

IBM Endpoint Manager  
Version 9.1

*Software Distribution User's Guide*





IBM Endpoint Manager  
Version 9.1

*Software Distribution User's Guide*



**Note**

Before using this information and the product it supports, read the information in "Notices" on page 79.

This edition applies to version 9, release 1, modification level 0 of IBM Endpoint Manager (product number 5725-C43) and to all subsequent releases and modifications until otherwise indicated in new editions.

© **Copyright IBM Corporation 2003, 2014.**

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

---

# Contents

## Chapter 1. Overview . . . . . 1

|   |   |
|---|---|
| What's new in Software Distribution application update V6.0 . . . . . | 1 |
| System requirements. . . . .  | 2 |
| Supported package types . . . . .                                     | 3 |

## Chapter 2. Best practices . . . . . 5

|                                      |   |
|--------------------------------------|---|
| Policy-based distributions . . . . . | 5 |
| Authorization . . . . .              | 5 |
| Prerequisites . . . . .              | 5 |
| Site organization . . . . .          | 6 |

## Chapter 3. Dashboards overview . . . . . 7

|   |    |
|---|----|
| Manage Software Distribution Packages dashboard . . . . .       | 7  |
| Manage Application Management Groups dashboard . . . . .        | 8  |
| Self Service Portal Registration Management dashboard . . . . . | 9  |
| Client Dashboard for Software Offers. . . . .                   | 11 |

## Chapter 4. Managing packages . . . . . 13

|  |    |
|--|----|
| SHA-256 task conversion . . . . .              | 13 |
| Creating a package or Fixlet. . . . .          | 14 |
| Adding tags to packages . . . . .              | 16 |
| Editing a package or Fixlet . . . . .          | 17 |
| Package type verification . . . . .            | 23 |
| Generating logs for individual tasks . . . . . | 24 |
| Software repositories migration. . . . .       | 25 |

## Chapter 5. Managing Application Management Groups. . . . . 27

|   |    |
|---|----|
| Creating a custom site. . . . .                                   | 29 |
| Setting up viewing permissions. . . . .                           | 29 |
| Creating Application Management Groups . . . . .                  | 30 |
| Adding tasks to an Application Management Group . . . . .         | 31 |
| From the Manage Software Distribution Packages dashboard. . . . . | 31 |
| From the Manage Application Management Groups dashboard . . . . . | 34 |
| Adding targets to an Application Management Group . . . . .       | 36 |

|  |    |
|--|----|
| Adding an exclusion to an Application Management Group . . . . .                                 | 38 |
| Deploying Application Management Groups . . . . .  | 40 |
| Orphaned owners . . . . .  | 43 |
| Transferring resources to the corresponding LDAP operator . . . . .                              | 43 |
| Transferring resources to a different operator . . . . .   | 44 |
| Software Distribution Self Service Portal overview . . . . .                                     | 45 |
| Configuring the Software Distribution Self Service Portal. . . . .                               | 47 |
| Generating a PIN for each computer . . . . .   | 51 |
| Registering computers through the Self Service Portal Registration Management dashboard. . . . . | 52 |
| Blocking computers from registration. . . . .  | 53 |
| Accessing the Software Distribution Self Service Portal . . . . .                                | 54 |
| Registering computers through the Self Service Portal . . . . .                                  | 55 |
| Software installation status . . . . .   | 57 |
| Installing software from the Self Service Portal . . . . .                                       | 57 |
| Viewing installation history . . . . .   | 58 |
| Uninstalling the Self Service Portal . . . . .   | 60 |

## Chapter 6. Microsoft Application Virtualization . . . . . 61

|   |    |
|---|----|
| Deploying App-V clients . . . . .         | 61 |
| Viewing App-V client status. . . . .      | 65 |
| Deploying App-V packages . . . . .        | 66 |
| Viewing App-V application usage . . . . . | 66 |

## Appendix A. Support. . . . . 69

## Appendix B. Frequently asked questions . . . . . 71

## Notices . . . . . 79

|   |    |
|---|----|
| Programming interface information . . . . .             | 81 |
| Trademarks . . . . .                                    | 81 |
| Terms and conditions for product documentation. . . . . | 82 |



---

## Chapter 1. Overview

The Software Distribution application is part of the IBM® Endpoint Manager for Software Distribution Systems Lifecycle Management suite. This application enables organizations to improve management of their desktop software distribution processes from a single, unified point of control, and storage-optimized library.

The Endpoint Manager architecture enables IT staff to control bandwidth so that packages can be delivered without affecting network performance regardless of network size or speed.

Some of the most significant cost-saving and time-saving features of Endpoint Manager Software Distribution include:

- Dynamic and policy-based bandwidth throttling to push large files over distributed networks without impacting line-of-business bandwidth.
- Support for roaming endpoints with pre-caching relay infrastructure.
- Features to optimize dynamic and evolving networks.
- Intelligent software distribution based on endpoint characteristics.
- Software distribution wizards and user self-provisioning.
- Continuous software application license usage and metering, including support for existing software repositories.
- Low-cost scalability with minimal infrastructure requirements.

---

### What's new in Software Distribution application update V6.0

This IBM Endpoint Manager for Software Distribution application update contains a set of features and improvements for the Software Distribution site.

The Software Distribution application update V6.0 contains the following new features and enhancements.

#### **Support for the installation of PKG files on Solaris**

You can now create and deploy installation tasks for PKG files to your Solaris endpoints from the Manage Software Distribution dashboard.

#### **Self Service Portal (SSP) support for AIX and Solaris**

The SSP can now add and remove computers with AIX and Solaris operating systems and the SSP Registration Management Dashboard can block users from these machines.

#### **SSP Registration Management Dashboard Enhancements**

You can now search, sort, and paginate computers in scroll view to enhance dashboard performance.

#### **Modifiable SPB variable during deployment**

Software Distribution tasks with SPB files support variable templating that enables the creation of customizable tasks.

#### **Installation files custom directory support**

Software Distribution tasks can now specify a custom file path location to download and run files instead of using the default location.

**Note:** An advanced option to automatically convert old tasks with SHA-1 validation, which were created from the Software Distribution dashboard, into tasks with SHA-256 validation was released in version 5.1. For more information, see “SHA-256 task conversion” on page 13.

---

## System requirements

The Endpoint Manager for Software Distribution application has different sets of system specifications for the server, console, and client.

### Server

- Microsoft Windows 2003
- Microsoft Windows 2008
- Microsoft Windows 2008 R2
- Microsoft Windows Server 2012
- Red Hat Enterprise Linux Server release 6.1 (64-bit architecture)
- Endpoint Manager version 9.0.649 or later

### Console

- Intel Pentium III–class processor with at least 2 GB RAM (larger deployments require additional resources)
- Microsoft Windows 7
- Microsoft Windows XP
- Microsoft Windows 2003
- Microsoft Windows Vista
- Microsoft Windows 2008
- Microsoft Windows 2008 R2
- Microsoft Windows Server 2012
- Internet Explorer 9.0

The minimum Endpoint Manager Console requirement is different for packages and Application Management Groups:

### Packages

Endpoint Manager version 8.0.627 or later

### Application Management Groups

Endpoint Manager version 8.2.1310 or later

### Self Service Portal

Endpoint Manager version 9.0.649 or later

### Clients

- Microsoft Windows XP
- Microsoft Windows 2003
- Microsoft Windows Vista
- Microsoft Windows 2008
- Microsoft Windows 2008 R2
- Microsoft Windows Server 2012
- Microsoft Windows 7
- Microsoft Windows 8
- Mac OS X 10.6
- Mac OS X 10.7



- Mac OS X 10.8
- Internet Explorer 9.0
- Safari 5.0
- Endpoint Manager version 9.0.649 or later

---

## Supported package types

The Endpoint Manager for Software Distribution application supports various package types that can be deployed to different endpoints.

The current version of Endpoint Manager for Software Distribution supports the following file types:

- BAT
- EXE
- Mac DMG
- PKG (for Mac and Solaris)
- MSI
- SPB (for Windows and Linux)
- SPB (for Windows, Linux, and AIX)
- RPM (for Linux and AIX)
- Microsoft Application Virtualization (App-V)

The following App-V clients and packages are supported:

- 4.5 SP1
- 4.5 SP2
- 4.6 Gold (32 and 64-bit)
- 4.6 SP1 (32 and 64-bit)
- 5.0 Gold (32 and 64-bit)

### Notes:

- To deploy SPB package types to your endpoints, you must first subscribe to the **Client Manager for TCM** site from your console. After you subscribe to the site, run the Deploy SIE task to each endpoint. This task is found in **All Content domain > Fixlets and Tasks > Tasks > By Site > Client Manager for TCM**.
- The inspector to check whether a Mac .pkg file is installed on an endpoint is not yet available.
- The Policy Action type of Mac PKG tasks is not supported in the Software Distribution task deployment process.



---

## Chapter 2. Best practices

Learn how to best optimize your use of Endpoint Manager for Software Distribution.

Use the following information as guidance for using this product.

---

### Policy-based distributions

Use client settings to drive the installation of packages through policies.

Client settings are a cross-platform data tag that can be used in a number of ways by the Endpoint Manager platform. For example, a client setting called *Role* might be set to “Facilities Management”, and an action might be present to install an Autodesk client on Windows systems with that condition. This practice allows predictable, centrally managed, role-based software provisioning, and rapid return to the wanted state after an OS reimage or migration.

---

### Authorization

Test the installation of software under the systems management account.

On a Windows system, Endpoint Manager defaults to installing software in the *LocalSystem* account. On a Mac OS X, Linux, or UNIX system, software is installed in the *root* account. Therefore, always test software installations under these accounts to ensure that they work correctly.

For more information, see the related articles for Windows or Mac on the Endpoint Manager support website Knowledge Base.

If a software package does not install under *LocalSystem*, run the `runascurrentuser.exe` tool to use the rights of the current user. For more information, see the article about Running As Current User. To automate this action, create Fixlets with the Software Distribution dashboard.

---

### Prerequisites

Endpoint Manager provides a powerful baseline concept that solves the dependency chain problem of prerequisite software.

For example, a piece of in-house software might require a particular version of Microsoft .Net, which might in turn require an upgrade of Windows Installer. Windows might also require a patch if Service Pack 3 is not installed. To define the prerequisite chain, bundle these four related Fixlets into a single baseline. Systems missing any component of the baseline can then install it, while systems that meet some or all of the prerequisites can omit that step and move on to the next one. All targeted systems are then brought to the same end state with a single action.

For more information about creating baselines, see the *IBM Endpoint Manager Console Operator's Guide*.

---

## Site organization

Use custom sites to organize your generated tasks to improve performance and usability.

Use custom sites to categorize content within your deployment. Custom sites help tune your Endpoint Manager installation optimum resource usage. For more information about creating custom sites, see the *IBM Endpoint Manager Console Operator's Guide*.

---

## Chapter 3. Dashboards overview

Endpoint Manager Software Distribution provides several dashboards for managing software distribution tasks in your deployment.

Learn about what these dashboards are and how you can access them from the console.

---

### Manage Software Distribution Packages dashboard

The Manage Software Distribution Packages dashboard is a tool where you can perform common tasks that are associated with managing the software in your deployment.

Before you can use the dashboard, you must deploy the tasks that are listed in the Install Server Tools under the Software Distribution Setup node.

These tasks include:

- TEM Server: Install TEM Upload Maintenance Service for Software Distribution
- TEM Server: Upgrade TEM Upload Maintenance Service
- TEM Server: Register Download Plug-in for Software Distribution

**Note:** The "TEM Server: Install TEM Upload Maintenance Service for Software Distribution" task is not relevant until the BES Server Plugin Service is installed on the Endpoint Manager server. The BES Server Plugin Service task, which schedules other services to run, must be run before any other setup tasks.

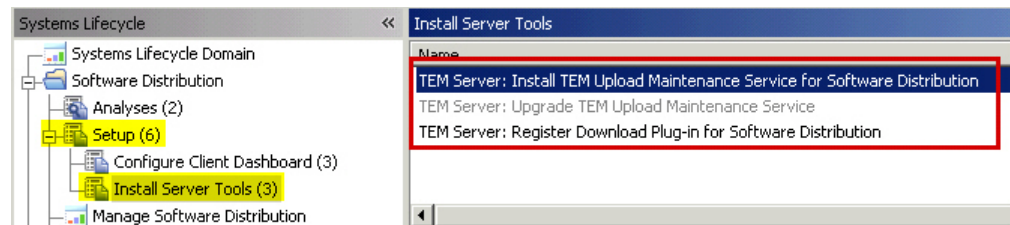


Figure 1. Prerequisite tasks under the Software Distribution Setup node

These tasks help the automation of processes that require communication with the Endpoint Manager Server and Web Reports.

These tasks are displayed in the List panel only if they are not currently installed.

To install the tasks, click each task to open the task window. Then, click the link in the Actions box of the applicable Task window, as shown in the following image. The Take Action dialog opens. You can set specific parameters for each task.

For more information about using the Take Action Dialog, see the *IBM Endpoint Manager Console Operator's Guide*.

## Dashboard location

You can access the Manage Software Distribution Packages dashboard from the top of the Software Distribution navigation tree of the Systems Lifecycle domain.

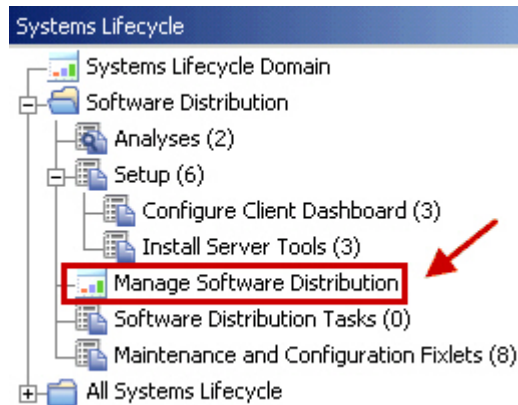


Figure 2. Software Distribution navigation tree

The Manage Software Distribution Packages dashboard is displayed under the **Packages** tab.

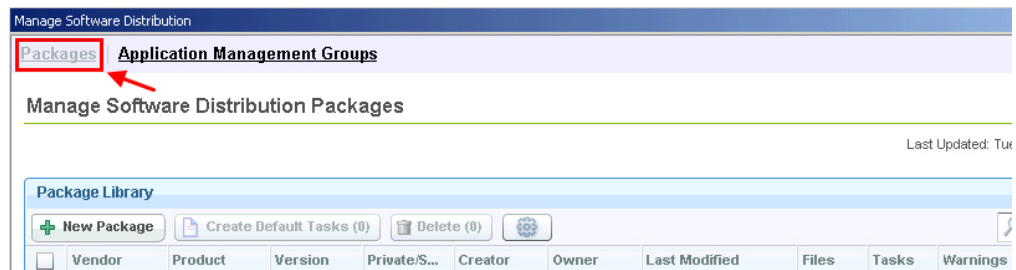


Figure 3. Manage Software Distribution Packages dashboard

---

## Manage Application Management Groups dashboard

The Manage Application Management Groups dashboard helps you to oversee and deploy offers to a certain group of computers in your network.

Offers contain a list of software that endpoint users can select to install on their machines. You can add and group offers from the Manage Application Management Groups dashboard. Endpoint users can view and install the available offers from the following options:

- Client dashboard. For more information about the Client dashboard, see “Client Dashboard for Software Offers” on page 11.
- Software Distribution Self Service Portal. For more information, see “Software Distribution Self Service Portal overview” on page 45.

You can access the Manage Software Distribution Packages dashboard from the top of the Software Distribution navigation tree of the Systems Lifecycle domain.

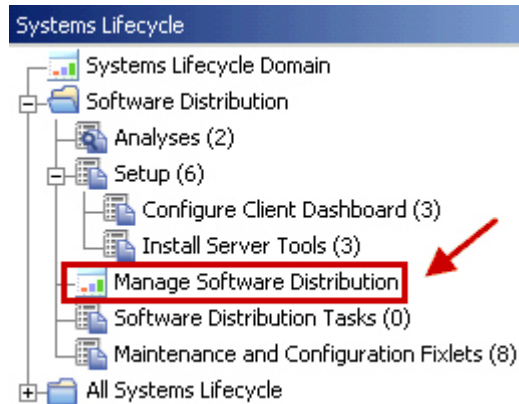


Figure 4. Software Distribution navigation tree

The Manage Application Management Groups dashboard is displayed under the **Application Management Groups** tab.

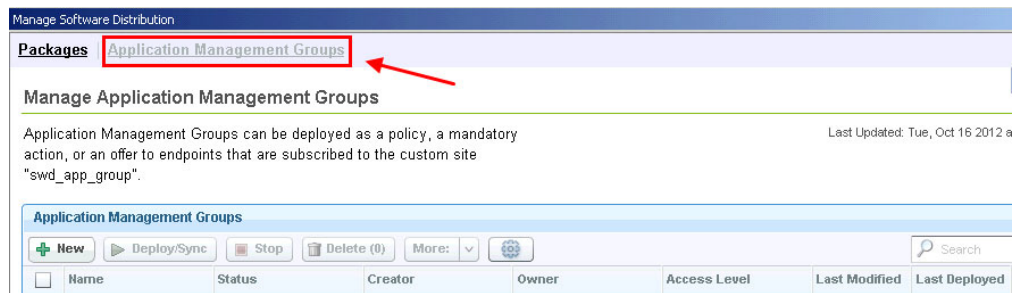


Figure 5. Manage Application Management Groups dashboard

## Self Service Portal Registration Management dashboard

Console operators must use this dashboard mainly to remove registered computers and to prevent endpoint users from registering certain computers in the Self Service Portal.

The Self Service Portal Registration Management dashboard supports computers that are on the following operating systems:

- Windows
- Mac
- Linux
- AIX
- Solaris

Operators can use the dashboard also to register computers to endpoint users to allow them to install software from the Self Service Portal. However, endpoint users are expected to complete computer registration from the portal.

### Dashboard location

You can access this dashboard from the Software Distribution navigation tree of the Systems Lifecycle domain.

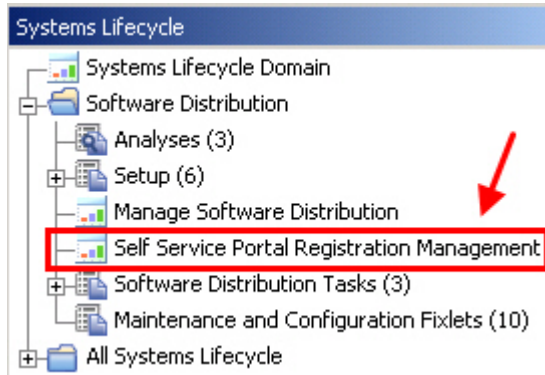


Figure 6. The Self Service Portal Registration Management dashboard from the navigation tree.

## Registration and blocking

The registration or blocking method that you might want to use depends on the list view. The dashboard provides the following viewing options:

### List By Users

Use this view to add computers to the registration or blocked list.

### List By Computers

Use this view to add users to the registration or blocked list.



Figure 7. Self Service Portal Registration Management dashboard

For more information about:

- Blocking, see “Blocking computers from registration” on page 53.
- Registering, see “Registering computers through the Self Service Portal Registration Management dashboard” on page 52.

## Removal of registered computers or users

To easily locate for the computer or user from the list, search or sort by the computer name or user name.



You can remove a computer or a user from registration in the following ways:

### Remove the computer or user from the registration list

When removed, endpoint users are able to self-register the computer again from the Self Service Portal.

### Adding the computer or user to the blocked list

The blocked computer is removed from the list of registered computers that is displayed in the Self Service Portal. By adding the computer or user to the blocked list, endpoint users are unable to self-register the computer again.

---

## Client Dashboard for Software Offers

The Client Dashboard for Software Offers is where endpoint users can select and accept software offers that were made available to them.

The software offers work in a similar way to regular actions except that the deployment does not occur until the endpoint user chooses to install the software.

Before endpoint users can access the dashboard, you must deploy the **Enable Client Dashboard for Software Offers** task on each endpoint. This task is listed in the Configure Client Dashboard under the Software Distribution Setup node.

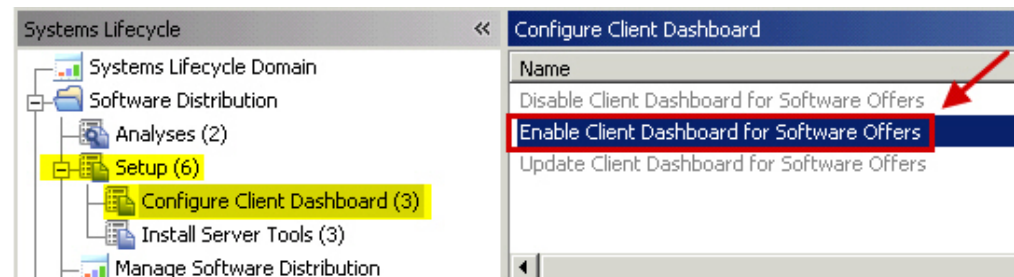


Figure 8. Enable Client Dashboard for Software Offers task navigation tree

The **Enable Client Dashboard for Software Offers** task displays in the List panel only if this task is not currently installed.

### Dashboard location

Endpoint users can access the dashboard from their system tray on Windows.

Click the **BigFix** icon to open the Endpoint Manager Support Center.

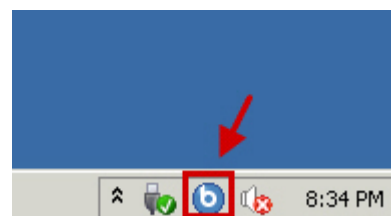


Figure 9. The Endpoint Manager Support Center on the Windows system tray

**Note:** You can configure the BigFix icon. For more information, see the topic about "Changing the Client Icon" from the *IBM Endpoint Manager Administrator's Guide*.

The software offers are displayed in the **Available Software** tab. Endpoint users can select and install the software packages that you send them. You can customize the title, version, size, and description from the Manage Software Distribution Package and Manage Application Management Groups dashboards.

You can also view the web portal registration PIN, which is a unique alphanumeric digit that is assigned to a computer. Endpoint users use this PIN to register computers in the Self Service Portal.

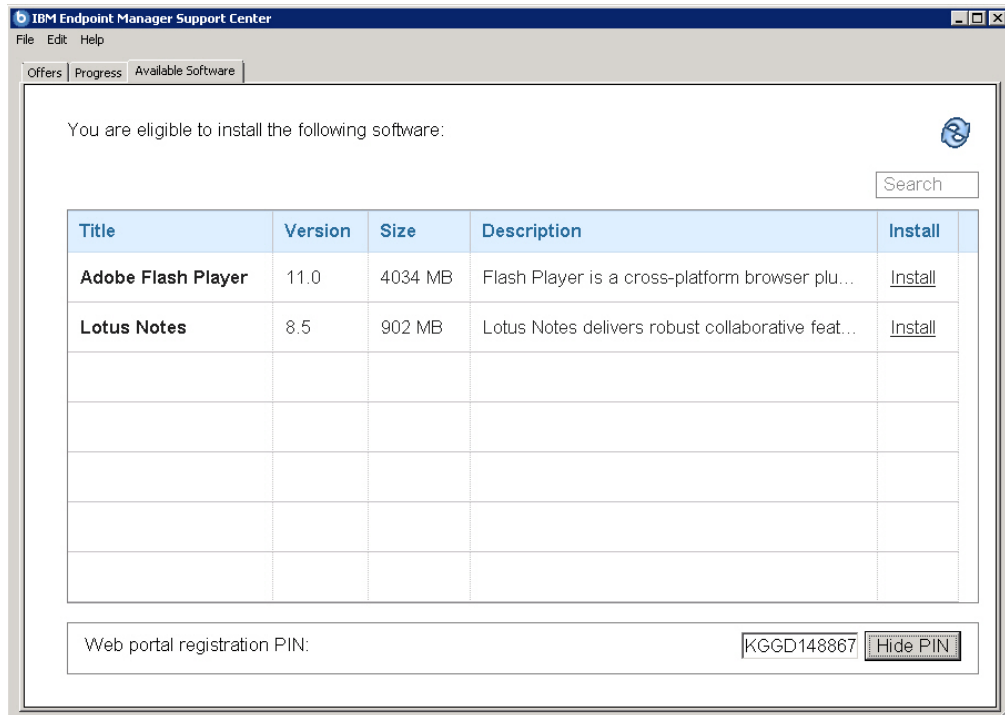


Figure 10. Client Dashboard for Software

---

## Chapter 4. Managing packages

You can bundle software distribution content into packages for faster deployment.

