycompany.com		*Ex: 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 value is set to Development and controls the status of the other Current System Stored Values related to e-mail, including:

- Current System DEV E-mail Recipient: Holds the test receiver e-mail account (ex: ServiceDeskTESTReceiver@company.com).

- Current System DEV E-mail Sender: Holds the test sender e-mail account (ex: ServiceDeskTESTSender@company.com).

- Current System Production E-mail Sender: Holds the production e-mail account (ex: support@company.com).

To configure test and production e-mail accounts:
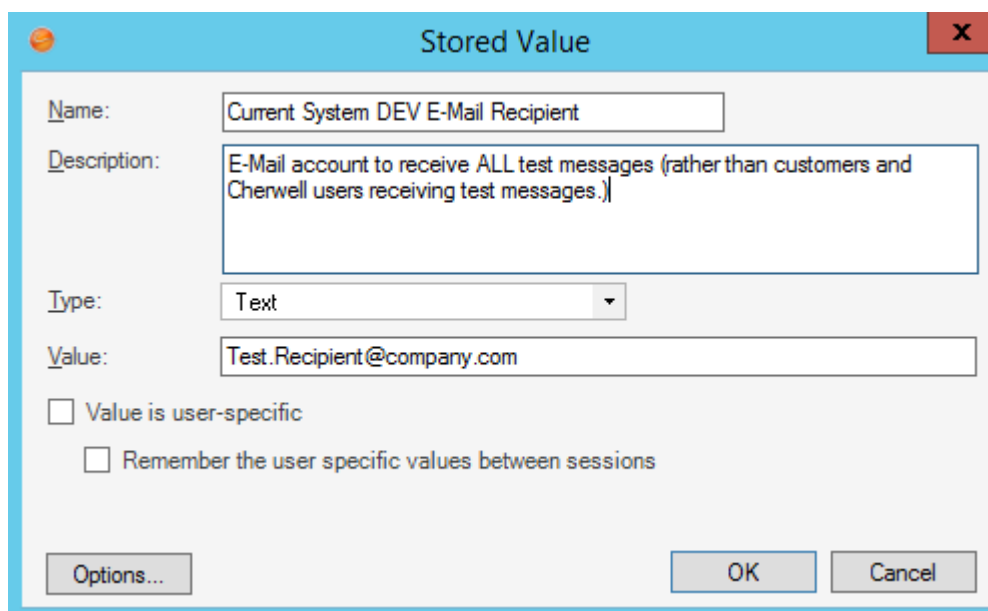
1. In the CSM Administrator main window, select the Settings category, and then select the Open Stored Values Manager task.

   The Stored Value Manager opens, listing the existing Stored Values.

2. In the Manager tree, click 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** (ex: ServiceDeskTESTReceiver@company.com).

5. Click OK.

6. Right-click the Current System DEV E-mail Sender Stored Value and select Edit.

7. In the Value field, provide the **test e-mail account address** (ex: ServiceDeskTESTSender@company.com).

8. Click 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** (ex: support@company.com).

Stored Value

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 E-mail Accounts

CSM global e-mail accounts are configured using CSM Administrator and are used to create test and production accounts.

To configure two separate CSM E-mail Accounts:

- **Test account:** Use this account while developing and testing the system. It is monitored by the E-mail Monitor during development and used as the sender account for automated test e-mails.

  Note: Use test sender account (ServiceDeskTESTSender@company.com) information on the E-mail Worksheet.

- **Production account:** Transition to this account after development. It is monitored by the E-mail Monitor during production and used as the sender account for all automated e-mails.

  Note: Use production account (ex: support@company.com) information on the E-mail Worksheet.

To set up a global e-mail account:

1. In the CSM Administrator main window, click the E-mail and Event Monitoring category, and then select the E-mail Accounts and Settings task.

   The E-mail Options window opens.

2. Click the Accounts page.

3. Click the Add button to select the type of e-mail 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 e-mails as messages are typed.

6. Click the Make Default Account button to make the selected account the default account for sending e-mails.

7. Click OK.

Implement E-mail Notifications

Use the Current System Stored Values to determine e-mail senders and recipients for e-mail notifications (ex: In One-Steps, Automation Processes, etc.). This is especially useful when e-mail templates are created, and ensures that e-mail 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 e-mail notifications sent to Customers.

Note: E-mail Actions in default Incident One-Steps use templates with the Current System Stored Values. Use these as a starting point, edit them, or create your own.

To implement e-mail notifications:

1. From a One-Step or Automation Process, create a new **Send E-mail** 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, click 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 E-mail 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 E-mail 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 e-mail address (from the e-mail 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 E-mail Account

When ready to transition the e-mail system to production, change the Current System Stored Values. By default, they are set to *Development* so that e-mails are not sent to Users and Customers during development. To activate all User and Customer e-mails, a User must set the Current System value to *Production*.

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.
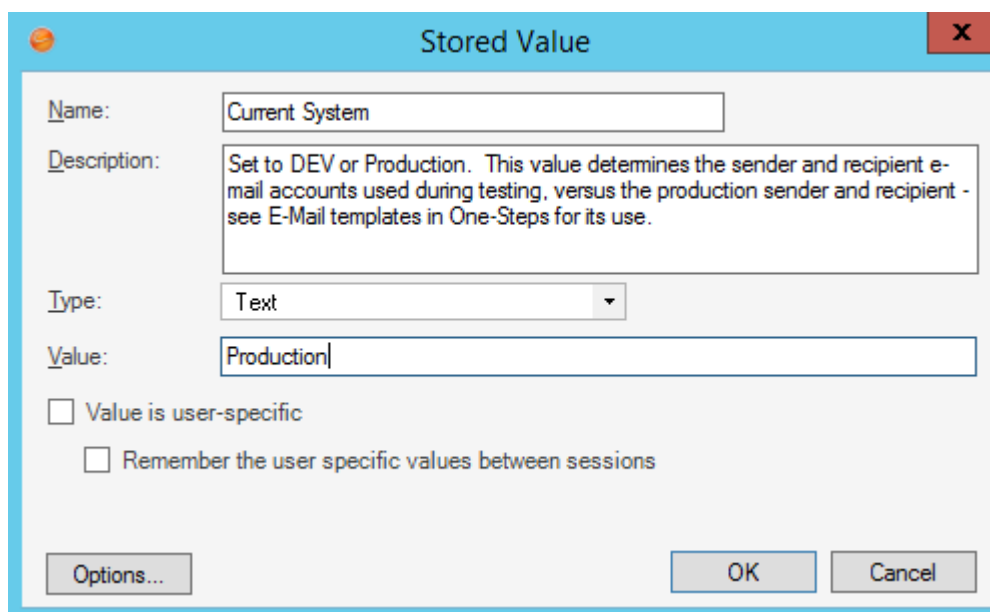
2. In the Manager tree, click the Global folder.

   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 CSM Business Object Records directly from the Outlook interface.

Configuring CSM Outlook Integration Configurations in CSM Administrator

Complete the following procedures to configure a CSM Outlook Integration Configuration. Configuration procedures are completed in CSM Administrator.

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 e-mail message with a particular conversation so that it can be associated with a CSM Record. CSM inserts Conversation IDs into e-mails to identify if a particular e-mail 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 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 e-mails.

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. Use to disable an Outlook Integration. The disable icon ⊘ indicates that an Outlook Integration is disabled. Enable/disable Outlook Integrations either by right-clicking on 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.
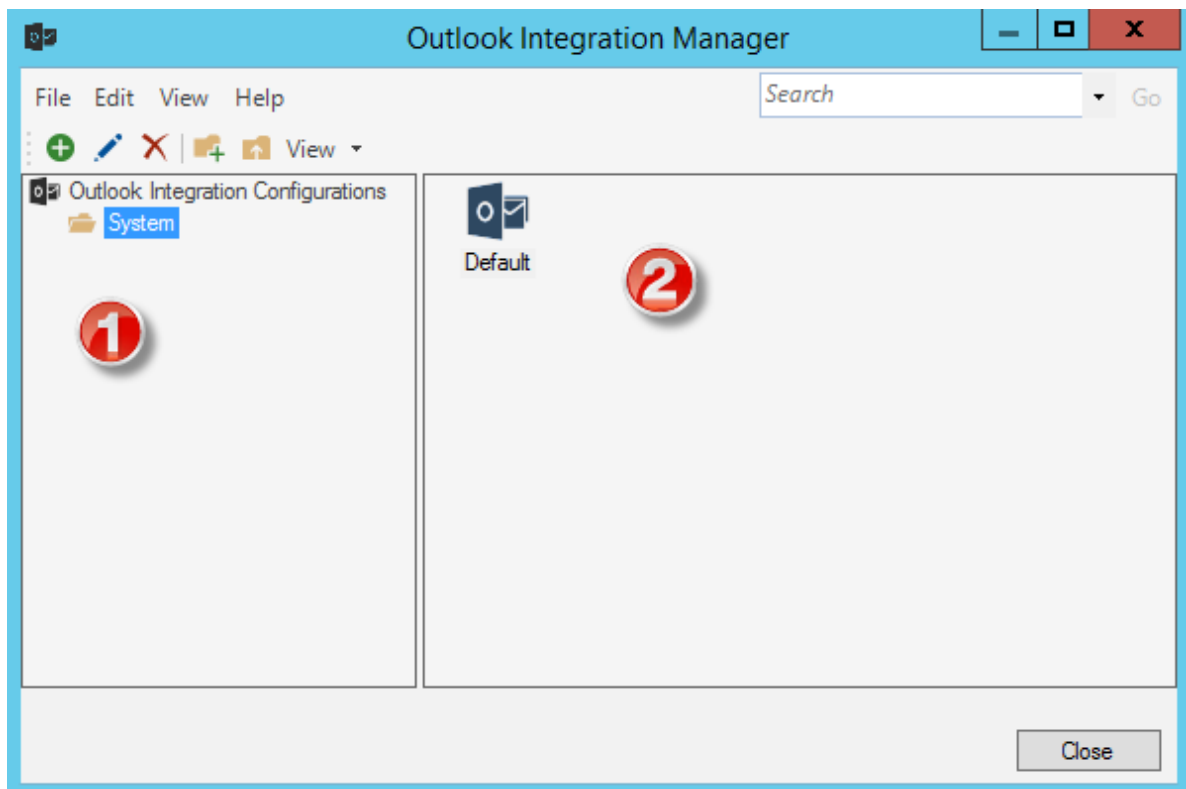
General Settings Options for an Outlook Integration

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 e-mails, 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 e-mails from a monitored folder with a Business Object Record (a Journal - Mail History Record is created). **Note:** An e-mail message is auto-linked only if CSM can identify a Customer from the e-mail, 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 e-mails 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 e-mail 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 e-mails 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 e-mails. Leave this box cleared so that other e-mail 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:** Click 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	Click this button to define Skip Item Rules for determining which incoming messages will be discarded based on defined criteria (ex: skip e-mails from automated systems).

Define Conversation ID Options	Define whether to have Conversation IDs added to outgoing e-mails.

A Conversation ID is a unique, alphanumeric identifier that correlates an e-mail message with a particular conversation so that it can be associated with a CSM Record. CSM inserts Conversation IDs into e-mails to identify if a particular e-mail 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 e-mail 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 e-mails.

Note: When a Conversation ID is found within an e-mail message, CSM can immediately find the record (ex: Incident) associated with the various e-mails. 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 e-mails. |
| Add to Body | Select this radio button to include the Conversation ID in the body of incoming e-mails.

Note: Do not delete Conversation IDs from e-mail 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 e-mails 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 e-mails are not automatically linked to Business Objects.

Note: Users can define Skip Item Rules for an E-mail Monitor.

To define Skip Item Rules:

Word/phrase	Provide the text to search for incoming e-mails.
Appears In	Select which part of incoming e-mails you want CSM to search for the specified word/phrase (ex: 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 checked, 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 checked, CSM attempts to find the Customer by e-mail 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 e-mail address in the e-mail field of the appropriate Customer Object, and then specify which field CSM should search in Customer objects. This is useful if e-mails are received from a particular company but do not necessarily know who at the company will be sending the e-mails (ex: If an e-mail comes in from Bob@Example.com, the system searches the Business Object and Field for Example.com). • Use Default E-mail Address Fields: Click this radio button to have CSM look in the Customer Object (and its associated children) in the field that is marked as the e-mail field. **Tip:** This is almost always the most appropriate option. • Search All Contact Manager Objects:Select this check box to have CSM search e-mail 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 (ex: 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-downs. **Note:** This is an advanced option for use when e-mail addresses are stored in a non-standard object for specialized use (ex: 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-downs). **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 e-mail 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 e-mail 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 e-mail (ex: 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 (click 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 e-mails from unknown addresses to a particular place for later review.

Define Which Business Objects can be Linked to Outlook E-mails

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 e-mails.

To define which Business Objects can be linked to Outlook e-mails:

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 e-mail. • Create Behavior: Defines behaviors when creating a new Business Object Record from an Outlook e-mail. • Available Actions: Adds One-Step Actions that can be executed on the linked Business Object Record.

Define General Options for Business Objects Linked to E-mails

Use the General page to define basic properties for Business Objects linked to Outlook e-mails. Define potential link items to show for the identified Customer: 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. The options in this area determine which Business Object Records the Cherwell Outlook Add-In lists as potential link items.

To define general properties for Business Objects linked to e-mails:

Related Items	Lists the most recent records based on a specified Relationship (ex: 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 (ex: 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 (ex: 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 unchecked, 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 E-mails

Use the Update Record Behavior page and the New Record Behavior page to define behaviors for updating or creating Business Object Records from Outlook e-mails.

To define update or create behaviors for Business Objects linked to e-mails:

Attach Outlook e-mail to to Business Object (ex: Incident)	Attaches incoming e-mails to linked Business Objects as Journal - Mail History Records.
Import Attachments as Part of E-mail	Imports e-mail attachments along with incoming e-mails. Options: Click 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 e-mail attachments to Business Object Records (not just to the internal copy of the e-mail). **Note:** If this option is selected, e-mail 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 e-mails with the text of the e-mail. **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 e-mails to the selected Business Object.

Attach Outlook E-mail to Customers	Attaches incoming e-mails to Customer Records as Journal - Mail History Records. Click the Options button to define which Customer Records to attach e-mails to: • **Attach to Customer (From address):** Attach e-mails to Customer Records that are identified from the addresses in the From line. • **Attach to Customers in CC Line:** Attach e-mails to Customer Records that are identified from e-mail addresses in the CC line. • **Attach to Parents of Customers (for example, company that contact works for):** Attach e-mails to Parent Records of Customer Records (for example, if an e-mail sender is a contact that works for a particular company, the e-mail 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 e-mail is attached to a specific Incident, the Customer who sent the e-mail, 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 e-mails and store them in Journal - Mail History Record as plain text. Do this to reduce the amount of space used by messages.
Actions	

Add	Click to select 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 e-mails. 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 e-mails. 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 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. Click the Ellipses button to open the Queue Manager and select a Queue. • Run a One-Step: Runs a One-Step related to the Business Object Record (of the type selected in the Objects page of the Configure Outlook Integration window). Click the Ellipses button to select an existing One-Step 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 E-mails

In addition to creating and updating records, there is a way to arbitrarily make other functionality available to execute against a linked record. For example, have 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-Steps. These Actions are shown as a drop-down 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 within the Cherwell Outlook Add-In.

To define available actions for Business Objects linked to e-mails:

Add	Select a type of Action in the drop-down. • **Add One-Step Action:** Adds One-Steps to the Actions drop-down in the Outlook Add-In to execute them directly from Outlook. Click the Ellipses button to open the Action Manager and select a different One-Step. **Note:** When this option is selected, the One-Step Manager opens, and select an existing One-Step 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 within the Outlook Add-In).
New Action General Options	• **Action:** Shows the name of the Action as it is recognized by CSM (ex: the name of the Dashboard). **Tip:** Click 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:** Click 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: Click 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:** Click 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:** Click 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, click the E-mail and Event Monitoring category, and then click 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, click on a **Role** (ex: IT Service Desk).

   b. In the Default Integration area, select a **Default Integration Configuration** in the drop-down.

   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. Click 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. Click Start>All Programs>Cherwell Service Management>Tools>Install or Uninstall Cherwell Outlook **Add-In**.
2. Click 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 e-mails to CSM Business Objects, and monitor specified folders.

Configure the Cherwell Outlook Add-In

To configure the Cherwell Outlook Add-In after it has been installed in Microsoft Outlook:

1. Click 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, click Connected. A window opens with CSM connection and login information, and the ability to edit the configuration.

2. Click Configure.

3. Check the **Enable Cherwell Integration** check box to enable the Cherwell Outlook Add-In.

4. Click 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. Click 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 (that is, Windows and/or LDAP must be supported login modes (CSM Administrator>Security>Edit Security Settings>check 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. Click 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 (ex: Inbox), and then click OK.

The Cherwell Group in the Outlook ribbon (Home tab) shows connected. Users can begin using the Cherwell Outlook Add-In.

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 server 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 server 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).
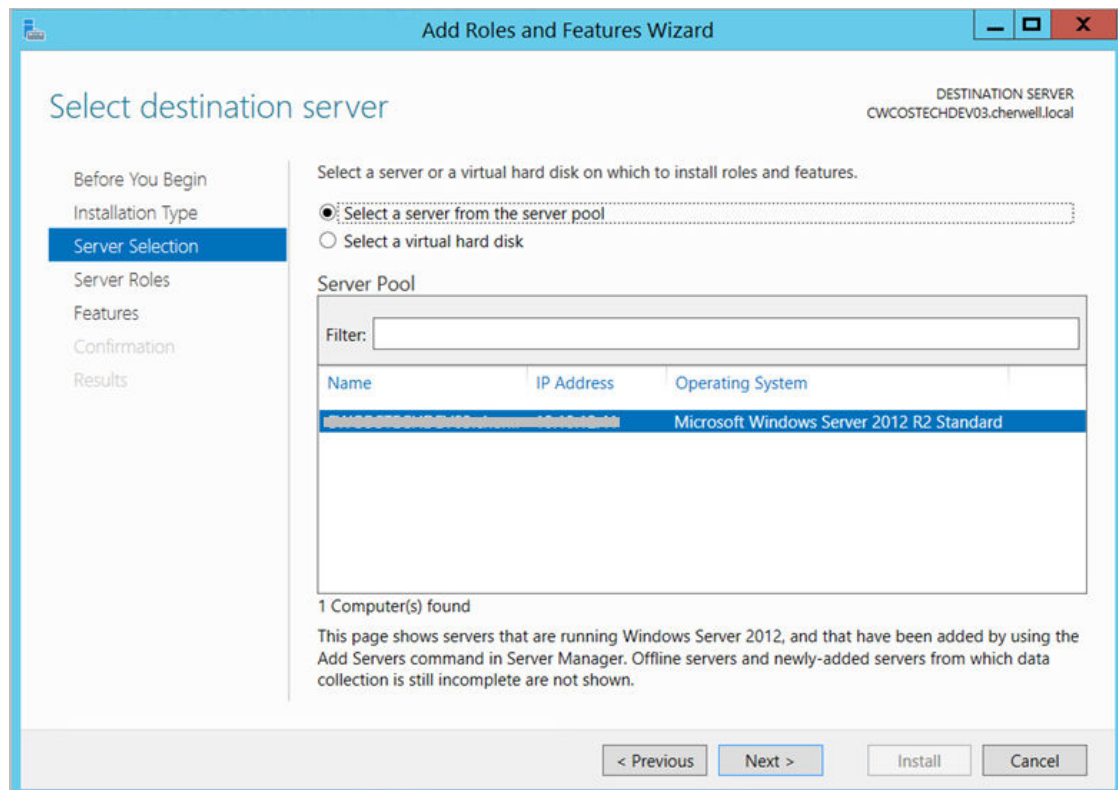
i. Click Next.

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 a SMTP Relay Server Connection, use the Administrator Client to configure CSM so that it directs e-mails to the Server connection.

To configure CSM for the SMTP Relay Server Connection, follow these steps:

1. In the CSM Administrator Client, click the E-mail and Event Monitoring category.
2. Select Edit e-mail accounts and settings. The E-mail Options Manager opens.
3. Click 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 e-mail address radio button.
10. Select the Allow arbitrary FROM adresses radio button.
11. Click Add to provide a FROM address. A Legal Return Request pop-up displays.
12. Provide an **e-mail address** in the e-mail address field.
13. Click OK.
14. Click Test Account to ensure the provided e-mail address complies with the Server Relay.
15. Click OK to save the changes and close the IMAP Account Manager.
16. Click OK to close the E-mail Options Manager.

Once the SMTP Relay Server Connection has been established and added to your CSM content, e-mails sent through CSM are automatically sent via the Relay Server Connection. To send an e-mail, select CSM Desktop Client > File > Send E-mail to open and send a new e-mail message.

About E-mail and Event Monitor

The Cherwell E-mail and Event Monitor Server is a CSM service that automatically monitors e-mail accounts and event streams, and then performs specified actions, such as creating or modifying records based on e-mail content or event details. In addition to connecting to the database server, it also has to be able to talk to the mail server (example: Microsoft Exchange). The E-mail and Event Monitor Server (referred to as the E-mail and Event Monitor) performs the following functions:

- E-mail monitoring: E-mail monitoring is a function performed by a CSM E-mail Monitor to scan an e-mail account's incoming mail and automatically perform actions based on specified conditions (example: Update an Incident record with e-mail content if an existing record can be found).

- Event monitoring: Event monitoring is a function performed by a CSM Event Monitor to detect system events (example: SMNP traps or file modifications) and automatically perform actions based on specified conditions.

> **Note:** CSM currently only supports e-mail monitoring. Event monitoring will be available in a future release.
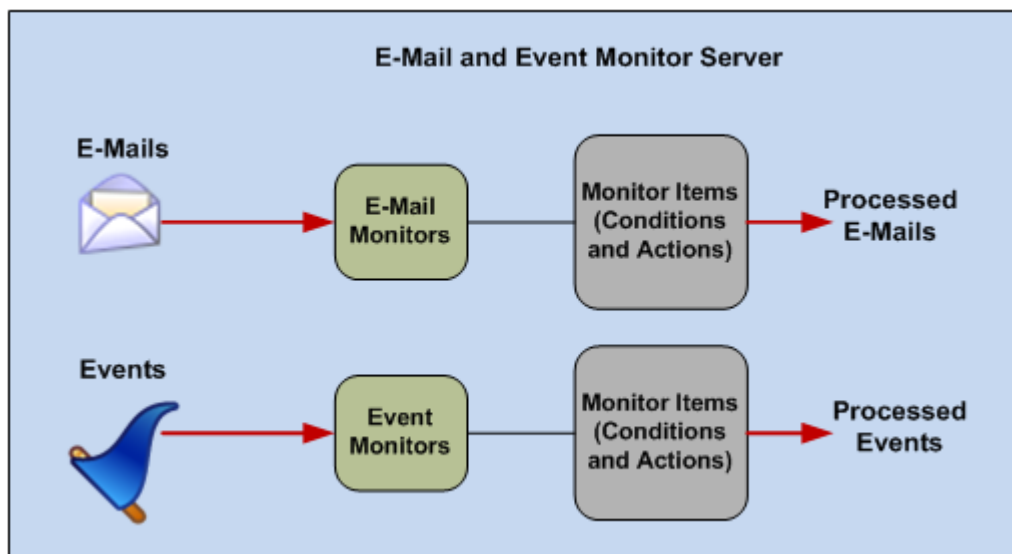
To use e-mail monitoring, there must be at least one e-mail account configured in CSM. E-mail Monitor processes incoming e-mails from a monitored account and performs actions, such as attaching e-mails to Business Object Records as Journal - Mail History Records, creating or updating records with the contents of incoming e-mails, and executing One-Steps™ against newly updated or created Business Object Records.

An E-mail Monitor is used to watch one particular e-mail account. Create as many individual Monitors as required, but do not create multiple Monitors that point to the same e-mail account unless all but one is disabled. Otherwise, the behavior of the E-mail 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 e-mails are processed according to business needs.

CSM provides a default E-mail Monitor (complete with defined Monitor Items). Implement this default design, edit it, or create a personal design using the E-mail and Event Monitoring Manager.

E-mail Monitor Good to Know

- Manage and create multiple Monitors using the E-mail and Event Monitoring Manager.

- Use E-mail Monitors to process incoming e-mails from monitored e-mail accounts.

- Each Monitor's behavior is configured using a series of Monitor Items, which include conditions and actions that define how e-mails are processed.

- 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 or Service Monitor to stop the server itself.

- Completing this process affects all enabled E-mail and Event Monitors. Also, even while the E-mail and Event Monitor Server is paused, monitored e-mail accounts, continue to receive e-mails, but those e-mails are not be processed. When the server is resumed, all E-mail and Event Monitors resume processing e-mails.

- 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 e-mail, 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.

OOTB E-mail Monitor

CSM provides an OOTB E-mail Monitor that includes several defined Monitor Items. Start with this Monitor when testing the CSM E-mail system. Later, edit the OOTB Monitor or create an E-mail Monitor to meet organizational needs.

All OOTB Monitor Items scan incoming e-mails for an existing Customer (using the E-mail Field of the Customer - Internal Business Object). If an existing Customer is not found, the Monitor uses the OOTB Customer Record as a placeholder.

The following is a summary of the OOTB E-mail Monitor Items:

- **Skip Certain Items:** Skip Item Rules are defined criteria that determine which e-mails 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 e-mails for a Conversation ID associated with an existing Incident Record. If an existing record is found, the Monitor searches the Subject line of the e-mail 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 e-mails for a Conversation ID associated with an existing Approval Record. If an existing record is found, the Monitor searches the Subject line of the e-mail 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 e-mails for a Conversation ID associated with an existing Approval Record. If an existing record is found, the Monitor searches the Subject line of the e-mail 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 e-mails for a Conversation ID associated with an existing Approval Record. If an existing record is found, the Monitor searches the Subject line of the e-mail 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 e-mails for a Conversation ID associated with an existing Incident Record. If an existing record is found, the Monitor attaches the e-mail to the Incident (including any e-mail 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 e-mail.

Using E-mail Monitoring

When working with E-mail monitoring, Users can:

- Pause/resume E-mail and Event Monitor Server processing.
- Process incoming e-mails.

> **Note:** To use e-mail monitoring, there must be at least one e-mail account set up in CSM.

To open the E-mail and Event Monitoring Manager:

1. In the CSM Administrator main window, click E-mail and Event Monitoring category, and then click the **E-mail and Event Monitoring Manager** task.

   > **Note:**
   >
   > Security rights control access to CSM functionality and are configured in the Security Group Manager in CSM Administrator (CSM Administrator>Security>Edit Security Groups).

Pause/Resume E-mail and Event Monitor Server Processing

Use the Pause/Resume Monitoring task (CSM Administrator>E-mail and Event Monitoring) to temporarily pause, and then resume E-mail and Event Monitor Server processing. This does not stop the E-mail and Event Monitor Server (service); rather, it suspends the server so that, when resumed, the server can pick up where it left off. Pause processing to suspend processing e-mails from monitored accounts, or resume processing to continue processing e-mails, starting with e-mails that are received from that point forward. The ability to pause or resume monitor processing is controlled by E-mail and Event Monitor security rights.

To pause or resume E-mail and Event Monitor Server processing:

1. In the CSM Administrator main window, click the E-mail and Event Monitoring category, and then click 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. Click OK.

Process Incoming E-mails

An E-mail Monitor processes e-mails from a monitored account according to a series of Monitor Items, which consist of actions that are performed based on a set of conditions. Configure conditions, such as finding an existing record, an existing Customer, and/or finding specified information in particular parts of an e-mail. If an incoming e-mail meets the conditions, the E-mail Monitor executes four defined actions:

- Attaching e-mails to Business Object Records as Journal - Mail History Records.
- Creating or updating Business Object Records with the contents of incoming e-mails.
- Adding newly updated or created Business Objects Records to a CSM Queue.
- Performing One-Steps against newly updated or created Business Object Records.

By default, each Monitor has Monitor Items for Skip Item Rules to exclude certain e-mails from being processed (ex: Company-wide administrative announcements) and default actions to perform if an incoming e-mail does not meet any of the conditions associated with the other Monitor Items. Configure as many additional Monitor Items as needed for a particular E-mail Monitor.

If the monitored account is an IMAP or Microsoft Exchange account, select what to do with e-mails after they are processed. Have the e-mails deleted, marked as read, or moved to a specified folder. E-mails from POP accounts are automatically deleted after they are processed (POP does not support folders).

Implementing E-mail Monitoring

When implementing e-mail monitoring:

- Use the OOTB E-mail Monitor as a starting point to implement and test e-mail monitoring.
- When ready to transition to production, configure the production E-mail and Event Monitor account.
- Create an E-mail Monitor.

Complete these steps to implement the OOTB E-mail Monitor:

1. Define the monitored account.
2. Send a test e-mail through the E-mail Monitor.

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

Define General Settings for the OOTB E-mail Monitor

The OOTB E-mail and Event Monitor provides several common monitor items. Use the E-mail and Event Monitoring Manager in CSM Administrator to define the monitored account and review OOTB monitor items.

To implement the OOTB E-mail Monitor:

1. In the CSM Administrator main window, click the E-mail and Event Monitor category, and then click the E-mail and Event Monitoring Manager task.

2. In the E-mail and Event Monitoring Manager, right-click the Demo Monitoring E-mail Monitor, and then select Edit.

3. On the E-mail and Event Monitor window, click the General page.

4. Define general properties:
   a. (Optional) Name: Provide an alternative **name** for the OOTB Monitor.

   b. (Optional) Description: Provide an alternative **description** for the OOTB Monitor.

   c. Account: In the drop-down, select the test sender account.

   d. Do not download linked images checkbox: Select this checkbox to automatically discard images that are attached to an incoming e-mail with a URL. Use this option if your server restricts outbound internet requests. Clearing this checkbox if your server restricts outbound internet requests causes the E-mail Monitor to timeout.

5. (Optional) Review the OOTB Customer Identification settings.

6. (Optional) Review the OOTB Monitor Items.

7. Click OK.

Send a Test E-mail through the E-mail Monitor

Test the OOTB E-mail Monitor to ensure that E-mail Accounts and E-mail and Event Monitor settings work properly.

To test the OOTB E-mail Monitor:

1. Send a basic e-mail to a test CSM account.
   a. Access the **test receiver account** (ex: ServiceDeskTESTReceiver@company.com) via an e-mail service.

   b. Create a **new e-mail**.

   c. Provide the **test sender e-mail address** in the To line of the e-mail.

   Note: This is the account monitored by the E-mail Monitor.

   d. Provide **Test** in the subject line.

   e. Provide **Test** in the body of the e-mail.

   f. Send the e-mail.

   The e-mail is automatically sent to the E-mail Monitor to be scanned for properties that match the defined Monitor Items. Since the e-mail does not contain any Monitor Item properties, the E-mail Monitor initiates the OOTB Monitor Item, which creates an Incident in CSM.

2. Open the Incident created by the e-mail.
   a. Open the **CSM Desktop Client**.

   b. Click Searching>All Incidents.

   A list of Incidents opens in the Main Pane.

   c. Click the **Created Date Time column header** to view the record first.

   d. Double-click the Incident to open the record in the Main Pane.

   Note: If the e-mail is not immediately visible in the list of Incidents, wait a few moments for the E-mail Monitor to recognize the account changes and scan the account. If Incident is still not visible, make sure the appropriate default E-mail Monitor settings are selected.

Configure the Production E-mail and Event Monitor Account

After testing the default E-mail Monitor using a test e-mail account and it is appropriate to transition to production, select the production e-mail account for the E-mail Monitor to use.

To select the production account:

1. In the CSM Administrator main window, click the E-mail and Event Monitor category, and then click the E-mail and Event Monitoring Manager task.

2. Right-click the Demo Monitoring E-mail Monitor, and then select Edit.

3. Click the General page.

4. Select a culture for the E-mail Monitor. For more information, see Managing the E-mail Monitor for Multiple Cultures.

5. Click the Account drop-down and select the production account (example: support@company.com).

6. Click OK.

   The E-mail and Event Monitor now monitors the production account.

7. Click **Close**.

Managing E-mail and Event Monitoring

E-mail and Event Monitors are managed using the E-mail and Event Monitoring Manager. CSM currently only supports e-mail monitoring, so the only items in the Manager are E-mail Monitors. Use this tool to:

- Create or Edit an E-mail Monitor.

- Disable an E-mail Monitor.

- Delete an E-mail Monitor.

- Pin an E-mail Monitor.

E-mail and Event Monitoring Manager

Use the E-mail and Event Monitoring Manager to complete general CSM Item Manager operations for E-mail 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.

To open the E-mail and Event Monitoring Manager from the CSM Administrator main window, click E-mail and Event Monitoring category, and then click the **E-mail and Event Monitoring Manager** task.
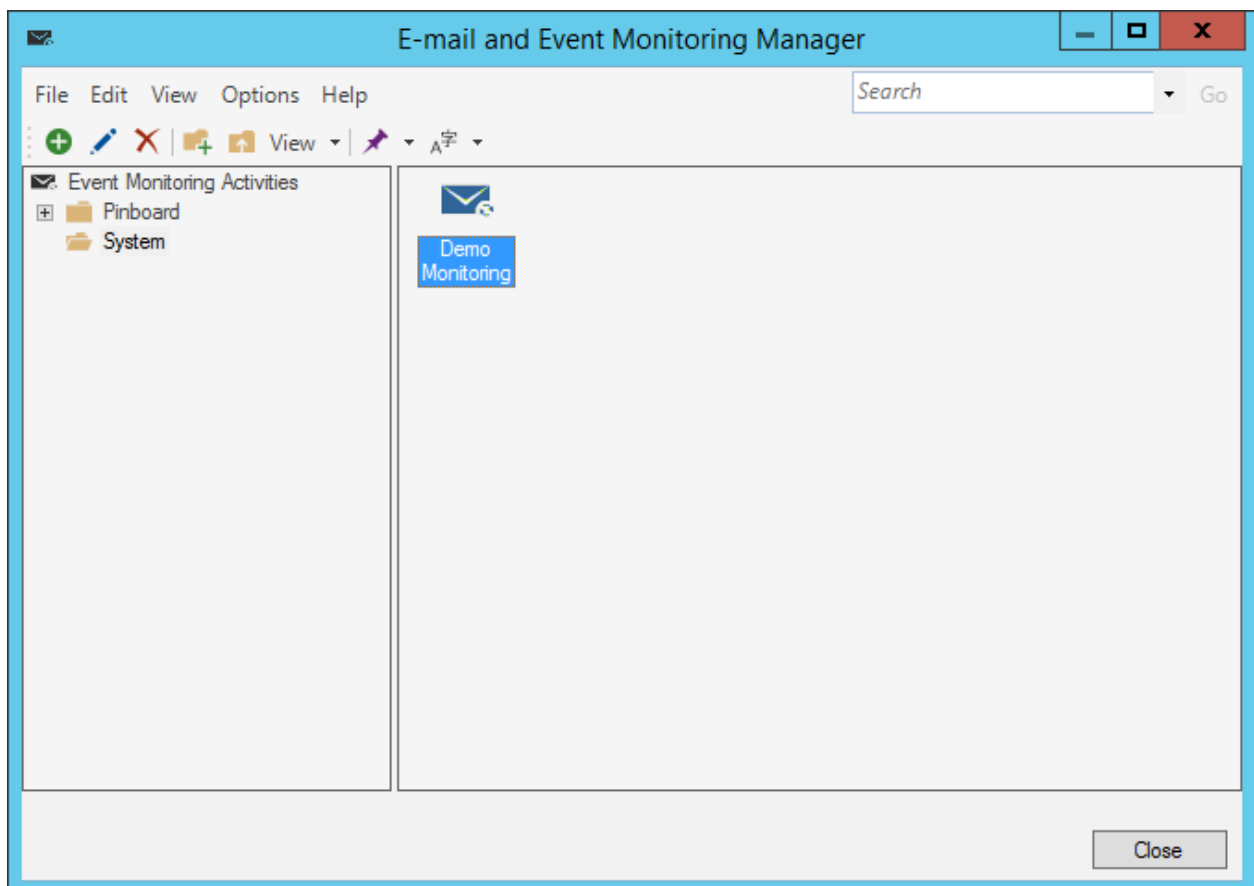
Create an E-mail Monitor

Use the E-mail and Event Monitoring Manager to create E-mail 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 e-mail account unless all but one is disabled; otherwise, the behavior of the E-mail Monitor is ambiguous.

To create a Monitor:

1. In the CSM Administrator main window, click E-mail and Event Monitoring category, and then click the **E-mail and Event Monitoring Manager** task.

2. Select a **scope** and subfolder (if needed).

3. Click the Create New button ⊕.

4. Define general options for the E-mail Monitor (General page):

   🖉 **Note:** To use e-mail monitoring, there must be at least one e-mail account set up.

5. Define identity customer options to associate with incoming e-mails (Customer Identification page).

6. Define conditions and associated actions for a Monitor (Monitors page).

7. Configure E-mail Monitors.

Define General Options for an E-mail Monitor

Use the General page in the E-mail Event Monitor window (accessed from the E-mail and Event Monitoring Manager) to define the general settings for the Monitor.

To define general settings for an E-mail Event Monitor:

Option	Description
Name	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 E-mail 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.
Description	Provide a name (this property can be searched in CSM Item Managers).
Monitor E-mail Account	Select an e-mail account to monitor. • Click the account drop-down to select an existing global e-mail account to monitor. • Click the Ellipses button to open the E-mail Accounts window and select an existing account or configure a new one if needed. • Select the Do not download linked images checkbox to automatically discard images that are attached to an incoming e-mail with a URL. Use this option if your server restricts outbound internet requests. Clearing this checkbox if your server restricts outbound internet requests causes the E-mail Monitor to timeout. **Tip:** To view e-mails accounts for all Users in the E-mail Accounts window, click View>Show E-mail Accounts for All Users. From this window, create e-mail accounts to be monitored, or edit or delete existing ones.

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 e-mails and e-mails that cannot be processed due to an error. • **Delete:** Deletes e-mails after they are processed, or if an error occurs during processing. • **Mark as read:** Marks e-mails as read after they are processed, or if an error occurs during processing. **Note:** If this option is selected, e-mails are left in the monitored folder. Periodically clear the monitored folder to prevent performance issues. • **Move to folder:** Moves e-mails to a specified folder after they are processed, or if an error occurs during processing. Select a folder in the drop-down.

Customer Identification Options for an E-mail Monitor

Use the Identify Customer page in the E-mail Event Monitor window (accessed from the E-mail 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 checked, 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 checked, CSM attempts to find the Customer by e-mail 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 e-mail address in the e-mail field of the appropriate Customer Object, and then specify which field CSM should search in Customer objects. • Use Default E-mail Address Fields: Click this radio button to have CSM look in the Customer Object (and its associated children) in the field that is marked as the e-mail field. This is almost always the most appropriate option. Search All Contact Manager Objects: Select this check box to have CSM search e-mail 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-downs. **Note:** This is an advanced option for use when e-mail 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-downs). **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 e-mail address (which can be done easily using a Text After Modifier).
Custom	Use information other than the sender's e-mail address (example: Subject) to identify Customers. In the drop-down, select what and where CSM should search: • Value to Find: Select the area of the e-mail (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 (click 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

Use the Monitors page to define Monitor Items, which consist of conditions and actions that tell a Monitor how to process incoming e-mails.

To define Monitor Items for an E-Mail Monitor:

Option	Description
Add	Adds a new monitor item.
Edit	Edits an existing monitor item.
Delete	Deletes an existing monitor item.
Copy	Cop the settings for an existing Monitor Item, and then edit the settings as necessary.
Up/Down Arrows	Click 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 E-mail Monitor Behaviors

Monitor items, with their associated conditions and actions, are at the heart of E-mail 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 E-mail 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 e-mails that the Monitor should not process.
- Default: Configure actions to execute if no other conditions in the list are found to be true.

Skip certain items is always at the top of the list, and Default is always at the bottom. Add new items between them. When adding a new item, define:

1. General settings for the Monitor Item: Name, description, and type of Business Object to associate with incoming e-mails.
2. How to identify existing records: Methods that CSM uses to identify existing records to associate with incoming e-mails.
3. Conditions for the Monitor: The conditions that must be met before the associated actions are executed.
4. Actions for the Monitor: The actions to execute if specified conditions are true.

> **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 E-mail Monitor

Skip Item Rules are defined criteria that determine which e-mails 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 (ex: If the text "[SPAM]" is found in the subject), then the e-mail message is not processed further through the list of Monitor Items. The e-mail message itself is processed according the account-specific settings for the monitored e-mail account (see the general settings for an E-mail Monitor).

Note: Define Skip Item Rules for an Outlook Integration Configuration.

To define Skip Item Rules:

1. In the CSM Administrator main window, click E-mail and Event Monitoring category, and then click the **E-mail and Event Monitoring Manager** task.

2. Click the Create New button ⊕.

   The E-mail Event Monitor window opens.

3. On the Monitors page, click Skip Certain Items..., and then click **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 e-mails.
Appears In	Select which part of incoming e-mails you want CSM to search for the specified word/phrase (ex: 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 E-mail 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. 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 e-mail.

Note: If an E-mail 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 e-mail (that passes the Skip Item Rules) received in the monitored account.

To configure the Default Monitor Item:

1. In the CSM Administrator main window, click E-mail and Event Monitoring category, and then click the **E-mail and Event Monitoring Manager** task.

2. Click the Create New button ⊕ .

3. On the Monitors page, click Default, and then click **Edit**.

4. Define general properties for the Default item (General page).

   Note: The name for the Default item (Default) cannot be edited.

5. Define how to identify existing records (ID Existing Record page).

6. Define actions for the Default item.

Configure New Monitor Items

Use the Monitors page in the E-mail Event Monitor window (accessed from the E-mail and Event Monitoring Manager) to add or edit Monitor Items.

To configure E-mail Monitor Items:

1. In the CSM Administrator main window, click E-mail and Event Monitoring category, and then click the **E-mail and Event Monitoring Manager** task.

2. Click the Create New button .

3. On the Monitors page, select a monitor and click **Add** or **Edit**.

4. Define general options: Name, description, and type of Business Object to associate with incoming e-mails.

5. Define identify existing record options: Methods that CSM uses to identify existing records to associate with incoming e-mails.

