# Table of Contents

About Management Center ............................................................................................................................................ 8  
Key Benefits .................................................................................................................................................................. 8  
Management Center Components .......................................................................................................................... 9  
Management Console.................................................................................................................................................10  
Management Server ....................................................................................................................................................11  
Database .......................................................................................................................................................................11  
Product Consoles ........................................................................................................................................................12  
Deployment Agent (CCA) ..........................................................................................................................................12  
Concurrency ..................................................................................................................................................................15  
Failover ........................................................................................................................................................................16  
Management Center Security.......................................................................................................................................17  
Security Challenges ......................................................................................................................................................17  
Authentication and Authorization .........................................................................................................................17  
Securing Communications using SSL ...................................................................................................................18  
Management Center Workflow ...................................................................................................................................19  
Step 1 Connect to the Management Server ......................................................................................................19  
Step 2 Create and Configure Deployment Groups ...........................................................................................19  
Step 3 Setup Membership Rules ............................................................................................................................20  
Step 4 Setup Security (Optional) ............................................................................................................................21  
Step 5 Set the Poll Period and Poll Variance .....................................................................................................21  
Step 6 Specify the Installation Schedule .............................................................................................................22  
Step 7 Assign Packages ..............................................................................................................................................22  
Step 8 Setup Alert Rules (Optional) ......................................................................................................................23  
Step 9 Setup Auditing (Optional) ...........................................................................................................................23  
Step 10 Setup Access Credentials ..........................................................................................................................24  
Step 11 Install the Deployment Agent (CCA) on Managed Computers.........................................................25  
Step 12 Install and Configure Failover Servers (Optional) ..............................................................................26  
Deployment Agent (CCA)...............................................................................................................................................28  
Access Credentials ......................................................................................................................................................28  
Deployment Agent (CCA) Communication with the Management Server ..................................................29  
Deployment Agent (CCA) Registering with the Management Server ...........................................................29  
Installing the Deployment Agent (CCA) .............................................................................................................31  
Prerequisites ...............................................................................................................................................................31  
Integrated Install Deployment Agent Functionality ...............................................................................................32
Deployment Groups........................................................................................................................................................................67
Default Deployment Group...............................................................................................................................................................67
Deployment Group ..............................................................................................................................................................................67
Configuring Deployment Groups.........................................................................................................................................................71
Move Computers between Deployment Groups..................................................................................................................................72
Deployment Group Settings General ......................................................................................................................................................73
Server Polling and Downloads ............................................................................................................................................................73
Event Data Uploads............................................................................................................................................................................74
Configuration Deployment Format............................................................................................................................................................75
Deployment Agent Permissions...............................................................................................................................................................75
Deployment Group Settings Installation ..............................................................................................................................................76
Agent Installation....................................................................................................................................................................................76
Configuration Installation.......................................................................................................................................................................79
AppSense Update Manager ..................................................................................................................................................................81
AppSense Update Manager Postponement Message.............................................................................................................................82
AppSense Update Manager Postponement Message for Windows 8 or Windows Server 2012 Users..............................................................82
AppSense Update Manager Countdown Message.................................................................................................................................83
AppSense Update Manager Countdown Message for Windows 8 or Windows Server 2012 Users...............................................................83
Deployment Group Settings Custom Failover Servers......................................................................................................................84
Custom Failover Servers.......................................................................................................................................................................84
Deployment Group Settings Auditing ..................................................................................................................................................87
Application Manager.............................................................................................................................................................................87
Environment Manager...........................................................................................................................................................................89
Performance Manager..........................................................................................................................................................................94
Management Center.............................................................................................................................................................................97
System Events.....................................................................................................................................................................................102
Anonymous Logging..............................................................................................................................................................................102
Event Filter..........................................................................................................................................................................................102
Deployment Group Packages..................................................................................................................................................................103
Changing Agent Version.......................................................................................................................................................................104
Changing Configurations and Configuration Versions..................................................................................................................105
Deployment Group Computers.............................................................................................................................................................106
Computers...........................................................................................................................................................................................106
Manually Added...................................................................................................................................................................................109
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Misgrouped</td>
<td>110</td>
</tr>
<tr>
<td>Deployment Group Alerts</td>
<td>111</td>
</tr>
<tr>
<td>Deployment Group Events</td>
<td>113</td>
</tr>
<tr>
<td>Packages</td>
<td>114</td>
</tr>
<tr>
<td>Packages View</td>
<td>114</td>
</tr>
<tr>
<td>Package Upload</td>
<td>116</td>
</tr>
<tr>
<td>Package Assignment</td>
<td>117</td>
</tr>
<tr>
<td>Package Installation</td>
<td>119</td>
</tr>
<tr>
<td>Remove a Package</td>
<td>120</td>
</tr>
<tr>
<td>Prerequisites</td>
<td>121</td>
</tr>
<tr>
<td>Prerequisites View</td>
<td>121</td>
</tr>
<tr>
<td>Upload a Prerequisite</td>
<td>122</td>
</tr>
<tr>
<td>Export a Prerequisite</td>
<td>122</td>
</tr>
<tr>
<td>Delete an Installer</td>
<td>123</td>
</tr>
<tr>
<td>Alerts</td>
<td>124</td>
</tr>
<tr>
<td>Alerts View</td>
<td>124</td>
</tr>
<tr>
<td>All Alerts</td>
<td>124</td>
</tr>
<tr>
<td>Delete Events</td>
<td>126</td>
</tr>
<tr>
<td>Alert Rules</td>
<td>127</td>
</tr>
<tr>
<td>Alert Rule</td>
<td>128</td>
</tr>
<tr>
<td>Alert Rule Criteria</td>
<td>132</td>
</tr>
<tr>
<td>Alert Rule Action</td>
<td>133</td>
</tr>
<tr>
<td>Configuring Alert Rules</td>
<td>133</td>
</tr>
<tr>
<td>SMTP</td>
<td>133</td>
</tr>
<tr>
<td>SNMP</td>
<td>134</td>
</tr>
<tr>
<td>Reports View</td>
<td>136</td>
</tr>
<tr>
<td>Reports</td>
<td>136</td>
</tr>
<tr>
<td>Default Reports</td>
<td>137</td>
</tr>
<tr>
<td>Report Filter</td>
<td>138</td>
</tr>
<tr>
<td>Generate a Report</td>
<td>139</td>
</tr>
<tr>
<td>View and Edit Reports</td>
<td>139</td>
</tr>
<tr>
<td>Import a Report</td>
<td>140</td>
</tr>
<tr>
<td>Delete a Report</td>
<td>140</td>
</tr>
<tr>
<td>Security</td>
<td>141</td>
</tr>
<tr>
<td>Server Permissions</td>
<td>141</td>
</tr>
</tbody>
</table>
About Management Center

AppSense Management Center is the framework that enables the AppSense products, Application Manager, Environment Manager and Performance Manager to be used across an entire enterprise. AppSense Management Center is a scalable multi-tier system which enables the central management and secure deployment of configuration information to thousands of endpoint and user environments. The Management Center incorporates comprehensive auditing and reporting with failover support provided for server resiliency.

Key Benefits

- Scalable and secure Management Framework for all AppSense products.
- Microsoft SQL Server backend.
- Microsoft Active Directory integration.
- Diagnostic capabilities.
- Management Server Failover and Proxy Support.
- Integrated Alerting System for notification of product events (Low, Medium, High, Critical).
- Role-based Access Control - server and object roles define view, modify and delete permissions allowing a fine level of granular security to manage user control over Management Server objects.
- Revision Control - supporting single user locking of configurations and adding metadata by saving changes.
- A rich management console built on the Microsoft .NET Framework.
- Built-in Reporting.
Management Center Components

The Management Center comprises of the Management Server, Microsoft SQL Server, Management Console and the Deployment Agent (CCA) 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 Server SQL database from where they can be downloaded along with product agents by the Deployment Agent for installation on managed machines.
Management Console

The AppSense Management Console provides an interface to the AppSense Management Server and the other components of AppSense 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 AppSense DesktopNow product consoles; Application Manager, 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 AppSense software agent, configuration packages and any prerequisites on the Management Server.

- **Alerts** - Add and manage alerts and alert rules for AppSense software events sent to the server from client computers.

- **Reports** - Import and generate a range of reports for AppSense products.

- **Security** - Manage server and object permissions and role-based access rights to the Management Center console views and settings.

**Note**

The Navigation pane is collapsible allowing you to create more viewing space for the other areas of the console. Click the arrow in the lower right corner of the pane to display a menu allowing you to show fewer buttons or to add and remove buttons.
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 Help.

Database

The Management Center relies on the availability on the network of a Microsoft SQL server for the storage and retrieval of AppSense 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 AppSense DesktopNow Install and Configure Guide.
Product Consoles

The AppSense product consoles, including Application Manager, 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 found at www.appsense.com/help

Deployment Agent (CCA)

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

The Deployment Agent (CCA) 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 (CCA) 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 (CCA) 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 (CCA) 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.

**Note**

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.

**Note**

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:
   - Select Default Web Site > Edit Bindings > Site Bindings
   - Select the row which has a HTTP or HTTPS Type, click Edit
   - 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

   **Note**
   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 (CCA) 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 (CCA). The Deployment Agent (CCA) 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 (CCA) 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 AppSense Management Center 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 AppSense 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 AppSense 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:


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.

Note
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 the AppSense Management Center and managed computers. 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 > AppSense > 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.
   [Tip] 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.

**Note**

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.


   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 Container 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.

   **Note**
   
   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 (CCA) checks the Management Server for changes to the AppSense 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.

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.

Tip
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.

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.

Note
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.
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 **Enable SMTP** 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 Manager
- 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 (CCA) on any endpoint, Access Credentials must be supplied. The list of credentials are used by the Management Server to install the Deployment Agent (CCA) 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.
   The Access Credentials work area displays.
4. 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 (CCA) on Managed Computers

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

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

1. Download the Deployment Agent (CCA) installation package from the Management Server website and run the installation package on the client computer.

2. The Deployment Agent (CCA) can be installed manually by running the installation package or silently using a command line prompt.

3. Deploy the Deployment Agent (CCA) 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


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 (CCA) is installed, the service registers with the Management Server at the website address you supplied during installation. After the Deployment Agent (CCA) 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 (CCA) 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 (CCA) 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.

**Note**
For more information about installing the Management Server, see the *AppSense 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 (CCA)

The Deployment Agent (CCA) is a software agent that must be deployed to all clients managed by the AppSense Management Center. The Deployment Agent (CCA) 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 AppSense agents and configurations and the collection and uploading of auditing information from any AppSense product agent.

The Deployment Agent (CCA) 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 (CCA) 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 (CCA) 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 AppSense product agents. The Deployment Agent (CCA) 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 (CCA).

These credentials must be supplied before attempting to install the Deployment Agent (CCA) 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 (CCA) 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 (CCA), 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 (CCA) Communication with the Management Server

When communicating with the Management Server, the Deployment Agent (CCA) 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 (CCA) 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 AppSense 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 (CCA) Registering with the Management Server

Once the Deployment Agent (CCA) 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 (CCA) is installed directly via the Install Deployment Agent option within the Management Console, it will automatically register with the Management Server.
- Deployment Agent (CCA) 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 (CCA) is installed manually from the command line including a valid Management Server URL and optionally, a specific Deployment Group with which to self-register.

Note

The Deployment Agent (CCA) can only self-register if Allow self-registration is selected in
If a Deployment Group (CCA) 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 (CCA) registers with the server, the AppSense 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 (CCA) upgrades can be installed mid-session without a reboot depending on the deployment group settings.
Installing the Deployment Agent (CCA)

The Deployment Agent (CCA) must be installed on all endpoints to be managed by AppSense 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 (CCA) 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 (CCA).

You can run the Install Deployment Agent functionality in small and medium scale enterprise environments to deploy the Deployment Agent (CCA) 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 (CCA) 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 (CCA) 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 (CCA) 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 (CCA) 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 (CCA) 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.

**Note**
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.

Note
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 (CCA) 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 (CCA) on any endpoint using the integrated Install Deployment Agent functionality if the credentials have not been set up.

Step 4 - Install Deployment Agent (CCA)


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.

Note
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 (CCA) using an Installation Schedule

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

The Deployment Agent (CCA) 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.

**Note**

You must specify Access Credentials before Management Center can install the Deployment Agent (CCA).

Management Center deploys the Deployment Agent (CCA) installation package that has been assigned to the group. If you did not assign a Deployment Agent (CCA) 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 (CCA) 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.