Packages are an important part of the Software Distribution product. They contain a list of files that are needed to install a specific software product, as well as Fixlets that install that product on your endpoints.

Packages establish management relationships between files and Fixlets.

You can use the Manage Software Distribution Packages dashboard to perform the following management tasks:

- Create packages.
- Create default tasks associated with new packages.
- Add files to existing packages.
- Create and manage associated Fixlets.
- Add tags to software packages.
- Set individual task logs.

For more information about the dashboard, see “Manage Software Distribution Packages dashboard” on page 7.

---

### SHA-256 task conversion

IBM Endpoint Manager version 9.1 provides the capability to follow the NIST security standards by configuring an enhanced security option. This setting enables SHA-256 as the hashing algorithm for digital signatures and content verification.

When the enhanced security mode is enabled, you can use the SHA-256 algorithm to verify the file download integrity. If you enable this option, SHA-256 downloads are required and all IBM Endpoint Manager 9.1 components no longer process action downloads that only specify a SHA-1 hash. For more information about security configurations, see Security Configuration Scenarios.

IBM Endpoint Manager for Software Distribution provides a method to convert tasks that were created using the Software Distribution dashboard from using the SHA1 algorithm to the SHA-256 algorithm.

**Note:** If you created tasks outside of the Software Distribution Dashboard, you must manually update your custom content to include a SHA-256 hash.

A master operator can convert tasks that are created by all master operators, while a non-master operator can only convert tasks that he created.

To convert SWD tasks that are using still the SHA-1 validation, complete the following steps:

1. Ensure that the enhanced security and SHA-256 downloads options are enabled from the IBM Endpoint Manager Administration Tool. For more information about setting the enhanced security option, see the following sources.
  - Security Configuration Scenarios - Windows Systems

- Security Configuration Scenarios - Linux Systems

**Important:** When you enable the enhanced security option, you configure a restricted security environment that might affect product performance. Also, you cannot roll back to a previous version of Endpoint Manager after the option is enabled. For more information, see Security Configuration Scenarios.

2. From the Manage Software Distribution dashboard, click **Settings**.
3. Click **Sha256 Conversion** to update existing content to include a SHA-256 hash.

**Note:** It might take several minutes to complete.

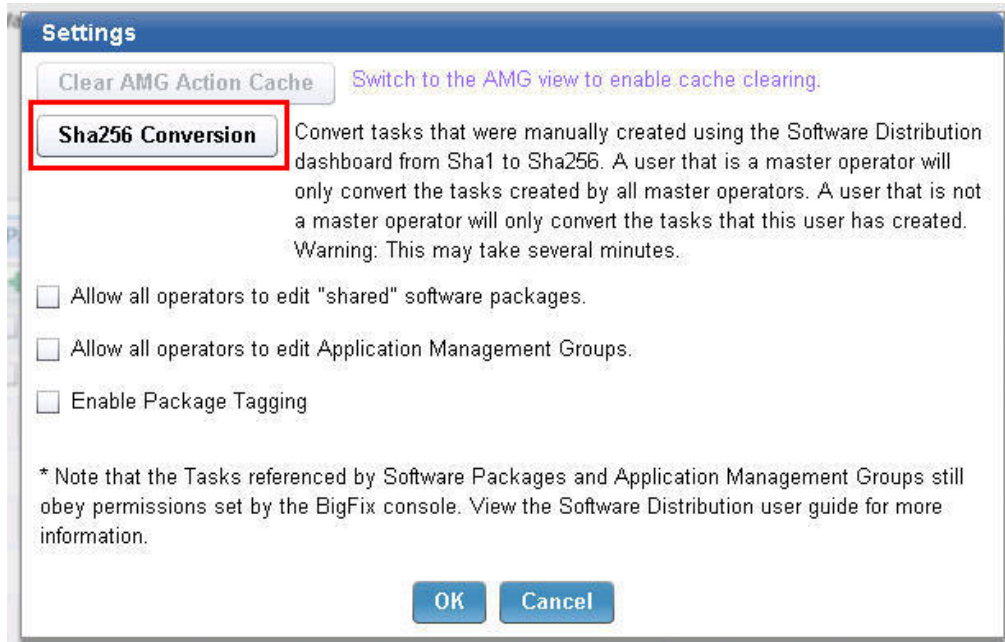


Figure 11. Settings dialog

## Creating a package or Fixlet

You must create a package before you can add files that are needed to install a specific software product.

From the Manage Software Distribution Packages dashboard, click **New Package**.

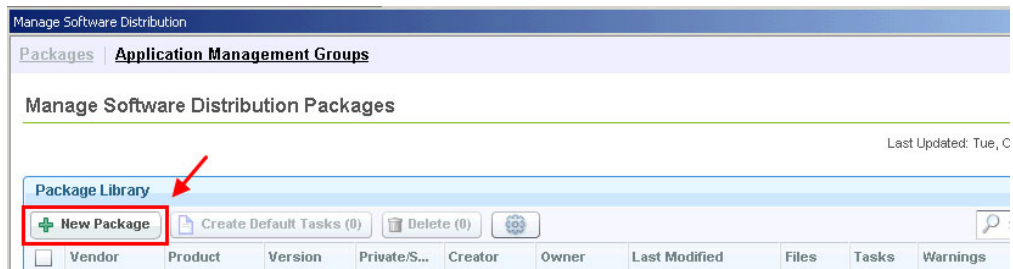


Figure 12. Manage Software Distribution Packages dashboard - New Package

Manually enter values the **Vendor**, **Product**, **Version**, and **Private/Shared** fields.

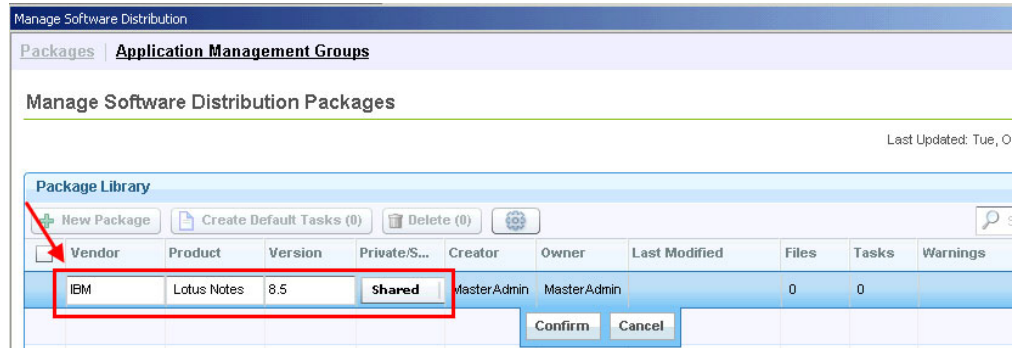


Figure 13. Adding a package

You must designate your package as either *Private* or *Shared*. Shared packages are visible to all Endpoint Manager console operators. Private packages are visible only to the user who created them.

If you designate a package as Shared, be aware that this package cannot be edited by all console operators. To allow all console operators to edit shared packages, click **Settings**.

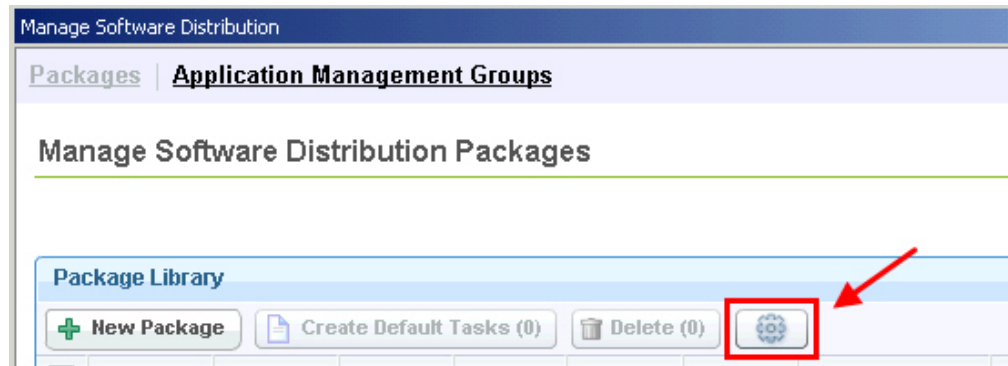


Figure 14. Settings button

Then, select **Allow all operators to edit shared software packages**.

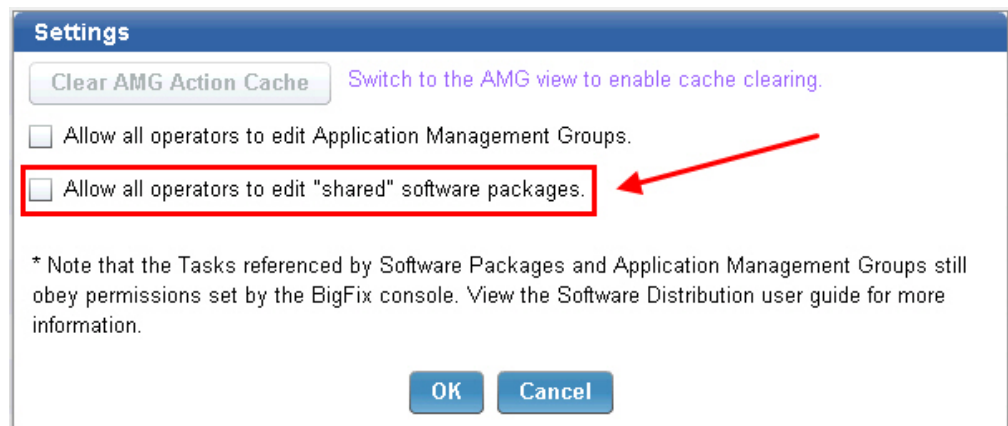


Figure 15. Edit shared packages setting

**Note:** If you do not have console permissions to edit a task, you cannot edit a task even if the option to allow all operators to edit shared packages is set.

**Note:** If you want to keep packages private but share tasks with designated operators, copy the tasks to a custom site. For more information about working with custom sites, see the *IBM Endpoint Manager Console Operator's Guide*.

After you enter all applicable fields, click **Confirm** on the right side of the window.

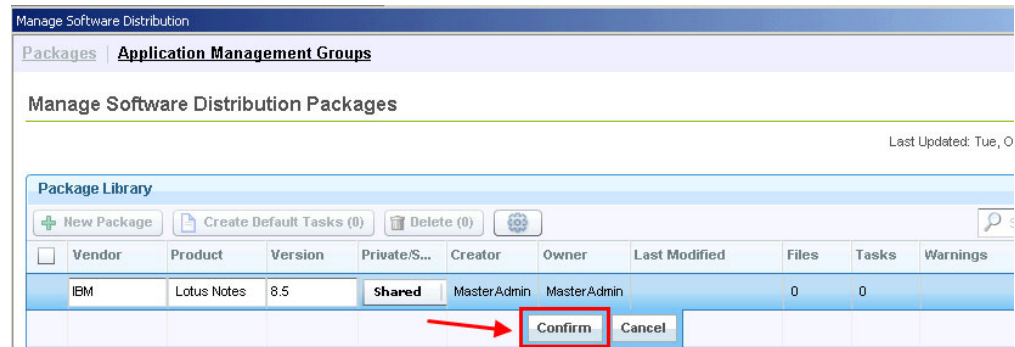


Figure 16. Confirming new package

After creating a package, you can see the package displayed under the Package Library.

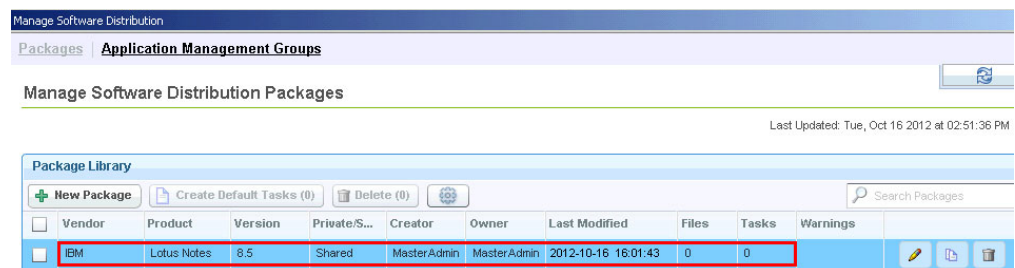


Figure 17. New package displayed under the Package Library

You now have an empty package. You can manage the files and Fixlets that you want to associate with this new package from the second window. The next step is to add files. For more information, see “Editing a package or Fixlet” on page 17.

## Adding tags to packages

To easily query Fixlets for each package, add a tag to the package from the Manage Software Distribution package dashboard.

The package tagging feature is not enabled by default. To enable the tagging feature, a master operator must first click **Settings** and select **Enable Package Tagging**.

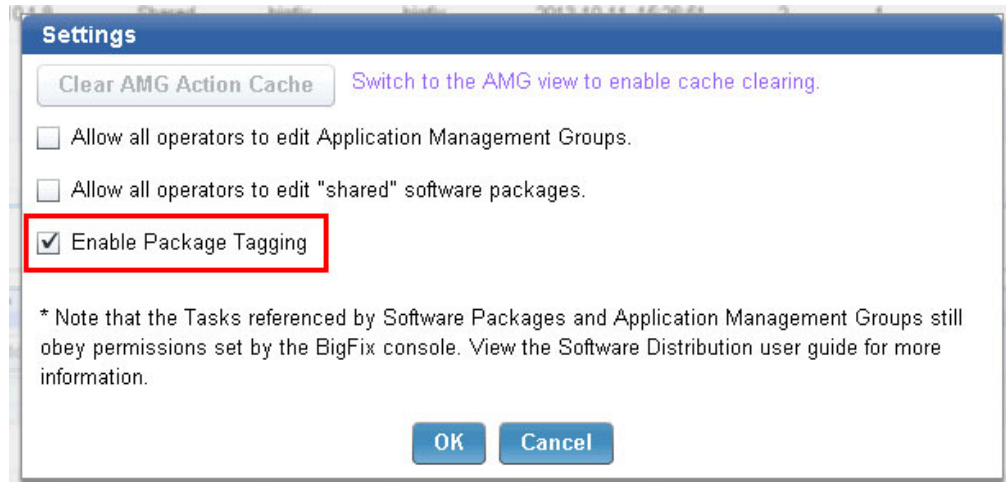


Figure 18. Settings dialog

When you add a tag to a package, the tasks that are related to that package would contain the same tag value.

The package tagging feature is available in the Software Distribution site version 48 and later.

**Note:** Tags are case-sensitive.

- To add a tag to a new package, click **New Package** and enter the package tag in the **Tag** column.
- To add a tag to an existing package, click **Edit** and enter the package tag in the **Tag** column.

When a tag is added to a package, any Fixlet that gets generated from that package would contain the same tag. The Fixlet has a Multipurpose Internet Mail Extensions (MIME) field that contains the tag value, which you can use to query Fixlets. For example, you can issue the following session relevance to query all Fixlets that have the tag value "mytag":

```
(name of it, id of it) of custom bes fixlets whose (mime field "x-fixlet-pkgTag" of it = "mytag")
```

## Editing a package or Fixlet

After creating a package, add the necessary files to install the software product that you want to deploy to your endpoints and then create the distribution tasks.

### Adding the installation files

To add a file to the package, click **Add Files** located under the **Manage Files** tab.

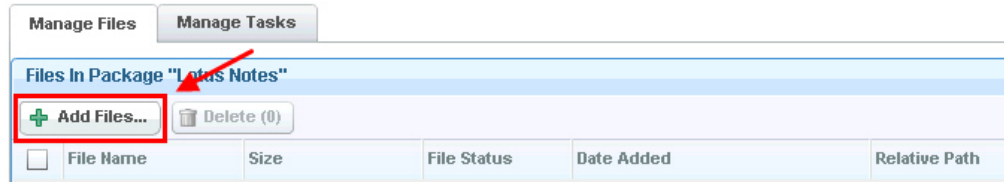


Figure 19. Managing files

This action opens the Add Files to Package window where you can add files and folders. For information about the types of files you can add, see “Supported package types” on page 3.

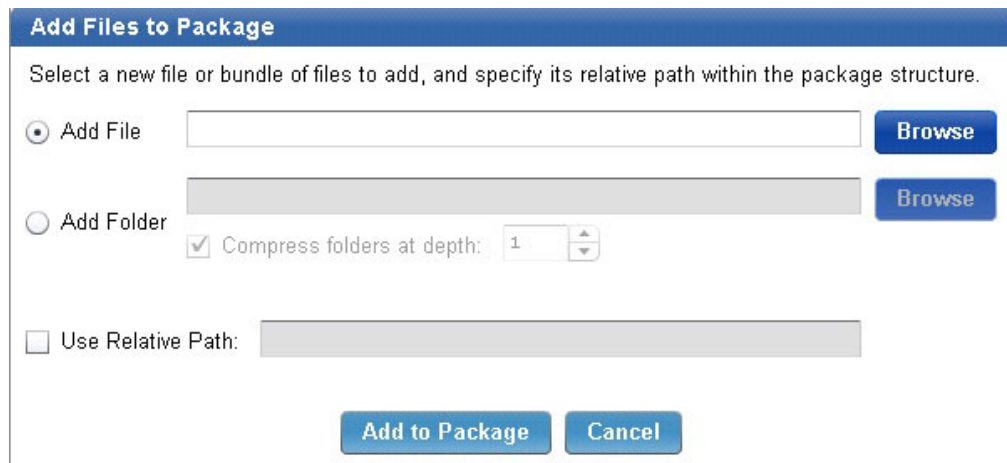


Figure 20. Adding files to a package

Select the **Add File** button. You can manually type the name of the file, or click **Browse** to locate a file stored in your system. Alternatively, you can click **Add Folder** to add an entire folder of content to your package. As in the previous example, type the name of the folder or browse to locate a folder in your system.

The Compression Depth feature, located within the **Add Folder** field, is used to compress files together at a specified folder depth. Use a depth of “0” to bundle all files together into one compression file.

**Note:** To maintain optimum performance, use the compression feature if pushing more than 50 files to an endpoint. Distributing many small files costs more network bandwidth, while distributing fewer large files costs more endpoint processor. Use the **Compress Folders at depth** option to tune this performance control for your environment.

Click **Use Relative Path** if you want to add the files into a specific folder of the package, and then enter the folder directory. For example, you must enter InstallPackage/Languages if you want to add another language file to your package with the following structure:

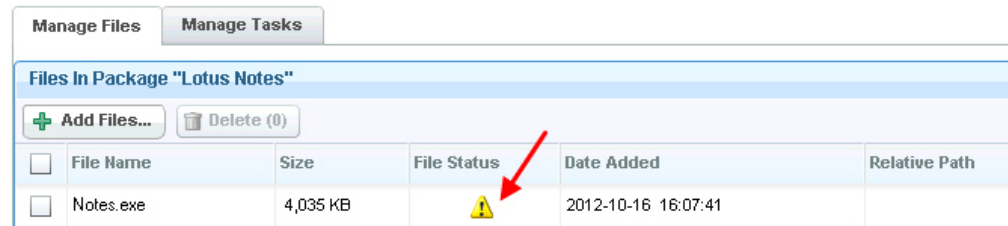
```
InstallPackage
- install.exe (file)
- Languages (folder)
- jpn.srt (file)
- eng.rt (file)
- Cache (folder)
```



Then click **Add to Package** at the bottom of the window. This action processes all the information for your package, analyzes the relevant files, and uploads them to the server.

While files are being uploaded to the server, check the **File Status** field in the dashboard. An exclamation mark indicates that files are not yet uploaded to the IBM Endpoint Manager.

You might need to click **Refresh** to view changes in file status before the dashboard auto-refreshes. The upload is complete when the file status changes to a check mark.



| <input type="checkbox"/> | File Name | Size     | File Status | Date Added          | Relative Path |
|--------------------------|-----------|----------|-------------|---------------------|---------------|
| <input type="checkbox"/> | Notes.exe | 4,035 KB | ⚠           | 2012-10-16 16:07:41 |               |

Figure 21. File status

## Creating distribution tasks

To create a distribution task for the package, click the **Manage Tasks** tab.

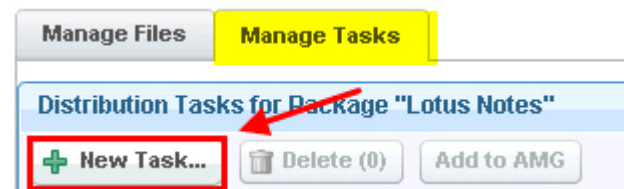


Figure 22. Adding a Fixlet to a package

**Note:** Add tasks only after you add files.

Click **New Task** to open the Create Distribution Task window, which displays all available files associated with your package that can be included in a distribution task.

**Note:** The Policy Action type of Mac PKG tasks is not supported in the Software Distribution task deployment process.

Select each file that you want to deploy to your endpoints, and click **Add**.

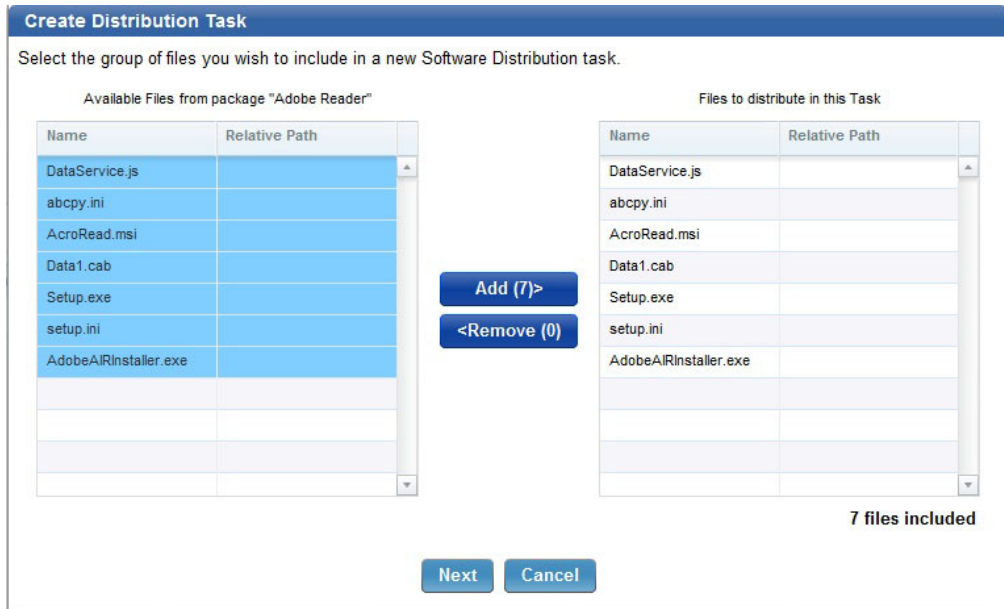


Figure 23. Creating a distribution task

You cannot create a task where all of the files are in a relative path. Software Distribution tasks require that the installation commands exist in the root of the package. If you attempt to add files to a package that has no files in its root folder, the task displays the following warning:

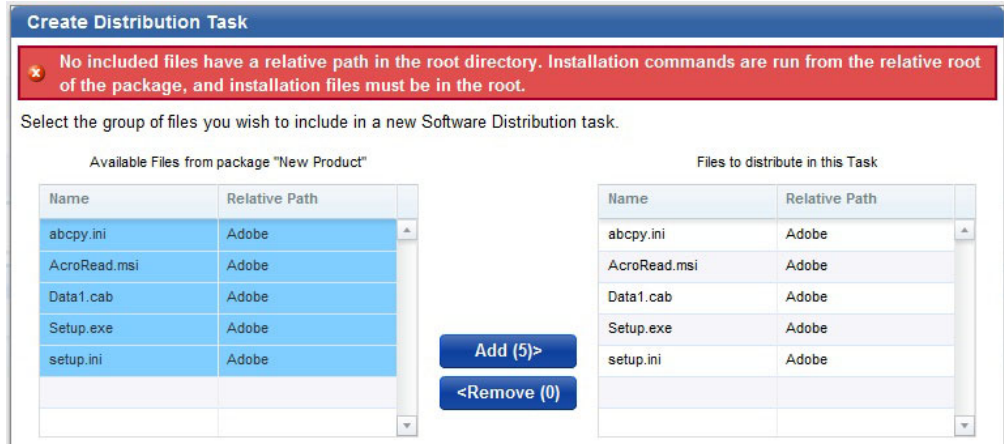


Figure 24. Warning message when files which are not in the root folder, are added to a package

Click **Next**. In this window, you define an installation command to be used when sending the software package to your endpoints, and customize a command-line message specific to your distribution task.