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 for a Monitor Item.

To define general settings for E-mail Monitor Items:

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 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 e-mails.

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 e-mail message. **Note:** This is the simplest and most reliable way of finding an existing record, but it only works if an incoming e-mail is a reply to a CSM e-mail. When an e-mail 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 e-mail message. • Ignore Short Subjects: CSM ignores subject lines that are less than 10 characters. **Note:** For this option to work correctly, the original e-mail 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 (ex: 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 e-mail message. This is useful receiving messages from automated systems, or if e-mail senders use a template that always includes the Record ID in the subject.
Look for number	CSM searches an e-mail subject for the first whole number.
Number at end of subject	CSM searches for a number as the last item in an e-mail subject
After term	CSM searches for a Record ID that appears after a particular term. Provide the term (ex: 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 e-mail message.
After term	CSM searches for a Record ID that appears after a particular term. Provide the term (ex: 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 of the Business Object chosen in the general settings and varies depending on the object (ex: 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 (ex: Approval), 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: Click 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: Click 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.

Field/
Operator/
Value
	Select these check boxes to have associated actions executed if the specified fields and values are found.
	
	• Field drop-down: Select a part of the e-mail message (ex: Subject and Body Combined) to search.
	
	• Operator drop-down: Select an operator.
	    • Equals: Finds e-mail items where value in field equals value in right-most drop-down.
	    • Not equal: Finds e-mail items where value in field does not equal value in right-most drop-down.
	    • Like: Finds e-mail items where the value matches the value and its wildcard in the right-most drop-down. (ex: Jo% will find Joe, John, etc.).
	
	    Note: Use % or * as the wildcard character. For example, enter John % to find all e-mail 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 e-mail items that do not match a value and its wildcard.
	    • Empty: Finds all e-mail items where the field value is empty.
	    • Not empty: Finds all e-mail items where the field value is not empty.
	    • Greater than: Finds all e-mail items where the value is greater than the value in the right-most drop-down box.
	    • Greater or equal: Finds all e-mail items where the value is greater than or equal to the value in the right-most drop-down box.
	    • Less than: Finds all e-mail items where the value is less than the value in the right-most drop-down box.
	    • Less or equal: Finds all e-mail 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 e-mail items that contain the text in the right-most drop-down box.
	    • Does not contain: Finds e-mail items that do not contain the text in the right-most drop-down box.
	    • Begins with: Finds e-mail items that begin with the value in the right-most drop-down box.
	    • Ends with: Finds e-mail items that end with the value in the right-most drop-down box.
	    • Is: Finds e-mail items where value in field is an exact match to value in right-most drop-down.
	
	• Value: Provide a keyword or phrase, select a date/time, etc.
	
	Note: The operators and values vary depending on the fields chosen. For example, if Has Attachments is selected in the Field drop-down, then the available operators are Equals or Not Equals, and the available values are True or False.

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 e-mail 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 E-mail 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 e-mails to Business Objects as Journal - Mail History Records.

Import attachments as part of e-mail	Imports e-mail attachments along with incoming e-mails. Options: Click 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, 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 e-mail attachments to Business Object Records (not just to the internal copy of the e-mail). **Note:** If this option is selected, e-mail 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 e-mails with the text of the e-mail. **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 e-mails to the selected Business Object.
Attach e-mail to Customers	Attaches incoming e-mails to Customer Records as Journal - Mail History Records. Click the Options button to define which Customer Records to attach e-mails to: • Attach to Customer (From Address): Select this check box to attach e-mails 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 e-mails to Customer Records that are identified from e-mail addresses in the CC line. • Attach to Parents of Customers (example: company that contact works for): Select this check box to attach e-mails to Parent Records of Customer Records (example: If an e-mail sender is a contact that works for a particular company, the e-mail 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 e-mail is attached to a specific Incident, the Customer who sent the e-mail, 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 e-mails 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	Click 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 e-mail contents and the values of those Fields. To retrieve data from within an e-mail message, insert the appropriate E-mail 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 e-mail 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 e-mails. Specify which Fields are updated and the values of those Fields. Defining custom actions is not needed to have an e-mail attached to a Business Object Record as a Journal - Mail History Record. Selecting the Attach e-mail 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. Click the Ellipses button to open the Queue Manager and select a Queue. • Run a One-Step: Runs a One-Step related to the Business Object Record (of the type selected in the General page of the Event Monitor Condition and Action window). Click the Ellipses button to select an existing One-Step or create a new one. If a One-Step is created or edited from here, that One-Step has access to e-mail-specific data, such as the e-mail address of the sender, the subject line, etc. If the One-Step is created elsewhere and needs to reference One-Step Tokens, set Show Custom Tokens to E-mail on the Conditions page of the One-Step.
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 e-mail attachments from the database, you must uncheck **all** these options:

- Import attachments as part of e-mail
- Attach e-mail attachments to Incident
- Attach inline images to Incident

Disable a Monitor

Use the E-mail and Event Monitoring Manager to disable specific Monitors. 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.

Good to know:

- Disabling a specific Monitor only disables a specific Monitor that is selected. It is not the same as pausing the E-mail and Event Monitor Server, which affects all enabled Monitors.
- When an E-mail Monitor is disabled, the monitored e-mail account continues to receive e-mails. However, those e-mails are not processed according to the rules in the disabled Monitor.

To disable an E-mail Monitor:

1. In the CSM Administrator main window, click E-mail and Event Monitoring category, and then click the **E-mail and Event Monitoring Manager** task.
2. Select the Monitor to disable.
3. Click Edit>Disabled (or **right-click>Disabled**).

   The selected Monitor is disabled, and a disable icon ⛔ appears on the item in the E-mail and Event Monitoring Manager.

Configuring E-mail Monitors

Complete the following procedures to configure E-mail Monitors. Configuration procedures are completed in CSM Administrator.

To configure E-mail Monitors:

1. Configure E-mail and Event Monitor security rights: Configure who can access E-mail and Event Monitor functionality and data.

2. Configure E-mail Monitor Behaviors: Configure Monitor Items that define how e-mails are processed (which actions to execute based on specified conditions).
   a. Configure Skip Item Rules: Configure rules for eliminating e-mails that should not be processed by the Monitor. This is always the first item in an E-mail Monitor and cannot be deleted.
   b. Configure Default Actions: Configure actions to execute if no other conditions in the list are found to be true. This is always the last item in an E-mail Monitor and cannot be deleted.
   c. Configure New Monitor Items: Configure additional items for processing e-mails according to organization needs.

System Analyzer

The System Analyzer is a tool that allows advanced Users to track behind-the-scenes operations in a live environment directly from the CSM Desktop Client. The System Analyzer can be used for troubleshooting and assessing performance.

About the System Analyzer

3-Minute Video: 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-Steps.
- System exceptions and errors.
- Technical logging information.

Track all messages or define breakpoints to pause the application when a specific message is found. The System Analyzer allows Users to step through operations individually to see what is happening behind-the-scenes.

The System Analyzer includes multiple features, including:

- System Analyzer window.
- Current Object views.
- Message category configuration.
- Export capabilities.
- Latency options.
- Breakpoints.
- Message detail views.

CSM provides an OOTB System Analyzer configuration. Use the configuration as-is, edit it, or define your own using the System Analyzer window.

System Analyzer Good to Know

- Open the System Analyzer in the CSM Desktop Client by clicking **Help>System Analyzer**.

- Categories allow you to filter which messages the System Analyzer tracks.

- The following message categories are selected by default: Business Object, BusOb Load Timing, Error, One-Step, 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.

- You can simulate Latency to understand how configuration affects the User experience for Customers accessing the server from a distance.

- Breakpoints allow you to pause CSM when a specific message is found.

- You can view Business Object Fields and values directly from the System Analyzer window to troubleshoot logging information related to table validation.

- You can export data from the System Analyzer using multiple formats, including CSV (.csv), HTML (.html, .htm), Plain Text (.txt), Rich Text (.rtf), and XML (.xml).

- CSM provides an OOTB System Analyzer configuration. Use the configuration as-is, edit it, or define your own using the System Analyzer window.

Always consider the following:

- CSM is highly configurable. As a result, a User's system may vary from the Out-of-the-Box content in our documentation.

- Security rights control access to CSM functionality and are configured in the Security Group Manager in CSM Administrator (CSM Administrator>Security>Edit Security Groups). System Analyzer security rights are grouped with Tools security rights. For more information, see Configure Tools Security Rights.

System Analyzer Window

The System Analyzer window opens independent of the CSM Desktop Client (Help>System Analyzer). Use the window to complete the following operations:

- 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.
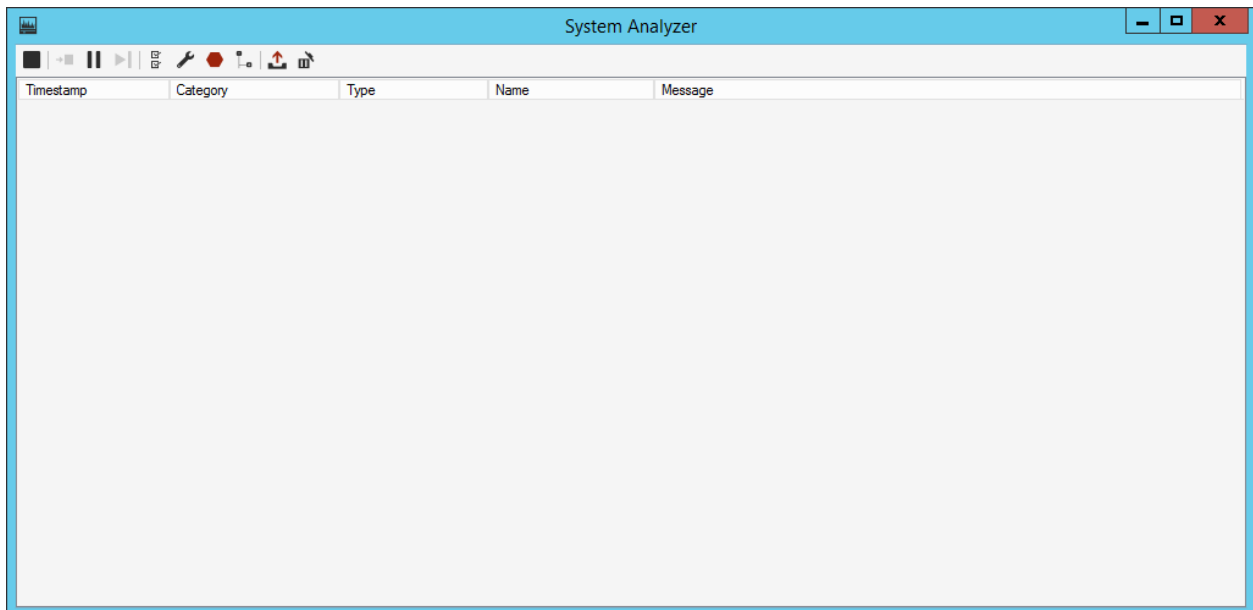
System Analyzer Main Pane

Use the System Analyzer Main pane to view operation information, such as:

- **Timestamp:** Date and time that the System Analyzer intercepted the operation.
- **Category:** Category of the message (example: Business Object, Table Validation, etc.)
- **Type:** Type of definition (example: Relationship, Field, etc.)
- **Name:** Name of the definition (example: Incident Links Similar Incidents, Incident.ServiceID, etc.)
- **Message:** Description (details) of the operation.

Good to know:

- You can export data from the System Analyzer Main pane by clicking the **Export** button to share information across systems.

System Analyzer Message Categories

The System Analyzer uses messages to display operations that occur behind-the-scenes of the CSM Desktop Client. The category is used to classify the messages listed in the Main Pane, which makes it easy for you to filter the information.

Good to know:

- Before running 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, 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
App Service Call	Tracks calls that have been made from the CSM Desktop Client to the Application Server. **Notes:** 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.	
One-Step	Tracks the execution of One-Steps.	(Select User) About to execute step Select User.
Other	Tracks all other miscellaneous messages. **Note:** These messages are often dependent on the type of system (2-tier or 3-tier) you are running.	

Category	Description	Example
Query	Tracks the execution of queries. **Note:** This type of message is only applicable if you are running a 2-tier system.	
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. **Note:** 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 unchecked.	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.	
Warning Log Message	Tracks logging information that is unexpected, but does not cause an error. **Note:** These messages are often dependent on the type of system (2-tier or 3-tier) you are running.	
Information Log Message	Tracks detailed (and technical) logging information. These messages are useful to members of the Support Team. **Note:** These messages are often dependent on the type of system (2-tier or 3-tier) you are running.	

Category	Description	Example
Verbose Log Message	Tracks detailed (and technical) logging information. These messages are useful for the Development Team. **Note:** These messages are often dependent on the type of system (2-tier or 3-tier) you are running.	

Using the System Analyzer

When working with the System Analyzer in the CSM Desktop Client, Users can:

Open the System Analyzer

To open the System Analyzer from the CSM Desktop Client menu bar, click Help>System Analyzer.

Run the System Analyzer

Use the System Analyzer window to run the System Analyzer.

Good to know:

- The System Analyzer immediately begins tracking messages by default. If the System Analyzer is stopped, click the Start button ▶ to begin tracking messages. You can stop tracking messages at any time by clicking the **Stop** button.

- Clear messages from the System Analyzer window at any time by clicking the **Clear** button.

- The System Analyzer only runs when the System Analyzer window is open.

To run the System Analyzer:

1. Open the System Analyzer.
2. (Optional) 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.

   A list of messages appear in the System Analyzer Main Pane.

4. (Optional) Navigate breakpoints using the System Analyzer toolbar:

   Click the **Pause** button to pause the System Analyzer (temporarily stop processing operations).

   If paused, click the Next Message button to step to the next operation.

   If paused, click the Run button to run the System Analyzer until the next breakpoint.

5. (Optional) Double-click a **message** in the System Analyzer window to view message details (example: Category, type, name, ID, and message).

   The System Analyzer Message window opens.

6. Close the System Analyzer window.

View Business Object Fields

Use the Current Object Values window (accessed within the System Analyzer 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 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.

   To open the System Analyzer:

   a. From the CSM Desktop Client menu bar, click Help>System Analyzer.

2. Click the Business Object Field Values button ⬚.

   The Current Object Values window opens.

3. (Optional) Define how Field values are displayed.

   Click the Show/Hide Fields button ⬚ to show or hide Fields that do not have values.

   Click the Sort Fields ⬚ button to sort Fields in folders based on type (example: SLA, Status, Time Tracking, etc.).

   Click 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, de-selecting 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. Click **Close**.

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 the following file formats:

- CSV (.csv)
- HTML (.html, .htm)
- Plain Text (.txt)
- Rich Text (.rtf)
- XML (.xml)

Good to know:

- Use the **Up/Down** arrows ▲ ▼ to organize the data in the pane. The data will display in this order in the exported file.

To export System Analyzer data:

1. Open the System Analyzer.

2. Click the Export Messages button ⬆.

   The Export System Analyzer Messages window opens.
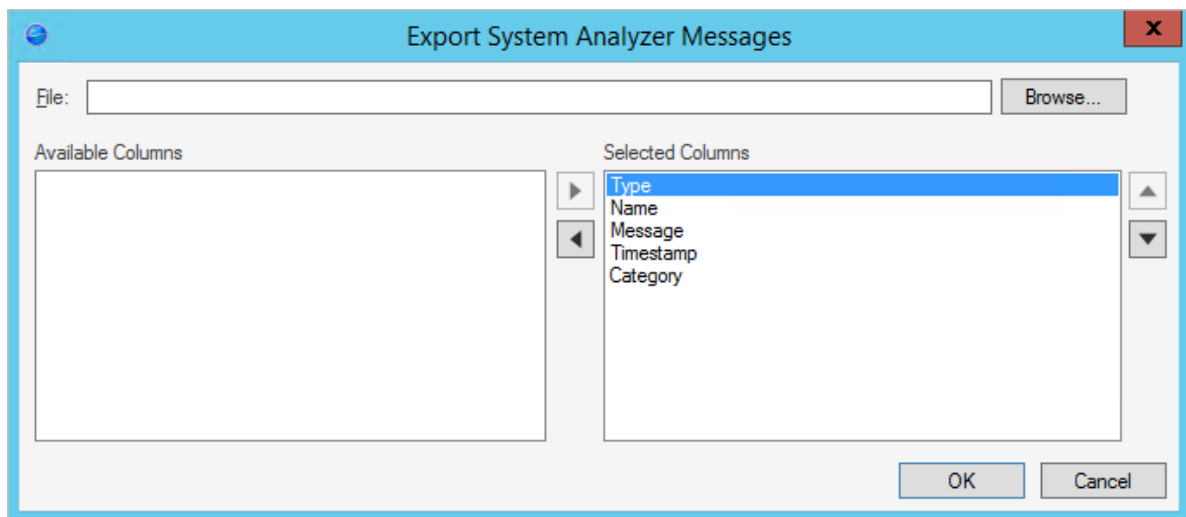
3. Click the Browse button to select a file location for the data.

4. Use the **Right/Left** arrows ▶ ◀ to select which System Analyzer data (columns) you want to export. Items in the Selected Columns pane will be exported.

Note: All columns are selected by default.

5. Click OK.

   The data is exported to the defined file location.

Configuring the System Analyzer

Complete the following procedures to configure the System Analyzer. Configuration procedures are completed in CSM Administrator and the CSM Desktop Client.

You can configure the System Analyzer in the following ways:

- Define System Analyzer security rights.
- Define how to track System Analyzer messages.
- Define System Analyzer latency simulation.
- Define System Analyzer breakpoints.

Define System Analyzer Messages

Use the Analyzer Messages window (accessed within the System Analyzer window) to define which messages to track (example: One-Step operations).

Good to know:

- The following message categories are selected by default: Business Object, BusOb Load Timing, Error, One-Step, 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.

- Click the Clear button [icon] to clear all options and click the Select button [icon] to select all standard options.

To define which System Analyzer messages to track:

1. Open the System Analyzer.

2. Click the Messages button [icon].

   The Analyzer Messages window opens.
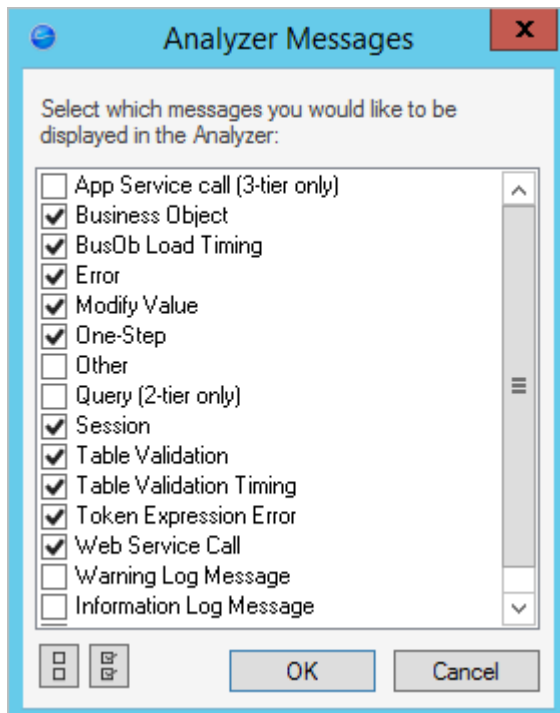
3. Define **message categories** by selecting or clearing the corresponding check box:

App Service (3-tier only)	Table Validation
Business Object	Table Validation Timing
BusOb Load Timing	Token Expression Error
Error	Web Service Call
Modify Value	Warning Log Message
One-Step	Information Log Message
Other	Verbose Log Message
Query (2-tier only)	

4. Click OK.

Define System Analyzer Latency

Use the System Analyzer Options window (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 in order 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 Options window.

To define System Analyzer latency:

1. Open the System Analyzer.

2. Click the Options button [image] .

   The System Analyzer Options window opens.
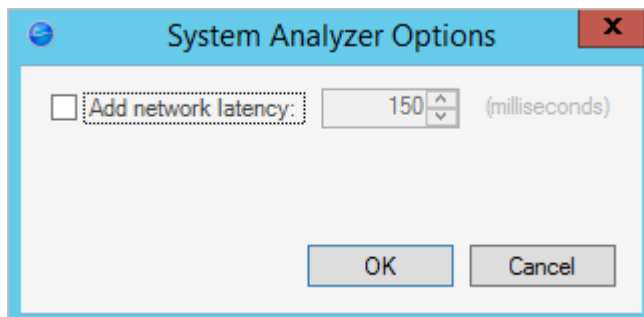
3. Select the **Add Network Latency** check box.

4. Click the Up button or **Down** button to define latency in 50 millisecond increments.

5. Click OK.

   The defined latency displays in the System Analyzer window.
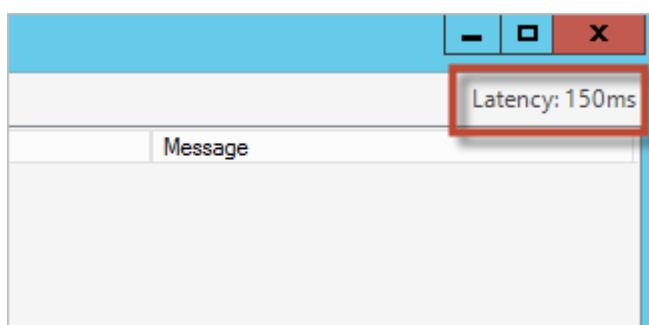
Define System Analyzer Breakpoints

Use the Breakpoints window (accessed within the System Analyzer window) to define breakpoints, which pause CSM when a specific operation is found.

Good to know:

- CSM 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 clicking the **Delete** button .

- Deselect all breakpoints by clicking the **Clear** button .

- Select all breakpoints by clicking the **Select** button .

- If a breakpoint is deselected, 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 window for later use.

To define a System Analyzer breakpoint:

1. Open the System Analyzer.

2. Click the Breakpoints button .

   The Breakpoints window opens.
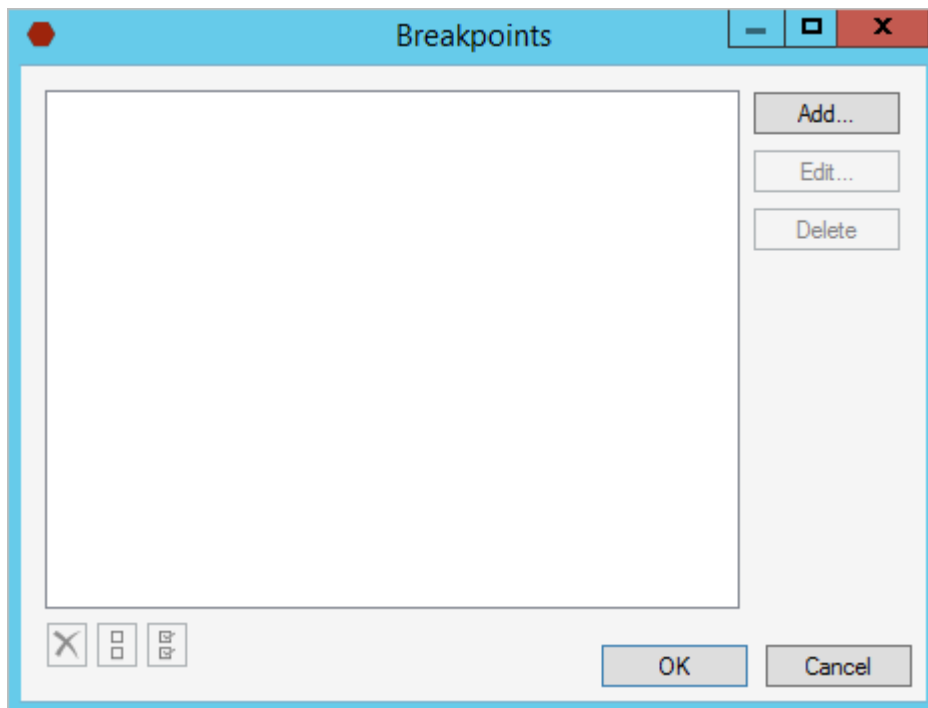
3. Click the Add button.

The Edit Breakpoint window opens.
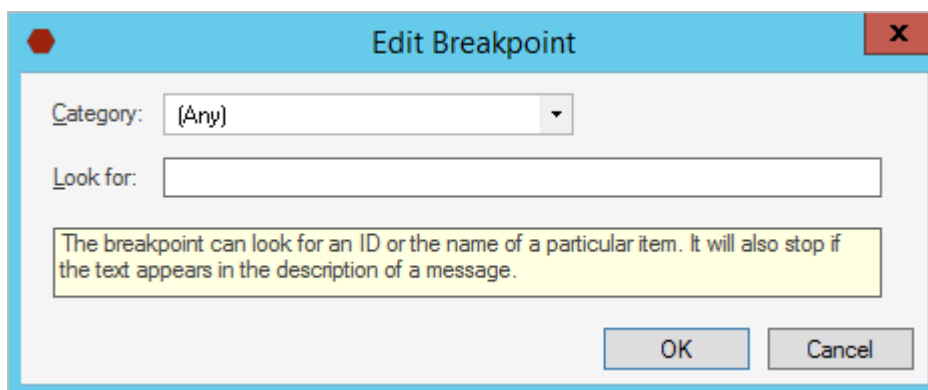
🖉 **Note:** Use the **Edit** button and **Delete** button to edit and delete existing breakpoints.

4. Define the breakpoint.
   a. Category: In the drop-down, select a **category** (example: Business Object).

   Tip: To search all categories for the breakpoint, select **(Any)** in the drop-down.

b. Look for: Specify **text** (example: Name, ID, or any other text) to serve as the breakpoint (example: ServiceID).

c. Click OK.

5. Click OK.

Performance

Use the CSM Health Check tool to analyze and optimize performance. Use performance best practices to review your system and analyze specific performance issues.

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:

- Discover missing indexes for Business Object database tables that contain a large number of records.
- See which Business Objects can be set as cacheable.
- Send Health Check results to Cherwell Support for analysis on request.
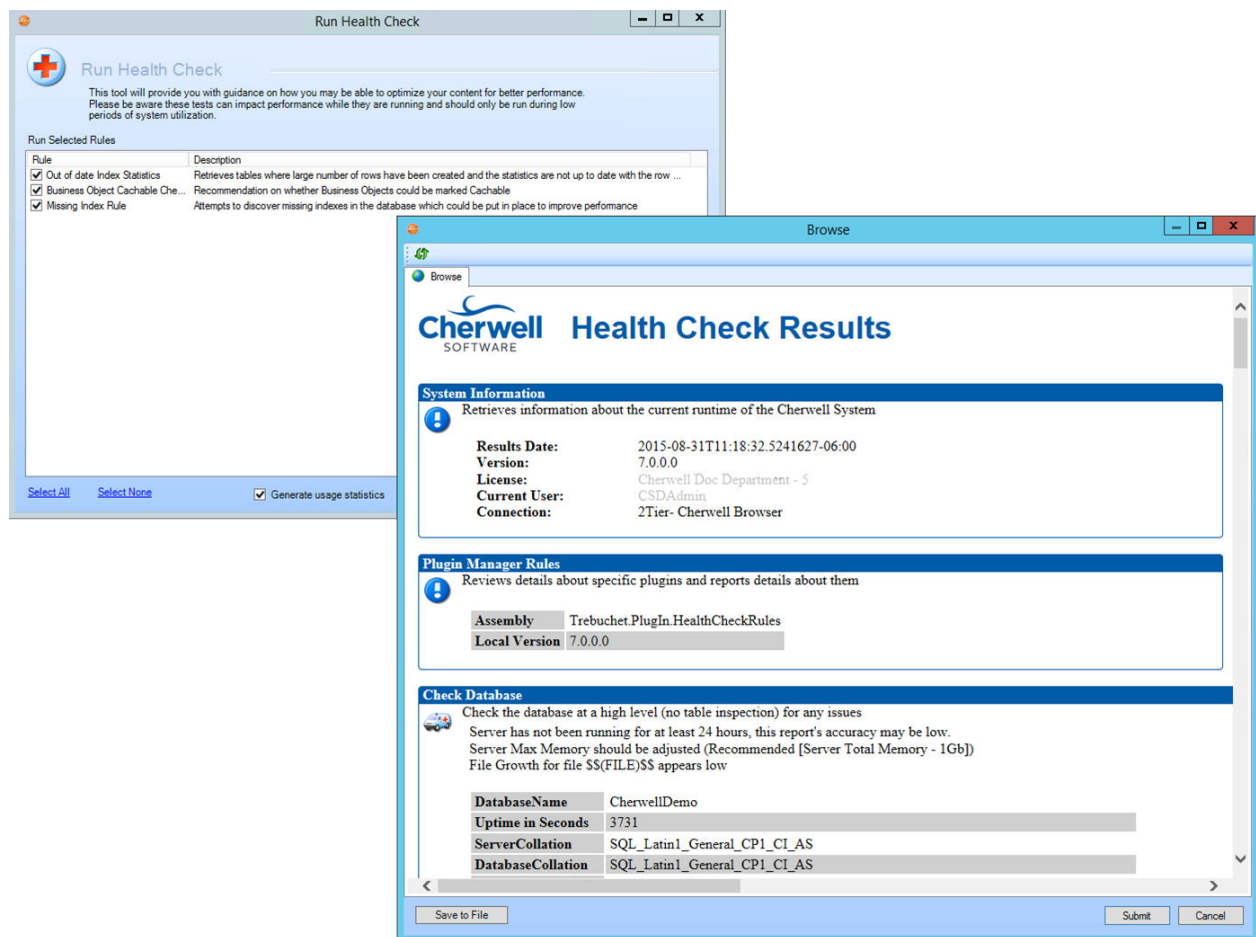
There are three levels of Health Check tests:

- Basic: Provides information about your CSM system 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: Provides system and database information not related to 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.

Run the Health Check Tool

To use the Health Check tool:

1. From the CSM Administrator main window, click 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 will 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.

   Click the Select None link to generate CSM system and the Health Check plug-in information only.

4. Click OK.

The Health Check results open in a separate window. Click Save to File to save the results to an HTML file; click Submit to send the results to Cherwell Support on request.

Configuring the Performance Health Check Tool

Health Check Security rights are configured in CSM Administrator. See Tools Security Rights.

Best Practices for Performance

Review the following system considerations as a prerequisite to analyzing and troubleshooting a specific performance issue.

Determine the Affected Location

Communicate with your team at a high level to find out if the entire system or a specific area of the system is perceived as slow. Specific areas might include:

- CSM Desktop Client
- CSM Administrator Client (ex: Publishing)
- CSM Browser Client
- CSM Customer Portal
- Certain Business Object (ex: Incident, Change Request)
- Internal databases (ex: CMDB)
- External databases (ex: Active Directory, SCCM)

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-premise: Installation method of the affected environment.

Evaluate the Installation Configuration

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:

- Available memory.
- Available Central Processing Units (CPUs).

  Note: If you are using a virtual machine, ensure that all memory and CPUs are dedicated.

- Available disk space.
- Load balancing.
- Subscription numbers.
- Separate installed applications.
- Distribution of servers (on one machine or several).

Note: Refer to the Sizing and Scalability documentation for information on minimum and recommended server configurations based on the number/type of CSM Clients.

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 resolution. If the issue is chronic, resources might need to be increased or expanded (ex: Hosted environments running a version of CSM of 7.0.0 or later should use a minimum of 6GB of available memory; if you require additional memory, submit a request from your IT team).

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 (ex: All affected Users are using wireless or accessing the VPN).

Note: If you have a hosted environment, run the evaluations using IP address 64.92.211.170.

Evaluate the Business Object Relationship Structure

Review your system structure to determine if Business Object Relationships are loading in a way that impacts performance. For example, when an Incident loads, the related Journal tab references all Journals that exist in a one-to-many Relationship between the Incident and Journal Business Objects; by default, all of these Journal records are loaded, even if they are not referenced by the Incident. Use the System Analyzer to determine which aspects of the Business Object structure are impacting performance.

You can prevent this from happening using the Advanced page of the Relationship Properties window for the Relationship by deselecting the Load Immediately check box and selecting the Don't Load When Constraints are Blank check box.

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 clicking 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 (ex: 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 Server 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. 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, click the Select button to select which Business Objects to re-index.

    Note: By default, all Business Objects are selected. Uncheck Business Objects to exclude them from reindexing, or select Clear All to uncheck 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.

Mitigate Database Growth

Use the E-mail Monitor, Blueprint Publish Log, and Automation Process Log to reduce database growth. Using E-mail Monitor Actions, you can define the following settings for each monitor:

- Attach e-mail to [Business Object (example: Incident)]: Attaches incoming e-mails to Business Objects as Journal - Mail History Records.

- Import attachments as part of e-mail: Imports e-mail attachments into the database along with incoming e-mails and allows you to define Attachment settings such as type and size.

- Attach e-mail attachments to [Business Object (example: Incident)]: Attaches e-mail attachments to Business Object Record's Attachment bar (not just to the internal copy of the e-mail).

- Preserve inline images within e-mail body: Preserves images within the body of incoming e-mails with the text of the e-mail.

- Attach inline images to [Business Object (example: Incident)]: Attaches images within the body of incoming e-mails to the selected Business Object.

- Attach e-mail to Customers: Attaches incoming e-mails to Customer Records as Journal - Mail History Records.

Using 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, you can reduce the size of the TrebuchetProcesses system table, which holds historical publishing data. Clear the log using CSM Administrator by clicking 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. Review the standards in the Assess the Memory and Computer Processing Unit (CPU) section for more information.

- 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 deselecting the Execute Before Saving a Record check box; this allows the system to only save the record if necessary.

Review Portal Configurations

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 clicking the Processes tab. Then, you can restart the process or server using the IIS Manager. When you restart the process or server, the memory will temporarily decrease, but will continue to increase afterward; 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 is occurring, you have two options:

- Using the Portal Logging Options window 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.

    Note: We do not recommend using LocalSystem for a long period of time since it can cause a security risk.

Server Tools

CSM provides the following tools to help manage server components:

- 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 Servers (Services), and restart some managed CSM Web Applications.

- The Service Monitor is a stand-alone Web Application that allows system administrators to remotely monitor and manage (start, stop, and restart) CSM Servers (services) and Web Applications and restart IIS, using a browser and an IIS-hosted web page. Service Monitor is installed using a stand-alone installer and is deployed using the Service Monitor web page.

CSM Servers (Services)

The CSM Servers are Microsoft Windows® Services (processes) dedicated to particular tasks. These services run in the background while monitoring for, and accepting, requests from CSM Clients. The available CSM Servers (Services) are:

- **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 (usually using an encrypted TCP connection).

  > **Note:** If the Application Server is installed under IIS, it often displays as *Application Server (IIS)* within the UI. The Application Server shows up as both Windows and IIS hosted service at the same time. Only one is available at a time.

- **Server Farm:** A Cherwell Server Farm is a framework that consists of a load balancer, multiple web servers, SQL Server, and Redis.

- **Automation Process Server:** The Cherwell Automation Process Server (formerly the Business Process Server) is a CSM Service that monitors events and executes background business rules in your system (example: Notifications and escalations). Automation Processes are configured in CSM Administrator.

- **E-mail and Event Monitor Server:** The Cherwell E-mail and Event Monitor Server is a CSM Service that automatically monitors e-mail accounts and event streams, and then performs specified actions, such as creating or modifying records based on e-mail content or event details. In addition to connecting to the database server, it also has to be able to talk to the mail server (example: Microsoft Exchange).

- **Scheduling Server:** The Scheduling Server is a CSM Service that 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).

Server Manager

	At-a-Glance
	• About the Server Manager

Getting Started	Using	Configuring

• CSM Servers (Services)
• CSM Web Applications Managed by Server Manager
	• Start/Stop/Restart a CSM Server, or Restart a Web Application	• Configure a CSM Server:
		  • Configure the Application Server
		  • Configure the Automation Process Server
		  • Configure the E-mail Event Monitor Server
		  • Configure the Scheduling Server
		• Configure Logging for a CSM Server
		• Configure Service Health Monitoring

About the Server Manager

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 Servers (Services), and restart some managed CSM Web Applications.

Use the Server Manager to:

- Monitor the status (running or stopped) of CSM Servers and Web Applications.
- Start, stop, and restart CSM Servers.
- Restart CSM Web Applications (Browser Client, Portal, and Web-Forms): A restart recycles the application pools.
- Configure CSM Servers: CSM Servers 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 Servers or Web Applications.
- Configure logging for CSM Servers or Web Applications.
- Configure the Service Health Monitor.

This Server Manager is automatically installed on the same machine where CSM Servers are installed.

Tip: Use the Service Monitor, a similar tool, to remotely monitor and manage services.

CSM Web Applications Managed by the Server Manager

The following CSM Web Applications can also be managed by the Server Manager:

- **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.

- **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.

- **Web-Forms™:** Cherwell Web-Forms™ is a browser-based application that allows Users to enter, view, and edit CSM Business Objects over the web without having to log in (example: Surveys, registration, ordering, etc.). This tool also allows for the remote execution of One-Steps.

The CSM Web Applications run under Microsoft Internet Information Services (IIS). CSM Web Applications are services that cannot be configured like CSM Servers, but they can be restarted by having their IIS application pools recycled and their events logged.

Server Manager Good to Know

- Use event logging to troubleshoot each CSM Server or Web Application to help determine the cause of failed processes.
- CSM Servers typically start automatically after installing the CSM suite.
- When restarting a web application (Browser Client, Portal Client or Web-Forms), the application pool recycles. CSM Web Applications cannot be stopped or started.
- CSM Servers and Web Applications can be restarted without resetting IIS because the restart modifies the web.config files for each, which causes the applications to be recompiled and restarted.
- The Application Server is special because it forms the interface between your Client applications and database (a 3-tier connection).
- In a typical single-server installation, all the CSM Servers are installed on the same physical machine; however, they can be split up for performance or access reasons.
- When running a standard CSM Server Installation, the CSM Servers are configured with reasonable defaults, use the Server Manager to view or change those defaults.
- The Application Server provides an organization with a 3-tier connection to the database.
- Connection and limit values can be changed; however, it is recommended not to change the values without contacting Cherwell Support.
- The Automation Process Server is a service that monitors events and executes background business rules in a system (example: Notifications and escalations).
- Automation Processes are configured and managed in CSM Administrator.
- While individual Automation Processes can be enabled or disabled in the CSM Administrator, the Automation Process Server must be running for any process to execute.
- The E-mail and Event Monitor Server is a service that automatically monitors e-mail accounts and event streams, and then performs specified actions, such as creating or modifying records based on e-mail content or event details.
- When a service is paused, there is an option to state a reason for performing that action.
- E-mail and Event Monitoring is configured and managed in CSM Administrator.
- The Scheduling Server is used to run time-based activities that have been defined in CSM Administrator.
- The Scheduling Server can be installed on multiple machines if different items need to be run at separate locations or for different purposes.

Using the Server Manager

When working with the Server Manager, Users can:

- Start/stop/restart a CSM Server, or restart a Web Application.
- Configure a CSM Server.
- Configure logging for a CSM Server or Web Application.

To open the Server Manager:

1. Click Start>All Programs>Cherwell Service Management>Tools>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 the following CSM Servers:

- Application Server
- Automation Process Server
- E-mail and Event Monitor Server
- Scheduling Server
- Trusted Agents Server (if installed and configured)

> **Note:** If using Trusted Agents for security or e-mail operations, restart the Trusted Agents server first.

Use the Server Manager to restart (recycle the application pools) the following CSM Web Applications:

- Browser Client
- Customer Portal
- Web-Forms

To start/stop/restart a CSM Server or restart a web application:

1. Click Start>All Programs>Cherwell Service Management>Tools>Server Manager.
2. From the Server drop-down, select a **CSM Server** or **web application**.

   The CSM Server or Web Application is shown in the Server drop-down.

3. Select an operation:
   To force a refresh of the server status, double-click the Server **Status** icon.

   To start a selected CSM Server or Web Application in the Server drop-down, click the Start Server button.

   To stop a selected CSM Server or Web Application in the Server drop-down, click the Stop Server button.

   To restart a selected CSM Server or Web Application, click the Restart Server button.

Configure a CSM Service

CSM Servers are configured by default during installation; however, use the Server Manager to change the settings, if needed. For example, change: the protocol used to communicate with the Cherwell Application Server, a connection to the database, or a method of logging server events.

Note: For the Cherwell Application Server, configure the settings that allow communications with CSM Clients in order to establish a 3-tier connection.

Configure the Application Server

Use the Server Manager to configure the Cherwell Application Server so that a 3-tier connection can be maintained between the CSM Applications and the Database.

