ivanti

Management Center

powered by AppSense

Product Guide

Version 10.1 FR1

Copyright Notice

Table of Contents

What's new in Management Center?

Management Center rebrand to Ivanti

The Management Center console has been updated to reflect the new company name of Ivanti.

You may still see references to the AppSense name used in certain areas, such as the Registry or Windows Services.

Console Refresh

The Management Center console has an icon set update in response to customer feedback on the 10.0 console.

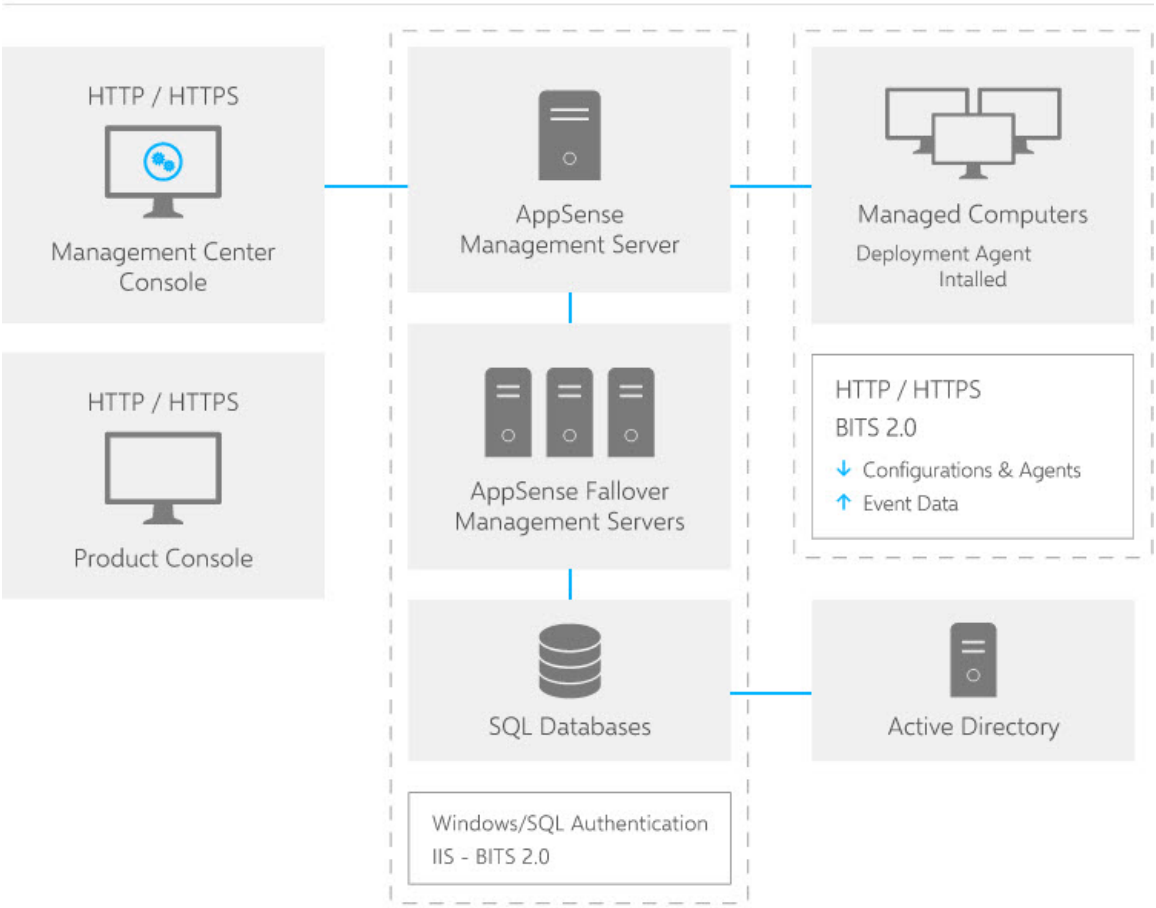
SQL Mirroring Support

Support for SQL Mirroring has been reinstated for 10.1 FR1. Please note that our best practice for this use case is to utilize SQL Always On.

About Management Center

Management Center Components

The Management Center comprises of the Management Server, Microsoft SQL Server, Management Console and the Deployment Agent installed on managed computers. The Deployment Agent uploads event data from managed computers to the Management Server and downloads product configurations and software updates from the Management Server. Product configurations are created using the product consoles and stored in the Management Center SQL database from where they can be downloaded along with product agents by the Deployment Agent for installation on managed machines.



Management Console

The Management Console provides an interface to the Management Server and the other components of the Management Center. The console allows you to manage Deployment Groups, Global Settings, Packages, Alerts and Alert Rules, Reports and Security.

Navigation Pane

The Navigation pane consists of the navigation tree and navigation buttons. The navigation tree is the area for managing nodes of the configuration. The navigation buttons allow you to view the different areas of the console, including:

- **Home** - Provides an overview of the Management Center with the first three step up steps to help you get up and running. From here you can launch the DesktopNow product consoles; Application Control, Environment Manager and Performance Manager. The work area also contains overview details of the server connection, deployment groups, computers and alerts.

  From within the Home view you can setup and manage the following:

  - Deployment Groups
  - Global Settings
  - Membership Rules
  - All Computers
  - Licensing
  - Events
- **Packages** - Manage DesktopNow software agent, configuration packages and any prerequisites on the Management Server.
- **Alerts** - Add and manage alerts and alert rules for DesktopNow software events sent to the server from client computers.
- **Reports** - Import and generate a range of reports for DesktopNow products.
- **Security** - Manage server and object permissions and role-based access rights to the Management Center console views and settings.

The Navigation pane is collapsible allowing you to create more viewing space for the other areas of the console.

Work Area

The Work Area provides the main area for managing the settings, controls and views of the selected node in the navigation pane. The contents of the work area vary according to the selected nodes in the navigation tree and the selected navigation buttons.

Actions

The Actions panel displays in the right-hand column and shows available controls for the current view.

Management Server

The Management Server manages communications with a Microsoft SQL database server for data access and storage, providing security control, communications for managing network discovery services and software deployment to managed computers, resource management and auditing.

- Management Server security manages network authorization for Management consoles and product consoles.
- Management Center handles download schedules, group management and file transfers, and network discovery services for integration with Active Directory.
- Auditing manages event data access and storage via the Management console alert rules which includes mechanisms for generating SNMP and SMTP alert notifications.
- Management Center supports a list of failover of servers which can take over the role of the Management Server to allow the system to continue functioning in the event of a hardware or environment failure.

For further information, see Server Configuration Portal Help.

Database

The Management Center relies on the availability on the network of a Microsoft SQL server for the storage and retrieval of DesktopNow software agents, configuration packages, license packages, and event and alert data.

The Microsoft SQL database server is administered by the Management Server and can be installed locally on the Management Server or on a separate server.

For more information about managing user permissions for the SQL database during installation and upgrades, see DesktopNow Install and Configure

SQL AlwaysOn

SQL Server AlwaysOn is the preferred SQL Server technology to support High Availability/Disaster Recovery screnarios and DesktopNow 10.x servers have been optimized to support this technology.

SQL mirroring is available for DesktopNow 10.1 FR1 customers who are currently in the process of transitioning to AlwaysOn technology. For more information see the DesktopNow Install and Configure Help.

Product Consoles

The DesktopNow product consoles, including Application Control, Environment Manager and Performance Manager, allow you to configure and save configurations to the Management Server's database for adding to deployment groups and deploying to managed computers.

For more information on the product consoles refer to the relevant product help system. All Help systems can be accessed from the Help Portal.

Deployment Agent

The Deployment Agent is installed on managed computers to manage communications between the product endpoint and the Management Center.

The Deployment Agent polls the Management Server to manage the download and installation of agents, configurations and software package updates, and also sends event data generated by the product agents to the Management Server.

The Deployment Agent can be downloaded and installed directly on managed computers from the Management Server web site or by using the Management Center console. You can specify the Access Credentials used by the Management Server. This must be done before you can install the Deployment Agent using the console. Other methods of installation are Active Directory group policy objects, or third-party deployment solutions such as Microsoft Systems Center Configuration Manager (SCCM).

Diagnostics

The Deployment Agent on managed computers runs a series of self-tests on first contact with the Management Server or when requested by the Management Server during a poll. Diagnostics can be enabled or disabled for any Management Server listed in the Failover Servers list.

Each failover server entry in the failover servers lists includes the Diagnostics Enabled check box option. The Management Server always requests a self-test when the Deployment Agent first polls due to a reboot or service restart.

All tests are run and an event, which indicates the test result, is raised in the Windows Event Log and sent to the Management Server. Each test contributes a success value to the results and, when tests fail, a detailed error report is also included in the event report. In the event of a test failure, the Management Console highlights, in red bold, the names of computers where the failure occurred and also highlights the deployment groups in the navigation pane containing computers on which the tests failed.

The Deployment Agent performs the following self-tests:

Connectivity

The connectivity test polls the Management Server. Any response, other than an HTTP 200 (Success) return value, indicates a failure and a detailed error message is returned. If this test fails, the results cannot be sent to the Management Server but can be viewed in the local Application Windows Event Log.

Package Download

This test downloads a file from the Management Server to the local hard disk, using BITS. Instead of downloading an MSI package, the test downloads a small XML file which can be easily validated and has a minimal impact on network bandwidth. The XML file is downloaded from the same directory as packages to ensure the same access rights affect both file types. Once the test is complete, the downloaded file is deleted.

Since BITS downloads can be delayed if the local computer is under heavy load, the download occurs within a new high priority BITS job, ensuring the test completes in a shorter time. A single BITS job is used to download files from all enabled failover URLs.

If any errors are reported during the download, the test fails. The description of the error is included in the test results.

Events Upload

This test attempts to upload an events file using BITS from the local hard disk to the Management Server. The events file contains no events to help minimize impact on network bandwidth, and is uploaded to the same directory as standard event uploads.

Since BITS uploads can be delayed if the local computer is under heavy load, the upload occurs within a new high priority BITS job ensuring the test completes in a shorter time.

If any errors are reported during the upload, the test fails. The description of the error is included in the test results.

This test only verifies that events can be sent from the Deployment Agent to the Management Server. No checks are made to ensure that the events can be uploaded to the database. When this fails, an event is added to the Management Server event log and raises a Management Center event, where possible.

Raising High Priority Events

The high priority events mechanism allows critical events to be sent to the Management Server database. A typical high priority event is the reporting of a failure to install packages. The test attempts a call by the Deployment Agent to the Management Server web page with an empty list of events. Any error values returned by the call are added to the self-test results.

Diagnostic failures are highlighted in red in the console. For example, a deployment group node and a corresponding problematic computer.

Change Default Ports

You can change the default port settings for communications with the Management Center after installation as follows:

1. In Internet Information Services (IIS) Manager:
    1. Select **Default Web Site > Edit Bindings** > **Site Bindings**
    2. Select the row which has a HTTP or HTTPS Type, click **Edit**.
    3. Change the TCP and SSL port settings according to requirements. Defaults are TCP:80 and SSL:443.
2. Change the port number in the URL path of Deployment Agents connecting to the Management Server, using one of the following methods:
    - Uninstall current Deployment Agents then reinstall on each target computer with the URL path specifying the new port number.
    - Add the NetBIOS name, the fully qualified domain name or the IP address with the new port number to the Failover Servers list and update currently installed Deployment Agents using the Install Deployment Agent functionality within the console.
    - Modify connectivity to the Management Server for the Management console and product consoles by editing the listed servers in the Select Management Server dialog box: http://<server name>:<port number>/ManagementServer

Prefix the address appropriately with HTTPS or HTTP depending on whether you are implementing the Management Center with SSL encryption and a valid certificate or in a workgroup environment without SSL.

Concurrency

Concurrency support ensures multiple users can connect to the Management Center simultaneously but not edit the same data simultaneously.

Users connecting with Management consoles are regulated by the principle that the first user to submit edits to a particular area are applied. Other users are notified that the settings have changed and the view is updated. However, multiple users can edit different data simultaneously. For example, a user editing the installation schedule, can submit changes at the same time another user submits changes to the group Membership settings.

Product consoles are regulated by a locking mechanism which ensures that the first user to access a configuration has exclusive editing control until the configuration is saved and unlocked. Other users can view the configuration while it is locked but not edit the data. When the configuration changes are saved and the configuration is unlocked, other users may attempt to access and edit the configuration.

Editing Management Center Settings

When different users compete to edit the same data in the Management console, the first to submit an edit is allowed, a notification is issued to the other users and the Management Console is refreshed.

Editing Product Configurations

Product configuration concurrency errors are prevented by a locking system which ensures that only one user can edit a configuration at any time. Product configurations can be unlocked when editing is finished to allow others users to modify the configuration.

When a configuration is locked, other users can only open the current saved version in read-only mode.

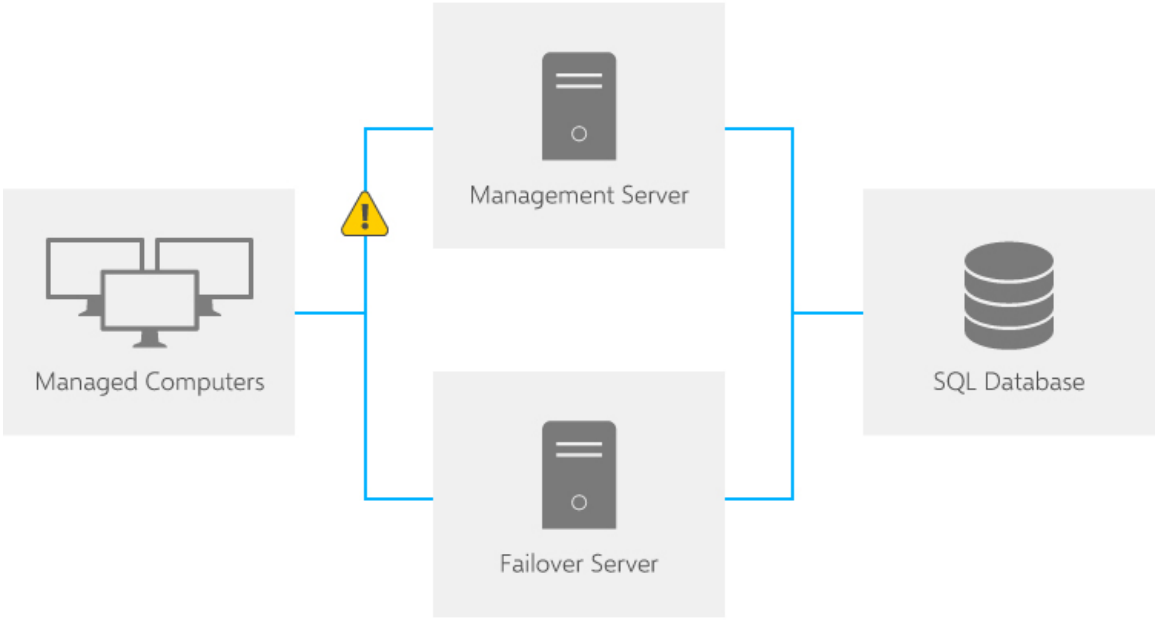
The locked status and details of the user who has locked the configuration display in both the Management console and in product consoles when editing a configuration.

Administrative users on the Management Center can override configurations which are locked by other users by resetting the lock. Select the **Packages** button in the navigation pane and then the **Configurations** node. Right-click a locked configuration and select **Undo Lock**.

Failover

The Management Center supports a list of failover servers which can take over the role of the Management Server to allow the system to continue functioning in the event of a hardware or environment failure. The primary Management Server and failover servers can use the same SQL database to ensure that existing data can be accessed at all times with any Management Server.

Failover in the Management Center provides support not only in the event of critical issues affecting the main Management Server but also to allow for system maintenance such as the decommissioning of a server or during a major upgrade or server overhaul.



Failover support ensures that the Deployment Agent on managed computers can maintain connectivity with alternative failover Management Servers, where the need arises, protecting data integrity and component communications.

Failover servers are maintained by the Management Center using the lists defined in the Management Console. The failover server lists are registered on managed computers via the Deployment Agent. The Deployment Agent can also register the Management Server URLs it uses, which are added to the list of failover servers in the Management Center. Each server is listed in order of priority.

In the event that the first listed Management Server is unavailable, the Deployment Agent attempts to connect with the next Management Server in the list until a connection is achieved.

The list of Management Servers can be managed both globally for all deployment groups or locally applying a unique list to each deployment group. A local list of Management Servers applied to a Deployment Group configuration overrides the global list.

Arranging Management Servers locally for each deployment group allows you to manage the Management Center infrastructure flexibly, for example by setting up servers geographically to conserve bandwidth or according to different connection types.

Management Center Security

The Ivanti Management Center powered by AppSense can be implemented in a secure distributed environment with Active Directory integration, Secure Socket Layers (SSL) for encrypted communications, authenticated Management Server and database connections.

Security Challenges

The security challenges for implementing the Management Center include:

- System integrity — Attempts to tamper with configuration and agent packages distributed to managed machines through the introduction of malware or modifications to software packages undermine the security policies which the management software is required to implement.
- Data confidentiality — Event and alert data is continuously relayed to the SQL database via the Management Server and could be vulnerable to the threat of access by unauthorized users.

Authentication and Authorization

Authentication using Active Directory integration ensures that Management Center and product software is only accessed or modified by authorized administrative users.

Connections from the Management Server to the database can be authenticated using Microsoft Windows authentication or Microsoft SQL authentication.

An appropriate certificate issued by a Certification Authority, following enterprise policy and procedure and installed on the Management Server, ensures the server can be validated before client connections are established. Client connections are from managed computers and computers hosting the Management Center console and product consoles.

Securing Communications using SSL

SSL provides confidentiality and integrity of communications to ensure sensitive data is accessible only by authorized users, including:

- Event data
- Agents and agent configuration data

If you are setting up SSL certificates on web servers using other supported operating systems and other versions of Microsoft SQL Server, see the following for further information: http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnnetsec/html/secnetht16.asp

Enable SSL Communications

SSL provides confidentiality and integrity of communications to ensure sensitive data is accessible only by authorized users, including:

- Event data
- Agents and agent configuration data

Set up Secure Socket Layers (SSL) for the Management Center, using a self-signed certificate.

You can run the Install Deployment Agent functionality within the console in small and medium scale enterprise environments to repair or modify the URL path for currently deployed Deployment Agents to change the http or https prefix and port number.

Setup SSL on IIS

1. In **Start** > **All Programs** > **Administrative Tools** > **Internet Information Services (IIS) Manager**, select the **<ServerName>** node and in the IIS section click **Server Certificates**.
2. Select **Create Self-Signed Certificate** in the Actions panel.
3. Provide a friendly name for the certificate and click **OK**.
4. Select the **Default Web Site** node and click **Edit Bindings** in the shortcut menu.
5. Click **Add** and in the Type drop-down list select **HTTPS**.
6. In the SSL Certificate drop-down list, select the friendly name of the certificate specified in step 3.
7. Click **OK** and Close.

Management Center Workflow

This section provides an overview of the steps to configure and set up Ivanti Management Center powered by AppSense. It includes the tasks required to setup Deployment Groups and push out Deployment Agents.

Step 1 Connect to the Management Server

1. Launch the Management console from **Start**> **All Programs**>**Ivanti**>**Management Center**.

   If you do not have a Management Server setup, or have more than one, the Select Management Server dialog displays.

2. Add or select the required server and click **Connect**.

   The Connect to Management Server dialog displays.

3. Select to connect as **Current User** or a **Custom User**.

   Select **Remember me** to automatically connect as this user in the future.

4. Click **OK**.

Step 2 Create and Configure Deployment Groups

To create a deployment group:

1. Select the **Home** button in the navigation pane.
2. Right-click the **Deployment Groups** node and select **New Deployment Group**.
3. Right-click the new node and select **Rename**. Give the node an intuitive name, for example, Terminal Servers UK.
4. Repeat the above steps for additional deployment groups, for example, Terminal Servers US.
5. Configure the following settings:
   - Server polling, downloads and uploads
   - Deployment Agent permissions
   - Agent and Configuration Installation schedules
   - Failover servers
   - Access credentials

Step 3 Setup Membership Rules

Membership rules determine which group a computer is assigned to. You can configure the rules by adding and excluding conditions for computers, groups and containers. Membership rules have a one to one relationship with deployment groups.

The **Discover** action places a computer into the first group that has a matching rule.

Rules are read in the order they are listed in the Membership Rules work area. You can use the **Move Up** and **Move Down** commands to order the rules.

1. Select the **Home** navigation button.
2. Select [**Server**] > **Deployment Groups** > [**Deployment Group**] > **Configure Membership Rules** button.

   The Membership Rules work area displays and lists all the deployment groups.
3. Select the deployment group in the list you want to add a condition to.
4. Select **Edit Conditions** in the Actions panel.

   The Edit Group Conditions dialog box displays.
5. Click **Add** and do one of the following:
   - Select **Computer by NetBIOS Name** and specify the NetBIOS name for the computer or browse to the computer.
   - Use **Active Directory** and select **Computer**, **Group** or **Containe**r and specify or browse to the Active Directory component.
6. Repeat to add additional conditions, if required and click **OK**.
7. Click **Submit** to submit the changes to the rule.

   Discovery takes place every five minutes. Click **Discover** to perform an immediate discovery of computers. You cannot configure this time within the console.
8. If required, expand the deployment group you have discovered computers for and select the Computers node.

   Details about the discovered computers display in the Computers work area.

Step 4 Setup Security (Optional)

The Management Center console installs with an Administrator account assigned to the user installing the software. This user is assigned a Server Administrator *server role* which gives full access and control to all areas and functions on the Management Server.

You can also add other user accounts and assign that server role or another of the default server roles, Modifier or Viewer. You can create custom server roles to which you can assign permissions from a comprehensive list.

You can also setup custom object roles which are used to setup security assignments in particular areas of the Management console. You can assign permissions to an object role to allow users to view, modify or delete objects in different areas of the console such as deployment groups, alert rules, packages or reports.

Object role access and control can be specified at a very granular level in some areas of the console allowing you to grant or restrict access either to a specific area such as a Deployment Group or to a particular object, such as a report or an alert rule.

1. Select the **Security** button in the navigation pane to setup security.
2. To view or edit the server permissions for a group or user expand the **Server Permissions** node.
3. Select either the **Groups** node or the **Users** node.

   The Groups or Users display in the All Groups/All Users work area.
4. To edit roles click a group or user, select the group or user and select **Edit Roles.**

   The Global Security Roles dialog box displays.
5. Allow or deny the roles and click **OK**.

