IBM Endpoint Manager
Version 9.1

Patch Management for AIX User's Guide

IBM Endpoint Manager
Version 9.1

Patch Management for AIX User's Guide

IBM

Note

Before using this information and the product it supports, read the information in “Notices” on page 47.

This edition applies to version 9, release 1, modification level 0 of IBM Endpoint Manager (product number 5725-C45) and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

Chapter 1. Overview

IBM® Endpoint Manager Patch Management for AIX® provides unified, real-time visibility and enforcement to deploy and manage patches to all endpoints from a single console. Patch Management keeps your AIX clients current with the latest packages, service packs, and fixes.

The Endpoint Manager Patch Management solution, which includes deploying a multi-purpose, lightweight agent to all endpoint devices, supports a wide variety of device types ranging from workstations and servers to mobile and point-of-sale (POS) devices.

This version of the Endpoint Manager Patch Management for AIX includes the following updates and new features:

- Updates to the installation action that is used by the existing technology level and service pack Fixlets.
- Network Installation Management (NIM) integration that focuses on the patch management features that NIM provides. The following dashboards are available to help run NIM-related tasks in an Endpoint Manager environment:
  - NIM Installation and Setup Dashboard
  - NIM Management Dashboard

Supported versions

Patch Management for AIX supports the latest Maintenance or Technology Level packages and Service Packs for AIX 5.1, 5.2, 5.3, 6.1, and 7.1.

The Patches for AIX Fixlet site includes inventory-only Fixlets for AIX Security Advisories, Critical Fixes, High Impact/Highly Pervasive Fixes and Program Temporary Fixes (PTFs) released since the last Maintenance Level Package update.

In addition, the Patches for AIX Fixlet site contains task messages to compare the patch level of a computer with the most currently available fixes. You can view your results in the IBM Endpoint Manager console after you have activated all analyses.

Chapter 2. Setup

Setting up your environment for patch management.

Site subscription

Sites are collections of Fixlet messages that are created internally by you, by IBM, or by vendors.

Subscribe to a site to access the Fixlet messages to patch systems in your deployment.

You can add a site subscription by acquiring a Masthead file from a vendor or from IBM or by using the Licensing Dashboard. For more information about subscribing to Fixlet sites, see the *IBM Endpoint Manager Installation Guide*.

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

Download plug-ins

Download plug-ins are executable programs that download a specified patch from the website of the patch vendor. To ease the process of caching, Fixlets have an incorporated protocol that uses download plug-ins.

For the Fixlet to recognize the protocol, the related download plug-in must be registered. You must use the Manage Download Plug-ins dashboard to register the download plug-in. After you register the plug-in, you can run the Fixlets to download, cache, and deploy patches from the IBM Endpoint Manager console.

If you already registered the plug-in, you can use the Manage Download Plug-ins dashboard to run the update. You must use the dashboard also to unregister and configure the download plug-in. For more information about the dashboard, see the following topics.

Note: Use the official mirror server configuration when you plan to download large amounts of packages. Specify the mirror server URL and credentials during the download plug-in registration or configuration to avoid being locked out of your account.

Note: If you install the download plug-in on relays, it is suggested that you also install it on the server.

Manage Download Plug-ins dashboard

Use the Manage Download Plug-ins dashboard to oversee and manage download plug-ins in your deployment.

You can use the Manage Download Plug-ins dashboard to register, unregister, configure, and upgrade the download plug-ins for different patch vendors. For more information about these features, see the following topics.

You must subscribe to the Patching Support site to gain access to this dashboard. To view the Manage Download Plug-ins dashboard, go to **Patch Management domain** > **All Patch Management** > **Dashboards** > **Manage Download Plug-ins**.

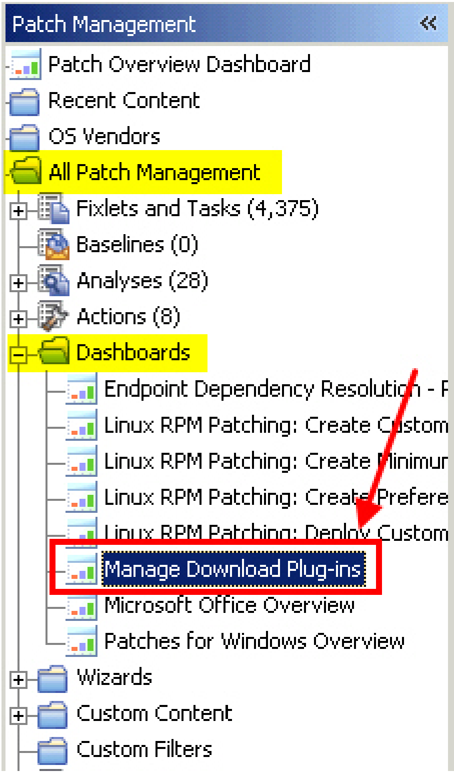
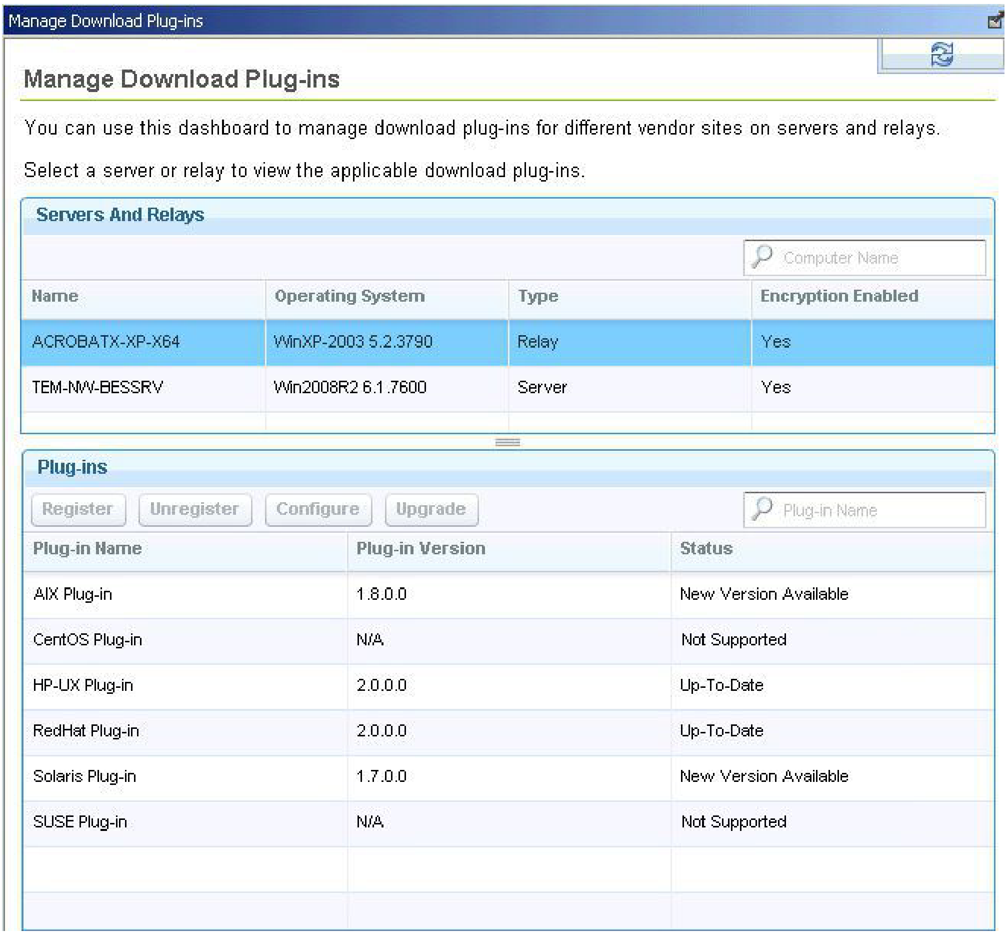

Patch Management
Patch Overview Dashboard
Recent Content
OS Vendors
All Patch Management
Fixlets and Tasks (4,375)
Baselines (0)
Analyses (28)
Actions (8)
Dashboards
Endpoint Dependency Resolution - F
Linux RPM Patching: Create Custom
Linux RPM Patching: Create Minimur
Linux RPM Patching: Create Prefere
Linux RPM Patching: Deploy Custom
Manage Download Plug-ins
Microsoft Office Overview
Patches for Windows Overview
Wizards
Custom Content
Custom Filters

Figure 1. Patch Management navigation tree

The dashboard displays all the servers and windows-only relays in your deployment. Select a server or relay to view all the plug-ins for that computer. The dashboard shows you also the version and status for each plug-in in one consolidated view.



Manage Download Plug-ins

Manage Download Plug-ins

You can use this dashboard to manage download plug-ins for different vendor sites on servers and relays.

Select a server or relay to view the applicable download plug-ins.

Servers And Relays

Computer Name

Name	Operating System	Type	Encryption Enabled
ACROBATX-XP-X64	WinXP-2003 5.2.3790	Relay	Yes
TEM-NW-BESSRV	Win2008R2 6.1.7600	Server	Yes

Plug-ins

Plug-in Name	Plug-in Version	Status
AIX Plug-in	1.8.0.0	New Version Available
CentOS Plug-in	N/A	Not Supported
HP-UX Plug-in	2.0.0.0	Up-To-Date
RedHat Plug-in	2.0.0.0	Up-To-Date
Solaris Plug-in	1.7.0.0	New Version Available
SUSE Plug-in	N/A	Not Supported

Figure 2. Manage Download Plug-ins dashboard

A plug-in can be in one of the following states:

- Not Installed
- New Version Available
- Up-To-Date
- Not Supported

Note: CentOS and SUSE Linux download plug-ins are not supported in relays.

The dashboard has a live keyword search capability. You can search based on the naming convention of the servers, relays, and plug-ins.

Registering the AIX download plug-in

Use the Manage Download Plug-ins dashboard to register the download plug-in for AIX.

You must complete the following tasks:

- Link your IBM ID to an IBM Customer Number (ICN) that is assigned to a valid contract. You can link multiple ICNs to your IBM ID. For linking instructions, see the steps that described in the announcement athttp://www-01.ibm.com/support/icn/.

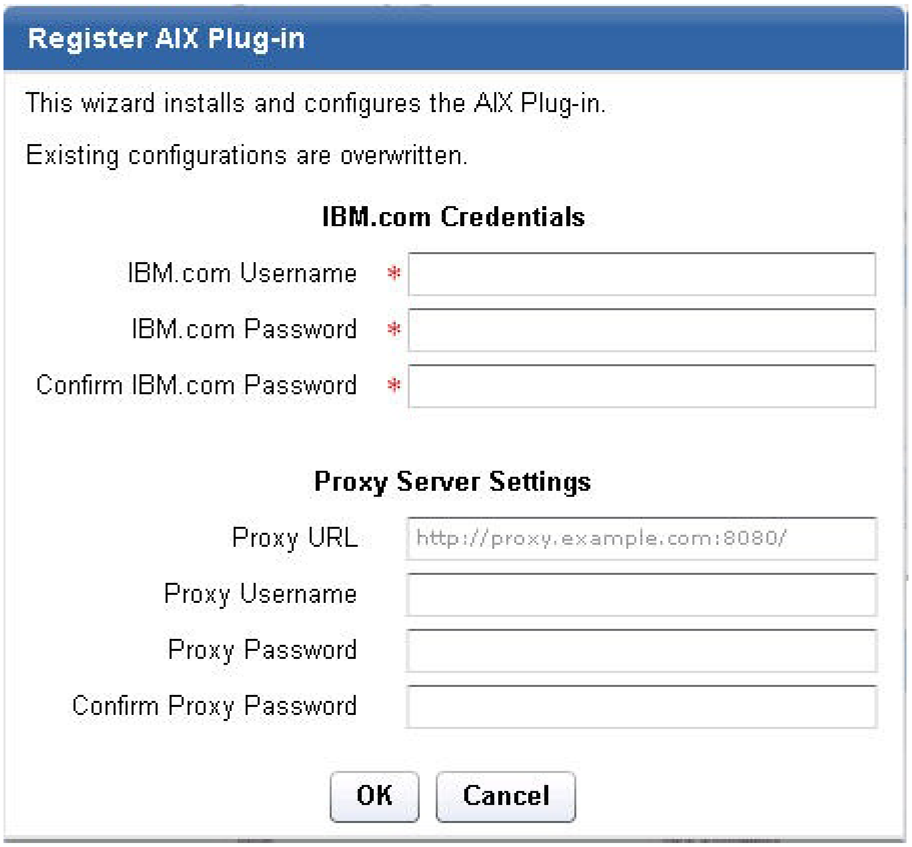
Note: To determine the ICNs associated with your current agreements with IBM, contact your IBM Business Partner or IBM Sales Representative. If you do not have an existing IBM ID or if you require further assistance, see the IBM Support Portal.

- Subscribe to the **Patching Support** site to gain access to the Manage Download Plug-ins dashboard.
- Enable the **Encryption for Clients** Fixlet on servers and relays for which you want to register the download plug-in.
- Activate the **Encryption Analysis for Clients** analysis and **Download Plug-in Versions** analysis.

When you register the download plug-in on a computer without the plug-in, the plug-in is automatically installed and the configuration file is created.

If a download plug-in is already installed on the computer, the configuration file is overwritten.

1. From the Patch Management domain, click **All Patch Management** > **Dashboards** > **Manage Download Plug-ins dashboard**.
2. From the Servers and Relays table, select the server or relay on which the download plug-in is to be registered.
3. From the Plug-ins table, select **AIX Plug-in**.
4. Click **Register**. The Register AIX Plug-in wizard displays.



Register AIX Plug-in

This wizard installs and configures the AIX Plug-in.

Existing configurations are overwritten.

IBM.com Credentials

IBM.com Username *

IBM.com Password *

Confirm IBM.com Password *

Proxy Server Settings

Proxy URL http://proxy.example.com:8080/

Proxy Username

Proxy Password

Confirm Proxy Password

Figure 3. Register AIX download plug-in wizard

5. Enter your IBM ID and password to download the available updates that you are entitled under an applicable warranty or support agreement.