**Note**

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

After the Deployment Agent (CCA) 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 (CCA) regularly polls the server for updates and changes to the deployment policy, according to the deployment group settings.
Install the Deployment Agent (CCA) Manually

You can manually install the Deployment Agent (CCA) on a managed computer by downloading and running the Deployment Agent (CCA) 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

   **Note**
   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 AppSense DesktopNow.

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

   **Note**
   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 Manager, Environment Manager and Performance Manager consoles, and prerequisites software.

3. In the Deployment Agent (CCA) 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**.


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

7. Click **Next** to proceed.

8. When the installation is complete, click **Finish** to exit the installation wizard.

   You have now successfully installed the AppSense Deployment Agent (CCA). 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 (CCA) in Silent Mode

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

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

**Note**

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 (CCA)

Allow Deployment Agent to Self-Register with a Deployment Group

You can set up a deployment group to allow the Deployment Agent (CCA) 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 (CCA) 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 (CCA) 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 (CCA) 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.
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 (CCA) 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:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>/url</td>
<td>Changes the url used to communicate with the Management Server. You can optionally include a Deployment Group with which to self-register. This requires <strong>Allow self-registration</strong> to be enabled in the Deployment Group Settings.</td>
</tr>
<tr>
<td>/imageprep</td>
<td>Prepares this computer for provisioning, the computer will be registered on the next poll. This command can be combined with the /unregister command.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td>When running /imageprep, the Deployment Agent (CCA) will automatically <strong>Check for and download new Configurations at Startup</strong> regardless of the Deployment Group Settings.</td>
</tr>
<tr>
<td>/unregister</td>
<td>Unregisters the Deployment Agent (CCA) from the Management Server and stops the Deployment Agent (CCA) service. Does not uninstall any AppSense agents or configurations. This requires <strong>Allow unregistration</strong> to be enabled in the Deployment Group Settings.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td>Once a computer has been unregistered the Deployment Agent (CCA) Service must be restarted for the computer to re-register.</td>
</tr>
<tr>
<td>/updateagents</td>
<td>Initiates install of agents assigned to the Deployment Group, overriding the Installation Schedule. This requires <strong>Allow update initiation</strong> 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 (CCA) is still applying updates.</td>
</tr>
<tr>
<td>/updateconfigs</td>
<td>Initiates install of configurations assigned to the Deployment Group, overriding the Installation Schedule. This requires <strong>Allow update initiation</strong> to be enabled in the Deployment Group Settings. The updating of configurations is asynchronous. Use /isupdating to check if the Deployment Agent (CCA) is still applying updates.</td>
</tr>
<tr>
<td>/isupdating</td>
<td>Determines whether a previous call to /updateagents or /updateconfigs is still processing updates.</td>
</tr>
</tbody>
</table>
Deployment Agent (CCA) Diagnostics

Diagnostics provide the administrator with an overall view of the health of the Deployment Agent (CCA) 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 (CCA) 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 (CCA) 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 (CCA) 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 (CCA) 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.

Note
This test only verifies that events can be sent from the Deployment Agent (CCA) 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

AppSense Management Center enables you to manage individual AppSense product licenses, and full AppSense DesktopNow licenses for computers across your Enterprise. Product licenses are managed using the AppSense DesktopNow Licensing console when AppSense 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 AppSense 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 AppSense, open the file and copy the license key, paste it in to the Add License Key dialog.
   - If you received a LIC file from AppSense, 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 (CCA) 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

AppSense DesktopNow 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 appsense.com 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 AppSense 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**.
   - **Note**
     - The base MSI package for the selected patch must have previously been uploaded.
   - The Package Upload wizard displays.
5. Check the details of the selected package and optionally enter a description.
6. Click **Next** to start the upload.
7. 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, 8.4 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.
   Note
   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

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

Note
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

Note
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

Note
This uninstalls all associated MSP files.

Rolling-Back Patches

Using AppSense 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 AppSense DesktopNow products, Application Manager, 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.

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 (CCA) 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 that have been generated in the 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 the Management 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 (CCA) 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 (CCA) 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 (CCA) never loses contact with the Management Server. A URL can be removed from the list of servers to which Deployment Agents connect, by deseleting the URL Enabled option.
Failover Servers List

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

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server</td>
<td>The URL address of the failover server. Displayed in one of the following formats and may also include port specifications:</td>
</tr>
<tr>
<td></td>
<td>• Server host name: <a href="http://MyServer:80/ManagementServer">http://MyServer:80/ManagementServer</a></td>
</tr>
<tr>
<td></td>
<td>• IP address: <a href="http://123.456.789.0/ManagementServer">http://123.456.789.0/ManagementServer</a></td>
</tr>
<tr>
<td></td>
<td>• Fully qualified path: <a href="http://MyServer.MyDomain.com/ManagementServer">http://MyServer.MyDomain.com/ManagementServer</a></td>
</tr>
<tr>
<td>Diagnostics</td>
<td>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.</td>
</tr>
<tr>
<td>Enabled</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Deployment Agent self-tests check the following:</td>
</tr>
<tr>
<td></td>
<td>• Connectivity.</td>
</tr>
<tr>
<td></td>
<td>• Package downloads.</td>
</tr>
<tr>
<td></td>
<td>• Event uploads.</td>
</tr>
<tr>
<td></td>
<td>• Ability to raise high priority events, such as failure to install packages.</td>
</tr>
<tr>
<td>Server</td>
<td>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.</td>
</tr>
<tr>
<td>Enabled</td>
<td>This can be used when decommissioning a server by preventing Deployment Agents connecting to the server.</td>
</tr>
</tbody>
</table>
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.
  
  **Caution**
  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 (CCA). These credentials must be supplied before attempting to install the Deployment Agent (CCA) 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.

   Tip
   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.

   Note
   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, AppSense software agent and configuration packages and computer details.

The Computers node includes the following sections:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Computer name.</td>
</tr>
<tr>
<td>Alerts</td>
<td>Number of active alerts.</td>
</tr>
<tr>
<td>Last Response</td>
<td>The period since the last poll.</td>
</tr>
<tr>
<td>Status</td>
<td>The latest information received when installing the Deployment Agent (CCA) and any status information sent from the endpoint, including pending diagnostics, failed deployments and failed diagnostics.</td>
</tr>
<tr>
<td>Deployed (%)</td>
<td>Indicates the status of the packages assigned to the deployment group for each computer. 100% indicates that the assigned packages have all been installed (or uninstalled).</td>
</tr>
</tbody>
</table>
Control Tabs

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

- **Computer Details** - displays information about the selected computer, and includes the computer hardware and system details.

- **Alerts** - allows you to monitor alerts for the selected computer, and includes the alert rule to which the alert belongs, the alert severity and the alert status.

- **Events** - allows you to monitor events on the selected computer, and includes the event number, the date and time the event occurred and the computer and username of where the event occurred if anonymous logging is not turned on.

- **Packages** - allows you to view packages on the selected computer, and includes the package name, version, the product to which the package belongs, the installation status, for example, installed, pending install or pending uninstall.

- **Diagnostics** - provides details of the diagnostics test on the selected computer and the result of each test performed.
  
  Test - indicates which test from the following has been performed:
  
  - Connectivity
  - Download of Packages
  - High Priority Events
  - Upload of 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 Log** - 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 (CCA) installed. Enter a full string or partial strings in the edit field to match computer names using wildcard characters, including:

1. Question mark (?) - Indicates a single character
2. 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** - AppSense product agents and configurations uninstall according to the Installation Schedule.
  
  - **Deployment Agent (CCA)** - The Deployment Agent (CCA) uninstalls after product agents have uninstalled, according to the Installation Schedule.

  **Note**
  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.

  **Note**
  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:

   a. Deployment Group > Computers > Move action - select the computer(s), click Move and select the required deployment group.

   b. 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.

   **Note**
   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:

1. 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.

2. 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.

3. A computer is moved to a different Active Directory group, which puts the computer in a different deployment group.

4. 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 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.

**Note**

Moving computers to another deployment group can cause AppSense 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.
Licensing

AppSense Management Center enables you to manage individual AppSense product licenses, and full AppSense DesktopNow licenses for computers across your Enterprise. Product licenses are managed using the AppSense DesktopNow Licensing console when AppSense 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 AppSense 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 AppSense, open the file and copy the license key, paste it in to the Add License Key dialog.
   - If you received a LIC file from AppSense, 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 (CCA) 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.
Events

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

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

Actions

- **Delete** - Deletes the selected alerts.
- **Delete All** - Deletes all alerts.
- **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 select **Show Event Details** in the Actions panel when on the Events node.

The following details for the selected event display:

- Date
- Time
- Event ID
- Product
- User
- Computer
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 AppSense product.

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.

**Note**
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**


Select the computer to which you want to deploy the Deployment Agent (CCA) 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.

1. Select one or more computers in the list.
2. Click **Move** in the Actions panel.
   - The Move Computers dialog box displays.
3. Select the deployment group to move the computers to and click **Move**.
   - The computers are relocated to the new group.
4. Check the destination deployment group to view the computer in the new location.
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 (CCA) 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.

**Note**

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%.

**Note**

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.

**Note**

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 (CCA) persists the configuration file using the file name `configuration.amp`. 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.

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

**Caution**
The Deployment Agent (CCA) 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 (CCA) 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 (CCA) 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.

  **Tip**
  If a computer has been unregistered by the CCA Command tool the Deployment Agent (CCA) 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 (CCA) 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:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Suggested Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automatically restart system and install - at next client poll, with user postponement.</td>
<td>You need to push out an update quickly, such as an important patch release or hot fix.</td>
</tr>
<tr>
<td>Automatically restart system and install - scheduled.</td>
<td>You need to push out updates in a predictable manner. For example, when an installation is required by a certain time of day.</td>
</tr>
<tr>
<td>At next system restart.</td>
<td>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.</td>
</tr>
</tbody>
</table>

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:

  - 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:

<table>
<thead>
<tr>
<th>Day</th>
<th>Start</th>
<th>End</th>
<th>Enabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sunday</td>
<td>00:00</td>
<td>00:00</td>
<td></td>
</tr>
<tr>
<td>Monday</td>
<td>00:00</td>
<td>00:00</td>
<td></td>
</tr>
<tr>
<td>Tuesday</td>
<td>00:00</td>
<td>00:00</td>
<td></td>
</tr>
<tr>
<td>Wednesday</td>
<td>00:00</td>
<td>00:00</td>
<td></td>
</tr>
<tr>
<td>Thursday</td>
<td>00:00</td>
<td>00:00</td>
<td></td>
</tr>
<tr>
<td>Friday</td>
<td>00:00</td>
<td>00:00</td>
<td></td>
</tr>
<tr>
<td>Saturday</td>
<td>00:00</td>
<td>00:00</td>
<td></td>
</tr>
</tbody>
</table>

  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.

**Note**

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 (CCA) 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.

**Tip**
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 (CCA) 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.

**Note**
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.
AppSense 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 (CCA), 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 (CCA) carries out the actions in the following sequence based on the packages assigned to the endpoint:

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

**Note**

When simultaneously deploying an agent and configuration for the same product, the Deployment Agent (CCA) 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.
AppSense 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.

**Note**
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.

AppSense 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.

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

**Note**
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.

AppSense 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.

**Note**
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 (CCA) 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:

- 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 (CCA) 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:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server</td>
<td>The URL address of the failover server. Displayed in one of the following formats and may also include port specifications:</td>
</tr>
<tr>
<td></td>
<td>• Server host name: <a href="http://MyServer:80/ManagementServer">http://MyServer:80/ManagementServer</a></td>
</tr>
<tr>
<td></td>
<td>• IP address: <a href="http://123.456.789.0/ManagementServer">http://123.456.789.0/ManagementServer</a></td>
</tr>
<tr>
<td></td>
<td>• Fully qualified path: <a href="http://MyServer.MyDomain.com/ManagementServer">http://MyServer.MyDomain.com/ManagementServer</a></td>
</tr>
<tr>
<td>Diagnostics</td>
<td>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.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Deployment Agent (CCA) 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.</td>
</tr>
<tr>
<td></td>
<td>Deployment Agent (CCA) self-tests check the following:</td>
</tr>
<tr>
<td></td>
<td>• Connectivity.</td>
</tr>
<tr>
<td></td>
<td>• Package downloads.</td>
</tr>
<tr>
<td></td>
<td>• Event uploads.</td>
</tr>
<tr>
<td></td>
<td>• Ability to raise high priority events, such as failure to install packages.</td>
</tr>
<tr>
<td>Server</td>
<td>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.</td>
</tr>
<tr>
<td>Enabled</td>
<td></td>
</tr>
</tbody>
</table>
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.