Step 5 Set the Poll Period and Poll Variance

The poll period controls how frequently the Deployment Agent checks the Management Server for changes to the DesktopNow product agents, configurations and deployment groups. You can specify how often to poll.

You can also specify the upload event data period.

After you define a poll period and upload event data period you can include a poll variance to reduce the potential server load when multiple Deployment Agents are set to poll at the same time.

1. Navigate to **Deployment Groups** > [**Deployment Group**] > **Settings** > **General** tab.
2. Specify the server polling and downloads period. The period can be set between 1 minute and 7 days. The default is 1 hour with a default poll variance of 20%, that is +/-12 minutes.
3. Specify the event data uploads. The period can be set between 1 minute and 1 day. The default is 30 minutes with a default poll variance of 50%, that is +/-15 minutes.

If you intend on installing the Deployment Agent manually on end-point computers and not through the Management Center, the **Allow self-registration** option must be selected in the Deployment Agent Permissions section.

Step 6 Specify the Installation Schedule

The Installation Schedule controls how agent and configuration packages install. If you do not enable the installation, agents and configurations will not install or uninstall. You can choose to install immediately, on computer startup, or on a schedule.

1. Expand the **Deployment Groups** > [**Deployment Group**] > **Settings** node.
2. Select the **Installation** tab.

3. Set the **Agent and Configuration Installation Schedules** to one of the following:
    - **Disable -** Agents/Configurations do not install.
    - **Automatically at next client poll -** Agents/Configurations install when the computer next polls.
    - **Automatically scheduled** - Agents/Configurations install according to the specified schedule.
    - **At next system restart** - Agents/Configurations install on next restart.
4. Click **Submit**.

The installation schedule uses the local time of the endpoint.

Step 7 Assign Packages

Check the availability of packages in the Packages view. The Management Center installation loads the latest software into the database. Where appropriate, you can add existing packages such as configurations and earlier versions of the software agent packages which you have previously backed up in MSI file format prior to running the current installation.

Apply security access rights to packages to restrict or enable access and control.

Use the Packages view to view, add and remove agents and configurations, and to export configurations. Select the **Packages** button in the navigation pane to display all the available packages, that is, all the agents and configurations.

To assign a package to a deployment group.

1. Select the **Home** button.
2. Select **Deployment Groups** > **[Deployment Group]** > **Packages** node.
3. To submit a package for assignment to the deployment group, select the package and click **Submit**.
4. To assign the package, select the package and click **Assign**.

Caution: You must enable the installation schedule for the deployment group before you can install agents and configurations.

Step 8 Setup Alert Rules (Optional)

The Alerts view provides a comprehensive list of default alert rules which you can enable or disable. You can also create new alert rules by specifying combinations of the event ID, computer name and user name. Configure alert rule notifications using mail server details for e-mail and SNMP messages about critical events you wish to monitor.

1. Select the **Alerts** button in the navigation pane.
2. Expand the **Alert Rules** node.
3. Select and expand the rule you want to use in the navigation pane.
4. If required, click the **Criteria** node and specify criteria, for example, a user name.
5. Expand the **Actions** node and do one of the following:
    - To send email messages when the alert criteria is met, select the **SMTP** node, select **EnableSMTP** and specify the email settings in the SMTP configuration area.
    - To generate SNMP traps when the alert rule criteria is met, select the **SNMP** node and select **Enable SNMP**.

Step 9 Setup Auditing (Optional)

Use Auditing to specify which events client computers send to the Management Server for each product agent. You can also specify to display computer and user names anonymously.

Events can be generated by:

- Application Control
- Environment Manager
- Performance Manager
- Management Center

1. Select the **Home** button in the navigation pane.
2. Expand the **Deployment Groups** > **[Deployment Group]** > **Settings** node.
3. Select the **Auditing** tab.

   The Auditing work area displays.
4. To display computer names anonymously, select **Always use anonymous MACHINE names in events**.
5. To display user names anonymously, select **Always use anonymous USER names in events**.
6. In the Event Filter expand the product name that you want to enable events for.
7. Select the **Enabled** column for the required events.

Step 10 Setup Access Credentials

Before you can install the Deployment Agent on any endpoint, Access Credentials must be supplied. The list of credentials are used by the Management Server to install the Deployment Agent when chosen by the user. You can add multiple users to the list and they are attempted in the order defined in the Access Credentials work area.

Access Credentials configured from the top level tree view apply to all Deployment Groups by default, unless specific credentials have been defined within a specific Deployment Group. In this case, the Deployment Group's Access Credentials precede the default credentials.

You can create default Access Credentials and credentials specific to a deployment group.

Global Access Credentials

1. Select the **Home** button in the navigation pane.
2. Select the **Global Settings** node.
3. Select the **Access Credentials** tab.
4. The Access Credentials work area displays.
5. Do one or more of the following:
    - To add a credential enter the User name and Password and select **Add**.
    - To remove a credential, highlight the required credential and select **Remove**.
    - To order credentials in the list highlight the required credential and select **Move Up** and **Move Down**.

Access Credentials for Deployment Groups

1. Select the **Home** button in the navigation pane.
2. Navigate to **Deployments Groups** > [**Deployment Group**].
3. In the Details section in the work area select the **Manage Credentials** button.

   The Manage Credentials dialog displays.
4. Do one or more of the following:
    - To add a credential enter a User name and Password and select **Add**.
    - To add the credentials to the global default list select **Add to Global Credentials**.
    - To remove a credential, highlight the required credential and select **Remove**.
    - To order credentials in the list highlight the required credential and select **Move Up** and **Move Down**.

Step 11 Install the Deployment Agent on Managed Computers

The Deployment Agent can be installed on client computers using any of the following methods.

- Before you can install the Deployment Agent you must setup the Access Credentials.
- 64-bit Deployment Agent packages can only install on 64-bit operating systems. 32-bit Deployment Agent packages can only install on 32-bit operating systems.

1. Download the Deployment Agent installation package from the Management Server website and run the installation package on the client computer.
2. The Deployment Agent can be installed manually by running the installation package or silently using a command line prompt.
3. Deploy the Deployment Agent to multiple client computers using the Install Deployment Agent functionality within the console or other third-party deployment mechanisms, such as Microsoft System Management Server, depending on the scale of deployment required.

Install using the Install Deployment Agent Functionality

1. Expand the **Deployment Groups** > **[Deployment Group]** nodes.
2. Select the **Computers** node.
3. All the computers within the deployment group display.
4. Select one or more of the computers and click **Install Deployment Agent** in the Actions panel.

The Client Access Log provides details on the installation process and the Deployed (%) column indicates the percentage of the package deployed.

Once the Deployment Agent is installed, the service registers with the Management Server at the website address you supplied during installation. After the Deployment Agent downloads the deployment group settings, the service implements the policies to install software, generate events and poll the server for further changes and package updates. The Deployment Agent regularly polls the server for updates and changes to the deployment policy, according to the deployment group settings.

Ensure that you provide a valid Management Server URL and prefix the address appropriately with HTTPS or HTTP depending on whether you are implementing the Management Center with SSL encryption and a valid certificate or in a workgroup environment without SSL.

Step 12 Install and Configure Failover Servers (Optional)

Failover Servers provide a list of alternate Management Servers to which the Deployment Agent can connect to. In the event of a connection failure the Deployment Agent attempts to connect to the next available server in the list. Management Servers are listed in order of priority, starting with the first in the list.

The Failover Servers list is automatically populated with the URLs that the Deployment Agents use to connect to the Management Server.

Install additional Management Servers and select to use the existing SQL Server name and database name. After installation, add the URL of the failover server to the list of servers in the Management Center console.

You can specify default failover servers and failover servers specific to a deployment group. Failover servers assigned to a particular deployment group can override the default failover servers.

For more information about installing the Management Server, see the DesktopNow Install and Configure Guide.

Default Failover Servers

1. Select the **Home** button in the navigation pane.
2. Select the **Global Settings** node > **Failover Servers** tab.
3. Do one of more of the following:
    - To add a server, select **Add Server**in the Actions panel.
    - The Add Failover Server dialog box displays. Specify the server you want to add.
    - To remove a server, highlight the required server in the list and select **Remove Servers** in the Actions panel.
    - To order existing servers, select **Move Up** and **Move Down**in the Actions panel.
    - To test a server connection, select **Test Server Connection**in the Actions panel.

      A message displays to confirm connection.

Deployment Group Failover Servers

1. Select the **Home** navigation button.
2. Expand the **Deployments Groups** > **[Deployment Group]** > **Settings** nodes.
3. Select the **Custom Failover Servers** tab.
4. Do one or more of the following:
    - To add a server, select **Add Server**in the Actions panel. The Add Failover Server dialog box displays. Specify the server you want to add.
    - To remove a server, highlight the server in the list and select **Remove Servers**.
    - To order existing servers, select **Move Up** and **Move Down**.
    - To test a server connection, select **Test Server Connection**. A message displays to confirm connection.
    - To override the default list of failover servers, select the **Override Default Failover Servers** option. The deployment group list of failover servers overrides the default servers for all Deployment Agents in the current deployment group.
    - To manage the default list of servers, select **Manage Default Failover Servers**.

Deployment Agent

The Deployment Agent is a software agent that must be deployed to all clients managed by the Management Center. The Deployment Agent runs as a Windows Service and performs tasks on the client when instructed by the Management Server. These tasks include the installation, upgrade and uninstall of DesktopNow agents and configurations and the collection and uploading of auditing information from any DesktopNow product agent.

The Deployment Agent polls the Management Servers periodically as determined by the poll period of the deployment group of which it is a member. Membership of a deployment group is determined by the set of membership rules as defined within the Management Console. During each poll, the Deployment Agent asks the Management Server which agents, configurations and prerequisites should be installed on the client, and which auditing events should be collected. The Deployment Agent uses this information to ensure only the correct set of agents and configurations are installed on the client and to filter the events collected by the DesktopNow product agents. The Deployment Agent periodically uploads all collected events to the Management Server.

Access Credentials

The Access Credentials are used to specify a list of credentials used by the Management Server to install the Deployment Agent.

These credentials must be supplied before attempting to install the Deployment Agent on any endpoint via the Management Console.

Configuration of these credentials can be setup globally for the Management Server in **Home** > **Global Settings** > **Access Credentials** tab or per Deployment Group in **Home** > **Deployment Groups** > [**Deployment Group**] > **Details** section > **Manage Credentials** button.

Access Credentials configured through Global Settings apply to all Deployment Groups by default, unless specific credentials have been defined within a specific Deployment Group. In this case, the Deployment Group's Access Credentials precede the default global credentials.

Caution: You will not be able to install the Deployment Agent on any endpoint using the integrated Install Deployment Agent functionality if the credentials have not been set up.

To add Access Credentials, enter a user name and password. These credentials are stored in the database. The Server Configuration Portal (SCP) creates an RSA public-private key pair that is stored in the Microsoft Cryptographic Provider of the server. This key is used to encrypt and decrypt the credentials stored in the database and therefore secures the information.

On attempting to install the Deployment Agent, the credentials supplied are tried in the order defined in the list. These credentials can be ordered by making use of the **Move Up** and **Move Down** options in the **Actions** panel.

Deployment Agent Communication with the Management Server

When communicating with the Management Server, the Deployment Agent will make use of the designated Client Authentication model as specified in the Management Server Configuration Utility during installation of the Management Server. This makes use of either Anonymous or Windows Authentication.

When Anonymous authentication is selected, the Deployment Agent communicates with the Management Server using a specific account designated for anonymous access, IUSR_[server name].

All interactions with the Management Server then inherit the permissions assigned to this account.

When Windows authentication is used, the computer credentials are used to communicate with the Management Server. An issue may occur resulting with the following message being displayed:

```
Unable to access the Master Key on the server, error was Keyset does not exist.
```

This is caused by the service accounts being unable to access the decryption certificate stored on the Management Server. To resolve this issue, any identities that are used by the services of Management Center must be granted sufficient permission to access the key store. This is achieved by using the following command line:

```
aspnet_regiis.exe -pa AppSenseMasterKey <DOMAIN>\<USERNAME>
```

Deployment Agent Registering with the Management Server

Once the Deployment Agent has been installed successfully, the Deployment Agent service registers with the Management Server.

There are a number of ways in which the Deployment Agent can register with the Management Server:

- Deployment Agent is installed directly via the Install Deployment Agent option within the Management Console, it will automatically register with the Management Server.
- Deployment Agent is installed manually using the ClientCommunicationsAgent.msi file as downloaded from the Management Server website, a valid Management Server must be supplied to allow the Deployment Agent to communicate and register with the Management Server.
- Deployment Agent is installed manually from the command line including a valid Management Server URL and optionally, a specific Deployment Group with which to self-register.

The Deployment Agent can only self-register if Allow self-registration is selected in **Home** > **Deployment Groups** > [**Deployment Group**] > **Settings** > **General** tab > **Deployment Agent Permissions**.

If a Deployment Group is not specified during the installation process or the relevant group does not allow the Deployment Agents to self-register, then the Management Server searches the membership rules, if a match is found the computer is placed in the group. If no match is found then the computer is placed in the catch-all (Default) Deployment Group.

After the Deployment Agent registers with the server, the Deployment Agent service implements the policies to install software, generate events and poll the server for further changes and package updates.

All available agent, configuration and prerequisite packages are stored within the Management Server database, which is populated by the Management Server installation procedure.

A list of assigned packages, configured for the specific deployment group is downloaded by the Deployment Agent on the managed endpoint device from the Management Server. This list is then compared with what is installed on the endpoint.

If this list of assigned packages differs from what is installed on the endpoint, the required packages are downloaded from the Management Server. Computer restart is co-ordinated according to the installation schedule settings as specified on the relevant deployment group. Packages are then installed on either computer shutdown or restart depending on the deployment group installation settings. Configurations and deployed Deployment Agent upgrades can be installed mid-session without a reboot depending on the deployment

group settings.

Installing the Deployment Agent

The Deployment Agent must be installed on all endpoints to be managed by Management Center. The Deployment Agent can be distributed using the integrated Install Deployment Agent functionality within the Management Console, by downloading the ClientCommunicationsAgent.msi package from the Management Server web site or by third-party deployment mechanisms.

Prerequisites

The following are prerequisites for all computers to allow Deployment Agent installation:

- Allow File and Print Sharing in the Firewall settings.

  The default Windows File and Print share exception opens up the following ports:

  - NetBIOS - TCP 139, UDP 137, UDP 138
  - LLMNR - TCP 5255, UDP 5355
  - SMB - TCP 445
  - RPC - TCP 135, TCP 445, UDP 445
- Access to ADMIN$ share and IPC$ share.

- Access to the Service Control Manager (SCM) with the following rights:
  - Create a service (SC_MANAGER_CREATE_SERVICE)
  - Query service status (SERVICE_QUERY_STATUS)
  - Service all access (SERVICE_ALL_ACCESS)
  - Service stop (SERVICE_STOP)
  - Service start (SERVICE_START)
  - Service delete (DELETE)
- Windows Installer service running.
- Server service running.

We recommend setting up deployment groups and configuring settings in the Management Console before installing the Deployment Agent.

You can run the Install Deployment Agent functionality in small and medium scale enterprise environments to deploy the Deployment Agent to multiple computers, or to repair or modify the URL path for currently deployed agents to change the http or https prefix and port number. The Install Deployment Group functionality is available in **Home** > [**Server**] > **Deployment Groups** > [**Deployment Group**] > **Computers**.

The IT administrators in organizations often create master images which include the operating system with all the required software and updates required for a new computer, as a labor saving approach to setting up multiple computers. It is recommended to install the Deployment Agent on a gold image prior to rolling out to computers in your organization.

Integrated Install Deployment Agent Functionality

The Management Console provides an **Install Deployment Agent** function which allows you to deploy the Deployment Agent to multiple computers which match the Management Center Deployment Group and Membership Rules. The Deployment Agent can be deployed either on a Microsoft Active Directory network or in a Microsoft Windows Workgroup in small or medium scale environments.

The software requirements for the target client computers are detected and the 32-bit or 64- bit version of the Deployment Agent, assigned to the deployment group of which the computer is a member, is downloaded. If no version of the Deployment Agent is assigned to the group then the latest version is downloaded.

Deployment Agents are copied to the target computers and installed silently, along with the correct URL of the Management Server.

The basic steps required to install the Deployment Agent are as follows:

Step 1 - Deployment Group

Home > [**Server**] > **Deployment Groups**

1. Create a Deployment Group.
2. Configure the polling settings in **Deployment Group** > **Settings** > **General** tab - Polling is where the Deployment Agent on the endpoint initiates communication with the Management Server. The poll period is split into the following:
    - Server Polling and Downloads - Deployment Agent downloads updates to the deployment groups and agent and configuration packages.
        - Poll variance - reduces the impact of multiple machines polling the Management Server at any one time.
    - Event Data Uploads - Deployment Agent uploads event data to the Management Server.
        - Poll variance - reduces the impact of multiple machines polling the Management Server at any one time.
3. Setup the agent and configuration installation schedules in the Installation tab.

A warning displays in Deployment Groups > [Deployment Group] > Computers if an installation schedule is set to Disable.

Step 2 - Membership Rules

Home > [**Server**] > **Membership Rules**

Every Deployment Group has a one to one relationship with a set of Membership Rules. The Membership Rules act like a filter to discover computers within Active Directory.

1. Highlight a Deployment Group, select **Edit Conditions** to add a new condition based on NetBIOS Name or Active Directory. Click **OK**.
2. Select **Submit** from the Membership Rules work area.
3. Select **Discover** from the Actions panel.
4. The discovered computers that match the Membership Rules are listed in the relevant **Deployment Group** > **Computers** node.

For the computers discovered by Membership Rules the Computer Status should initially display: No Deployment Agent deployed.

Step 3 - Access Credentials

Custom - **Home** > [**Server**] > **Deployment Groups** > [**Deployment Group**] > **Details** section > **Manage Credentials** button

or

Global - **Home** > [**Server**] > **Global Settings** > **Access Credentials** tab

Enter the user credentials; user name and password, for an account which has local administrator privileges on the endpoint that the Deployment Agent is being installed.

You can add multiple accounts, they will be attempted in order of the list.

Caution: You will not be able to install the Deployment Agent on any endpoint using the integrated Install Deployment Agent functionality if the credentials have not been set up.

Step 4 - Install Deployment Agent

Home > [**Server**] > **Deployment Groups** > [**Deployment Group**] > **Computers**

1. Select the computer or computers on which you want to install the Deployment Agent.
2. Select **Install Deployment Agent** from the Actions panel.

   The Client Access Log provides details on the installation progress. The Deployed (%) column indicates the percentage of all the packages assigned to the group that have been deployed.

If the computer is in a Workgroup you must make sure that Anonymous authentication is selected as the client authentication method in the SCU.

Install the Deployment Agent using an Installation Schedule

You can deploy the Deployment Agent assigned to a group to the computers listed in the Computers page using an installation schedule.

The Deployment Agent can be deployed either on a Microsoft Active Directory network or, in small or medium scale environments, in a Microsoft Windows Workgroup.

The Management Center uses group membership rules to create a list of computers to which it can deploy the Deployment Agent. Active Directory is queried for active directory types for membership rules by computers, groups and containers. Alternatively, you can manually include or exclude computers from the list by NetBIOS Name.

You must specify Access Credentials before installing the Deployment Agent.

Management Center deploys the Deployment Agent installation package that has been assigned to the group. If you did not assign a Deployment Agent installation package, Management Center detects the latest available version for the target computers and downloads the 32-bit or 64-bit version as required.

Deployment Agents are installed silently, along with the correct URL of the Management Server.

To install the Deployment Agent using the Install Deployment Agent Functionality:

1. Select the **Home** navigation button.
2. Expand [**Server**] > **Deployment Groups** > [**Deployment Group**] > **Settings** > **Installation** tab.
3. Setup the Installation schedule.
4. Navigate to **Deployment Groups** > [**Deployment Group**] > **Computers**.
5. Select the computer you want to deploy to and select **Install Deployment Agent** from the Actions panel.
6. You can review installation feedback on the **Client Access Log** tab in the work area.

A warning displays in **Deployment Groups** > **[Deployment Group]** > **Computers** if the installation schedule is set to **Disable.**

After the Deployment Agent is installed it registers with the Management Server. After registering, the deployment agent implements the policies to install software, generate events and poll the server for further changes and package updates. The Deployment Agent regularly polls the server for updates and changes to the deployment policy, according to the deployment group settings.

Install the Deployment Agent Manually

You can manually install the Deployment Agent on a managed computer by downloading and running the Deployment Agent installation package on a client computer.

1. Launch a web browser such as Microsoft Internet Explorer and navigate to the Management Server web site at the following address: *http://<computer name>/ManagementServer*

   If you have configured SSL communications, use the HTTPS prefix for the Management Server web site: *https://<computer name>/ManagementServer/*

   The Management Center download page displays where you can download the Deployment Agent, product consoles, release notes and components which are prerequisites for installing DesktopNow.

2. Download and run the appropriate 32-bit or 64-bit Deployment Agent installation MSI package.

   Make a note of the Management Server URL displayed in the download page.
   From the website you can also download the Management Console, EULA, release notes, Application Control, Environment Manager and Performance Manager consoles, and prerequisites software.

3. In the Deployment Agent installation Welcome screen, click **Next**.
4. Accept the End User License Agreement and click **Next**.
5. Leave the default installation directory unchanged, and click **Next**.

6. The Deployment Agent Settings screen displays: Enter the Management Server computer name, *http://<Computer Name>:Port Number/*.

   If you have configured SSL communications, use the HTTPS prefix for the Management Server web site: *https://<computer name>:Port Number/*

7. Click **Next** to proceed.
8. When the installation is complete, click **Finish** to exit the installation wizard.

You have now successfully installed the Deployment Agent. The host computer is able to connect to your Management Server ready to download product Agents, license and configuration software packages according to the settings configured for the deployment group to which the current computer belongs.

Install the Deployment Agent in Silent Mode

You can install the Deployment Agent silently via a third-party deployment mechanism using the command line prompt.

```
msiexec.exe /qn /i "<MSI file path>\ClientCommunicationsAgent.msi" WEB_SITE="http://<Management Server Name>:Port Number" GROUP_NAME="<DeploymentGroup>"
```

Use the HTTPS prefix for the Management Server web site only if you intend to install an SSL certificate on the server computer and managed computers are located in the same Active Directory domain as the Management Server.