To configure the Application Server:

1. Click Start>All Programs>Cherwell Service Management>Tools>Server Manager.

2. In the Server field drop-down, select Application Server.
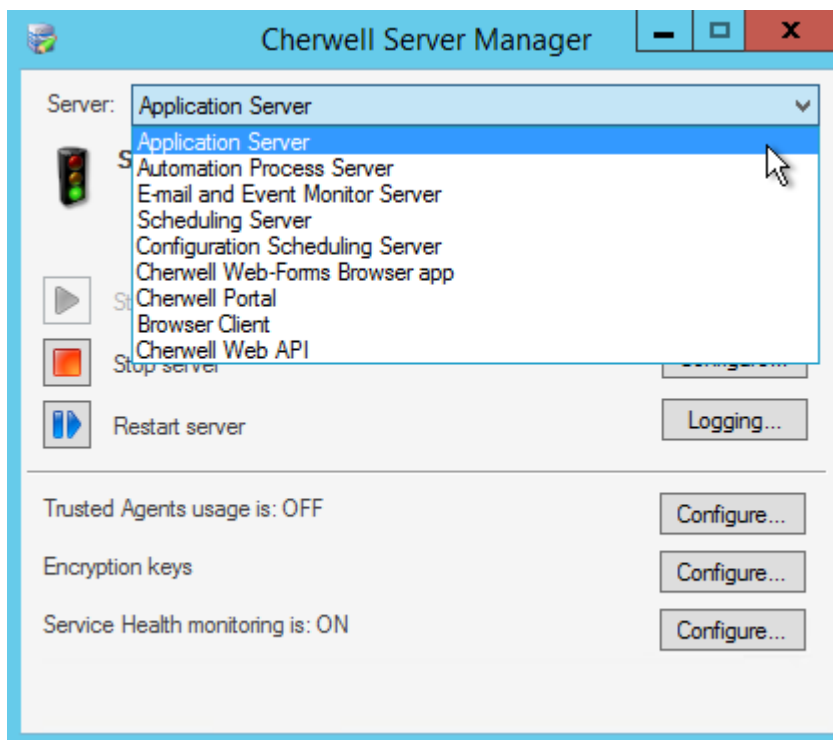
3. Click the Configure button.
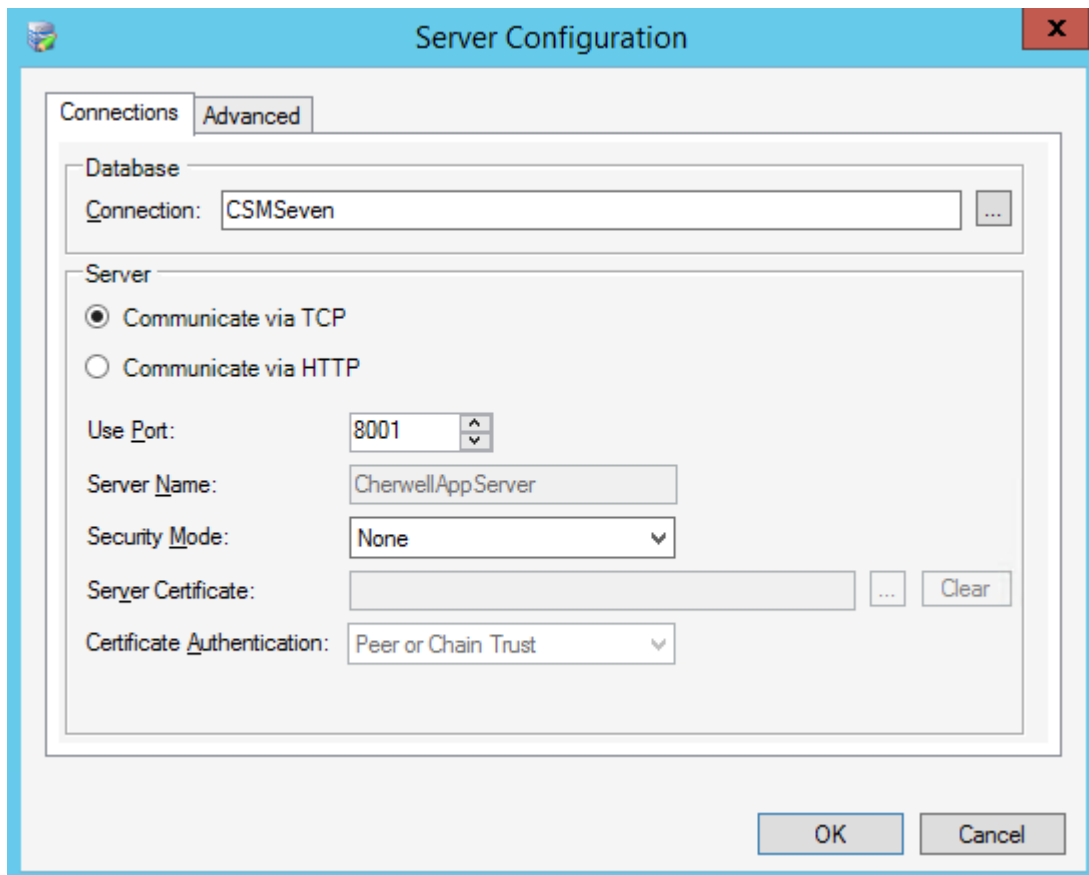
4. Define the Server Configuration window Connections options:

Item	Description
Database	Select the connection the server should use to connect to the CSM Database.
Connection	Which 2-tier connection the application server should use to connect to the CSM Database. Typically, this is the connection named Cherwell, but CSM should detect the default connection name. If the name of the correct database connection is not displayed, click the Ellipses button [...] to open the Connection window and select an existing connection or configure a new connection.
Server	Provide the server information.
Communicate via TCP	Select this radio button to use Transmission Control Protocol (TCP) to communicate with the Application Server. This is the default.

Item	Description
Communicate via HTTP	Select this radio button to use HyperText Transfer Protocol (HTTP) to communicate with the Application Server.
Use Port	Confirm the port number used by the Client to connect to the Application Server, the default is 8001. Do not change the port number, otherwise all clients have to specify a different port in the address for the server.
Server Name	The server name normally shows Cherwell AppServer, although older installations might display TrebuchetServer. **Note:** In older CSM versions, this field could be customized. If this was done previously, then the field can be edited. Otherwise, the field is read-only.
Security Mode	The settings between the Client applications and the Application Server. None: Communications are neither encrypted nor signed. This is only recommended in development or test environments running within a company's secure intranet. Encrypted: Communications are signed and encrypted using the specified server certificate. The encryption is at the transport level using SSL/TLS.
Server Certificate	If the Security Mode is set to Encrypted, click the Ellipses button to select a certificate to use for signing or encryption. In the window, select a certificate from one of several different certificate stores.

Item	Description
Certificate Authentication	If one of the certificate-based options is selected, specify if and how to authenticate the certificate. Individual clients can override this to make their checks more or less enforced. None: No validation of the server certificate is performed by the client. This is useful for self-signed certificates where authentication is not a concern. This validation still allows for encrypted communications if the Security Mode is set to Encrypted. Peer Trust: The certificate is valid if it is in the client's trusted people store. Peer or Chain Trust: The certificate is valid if it is in the client's trusted people store, or if the chain builds to a certification authority in the client's trusted root store. Chain Trust: The certificate is valid if the chain builds to a certification authority in the client's trusted root store. This is the most secure option.

5. Click the Advanced tab.

> **Note:** These settings provide limiting values to help prevent Denial of Service attacks. Do not change these values without consulting the Cherwell Support team.
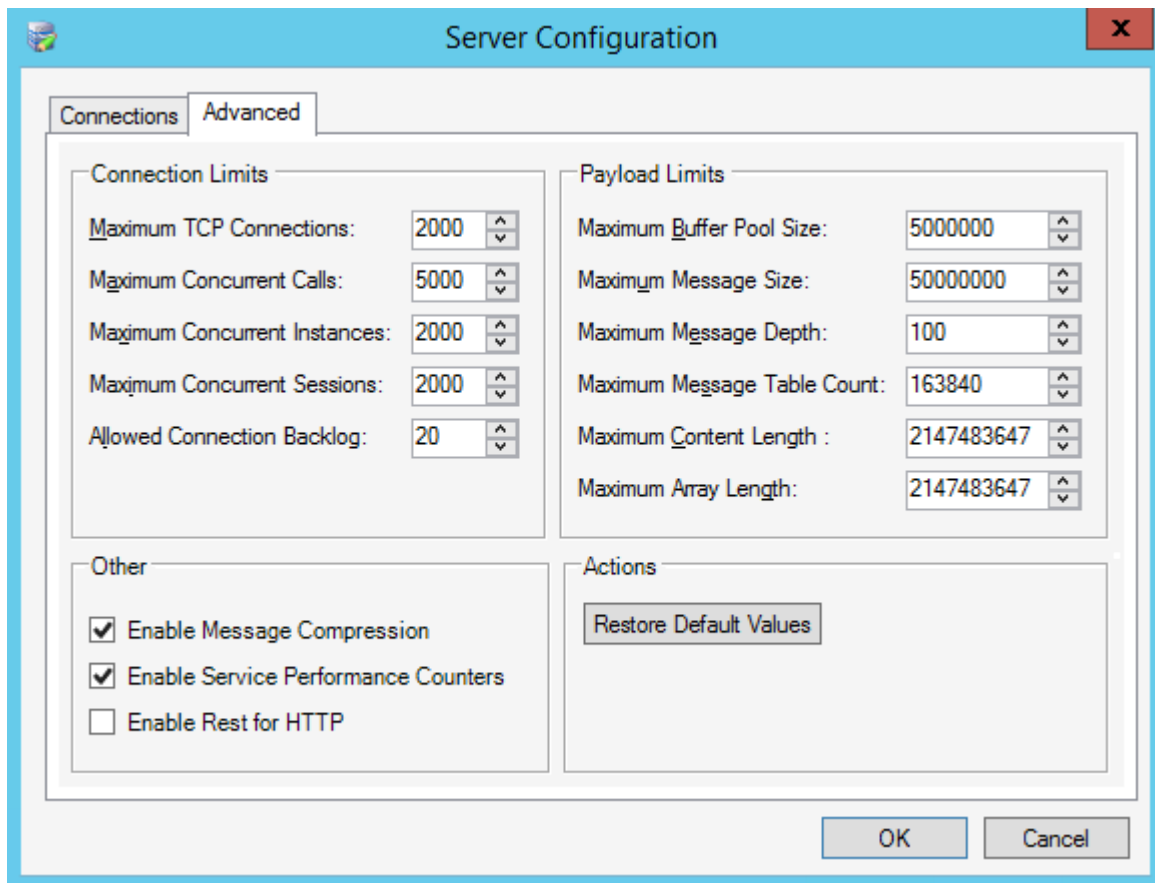
6. Define the Server Configuration window Advanced options:

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.

Item	Description
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.
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.

7. **Optional:** Configure logging for the Application Server. The logging settings for the Application Server will also apply to the System Upgrade and System Restore Utilities.

Configure the Automation Process Server

Use the Server Manager to configure the Automation Process Server. When configuring the Automation Process Server, define:

- **Connection:** Which 2-tier connection the CSM Server should use to connect to the CSM database. Typically this is the connection named *Cherwell*, but CSM should detect the default connection name.
- **Login credentials:** The credentials used by the CSM Server to log into CSM.
- **Default Role:** The default Role to use, if Views are separated based on the Role of the logged-in User. (By default, Server Manager does not identify Roles based on the logged-in User.)
- **Pause/Resume processing:** Stop or restart service processing.

To configure the Automation Process Server:

1. Click Start>All Programs>Cherwell Service Management>Tools>Server Manager.
2. In the Server field drop-down, select Cherwell Automation Process Server.
3. Click the Configure button.

   The Automation Process Server Configuration window opens.

4. Select which connection this CSM Server should use to connect to the CSM Database.

   If the name of the correct database connection is not displayed, click the Ellipses button to open the Connection window and select an existing connection or configure a new connection.

5. Select the login option for this CSM Server (that is, the method this CSM Server uses to log in to CSM):

Option	Description
Windows Authentication	Uses Windows login credentials. To use this feature, Windows must be a supported login mode (Open CSM Administrator>Security>Edit security settings, select the Desktop Client, Browser Client, or **Browser Portal**, and in the Supported login modes section, select Windows). This CSM Server logs in to CSM using the account associated with the Windows credentials used by the Windows server.
User ID and Password	Uses Cherwell login credentials. Provide the **username** and **password**. This is usually an administrative account with broad system access, such as CSDAdmin.

Option	Description
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 CSM Server 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. **Test:** Click this button to confirm that the login/connection works.

7. (Optional) If needed, you can click the Pause/Resume Processing button to stop or restart the Server processing. If you click the button while the Server is running, the server is paused, and you can enter the reason the service was paused. For example, an administrator may be troubleshooting and wants to let his team know the reason the service was paused. Click the button to resume processing.

> **Note:** There are two different methods that allow the service to be stopped. The first is to actually stop the service from running in the Service control panel applet or by using the Stop button in the Server Manager. While this works, it requires direct access to the machine/image on which the service is running. The second method is to pause/resume processing. This can be done from the CSM Administrator by any user with sufficient security rights. In this case, the service is still running, but it will not process any records. The advantage of this approach is that it does not require access to the machine/image on which the service is running.

8. Click OK.

Configure the E-mail and Event Monitor Server

Use the Server Manager to configure the E-mail and Event Monitor Server:

- **Connection:** Which two-tier connection the CSM Server should use to connect to the CSM database. Typically this is the connection named *Cherwell*, but CSM should detect the default connection name.

- **Login credentials:** The credentials used by the CSM Server to log into CSM.

- **Default Role:** The default Role to use, if Views are separated based on the Role of the logged-in User. (By default, Server Manager does not identify Roles based on the logged-in User.)

- **Pause/Resume processing:** Stop or restart service processing.

- **Thread Management:** Enable multi-threaded processing and the number of threads used to manage E-mail Monitors.

To configure the E-mail and Event Monitor Server:

1. Click Start>All Programs>Cherwell Service Management>Tools>Server Manager.

2. In the Server field drop-down, select Cherwell E-mail Event Monitor Server.

3. Click the Configure button.

   The E-mail Event Monitor Server Configuration window opens.

4. Select which connection this CSM Server should use to connect to the CSM database:
   a. Connection: If the name of the correct database connection is not displayed, click the Ellipses button to open the Connection window and select an existing connection or configure a new connection.

   b. If your e-mail account is configured to use Trusted Agent for e-mail, this should be a three-tier connection; otherwise, it should be a two-tier connection.

5. Select the login option for this CSM Server (that is, the method this CSM Server uses to log in to CSM):

Option	Description
Windows Authentication	Uses Windows login credentials. To use this feature, Windows must be a supported login mode (Open CSM Administrator>Security>Edit security settings, select the Desktop Client, Browser Client, or **Browser Portal**, and in the Supported login modes section, select Windows). This CSM Server logs in to CSM using the account associated with the Windows credentials used by the Windows server.

Option	Description
User ID and Password	Uses Cherwell login credentials. Provide the **username** and **password**. This is usually an administrative account with broad system access, such as CSDAdmin.
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 CSM Server 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. **Test:** Click this button to confirm that the login/connection works.

7. If you have a large number of E-mail Monitors that run under a large load, you can enable multi-threading to improve processing performance:
    a. **Enable Multi-threading:** Select this check box to enable processing through multiple threads.

    b. **No. of threads:** Specify up to 10 threads. The enabled E-mail Monitors are divided evenly based on the number of threads you specify. For example, if you have 10 enabled Monitors and specify 2 threads, each thread processes 5 Monitors.

8. (Optional) If needed, you can click the Pause/Resume Processing button to stop or restart the Server processing. If you click the button while the Server is running, the server is paused, and you can enter the reason the service was paused. For example, an administrator may be troubleshooting and wants to let his team know the reason the service was paused. Click the button to resume processing.

> **Note:** There are two different methods that allow the service to be stopped. The first is to actually stop the service from running in the Service control panel applet or by using the Stop button in the Server Manager. While this works, it requires direct access to the machine/image on which the service is running. The second method is to pause/resume processing. This can be done from the CSM Administrator by any user with sufficient security rights. In this case, the service is still running, but it will not process any records. The advantage of this approach is that it does not require access to the machine/image on which the service is running.

9. Click OK.

Configure the Scheduling Server

Use the Server Manager to configure the Scheduling Server on each machine where it is installed. Each machine can then run time-based activities that have been previously set up. This include backups, database maintenance, data imports, etc.

When configuring the Scheduling Server, define:

- **Connection:** Which 2-tier connection the CSM Server should use to connect to the CSM database. Typically this is the connection named *Cherwell*, but CSM should detect the default connection name.
- **Login credentials:** The credentials used by the CSM Server to log into CSM.
- **Default Role:** The default Role to use, if Views are separated based on the Role of the logged-in User. (By default, Server Manager does not identify Roles based on the logged-in User.)
- **Pause/Resume processing:** Stop or restart service processing.
- **Scheduler Group:** Which Scheduler Items to run if there is more than one group.

To configure the Scheduling Server:

1. Click Start>All Programs>Cherwell Service Management>Tools>Server Manager.
2. In the Server field drop-down, select Cherwell Scheduling Server.
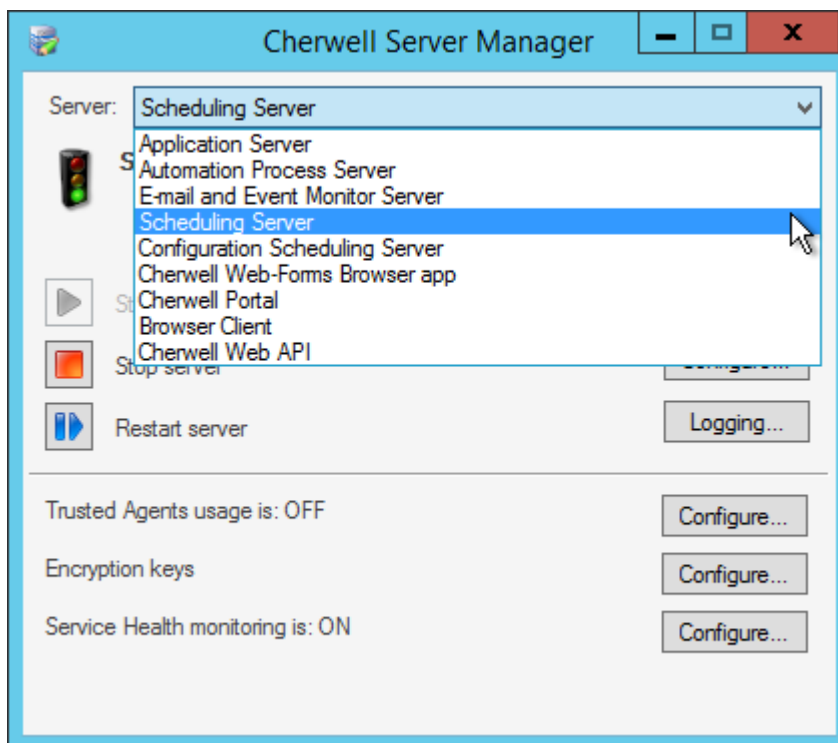
3. Click the Configure button.

The Scheduling Server Configuration window opens.

4. Select which connection this CSM Server should use to connect to the CSM database:
   a. Connection: If the name of the correct database connection is not displayed, click the Ellipses button to open the Connection window and select an existing connection or configure a new connection.

5. Select the login option for this CSM Server (that is, the method this CSM Server uses to log in to CSM):

Option	Description
Windows Authentication	Uses Windows login credentials. To use this feature, Windows must be a supported login mode (Open CSM Administrator>Security>Edit security settings, select the Desktop Client, Browser Client, or **Browser Portal**, and in the Supported login modes section, select Windows). This CSM Server logs in to CSM using the account associated with the Windows credentials used by the Windows server.

Option	Description
User ID and Password	Uses Cherwell login credentials. Provide the **username** and **password**. This is usually an administrative account with broad system access, such as CSDAdmin.
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 CSM Server 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. **Test:** Click this button to confirm that the login/connection works.

7. Select a Scheduler Group to run, if you have more than one predefined.

   a. Click the Ellipses button ![ellipses].

      The Choose Schedule Group window opens.

      > **Note:** The actions for scheduled items are selected and configured in CSM Administrator (**CSM Administrator>Scheduling>Edit Schedule**). Most Users will use the (Default) group. However, if additional items need to be run at different times or for different purposes, these can be placed in separate groups, and run by different servers (example: A SaaS customer might need to import Users into Active Directory at their company, which cannot be done in the SaaS environment. They could use one Scheduling Server to import to Active Directory at the company, and another SaaS Scheduling Server to run Default actions).

   b. Select a schedule group for this Scheduling Server, and then click OK.

      > **Note:** Schedule groups can be used with multiple Scheduling Servers. This enables the Scheduling Servers to collaborate on job processing.

8. (Optional) If needed, you can click the Pause/Resume Processing button to stop or restart the Server processing. If you click the button while the Server is running, the server is paused, and you can enter the reason the service was paused. For example, an administrator may be troubleshooting

and wants to let his team know the reason the service was paused. Click the button to resume processing.

> **Note:** There are two different methods that allow the service to be stopped. The first is to actually stop the service from running in the Service control panel applet or by using the Stop button in the Server Manager. While this works, it requires direct access to the machine/image on which the service is running. The second method is to pause/resume processing. This can be done from the CSM Administrator by any user with sufficient security rights. In this case, the service is still running, but it will not process any records. The advantage of this approach is that it does not require access to the machine/image on which the service is running.

9. Click OK.

Configure Logging for a CSM Server or Web Application

Use the Server Manager to configure event logging for CSM Servers or Web Applications.

Use these guidelines to configure logging:

- When logging is enabled for the Browser Client, Cherwell Portal, or Cherwell Web API, the log file includes information captured for all CSM Web Applications, as well as SAML, Bomgar, and Cherwell Mobile Client.
- When logging is enabled for the Application Server, the logging settings will also apply to the System Upgrade and System Restore Utilities.
- Logging can be enabled for each Desktop Client. For more information, refer to Configure User General Settings.
- Logging may need to be enabled for multiple services. For example, if you use the Desktop Client with a 3-Tier connection using Trusted Agents, enable logging for the Application Service and the Trusted Agents Service to log all 'authlog' messages.

Event logging records significant events and errors, and is used for troubleshooting. When configuring event logging, designate:

- Where to log events.
- Which classification of server events to log (debug, stats, information, warning, error, or fatal).

Logging can be configured to go to an event log, set up file locations, or to a Splunk server. 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. 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. For more information on integrating Splunk and CSM, see Splunk Integration (Splunk Integration, http://docs.splunk.com/Documentation).

To configure logging for a CSM Server or Web Application:

1. Click Start>All Programs>Cherwell Service Management>Tools>Server Manager.
2. Select a server from the drop-down list.
3. Click the Logging button.

   The Logging Options window for the selected Server opens.

4. Select where to log CSM events (select one or more options):
   a. **Log to event log:** Select this check box to log CSM events so that they can be viewed by the Windows Event Viewer. Then, select which events to log:

Debug and above: Very verbose messages. Leaving this on continuously can get space and resource intensive.

Stats and above: Detailed messages that track performance.

Info and above: Informational messages that can be used to diagnose a problem with your Server.

Warning and above: Warning messages that occurred while the Server was running.

Error and above: Errors that were encountered while the Server was running.

Fatal only: Errors that were encountered while the Server was running that caused the Server to stop.

> **Note:** We recommend 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.

b. Log to file: Select this check box to write the logs to a specific file and location. Then, set your file limits.

Log Level: Select an event classification as described above (example: Debug and above, Info and above, etc.)

File Name: Click 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.

> **Note:** 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.

c. **Log to Splunk:** Select this check box to write the logs to a Splunk server, and then configure Spunk logging.

5. Click OK to close the Logging options window.

Configure Logging to a Splunk Server

Use the Server Manager to configure event logging 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. Click Start>All Programs>Cherwell Service Management>Tools>Server Manager.

2. In the Server drop-down, select a **Server** or **web application**.

3. Click the Logging button.

   The Logging Options window for the selected Server opens.

4. Select the Log to Splunk check box.

5. Select the log level from the drop-down:
   Debug and above: Very verbose messages. Leaving this on continuously can get space and resource intensive.

   Info and above: Informational messages that can be used to diagnose a problem with your Server.

   Stats and above: Detailed messages that track performance.

   Warning and above: Warning messages that occurred while the Server was running.

   Error and above: Errors that were encountered while the Server was running.

   Fatal only: Errors that were encountered while the Server was running that caused the Server to stop.

6. Click the Configure button.

7. 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.

8. Click Test to test the CSM Connection to the Splunk Server.

9. Click OK.

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. Click 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. Click 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. Click Test to test the CSM Connection to the Splunk Server.

    e. Click OK.

7. Close the Encryption Key Management Window.

8. Configure encryption keys for another server or web application, as necessary.

Configure Service Health Monitoring

The Service Health Monitor enables you to detect that the following services are running normally:

- Automation Process Server
- E-mail Event Monitor
- Scheduling Server

The Service Health Monitor sends heartbeat signals at a defined interval to Splunk® Enterprise. Use Splunk to view status information for each service, including the amount of time the most active task has been running.

Note: Splunk® Enterprise is required for this feature.

Configuring Service Health Monitoring

Use the following process to configure the Service Health Monitor:

1. Install and configure Splunk. For additional information, see to the Splunk documentation.
2. Enable the Service Health Monitor in the CSM Server Manager.
3. Implement provided Dashboards in Splunk.
4. Analyze Service Monitor logs.

Enabling The Service Health Monitor in CSM

To enable the Service Health Monitor in the Server Manager:

1. Click Start>All Programs>Cherwell Service Management>Tools>Server Manager.
2. Click the Configure button.
3. On the Service Health Monitoring page, select the Service Health Monitoring check box. This check box enables monitoring for all services.

   Note: To disable monitoring for all services, clear the check box.

4. Specify a Monitoring Interval (in minutes).

   Note: If you modify the monitoring interval, modify your Splunk Dashboards to accommodate the change.

5. Click the Configure button.
6. 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.

7. Click Test to test the CSM Connection to the Splunk Server.
8. Save your changes.

Analyzing Service Monitor Logs

Once Service Health Monitor has been configured, use the following search query in Splunk to see log messages related to CSM services:

```
MessageName="ServiceHeartbeat"
```

Each message has a header and details associated with the message:

- **Header**

  Indicates the service which is logging the message, its status, and how long the most active task for that service has been busy.

- **Details**

  Describes tasks running for the service and provides the status for each task.

The following message is an example from Splunk:

```
{ [-]
   MessageName: Service Heartbeat
   ServiceInstanceIdentifier: 192.xxx.x.xTrebuchet.API
   ServiceInternalStatus: Running
   ServiceName: Automation Process Server
   Service_Busiest_Task_InMinutes: 0
   TaskHealth: [ [-]
     { [-]
       TaskAdditionalDetails: Thread internal state:Background, WaitSleepJo
in
       TaskBusySinceInMinutes: 0
       TaskCurrentAction: SchduleItemID:941237d6237f4bbf7a2d614e20885095546
497c2de,
BusObTypeId:6dd53665c0c24cab86870a21cf6434ae,BusObRecId:941237d59d57182cd39
1ad437281d6f002e7dd94c2,
ProcessID:93aec5569c9c091ddb1f4740f2a0c8fb231439254b,ProcessInstanceID:9412
37d623bcc25ff49e5544f391da26d314d8ecab
       TaskId: BP Executor
```

```
    TaskStatus: Running
}
```

Sample Service Monitoring Dashboard

Two sample Splunk dashboards are provided to help you quickly access CSM service health data.

- **Heartbeat Status**

  Shows the status for each service and reports missed heartbeats. To prevent false alarms, the interval for the Dashboard to report an error is set to 10 minutes, which is twice the default heartbeat interval set in CSM.

- **Service Efficiency Indicator**

  Shows how quickly services are executing tasks. Lower values indicate that tasks are executing quickly. Higher values can be normal for some services, such as the Scheduling Server.
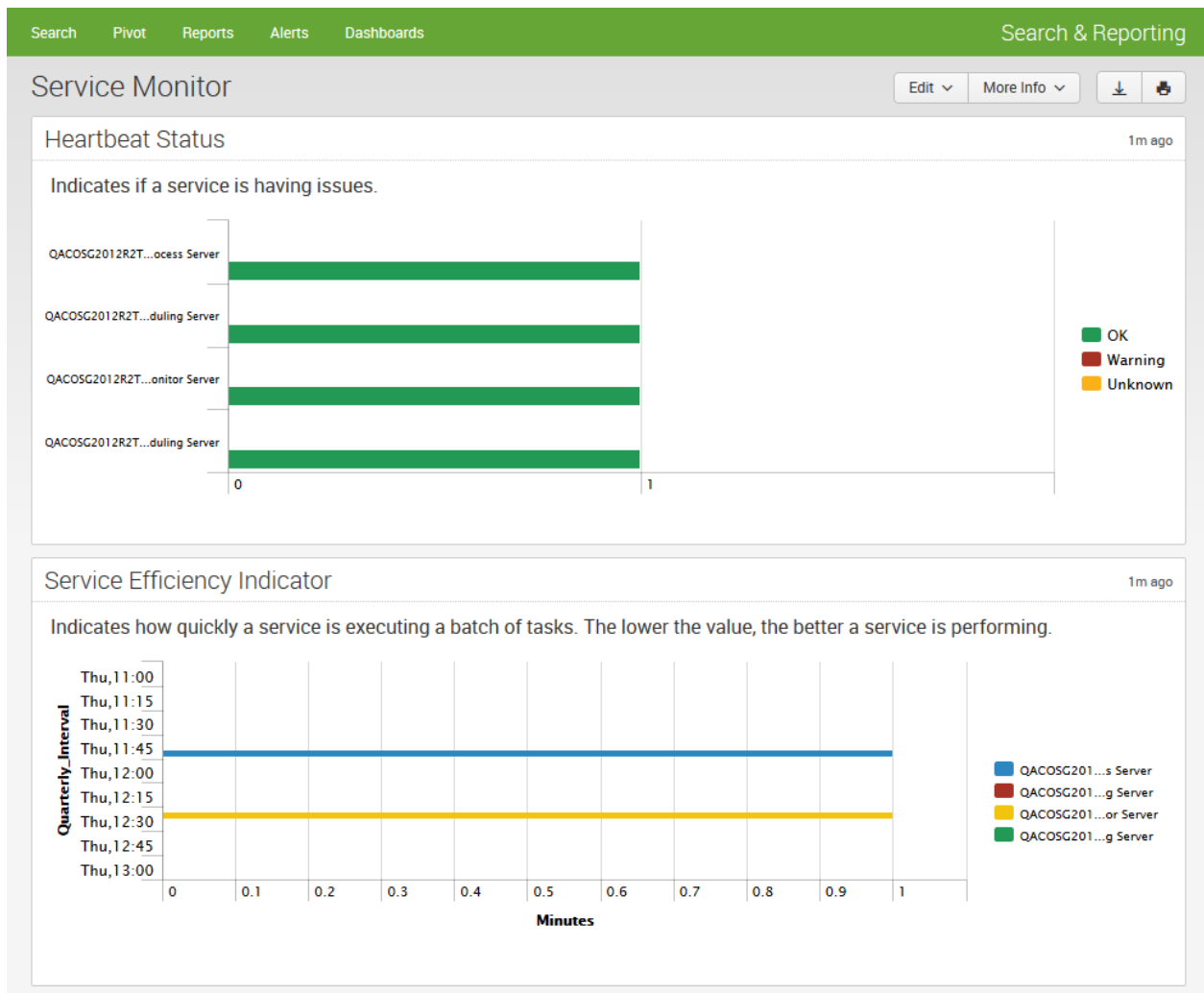
Modify the Dashboards to meet your needs or create your own Dashboards and searches in Splunk. For example, you might want to create a Dashboard to show threshold breaches for certain services.

To implement these Dashboards, copy the text in the shaded area below to a basic text editor, such as Notepad, and then add it to a Dashboard in Splunk.

```
<dashboard>
  <label>Service Monitor</label>
  <row>
    <panel>
      <title>Heartbeat Status</title>
      <chart>
        <title>Indicates if a service is having issues.</title>
        <search>
          <query>MessageName="Service Heartbeat" AND ServiceName="*server*
" |
          stats max(_time) AS last_seen by ServiceName, host | eval
          timediff=(now()-last_seen)/60    |
          eval status=case(timediff&gt;14400, "Unknown", timediff&gt;10
          AND timediff&lt;2880, "Warning", timediff&lt;10, "OK")  |
          eval Service = (host + "-" + ServiceName) | chart count by
          Service , status</query>
          <earliest>0</earliest>
        </search>
        <option name="charting.axisLabelsX.majorLabelStyle.overflowMode">el
lipsisNone</option>
        <option name="charting.axisLabelsX.majorLabelStyle.rotation">0</opt
ion>
        <option name="charting.axisTitleX.visibility">visible</option>
        <option name="charting.axisTitleY.visibility">visible</option>
        <option name="charting.axisTitleY2.visibility">visible</option>
        <option name="charting.axisX.scale">linear</option>
        <option name="charting.axisY.scale">linear</option>
        <option name="charting.axisY2.enabled">0</option>
        <option name="charting.axisY2.scale">inherit</option>
        <option name="charting.chart">bar</option>
```

```
        <option name="charting.chart.bubbleMaximumSize">50</option>
        <option name="charting.chart.bubbleMinimumSize">10</option>
        <option name="charting.chart.bubbleSizeBy">area</option>
        <option name="charting.chart.nullValueMode">gaps</option>
        <option name="charting.chart.showDataLabels">none</option>
        <option name="charting.chart.sliceCollapsingThreshold">0.01</option
>
        <option name="charting.chart.stackMode">default</option>
        <option name="charting.chart.style">shiny</option>
        <option name="charting.drilldown">all</option>
        <option name="charting.layout.splitSeries">0</option>
        <option name="charting.layout.splitSeries.allowIndependentYRanges">
0</option>
        <option name="charting.legend.labelStyle.overflowMode">ellipsisMidd
le</option>
        <option name="charting.legend.placement">right</option>
                <option name="refresh.auto.interval"> 120 </option>
                <option name="charting.legend.labels">[OK,Warning,Unknown]<
/option>
        <option name="charting.seriesColors">[0x229954,0xA93226,0xFBB117]</
option>
      </chart>
    </panel>
  </row>
  <row>
    <panel>
      <title>Service Efficiency Indicator</title>
      <chart>
        <title>Indicates how quickly  a service is executing a batch of
        tasks. The lower the value, the better a service is performing.</ti
tle>
        <search>
          <query>MessageName="Service Heartbeat"   | search ServiceName="*"
|
```

```
            bucket _time    span=15m | eval Quarterly_Interval=strftime(_time
, "%a,%H:%M ") |
            eval Service = (host + "-" + ServiceName) | chart MAX(Service_Bu
siest_Task_InMinutes)
            as ServiceDelay by Quarterly_Interval Service</query>
          <earliest>-2h@m</earliest>
          <latest>now</latest>
        </search>
        <option name="charting.axisLabelsX.majorLabelStyle.overflowMode">el
lipsisNone</option>
        <option name="charting.axisLabelsX.majorLabelStyle.rotation">0</opt
ion>
        <option name="charting.axisTitleX.visibility">visible</option>
        <option name="charting.axisTitleY.visibility">visible</option>
        <option name="charting.axisTitleY2.visibility">visible</option>
        <option name="charting.axisX.scale">linear</option>
        <option name="charting.axisY.scale">linear</option>
        <option name="charting.axisY2.enabled">0</option>
        <option name="charting.axisY2.scale">inherit</option>
        <option name="charting.chart">bar</option>
        <option name="charting.chart.bubbleMaximumSize">50</option>
        <option name="charting.chart.bubbleMinimumSize">10</option>
        <option name="charting.chart.bubbleSizeBy">area</option>
        <option name="charting.chart.nullValueMode">gaps</option>
        <option name="charting.chart.showDataLabels">all</option>
        <option name="charting.chart.sliceCollapsingThreshold">0.01</option
>
        <option name="charting.chart.stackMode">default</option>
        <option name="charting.chart.style">shiny</option>
        <option name="charting.drilldown">all</option>
        <option name="charting.layout.splitSeries">0</option>
        <option name="charting.layout.splitSeries.allowIndependentYRanges">
0</option>
        <option name="charting.legend.labelStyle.overflowMode">ellipsisMidd
```

```
le</option>
        <option name="charting.legend.placement">right</option>
        <option name="charting.axisTitleY.text">Minutes</option>
        <option name="refresh.auto.interval"> 120 </option>
            <option name="charting.seriesColors">[0xA93226,0xF1C40F,0x2
29954,0x2E86C1]</option>
      </chart>
    </panel>
  </row>
</dashboard>
```

Service Monitor

	At-a-Glance
	• About the Service Monitor

Getting Started	Using	Configuring (Advanced Users Only)
• Install the Service Monitor • CSM Servers (Services) • CSM Web Applications Managed by Service Monitor	• Open the Service Monitor • Start/Stop/Restart a CSM Server or Web Application • Reset IIS from the Service Monitor	• Configure Service Monitor Behavior and Access by Editing the Config File (Advanced Users Only) • Install the Service Monitor from the Command Line (Advanced Users Only)

About the Service Monitor

Important: The Service Monitor is currently available only for On-Premise Customers and Cherwell Support in order to monitor application performance.

The Service Monitor is a stand-alone Web Application that allows system administrators to remotely monitor and manage (start, stop, and restart) CSM Servers (services) and Web Applications and restart IIS, using a browser and an IIS-hosted web page. Service Monitor is installed using a stand-alone installer and is deployed using the Service Monitor web page.

Use the Service Monitor to:

- Monitor the status (running and stopped) of CSM Servers and Web Applications.
- Start, stop, and restart CSM Servers and Web Applications (Browser Client, Portal, Web-Forms, and Web Services).
- Reset IIS.

The Service Monitor is accessed via a web page, making the Service Monitor is ideal for hosted Customers because Users can remotely monitor and manage services. Use the Server Manager, a similar tool, to locally monitor and manage services. The figure shows the status of different servers and the server start/restart/stop options.

The Service Monitor is comprised of two components:

- A service-hosted Windows Communication Foundation (WCF): This component improves security by providing each log-in with a new session ID. Along with encryption, this ensures that HTTP messages are not hijacked by a malicious client.
- An Internet Information Services (IIS)-hosted website: This component allows end Users and administrators to securely manage remote IIS Servers. The URL http:// <domain>cherwellservicemonitor/.

Users install the Service Monitor using an installation wizard. All access is controlled using Windows Authentication credentials and is verified in the WCF service for each request.

> **Note:** Cherwell Service behavior and access is established during the installation. For specific control, Advanced Users can install the Service Monitor from the Command Line (Advanced Users Only) or edit the Cherwell Monitor config file (Advanced Users only).

CSM Web Applications Managed by the Service Monitor

The following CSM Web Applications can be managed by the Service Monitor:

- **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.

- **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.

- **Web-Forms™:**

  Cherwell Web-Forms™ is a browser-based application that allows Users to enter, view, and edit CSM Business Objects over the web without having to log in (example: Surveys, registration, ordering, etc.). This tool also allows for the remote execution of One-Steps.

- **Cherwell Web Service (Web API):**

  The Cherwell Web Service (CWS) is an API for communicating with CSM using Simple Object Access Protocol (SOAP) over HTTP. CWS must be running for the Mobile applications to operate, and is also required for a number of other features (RSS feeds, SAML security access, Bomgar® integration, etc.).

Service Monitor Good to Know

- Service Monitor is installed using a stand-alone installation wizard and is deployed using the Service Monitor web page.

- Service Monitor is ideal for remotely managing servers and Web Applications (example: Ideal for hosted customers). Use the Server Manager, a similar tool, to locally monitor and manage services.

- All User access is controlled through Windows Authentication and is verified in the WCF service for each request.

- Cherwell Service behavior and access is established during the installation. For specific control, install the Service Monitor from the Command Line (Advanced Users Only) or edit the Cherwell Monitor config file (Advanced Users only).

- Use the Cherwell Monitor Log (.txt) file to track Service Monitor operations (ex. Each time a User clicks a Service Monitor button).

- CSM Servers typically start automatically after the CSM suite is installed.

- Servers and Web Applications can be restarted without resetting IIS because the restart modifies the web.config files for each, which causes the applications to be recompiled and restarted.

- The Application Server is special because it forms the interface between the Client applications and database (a 3-tier connection).

- If the Application Server is installed under IIS Server, only one server can be running. The other is listed as unavailable.

Installing the Service Monitor

Use the Service Monitor to specify:

- Server name.
- Server type.
- User access.

Contact Cherwell Support to receive the Service Monitor installation file.

To install the Service Monitor:

1. Double-click the Cherwell Service Monitor.exe file.

   The Cherwell Service Monitor Wizard opens.

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

   The License Agreement page opens.

3. Read the license agreement. The license agreement can also be printed. To accept the license terms, select the I accept the terms in the license agreement check box, and then click Next.

   The Monitor Configuration page opens.

4. Specify the general server details:
   a. Displayed Name of Server: Use the default name (Cherwell Service Monitor) or provide another name. This is displayed on the Service Monitor web page banner.
   b. Select the type of server to be monitored, either:

      Production: Select this radio button to install the Service Monitor on a live system used in a production environment.

      Non-production: Select this radio button to install the Service Monitor on a development or test server.
   c. Select the default access to the Service Monitor, either:

      Don't Allow Access to the Service Monitor: Select this check box to prevent Users from accessing the Service Monitor.

      Allow read-only access to the Service Monitor: Select this check box to allow Users to view the Service Monitor but not make changes.

      Note: This is the default access for Users who do not have explicitly-defined access within Service Monitor. For specific control over Service Monitor behavior and access, install the Service Monitor from the Command Line (Advanced Users Only) or edit the Cherwell Monitor Configuration file.

5. Click Next.

The Destination Folder page opens.

6. Select the folder location to install the Service Monitor installation files. Click Next to accept the default or click Change to browse and select the desired folder location. Using the default installation folder is recommended.

On 32-bit machines, CSM files are installed to C:\Program Files\Cherwell Service Management.

On 64-bit machines, CSM files are installed to C:\Program Files (x86)\Cherwell Service Management.

> **Note:** Even though CSM files are installed to the (x86) directory, CSM runs as a 64-bit application on 64-bit machines. CSM installs to the x86 directory because Windows installers do not easily support installing applications that are both 32-bit and 64-bit. CSM does not install to C:\Inetpub because IIS removes files in this directory in certain scenarios.

7. Click Next.

The Ready to Install the Program page opens.

8. Click Install.

When the install is complete, the Install Complete page opens.

9. Click Finish.

Open the Service Monitor

To open the Service Monitor:

1. Browse to **http://<domain>/CherwellServiceMonitor/**. The domain is the same name given during the installation process.

   After authentication is complete, the Service Monitor page opens.

Reset IIS from the Service Monitor

Use the Reset IIS Action (under Actions) on the Service Monitor web page to reset IIS, which restarts anything running under IIS (example: Web Applications).

To reset IIS from the Service Monitor:

1. Open the Service Monitor.
2. In the Actions area, click Reset **IIS**.

   Tip: To refresh the services and update the web page, click Refresh.

Start/Stop/Restart a CSM Server or Web Application from the Service Monitor

Use the Service Monitor to stop, start, or restart the following CSM Servers:

- Application Server
- Automation Process Server
- E-mail and Event Monitor Server
- Scheduling Server
- Trusted Agents Server (if installed and configured)

  Note: If using Trusted Agents for security or e-mail operations, restart the Trusted Agents server first.

Use the Service Monitor to stop, start, or restart the following CSM Web Applications:

- Browser Client
- Customer Portal
- Web-Forms
- Cherwell Web Service

To start/stop/restart a CSM Server or restart a Web Application:

1. Open the Service Monitor.
2. Locate a **CSM Server** or **Web Application.**
3. Click an operation:

   Start: Start a CSM Server or Web Application.