  **Caution**
  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 Manager

<table>
<thead>
<tr>
<th>ID</th>
<th>Name</th>
<th>Description</th>
<th>Log Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>9000</td>
<td>Denied Execution</td>
<td>Prohibited execution request.</td>
<td>Warning</td>
</tr>
<tr>
<td>9001</td>
<td>Allowed Execution</td>
<td>Allowed execution request.</td>
<td>Information</td>
</tr>
<tr>
<td>9002</td>
<td>Overwrite Changed Owner</td>
<td>Overwrite of an allowed executable.</td>
<td>Warning</td>
</tr>
<tr>
<td>9003</td>
<td>Rename Changed Owner</td>
<td>Rename of a prohibited executable.</td>
<td>Warning</td>
</tr>
<tr>
<td>9004</td>
<td>Application Limit Denial</td>
<td>Application limit denial.</td>
<td>Warning</td>
</tr>
<tr>
<td>9005</td>
<td>Time Limit Denial</td>
<td>Time limit denial.</td>
<td>Warning</td>
</tr>
<tr>
<td>9006</td>
<td>Self-Authorization</td>
<td>Self-authorization decision by user.</td>
<td>Warning</td>
</tr>
<tr>
<td>9007</td>
<td>Self-Authorized allow</td>
<td>Self-authorization execution request.</td>
<td>Warning</td>
</tr>
<tr>
<td>9009</td>
<td>Scripted Rule Timeout</td>
<td>Script execution timed out.</td>
<td>Warning</td>
</tr>
<tr>
<td>9010</td>
<td>Scripted Rule Fail</td>
<td>Script failed to complete.</td>
<td>Warning</td>
</tr>
<tr>
<td>9011</td>
<td>Scripted Rule Success</td>
<td>Script completed successfully</td>
<td>Information</td>
</tr>
<tr>
<td>9012</td>
<td>Trusted Vendor Denial</td>
<td>Digital Certificate failed Trusted Vendor check.</td>
<td>Warning</td>
</tr>
<tr>
<td>9013</td>
<td>Network Item denied</td>
<td>Prohibited Network Item request.</td>
<td>Warning</td>
</tr>
<tr>
<td>9014</td>
<td>Network Item allowed</td>
<td>Allowed Network Item request.</td>
<td>Information</td>
</tr>
<tr>
<td>9015</td>
<td>Application Started</td>
<td>An allowed application started running.</td>
<td>Information</td>
</tr>
<tr>
<td>9016</td>
<td>Unable to Change Ownership</td>
<td>The file’s ownership could not be changed.</td>
<td>Error</td>
</tr>
<tr>
<td>ID</td>
<td>Name</td>
<td>Description</td>
<td>Log Type</td>
</tr>
<tr>
<td>------</td>
<td>----------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td>9017</td>
<td>Application Termination</td>
<td>A prohibited application has been terminated by Application Manager.</td>
<td>Information</td>
</tr>
<tr>
<td>9018</td>
<td>Application User Rights Changed</td>
<td>The application’s user rights have changed.</td>
<td>Information</td>
</tr>
<tr>
<td>9019</td>
<td>AM allowed install</td>
<td>Allowed web Installation request.</td>
<td>Information</td>
</tr>
<tr>
<td>9020</td>
<td>AM restricted install</td>
<td>Restricted web installation request.</td>
<td>Information</td>
</tr>
<tr>
<td>9021</td>
<td>Windows restricted install (Basic Discovery Mode)</td>
<td>Windows restricted web installation request.</td>
<td>Information</td>
</tr>
<tr>
<td>9022</td>
<td>Web Installation Fail</td>
<td>Web installation failed to complete</td>
<td>Warning</td>
</tr>
<tr>
<td>9023</td>
<td>Self-Elevation</td>
<td>Self-Elevation request</td>
<td>Information</td>
</tr>
<tr>
<td>9024</td>
<td>URL Redirection</td>
<td>URL Redirection has occurred.</td>
<td>Information</td>
</tr>
<tr>
<td>9051</td>
<td>Policy Change granted</td>
<td>A Policy Change Request has been granted</td>
<td>Information</td>
</tr>
<tr>
<td>9052</td>
<td>Policy Change invalid response code</td>
<td>An invalid response code has been entered for a Policy Change request.</td>
<td>Error</td>
</tr>
<tr>
<td>9053</td>
<td>User-requested allow</td>
<td>An allowed Policy Change application has started</td>
<td>Information</td>
</tr>
<tr>
<td>9054</td>
<td>User-requested elevate</td>
<td>An elevated Policy Change application has started</td>
<td>Information</td>
</tr>
<tr>
<td>9096</td>
<td>Configuration merge success</td>
<td>The configuration merge has completed successfully</td>
<td>Information</td>
</tr>
<tr>
<td>9097</td>
<td>Configuration merge fail</td>
<td>The configuration merge has failed</td>
<td>Error</td>
</tr>
<tr>
<td>9098</td>
<td>Configuration merge timeout</td>
<td>The configuration merge is still waiting for expected files</td>
<td>Warning</td>
</tr>
<tr>
<td>9099</td>
<td>Agent not licensed</td>
<td>AppSense Application Manager is not licensed.</td>
<td>Error</td>
</tr>
</tbody>
</table>
## Environment Manager

<table>
<thead>
<tr>
<th>ID</th>
<th>Name</th>
<th>Description</th>
<th>Log Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>9300</td>
<td>Self healing process started</td>
<td>A process being monitored for self healing stopped and has been restarted.</td>
<td>Information</td>
</tr>
<tr>
<td>9301</td>
<td>Self healing registry key replaced</td>
<td>A registry key being monitored for self healing was changed and has now been reset.</td>
<td>Information</td>
</tr>
<tr>
<td>9302</td>
<td>Self healing registry key removed</td>
<td>A registry key being monitored for self healing was inserted and has now been removed.</td>
<td>Information</td>
</tr>
<tr>
<td>9303</td>
<td>Self healing file replaced</td>
<td>A file being monitored for self healing was modified or removed and has now been replaced.</td>
<td>Information</td>
</tr>
<tr>
<td>9304</td>
<td>Self healing file removed</td>
<td>A file being monitored for self healing was added and has now been removed.</td>
<td>Information</td>
</tr>
<tr>
<td>9305</td>
<td>Self healing service stopped</td>
<td>A service being monitored for self healing started and has now been stopped.</td>
<td>Information</td>
</tr>
<tr>
<td>9306</td>
<td>Self healing service started</td>
<td>A service being monitored for self healing stopped and has now been restarted.</td>
<td>Information</td>
</tr>
<tr>
<td>9307</td>
<td>Self healing registry value replaced</td>
<td>A registry value being monitored for self healing was changed and has now been reset.</td>
<td>Information</td>
</tr>
<tr>
<td>9308</td>
<td>Self healing registry removed</td>
<td>A registry value being monitored for self healing was inserted and has now been removed.</td>
<td>Information</td>
</tr>
<tr>
<td>9399</td>
<td>Software is not licensed</td>
<td>The Environment Manager software has not been licensed.</td>
<td>Error</td>
</tr>
<tr>
<td>9400</td>
<td>Lockdown edit control blocked drive</td>
<td>An edit control has had a blocked drive entered into it.</td>
<td>Information</td>
</tr>
<tr>
<td>9401</td>
<td>Lockdown edit control blocked text</td>
<td>An edit control has had blocked text entered into it.</td>
<td>Information</td>
</tr>
<tr>
<td>9402</td>
<td>Lockdown accelerator keys blocked</td>
<td>An application has had accelerator keys blocked.</td>
<td>Information</td>
</tr>
<tr>
<td>9403</td>
<td>Lockdown dialog blocked</td>
<td>An application has had a dialog box blocked.</td>
<td>Information</td>
</tr>
<tr>
<td>9404</td>
<td>Lockdown MSAA access blocked</td>
<td>An application has had access blocked for a control using MSAA detection.</td>
<td>Information</td>
</tr>
<tr>
<td>ID</td>
<td>Name</td>
<td>Description</td>
<td>Log Type</td>
</tr>
<tr>
<td>------</td>
<td>-----------------------------------</td>
<td>---------------------------------------------------------------</td>
<td>-----------</td>
</tr>
<tr>
<td>9405</td>
<td>User logon action success</td>
<td>A user logon action completed successfully.</td>
<td>Information</td>
</tr>
<tr>
<td>9406</td>
<td>User logon action fail</td>
<td>A user logon action failed to complete successfully.</td>
<td>Error</td>
</tr>
<tr>
<td>9407</td>
<td>User logoff action success</td>
<td>A user logoff action completed successfully.</td>
<td>Information</td>
</tr>
<tr>
<td>9408</td>
<td>User logoff action fail</td>
<td>A user logoff action failed to complete successfully.</td>
<td>Warning</td>
</tr>
<tr>
<td>9409</td>
<td>Computer startup action success</td>
<td>A computer startup action completed successfully.</td>
<td>Information</td>
</tr>
<tr>
<td>9410</td>
<td>Computer startup action fail</td>
<td>A computer startup action failed to complete successfully.</td>
<td>Warning</td>
</tr>
<tr>
<td>9413</td>
<td>Computer network available</td>
<td>A computer network available action completed successfully.</td>
<td>Information</td>
</tr>
<tr>
<td>9414</td>
<td>Computer network available action fail</td>
<td>A computer network available action failed to complete successfully.</td>
<td>Information</td>
</tr>
<tr>
<td>9420</td>
<td>User session reconnect action success</td>
<td>A user session reconnect action completed successfully.</td>
<td>Information</td>
</tr>
<tr>
<td>9421</td>
<td>User session reconnect action fail</td>
<td>A user session reconnect action failed to complete successfully.</td>
<td>Warning</td>
</tr>
<tr>
<td>9422</td>
<td>User session disconnect action success</td>
<td>A user session disconnect action completed successfully.</td>
<td>Information</td>
</tr>
<tr>
<td>9423</td>
<td>User session disconnect action fail</td>
<td>A user session disconnect action failed to complete successfully.</td>
<td>Warning</td>
</tr>
<tr>
<td>9424</td>
<td>User session locked action success</td>
<td>A user session locked action completed successfully.</td>
<td>Information</td>
</tr>
<tr>
<td>9425</td>
<td>User session locked action fail</td>
<td>A user session action failed to complete successfully.</td>
<td>Warning</td>
</tr>
<tr>
<td>9426</td>
<td>User session unlocked action success</td>
<td>A user session unlocked action completed successfully.</td>
<td>Information</td>
</tr>
<tr>
<td>9427</td>
<td>User session unlocked action fail</td>
<td>A user session unlocked action failed to complete successfully.</td>
<td>Warning</td>
</tr>
<tr>
<td>9428</td>
<td>Process start action success</td>
<td>A process start action completed successfully.</td>
<td>Information</td>
</tr>
<tr>
<td>9429</td>
<td>Process start action fail</td>
<td>A process start action failed to complete successfully.</td>
<td>Warning</td>
</tr>
<tr>
<td>ID</td>
<td>Name</td>
<td>Description</td>
<td>Log Type</td>
</tr>
<tr>
<td>------</td>
<td>--------------------------------------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>-----------</td>
</tr>
<tr>
<td>9430</td>
<td>Process stopped action success</td>
<td>A process stopped action completed successfully.</td>
<td>Information</td>
</tr>
<tr>
<td>9431</td>
<td>Process stopped action fail</td>
<td>A process stopped action failed to complete successfully.</td>
<td>Warning</td>
</tr>
<tr>
<td>9432</td>
<td>Network connection action success</td>
<td>A network connected action completed successfully.</td>
<td>Information</td>
</tr>
<tr>
<td>9433</td>
<td>Network connection action fail</td>
<td>A network connected action failed to complete successfully.</td>
<td>Warning</td>
</tr>
<tr>
<td>9434</td>
<td>Network disconnected action success</td>
<td>A network disconnected action completed successfully.</td>
<td>Information</td>
</tr>
<tr>
<td>9435</td>
<td>Network disconnected action fail</td>
<td>A network disconnected action failed to complete successfully.</td>
<td>Warning</td>
</tr>
<tr>
<td>9436</td>
<td>User logon (pre-session) action success</td>
<td>A user logon (pre-session) action completed successfully.</td>
<td>Information</td>
</tr>
<tr>
<td>9437</td>
<td>User logon (pre-session) action fail</td>
<td>A user logon (pre-session) action failed to complete successfully.</td>
<td>Information</td>
</tr>
<tr>
<td>9438</td>
<td>User logon (pre-desktop) action success</td>
<td>A user logon (pre-desktop) action completed successfully.</td>
<td>Information</td>
</tr>
<tr>
<td>9439</td>
<td>User logon (pre-desktop) action fail</td>
<td>A user logon (pre-desktop) action failed to complete successfully.</td>
<td>Information</td>
</tr>
<tr>
<td>9440</td>
<td>User logon (desktop created) action success</td>
<td>A user logon (desktop created) action completed successfully.</td>
<td>Information</td>
</tr>
<tr>
<td>9441</td>
<td>User logon (desktop created) action fail</td>
<td>A user logon (desktop created) action failed to complete successfully.</td>
<td>Information</td>
</tr>
<tr>
<td>9480</td>
<td>Configuration merge update</td>
<td>The configuration merge folder has been updated.</td>
<td>Information</td>
</tr>
<tr>
<td>9481</td>
<td>Configuration merge start</td>
<td>The configuration merge has started.</td>
<td>Information</td>
</tr>
<tr>
<td>9482</td>
<td>Configuration merge complete</td>
<td>The configuration merge has completed successfully.</td>
<td>Information</td>
</tr>
<tr>
<td>9483</td>
<td>Configuration merge fail</td>
<td>The configuration merge has failed.</td>
<td>Information</td>
</tr>
<tr>
<td>9484</td>
<td>Configuration merge timeout</td>
<td>The configuration merge has timed out waiting for expected files.</td>
<td>Information</td>
</tr>
<tr>
<td>ID</td>
<td>Name</td>
<td>Description</td>
<td>Log Type</td>
</tr>
<tr>
<td>------</td>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>9495</td>
<td>Not configured</td>
<td>AppSense Environment Manager has not been configured.</td>
<td>Warning</td>
</tr>
<tr>
<td>9496</td>
<td>Configuration unsupported</td>
<td>An old configuration has been found.</td>
<td>Warning</td>
</tr>
<tr>
<td>9650</td>
<td>Managed application start</td>
<td>A managed application has started</td>
<td>Information</td>
</tr>
<tr>
<td>9651</td>
<td>Managed application stop</td>
<td>A managed application has stopped</td>
<td>Information</td>
</tr>
<tr>
<td>9652</td>
<td>Personalization load error</td>
<td>Personalization settings for a managed application failed to load.</td>
<td>Error</td>
</tr>
<tr>
<td>9653</td>
<td>Personalization save error</td>
<td>Personalization settings for a managed application failed to save.</td>
<td>Error</td>
</tr>
<tr>
<td>9654</td>
<td>Blacklisted process started</td>
<td>A managed process has launched a blacklisted process.</td>
<td>Information</td>
</tr>
<tr>
<td>9655</td>
<td>Personalization not saved</td>
<td>Personalization settings not saved as another group application is running.</td>
<td>Information</td>
</tr>
<tr>
<td>9656</td>
<td>Offline resiliency save started</td>
<td>Offline resiliency save has been started for a managed application.</td>
<td>Information</td>
</tr>
<tr>
<td>9657</td>
<td>Offline resiliency save complete</td>
<td>Offline resiliency has successfully saved a managed application’s personalization settings.</td>
<td>Information</td>
</tr>
<tr>
<td>9658</td>
<td>Personalization settings purged</td>
<td>Personalization settings purged as offline mode is disabled.</td>
<td>Information</td>
</tr>
<tr>
<td>9659</td>
<td>Personalization settings updated</td>
<td>User personalization settings updated from personalization server.</td>
<td>Information</td>
</tr>
<tr>
<td>9660</td>
<td>Personalization failed</td>
<td>Personalization for a managed application failed.</td>
<td>Error</td>
</tr>
<tr>
<td>9661</td>
<td>Timeout Communicating with Personalization Server</td>
<td>A timeout occurred while trying to communicate with the Personalization Server.</td>
<td>Warning</td>
</tr>
<tr>
<td>9662</td>
<td>Trigger Action Times</td>
<td>All the actions have run for the trigger.</td>
<td>Information</td>
</tr>
<tr>
<td>9663</td>
<td>PreCache Application Success</td>
<td>Successfully Precached Managed Application.</td>
<td>Information</td>
</tr>
<tr>
<td>9664</td>
<td>PreCache Group Success</td>
<td>Successfully PreCached Managed Application Group.</td>
<td>Information</td>
</tr>
<tr>
<td>ID</td>
<td>Name</td>
<td>Description</td>
<td>Log Type</td>
</tr>
<tr>
<td>------</td>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>9665</td>
<td>PreCache Managed Application Failure</td>
<td>Failed to PreCached Managed Application.</td>
<td>Error</td>
</tr>
<tr>
<td>9666</td>
<td>PreCache Group Failure</td>
<td>Failed to PreCached Managed Application Group.</td>
<td>Error</td>
</tr>
<tr>
<td>9667</td>
<td>Personalization Profile Import</td>
<td>A Profile Import is Active</td>
<td>Information</td>
</tr>
<tr>
<td>9680</td>
<td>Endpoint of Self Service start failure</td>
<td>The Endpoint Self-Service process failed to start</td>
<td>Error</td>
</tr>
</tbody>
</table>