- /i - Install
- /qn — Quiet mode install without the user interface.
- WEB_SITE — Enter the Management Server web site address using the name of the host computer.
- GROUP_NAME — (Optional) Enter the Deployment Group name to which the Deployment Agent should register. The Deployment Agent can only register with a group which is set up to allow the Deployment Agent to self-register. Otherwise, the Deployment Agent attempts to register with the Management Server deployment groups according to group membership precedence:
  - GROUP_NAME self-register
  - Deployment Groups - membership rules
  - (Default)Group – if no match is found

Configuring the Deployment Agent

Allow Deployment Agent to Self Register with a Deployment Group

You can set up a deployment group to allow the Deployment Agent to self-register with a specific group. This option is disabled by default but provides an alternative method for installing Deployment Agents on managed computers to register with a specific deployment group on the Management Center rather than predefining the group membership in the Management Console.

1. Select the **Home** button in the navigation pane.
2. Expand the **[Server]** > **Deployment Groups** > **[Deployment Group]** node.
3. Select the **Settings** node.
4. Select the **General** tab.
5. Select the **Allow self-registration** option.

Any user can now choose during Deployment Agent installation for the computer to join the deployment group.

Allow Deployment Agent to Unregister from a Deployment Group

You can set up a deployment group to allow a local administrator to request the Deployment Agent unregisters computers from a specific group. This option is disabled by default.

1. Select the **Home** button in the navigation pane.
2. Expand the **[Server]** > **Deployment Groups** > **[Deployment Group]** node.
3. Select the **Settings** node.
4. Select the **General** tab.
5. Select the **Allow unregistration** option.

An administrator can now command the Deployment Agent to unregister computers from this deployment group.

Allow Deployment Agent Initiate Updates

You can set up a deployment group to allow a local administrator to request the Deployment Agent initiates updates of agents and configurations outside of any installation schedule that is set up. This option is disabled by default.

1. Select the **Home** button in the navigation pane.
2. Expand the **[Server]** > **Deployment Groups** > **[Deployment Group]** node.
3. Select the **Settings** node.

4. Select the **General** tab.
5. Select the **Allow update initiation** option.

An administrator can now command the Deployment Agent to immediately install or uninstall packages for this deployment group regardless of the installation schedule.

CCA Command Tool

The CCA Command tool, CcaCmd.exe, allows an administrator to configure the Deployment Agent from an endpoint giving an advanced level of control over the Deployment Agent and its behavior.

Administrators may use it to prepare a master image for provisioning. The commands can be run individually or in a batch file as part of an existing provisioning script.

Before Using the CCA Command Tool

Before you can use CcaCmd.exe the following conditions must be met:

1. ClientCommunicationsAgent.msi installed on the endpoint.
2. The following permissions must be enabled in **Home** > [**Server**] > **Deployment Groups** > [**Deployment Group**] > **Settings** > **Deployment Agent Permissions**:
    - **Allow self-registration** - maps to CCA Command tool switch /URL
    - **Allow unregistration** - maps to CCA Command tool switch /UNREGISTER and /IMAGEPREP
    - **Allow update initiation** - maps to CCA Command tool switch /UPDATEAGENTS and /UPDATECONFIGS
3. You must be a member of the local administrators group and running with an elevated token.

Using the CCA Command Tool

The CcaCmd.exe commands are as follows:

Command	Description
/url	Changes the url used to communicate with the Management Server. You can optionally include a Deployment Group with which to self register. This requires **Allow self-registration** to be enabled in the Deployment Group Settings.
/imageprep	Prepares this computer for provisioning, the computer will be registered on the next poll. This command can be combined with the /unregister command.

Command	Description
	When running /imageprep, the Deployment Agent will automatically **Check for and download new Configurations at Startup** regardless of the Deployment Group Settings.
/unregister	Unregisters the Deployment Agent from the Management Server and stops the Deployment Agent service. Does not uninstall any DesktopNow agents or configurations. This requires **Allow unregistration** to be enabled in the Deployment Group Settings. Once a computer has been unregistered the Deployment Agent Service must be restarted for the computer to re-register.
/updateagents	Initiates install of agents assigned to the Deployment Group, overriding the Installation Schedule. This requires **Allow update initiation** to be enabled in the Deployment Group Settings. A system restart is triggered if requested by the installer. The system restart can be suppressed by supplying the /suppressreboot option. The updating of agents is asynchronous. Use /isupdating to check if the Deployment Agent is still applying updates.
/updateconfigs	Initiates install of configurations assigned to the Deployment Group, overriding the Installation Schedule. This requires **Allow update initiation** to be enabled in the Deployment Group Settings. The updating of configurations is asynchronous. Use /isupdating to check if the Deployment Agent is still applying updates.
/isupdating	Determines whether a previous call to /updateagents or /updateconfigs is still processing updates.

Deployment Agent Diagnostics

Diagnostics provide the administrator with an overall view of the health of the Deployment Agent in terms of the relationship and communication with the Management Server.

Diagnostics can be enabled or disabled for each Management Server from the **Home** > **Deployment Groups** > **Global Settings** > **Failover Servers** tab by selecting the Diagnostics Enabled option next to the relevant Management Server. This option is disabled by default.

When the **Diagnostics Enabled** option is selected, the Deployment Agent on managed endpoint devices runs a series of self-tests on first contact with the Management Server or when requested by the Management Server during a poll.

Additionally, to perform a manual diagnostics test select the **Request Diagnostics** option from the Actions panel available from the All Computers node.

An event which indicates the test result, is raised in the Windows Event Log on the managed endpoint device and sent to the Management Server.

Each test provides a success or failure result and, where a test fails, a detailed error report is included in the event report.

In the event of a test failure the Management Console highlights, in red, the names of the computers where the failure occurred and also highlights the deployment groups in the navigation pane containing computers on which the tests failed.

There are four specific tests that are run when diagnostics are requested:

Connectivity

The connectivity test involves the Deployment Agent attempting to poll the Management Server. Any response, other than an HTTP 200 (Success) return value, indicates a failure and a detailed error message is returned. If this test fails, the results cannot be sent to the Management Server (as there is no connectivity) but can be viewed in the local Application Windows Event Log on the endpoint device.

Download of Packages

This test downloads a sample file from the Management Server to the local hard disk of the endpoint device, using the Background Intelligent Transfer Service (BITS).

Instead of downloading a full MSI package, the Deployment Agent downloads a small XML file which can be easily validated and has a minimal impact on network bandwidth. The XML file is downloaded from the same directory as standard MSI packages to ensure the same access rights affect both file types. Once the test is complete, the downloaded file is deleted.

Since BITS downloads can be delayed if the local computer is under heavy load, the download occurs within a new high priority BITS job, ensuring the test completes in a shorter time. A single BITS job is used to download files from all enabled failover URLs.

If any errors are reported during the download, the test fails. A description of the error is included in the test results.

High Priority Events

The high priority events diagnostics test allows critical events to be sent to the Management Server database from the managed endpoint device. A typical high priority event is the reporting of a failure to install packages. The test attempts a call by the Deployment Agent from the managed endpoint to the Management Server with an empty list of events. Any error values returned by the call are added to the results.

Upload of Events

The diagnostics test attempts to upload an events file using BITS from the local hard disk on the endpoint device to the Management Server. The events file is empty so as to help minimize impact on network bandwidth, and is uploaded to the same directory on the Management Server as standard event uploads.

```
%\ProgramFiles%\AppSense\ManagementCenter\Server\WebSite\Deployment\Events
```

Since BITS uploads can be delayed if the local computer is under heavy load, the upload occurs within a new high priority BITS job ensuring the test completes in a shorter time.

If any errors are reported during the upload, the test fails. The description of the error is included in the test results.

This test only verifies that events can be sent from the Deployment Agent on the managed endpoint device to the Management Server. No checks are made to ensure that the events can be uploaded to the database. When this fails, an event is added to the Management Server event log and raises a Management Center event, where possible.

The Computers view within a specific Deployment Group provides a Diagnostic State which indicates the current state of the diagnostics taking place on the endpoint device.

There are four diagnostics states including:

- Untested
- Pending
- Requested
- Completed

The diagnostics test results are reported to the Management Server and displayed in the Diagnostics tab in the Management Panel area of the Computers view within the relevant deployment group, including a breakdown of the test type and the result of each test.

Licensing

Management Center enables you to manage individual DesktopNow product licenses, and full suite licenses for computers across your Enterprise. Product licenses are managed using the DesktopNow Licensing console when the Management Center is not being used.

Licensing allows you to:

- Add licenses for DesktopNow products.
- Import and export licenses in MSI file format.

License Agreement

License details are included in the License Agreement which is issued when an order for DesktopNow software has been completed.

The License Agreement includes the following information:

Product, Feature, and Version Details

- Issue Date
- Expiry Date
- Customer Name
- Serial ID

Together with the license agreement you will receive either a TXT file or a LIC file. Use file to add or import the license.

If a product license or an evaluation license expires you will receive limited or no functionality on the endpoint. An Event is raised for each unlicensed product.

Managing Licenses

The following procedures describe how to add a license and import or export a license.

Add a License

1. In the Management Console, select the **Home** navigation button.
2. Select the **Licensing** node.
3. In the Actions panel click **Add License.**

   The Add License Key dialog displays.

4. Enter the license key and click **Add**.

   If you received a TXT file from Ivanti, open the file and copy the license key, paste it in to the Add License Key dialog.

   If you received a LIC file from Ivanti, refer to the Import a License File section.

   Details of the license are displayed in the console and the license key is added to the following location: %ALLUSERSPROFILE%\AppSense\Licenses

5. Some license types may need activating. Click **Activate License,** enter the activation code and click **Enter**.

   Once a license is active the icon changes to indicate the current license state.

6. Any product license added to the Management Center, is automatically deployed to the managed endpoint at time of polling. Managed endpoints are any devices which have the Deployment Agent installed.

   The endpoint automatically uses the first valid license if finds. You do not have to assign a particular license to a particular group or endpoint.

Import a License File

1. In the Management Console, select the **Home** navigation button.
2. Select the **Licensing** node.
3. In the Actions panel, click **Import Licenses.**

   The Open dialog displays.

4. Select the required license LIC file.
5. Click **Open**.

   Details of the license are displayed in the console and the license key is added to the following location: %ALLUSERSPROFILE%\AppSense\Licenses

Export a License File

Export licenses to MSI or LIC file format for saving to other computers which can be remotely accessed.

1. In the Management Console, select the **Home** navigation button.
2. Select the **Licensing** node.
3. In the Actions panel, click **Export Licenses**.

   The Save As dialog displays.

4. Browse to the required location, provide a name for the file and click **Save** to save the file.

Patching

Ivanti DesktopNow powered by AppSense products can be patched using a Windows Installer patch (MSP file). A patch is an MSP file which, when installed, updates files and registry keys on an existing installed product. Installing an MSP can reduce system downtime as reboots are not always required. DesktopNow product patching gives all of the usual benefits associated with Windows Installer Patching, including ease of deployment and the ability to rollback to an earlier version.

Patch Distribution

- **Public Hotfix** - Issued publicly on myAppSense to address a widely reported issue and should only be installed to address the specific problem. Public Hotfixes are cumulative in that they contain all previous Private and Public Hotfixes. Public Hotfixes are distributed as an MSP.
- **Service Pack** - Contains all of the fixes from the last Private or Public Hotfix and any previous Service Packs, plus any fixes that have been found for which a Private or Public Hotfix was not issued. Service Packs are distributed as an MSP.

Installing Patches Using the Management Center

To install a patch using Management Center you must first upload the MSP and then assign it to a deployment group for deployment to the endpoints.

Upload an MSP

1. Open the Management Console and in the navigation pane select the **Packages** navigation button.
2. Click on the required product, for example Environment Manager. The package library for the selected product displays in the work area.
3. From the Actions panel, select **Add Package**.

   The Browse for Package dialog displays.
4. Locate the required MSP file and click **Open**.

   The base MSI package for the selected patch must have previously been uploaded.
5. The Package Upload wizard displays.
6. Check the details of the selected package and optionally enter a description.
7. Click **Next** to start the upload.
8. When the upload has competed successfully click **Finish**.

   The MSP can now be seen in the package library.

Deploy an MSP to an endpoint

1. In the Management Console navigate to: **Home** > **Deployment Groups** > [**Deployment Group**] > **Packages**.

   The Packages work area displays a list of DesktopNow products and the associated packages.

2. Highlight the required product package and from the Actions panel select **Change Agent Version**.

   A dialog to change the packages used by the group displays.

3. Select the required patch package. For example, 8.6 SP2 HF3

4. Click **Finish**.

   The packages list updates.

5. Once all changes have been made, from the bottom of the work area, click **Review and Submit**.

   The Submit Changes for [Deployment Group] dialog displays.

6. Review the changes to be made to the deployment groups and click **Submit**.

   A warning may display informing you that changes to an agent can cause reboots at the times defined by the installation schedule.

7. If the warning message displays, click **Yes** to assign the changes. Alternatively, click **Submit** to assign the changes.
8. The patch deploys to the deployment group computers according to the Installation Schedule.

Installing and Uninstalling Patches Using the Command-Line

DesktopNow patches can be installed from the command-line as well as from the Management Center.

It is recommended that Logging is switched on when using the following commands.
To enable Logging add `/l*vx Patch.log` immediately after the `/i` or `/p`.
For example: `msiexec.exe /i /l*vx Patch.log Agent.msi`

Install an MSP

To install an MSP type the following command:

```
msiexec.exe /p Agent.msp
```

Do not use `/update` when installing the MSP file as this will remove all existing features.

Install an MSI and MSP

To install an MSI and MSP in a single operation type the following command:

```
msiexec.exe /i Agent.msi PATCH=C:\FullPath\Agent.msp
```

Uninstall an MSP

To uninstall an MSP type the following command:

```
msiexec.exe /i Agent.msi MSIPATCHREMOVE=C:\FullPath\Agent.msp
```

Uninstall an MSI and MSP

To uninstall an MSI and MSP type the following command:

```
msiexec.exe /x Agent.msi
```

This uninstalls all associated MSP files.

Rolling-Back Patches

Using Management Center to install patches, provides additional advantages such as the facility to downgrade newer versions of MSI files as well as removing MSP files to apply previous versions. To roll back to an older patch, just reassign the older version to the deployment group.

Home

Connect to the Management Server

Connect the Management console and Product consoles to the Management Server using the Select Management Server dialog box.

You can add, edit and delete listed servers. When adding or editing a server, provide the friendly name, enter a server name or IP address and provide the connection type (HTTP, HTTPS) and port number. You can also browse the network or Active Directory to select a server.

When connecting, you are prompted for credentials using the current user account or a custom user for which you need to provide name, password and domain.

In the product consoles, you connect to the Management Server when attempting to open a live configuration on a remote computer or when saving a configuration.

Select Management Server

The Select Management Server dialog displays when you select **Home** > [**Server**] > **Actions** panel > **Connect...**.

The dialog allows you to connect to a Management Server and maintain the list of Management Servers with which you regularly connect.

Settings

- **New Server** – Click to add a server to the list by providing details in the Add Server dialog box, including friendly name, server name (computer name or IP address), connection type and port number (HTTP/80, HTTPS/443).
- **Edit Server** – Click to edit a listed server by providing details in the Edit Server dialog box, including, friendly name, server name (computer name or IP address), connection type and port number (HTTP/80, HTTPS/443).
- **Delete Server** – Remove the highlighted server from the list.
- **Remove Cached Credentials** - Select to delete any cached connection credentials.

The Management Server dialog prompts you to provide credentials for connecting to the selected server either using the currently connected user account or a custom user. You can browse for a user on the active directory or local network, provide a password and, where appropriate, the domain.

If **Remember me** is selected the credentials are cached.

Management Server

The Management Server node provides an overview of the Management Center with getting started points.

The overview has Launch Console buttons for each of the DesktopNow products, Application Control, Environment Manager and Performance Manager.

The lower section of the work area presents a summary of the connection status of the Management Server and details on deployment groups, computers and alerts.

Deployment Statistics

For each of the DekstopNow products Application Control, Environment Manager and Performance Manager, data is gathered and reported on in the following three areas:

- **Number of agents installed**
- **Number of configurations installed**
- **Polled in Last 30 Days** - Number of computers with an installed agent that have polled the Management Server within the last 30 days.

  Agents and configurations are included in each count if they have a status of Installed, Pending Uninstall, or Unmanaged.

Connection

- **Connected To** - Indicates the name of the server the Management console is connected to.
- **User** - The name of the user currently logged on. Click the link to view and edit the server permissions for the current user. Note that you can only edit if you have permission.
- **Global Permissions** - The global permissions of the current user. For example, Modifier and Viewer.

  Click the link to display the system wide server roles.

Deployment Groups

- **Deployment Groups** - Displays the number of deployment groups defined within the Management Server.
- **Deployed** - Displays the number of deployment groups that are deployed.
- **With Errors** - Displays the number of deployment groups with errors, for example a failed package deployment.

Computers

- **All** - Displays the number of managed computers defined in the Management Server.
- **Deployed** - Displays the number of computers with packages deployed.
- **Offline** - Displays the number of computers offline. A computer shows as offline if the Deployment Agent does not poll back within twice the default poll period.

- **With Errors** - Displays the number of computers with errors. An error occurs if an attempt has been made to deploy a package and it has failed.

  Click a link to go to the **All Computers** view.

Alerts

- **All** - Displays the total number of alerts.
- Alert rules allow you to specify the event criteria to match with an incoming event to generate an alert. Alert rules allocate a severity for an alert and matches against the specified event ID. Alert rules can also match against any value for computer or user to generate more specific alerts.
- **Critical** - Displays the number of critical alerts.
- **New** - Displays the number of new alerts.
- **New in Last 24 Hours** - Displays the number of new alerts in that have be generated in last 24 hours.

  Click on any of the links to view further detail.

Actions

The Actions panel provides the following options:

- **Connect** - Launches the Select Management Server dialog. Select a Management Server to connect to. If already connected to a Management Server it is automatically disconnected when another one is selected.
- **Download Page**(*only available when connected to a Management Server*)- Displays the Management Center download page in a web browser. All available software releases are listed for download.

- **Settings** - Launches the Settings dialog.
    - **Show 'Getting Started' on home screen** - De-select to hide the Management Center Getting Started section from the Server Overview screen when you next launch the console.
    - **Communication Settings** - Timeout values are set to determine the amount of time the Management Console should wait to get a response from the Management Server, the default values are set to 60 seconds. Be aware that if you set the value too low theManagement Console may not be able to communicate with the server and if the value is set too high then the Management Console may stall if there is a communications issue.
        - General Timeout value is used by the Management Console when communicating with the Management Server.
        - Report Timeout value is used by the Management Console when generating a report.
- **Details** - Launches the Server Details dialog which displays all of the server details.

Global Settings

Global Failover Servers

Failover servers can be setup so that in the event of the following they can take over the role of the Management Server:

- A connection, hardware or environment failure.
- Decommissioning a Management Server.
- Conducting an update.
- Overhauling a Management Server.

When installed on managed endpoints the Deployment Agent downloads the list of servers and maintains the list as a reference. If a Management Server is unavailable, the managed computer refers to the list and attempts to register with the next available server. The list of servers consists of one or more URLs. You can specify a server using the server NetBIOS name, the fully qualified domain name or the IP address.

The failover servers can be maintained in a:

- Global default list, which applies to all deployment groups.
- Custom deployment group list, which can be set to override the default list.

The global or default list of failover servers is maintained in the following location of the Management Console:

Home >**Global Settings**> **Failover Servers**tab

This tab allows you to add and remove failover servers. The list of servers is shown in order of priority. To change the order use the **Move Up** and **Move Down** options in the Actions panel. To validate connections, select **Diagnostics Enabled**, to set a diagnostics check prompt on any client computer connecting with a particular server. By default, the Server is enabled but the **Server Enabled** option allows you to disable the server to prevent further connections.

When the Deployment Agent successfully registers with a Management Server, the URL of the server is added to the server list if the URL does not already exist. This ensures the Deployment Agent never loses contact with the Management Server. A URL can be removed from the list of servers to which Deployment Agents connect, by deselecting the URL Enabled option.

Failover Servers List

The Management Server list includes the options shown in the following table:

Column	Description
Server	The URL address of the failover server. Displayed in one of the following formats and may also include port specifications: ◦ Server host name: http://MyServer:80/ManagementServer ◦ IP address: http://123.456.789.0/ManagementServer ◦ Fully qualified path: http://MyServer.MyDomain.com/ManagementServer
Diagnostics Enabled	Not selected by default. When selected for Management Servers, all connecting Deployment Agents on managed computers perform self-tests at startup and on request to ensure that connectivity is available. Deployment Agent self-tests report events to the Management Server, except in the case of connectivity issues or failure, and also reports to the local Windows Event Log. Deployment Agent self-tests check the following: ◦ Connectivity. ◦ Package downloads. ◦ Event uploads. ◦ Ability to raise high priority events, such as failure to install packages.
Server Enabled	Selected by default. When selected, the server is available. When deselected, the server is unavailable for any further connections. Client computers automatically redirect to the next available server in the list. This can be used when decommissioning a server by preventing Deployment Agents connecting to the server.

Actions

- **Add Server** — Launches the Add Failover Server dialog. Enter a URL or browse for a server to add to the list. Select the Connection Type, HTTP or HTTPS, and the connection port.

- **Remove Servers** — Removes selected Servers from the list of failover servers.

  Any servers removed from the servers list which are still listed by Deployment Agents on managed computers registering with the server, can be added back into the list automatically. To avoid this occurring, it may be necessary to disable redundant or decommissioned servers until all managed computers have been updated with the correct list of available servers.

- **Move Up** — Moves the selected server to a higher position in the list and in the order of priority.
- **Move Down** — Moves the selected server to a lower position in the list and in the order of priority.
- **Test Server Connection** — When selected, the Management Server performs a connection test to each selected server in the list and reports any successes or failures.

Global Access Credentials

The credentials are used by the Management Server to authenticate access to the clients when installing the Deployment Agent. These credentials must be supplied before attempting to install the Deployment Agent on any endpoint via the Management Console.

The Global Settings Access Credentials apply to all Deployment Groups by default, unless specific credentials have been defined within a specific Deployment Group. In this case, the Deployment Group's Access Credentials override the default global Access Credentials.

The credentials are attempted in the order listed, to change the order use the **Move Up** and **Move Down** options.

To add new credentials, enter a user name and password and click **Add**. The credentials are stored in the database, the Server Configuration Portal (SCP) creates an RSA public-private key pair that is stored in the Microsoft Cryptographic Provider of the server. This key is used to encrypt and decrypt the credentials stored in the database and therefore secures the information.