**Create Distribution Task**

Define the installation command which will be run to install the selected software package on endpoints. The installation command will be run from the root folder of the software package.

**Installation Command:**

Show Advanced Options

Also create an associated uninstall task.

Apply MST file(s) to install command. **Transform Option:**

Select the MST files you want to apply. A task will be created for each MST file selected.

| MST File                | Full execution command |
|-------------------------|------------------------|
| No MST files available. |                        |

Create an individual log for this Task

**Name of the log file:**  Use the default name: {Action ID}.log  
 Use a custom name:  .log

Upload this log file to the Server upon completion of this Task

Use custom working directory:  /tmp

**Run Command As:**

System User  Current User (Windows Only)

Figure 25. Defining installation command

**Note:** If you added a PKG file, select whether it is a Mac or Solaris file.

You can also configure the following advanced options for the distribution task:

**Force installation**

This option is only applicable to SPB files.

You can specify the values for the SPB built-in variables, such as the installation path, folder name, file separator, either during the creation of the task or at deployment time.

To modify variables at deployment time, you must select them during task creation. The selected variables can then be edited in the Fixlet description page.

**Create an associated uninstall task**

Select this option to create a task to uninstall the selected software package.

**Apply MST files to the installation command**

If your installation command is an MSI, then select **Apply MST file to install command**. A list of all the MSTs that can be applied to the MSI is displayed.

### Create an individual log

Configure the task to generate an individual log file upon the completion of the action. For more information, see “Generating logs for individual tasks” on page 24.

### Use a custom directory

Specify a full path location, including the drive, to download and run the installation files. For example, C:/SWD.

Files are downloaded and extracted to this custom directory instead of the default \_\_Download/ directory. Tasks run from the specified location instead of the default ../\_BESData/actionsite directory. A folder called tmp is created in the specified path, and is cleared before running any new tasks.

You can configure to remove the files from the client in the tmp folder when the action completes.

You can run the command either as a system user or as a current user. The default is to run the task as a system user, but certain packages require the current user to install the software package successfully. Click **Next**.

Use the three drop-down lists to specify operating system, name, and syntax parameters for targeting using additional conditions. You can combine relevance expressions in the box indicated, or add generated relevance. Click **Create Task** when you complete these steps.

The screenshot shows the 'Create Distribution Task' dialog box. The 'Define additional targeting conditions' section has two radio buttons: 'Do not use any additional targeting conditions.' (unselected) and 'Target using the following conditions:' (selected). Under 'Create Expressions:', there is a table with one row. The first column is '1'. The second column has three dropdown menus: 'Operating System', 'Name', and 'is'. The 'Operating System' dropdown is highlighted with a red box and a red arrow. The third column has a text input field with 'Ex: WinXP' and a 'Match case' checkbox. Below the table, there is a text box for 'Combine Expressions:' with the text 'Combine relevance expressions using logical operator. Example: "(1 OR 2) AND NOT 3"'. Below that is a 'Generated Relevance:' section with a text area. At the bottom, there are three buttons: 'Back', 'Create Task', and 'Cancel'.

Figure 26. Defining additional target conditions

In the next window, click the link in the Actions box to deploy the action, and set parameters in the Take Action dialog.

**Note:** Ensure that you test a Fixlet before deploying it in a production environment.

To verify if the task has completed successfully, check whether the software was installed on the endpoints. For more information, see “Package type verification” on page 23.

You can edit a task only if you have the appropriate console permissions to view and edit the task, regardless of the permissions set through the Manage Software Distribution dashboard. If you do not have console permission to edit a task and you attempt to do so, an error message displays.

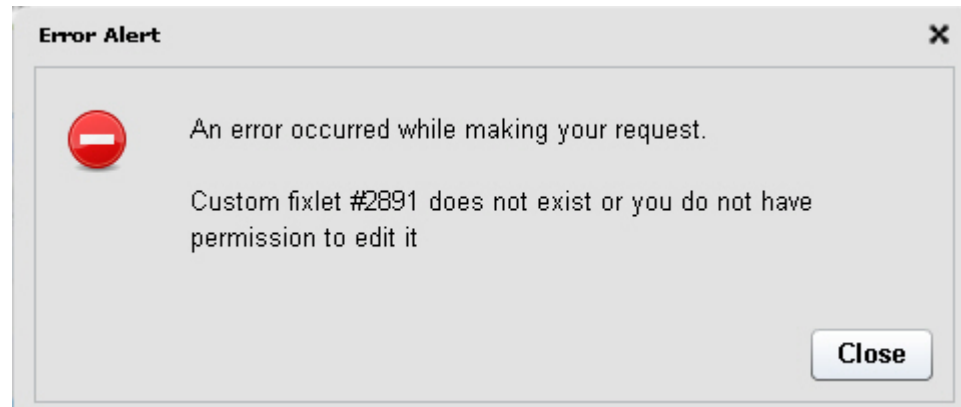


Figure 27. Permission restriction warning

A similar error message displays when you attempt to delete a Software Distribution package through the Manage Software Distribution dashboard without having the appropriate permission.

## Package type verification

Check the state of your endpoints where you deployed the distributed task to verify whether the software was installed successfully.

Ensure that the software installation for each package type is successful by checking the state of the endpoint before and after deploying the task.

Table 1. How to verify the installation of different package types

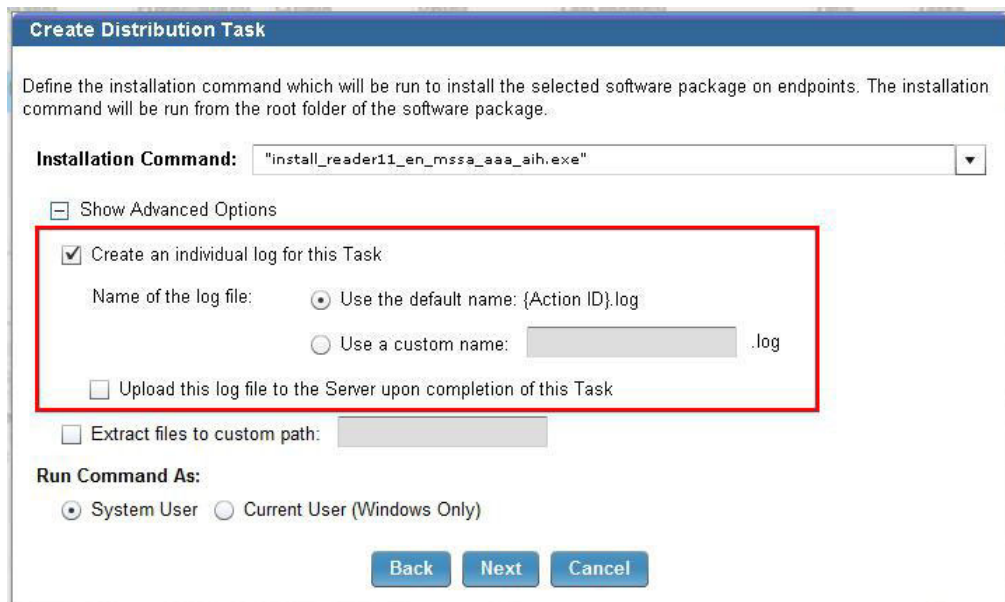
| Package Type | System state of the endpoint before the installation  | System state of the endpoint after the installation  |
|--------------|---|--|
| MSI          | The task must be relevant, which means that the software that you want to install has not been installed yet.   | The task must no longer be relevant to mean that the software installation was successful.   |
| EXE          | The software that you want to install must not be listed in the <b>Control Panel &gt; Programs and Features</b> .   | The software that you installed must be listed in the <b>Control Panel &gt; Programs and Features</b> .  |
| BAT          | The folder for the software that you want to install must not be found in C:\Program Files (x86)\BigFix Enterprise\BES Client\__BESTData\actionsite\__Download. | A new folder for the installed software must be found in C:\Program Files (x86)\BigFix Enterprise\BES Client\__BESTData\actionsite\__Download. |
| PKG          | The package must not be listed when you run the command <b>pkgutil --pkgs</b> .   | Run the command <b>pkgutil --pkgs</b> . The package must be listed to mean that the software installation was successful.                      |

## Generating logs for individual tasks

Configure a distribution task to generate an individual log file upon its completion. You can enable the individual task logging feature to generate log entries for new and existing tasks. You can also upload the logs to the server for parsing purposes.

The log collection does not negatively affect the server as the size of each log file is limited to 1 MB. However, volume management can be used to partition the log directory with limited space so any resource issues affect the log storage only. This practice prevents the server from being overwhelmed.

1. From the Create Distribution Task window of the Manage Software Distribution Packages dashboard, click **Next** until you see the **Show Advanced Options** under the installation command.
2. Click **Show Advanced Options**.
3. Click **Create an individual log for this Task**.



The screenshot shows the 'Create Distribution Task' window. The 'Installation Command' field contains the text '"install\_reader11\_en\_mssa\_aaa\_aih.exe"'. Below this, the 'Show Advanced Options' checkbox is checked. Underneath, the 'Create an individual log for this Task' checkbox is also checked. The 'Name of the log file' section has two radio buttons: 'Use the default name: {Action ID}.log' (selected) and 'Use a custom name: [text box].log'. There is also an unchecked checkbox for 'Upload this log file to the Server upon completion of this Task'. At the bottom, there are 'Back', 'Next', and 'Cancel' buttons.

Figure 28. Create individual log

4. Select the name that you want for the log file. The default name for the log is `<Action_ID>.log`. If you want to specify a different name, enter any alphanumeric characters.

**Note:** Underscores are acceptable.

5. If you want to upload the file to the server when the task completes, click **Upload this log file to the Server upon completion of this Task**.
6. Follow the remaining instructions in the Create Distribution Task window.

If you configured the task to upload the log files to the server, a new folder that is called `LogsToBeUploaded` is created in `\BES Client\__BESData\__Global\SWDDeployData`.

**Note:** Generally, deployment results of all deployed software are logged in a single log file that is located in `\BES Client\__BESData\__Global\SWDDeployData\SWD_DeploymentResults.log`.

The logs that are uploaded to the server are in `\BES Server\UploadManagerData\BufferDir\shal\<last 2 digits of the compute ID>`.

The file name format of the logs that are in the server is not the same as the logs that are in the client. When a log file is uploaded to the server, a prefix string SWD is added to the log file name. You can change this prefix in the action script of the task.

**CAUTION:** The server mirrors the client folder. When you delete the logs in the client folder, the logs in the server side are also deleted. Ensure that you backed up the server log directory before you delete the log files from the client folder by using Fixlet 13. If the server space becomes too large, back up the logs in the server then clean the client folder.

---

## Software repositories migration

The Software Distribution Upload Manager is a stand-alone tool that helps you to upload any packages that already exist in your deployment before installing Software Distribution.

The tool uploads your packages to the IBM Endpoint Manager server. You can use the dashboard to create related default Software Distribution tasks.

Before Endpoint Manager can deploy software packages, it needs a tool to analyze, archive, and upload those packages to the IBM Endpoint Manager server. The tool is called `uploadmanager.exe`. This tool requires access to the IBM Endpoint Manager server and database. You can find the tool on your IBM Endpoint Manager server in the `BES Server\BESReportsServer\wwwroot\SiteData\bes_bfenterprise\Sites\Software Distribution` folder. The tool must be copied to a working directory before use.

The tool can be used to create a script to import a library in two ways:

- A script can be written to produce a list of directory names that are passed into the Upload Manager as an `inputdirslist`. This process is the ideal approach for libraries that are structured. For example, if the software repository reliably follows the pattern of `/VENDOR/PRODUCT/VERSION` folders, a simple listing of those folders is sufficient.
- A script can be written that iterates the file system and calls the tool repeatedly on a per product directory basis. This process is the ideal approach for libraries that are not structured, in which the external script must test a directory for applicability.

Packages that are uploaded in this manner have their files uploaded and their metadata entered with estimated values derived from file analysis. To generate Fixlets using these estimated values, select the uploaded packages and click **Create Default Tasks**.

**Note:** All Fixlets generated in this manner are marked as Validation Required.

For access to the upload manager, see the BigFix software download website. For detailed usage instructions, see this technote.

### Return codes

Use the following `uploadmanager.exe` return codes when troubleshooting failures:

Return Code 0 = success  
Return Code 1 = incorrect command line usage  
Return Code 2 = partial upload failure  
Return Code 4 = full upload failure  
Return Code 8 = dsn login failed  
Return Code 16 = json error;  
Return Code 32 = compression partial failure  
Return Code 64 = compression full failure  
Return Code 128 = file access error  
Return Code 256 = tempfile deletion failure  
Return Code 512 = database query error  
Return Code 1024 = Invalid file/folder error



---

## Chapter 5. Managing Application Management Groups

Group software distribution tasks and client computers for faster deployment, especially in large networks.

Most software deployments are controlled by console operators. Operators choose which software to deploy to different computers or groups of computers. Operators can also choose whether to have the software installed as a mandatory action or to comply to a policy.

Endpoint Manager has a mechanism called *Offers* to handle self-provisioning of software. Some software can be made optionally available to endpoint users who can choose to install the software from the following options:

- Client Dashboard for Software Offers. For more information, see “Client Dashboard for Software Offers” on page 11.
- Software Distribution Self Service Portal. For more information, see “Software Distribution Self Service Portal overview” on page 45.

To simplify the distribution of software offers and actions, group the tasks and endpoints into different Application Management Groups. *Application Management Groups* are collections of tasks that can be organized into groups of content and delivered to targeted groups of client computers. These tasks are viewed by Endpoint Manager clients as offers, policy actions, or mandatory actions. For more information about where to deploy offers, see “Manage Application Management Groups dashboard” on page 8.

### User permissions

Application Management Group access level is determined at the time of its creation and cannot be altered.

#### Master Operator

If the Application Management Group is owned by a master operator, then the Application Management Group is fully accessible to all master operators.

A master operator-controlled Application Management Group has the following properties:

- All master operators can edit, delete, deploy, or stop the Application Management Group.
- Non-master operators can view and copy the Application Management Group.
- All users can make a copy of the Application Management Group.
- If the owner of the Application Management Group is demoted from a master operator to a non-master operator, the owner loses access to the Application Management Group.

#### Non-master Operator

If the Application Management Group is owned by a non-master operator, then the Application Management Group is fully accessible only by the owner.

An owner-controlled Application Management Group has the following properties:

- Only the owner can edit, delete, deploy, or stop the Application Management Group. You can set to allow all console operators to edit the Application Management Group. See "Settings."
- Master operators can only stop the Application Management Group that is owned by a non-master operator.
- All users can make a copy of the Application Management Group.
- If the owner of the Application Management Group is promoted from a non-master operator to a master operator, the owner gains full access. Other master operators can only stop or delete the Application Management Group that is now owned by a master operator.

## Settings

To allow all console operators to edit the Application Management Group, click **Settings**.



Figure 29. Settings button

Then, select **Allow all operators to edit Application Management Groups**.

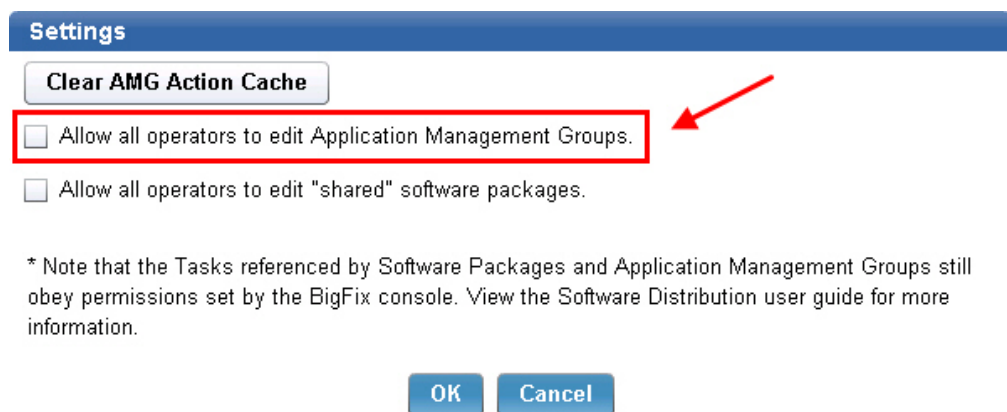


Figure 30. Edit Application Management Groups setting

---

## Creating a custom site

Creating a custom site to host the Application Management Group deployments reduces the effect on the performance of the master action site.

When you access the Manage Application Management Groups dashboard for the first time, you are prompted to create a custom site.



Figure 31. Creating a custom site

**Note:** You must be a master operator to create a custom site.

The default custom site name is *swd\_app\_group*. You can enter any name for the custom site, and click **Create**.

The custom site stores the Application Management Group computer groups that are created from the dashboard.

After you create the custom site, you must complete the following tasks:

- Subscribe all Software Distribution endpoints to the custom site.
- Give write access to all operators who are going to use the Manage Application Management Groups dashboard.

---

## Setting up viewing permissions

Users of the Manage Application Management Groups dashboard who are master operators must set their permissions to view issued actions of other operators.

1. Select a master operator from the Operator list.
2. Click the **Details** tab.
3. Select **Yes** from the **Show Other Operator's Actions** drop-down menu.

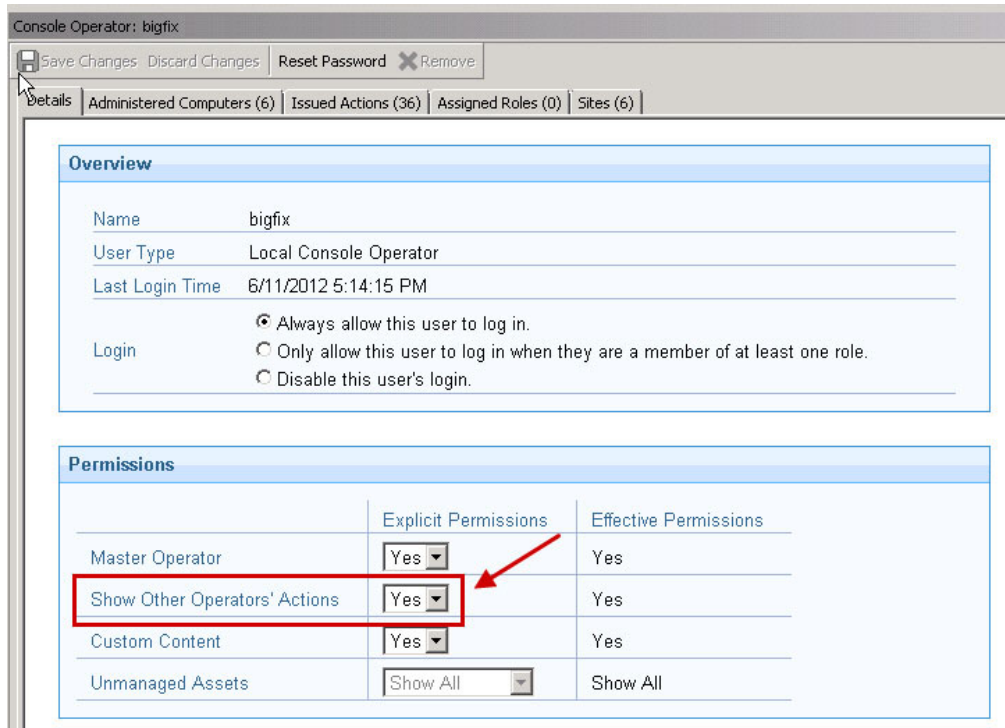


Figure 32. Viewing permissions

4. Click **Save Changes**.

## Creating Application Management Groups

An Application Management Group is a collection of tasks and targets. When an Application Management Group is deployed, its tasks are distributed as offers or actions to all of its targets.

You must complete the following tasks:

- Create a custom site to limit the performance impact on the master action site. You must create a custom site when you access the Application Management Group dashboard for the first time. For more information, see creating a custom site.
- If you are a master operator, ensure that you set the viewing permissions correctly. For more information, see “Setting up viewing permissions” on page 29.
- Upgrade the Endpoint Manager console and client to version 8.2.1310. The Client dashboard does not work correctly for earlier versions.
- Run the Enable Client Dashboard for Software Offers task. You can find this task under the Configure Client Dashboard, which is in the Software Distribution Setup node of the navigation tree.

**Note:** You must subscribe at least one computer to the custom site and assign appropriate operator permissions.

1. From the Manage Application Management Group dashboard, click **New**.

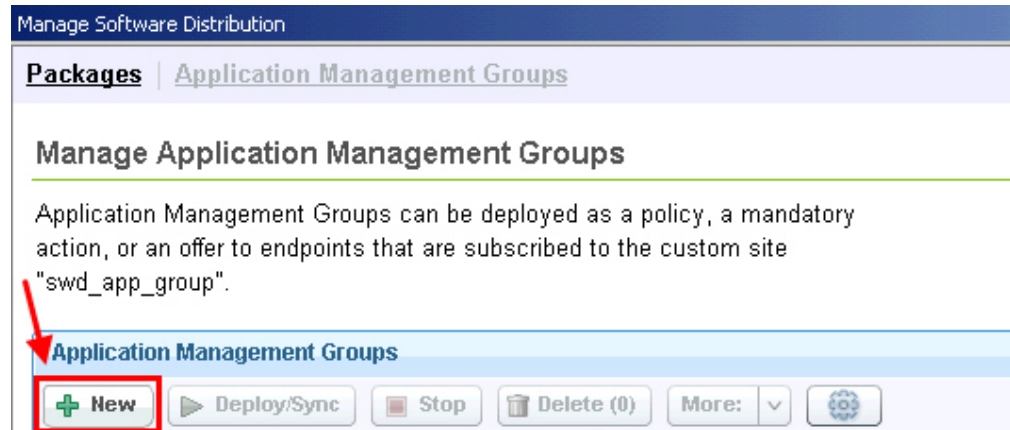


Figure 33. New Application Management Group

2. Enter a name for the group in the **Name** field.
3. Click **Confirm**. You can now see the new group displayed under the Application Management Groups Library.

You now have an Application Management Group.

The next steps are to add tasks and targets. For more information, see Adding tasks and Adding targets.

You can manage the tasks and targets that you want to associate with the Application Management Group from the Tasks and Targets tabs.

## Adding tasks to an Application Management Group

You can use any of the software distribution dashboards to select the tasks you want to add to an Application Management Group.

### From the Manage Software Distribution Packages dashboard

You can add tasks to existing Application Management Groups from the Manage Software Distribution Packages dashboard.

1. On the **Manage Tasks** tab, select one or more task that you want to add in an Application Management Group.
2. Click **Add to AMG**.

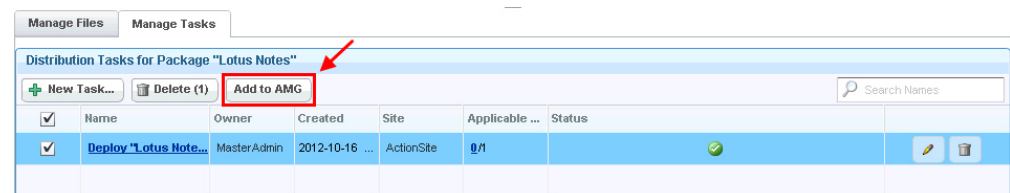


Figure 34. Adding tasks from the Manage Software Distribution Packages dashboard

The Add to AMG dialog opens.