   Stop: Stop a CSM Server or Web Application.

   Restart: Restart a CSM Server or Web Application, click .

   Refresh: Refresh the services and update the web page (under Actions).

   Note: If a service is already running, the start option is disabled.

Configuring the Service Monitor for Advanced Users

Cherwell Service behavior and access is established during the installation. For specific control, install the Service Monitor from the Command Line (Advanced Users Only) or edit the Cherwell Monitor config file (Advanced Users only).

Configure Service Monitor Behavior and Access by Editing the Config File (Advanced Users Only)

Default behaviors and access are established during install, but advanced Users can edit the Service Monitor config file (CherwellServiceMonitorConfiguration.xml) to change the options.

To edit the Service Monitor config file:

1. Locate the config.xml file at:

   C:\Program Files (x86)\Cherwell Service Management\CherwellMonitor\App_Data.

2. Open the file with Notepad.

   From here, the access commands and settings can be edited and tailored to fit the needs of administrators or advanced Users. For a table of command definitions and values, see Install the Service Monitor from the Command Line (Advanced Users Only).

3. Make any desired changes to the config file and **Save** (using File>Save or CTRL+S).

Install the Service Monitor from the Command Line (Advanced Users Only)

Advanced Users can install the Service Monitor from the command line. When installing from the command line, define:

- Settings: Where to install the files, what type of server to monitor, what title to display on the website banner, and default access.
- Access: Who can view and make changes to the Service Monitor (access is generally defined through default rights, and access is specifically defined via a list of Users.

The tables list the settings and access commands.

Note: Installs for ALL USERS by default.

Available Settings	Definition	Default Values
`INSTALLDIR`	Location/folder in which to install the Service Monitor files.	[programfilesfolder]\Cherwell Service Management (default)
`CW_ISPRODUCTION`	Type of server to be monitored.	• True = Production (default) • False = Non-production
`CW_TITLE`	Title to be displayed on the Service Monitor web page.	Cherwell Service Monitor (default)
`CW_DEFAULTACCESSISREADONLY`	Default access to the Service Monitor. This is the default access for Users who are not explicitly given access through the Read/Write Permissions List.	• 1 = Read-only (default) • 0 = Access denied.
The following are set only through the command line. **Note:** View = Read-only access (example: View service status in the Service Monitor but no edit); Edit = Full read/write access (example: View service status AND start/stop/restart services in the Service Monitor.		

`CW_USERSWHOCANALWAYSEDIT`	List of Users who explicitly can edit the Service Monitor (full read/write access).	Blank (default), but information is required. Comma delimited list of Users.
`CW_USERSWHOCANNEVEREDIT`	List of Users who explicitly cannot edit the Service Monitor (access denied).	Format: DOMAIN\Username if the server is joined by a domain. Ex. Cherwell \Henri.Bryce
`CW_ANONYMOUSUSERCANVIEW`	Non-authenticated Users can view but not edit (read-only access).	• True • False (default)
`CW_ANONYMOUSUSERCANEDIT`	Non-authenticated Users can edit the Service Monitor (full read/write access).	• True • False (default)
`CW_ADMINISTRATORSCANVIEW`	Allow Users in the OS-level Administrator Group to view but not edit the Service Monitor (read-only access).	• True • False (default)
`CW_ADMINISTRATORSCANEDIT`	Allow Users in the OS-level Administrator Group to edit the Service Monitor (full read/write access).	• True • False (default)

The following is an example command line:

```
"Cherwell Service Monitor.exe" /s /v"/qn CW_USERSWHOCANALWAYSEDIT="user lis
t" CW_DEFAULTACCESSISREADONLY="1""
```

Anything Variable that is passed and has spaces requires the quotes be proceeded by a \. If there are not spaces, this is not required ; however, it will not hurt anything if they are used:

```
"Cherwell Service Monitor.exe" /s /v"/qn CW_USERSWHOCANALWAYSEDIT=\"user li
st\" CW_DEFAULTACCESSISREADONLY=\"1\""
```

CSM Sizing and Scalability

You can scale and size your CSM system in several ways:

- The number of records, Attachments, and reports stored in your system.
- How many concurrent Users CSM supports based on usage scenarios.
- Installation location of the CSM database and server components.

Technical Architecture

Installation configurations vary; however, a typical installation is called a *single-server installation* because the Cherwell Application Server and supporting servers (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 servers (services), and CSM Web Applications.
- **(Tier 3) Client machines:** House the client-only files/administrator tools (the Desktop Client, CSM Administrator, and all the supporting tools/utilities.

The following figure shows a typical single-server installation.

Network Configuration Examples

Network configurations can range from basic to those that contain full redundancy and scalability. Examples of four setups are given with a brief description. These do not represent the only way a network can be set up, but they show our recommendations.

HTTP/TCP Communications:

The diagram below shows how various components of the deployment communicate under a typical implementation.

Note: The ports used by the different services can vary.
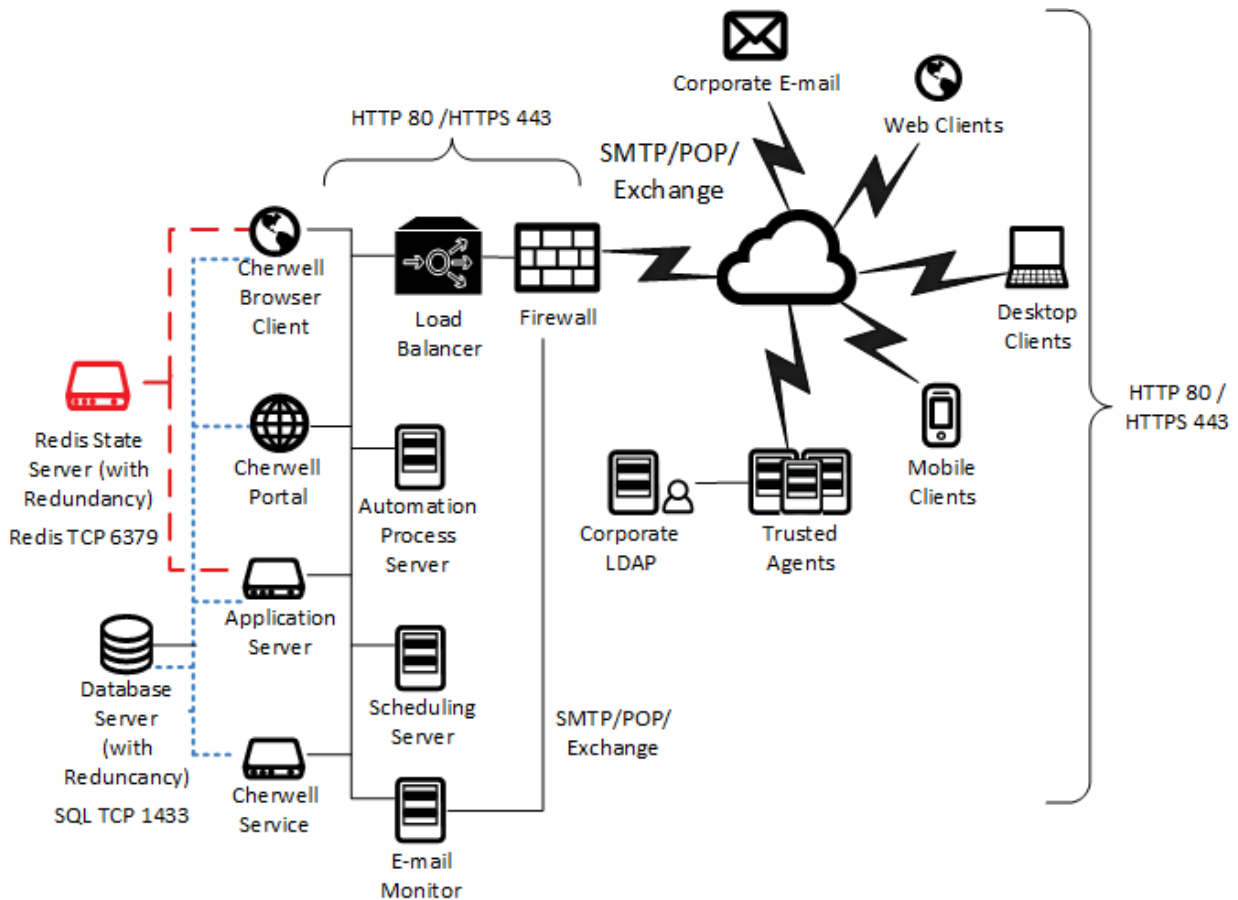
Consolidated Layout

This configuration works well for smaller establishments with a low number of Users. The configuration is deployed as either a physical server or a virtual server (SaaS, for instance). This configuration is also referred to as a single-sever scenario.

Consolidated sizing:

- Small/med customers: Up to 1,000 concurrent Users.
- Cannot scale beyond 14 cores (approximately 1,000 Users).
- Does not address high availability.
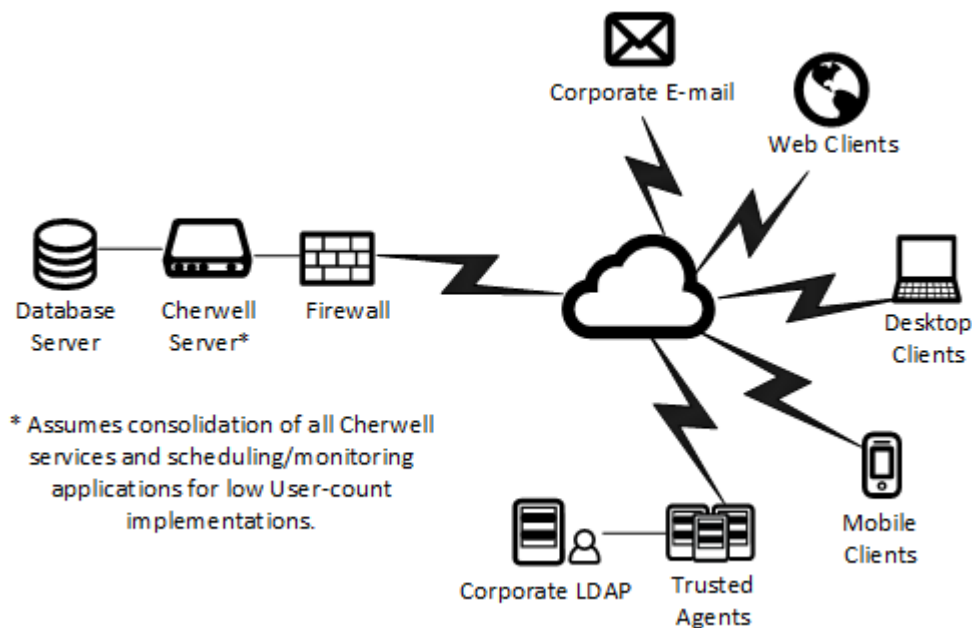
Rules of Thumb

- 50 to 100 licenses = 150-300 technicians, 30 percent technicians concurrent (1:3).
- 900 Portal Users = 18,000-20,000 User pool, 5 percent concurrent coverage.
- 1 CPU cor per 75 concurrent Users. 2 minimum: 1 for OS, 1 for CSM.
- 50 MB of memory per session for application and web servers.
- 600 MB of storage per license per year.

Dedicated Layout

This setup is the most common for Customers. Each front-end and back-end service is broken on its own machine. For Scheduling service, it scales horizontally and can have active instances on multiple machines. There are two ways to scale out the Scheduling service:

- Split the workload using Groups.

- Distribute the workload across multiple servers per Group.

If scaling horizontally, consider the balance between the CPU off-loading and the impact on SQL. This configuration offers high availability using a master/slave and clustering.
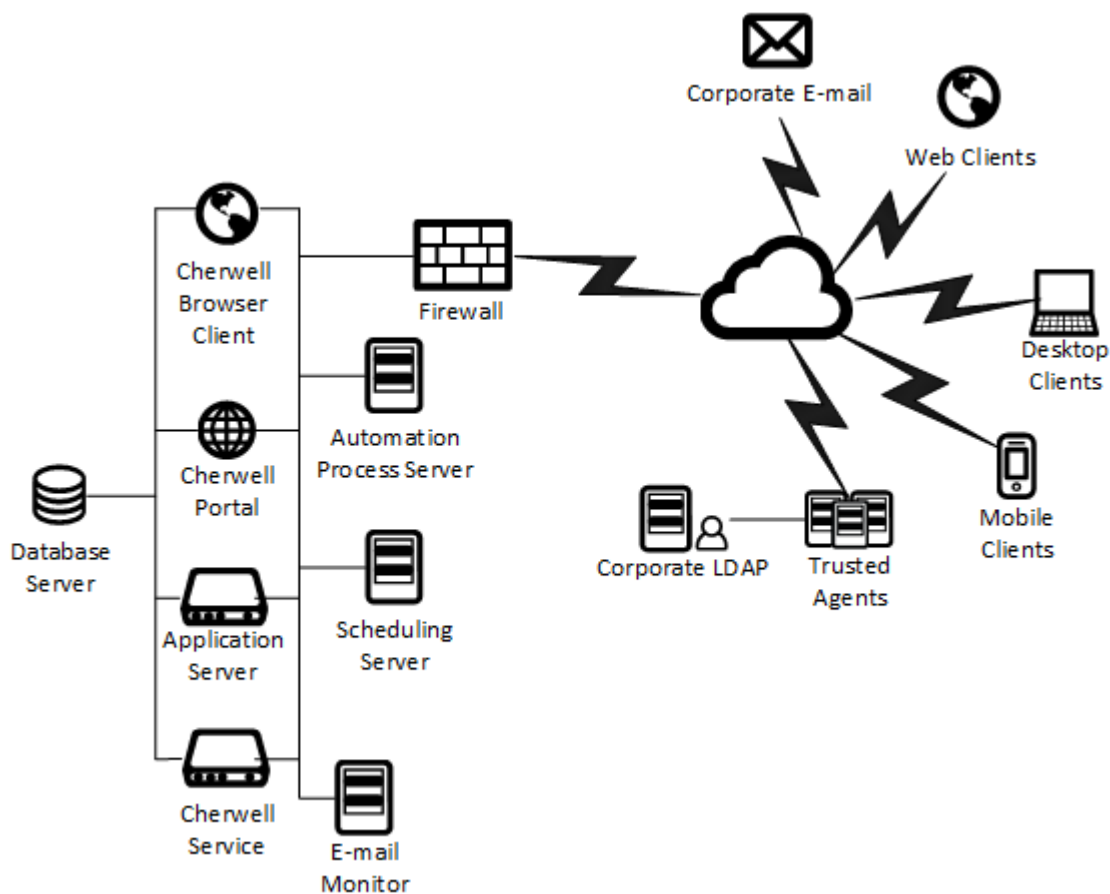
Advanced Layout

This setup is the most complicated and should only be used in an environment with advanced technical support. This approach offers full redundancy and scalability. This configuration can also be referred to as a server farm configuration. For more in-depth information, see the Cherwell Server Farm section.
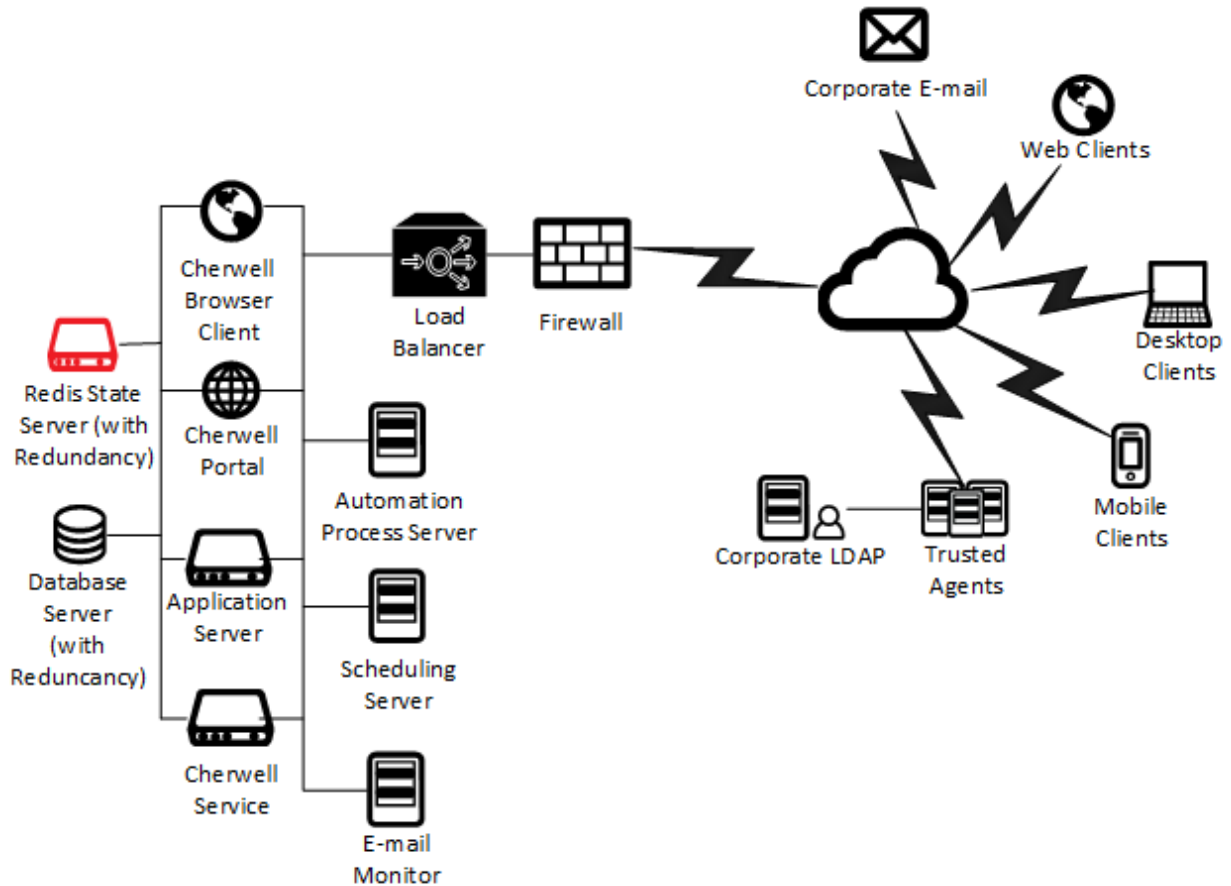
Sizing and Scalability Considerations

Installation Considerations

Database Installation Considerations

CSM uses Microsoft SQL Server as a back-end database (see the system requirements for supported versions). SQL Server can often be installed on the same server as CSM. However, organizations with a centralized database server should host CSM on that server instead. This setup is more efficient because it simplifies management and ensures that CSM data participates in an existing backup/recovery plan.

When moving the CSM database to a separate server, consider the following:

- Network activity exists between the CSM Server and database server (typically via TCP/IP). 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, separating secondary services might improve efficiency. Typically, this includes secondary services expected to use a significant amount of data.
- Server Farms: The Cherwell Server and CSM Web Applications also support enabling of Server Farms starting with CSM 6.0. This utilizes a Redis cache to handle state management between multiple servers when used with a hardware load balancer. For more in-depth information, see the Cherwell Server Farm section

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 mount of overhead, but in the case of the Trusted Agents for e-mail, the impact can be as much as a 40% reduction in the throughput of e-mails.

Scaling Variables

Use the minimum system requirements as a guide, then scale CSM based on the specific projections of the organization. For more information on scaling in a single-server configuration, see the Consolidated Layout section. The table below lists variables that will affect your system's scalability:

Variable	Notes
Total number of Users	
Concurrent licenses used	• Consider factoring 600 MB of storage per license per year.
Number of records created (ex. Incident or Change)	• If the record count is especially high, consider increasing the memory and processors on both servers.
Number and complexity of system relationships	
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.
Using a server farm	• Utilizing one or more services as a server farm incurs overhead that lowers the number of concurrent Users serviced by a single machine. While the total number of Users supported is higher, the hardware requirements per User also increases. • 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. For more information, see Cherwell Server Farms.

CSM Scalability Report

Scalability testing was conducted by Cherwell Software for the CSM Desktop Client and the CSM Web applications (Browser Client and Customer Portal). Sample tests were performed to replicate a generic usage scenario with reasonable delays to represent concurrent Users utilizing the system on an average day.

The tests used a random wait between operations, averaging 20 seconds, to mimic real-world User activity. Actual User loads are determined by a number of factors including User responsibilities within the organization, Customer interactions, management policies, system customizations, etc. Higher User quantities for a database might be obtained by utilizing additional servers. Having a high number of Users in the system does not mean a high number of identical actions being executed within the same time. The test scripts were run using a scenario where there is a high number of Users acting independently within the system and executing random actions at random intervals to mimic real-world usage of the system.

Scalability Testing Results

Following are the test results for a single-server configuration:

Concurrent Users	CPU	Memory	Storage per License per Year
75	1 core	50 MB memory per concurrent session	600 MB

Following are the test results for a Cherwell Server Farm configuration:

For in-depth information, see Cherwell Server Farm.

Concurrent Users	CPU	Memory	Storage per License per Year
50	1 core	60 MB memory per concurrent session	600 MB

Notes:

- These numbers apply for concurrent Users.
- Higher User quantities for a database might be obtained by utilizing additional servers.
- Having a high number of Users in the system does not mean a high number of identical actions being executed within the same time. The test scripts were run using a scenario where there is a high number of Users acting independently within the system and executing random actions at random intervals to mimic real-world usage of the system.

Systems Used for Scalability Testing

Test servers:

- All tests were conducted on High Frequency Intel Xeon E5-2666 v3 (Haswell) Processors.
- All tests were run on AWS configured with Microsoft Windows Server 2012 R2.
- AWS machines were not dedicated machines. However, it is expected that if an installation of CSM coincides with other applications or services, then additional hardware is required to meet these benchmarks. Future versions of CSM might introduce features and functionality which can require additional hardware to attain acceptable performance. Business Process integration (Scheduling Service, E-mail Integration, etc.) might also have an impact on the hardware required for acceptable performance.

> **Note:** Tests were conducted using AWS machines with the specifications above. Results can differ on varied environments, but similar results can be expected for similarly configured environments.

All tests ran against a SQL Server engine on a separate server with the following specifications:

- SQL Server 2014 Standard on Windows Server 2012 R2 for a c4.xlarge instance type with a
- 30 GB hard disk configured as a gp2 volume Type; 90/3000 IOPS

Scalability Testing Content and Operations

For CSM Web applications, all tests were conducted against the demo.czar file in an as-is condition with no custom Business Objects or operations.

For the CSM Desktop Client, the following modifications were made:

- Some One-Steps were created to simulate record create, update, and delete operations.
- The calculation on the Linked SLA field in the Incident table was removed.

Scalability Testing Operations

For CSM Web applications, we tested performance using the following operations:

- Login.
- Create Incident - create new, populate fields, save.
- Create Change Request.
- Search Incidents.
- View Incidents.
- View Dashboard.
- Logout.

For the CSM Desktop Client, we tested performance using the following operations (each User repeated these items twice per test case):

- Search Change Requests and step through 50 of them.
- Run the All Incident Search.
- View the top Incident.
- Clone the current Incident and save it.
- Delete the newly saved Incident.
- Do a Quick Search for a known keyword and step through the first 50 results.
- Run the *All Changes* change request search.
- Do a Quick Search for a known keyword and step through the first 50 results.
- Simulate a Dashboard three (3) times. The Dashboard simulation is done by executing the following search operations in parallel:
    - Discussion - All Discussions.
    - Incident - All security.
    - Incident - Closed Incidents.
    - Customer - All Customers.
    - Customer - Company.

- Search through Tasks without stepping through them.
- Create, update, or delete an Incident.
- Search for an Incident, close, and reopen it.

Cherwell Server Farms

A Cherwell Server Farm is a configuration where a number of servers (physical or virtual) are configured to work together as a single unit, as opposed to a single-server scenario where there is only one instance of each Cherwell Server running.

About Cherwell Server Farms

Using multiple servers allows for:

- A level-of-fault tolerance.
- Individual servers to also be taken offline.
- Operating system and hardware maintenance without reducing end-User availability.

Note: Services that are not load balanced should not be installed on more than one machine. Set up another single-server connection for services that cannot be load balanced.

There is near-linear growth using the Cherwell Server Farm. The more servers added to the farm, the more Users CSM servers 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 in order to support more Users. If two servers support 100 Users, then three servers can support 150 Users.

Important: Using the Cherwell Server Farm can increase the stress on SQL Server, the load balancer, and Redis Server. When creating a Cherwell Server Farm it is imperative to consider the impact of an increased load on the entire infrastructure. Do not just add servers.

Specific CSM Installation Requirements

There are some specific CSM installation requirements to be able to enable a Cherwell Server Farm:

- CSM must be installed as an IIS service, not a Windows service.
- Windows IIS features *HTTP Activations and non-http activations* must be installed.

Components

Server farms can be configured differently from business to business, but all server farms should have similar components set up in the same way.

> **Note:** Setting up and configuring a Cherwell Server Farm is for advanced Users only. If unfamiliar with the functionality, please contact Cherwell Professional Services for assistance at support@cherwell.com.

A server farm will contain at a **minimum** the following components:

- **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 User's requests. All servers need to 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 (a box) and a virtual server (a software server, installed on a physical server; or, a VM 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.

Operations and Resources

Server Farms require a number of components to work together. This comes at a measurable cost of extra CPU and network, especially when it comes to the web server.

The following table contains the high-level sequence of events every time the web server serves a web request. The Resource Required column offers some insight into the consequences of scaling up a User base. The *Added by Cherwell Server Farm* column indicates if the Operation is added when configuring a Cherwell Server Farm. Based on the information in the table, consider additional resource usage.

Operation	Added by Cherwell Server Farm	Resource Required
Request begins		
Web Server sends a Redis request to get latest Session State	Yes	CPU, negligible
Redis Server retrieves state and send it over the network	Yes	CPU, light
Web Server waits for 3-5MB of data to be transferred to the web server from Redis	Yes	Network 3-5mb/User
Web Server decompresses 3-5MB of data	Yes	CPU
Web Server deserializes 3-5MB of JSON	Yes	CPU
Web Server Execute request as usual		
Web Server serializes session state	Yes	CPU, light
Web Server compresses session state	Yes	CPU, light
Web Server send 3-5MB of state to Redis	Yes	Network 3-5mb/User
Redis Server stored session	Yes	CPU, light
Web Server ends request		

Resource Considerations

Based on the table above, there are several impediments to consider.

Memory Usage

- Web server: Non load-balanced Cherwell Servers are memory intensive, but load-balanced servers (without session pinning) free up memory as soon as a request is ended. This makes memory a less probable bottle neck.

- Redis: 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. A good rule is 10 MB x Expected peak number of Users.

CPU

- Web server: The cost of deserializing session is four times the cost of serialization.

- Redis: If using a single-server scenario (no slaves), the rule is that 5000 Users will probably use about 15% of your CPU. Remember to assign 2 CPUs to your Redis machines. One will be used by the system, the other one by your Redis process.

Network

- Traffic between the Browser 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 Server(s).
  Network traffic between Broswer 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.

- Traffic between each web server and Redis: This number is highly dependent on your content. Each *page* on the browser might turn into multiple web requests, depending on the page content.
  Rule of thumb: Estimate between 6-10 MB of memory usage per User session. For example: 1,000 concurrent Users x 10 MB/User = 10 GB of RAM per server

Purpose of Redis

At the center of the Cherwell Server Farm is the Redis that is used as the in-memory cache. Redis is an in-memory data structure store, and is used as a database, cache, and message broker.

By connecting every web server to the same Redis, the applications can share state and collaborate. In other words, whenever 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 pickup 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. Things are different for Cherwell Web Server because IIS holds state for each User in form of session, and it can reach the size of a few MB (3-5MB is the typical size). For every web request going from the browser to the server, there is an exchange of session state twice with Redis:

- When the request starts, in order to retrieve session from Redis.
- When the request ends, in order to save session to Redis.
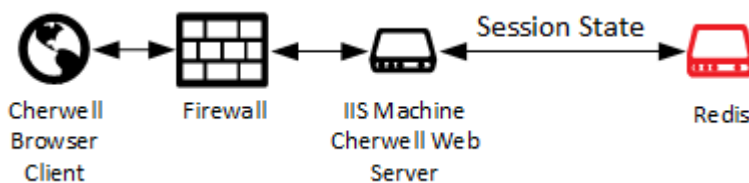
Session Caching

Session caching is a strategy used to load balance Users across servers and allows for better use of resources while maintaining scalability and high availability. There are two main benefits of session caching:

- Enhances the average response time to virtually the same as a non load-balanced web server for the majority of requests.
- Reduces the Cherwell Server Farm demands on your network by an average of 50 percent.

Session caching is for advanced Users only. If you are an advanced User, see Advanced Session Caching and Pinning.

Configuring Cherwell Server Farm in CSM Administrator

There are several ways to configure a server farm. We discuss the most common and the best practices of configuring a Cherwell Server Farm. A server farm allows high volumes of Users to utilize several medium (4-core or higher) servers. A server farm consists of multiple Cherwell Servers connecting to multiple Redis Servers. The process to configure the Cherwell Server Farm has to be completed for each Cherwell Server. Use the Export and Import buttons to make it easier.

Some key points:

- Members of a Cherwell Server Farm should not share a hypervisor. VMs should be distributed across several hypervisors.

- A load balancer is required (CSM does not provide this).

  Note: The Microsoft Windows IIS Server module known as *ARR* (Application Request Routing) is not recommended.

- Performance could be penalized by enabling a server farm because it brings overhead to the individual servers participating in the farm.

Important: Ensure the configuration is the same across servers.

Configuring a Cherwell Server Farm

A server farm can only be used when the Cherwell Application Server is hosted in IIS. Http and Rest are required for the Application Server.

To configure a Cherwell Server Farm:

1. Click Start>All Programs>Cherwell Service Management>Tools>Server Manager.

2. Click Configure.
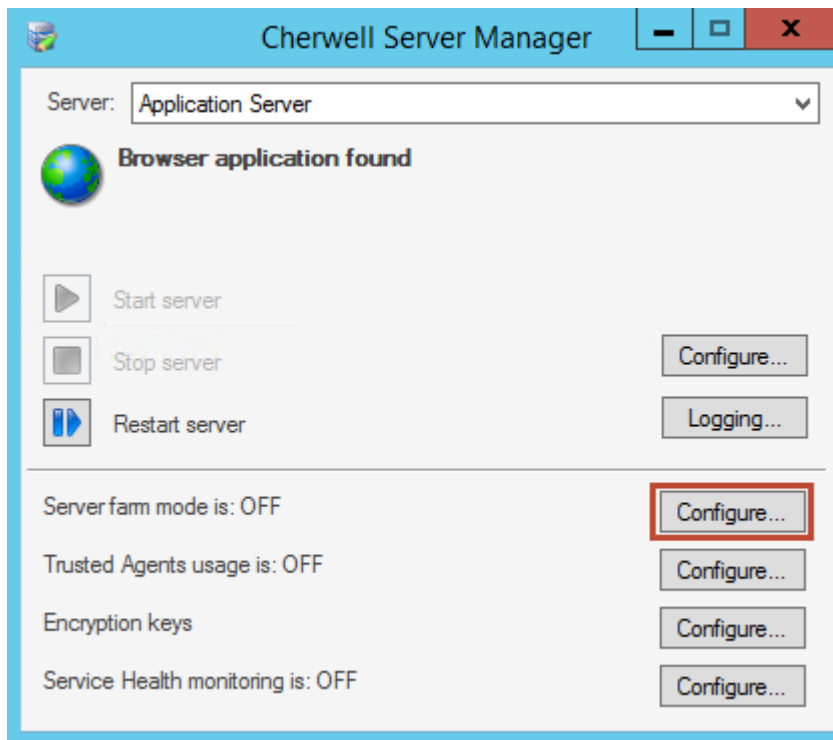
An Alert window opens warning to stop the server farm before changing settings.
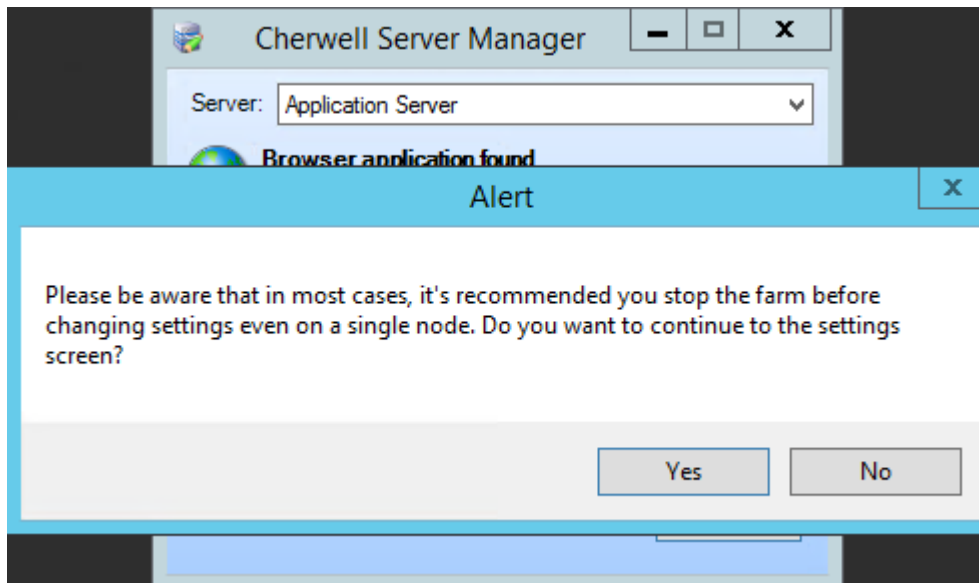
3. Click Yes to continue.

4. Define Website options:
   a. Use the up and down arrows to select the Session expiration.

   b. Select the Enable server farm mode check box.

   c. Use the up and down arrows to select the Session cache expiration.

   d. Select the Enable session caching check box.

5. Use the Import/Export buttons to enter the Redis information in a server, export the information, and then import it in another server.

6. Define New Redis Server options:
   a. Provide the **Host IP address** for the Redis Server.

   b. Use the up and down arrows to select the Port.

   c. Click Add.
      The IP address and Port appear in the Connect to list. Repeat this step to add all Redis Servers.

7. Provide the **Password** for the Redis Server.

> **Note:** If there are multiple servers in a master/slave configuration, ensure all servers share the same password.

8. Use the Connection Timeout 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.

9. 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.

> **Note:** If you have a master/slave with sentinel configuration and a slave becomes a master, the Sync Timeout setting determines how many seconds will elapse before your application switches to the new master.

10. Click OK.

Export a Server Farm Configuration

A server farm configuration can be exported to an XML file and used for several server configurations.

Note: A server farm can only be used when the Cherwell Application Server is hosted in IIS.

To Export Server Farm Configuration Information:

1. Click Start>All Programs>Cherwell Service Management>Tools>Server Manager.
2. Click Configure.

3. An Alert window opens warning to stop the server farm before changing settings.

4. Click Yes to continue.

5. In the Configuration window, select the Enable server farm mode check box.

6. Click Export.

7. Navigate to the location where to save the file.

8. Click Save.

9. After the file is saved, go to the Server Manager for different Cherwell Application Servers and Import a Server Farm Configuration.
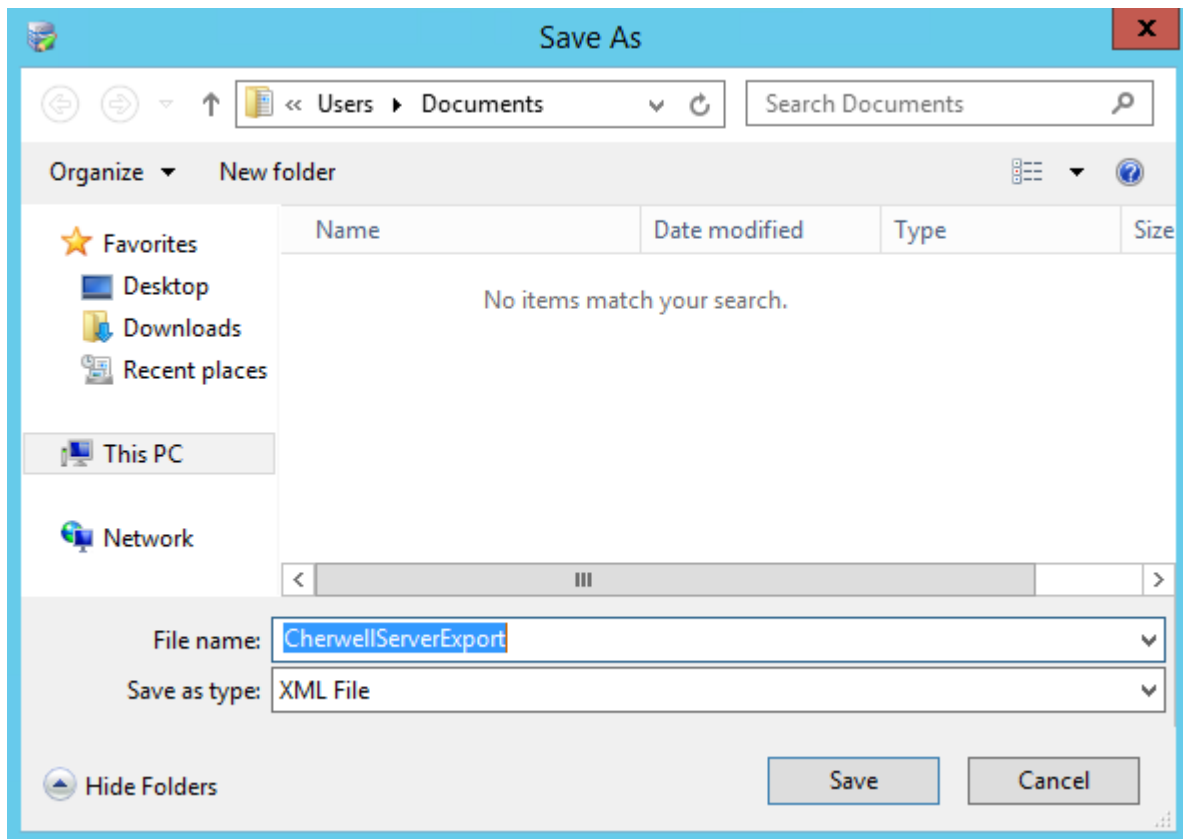
Import a Server Farm Configuration

A server farm configuration can be imported from a saved XML file. The XML file can be used across several server configurations.

🖊️ **Note:** A server farm can only be used when the Cherwell Application Server is hosted in IIS.

To Import Configurations to a Server Farm:

1. Click Start>All Programs>Cherwell Service Management>Tools>Server Manager.
2. Click Configure.

3. An Alert window opens warning to stop the server farm before changing settings.

4. Click Yes to continue.

5. In the Configuration window, select the Enable server farm mode check box.

6. Click Import.

7. Navigate to the location where the XML to import file is stored.
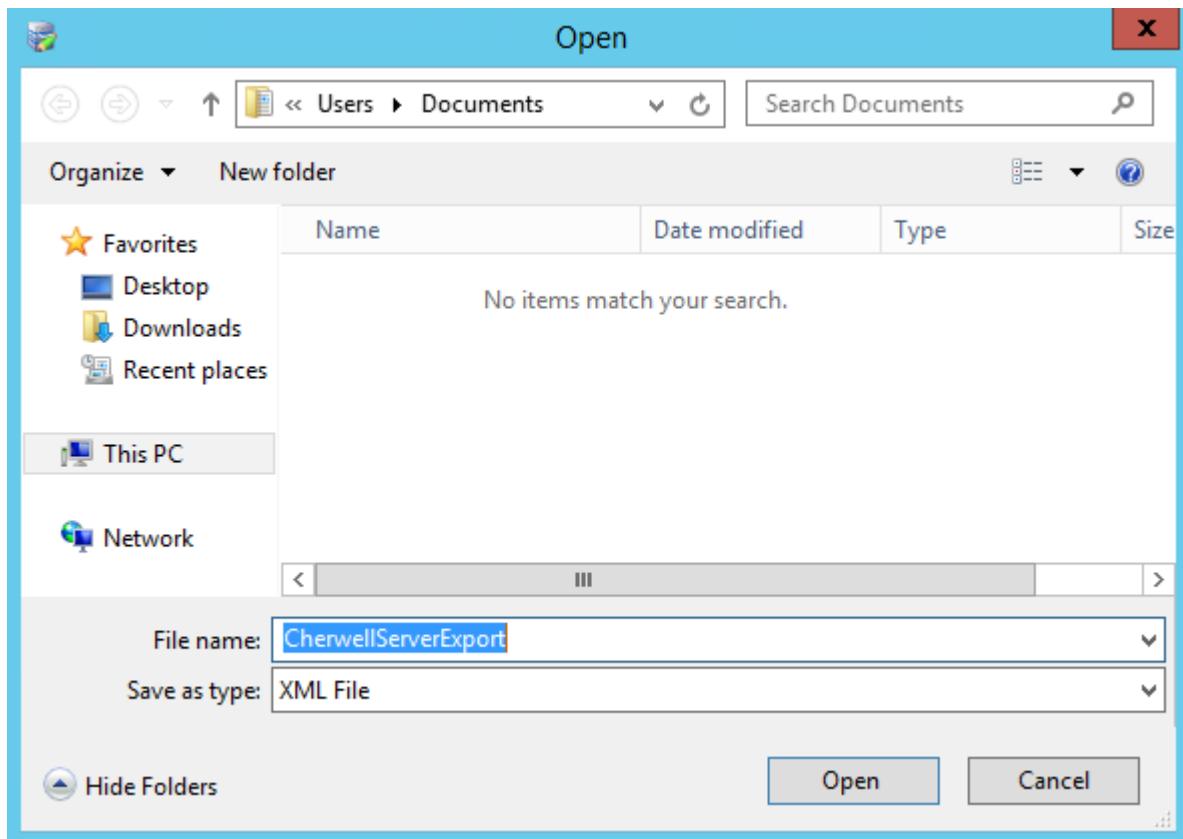
8. Click Open.

The window closes, and the configuration information appears in the Connect to section.

9. Click OK.

Configuration Best Practices

There are several ways to configure a server farm. This topic describes the most common and the best practices of configuring a Cherwell Server Farm.