Managing the Global Access Credentials

1. Select the **Home** button in the navigation pane.
2. Select the **Global Settings** node.
3. Select the **Access Credentials** tab.
4. Do one or more of the following:
   - To add a credential enter a User name and password, select **Add**.
   - The credentials are entered into the list below.
   - To remove a credential, highlight the required credential and select the **Remove** button.
   - To order credentials in the list highlight the required credential and select the **Move Up** or **Move Down** buttons until in the preferred order.

Membership Rules

Membership rules determine which group a computer is assigned to. You can configure the rules by adding and excluding conditions based on computer by NetBIOS name, or path references to Active Directory computers, computer groups or containers. Membership Rules have a one to one relationship with Deployment Groups. A membership Rule is automatically created on creation of every Deployment Group.

The (Default) Deployment Group has a non-editable set of membership rules to Include All. You cannot add, or remove a condition or change the priority for this group.

Multiple Membership Conditions for the same Rule always evaluate using OR Boolean logic.

Membership Rules are processed in the order the Deployment Groups are listed in the Membership Rules work area. Therefore, if a computer matches multiple membership conditions in different Deployment Groups, it is added to the first Deployment Group in the list where a membership condition matches. To change the order of the Deployment Groups use the **Move Up** and **Move Down** options in the Actions pane.

1. Select the **Home** navigation button.
2. Select the **Membership Rules** node.

   The Edit Group Conditions dialog displays.
3. Click **Add** and do one of the following:
   - Select **Computer by NetBIOS Name** and specify the NetBIOS name for the computer or browse to the computer.
   - Use **Active Directory** and select **Computer**, **Group** or **Container** and specify or browse to the Active Directory component.
4. Repeat to add additional conditions, if required and click **OK**.
5. If you want to automatically discover computers that match the membership rules select **Automatically discover computers every...** You can set the discovery as frequent as every hour, intervals in between, or as infrequent as 1 week.

   Click **Discover** to perform an immediate discovery of computers.
6. Click **Submit** to submit the changes to the rule.
7. If required, expand the deployment group you have discovered computers for and select the Computers node.

   Details display about the discovered computers in the Computers work area.

Asterisk (*) and question mark (?) wildcard characters are supported in groups. The asterisk represents one or more characters, and the question mark wildcard represents a single character.

Actions

- **Edit Conditions** - Displays the Edit Group Conditions dialog box allowing you to include and exclude conditions for computers, groups and containers.
- **Move Up** - Moves the selected membership rule up.
- **Move Down** - Moves the selected membership rule down.
- **Discover** - Discovers computers and places the computers into the first group that has a matching rule.

  Only users with Server Administrator or Group Administrator permissions can execute the Discover action.

  Discovery Settings

  Automatically discover computers every [ ] - select to automatically discover computers from one of the following intervals:

  - 1 Hour
  - 4 Hours
  - 12 Hours
  - 24 Hours
  - 1 Week

All Computers

The Computers node allows you to manage the list of computers across all Deployment Groups for the Management Server. Management options allow you to add, move, delete computers and monitor alerts, events, DesktopNow software agent and configuration packages and computer details.

The Computers node includes the following sections:

Column	Description
Name	Computer name.
Deployment Group	The Deployment Group of which the computer is a member.
Alerts	Number of active alerts.
Last Response	The period since the last poll.
Status	The latest information received when installing the Deployment Agent and any status information sent from the endpoint, including pending diagnostics, failed deployments and failed diagnostics.
Deployed (%)	Indicates the status of the packages assigned to the deployment

Column	Description
	group for each computer. 100% indicates that the assigned packages have all been installed (or uninstalled).

Control Tabs

The following tabs display at the bottom on the Computers work area:

Tab	Description
Computer Details	The Computer details tab displays information about the selected computer, and includes: •Property – Computer hardware and system properties. •Value – Computer hardware and system details.
Alerts	The Alerts tab allows you to monitor alerts for the selected computer, and includes: •ID – Event for which the alert is generated. •Rule – Alert rule. •Computer – Where the alert originated. •Deployment Group – Deployment group from which the alert originated. •Last Event – When the alert is raised on the Server. •Status – Alert status: New, Acknowledged or Resolved.
Events	The Events tab allows you to monitor events on the selected computer, and includes: •ID – Event number. •Date/Time – Date and time the event occurred. •Computer – Where the event occurred. •User – Who caused the event.
Packages	The Packages tab allows you to view packages on the selected computer, and includes: •Product – The product to which the package belongs. •Name – Title of the software agent or configuration package on the currently selected computer.

Tab	Description
	•Installed Version – Number of the current software package version on the selected computer. •Installation Status – Indicates the progress of the package. Possible states include: ◦Pending Install ◦Checking Prerequisites ◦Downloading ◦Download Failed ◦Installing ◦Installed ◦Install Failed ◦Unmanaged - for more information on this state see Deployment Statistics ◦Pending Upgrade ◦Upgrading ◦Upgraded ◦Upgrade Failed ◦Pending Uninstall ◦Uninstalling ◦Uninstall Failed ◦Uninstalled ◦Install Prerequisite Failed •Status Message – Displays status messages received from the endpoint when a problem occurs during package installation or removal.
Diagnostics	The Diagnostics tab provides details of the diagnostics test on the selected computer and the result of each test performed. •Test – Indicates which test is performed. ◦Connectivity

Tab	Description
	◦Download Packages ◦Upload Events ◦High Priority Events •Result – Indicates the current state of the diagnostics taking place on the computer, for example, untested, pending, requested or completed with test passed or test failed.
Client Access Logs	Provides progress updates on the installation of the Deployment Agent.

Computer Find

You can use Computer Find to locate a specific computer or range of computers in the list of computers that have the Deployment Agent installed. Enter a full string or partial strings in the edit field to match computer names using wildcard characters, including:

- Question mark (?) — Indicates a single character
- Asterisk (*) — Indicates zero or more characters

Computer Find facility searches for computers by deployment group beginning with the (Default) group. The search continues in turn to each group until a match is found. When there are no more matches, a message box notifies you that there are no more results.

Navigate through results using the **Find Next** and **Find Previous** buttons.

Actions

- **Move** — Launches the Move Computers dialog for selecting a different group to relocate the highlighted computer.

- **Delete** — Deletes selected computers from the system.

  Deleted computers remain listed in this group until all software packages have been removed with *Pending delete* status displayed next to the computer name in the overview panel.

  Agents and packages are deleted as follows:

  - Product Agents and Configurations — Ivanti product agents and configurations uninstall according to the Installation Schedule.
  - Deployment Agent — The Deployment Agent uninstalls after product agents have uninstalled, according to the Installation Schedule.

  When the Agent Schedule is disabled the Configuration Schedule is ignored and therefore no agent *or* configuration packages uninstall.

- **Delete All** — Deletes all computers in the group. Deleted computers are moved to the (Default) group to await the uninstall process to remove software packages.
- **Unregister**— Unregisters the computer from server.

  If you select this option before the packages and agents have successfully been deleted from this computer, the Deployment Agent re-registers the computer again on the next poll period.

- **Restore** — Restores a computer set to Delete or Unregister.
- **Show Event Details** — Launches the Event Details dialog for viewing information about the selected event.
- **Request Diagnostics** — Starts a diagnostics check on selected computers to test connectivity with the main Management Server and any failover servers for which Run Diagnostics is selected in the Failover Servers node.
- **Clear Filter** — Clears any filters that have been applied to the display. To apply a filter to the display right-click on the column you want to filter and select Filter Editor. The Filter Editor is used to filter the list based on the entered criteria.

Manually Added

The Manually Added node displays if any computers have been manually added to a deployment group, and not discovered and placed in a group by use of Membership Rules.

The work area displays the name of the computer and the expected group to which the computer has been manually added.

Remove the Manually Added Status

1. Navigate to **All Computers** > **Manually Added**.
2. Select the computer that you want to remove the manually added status from, and from the Actions panel select **Remove**.

   A message displays informing you that the expected groups for the selected computers will revert to the groups determined by membership rules and that managed computers will not change groups until they are moved.

   To move a computer you can select one of the following:

   - **Deployment Group** > **Computers** > **Move** action - select the computer(s), click **Move** and select the required deployment group.
   - **Deployment Group** > **Computers** > **Misgrouped** > **Regroup** action - select the computer(s), click **Regroup** and the computers are automatically re-assigned to the deployment groups based on the Membership Rules.
3. Click **OK** to confirm the removal.

If the removed computer has not been moved to a deployment group it may be listed in the Misgrouped node. This happens if there's a membership rule that puts the computers in a different group.

Misgrouped

The Misgrouped node is added when a computer has:

- Been manually added to a group, but the computer subsequently registers with a different group because that's the group it had been in.
- Been added to Active Directory which puts the computer in a certain group, but the computer subsequently registers with a different group because that's the group it had been in.
- Moved to a different Active Directory group, which puts the computer in a different deployment group.
- Been deleted from the Manually Added node and Membership Rules puts the computer in a different group.

The Misgrouped node is added to the All Computers node and the Computers node for the deployment group.

You have the option to remove the computers from the misgrouped list using one of the following methods:

- **Move** - manually select which deployment group to place the computers.
- **Regroup** - automatically place the computers in the deployment group as defined by the Membership Rules and Manually Added List.

Moving computers to another deployment group can cause DesktopNow configurations and agents to be installed or uninstalled when the Deployment Agent next polls. Agents are installed according to the installation schedule of the target deployment group. Installation Schedules are set up in Deployment Group > Settings > Installation tab.

If there are no misgrouped computers the Misgrouped node does not display in the navigation tree.

Deployment Groups

Default Deployment Group

The **Default** deployment group node includes computers which are registered to the Management Server but do not match the membership criteria of existing deployment groups. If an existing deployment group is deleted, computers within the deleted group are moved to this node.

The default deployment group contains the same settings and nodes as a new deployment group.

You can move the computers to another deployment group by selecting them and then clicking **Move** in the Actions column.

Deployment Group

When you create a new deployment group the overview work area displays the following sections:

Details

Displays the name and description of the deployment group. Click in either field to make any amendments.

The access credentials display with the **Manage Credentials** button to add and manage the credentials specifically for the deployment group.

Manage Credentials

Access Credentials provide a global list of access credentials for all deployment groups. The Access Credentials list for Deployment Groups overrides any global Access Credentials within that group. You can add multiple users to the list and they are attempted in the order defined in the work area.

1. Select the **Home** node in the navigation pane.
2. Expand the **Deployment Groups** node.
3. Select the [**Deployment Group**] node.
4. In the Details section select the **Manage Credentials** button.
5. Do one or more of the following:
    - To add a credential enter the user name and password and select **Add**.
    - To remove a credential, highlight the required credential and select the **Remove** button.
    - To order credentials in the list select the required credential and select the **Move Up** or **Move Down** buttons.

Settings

Directly access the following settings for the deployment group:

- **General** - setup the server polling, downloads and event data upload periods, configuration deployment format and deployment agent permissions.
- **Installation** - setup the agent and configuration installation schedules.
- **Custom Failover Servers** - setup the list of failover servers specific to this deployment group.
- **Auditing** - setup anonymous logging and event filters.

Membership Rules

The Membership Rules section displays a list of all membership rules for the deployment group.

Configure Membership Rules

Click the **Configure Membership Rules** button to change the view to **Home** > [**Server**] > **Membership Rules** to setup or manage the membership rules for the deployment group.

Assigned Packages

The Assigned Packages section displays a list of all assigned packages for each installed DesktopNow product with details of package type, agent or configuration and version number, number of packages installed and the number of computers in the group, with agents installed, that have polled the management server within the last 30 days.

Assign Packages

Click the Assign Packages button to changes the view to **Home** > [**Server**] > **Deployment Groups** > [**Deployment Group**] > **Packages** to change agent or configuration versions.

Computer

The Computer section displays the following:

- Total number of computers within the selected deployment group.
- Number of completely deployed computers i.e. packages are 100% deployed.
- Total number of Computers which are currently offline.

  A computer is considered offline if the installed Deployment Agent does not poll back within twice its default poll period.

  The Server Polling period is set up in the Deployment Groups > [Deployment Group] > Settings > General tab, the default poll period is set at 1 Hour.

- Number of computers which have either a deployment or diagnostic error.

  A computer shows with errors if an attempt to deploy a package has failed or has a diagnostic error. The relevant Computer displays in red in the Computers node and also the Group to which the computer belongs.

Click on any of the numbers to change the view to the **Home** > [**Server**] > **Deployment Groups** > [**Deployment Group**] > **Computers** node.

Alerts

The Alerts section displays the following:

- Total number of unresolved alerts that the user has permission to view for the deployment group.
- Total number of unresolved alerts which belong to an alert rule that has Critical severity.
- Total number of alerts which have a status set to New.
- Total number of unresolved alerts that have been raised in the last 24 hours.

The Critical, New and Created in Last 24 hrs alert categories are not mutually exclusive,therefore, an alert can potentially be seen in all 3 categories.

Click on any of the numbers to change the view to the **Home** > [**Server**] > **Deployment Groups** > [**Deployment Group**] > **Alerts** node.

Events

The Events section displays the total number of events in the system which belong to the selected deployment group that the user has permission to view and the total events raised in the last 24 hours.

Click on any of the numbers to change the view to the **Home** > [**Server**] > **Deployment Groups** > [**Deployment Group**] > **Events** node.

Actions

Security — Launches the Security for [Deployment Group Name] dialog in which you can change the Allow/Deny settings in the list of available Security Roles and change the owner of the current object.

Configuring Deployment Groups

Once created, Deployment Groups can be configured in a number of ways, this is a suggested workflow so you can see all elements that need to be setup.

Step 1 Create Deployment Group

Home > [**Server**] > **Deployment Groups** > **New Deployment Group** in the Actions panel.

A new deployment group is created. The new group is created with the name NewDeploymentGroup. To rename the node you can right-click and select **Rename** from the context menu, alternatively you can click on the **Name** field in the Details section in the deployment group work area.

Step 2 Deployment Group Settings

Home > [**Server**] > **Deployment Groups** > [**Deployment Group**] > **Settings**

Configure the following for the deployment group:

- Settings
- Packages
- Computers
- Alerts
- Events

Step 3 Setup Membership Rules

Home > [**Server**] > **Membership Rules**

Edit the conditions to set up the membership rules. You can move the membership rules up and down, this is important because when discovering computers the computer is placed in the first deployment group that has a matching rule.

Step 4 Discover Computers

Home > [**Server**] > **Membership Rules** > **Discover** in the Actions panel

Click **Discover** in the Actions panel to find computers that match the group membership rules. Matching computers display in the list.

Step 5 Install Deployment Agent

Home > [**Server**] > **Deployment Groups** > [**Deployment Group**] > **Computers** > **Install Deployment Agent** in the Actions panel.

Select the computer to which you want to deploy the Deployment Agent and select **Install Deployment Agent** in the Actions panel.

The Client Access Log tab in the Computers work area displays details on the installation progress.

Move Computers Between Deployment Groups

You can move computers between different deployment groups by highlighting a listed computer in a deployment group and selecting **Move** in the Actions panel.

You can select this option in the Computers node of any deployment group.

- Select one or more computers in the list.
- Click **Move** in the Actions panel.

  The Move Computers dialog box displays.
- Select the deployment group to move the computers to and click **Move**.

  The computers are relocated to the new group.
- Check the destination deployment group to view the computer in the new location.

Deployment Group Settings

Deployment Group Settings General

The **Deployment Group** > **Settings** > **General** tab provides the following options to configure the deployment group.

Server Polling and Downloads

The Server Polling and Downloads period determines how frequently the Deployment Agent communicates with the Management Server to check for changes related to assigned product agents, configurations or deployment group settings.

The period can be set to occur as low as 1 minute or as high as 7 days. The default is 1 hour and the following are selectable values:

- Minutes - 1, 5, 15, 30
- Hours - 1, 4, 8, 12
- Days - 1, 2, 5, 7

Server Polling and Downloads

Sets the frequency the client computer checks the server for changes to the deployment group. When new settings, agents or configurations are detected, the client downloads the relevant components and installs them. The client computer also initiates diagnostics tests when a request is detected on this poll period. The default computer poll period is 1 Hour.

Product agents and configurations install according to the installation schedule. Select **Settings** node > **Installation** tab to configure the schedule settings.

Poll Variance

After the period is determined, you can include a poll variance to reduce the impact of multiple Deployment Agents polling at any one time. The variance ranges from 0 to 100 percent and works by staggering when the Deployment Agents poll. For example, if a poll period is set to 10 minutes with a variance of plus or minus (+/-)10% the Deployment Agent will poll between 9 and 11 minutes. The default variance is 20%.

The Server Polling and Downloads ranges from 1 minute to 7 days. The options for setting the poll period are limited to avoid overloading the demand on network bandwidth which very short poll periods would cause and the risk of missing critical updates and downloads that much longer poll periods might cause.

Event Data Uploads

The Event Data Uploads period determines how frequently the Deployment Agent uploads event data from the managed endpoint device to the Management Server database.

The period can be set to occur as low as 1 minute or as high as 1 day. The default is set to 30 minutes and the following are selectable values:

Minutes - 1, 5, 15, 30

Hours - 1, 4, 8, 12

Day - 1

After the period is determined, you can include a variance to reduce the impact of multiple Deployment Agents uploading at any one time.

Event Data Uploads

Sets the frequency with which client endpoints upload event data.

The upload poll period variance works in the same manner as the computer poll period variance and is used to stagger the times when the Deployment Agents upload event data to the Management server. The default upload poll period is 30 minutes.

The Event Data Uploads ranges from 1 minute to 1 day. The options for setting the poll period are limited to avoid overloading the demand on network bandwidth which very short poll periods would cause and the risk of missing critical updates and downloads that much longer poll periods might cause.

Configuration Deployment Format

Select the format in which to deploy configurations:

- Windows Installer MSI
- Native Configuration

When deploying a native configuration the Deployment Agent persists the configuration file using the file name configuration.a?mp. The file name is saved into the registry so that each product knows where to find the configuration.

Native configuration files contain the version of the configuration and upgrade and product code, these values are the same as those stored in the MSI file which means they can be converted to an MSI and back again.

- Location - select the ellipsis to select the required folder location.

The native configuration path can only be a valid local path, it cannot be empty or be a network path.

Caution: The Deployment Agent expands environment variables included within the native configuration path under the context of the LocalSystem account. This means environment variables such as %UserProfile% will be expanded to "C:\Windows\System32\config\SystemProfile" and not the user profile of the currently logged on user. Use of the user profile environment variables is not recommended.

Deployment Agent Permissions

- **Allow self-registration** - Select this option to allow local administrators to force the Deployment Agent to self-register with this deployment group. Self-registering Deployment Agents are installed using a command line with the GROUP_NAME parameter specifying the group with which the Deployment Agent registers.

  This option is disabled by default but provides an alternative method for installing Deployment Agents on managed computers to register with a specific Deployment Group on the Management Center rather than predefining the group membership in the Management Console.

  This option is disabled for the (Default) Deployment Group.

- **Allow unregistration** - Select this option to allow local administrators to request Deployment Agents unregister computers from this deployment group.

  If a computer has been unregistered by the CCA Command tool the Deployment Agent service must be restarted for it to be re-registered.

- **Allow update initiation** - Select this option to allow local administrators to request Deployment Agents immediately install and uninstall packages for this deployment group regardless of the deployment group installation schedule.

Deployment Group Settings Installation

The Installation tab allows you to configure the deployment group installation schedule for Agents and Configurations.

Software agents and configurations are installed according to the installation schedule for the deployment group. Licenses are installed immediately upon download by the Deployment Agent from the Management Server.

Agent Installation

Agent installation defines the manner in which updates to Deployment Agents are pushed to the endpoints. Regardless of the selected agent schedule, the Deployment Agent begins downloading packages immediately after the next time it polls the server. Downloaded packages are stored on the endpoint until the scheduled installation time.

For the following situations, we recommend that you use the settings described:

Setting	Suggested Use
Automatically restart system and install - at next client poll, with user postponement.	You need to push out an update quickly, such as an important patch release or hot fix.
Automatically restart system and install - scheduled.	You need to push out updates in a predictable manner. For example, when an installation is required by a certain time of day.
At next system restart.	The update can wait until the end user schedules a computer restart, or when a remote computer restart can be scheduled out of normal working hours to install an update - this is the recommended setting for servers.

To prevent assigned agents from being downloaded, installed or uninstalled check the **Do not install** option.

Restart and Install Agents

Select from the following options:

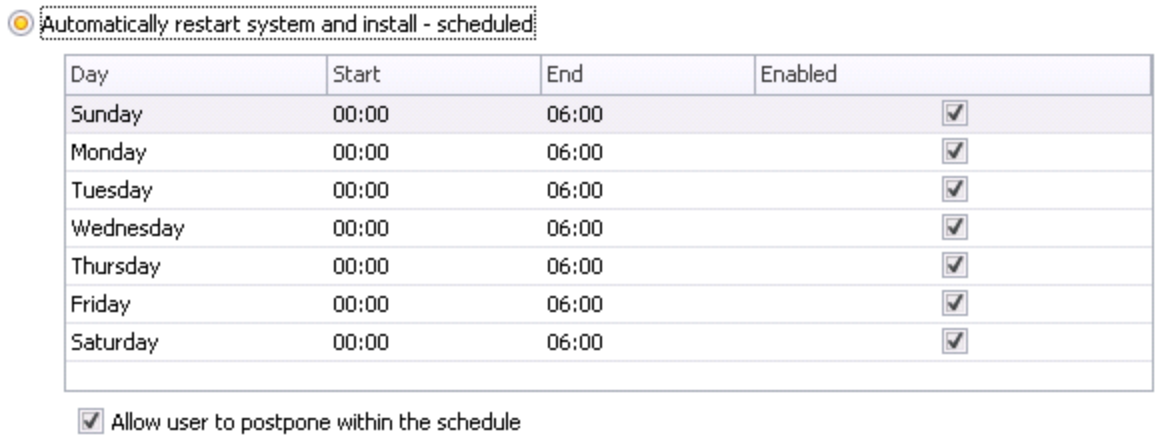
- **Automatically restart system and install - at next client poll** - select to check for agent updates next time the client polls the Management Server. If agent updates are found an automatic system restart takes place to install the agent.

  If selected the following option displays:

  - Select **Allow user postponement for up to -** options available to postpone a system restart for up to 8 hours, you can select hourly intervals from 1 hour to 8 hours.

- **Automatically restart system and install - scheduled** - select to check for agent updates next time the client polls the Management Server. If agent updates are found an automatic system restart takes place to install the agent only within the set scheduled period.