3. Select the Application Management Group to which you want to add the selected tasks, and click **Next**.

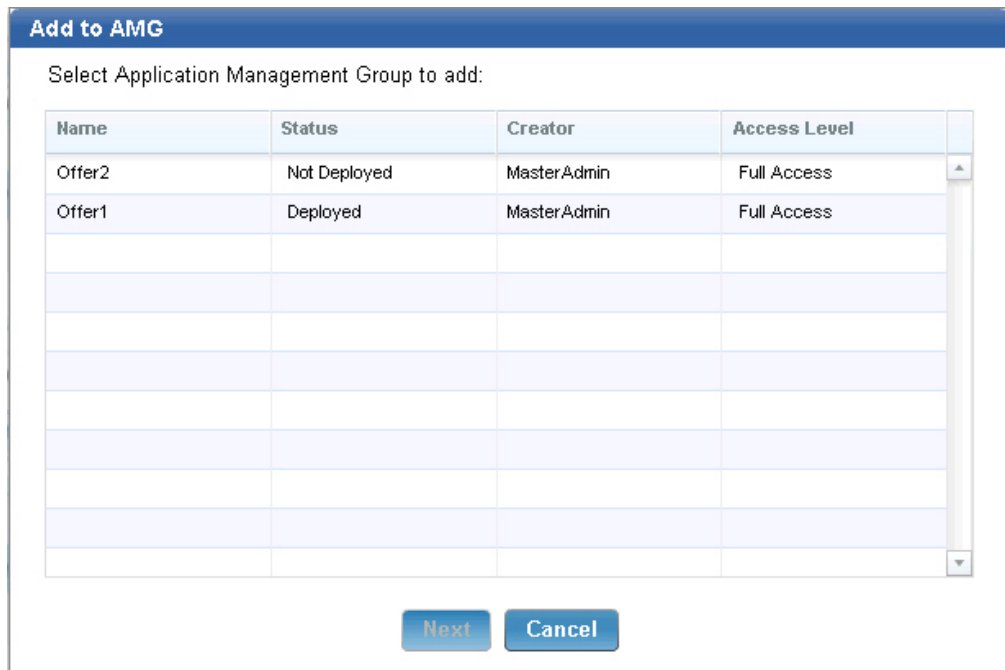


Figure 35. Select an Application Management Group

**Note:** If the status of the selected Application Management Group is "Deployed", you must deploy the Application Management Group again after adding the task. For more information, see "Deploying Application Management Groups" on page 40.

4. Select how you want to deploy the task. You can select from the following options:

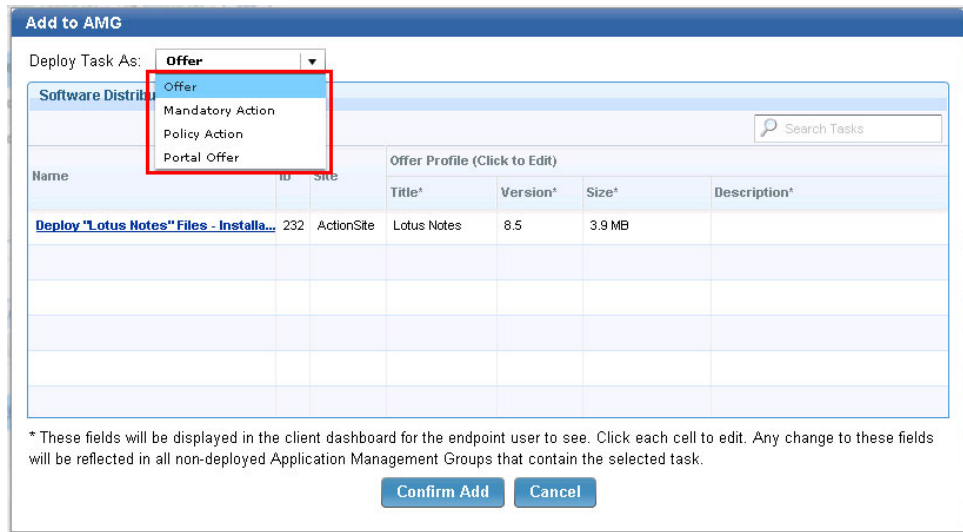
**Offer** This action handles self-provisioning of software from the Client Dashboard for Software Offers.

**Mandatory Action**  
This action runs once and expires.

**Policy Action**  
This action continually runs and checks whether your computers comply to the policy.

**Portal Offer**  
This action handles self-provisioning of software from the Software Distribution Self Service Portal.

**Note:** Deploying a Portal Offer does not immediately create an action. You must deploy the Application Management Group when a task is added to have the offer shown in the Self Service Portal.



- Optional: If you want to edit the profile for the mandatory action, client, or portal offer, double-click the appropriate cells.  
For mandatory actions, you can update the expiration time. For offers, you can update the title, version, size, or description and make it meaningful and appropriate for the endpoint clients.

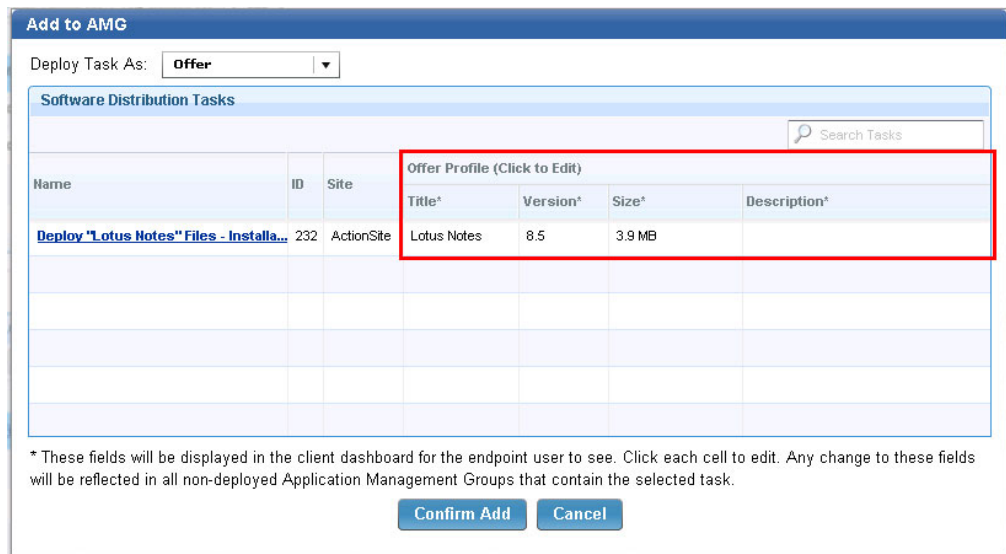


Figure 36. Edit offer profile from the Add Tasks dialog

**Note:** All Application Manager Groups that are not yet deployed and that contain the same offer or action are also updated. Each offer or action can have only one profile. The offer or action profile remains the same in other Application Management Groups.

- Click **Confirm Add**. The task is now added to the Application Management Group that you selected.

If you already added targets to the Application Management Group, you can now deploy the Application Management Group. For more information, see “Deploying Application Management Groups” on page 40. Otherwise, start adding targets to the Application Management Group. For more information, see Adding targets.

## From the Manage Application Management Groups dashboard

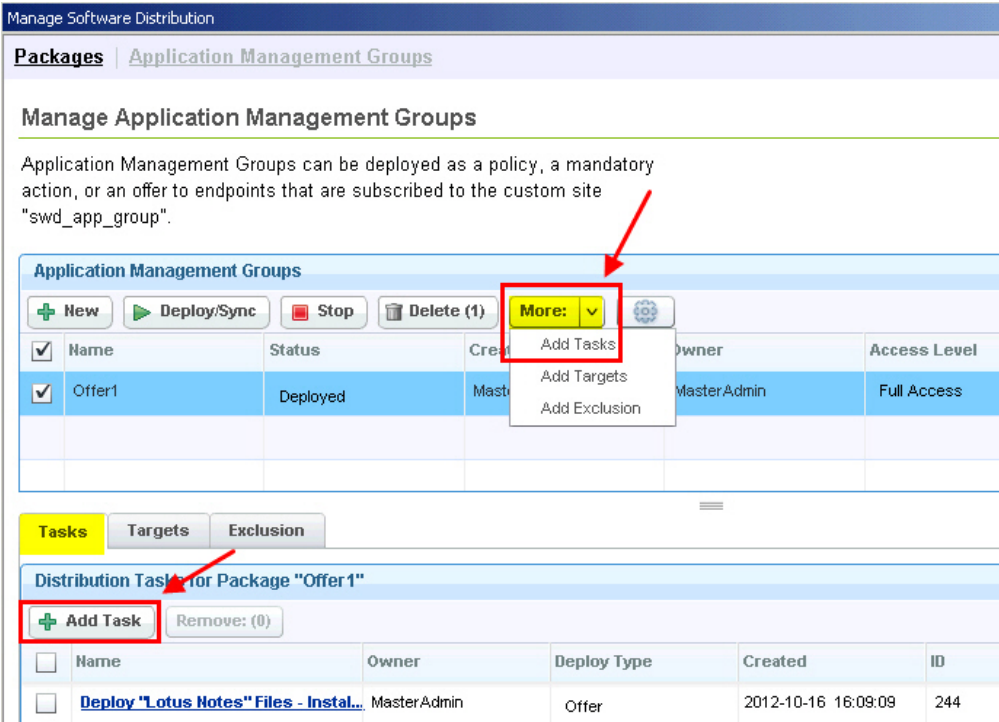
You can also add tasks to an Application Management Group from the Manage Application Management Group dashboard.

1. Select the Application Management Group to which you want to add tasks.

**Note:** If the status of the selected Application Management Group is "Deployed", you must deploy the Application Management Group again after adding the tasks. For more information, see "Deploying Application Management Groups" on page 40.

2. Open the Add Tasks dialog. There are two ways to add tasks from this dashboard:

- Click **More** > **Add Tasks**.
- Click **Tasks** > **Add Tasks**.



The screenshot shows the 'Manage Application Management Groups' dashboard. At the top, there are tabs for 'Packages' and 'Application Management Groups'. Below the title, there is a description: 'Application Management Groups can be deployed as a policy, a mandatory action, or an offer to endpoints that are subscribed to the custom site "swd\_app\_group".' A table lists the groups, with one row for 'Offer1' in a 'Deployed' state. A 'More:' dropdown menu is open over the 'Offer1' row, showing options: 'Add Tasks', 'Add Targets', and 'Add Exclusion'. Below the table, there are tabs for 'Tasks', 'Targets', and 'Exclusion'. The 'Tasks' tab is active, showing a section for 'Distribution Tasks for Package "Offer1"'. An 'Add Task' button is highlighted with a red box. Below this, a table lists tasks, with one task: 'Deploy "Lotus Notes" Files - Instal...' created by 'MasterAdmin' on '2012-10-16 16:09:09' with ID '244'.

Figure 37. Adding tasks from the Manage Application Management Groups dashboard

The Add Tasks dialog opens and lists all the available software distribution tasks. These tasks were created from the Manage Software Distribution Packages dashboard, and are viewed by endpoint users as offers from the Client Dashboard for Software Offers.

3. Select how you want to deploy the task. You can select from the following options:

**Offer** This action handles self-provisioning of software from the Client Dashboard for Software Offers.

**Mandatory Action**

This action runs once and expires.



### Policy Action

This action continually runs and checks whether your computers comply to the policy.

### Portal Offer

This action handles self-provisioning of software from the Software Distribution Self Service Portal.

**Note:** Deploying a Portal Offer does not immediately create an action. You must deploy the Application Management Group when a task is added to have the offer shown in the Self Service Portal.

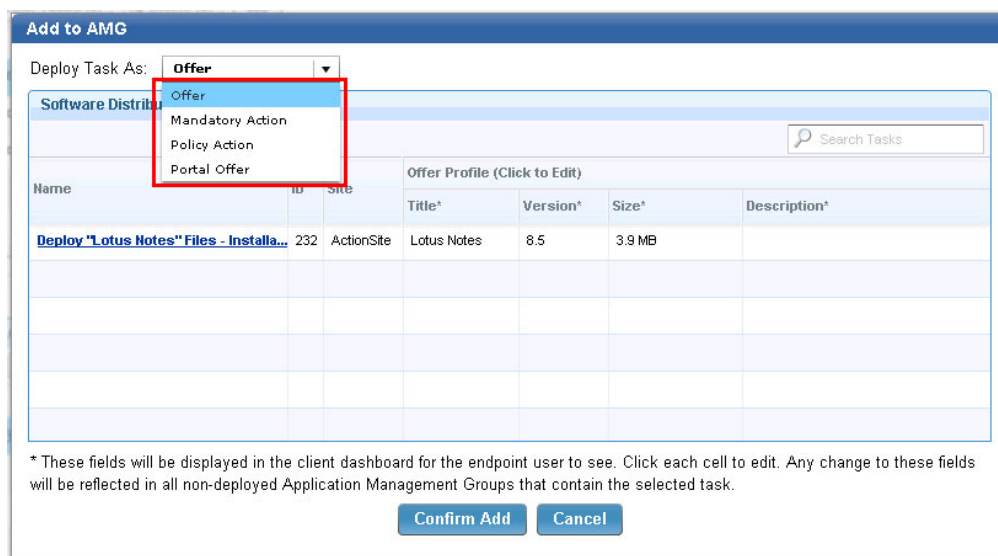


Figure 38. Add Tasks dialog

4. Select the tasks that you want to deploy to a particular group of clients.
5. Optional: If you want to edit the profile for the mandatory action, client, or portal offer, double-click the appropriate cells.

For mandatory actions, you can update the expiration time. For offers, you can update the title, version, size, or description and make it meaningful and appropriate for the endpoint clients.

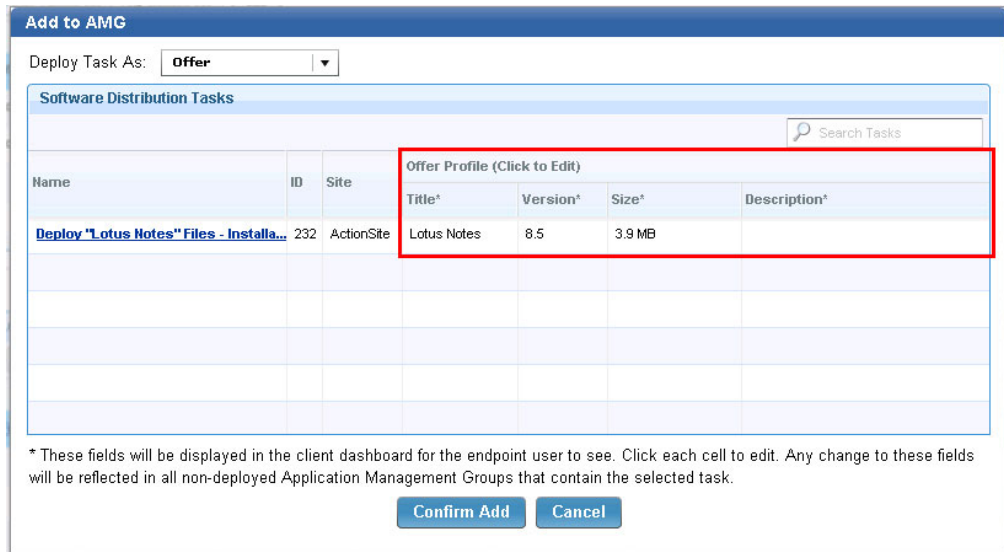


Figure 39. Edit offer profile from the Add Tasks dialog

**Note:** All Application Manager Groups that are not yet deployed and that contain the same offer or action are also updated. Each offer or action can have only one profile. The offer or action profile remains the same in other Application Management Groups.

6. Click **Confirm Add**. The **Software Distribution** tasks that you added are shown on the **Tasks** tab.

If you already added targets to the Application Management Group, you can now deploy the Application Management Group. For more information, see “Deploying Application Management Groups” on page 40. Otherwise, start adding targets to the Application Management Group. For more information, see Adding targets.

## Adding targets to an Application Management Group

You can add targets to an Application Management Group from the Manage Application Management Group dashboard.

You can use the Add Target dialog to add Computer Groups or Active Directory Groups to the named target group.

Targets are computer groups that operators issue software distribution tasks to. These groups were previously defined in your console environment.

1. Select the Application Management Group to which you want to add targets.

**Note:** If the status of the selected Application Management Group is "Deployed", you must deploy the Application Management Group again after adding the targets. For more information, see “Deploying Application Management Groups” on page 40.

2. Open the Add Targets dialog. There are two ways to add targets from this dashboard:
  - Click **More > Add Targets**.
  - Click **Targets > Add Targets**.

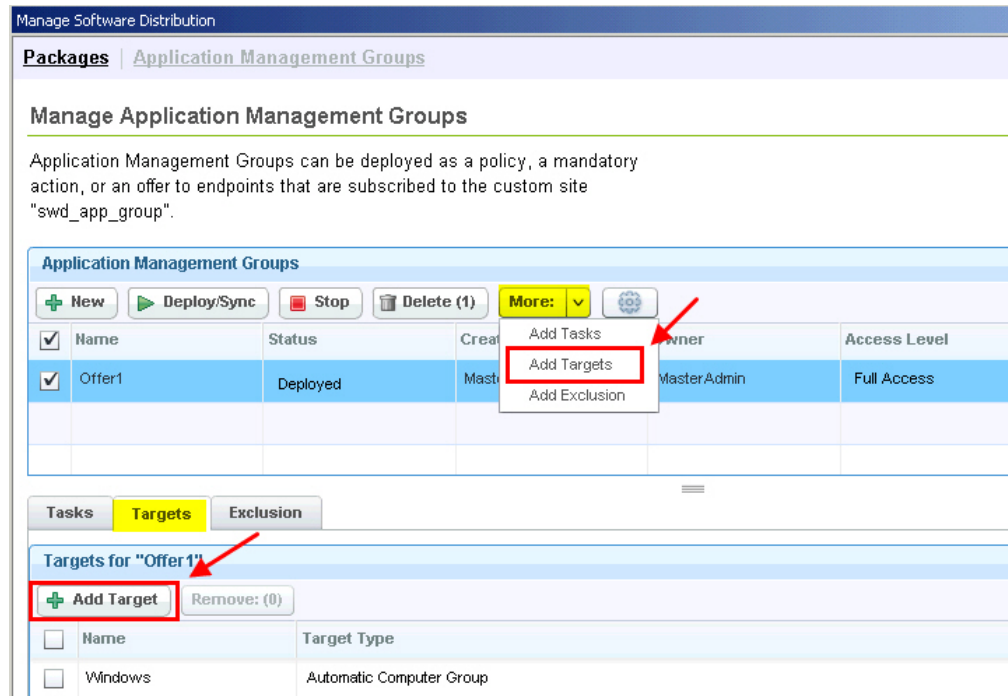


Figure 40. Adding targets from the Manage Application Management Groups dashboard

The Add Targets dialog opens.

3. You can select targets either from a Computer Group or from an Active Directory Group.
  - If you select Computer Group as the target, select the available targets for that group, and click **Add**.

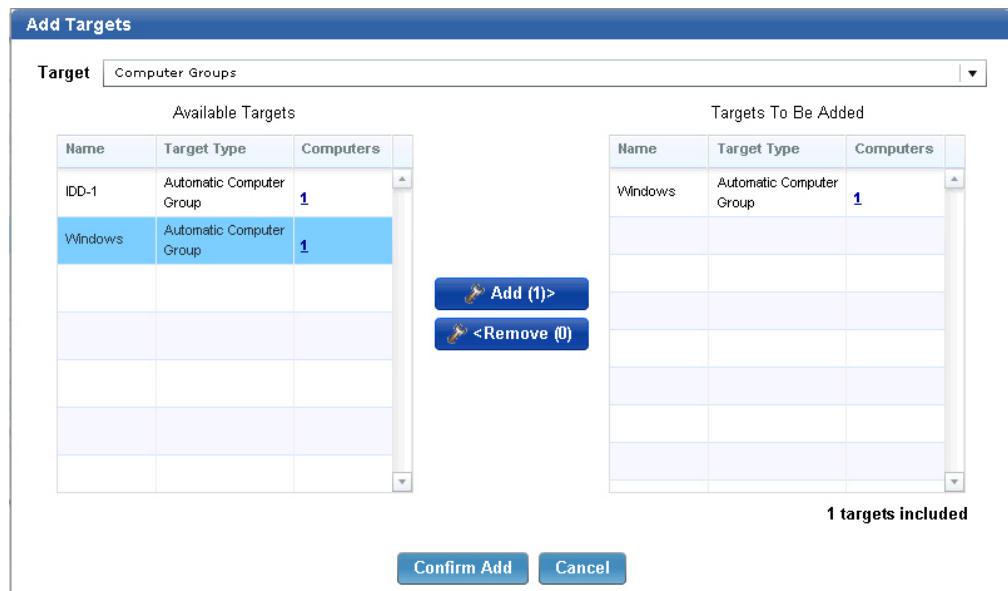


Figure 41. Add target- Computer Group

- If you select Active Directory Group as the target, enter the targets for that group, and click **Add**.

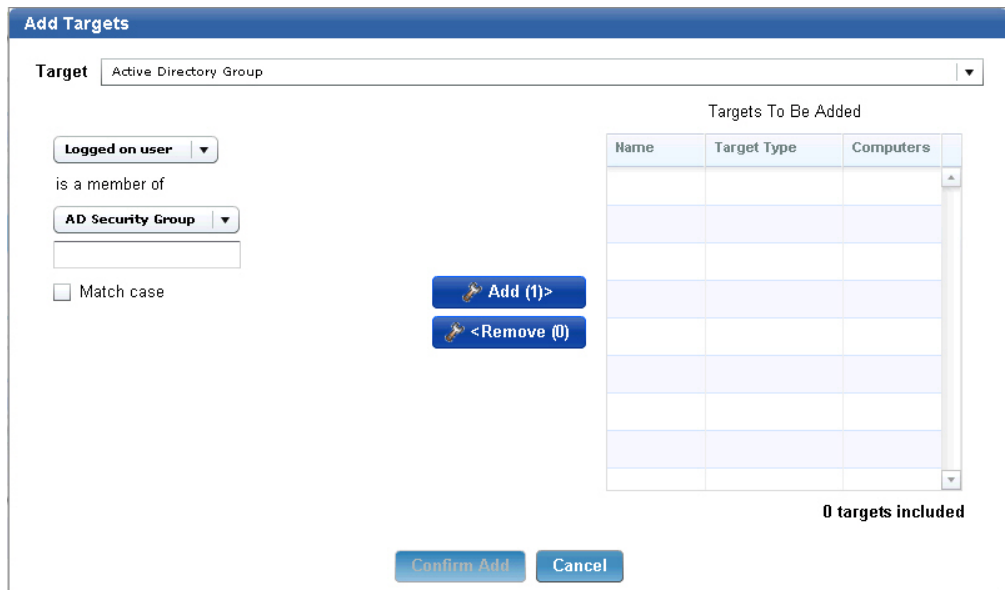


Figure 42. Add target- Active Directory Group

4. Click **Confirm Add**. The targets that you added are shown under the Targets tab.

**Note:** When new targets are added, only the definition of the Application Management Group changes. The same offer becomes relevant to other targeted computers.

If you already added tasks to the Application Management Group, you can now deploy the Application Management Group. For more information, see “Deploying Application Management Groups” on page 40. Otherwise, start adding tasks to the Application Management Group. For more information, see Adding tasks.

## Adding an exclusion to an Application Management Group

You can add a target as an exclusion to remove it from the Application Management Group. When the Application Management Group is deployed, the tasks are distributed only to the targeted computer groups and not to the excluded computer group.

Only one exclusion can be added for each Application Management Group. An existing exclusion is overwritten each time you add an exclusion.

1. Select the Application Management Group to which you want to add an exclusion.

**Note:** If the status of the selected Application Management Group is “Deployed”, you must deploy the Application Management Group again after you add the exclusion. For more information, see “Deploying Application Management Groups” on page 40.

2. Open the Add an Exclusion dialog. There are two ways to add an exclusion from this dashboard:
  - Click **More > Add Exclusion**.
  - Click **Exclusion > Add Exclusion**.