6. Optional: Enter the proxy parameters if the downloads must go through a proxy server.

   Proxy URL
   The URL of your proxy server. It must be a well-formed URL, which contains a protocol and a host name. The URL is usually the IP address or DNS name of your proxy server and its port, which is separated by a colon. For example: `http://192.168.100.10:8080`.

   Proxy Username
   Your proxy user name if your proxy server requires authentication. It is usually in the form of `domain\username`.

   Proxy Password
   Your proxy password if your proxy server requires authentication.

   Confirm Proxy Password
   Your proxy password for confirmation.

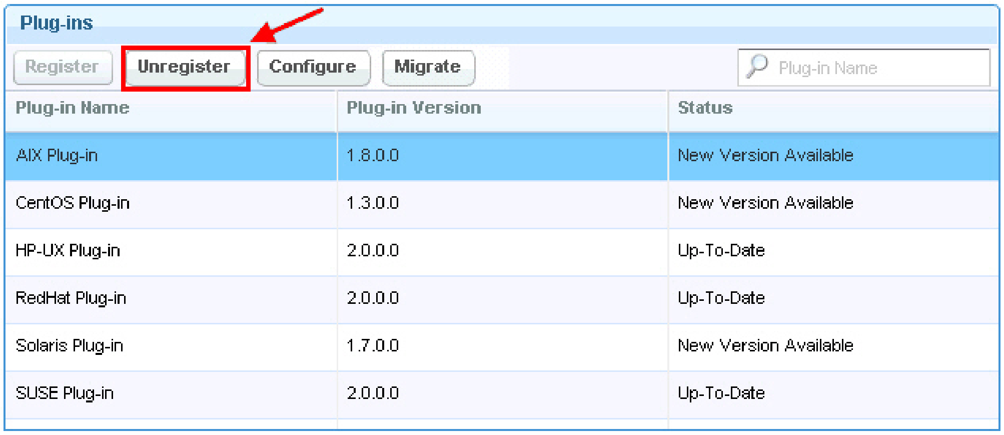
7. Click **OK**. The Take Action dialog displays.
8. Select the target computer.
9. Click **OK**.

You successfully registered the AIX download plug-in.

Unregistering the AIX download plug-in

Use the Manage Download Plug-ins dashboard to unregister the download plug-in for AIX.

1. From the Patch Management domain, click **All Patch Management** > **Dashboards** > **Manage Download Plug-ins dashboard**.
2. From the Servers and Relays table, select the server or relay on which the download plug-in is to be unregistered.
3. From the Plug-ins table, select **AIX Plug-in**.
4. Click **Unregister**.



Plug-in Name	Plug-in Version	Status
AIX Plug-in	1.8.0.0	New Version Available
CentOS Plug-in	1.3.0.0	New Version Available
HP-UX Plug-in	2.0.0.0	Up-To-Date
RedHat Plug-in	2.0.0.0	Up-To-Date
Solaris Plug-in	1.7.0.0	New Version Available
SUSE Plug-in	2.0.0.0	Up-To-Date

Figure 4. Unregister the AIX download plug-in

The Take Action dialog displays.

5. Select the target computer.
6. Click **OK**.

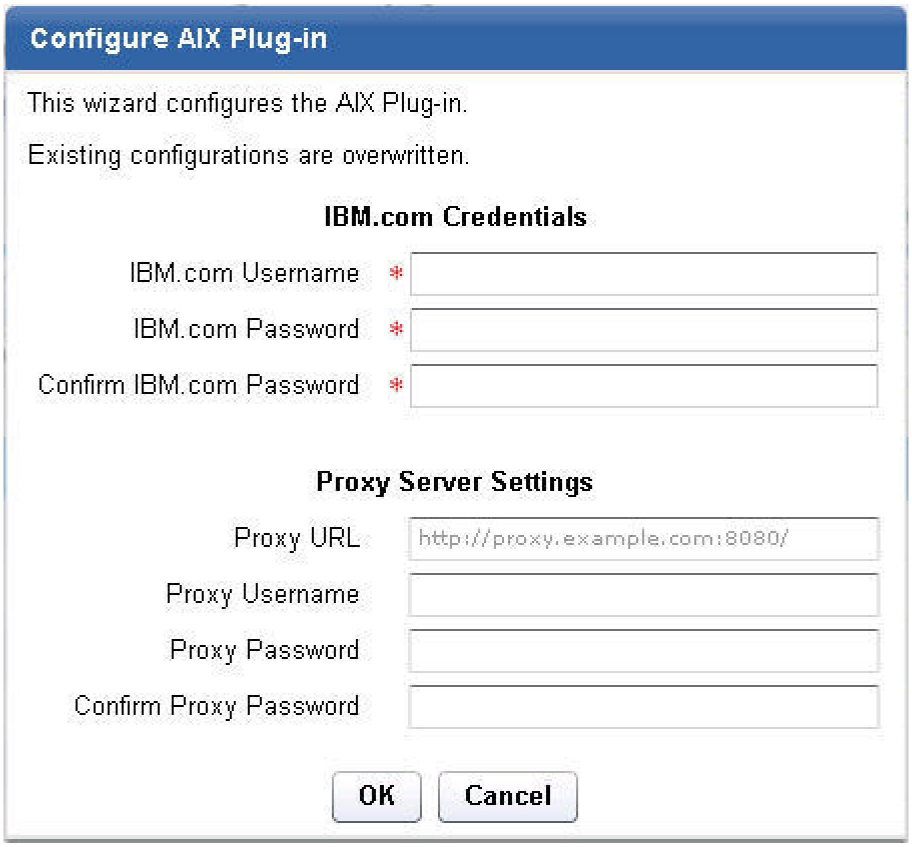
You successfully unregistered the AIX download plug-in.

Configuring the AIX download plug-in

Use the Manage Download Plug-ins dashboard to configure the download plug-in for AIX.

You might want to take note of your existing configuration for the download plug-in. Existing configurations are overwritten when you configure the download plug-in.

1. From the Patch Management domain, click **All Patch Management** > **Dashboards** > **Manage Download Plug-ins dashboard**.
2. From the Servers and Relays table, select the server or relay on which the download plug-in is to be configured.
3. From the Plug-ins table, select **AIX Plug-in**.
4. Click **Configure**. The Configure AIX Plug-in wizard displays.



Configure AIX Plug-in

This wizard configures the AIX Plug-in.

Existing configurations are overwritten.

IBM.com Credentials

IBM.com Username *

IBM.com Password *

Confirm IBM.com Password *

Proxy Server Settings

Proxy URL: http://proxy.example.com:8080/

Proxy Username

Proxy Password

Confirm Proxy Password

Figure 5. Configure AIX download plug-in wizard

5. Enter your IBM ID and password to download the available updates that you are entitled under an applicable warranty or support agreement.

   Note: Ensure that you linked your IBM ID to an IBM Customer Number (ICN) that is assigned to a valid contract. You can link multiple ICNs to your IBM ID. For linking instructions, see the steps that are described in the announcement athttp://www-01.ibm.com/support/icn/.

To determine the ICNs associated with your current agreements with IBM, contact your IBM Business Partner or IBM Sales Representative. If you do not have an existing IBM ID or if you require further assistance, see the IBM Support Portal.

6. Optional: Enter the proxy parameters if the downloads must go through a proxy server.

   Proxy URL
   The URL of your proxy server. It must be a well-formed URL, which contains a protocol and a host name. The URL is usually the IP address or DNS name of your proxy server and its port, which is separated by a colon. For example: `http://192.168.100.10:8080`.

   Proxy Username
   Your proxy user name if your proxy server requires authentication. It is usually in the form of `domain\username`.

   Proxy Password
   Your proxy password if your proxy server requires authentication.

   Confirm Proxy Password
   Your proxy password for confirmation.

7. Click **OK**. The Take Action dialog displays.
8. Select the target computer.
9. Click **OK**.

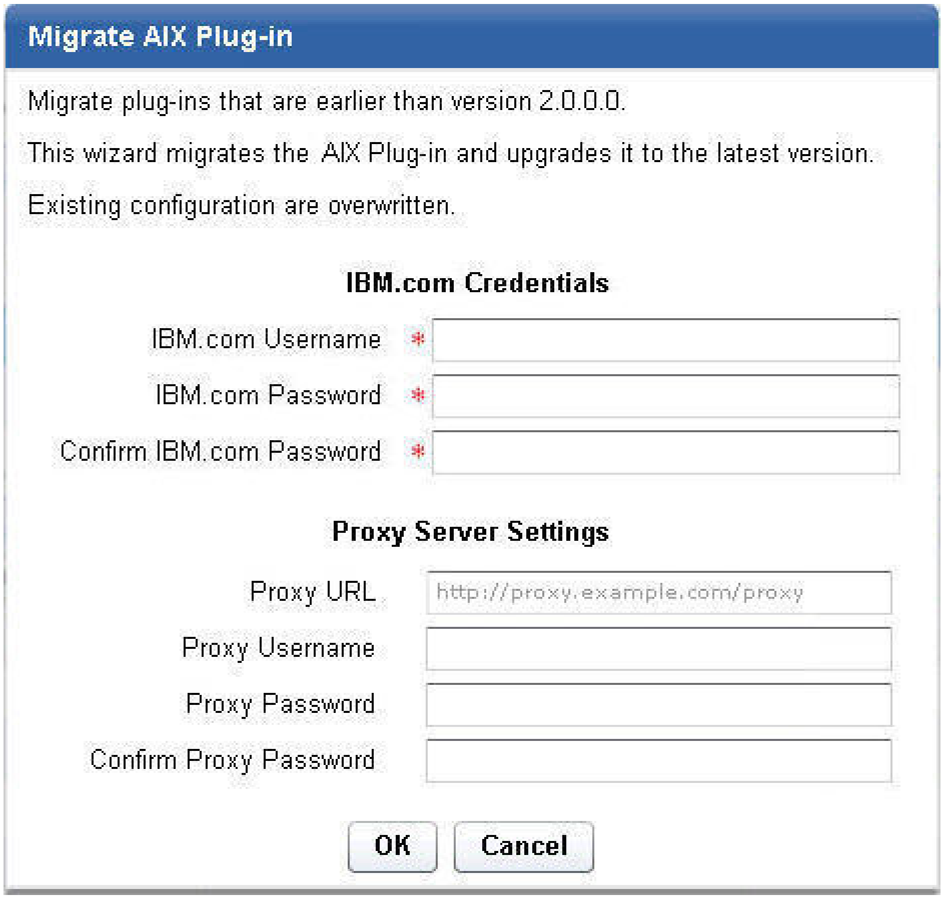
You successfully configured the AIX download plug-in.

Migrating the AIX download plug-in

You must migrate the AIX download plug-in if the plug-in version is earlier than 2.0.0.0. You only need to do this once. The download plug-in is upgraded to the latest version after migration.

You might want to take note of your existing configuration for the download plug-in. Existing configurations are overwritten when you migrate the download plug-in.

1. From the Patch Management domain, click **All Patch Management** > **Dashboards** > **Manage Download Plug-ins dashboard**.
2. From the Servers and Relays table, select the server or relay on which the download plug-in is to be migrated.
3. From the Plug-ins table, select **AIX Plug-in**.
4. Click **Migrate**. The Migrate AIX Plug-in wizard displays.



Migrate AIX Plug-in

Migrate plug-ins that are earlier than version 2.0.0.0.

This wizard migrates the AIX Plug-in and upgrades it to the latest version.

Existing configuration are overwritten.

Figure 6. Migrate AIX download plug-in wizard

5. Enter your IBM ID and password to download the available updates that you are entitled under an applicable warranty or support agreement.
6. Optional: Enter the proxy parameters if the downloads must go through a proxy server.

   Proxy URL
   The URL of your proxy server. It must be a well-formed URL, which contains a protocol and a host name. The URL is usually the IP address or DNS name of your proxy server and its port, which is separated by a colon. For example: `http://192.168.100.10:8080`.

   Proxy Username
   Your proxy user name if your proxy server requires authentication. It is usually in the form of `domain\username`.

   Proxy Password
   Your proxy password if your proxy server requires authentication.

   Confirm Proxy Password
   Your proxy password for confirmation.
7. Select the target computer on which the download plug-in is to be upgraded.
8. Click **OK**.

You successfully migrated and upgraded the AIX download plug-in.

Upgrading the AIX download plug-in

Use the Manage Download Plug-ins dashboard to upgrade the download plug-in for AIX.

1. From the Patch Management domain, click **All Patch Management** > **Dashboards** > **Manage Download Plug-ins dashboard**.
2. From the Servers and Relays table, select the server or relay on which the download plug-in is to be upgraded.
3. From the Plug-ins table, select **AIX Plug-in**.
4. Click **Upgrade**. The Take Action dialog displays.
5. Select the target computer.
6. Click **OK**.

You now have the latest version of the AIX download plug-in installed.

Chapter 3. Patch Management for AIX

Use the Fixlets on the Patches for AIX Fixlet site to apply AIX patches to your deployment.

Fix pack download configuration

Configure the target AIX systems and the Endpoint Manager server to download filesets from the internet.

Before you deploy any updates using the internet download option, register the AIX Download Plug-in from the Manage Download Plug-ins dashboard. See Manage Download Plug-ins dashboard. The download plug-in gathers a list of filesets that are included in the specified fix pack and downloads them one at a time. The download plug-in gathers the fix packs at run time.

Note: The download plug-in is not required when you deploy updates through NFS mount.

You can also use the AIX Download Cacher to download fix packs. To enable the AIX Download Cacher to download filesets, deploy the **Run Download Cacher Tool - AIX** task. For more information about the download cacher, see “Using the Download Cacher” on page 14.

Downloading large files from the internet requires large amounts of available disk space on the `/var` partition, where the BES Data directory is located. To accommodate large files from the internet, deploy the following tasks:

AIX: Increase Disk Space - BES Data Folder task (ID #57)

AIX sets partition sizes to a predetermined minimum that allows the unused disk space to be dynamically provisioned to various partitions as needed.

This task expands the partition that contains the Endpoint Manager client data directory to make enough room for a fix pack to be transferred and extracted.