**Personalization Server Events**

<table>
<thead>
<tr>
<th>ID</th>
<th>Name</th>
<th>Description</th>
<th>Log Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>9600</td>
<td>Failed to connect to Personalization Database</td>
<td>The Personalization Server failed to connect to the Personalization Database.</td>
<td>Error</td>
</tr>
<tr>
<td>9601</td>
<td>Windows Impersonation Logon Failed.</td>
<td>The Personalization Server failed to log on, using Windows Impersonation, with the credentials supplied via the Server Configuration Utility.</td>
<td>Error</td>
</tr>
<tr>
<td>9602</td>
<td>Failed database compatibility check</td>
<td>The protocol version used by the Personalization Server database is incompatible with the version used by the Personalization Server.</td>
<td>Error</td>
</tr>
</tbody>
</table>
## Performance Manager

<table>
<thead>
<tr>
<th>ID</th>
<th>Name</th>
<th>Description</th>
<th>Log Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>9100</td>
<td>User Memory Usage Warning</td>
<td>Amount of memory consumed by a user has exceeded a warning level set in a User Memory Limit.</td>
<td>Information</td>
</tr>
<tr>
<td>9101</td>
<td>User memory usage warning lapsed</td>
<td>Amount of memory consumed by a user has fallen back to a safe level as defined in a User Memory Limit.</td>
<td>Information</td>
</tr>
<tr>
<td>9102</td>
<td>User memory usage blocked</td>
<td>Amount of memory available to this user as defined in a User Memory rule has been exceeded. No more memory allocation will be allowed.</td>
<td>Warning</td>
</tr>
<tr>
<td>9103</td>
<td>User memory usage blocking lapsed</td>
<td>Amount of memory consumed by a user has fallen back to a safe (non-blocked) level as defined in a User Memory Limit.</td>
<td>Information</td>
</tr>
<tr>
<td>9104</td>
<td>Thread Throttling Clamping On</td>
<td>Total CPU Usage has exceeded a threshold and will be clamped.</td>
<td>Information</td>
</tr>
<tr>
<td>9105</td>
<td>Thread Throttling Clamping Off</td>
<td>Total CPU Usage has fallen under a threshold and clamping will stop.</td>
<td>Information</td>
</tr>
<tr>
<td>9106</td>
<td>Application CPU Usage clamping On</td>
<td>An Application has exceeded its configured hard CPU Usage limit and will be limited to that configured limit.</td>
<td>Information</td>
</tr>
<tr>
<td>9107</td>
<td>Per Application Memory Usage Exceeded</td>
<td>Memory usage for a particular application has exceeded a threshold.</td>
<td>Information</td>
</tr>
<tr>
<td>9108</td>
<td>Per Application Memory Usage Reduced</td>
<td>Memory usage for a particular application has dropped below a threshold.</td>
<td>Information</td>
</tr>
<tr>
<td>9109</td>
<td>Per Application Memory Usage Terminated</td>
<td>An application has been terminated because it used too much memory.</td>
<td>Warning</td>
</tr>
<tr>
<td>9110</td>
<td>Application CPU Usage Clamping Off</td>
<td>An application has now fallen below its CPU Usage limit and will no longer be clamped.</td>
<td>Information</td>
</tr>
<tr>
<td>9115</td>
<td>Working set trimmed</td>
<td>Working set for an application has been trimmed.</td>
<td>Information</td>
</tr>
<tr>
<td>9116</td>
<td>CPU Affinity changed</td>
<td>CPU Affinity of an application has changed.</td>
<td>Information</td>
</tr>
<tr>
<td>9119</td>
<td>Per Application Hard Memory Limit Reached</td>
<td>Memory usage for an application reached its hard memory limit</td>
<td>Warning</td>
</tr>
<tr>
<td>9120</td>
<td>Thread Throttling - Clamped Processes</td>
<td>Total CPU Usage has exceeded a threshold and applications will be clamped.</td>
<td>Information</td>
</tr>
<tr>
<td>ID</td>
<td>Name</td>
<td>Description</td>
<td>Log Type</td>
</tr>
<tr>
<td>------</td>
<td>-------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td>9121</td>
<td>Application CPU Soft Limit - Started</td>
<td>Because of the overall CPU Usage a CPU soft limit will be applied to an application.</td>
<td>Information</td>
</tr>
<tr>
<td>9122</td>
<td>Application CPU Soft Limit - Stopped</td>
<td>An application will be no longer controlled by a CPU soft limit.</td>
<td>Information</td>
</tr>
<tr>
<td>9123</td>
<td>Application CPU Reservation Applied</td>
<td>A CPU Usage reservation was applied to an application.</td>
<td>Information</td>
</tr>
<tr>
<td>9124</td>
<td>Disk - Process I/O Queued</td>
<td>One or more processes were subject to I/O queuing.</td>
<td>Information</td>
</tr>
<tr>
<td>9150</td>
<td>Windows Performance Counter Error</td>
<td>The Windows performance counters on this machine are missing or broken.</td>
<td>Error</td>
</tr>
<tr>
<td>9170</td>
<td>Settings not found in package</td>
<td>Some configuration settings were not found in the configuration package.</td>
<td>Error</td>
</tr>
<tr>
<td>9171</td>
<td>Settings not valid in package</td>
<td>Some configuration settings in the configuration package were not valid.</td>
<td>Error</td>
</tr>
<tr>
<td>9172</td>
<td>Settings loaded from package</td>
<td>The configuration settings were successfully loaded from the configuration package.</td>
<td>Information</td>
</tr>
<tr>
<td>9173</td>
<td>Settings applied live to the Agent</td>
<td>The configuration settings were applied live to a running Performance Manager Agent.</td>
<td>Information</td>
</tr>
<tr>
<td>9174</td>
<td>Package has been loaded and all settings applied</td>
<td>All settings in the package have been applied to the Agent.</td>
<td>Information</td>
</tr>
<tr>
<td>9175</td>
<td>The package is invalid</td>
<td>The configuration package is invalid.</td>
<td>Error</td>
</tr>
<tr>
<td>9176</td>
<td>Package not found</td>
<td>The configuration package does not exist.</td>
<td>Warning</td>
</tr>
<tr>
<td>9177</td>
<td>Valid License Found</td>
<td>Performance Manager is licensed.</td>
<td>Information</td>
</tr>
<tr>
<td>9198</td>
<td>Invalid License Found</td>
<td>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.</td>
<td>Error</td>
</tr>
<tr>
<td>9199</td>
<td>Valid License Not Found</td>
<td>Performance Manager is not licensed.</td>
<td>Error</td>
</tr>
<tr>
<td>9200</td>
<td>Application Analyzed</td>
<td>Memory Optimizer has analyzed a known application.</td>
<td>Information</td>
</tr>
<tr>
<td>9201</td>
<td>Component Analyzed</td>
<td>Memory Optimizer has analyzed a known component.</td>
<td>Information</td>
</tr>
<tr>
<td>ID</td>
<td>Name</td>
<td>Description</td>
<td>Log Type</td>
</tr>
<tr>
<td>------</td>
<td>-------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>9202</td>
<td>Component Optimized</td>
<td>Memory Optimizer has optimized a known component.</td>
<td>Information</td>
</tr>
<tr>
<td>9203</td>
<td>Component failed to Optimize</td>
<td>AppSense Performance Manager has failed to optimize a component</td>
<td>Warning</td>
</tr>
<tr>
<td>9204</td>
<td>Application Identified At Runtime</td>
<td>Memory Optimizer has analyzed a running process and added a new application to the optimization database.</td>
<td>Information</td>
</tr>
<tr>
<td>9205</td>
<td>Component Identified At Runtime</td>
<td>Memory Optimizer has analyzed a loaded component in a process and added it to the optimization database.</td>
<td>Information</td>
</tr>
<tr>
<td>9206</td>
<td>Database Analyzed</td>
<td>Memory Optimizer has analyzed all known applications within the optimization database.</td>
<td>Information</td>
</tr>
<tr>
<td>9207</td>
<td>Database Optimized</td>
<td>Memory Optimizer has optimized all known applications within the optimization database.</td>
<td>Information</td>
</tr>
<tr>
<td>9208</td>
<td>Application Optimized</td>
<td>Memory Optimizer has optimized a known application.</td>
<td>Information</td>
</tr>
<tr>
<td>9209</td>
<td>Database Cleaned</td>
<td>Memory Optimizer has cleaned the optimization database.</td>
<td>Information</td>
</tr>
<tr>
<td>9210</td>
<td>Application Cleaned</td>
<td>Memory Optimizer has cleaned a known application.</td>
<td>Information</td>
</tr>
<tr>
<td>9211</td>
<td>Component Cleaned</td>
<td>Memory Optimizer has cleaned a known component.</td>
<td>Information</td>
</tr>
<tr>
<td>9212</td>
<td>Out Of Memory</td>
<td>Memory Optimizer has run out of memory and cannot rebase any more DLLs.</td>
<td>Error</td>
</tr>
<tr>
<td>9216</td>
<td>Statistics Collection Strategy</td>
<td>Details of the statistics configuration.</td>
<td>Information</td>
</tr>
<tr>
<td>9217</td>
<td>Invalid Local Database Folder</td>
<td>The local statistics database folder is invalid.</td>
<td>Error</td>
</tr>
<tr>
<td>9218</td>
<td>General Local Statistics Service Error</td>
<td>An error occurred in the Local Statistics Service.</td>
<td>Error</td>
</tr>
<tr>
<td>9219</td>
<td>Disk Cleanup Started</td>
<td>Started cleaning up the local statistics database folder.</td>
<td>Information</td>
</tr>
<tr>
<td>9220</td>
<td>Disk Cleanup of Single Database</td>
<td>Deleted a single old local database.</td>
<td>Information</td>
</tr>
<tr>
<td>9221</td>
<td>Disk Cleanup Complete</td>
<td>Started cleaning up the local statistics database folder.</td>
<td>Information</td>
</tr>
<tr>
<td>9222</td>
<td>Consolidation Search Started</td>
<td>Started searching for databases to consolidate.</td>
<td>Information</td>
</tr>
<tr>
<td>ID</td>
<td>Name</td>
<td>Description</td>
<td>Log Type</td>
</tr>
<tr>
<td>------</td>
<td>-------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td>9223</td>
<td>Single File Consolidation Started</td>
<td>Started to transfer a local statistics database for consolidation.</td>
<td>Information</td>
</tr>
<tr>
<td>9224</td>
<td>Single File Consolidation Completed</td>
<td>Completed the transfer of a local statistics database for consolidation.</td>
<td>Information</td>
</tr>
<tr>
<td>9225</td>
<td>Consolidation Search Completed</td>
<td>Finished searching for databases to consolidate.</td>
<td>Information</td>
</tr>
<tr>
<td>9226</td>
<td>Statistics Scheduled Collection</td>
<td>Statistics collection is now scheduled at a new collection level.</td>
<td>Information</td>
</tr>
<tr>
<td>9228</td>
<td>Database Import Failed</td>
<td>An incoming database could not be imported.</td>
<td>Error</td>
</tr>
<tr>
<td>9229</td>
<td>Database Connection Failed</td>
<td>Could not connect to the configured Reporting Database.</td>
<td>Error</td>
</tr>
<tr>
<td>9230</td>
<td>Disk Cleanup Started</td>
<td>Started searching for old received databases to delete.</td>
<td>Information</td>
</tr>
<tr>
<td>9231</td>
<td>Disk Cleanup Completed</td>
<td>Finished searching for old received databases to delete.</td>
<td>Information</td>
</tr>
<tr>
<td>9232</td>
<td>Purge of Reporting Database Started</td>
<td>Started purging the Reporting Database.</td>
<td>Information</td>
</tr>
<tr>
<td>9233</td>
<td>Purge of Reporting Database Completed</td>
<td>Finished purging the Reporting Database.</td>
<td>Information</td>
</tr>
<tr>
<td>9234</td>
<td>Error in Central Statistics Server</td>
<td>An error occurred in the Central Statistics Service.</td>
<td>Information</td>
</tr>
<tr>
<td>9235</td>
<td>Deployment Agent updated native configuration</td>
<td>Detected Deployment Agent has updated the endpoint native configuration path.</td>
<td>Information</td>
</tr>
<tr>
<td>9236</td>