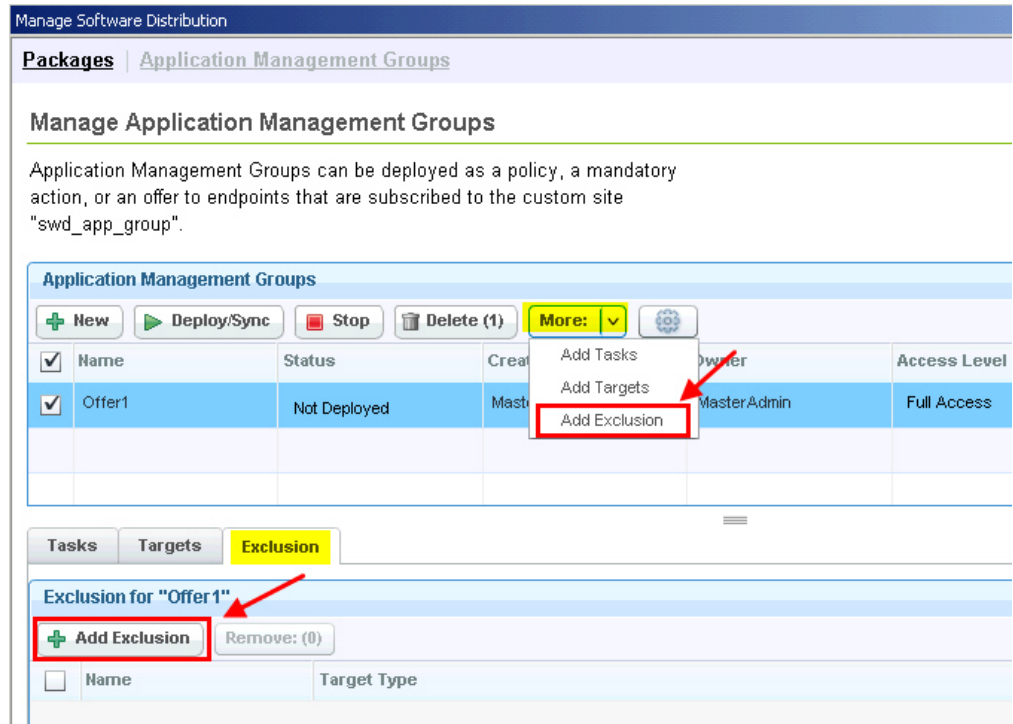


Figure 43. Adding an exclusion

The Add an Exclusion dialog opens.

3. Select one computer group from the list of available computer groups.

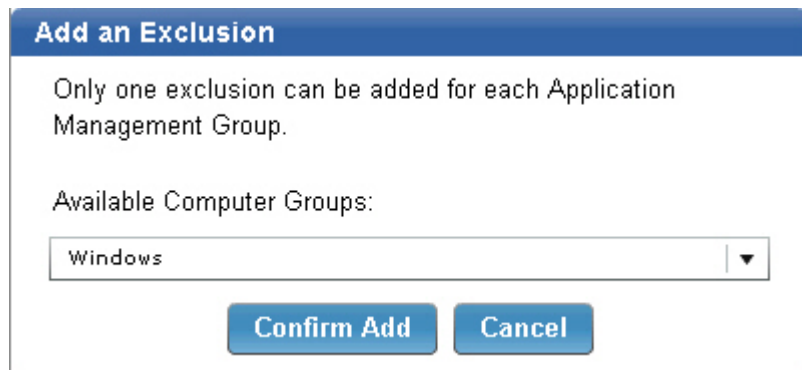


Figure 44. Selecting an exclusion from available computer groups

4. Click **Confirm Add**.

The following scenario is an example of computers being excluded from an Application Management Group.

**Note:** The letters refer to individual computers.

Target1: Computer Group 1 (A, B)  
 Target2: Computer Group 2 (B, C)  
 Target3: Computer Group 3 (C, D)  
 Exclusion: Computer Group 2 (B, C)

As a result, no computers in "Computer Group 2" are applicable. When the Application Management Group is deployed, the tasks are distributed only to computers "A" and "D".

## Deploying Application Management Groups

Learn how Application Management Groups are deployed and how they relate to Endpoint Manager computer groups.

When an Application Management Group is deployed, the following entities are created:

- An automatic computer group.
- An action for each task.

### Computer groups

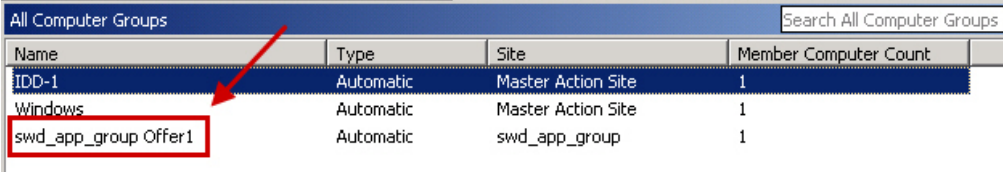
The Application Management Group computer group is stored at the custom site, which was created during the initial setup process. For example, if five Application Management Groups are deployed, then five automatic computer groups are created, one for each Application Management Group.

The computer group definition contains all the targets that are listed in the Application Management Group.

The computer groups use the following naming convention:

*name\_of\_the\_custom\_site name\_of\_the\_Application\_Management\_Group*

For example, if you named the custom site as "swd\_app\_group" during the setup process and have an Application Management Group called "Offer1", you can find a computer group called "swd\_app\_group Offer1" in the "swd\_app\_group" site.



| Name                 | Type      | Site               | Member Computer Count |
|----------------------|-----------|--------------------|-----------------------|
| IDD-1                | Automatic | Master Action Site | 1                     |
| Windows              | Automatic | Master Action Site | 1                     |
| swd_app_group Offer1 | Automatic | swd_app_group      | 1                     |

Figure 45. Computer group naming convention

### Actions

The number of actions that are created upon deployment depends on the operator site. There can be one action per task per operator site. For example, a non-master operator creates two Application Management Groups and adds the same task to both groups. When the two groups are deployed, only one action is created. If another operator creates an Application Management Group and adds the same task as the first operator and deploys the group, a separate action is created. In this example, a total of two actions were created, one for each operator.

Master operators use the same operator site, so if five different master operators use the same task in their Application Management Groups, only one action is created for that task.

The actions use the following naming convention:

SWD AMG Action: *title\_of\_the\_originating\_task*

Each action references the ID of the automatic computer group in the custom site. For example, if you have a computer group called "swd\_app\_group Offer1" and this computer group has ID 44. The action contains a relevance clause that checks to see if the endpoint is a member of the computer group whose ID is 44.

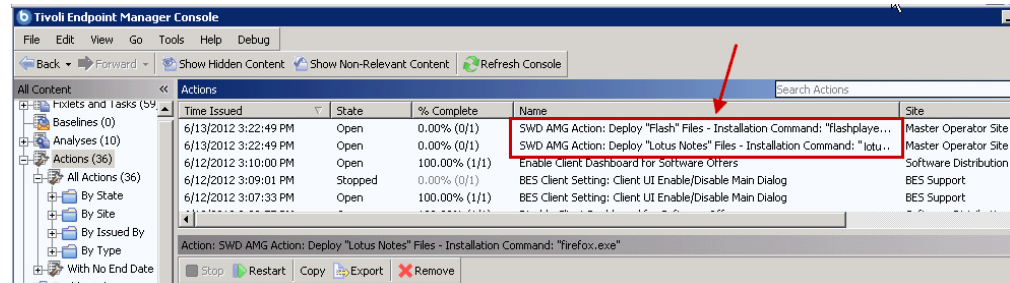


Figure 46. Action naming convention

## Deployment

To deploy an Application Management Group, select the group that you want to deploy, and click **Deploy/Sync**.

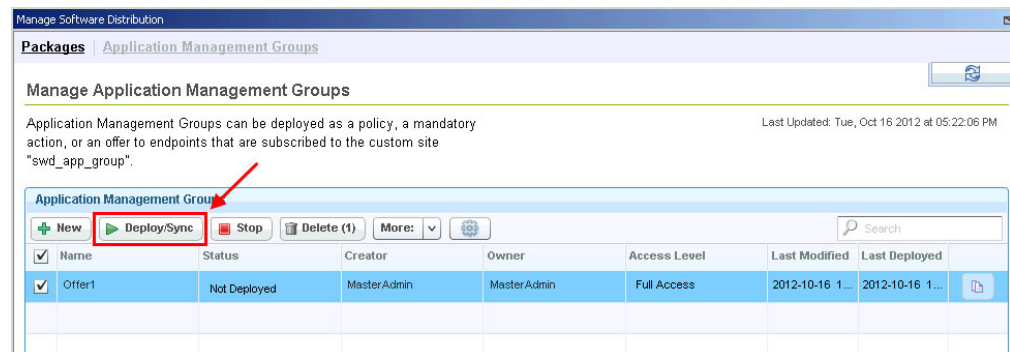


Figure 47. Deploy an Application Management Group

You might be prompted to enter your Endpoint Manager credentials twice, first for the creation of the Fixlets, and second for the creation of the computer group.

Set the advanced options to force the program to space out the running of actions. This can help reduce the load on the network in bandwidth-intensive actions such as large downloads. It is especially useful for allowing Relays to effectively service hundreds of attached Clients. This option is mainly for mandatory and policy actions.

Each computer can have a different start time.

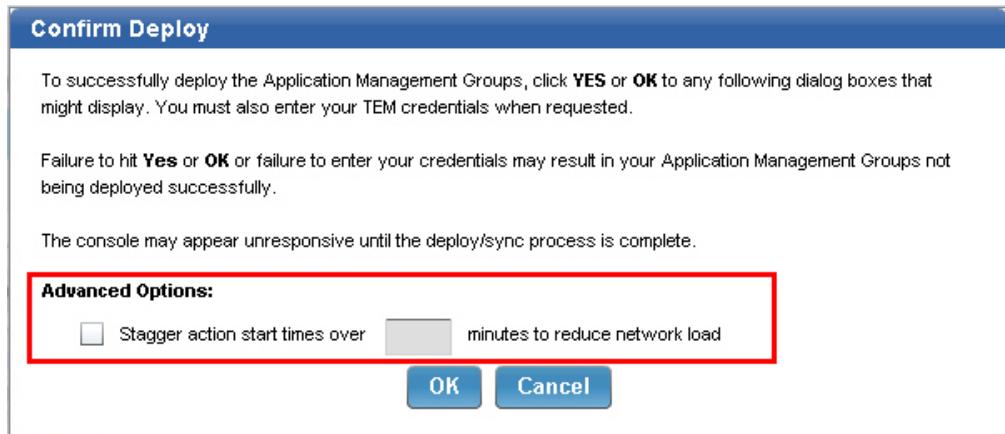


Figure 48. Stagger action

When the Application Management Group is deployed, the status changes to Deployed.

You can continue to add new tasks or targets to a deployed Application Management Group. However, the status changes from "Deployment" to "Out of Sync" because the Application Management Group does not get automatically updated with the new tasks or targets.

## Out of Sync state

If an Application Management Group was deployed before the addition or removal of a task or target, the Application Management Group becomes out of sync.



| Application Management Groups  |        |   |             |              |               |                 |   |
|--|--------|---|-------------|--------------|---------------|-----------------|---|
| <span>New</span> <span>Deploy/Sync</span> <span>Stop</span> <span>Delete (1)</span> <span>More: v</span> <span>Search</span> |        |   |             |              |               |                 |   |
| Name   | Status | Creator   | Owner       | Access Level | Last Modified | Last Deployed   |   |
| <input checked="" type="checkbox"/>  | Offer1 | Out of Sync  | MasterAdmin | MasterAdmin  | Full Access   | 2012-10-16 1... | 2012-10-16 1...  |

Figure 49. Out of Sync state

You must deploy the Application Management Group to put it back to a synchronized state.

Click the yellow icon to view the last deployed model.



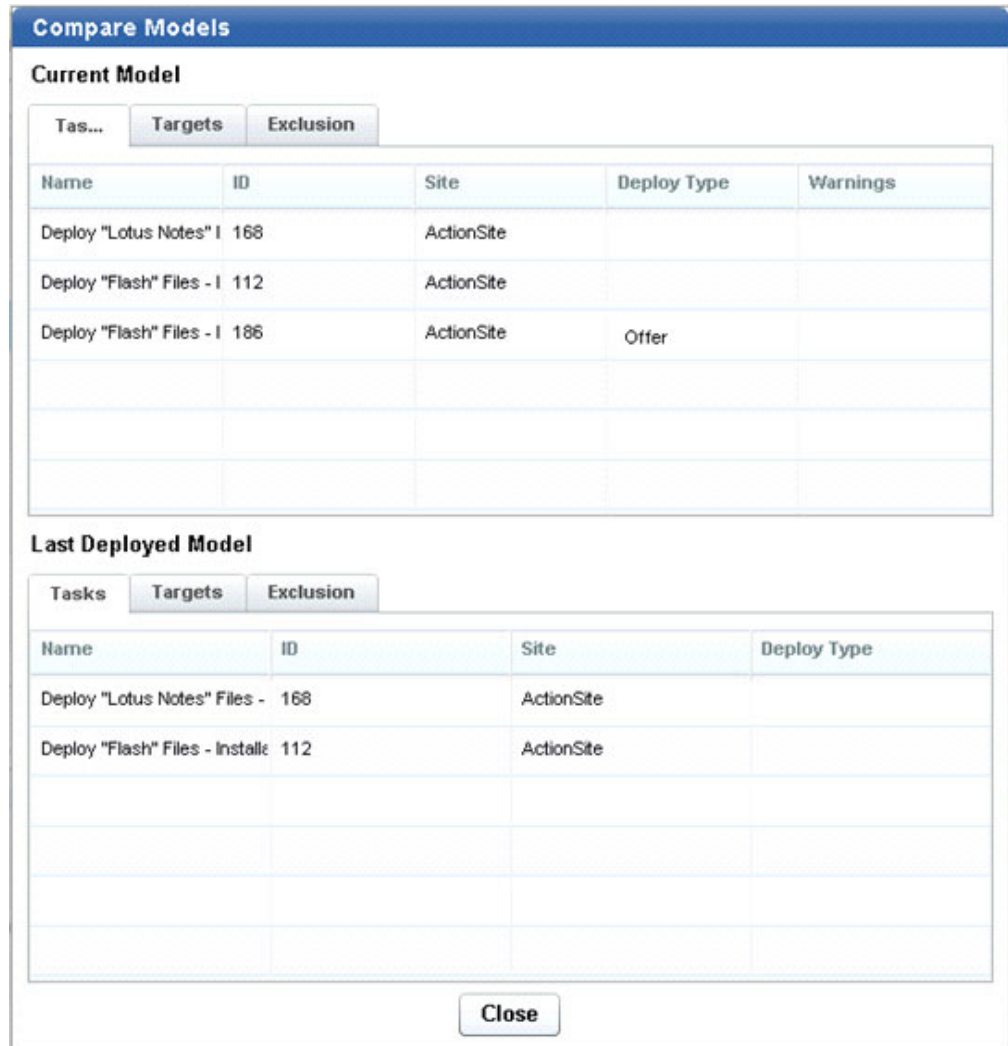


Figure 50. Compare Models dialog

## Orphaned owners

When a local operator is converted to an LDAP operator, the association between the operator name and shared packages and Application Management Groups of that local operator remains. However, that local operator no longer exists. Master operators must transfer resources of orphaned owners to an owner that exists.

### Transferring resources to the corresponding LDAP operator

You can associate a resource of a converted local operator to its corresponding LDAP operator.

All the Application Management Groups of an orphaned owner must be stopped for the transfer process to complete.

1. From the Manage Software Distribution dashboard, you are prompted to select a new owner to replace the orphaned owner.

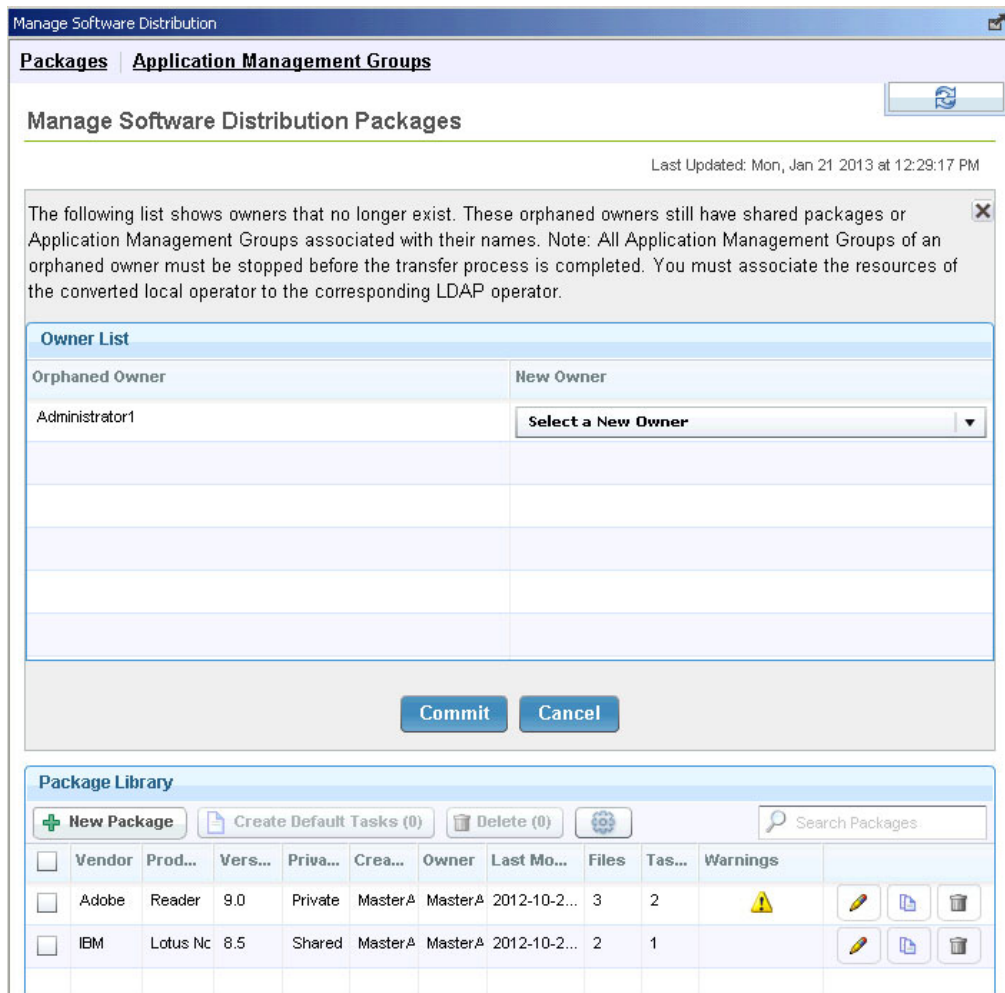


Figure 51. Transferring orphaned owners

2. Select the correct LDAP operator from the drop-down list.
3. Click **Commit**.

The resources that used to belong to the orphaned owner now belongs to its corresponding LDAP operator. All console permissions remain the same for the new operator.

## Transferring resources to a different operator

You can associate a resource of a converted local operator to a different operator instead of the corresponding LDAP operator.

You must ensure that the new operator has the correct permissions to view and edit the tasks that are referenced by the software package or Application Management Group before initiating the transfer of ownership. Otherwise, the Tasks in the Package or Application Management Group might not correctly transfer over to the new operator.

All the Application Management Groups of an orphaned owner must be stopped for the transfer process to complete.

1. From the Manage Software Distribution dashboard, you are prompted to select a new owner to replace the orphaned owner.

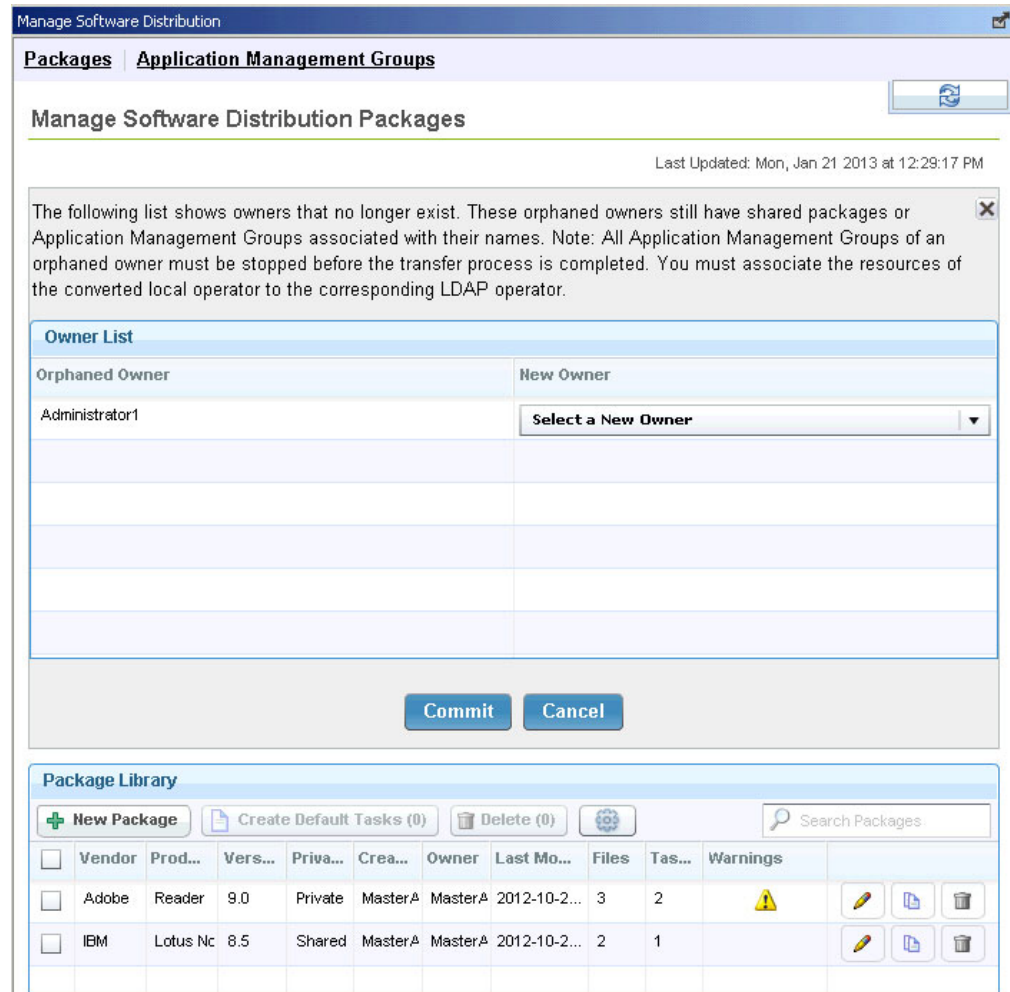


Figure 52. Transferring orphaned owners

2. Select a new owner instead of the corresponding LDAP operator from the drop-down list.
3. Click **Commit**.

The resources that used to belong to the orphaned owner now belongs to a new operator.

## Software Distribution Self Service Portal overview

The Software Distribution Self Service Portal is a web-based software portal for user self-provisioning. The Self Service Portal supports endpoints that are on Windows, AIX, and Solaris.

Software can be made available to endpoint users from the Self Service Portal by adding *Portal Offer* tasks to an Application Management Group. For more information, see “Adding tasks to an Application Management Group” on page 31.

Computer registration is required to enable endpoint users to view the software that was made available to a computer. A software can be in the following state: available, pending, successful, or failed. For more information, see “Software installation status” on page 57

From the web portal, endpoint users can select any of the available software and remotely install it on the registered computers.

**Note:** When an endpoint user logs in to the Self Service Portal, the software offer list does not change until the user logs out of the portal. If the console operator updated the Application Management Group after the user logs in to the portal, the change takes effect only after the user logs out and logs in again.

The following table displays a typical Self Service Portal workflow.