AIX: Change BES Client Download Limits task (ID #59)

This task extends the default Endpoint Manager client limitation for file transfers of 2 GB to allow large file transfers.

AIX: Remove File Size Limit for Root User task (ID #60)

This task removes the default AIX limitation of 1 GB for the allowed file size.

Note: These configuration changes are unnecessary if you are installing over an NFS mount.

Fileset installation states

Fileset installations can be in either an Applied or a Committed state.

The two fileset installation states have the following traits:

Applied

Applied installations create backups of the filesets that are being replaced. These backups can be used to revert updates.

All installation actions, either through released content or custom content that is generated by the **AIX Fileset Deployment Wizard**, are done in the applied state.

Note: Reverting technology level updates is not supported by AIX and might have unexpected results.

Committed

Committed installations have no backups and cannot be reverted.

Commit applied installations after confirmation to free up the disk space that is used by the installation backups.

The **Commit Applied Filesets** Fixlet can be used to facilitate the process for the committed state.

Using the Download Cacher

You can use the AIX Download Cacher utility to deploy service pack, concluding service pack, or technology level fixes. The Download Cacher uses HTTP to download specific fix packs. Ensure that HTTP network traffic is not blocked in your environment.

The AIX Download Cacher tool is a Perl executable that automatically downloads and caches AIX technology levels, service packs, or concluding service packs to facilitate deployment of AIX Fixlets.

To access the tool from the Endpoint Manager console:

1. Click **All Patch Management** > **Fixlets and Tasks** > **By Site** > **Patches for AIX** > **Run Download Cacher Tool - AIX**.
2. Select the appropriate link in the Actions box to start the download.

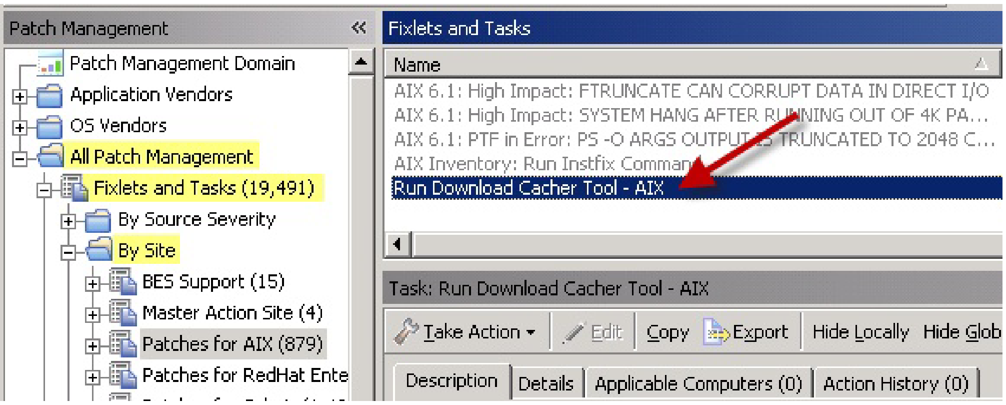
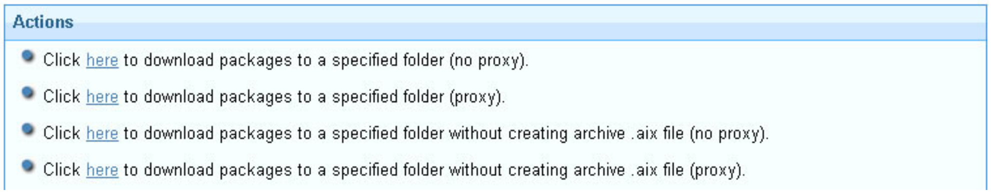


Figure 7. Run Download Cacher Tool - AIX task

To build a directory of filesets that can be used as an NFS source for a fix pack update, use either of these actions:

- **download packages to a specified folder without creating archive .aix file (no proxy)**

- **download packages to a specified folder without creating archive .aix file (proxy)**



Actions

- Click here to download packages to a specified folder (no proxy).
- Click here to download packages to a specified folder (proxy).
- Click here to download packages to a specified folder without creating archive .aix file (no proxy).
- Click here to download packages to a specified folder without creating archive .aix file (proxy).

Figure 8. Action box of the AIX Download Cacher task

You can run the Download Cacher manually. For more information, see the following technote: http://www-01.ibm.com/support/docview.wss?uid=swg21506031.

```
Usage
AIXDownloadCacher.exe --dir <path to output directory>
 --fixid <Fix Pack ID> [optional parameters]
Required Parameters
--dir <path to output directory>
 Directory where downloaded files will be saved. This directory is also used
 for temporary storage of downloaded files before being compressed into a
 single archived file.
--fixid <Fix Pack ID>
 AIX Fix Pack ID or Interim Fix APAR ID to be downloaded (for example,
 5300-04-03 or IZ93611).
Optional Parameters
--proxyserver <servername:port>
 Name and port of proxy server (for example, http://myproxy.company.com:8080).
--proxyuser <username>
 Proxy username if required by server.
--proxypass <password>
 Proxy password if required by server.
--logdir <path to log directory>
 Specify the directory to write the log file to. Defaults to the current working
 directory.
--repo <path to local repository of .bff files>
 Specify the location of the local cache to check before attempting to download
 files from the Internet. Missing files are added to the cache directory
 if write access is enabled.
--base
 Specify the base Technology Level (for example, 6100-00) to use when building
 the fileset list for the specified fix pack ID. Defaults to the TL of the
 fix pack (for example, 6100-03). This option is ignored with interim fixes.
--no-archive
 Skip creation of .aix archive file. The output directory will contain
 the individual filesets.
--clean
 Remove temporary files after each run. Enabling this option disables the
 ability to resume failed and incomplete downloads. Default behavior is to
 remove temporary files only after all files for the fileset have been
 downloaded and a complete archive has been created.
--sha1
 Renames archived.aix file to its sha1 value.
--version
 Display version information.
--help
  Displays usage information.
Examples:
Download Fix Pack 6100-04-05 through a proxy server using a local repository.
 AIXDownloadCacher --dir "C:\temp" --fixid 6100-04-05
 --proxyserver http://proxy.server.com:8080 --proxyuser myuser
 --proxypass secretpass --repo "D:\AIXCache"
```

```
Download Fix Pack 7100-03-06 for systems already at TL 02, force removal of
temp files on failures and rename .aix archive file to its sha1 value.
 AIXDownloadCacher --dir "C:\temp" --fixid 7100-03-06 --base 7100-02
 --clean --sha1
Download Fix Pack 6100-06-03 with complete TL without compressing filesets
into .aix archive file.
 AIXDownloadCacher --dir "C:\temp" --fixid 6100-06-03 --base 6100-00 --no-archive
```

Notes:

- If you run the tool without specifying any parameters, you are prompted to enter the parameters at the command line.
- The `--sha1` parameter works only with created archive files and is ignored if it used with the `--no-archive` parameter.

AIX Deployment Wizard

Use the AIX Deployment Wizard to deploy fileset updates, service packs, conclusive service packs, or technology levels to AIX systems that have the Endpoint Manager client.

Creating Fixlets for AIX fileset updates

You can use the AIX Deployment Wizard to deploy fileset updates and program temporary fixes (PTFs).

Before you use the wizard to deploy fileset updates, obtain the filesets that you want from the IBM website.

You can access the AIX fixes from the following link: http://www-933.ibm.com/support/fixcentral/?productGroup0=ibm/systemp&productGroup1=ibm/aix

Note: For detailed instructions about using the IBM software support website, see the following technote: http://www-01.ibm.com/support/docview.wss?uid=swg21505749.

To deploy PTFs, you must identify the technology level for which you are downloading the PTF to reduce the size of your download.

AIX service pack and technology level updates are developed, tested, and released as fix pack bundles. They are intended to be installed as full bundles rather than as individual filesets.

1. From the Endpoint Manager console, click **Patch Management** > **OS Vendors** > **IBM AIX** > **AIX Deployment Wizard**.

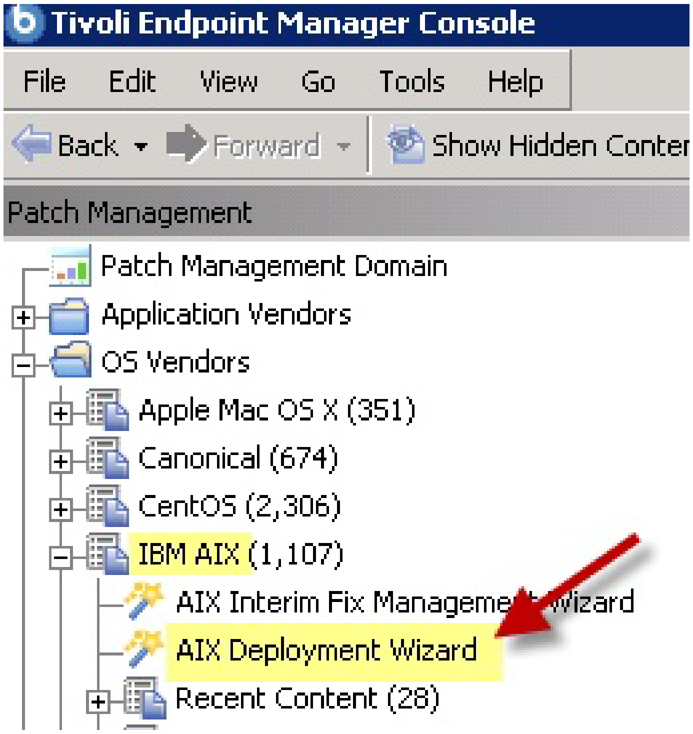
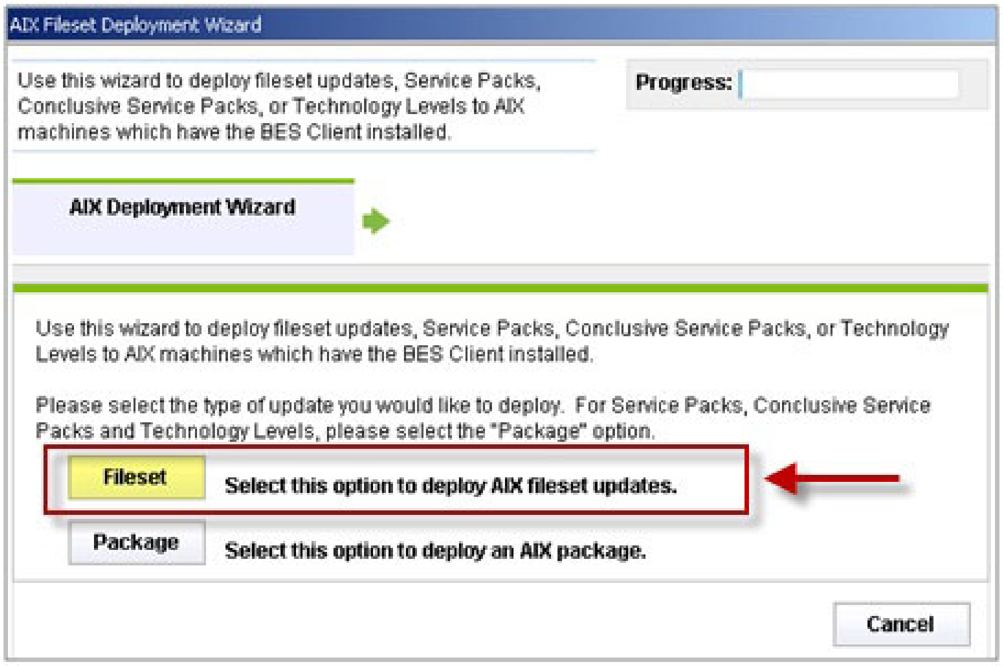


Figure 9. The AIX Deployment Wizard from the navigation tree

2. Click **Fileset** to deploy AIX fileset updates.



Use this wizard to deploy fileset updates, Service Packs, Conclusive Service Packs, or Technology Levels to AIX machines which have the BES Client installed.

Use this wizard to deploy fileset updates, Service Packs, Conclusive Service Packs, or Technology Levels to AIX machines which have the BES Client installed.

Please select the type of update you would like to deploy. For Service Packs, Conclusive Service Packs and Technology Levels, please select the "Package" option.

Fileset Select this option to deploy AIX fileset updates.

Package Select this option to deploy an AIX package.

Figure 10. Fileset option in the AIX Deployment Wizard

3. Enter the location of the filesets. You can provide this information by using the following options:
   - Download from URL

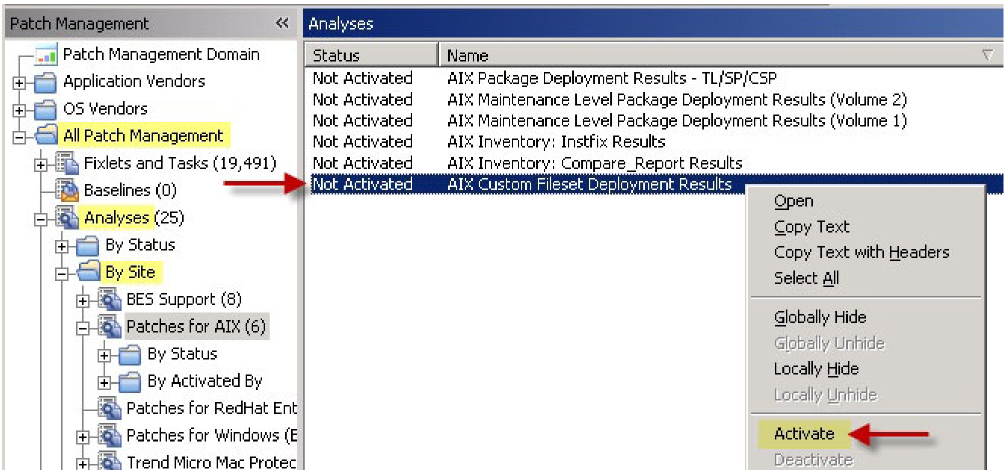
- File (for single filesets)
- Folder (for multiple filesets)

4. Click **Next**.
5. Select the relevant platforms and customize the text fields as necessary.
6. Optional: Select the check box if you want to create a one-time action rather than a reusable Fixlet.
7. Optional: Select the other check box to create a preview-only action. This preview runs the preinstalled verification checks. The results of those checks are available in the **AIX Pre-Install Verification Results** analysis.
8. After you set the necessary parameters, click **Finish**.