Tested Redis Connections

CSM has been tested with Redis in the following environments:

- Windows with a single instance.
- Linux master/slave with sentinel.
- Windows master/slave with a sentinel.
  When configuring a cluster environment in Trebuchet Server Managers, Users only need to provide one IP for the cluster. In master/slave environment, add the IPs of the master and all slaves in the Connect to field when configuring.
- Redis Labs Enterprise Cluster.
  When configuring a RedisLab Enterprise Cluster environment in Trebuchet Server Managers, Users only need to provide one IP for RLEC. In master/slave environment, add the IPs of the master and all slaves in the Connect to field when configuring.

Recommendations

Hardware: Use the same hardware across server for easier management and performance predictability.

IIS ARR as a load balancer: Cherwell does not recommend using IIS ARR. While it can be made to work, ensure all of its response-caching features are disabled.

Using virtual machines: Be careful when using VMs. If all VMs are on the same server and the server goes down, the web farm stops working.

Cherwell Server Farm Q&A

Question: Could I take one physical box, divide it into two virtual machines, and install Cherwell Services on them as two different participants of the server farm?

Answer: You can, 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 VMs reside on different hardware is a better option.

Question: Can I mix and match server types on a single box?

Answer: Yes you can. 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: Are there specific CSM installation requirements for the Cherwell Server Farm?

Answer: CSM must be installed as an IIS service, not a Windows service. Windows Server IIS features *HTTP Activations and non-http activations* must be installed.

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. This is because of the overhead associated with the Cherwell Server Farm topology. The UI 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: What about the Scheduling service? Can it be load balanced?

Answer: The Scheduling service is a queued, single-threaded, back-end service like the others, though it is unique in one respect. It is the only queued service that can be scaled horizontally with active instances across several servers.

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. Remember, each of these services can have a single instance active at a time. If installed on multiple process servers, the redundant services must remain inactive, reside in separate cluster pools, be monitored by a health probe, and only become active when a corresponding active service goes offline.

SQL Server

Question: What type of cluster model does Cherwell recommend for SQL?

Answer: Always-On Availability Groups.

Question: What is the formula for determining the total amount of disk storage needed?

Answer: A starter rule of thumb 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, i.e. 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 files be distributed across separate disks?

Answer: Yes. For example: Data, Logs, temp, and DB.

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: Max 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.

Advanced Cherwell Server Farm

A simple configuration of the Cherwell Sever Farm is sufficient in most instances. The information in the Advanced Cherwell Server Farm section is intended for those who are comfortable and knowledgeable with the components and configuration of a Cherwell Server Farm.

> ✏️ **Warning:** Do not attempt to implement these processes if you are not an advanced User. You can cause serious network and system issues. Please contact Cherwell Professional Services for assistance at support@cherwell.com.

Implementing a Cherwell Server Farm

🖊 **Warning:** Do not attempt to implement these processes if you are not an advanced User. You can cause serious network and system issues. Please contact Cherwell Professional Services for assistance at support@cherwell.com.

To implement a Cherwell Server Farm (high level):

1. Distribute the requests to a single server across multiple servers.

2. Use a load balancer to distribute requests among servers.

3. Size the infrastructure to increase the number of Users and considering the levels of reliability you want to provide.

Setting up a Single-server farm

Consider setting 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.

To set up a single-server farm:

1. Install the Cherwell Application Server and Cherwell Web Server on a single machine.

2. In the Server Manager, turn on Server Farm features and connect to Redis. For more information, see Configure a Cherwell Server Farm in CSM Administrator.

3. Do not setup a load balancer.
   At this point you have a single server that behaves as if it is part of a farm. Open the Portal and Browser Client to see the data being stored in Redis.

There are several reasons to implement a Cherwell Server Farm. The most obvious, or recognizable, reasons are:

- Scale the number of users.

- Provide the ability to scale the number of Users that a Cherwell Server Farm can serve. The idea is if there are more Users, you can add more hardware and be able to horizontally grow 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. Using a Cherwell Server Farm allows you to add low-cost commodity boxes to the farm without having to exponentially pay more.
  Cherwell Server Farm provides the ability to:
    - Scale.

    - Scale cheaply.

    - Scale a lot more (without constraints of single server).

- Offer high availability.

Provide high availability (HA) so that even when one server goes down (because of a hardware failure) Users can continue using the application. Cherwell Server Farm eliminates a single point of failure (one server could go down, but the overall application can still be used by its Users).

High availability has different levels of service. In a perfect world, when a server goes down, there is no effect to the end User. Many environments need such level of HA, but others are prepared to sustain different levels of HA given the cost of maintaining perfect HA. For example, administrators trade faster performance for a level of service where some Users could be logged off if the server goes down, but they would be able to immediately log in again to continue working.

Distributing the Requests to a Single Server across multiple servers

After distributing the requests, the overall configuration changes from a single server to a multiple server.
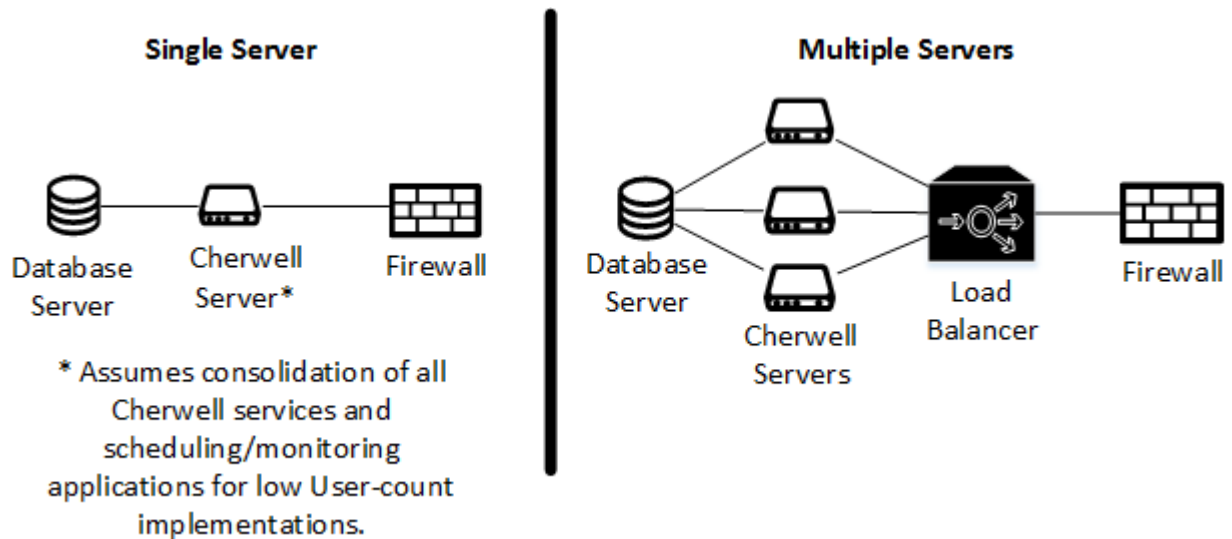
The main differences are the addition of the load balancer and extra Cherwell Servers. The Cherwell Server Farm uses a number of servers; the exact number depends on your specific scenario. Cherwell runs on different physical or virtual servers. Different Cherwell Servers (like the Application Server and the Web Servers) are installed multiple times on different boxes.

Using a Load Balancer

You most likely already have a firewall between the Cherwell Server and the web. With a Cherwell Server Farm, the firewall remains, and load-balancing capabilities are added (your current appliance might already support it). In a single-server scenario, all traffic that comes in for Cherwell goes to the same server. In a Cherwell Server Farm, Users are redirected to different Cherwell machines according to a number of load-distribution strategies.

The Cherwell Servers that can be load balanced are the Cherwell Application Server and the Web Server. 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. Cherwell 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 flowcharts show three examples of how a load balancer can be configured to handle requests.

**Traditional Load
Balancer**

Incoming request

↓

Elect a server based
on Round Robin,
Response Time, or
other metric

↓

Route the
request to the
elected server
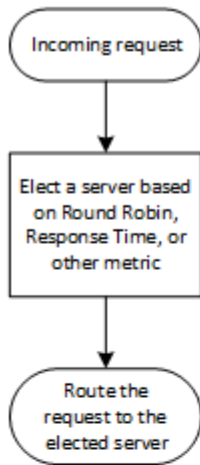
**Traditional Session-Pinned
Load Balancer Behavior**

Incoming request

↓

Is this session
pinned? — No → Elect a server based
on Round Robin,
Response Time, or
other metric

↓ Yes

Route the
request to the
elected server ←
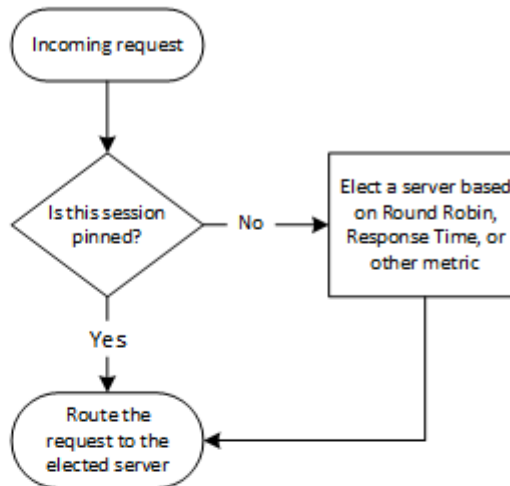
**Time Windows with Session Caching
and Pinning Load Balancer Behavior**

Incoming request

↓

Is this session
pinned? — No →

↓ Yes

Has the
pinned session
timed out — Yes → Elect a server based
on Round Robin,
Response Time, or
other metric

↓ No

Route the
request to the
elected server ←
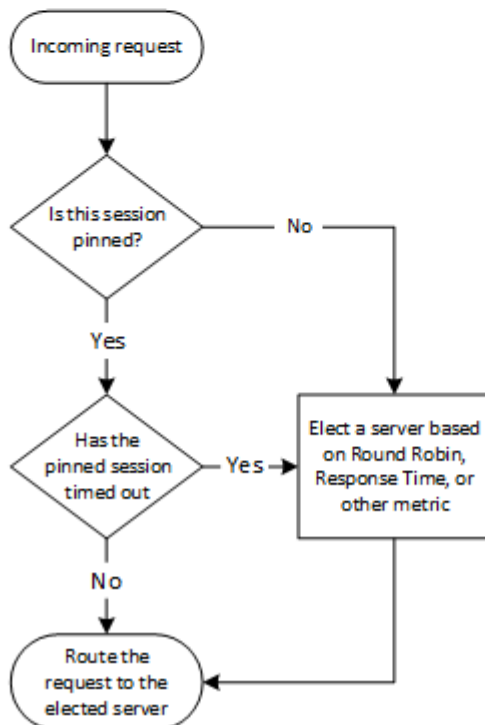
Load-Balancing Methods

These are examples of commonly supported load-distribution methods available to most load balancers:

- **Round Robin:**

  (Most Common) The system passes each new connection request to the next server in line, eventually distributing connections evenly across the array of machines being load balanced. This method works well in most configurations, especially if the equipment that is being load balancing is roughly equal in processing speed and memory.

- **Least Connections:**
    - Node:(Most Common) The system passes a new connection to the node that has the least number of current connections out of all pools of which a node is a member. This method works best in environments where the servers or other equipment you are load balancing have similar capabilities. This is a dynamic load balancing method, distributing connections based on various aspects of real-time server performance analysis, such as the number of current connections per node, or the fastest node response time.

    - Member: The system passes a new connection to the node that has the least number of current connections in the pool. This method works best in environments where the servers or other equipment you are load balancing have similar capabilities. This is a dynamic load-balancing method, distributing connections based on various aspects of real-time server performance analysis, such as the current number of connections per node or the fastest node response time.

- **Dynamic Ratio (member):**

  This method is similar to Ratio (node) mode, except that weights are based on continuous monitoring of the servers and are continually changing. This is a dynamic load-balancing method, distributing connections based on various aspects of real-time server performance analysis, such as the number of current connections per node or the fastest node response time.

- **Ratio Least Connections:**
    - Node: The system selects the node according to the ratio of the number of connections each node has active.

    - Member: The system selects the pool member according to the ratio of the number of connections each pool member has active.

- **Ratio (member):**

  The number of connections that each machine receives over time is proportionate to a ratio weight defined for each machine within the pool.

- **Weighted Least Connections:**
    - Node: The system uses the value specified in the node's connection limit and the number of current connections to a node to establish a proportional algorithm. This algorithm requires all nodes used by pool members to have a non-zero connection limit specified.

    - Member: The system uses the value specified in connection limit to establish a proportional algorithm for each pool member. The system bases the load-balancing decision on that

proportion and the number of current connections to that pool member. For example, member_a has 20 connections and its connection limit is 100, so it is at 20 percent of capacity. Similarly, member_b has 20 connections and its connection limit is 200, so it is at 10 percent of capacity. In this case, the system selects member_b. This algorithm requires all pool members to have a non-zero connection limit specified.

- **Least Sessions:**

  The system passes a new connection to the node that currently has the least number of persistent sessions. This method works best in environments where the servers or other load-balanced equipment have similar capabilities. This is a dynamic load-balancing method, distributing connections based on various aspects of real-time server performance analysis, such as the number of current sessions. Use of this load-balancing method requires that the virtual server reference a type of persistence profile that tracks persistence connections.

- **Observed:**
  - Node: The system ranks nodes based on the number of connections. Nodes that have a better balance of fewest connections receive a greater proportion of the connections. This method differs from Least Connections (node), in that the Least Connections method measures connections only at the moment of load balancing, while the Observed method tracks the number of layer-four connections to each node over time and creates a ratio for load balancing. This dynamic load-balancing method works well in any environment, but can be particularly useful in environments where node performance varies significantly.

  - Member: The system ranks nodes based on the number of connections. Nodes that have a better balance of fewest connections receive a greater proportion of connections. This method differs from Least Connections (member) in that the Least Connections method measures connections only at the moment of load balancing, while the Observed method tracks the number of layer-four connections to each node over time and creates a ratio for load balancing. This dynamic load-balancing method works well in any environment but can be particularly useful in environments where node performance varies significantly.

- **Predictive:**
  - Node: The system uses the ranking method used by the Observed (member) methods, except that the system analyzes the trend of the ranking over time, determining whether a node's performance is improving or declining. The nodes in the pool with better performance rankings that are currently improving, rather than declining, receive a higher proportion of the connections. This dynamic load-balancing method works well in any environment.

  - Member: Uses the ranking method used by the Observed (member) methods, except that the system analyzes the trend of the ranking over time, determining whether a node's performance is improving or declining. The nodes in the pool with better performance rankings that are currently improving, rather than declining, receive a higher proportion of the connections. This dynamic load-balancing method works well in any environment.

Sizing an Infrastructure

There are a number of questions you need to answer if you are thinking about an expandable User base that goes beyond what a single server can serve:

- What is the total number of Users I want to support?
- What is the typical number of parallel Users that I need to support?
- Are there any peak of usage where a high percentage of your Users might flood the system? If so what does that look like?

Once you have those numbers, then consider:

- Is your SQL Server sized correctly?
- Can your internal and external network pipe support such traffic?
- How much hardware do you need for the different Cherwell Services?

Architecture Guidelines

Warning: Do not attempt to implement these processes if you are not an advanced User. You can cause serious network and system issues. Please contact Cherwell Professional Services for assistance at support@cherwell.com.

In a single-server scenario (single machine), all the Cherwell Services are typically installed on the same machine, as shown in the architecture. In the green box, both Browser Client Server and Application Servers are in the same machine along with a variety of other servers.
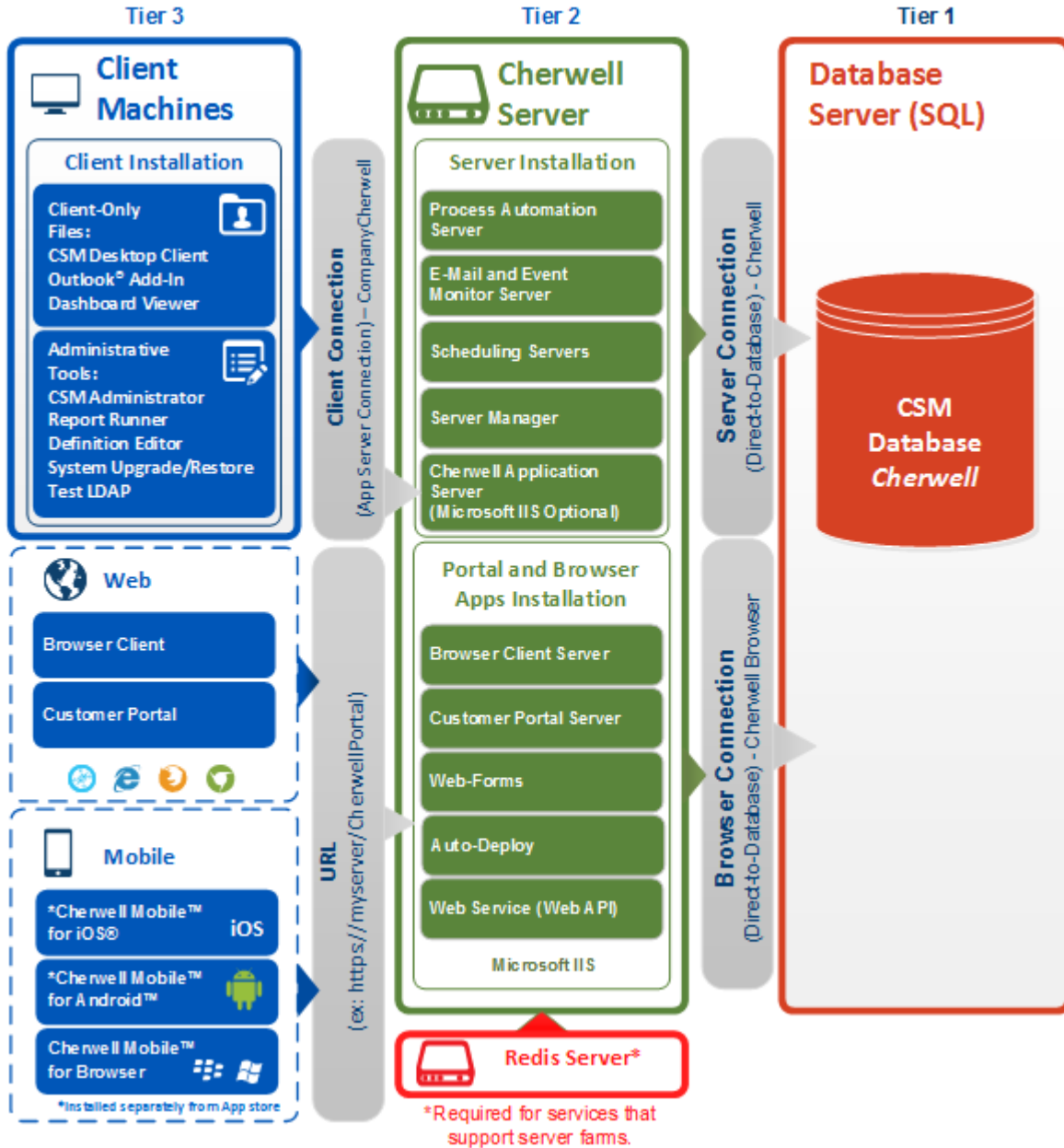
In a Cherwell Server Farm, services can be distributed onto different machines depending on the expected traffic. A Cherwell Server Farm is comprised of a number of Cherwell Servers that are distributed across hardware depending on the abilities of the server.

Coordinated Servers

Some servers can be load balanced, for example the application server and web server. These servers can be run in a load-balanced mode where servers on different boxes can work together as a single unit.

They are coordinated by communicating with a centralized session-state storage, Redis. In order to scale the service provided by these servers, more servers need to be added to the Cherwell Server Farm. Should one of those servers go down, Users experience a performance degradation inversely proportional to the number of machines.

Independent Servers

Some servers can collaborate even if they are not aware of each other. These are servers that process items from a queue. Typically, more than one of the servers can be fired up without having to change anything. The servers pick up items from a queue and process them individually. To scale the service provided by these servers, install and run the server on multiple machines. Should one of those machines go down, Users experience a performance loss that is inversely proportional to the number of machines.

Single-Instance Servers

For other servers, you cannot run more than one instance at a time. To scale these you need a bigger, faster machine. If that machine goes down, the service is interrupted. These servers process items from a queue. If a machine breaks and is offline for a few minutes, quickly bring the machine back online (or bring an identical machine back online). The new machine begins where the original machine left off, delaying the delivery or the processing by an interval of time. Since these machines work off of a queue, and not in real time, it is possible that Users might not notice the service interruption.

Advanced Redis Information

> **CAUTION:** Do not attempt to implement these processes if you are not an advanced User. You can cause serious network and system issues. Please contact Cherwell Professional Services for assistance at support@cherwell.com.

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.

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/slave 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.

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 rule of thumb, 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 in order 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:

- For the purposes of sizing Redis, set up a farm with a single server.
- Load into the system with 10 Users, and then measure the load in Redis.
- Load into the system with 20 Users, and then measure the load in Redis.
- Load into the system with 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, it is easy to 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
```

Current Sizing Limitations

There are some physical limits to the number of Users that can be supported based on the current configuration:

- Physical memory on a machine: Adding memory to a machine should be easy. It is common to have servers with hundreds of GB or even 2TB of data. Assuming a single User footprint of 4MB, that means being able to support 10,000 concurrent Users with 40GB of RAM.

- Network traffic: Once the RAM is sized, your next concern is throughput. The calculation would be similar to the table below (input rows are indicated, others are calculated).

Organizational specifics for sizing can vary depending on the assumptions made. Generally, based on the common numbers expect 10,000 Users to require 10 GIG+ per second to go through a network. These numbers are only the Redis traffic. Web and SQL traffic also increases the number. The increase happens in such a way that it is impossible to project, but should be fairly easy to find if metrics are run on the network. As Redis becomes the bottleneck, performance needs to be addressed across the board.

The calculations in the table below are based on default Cherwell Server Farm settings. Using Session Caching can drastically reduce the network traffic.

The example calculations below are from proven averages.

Example: For every page, you need to read from Redis an average of four times, and to figure out the actual traffic you have to double that (every time there is a read, there must be a write). The following table gives an idea of how to calculate the traffic:

Calculating Redis Network Traffic		
Input: Clicks per User per minute	2	How many times per minute does an average User click a button or a link? Once every 30 second is a good average between active Users and Users that wait between performing actions (or that just leave their browser open without even looking at it).
Input: Users	10,000	What is a reasonable peak of maximum concurrent Users? The number of concurrent Users that are using the system.
Input: Redis reads per click	4	Reads per click: Every time a User clicks a button, *something* happens. It can navigate from one page to another, or save an object being. Depending on content, the Browser Client is rendering a page that might make a number of changes when session caching is on.
Input: Redis Writes per click	4	This varies depending on content and the page the User is on.
Redis requests per minute	160,000	Calculated = Clicks x Users x (Reads + Writes)
Input: State size per User in MB	4	Varies depending on the content and the page that the User is on.
Redis Network Traffic per minute in MB	640,000	Calculated = Requests per minute x 4
Requests per second	2,667	Calculated = Requests per minute/60
Redis traffic per second in MB	10,667	Calculated = Traffic per minute/60

Redis Requirements

Redis can be configured in multiple ways. Our recommendations are based on testing results for working optimally with a general configuration of CSM.

For more information and support, refer to Redis.Io.

Redis Labs Enterprise Cluster

CSM 8.3.2 and later is compatible with Redis Labs Enterprise Cluster (RLEC). Use RLEC to configure Redis environments. Any version of RLEC will work with CSM.

Hardware Requirements

Sizing Redis is not just a matter of sizing its memory, but also fine tuning the rest of the resources. Be aware that:

- A machine (or virtual machine) should be dedicated to Redis.
- In the dedicated machine, there should be exactly two CPUs. One CPU 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.
- CPU speed is not a crucial factor. The Redis CPU remains dormant most of the time. It takes a lot of traffic to increase the CPU to a heavy load. With the current configuration of Redis, by the time the CPU is getting fatigued, the network connection might already be the bottleneck. Pay attention to the network connection between the servers and Redis and between the Redis Servers (if clustered).

If the network connection is fast but you experience bottlenecks, contact the Cherwell Professional Consulting Services team at support@cherwell.com.

Redis Configuration

Redis can be configured to run in single mode or a cluster configuration. 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 slaves. 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).

Connections

Run Redis in standalone, master/slave, or cluster mode. Ideally the minimum configuration is master/slave with sentinels.

For more information on Redis sentinels, refer to Redis Sentinel Documentation.

Sentinels

A sentinel is a component of Redis that keeps an eye on both the master and the slave. It identifies when the master goes down and immediately promotes the slave as the master. Ideally the minimal configuration has two sentinels, one for master and one for slave. When the sentinel switches the master, CSM switches as well if both are listed in Connect to field on the Server Manager.

Master/Slave

A master/slave connection has one copy of the master data kept in a slave. The slave 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 slave copy each other, one is always master and one is slave. If the master goes down, the slave does not know unless there is a sentinel. If the master goes down, it becomes the slave when it comes up again. CSM does not need to know who is master and who is slave, just the nodes for Redis in the chain.

Backup vs. Slave

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/slave 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 errored out and IIS went down. This is why the save directive is not recommended.

Redis Q&A

Question: What if my Redis Server goes down? Is that a single point of failure?

Answer: Yes it is. Fortunately, you can set up Redis with high availability, see Redis Configuration.

Configuration

Question: How many slaves should I have for a master?

Answer: For high availability, have at least three Redis Servers and three sentinels.

Question: How often does Redis fail?

Answer: Our tests have not experienced an unstable Redis. Failures are usually due to hardware problems. Except:

- 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 slaves, 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 slave to master. A single sentinel does not necessarily have the authority to switch a master to a slave, because there might be other sentinels that disagree with it. For the master to actually be swapped with a slave, 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.

Advanced Session Caching and Pinning

> **CAUTION:** Do not attempt to implement these processes if you are not an advanced User. You can cause serious network and system issues. Please contact Cherwell Professional Services for assistance at support@cherwell.com.

In a typical load-balanced scenario, every request that is received from a browser is redirected by the load balancer to a server on the farm. The load balancer chooses the server to assign a request based on its own internal logic, which could be round robin, random, or performance-based. Regardless of the strategy the load balancer uses, the Cherwell Web Server cannot predict what the load balancer will do next. In other words, given one web request served by a particular Cherwell Web Server, the farm can make no assumptions regarding which server is serving the next request from the same User.

With a properly configured load balancer and session caching, we instruct the Cherwell Web Server to assume that the load balancer will keep sending the same User to the same server for a period of time. In other words, instead of continually distributing Users across the farm, once a load balancer sends a User to a server, it will continue to do so for a while (seconds or minutes). People use the term *session pinning/* (also called session affinity or sticky sessions) or *User pinning* to identify this functionality.

Session pinning and session caching are similar terms and work together in the Cherwell Server Farm but are technically different:

- Session pinning, or User pinning, is what the load balancer does in order to redirect Users to the same server for a window of time.
- Session caching is what the Cherwell Web Server needs to do in order to better support session pinning.

Benefits of Session Caching and Session Pinning

Enabling session pinning on a load balancer and session caching on your Cherwell Web Server optimizes your CPU and network.

When the first request comes in for a User, there is no difference between having it on or off. The exception is after the request is made, the system caches sessions in-memory for a configurable amount of time. Beginning with the second request, the process changes because the server assumes it has the latest version of the cache and does not need to retrieve it from Redis, decompress it, and deserialize it. This process results in a lighter CPU and network footprint.

Time Windows with Session Caching and Session Pinning

The purpose of User pinning is to eliminate the network traffic and deserialization effort each time a request is received. As a general rule, session caching and server pinning should have the same timeout value. Set the server pinning window to be the same as your session caching window (for exampe,15 seconds).

Burst caching

Burst caching offers a performance boost while keeping RAM fairly clean by purging state caches every few seconds. A web farm typically receives requests in bursts as the browser loads a page. For example, when presented with a Dashboard, there are a number of requests within a few seconds as the page loads all of its elements and makes all of its data calls, and then no requests until the User clicks. In cases like the example, you might decide to set your session caching for 15 seconds. The server keeps the session in-memory for 15 seconds. Every burst of requests that come in within those 15 seconds requires one single Redis read and deserialization. If the User clicks after 30 seconds they are redirected to a different server. By then the 15-second window has expired and the session is retrieved from Redis by the new server.

Session timeout

The concept of session timeout refers to how long a User can remain inactive without having to log in again. It is a setting in the Cherwell Administration Options. A typical setting is anywhere from 30 minutes to 2 hours.

Performance Impact

As explained above, session caching allows you to drastically reduce the number of reads from Redis, lightening the network traffic by almost 50 percent and removing the need to decompress and deserialize for every request.

You still have to write your session to Redis for every request (in case the server goes down, another server can continue seamlessly), but serializing is a lot cheaper than deserializing.

In the test we conducted, we noticed that for the majority of the pages, as far as User response time is concerned, a Cherwell Server Farm with session caching on will behave just as fast as a single-server scenario. Some write operations can be slower than comparable single-server setups, but the overall User experience is good, with the additional benefits of high availability and scalability.

Session Caching and Session Pinning Q&A

Question: Could I have session pinning without session caching?

Answer: The Cherwell Server Farm will not know that pinning is in place and will not be able to optimize accordingly. Your performance would be the same as if you did not have pinning enabled.

Question: Can I have session caching enabled without session pinning?

Answer: No, it can cause problems and performance issues and split Users across multiple competing servers.

Question: For burst caching, what should I set my server pinning window to be?

Answer: The recommended setting for bursts caching is for it to be ste as long as your session caching window (for example,15 seconds).

Configuration Scenarios

CAUTION: Do not attempt to implement these processes if you are not an advanced User. You can cause serious network and system issues. Please contact Cherwell Professional Services for assistance at support@cherwell.com.

No two Cherwell Server Farms are identical because of the load they are under, the CSM content and configuration, as well as their usage can differ dramatically from Customer to Customer. We offer three examples of configurations. The objective of the sample scenarios is to clarify the options and what variables can be manipulated to adapt your organizational needs. In the examples, we assume that your network, load balancer, and SQL infrastructure are inherently scalable to the size needed. The three example scenarios are:

- Minimal server farm.
- Server farm and independent services.
- Maximum distribution of services.

Design Rules of Thumb

When designing the configuration for the Cherwell Server Farm, remember these rules of thumb:

- 1 CPU core per 50 concurrent Users; minimum of two to start.
- 10 MB of memory per session for Redis Servers; 2 CPU cores per server.
- 50 MB of memory per session for Cherwell Application and Web Servers, plus Redis memory.
- 500 MB of storage per license per year.
- Redis must be deployed in a high-speed, low-latency, directly-connected environment. This is typically a 10 GbE network (dedicated is best).
- 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. Performance and high availability rule of thumb is: three load-balanced servers = a single server.

Hardware Considerations

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. The example scenarios assume each machine in the Cherwell Server Farm is a commodity box.

Cost considerations for Commodity Hardware

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 cheaper 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.

Minimal Scenario

In this scenario, only the application and web servers are load balanced and provide high availability. All other servers are located on one machine. If the machine with multiple servers goes down, remedial action should be taken to bring it online as soon as possible. A minimal configuration has the following characteristics:

- Only the coordinated servers are load balanced.
- All coordinated servers are on individual machines.
- All other servers are on a dedicated machine.
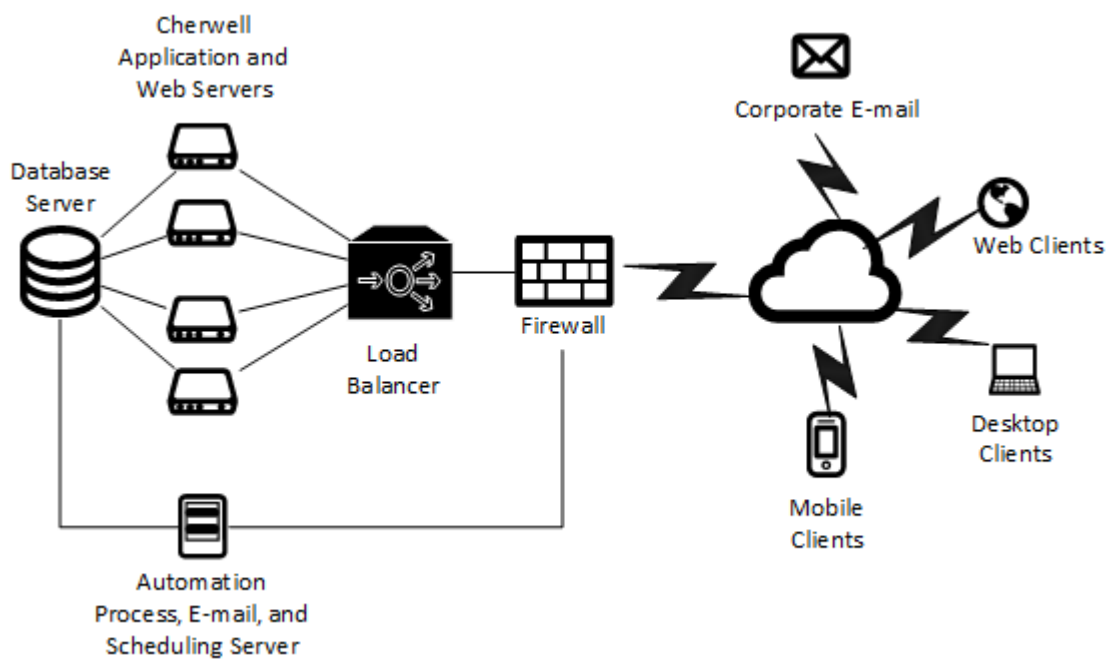
Independent Services Scenario

This scenario is similar to the minimal scenario by having the application and web servers load balanced. The difference is that there are steps taken to provide scalability and higher availability for the other servers:

- More than one instance of all independent servers are on so they can collaborate handling the workload.

- The single-instance servers are all installed in a single machine, but there is a replicated machine that remains offline. Should the first machine go down, the second machine can quickly be brought online to serve Users.
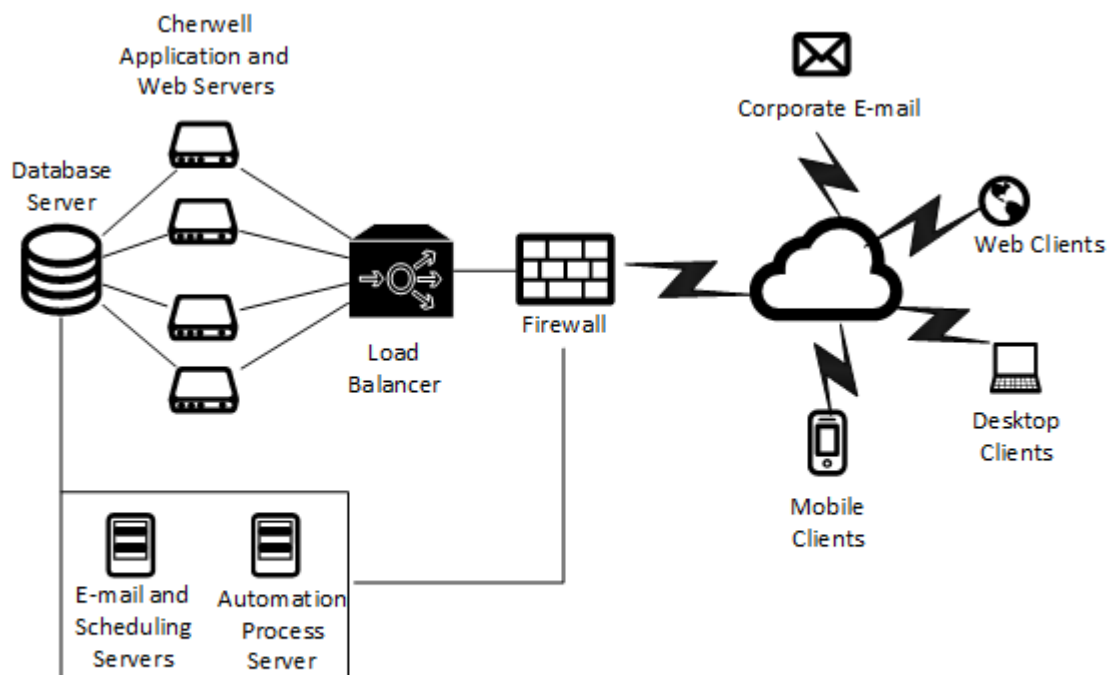
Maximum Distribution of Services Scenario

In the maximum distribution scenario, no single machine has enough performance to be able to run more than one single Cherwell server at the time. Therefore install the servers onto multiple boxes. The main concept remains the same, but there are more machines in the Cherwell Server Farm and one dedicated machine for each server. In the diagram, there are three machines dedicated to the application server and three machines for the web server.
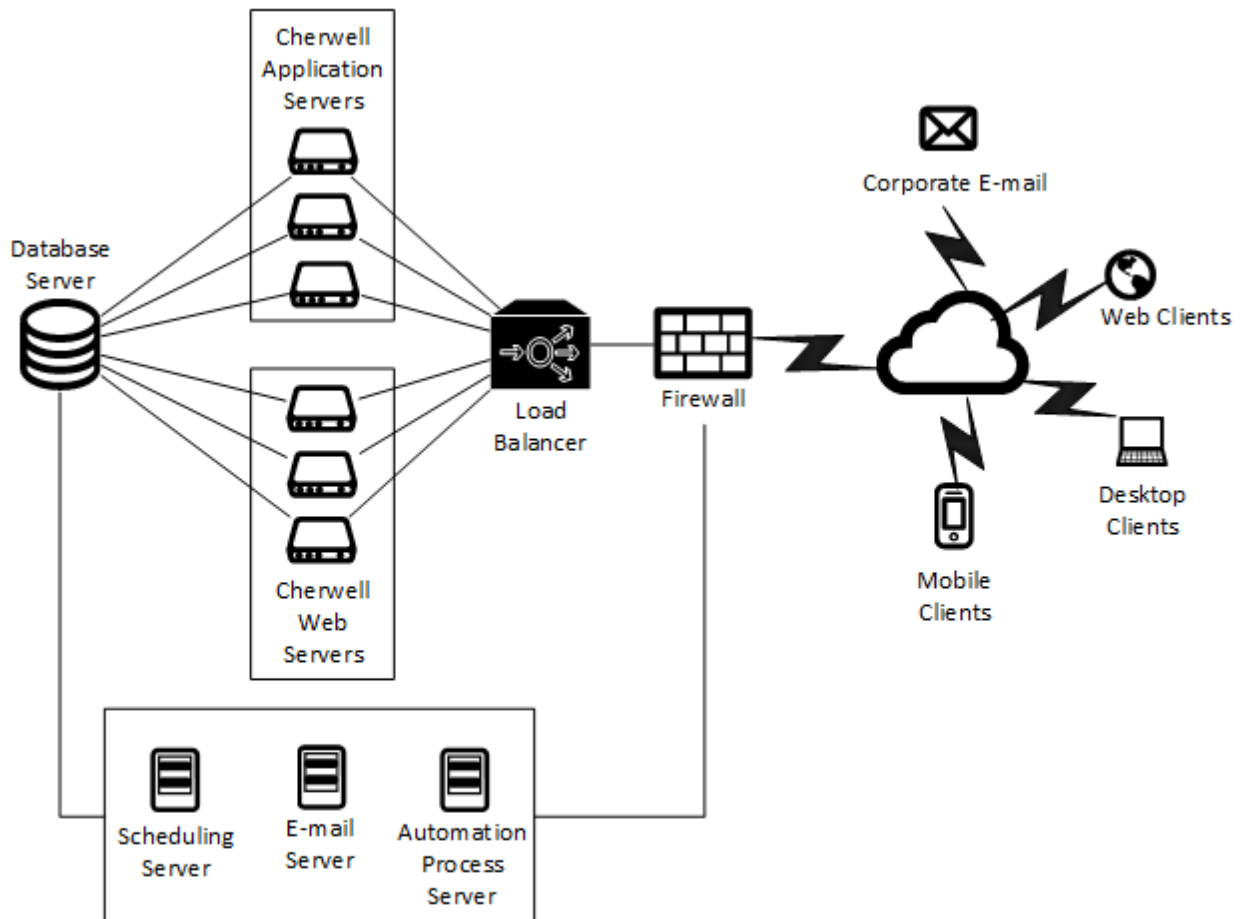
Migration to a Cherwell Server Farm

The migration procedures focus on the Desktop Client and Web Applications because the majority of systems have a primary need of a server farm in order to provide scalability and high availability for those types of clients.

> **CAUTION:** Do not attempt to implement these processes if you are not an advanced User. You can cause serious network and system issues. Please contact Cherwell Professional Services for assistance at support@cherwell.com.

To migrate to a Cherwell Server Farm:

- Establish a baseline
- Calculate the numbers of servers needed
- Incorporate Redis

Establish a Baseline

Start by isolating the web and application servers from all the other servers. Your scheduling or e-mail servers might be using the resources needed to serve the Desktop Client and Web Applications. Create a single-server environment where the web and app server have a dedicated machine and all other services are together in one machine.

Calculate the Number of Servers Needed

To calculate the number of server, have a few data points ready:

- USER_POPULATION: What is your total number of Users?
- CONCURRENT_USER_PEAK: What is the peak number of concurrent Users I want to support?
- USER_LOAD_THRESHOLD: At what point do you start experiencing slowness?
- MACHINE_FAILURE_TOLERANCE: How many machines do I expect could go down at the same time?

Example: You have an environment with three thousands Users, a typical peak usage of one thousand Users, and the system performance starts slowing at around three hundred Users.

Load Balanced Servers Required		
USER_POPULATION	20000	<< How many total Users?
CONCURRENT_USER_PEAK	1000	<< Max number of typical concurrent users?
USER_LOAD_THRESHOLD	300	<< Users that can be supported on a single server, in server farm mode, without slow downs.
MACHINE_FAILURE_TOLERANCE	2	<< How many machines could go down without degradation of service?
Typical PEAK Load		
SINGLE_SERVER_COVERAGE	30%	<< Percent coverage of peak demand of a single server with Server Farm On.
Servers Required Minimum	4	<< How many servers cover 100 percent.
LOAD_BALANCED_SERVERS_REQUIRED	6	<< How many to support typical peak usage with fault tolerance.
	1800	<< Number of concurrent Users supported assuming all servers are operational.
100% Load		
SINGLE_SERVER_COVERAGE	2%	<< Percent coverage of 100 percent demand of a single server with Server Farm On.
Servers Required Minimum	67	<< How many servers cover 100 percent.
LOAD_BALANCED_SERVERS_REQUIRED	69	<< What is required to support 100 percent of Users being online at the same time.

Input Fields >> (label to the left of the Input Fields rows)

Based on the calculations above, you would need six servers to be able to comfortably serve a typical peak User population, but you would need 69 servers to support 100 percent of Users coming online at the same time.

The calculation above does not take into consideration if the Users are Web or Desktop Client Users. There is a possibility that the environment is heavy loaded on one type of client. If this is true, start with a configuration where both application and web servers are distributed across the LOAD_BALANCED_SERVERS_REQUIRED. If that is insufficient, select one of two strategies:

- Add more hardware, keeping web and application servers on the same box. See Minimal Scenario.

- Separate the application and web servers and perform the above calculation for the DIFFERENT load that you expect on each platform. See Maximum Distribution Scenario. At the end there is a number of LOAD_BALANCED_SERVERS_REQUIRED for web and application.

Example: Migrating from large servers to commodity hardware

If the core machine is 8 2.4gHz, and you want to use commodity hardware instead, consider using two 4-core 2.4gHz machines, or three 3-core 1.8ghz machines. The calculation is not perfect science, but the cost saving should allow you to err on the side of caution.

If the original LOAD_BALANCED_SERVERS_REQUIRED is six, consider a multiplier of two or three depending on the commodity hardware you chose to use, for a total of 12 or 18 commodity machines instead of six servers.

Advanced Server Farm QA

The Q&A below contain additional information that can be helpful.

Upgrades

Question: What do I do if an upgrade is needed on a system?

Answer: Certain components of the system can be upgraded without stopping but others require taking everything offline.

Stop the entire farm if:

- Upgrading any Cherwell component.
- Changing configuration elements, especially:
    - Connection to the SQL database.
    - Connection to Redis.
    - Logging.

In the following cases do not stop the entire farm, instead take servers offline one (or more, but not all) at a time:

- Changing hardware
- Adding or removing servers
- Installing virus scan on the system
- Installing windows updates

Configuration

Question: Given a high availability configuration what can go wrong?

Answer: One server in the farm could go down, Redis master could go down, but the server farm remains up and running (provided that there are other web servers running, the Redis master is backed up to a slave, and a sentinel was able to detect the failure of the master). If, as a whole, the load balancer, SQL, or Redis go down, they take down the entire farm, even if the servers in the farm are still running.

Question: How do I know if I have to break up 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 your machine and the performance load you have, a shared machine might not be enough.

Trusted Agents

Trusted Agents is a feature that offers cross-network access between your CSM servers and other private resources, such as LDAP directories and relational databases. This enables CSM to securely access resources on a separate network without a VPN connection or complex firewall configuration.

About Trusted Agents

Trusted Agents can be used to:

- Provide CSM SaaS customers secure access between resources on their private network and the Cherwell data center.
- Enable secure access to private resources across networks in your organization.
- Enable secure access between a Cherwell partner's CSM network and private resources on your network.

When Trusted Agents are enabled, Trusted Agents connect to CSM servers using firewall friendly protocols. The CSM servers then call Trusted Agents to perform operations on behalf of the CSM servers. In the case of SaaS customers, Cherwell IT configures the hosted side (Cherwell servers), and you install and configure one or more Trusted Agents servers on your network to facilitate communications between the Cherwell servers and your private resources.

Note: The Trusted Agents feature requires the presence of one or more Trusted Agents within the same corporate network as the target directory, domain, or database.

Supported Private Resources

Trusted Agents support 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.

For example, CSM has a supported list of LDAP directories. This list of supported LDAP directories is the same whether connecting directly or connecting through a Trusted Agent.

In addition, you can create service groups to control which private resources use Trusted Agents and to route requests to each service group. For more information, refer to Configure Trusted Agents Service Groups.

Private Resource Type	CSM Operations
LDAP Directory	LDAP Authentication. LDAP-mapped user import. LDAP-mapped Business Object import.
Windows Domain	Windows Authentication.
Relational Database	Bulk import of mapped Business Objects. **Note:** Bi-directional and real-time data imports are not supported at this time.

Private Resource Type	CSM Operations
E-mail	**All** e-mail operations within CSM.

Trusted Agents Components

The following table describes the key components that participate in Trusted Agents scenarios.

Component	Definition
Private CSM Network	The network in which CSM servers are running. This network is separate from the network in which one or more Private Resources reside, so Trusted Agents are required for communication 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 Agents Hubs.
Trusted Agent	A software component that acts as a proxy for communication between a Trusted Agents 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 Agents Service.
Trusted Agents 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 Agents Hub at startup, and CSM servers communicate to Trusted Agents by sending requests to the Trusted Agents Hub, which selects the Trusted Agent to receive each request. Trusted Agents Hubs may be scaled out using Redis just as CSM Browser Client can be scaled out.
Trusted Agents Service Group	A configurable set of Trusted Agent Services that can be created in CSM Administrator and selected when configuring Trusted Agent usage for external data sources, LDAP directories, and Windows Domains. Trusted Agents 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.
Trusted Agents Server	The physical or virtual machine that hosts a Trusted Agents Service and is collocated on a private network with the Private Resource(s) that should be accessible to CSM servers. A Trusted Agents Server can host only one Trusted Agents Service, but multiple Trusted Agents Servers can be used to support request routing and fault tolerance.

Component	Definition
Trusted Agents Service	A Windows service that hosts Trusted Agents. Each Trusted Agents Service hosts three Trusted Agents: one for External Data, one for LDAP, and one for Windows Domains.

Configuring Trusted Agents

Trusted Agents configuration requires steps on two networks and potentially multiple servers. Follow the general process shown in the following table.

Step	Configuration Task	Task Location
1.	Install the Trusted Agents Server.	A server on the same network as your private resource.
2.	Configure the Trusted Agents Server.	The same server where you installed the Trusted Agents Server on the same network as your private resource.
3.	Enable the Trusted Agents Hub.	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.
4.	Grant Security rights to control access to Trusted Agent configuration options in CSM Administrator.	From CSM Administrator.
5.	Connect to the Trusted Agents 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 Agents • Scaling Trusted Agents for Request Routing. • Importing Directory Service Data Into Business Objects • Using E-mail	From CSM Administrator.
6.	Create Trusted Agents Service groups. This step is required if you want to route requests to only specific Trusted Agent Services.	From CSM Administrator.

Install the Trusted Agents Service

The Trusted Agents Service is installed on the same network as the private resource to which it connects. For example, if you want to use Trusted Agents for LDAP authentication, install the Trusted Agents Server on the same network as your directory service.

To install the Trusted Agents Service:

1. Go to the **Cherwell Disk Image** folder.
2. Open the **Utilities** folder.
3. Double-click the Cherwell Trusted Agents Server file.

   The User Account Control window opens.

4. Click Yes to continue the installation.

   The Trusted Agents Install Wizard opens.

5. Click Next on the Welcome page.
6. Click the I accept the terms in the license agreement radio button.
7. Click Next.
8. Click Next or click Change to browse to a different location to install.
9. Click Install.

   The status bar shows the install progress.

10. Click Finish.

Configure the Trusted Agents Service

The Trusted Agents Service is installed on a same machine in the same network as your private resources.

To configure the Trusted Agents Service:

1. Go to the installed directory (from the path specified during the installation) to run the Trebuchet.ServerConfigTool.exe. The default path from the install is: C:\Program Files (x86)\Cherwell\Cherwell Trusted Agents Server.
2. Double-click Trebuchet.ServerConfigtool.exe to open the Server Manager.
3. Select **Trusted Agent Server** from the Server drop-down.
4. Click the Configure button to open the Trusted Agent Server Configuration.
5. In the Trusted Agents Service Configuration window:

Option	Description
General Settings: Display name	Provide the name of the service (this appears in the CSM Administrator interface).
Hub Connection	
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 Agents Hub configuration. **Note:** This key is used to ensure that only properly configured Trusted Agents are permitted to connect to the Hub. Any value can be used as long as the same value is used when configuring the Trusted Agents Hub. Each user should have a unique value. We recommend that the key be at least 64 characters in length.
Test	Click to test the connection.
Cherwell Connection	
Connection	Use the Ellipsis button to browse and locate the database to connect to.
Login to Cherwell - Choose one option	
Windows authentication	Use the Windows credentials for the account that is used to run the Trusted Agent Service.

Option	Description
User ID and Password	Provide a CSM User ID and Password.
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.
Test	Click to verify the user and password information.
Advanced Settings	
Hub Ping Frequency	Enter the frequency, in seconds, to send a ping to the hub. If a ping is not received by the hub within the expected Agent Registration timeout, then the Agent's registration with the Hub is considered expired and no further requests are sent to the Agent until the next registration request or ping is received from the Agent. **Note:** Use -1 to indicate that no pings should be sent to the Hub. This is not recommended because pings help ensure that the Trusted Agents Hub has updated availability and registration information for the Trusted Agents Service.

6. Click OK.

7. Restart the Cherwell Trusted Agents Server.

8. Restart IIS.

Configure the Trusted Agents Hub in the Server Manager

The Trusted Agents Hub is configured in the CSM Server Manager on the same machine running the CSM Browser Client.

Note: If you are using a server farm, you must perform this step on each server.

To set up the Trusted Agents Hub:

1. Click Start>All Programs>Cherwell Service Management>Tools>Server Manager to open the Cherwell Server Manager.

   Note: Depending on your operating system, you may need to search for the Server Manager to open it.

2. Click the Configure button next to Trusted Agents usage.
3. In the Trusted Agents Hub Configuration dialog:

Option	Action
General Settings: Enable Trusted Agents	Select the check box.
Hub Connection	
Hub URL	Provide the address that is 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 Agents Server configuration. *Note:* This key is used to ensure that only properly configured Trusted Agents are permitted to connect to the Hub. Any value can be used as long as the same value is used when configuring Trusted Agents Servers. Each Customer should have a unique value. We recommend that the key be at least 64 characters in length.
Test	Click to test the connection. *Note:* You must restart IIS after this field is updated to view the changes.

Option	Action
Advanced Settings	
Agent Operation Timeout	The amount of time the Trusted Agents Hub waits for an operation to complete, send data back, or how long an operation takes to send a progress update before timing out. **Note:** Use -1 to disable timeouts.
Agent Registration Timeout	The amount of time the Trusted Agents Hub waits for a ping from the Trusted Agent before it assumes the Trusted Agent is down.

4. Click OK.

5. Restart all Cherwell services and IIS.

Connect to the Trusted Agents Hub from CSM Administrator

To access Trusted Agents configuration settings in CSM Administrator, you must first connect to the Trusted Agents Hub.

Trusted Agents must be configured before you can connect to the Trusted Agents Hub from CSM Administrator.

1. In CSM Administrator, click 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 Agents Hub.

   The Shared Key used by the Trusted Agents Server and the Trusted Agents Hub.
3. Click Test to verify that you can connect to the Trusted Agents Hub.

Configure Trusted Agents Service Groups

Trusted Agent service groups are a configurable set of Trusted Agent Services that are created in CSM Administrator and selected when you configure Trusted Agents for external data sources, LDAP directories, and Windows Domains.

Trusted Agents service 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.

For more information on using Trusted Agent service groups, refer to:

- Scaling Trusted Agents for Request Routing
- Import External Data Using Trusted Agents

To configure the Trusted Agents service groups, you must:

1. Configure Trusted Agents.
2. Connect to the Trusted Agents Hub from CSM Administrator

To add Trusted Agents service groups:

1. In CSM Administrator, click the Trusted Agents category, and then the Edit Trusted Agents service groups task.
   The Trusted Agents dialog opens. If Trusted Agents is correctly configured and running, all Trusted Agents Services appear under the All Agent Services node.
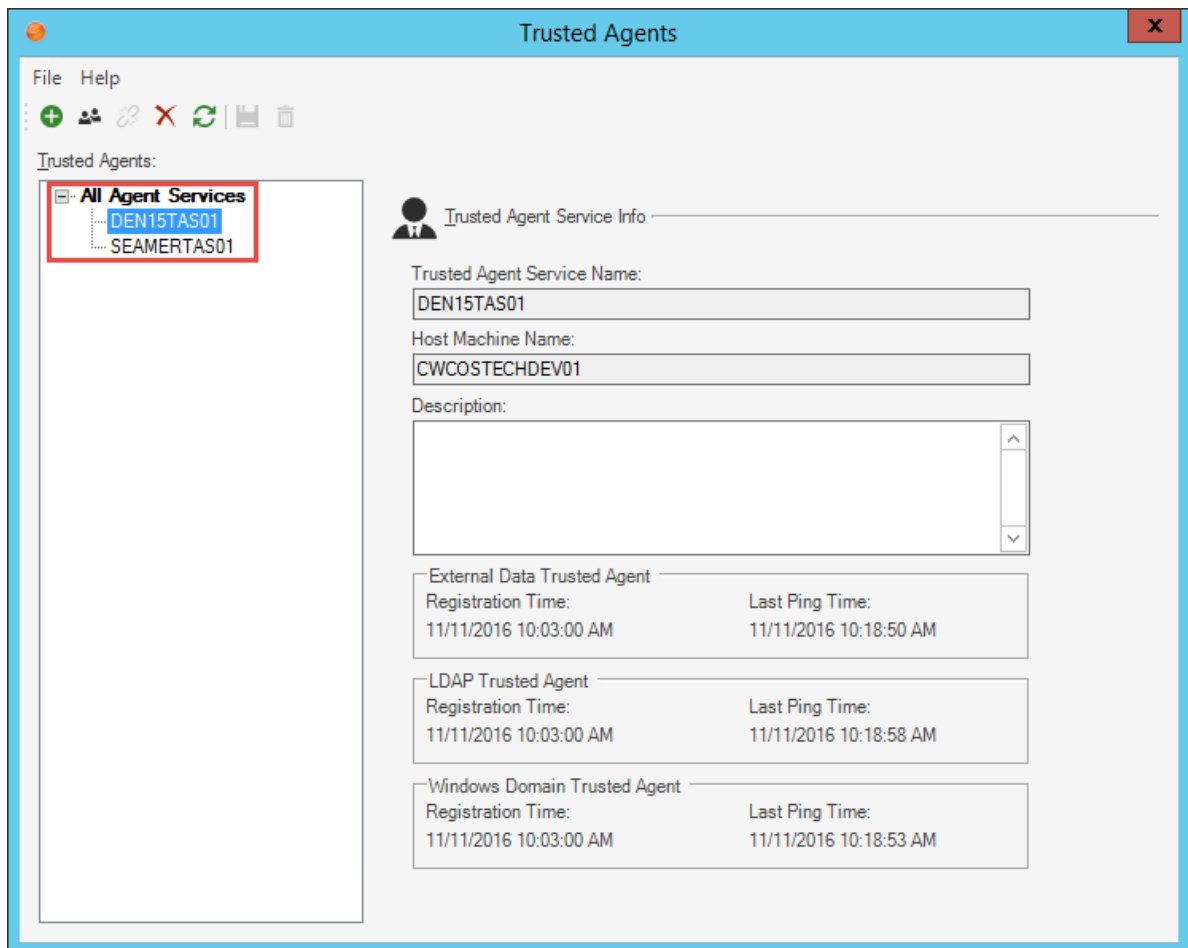
> **Note:** Trusted Agents Services are shown when they are successfully connected to the Trusted Agents Hub. If no Trusted Agents Services are present in this dialog, connect your services to the Trusted Agents Hub first, and then use this dialog to configure your services and groups.

2. Click the Create icon.

3. In the Trusted Agent Group Info section, provide a Name and Description for the service group.

4. Click 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 click the Add trusted agent service to group ![icon] icon.

7. Select a Trusted Agent Service to assign to the service group.

8. Click OK.

9. Assign a Trusted Agents Service to each service group, as shown in the following example.

Configuring Trusted Agents Features

The following topics describe how to use Trusted Agent with CSM features.

Using Trusted Agents Server with LDAP

You can use your LDAP connection with Trusted Agents to:

- Authenticate Users.
- Import Directory Service Users.
- Import Directory Service Data into Business Objects.

Before enabling LDAP for Trusted Agents, you must first configure Trusted Agents.

To enable LDAP for Trusted Agents:

1. Verify that CSM is configured for LDAP:
   In CSM Administration, click the Security category and then click 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 based on the information in Configuring CSM Directory Services Settings.

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 Agents 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. This setting is not required for Trusted Agents, but it may complement its use by reducing round trips between the CSM Administrator and LDAP directories for activities initiated within CSM Administrator. This setting does not impact LDAP interactions that are initiated by Cherwell servers in the SaaS environment.

7. Click OK.

Using Trusted Agents Server with Windows Domains

Trusted Agents for Windows domains do 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 Agents.

Note: LDAP directory configuration is not required when using Windows.

Before enabling Windows domains for Trusted Agents, you must first configure Trusted Agents.

To enable Windows domains for Trusted Agents:

1. Verify that CSM is configured for Windows domains:
   In CSM Administration, click the Security category and then click 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. Add or edit a Windows Domain connection, and then verify that the Windows Domain settings are applied.

2. On the Windows Domain Settings dialog, select the Trusted Agents page.

3. Select the Use Trusted Agents check box.

   Note: If you want to disable Trusted Agents 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. Click OK.

Import External Data Using Trusted Agents

To import external data using Trusted Agents, you must first:

1. Configure Trusted Agents.
2. Connect to the Trusted Agents Hub from CSM Administrator
3. Optionally, configure Trusted Agents service groups.

🖊 **Note:** You can import data using Trusted Agents, but you cannot link data. In additional, data imports are not bi-directional and real-time updates are not support at this time.

To import external data using Trusted Agents:

1. Open or create a Blueprint.
2. Select an existing Business Object or create a new Business Object.
3. Go to Managers>External Connections.
   Trusted Agents are compatible with any connections available in CSM.
4. Click Create New.
5. Click Next on the Welcome page.
6. On the Login options page, select the Use Trusted Agents checkbox, 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. For more information, see Create an External Connection.
8. Map to a Business Object or create a new external Business Object.
   For additional information, see Map an Existing Business Object to Import External Data.

   🖊 **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 Agents.

9. Click the Database category, and then click the Import Data task.
10. Complete the steps in the External Data Import Wizard. For additional information, see Import External Data into an External Business Object.

Using Trusted Agents with E-Mail

To use Trusted Agents with e-mail, you must first:

1. Configure Trusted Agents.
2. Connect to the Trusted Agents Hub from CSM Administrator.
3. Optionally, configure Trusted Agents service groups.

Note: Using Trusted Agents with e-mail will increase e-mail processing time.

To configure an e-mail account to use Trusted Agents:

1. In CSM Administrator, select the E-Mail and Event Monitoring category.
2. Select the Edit e-mail accounts and settings task.
3. Select the e-mail account you wish to configure and click the Edit... button.
4. In the E-Mail Options page, 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 e-mail requests.

Note: When using Trusted Agents, outgoing e-mail messages will always be sent from the Server, not the Client. This setting (viewable in the From Settings page) will be changed automatically.

Scaling Out the Trusted Agents Service

While a single Trusted Agents Service can be used to provide access to one or more Private Resources in a single private network, additional Trusted Agents Services may be used for:

- Fault Tolerance
- Request Routing

Scaling Trusted Agents for Fault Tolerance

More than one Trusted Agents Service can be provisioned within a single private network to allow for increased redundancy of communication with Private Resources. If one Trusted Agents Service goes down or is otherwise unavailable, additional Trusted Agents Service(s) can facilitate communications with the same Private Resources.

The Trusted Agents 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 Agents on a single private network, install and configure more than one Trusted Agents Service on that private network, and configure each to use the same Trusted Agents Hub URL and Shared Key. No further configuration is required. There is no enforced limit on the number of Trusted Agents Services that can be provisioned and connected to a single Hub.

Scaling Trusted Agents for Request Routing

You can use Trusted Agents Groups to allow request routing to specific groups of Trusted Agents Services, whether in the same or different private networks. If Private Resources reside in multiple private networks, Trusted Agents Services may be provisioned in each of those private networks to allow communication with those Private Resources. Trusted Agents Groups may be used to route requests to the appropriate Trusted Agents 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 AD trust between them, authentication requests may be more efficient if "Denver" domain requests are routed to Denver AD domain controllers and "Seattle" authentication requests are routed to "Seattle" AD domain controllers. Routing of requests in this way can be accomplished using Trusted Agents Service scale-out. The diagram below shows how this scale-out might occur.
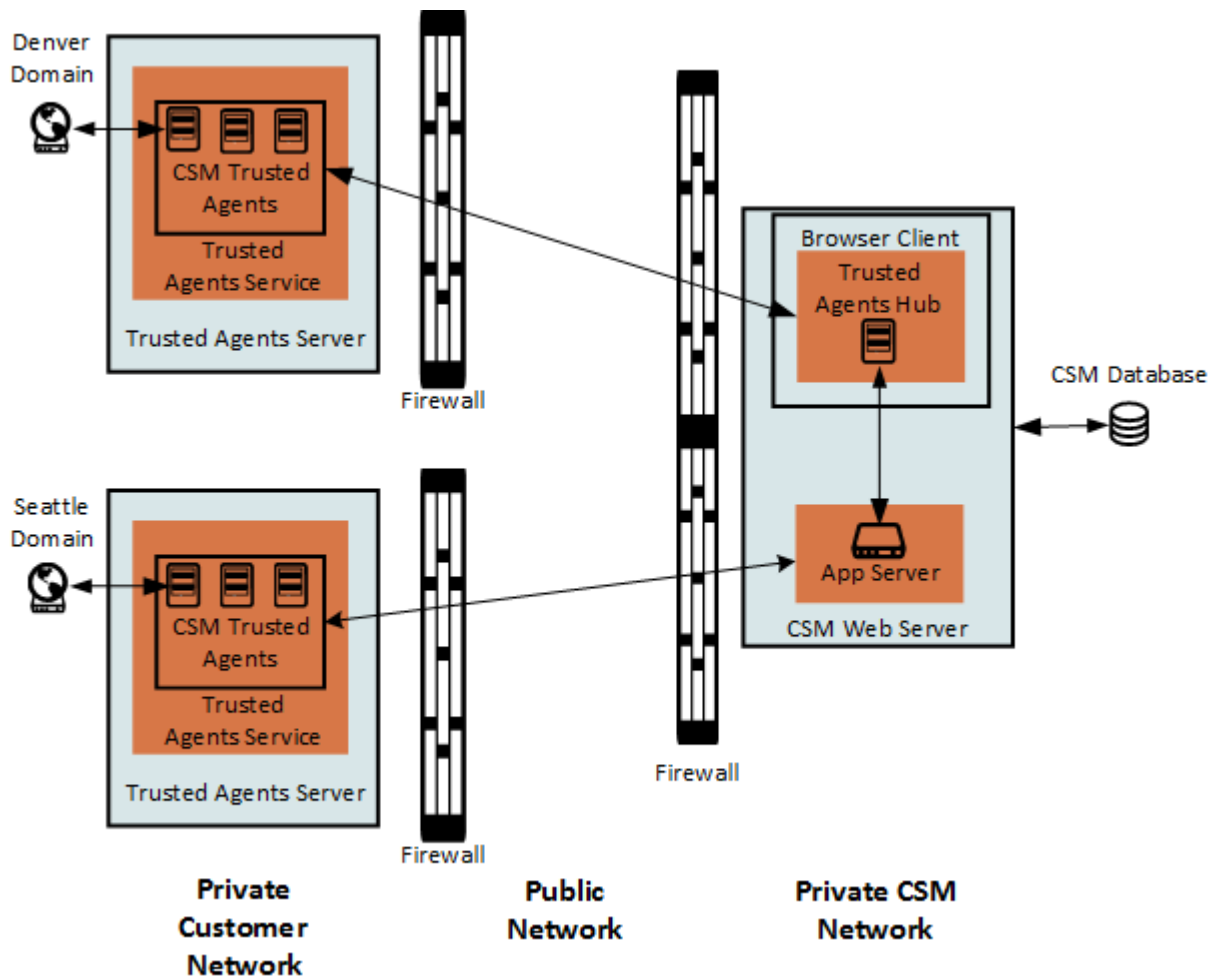
Configuring Trusted Agents for Request Routing

Before you configure request routing, you must:

1. Configure Trusted Agents.
2. Connect to the Trusted Agents Hub from CSM Administrator
3. Configure Trusted Agents service groups.

To configure the Trusted Agents Service scale-out for request routing:

1. Configure service groups as described in Configure Trusted Agents Service Groups.
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. Click the Trusted Agents page.
   Verify that the requests are routed to the correct Trusted Agents group. For example, Denver domain requests can be routed to the Denver Trusted Agents group by selecting that group when configuring the Denver LDAP settings.
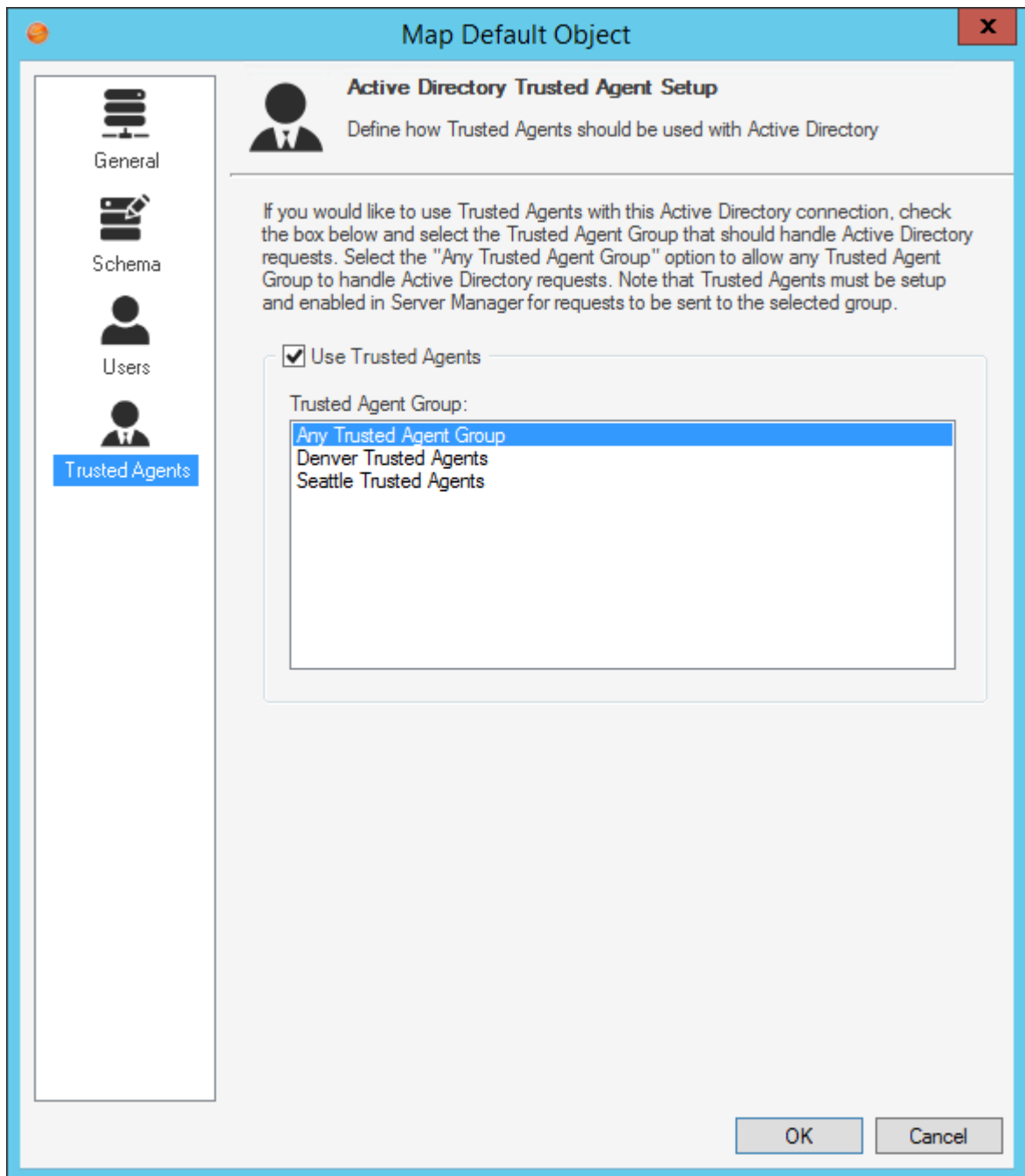
Trusted Agents Server Technical Architecture

Installation configurations vary; however, a typical installation is called a single-server installation where the Cherwell Application Server and supporting servers (services) are installed on one machine.

The diagram below provides an example of one possible Trusted Agents configuration. While other deployment architectures are possible, this diagram provides a simple visual representation of the relationship between the components.
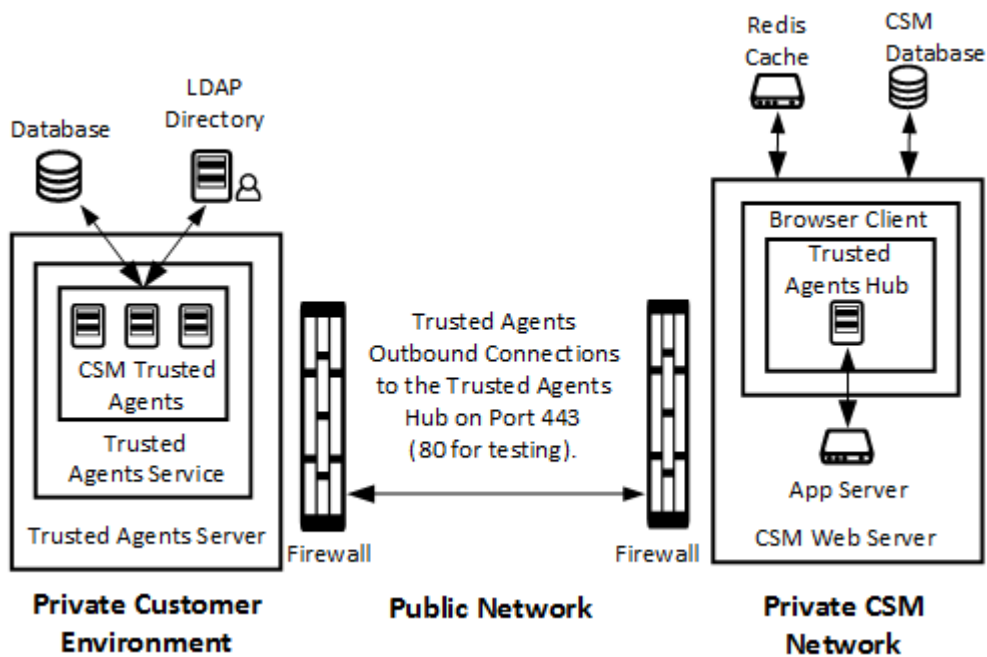
Communication Between Trusted Agents and Private Resources

The connections between Trusted Agents 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 Agents 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 Agents 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 Agents connect to and interact with Private Resources is exactly the same as 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 Agents simply provide 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 Agents first, when possible. Then, when the connection is working properly, you can update the connection settings to indicate that Trusted Agents should be used.

Communication Between Trusted Agents and the Trusted Agents Hub

Unlike connections to Private Resources, the connection between a Trusted Agent and a Trusted Agents Hub is established when the Trusted Agent is started and is maintained until the Trusted Agent is stopped, the Trusted Agents 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 Agents Hub until the Trusted Agent is stopped.

This long-lived and resilient connection is established to ensure a Trusted Agents Hub can send requests to Trusted Agents as needed. Since Trusted Agents reside inside a private network that is different than the network of the Trusted Agents Hub, a Trusted Agents 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 Agents 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 web application, which hosts the Trusted Agents Hub. The port number is dependent on the protocol specified for the Trusted Agents Hub URL when the Trusted Agents Service is configured in Cherwell Server Manager.

🖉 **Note:** Production environments should always use HTTPS (TLS/SSL) for the connection between Trusted Agents and Trusted Agents Hubs to protect sensitive authentication information and business object data.

Trusted Agents use a technology called SignalR to establish a persistent, bi-directional connection with a Trusted Agents 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 Agents 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 Agents 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

Communication Used for Bulk External Data Imports

When you use Trusted Agents to perform a bulk external data import, a Trusted Agent establishes a connection to the CSM Application Server similar to how CSM Administrator or the CSM Desktop Client establish a 3-tier connection to the Application Server. The settings for this Application Server connection are configured using the Trusted Agent Server Settings dialog in Cherwell Server Manager.

The connection from the Trusted Agent to the 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 choose the 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 CSM Application Server, create an External Connection that uses Trusted Agents, maps data from the External Connection to a CSM Business Object, and initiates an import of external data into that Business Object.
2	The CSM Application Server recognizes that the External Connection is configured to use Trusted Agents and that Trusted Agents are enabled in Server Manager. The Application Server sends a request to the Trusted Agents Hub to import external data through a Trusted Agent.
3	The Trusted Agents Hub attempts to find an active Trusted Agent that is configured to handle external data import requests (i.e., a Trusted Agent for External Data). If the External Connection indicates that only agents in a specific Trusted Agents Group should be used to process the request, the Trusted Agents Hub further restricts the selection process to only include Trusted Agents in that group. When a Trusted Agent is selected, the Trusted Agents 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 CSM 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 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.
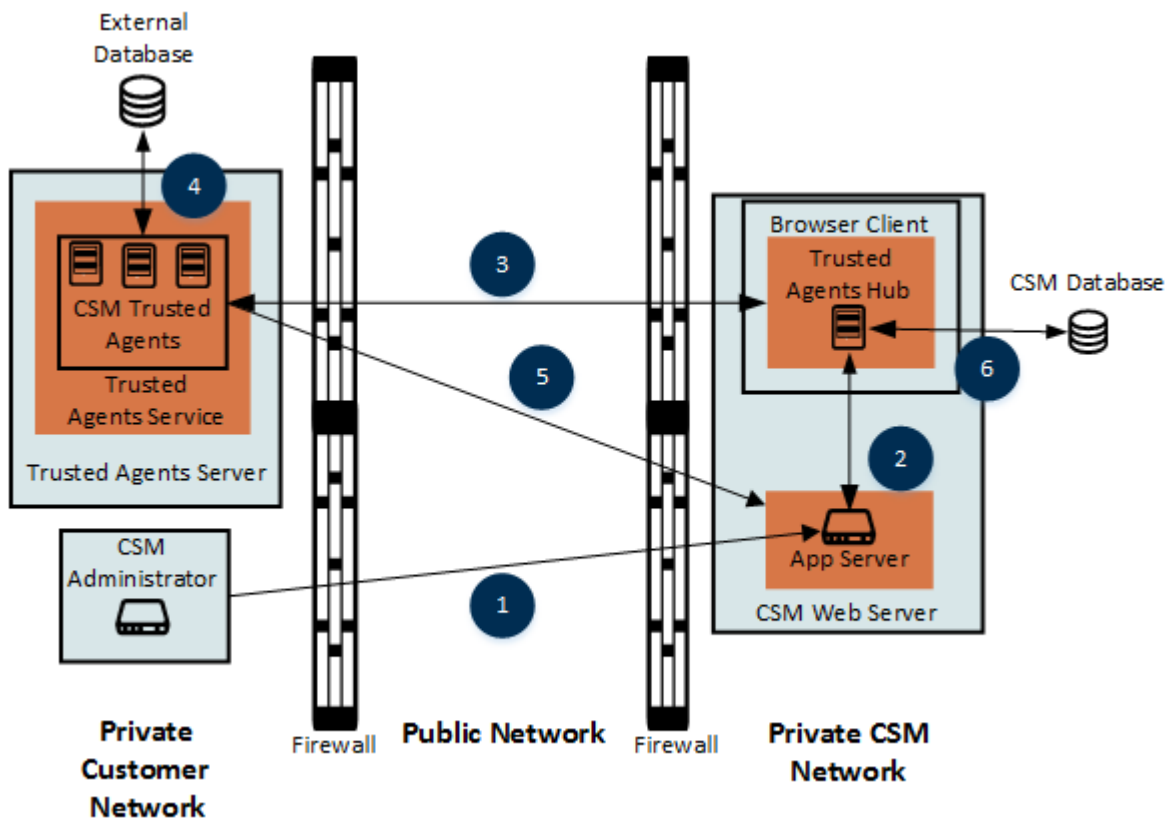
Trusted Agents Network Communication

Each Trusted Agent establishes its own connections to both the Trusted Agent Hub and to the Private Resources it accesses. Trusted Agents may also communicate with the CSM Application Server for some operations, including bulk data import.

Trusted Agents Status

When started, each Trusted Agent registers itself with the Trusted Agents Hub and begins to send "ping" requests to the Trusted Agents Hub regularly to confirm to the Trusted Agents 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 Agents Service log and the Trusted Agents Hub log if Debug level logging is enabled.

Additionally, CSM Administrator provides Trusted Agent registration and last ping time information.

Trusted Agents Logging

Use the Server Manager to configure logging for Trusted Agents. Extensive and detailed logging is available for Trusted Agents connectivity and operations, including activities that occur on CSM servers, Trusted Agents Hubs, and Trusted Agents. The logging information gathered is extremely helpful when troubleshooting 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.

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 log data can be indexed and made easily searchable. Download and install Splunk onto a server and configure it for logging events. For more information on integrating Splunk and CSM, see Splunk Integration and the Splunk documentation.

The logging information collected is determined by the service/server with logging enabled.

Detailed logging information for:	Then enable logging for:
Trusted Agents Hub	Browser Client **Warning:** • When using file logging, the log file must be writable by the IIS application pool in which the Browser Client is running. • When using file logging, 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.
Trusted Agents	Trusted Agents Service
Initiation of Trusted Agents operations from CSM Servers	Application or Scheduling server

When configuring event logging, designate:

Log to	Option description
Event log	Log level: • Debug and above: Very verbose messages. Leaving this on continuously is space and resource intensive. • Stats and above: Detailed messages that track performance. • Info and above: Informational messages that can be used to diagnose a problem with your Server. **Note:** To see e-mail success and failure messages, choose Info and above or Debug and above. • Warning and above: Warning messages that occurred while the Server was running. • Error and above: Errors that were encountered while the Server was running. • Fatal only: Errors that were encountered while the Server was running that caused the Server to stop. **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. **Note:**
File	• Log Level: Select an event classification as described above (example: Debug and above, Info and above, etc.) • File Name: Click 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.

Configure Logging for Trusted Agents

To configure logging for Trusted Agents:

1. Click Start>All Programs>Cherwell Service Management>Tools>Server Manager to open the Cherwell Server Manager.

   Note: Depending on your operating system, you may need to search for the Server Manager to open it.

2. From the Server drop-down, select a Trusted Agents Server.

3. Click the Logging button.

To select one or more options for where to log Trusted Agents events:

   Note: For option details, see Trusted Agents Logging.

1. Log to event log: Select this check box to log events, and then select which events to log.

2. Log to file: Select this check box to write the logs to a specific file and location. Then, set your file limits.

3. Log to Splunk: Select this check box to write the logs to a Splunk server, and then configure Splunk logging.

4. Click OK.

Trusted Agents Troubleshooting

This section outlines some issues that could possibly arise while using Trusted Agents and how to rectify these issues. If you have an issue that is not listed below, contact Cherwell Support for assistance.

Trusted Agents Operations Are Failing

If Trusted Agents 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 Agents Logging for more information.

Verifying that a Trusted Agents Hub is Operational

A Trusted Agents Hub runs within the context of a CSM Browser Client web application. When enabled and operational, a Trusted Agents Hub will respond at a well-known relative URL within the Browser Client web site. This relative URL is "/SignalR/Hubs". For example, if your Browser Client web application is accessible at https://www.example.com/CherwellClient, then the Trusted Agents Hub would be accessible at URL:

https://www.example.com/CherwellClient/SignalR/Hubs

If Trusted Agents usage is enabled using Cherwell Server Manager on a machine that is hosting the Browser Client web application, this URL will respond with a JavaScript file that begins with content similar to the example below:

```
/*!
 * ASP.NET SignalR JavaScript Library v2.2.0
 * http://signalr.net/
 *
 * Copyright Microsoft Open Technologies, Inc. All rights reserved.
 * Licensed under the Apache 2.0
 * https://github.com/SignalR/SignalR/blob/master/LICENSE.md
 *
 */
```

If you do not receive this file when you access this URL, the Trusted Agents Hub is not operational. The most likely causes are: Trusted Agents usage is not enabled in Cherwell Server Manager, or Internet Information Services (IIS) or the Browser Client web application needs to be restarted after enabling Trusted Agents usage.

Trusted Agents are Not Connecting to the Trusted Agents Hub

The following are common causes for a Trusted Agent failing to connect to a Trusted Agents Hub. If addressing these causes does not resolve the connection issue, enable Debug level logging to determine more information about the cause of the problem.

- The Trusted Agents Hub is not enabled and operational. See Verifying that a Trusted Agents Hub is Operational for information about ensuring the Hub is operational.
- The network connection between the Trusted Agent and Trusted Agents Hub is experiencing a problem. Ensure that you can connect to the Browser Client web application from the machine that is hosting the Trusted Agents Service.
- A firewall is preventing outbound communication from a Trusted Agent to the Trusted Agents Hub on port 443 (if using HTTPS) or port 80 (if not using HTTPS). Note that HTTPS should be used for all production Trusted Agents deployments.
- The URL specified for the Trusted Agents Hub is not valid or does not point to the CSM Browser Client web application.
- The Shared Key specified for the Trusted Agent Service in Cherwell Server Manager on the Trusted Agents Server does not match the Shared Key specified when configuring the Trusted Agents Hub using Cherwell Server Manager on the Cherwell web server.

LDAP Authentication through a Trusted Agent is Not Working

The most common cause of LDAP authentication problems is LDAP misconfiguration due to the number and variety of LDAP directory types and LDAP settings. For LDAP authentication, Trusted Agents simply relay authentication requests from CSM servers and then use the same LDAP configuration settings that are specified in CSM Administrator.

If LDAP authentication is not working through Trusted Agents, attempt to verify the LDAP settings by running CSM Administrator on the same network as the LDAP directory and enabling "Client-side LDAP" so that LDAP queries are executed directly by CSM Administrator rather than sending them to the CSM Application Server for execution. After verifying the LDAP settings work correctly when on the same network as the LDAP directory, you can then enable Trusted Agents usage.

Authentication Requests are Not Being Routed to Trusted Agents

Authentication requests are only sent to Trusted Agents if those requests originate from or are being processed by a CSM server, such as the CSM Application Server, CSM Scheduling Server, or CSM Browser Client web application. As a result, requests that originate on a CSM client, such as CSM Administrator, are only sent through a Trusted Agent if that CSM client has a 3-tier connection to a CSM Application Server and the request is processed by the CSM Application Server.

Other reasons why requests may not be sent through a Trusted Agent include the following:

- Trusted Agent usage has not been enabled on the CSM server(s) using Cherwell Server Manager.
- There are no Trusted Agents available to process the request. This situation is noted in a Debug log by the Trusted Agents Hub.

CommunicationException When Importing a Large Number of Records

When attempting to import a large number of records from an external database through a Trusted Agent, the following error may occur depending on the configuration of the Maximum Message Size for the CSM Application Server:

```
System.ServiceModel.CommunicationException: The maximum message size

      quota for incoming messages (50000000) has been exceeded. To increas
e the

      quota, use the MaxReceivedMessageSize property on the appropriate bin
ding

      element.
```

If this error occurs, you can increase the Maximum Message Size in Server Manager to accommodate larger messages. Start by selecting Application Server and then click the Configure… button. In the Server Configuration dialog, select the Advanced tab. The maximum value is 2147483647.

Server Configuration

Connections | **Advanced**

Connection Limits

Maximum TCP Connections: `2000`

Maximum Concurrent Calls: `5000`

Maximum Concurrent Instances: `2000`

Maximum Concurrent Sessions: `2000`

Allowed Connection Backlog: `20`

Payload Limits

Maximum Buffer Pool Size: `5000000`

Maximum Message Size: `50000000`

Maximum Message Depth: `100`

Maximum Message Table Count: `163840`

Maximum Content Length: `2147483647`

Maximum Array Length: `2147483647`

Other

☑ Enable Message Compression
☑ Enable Service Performance Counters
☐ Enable Rest for HTTP

Actions

`Restore Default Values`

`OK`   `Cancel`

Trusted Agent Server Not Processing Inbound/ Outbound E-Mail

If the Trusted Agent server is not processing outbound email, restart the Trusted Agent server. If inbound e-mail is not being processed, restart both the Trusted Agent server and the E-mail Monitor server (in that order).

Globalization

You can use Globalization tools to translate text, referred to as "strings," into one or more single-byte languages. This ensures that Users can use a single CSM installation to view the same data in multiple languages.

You can translate strings for all content, for specific Business Objects and their associations, Lookup Table data, Portal content strings, and Portal resource strings.

About Globalization

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-Steps, and Expressions. This method is recommended for maintaining an existing translation.

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. The language determines the strings presented to Users, while the locale determines date/time formats, currency values, etc. Cultures can be set globally and assigned to Roles and to individual Users.

  See Configure Security for Cultures.

  - **Primary Culture**
    The primary culture is the culture used by the majority of a CSM system. In most cases, the culture is based on the language used when you installed or upgraded CSM.

  - **Preferred Culture**
    Refers to the first 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.

  - **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 Search Group.

  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 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 set of Language Packs based on existing languages in your system when you create a Language Pack.

String Types

Each CSM system includes these types of strings

String Type	Description	Can Be Translated?
Content	Strings for Business Objects, Forms, Dashboards, Expressions, One-Steps, etc. This includes OOTB content and customer-created content.	Yes
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.	Yes
Portal Platform	Portal-based resource strings for toolbars, menus, errors, and more.	Yes
Portal Content	Portal-based strings for User-defined header and footer, menus, toolbars, and more.	Yes
Platform	Typically client-based strings, such as those for menu items, toolbars, controls, and tooltips. Platform strings are provided for English, German, French, Spanish, and Brazilian Portuguese.	No

To translate various string types, select the scope when you create a Language Pack.

Fall-back 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.

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

The Globalization Process

Follow this general process to translate strings.

Task	Notes
1. Enable Globalization features for your system.	See Enable Globalization.
2. Populate your system with cultures.	See Manage Cultures.
3. Define security by assigning cultures to Roles or to Users.	See Configure Security for Cultures.
4. Create Language Packs.	See Create a Language Pack.
5. 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-Steps, and Expressions. This method is recommended for maintaining an existing translation.
6. Apply Language Packs to your system.	See Apply a Language Pack.

Task	Notes
7. 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.
8. Verify that your Portal strings have been translated and add the Language Selector to each Portal Site.	See Translating Strings for Portal Sites.
9. Enable cultures so that translations are visible to Users.	See Enable and Disable Cultures.

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
- E-mail addresses
- Date formats
- True/false values, unless they appear in a sentence string
- The word "System," unless it appears in a sentence string

mApps Compatibility

Due to changes made to support Globalization, the following guidelines apply to mApps:

- mApps created using CSM 9.2.0 or later cannot be applied to an earlier version of CSM.
- When you apply a mApp to that was created on a version earlier than CSM 9.2.0, you are prompted to select a target culture for the mApp. You must perform this task even if Globalization is not enabled for your system.

Globalization and Cherwell Mobile

Globalization support is currently not available for Cherwell Mobile for iOS or Cherwell Mobile for Android.

Strings and User's Operating System

A User's Culture determines which language is presented to that User. There are exceptions where strings are determined by the User's Operating System, however. For example, calendar strings on the Business Hours dialog and some date/time values, such as month and day names, are determined by a User's Operating System.

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.) If this occurs, you can manually edit values in the Data Editor to reflect values for your primary culture.

Configuring Globalization

The following sections explain how to configure globalization for your system and perform globalization tasks.

Enable Globalization

You must enable Globalization for your system before you can use most of its features. For example, you must enable Globalization before you can:

- Assign cultures to Roles and specific User accounts.
- Use the culture selector to change cultures.
- Configure localization support for Lookup Tables.

To enable Globalization:

1. In the CSM Administrator Main Window, select the Globalization category, and then select Globalization Settings.
2. On the General tab of the Globalization Management page, select the Enable Globalization check box.

    Note: The Primary Culture for your system is shown on this page. This is the culture used in the majority of your CSM system.

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 your database and the changes are automatically published.

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. Click the Plus sign to the right of the drop-down.
   The Add Culture dialog opens, and the Cultures drop-down contains cultures you can add to your system.
4. Select the culture to add to your system.
5. Click OK.

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 Fall-back Mechanism

Delete Cultures

When you delete a culture, the definitions are removed from the database and the changes are automatically published.

The Primary Culture cannot be deleted or removed from the list of cultures.

To delete a culture, select it in the list, and then click the Delete icon.

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.

Update Foreign Keys for Validated Fields

You can easily update foreign keys for Fields that are validated from tables to ensure that Users see correct values after they have been translated and that existing records are updated with the foreign keys. Updates also apply to values that are auto-populated from a Field that has foreign key storage enabled.

See Storing Foreign Keys for Validated and Auto-populated Fields.

To update foreign keys for validated Fields:

1. In the CSM Administrator Main Window, select the Globalization category, and then select Update Business Object Validation Foreign Keys.

   The Update Foreign Keys dialog opens.

2. Select one of these options:
   Update all Business Objects

   Select this option to update foreign keys for validated and auto-populated Fields in all Business Objects.

   Update a Business Object

   Select this option to update foreign keys for validated and auto-populated Fields in a single Business Object, and then select the Business Object from the list.

3. Select the Overwrite Existing Values check box to replace values for the Field.

4. Click OK.

Configure Localization Support for Lookup Tables

Use the following process to enable localization support for Lookup Tables:

1. Verify that Globalization is enabled for your system.
2. Verify that you have multiple cultures enabled for your system.
3. Review the information about current culture Fields and specific culture Fields. See About Globalization and Lookup Tables.
4. Enable localization support for Lookup Tables. See Enable Localization Support for a Lookup Table.
5. Use the Data Editor to translate values for culture-specific Fields. See Translating Values for Culture-Specific Fields.
6. Publish your Blueprint.
7. Optionally, set and update foreign key values to ensure that Lookup Table values is updated in existing records in your system. See Update Foreign Keys for Validated Fields.
8. Verify security settings for Lookup Tables. See Configure the Default Domain, Anonymous Login, and Lookup Table Security Settings.

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 and Update Foreign Keys for Validated 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.

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 primary 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.
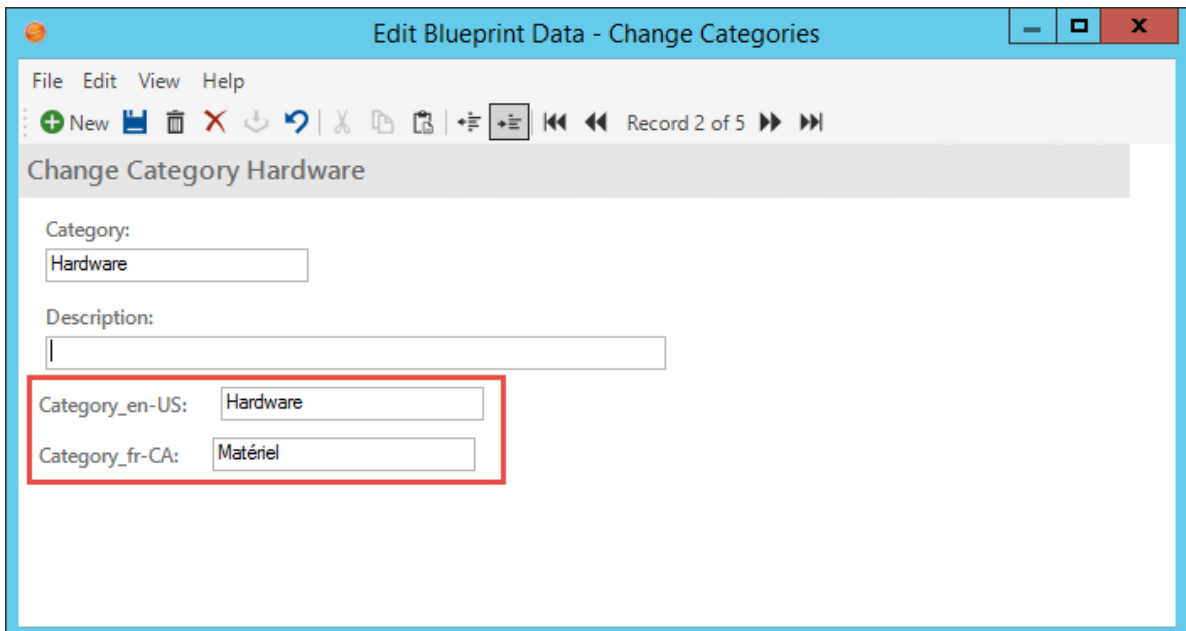
Translating Values for Culture-Specific Fields

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.

Adding Cultures After Lookup Tables Are Configured

When you add cultures after you have enabled localization support for a Lookup Table, you must follow these steps to ensure that values are available for the new culture.

To add cultures to configured Lookup Tables:

1. Add cultures to your system.
2. Create a Blueprint.
3. From the Object Manager, select a Lookup Table that is configured for localization.
4. From the Tasks pane, click Manage culture fields.
5. On the Manage the culture-specific fields dialog, select these options:

Option	Selection
Copy the neutral-culture field values to specific culture fields	Select
Select the culture that the neutral-culture field's values is currently in	Typically, you select your primary culture.
Overwrite existing culture-specific field values	Clear
Copy the neutral-culture value to all the culture-specific fields	Clear
Open the Data Editor	Select if you want to manually translate values for the new culture. Alternatively, you can apply a Language Pack that has translated values after you publish your Blueprint. Be sure to select the Only update strings without translations option in the Apply Language Pack Wizard.
Add culture-specific fields to the default Form and Grid	Select
Purge orphaned culture-specific fields	Clear

6. Click OK.
7. Publish your 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.

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

Setting Global Cultures

The cultures you set globally are applied to all Users and Roles, unless you explicitly override the global settings.

By default, the preferred culture is used.

To set cultures at a global level:

1. Verify that globalization is enabled for your system.
2. In the CSM Administrator main window, click the Settings category, and then click the Edit System Settings task.
3. Select the Globalization page.
4. 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.

5. Click OK.

Setting Cultures for Roles

You can specify cultures for specific Roles. These settings override culture settings made at the global level.

By default, the global setting is used.

To set cultures at the Role level:

1. Verify that globalization is enabled for your system.
2. In the CSM Administrator main window, click the Security category, and then click the Edit Roles task.
3. 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.

4. Click OK.

Setting Cultures for Users

You can specify cultures for specific Users. These settings 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. Verify that globalization is enabled for your system.
2. In the CSM Administrator main window, click the Security category, and then click the Edit Users task.
3. 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.

4. Save your changes.

Managing Globalization

The following sections explain how to work with Language Packs and to translate strings.

Managing Language Packs

A Language Pack is a set of strings that enable support for a specific language and locale. Each Language Pack has a set of strings in a source language; these strings are translated to a target language. You can 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.

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.

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 CSM Portal strings.

You can then use the Language Pack Editor to translate the strings or export the strings and send them to a vendor for translation.

1. In the CSM Administrator Main Window, select the Globalization category, and then select Manage Language Packs.
2. On the Manage Language Packs page, click Create.
3. Click Next on the Language Pack Wizard Welcome page.
4. 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.
5. Click Next.
   The Identify the Scope of the Language Pack page opens.
6. Identify the scope for your Language Pack. You can choose to:
   System Strings:
   - Definitions

     Extract all content strings or strings for specific Business Objects.

     When you extract specific Business Objects, all strings associated with those Business Objects are extracted.

   - Portal

     Extract Portal platform strings, Portal content strings, or both.

   - 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. See Enable Localization Support for a Lookup Table.

   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.

   For more information, refer to String Types.
7. Click Next.
   If you chose to create the Language Pack with specific Business Objects, the Identify Specific Business Objects page opens.

8. Select the Business Objects 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 click the Type column to sort the list.

9. Click Next.
If you chose to choose to include Lookup Tables in your Language Pack, the Identify Specific Lookup Tables page opens.

10. Select the Lookup Tables to apply translations to.

11. Click Next.
If you chose to include Portal strings in your Language Pack, the Identify Specific Sites page opens.

12. Select the Sites to apply translations to.

13. 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 Fall-back Mechanism.

14. On the Define Properties page, provide a name and description for your Language Pack.

15. On the Summary page, review the options you selected.

16. Click Back to change your options; click Finish to complete the wizard.

Edit a Language Pack

Each Language Pack contains a row for each string for the scope chosen when the Language Pack was created.

Use the Language Pack Editor to manage strings in a Language Pack.
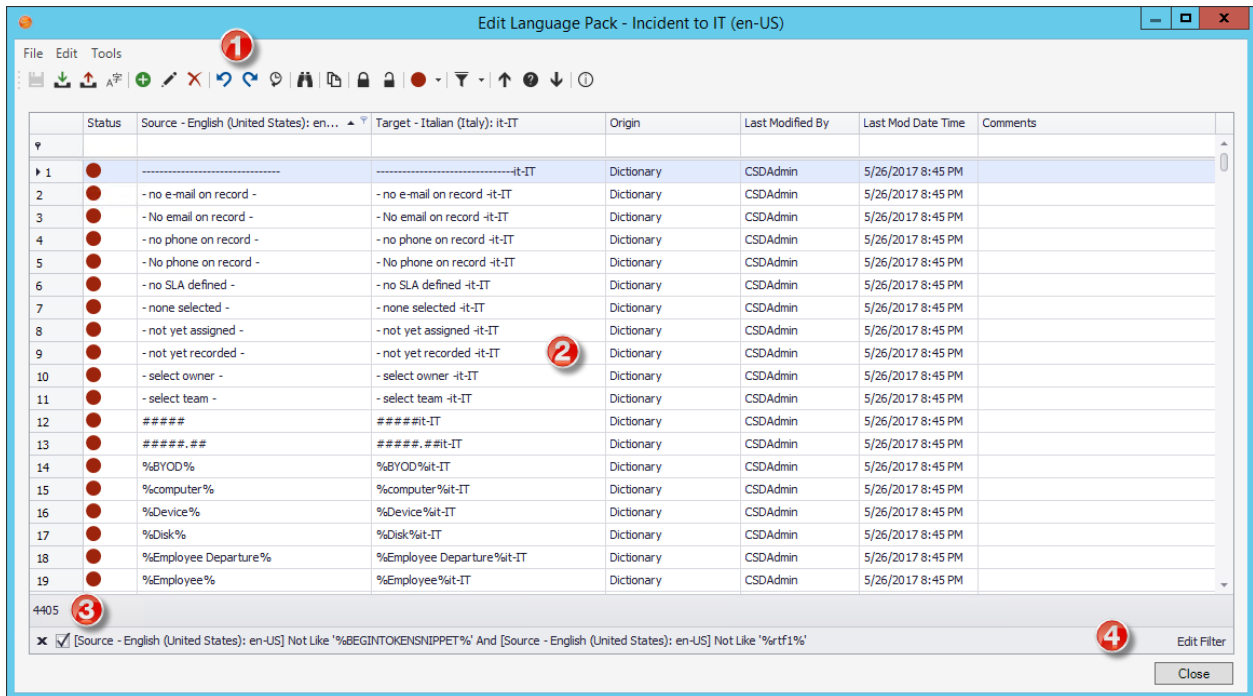
1. Language Pack toolbar

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 Updating Strings From Definitions.
⬆	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 Updating Strings From Definitions.
	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.	
❷	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. In the CSM Administrator Main Window, select the Globalization category, and then select Manage Language Packs.

2. Select a Language Pack, and then click 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 to not need to be translated. Text associated with a Token can be translated and its location in the string can be changed, however.
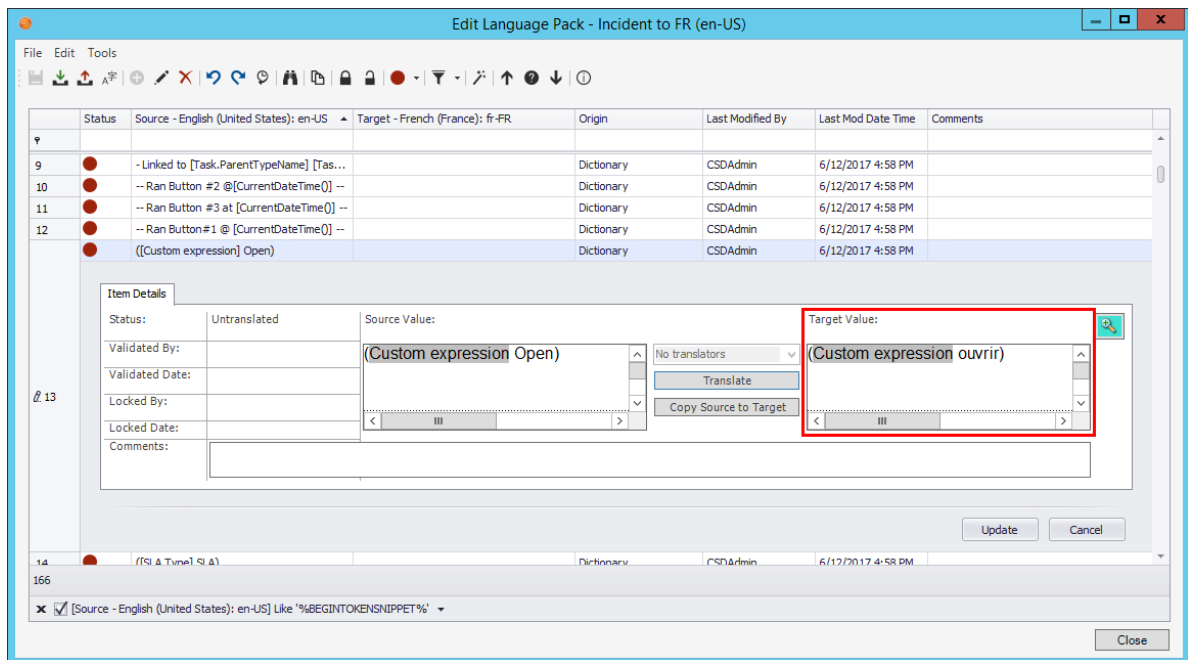
To translate text associated with Tokens in a Language Pack:

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.
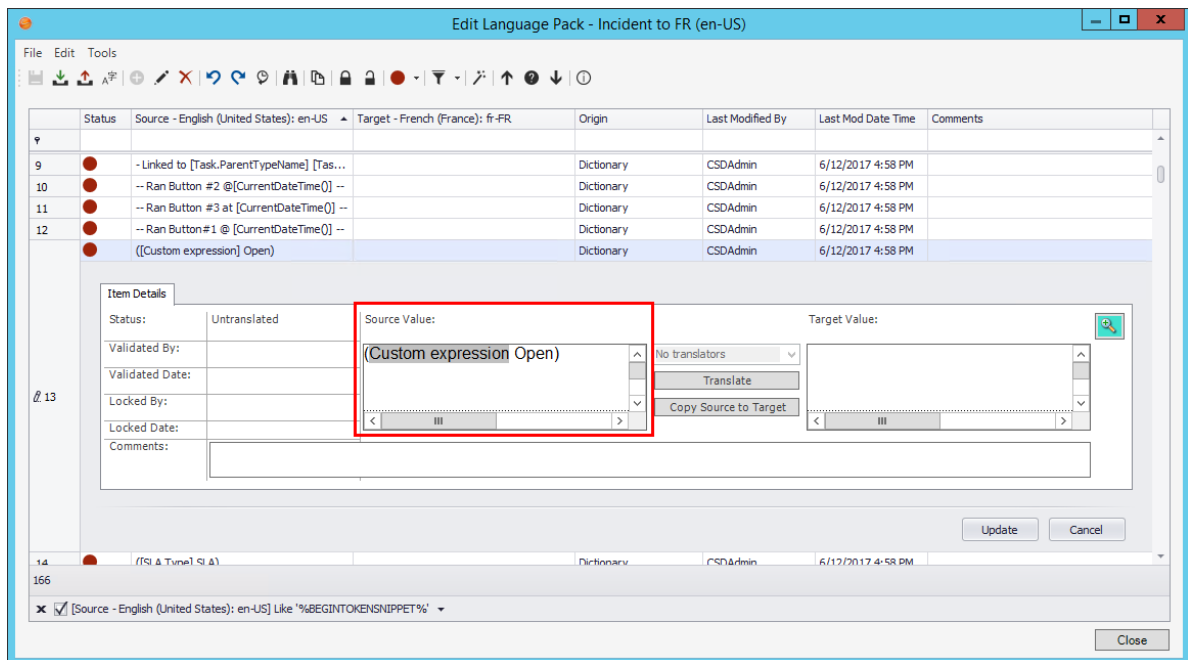
4. Click Copy Source to Target, and then translate the editable portion of the string.

5. Click Copy Source to Target, and then click the Expand icon (   ).

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 Token Expressions.
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.
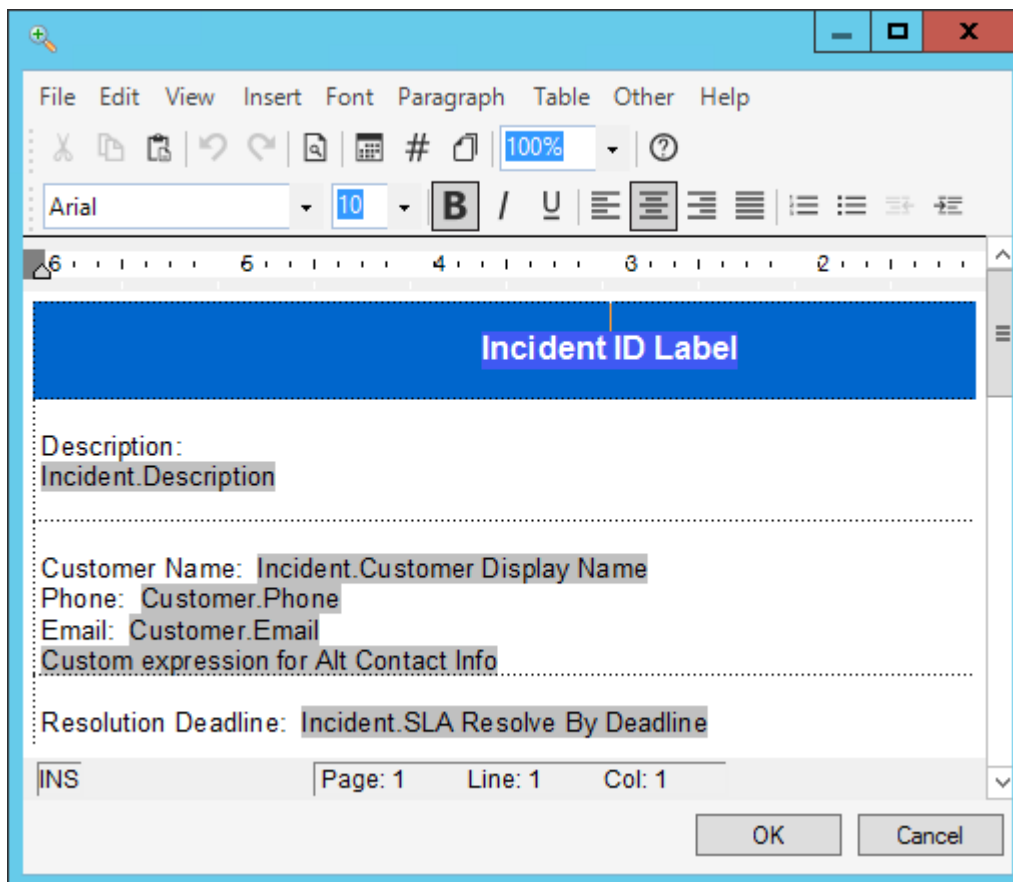
5. Use the Editor to translate and format editable text, and then click OK.
6. Click Update.

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.

Updating Strings From Definitions

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 system changes.

For example, if you add new Fields to a Business Object included in your Language Pack, use this option to add strings for that field.

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 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. 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 (![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.

To create a custom filter:

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.
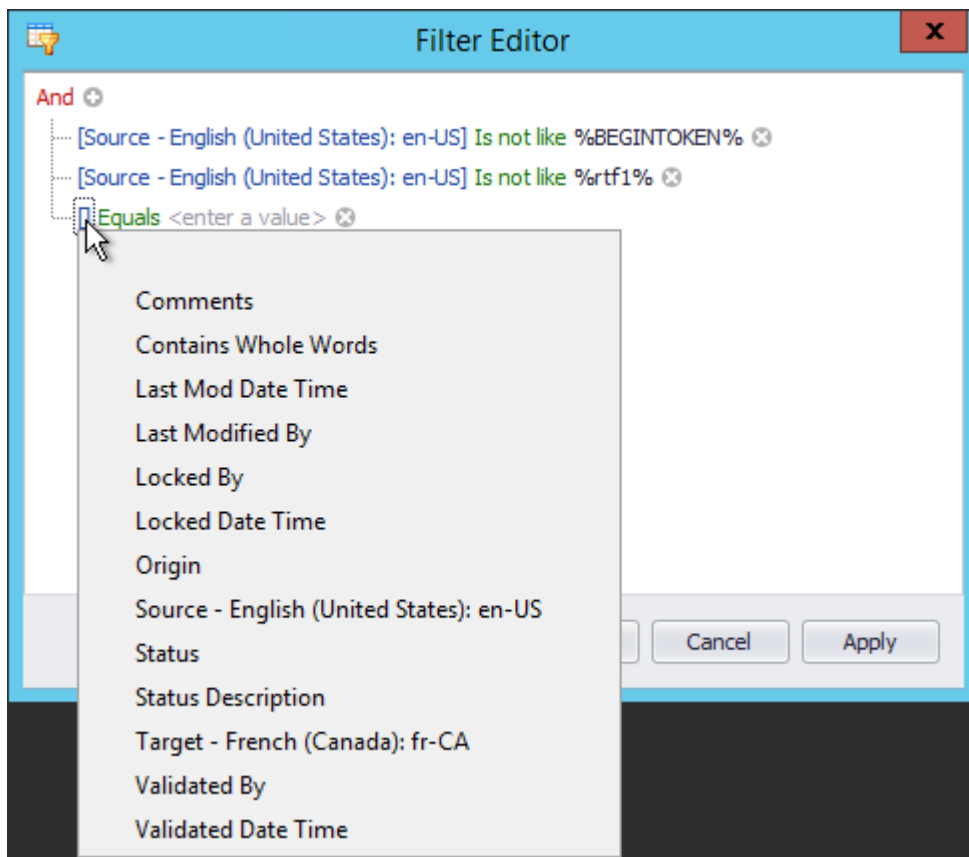
5. Add as many conditions as needed to filter the strings to the list you need.
6. Click Apply.

Apply a Language Pack

Use the Apply a Language Pack wizard to apply translated strings in a Language Pack bundle to your system.

You can apply the Language Pack bundle to the scopes and Business Objects in the bundle or you can change these settings when you apply the bundle. For example, a Language Pack may contain translated strings for the Incident and Problem Business Objects. You can choose to apply only strings for Incident.

Once a Language Pack bundle is applied, Users will see strings in the language associated with the Language Pack bundle if their security settings are set appropriately. For more information, see Configure Security for Cultures.

To apply a Language Pack bundle:

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 Apply.
   The Apply Language Pack wizard opens.
3. Click Next.
   The Identify Scope page opens.
4. The scopes applied to the Language Pack when it was created are selected by default. You can change the scope if you want to apply translations to identical strings in that scope.
5. Click Next.
   If you chose to apply the Language Pack bundle to specific Business Objects, the Identify Specific Business Objects page opens.
6. The Business Objects chosen for the Language Pack when it was created are selected by default. You can change the Business Objects if you want to apply translations to identical strings in different Business Objects.
7. Click Next.
   If you chose to apply the Language Pack bundle to Lookup Tables, the Identify Specific Lookup Tables page opens.
8. The Lookup Tables applied to the Language Pack when it was created are selected by default. Select the Lookup Tables to apply translations to.
9. Click Next.
   The Identify Portal Sites page opens.
10. The Sites applied to the Language Pack when it was created are selected by default. Select the Sites to apply translations to.
11. Click 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.

13. Click Next.
    The Choose When Translations are Published page opens.

14. Choose one of these options:
    Publish Changes Immediately

    Select this option to publish the translations when you complete the wizard.

    Save Changes to a Blueprint

    Select this option to save the translations to a Blueprint that you can publish later. If you select this option, you must choose a file name and location for the Blueprint when you complete the wizard.

15. Click Next.
16. On the Summary page, review the options you selected.
17. Click Back to change your options; click Finish to complete the wizard.

> **Note:** If you receive errors when you apply a Language Pack with a large number of strings, you may need to increase database connection timeout values. For more information, refer to Define Global Database Options.

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.

8. Open the .tsv file in a text editor and verify that it is encoded as UTF-8. For steps on viewing and setting the encoding, refer to your editor's documentation.

Once the exported file has been translated, you can import the Language Pack back into CSM. See 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. Click Import.
   The Import Language Pack dialog opens.
3. Click the Ellipses icon 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 click OK, the Merge Language Pack wizard opens after the import is complete.
   See Merge Language Packs.
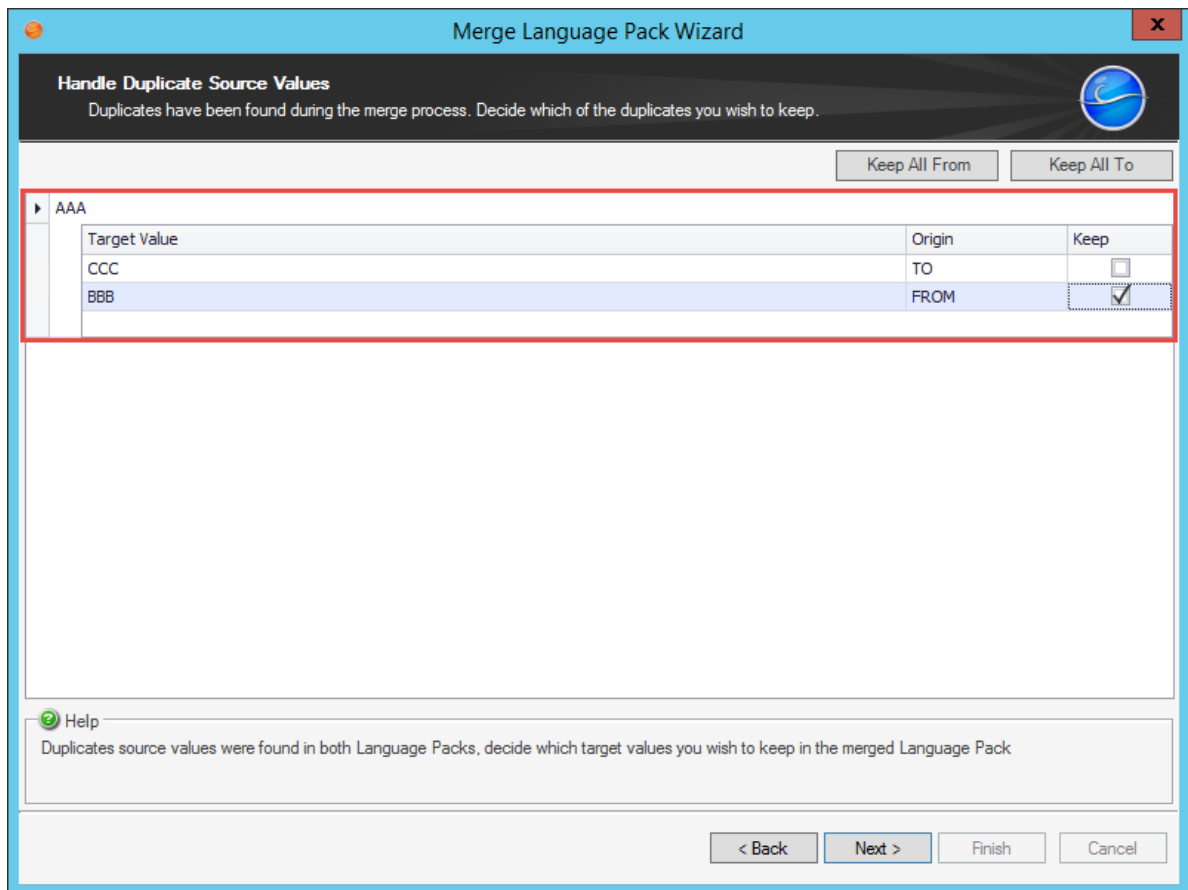
Merge Language Packs

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.

In the example above, select BBB to merge that value.

10. Click Next.
11. On the Summary page, review the options you selected.
12. Click Back to change your options; click Finish to complete the wizard.

View Language Pack Properties

You can view the properties for each Language Pack bundle, including:

- Target culture
- Source culture
- 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.

Translating 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, Forms, and Grids, as you work with Blueprints and mApps in CSM Administrator. 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 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.
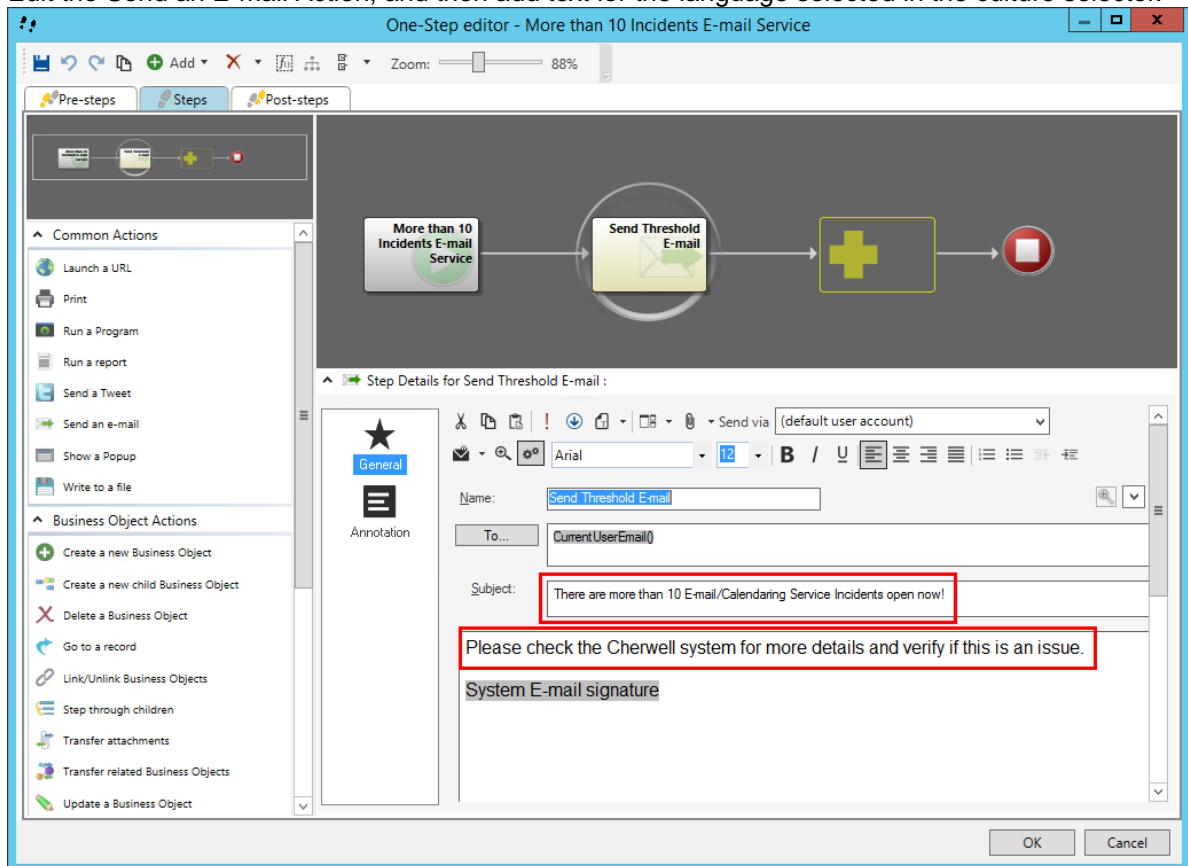
4. Click OK.
5. Use the culture selector to switch languages.

6. Edit the One-Step 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.

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.

Managing Translations for Individual Definitions

You can perform several localization tasks related to individual definitions from a Blueprint or a mApp in CSM Administrator.

- **View Translations**

  See Viewing Translations for Definitions.

- **Apply Language Pack Bundles**

  See Applying Language Pack Bundles to Definitions.

- **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

You can view translated strings and property information for individual definitions from a Blueprint or a mApp.

You can:

- Use the Item Managers to view translations for definitions, such as One-Steps, 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 text for a Form Control.

This option is available when Globalization is not enabled.

To view translations for a definition:

1. In CSM Administrator, create a Blueprint or mApp.
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 the text for 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.

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.
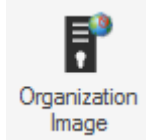
To prevent a definition from being translated:

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.

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.)

This option is available when Globalization is not enabled.

To remove translation restrictions from a definition:

1. In CSM Administrator, create a Blueprint or mApp.
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.
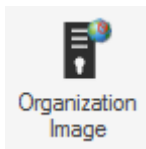
4. You can then:
   Right-click and select Localization > Allow item to be localized.

   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

You can apply one or more Language Pack bundles to one or more definitions. Translations will be applied to strings contained in the definition, but not to strings referenced by the definition. To see which strings will be translated, you can view the strings in each definition before applying translations.

You can:

- Use the Item Managers to apply Language Pack bundles to definitions, such as One-Steps, Stored Values, and Expressions.
- Use the Definition Reviewer to apply Language Pack bundles to Forms, Grids, and Form Arrangements.

This option is only available when Globalization is enabled.

To apply Language Packs to definitions:

1. In CSM Administrator, create a Blueprint or mApp.
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.
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 Bundles (Item Managers 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. Click OK.

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-Steps, 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.

This option is only available when Globalization is enabled.

To delete translations for definitions:

1. In CSM Administrator, create a Blueprint or mApp.
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.
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 Translated Content on Forms

When globalization and multiple cultures are enabled for your system, you can apply these localization properties to controls to each Adaptive Layout for each Form:

- Control size
- Control location

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.

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. See Switching Cultures.
   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

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.
4. Select Copy size, Copy position, or both.
5. Click Apply.
   The size and position values for the control are copied to the selected cultures.

Optimizing Content for Localization

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 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.

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.
4. Always update foreign key values after you run the Content Optimization Tool. For more information, see Update Foreign Keys for Validated Fields.
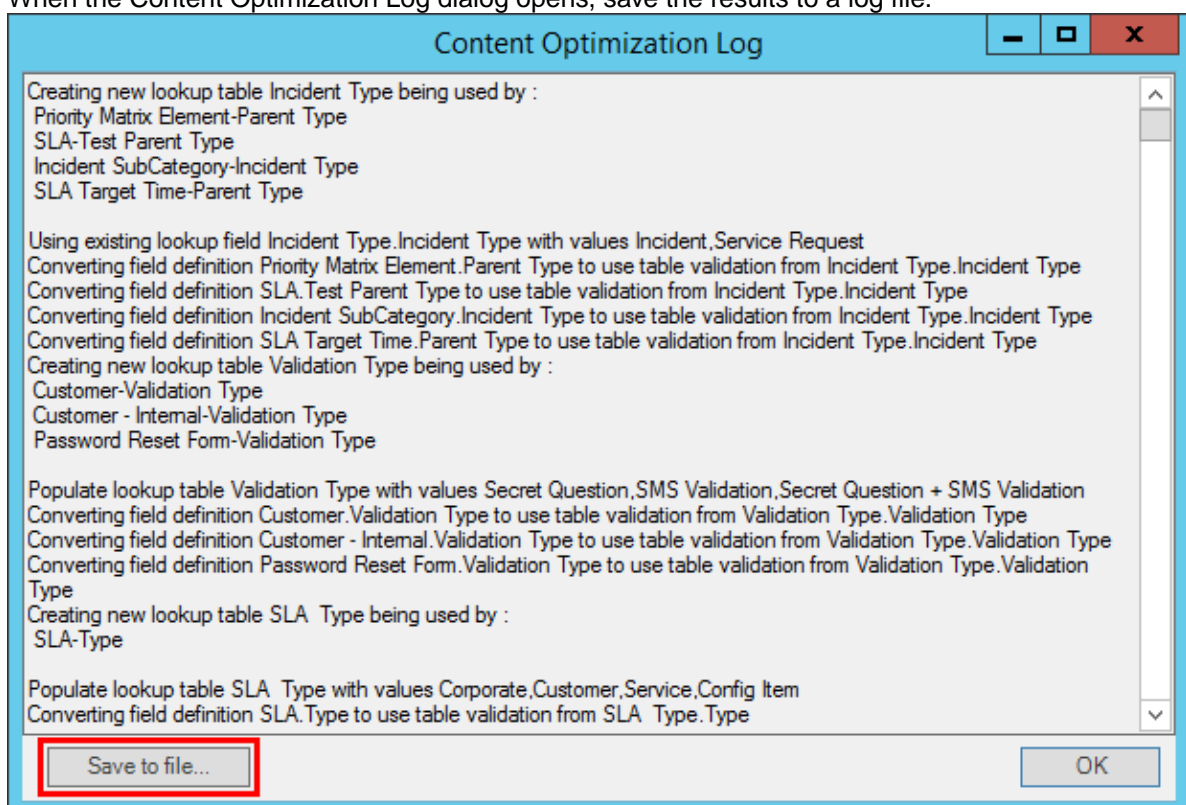
Running the Content Optimization Tool

⭐ **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

Important: Read the information in Optimizing Content for Localization before you use the Content Optimization Tool.

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.

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

> **Important:** Read the information in Optimizing Content for Localization before you use the Content Optimization Tool.

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.

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

⭐ **Important:** Read the information in Optimizing Content for Localization before you use the Content Optimization Tool.

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.

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

Important: Read the information in Optimizing Content for Localization before you use the Content Optimization Tool.

The Content Optimization Tool can enable localization support for Text Fields that are not used for validation.

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

Language Packs enable you to provide multiple translations for a single Portal Site. Users can switch between enabled languages as they work in the Portal.

Use this process to translate content for your CSM Portal Sites using Language Packs:

1. Verify that you have Portal Sites created and configured. See Building/Managing a Portal.
2. Verify that Globalization features are enabled for your system. See Enable Globalization.
3. Verify security settings for cultures. See Configure Security for Cultures.
4. Create a Language Pack that contains Portal strings. See Create a Language Pack.
5. Translate the strings using the Language Pack Editor or an external vendor. See Edit a Language Pack.
6. Apply the Language Pack. See Apply a Language Pack.

   > **Note:** When you apply a Language Pack that contains Portal strings, a Site Localization is automatically added to the Sites contained in the Language Pack.

7. Use the Localization page of the Site Manager to review and modify the name of your localized Site as needed. This name is shown to Users in the Language Selector. See Define Localization Properties for a Site.
8. Add the Language Selector to the Portal site.

Adding the Language Selector to the Portal Site

1. In CSM Administrator, edit your site.
2. Select the Localization page.