  If selected, the schedule table displays:



  Click on a Start or End time to display a drop down list, select the required time. The Agent packages are installed according to the specified days and times enabled in the list.

  Setting the Installation Schedule

  The Deployment Agent installs packages after the start time, and before the end time. For example, with a start time of 08:00 and an end time of 18:00, packages install between 08:00 and 18:00.

  A scheduled end time can be set before the start time to invert the installation period. For example, with a start time of 18:00 and an end time of 08:00, packages install after 18.00 and before 08.00 on the specified day.

  After an agent schedule with user postponement has started, you cannot shorten the end time for computers that have already polled. In this case, if you need to change the installation time, you can set a new schedule that starts in the future. If you do reduce the end time on an active schedule, only computers that have not polled are affected.

  - **Allow user postponement within the schedule** to allow the end user to postpone the installation of agents within the installation schedule time frame. The end user receives the postponement message at the beginning of the installation schedule, before being forced to install at the end of the installation schedule.

The user can select to restart immediately or postpone for 10 minutes, 30 minutes or 1 hour, provided the delay does not exceed the end of the schedule time. To prevent a single user logging off other users, the postponement message only displays on computers where a single user is logged in. If at the start of the scheduled installation period two or more users are logged in then the Deployment Agent skips the postponement message and, at the end of the scheduled period, displays the countdown message to all users before restarting the computer.

If a user prevents the agent installation by, for example, shutting down the computer before the end of the schedule period, the scheduled installation takes place automatically the next time the computer starts.

A countdown message displays when there are only 5 minutes remaining in the schedule with a warning that a restart will be forced.

If the user postponement option is not enabled the Deployment Agent delays the restart by 2 minutes to allow users to save any work.

- **At next system restart** - Assigned agents install when the endpoints are started and before user logon. This is the default setting for all Deployment Groups with the exception of the (Default) group which has a default setting of Disable.

Additional Options

- **Within Restart, install Agents during [ ] phase:**
  - **Shutdown** - select to install agents at time of endpoint shutdown.
  - **Startup** - select to install agents at time of endpoint restart, install takes place before user logon.
- **Install agents immediately if no restart required** - select to install agents, that do not require a restart, immediately.

Configuration Installation

The configuration installation schedule controls when configurations install. To prevent assigned configurations from being downloaded or installed check the **Do not install** option.

If you attempt to uninstall a configuration when the Agent Schedule is set to **Do not install**, the Configuration Schedule is ignored. Therefore, no agent or configuration packages uninstall.

Configuration Install Behavior

Select from the following options:

- **Automatically install - at next client poll** - select to check for configuration updates next time the client polls the Management Server. If configuration updates are found they install automatically.

- **Automatically install - scheduled** - select to check for configuration updates next time the client polls the Management Server. If configuration updates are found they automatically install within the set scheduled period. If selected, the schedule table displays. Click on a Start or End time to display a drop down list, select the required time. The configuration packages install according to the specified days and times enabled in the list.

  Once the Deployment Agent on the managed computer polls the Management Server for the list of packages to install and their associated installations schedule, the packages install at the scheduled time. If the installation of any of these prerequisites or agents fail, installation is re-attempted at computer startup.

  If simultaneously deploying agents and configurations for the same product the Deployment Agent ensures both install on computer startup *regardless* of the configuration installation schedule.

  When a configuration is deployed but no agent change is required deployment occurs according to the installation schedule.

  Regardless of the selected configuration schedule, the Deployment Agent begins downloading immediately after the next time it polls the server. Downloads are stored on the endpoint until the scheduled installation time.

  The Deployment Agent installs packages after the start time, and before the end time. For example, with a start time of 08:00 and an end time of 18:00, packages install *between* 08:00 and 18:00.
  A scheduled end time can be set before the start time to invert the installation period. For example, with a start time of 18:00 and an end time of 08:00, packages install after 18.00 and before 08.00 on the specified day.

  - **Mirror Agent installation schedule** - select to set the schedule to the same as the Agent schedule.
- **At next system restart** - configurations install when the endpoints are started and before user logon.

Additional Options

- **Check for and download new Configurations at startup** - select to check the Management Server for any new configurations and to download and replace them at computer startup. This stalls logon until it's complete.

  Once the Configuration on the managed computer has polled the Management Server for the list of packages to install and their associated installation schedule, the packages are installed at the scheduled time. If the installation of any of these prerequisites or agents fail, installation is re-attempted at computer startup.

Caution: The status of the check box at shutdown is retained at startup. If the setting was disabled on shutdown the Deployment Agent will not contact the server on startup to check if the setting is now enabled.

Ivanti Update Manager

Agent installations and upgrades are performed at computer shutdown or restart, depending on the deployment group settings. If done at restart, it is before the user logs on, meaning that functionality provided by the agents is never compromised while end users are logged on. You can use the AppSense Update Manager to control when the endpoint computer restarts to install agents.

End-point Install and Uninstall Order

The agent schedule installs, updates, or uninstalls agents, including the Deployment Agent, at computer startup or shutdown depending on the deployment group settings. If you set the configuration schedule to **At next system restart,** configurations also install at computer startup or during shutdown if paired agent is being installed or updated at the same time. The Deployment Agent carries out the actions in the following sequence based on the packages assigned to the endpoint:

- Upgrade of the Deployment Agent.
- Uninstall DesktopNow product configurations which are no longer assigned.
- Uninstall DesktopNow product agents which are no longer assigned.
- Install or upgrade software prerequisites, for example MS Core XML Services (MSXML).
- Install or upgrade assigned DesktopNow product agents.
- Install or upgrade assigned DesktopNow product configurations.
- Uninstall the Deployment Agent.

When simultaneously deploying an agent and configuration for the same product, the Deployment Agent ensures that both are installed on computer startup or computer shutdown, depending on the deployment group settings, regardless of the configuration schedule. This ensures configurations which depend on an upgraded agent are not installed too soon. When a configuration is deployed, but no change is made to its product agent, deployment occurs according to the installation schedule.

Ivanti Update Manager Postponement Message

If the administrator has selected to allow the end user to postpone installation of agents a postponement message displays when there are agents ready to install.

The message gives the user the option to postpone the installation and therefore the system restart until a more convenient time so that they have the opportunity to save work before a system restart is forced.

The postponement message only displays if only one user is logged on. This prevents a user logging off other users on the system.

The user can select from the following options:

- Restart Now - initiates a system restart which installs the package upon computer startup and before log on.
- Be reminded in 10 minutes
- Be reminded in 30 minutes
- Be reminded in 1 hour

Available Postponement Periods for Scheduled Installations

The available postponement time periods are determined by the installation schedule. For example, a postponement time will not be offered if it would delay the installation past the scheduled installation time.

Or, if the scheduled installation time is less than the minimum postponement time the option to postpone does not display and only the Restart Now option is available.

The default postponement period is always the shortest selectable time period.

Ivanti Update Manager Postponement Message for Windows 8 or Windows Server 2012 Users

Windows 8 or Windows Server 2012 users have an additional notification which displays on the Start screen when a postponement message displays on the desktop.

If you click the notification the desktop displays where the postponement message can be seen and actioned.

Notifications can be turned off in Group Policy or PC Settings.

Ivanti Update Manager Countdown Message

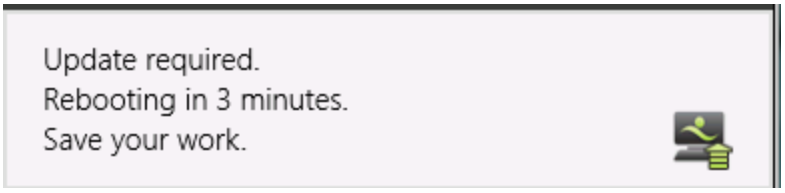
When there are no more postponement intervals available the countdown message displays.

The AppSense Update Manager countdown message only displays the **Restart now** button for single user sessions. If there are multiple users the countdown message displays for information only informing the users of the remaining time before a restart will take place with no option to restart.

The maximum countdown time is 5 minutes, the countdown time can reduce if the scheduled installation time is in less than 5 minutes.

If a user prevents the agent installation by, for example, shutting down the computer before the end of the schedule period, the scheduled installation takes place automatically the next time the computer starts.

Ivanti Update Manager Countdown Message for Windows 8 or Windows Server 2012 Users



Windows 8 or Windows Server 2012 users have an additional notification which displays on the Start screen. The notifications display every minute for the countdown period prior to a restart and they persist for 30 seconds.

If you click the notification the desktop displays where the countdown message can be seen with the option to restart now.

Notifications can be turned off in Group Policy or PC Settings.

The Postponement message and the Countdown message display in the following languages:

- US English
- UK English
- French
- German

Deployment Group Settings Custom Failover Servers

Failover servers can be setup so that in the event of the following they can take over the role of the Management Server:

- A connection, hardware or environment failure.
- Decommissioning a Management Server.
- Conducting an update.
- Overhauling a Management Server.

The Deployment Agent on managed computers downloads the list of servers and maintains the list as a reference. If a Management Server is unavailable, the managed computer refers to the list and attempts to register with the next available server in the list. The list of servers consists of one or more URLs. Each URL can specify a server using the server NetBIOS name, the fully qualified domain name or the IP address.

The failover servers can be maintained in a:

- Global default list, which applies to all deployment groups.
- Custom deployment group list, which can be set to override the default list.

Custom Failover Servers

The Custom Failover Servers tab allows you to add and remove failover servers. The list of servers is shown in order of priority and you can move the servers up and down in the list to change the order of priority. You can also validate connections and set a diagnostics check prompt on any client computer connecting with a particular server. By default, the server URL is enabled but an option allows you to disable the server to prevent further connections.

When the Deployment Agent successfully registers with a Management Server, the URL of the server is added to the server list if the URL does not already exist. This ensures the Deployment Agent never loses contact with the Management Server. To remove a URL from the list of servers to which Deployment Agents connect, deselect the Server Enabled option.

The Deployment Groups Custom Failover Servers tab includes the following sections:

- **Override Default Failover Servers** - Overrides the list of failover servers and applies the settings in the list to all computers in the local deployment group.
- **Manage Default Failover Servers** - Link to the default Failover Servers listed in the Home View.

Failover Servers List

The Management Server list includes the options shown in the following table:

Column	Description
Server	The URL address of the failover server. Displayed in one of the following formats and may also include port specifications: • Server host name: http://MyServer:80/ManagementServer • IP address: http://123.456.789.0/ManagementServer • Fully qualified path: http://MyServer.MyDomain.com/ManagementServer
Diagnostics Enabled	When selected for Management Servers, all connecting Deployment Agents on managed computers perform self-tests at startup and on request to ensure that connectivity is available.
	Deployment Agent self-tests report events to the Management Server, except in the case of connectivity issues or failure, and also reports to the local Windows Event Log.
	Deployment Agent self-tests check the following: • Connectivity. • Package downloads.

Column	Description
	• Event uploads. • Ability to raise high priority events, such as failure to install packages.
Server Enabled	Selected by default. When selected, the server is available. When deselected, the server is unavailable for any further connections. Client computers automatically redirect to the next available server in the list. This can be used when decommissioning a server by preventing Deployment Agents connecting to the server.

Actions

- **Add Server** — Launches the Add Failover Server dialog box for entering a server name or browsing for a failover server to add to the list.
- **Remove Selected Server** — Removes selected Servers from the list of failover servers.

  Any servers removed from the servers list which are still listed by Deployment Agents on managed computers registering with the server, can be added back into the list automatically. To avoid this occurring, it may be necessary to disable redundant or decommissioned servers until all managed computers have been updated with the correct list of available servers.
- **Move Up** — Moves the selected server to a higher position in the list and in the order of priority.
- **Move Down** — Moves the selected server to a lower position in the list and in the order of priority.
- **Test Server Connection** — When selected, the Management Server performs a connection test to each selected server in the list and reports any successes or failures.

Deployment Group Settings Auditing

The Auditing tab in the Deployment Group > Setting node allows you to specify which events client computers send to the Management Server for each product agent. You can also select to display user and computer names in events anonymously.

Events can be generated for all products, click on a product to see the Event IDs and Descriptions.

Application Control

Event ID	Event Name	Event Description	Event Log Type
9000	Denied Execution	Prohibited execution request.	Warning
9001	Allowed Execution	Allowed execution request.	Information

Event ID	Event Name	Event Description	Event Log Type
9002	Overwrite Changed Owner	Overwrite of an allowed executable.	Warning
9003	Rename Changed Owner	Rename of a prohibited executable.	Warning
9004	Application Limit Denial	Application limit denial.	Warning
9005	Time Limit Denial	Time limit denial.	Warning
9006	Self-Authorization	Self-authorization decision by user.	Warning
9007	Self-Authorized allow	Self-authorization execution request.	Warning
9009	Scripted Rule Timeout	Script execution timed out.	Warning
9010	Scripted Rule Fail	Script failed to complete.	Warning
9011	Scripted Rule Success	Script completed successfully	Information
9012	Trusted Vendor Denial	Digital Certificate failed Trusted Vendor check.	Warning
9013	Network Item denied	Prohibited Network Item request.	Warning
9014	Network Item allowed	Allowed Network Item request.	Information
9015	Application Started	An allowed application started running.	Information
9016	Unable to Change Ownership	The file's ownership could not be changed.	Error
9017	Application Termination	A prohibited application has been terminated by Application Control.	Information
9018	Application User Rights Changed	The application's user rights have changed.	Information
9019	AM allowed install	Allowed web Installation request.	Information
9020	AM restricted install	Restricted web installation request.	Information
9021	Windows restricted install (Basic Discovery Mode)	Windows restricted web installation request.	Information

Event ID	Event Name	Event Description	Event Log Type
9022	Web Installation Fail	Web installation failed to complete	Warning
9023	Self-Elevation	Self-Elevation request	Information
9024	URL Redirection	URL Redirection has occurred.	Information
9051	Policy Change granted	A Policy Change Request has been granted	Information
9052	Policy Change invalid response code	An invalid response code has been entered for a Policy Change request	Error
9053	User-requested allow	An allowed Policy Change application has started	Information
9054	User-requested elevate	An elevated Policy Change application has started	Information
9096	Configuration merge success	The configuration merge has completed successfully	Information
9097	Configuration merge fail	The configuration merge has failed	Error
9098	Configuration merge timeout	The configuration merge is still waiting for expected files	Warning
9099	Agent not licensed	AppSense Application Control is not licensed.	Error

Environment Manager

Event ID	Event Name	Event Description	Event Log Type
9300	Self healing process started	A process being monitored for self healing stopped and has been restarted.	Information
9301	Self healing registry key replaced	A registry key being monitored for self healing was changed and has now been reset.	Information
9302	Self healing registry key removed	A registry key being monitored for self healing was inserted and has now been removed.	Information
9303	Self healing file replaced	A file being monitored for self healing was modified or removed and has now been replaced.	Information
9304	Self healing file removed	A file being monitored for self healing was added and has now been removed.	Information
9305	Self healing service stopped	A service being monitored for self healing started and has now been stopped.	Information
9306	Self healing service started	A service being monitored for self healing stopped and has now been restarted.	Information
9307	Self healing registry value replaced	A registry value being monitored for self healing was changed and has now been reset.	Information
9308	Self healing registry removed	A registry value being monitored for self healing was inserted and has now been removed.	Information
9399	Software is not licensed	The Environment Manager software has not been licensed.	Error
9400	Lockdown edit control blocked drive	An edit control has had a blocked drive entered into it.	Information

Event ID	Event Name	Event Description	Event Log Type
9401	Lockdown edit control blocked text	An edit control has had blocked text entered into it.	Information
9402	Lockdown accelerator keys blocked	An application has had accelerator keys blocked.	Information
9403	Lockdown dialog blocked	An application has had a dialog box blocked.	Information
9404	Lockdown	An application has had access blocked for a control using MSAA detection.	Information
9405	User logon action success	A user logon action completed successfully.	Information
9406	User logon action fail	A user logon action failed to complete successfully.	Error
9407	User logoff action success	A user logoff action completed successfully.	Information
9408	User logoff action fail	A user logoff action failed to complete successfully.	Warning
9409	Computer startup action success	A computer startup action completed successfully.	Information
9410	Computer startup action fail	A computer startup action failed to complete successfully.	Warning
9413	Computer network available	A computer network available action completed successfully.	Information
9414	Computer network available action fail	A computer network available action failed to complete successfully.	Information
9420	User session reconnect action success	A user session reconnect action completed successfully.	Information
9421	User session reconnect action fail	A user session reconnect action failed to complete successfully.	Warning
9422	User session disconnect action success	A user session disconnect action completed successfully.	Information

Event ID	Event Name	Event Description	Event Log Type
9423	User session disconnect action fail	A user session disconnect action failed to complete successfully.	Warning
9424	User session locked action success	A user session locked action completed successfully.	Information
9425	User session locked action fail	A user session action failed to complete successfully.	Warning
9426	User session unlocked action success	A user session unlocked action completed successfully.	Information
9427	User session unlocked action fail	A user session unlocked action failed to complete successfully.	Warning
9428	Process start action success	A process start action completed successfully.	Information
9429	Process start action fail	A process start action failed to complete successfully.	Warning
9430	Process stopped action success	A process stopped action completed successfully.	Information
9431	Process stopped action fail	A process stopped action failed to complete successfully.	Warning
9432	Network connection action success	A network connected action completed successfully.	Information
9433	Network connection action fail	A network connected action failed to complete successfully	Warning
9434	Network disconnected action success	A network disconnected action completed successfully.	Information
9435	Network disconnected action fail	A network disconnected action failed to complete successfully.	Warning
9436	User logon (pre-session) action success	A user logon (pre-session) action completed successfully.	Information
9437	User logon (pre-session) action fail	A user logon (pre-session) action failed to complete successfully.	Information
9438	User logon (pre-desktop) action success	A user logon (pre-desktop) action completed successfully.	Information

Event ID	Event Name	Event Description	Event Log Type
9439	User logon (pre-desktop) action fail	A user logon (pre-desktop) action failed to complete successfully.	Information
9440	User logon (desktop created) action success	A user logon (desktop created) action completed successfully.	Information
9441	User logon (desktop created) action fail	A user logon (desktop created) action failed to complete successfully.	Information
9480	Configuration merge update	The configuration merge folder has been updated.	Information
9481	Configuration merge start	The configuration merge has started.	Information
9482	Configuration merge complete	The configuration merge has completed successfully.	Information
9483	Configuration merge fail	The configuration merge has failed.	Information
9484	Configuration merge timeout	The configuration merge has timed out waiting for expected files.	Information
9495	Not configured	AppSense Environment Manager has not been configured.	Warning
9496	Configuration unsupported	An old configuration has been found.	Warning
9650	Managed application start	A managed application has started	Information
9651	Managed application stop	A managed application has stopped	Information
9652	Personalization load error	Personalization settings for a managed application failed to load.	Error
9653	Personalization save error	Personalization settings for a managed application failed to save.	Error

Event ID	Event Name	Event Description	Event Log Type
9654	Blacklisted process started	A managed process has launched a blacklisted process.	Information
9655	Personalization not saved	Personalization settings not saved as another group application is running.	Information
9656	Offline resiliency save started	Offline resiliency save has been started for a managed application.	Information
9657	Offline resiliency save complete	Offline resiliency has successfully saved a managed application's personalization settings.	Information
9658	Personalization settings purged	Personalization settings purged as offline mode is disabled.	Information
9659	Personalization settings updated	User personalization settings updated from personalization server.	Information
9660	Personalization failed	Personalization for a managed application failed.	Error
9661	Timeout Communicating with Personalization Server	A timeout occurred while trying to communicate with the Personalization Server.	Warning
9662	Trigger Action Times	All the actions have run for the trigger.	Information
9663	PreCache Application Success	Successfully Precached Managed Application.	Information
9664	PreCache Group Success	Successfully PreCached Managed Application Group.	Information
9665	PreCache Managed Application Failure	Failed to PreCached Managed Application.	Error
9666	PreCache Group Failure	Failed to PreCached Managed Application Group.	Error
9667	Personalization Profile Import	A Profile Import is Active	Information

Event ID	Event Name	Event Description	Event Log Type
9680	Endpoint of Self Service start failure	The Endpoint Self-Service process failed to start	Error

Performance Manager

Event ID	Event Name	Event Description	Event Log Type
9100	User Memory Usage Warning	Amount of memory consumed by a user has exceeded a warning level set in a User Memory Limit.	Information
9101	User memory usage warning lapsed	Amount of memory consumed by a user has fallen back to a safe level as defined in a User Memory Limit.	Information
9102	User memory usage blocked	Amount of memory available to this user as defined in a User Memory rule has been exceeded. No more memory allocation will be allowed.	Warning
9103	User memory usage blocking lapsed	Amount of memory consumed by a user has fallen back to a safe (non-blocked) level as defined in a User Memory Limit.	Information
9104	Thread Throttling Clamping On	Total CPU Usage has exceeded a threshold and will be clamped.	Information
9105	Thread Throttling Clamping Off	Total CPU Usage has fallen under a threshold and clamping will stop.	Information
9106	Application CPU Usage clamping On	An Application has exceeded its configured hard CPU Usage limit and will be limited to that configured limit.	Information
9107	Per Application Memory Usage Exceeded	Memory usage for a particular application has exceeded a threshold.	Information

Event ID	Event Name	Event Description	Event Log Type
9108	Per Application Memory Usage Reduced	Memory usage for a particular application has dropped below a threshold.	Information
9109	Per Application Memory Usage Terminated	An application has been terminated because it used too much memory.	Warning
9110	Application CPU Usage Clamping Off	An application has now fallen below its CPU Usage limit and will no longer be clamped.	Information
9115	Working set trimmed	Working set for an application has been trimmed.	Information
9116	CPU Affinity changed	CPU Affinity of an application has changed.	Information
9119	Per Application Hard Memory Limit Reached	Memory usage for an application reached its hard memory limit	Warning
9120	Thread Throttling - Clamped Processes	Total CPU Usage has exceeded a threshold and applications will be clamped.	Information
9121	Application CPU Soft Limit - Started	Because of the overall CPU Usage a CPU soft limit will be applied to an application.	Information
9122	Application CPU Soft Limit - Stopped	An application will be no longer controlled by an CPU soft limit.	Information
9123	Application CPU Reservation Applied	A CPU Usage reservation was applied to an application.	Information
9124	Disk - Process I/O Queued	One or more processes were subject to I/O queuing.	Information
9150	Windows Performance Counter Error	The Windows performance counters on this machine are missing or broken.	Error
9170	Settings not found in package	Some configuration settings were not found in the configuration package.	Error