After completion, the generated one-time action or Fixlet displays in the Endpoint Manager console. You can use it to deploy the AIX update to the relevant computers.

To view detailed information about the results of deploying your AIX fileset update, activate the **AIX Custom Fileset Deployment Results** analysis (ID #22).

Click **All Patch Management** > **Analyses** > **By Site** > **Patches for AIX** > **AIX Custom Fileset Deployment Results** > **Activate**.



Status	Name
Not Activated	AIX Package Deployment Results - TL/SP/CSP
Not Activated	AIX Maintenance Level Package Deployment Results (Volume 2)
Not Activated	AIX Maintenance Level Package Deployment Results (Volume 1)
Not Activated	AIX Inventory: Instfix Results
Not Activated	AIX Inventory: Compare_Report Results
Not Activated	AIX Custom Fileset Deployment Results

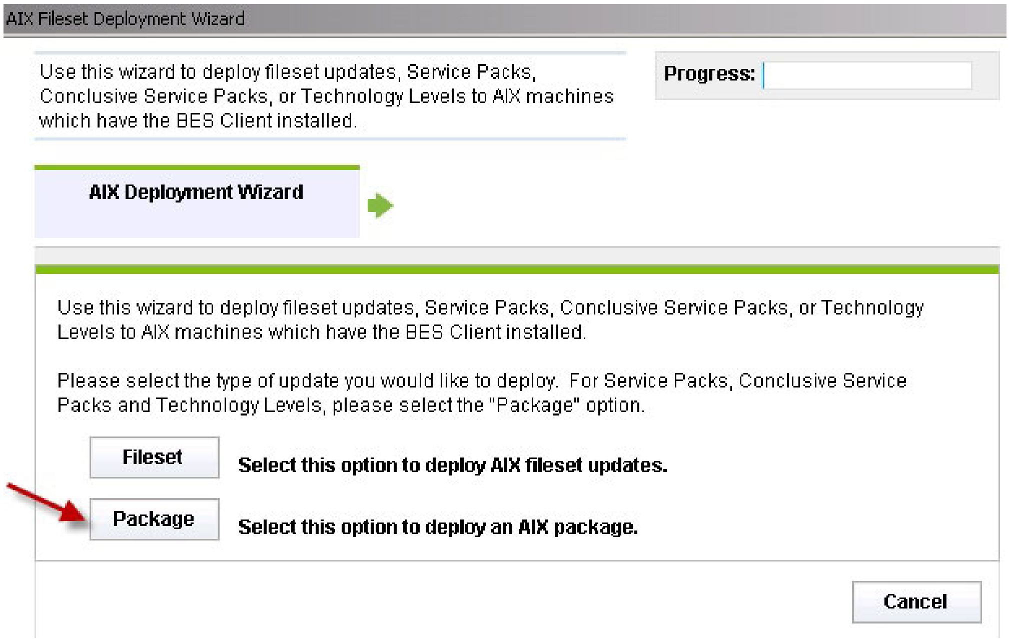
Figure 11. Activating the AIX Custom Fileset Deployment Results analysis

Creating Fixlets for AIX package updates

You can use the AIX Deployment Wizard to deploy packages for service packs, concluding service packs, and technology levels.

Before you use the wizard to deploy package updates, obtain the updates that you want from the IBM website by using the download cacher. For more information, see “Using the Download Cacher” on page 14.

1. From the Endpoint Manager console and click **Patch Management** > **OS Vendors** > **IBM AIX** > **AIX Deployment Wizard**.
2. Click **Package**.



AIX Fileset Deployment Wizard

Use this wizard to deploy fileset updates, Service Packs, Conclusive Service Packs, or Technology Levels to AIX machines which have the BES Client installed.

Use this wizard to deploy fileset updates, Service Packs, Conclusive Service Packs, or Technology Levels to AIX machines which have the BES Client installed.

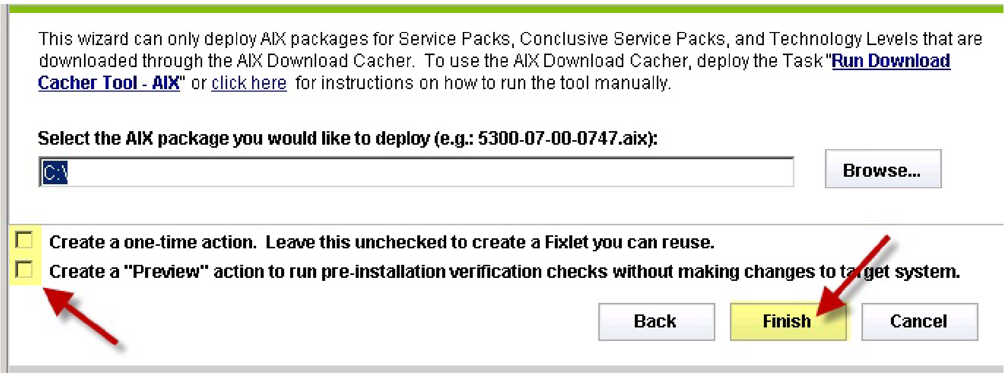
Please select the type of update you would like to deploy. For Service Packs, Conclusive Service Packs and Technology Levels, please select the "Package" option.

Fileset Select this option to deploy AIX fileset updates.

Package Select this option to deploy an AIX package.

Figure 12. Package option in the AIX Deployment Wizard

3. Enter the location of the AIX package that you want to deploy.
4. Optional: Select the check the box if you want to create a one-time action rather than a reusable Fixlet.
5. Optional: You can also select the other check box to create a preview-only action. This preview runs the preinstalled verification checks. The results of those checks are available in the **AIX Pre-Install Verification Results** analysis.
6. After you set the necessary parameters, click **Finish**.



This wizard can only deploy AIX packages for Service Packs, Conclusive Service Packs, and Technology Levels that are downloaded through the AIX Download Cacher. To use the AIX Download Cacher, deploy the Task "Run Download Cacher Tool - AIX" or click here for instructions on how to run the tool manually.

Select the AIX package you would like to deploy (e.g.: 5300-07-00-0747.aix):

C:\

□ Create a one-time action. Leave this unchecked to create a Fixlet you can reuse.

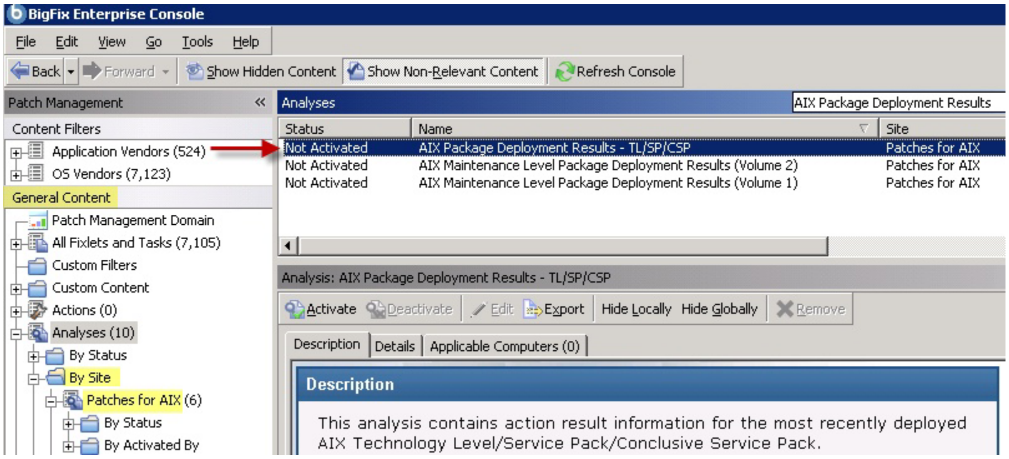
□ Create a "Preview" action to run pre-installation verification checks without making changes to target system.

Figure 13. Finishing the configuration for AIX package updates

After completion, the generated one-time action or Fixlet displays in the Endpoint Manager console. You can use it to deploy the AIX update to the relevant computers.

To view the detailed information about the results of deploying your AIX package update, activate the **AIX Package Deployment Results - TL/SP/CSP** analysis.

Click **All Patch Management** > **Analyses** > **By Site** > **Patches for AIX** > **AIX Package Deployment Results - TL/SP/CSP** > **Activate**.


BigFix Enterprise Console
File Edit View Go Tools Help
Back Forward Show Hidden Content Show Non-Relevant Content Refresh Console
Patch Management
Content Filters
Application Vendors (524)
OS Vendors (7,123)
General Content
Patch Management Domain
All Fixlets and Tasks (7,105)
Custom Filters
Custom Content
Actions (0)
Analyses (10)
By Status
By Site
Patches for AIX (6)
By Status
By Activated By
Analyses
AIX Package Deployment Results
Status
Name
Site
Not Activated
AIX Package Deployment Results - TL/SP/CSP
Patches for AIX
Not Activated
AIX Maintenance Level Package Deployment Results (Volume 2)
Patches for AIX
Not Activated
AIX Maintenance Level Package Deployment Results (Volume 1)
Patches for AIX
Analysis: AIX Package Deployment Results - TL/SP/CSP
Activate Deactivate Edit Export Hide Locally Hide Globally Remove
Description Details Applicable Computers (0)
Description

This analysis contains action result information for the most recently deployed AIX Technology Level/Service Pack/Conclusive Service Pack.

Figure 14. Activating the AIX Package Deployment Results - TL/SP/CSP analysis

Creating Fixlets for firmware updates

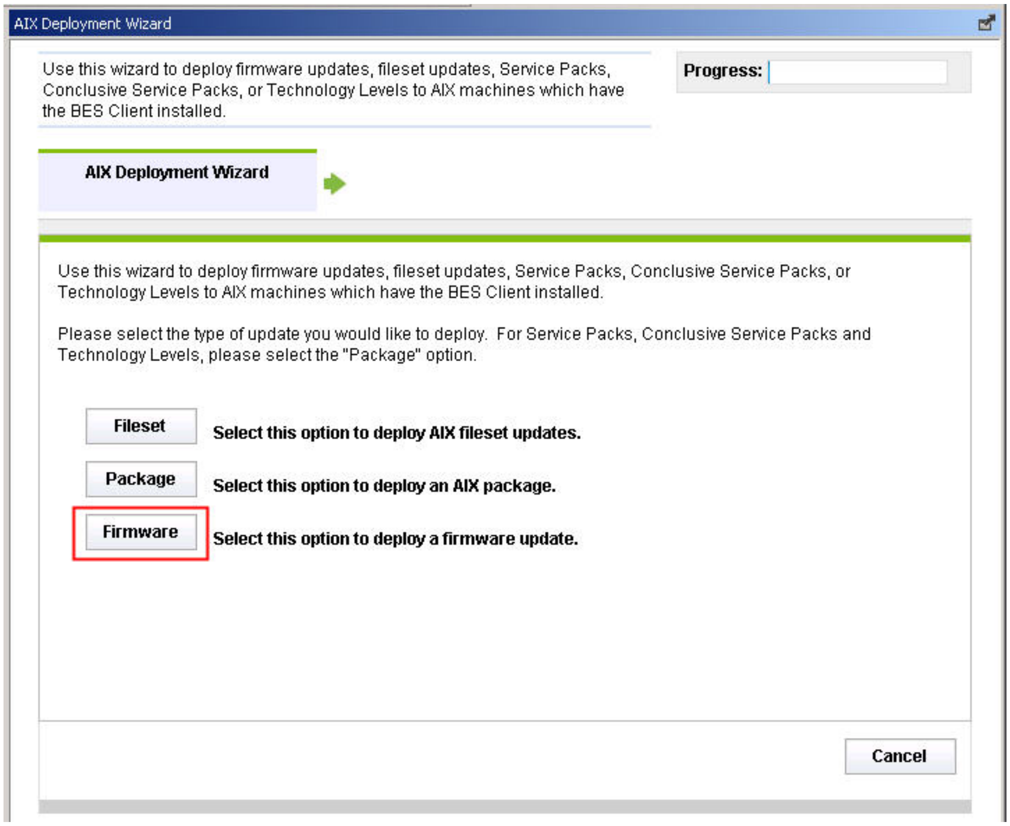
You can use the AIX Deployment Wizard to deploy packages for firmware updates, which are also known as microcode updates. These updates can be in either `.rpm` or `.iso` format.

To deploy firmware updates from the AIX Deployment Wizard, you must first obtain the updates that you want from Fix Central.

Note: Currently, IBM Endpoint Manager does not provide any tools to help download firmware updates.

CAUTION: Do not rename any of the downloaded files. The AIX Deployment Wizard uses the file name when it attempts to parse the new firmware version information.

1. From the Endpoint Manager console, click **Patch Management** > **OS Vendors** > **IBM AIX** > **AIX Deployment Wizard**.
2. Click **Firmware**.



Use this wizard to deploy firmware updates, fileset updates, Service Packs, Conclusive Service Packs, or Technology Levels to AIX machines which have the BES Client installed.

Use this wizard to deploy firmware updates, fileset updates, Service Packs, Conclusive Service Packs, or Technology Levels to AIX machines which have the BES Client installed.

Please select the type of update you would like to deploy. For Service Packs, Conclusive Service Packs and Technology Levels, please select the "Package" option.

Fileset: Select this option to deploy AIX fileset updates.

Package: Select this option to deploy an AIX package.

Firmware: Select this option to deploy a firmware update.

Figure 15. Firmware option in the AIX Deployment Wizard

3. Enter the location of the AIX package that you want to deploy.
4. Optional: Select the check box if you want to create a one-time action rather than a reusable Fixlet.
5. After you set the necessary parameters, click **Finish**.

After completion, the generated one-time action or Fixlet displays in the Endpoint Manager console. You can use it to deploy the AIX firmware update to the relevant computers.

