

IBM Endpoint Manager

OS Deployment V3.6 User's Guide

IBM

IBM Endpoint Manager

OS Deployment V3.6 User's Guide



Note

Before using this information and the product it supports, read the information in "Notices" on page 139.

Contents

Chapter 1. Product overview 1

Understanding OS Deployment components and terms	1
What's new in version 3.6	6
Features added in previous versions	7
System requirements	10
Process overview	12
Enable OS Deployment and Bare Metal Imaging site	13
Navigation tree overview	13

Chapter 2. Configuring the OS Deployment Environment. 17

Install BES Server Plugin Service	18
Install Upload Maintenance Service	18
Upgrade Upload Maintenance Service	19
Update Server Whitelist for OS Deployment	20
Managing the Linux Image provider	20
Deploying the Management Extender for Bare Metal Targets	21
Activating Analyses	23
SSL Encryption Analysis for OS Deployment	23
OS Deployment Server Information	24
Re-image Failure Information	24
Hardware Information	25
Bundle Creator Machine Information	25
Bare Metal Target information	25
Health Checks Dashboard	26
Enable Encryption for Clients	27
Verifying Secure Hash Algorithm (SHA-256) readiness	28

Chapter 3. Managing MDT Bundles and Deployment Media for Windows targets 29

Bundle and Media Manager Dashboard	29
Installing MDT Bundle Creators	30
Creating MDT Bundles	31
Creating Windows Deployment Media	32
Creating and managing MDT bundles manually	37
MDT Bundle creation process	38
Prerequisites	39
MDT Bundle Creation Options	42
Upload MDT Bundle Dashboard	45
Troubleshooting MDT Bundle errors	46

Chapter 4. Managing Images and Drivers. 49

Preparing drivers for Windows deployments	49
Importing and managing drivers for Windows deployments	50
Managing Windows driver bindings	54
Capturing Windows Images	56
Specify SMB Share Information	58
Choosing Capture Options	59
Importing Windows and Linux images	60

Chapter 5. Re-imaging 65

Re-imaging Windows Systems	66
Deploy Image to Computer	68
Re-imaging Linux Systems	81
Managing templates	86

Chapter 6. Bare Metal deployments . . . 89

Managing Bare Metal OS Deployment Servers	89
Ports used by the Bare Metal OS Deployment Server	92
Configuring the DHCP server	92
Creating bare metal profiles	94
Creating Bare Metal Profiles for Windows Images	95
Creating Bare Metal Profiles for Linux Images	102
Working with Bare Metal Profiles	104
Managing Bare Metal Targets	105
Booting Windows targets without using PXE	106
Deploying a bare metal profile from the target binding menu	106
Deploying bare metal profiles based on target properties	108
Deploying a bare metal profile from the IBM Endpoint Manager console	111
Wiping target disks	112

Chapter 7. Creating and deploying scripting environments 113

Prerequisites	114
Creating a scripting environment	114
Managing scripting environments	116
Deploying scripting environments to Bare Metal Targets	116
Troubleshooting scripting environment problems	117

Chapter 8. Maintenance and troubleshooting 119

Deployment Activity Dashboard	119
Maintenance and Configuration tasks	122
Troubleshooting	122
Problems and limitations	125
CPU usage reaches 100% during installation or upgrade of a Bare Metal Server	125
Duplicate client computer entry in the Server database after a Linux re-image	125
Re-image install on RedHat Enterprise Linux (RHEL) 7 stops during boot sequence	126
Login prompt not displayed on RedHat Enterprise Linux (RHEL) 7 after Bare Metal deployment	126
Copy image settings error on manual driver bindings	126