Event ID	Event Name	Event Description	Event Log Type
9171	Settings not valid in package	Some configuration settings in the configuration package were not valid.	Error
9172	Settings loaded from package	The configuration settings were successfully loaded from the configuration package.	Information
9173	Settings applied live to the Agent	The configuration settings were applied live to a running Performance Manager Agent.	Information
9174	Package has been loaded and all settings applied	All settings in the package have been applied to the Agent.	Information
9175	The package is invalid	The configuration package is invalid.	Error
9176	Package not found	The configuration package does not exist.	Warning
9197	Valid License Found	Performance Manager is licensed.	Information
9198	Invalid License Found	Performance Manager has detected a product license which is not compatible with the current used Performance Manager version. Use the Licensing Console to upgrade your Performance Manager license.	Error
9199	Valid License Not Found	Performance Manager is not licensed.	Error
9200	Application Analyzed	Memory Optimizer has analyzed a known application.	Information
9201	Component Analyzed	Memory Optimizer has analyzed a known component.	Information
9202	Component Optimized	Memory Optimizer has optimized a known component.	Information
9203	Component failed to Optimize	Performance Manager has failed to optimize a component	Warning

Event ID	Event Name	Event Description	Event Log Type
9204	Application Identified At Runtime	Memory Optimizer has analyzed a running process and added a new application to the optimization database.	Information
9205	Component Identified At Runtime	Memory Optimizer has analyzed a loaded component in a process and added it to the optimization database.	Information
9206	Database Analyzed	Memory Optimizer has analyzed all known applications within the optimization database.	Information
9207	Database Optimized	Memory Optimizer has optimized all known applications within the optimization database.	Information
9208	Application Optimized	Memory Optimizer has optimized a known application.	Information
9209	Database Cleaned	Memory Optimizer has cleaned the optimization database.	Information
9210	Application Cleaned	Memory Optimizer has cleaned a known application.	Information
9211	Component Cleaned	Memory Optimizer has cleaned a known component.	Information
9212	Out Of Memory	Memory Optimizer has run out of memory and cannot rebase any more	Error
9216	Statistics Collection Strategy	Details of the statistics configuration.	Information
9217	Invalid Local Database Folder	The local statistics database folder is invalid.	Error
9218	General Local Statistics Service Error	An error occurred in the Local Statistics Service.	Error
9219	Disk Cleanup Started	Started cleaning up the local statistics database folder.	Information

Event ID	Event Name	Event Description	Event Log Type
9220	Disk Cleanup of Single Database	Deleted a single old local database.	Information
9221	Disk Cleanup Complete	Started cleaning up the local statistics database folder.	Information
9222	Consolidation Search Started	Started searching for databases to consolidate.	Information
9223	Single File Consolidation Started	Started to transfer a local statistics database for consolidation.	Information
9224	Single File Consolidation Completed	Completed the transfer of a local statistics database for consolidation.	Information
9225	Consolidation Search Completed	Finished searching for databases to consolidate.	Information
9226	Statistics Scheduled Collection	Statistics collection is now scheduled at a new collection level.	Information
9228	Database Import Failed	An incoming database could not be imported.	Error
9229	Database Connection Failed	Could not connect to the configured Reporting Database.	Error
9230	Disk Cleanup Started	Started searching for old received databases to delete.	Information
9231	Disk Cleanup Completed	Finished searching for old received databases to delete.	Information
9232	Purge of Reporting Database Started	Started purging the Reporting Database.	Information
9233	Purge of Reporting Database Completed	Finished purging the Reporting Database.	Information
9234	Error in Central Statistics Server	An error occurred in the Central Statistics Service.	Information

Event ID	Event Name	Event Description	Event Log Type
9235	Deployment Agent updated native configuration	Detected Deployment Agent has updated the endpoint native configuration path.	Information
9236	Memory exceeded minimum threshold new processes eligible for memory limitations	The system memory has exceeded the minimum threshold. New processes will be eligible for memory limitations.	Information
9237	Memory exceeded minimum threshold	The system memory has fallen back below the minimum threshold. New processes will not be monitored for memory limitations.	Information

Management Center

Event ID	Event Name	Event Description	Event Log Type
9090	Service Ended Unexpectedly (Application Control)	The Application Control Agent has ended unexpectedly.	Information
9091	Service Restarted (Application Control)	The Application Control Agent has restarted.	Information
9092	Service Terminated (Application Control)	The Application Control Agent has been terminated due to being in the starting or stopping state for a prolonged period.	Information
9093	Service Unrecoverable (Application Control)	The Application Control Agent has exceeded the maximum restart attempts.	Information
9190	Service Ended Unexpectedly (Performance Manager)	The Performance Manager Agent has ended unexpectedly.	Information
9191	Service Restarted (Performance Manager)	The Performance Manager Agent has restarted.	Information

Event ID	Event Name	Event Description	Event Log Type
9192	Service Terminated (Performance Manager)	The Performance Manager Agent has been terminated due to being in the starting or stopping state for a prolonged period.	Information
9193	Service Unrecoverable (Performance Manager)	The Performance Manager Agent has exceeded the maximum restart attempts.	Information
9390	Service Ended Unexpectedly (Environment Manager)	The Environment Manager User Virtualization Service ended unexpectedly.	Information
9391	Service Restarted (Environment Manager)	The Environment Manager User Virtualization Service has restarted.	Information
9392	Service Terminated (Environment Manager)	The Environment Manager User Virtualization Service has been terminated due to being in the starting or stopping state for a prolonged period.	Information
9393	Service Unrecoverable (Environment Manager)	The Environment Manager User Virtualization Service has exceeded the maximum restart.	Information
9700	Action Notification Success	An action notification was dispatched successfully.	Information
9701	Action Notification Failure	An action notification has failed to dispatch.	Information
9702	Package Modified	Package created, modified or deleted.	Information
9703	User Modified	A user was created, modified or deleted.	Information
9704	Priority Event Failure	A priority event failed to upload to the Management Server.	Information
9705	Event Upload Failure	One or more events failed to upload to the Management Server.	Information

Event ID	Event Name	Event Description	Event Log Type
9707	Events Purged.	Events within the Management Server were deleted.	Information
9708	Platform Mismatch Package	Product agent is not compatible with client platform.	Information
9710	Package Installation Success	A package has been installed or uninstalled successfully by the Deployment Agent.	Information
9711	Package Installation Failure	A package has been unsuccessfully installed or uninstalled by the Deployment Agent.	Information
9712	Computer Registration	A computer has been assigned to a deployment group.	Information
9713	Failover Change URL	The Deployment Agent reverted to another Management Server due to connectivity problems.	Information
9715	Computer Self-registration	A computer has self registered with a deployment group.	Information
9716	Computer Self-registration Failed	A computer has failed to self-register with a deployment group.	Information
9718	Deployment Agent Installed License	The Deployment Agent installed a license.	Information
9720	BITS Server Extensions Not Installed	The Events Dispatcher service could not detect that BITS Server Extensions was installed.	Information
9730	Prerequisite Failed Check	A prerequisite failed due to 'fail-if' check.	Information
9731	Prerequisite Failed to Install	A prerequisite failed to install.	Information
9732	RPC Access Denied	Blocked endpoint request by the user (not running as an Administrator)	Warning

Event ID	Event Name	Event Description	Event Log Type
9733	RPC Set Deployment URL and Group Name	Administrator endpoint request to set Deployment Server URL and optional Group Name	Information
9734	RPC Update Agents	Administrator endpoint request to update all local agents.	Information
9735	RPC Update Configs	Administrator endpoint request to update all local configurations	Information
9736	RPC Query Updating Status	Administrator endpoint request to query update status for agent and configurations	Information
9737	RPC Image Prep	Administrator endpoint request for Image Prep	Information
9738	RPC Unregister	Administrator endpoint request to unregister from the Management Server.	Information
9740	Security Role Modified	A security role was created, modified, or deleted.	Information
9743	Computer self unregistration	A computer has unregistered from a deployment group.	Information
9744	Computer self unregistration failed	A computer has failed to unregister from the deployment group.	Information
9745	SQL AlwaysOn Failover	A SQL/Network error has occurred.	Information
9750	Deployment Agent HTTP error	The Deployment Agent failed to contact to the Management Server.	Information
9751	Deployment Agent registration	The Deployment Agent registered with the server.	Information
9752	Deployment Agent joined group	The Deployment Agent joined its assigned deployment group.	Information
9754	Deployment Agent Diagnostics Test	The Deployment Agent ran a diagnostics test on a server.	Information

Event ID	Event Name	Event Description	Event Log Type
9755	BITS Error	BITS Error.	Error
9756	Deployment Agent BITS Service Error	The Deployment Agent identified an error with the BITS service. The service cannot be started, either because the service it is disabled or because it has no enabled devices associated with it.	Error
9760	Deployment Agent Deployed Successfully	The Deployment Agent has been successfully deployed to a discovered machine.	Information
9761	Deployment Agent Deployment Failure	The Deployment Agent has failed to deploy to a discovered machine.	Information
9790	Service ended unexpectedly	The Deployment Agent has ended unexpectedly.	Information
9791	Service restarted	The Deployment Agent has restarted.	Information
9792	Service terminated	The Deployment Agent has been terminated due to being in the starting or stopping state for a prolonged period.	Information
9793	Service unrecoverable	The Deployment Agent has exceeded its maximum restart attempts.	Information
9795	Condition Modified	A deployment group condition has been modified. This may affect which computers get assigned to the deployment group.	Information
9901	License not valid	[product name] was checked for a valid license and failed.	

System Events

Event ID	Event Name	Event Description
Event ID	Event Name	Event Description
8000	Service Started	[ProductName] Agent: Service Started.
8001	Service Stopped	[ProductName] Agent: Service stopped.
8095	No Configuration found	[ProductName] cannot find a valid configuration.
8096	Configuration Upgraded	A configuration for a previous version of [ProductName] has been detected and upgraded.
8099	Invalid License	[ProductName] software is not licensed.

Anonymous Logging

- Always use anonymous MACHINE name in events — Events for actions performed on specific computers are reported without recording the computer name.
- Always use anonymous USER name in events — Events for actions by specific users are reported without recording the user name.

Event Filter

Provides expandable lists of events by product which you can select either individually or by product group to generate and send to the Management Server.

The following details the Event Filter columns.

Column	Description
Product event ID	Indicates the product name and the four digit event ID numbers for the events available for the selected product.
Event description	Description of the event. You may wish to disable certain types of events which are generated in large quantity to avoid inundating the server.
Enabled	Select to enable an event. Select this option in the top level list item to enable all events in the group.

Deployment Group Packages

The Deployment Group Packages sub-node allows you to manage the list of software packages and assign package versions to the current deployment group for download to the managed endpoints.

The view displays the list of products, available packages and assignments.

Packages include installed Patches, Agents and Configuration files together with details such as the name of the product, the platform on which the package is supported for example, 32-bit or 64-bit and their version numbers.

Product agent packages are saved to the Management server database by default as part of the Management Center installation. Configuration packages for each product can be added to the database via the consoles by saving the configurations to the Management Server. The following products are supported:

- Application Control
- Environment Manager
- Performance Manager

When the installation schedule for a group is disabled, a warning displays in the packages panel notifying you that the packages will not be installed. The warning is removed in either of the following circumstances:

- The installation schedule is enabled.
- All packages are unassigned from the group.

Review and Submit

The Review and Submit button is used to check and deploy any changes to the settings for a particular product patch, agent or configuration.

Package Installation

Depending on the Installation Settings for the deployment group the AppSense Update Manager coordinates the installation of packages. This can result in a computer reboot if new or updated agent packages are deployed.

Actions

- **Quick Setup** - Highlight a product and select this action to display the Quick Setup wizard. Using the quick setup wizard you can quickly assign all of the packages for a product to a group.

  You can also access the Quick Setup wizard by double-clicking the package type.

- **Change Agent Version** (*only available for Agents*) - Select this option to chose the agent to assign to your deployment group.

- **Change Configuration** (*only available for Configurations*) - Use this option to specify the Configuration file and version to assign to your deployment group
- **Change Revision** (*only available for Configurations*) - This option allows you to select a different version of the configuration file used in your deployment group.
- **Always Use Latest** (*only available for Configurations*) - If the configuration assigned to the deployment group is not the latest version. This option is available, to replace the assigned configuration with the latest version available and click **Yes** to confirm.
- **Remove** - Highlight a package to be removed and select this option remove it from the deployment group. The package is removed at the next poll period.

Changing Agent Version

To change the version of the agent to be used by your selected deployment group, do the following:

1. Select **Home** > [**Server**] > **Deployment Groups** > [**Deployment Group]** > **Packages**

   The Packages work area displays and provides a list of all the AppSense products and their assigned packages.

2. Navigate to the Product associated with the version of the agent to be changed.
3. Highlight the agent to be changed.
4. Click **Change Agent Version** from the Actions panel.
5. The Select the 32/64 Bit Agent Version dialog displays, the dialog title will change depending on the version you highlighted.
6. Select the Agent to be used by the deployment group.

   The latest software patches require Deployment Agent version 8.6 or later to support deployment and reduce the number of endpoint reboots.

7. Click **Finish**.

Changing Configurations and Configuration Versions

To change the configuration file to be used by your selected deployment group, do the following:

1. Select **Home** > [**Server**] > **Deployment Groups** > [**Deployment Group**] > **Packages**

   The Packages work area displays and provides a list of all the AppSense products and their associated packages.

2. Navigate to the Product associated with the configuration file to be changed.
3. Highlight the configuration file.

4. Click **Change Configuration** from the Actions options.

   The Select the Configuration wizard page displays.

5. Select the Configuration file to be used by your group.
6. Click **Next**.

   The Select the Configuration Version page displays.

7. Select the Configuration Version to be used.

   If you want to always use the latest configuration version, select **Always Use Latest** in the Version column.

8. Click **Finish**.

Deployment Group Computers

The Computers node allows you to manage the list of computers in the current deployment group. Management options allow you to delete computers and monitor alerts, events, DesktopNow software agent and configuration packages and computer details.

Computers

The Computers list displays the computer name, number of active alerts the computer is showing, the period of time since the last poll. A computer is considered offline if the installed Deployment Agent does not poll back within twice its default poll period. A red indicator displays if the computer is offline. The list also displays, a status message and the deployed state of the computer, expressed as a percentage.

Control Tabs

The following tabs display at the bottom on the Computers work area:

Tab	Description
Computer Details	The Computer details tab displays information about the selected computer, and includes: •Property – Computer hardware and system properties. •Value – Computer hardware and system details.
Alerts	The Alerts tab allows you to monitor alerts for the selected computer, and includes: •ID – Event for which the alert is generated. •Rule – Alert rule.

Tab	Description
	•Computer – Where the alert originated. •Deployment Group – Deployment group from which the alert originated. •Last Event – When the alert is raised on the Server. •Status – Alert status: New, Acknowledged or Resolved.
Events	The Events tab allows you to monitor events on the selected computer, and includes: •ID – Event number. •Date/Time – Date and time the event occurred. •Computer – Where the event occurred. •User – Who caused the event.
Packages	The Packages tab allows you to view packages on the selected computer, and includes: •Product – The product to which the package belongs. •Name – Title of the software agent or configuration package on the currently selected computer. •Installed Version – Number of the current software package version on the selected computer. •Installation Status – Indicates the progress of the package. Possible states include: ◦Pending Install ◦Checking Prerequisites ◦Downloading ◦Download Failed ◦Installing ◦Installed ◦Install Failed ◦Unmanaged - for more information on this state see Deployment Statistics ◦Pending Upgrade

Tab	Description
	◦Upgrading ◦Upgraded ◦Upgrade Failed ◦Pending Uninstall ◦Uninstalling ◦Uninstall Failed ◦Uninstalled ◦Install Prerequisite Failed •Status Message – Displays status messages received from the endpoint when a problem occurs during package installation or removal.
Diagnostics	The Diagnostics tab provides details of the diagnostics test on the selected computer and the result of each test performed. •Test – Indicates which test is performed. ◦Connectivity ◦Download Packages ◦Upload Events ◦High Priority Events •Result – Indicates the current state of the diagnostics taking place on the computer, for example, untested, pending, requested or completed with test passed or test failed.
Client Access Logs	Provides progress updates on the installation of the Deployment Agent.

Computer Search

You can use Computer Search to locate a specific computer or range of computers in the list of computers that have the Deployment Agent installed. Enter a full string or partial strings in the edit field to match computer names using wildcard characters, including:

- Question mark (?) — Indicates a single character
- Asterisk (*) — Indicates zero or more characters

Computer Search finds computers by deployment group beginning with the (Default) group. The search continues in turn to each group until a match is found. When there are no more matches, a message box notifies you that there are no more results.

Search through results using the **Find Next** and **Find Previous** buttons.

Actions

- **Discover** — Click to discover the computers that match membership rules and assign them to deployment groups. If no rules match, the computer is assigned to the (Default) group.
- **Add Computers** — Click to manually add computers to the list. The Select Computers dialog displays, navigate to select the required computers.
- **Install Deployment Agent** — Highlight the computers on which you want to install the Deployment Agent then click **Install Deployment Agent**. The Access Credentials must have been setup before you can install the Deployment Agent.
- **Poll Now** — Click to immediately poll any endpoints you have selected from within a specific Deployment Group.
- **Move** — Highlight the computers you want to move then click **Move**. The Move Computers dialog box displays, select the deployment group to move the computer to.
- **Delete** — Highlight the computers you want to delete then click **Delete** to remove the selected computers.

  Deleted computers remain listed in this group until all software packages have been removed with *Pending delete* status displayed next to the computer name in the overview panel.

  Agents and packages are deleted as follows:

  - Deployment Agent — The Deployment Agent uninstalls after product agents have uninstalled, according to the Installation Schedule.
  - Product Agents and Configurations — DesktopNow product agents and configurations uninstall according to the Installation Schedule.

    When the Agent Schedule is disabled the Configuration Schedule is ignored and therefore no agent *or* configuration packages uninstall.

- **Delete All** — Deletes all computers in the group. Deleted computers are moved to the (Default) group to await the uninstall process to remove software packages.
- **Unregister**— Unregisters the selected, deleted computer from Management Server.

  If you select this option before the packages and agents have successfully been deleted from this computer, the Deployment Agent re-registers the computer again on the next poll period.

- **Restore** — Restores a computer set to Delete or Unregister.
- **Show Event Details** — Launches the Event Details dialog for viewing information about the selected event.
- **Request Diagnostics** — Starts a diagnostics check on selected computers to test connectivity with the main Management Server and any failover servers for which **Run Diagnostics** is selected in the Failover Servers node.
- **Clear Filter** — Clears any filters that have been applied to the display. To apply a filter right-click on the column you want to filter and select Filter Editor. The Filter Editor is used to filter the list based on the entered criteria.

Manually Added

The manually added node displays computers that have been manually added to the Deployment Group, and not discovered and placed in a group by use of Membership Rules. Membership Rules can be overridden by manually adding a computer.

Manually Add a Computer

1. Select the **Home** navigation button.
2. Navigate to a deployment group and select **Computers**.
3. Select **Add Computers** from the Actions panel.

   The Select Computers dialog displays.
4. Select the required computers and click **OK**.

   If the selected computer is currently registered in another deployment group, you are given the option to move the computer.
   Click **Yes** to move the computer.

   The added computer displays in the Computers work area for the deployment group.

A Manually Added sub node appears in the deployment group Computers node and also in the All Computers node. All manually added computer names are listed.

Remove the Manually Added Status

The Manually Added list is for reference and computers can be removed from it at any point.

1. Navigate to a deployment group and select **Computers** > **Manually Added**.
2. Select the computers from which you want to remove the manually added status and from the Actions panel select **Remove**.

   A message displays informing you that the expected groups for the selected computers will revert to the groups determined by membership rules and that managed computers will not change groups until they are moved.

   To move a computer you can follow one of these processes:

   1. Select the **Computers** node for the required deployment group and click **Move** from the Actions panel.
   2. Select the **Computers** > **Misgrouped** node for the deployment group and click **Regroup** from the Actions panel - the computers are automatically re-assigned to the deployment groups based on the Membership Rules and Manually Added status.
3. Click **OK** to confirm the removal.

If the removed computer has not been moved to a deployment group it may be listed in the Misgrouped node. This happens if there's a membership rule that puts the computers in a different group.

Misgrouped

The Misgrouped node is added to a group and the All Computers node when:

- A computer has been manually added to a group, but the computer subsequently registers with a different group because that's the group it had been in.
- A computer has been added to Active Directory which puts the computer in a certain group, but the computer subsequently registers with a different group because that's the group it had been.
- A computer is moved to a different Active Directory group, which puts the computer in a different deployment group.
- A computer has been deleted from the Manually Added node and Membership Rules puts the computer in a different group.

The Misgrouped node is added to the Computers node for the deployment group and the All Computers node.

You have the option to remove the computers from the misgrouped list using one of the following methods:

- **Move** - manually select which deployment group to place the computers.
- **Regroup** - automatically place the computers in the deployment group as defined by the Membership Rules and Manually Added List.

Moving computers to another deployment group can cause DesktopNow configurations and agents to be installed or uninstalled when the Deployment Agent next polls. Agents are installed according to the installation schedule of the target deployment group. Installation Schedules are set up in the deployment group Settings > Installation tab.

If there are no misgrouped computers the Misgrouped node does not display in the navigation tree.

Deployment Group Alerts

The Alerts node, **Home** > [**Server**] > **Deployment Groups** > [**Deployment Group**] > **Alerts**, allow you to manage the list of alerts for all the members of the current deployment group and provides a list of the events raised for the selected item in that group in a tabbed panel in the lower area of the view. Actions allow you to process alerts by flagging them as acknowledged or resolved, or delete alerts from the list.

For managing alerts for all deployment groups, see Alerts View

Column	Description
Severity	Severity level based on the alert rule.
ID	ID of the event for which the alert is generated.
Rule	Alert rule.
Computer	Computer name on which the alert originated.
Deployment Group	Deployment group from which the alert originated.
Last Event	Time the last event was raised for this alert rule.
Status	Status of the alert: Acknowledged, Resolved, New.

Events

Column	Description
ID	Event ID.
Date/Time	Time the event is raised on the client computer.
Computer	Computer on which the event occurred. This may be reported as anonymous if Always use anonymous MACHINE name in events is selected in Auditing.
User	User action which caused the event. This may be reported as anonymous if Always use anonymous USER name in events is selected in Auditing.