Activate the **AIX Firmware Level** analysis, which reports the permanent and temporary firmware versions and the system version that it is running on (temporary or permanent).

Related tasks:

"Deploying firmware updates" on page 24
You can deploy firmware updates, also known as microcode updates, by using the custom content that was created by the AIX Deployment Wizard.

Deploying technology level and service pack patches

You can deploy maintenance or technology level and service pack patches through the released or custom content.

If you want to deploy patches through the internet download option, register the AIX Download Plug-in. See "Fix pack download configuration" on page 13.

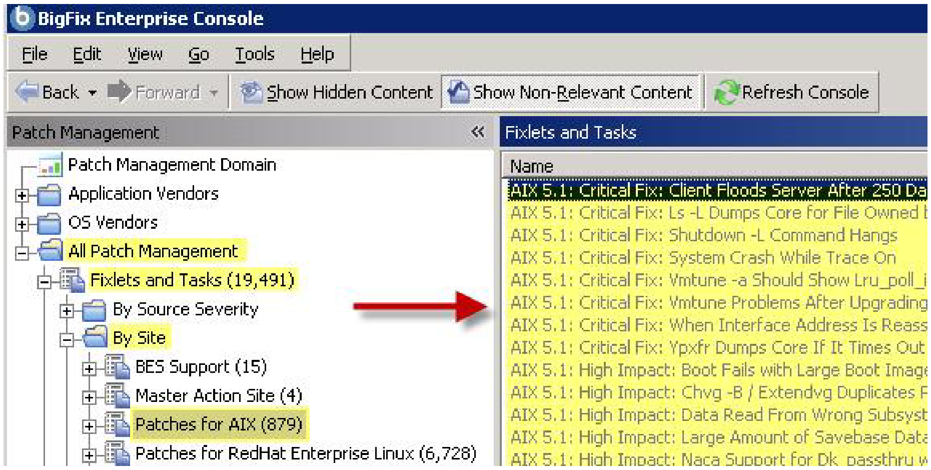
For Endpoint Manager version 8.1 and earlier, run the **Determine OS Level** Fixlet.

AIX determines the operating system level by comparing the installed filesets to a list of known Authorized Program Analysis Reports (APARs).

Use the NFS method to use a local repository as the source of the filesets for the fix pack to be installed. This method enables faster installations and uses less bandwidth.

- To deploy patches through the released content, either through the internet download option or through an NFS mount, complete the following steps:
  1. From the IBM Endpoint Manager console, click **All Patch Management** > **Fixlets and Tasks** > **By Site** > **Patches for AIX**.

     A list of Fixlets is displayed on the right.

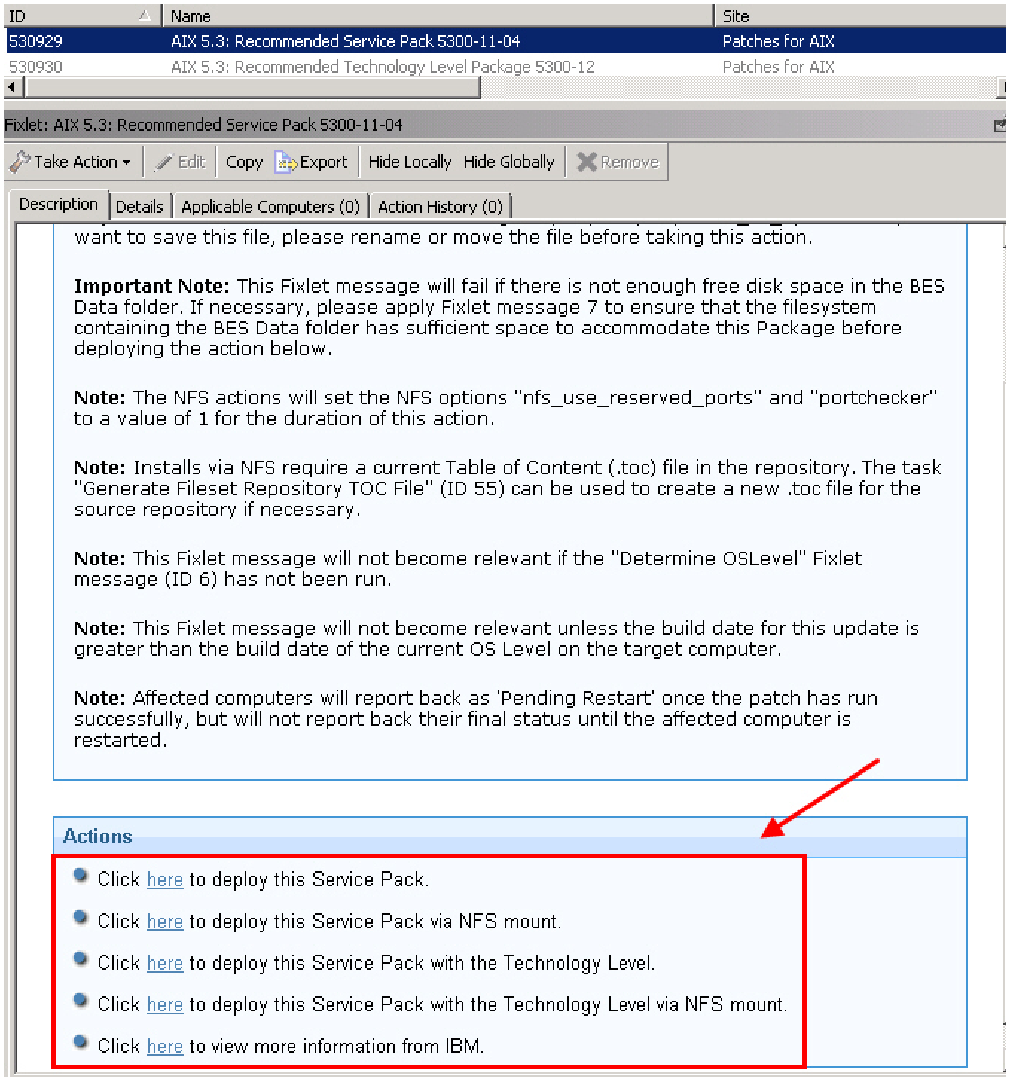


AIX 5.1: Critical Fix: Client Floods Server After 250 Da
AIX 5.1: Critical Fix: Ls -L Dumps Core for File Owned b
AIX 5.1: Critical Fix: Shutdown -L Command Hangs
AIX 5.1: Critical Fix: System Crash While Trace On
AIX 5.1: Critical Fix: Vmtune -a Should Show Lru_poll_i
AIX 5.1: Critical Fix: Vmtune Problems After Upgrading
AIX 5.1: Critical Fix: When Interface Address Is Reass
AIX 5.1: Critical Fix: Ypxfr Dumps Core If It Times Out
AIX 5.1: High Impact: Boot Fails with Large Boot Image
AIX 5.1: High Impact: Chvg -B / Extendvg Duplicates F
AIX 5.1: High Impact: Data Read From Wrong Subsyst
AIX 5.1: High Impact: Large Amount of Savebase Data
AIX 5.1: High Impact: Naca Support for Dk_passthru w

Figure 16. Fixlet list panel view

  2. Select a Fixlet to deploy a technology level or service pack update from the list.

     For this example, the Fixlet *AIX 5.3: Recommended Service Pack 5300-11-04* was selected.



ID	Name	Site
530929	AIX 5.3: Recommended Service Pack 5300-11-04	Patches for AIX
530930	AIX 5.3: Recommended Technology Level Package 5300-12	Patches for AIX

Fixlet: AIX 5.3: Recommended Service Pack 5300-11-04

want to save this file, please rename or move the file before taking this action.

Important Note: This Fixlet message will fail if there is not enough free disk space in the BES Data folder. If necessary, please apply Fixlet message 7 to ensure that the filesystem containing the BES Data folder has sufficient space to accommodate this Package before deploying the action below.

Note: The NFS actions will set the NFS options "nfs_use_reserved_ports" and "portchecker" to a value of 1 for the duration of this action.

Note: Installs via NFS require a current Table of Content (.toc) file in the repository. The task "Generate Fileset Repository TOC File" (ID 55) can be used to create a new .toc file for the source repository if necessary.

Note: This Fixlet message will not become relevant if the "Determine OSLevel" Fixlet message (ID 6) has not been run.

Note: This Fixlet message will not become relevant unless the build date for this update is greater than the build date of the current OS Level on the target computer.

Note: Affected computers will report back as 'Pending Restart' once the patch has run successfully, but will not report back their final status until the affected computer is restarted.

Actions

- Click here to deploy this Service Pack.
- Click here to deploy this Service Pack via NFS mount.
- Click here to deploy this Service Pack with the Technology Level.
- Click here to deploy this Service Pack with the Technology Level via NFS mount.
- Click here to view more information from IBM.

Figure 17. Sample Fixlet

3. Review the text in the **Description** tab.
4. Click the appropriate link in the Actions box to start the deployment.
5. Optional: If you decide to deploy the patches on NFS mount, you must enter the full path to NFS repository (for example, "`myServer:/AIX/fileset repo`" `myServer:/Local/Repo`).

- To deploy patches through custom content, you must create the Fixlet or a custom action by using the **AIX Deployment Wizard**. For more information about how to use the wizard, see “Creating Fixlets for AIX package updates” on page 18.

  Note: This deployment method provides an extra layer of security by prompting you to manually provide authentication credentials.

Deploying interim fixes

Use the AIX Interim Fix Management Wizard to install interim fixes on AIX systems.

Before you can deploy the patches, you must download the interim fixes from the AIX website. The Authorized Program Analysis Reports (APAR) provides a link to where you can download the interim fix if one is available.

You can use the AIX Download Cacher to download interim fixes. For more information, see "Using the Download Cacher" on page 14.

1. From the Endpoint Manager console, click **Patch Management** > **OS Vendors** > **IBM AIX** > **AIX Interim Fix Management Wizard**.
2. Click **Install**.
3. Enter where the interim fixes are located. You can provide this information in one of the following ways:
   - Download from URL
   - File
   - Folder

   Note: All interim fixes must have an `.epkg.Z` file extension.
4. Click **Next**.
5. Select the relevant platforms and customize the fields as necessary.
6. Optional: Select the check box if you want to create a one-time action rather than a reusable Fixlet.
7. Click **Finish**.
8. Deploy the action.

To view the results of the deployment, activate the **AIX Interim Fixes** analysis (ID #43). This analysis displays only installed interim fixes on a per-system basis.

Deploying firmware updates

You can deploy firmware updates, also known as microcode updates, by using the custom content that was created by the AIX Deployment Wizard.

Run the **Determine Firmware Level** task on all target AIX systems. This task collects firmware version information, which is used to identify the relevant systems. This task remains relevant to all AIX systems, providing the option to update system firmware information as often as might be required. No firmware related content becomes relevant until you run this task.

Note: The firmware information is updated automatically as part of each IBM Endpoint Manager generated firmware deployment. You do not need to run the **Determine Firmware Level** task after deploying firmware updates with IBM Endpoint Manager content.

After creating a one-time action or Fixlet for a firmware update, you deploy it to the relevant computers. For information about creating custom content, see "Creating Fixlets for firmware updates" on page 20.

1. From the Endpoint Manager console, navigate to where the custom content is located.
2. Select a firmware update Fixlet.
3. Review the text in the **Description** tab.
4. Click the appropriate link in the Actions box to start the deployment.

Firmware updates are deployed to the temporary side of the service processor. After you verify that the installation of the firmware version is successful, you must commit the firmware fix by using the **Commit Firmware Fix Permanently** Fixlet. This action might take several minutes to run.

Attention: When an update is committed to the permanent side, it cannot be undone.

Note: Rejecting a firmware update requires physical interaction with the target servers and cannot be performed using IBM Endpoint Manager.

Uninstalling all interim fixes

Interim fixes lock their target filesets to prevent any changes to the filesets while the interim fix is installed.

- To uninstall all interim fixes by using the **Uninstall All Interim Fixes** Fixlet, complete the following steps:
  1. From the Endpoint Manager console, click **Patch Management** > **OS Vendors** > **IBM AIX** > **Maintenance**.
  2. Click **Uninstall All Interim Fixes** (ID #63).
  3. Deploy the action.
- To uninstall all interim fixes by using the **AIX Interim Fix Management Wizard**, complete the following steps:
  1. From the Endpoint Manager console, click **Patch Management** > **OS Vendors** > **IBM AIX** > **AIX Interim Fix Management Wizard**.
  2. Click **Uninstall**.
  3. Click **Uninstall all interim fixes**.
  4. Click **Finish**.
  5. Deploy the action.

  Note: You can use the **AIX Interim Fix Management Wizard** also to remove individual interim fixes.

Individual AIX fileset updates

Deploy AIX technology level and service pack updates as a full fix pack bundle and not as individual filesets. Updating individual filesets might cause unexpected results.

If you still want to update individual filesets, download the `.bff` file that you want to deploy. Then use the fileset option of the AIX Deployment Wizard to generate the necessary Fixlet. For more information, see the steps in "Creating Fixlets for AIX fileset updates" on page 16.

Troubleshooting Failed OS Updates

Learn which common factors affect the outcome of a deployment.

The most common reasons for failure include:

- Filesets that are locked by interim fixes.
- Missing filesets from a local NFS repository.
- An outdated table of contents (`.toc`) file in the repository.

In each case, begin troubleshooting by generating a list of filesets that are lower than the latest levels of the service packs recognized by the AIX operating system.

Use the `instfix` command to identify filesets that are not at the latest level. The following command processes all known service packs and provides details for any packages with known updates.

An example command includes the following format:

```
for LEVEL in `instfix -i | grep SP | grep "Not all" | awk '{print $5}'`;
do instfix -ciqk $LEVEL | grep :-:; done
```

The output of this example is in the following format:

```
<Service Pack>:<Package Name>:<Installed Version>:<Expected Version>:
<Version Status (+,=,-)>:<Package Description>
```

An example output includes the following format:

```
 61-04-111140_SP:perfagent.tools:6.1.4.11:6.1.6.16:-:AIX 6100-04-11 Service Pack
```

With the results of the `instfix` command, you can check locked filesets by using the **AIX Interim Fix** analysis. Remove interim fixes with the **Uninstall All Interim Fixes** task.