*Table 2. Self Service Portal workflow*

| <b>Task</b>  | <b>Person responsible</b> | <b>For more information</b>  |
|--|---------------------------|--|
| Add portal offer tasks to an Application Management Group.                     | Console operator          | See “Adding tasks to an Application Management Group” on page 31.  |
| Set up and configure the software distribution self service portal components. | Console operator          | See “Configuring the Software Distribution Self Service Portal” on page 47.  |
| Generate a PIN for each computer.  | Console operator          | See “Generating a PIN for each computer” on page 51.   |
| Block certain computers from being registered.                                 | Console operator          | See “Blocking computers from registration” on page 53.   |
| Access the Self Service Portal.  | Endpoint user             | See “Accessing the Software Distribution Self Service Portal” on page 54.  |
| Register computers to users.   | Endpoint user             | See “Registering computers through the Self Service Portal” on page 55.<br><br><b>Note:</b> If endpoint users are unable to complete self-registration, console operators can register the computers for the users from the Self Service Portal Registration Management dashboard. However, this option is not encouraged. For more information, see “Registering computers through the Self Service Portal Registration Management dashboard” on page 52. |
| Install software from the Self Service Portal.                                 | Endpoint user             | See “Installing software from the Self Service Portal” on page 57.   |
| View the software installation history page.                                   | Endpoint user             | See “Viewing installation history” on page 58.   |
| Uninstall the Self Service Portal.   | Console operator          | See “Uninstalling the Self Service Portal” on page 60.   |
| Troubleshoot.  | Console operator          | See Appendix B, “Frequently asked questions,” on page 71.  |

## Configuring the Software Distribution Self Service Portal

Console operators can use the Software Distribution Self Service Portal Setup and Configuration wizard to install the components that are required for the portal.

Ensure that you meet the following criteria:

- You must set up an LDAP server.
- You must have at least the IBM Endpoint Manager version 9.0.0 or later installed.

The Software Distribution Self Service Portal Setup and Configuration wizard provides an easy, step-by-step guided process to configure the required components. This wizard checks and notifies you of the status of each of the required steps.

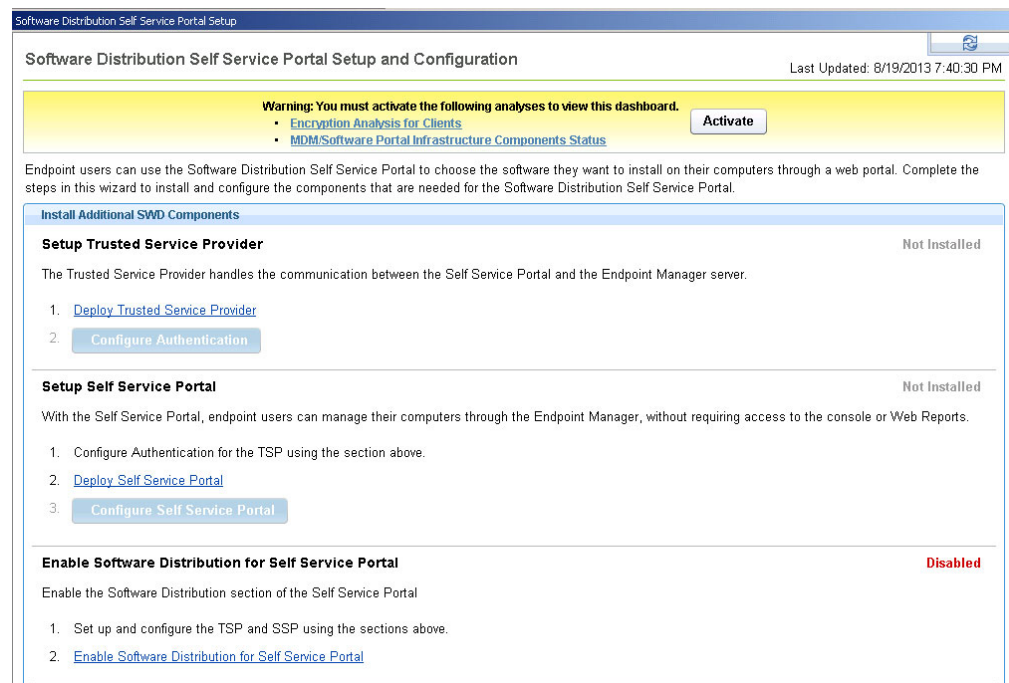


Figure 53. Software Distribution Self Service Portal Setup and Configuration wizard

These steps do not apply to multi-tenant environments or where more than one Self Service Portal or Trusted Service Provider are deployed. Such cases require manual configuration of the components. For more information about multitenancy setup, search for *Multitenancy* in the IBM Endpoint Manager wiki at [https://www.ibm.com/developerworks/community/wikis/home?lang=en#/wiki/Tivoli Endpoint Manager/page/Home](https://www.ibm.com/developerworks/community/wikis/home?lang=en#/wiki/Tivoli%20Endpoint%20Manager/page/Home).

**Note:** If you already configured the Trusted Service Provider and the Self Service Portal, skip this task and complete the following actions:

- Run the appropriate upgrade Fixlets.
- Run the **Enable Software Distribution for Self Service Portal** task.
  1. From the Systems Lifecycle domain, click **Software Distribution > Setup > Software Distribution Self Service Portal Setup**.
  2. Click **Activate** to activate the necessary analyses to view the dashboard.

3. Deploy and configure the Trusted Service Provider, if you have not already done so. The Trusted Service Provider manages the communication between the IBM Endpoint Manager server and an external LDAP server.

**Note:** If you already configured the Trusted Service Provider, skip the following steps and just run the appropriate upgrade Fixlets.

- a. Click **Deploy Trusted Service Provider** to run the Fixlet that is used to install the Software Distribution Trusted Service Provider.

**Note:** The Trusted Service Provider must be installed on a computer that can access the LDAP server and can be accessed from the Self Service Portal.

- b. Click **Configure Authentication** to direct the Trusted Service Provider to your external LDAP server and to set your credentials. The Configure Authentication dialog displays.

Figure 54. Configure Authentication dialog

- c. Enter the LDAP server information. This information is provided by your LDAP administrator.

**Note:** You can choose the LDAP login attribute that the endpoint users use to log in to the Self Service Portal. For example, it can be an email address or a user ID.

- d. Click **Test Settings** to check that you can communicate with your LDAP server.

- e. Enter the host name of the Trusted Service Provider. The host name is pre-populated and does not need to be changed in most circumstances.
  - f. Click **Configure Authentication** to create and run the action.
4. Deploy and set up the Self Service Portal to communicate with the Trusted Service Provider, if you have not already done so.

**Note:** If you already configured the Self Service Portal, skip the following steps and just run the appropriate upgrade Fixlets.

- a. Click **Deploy Self Service Portal** to install the portal.
- b. Click **Configure Self Service Portal**. The Configure Self Service Portal dialog displays.

**Configure Self Service Portal**

The Self Service portal allows end users to manage their own mobile devices and requires that it be configured to communicate with the Trusted Service Provider in order to do this.

**Configure Web Reports Access**

Web Reports URL:

Web Reports User:

Web Reports Password:

**Configure IEM Operator Credentials**

IEM Console Operator:

IEM Console Password:

**SSL Settings**

This SSP was installed with the Enrollment Extender. The SSP will share the Enrollment Extender's SSL certificates, so no new certificates need to be set.

\*Note this will create two separate Actions.

Figure 55. Configure Self Service Portal dialog

- c. Enter the information to access the web reports.
- d. Enter the credentials for the console operator.
- e. Configure the SSL settings, if necessary.
- f. Click **Configure SSP** to create and run the action.

**Note:** Configuring the Self Service Portal creates two actions in the console. Ensure that both actions complete before you proceed. These actions can take several minutes to complete.

When you have successfully configured the Self Service Portal, the URL to access the portal displays in the dashboard.

## Setup Self Service Portal

OK

With the Self Service Portal, endpoint users can manage their computers through the Endpoint Manager, without requiring access to the console or Web Reports.

1. Configure Authentication for the TSP using the section above. ✓
2. [Deploy Self Service Portal](#) ✓
3. [Configure Self Service Portal](#) ✓

You have successfully configured the Self Service Portal. Go to <https://karen-w2k8a/ssp> to use the Self Service Portal

Figure 56. Self service portal URL

5. Click **Enable Software Distribution for Self Service Portal**, if you have not already done so.

The wizard shows that you completed all the required steps as shown in the following screen capture:

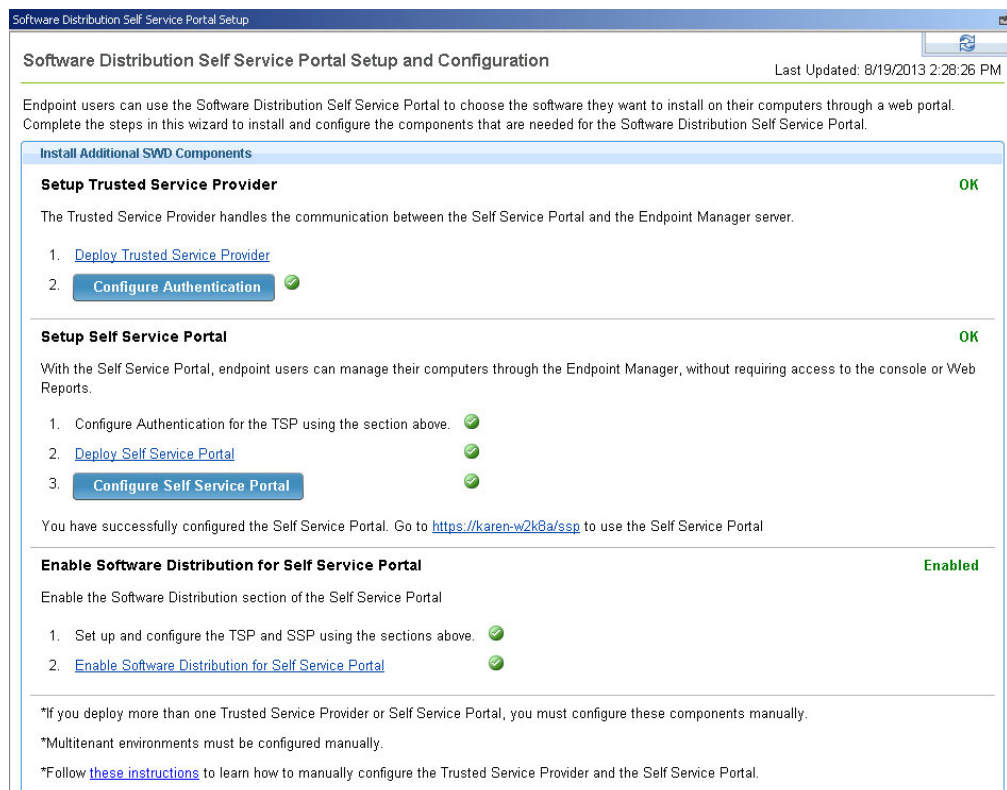


Figure 57. Successfully installed and configured the software distribution Self Service Portal.

Configuration files for the Trusted Service Provider and the Self Service Portal are created in the folder `path_to_TEM_Server_directory\MDM Provider\config`. The default path is `C:\Program Files\BigFix Enterprise\Management Extender\MDM Provider\config`.

Use Trusted Service Provider and Self Service Portal diagnostic pages and configuration files to ensure that these components were successfully configured.

### For the Trusted Service Provider

- Use the Trusted Service Provider diagnostics page to check if the Trusted Service Provider was successfully configured.



This page examines SSL certificates, and attempts to connect to the LDAP and to the IBM Endpoint Manager. It also attempts to perform a sample relevance query.

The URL syntax for the Trusted Service Provider diagnostic page is as follows: `https://<your_host_name>/diagnostics`

- Check the configuration file.
  1. Open the **tsp-config.yaml** file, which can be found in `path_to_TEM_Server_directory\MDM Provider\config`. The default path is `C:\Program Files\BigFix Enterprise\Management Extender\MDM Provider\config`.
  2. Reconfigure the Trusted Service Provider if any one of the following fields is missing:
    - `:organization_name:`
    - `:hostname:`
    - `:ldap_admin_user:`
    - `:ldap_admin_pass:`
    - `:wr_path:`
    - `:wr_user:`
    - `:wr_pass:`
    - `:tem_user:`
    - `:tem_pass:`
    - `:tem_server:`

#### For the Self Service Portal

- Use the Self Service Portal diagnostics page to check if the Self Service Portal was successfully configured.

This page examines the connection to the Trusted Services Provider, which is required for authenticated enrollment.

The URL syntax for the Self Service Portal diagnostic page is as follows: `https://<your_host_name>/ssp/diagnostics`

- Check the configuration file.
  1. Open the **ssp-config.yaml** file, which can be found in `path_to_TEM_Server_directory\MDM Provider\config`. The default path is `C:\Program Files\BigFix Enterprise\Management Extender\MDM Provider\config`.
  2. Reconfigure the Self Service Portal if any one of the following fields is missing:
    - `:install_mode:`
    - `:organization_name:`
    - `:tsp_host:`
    - `:tsp_port:`
    - `:hostname:`

## Generating a PIN for each computer

Console operators must generate a unique personal identification number (PIN) that is used to identify each computer for Self Service Portal registration.

- To generate a web portal registration PIN for each Windows and Mac computer, complete the following steps:

1. From the Systems Lifecycle domain, click **Software Distribution > Setup > Configure Client Dashboard**.
2. Deploy **Fixlet 14: Enable Client Dashboard for Software Offers and Generate a PIN for Self Service Portal Registration (Windows, Mac)**.
3. If you already enabled the client dashboard before, ensure that it is up-to-date by deploying **Fixlet 16: Update Client Dashboard for Software Offers and Generate a PIN for Self Service Portal Registration (Windows, Mac)**.

**Note:** The PIN is displayed in the client dashboard. However, if you want to generate a PIN for a Windows and Mac computer without showing the client dashboard, deploy only **Fixlet 20: Generate a PIN for Self Service Portal Registration**.

- To generate a web portal registration PIN for each Linux computer, deploy **Fixlet 20: Generate a PIN for Self Service Portal Registration**.

#### Windows computers

The PIN is displayed in the **Available Software** tab of the client dashboard, which is also known as the Endpoint Manager Support Center.

**Note:** Earlier versions of the client dashboard do not display the PIN. You can locate the PIN at `HKEY_LOCAL_MACHINE\SOFTWARE\BigFix\EnterpriseClient\SSP_PIN`.

#### Mac, Linux, AIX, and Solaris computers

You can locate the PIN at `/var/opt/BESClient/SSP_PIN`.

## Registering computers through the Self Service Portal Registration Management dashboard

Endpoint users must register their own computers through the Self Service Portal. If necessary, console operators can register computers for endpoint users by using the Self Service Portal Registration Management dashboard.

Use this task if you are a console operator and need to register computers for the Self Service Portal.

You can add computers or users to the registration list by using the Self Service Portal Registration Management dashboard. For more information about the dashboard, see “Self Service Portal Registration Management dashboard” on page 9.

1. From the Systems Lifecycle domain, click **Software Distribution > Self Service Portal Registration Management**.
2. You can register computers either by adding users to the listed computers or by adding computers to the listed users.

#### To register a computer to a user:

- a. Click the **List by Users** tab.
- b. Click the corresponding computers link from the Registered column.
- c. Select the computer name from the down-down list.
- d. Click **Register Computer**.

#### To register a user to a computer:

- a. Click the **List by Computers** tab.
- b. Click the corresponding users link from the Registered column.

- c. Enter the user name of the endpoint user that you want to add to the computer.
  - d. Click **Register User**.
3. Click **OK** to confirm.

The action might take a few minutes to complete. The dashboard shows the updates only when the action is complete. When the action completes, the computer or user that you added is shown in the dashboard.

**Note:** You can remove computers or users from the registration list by clicking a corresponding link from the Registered column, and then clicking **Remove Computer** or **Remove User**.

Registration information is stored in the following locations:

**Windows computers**

HKEY\_LOCAL\_MACHINE\SOFTWARE\BigFix\EnterpriseClient\SSP\_Green

**Mac and Linux computers**

/var/opt/BESClient/SSP\_Green

## Blocking computers from registration

Console operators can use the Self Service Portal Registration Management dashboard to prevent users from registering computers in the Self Service Portal. Use this procedure if you are a console operator and want to block a user from registering a computer in the Self Service Portal.

Use the Self Service Portal Registration Management dashboard to add either computers or users to the blocked list. For more information about the dashboard, see “Self Service Portal Registration Management dashboard” on page 9.

1. From the Systems Lifecycle domain, click **Software Distribution > Self Service Portal Registration Management**.
2. You can block computers either by adding users to the listed computers or by adding computers to the listed users.

**To block a computer from being added to a user:**

- a. Click the **List by Users** tab.
- b. Click the corresponding computers link from the Blocked column.
- c. Select the computer name from the down-down list.
- d. Click **Block Computer**.

**To block a user from being added to a computer:**

- a. Click the **List by Computers** tab.
  - b. Click the corresponding users link from the Blocked column.
  - c. Enter the user name of the endpoint user that you want to add to the computer.
  - d. Click **Block User**.
3. Click **OK** to confirm.

The action might take a few minutes to complete. The dashboard shows the updates only when the action is complete. When the action completes, the computer or user that you added is shown in the dashboard.

**Note:** You can also remove computers or users from the blocked list by clicking a corresponding link from the Blocked column, and then clicking **Remove Computer** or **Remove User**.

Information about blocked users and computers are stored in the following locations:

**Windows computers**

HKEY\_LOCAL\_MACHINE\SOFTWARE\BigFix\EnterpriseClient\SSP\_Red

**Mac and Linux computers**

/var/opt/BESClient/SSP\_Red

## Accessing the Software Distribution Self Service Portal

Endpoint users can access the Software Distribution Self Service Portal by using any web browser.

Obtain the URL of the Self Service Portal from your administrator. This web address is determined by your administrator and is different for every deployment.

1. From your web browser, enter the appropriate URL. The syntax of the URL is as follows: `https://<ssphostname>:<port>/ssp`.
2. Log in to the self service portal. By default, the email address and password that are specified in your LDAP account are used.

**Note:** The console operator can specify the login attribute during the configuration of the Trusted Service Provider. The login attribute can be the user name or any other field available in LDAP.

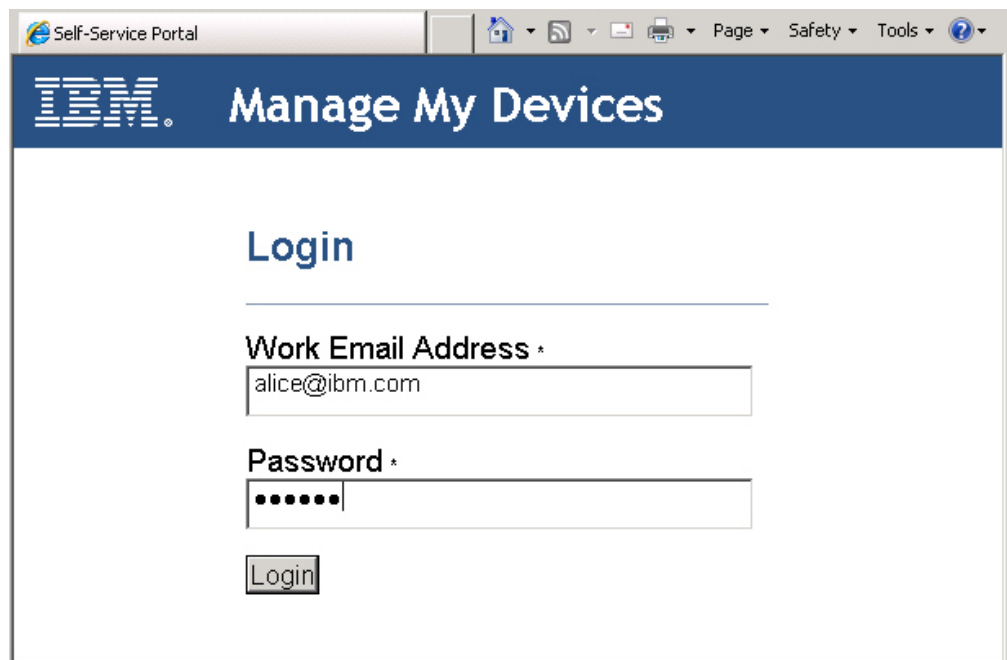


Figure 58. Self service portal login page

**Note:** When you are logged in to the Self Service Portal, changes made to the Application Management Group by your administrator do not immediately take effect. You can see the changes in your next login session.

You can add a computer or install software on one of the registered computers. For more information, see the following topics:

- “Registering computers through the Self Service Portal”
- “Installing software from the Self Service Portal” on page 57

## Registering computers through the Self Service Portal

Endpoint users must register computers to themselves from the Self Service Portal by using a personal identification number (PIN). Use this procedure if you are an endpoint user and want to register a computer to your account from the Self Service Portal.

Ensure that you have the latest version of the client dashboard.

1. Log in to the Self Service Portal. For more information, see “Accessing the Software Distribution Self Service Portal” on page 54.
2. If you enabled the Mobile Device Management Self Service Portal, click **Available Software** tab.
3. Click **Add a Computer** or the computer icon.

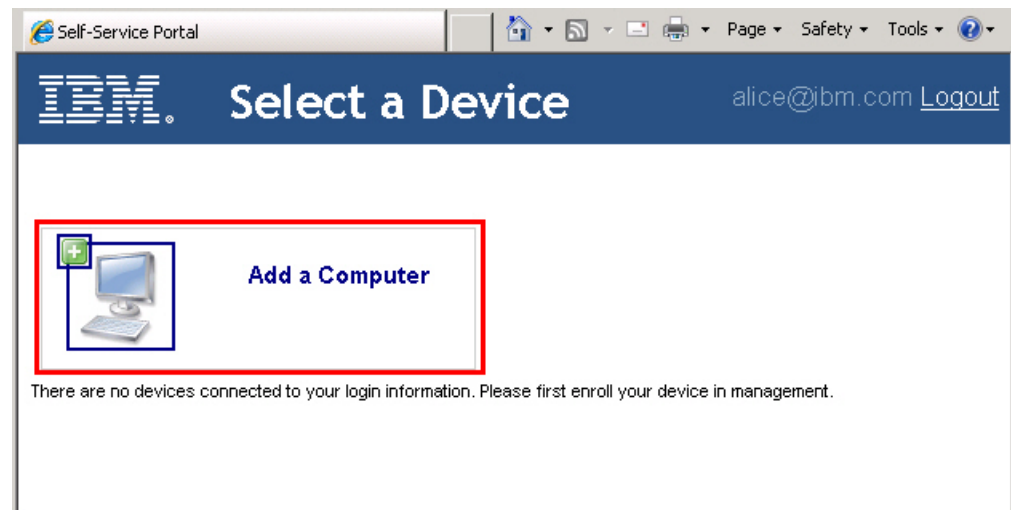


Figure 59. Add a computer

4. Locate the PIN of the computer that you want to register.

### Windows computers

You can view the PIN from the bottom of the **Available Software** tab of the client dashboard.

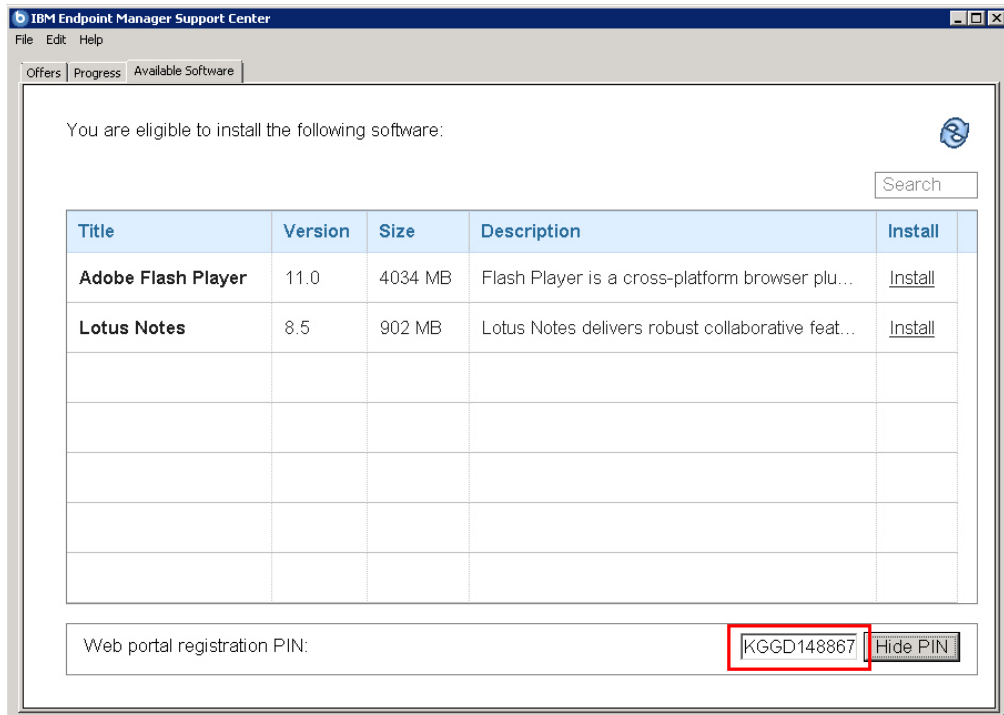


Figure 60. Web portal registration PIN in the Client Dashboard for Software

The client dashboard is also known as the Endpoint Manager Support Center. For more information about this dashboard, see “Client Dashboard for Software Offers” on page 11.