Actions

- **Delete Events** — Allows you to select a range of times within which all events will be deleted.
- **Acknowledge** — Flags selected alerts as acknowledged.
- **Resolve** — Flags selected alerts as resolved.
- **Delete** — Deletes all selected alerts.
- **Delete All** — Deletes all alerts.
- **Show Event Details** — Launches the Event Details dialog box for viewing information about the selected event.

Deployment Group Events

The **Home** > [**Server**] > **Deployment Groups** > [**Deployment Group**] > **Events** node lists the events raised by computers in the deployment group according to the configuration settings in the **Deployment Group** > **Settings** > **Auditing** tab.

The Events node lists all of the events reported to the Management Server for viewing and managing.

Column	Description
ID	Event ID number.
Date/Time	The date and time the event was received by the Management Server.
Computer	Name of the Computer on which the event occurred. This may be reported as anonymous if Always use anonymous MACHINE name in events is selected in Auditing.
User	User profile for which the event was generated. This may be reported as anonymous if Always use anonymous USER name in events is selected in Auditing.

Actions

- **Delete** — Deletes the selected events.
- **Delete All** — Deletes all events.
- **Show Event Details** — Launches the Event Details dialog box for viewing information about the selected event.

Event Details

The Event details dialog displays when you double-click an event or select **Show Event Details** in the Actions pane on the right-hand side of a work area.

The Event details dialog allows you to scroll through the list of events to reveal further details about the events, and includes:

- Date
- Time

- Event ID
- Product
- User
- Computer

Packages

Packages View

The Packages view; select the **Packages** navigation button, allows you to upload, delete and view packages which can later be deployed to a managed Endpoint. A package can be one of the following:

- Software Agent - an executable component of the DesktopNow software which takes actions according to DesktopNow product configuration settings. Agent packages are MSI files.
- Configuration file - an installation package that consists of all of your user defined settings for the DesktopNow products. Configuration packages can be MSI or native file format, for example aemp.
- Prerequisite - components required to run the DesktopNow products. MSI or EXE files.
- Patch - An MSP file which contains updates to files or registry keys of an existing MSI file.

The DesktopNow Installer automatically loads agent packages and prerequisites into the Management Center database, including the DesktopNow Deployment Agent and the product agents.

Configuration packages can be added separately by saving to the Management Center from the product consoles or by using the **Add Package** action to select configurations stored as files locally or on the network. Additional product agents which are stored as MSI files locally or on the network can also be added using the Add Package action. The Assigned column indicates which package is currently assigned within a deployment group. The security option allows you to change ownership of specific packages and allocate permissions for users and groups to manage the packages.

Actions

- **Add Package** — Launches the Browse for package dialog which allows you to navigate the local disk or network to select agent MSI files, configuration MSI or a?mp files or patch MSP files to add to the list of available packages on the server. Once you have selected the files, the Agent Upload dialog displays allowing you to install the packages in the database. Multiple packages can be selected for upload.
- **Undo Lock** — Select to remove the lock on a configuration. The Undo Lock dialog displays, select **Yes** to remove the lock and save any edits, **No** to undo any edits and delete the work in progress configuration or **Cancel** to cancel the action.

  When a configuration is opened a work in progress configuration is created where the edits can be made. A work in progress configuration cannot be deployed and remains in this state until it is unlocked.

- **Remove** — Deletes the highlighted packages from the database. If the package is assigned to any deployment group it is removed from the group and uninstalled from the groups

computers.

- Only System Administrators, Package Administrators and users with PackageModifier privileges can remove a package.

> **Caution:** If you select a package to delete that has dependents, all of the dependents will also be deleted.
> For example, if you select 8.7 and 8.7 has the following dependents; 8.7 SP1 and 8.7 SP1 HF1, then those dependents will also be deleted. The Delete Packages dialog displays a list of all dependents and indicates whether any of them are deployed to endpoints.

- **Export Configuration** (*Configurations only*) — Launches the Save As dialog box allowing you to browse to a location and save a copy of the selected configuration as a Windows Installer File (MSI).
- **Security** — Launches the Security for [ObjectName] dialog box in which you can change the Allow/Deny settings in the list of available Security Roles and change the owner of the current object.
- **Rename** — Launches the **Rename Package** dialog box in which you can change the name of the package.
- **Edit Description** — Allows you to customize the description of a package.

Package Upload

Packages are uploaded to the Management Server using the Package Upload Wizard accessed from the Add Package option on the Actions panel.

Only **System Administrators, Package Administrators** and users with **PackageCreator** and **PackageModifier** privileges can upload a package.

This dialog is only required for uploading packages to the database under the following circumstances:

- Updating different versions of product agent packages.
- Uploading configuration packages saved to disk.
- Uploading a patch for distribution.

Add Packages

1. Navigate to the Package Library node and from the Actions panel select **Add Package(s)**.

   The Browse for Package(s) dialog displays.

2. Navigate to the package location and select the package or packages to upload.
3. Click **Open**.

   The Package Upload Details dialog displays.

4. Check the package details and click **Next** to continue with the upload.

   The Package Upload Prerequisites dialog displays. (*only applicable for Agents*)

   A list of all prerequisites required by the agent display. Installed prerequisites have a green tick. If a prerequisite is missing a Browse option displays in the Action column for you to browse to locate and add the missing prerequisite to the Management Center.

5. Once all prerequisites have been located click **Next**. The packages are uploaded, the status bar along the bottom of the dialog indicates the progress. Once complete the Package Upload Complete dialog displays.
6. Click **Finish** to exit the Package Upload wizard.

Package Assignment

Once an agent, patch or configuration package has been uploaded to the Management Server it is available for assignment to a deployment group.

Select the **Home** button in the Navigation pane and select [**Server**] > **Deployment Groups** > [**Deployment Group**] > Packages.

The assigned packages for each product are listed in the work area.

The package type - agent or configuration, product version number, the architecture platform and the description displays for each package.

Actions

- **Quick Setup** - Select to display the Quick Setup wizard for the highlighted product. You can use the quick setup wizard to assign all of the packages for a product to a group.

  You can also access the Quick Setup Wizard by double-clicking the package type.

- **Change Agent Version** (*only available for Agents*) - Select to chose an agent to assign to the deployment group.

  Caution: The latest software patches require Deployment Agent version 8.6 to support deployment and reduce the number of endpoint reboots.
  If Deployment Group 8.6 is a prerequisite for the agent selected, a warning message displays at the top of the work area.

- **Change Configuration** (*only available for Configurations*) - Select to specify a Configuration file and version to assign to the deployment group.
- **Change Revision** (*only available for Configurations*) - Select to assign a different version of the configuration file to the deployment group.
- **Always Use Latest** (*only available for Configurations*) - Select to replace the assigned configuration with the latest version available and click **Yes** to confirm.

- **Remove** - Select to remove the highlighted package from the deployment group. The package is uninstalled in-line with the Installation Schedule.

  Any changes made on this view must be submitted. Click **Review and Submit** at the bottom of the work area to review your pending changes and submit them.

  Caution: Installing, Uninstalling and upgrading agents may require a computer reboot.

Using Quick Setup

Assign a package use the Quick Setup wizard.

The Change Agent Version and Change Configuration Files pages in the wizard can be used to independently.

1. Open the Management Console and in the Navigation pane select **Home**.
2. Navigate to **[Server]** > **Deployment Groups** > **[Deployment Group]** > **Packages**.

   The Packages work area displays a list of all DesktopNow products and their associated packages.
3. Highlight the required product in the work area, for example Environment Manager.
4. In the Actions panel, select **Quick Setup**.

   The Change the packages used by this deployment group dialog displays.
5. Select the required version from the list and click **Next**.
6. Click **Finish**.
7. When you have assigned all packages, click **Review and Submit**.

   The Submit Changes dialog displays a list of all the packages. If you want to remove an individual package click **Undo** next to the package. To exit the dialog, but keep your packages ready for submission at a later time, click **Cancel**.
8. Check the package details are correct and click **Submit**.

   The package is downloaded to the Managed Computer at the next poll period and is held in the Deployment Agent download folder. Agent and Configuration packages install based on the deployment group Installation Schedule.

Package Installation

Once packages are assigned to deployment groups they can be installed on to managed endpoints.

The Deployment Agent must be installed on a computer before any other package can be installed. Alternatively, packages can be installed manually on a computer or by a 3rd party deployment tool, such as Microsoft System Center Configuration Manager (SCCM).

Within the Home navigation view navigate to one of the following locations:

[**Server**] > **All Computers** - displays a global overview of all computers, highlight a computer and select the Packages tab to display a list of packages assigned to that computer.

[**Server**] > **Deployment Groups** > [**Deployment Group**] > **Computers** - displays an overview of all computers within the deployment group, highlight a computer and select the Packages tab to display a list of packages assigned to that computer.

Packages Tab

The Packages tab displays all packages assigned to the selected computer. The display includes the package type - indicated by use of the Agent or Configuration icon, product name, package name, installed version number, installation status and status message.

The Installation Status indicates the progress of the assigned packages, any failed States have a reason displayed in the Status Message Column. Computers display in red in the Computers list if any of their packages are in a failed state.

States

Pending Install

Checking Prerequisites

Installing Prerequisites

Downloading

Download Failed

Installing

Installed

Install Failed

Pending Upgrade

Upgrade Failed

Pending Uninstall

Uninstalling

Uninstall Failed

Uninstalled

Install Prerequisite Failed

Unmanaged - for more information on this state see Deployment Statistics

Remove a Package

You can remove packages from the Management Server. Removing packages permanently removes it from the Management Server and unassigns it from any deployment groups.

1. Select **Packages** from the Navigation Pane.
2. Navigate to the Product that the package to be removed is associated with.
3. Highlight the package that you want to remove.
4. Select **Remove** on the Actions panel.

   A warning message displays.
5. Click **Yes**.

Deployment Statistics

The deployment statistics report on the number of agents and configurations deployed for each of the DesktopNow products. This allows a user to see if they are compliant on license count with the number of licenses they have purchased versus how many agents are deployed.

For each product, data is gathered and reported on in the following three areas:

- Number of agents installed
- Number of configurations installed
- Number of computers with an installed agent that have polled in within the last 30 days

Agents and configurations are included in each count if they have a status of Installed, Pending Uninstall, or Unmanaged.

Statistics display on the Home page showing a general overview of all computers polling to the management server. They also display on the Deployment Group Summary page, showing an overview of all computers in that deployment group.

Unmanaged Packages

An unmanaged package state occurs when an agent is installed on a computer that has a polling Deployment Agent, but no agent package is present in the database for that product, and the install schedule for that deployment group is set to Do not Install Agents.

Unmanaged packages are ignored for all purposes other than deployment statistic counting and are effectively treated as installed.

When dealing with unmanaged packages, you must account for the following:

- Packages installed on a computer are not in the database

  If the Management Server that a managed computer polls into has no agent packages for that product present in the database, and the install schedule set to Do not Install Agents, then agent packages that the Deployment Agent reports as present on the endpoint appear as unmanaged. These packages are included in deployment statistical counts, both globally for the server, and at the deployment group level.

  If an agent package matching the product of the unmanaged agent package is then afterwards added to the Management Server database, then the state of the package changes to Pending Uninstall. The agent package will otherwise remain unaffected, and still be included in the deployment statistic counts, while the deployment group install settings remain set to Do Not Install Agents. No uninstall instructions are sent to the Deployment Agent. The state changes to Installed, if the version of the package matching the previously unmanaged package is then assigned to the deployment group packages.

  In any other case, the agent package is removed as per the agent install schedule.

- Packages are in the database but not assigned to the deployment group

  If the deployment group the managed computer polls into has the install schedule set to Do Not Install Agents, then agent packages appear as Pending Uninstall. They are still included in deployment statistical counts, but no instruction is sent to the Deployment Agent.

  If all agent packages for the product are then afterwards deleted from the Management Center database, and the deployment group install schedule remains set to Do Not Install Agents, then the package state changes to Unmanaged.

  In any other case the agent package is removed as per the agent install schedule.

Prerequisites

Prerequisites View

The Prerequisites view lists all prerequisites that are required for the consoles and the uploaded packages. The view identifies if the prerequisite is installed or missing. The name, platform and version number is also provided for the prerequisites.

The DesktopNow Installer automatically loads prerequisites. However, this can be bypassed allowing you to install prerequisites at a later stage, hence you may have missing prerequisites displayed in the Prerequisites view. You may also upload a package, for example, an agent, that requires prerequisites that are not currently installed. Use the Upload Installer action to upload missing prerequisites.

You can also use the view to delete any prerequisites that are no longer required, and to export them, for example, to provide to another user.

Actions

- **Upload Installer** — Available when a required prerequisite installer is missing. Select the missing prerequisite and select **Upload Installer** to display the Upload Prerequisite dialog. Enter the file location and name or select the ellipsis to browse for the file. Click **Next** to upload the prerequisite file.
- **Export Installer** — Select a prerequisite and select to export the installer for the prerequisite. The Browse For Folder dialog displays, navigate to the required destination folder and click **OK**.

  The name of the prerequisite installer remains the same and cannot be changed.
- **Delete Installer** — Select a prerequisite and select to delete the installer for the prerequisite. A warning message displays for you to confirm the deletion, click **Yes** to continue.

Upload a Prerequisite

Missing prerequisites occur if you bypass installing them in the DesktopNow Installer. Uploaded packages, for example, agents, may also require certain prerequisites that are not currently installed.

The Prerequisites view displays all installed and missing prerequisites required for the consoles and uploaded packages.

1. Select the **Packages** navigation button.
2. Select the **Prerequisites** node.

   The All Prerequisites work area displays.
3. Select the missing prerequisite in the All Prerequisites work area.
4. Select **Upload Installer** in the Actions panel.

   The Upload Prerequisite dialog displays.
5. Browse to the prerequisite, select it and click **Open**.
6. Click **Next** in the Upload Installer dialog.

   The prerequisite is uploaded.
7. Click **Finish**.

   The prerequisite displays in the All Prerequisites work area.

Export a Prerequisite

You can export installed prerequisites, for example, to provide to another user.

1. Click the **Packages** button in the navigation pane.
2. Click the **Prerequisites** node.

   The All Prerequisites work area displays.
3. Select the prerequisite that you want to export in the work area.
4. Select **Export Installer** on the Actions panel.

   The Browse For Folder dialog box displays.
5. Navigate to folder that you want to locate the prerequisite and click **OK**.

The file is exported.

Delete an Installer

You can delete the installer part of prerequisites that are no longer required.

1. Select the **Packages** button in the navigation pane.
2. Select the **Prerequisites** node.

   The All Prerequisites work area displays.
3. Select the prerequisite that you want to delete in the All Prerequisites work area.
4. Select **Delete Installer** on the Actions panel.

   A warning message displays
5. Click **Yes** to confirm deletion.

Alerts

Alerts View

The Alerts view; select the **Alerts** navigation button, allows you to manage alerts and alert rules.

Alerts are triggered by events sent from managed computers according to the alert rules. A predefined set of alert rules is available and you can modify these or create your own. Alert rules must be enabled for alerts to be raised. Some predefined alert rules are *not* enabled by default.

Each alert rule can generate an alert based on an individual event or range of events and can also include criteria for matching events originating on specific computers and from specific users. Alert rules can also include actions for generating alerts via SNMP and SMTP e-mail notifications.

All Alerts

Alert filters sort and handle alerts for events generated by computers in all deployment groups, shown in the following table according to the rules you define in Alert Rules.

For more information about managing alerts for specific deployment groups or computers, see Deployment Group Alerts.

You can filter alerts according to a range of criteria including the acknowledged and resolved states which you apply using the available actions. You can also delete alerts from the lists of alerts or according to the acknowledged or resolved states.

Expand the top-level node to display specific alert filter criteria.

Alert Filters

Filter	Description
All	Displays a global overview of all alerts from computers across all deployment groups.
Created in last day	Displays alerts which have a status of new and that have been raised in the last 24 hours.
Critical	Displays alerts for critical severity events. Critical events have a red indicator preceding the alert. A critical alert is defined in Alerts > Alert Rules > Alert Rule > Details > Severity.
High	Displays alerts for high severity events. High event have an orange indicator preceding the alert. A high alert is defined in Alerts > Alert Rules > Alert Rule > Details > Severity.

Filter	Description
Medium	Displays alerts for medium severity events. Medium events have a yellow indicator preceding the alert. A medium alert is defined in Alerts > Alert Rules > Alert Rule > Details > Severity.
Low	Displays alerts for low severity events. Low events have a green indicator preceding the alert. A low alert is defined in Alerts > Alert Rules > Alert Rule > Details > Severity.
New	Displays alerts for new events. A new alert is defined in the alert **Status** column.
Acknowledged	Displays alerts flagged as acknowledged.
Resolved	Displays alerts flagged as resolved.

Alert Status

When an alert rule gets triggered by an event the Management Server checks if there is an alert for that rule with a status of **New**. If there is, the Management Server adds the event to that alert. If there isn't an alert then a new alert is raised and the event is added to that. Therefore, it is important that once an alert has been seen and the appropriate action taken you set the status to **Acknowledged** or **Resolved** so that you can see a new alert if the problem recurs.

Update the **New** status to **Acknowledged** or **Resolved** in the Status column or from the Actions pane.

Highlight an alert to display a list of all events raised for that alert in the Events tab. Select **Show Event Details** in the Actions pane for further details on a specific event.

Alert Actions

- **Delete Events** — Launches the Delete Events dialog allowing you to select events in a date and time range to delete from the database.
- **Acknowledge** — Flags the selected alerts as acknowledged.
- **Resolve** — Flags the selected alerts as resolved.
- **Delete** — Deletes selected alerts or events.
- **Delete All** — Deletes all alerts. Events remain in the database.
- **Show Event Details** — Launches the Event Details dialog displaying information about the currently highlighted event.

Delete Events

There are three Delete options available:

Delete Events - Launches the Delete Events dialog allowing you to select events in a date and time range to delete from the database.

Delete - Deletes selected alerts or events.

Delete All - Deletes all alerts. Events remain in the database.

You can delete alerts from the lists of alerts or according to the acknowledged or resolved states.

Delete Options

The Delete Events dialog allows you to delete events from the database within a specified date and time range, or all events.

- **Delete all events** — Deletes all events in the Management Server database. Disables the date and time range selection options.
- **Delete events from range** — Deletes events specified within the date range specified the From and To fields.
- **From** — Allows you to specify a start date and time for events to delete from the database.
- **To** — Allows you to specify an end date and time for events to delete from the database.
- You can enter date and time values or select a date from the calendar which displays when you expand the drop-down list for each setting. The time values can be adjusted either by entering values directly or using the keyboard arrow keys to scroll to the required hour, minute and second values.
- **Skip events that are associated with an alert** — Events associated with an alert are not deleted from the database.

Alert Rules

Alert rules allow you to set up alert notifications matched with incoming events sent from client computers to the Management Server. Alert notifications can be sent via SNMP or as e-mail notifications via SMTP. You can assign severity levels to alert notifications according to requirements.

Alert Rules

Rule - Name of the current alert rule.

Enabled - When selected, enables the highlighted alert rule.

Alert Rules Actions

New Rule — Creates a new Rule sub-node below the Alert rules node.

Enable — Enables the highlighted rules and processes related event types to generate alerts according to rule policies.

Disable — Disables the highlighted rules.

Delete — Deletes the highlighted rules.

Security — Opens the Security dialog for the selected alert rule

Alert Rules Sub-nodes

After creating a rule in the Alert rules node, expand the Rule node to configure the **Criteria** and **Actions**.

Alert Rule

The Alert Rule node allows you to specify alert rule names, descriptions, status and severity and view rule criteria and actions. The Actions panel allows you to edit the criteria and actions for the rule in the Criteria and Actions nodes.

The work area contains the following:

Details

- **Name** — Editable text box for entering an alert rule name which should include the number of the event to which the rule applies for easy reference.
- **Description** — Editable text box for entering an alert rule description. The text box expands to allow you to enter detailed descriptions. Click **OK** to confirm the description you have entered.
- **Severity** — Drop-down list for selecting a severity level to apply to the alert rule.
- **Status** — Drop-down list from which to select options to enable or disable the current rule.

Criteria

The Criteria list provides details of the alert rule criteria. You can edit these criteria by expanding the Alert Rule node to display the Criteria node or by selecting the **Edit Criteria** option in the Actions panel.

The Criteria list includes:

- **Event ID** — Events with this ID number generate alerts of this type. For event ID numbers and their descriptions, see the node in the console Deployment Groups.
- **Computer Name** — Events on this computer generate alerts of this type.
- **User Name** — Events caused by this user on the specified computer generate alerts of this type.

Actions

The Actions list displays details of the alert rule actions to perform when an alert of this type is generated. You can edit these actions by expanding the Rule node to display the node or by selecting the **Edit Actions** option in the right-hand Actions panel.

Actions include:

SMTP — Indicates whether SMTP e-mail generation is enabled or disabled.

SNMP — Indicates whether SNMP trap generation is enabled or disabled.

Alert Rule Actions

- **Edit Criteria** — Switches the view to the sub-node for specifying event ID, computer name and user name criteria for generating alerts based on the current rule.
- **Edit Actions** — Switches the view to the Actions sub-node for configuring SNMP and SMTP e-mail notifications about alerts generated by this rule.
- **Delete** — Deletes the highlighted rules.

Default Alert Rules

Alert Rule	Event ID	Severity
Application Execution Denied	9000	High
Application Manager agent ended unexpectedly	9090	Critical
Application Manager agent restarted	9091	Low
Application Manager agent terminated	9092	High
Application Manager unrecoverable	9093	Critical
Application Manager not licensed	9099	Critical
Component Analyzed	9021	Low
Component failed to optimize	9203	High
Component optimized	9202	Low
Computer Assigned to Deployment Group	9712	Medium
Computer startup action fail	9410	High
Computer startup action success	9409	Low
Computer successfully registered with Management Server	9751	Low
CPU clamping off	9105	Medium
CPU clamping on	9104	Medium
Environment Manager agent ended unexpectedly	9390	Critical
Environment Manager agent restarted	9391	Low
Environment Manager agent terminated	9392	HIgh

Alert Rule	Event ID	Severity
Environment Manager agent unrecoverable	9393	Critical
Environment Manager not licensed	8399	Critical
Events failed to upload to the Management Server	9705	High
Events within the Management Server database were deleted	9707	Medium
No valid Application Manager configuration found	9095	Critical
No valid Environment Manager configuration found	9495	Critical
No valid Performance Manager configuration found	9195	Critical
Overwrite changed owner	9002	Medium
Package created, modified or deleted	9702	Medium
Package install or uninstall was successful	9710	Low
package install or uninstall was unsuccessful	9711	Critical
Performance Manager agent ended unexpectedly	9190	Critical
Performance Manager agent restarted	9191	Low
Performance Manager agent terminated	9192	High
Performance Manager agent unrecoverable	9193	Critical
Performance Manager agent not licensed	9199	Critical
Product agent is not compatible with client platform	9708	Medium
Rename changed owner	9003	Medium
Scripted rule failed	9010	High
Security rile created, modified or deleted	9740	High
Self healing file removed	9304	High
Self healing file replaced	9303	High
Self healing registry key removed	9302	High
Self healing registry key replaced	9301	High
User logoff action fail	9408	High

Alert Rule	Event ID	Severity
User logoff action success	9407	Low
User logon fail	9406	High
User logon success	9405	Low
User was created, modified or deleted	9703	High

Alert Rule Criteria

Alert Rule Criteria allow you to specify details of the events which generate this alert and filters to indicate specific computers on which the events occur and specific users causing the events. You can use any combination of these values to create the alert rule.