<td>Memory exceeded minimum threshold new processes eligible for memory limitations</td>
<td>The system memory has exceeded the minimum threshold. New processes will be eligible for memory limitations.</td>
<td>Information</td>
</tr>
<tr>
<td>9237</td>
<td>Memory exceeded minimum threshold</td>
<td>The system memory has fallen back below the minimum threshold. New processes will not be monitored for memory limitations.</td>
<td>Information</td>
</tr>
<tr>
<td>ID</td>
<td>Name</td>
<td>Description</td>
<td>Log Type</td>
</tr>
<tr>
<td>-----</td>
<td>-------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-----------</td>
</tr>
<tr>
<td>9090</td>
<td>Service Ended Unexpectedly</td>
<td>The Application Manager Agent has ended unexpectedly.</td>
<td>Information</td>
</tr>
<tr>
<td></td>
<td>(Application Manager)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9091</td>
<td>Service Restarted</td>
<td>The Application Manager Agent has restarted.</td>
<td>Information</td>
</tr>
<tr>
<td></td>
<td>(Application Manager)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9092</td>
<td>Service Terminated</td>
<td>The Application Manager Agent has been terminated due to</td>
<td>Information</td>
</tr>
<tr>
<td></td>
<td></td>
<td>being in the starting or stopping state for a prolonged period.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(Application Manager)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9093</td>
<td>Service Unrecoverable</td>
<td>The Application Manager Agent has exceeded the maximum</td>
<td>Information</td>
</tr>
<tr>
<td></td>
<td></td>
<td>restart attempts.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(Application Manager)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9190</td>
<td>Service Ended Unexpectedly</td>
<td>The Performance Manager Agent has ended unexpectedly.</td>
<td>Information</td>
</tr>
<tr>
<td></td>
<td>(Performance Manager)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9191</td>
<td>Service Restarted</td>
<td>The Performance Manager Agent has restarted.</td>
<td>Information</td>
</tr>
<tr>
<td></td>
<td>(Performance Manager)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9192</td>
<td>Service Terminated</td>
<td>The Performance Manager Agent has been terminated due to</td>
<td>Information</td>
</tr>
<tr>
<td></td>
<td></td>
<td>being in the starting or stopping state for a prolonged period.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(Performance Manager)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9193</td>
<td>Service Unrecoverable</td>
<td>The Performance Manager Agent has exceeded the maximum</td>
<td>Information</td>
</tr>
<tr>
<td></td>
<td></td>
<td>restart attempts.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(Performance Manager)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9390</td>
<td>Service Ended Unexpectedly</td>
<td>The Environment Manager User Virtualization Service ended</td>
<td>Information</td>
</tr>
<tr>
<td></td>
<td></td>
<td>unexpectedly.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(Environment Manager)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9391</td>
<td>Service Restarted</td>
<td>The Environment Manager User Virtualization Service has</td>
<td>Information</td>
</tr>
<tr>
<td></td>
<td></td>
<td>restarted.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(Environment Manager)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9392</td>
<td>Service Terminated</td>
<td>The Environment Manager User Virtualization Service has been</td>
<td>Information</td>
</tr>
<tr>
<td></td>
<td></td>
<td>terminated due to being in the starting or stopping state for a</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>prolonged period.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(Environment Manager)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ID</td>
<td>Name</td>
<td>Description</td>
<td>Log Type</td>
</tr>
<tr>
<td>------</td>
<td>-------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td>9393</td>
<td>Service Unrecoverable (Environment Manager)</td>
<td>The Environment Manager User Virtualization Service has exceeded the maximum restart.</td>
<td>Information</td>
</tr>
<tr>
<td>9700</td>
<td>Action Notification Success</td>
<td>An action notification was dispatched successfully.</td>
<td>Information</td>
</tr>
<tr>
<td>9701</td>
<td>Action Notification Failure</td>
<td>An action notification has failed to dispatch.</td>
<td>Information</td>
</tr>
<tr>
<td>9702</td>
<td>Package Modified</td>
<td>Package created, modified or deleted.</td>
<td>Information</td>
</tr>
<tr>
<td>9703</td>
<td>User Modified</td>
<td>A user was created, modified or deleted.</td>
<td>Information</td>
</tr>
<tr>
<td>9704</td>
<td>Priority Event Failure</td>
<td>A priority event failed to upload to the Management Server.</td>
<td>Information</td>
</tr>
<tr>
<td>9705</td>
<td>Event Upload Failure</td>
<td>One or more events failed to upload to the Management Server.</td>
<td>Information</td>
</tr>
<tr>
<td>9707</td>
<td>Events Purged</td>
<td>Events within the Management Server were deleted.</td>
<td>Information</td>
</tr>
<tr>
<td>9708</td>
<td>Platform Mismatch Package</td>
<td>Product agent is not compatible with client platform.</td>
<td>Information</td>
</tr>
<tr>
<td>9710</td>
<td>Package Installation Success</td>
<td>A package has been installed or uninstalled successfully by the Deployment Agent.</td>
<td>Information</td>
</tr>
<tr>
<td>9711</td>
<td>Package Installation Failure</td>
<td>A package has been unsuccessfully installed or uninstalled by the Deployment Agent.</td>
<td>Information</td>
</tr>
<tr>
<td>9712</td>
<td>Computer Registration</td>
<td>A computer has been assigned to a deployment group.</td>
<td>Information</td>
</tr>
<tr>
<td>9713</td>
<td>Failover Change URL</td>
<td>The Deployment Agent reverted to another Management Server due to connectivity problems.</td>
<td>Information</td>
</tr>
<tr>
<td>9715</td>
<td>Computer Self-registration</td>
<td>A computer has self registered with a deployment group.</td>
<td>Information</td>
</tr>
<tr>
<td>9716</td>
<td>Computer Self-registration Failed</td>
<td>A computer has failed to self-register with a deployment group.</td>
<td>Information</td>
</tr>
<tr>
<td>9718</td>
<td>Deployment Agent Installed License</td>
<td>The Deployment Agent installed a license.</td>
<td>Information</td>
</tr>
<tr>
<td>9720</td>
<td>BITS Server Extensions Not Installed</td>
<td>The Events Dispatcher service could not detect that BITS Server Extensions was installed.</td>
<td>Information</td>
</tr>
<tr>
<td>ID</td>
<td>Name</td>
<td>Description</td>
<td>Log Type</td>
</tr>
<tr>
<td>-----</td>
<td>-------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>--------------</td>
</tr>
<tr>
<td>9730</td>
<td>Prerequisite Failed Check</td>
<td>A prerequisite failed due to ‘fail-if’ check.</td>
<td>Information</td>
</tr>
<tr>
<td>9731</td>
<td>Prerequisite Failed to Install</td>
<td>A prerequisite failed to install.</td>
<td>Information</td>
</tr>
<tr>
<td>9732</td>
<td>RPC Access Denied</td>
<td>Blocked endpoint request by the user (not running as an Administrator)</td>
<td>Warning</td>
</tr>
<tr>
<td>9733</td>
<td>RPC Set Deployment URL and Group Name</td>
<td>Administrator endpoint request to set Deployment Server URL and optional Group Name</td>
<td>Information</td>
</tr>
<tr>
<td>9734</td>
<td>RPC Update Agents</td>
<td>Administrator endpoint request to update all local agents.</td>
<td>Information</td>
</tr>
<tr>
<td>9735</td>
<td>RPC Update Configs</td>
<td>Administrator endpoint request to update all local configurations</td>
<td>Information</td>
</tr>
<tr>
<td>9736</td>
<td>RPC Query Updating Status</td>
<td>Administrator endpoint request to query update status for agent and configurations</td>
<td>Information</td>
</tr>
<tr>
<td>9737</td>
<td>RPC Image Prep</td>
<td>Administrator endpoint request for Image Prep</td>
<td>Information</td>
</tr>
<tr>
<td>9738</td>
<td>RPC Unregister</td>
<td>Administrator endpoint request to unregister from the Management Server.</td>
<td>Information</td>
</tr>
<tr>
<td>9740</td>
<td>Security Role Modified</td>
<td>A security role was created, modified, or deleted.</td>
<td>Information</td>
</tr>
<tr>
<td>9743</td>
<td>Computer self unregistration</td>
<td>A computer has unregistered from a deployment group.</td>
<td>Information</td>
</tr>
<tr>
<td>9744</td>
<td>Computer self unregistration failed</td>
<td>A computer has failed to unregister from the deployment group.</td>
<td>Information</td>
</tr>
<tr>
<td>9745</td>
<td>SQL AlwaysOn Failover</td>
<td>A SQL/Network error has occurred.</td>
<td>Information</td>
</tr>
<tr>
<td>9750</td>
<td>Deployment Agent HTTP error</td>
<td>The Deployment Agent failed to contact to the Management Server.</td>
<td>Information</td>
</tr>
<tr>
<td>9751</td>
<td>Deployment Agent registration</td>
<td>The Deployment Agent registered with the server.</td>
<td>Information</td>
</tr>
<tr>
<td>9752</td>
<td>Deployment Agent joined group</td>
<td>The Deployment Agent joined its assigned deployment group.</td>
<td>Information</td>
</tr>
<tr>
<td>9754</td>
<td>Deployment Agent Diagnostics Test</td>
<td>The Deployment Agent ran a diagnostics test on a server.</td>
<td>Information</td>
</tr>
<tr>
<td>ID</td>
<td>Name</td>
<td>Description</td>
<td>Log Type</td>
</tr>
<tr>
<td>-------</td>
<td>-------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>9755</td>
<td>BITS Error</td>
<td>BITS Error.</td>
<td>Error</td>
</tr>
<tr>
<td>9756</td>
<td>Deployment Agent BITS Service Error</td>
<td>The Deployment Agent identified an error with the BITS service. The service cannot be started, either because the service is disabled or because it has no enabled devices associated with it.</td>
<td>Error</td>
</tr>
<tr>
<td>9760</td>
<td>Deployment Agent Deployed Successfully</td>
<td>The Deployment Agent has been successfully deployed to a discovered machine.</td>
<td>Information</td>
</tr>
<tr>
<td>9761</td>
<td>Deployment Agent Deployment Failure</td>
<td>The Deployment Agent has failed to deploy to a discovered machine.</td>
<td>Information</td>
</tr>
<tr>
<td>9790</td>
<td>Service ended unexpectedly</td>
<td>The Deployment Agent has ended unexpectedly.</td>
<td>Information</td>
</tr>
<tr>
<td>9791</td>
<td>Service restarted</td>
<td>The Deployment Agent has restarted.</td>
<td>Information</td>
</tr>
<tr>
<td>9792</td>
<td>Service terminated</td>
<td>The Deployment Agent has been terminated due to being in the starting or stopping state for a prolonged period.</td>
<td>Information</td>
</tr>
<tr>
<td>9793</td>
<td>Service unrecoverable</td>
<td>The Deployment Agent has exceeded its maximum restart attempts.</td>
<td>Information</td>
</tr>
<tr>
<td>9795</td>
<td>Condition Modified</td>
<td>A deployment group condition has been modified. This may affect which computers get assigned to the deployment group.</td>
<td>Information</td>
</tr>
<tr>
<td>9901</td>
<td>License not valid</td>
<td>[product name] was checked for a valid license and failed.</td>
<td>Information</td>
</tr>
</tbody>
</table>
System Events