Earlier versions of the client dashboard do not display the PIN. You can locate it at HKEY\_LOCAL\_MACHINE\SOFTWARE\BigFix\EnterpriseClient\SSP\_PIN.

### Mac and Linux computers

You can locate the PIN at /var/opt/BESClient/SSP\_PIN.

**Note:** If you cannot locate your PIN, contact your IT administrator.

5. Enter the PIN in the Self Service Portal.

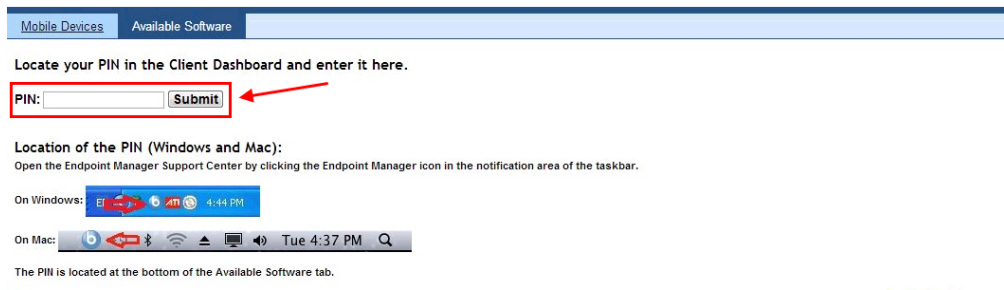


Figure 61. Enter the PIN

When the computer registration is complete, the computer is added in the Self Service Portal.

The endpoint user can view and select the available software to install on the registered computer. For more information, see “Installing software from the Self Service Portal.”

## Software installation status

The Self Service Portal shows the status of each software installation.

You can view the software status from either of the following pages:

### Software offer list page

It shows the most recent status of the software.

### History page

It shows the status of all attempted software installations made for a particular computer.

The software offer list and history views show the status of the software installation. The status can be one of the following values:

#### Available

The software shows this status if the user never deployed the software before.

#### Pending

The software shows this status immediately after the user clicks **Install**.

#### Success

The software shows this status if the software installation succeeded the last time that the user installed it.

**Fail** The software shows this status if the software installation failed the last time that the user installed it.

The software installation can fail for different reasons:

- When the associated task in the IBM Endpoint Manager console to install the software evaluates to fail.
- When the associated task in the IBM Endpoint Manager console expires before evaluating to success.
- When the associated task is deleted from a package after it is deployed in an Application Management Group.
- When the Self Service Portal cannot contact the IBM Endpoint Manager server to issue the task to install the software. In this case, no task is created in the IBM Endpoint Manager console.

**Note:** Previously installed software is still shown in the software offer list with the following status: "pending", "success", or "fail". The reason for retaining the software in the offer list is to provide the endpoint users with the option for reinstalling the software.

## Installing software from the Self Service Portal

Use this procedure if you are an endpoint user and want to install software on your computers from the Self Service Portal.

- Ensure that you registered your computers for the Self Service Portal. See “Registering computers through the Self Service Portal” on page 55.
- Familiarize yourself with the different software installation statuses. See “Software installation status.”

1. Log in to the Self Service Portal. For more information, see “Accessing the Software Distribution Self Service Portal” on page 54.
2. If you enabled the Mobile Device Management Self Service Portal, click **Available Software** tab.
3. Click a computer to view the available software for that computer.

**Note:** Previously installed software is still shown in the list with the following status: "pending", "success", or "fail". The reason for retaining the software in the offer list is to provide you with the option for reinstallation.

4. Select the available software that you want to install.

**Note:** The list of software might not contain the changes that are made by your administrator during your current login session. You can see the changes only after you log out and log in again.

5. Click **Install**.

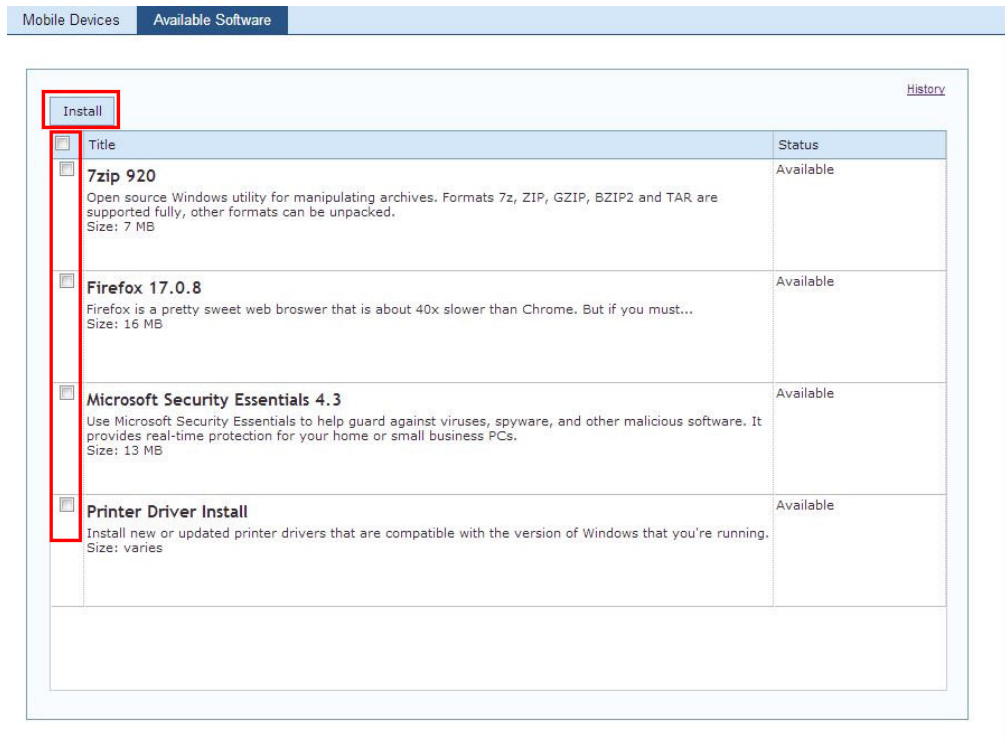


Figure 62. Install available software

The status of the software immediately changes from "Available" to "Pending" while the software is being installed to the selected computer.

## Viewing installation history

Each registered computer has a history view that shows a record for each attempted software that is requested through the Self Service Portal. Use this procedure if you are an endpoint user and want to view the installation history of a registered computer from the Self Service Portal.

The history view of a computer shows the status of each attempted software installation. For more information about the possible status, see “Software installation status” on page 57.



1. Log in to the Self Service Portal. For more information, see “Accessing the Software Distribution Self Service Portal” on page 54.
2. If you enabled the Mobile Device Management Self Service Portal, click **Available Software** tab.
3. Click the computer whose installation history you want to view. You can see all the software that is available to that computer.
4. Click **History**.

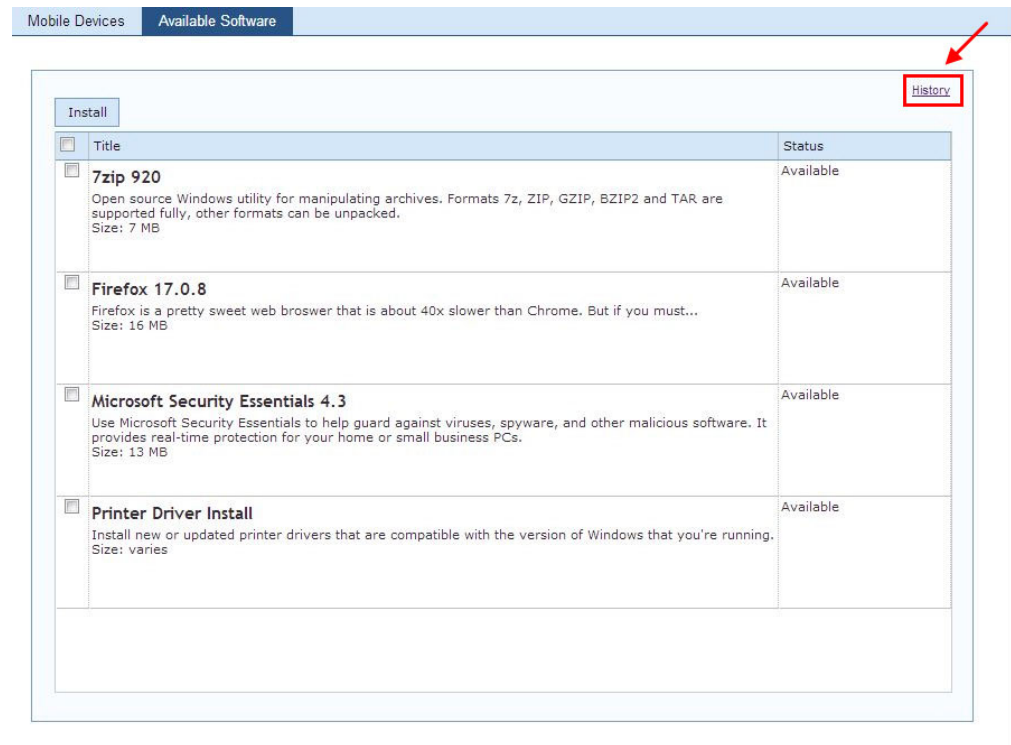


Figure 63. History link

The History view of all attempted software installations for the selected computer is displayed as shown in the following image.

[Back](#)

| Title          | Status  | Created                   |
|----------------|---------|---------------------------|
| 7zip 920       | Success | 2013-08-21 16:13:49 -0700 |
| 7zip 920       | Success | 2013-08-21 16:10:04 -0700 |
| Firefox 17.0.8 | Success | 2013-08-21 15:50:06 -0700 |
| 7zip 920       | Success | 2013-08-21 15:50:06 -0700 |
| 7zip 920       | Success | 2013-08-21 15:31:44 -0700 |
| 7zip 920       | Success | 2013-08-21 13:56:42 -0700 |
| 7zip 920       | Success | 2013-08-21 13:11:19 -0700 |
| Firefox 17.0.8 | Success | 2013-08-21 13:10:44 -0700 |
| Firefox 17.0.8 | Success | 2013-08-21 13:10:23 -0700 |
| 7zip 920       | Success | 2013-08-21 13:07:41 -0700 |
| 7zip 920       | Success | 2013-08-21 12:49:36 -0700 |
| 7zip 920       | Success | 2013-08-21 12:47:31 -0700 |
| Firefox 17.0.8 | Success | 2013-08-21 12:35:01 -0700 |
| 7zip 920       | Success | 2013-08-21 12:34:31 -0700 |
| 7zip 920       | Success | 2013-08-21 12:20:40 -0700 |
| Firefox 17.0.8 | Success | 2013-08-20 16:56:43 -0700 |
| Firefox 17.0.8 | Success | 2013-08-20 23:51:49 +0000 |
| 7zip 920       | Success | 2013-08-20 16:43:01 -0700 |

Figure 64. Transaction history

## Uninstalling the Self Service Portal

Unsubscribing to the Software Distribution site does not automatically uninstall the Self Service Portal.

- To uninstall the Software Distribution Self Service Portal, deploy the following Fixlets from the **Software Distribution** site. The Fixlet that you deploy depends on the uninstallation level that you want.

### Fixlet 201: Disable Software Distribution for Self Service Portal

Use this Fixlet to disable the Software Distribution component for the Self Service Portal.

### Fixlet 146: Remove Self Service Portal

Use this Fixlet to completely uninstall the Self Service Portal. When the portal is removed, users are no longer able to use the self service portal to view and manage their computers and mobile devices.

- To uninstall the Mobile Device Management Self Service Portal, deploy the following Fixlets from the **Mobile Device Management** site. The Fixlet that you deploy depends on the uninstallation level that you want.

### Fixlet 300: Disable Mobile Device Management for Self Service Portal

Use this Fixlet to disable the Mobile Device Management component for the Self Service Portal.

### Fixlet 146: Remove Self Service Portal for Mobile Device Management

Use this Fixlet to completely uninstall the Self Service Portal. When the portal is removed, users are no longer able to use the self service portal to view and manage their computers and mobile devices.

---

## Chapter 6. Microsoft Application Virtualization

Endpoint Manager for Software Distribution supports the distribution and management of Microsoft Application Virtualization (App-V) packages.

The App-V packages distribution and management support does not need a separate Microsoft System Center App-V Management Server for streaming and metering. The Microsoft App-V Sequencer creates a virtualized application that can be distributed by using Software Distribution.

To use your **App-V** site, go to the **License Overview** dashboard under the Endpoint Management domain in your console and enable the **Client Manager for Application Virtualization** site. Subscribe to this site any desktops that require an App-V client.

---

### Deploying App-V clients

Use the App-V Client Wizard from the IBM Endpoint Manager console to install and configure App-V clients.

With the App-V Client Wizard, you can specify and upload client installers for use. You can also set up and apply configuration templates as policies.

The following App-V clients and packages are supported:

- 4.5 SP1
- 4.5 SP2
- 4.6 Gold (32 and 64-bit)
- 4.6 SP1 (32 and 64-bit)
- 5.0 Gold (32 and 64-bit)

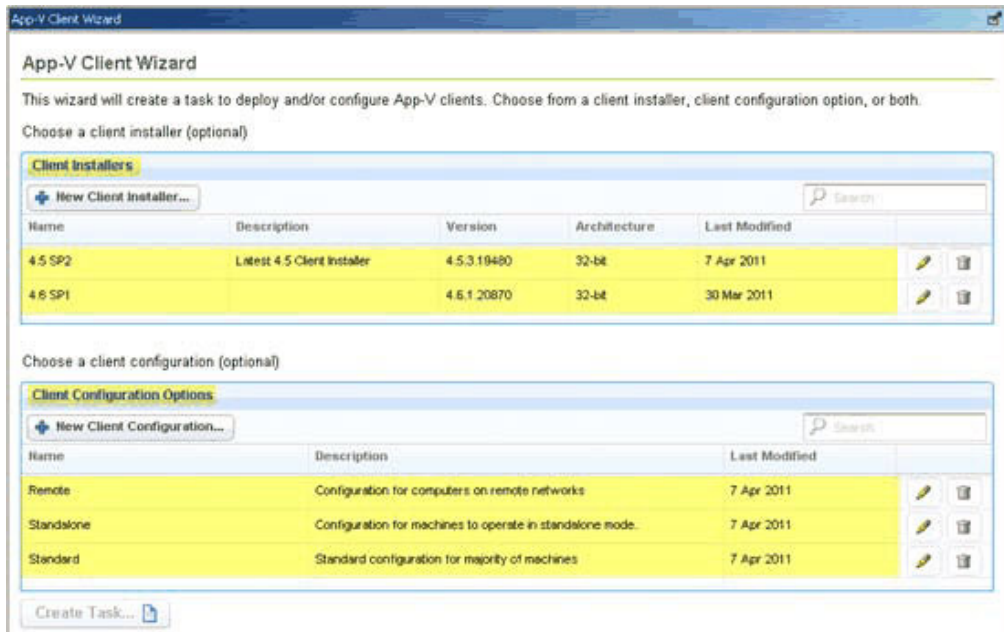


Figure 65. App-V Client Wizard

To create another deployment option, choose the **New Client Installer** option and specify the location of the App-V Client installer and information about the installer that is being uploaded.

You can edit previous installer entries by double-clicking the row or clicking **Edit** on the right side of the row. Click the **Trash** icon to delete the entry.

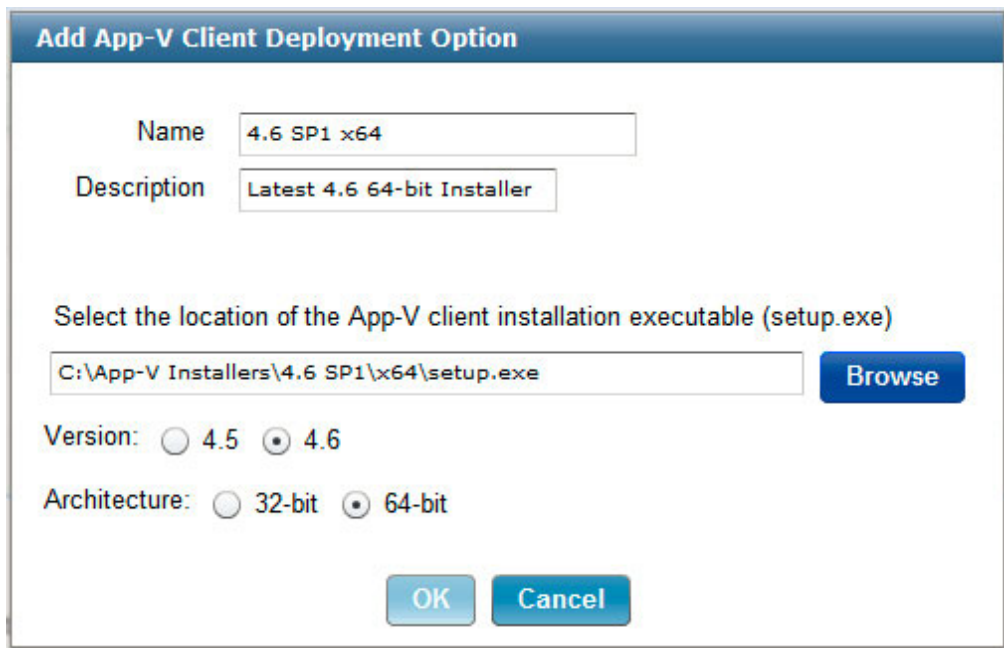


Figure 66. Add App-V Client Deployment Option

To create a configuration, choose **New Client Configuration** and choose all options to be set on the client. You can specify many settings for configuration, optional servers, and permissions for non-administrative users.

You can view previous configuration entries by double-clicking the row or clicking **Edit**.

**Add App-V Client Configuration Option**

Name

Description

Allow Independent File Streaming

Require Authorization If Cached

Allow Disconnected Operation

Limit disconnected operation to (days):

Work Offline

Configure Client to use App-V Server

Protocol  Path

**Permissions**

|  |   |
|--|---|
| <input type="checkbox"/> AddApp                | <input type="checkbox"/> ManageServers                |
| <input type="checkbox"/> ChangeCacheSize       | <input checked="" type="checkbox"/> ManageTypes       |
| <input type="checkbox"/> ChangeFSDrive         | <input checked="" type="checkbox"/> PublishShortcut   |
| <input type="checkbox"/> ChangeLogSettings     | <input checked="" type="checkbox"/> RefreshServer     |
| <input type="checkbox"/> ChangeRefreshSettings | <input checked="" type="checkbox"/> RepairApp         |
| <input checked="" type="checkbox"/> ClearApp   | <input checked="" type="checkbox"/> ToggleOfflineMode |
| <input type="checkbox"/> DeleteApp             | <input type="checkbox"/> UnloadApp                    |
| <input type="checkbox"/> ImportApp             | <input type="checkbox"/> UpdateOSDFile                |
| <input checked="" type="checkbox"/> LoadApp    | <input type="checkbox"/> ViewAllApplications          |
| <input checked="" type="checkbox"/> LockApp    |   |

Figure 67. Add App-V Client Configuration Option

**Note:** The App-V client must have the "AllowIndependentFileStreaming" setting enabled to run in stand-alone mode. You can configure this setting in the App-V Client Deployment Dashboard.

To create a task, select from these available client installers and configuration options:

- If you create a task by using a client installer, the new task installs only the client and leaves the configuration as the default.
- If you create a task by using a configuration, the new task changes the configuration on an existing deployed App-V client.
- If you create a task by using both the client installer and configuration, a task deploys and configures App-V.

When you select at least one item, you can create a task.

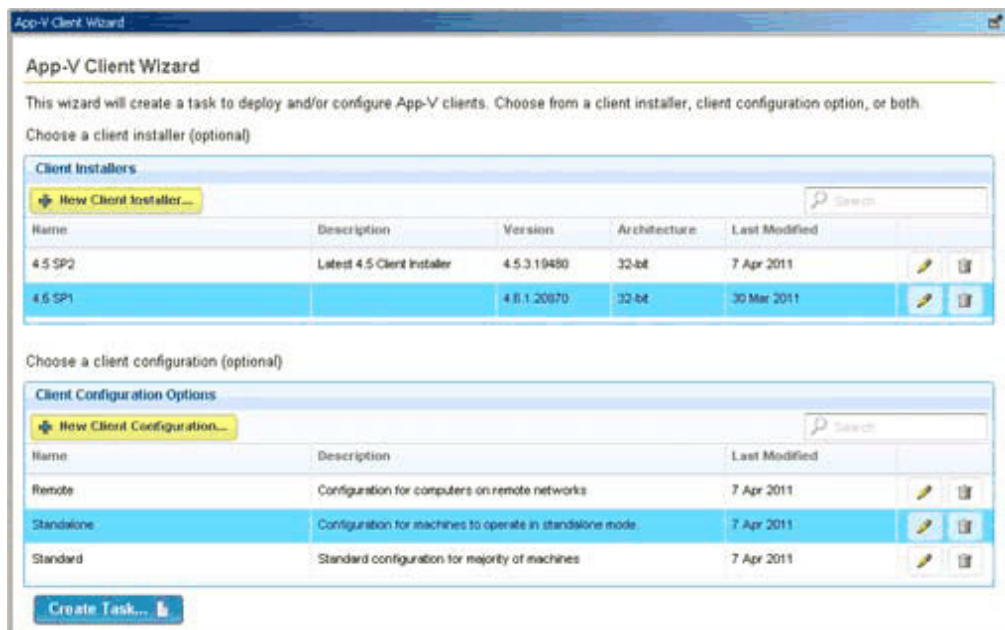


Figure 68. Creating a task from the App-V Client Wizard

Created tasks can be found in the Systems Lifecycle domain under the App-V Client Tasks subnode of the Software Distribution navigation tree.

You can also create tasks to uninstall the App-V client, or to restart the App-V client service due to a pending configuration change.

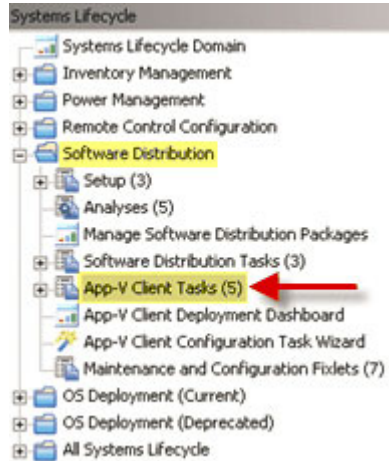


Figure 69. App-V Client Tasks navigation tree

## Viewing App-V client status

The App-V Client Deployment Dashboard displays a summary of App-V client deployments, including installed versions and configuration settings.

The configuration pie chart displays the top five configurations, grouping everything else in Other Configurations.