If no locked filesets are identified and a local NFS repository is used, the following command can identify filesets that are missing from the `.toc` file of the local repository. In the following example, the version adds zeros to maintain the format of xx.xx.xxxx.xxxx.

```
grep -n "<Package Name> <Package Version>" /path/to/.toc
```

An example command includes the following format:

```
grep -n "perfagent.tools 06.01.0004.0011" /AIX/Repo/OS_6100/.toc
```

If filesets are missing from the `.toc` file, but the fileset exists in the repository, you can rebuild the `.toc` file by using the **Generate Fileset Repository TOC File** task. If files are missing, run the AIX Download Cacher Tool through the **Run Download Cacher - AIX** task. When prompted, specify the path to the repository. For more information about using the AIX Download Cacher, see http://www-01.ibm.com/support/docview.wss?uid=swg21506031.

Chapter 4. Network Installation Management (NIM) integration

Endpoint Manager provides an alternative solution for updating and managing multiple AIX system through Network Installation Management (NIM). Endpoint Manager supports the NIM patch management features in this release.

You can use NIM from the Endpoint Manager console to remotely manage AIX installations and updates in multiple AIX systems in your environment.

For more information about NIM, see the *IBM AIX Information Center*. The AIX information centers are version-specific. To see the list of available AIX information centers, see the IBM AIX resources at: http://www-03.ibm.com/systems/power/software/aix/resources.html

The **Patches for AIX** site provides dashboards that you can use to install, configure, and manage your NIM environment. For more information about these dashboard, see “NIM dashboards overview.”

NIM dashboards overview

IBM Endpoint Manager provides dashboards to install, configure, and manage your NIM environment.

You must subscribe to the **Patches for AIX** site to access these dashboards from the **Dashboards** node of the said site.

NIM Installation and Setup Dashboard

Use the NIM Installation and Setup Dashboard to install NIM filesets and to configure the NIM master and the NIM client.

You can use the dashboard to complete the following NIM tasks:

- Install the filesets that are required to create a NIM master or a NIM client.
- Configure the NIM master.
- Initialize the NIM master and the NIM client.
- Define and configure the NIM resources.
- Define the NIM clients to the NIM master.

NIM Management Dashboard

The NIM Management Dashboard is designed primarily to help you use an existing NIM environment. The dashboard helps you to create content to update the NIM lpp_source resources, which can then be used to update the SPOT resources, NIM master, and NIM client systems.

The dashboard also provides a small collection of general NIM maintenance tasks that you can use. The following tasks are available:

- Rebuild the NIM master configuration file.
- Rebuild the NIM client configuration file.
- Synchronize the date and time of the NIM master and NIM client.

- Enable or disable the push permissions on the NIM masters.

Note: The primary NIM operations that are generated from this dashboard have their standard output (STDOUT) and standard error output (STDERR) stored in a text file. The time stamp and ID of the action that is running the command is also stored in the text file. These files can be found at `<Path to Endpoint Manager Data Directory>__NIM_Logs/NIM_Operations_<yyyymmdd>.log`. For example, `/var/opt/BESClient/__BESData/__NIM_Logs/NIM_Operations_20130520.log`.

Setting up a new NIM environment

To best utilize the NIM integration features, use the NIM Installation and Setup Dashboard when you install the NIM master, NIM clients, and NIM lpp_source resource.

Set up a new NIM environment through the NIM Installation and Setup Dashboard in four steps.

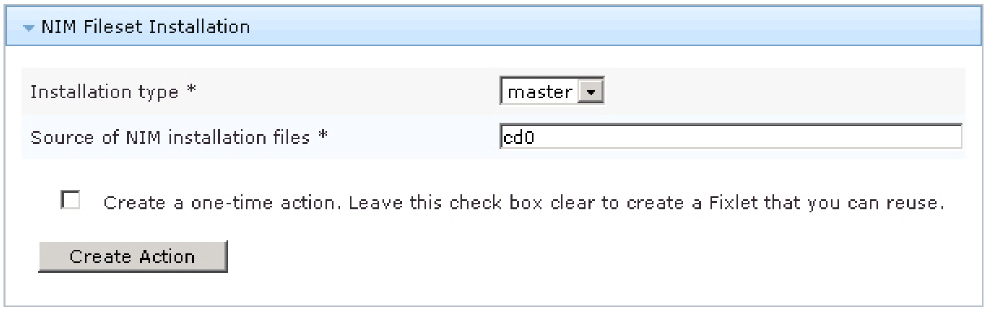
1. Install NIM filesets.
2. Configure the NIM master.
3. Configure the NIM client.
4. Initialize the NIM client.

Installing NIM filesets

Use the NIM Installation and Setup Dashboard to install the required filesets for the NIM master or the NIM client.

- Most recent AIX systems, by default, have the `bos.sysmgt.nim.client` fileset installed. No additional installations are required to establish a NIM client.
- The NIM master and client filesets are available from the `bos.sysmgt` Licensed Program Product source, which is provided in the AIX installation media.

1. From the Endpoint Manager console, click **All Patch Management** > **Dashboards** > **Patches for AIX** > **NIM Installation and Setup Dashboard**.
2. Click **NIM Fileset Installation** to display the fields under that header.



NIM Fileset Installation

Installation type *	master
Source of NIM installation files *	cd0

□ Create a one-time action. Leave this check box clear to create a Fixlet that you can reuse.

Figure 18. NIM fileset installation

3. Select the installation type.
4. Enter the source of the NIM installation files. For example, cd0

   You can use the NIM installation files from CD devices, local directories, or NFS sources.

   Note: The dashboard automatically detects the installation source type, whether the entered value is from a CD device, NFS source, or local directory.

Note: If an NFS path is used as the source of the NIM installation files, an attempt to generate a new `.toc` file is made by using the `inutoc` command. If the remote path is in a read-only mode, the directory must be in a valid state for use by the `installp` command before the files can be used.

5. Optional: Select the check box to create a one-time action rather than to create a reusable Fixlet.
6. Click **Create Action**.
7. Deploy the action.

The following filesets are installed on the target AIX systems:

NIM master

- `bos.sysmgt.nim.master`
- `bos.sysmgt.nim.client`
- `bos.sysmgt.nim.spot`

NIM client

`bos.sysmgt.nim.client`

Configuring the NIM master

After you install the NIM master filesets, use the NIM Installation and Setup Dashboard to initialize the NIM master and set up the NIM resources. At initialization, a NIM master is designated with permissions to run commands remotely on the NIM clients that are registered to that NIM master.

- Ensure that you have sufficient disk space to store the lpp_source resources.
- The NIM master must be at the same operating system, technology level, and service pack levels, or higher, as the NIM clients in the NIM environment.
- Only one NIM master can exist within a NIM environment.
- NIM masters cannot be clients to any other NIM master.
- You can use any of the available methods to set up the NIM master and NIM resources:

  Manual Setup

  This method provides the greatest control over initializing the NIM environment, environment options, and NIM resources. It does not use any setup automation scripts on AIX.

  If you want to have the greatest control over the NIM environment setup options, use this method. You might also want to use this method when the EZNIM or Basic Setup methods fail because of automation errors.

  EZNIM

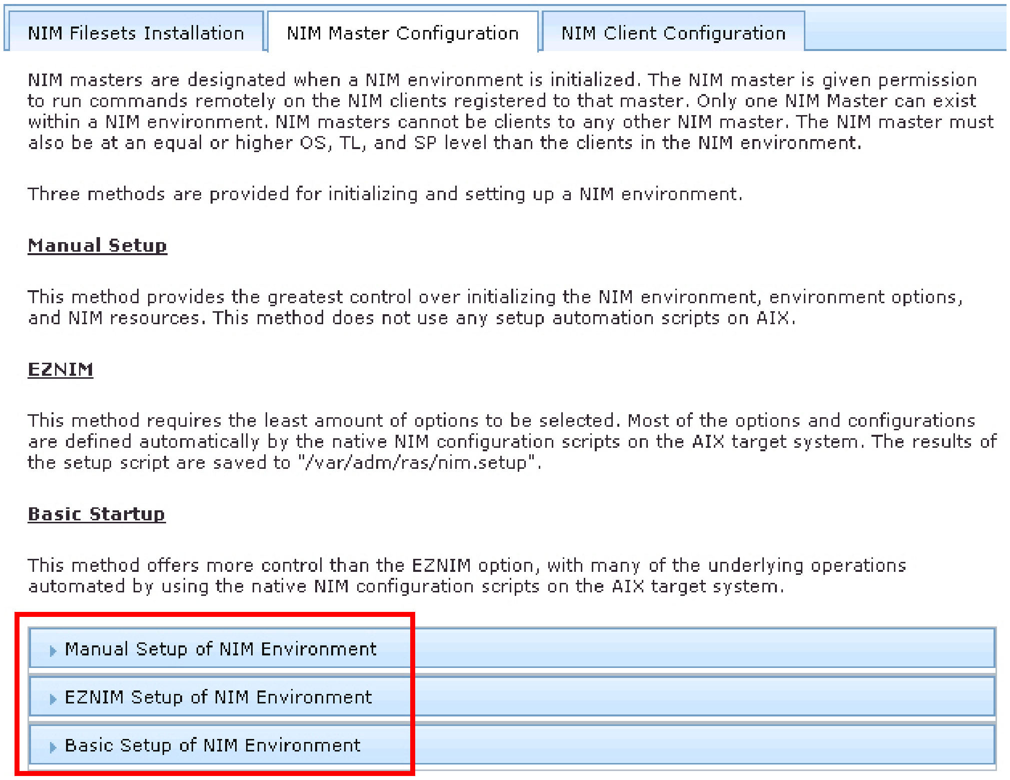
  This method requires the least number of options to be selected. Most of the options and configurations are defined automatically by the native NIM configuration scripts on the AIX target system. The results of the setup script are saved to `/var/adm/ras/nim.setup`.

  This option automatically attempts to install the NIM master filesets if they are missing.

  Basic Setup

  This method offers more control than the EZNIM option. Many of the underlying operations are automated by using the native NIM configuration scripts on the AIX target system.

1. From the Endpoint Manager console, click **All Patch Management** > **Dashboards** > **Patches for AIX** > **NIM Installation and Setup Dashboard**.
2. Click **NIM Master Configuration**.
3. Select a method to configure the NIM master and NIM resource.



NIM masters are designated when a NIM environment is initialized. The NIM master is given permission to run commands remotely on the NIM clients registered to that master. Only one NIM Master can exist within a NIM environment. NIM masters cannot be clients to any other NIM master. The NIM master must also be at an equal or higher OS, TL, and SP level than the clients in the NIM environment.

Three methods are provided for initializing and setting up a NIM environment.

Manual Setup

This method provides the greatest control over initializing the NIM environment, environment options, and NIM resources. This method does not use any setup automation scripts on AIX.

EZNIM

This method requires the least amount of options to be selected. Most of the options and configurations are defined automatically by the native NIM configuration scripts on the AIX target system. The results of the setup script are saved to "/var/adm/ras/nim.setup".

Basic Startup

This method offers more control than the EZNIM option, with many of the underlying operations automated by using the native NIM configuration scripts on the AIX target system.

Manual Setup of NIM Environment
EZNIM Setup of NIM Environment
Basic Setup of NIM Environment

Figure 19. NIM master configuration

- To use the manual setup method, complete the following steps:
  a. Click **Manual Setup of NIM Environment**.
  b. Install the NIM master filesets, if you did not yet do so.
  c. Enter the information under the Initialize NIM Master Options section.
  d. Configure the NIM resources that you want to use.
     – lpp_source resource
     – SPOT resource
     – root resource
     – dump resource
     – paging resource
     – home resource
     – share_home resource
     – tmp resource

     Note: The lpp_source and SPOT resources are, by default, selected to be used.
- To use the EZNIM setup method, complete the following steps:
  a. Click **EZNIM Setup of NIM Environment**.

b. Enter the software source to initialize the NIM environment. The source can be from a CD device, NFS source, or local directory. For example, `cd0`

c. Enter the volume group for the NIM resources. For example, `rootvg`

d. Enter the file system for the NIM resources. For example, `/export/nim/eznim`

e. Optional: Select any of the available options.

- To use the basic setup method, complete the following steps:
  a. Click **Basic Setup of NIM Environment**.
  b. Enter the primary network interface for the NIM master. For example, `en0`
  c. Enter the input device for the installation images. For example, `cd0`
  d. Optional: Select the options from the appropriate drop-down lists for the following actions:
     - Remove all newly-added NIM definitions and filesystems when the basic setup operation fails.
     - Define the NIM system bundles and NIM bosinst_data.
     - Add a prefix level to the resource name.
     - Create diskless or dataless machine resources.
  e. Configure the options for the lpp_source resource.
  f. Configure the options SPOT resource.

For more information about the NIM parameters, see the *IBM AIX information center*.

Note: The AIX information centers are version-specific. To see the list of available AIX information centers, see the IBM AIX resources at: http://www-03.ibm.com/systems/power/software/aix/resources.html.

4. Optional: Select the check box to create a one-time action rather than to create a reusable Fixlet.
5. Click **Create Action**.
6. Deploy the action.