<table>
<thead>
<tr>
<th>ID</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8000</td>
<td>Service Started</td>
<td>[ProductName] Agent: Service Started.</td>
</tr>
<tr>
<td>8095</td>
<td>No Configuration found</td>
<td>[ProductName] cannot find a valid configuration.</td>
</tr>
<tr>
<td>8096</td>
<td>Configuration Upgraded</td>
<td>A configuration for a previous version of [ProductName] has been detected and upgraded.</td>
</tr>
<tr>
<td>8099</td>
<td>Invalid License</td>
<td>[ProductName] software is not licensed.</td>
</tr>
</tbody>
</table>

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.

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

  **Note**
  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 choose 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:

   
   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.

   **Note**
   The latest software patches require Deployment Agent (CCA) 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:

   
   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.
   
   **Note**
   
   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, AppSense 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:

- **Computer Details** - displays information about the selected computer, and includes the computer hardware and system details.
- **Alerts** - allows you to monitor alerts for the selected computer, and includes the alert rule to which the alert belongs, the alert severity and the alert status.
- **Events** - allows you to monitor events on the selected computer, and includes the event number, the date and time the event occurred and the computer and username of where the event occurred if anonymous logging is not turned on.
- **Packages** - allows you to view packages on the selected computer, and includes the package name, version, the product to which the package belongs, the installation status, for example, installed, pending install or pending uninstall.
- **Diagnostics** - provides details of the diagnostics test on the selected computer and the result of each test performed.
  
  **Test** - indicates which test from the following has been performed:
  - Connectivity
  - Download of Packages
  - High Priority Events
  - Upload of 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 Log** - 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 (CCA) 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 (CCA) 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 (CCA)** - The Deployment Agent (CCA) uninstalls after product agents have uninstalled, according to the Installation Schedule.
- **Product Agents and Configurations** - AppSense product agents and configurations uninstall according to the Installation Schedule.

**Note**
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.

**Note**
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:
   a. Select the Computers node for the required deployment group and click Move from the Actions panel.
   b. 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.

**Note**

Moving computers to another deployment group can cause AppSense 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

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

Events

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

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

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

The AppSense DesktopNow Installer automatically loads agent packages and prerequisites into the Management Center database, including the AppSense Deployment Agent (CCA) 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 amp 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.

  **Note**
  
  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 group’s 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 8.6 and 8.6 has the following dependents; 8.6 SP1 and 8.6 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.


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 choose an agent to assign to the deployment group.

  **Caution**
  The latest software patches require Deployment Agent (CCA) version 8.6 to support deployment and reduce the number of endpoint reboots.
  If Deployment Group (CCA) 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.

**Note**
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.
   The Packages work area displays a list of all AppSense 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
- Downloading
- Download Failed
- Installing
- Installed
- Install Failed
- Pending Upgrade
- Upgrading
- Upgraded
- Upgrade Failed
- Pending Uninstall
- Uninstalling
- Uninstall Failed
- Uninstalled
- Install Prerequisite Failed
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.
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.

AppSense 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 AppSense 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

<table>
<thead>
<tr>
<th>Filter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>All</td>
<td>Displays a global overview of all alerts from computers across all</td>
</tr>
<tr>
<td></td>
<td>deployment groups.</td>
</tr>
<tr>
<td>Created in</td>
<td>Displays alerts which have a status of new and that have been raised in the</td>
</tr>
<tr>
<td>last day</td>
<td>last 24 hours.</td>
</tr>
<tr>
<td>Critical</td>
<td>Displays alerts for critical severity events. Critical events have a red</td>
</tr>
<tr>
<td></td>
<td>indicator preceding the alert. A critical alert is defined in Alerts &gt; Alert</td>
</tr>
<tr>
<td></td>
<td>Rule &gt; Details &gt; Severity.</td>
</tr>
<tr>
<td>High</td>
<td>Displays alerts for high severity events. High event have an orange indicator</td>
</tr>
<tr>
<td></td>
<td>preceding the alert. A high alert is defined in Alerts &gt; Alert Rules &gt; Alert</td>
</tr>
<tr>
<td></td>
<td>Rule &gt; Details &gt; Severity.</td>
</tr>
<tr>
<td>Medium</td>
<td>Displays alerts for medium severity events. Medium events have a yellow</td>
</tr>
<tr>
<td></td>
<td>indicator preceding the alert. A medium alert is defined in Alerts &gt; Alert</td>
</tr>
<tr>
<td></td>
<td>Rules &gt; Alert Rule &gt; Details &gt; Severity.</td>
</tr>
<tr>
<td>Low</td>
<td>Displays alerts for low severity events. Low events have a green indicator</td>
</tr>
<tr>
<td></td>
<td>preceding the alert. A low alert is defined in Alerts &gt; Alert Rules &gt; Alert</td>
</tr>
<tr>
<td></td>
<td>Rule &gt; Details &gt; Severity.</td>
</tr>
<tr>
<td>New</td>
<td>Displays alerts for new events. A new alert is defined in the alert Status</td>
</tr>
<tr>
<td></td>
<td>column.</td>
</tr>
<tr>
<td>Acknowledged</td>
<td>Displays alerts flagged as acknowledged.</td>
</tr>
<tr>
<td>Resolved</td>
<td>Displays alerts flagged as resolved.</td>
</tr>
</tbody>
</table>

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 box 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 box 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 in 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

<table>
<thead>
<tr>
<th>Alert Rule</th>
<th>Event ID</th>
<th>Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Execution Denied</td>
<td>9000</td>
<td>High</td>
</tr>
<tr>
<td>Application Manager agent ended unexpectedly</td>
<td>9090</td>
<td>Critical</td>
</tr>
<tr>
<td>Application Manager agent restarted</td>
<td>9091</td>
<td>Low</td>
</tr>
<tr>
<td>Application Manager agent terminated</td>
<td>9092</td>
<td>High</td>
</tr>
<tr>
<td>Application Manager unrecoverable</td>
<td>9093</td>
<td>Critical</td>
</tr>
<tr>
<td>Application Manager not licensed</td>
<td>9099</td>
<td>Critical</td>
</tr>
<tr>
<td>Component Analyzed</td>
<td>9021</td>
<td>Low</td>
</tr>
<tr>
<td>Component failed to optimize</td>
<td>9203</td>
<td>High</td>
</tr>
<tr>
<td>Component optimized</td>
<td>9202</td>
<td>Low</td>
</tr>
<tr>
<td>Computer Assigned to Deployment Group</td>
<td>9712</td>
<td>Medium</td>
</tr>
<tr>
<td>Computer startup action fail</td>
<td>9410</td>
<td>High</td>
</tr>
<tr>
<td>Computer startup action success</td>
<td>9409</td>
<td>Low</td>
</tr>
<tr>
<td>Computer successfully registered with Management Server</td>
<td>9751</td>
<td>Low</td>
</tr>
<tr>
<td>CPU clamping off</td>
<td>9105</td>
<td>Medium</td>
</tr>
<tr>
<td>CPU clamping on</td>
<td>9104</td>
<td>Medium</td>
</tr>
<tr>
<td>Environment Manager agent ended unexpectedly</td>
<td>9390</td>
<td>Critical</td>
</tr>
<tr>
<td>Environment Manager agent restarted</td>
<td>9391</td>
<td>Low</td>
</tr>
<tr>
<td>Environment Manager agent terminated</td>
<td>9392</td>
<td>High</td>
</tr>
<tr>
<td>Environment Manager agent unrecoverable</td>
<td>9393</td>
<td>Critical</td>
</tr>
<tr>
<td>Environment Manager not licensed</td>
<td>8399</td>
<td>Critical</td>
</tr>
<tr>
<td>Events failed to upload to the Management Server</td>
<td>9705</td>
<td>High</td>
</tr>
<tr>
<td>Alert Rule</td>
<td>Event ID</td>
<td>Severity</td>
</tr>
<tr>
<td>--------------------------------------------------------</td>
<td>----------</td>
<td>----------</td>
</tr>
<tr>
<td>Events within the Management Server database were deleted</td>
<td>9707</td>
<td>Medium</td>
</tr>
<tr>
<td>No valid Application Manager configuration found</td>
<td>9095</td>
<td>Critical</td>
</tr>
<tr>
<td>No valid Environment Manager configuration found</td>
<td>9495</td>
<td>Critical</td>
</tr>
<tr>
<td>No valid Performance Manager configuration found</td>
<td>9195</td>
<td>Critical</td>
</tr>
<tr>
<td>Overwrite changed owner</td>
<td>9002</td>
<td>Medium</td>
</tr>
<tr>
<td>Package created, modified or deleted</td>
<td>9702</td>
<td>Medium</td>
</tr>
<tr>
<td>Package install or uninstall was successful</td>
<td>9710</td>
<td>Low</td>
</tr>
<tr>
<td>Package install or uninstall was unsuccessful</td>
<td>9711</td>
<td>Critical</td>
</tr>
<tr>
<td>Performance Manager agent ended unexpectedly</td>
<td>9190</td>
<td>Critical</td>
</tr>
<tr>
<td>Performance Manager agent restarted</td>
<td>9191</td>
<td>Low</td>
</tr>
<tr>
<td>Performance Manager agent terminated</td>
<td>9192</td>
<td>High</td>
</tr>
<tr>
<td>Performance Manager agent unrecoverable</td>
<td>9193</td>
<td>Critical</td>
</tr>
<tr>
<td>Performance Manager agent not licensed</td>
<td>9199</td>
<td>Critical</td>
</tr>
<tr>
<td>Product agent is not compatible with client platform</td>
<td>9708</td>
<td>Medium</td>
</tr>
<tr>
<td>Rename changed owner</td>
<td>9003</td>
<td>Medium</td>
</tr>
<tr>
<td>Scripted rule failed</td>
<td>9010</td>
<td>High</td>
</tr>
<tr>
<td>Security rule created, modified or deleted</td>
<td>9740</td>
<td>High</td>
</tr>
<tr>
<td>Self healing file removed</td>
<td>9304</td>
<td>High</td>
</tr>
<tr>
<td>Self healing file replaced</td>
<td>9303</td>
<td>High</td>
</tr>
<tr>
<td>Self healing registry key removed</td>
<td>9302</td>
<td>High</td>
</tr>
<tr>
<td>Self healing registry key replaced</td>
<td>9301</td>
<td>High</td>
</tr>
<tr>
<td>User logoff action fail</td>
<td>9408</td>
<td>High</td>
</tr>
<tr>
<td>Alert Rule</td>
<td>Event ID</td>
<td>Severity</td>
</tr>
<tr>
<td>----------------------------------------</td>
<td>----------</td>
<td>----------</td>
</tr>
<tr>
<td>User logoff action success</td>
<td>9407</td>
<td>Low</td>
</tr>
<tr>
<td>User logon fail</td>
<td>9406</td>
<td>High</td>
</tr>
<tr>
<td>User logon success</td>
<td>9405</td>
<td>Low</td>
</tr>
<tr>
<td>User was created, modified or deleted</td>
<td>9703</td>
<td>High</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Regular Expression</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9700</td>
<td>Match only event 9700</td>
</tr>
<tr>
<td>97[0-9][0-9]</td>
<td>Match any Management Center event</td>
</tr>
<tr>
<td>9000</td>
<td>9001</td>
</tr>
</tbody>
</table>