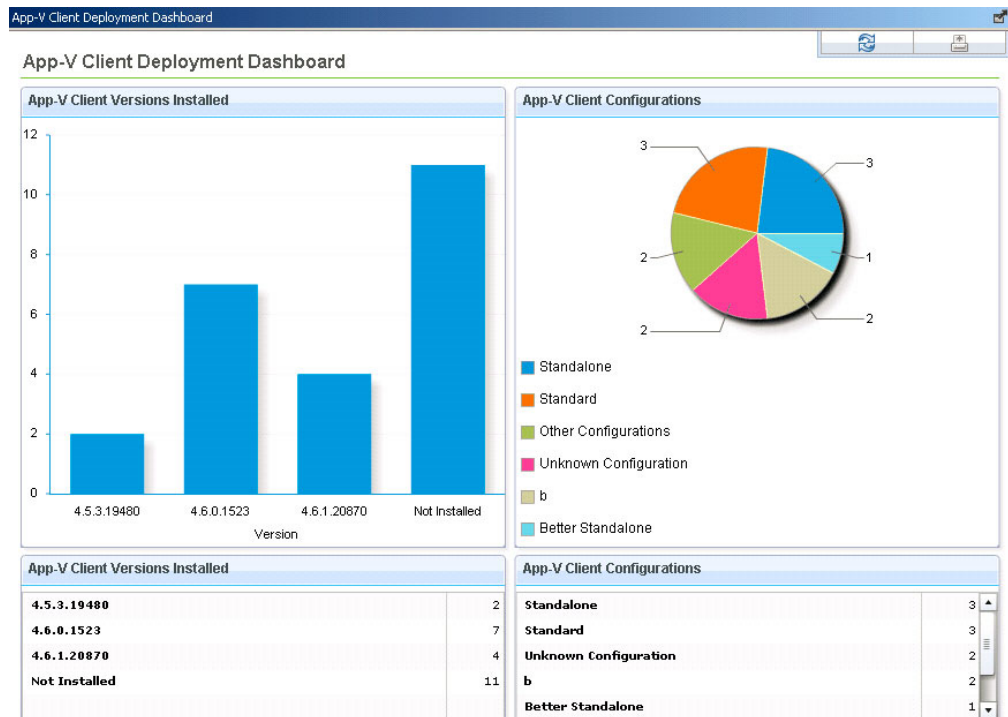


Figure 70. App-V Client Deployment Dashboard

Click a bar, pie slice, or entry in the tables to see a listing of those computers.

| Computer Name  | OS               | CPU           | Last Report Time      |
|----------------|------------------|---------------|-----------------------|
| WXP38EN-----01 | WinXP 5.1.2600   | 2400 MHz Xeon | 3/23/2011 10:35:46 AM |
| WXP26E-----09  | WinXP-2003 5...  | 2400 MHz Xeon | 3/3/2011 2:13:59 PM   |
| W0326EN-----04 | Win2003 5.2.3... | 2400 MHz Xeon | 3/1/2011 1:46:28 PM   |
| WXP38EN-----04 | WinXP 5.1.2600   | 2400 MHz Xeon | 2/28/2011 5:33:24 PM  |
| W0328EN-----08 | Win2003 5.2.3... | 2400 MHz Xeon | 2/28/2011 4:23:46 PM  |
| W0328EN-----07 | Win2003 5.2.3... | 2400 MHz Xeon | 2/28/2011 4:22:39 PM  |
| W0328EN-----05 | Win2003 5.2.3... | 2400 MHz Xeon | 2/28/2011 4:22:21 PM  |

Figure 71. Computers with App-V

## Deploying App-V packages

Deploy the App-V package in stand-alone mode to endpoints with the App-V client installed.

A complete App-V package includes the following files:

- An `.sft` file, which contains the data of the sequenced application.
- An `.osd` file for each application in the App-V package.
- A `manifest.xml` file, which contains information about the entire App-V package.
- Icon files used to display the application on the endpoint.

If these files are packaged together, the Software Distribution dashboard generates a default installation command to deploy the App-V package in stand-alone mode (without streaming servers) to endpoints with the App-V client installed.

The App-V Sequencer might also generate an `.msi` file. This file can be used to deploy and install the package with the Software Distribution dashboard if the following conditions are met:

- The MSI is accompanied by all other files in the App-V package, as previously described.
- The App-V client is already installed on the endpoint.
- The App-V client has the "AllowIndependentFileStreaming" setting enabled.
- If App-V runs in a stand-alone configuration (no streaming server), the App-V client has the "RequireAuthorizationIfCached" setting set to 0. Otherwise, the application installs, but fails when the App-V client fails to contact the streaming server.

These conditions are tested by the task relevance. However, you must build a package in stand-alone mode before it can be deployed.

## Viewing App-V application usage


The App-V Application Usage Report is a Web Report that displays information about how applications are used in your deployment.


The report can be found under the Systems Lifecycle category and then App-V Application Usage Report.





Choose a category to view reports:

 **Starred**  
My favorite reports

 **My Authored**  
Reports that I've created

 **Endpoint Protection**

 **Systems Lifecycle**

Figure 72. Web Reports

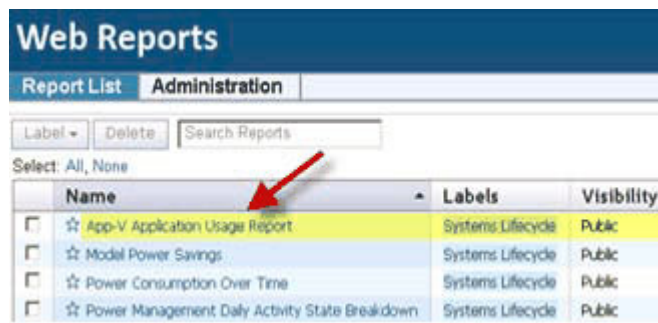


Figure 73. Report List

Within this report, you choose the last launch filtering criteria.

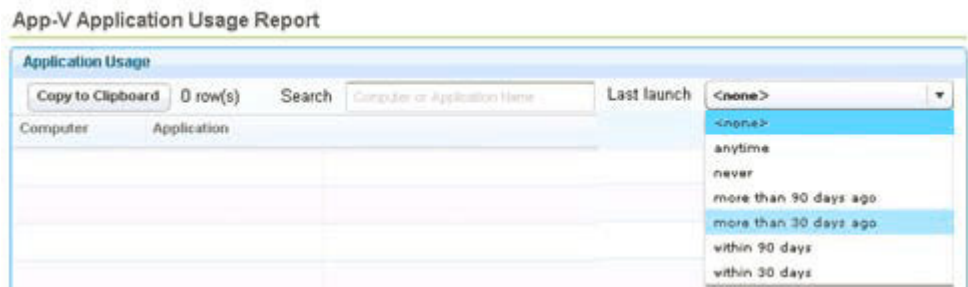


Figure 74. App-V Application Usage Report

Data is retrieved from the Web Reports server. You can search through the data by using the Search box. You can also copy data to the clipboard for importing into another program by using the “Copy to Clipboard” function.

**Note:** Web Reports performance can be degraded when the amount of data becomes large. To further filter data beyond “Last Launch” criteria, first use the

standard Web Reports filter dialog.

---

## Appendix A. Support

For more information about this product, see the following resources:

- [http://pic.dhe.ibm.com/infocenter/tivihelp/v26r1/topic/com.ibm.tem.doc\\_9.1/welcome/welcome.html](http://pic.dhe.ibm.com/infocenter/tivihelp/v26r1/topic/com.ibm.tem.doc_9.1/welcome/welcome.html)
- IBM Endpoint Manager Support site
- IBM Endpoint Manager wiki
- Knowledge Base
- Forums and Communities



---

## Appendix B. Frequently asked questions

This section is designed to help you better understand Endpoint Manager for Software Distribution through questions and answers.

### **What is the definition of a package?**

Packages are bundles of content and are the most important part of the software Distribution product. Packages contain a list of the files that are needed to install a specific software product. The list also includes the Fixlets that are needed to install the product on the actual endpoints. The Package establishes management relationships between files and Fixlets.

### **What is the definition of an Application Management Group?**

Application Management Groups are collections of tasks that can be organized into groups of content and delivered to targeted groups of client computers. These tasks are viewed by Endpoint Manager clients as offers.

### **What is the role of MSTs in Software Distribution?**

An MST, or Microsoft Transform file, is a subfile of an MSI, or Microsoft Installer file. Transform files are used to set or override installation options such as the product language, license key, or component selections. In the context of Software Distribution, you can use the Create Distribution Task wizard to automatically generate tasks for a package. The wizard creates a task for every MST included in a package. Each task contains a single .mst file.

**Note:** If you want to apply multiple .mst files in a single task, you must enter the installation command in the wizard.

**Note:** You can have different tasks apply different MSTs, but you can only apply one MST per Software Distribution task.

### **I created a Fixlet from the *Create Fixlet Wizard* – why does not it work?**

See the Fixlet Authoring support page on the Endpoint Manager support website for general Fixlet authoring support.

### **I created a Fixlet in Current User mode and deployed it to the endpoints. Why did it not get installed at the endpoints?**

The logged in user must have Administrator privileges to install the software.

### **Why do I need installation files in the root directory to create a Fixlet?**

See the Technote on structuring software distribution packages in the Endpoint Manager support website.

### **Can I find the list of packages that are installed on an endpoint?**

Because Endpoint Manager does not repackage the software in a new format, it uses vendor-specified tags, such as the package GUID. These attributes are already gathered in Endpoint Manager inventory for many common packaging systems. Alternatively, analyses can be used to identify attributes that indicate that a piece of software is installed. The Endpoint Manager SAM scanner is useful in this regard.

### **Are there any recommendations in creating packages?**

See the Technote on structuring software distribution packages in the Endpoint Manager support website.

**What are the currently supported file types?**

Endpoint Manager for Software Distribution can deploy any type of file. Auto-generation of package installation commands is supported for .exe, .msi, .bat, .dmg, .pkg, .rpm, .spb, and App-V files.

**If I have deployed a software, why is my computer still relevant to the package?**

The auto-generated Fixlet relevance is generalized to support common package characteristics. To further customize the applicability relevance of a Software deployment Fixlet, use the **Target using the following applicability conditions** option in either the Create Distribution Task dialog or Edit Distribution Task dialog.

**What should I do if my software package has setup.exe and .msi in it?**

This depends on the type of software that you are installing. Check with the specific software vendor for their recommendations.

**What is a “relative path”?**

The relative path concept can be used when you add files to a package. For example, an MSI transform file can be added to an existing package and placed into a subfolder by using this feature. Open actions that are based on this package must be re-created before they can take advantage of the new file. For more guidance, see the related Technote on the Endpoint Manager support website.

**How do I bundle multiple installations into a single package?**

This practice is not suggested. Instead, create individual Fixlets and use baselines to specify ordering. For more information, see the Best Practices section.

**Why are my SPB tasks not becoming relevant?**

To deploy SPB package types, you must first run the 'Deploy SIE' task from the *Client Manager for TCM* site on your endpoints. For more information about working with SPB package types, see the “Supported package types” on page 3 section.

**How do I know which actions are associated with the Manage Application Management Groups dashboard?**

Actions that are created with the Manage Application Management Groups dashboard have titles with the following format: SWD AMG Action: *title\_of\_the\_originating\_task*.

**When I deploy an Application Management Group, why do I get an error that tells me the computer group exists? What do I do?**

Deploying an Application Management Group creates an automatic computer group for that Application Management Group. During the stop process, you might receive a dialog request to delete the computer group. If you click cancel on this request, the group is not deleted. The next time that you attempt to deploy the Application Management Group, you will see an error that tells you that the computer group exists. To work around the error, delete the computer group and then deploy the Application Management Group again.

**What do I do if I get a different error when I attempt to deploy an Application Management Group?**

If you encounter a problem when you deploy an Application Management Group, complete the following steps:

1. Stop the Application Management Group to put it in a "Not Deployed" state.

2. Delete the corresponding computer group for that Application Management Group.
3. Deploy the Application Management Group again.

### **Why are my Application Management Group actions not showing in the Client Dashboard?**

If you encounter a problem with the Client Dashboard, complete the following steps:

1. Check that the client is subscribed to the Application Management Group custom site.
2. Check that the client is a member of at least one of the targets that are listed in the Application Management Group.
3. Check that there is an automatic computer group for that Application Management Group in the custom site. If it is not there, stop the Application Management Group and deploy again.
4. Check that the ID referenced by the action matches the ID of the corresponding computer group in the custom site. If the IDs do not match, do the following steps:
  - a. Stop the Application Management Group.
  - b. Delete the corresponding computer group in the custom site.
  - c. Deploy the Application Management Group again.
5. Check that the originating task is relevant on the client.

### **The Manage Software Distribution Packages dashboard reports that my files are still uploading, but the uploads cannot take this long. How do I debug this issue?**

1. Click **Refresh** from the dashboard to see if the uploading status goes away.
2. Check to see if the files are actually on the server. The files are stored on the Endpoint Manager server in *path\_to\_TEM\_server\_directory\wwwrootbes\Uploads\sha1\_of\_the\_file*. The default path is C:\Program Files\BigFix Enterprise\BES Server\wwwrootbes\Uploads\*sha1\_of\_the\_file*.

If the files are not there, check the disk space on the server and try uploading the files again.

If the files are there, check if the Upload Maintenance Service is running. The Upload Maintenance Service is responsible for detecting that the uploads have completed and is responsible for changing the file status from "Uploading" to "Complete". To verify that this service is running, complete the following steps:

- a. Open the Windows Task Manager.
- b. View the running processes. The Upload Maintenance Service is shown under processes as *uploadmaintenanceservice.exe*.
- c. If you do not see this process running, ensure that the **BES Plugin service** and the **Upload Maintenance Service** are installed. The installation tasks for these two services can be found in **Systems Lifecycle > Software Distribution > Setup > Install Server Tools**.

The Upload Maintenance Service log files are in *path\_to\_TEM\_server\_directory/Applications/Logs*. By default, the path is C:\Program Files\BigFix Enterprise\BES Server\Applications\Logs.

**I removed a computer group as a target from a deployed Application Management Group. Then, I resynchronized the Application Management Group. Why are the actions from this Application Management Group still relevant for computers from the removed computer group?**

During resynchronization, the existing automatic computer group for the Application Management Group is updated with the new listing of computer group targets. Occasionally, the client receives the action before its computer group information is updated. To avoid this issue, stop and redeploy the Application Management Group whenever a computer group is removed from a deployed Application Management Group.

**Where can I find the Manage Software Distribution dashboard debug log?**

Follow the steps to turn on the debug mode for the dashboard.

1. Click the Manage Software Distribution dashboard and press ALT+CTRL+SHIFT+D. The Debug Settings window opens.
2. Select the **Track function calls in Diagnostic Panel** check box.
3. In the Log Settings section, move the slider for **Levels to Include** to **Debug**.
4. Close the Debug Settings window.
5. Press Ctrl+F5 to reload the dashboard.
6. When the error message is displayed, press Alt+Ctrl+Shift+D again.
7. Click **View Dashboard Log**.

**I am seeing duplicate Application Management Groups-related actions for master operators. What do I do?**

Complete the following steps:

1. From the Manage Application Management Groups dashboard, click the **Settings** icon.
2. Click **Clear AMG Action Cache**.

**Note:** The cache must be cleared if a master operator deployed an Application Management Group before Software Distribution site version 35.

**How do I create an offer for the self service portal?**

To create an offer that becomes available in the self service portal, you must add a *Portal Offer* task to an Application Management Group.

**I deployed an Application Management Group that contained portal offers. Then, I stopped the deployment. Why are the software offers still showing in the Self Service Portal. Is this behavior expected?**

The list of software offers for a computer is generated once for each user login session. This session is considered as the time that a user is logged on to the portal. The software list does not update to incorporate changes in Application Management Group status until the user logs out and logs back in again.

**Where can I find the logs for the Self Service Portal and Trusted Service Provider?**

The Self Service Portal and Trusted Service Provider log files are in *path\_to\_TEM\_Server\_directory*\MDM Provider\log. The default path is C:\Program Files\BigFix Enterprise\Management Extender\MDM Provider\log.

**I changed my Trusted Service Provider password, and now the endpoint user cannot log in to the Self Service Portal. What do I do?**

Update the password in the **tsp-config.yaml** file, which can be found in



*path\_to\_TEM\_Server\_directory*\MDM Provider\config. The default path is C:\Program Files\BigFix Enterprise\Management Extender\MDM Provider\config.

### **I encountered an issue with the Self Service Portal. Where can I get the information for troubleshooting?**

Check **Analysis 19: Software Distribution Self Service Portal** to view information about the portal.

### **Is there a way to check if the Trusted Service Provider and the Self Service Portal were successfully configured?**

#### **For the Trusted Service Provider**

- Use the Trusted Service Provider diagnostics page to check if the Trusted Service Provider was successfully configured.

This page examines SSL certificates, and attempts to connect to the LDAP and to the IBM Endpoint Manager. It also attempts to perform a sample relevance query.

The URL syntax for the Trusted Service Provider diagnostic page is as follows: `https://<your_host_name>/diagnostics`

- Check the configuration file.
  1. Open the **tsp-config.yaml** file, which can be found in *path\_to\_TEM\_Server\_directory*\MDM Provider\config. The default path is C:\Program Files\BigFix Enterprise\Management Extender\MDM Provider\config.
  2. Reconfigure the Trusted Service Provider if any one of the following fields is missing:
    - :organization\_name:
    - :hostname:
    - :ldap\_admin\_user:
    - :ldap\_admin\_pass:
    - :wr\_path:
    - :wr\_user:
    - :wr\_pass:
    - :tem\_user:
    - :tem\_pass:
    - :tem\_server:

#### **For the Self Service Portal**

- Use the Self Service Portal diagnostics page to check if the Self Service Portal was successfully configured.

This page examines the connection to the Trusted Services Provider, which is required for authenticated enrollment.

The URL syntax for the Self Service Portal diagnostic page is as follows: `https://<your_host_name>/ssp/diagnostics`

- Check the configuration file.
  1. Open the **ssp-config.yaml** file, which can be found in *path\_to\_TEM\_Server\_directory*\MDM Provider\config. The default path is C:\Program Files\BigFix Enterprise\Management Extender\MDM Provider\config.
  2. Reconfigure the Self Service Portal if any one of the following fields is missing:

- :install\_mode:
- :organization\_name:
- :tsp\_host:
- :tsp\_port:
- :hostname:

### Where are the PIN and registration information stored?

The information can be found in the following registry keys.

- For Windows computers

#### PIN for Registration

HKEY\_LOCAL\_MACHINE\SOFTWARE\BigFix\EnterpriseClient\SSP\_PIN

#### Registered Users

HKEY\_LOCAL\_MACHINE\SOFTWARE\BigFix\EnterpriseClient\  
SSP\_Green

#### Blocked Users

HKEY\_LOCAL\_MACHINE\SOFTWARE\BigFix\EnterpriseClient\SSP\_Red

- For Mac, Linux, AIX, and Solaris computers

#### PIN for Registration

/var/opt/BESClient/SSP\_PIN

#### Registered Users

/var/opt/BESClient/SSP\_Green

#### Blocked Users

/var/opt/BESClient/SSP\_Red

### The user reports that the software installation from the Self Service Portal failed. The failure existed when I deleted a task from a package after it was deployed in an Application Management. How do I fix this issue?

The task does not exist, so it cannot be issued. It also is not shown in the actions view of the console. You need to find and stop all Application Management Groups that have a reference to the deleted task. Then, delete the reference to the no longer existent task, and redeploy those Application Management Groups.

### Will unsubscribing to the Software Distribution site remove the Self Service Portal?

No, unsubscribing to the Software Distribution site does not remove the Self Service Portal. For more information about removing the Self Service Portal, see "Uninstalling the Self Service Portal" on page 60.

### I got an error that says "Could not connect to Trusted Services Provider" when I tried logging in to the Self Service Portal. What do I do?

This error usually happens when the Self Service Portal is removed and installed back again. If you get this error, complete the following steps:

1. Go to the Self Service Portal diagnostics page at [https://<your\\_host\\_name>/ssp/diagnostics](https://<your_host_name>/ssp/diagnostics).
2. If the **TSP connection test** and **TSP root CA** shows as "Connection refused", delete the certificate file for the Self Service Portal. You can find the certificate file in `path_to_TEM_server_directory\BigFix Enterprise\Management Extender\MDM Providers\MDMExtender\private\ssp\trusted_certs\your_certificate_file.pem`

**Note:** The certificate file is automatically generated the next time you log in to the Self Service Portal.

**I deleted a software distribution task, but its packages in the SHA1 folder that is stored in the C:\Program Files\BigFix Enterprise\BES Server\wwwrootbes\Uploads folder are not being deleted automatically. Why is that and what must I do?**

If you used the **Software Distribution Wizard** to create the task, no automatic cleanup occurs. This behavior is expected of the wizard. You must locate and delete the files or folders from the repository manually. Any cleanup of payloads must be done manually. It is suggested that you use the **Manage Software Distribution** dashboard instead of the **Software Distribution Wizard** to create software distribution tasks.

If you used the **Manage Software Distribution** dashboard to create the task, and yet its packages are not automatically deleted upon deleting of the task, ensure that you have:

- Deleted the files from the software distribution package
- Deleted all tasks that reference the file
- Stopped all open actions that reference the file

If any of these measures were not taken, the file and sha1 folder remains.

**Note:** The upload maintenance service for software distribution does the actual cleanup. To check the cleanup activity, see the log file that is found at C:\Program Files (x86)\BigFix Enterprise\BES Server\Applications\Logs\swd\_uploadmaintenanceservice.log.

**The installation of .pkg files on Mac endpoints was successful, but the task remains relevant. Why is that? How do I verify whether the software installation was truly successful?**

The task remains relevant because the inspector to check whether the Mac .pkg files are installed on an endpoint is not yet available. For information on how to manually check whether the package was deployed successfully, see “Package type verification” on page 23.

**Note:** Reinstalling a .pkg file does not cause any issues.

**Can I easily migrate created software packages from one IBM Endpoint Manager Deployment to another?**

No. Software packages are composed of Fixlets, database information, and uploaded files, and can not currently be easily exported and imported.

**Why does the status of a software deploy action not accurately reflect the installation status of the deployed application?**

Software distribution is unable to determine whether a software installation was successful in many cases. The issues that are related with the actual package installation are outside of the control of Software Distribution. It runs the package, but cannot track the result of that execution.

**Why are Solaris .pkg files failing to install?**

Solaris .pkg files may fail due to conflicts. The default option is to quit when encountering a conflict. If you would like to ignore conflicts and proceed with the installation, you can edit the Actionsript to change these values. These three settings, conflict, idepend, and rdepend, are set to 'quit' by default. Change 'quit' to 'nocheck' and then rerun the task.



---

## Notices

This information was developed for products and services that are offered in the USA.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

*IBM Director of Licensing  
IBM Corporation  
North Castle Drive, MD-NC119  
Armonk, NY 10504-1785  
United States of America*

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

*Intellectual Property Licensing  
Legal and Intellectual Property Law  
IBM Japan Ltd.  
19-21, Nihonbashi-Hakozakicho, Chuo-ku  
Tokyo 103-8510, Japan*

**The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:**

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those

websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licenses of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

*IBM Corporation  
2Z4A/101  
11400 Burnet Road  
Austin, TX 78758 U.S.A.*

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

Portions of this code are derived from IBM Corp. Sample Programs.

© Copyright IBM Corp. \_enter the year or years\_. All rights reserved.

---

## Programming interface information

---

### Trademarks

IBM, the IBM logo, and [ibm.com](http://ibm.com) are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at [www.ibm.com/legal/copytrade.shtml](http://www.ibm.com/legal/copytrade.shtml).

Adobe, Acrobat, PostScript and all Adobe-based trademarks are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, other countries, or both.

IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

ITIL is a registered trademark, and a registered community trademark of The Minister for the Cabinet Office, and is registered in the U.S. Patent and Trademark Office.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Java™ and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.

Linear Tape-Open, LTO, the LTO Logo, Ultrium, and the Ultrium logo are trademarks of HP, IBM Corp. and Quantum in the U.S. and other countries.

---

## Terms and conditions for product documentation

Permissions for the use of these publications are granted subject to the following terms and conditions.

### Applicability

These terms and conditions are in addition to any terms of use for the IBM website.

### Personal use

You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative work of these publications, or any portion thereof, without the express consent of IBM.

### Commercial use

You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of IBM.

### Rights

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.







Product Number: 5725-C43

Printed in USA