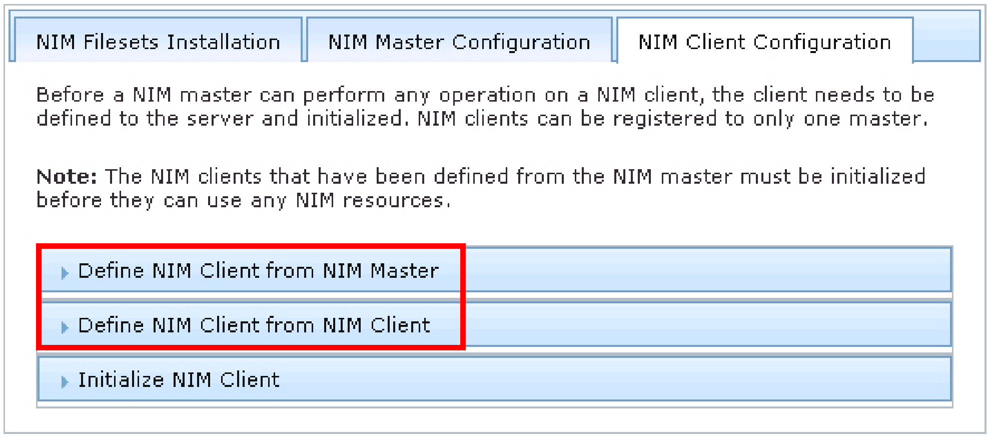
Configuring the NIM client

Use the NIM Installation and Setup Dashboard to define a NIM client to the NIM master. The NIM master cannot take any operation on a NIM client if the NIM client is not defined.

- Ensure that the required NIM client filesets are installed.
- When you define a NIM client to the NIM master, the NIM master must be able to resolve the host name of the NIM client and vice versa. If the host name is not resolved, you get only limited NIM functions.
- There are two ways to define NIM clients to a NIM master. The NIM master can define NIM clients to itself or, if allowed by the NIM environment, the NIM client can define itself to the NIM master.
- When you define a NIM client through the NIM master, the NIM master does not contact the NIM client. As a result the NIM client must be initialized separately. See “Initializing the NIM client” on page 33.
- A NIM client can be registered to only one NIM master at a time.
- NIM masters cannot be clients to any other NIM master.

1. From the Endpoint Manager console, click **All Patch Management** > **Dashboards** > **Patches for AIX** > **NIM Installation and Setup Dashboard**.

2. Click **NIM Client Configuration**.
3. Select the method that you want to use to define the NIM client to the NIM master.



NIM Filesets Installation
NIM Master Configuration
NIM Client Configuration

Before a NIM master can perform any operation on a NIM client, the client needs to be defined to the server and initialized. NIM clients can be registered to only one master.

Note: The NIM clients that have been defined from the NIM master must be initialized before they can use any NIM resources.

Define NIM Client from NIM Master
Define NIM Client from NIM Client
Initialize NIM Client

Figure 20. Ways to define the NIM client the NIM master

- If you want to define the NIM client from a NIM master, complete the following steps:
  a. Click **Define NIM Client from NIM Master**.
  b. Enter the machine name. For example, `clientname`
  c. Enter the machine type. For example, `stand-alone`
  d. Enter the hardware platform type. For example, `chrp`
  e. Select the kernel to use to boot the network.
  f. Select the communication protocol that is used by the NIM client.
  g. Enter the required information for the primary network installation interface:
     – NIM network name. For example, `master_net`
     – Host name. For example, `client_hostname`
     – Cable type (for Ethernet only)
  h. Optional: Enter extra network information:
     – Network speed setting
     – Network duplex setting
     – Network adapter hardware address. For example, `0`
     – Network adapter logical device name

     Note: You can also create a NIM network for the NIM client. If you choose to do so, you must provide the Subnet mask, default gateway that is used by the machine and master, network type, and Ethernet type.
  i. Optional: Enter the IPL ROM emulation device.
  j. Optional: Enter the CPU ID.
  k. Optional: Enter the machine group.
  l. Optional: Enter any comments.
- If you want to define a new NIM client to the NIM environment from another NIM client, complete the following steps:
  a. Click **Define NIM Client from NIM Client**.

   b. Enter the machine name. For example, `clientname`
   c. Enter the primary network installation interface. For example, `en0`
   d. Enter the host name of the network installation master. For example, `master_hostname`
   e. Optional: Enter the hardware platform type. For example, `chrp`
   f. Optional: Select the kernel to use to boot the network.
   g. Optional: Select the communication protocol that is used by the NIM client.
   h. Optional: Enter any comments.

   For more information about the NIM parameters, see the *IBM AIX information center*.

   Note: The AIX information centers are version-specific. To see the list of available AIX information centers, see the IBM AIX resources at: http://www-03.ibm.com/systems/power/software/aix/resources.html.

4. Optional: Select the check box to create a one-time action rather than to create a reusable Fixlet.
5. Click **Create Action**.
6. Deploy the action. The created action targets a NIM master and defines clients to that target system.

You must initialize the NIM clients that were defined through the NIM master so that the NIM clients can use the NIM resources. See "Initializing the NIM client."

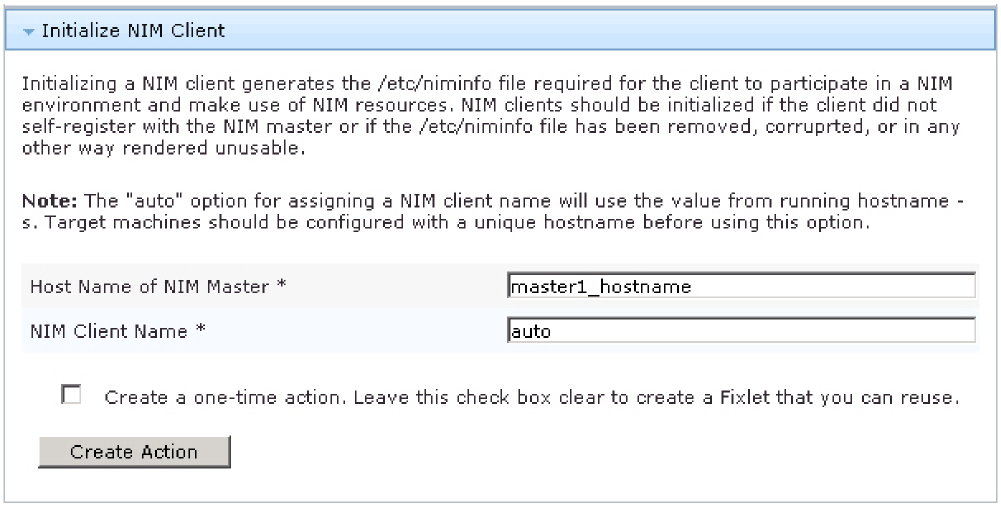
Initializing the NIM client

Initialize a NIM client to generate the `/etc/niminfo` file that is required to work in a NIM environment and to use the NIM resources.

You might need to initialize the NIM client for the following reasons:

- The NIM client failed to register itself to the NIM master.
- The `/etc/niminfo` file on the NIM client is removed, corrupted, or in any other way rendered unusable.

1. From the Endpoint Manager console, click **All Patch Management** > **Dashboards** > **Patches for AIX** > **NIM Installation and Setup Dashboard**.
2. Click **NIM Client Configuration**.
3. Click **Initialize NIM Client** to display the fields under that header.



Initialize NIM Client

Initializing a NIM client generates the /etc/niminfo file required for the client to participate in a NIM environment and make use of NIM resources. NIM clients should be initialized if the client did not self-register with the NIM master or if the /etc/niminfo file has been removed, corruprted, or in any other way rendered unusable.

Note: The "auto" option for assigning a NIM client name will use the value from running hostname -s. Target machines should be configured with a unique hostname before using this option.

Host Name of NIM Master *	master1_hostname
NIM Client Name *	auto

□ Create a one-time action. Leave this check box clear to create a Fixlet that you can reuse.

Figure 21. NIM client initialization

4. Enter the host name of the NIM master. For example, `master1_hostname`
5. Enter the name of the NIM client that is defined on the NIM master. For example, `clientname`

   Note: To assign the NIM client name with the value that results from running the `hostname -s` command, enter `auto` as the NIM Client Name. Before you use the auto option, the target machines must be configured with a unique host name.
6. Optional: Select the check box to create a one-time action rather than to create a reusable Fixlet.
7. Click **Create Action**.
8. Deploy the action.

Updating existing clients and resources

To use an existing NIM environment, update the clients and resources through the NIM Management Dashboard.

The NIM Management Dashboard allows all updates to be performed together in a single action or independently as separate actions.

1. Update the NIM lpp_source resource.
2. Update the NIM master.
3. Update the NIM clients.

Updating the NIM lpp_source resource

The lpp_source resource is a directory with a collection of filesets that are used for the NIM update actions. Update the lpp_source resource to make the new installation files available to the NIM master and NIM clients.

New filesets must be downloaded before beginning the update action. New filesets can be downloaded from any of the following tools that are provided by IBM:

- AIX Download Cacher
- Fix Central
- Service Update Management Assistant (SUMA)

NIM resources cannot be modified while they are allocated to NIM machines. The generated actions deallocate the resource from all clients.

1. From the Endpoint Manager console, click **All Patch Management** > **Dashboards** > **Patches for AIX** > **NIM Management Dashboard**.
2. Click **NIM Update Operations**.
3. Click **Update NIM Components from NIM Master**.
4. Configure the settings according to the actions that you want to include in the generated Fixlet or one-time action.
5. Select to add packages to the existing NIM lpp_source resource from the appropriate option.
6. Enter the lpp_source resource name. For example, `lpp_source1`
7. Enter the source of the update packages. The packages can be from a CD device, local directory, or NFS path. For example, `cd0`
8. Optional: Enter the name of the packages. For example, `all`
9. Optional: Select whether to use lppmgr to remove the filtered images from the lpp_source resource, and set the lppmgr filter options.
10. Optional: Select the check box to create a one-time action rather than to create a reusable Fixlet.
11. Click **Create Action**.
12. Deploy the action.

Updating NIM SPOT resource

The NIM Management Dashboard helps you to create Fixlets that you can use to update the NIM SPOT resource through the NIM master.

- New filesets must be downloaded before beginning the update action. New filesets can be downloaded from any of the following tools that are provided by IBM:
  - AIX Download Cacher
  - Fix Central
  - Service Update Management Assistant (SUMA)
- NIM resources cannot be modified while they are allocated to NIM machines. The generated actions deallocate the resource from all clients.
- NIM client updates are initiated by the NIM master and do not directly report back to the Endpoint Manager console.

1. From the Endpoint Manager console, click **All Patch Management** > **Dashboards** > **Patches for AIX** > **NIM Management Dashboard**.
2. Click **NIM Update Operations**.
3. Click **Update NIM Components from NIM Master**.
4. Configure the settings according to the actions that you want to include in the generated Fixlet or one-time action.

   Note: If you are adding new files, you must first update the lpp_source resource to be able to use it to update the SPOT resource, NIM master, and NIM client systems.

   Note: If you are updating to a new technology or service pack level, the NIM master must be updated before or at the same time as the NIM clients.
5. Select to update the SPOT resource from the appropriate option.
6. Enter the lpp_source resource where the installation images are located.

7. Enter the names of the fixes that are to be installed.

   Tip: To include all the fixes that are in the source location, enter `update_all`
8. Optional: Select the check box to create a one-time action rather than to create a reusable Fixlet.
9. Click **Create Action**.
10. Deploy the action.

Updating the NIM master

The operating system of the NIM master must always be at the same or later version than all NIM clients it manages. Attempts to update NIM clients to a version later than the NIM master would fail.

If you are adding new files, you must first update the lpp_source resource to be able to use it to update NIM master.

1. From the Endpoint Manager console, click **All Patch Management** > **Dashboards** > **Patches for AIX** > **NIM Management Dashboard**.
2. Click **NIM Update Operations**.
3. Click **Update NIM Components from NIM Master**.
4. Configure the settings according to the actions that you want to include in the generated Fixlet or one-time action.
5. Select to update the NIM master from the appropriate option.
6. Enter the lpp_source resource where the installation images are located.
7. Optional: If you want to set the updated filesets to a committed state, select the appropriate option.

   Note: Filesets that are in the Applied state must be committed after confirmation to free disk space.
8. Optional: If you want to restart the system after the update, select the appropriate option.
9. Optional: Select the check box to create a one-time action rather than to create a reusable Fixlet.
10. Click **Create Action**.
11. Deploy the action.

Updating the NIM clients

Updating the NIM Client installs the latest filesets from the specified lpp_source resource on the NIM client.

- If you are adding new files, you must first update the lpp_source resource to be able to use it to update NIM client systems.
- Push updates to NIM clients from the NIM master. This method for updating client initiates the update procedure from the NIM master. Push permissions must be enabled on the NIM clients or this action fails. For more information, see “Enabling or disabling push permissions” on page 39.

1. From the Endpoint Manager console, click **All Patch Management** > **Dashboards** > **Patches for AIX** > **NIM Management Dashboard**.
2. Click **NIM Update Operations**.
3. Click **Update NIM Components from NIM Master**.
4. Configure the settings according to the actions that you want to include in the generated Fixlet or one-time action.

5. Select to update the NIM client from the appropriate option.
6. Enter the names of the NIM clients that you want to update. To include all the NIM clients in your NIM environment, enter `all`.

   Tip: To include all the NIM clients in your NIM environment, enter `all`.
7. Enter the lpp_source resource where the installation images are located.
8. Optional: If you want to set the updated filesets to a committed state, select the appropriate option.

   Note: Filesets that are in the Applied state must be committed after confirmation to free disk space.
9. Optional: If you want to restart the system after the update, select the appropriate option.
10. Optional: Select the check box to create a one-time action rather than to create a reusable Fixlet.
11. Click **Create Action**.
12. Deploy the action.

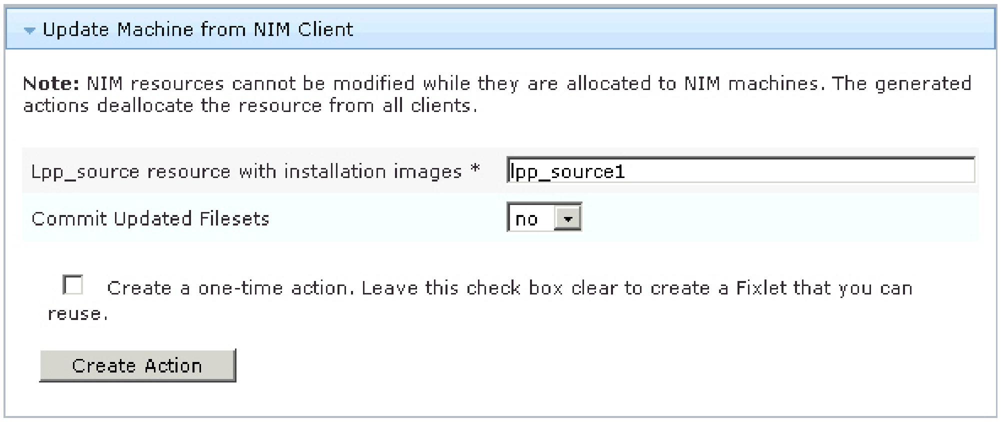
Optionally, NIM clients can initiate the installation process and pull the updates from the NIM master. Details on this process can be found in “Updating a system from a NIM client.”