- **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**

<table>
<thead>
<tr>
<th>Regular Expression</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>^AB</td>
<td>Matches all computers whose NetBIOS name starts with AB</td>
</tr>
<tr>
<td>^SALES_COMP1$</td>
<td>Only matches SALES_COMP1 computer</td>
</tr>
<tr>
<td>SALES_COMP1</td>
<td>Matches any computer containing SALES_COMP1, so will match PRESALES_COMP1 and SALES_COMP10 and so on</td>
</tr>
</tbody>
</table>

- **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.

  **Example**

<table>
<thead>
<tr>
<th>Regular Expression</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>^FRED\BLOGGS$</td>
<td>Matches user FRED.BLOGGS</td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Property</th>
<th>Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Server Settings</strong></td>
<td></td>
</tr>
<tr>
<td>Server</td>
<td>Enter the path to the e-mail server through which e-mail notifications are sent to the specified user.</td>
</tr>
<tr>
<td>User Name</td>
<td>User name with which the Management system accesses the e-mail server.</td>
</tr>
<tr>
<td>Password</td>
<td>Password for the user profile with which the Management System accesses the e-mail server.</td>
</tr>
<tr>
<td><strong>E-mail Settings</strong></td>
<td></td>
</tr>
<tr>
<td>To</td>
<td>Address to which e-mail notifications are sent about the current alert.</td>
</tr>
<tr>
<td>From</td>
<td>Address from which e-mail notifications are sent about the current alert.</td>
</tr>
<tr>
<td>Subject</td>
<td>Subject line displayed in e-mail notifications about the current alert.</td>
</tr>
</tbody>
</table>
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 AppSense 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:
  a. Within the Services control panel, launch the property sheet of the SNMP Service.
  b. On the Traps tab, set Community name to be public and click Add to list.
  c. Under Trap Destination click Add and enter the name of the local machine.
  d. 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.
  e. 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:
  a. Select the Alerts button in the navigation pane.
  b. Expand the Alert Rules node.
c. Expand the rule that you want to generate the SNMP trap for.

d. Select the **SNMP** node. The SNMP work area displays.

e. 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 AppSense products, based on events sent to the server.

Reports

The AppSense 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 www.appsense.com/support.

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.

  **Tip**
  
  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 DesktopNow 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 AppSense DesktopNow Installer. If the DesktopNow 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 Manager 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.


**Web Installation Activity** - Summary of web installations allowed or denied due to Application Manager 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 AppSense 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:
   a. Select the Reporting node. All reports display.
   b. Select a report and select Generate Report on the Actions panel.
      Reports corresponding to the product display.
   d. 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 AppSense. 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 Owner** - Orders the list of objects by owner.

- **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 (CCA) 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.

**Note**
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.
6. The Global Security Roles dialog box displays.
7. Select whether to allow or deny Modifier, Server Administrator or Viewer permissions.
8. Click OK.
Configure Security for View Permission Only for Groups

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.
7. Select the deployment group to which you want to provide access.
8. Select Security in the Actions panel.
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.
Troubleshooting

This section provides procedures for troubleshooting issues you may encounter with your Management Center implementation.

Deployment Agent (CCA) Fails to Connect to a Management Server

When a computer hosting the Deployment Agent (CCA) fails to connect to the Management Server, check the Windows Application Event Log for event 9750 which indicates if there has been a connection failure with the Management Server.

A connection failure can occur for the following reasons and you are recommended to check these items and take the recommended actions:

- Incorrect URL
- SSL State change to the Management Server

Recommended Actions:

- Use the Install Deployment Agent functionality within the console to connect and repair or modify the server URL for the Deployment Agent on managed computers to point to the Management Server, ensuring that the URL path uses the correct HTTP or HTTPS prefix and port number.

  For more information about using the Install Deployment Agent functionality, see Installing the Deployment Agent (CCA).

- If you enable SSL after the Management Server is installed and setup without SSL, manage the changeover using the Failover Servers list in the Management Center. Provide the new SSL secured failover server at the top of the list while retaining the old server until all Deployment Agents (CCA) have registered with the Management Server using the new SSL secure server.
Diagnostics Errors

Deployment Agent (CCA) diagnostics errors can occur when the system is incorrectly configured. Use the AppSense Management Server Configuration utility to check for variances to repair: Start > All Programs > AppSense > Management Center.

If no variances are detected, but the diagnostics test reports errors downloading packages or uploading events, check also that the Background Intelligent Transfer Service in the Windows service control panel is running on the Deployment Agent controlled machine and restart the service, as follows:

1. Select Start > All Programs > Administrative Tools > Services.
2. In the right-hand pane of the Services dialog box, locate and double-click Background Intelligent Transfer Service in the Name column.
3. Select the General tab of the Background Intelligent Transfer Service Properties dialog and ensure that:
   - The Startup type is set to Automatic.
   - The service is running. Start the service if necessary.
4. Click OK to close the Background Intelligent Transfer Service Properties dialog box.
5. In the right-hand pane of the Services dialog, locate and right-click the AppSense Client Communication Agent.
6. Select Restart in the pop-up menu and rerun diagnostics.

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

A

**AAMP:** See AppSense Application Manager Package

**Adler-32:** A checksum algorithm that can be applied to application files. See also: SHA-1 and SHA-256.

**ADM:** See Microsoft Administrative Template

**AEMP:** See AppSense Environment Manager Package

**agent:** An executable component that implements the product configuration settings. The DesktopNow agent is software that runs as a Windows service to carry out tasks on a computer, as specified by the configuration deployed to that computer.

**Allowed Items:** Files, folders, drives or digitally signed files or groups of files in a DesktopNow configuration Privilege Discovery that are allowed to run when file execution requests are matched with the rule security settings and would otherwise be denied by other configuration settings. See also: Denied Items

**AM Web Service:** The Application Manager web service that can be installed on any machine and used to collect data from the enabled Privilege Discovery feature.

**AMDX:** See Microsoft Administrative Template XML-Based.

**ANAC:** See Application Network Access Control.

**APMP:** See AppSense Performance Manager Package.

**App-V:** See Microsoft Application Virtualization.

**Application Group:** Environment Manager - A collection of applications with common registry keys and folders that are managed as a single group for Environment Manager Personalization. Performance Manager - A custom list of applications to which you assign rules for controlling CPU, memory or disk resources. Application Groups are associated with particular types of applications, desktop applications, services, or 16-bit applications.

**Application Limit:** An Application Manager setting, applied to an Allowed Item, that specifies the number of instances of an application that a user can run.

**Application Network Access Control (ANAC):** An approach to computer network security that controls outbound network connections by IP Address, host name, URL, UNC, or port, based on the outcome of rules processing. In Application Manager ANAC is implemented using Network Connection Items and Reverse DNS Lookup.

**Application Termination:** An Application Manager feature that allows you to set triggers, behavior, and warning messages for terminating applications on managed computers.

**AppSense Application Manager Package (AAMP):** The configuration file that stores settings created in Application Manager Configuration and is then deployed to endpoints. The agent uses the configuration settings to determine whether or not an execute request is to be denied.

**AppSense Environment Manager Package (AEMP):** The configuration file that stores settings created in Environment Manager Policy Configuration and is then deployed to endpoints to manage the policy configuration on those endpoints as defined in the settings.
**AppSense Performance Manager Package (APMP):** The configuration file that stores the policies created in Performance Manager for managing performance and resources on managed endpoints, and is then deployed to endpoints to manage performance as defined.

**Audit Only:** Security Level assigned to users, groups or devices in an Application Manager Privilege Discovery that audits events according to the auditing configuration without applying the rule. Used for passive monitoring in evaluations to assess application usage on the host environment.

**base configuration:** In endpoint configuration merging, the first configuration in the merge onto which the other configurations are added.

**cascadeBHO.dll:** An Application Manager Browser Helper Object (BHO) loaded by Internet Explorer that is used as part of the URL Redirection and Elevated Web Sites features.

**Citrix XenApp:** A thin client product that allows users to connect to their corporate applications. XenApp can either host applications on central servers and allow users to interact with them remotely or stream and deliver them to user devices for local execution.

**client computer:** The device on which user login sessions are hosted.

**Client Debug Setup Utility:** An Environment Manager standalone utility, installed from the EM Tools Installer, which enables and disables the generation of diagnostic logs used by AppSense Support when diagnosing reported issues.

**COM:** A binary-interface standard for software components introduced by Microsoft. It is used to enable inter-process communication and dynamic object creation in programming languages.

**configuration:** A collection of settings created in the product console, in which a navigation tree of component settings graphically represents the configuration while it is created and modified by the administrator.

**configuration file:** A DesktopNow configuration saved as a native configuration file (*.aamp, *.aemp, or *.apmp) or an XML file, or exported from the product console in Windows Installer MSI file format. The file can be installed on any computer and the configuration rules applied when a DesktopNow Agent is present and running as a service on the computer. See also: AppSense Application Manager Package (AAMP), AppSense Environment Manager Package (AEMP), and AppSense Performance Manager Package (APMP)

**Configuration Profiler:** In the product console, a feature that generates reports detailing the current settings in the configuration. Filtering options allow you to query settings affecting specific users or groups, devices, and files or folders.

**Constant Special Item ID List:** A set of values that provide a unique, system-independent way to identify special folders used frequently by applications, but which may not have the same name or location on any given system.

**CSIDL:** See Constant Special Item ID List.
DAC: See Discretionary Access Control.

Database Management System (DBMS): Computer management software that manages databases installed on a system or network.

DBMS: See Database Management System.

Denied Items: Items that are not allowed to run when file execution requests are matched with the rule security settings and would otherwise be allowed by other configuration settings. See also: Allowed Items

Deployment Agent (CCA): A software service installed on computers to provide communication between the product agent running on a managed computer and the AppSense Management Center. The Deployment Agent (CCA) sends event data generated by the product agents to the Management Server and also polls the Management Server to manage the download and installation of software configuration, agent and package updates.