Criteria values support the use of regular expressions for specifying multiple values or ranges.

Delimiter characters must be used where appropriate. For example, when specifying a domain and computer name or user name, such as:

`Domain`\\Computer `or` Domain\\User.

The Criteria node includes:

- **Event ID** — Enter the ID number of the event type for which you wish to generate this alert. Use regular expressions to specify multiple values or ranges.

  Examples

Regular Expression	Description
9700	Match only event 9700
97[0-9][0-9]	Match any Management Center event
9000|9001	Match either the 9000 or 9001 events

- **Computer Name** — Enter the name of the computer from which the specified event must originate to generate this alert. Use regular expressions to specify multiple values or ranges.

  Examples

Regular Expression	Description
^AB	Matches all computers whose NetBIOS name starts with AB
^SALES_COMP1$	Only matches SALES_COMP1 computer
SALES_COMP1	Matches any computer containing SALES_COMP1, so will match PRESALES_COMP1 and SALES_COMP10 and so on

- **User Name** — Enter the name of the user that causes the specified event to generate this alert. Use regular expressions to specify multiple values or ranges.

  Examples

Regular Expression	Description
^FRED\.BLOGGS$	Matches user FRED.BLOGGS

Alert Rule Action

Configuring Alert Rules

Alert rules allow you to set up alert notifications matched with incoming events sent from client computers to the Management Server. Alert notifications can be sent via SNMP or as e-mail notifications via SMTP. You can assign severity levels to alert notifications according to requirements.

SMTP

The SMTP node allows you to enable or disable e-mail notifications and configure the user to which e-mail notifications are sent regarding this alert.

SMTP Enable

Enable SMTP — When selected, SMTP e-mail notifications are enabled according to the configuration settings when alert rule criteria are met.

SMTP Configuration

SMTP configuration settings allow you to specify the server to which e-mails are sent and the e-mail header details including To, From and Subject details.

Expand Server Settings and E-mail Settings to display the configuration settings.

Property		Configuration
Server Settings	Server	Enter the path to the e-mail server through which e-mail notifications are sent to the specified user.
	User Name	User name with which the Management system accesses the e-mail server.
	Password	Password for the user profile with which the Management System accesses the e-mail server.
E-mail Settings	To	Address to which e-mail notifications are sent about the current alert.
	From	Address from which e-mail notifications are sent about the current alert.
	Subject	Subject line displayed in e-mail notifications about the current alert.

Create a SMTP Alert for Application Execution Denied

You can setup an SMTP alert to send an email when an application execution is denied.

1. Select the **Alerts** button in the navigation pane.
2. Expand the **Alert Rules** node.
3. Select and expand the rule the *Application Execution Denied* rule in the navigation pane.
4. If required, click the **Criteria** node and specify criteria, for example, a user name.
5. Expand the **Actions** node.
6. To send email messages when the alert criteria is met, select the **SMTP** node, select **Enable SMTP** and specify the email settings in the SMTP configuration area.

SNMP

The SNMP node allows you to enable or disable trap generation when alert rule criteria are met.

SNMP Configuration

Enable SNMP — When selected, SNMP traps are generated when alert rule criteria are met.

Create a SNMP Trap

The following steps detail how to generate SNMP traps with the Management Center. These steps should be followed for each Management Server if multiple servers are using the same database.

- Enable the Microsoft SNMP Service on the Management Server

  On Windows Server 2008 R2 or later, use Microsoft Server Manager to ensure that the feature **SNMP Services** > **SNMP Service** is installed.

- Configure the SNMP Service to Raise SNMP Traps:
  - Within the **Services** control panel, launch the property sheet of the SNMP Service.
  - On the Traps tab, set **Community name** to be *public* and click **Add to list**.
  - Under **Trap Destination** click **Add** and enter the name of the local machine.
  - On the Security tab, enable **Send authentication trap**, ensure *public (READ_ONLY)* is added to the **Accepted Community Names** and also enable **Accept SNMP packets from any host**.
  - Restart the SNMP Service and then the AppSense Alerts Service.
- Enable SNMP in the Management Console:

  To generate SNMP traps when the criteria for an alert rule are met:

  - Select the **Alerts** button in the navigation pane.
  - Expand the **Alert Rules** node.
  - Expand the rule that you want to generate the SNMP trap for.
  - Select the **SNMP** node. The SNMP work area displays.
  - Select **Enable SNMP**.

Reports View

The Reports view; select the **Reports** navigation button, allows you to generate a range of reports for the Management Center and each of the DesktopNow products, based on events sent to the server.

Reports

The DesktopNow Installer installs the report templates which are in REPDEFX format. New report templates and updates to existing templates are periodically made available for download from the Ivanti Community.

The Reporting node displays a summary of all the available report templates listed in alphabetical order. The Reporting sub nodes list the report templates by product, such as, Management Center.

Select a template and click **Generate Report** to view results in the work area.

Actions

- **Generate Report** — Generates results for the currently selected template. Specify report filters using the available parameters in the Actions area of the view when the report is selected.
- **Import Reports** — Launches the Open dialog box for browsing to additional report templates downloaded to your local disk or network source. Report templates are packaged in REPDEFX format. Multiple reports can be selected for import.

  If you import an update to an existing template a warning message displays informing you that an existing template will be replaced. Click **Yes** to continue.

  If the software was installed manually using the product MSIs there will be no default reports, use the **Import Reports** option to upload the report packages. From the Open dialog, navigate to the installation folder*Software**Products**Reports*, all available report packs are listed in ARPX format, select the required product report packs and click **Open**. The Reports are added to the database and can be seen in the Management Console. The warning message, described above, displays if you attempt to upload an existing report.
- **Remove Reports** — Deletes any reports which you have selected from the list in the Reports work area. You can select multiple reports. A confirmation box displays and lists the names of the reports you have selected to delete. Click **OK** to complete the action.
- **Security** — Launches the Security for [ObjectName] dialog box. You can change the Allow/Deny settings in the list of available Security Roles and change the owner of the current object.

Default Reports

The default report templates are loaded into the Management Console when the Management Center is installed using the DesktopNow Installer. If the software is installed manually using the product MSIs then you must import the reports from the installation media *Software**Products**Reports*

Default Environment Manager Reports

Computer Startup Action - Provides details of Computer Startup events.

Removable Storage Control Action - Provides details of Removable Storage Control events.

Self Healing Action - Provides details of Self Healing events.

User Logon/Logoff Action - Provides details of User Logon/Logoff events

Default Application Control Reports

Allowed Application Activity - Details of the execution of allowed applications.

Allowed Application Activity (By Client) - Collated details of the execution of allowed applications - Collated by Client Summary.

Allowed Application Activity (By Computer)- Collated details of the execution of allowed applications - Collated by Computer Summary.

Application Activity - Summary of Application Activity.

Application Activity- Detailed - Details of Application Activity.

Application Termination Activity - Application Termination Report.

Client Activity - Summary of Client Activity.

Client Activity- Detailed - Details of Client Activity Report.

Computer Activity - Summary of Computer Activity.

Computer Activity - **Detailed** - Details of Computer Activity.

Event Activity - Summary of Event Activity.

Event Activity - Detailed - Details of Event Activity.

Self-Elevation - Summary of Self-Elevation occurrences.

User Activity - Summary of User Activity.

User Activity - Detailed - Details of User Activity.

User Privilege Management Activity - User Privilege Management Report.

Web Installation Activity - Summary of web installations allowed or denied due to Application Control rules.

Web Installation Discovery - Summary of web installations which were denied due to lack of privileges.

Web Installation Failed - Summary of web installations that failed due to interruption or user cancellation.

Default Performance Manager Reports

Application CPU Usage - Provides details of application CPU usage events

Application memory event details - Provides details of application memory usage events.

Thread throttling - Provides details of thread throttling events.

User memory usage - Provides details of user memory usage events.

Default Management Center Reports

Alerts - Detailed report of alerts and their associated alert rules.

Computers - Overview of Computers.

Deployment Groups - Overview of Deployment Groups.

Events - Detailed report of events and their associated parameters, including event definitions.

Events Definitions - Overview of all Events Definitions.

Package Audit - Overview of Package audit data

Report Filter

The report facility allows you to produce tailored reports by use of the filter parameters.

The filter parameters are available to the right of the work area when you select a specific report template. You can select a specific report template in one of the following ways:

- Reports > Reporting > double-click a report from the list in the work area.
- Reports > Reporting > [Product] > [Reports Template]
- Reports > Reporting > [Product] > double-click a report from the list in the work area.

Report parameters vary according to the product and report type you are generating. Common filter parameters include time and date ranges, event types, computers and users.

Wildcards

Asterisk (*) and question mark (?) wildcard characters are supported in the report parameters. The asterisk represents zero or more characters, and the question mark wildcard represents a single character.

Generate a Report

The Management Center contains a number of predefined reports for each of the products in the DesktopNow suite. You can generate reports to create useful information about events, logon / logoff actions, user activity and so on.

1. Select the **Reports** button in the navigation pane.
2. Do one of the following:
    - Select the **Reporting** node.

      All reports display.
    - Select a report and select **Generate Report** on the Actions panel.
    - Expand the **Reporting** > [**Product**] node.

      Reports corresponding to the product display.
    - Enter filtering criteria in the right pane if required and select **Generate Report**.
3. The generated report displays in the center pane of the console.
4. Use the viewing and editing options to Print, Magnify or Save.

View and Edit Reports

As a report is generated it displays in the work area. Multiple reports can be generated, a new tab in the work area is created for each report. Select a tab to toggle the view between generated reports. Reports can be printed or exported to a range of supported electronic formats. Page margins can be manually adjusted using the control handles displayed in each Report view.

Reports display with a toolbar which includes a flexible range of display and navigation tools, as follows:

- **Document Map** - Shows the report navigation panel which displays the list of contents for the report. Select a heading in the list to jump to a specific location in the report. The document map can be docked to remain hidden when not in use and shown as a tab at the left-hand side of the report. The document map slides open when the cursor hovers over the tab.
- **Search** - Displays the Find dialog. You can search the report for references containing specific characters, words or phrases and includes case and whole word matching.
- **Print** - Displays the Print dialog for printing a report.
- **Print Direct** - Prints the document directly to your default printer.
- **Page Setup** - Allows you to set page layout options including page size, paper source, orientation and margins. Margins can be adjusted manually using the handles shown in the report display.
- **Hand Tool** - Provides easy scrolling of the current report.
- **Zoom** - Allows you to adjust the zoom to a specified value or to make incremental adjustments manually by clicking the buttons to zoom in or out.
- **Page Navigation** - Buttons allow you to jump to the next, previous, first and last pages.
- **Multiple Page Display** - Allows you to select multiple pages to display simultaneously.
- **Color** - Displays a selection palette. You can select an alternative background color for the generated report.

- **Watermark** - Allows you to add a watermark to report pages before printing with a range of watermark display options.
- **Export Document** - Allows you to save the report to disk in a range of output formats including, PDF, Text, CSV, HTML, MHT, Excel (XLS), RTF and BMP.
- **Send E-mail** - Allows you to send the report by e-mail. You are prompted to save the report in one of a range of output formats to a temporary location on the disk. An e-mail is created using your e-mail application and includes the saved report as a file attachment. Complete the address details and add any additional information before sending the e-mail. File attachment output formats include, PDF, Text, CSV, MHT, Excel (XLS), RTF, BMP.
- **Exit** - Closes the report currently displayed.

Import a Report

The Management Center contains a number of predefined reports. Additional reports are occasionally released by Ivanti. New reports can be imported into the Management Center for use against raised events.

1. Select the **Reports** button on the navigation pane.
2. Select the **Reporting** node.

   The All Reports work area displays.
3. Click **Import Reports** on the Actions panel.

   The Open dialog box displays.
4. Browse to and select the report to import and click **Open**.

   The report displays in the work area.
5. To generate the report, click **Generate Report** on the Actions panel.

Delete a Report

The Management Center contains a number of reports. You can delete reports, for example, reports that are no longer required or that are redundant.

1. Select the **Reports** button on the navigation pane.
2. Select the **Reporting** node.

   The All Reports work area displays.
3. Select the report that you want to delete in the work area.
4. Click **Remove Reports** on the Actions panel.

   A warning message displays.
5. Click **Yes** to confirm deletion.

Security

The Security view; select the **Security** navigation button, allows you to setup and manage user and group permissions on the Management Center. Security roles which specify different levels of access allow you to allocate server-wide security permissions or assign object security permissions in certain areas of the Management Console. For example, it may be necessary to lockdown access to specific deployment groups to geographically dispersed administrators so that they can only manage their own local managed endpoints whilst still being able to view (have read-only access) to other deployment groups.

Server Permissions

Server Permissions allow you to define the level of access for designated users and groups throughout the Management Center and specify rights for editing settings and performing actions.

You can add groups or users by browsing the local computer or domain and allocate a security level from the list of predefined Security Roles or allocate custom roles which you create.

You can add Server Permissions by active directory group or user.

Add by Group

Select **Server Permissions** > **Groups** > **Add Group**. The Select Groups dialog displays.

Browse and select from the local computer or domain.

Add by User

Select **Server Permissions** > **Users** > **Add User**. The Select Users dialog displays.

Browse and select from the local computer or domain.

Edit Assigned Roles

To edit the roles assigned to the groups or users select **Server Permissions** > **Groups or Users** > **Edit Roles**. The Global Security Roles dialog displays.

The Global Security Roles dialog displays the list of default Server Roles and any other

server roles that have been created.

Select **Allow** to assign a role to the group or user.

Server Permission Actions

Add User/Add Group - Launches the Select Users or Select Groups dialog boxes for adding users or groups to the list.

Edit Roles - Launches the Global Security Roles dialog box in which you can change the Allow/Deny settings in the list of available Security Roles.

Remove - Deletes the highlighted groups and users from the list.

Object Permissions

Object Permissions are access rights which are allocated to users and groups to view and edit or perform actions for specific areas in the Management Center. Objects include any specific areas of the Management Center, settings or items such as the following:

- Groups – view and edit.
- Packages – manage agents and configurations.
- Reports – view and generate all reports or individual reports.
- Alert Rules – view and edit all alert rules or individual alert rules.

Object permissions are granted to users or groups for specific objects by allocating Security Roles or assigning ownership.

Ownership

Displays the list of objects and the owner allocated to the object. You can change the current ownership assignments for each object.

The following are controlled objects:

- Group – view and edit.
- Package – manage agents and configurations.
- Report – view and generate all reports or individual reports.
- Alert Rule – view and edit all alert rules or individual alert rules.

You can toggle the display to group the objects by type, which is the default, or by owner. Select **Group by Owner** or **Group by Type** in the Actions pane to alter the display.

Ownership of an object grants full control and overrides any restrictions which might also apply to the user or group.

To change the object owner, highlight an object and select **Change Ownership** in the Actions pane. The Security Form dialog displays, select a group or user from the list, alternatively to select a group or user that is not listed, click **Add** to display the Select Users or Groups dialog, enter or browse to select the group or user that you want to be the object owner.

User Access

Displays the list of objects that have been modified for user access.

You can toggle the display to group the objects by type, which is the default, or by user. Select **Group by User** or **Group by Type** in the Actions pane to alter the display.

To change the user access highlight an object and select **Edit Roles** in the Actions pane. The Security for [object type name] dialog displays.

The Security for [object type name] dialog displays the following two tabs:

- **Permissions** - Add or Remove groups or users permission to access the object. If you assign permissions to a group or user that does not have rights to the object area in the Management Console, a warning message displays.

  Click **Yes** to allow the user to login.

  Select the security role to assign to the group or user for the object type.

  Object Security Roles are created in **Security** > **Security Roles** > **Object**.

- **Owner** - Change the owner of the object. You can select an owner from the list or **Add** a new group or user. The owner is granted full control over the object.

Object Permissions Actions

Ownership Actions

Group by Owner - Orders the list of objects by owner.

Group by Type - Orders the list of objects by object type.

Change Ownership - Allows you to assign or change ownership of the current object.

User Access Actions

Group by User - Orders the list of objects by user.

Group by Type - Orders the list of objects by object type.

Delete - Deletes the highlighted groups and users from the list.

Edit Roles - Launches the Security for {ObjectName} dialog box in which you can change the Allow/Deny settings in the list of available Security Roles and change the owner of the current object.

Security Roles

Server Security Roles

Server Security roles are global settings across the whole of the Management Server.

Predefined Server Security Roles

Modifier — permission to edit/modify Groups, Packages, Reports, and Alerts. You cannot create new ones Groups, Packages, Reports, or Alerts.

Server Administrator — full permission. You can see all objects and add, edit, delete objects, even if you are not the owner of the objects. This role is assigned by default to the user installing the Management Center and has Server Administrator permissions enabled, see Role Definition.

Viewer — permission only to view an object.

Custom Server Security Roles

Select **New Server Role** from the Actions pane to define a new role. The Role Definition dialog displays.

The Role Definition dialog lists all server role permissions, select to enable which permissions you want to assign to the new role. The following permissions are available:

- Server Administrator - which are assigned to the Server Administrator role.
- Failover Server Administrator
- Failover Server Viewer
- Deployment Administrator

The following have Administrator, Creator, Modifier and Viewer permissions available:

- Group
- Security
- Package
- Report
- Alert Rule

New Server Role Examples

Example 1

If an administrator wants to delegate the administration of the groups

to someone else they can create a Restricted Group Administrator role with the following

permissions:

- Group Administrator
- Package Viewer
- Package Creator
- Report Viewer
- Alert Rule Viewer
- Deployment Administrator

A user that is assigned the Restricted Administrator role will be able to do the following:

- Create, modify and delete groups and assign computers to those groups.
- Deploy the Deployment Agent to computers.
- View all the packages and be able to assign them to the groups.
- Add new packages and be able to delete those packages.
- Produce reports.

However, the user will not be able to do the following:

- Delete any existing packages.
- Delete any alerts or events.
- Remove or add any reports.
- Change the security for any objects other than the ones they created, or added.

Example 2

If there are individuals that are responsible for creating and maintaining product configurations but do not

require any access to the management console itself then the administrator can create a Package Editor role with the following permission:

- Package Administrator

A user that is assigned this role will be able to open, edit and save configurations to the Management Server using the product consoles.

Object Security Roles

Object Security Roles are settings specific to objects.

Predefined Object Security Roles

- Viewer — permission only to view the object.
- Modifier — permission to perform edit actions, but not delete actions, on the object.
- Full Control — permission to perform edit and delete actions on the object.

Server Roles override Object Roles.

Custom Object Security Roles

Select **New Object Role** from the Actions pane to define a new role. The Role Definition dialog displays.

The Role Definition dialog lists all object role permissions, select to enable which permissions you want to assign to the new role. The following permissions are available:

- Full Control
- Security
- View
- Modify
- Change Ownership
- Report Export
- Computer Assignment
- Alert Rule Assignment
- Event View
- Installation Schedule Modify
- Package Assignment

New Object Role Example

If an administrator wants to delegate the responsibility for assigning packages to a particular group they can create a Package Manager object role with the following permissions:

- View
- Package Assignment

If a user is then added to the Security for a group and given the Package Manager role, the user will only be able to see that group (assuming they have no other roles assigned to them). They will be able to see all of the settings for the group but the only thing they can change would be the packages assigned to the group.

Security Rules Actions

Server

- New Server Role - Define a new server role.
- Properties - View role details.

Object

- New Object Role - Define a new object role.
- Properties - View role details.

Configuring Security

Configure Security for a Group or User

You can configure security for groups or users that are allowed to log onto the Management console. You can grant Server Administrator permission (full permission), Modifier or Viewer permission.

1. Select the **Security** button in the navigation pane.
2. To configure security for a group, expand the **Server Permissions** node and select the **Groups** node.
3. To configure security for a user, expand the **Server Permissions** node and select the **Users** node.
4. Select a group or user.
5. Select **Edit Roles** on the Actions menu. The Global Security Roles dialog box displays.
6. Select whether to allow or deny **Modifier, Server Administrator** or **Viewer permissions**.
7. Click **OK**.

Configure Security for a Group or User

You can configure security for groups that are allowed to log onto the Management console. You can grant permission to only view elements in the console.

1. Select the **Security** button in the navigation pane.
2. Expand the **Server Permissions** node and select the **Groups** node.
3. Select **Add Group** on the Actions menu. The Select Groups dialog box displays.
4. Locate the group that you want to specify view permission for and click **OK**.
5. Select the group in the work area.
6. Select **Edit Roles** on the Actions menu. The Global Security Roles dialog box is display.
7. Select the **Viewer** option in the Allow column.
8. Select the **Modifier** and **Server Administrator** options in the Deny column.
9. Click **OK**.

Configure Security to Provide Access to a Certain Deployment Group

You can configure security for users that are allowed to log onto the Management console. You can grant permission to a group or user to have access to only a particular deployment group.

1. Select the **Security** button in the navigation pane.
2. Expand the Server Permissions node and select the **Users** node.
3. Click **Add User** on the Actions menu. The Select Users dialog box display.
4. Locate the user you want to provide access to a certain deployment group and click **OK**.
5. Select the **Home** button in the navigation pane.
6. Navigate to the [**Server**] > **Deployment Groups** node.
7. Select the deployment group to which you want to provide access.
8. Select **Security** in the Actions panel. The Security for [Deployment Group] dialog box displays.
9. Select the **Permissions** tab and click **Add**. The Select Users or Group dialog box displays.

10. Locate the user specified in Step 4 and click **OK**.
11. In the Roles area select the **Viewer**, **Modifier** and **Full Control** options in the Allow column.
12. Click **OK**.