Updating a system from a NIM client

The NIM Management Dashboard helps you to create Fixlets that you can use to update an AIX system from a NIM client.

NIM machines can have only one lpp_source resource that is allocated to them at a time. The generated action deallocates any existing lpp_source resource allocations.

1. From the Endpoint Manager console, click **All Patch Management** > **Dashboards** > **Patches for AIX** > **NIM Management Dashboard**.
2. Click **NIM Update Operations**.
3. Click **Update Machine from NIM Client**.
4. Enter the lpp_source resource where the installation images are located.


Update Machine from NIM Client

Note: NIM resources cannot be modified while they are allocated to NIM machines. The generated actions deallocate the resource from all clients.

Lpp_source resource with installation images * lpp_source1

Commit Updated Filesets no

□ Create a one-time action. Leave this check box clear to create a Fixlet that you can reuse.

Figure 22. Update a system from a NIM client

5. Optional: If you want to set the updated filesets to a committed state, select the appropriate option.

Note: Filesets that are in the Applied state must be committed after confirmation to free disk space.

6. Optional: If you want to restart the system after the update, select the appropriate option.
7. Optional: Select the check box to create a one-time action rather than to create a reusable Fixlet.
8. Click **Create Action**.
9. Deploy the action.

Rebuilding the NIM master configuration file

The NIM Management Dashboard provides a task to rebuild the `/etc/niminfo` file on the targeted NIM master servers.

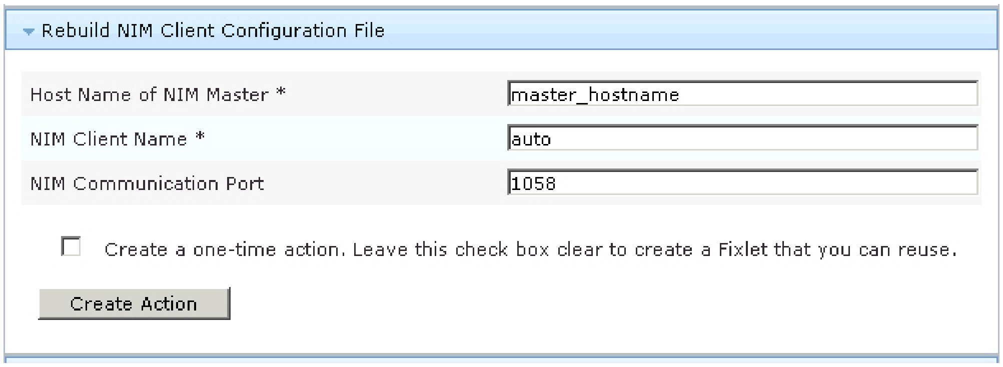
1. From the Endpoint Manager console, click **All Patch Management** > **Dashboards** > **Patches for AIX** > **NIM Management Dashboard**.
2. Click **General NIM Management Operations**.
3. Click **Rebuild NIM Master Configuration File**.
4. Click **NIM Master: Rebuild niminfo Config File**.
5. Deploy the action.

Rebuilding the NIM client configuration file

The NIM Management Dashboard helps you create a Fixlet to connect to the NIM master to rebuild the `/etc/niminfo` file on a NIM client.

The NIM client must be configured on the target NIM master. If the NIM client is not configured on the target NIM master, the `/etc/niminfo` file is not generated.

1. From the Endpoint Manager console, click **All Patch Management** > **Dashboards** > **Patches for AIX** > **NIM Management Dashboard**.
2. Click **General NIM Management Operations**.
3. Click **Rebuild NIM Client Configuration File**.
4. Enter the host name of the NIM master.



Rebuild NIM Client Configuration File

Host Name of NIM Master *	master_hostname
NIM Client Name *	auto
NIM Communication Port	1058

□ Create a one-time action. Leave this check box clear to create a Fixlet that you can reuse.

Figure 23. Rebuild the NIM client configuration file

5. Enter the NIM client name.

Note: To assign the NIM client name with the value that results from running the `hostname -s` command, enter `auto` as the NIM Client Name. Before you use the auto option, the target machines must be configured with a unique host name.

6. Optional: Enter the NIM communication port.
7. Optional: Select the check box to create a one-time action rather than to create a reusable Fixlet.
8. Click **Create Action**.
9. Deploy the action.

Synchronizing the date and time

The NIM Management Dashboard provides a task to synchronize the date and time on the targeted NIM client systems with the NIM master that they are registered to.

1. From the Endpoint Manager console, click **All Patch Management** > **Dashboards** > **Patches for AIX** > **NIM Management Dashboard**.
2. Click **NIM Update Operations**.
3. Click **General NIM Management Operations**.
4. Click **Synchronize Date and Time**.
5. Click **NIM Client: Sync Date and Time with NIM Master**.
6. Deploy the action.

Enabling or disabling push permissions

The NIM Management Dashboard provides tasks that you can use to enable the NIM master to remotely run commands on the NIM client.

The permission option is set on a per-client basis. If push permissions are disabled, the NIM client can still use the allocated NIM resources, but the individual clients must start all commands.

1. From the Endpoint Manager console, click **All Patch Management** > **Dashboards** > **Patches for AIX** > **NIM Management Dashboard**.
2. Click **NIM Update Operations**.
3. Click **General NIM Management Operations**.
4. Click **Enable/Disable Push Permissions**.
5. Click the available tasks to enable or disable the NIM master push permissions on the target NIM client systems.
6. Deploy the action.

Adding new resources to an existing NIM environment

Use the NIM Master Configuration options of the NIM Installation and Setup Dashboard to add new resources to an existing NIM environment.

If new filesets are to be added to a new lpp_source resource, those filesets must be downloaded prior to adding the new resource. New filesets must be downloaded before beginning the update action. New filesets can be downloaded from any of the following tools that are provided by IBM:

- AIX Download Cacher
- Fix Central
- Service Update Management Assistant (SUMA)

Only one instance of a specified resource type, such as lpp_source, can be added per action. Separate actions are required to add multiple instances of a specified resource type.

1. From the Endpoint Manager console, click **All Patch Management** > **Dashboards** > **Patches for AIX** > **NIM Installation and Setup Dashboard**.
2. Click **NIM Master Configuration**.
3. Click **Manual Setup of NIM Environment**.
4. Select the resource to be added.
5. Set the options for the selected resource.
6. Optional: Select the check box to create a one-time action rather than to create a reusable Fixlet.
7. Click **Create Action**.
8. Deploy the action.

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
- IBM Endpoint Manager Support site
- IBM Endpoint Manager wiki
- Knowledge Base
- Forums and Communities

Appendix B. Frequently asked questions

The questions and answers in this section can help you to better understand Patch Management for AIX.

Why would a patch complete successfully, but ultimately fail?

Under specific circumstances, a patch is successfully applied but the relevance conditions indicate that it is still needed in your deployment. Check to see if there are any special circumstances that are associated with the patch, or contact IBM Software Support.

If a patch fails to install, what should I do?

Ensure that you applied the patch to the correct computers or manually download the patch.

Can I update a single fileset instead of performing full technology level or service pack updates?

Updates are developed and tested as bundles, and updating individual filesets might cause unexpected results. However, if you would still like to update individual filesets, you can do so by downloading the .bff file that you want to deploy and using the fileset option of the AIX Deployment Wizard to generate the necessary Fixlet.

Why did the update of my AIX system fail?

There are several reasons why an update can fail. The best place to start investigating is with the log files saved in /var/adm/ras.

Below are some of the more common reasons for failed updates.

Problem: Insufficient free space in the BES Data Directory (typically `/var/opt/BESClient/__Data/`)

Solution: Free space or expand the current partition using the **`chfs -a`** command

Problem: Warning that filesets are locked or in EFIXLOCKED state

Solution: Filesets can be locked as the result of installed Interim Fixes. Interim Fixes can be viewed either by using the "AIX Interim Fixes" Analysis or by running the command "emgr -l". It is recommended that all Interim Fixes be removed prior to deploying updates. Interim FIxes can be removed by using the "AIX Interim Fix Management Wizard".

Problem: Error: "Installation failed due to BUILDDATE requisite failure"

Solution: If the build date of an installed fileset is more recent than the build date of the fileset being installed a warning is displayed and the entire update action might fail. To correct this, upgrade to a more recent technology level or service pack.

Why do NFS actions set the "nfs_use_reserved_ports" and "portchecker" values to 1?

Some Linux operating systems use reserved ports that are less than 1024. These settings are temporarily changed to a value of 1 to avoid failures in connecting to remote servers that use these ports.

What are the requirements for an AIX repository?

NFS installations use the Table of Contents (`.toc`) file in the repository to match packages with their corresponding file names. Use the "Generate Fileset Repository TOC File" task to generate a current `.toc` file.

Are there tools available to help build a repository?

Yes. The AIX Download Cacher provides two methods for building a repository:

`--no-archive`
Use this parameter to download files, without creating an archive `.aix` file, to the directory specified by the `--dir` parameter.

`--repo <dir>`
Use this parameter to save a copy of individual downloaded files to the repository specified by the **`--repo`** parameter.

Note: If the **`--repo`** parameter is used with the **`--no-archive`** parameter, the fix pack files are either:

- Copied from the repo directory to the output directory, which is specified by **`--dir`** parameter.
- Downloaded from the internet and saved to both the output directory and the repo directory.

Will any files that are missing from the AIX repository be automatically added during an NFS installation?

No. For NFS installation actions, all required files must exist in the specified NFS location.

How do I verify if the download plug-in was registered correctly?

Run a Fixlet with an action task to verify if the download plug-in is registered correctly. Verify that the patch download is successful. Otherwise, you might need to unregister the download plug-in and register it again.

How do I register a download plug-in? Do I use the register download plug-in task or the Manage Download Plug-in dashboard?

To register a download plug-in, you must use the Manage Download Plug-in dashboard in the Patching Support site. Existing register download plug-in tasks are being deprecated. To learn more about plug-in registration, see “Registering the AIX download plug-in” on page 5.

Note: You must also use the Manage Download Plug-in dashboard to unregister, configure, and upgrade download plug-ins. The existing unregister and edit download plug-in tasks are being deprecated. For more information about the dashboard, see the section on Manage Download Plug-ins dashboard in the IBM Endpoint Manager Information Center.

I was expecting the password to be obfuscated, but it is still in clear text. Why is that?

Check if your download plug-in version is earlier than 2.0. If so, you are still using an old version of the download plug-in that stores credentials in clear text. To encrypt credentials, upgrade your download plug-in to version 2.0 or later from the Manage Download plug-ins dashboard in the Patching Support site.

Where can I find the AIX Patching log files?

Here is a list of the log files and their locations:

- AIX Download Cacher: Default log directory of the Endpoint Manager client on the target system.
- AIX Download Plug-in: `AIXProtocol/logs` directory of the default `DownloadPlugin` directory on the Endpoint Manager Server (For example: `C:\Program Files (x86)\BigFix Enterprise\BES Server\DownloadPlugins\AIXProtocol\logs`).
- Installation Logs: `/var/adm/ras/` on the target system. Logs are unique for each operating system level.

When should I create a repository for a single fix pack?

Create a repository for a single fix pack when you are using the technology level and service pack updates using the NFS actions. Issues might occur when the installer automatically attempts to install the latest version of any fileset that it finds in the source directory. For example, if you want to update a system to a specific technology level and service pack level, you must store it in its own isolated location to ensure that is not overridden by later versions.

What are the requirements for using an existing repository of filesets that is accessible on NFS mount?

All fix pack files must be in the NFS directory with a current `.toc` file. Each fix pack must be stored in its own dedicated share space.

How are the fix packs installed when I deploy technology level or service pack updates?

Fix packs are installed in an "applied" state that can later be rejected, if needed. Applied filesets must be committed after they are verified. They can be committed by using the **Commit Applied Filesets** task. Technology level updates cannot be rejected; attempting to do so might produce unexpected results.

Why did the OS level of my new NIM master change after I installed the NIM filesets?

The OS level is determined by comparing a list of installed filesets with a list of known APARs. When you install new filesets, the target system might become applicable to APARs that were not previously applicable. The OS level is changed to reflect these newly-applicable APARs.

What's the difference between installing the NIM master filesets from the "Install NIM Filesets" and "NIM Master Configuration" tabs?

There is no difference. The installation of the NIM master filesets is added to the "NIM Master Configuration" tab to simplify and consolidate the process of setting up a NIM master.

What happens if I previously installed the master filesets then chooses to install the master filesets during the manual NIM Master configuration?

The second installation attempt detects that filesets are already installed and exits without doing anything. However, if the second installation has a later version of the filesets, then an update is performed.

Can I configure a NIM master outside the dashboard and then configure the client from the dashboard?

Yes, this is possible. If you have preexisting NIM environments, you generate NIM content to manage existing clients or add new clients.

What is an IBM ID? Do I need one?

An IBM ID is a free, single ID and password that you can use across the ibm.com domain. Updates to operating systems and other software products are entitled only to customers under an applicable warranty or support agreement. To this end, an IBM ID is required for the AIX download plug-in to successfully download updates.

What is an IBM Customer Number (ICN)?

ICNs are unique numbers that are assigned to customer agreements with IBM, including software maintenance agreements.

Why do I need to link my IBM ID to an IBM Customer Number (ICN)?

For a list of benefits of linking your ICNs and your IBM ID, see the announcement at http://www-01.ibm.com/support/icn/.

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.

Licensees 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 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.

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-C45

Printed in USA