DFS: See Distributed File System.

digital signature: A means to accurately validate the authenticity of a file according to the actual contents of the file itself by using a mathematical technique (a cryptographic hashing algorithm). If the file is altered in any way then the SHA-1 hash is also altered. Application Manager has a Signature Wizard that allows you to apply digital signatures either to an individual file or a group. The signature can be used as a security measure when adding files as Allowed Items, Denied Items and Trusted Vendors. Application Manager uses the industry standard SHA-1, SHA-256 and Adler-32 hashes.

Discretionary Access Control (DAC): A type of access control defined by the Trusted Computer System Evaluation Criteria as a means of restricting access to objects based on the identity of subjects and/or groups to which they belong.

Distributed File System (DFS): Any file system that allows access to files from multiple hosts sharing via a computer network.

DLL: See Dynamic Link Library.

DNS: See Domain Name System.

Domain Name System (DNS): A system that translates a computer’s fully qualified domain name into an IP address.

Dynamic Link Library (DLL): A collection of software functionality that a running executable can call upon as needed, for example to communicate with a specific device such as a printer or to perform particular tasks.
EM: See Environment Manager.

EM Tools: A collection of standalone tools installed from the EM Tools Installer, which assist administrators when creating configurations and working with the Personalization Database.

EmMon: See Environment Manager Monitor.

EMP: See Environment Manager Personalization.

EMP File Utility: A standalone utility, installed from the EM Tools Installer, which imports and exports files to and from the Environment Manager Personalization database.

EMP Migrate Utility: A standalone utility, installed from the EM Tools Installer, which allows user data to be copied from a source database to a target database.

EMP Registry Utility: A standalone utility, installed from the EM Tools Installer, which relocates registry keys when multiple versions are stored in user profiles in the Personalization database.

Endpoint Analysis (EPA): In Application Manager, the functionality to monitor managed endpoints to provide a list of applications that are present and that have run on a particular computer.

Environment Manager (EM): An AppSense user virtualization solution that ensures users always receive a consistent, predictable, and personalized working experience.

Environment Manager Logging Setup Tool: In Environment Manager, a standalone utility, installed from the EM Tools Installer, which enables and disables the generation of diagnostic logs used by AppSense Support when diagnosing reported issues.

Environment Manager Monitor (EmMon): In Environment Manager, a standalone utility, installed from the EM Tools Installer, that provides a user interface to view and analyze log files from the Environment Manager Agent. This tool replaces Environment Manager LogViewer.

Environment Manager Personalization (EMP): An Environment Manager feature that captures a user’s application and desktop changes to a central database and reapply them for the user upon logon or application start, regardless of operating system or delivery mechanism.

Environment Manager Support console: An abridged version of the Environment Manager console, available to users with the Support Console role, that offers read-only access to Environment Manager configurations and full access to Personalization Analysis functionality.

EPA: See Endpoint Analysis.
F

**FBR Explorer:** A standalone utility, installed from the EM Tools Installer, which opens any File Based Registry (FBR) enabling the keys and values stored for an application to be viewed.

**filter driver:** An optional driver that adds value to or modifies the behavior of a device. A filter driver can service one or more devices.

**fixed node:** In the product console navigation tree, a node that cannot be deleted or edited.

**Folder Redirection:** A Microsoft Windows component that can be controlled by group policy. Environment Manager simplifies its configuration.

G

**Globally Unique Identifier (GUID):** A unique reference number used as an identifier in computer software.

**Group Management:** In Application Manager, a library for compiling reusable groups of files, folders, drives, signatures, and network connections that can be associated with rules in the configuration. For example, Groups can be used to manage licenses for a suite of software or common sets of applications for assigning to certain user groups.

**Group Policy:** A set of configuration rules that can be defined to manage the working environment of users and computers.

**GUID:** See Globally Unique Identifier.

L

**Local Security Authority (LSA):** A required Windows component that deals with login authentication and security policies.

**lockdown:** An Environment Manager mechanism to restrict or disable access to specific application and operating system functionality, keyboard shortcuts, Microsoft Office application menus, and toolbars.

**LSA:** See Local Security Authority.
**M**

**managed application:** Applications that have their settings and any changes made to those settings captured by Environment Manager Personalization.

**Management Server:** The machine on which product configurations and configuration versions are stored, from which configurations can be deployed to machines designated by the administrator.

**Masquerading Applications:** Applications that are allowed to run against the personalization caches of another application in order to use its Personalization data. This is especially useful when using multiple applications on multiple endpoints in situations where using a Personalization Group is not feasible.

**Microsoft Administrative Template (ADM):** The file type of the administrative template files that are used by Environment Manager Group Policies to describe where registry-based policy settings are stored in the registry.

**Microsoft Administrative Template XML-Based (ADMX):** The file type for XML based administrative template files that are used by Environment Manager Group Policies to describe where registry based policy settings are stored in the registry for Microsoft Windows Vista and Server 2008.

**Microsoft Application Virtualization (App-V):** An application virtualization and application streaming solution that allows application to be deployed in real-time to clients and virtual application servers. It was formerly known as Microsoft SoftGrid.

**MSI:** The file type for a Microsoft Installer file, an installer file package format used by Windows.

**N**

**NetBIOS:** See Network Basic Input/Output System.

**Network Basic Input/Output System (NetBIOS):** A program that allows applications on different computers to communicate within a local area network (LAN).

**Network Connection Item:** In Application Manager, a network resource that can be added to a rule as an Allowed or Denied Item.


**node:** Application Manager and Performance Manager - A branch in the navigation tree in the product console. Environment Manager - In a configuration, a container that houses conditions and actions within triggers.

**NTFS:** See New Technology File System.
ODBC: See Open Database Connectivity.

Open Database Connectivity (ODBC): A standard software interface for accessing Database Management Systems (DBMS), making communication between applications and databases easier.

Open Software Description (OSD): A file format generated by App-V to define how an application is launched and configured.

organizational unit: A container that holds users and computers in Active Directory.

OSD: See Open Software Description.

OU: See organizational unit.

Personalization Analysis: An Environment Manager feature that monitors which applications are being controlled by Environment Manager, including how much data is being stored, and enables managers to convert discovered applications to UV Services and to roll back to Personalization restore points.

Personalization Group: A group of users, based on common requirements, that can be treated as a single entity for Environment Manager Personalization configuration. This allows group members to have the same managed applications, Application Groups, and user personalization settings.

Personalization Server: The server that acts as a broker between the client and database, providing a secure channel to read and write the Personalization data.

Personalization Virtualization Component (PVC): The component responsible for redirecting reads and writes of profile data from within a managed application.

Privilege Discovery: The Application Manager functionality to monitor endpoints in order to identify applications that use administrative privileges.

Process Rules: Application Manager rules that manage access for a parent process to run child processes that might be managed differently in other rules.

PVC: See Personalization Virtualization Component.
R

**registry hive:** A section of the registry that is a logical grouping of registry keys, subkeys and values. Registry hives are denoted by the prefix HKEY.

**regular expression:** An expression that describes or matches a set of strings. Regular expressions are usually used to give a concise description of a set without having to list all elements and to search and manipulate bodies of text based on certain patterns.

**Restricted:** The Security Level assigned to users, groups or devices in an Application Manager Privilege Discovery at which only authorized applications can run. These include files owned by members of the Trusted Owners list and files listed in Allowed Items, Trusted Vendors and Trusted Ownership.

**reusable condition:** A condition that can be used multiple times within a configuration, ideal for grouping common sets of conditions together that need to run regularly in a variety of circumstances.

**reusable node:** A node that can be used multiple times within a configuration, ideal for grouping common sets of actions together that need to run regularly in a variety of circumstances.

S

**Secure Hash Identifier (SHA-1):** A cryptographic hash function designed by the United States National Security Agency and a U.S. Federal Information Processing Standard published by the United States NIST. SHA-1 produces a 160-bit (20-byte) hash value known as a message digest. A SHA-1 hash value is typically rendered as a hexadecimal number, 40 digits long.

**Security Identifier SID:** A data structure of variable length that identifies user, group, and computer accounts. Every account on a network is issued a unique SID when the account is first created. Internal processes in Windows refer to an account’s SID rather than the account’s user or group name. Likewise, Application Manager also refers to a user or group SID unless the SID could not be found when added to the configuration.

**Security Level:** Application Manager configuration settings that specify how to manage requests to run unauthorized applications by the users, groups, or devices that a rule matches. Security levels include Restricted, Self-Authorizing, Audit only, and Unrestricted.

**Self Heal:** Environment Manager mechanism to automatically restore environment items, including files, processes, services, or registry keys.

**Self-Authorizing:** The Security Level at which the user, group, or device is granted control to choose whether to block or run an unauthorized application on the host computer. The Self-Authorizing Security Level can be assigned in an Application Manager Privilege Discovery to match a file execute request for users, groups, or devices.

**Server Configuration Portal (SCP):** A utility for configuring AppSense servers and databases. During product installation it is used to create server instances, databases and user accounts but can be used at any time for maintenance and troubleshooting.

**SHA-1:** See Secure Hash Identifier.

**SHA-256:** A hash function computed with 32-bit words. See also: SHA-1 and Adler-32.

**SID:** See Security Identifier.
Site: In Environment Manager, a logical grouping of clients and Personalization Servers communicating with a database.


Time Limits: Settings applied to entries in the Allowed Items and Denied Items nodes of an Application Manager Privilege Discovery that determine day and time ranges when the controls apply. For example, an entry in the Denied Items node of a rule can restrict use of the local web browser to users except between the hours of 12pm and 2pm on specific days of the week.

Transmission Control Protocol (TCP): A standard that defines how to establish and maintain a network conversation via which application programs can exchange data. TCP works with the Internet Protocol (IP), which defines how computers send packets of data to each other.

trigger: Preset User and Computer events that trigger actions and conditions.

Trusted Applications: Files that are authorized to run by an Application Manager configuration and can execute files that are normally prohibited. Trusted Applications are designated in the Default Rules and include specified Trusted Content, which includes files normally prohibited but allowed when run executed as a child process of the associated Trusted Application. Application matching takes place when a file is prohibited by a rule or fails Trusted Ownership checking.

Trusted Ownership: A secure method Application Manager uses to prevent users running unauthorized applications. On NTFS formatted drives, files have owners and Application Manager is configured by default to only allow files to be executed if the file owner is a member of the Trusted Owners list. If a user tries to run a file that is not owned by a trusted owner, the execute request is denied and a message notifies the user.

Trusted Vendors: Digital certificates signed by trusted sources. In Application Manager, Trusted Vendor checking allows applications that fail Trusted Ownership checking to match digital certificates with the Trusted Vendors list. A list of Trusted Vendors can be defined for each User, Group, Device, Custom, Scripted, and Process rule of the configuration. DesktopNow queries each file execution that fails Trusted Ownership checking to detect the presence of a digital certificate. If the file has a digital certificate that is signed by a certificate authority matching a valid entry in the Trusted Vendor list, the file is allowed to run.
**UNC:** See Universal Naming Convention.

**Universal Naming Convention (UNC):** A NetBIOS naming format for identifying the location of servers, printers, and other resources on a local area network (LAN). UNC begins with two backslashes (\") and takes the form: \"\Computer_name\Share_name"

**Unrestricted:** The Security Level assigned to users, groups or devices in an Application Manager Privilege Discovery at which all actions are permitted without event logging or auditing.

**User Personalization:** In Environment Manager, the ability to capture application and desktop changes on a central database and reapply saved settings for users when triggered, such as at logon or application start.

**User Privileges Management:** An Application Manager feature that provides a granular approach to delegating administrative rights to users and applications by assigning rights according to merit. This level of control can be deployed to elevate or restrict privileges on a case by case basis according to the preferred approach taken in the environment.

**User Virtualization (UV):** The independent management of all aspects of the user on the desktop. The user's personality is decoupled from the operating system and applications managed independently and applied to a desktop as needed without using scripting, group policies, or user profiles, regardless of how the desktop is delivered.

**UV:** See User Virtualization.

**UV Service:** The NT Service that is responsible for managing user virtualization on the endpoint. Stopping this service will prevent the endpoint from being managed by Environment Manager.

**Virtual Desktop Infrastructure (VDI):** The server computing model enabling desktop virtualization, encompassing the hardware and software systems required to support the virtualized environment.

**Windows Management Instrumentation (WMI):** A set of extensions to the Windows Driver Model that provides an operating system interface through which instrumented components can provide information and notification.

**Windows Script Host (WSH):** The file format for Windows Script Host, an automation technology for Windows that provides language-independent scripting abilities similar to batch files, and is used to create logon scripts, automation, and batch files.

**WMI:** See Windows Management Instrumentation.

**WSH:** See Windows Script Host.