3. Select the **Show Language Selector on application bar** check box.
4. Click OK.

Translating Service Catalog Strings

Strings presented to Users in the Service Catalog may come from multiple sources. For example, the following table illustrates the types of strings in the OOTB Service Catalog, where they originate, and how to translate them.

Label	Business Object.Field	Business Object Type	Translation Process
1	Service.Service Name Service.Service Description	Major	1. Open Service records in the Desktop Client or CSM Browser Client. 2. Use the culture selector to switch cultures, and then manually translate values for the Name and Description Fields for each Service record.

Label	Business Object.Field	Business Object Type	Translation Process
2	Incident Category.Incident Category Incident Category.Category Description Incident SubCategory.Subcategory Description	Lookup Table	1. Enable localization support for the Lookup Tables used by the Portal. 2. Create a Language Pack and include the Incident Category Lookup Table. 3. Translate Incident Category values as described in Translating Values for Culture-Specific Fields.

Applying Translations to mApps

You can apply translations to mApps if:

- Globalization is enabled for your system.
- Multiple cultures are enabled.
- You have applied Language Packs that include translations for the enabled cultures.

The enabled cultures are included with the mApp, along with translations for definitions included in the mApp.

To apply translations to a mApp:

1. Create a mApp.
2. Define mApp 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 properties for each culture.
   If you do not define mApp properties for each enabled culture, you will receive an error when you prepare the mApp for distribution.
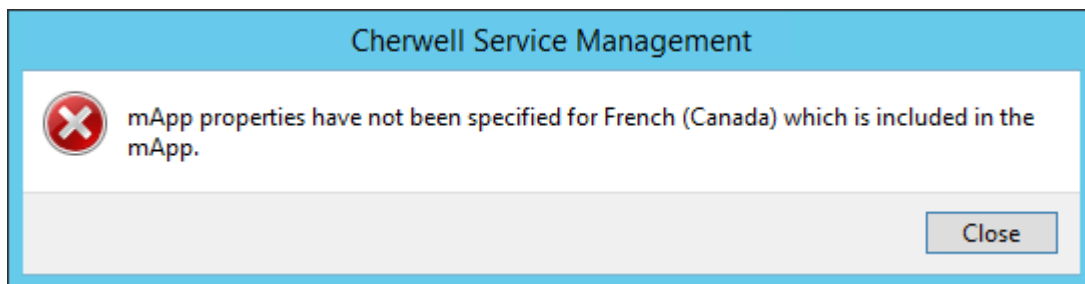
4. Prepare a mApp for Distribution and verify that mApp properties have been defined for all cultures included in the mApp.
5. Apply the mApp. The cultures and translations included in the mApp will be listed on the Localization page of the Apply mApp Wizard.

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 e-mail 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 e-mail 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-Steps that run based on the rule have been translated.

Configuring Record Translation

For this procedure, some experience with designing Forms and One-Steps is highly recommended. Work with your system administrator if your CSM experience is limited.

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.

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 to perform the translation.	See Configure a Translation One-Step.

In the following steps, you will configure the translation Web Service.

1. Verify that you have an API key for your selected translation service.
2. In the CSM Administrator Client, create a new Blueprint.
3. Open the Web Services Manager, and click 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, refer to 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.

In the following steps, you will configure the Business Object Form with Fields for translation.

7. In the CSM Administrator Client, create a new Blueprint.

8. From the list of Business Objects, select the Business Object to be configured for translation. For example, select Incident.

9. Click Edit Business Object.
   The Business Object Editor opens.

10. 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.

11. Return to the Object Manager and click Edit form.
    The Form Editor opens. Edit the Form to facilitate translation. For example, add the Translated
    Description Field next to the Description Field.

12. Save the Blueprint.
    The Business Object is now formatted for translation.

13. Create a One-Step to perform the translation in the Business Object Record. Refer to Configure a Translation One-Step.

14. Save and publish the Blueprint.

Configure a Translation One-Step

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 the Create New button ⊕ to create a new One-Step.

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 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.
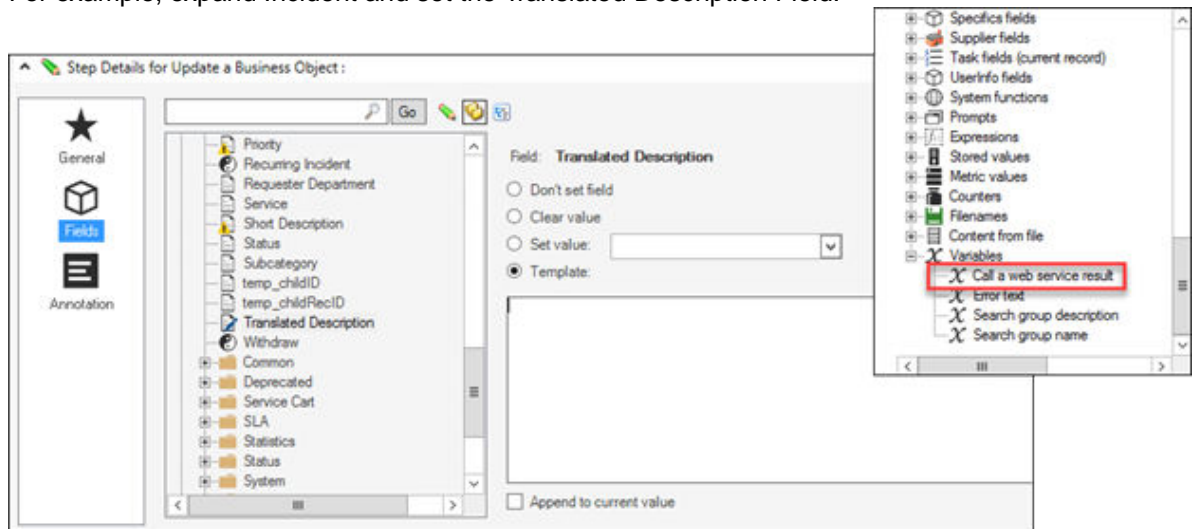
The Field is now set to the variable that contains the translated text.

10. Optional: Right-clickcall 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.
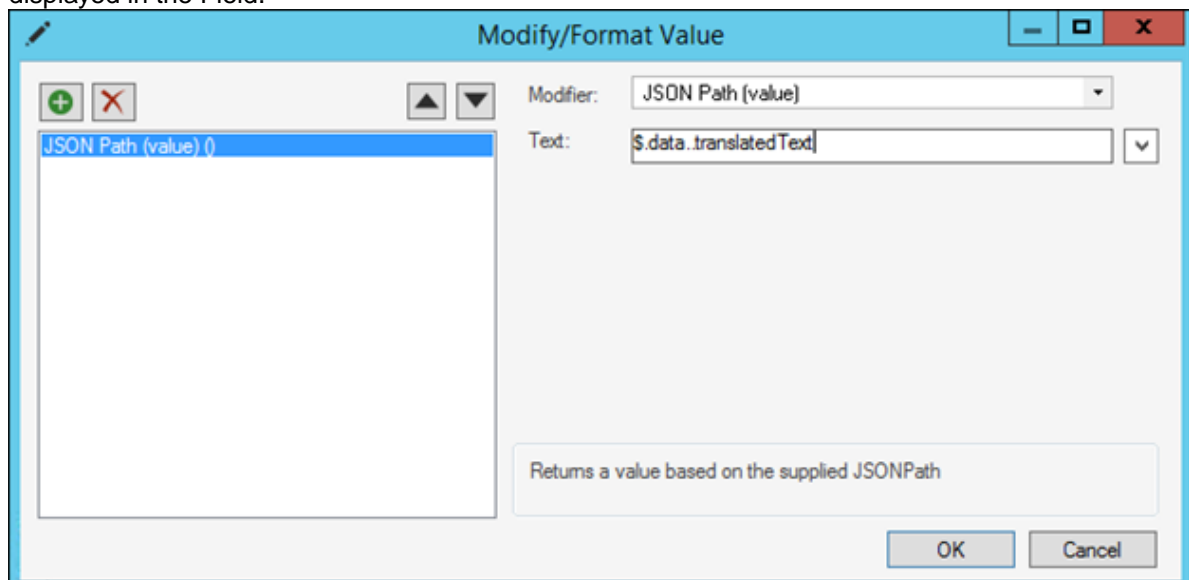
11. Optional: Define an automatic action so that the translation One-Step is executed automatically when the Business Object is saved.

Using Globalization with CSM Features

The following sections explain how to switch cultures and work with CSM after strings have been translated for enabled cultures.

Switching Cultures

When Globalization and multiple cultures are enabled, Users whose security settings allow them to use multiple cultures can switch cultures to change the language for:

- **Platform Strings**

  Typically client-based strings, such as those for menu items, toolbars, controls, and tooltips.

- **Content Strings**

  Strings for Business Objects, Forms, Dashboards, Expressions, One-Steps, etc. This includes OOTB content and customer-created content.

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.

> **Note:** Multi-tab browsing support allows you to open tabs in multiple languages in the Browser Client and Customer Portal and work in the tabs within the same session.

Using the Culture Selector in the CSM Browser Client

The following culture selector is available in the CSM Browser Client.

1. Select a platform culture.
2. Select a content culture.

Using the Culture Selector in the CSM Portal

The following culture selector is available in the CSM Portal. Select a culture to see translated content and platform strings, if they are available.
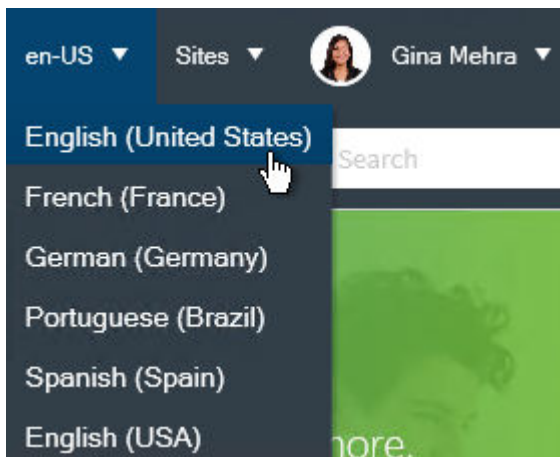
Using the Culture Selector in the Windows Clients

The following culture selector is available in the CSM Desktop Client and CSM Administrator.

Note: In the CSM Desktop Client, only enabled cultures appear. In the CSM Administrator, all cultures in the system are available.
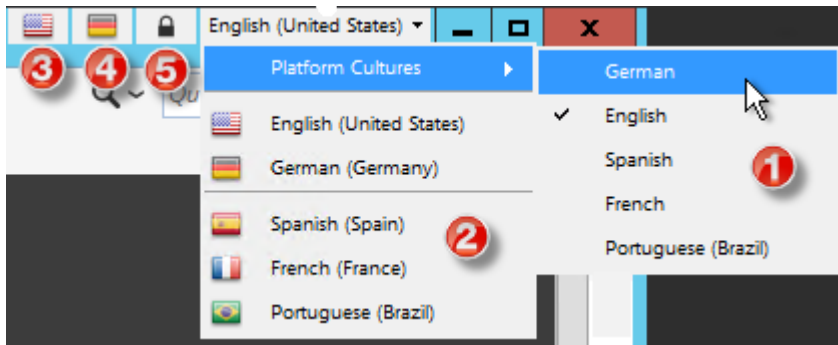
1. Select Platform Cultures > Culture Name to change the culture for the platform strings.

2. Select a culture to change content strings.

3. Click the first flag icon to switch to the preferred culture for your system.

4. Click the second flag icon to switch to the previously used culture. This is always a different culture than the preferred culture.

5. Click the lock icon to lock or unlock platform strings. When strings are unlocked, the platform strings (if available) switch to the content strings you select. When strings are locked, only content strings change.

Using Translated Lookup Table Values in Search Queries

Pre-requisite: Complete the steps in Configure Localization Support for Lookup Tables.

Once you apply translations to Lookup Tables, Users can select translated values as they build search queries.

To search for translated values:

1. Create or edit a Search Group.

2. From the Comparison Clause list, create a Lookup Table Field. For example, within the Incident association, select the Incident.Call Source field.

3. Select an operator, and then select the drop-down list on the right.
   Specific Culture Values are listed.
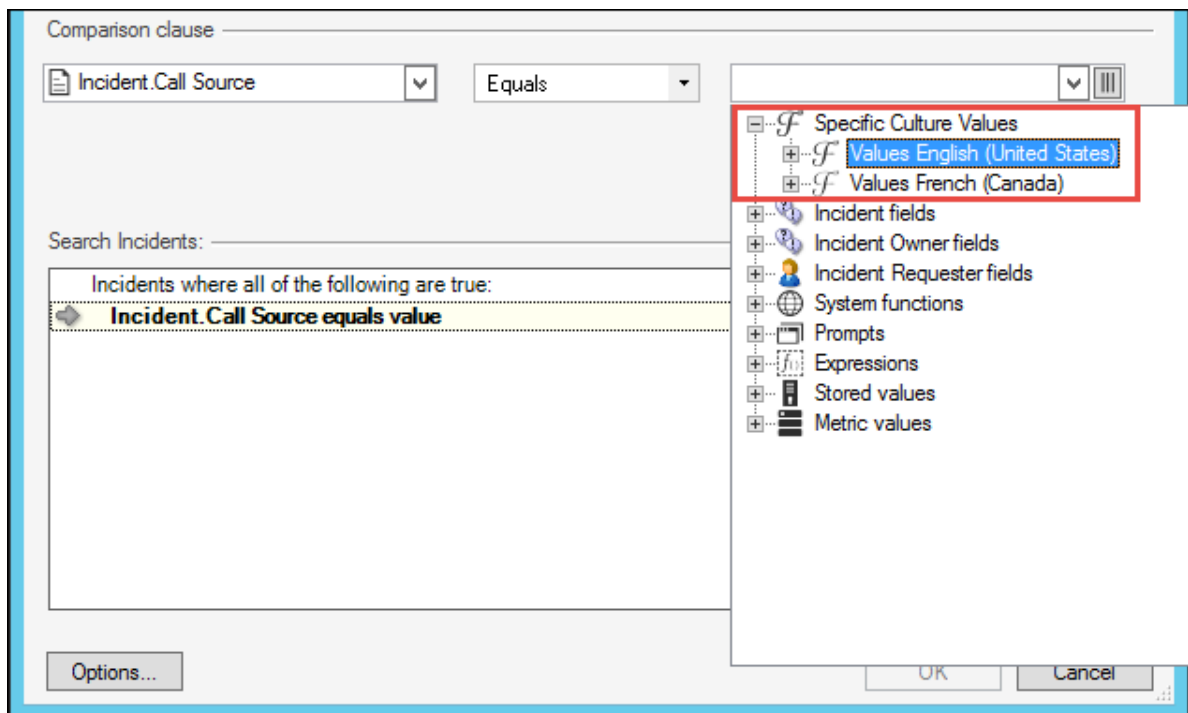
4. Expand the language that contains the value you want to search for, and then select the value.
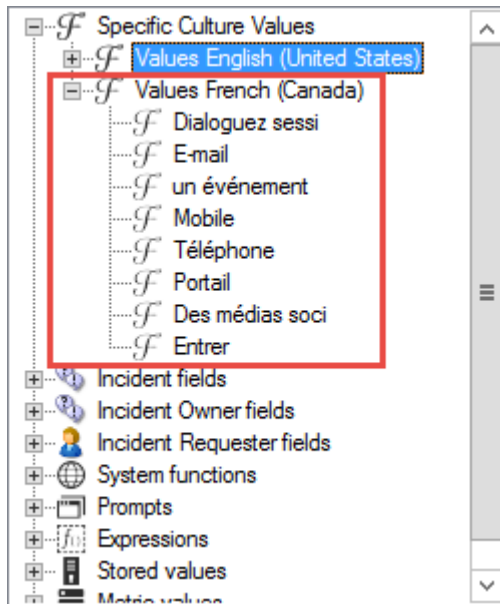
Using Reports with Multiple Cultures

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 after you enable Globalization.

Selecting a Report Culture

The first time you run or edit each existing Report in the CSM Desktop Client after Globalization is enabled, you are prompted that the Report does not have an associated culture. The primary culture is detected, however, and you are asked if you want to use that culture.

Note: The primary culture is chosen by the administrator who upgraded your system to CSM 9.2.0 or later.

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.

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+P	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

The following sections describe best practices for working with Globalization features.

Consider Impact of Translations

If you intend to globalization your system at some point, always design your customizations with translations in mind. Some translations may require Form adjustments, for example.

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.
- You can you backfill translated values in existing records.

Use the Content Optimization Tool to easily convert validation lists to Lookup Tables.

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 smaller 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.

Troubleshooting Globalization
Troubleshooting the Culture Selector

Use these troubleshooting tips to solve issues that prevent Users from seeing the culture selector.

1. If cultures do not appear in the CSM Desktop Client, verify that you have enabled cultures for your system. For more information, see Manage Cultures.

2. Verify that culture security settings are correctly applied. For more information, see Configure Security for Cultures.

3. If Users cannot see the culture selector in CSM Desktop Client, suggest that they reload definitions (Help > Reload Definitions. If User are still unable to see the culture selector, suggest that they close and reopen CSM Desktop Client.

4. If Users cannot see the culture selector in the CSM Browser Client or CSM Portal, suggest that they clear their browser cache. If Users are still unable to see the culture selector, restart Internet Information Services (IIS).

Handling Warnings When Applying Foreign Keys

When you apply foreign keys to a Field that supports localization, you may receive a warning that states that a Field "must be filled in before the record can be saved."

This warning occurs because rules for required Fields are respected when a record is updated, and the process for applying foreign keys for Fields with multiple cultures may update records.

You can safely dismiss the warnings as you apply foreign keys.

Handling Conflicts During Blueprint Publishing

As you work with Globalization features, you may encounter conflicts when you publish a Blueprint.

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.

To resolve conflicts, select the Use my Blueprint option on the Blueprint Conflict Resolution dialog. For more information, see Develop Blueprints Concurrently.

Handling Multiple Legal Value Messages in the Log File

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.

To solve this problem, you can:

- Remove duplicate values from the Lookup Table Field for all languages.
- Select the On Conflict Use First Match check box in the Validation area of the Validation/Auto-populate page of the Field Properties dialog.

Administrative Resources

CSM Command-Line Options

There are situations where it is useful to launch CSM and have it automatically execute an instruction. For example, a third-party tool might launch the CSM application to have the User taken to a specific Incident record. CSM supports a number of command-line options for making this possible.

A command also allows a hyperlink to be created in an e-mail that, when clicked, launches the Cherwell application and executes an instruction. Of course, for this to work, CSM must be installed on the machine.

Note: 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 new window (in the future, support for launching in the current window will be added).

As well as the CSM Desktop Client application, CSM Administrator also has useful command-line options (ex. Executing a backup). In fact, most of the CSM applications support some form of command-line launching, even if it is only specifying a connection, User ID, and password.

Command-Line Flags

To use the command-line options, execute Cherwell with arguments. For example, to make a desktop shortcut that specifies a connection and User ID, specify the arguments as part of the shortcut's Target:
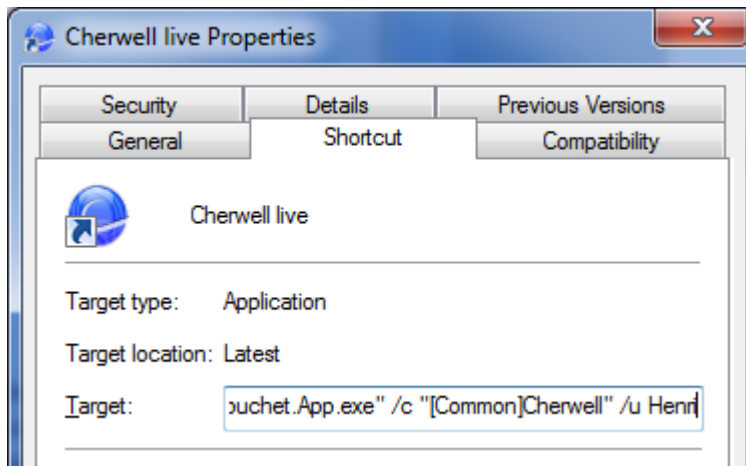
When launching the CSM Destop Client application, the actual application to run is called Trebuchet.App.exe (Trebuchet is the internal library name for the CSM application). This is usually found in the directory C:\Program Files\Cherwell Service Management.

> **Note:** Arguments can either be prefixed with a forward slash or with a dash, so /? and -? are equivalent.

General Command-Line Flags

This first set of command-line options work with most of the CSM applications. Use general command-line flags for:

- Help
- Connection
- User ID and Password
- Platform Culture
- Content Culture

Help

Argument: /?

Many applications provide a display of their supported command-line options by specifying this option.

Connection

Argument: /c "[Common]*connection*"

Specify which Cherwell connection should be used by the application. To use a common connection—a connection that is available to all Users of the machine—prefix the connection with [Common]. To use a connection that is associated with the current User, prefix the connection with [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.

User ID and Password

Arguments: /u "*username*" /p "*password*"

Specifies the User ID and password to use when logging in. This only works when Cherwell authentication (as opposed to Windows or LDAP) is enabled.

> **Note:** Putting a password into a shortcut is a potential security issue, since other Users are able to edit the properties of the shortcut and read the password.

Culture

Argument: /l *language-culture pair* /r *language-culture pair*

Example language culture pairs: de-DE, fr-FR, pt-BR.

Use /l to set the culture for content strings; use /r to set the culture for platform strings. For more information, see String Types.

Execute a Command

There are a number of commands that can be executed from the command-line. They all follow the same basic pattern:

Trebuchet.App.exe /GR *recordType argument*

recordType is the type of business object to execute against. This can either be the name or internal ID of the object. For example, to find a particular Incident, specify a record type of Incident.

argument is different depending on the type of command.

Goto Record

Arguments: /GR recordType RecID

This command takes the system to a particular record, identified by its internal Record ID. This is a special value used within Cherwell to uniquely identify records. For *most* types of records, this is a long string that looks similar to:

939cd1f313b3b6866ef7d043faa258398c765d444a

Obtain this value by running a One-Step that populates or writes to a field or a file the value in the RecID field (One key 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 Cherwell and bring up a record, sometimes the RecID comes from a query or other mechanism.

Goto Record by Public ID

Arguments: /GP recordType PublicID

The Public ID of a Business Object is the ID by which it is normally identified by Users (vs. by the system). For an Incident this would be the Incident ID, for a Change the Change ID, etc. The Public ID does not need to be a number. For example, the Public ID for a Customer is the Customer's full name.

To go to Change 12345, execute a command like this:

Trebuchet.App.exe /GP Change 12345

Goto Search Group

Arguments: /GS recordType searchGroup

This option launches a named global search and displays the results.

Note: Use the following format for the search group to launch non-global searches: Scope;Scope-Owner;SearchGroup

The scope can be any supported scope – Global, Team, Persona (the internal name for Role), User, etc. The tricky thing is providing the scope-owner. The scope-owner must be the internal ID of the owner. This is a long, 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.

Search for Text

Format: CherwellClient://commands/search?rectype=*recordType*&search=*searchText*

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 needs to be URL encoded.

New Process

Argument: /NP

Normally, when launching Cherwell (with or without any additional command-line arguments) the system looks to see if Cherwell 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.

There are times when this is undesired. For example, to log in to two different connections. If Cherwell is already running, arguments related to connection, User-ID and password are ignored. By specifying the NP argument, Cherwell does not try to find an existing instance of Cherwell and always launches a new one.

Note: If Cherwell is run from two different directories, it always creates a new instance.

Administrative Command-Line Options

In addition to being able to launch the Cherwell application and make it execute certain operations, CSM Administrator also has several command-line options. In addition to specifying a connection, User ID, and password (as with other Cherwell applications) use the Administrative Command-Line Options to back up the system, run system maintenance, and restore the system.

Back up the system

There are times when: there is no need to use the CSM Scheduler to do backups, there is a preference to use a different scheduler, or Users would like the backup to be done on a system that does not have the scheduler running. This is common when installed in a SAAS environment.

The format for backing up Cherwell is:

Trebuchet.Admin.exe /c "[Common]*connection name*" /u "UserID" /p "Password"

/b "*backup-filename*" [/r "rollover options"]

The connection, User ID, and password work the same as for any other application. Other arguments used with backing up a system include:

- /b – This is the filename that the backup should go to. If the extension is .car, then the backup is an uncompressed archive. If the extension is .czar, or not included, the backup is compressed in a .czar file format.
- /r – Rollover options. To have the filename automatically have date/time information be appended, use this optional argument. There are several rollover options:
  - **Unmodified:** No value 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.

Run system maintenance

Execute system maintenance options via the command-line, using the following format:

Trebuchet.Admin.exe /c "[Common]*connection name*" /u "UserID" /p "Password"

/db delimited-list-of-options

The list of maintenance operations to run should be comma-delimited and can include any of the following:

- **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** – Clears up obsolete authorization data.

As an example, to rebuild the full text catalog and refresh queue status, execute the following command (all in one line):

Trebuchet.Admin.exe /c "[Common]Cherwell" /u "Henri" /p "password"/db RebuildFullTextCatalog,RefreshQueueStatus

System Restore:

When executing a system restore using the command line, a prompt appears if CSM needs to be upgraded.
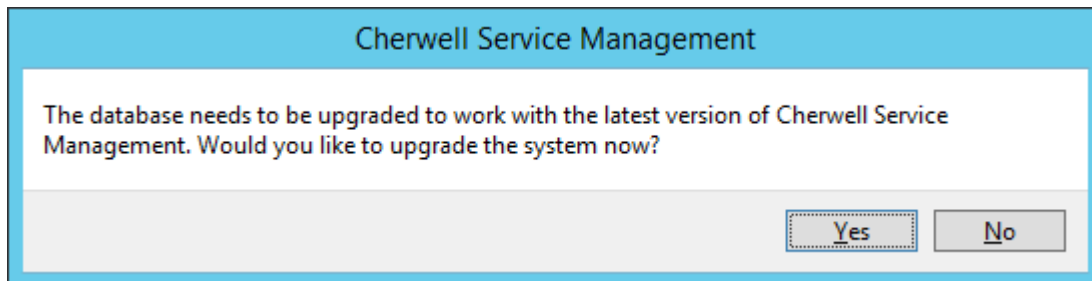
Linking Directly to CSM Objects

You can provide links (also known as deep linking) to CSM objects, such as records and saved Search Groups. This is useful for adding links to e-mails 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.

Use these URL commands to:

- Go to Record by Record ID
- Go to Record by Public ID
- Go to Record in Edit Mode Format
- Create Record by Business Object Name
- Create Record for a Specific Locale
- Go to a Search Group
- URL Search for Text
- Open a Dashboard
- Run a Report
- Go to an HTML Page

Parameter Key

Parameters are in italics and should be replaced with the values as noted in the following table.

Note: Parameter values that contain spaces must be URL-encoded.

Parameter	Replacement Value
ServerName	The server name or IP address for the Browser Client or 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

Parameter	Replacement Value
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 by Record ID

Client	URL Command	Example
Desktop Client	CherwellClient://commands/goto?rectype=*BusinessObjectName*&recid=*Record ID*	CherwellClient://commands/goto?rectype=*incident*&recid=*93d6067b6f6e1a17a2364744bc984bdb2715f624fa*
Browser Client	https://*ServerName*/CherwellClient/Access/*BusinessObjectID*/*Record ID*	https://*ServerName*/CherwellClient/Access/*incident/93d6067b6f6e1a17a2364744bc984bdb2715f624fa*
Portal	https://*ServerName*/CherwellPortal/*SiteName*/*BusinessObjectID*/*Record ID*	https://*ServerName*/CherwellPortal/IT/*incident/93d6067b6f6e1a17a2364744bc984bdb2715f624fa*

Go to Record by Public ID

Client	URL Command	Example
Desktop Client	CherwellClient://*BusinessObjectName*/*PublicID*	CherwellClient://commands/goto?rectype=incident&PublicID=123456
Browser Client	https://*ServerName*/CherwellClient/Access/*BusinessObjectName*/*PublicID*	https://*ServerName*/CherwellClient/Access/*incident/123456*
Portal	https://*ServerName*/CherwellPortal/*SiteName*/*BusinessObjectName*/*PublicID*	https://*ServerName*/CherwellPortal/IT/*incident/123456*

Go to Record in Edit Mode

...ent	URL Command	Example
...wser Client	https://*ServerName*/CherwellClient/Access/Command/ Queries.GoToRecord? BusObID=*BusinessObjectName*&PublicID=*PublicID*&EditMode=*True*	https://*ServerName*/CherwellClient/Access/ Command/Queries.GoToRecord? BusObID=*incident*&PublicID=*123456*&EditMode=*True*
...tal	https://*ServerName*/CherwellPortal/*SiteName*/Command/ Queries.GoToRecord? BusObID=*BusinessObjectName*&PublicID=*PublicID*&EditMode=*True*	https://*ServerName*/CherwellPortal/IT/Command/ Queries.GoToRecord? BusObID=*incident*&PublicID=*123456*&EditMode=*True*

Create Record by Business Object Name

Client	URL Command	Example
Browser Client	https://*ServerName*/CherwellClient/ Access/New/*BusinessObjectName*	https://*ServerName*/ CherwellClient/Access/New/ *incident*
Portal	https://*ServerName*/CherwellPortal/ *SiteName*/New/*BusinessObjectName*	https://*ServerName*/ CherwellPortal/IT/New/ *incident*

Create Record for a Specific Locale

The following example shows the URL for creating an incident in the Portal for a French locale.

Client	URL Command	Example
Portal	https://*ServerName*/CherwellPortal/ *SiteName*/New/*BusinessObjectName*? Locale=*locale*	https://*ServerName*/ CherwellPortal/IT/New/ *Incident*?Locale=*fr-FR*

Go to a Search Group

Use the following examples to run a Global Search Group.

To run Search Groups 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	Example
CherwellClient://commands/goto?rectype=*recordType*&group=*Search %20Group%20Name*	CherwellClient://commands/goto?rectype=*incident*&group *%20Incidents*
https://*ServerName*/CherwellClient/Access/Command/Queries.SearchByID? Scope=*Global*&ScopeOwner=*(None)*&Owner=*BusinessObjectID*&Name=*Saved %20Search%20Name*	http://localhost/CherwellClient/Access/Command/ Queries.SearchByID? Scope=*Global*&ScopeOwner=*(None)*&Owner=incident&N *%20Incidents*
https://*ServerName*/CherwellPortal/*SiteName*/Command/Queries.SearchByID? Scope=*Global*&ScopeOwner=*(None)*&Owner=*BusinessObjectID*&Name=Saved %20Search%20Name	https://*ServerName*/CherwellPortal/IT/Command/ Queries.SearchByID? Scope=*Global*&ScopeOwner=*(None)*&Owner=*incident*&N %20Incidents

Search for Text Format

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.

Client	URL Command	Example
Desktop Client	CherwellClient://commands/search? rectype=*recordType*&search=*searchText*	CherwellClient://commands/ search? rectype=*incident*&search=*Printer %20%problem*

Open a Dashboard

Client	URL Command	Example
Browser Client	https://*ServerName*/CherwellClient/Access/ Dashboard/*Dashboard%20Name*	https://*ServerName*/ CherwellClient/Access/ Dashboard/*CMDB%20Assets*
Portal	https://*ServerName*/CherwellPortal/ *SiteName*/Dashboard/*Dashboard%20Name*	https://*ServerName*/ CherwellPortal/IT/Dashboard/ *CMDB%20Assets*

Open a Dashboard by ID

Client	URL Command	Example
Browser Client	https://*ServerName*/CherwellClient/Access/Dashboard/by-id/*Dashboard%20ID*	https://*ServerName*/CherwellClient/Access/Dashboard/by-id/*93c6d34533492283691b0b4531802a4e6552e8baf5*
Portal	https://*ServerName*/CherwellPortal/*SiteName*/Dashboard/by-id/*Dashboard%20ID*	https://*ServerName*/CherwellPortal/IT/Dashboard/by-id/*93c6d34533492283691b0b4531802a4e6552e8baf5*

Run a Report

Client	URL Command	Example
Browser Client	https://*ServerName*/CherwellClient/Access/Report/*ReportName*	https://*ServerName*/CherwellClient/Access/Report/*My%20Task%20List*

Run a Report by ID

Client	URL Command	Example
Browser Client	https://*ServerName*/CherwellClient/Access/Report/by-id/*ReportID*	https://*ServerName*/CherwellClient/Access/Report/by-id/*939015c2ff09e43342f1094612a5cfc84de38baa37*

Go to an HTML Page

Client	URL Command	Example
Portal	https://*ServerName*/CherwellPortal/*SiteName*/Page/*PageName*	https://*ServerName*/CherwellPortal/IT/Page/*IT%20Home*

Go to a Calendar

Client		Example
Browser Client	https://*ServerName*/CherwellClient/Access/Calendar/*CalendarName*	https://*ServerName*/CherwellClient/Access/Calendar/*Change%20Calendar*

Client		Example
Portal	https://*ServerName*/CherwellPortal/*SiteName*/Calendar/*CalendarName*	https://*ServerName*/CherwellPortal/IT/Calendar/*IT%20Calendar*

Friendly Links and URL Encoding in CSM

Providing links to send inside of CSM works by either using the e-mail options or from a One-Step, but the display text of the link is the same as the content of the link. Sending links from One-Steps uses display text that is different than the actual link.

Note: This works for launching CSM *and* links to other websites or files.

To create a link with a different display text in a CSM e-mail message or One-Step, instead of providing the hyperlink, right-click in the body of the message, and select Expressions>New custom Expression, and then change the Expression to Text.


Inserting a custom text Expression into a One-Step

The format for the text needs to be as follows:

[LINK]friendly-text;URL

The word LINK in square brackets tells Cherwell to treat this as a link, the friendly text is what is displayed as the link text, and the URL after the semi-colon is the actual hyperlink.

Note: There are no line breaks entered into the Expression, the new line is caused by wrapping. When then User gets this e-mail, the link looks similar to: Goto Incident 10928. When clicked, the User is taken to the record.
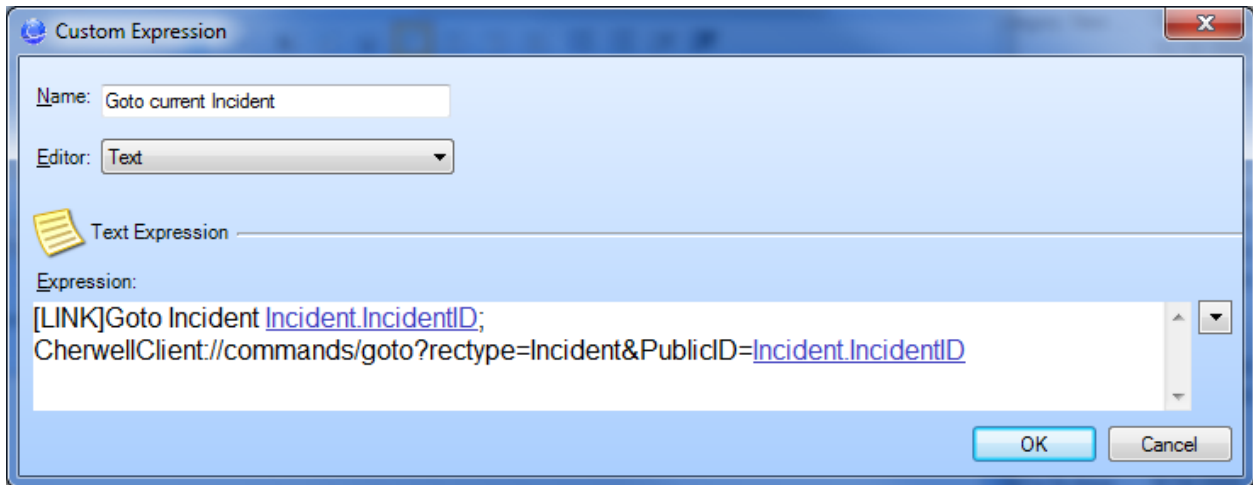
URL Encoding

The format allowed for URLs is fairly proscribed. For example, the link cannot include spaces or certain punctuation characters. Passing an ID like IncidentID is not an issue, but passing search text can cause a problem.

To resolve the issue, *URL encode* the URLs—this converts certain characters in a URL into a code that is allowed. For example, spaces are converted into the sequence %20.

To pass field values that might contain unsupported characters, the values must be URL encoded.

To perform URL encoding:

1. **Right-click** in the Inserted field of the One-Step.

2. In the Modifier drop-down, select URL Encode from the list of modifiers.
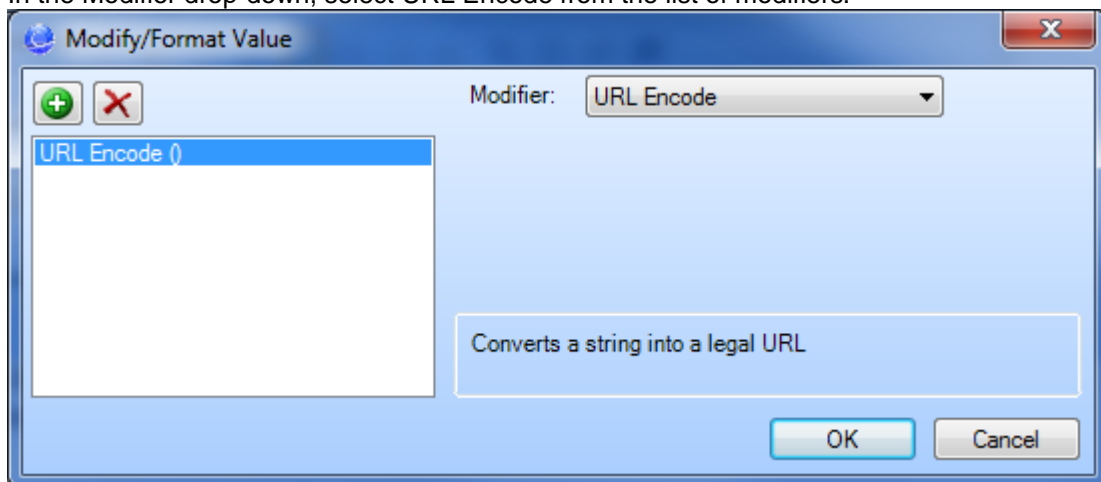
Use an HTTP POST with Credentials to Link in the Portal or Browser Client

We recommend using an HTTP POST to link in the Portal or Browser Client. To ensure security, use Windows, LDAP, or SAML authentication.

To use the HTTP POST with credentials in the Portal or Browser Client:

1. Build a custom **HTTP POST** to a URL (example: https://myserver/cherwellportal/mysite/Command/Queries.GotoRecord?AutoCreateSession=true).

2. Post **form data** using the following JSON format:

```
{

"Params": {

"username": "fred",

"password": "Management55",

"BusObId": "Incident",

"RecId": "938bc5d3322ed241397ff14944b488b99ea2672a76"

}

}
```

3. Add a secondary **HTTP GET** to navigate to the Portal (example: https://myserver/cherwellportal/mysite).

   🖉 **Note:** This command loads the configured site.

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.

Here are some tips for finding Internal IDs for CSM objects:

- Export an object, such as a Search Group 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. For more information, refer to Import/Export a CSM Item.
- Find the Internal IDs for Business Objects, Fields, and Relationships in the CSM Administrator.
- Use an appropriate 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 the Cherwell REST API.