**Appendix A. Setting up OS
Deployment in an air-gapped network . 129**

**Appendix B. Bare Metal OS
Provisioning using RAD Profiles . . . 133**

**Appendix C. Frequently asked
questions 135**

Appendix D. Support 137

Notices 139
Programming interface information 141

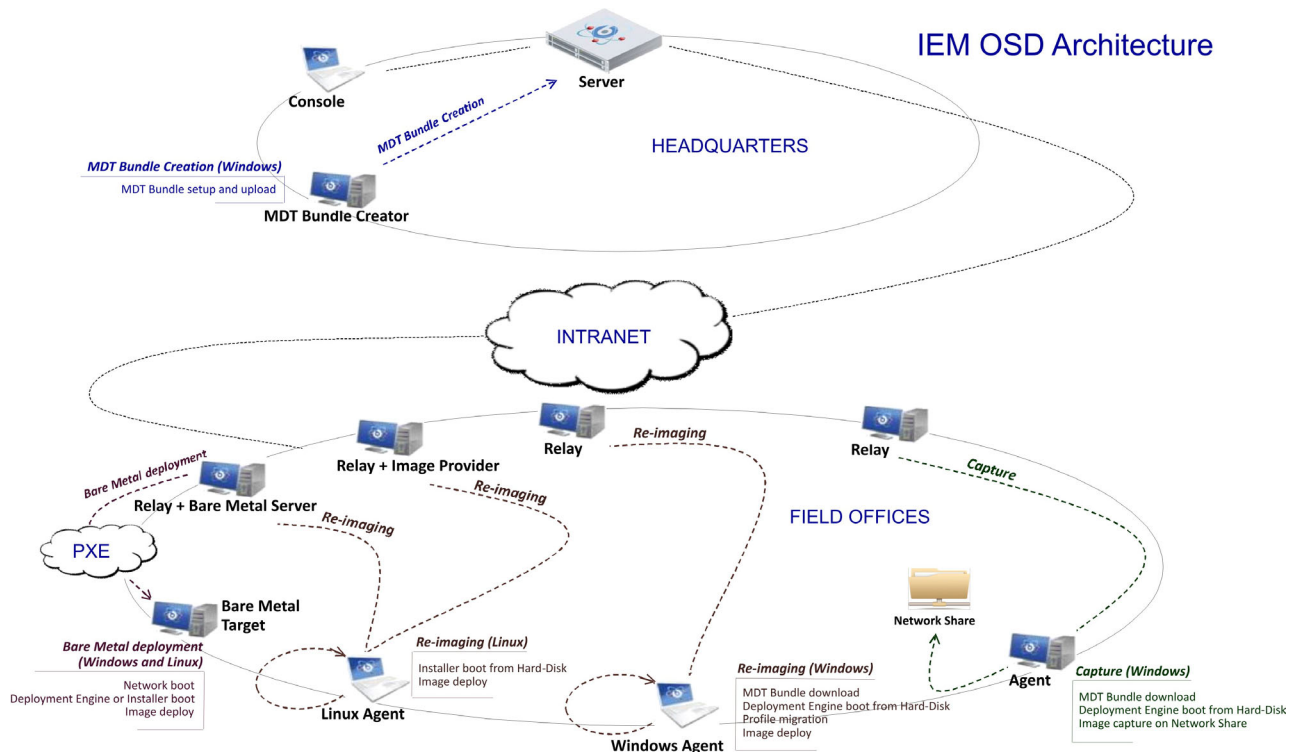
Trademarks 141
Terms and conditions for product documentation 142

Chapter 1. Product overview

OS Deployment provides complete OS provisioning and system re-imaging capabilities for Windows and Linux targets. The solution was created to deploy a fully-configured operating system to multiple computers across an enterprise. Using innovative image deployment technology, IBM® Endpoint Manager for OS Deployment is ideal for rapid, hardware-independent imaging and flexible, centralized image refresh.

You can deploy, configure, and manage Tivoli Provisioning Manager for OS Deployment servers for Bare Metal deployments from the IBM Endpoint Manager infrastructure. After you set up the Bare Metal OS Deployment servers, you can create profiles containing images that become available when computers in the network PXE boot to that server. Computers then select profiles that are downloaded along with all the drivers needed to run the imaging process.

The following graphic shows a high-level view of the OS Deployment process and components.



Understanding OS Deployment components and terms

OS Deployment is an IBM Endpoint Manager Platform-based application. Before you begin working with OS Deployment in your environment, become familiar with the key product components and concepts.

Agent

An IBM Endpoint Manager Agent (henceforth referred to as client or target) is installed on every computer that must be managed. It continuously assesses the state of the endpoint against the stated policy. As soon as the agent notices that the target is out of compliance with a policy or checklist, it informs the server, runs the configured remediation task, and immediately notifies the server of the task status and result. A computer with the IBM Endpoint Manager agent installed is also referred to as a client. In an OS Deployment network, agents are recipients of deployment actions. They can receive OS upgrades, and can be reimaged by preserving existing user data. An agent is automatically installed during Bare Metal Provisioning.

Bare Metal OS Deployment Server

A Bare Metal server, also referred to as Bare Metal Server or OS Deployment Server, is a PXE server that manages OS deployments to bare metal targets. The console operator prepares Bare Metal profiles from images that are stored in the Image Library, and sends the profiles to the Bare Metal Server for deployment on targets. You install this component on a relay in your OS Deployment network. The Bare Metal Server embeds the Image Provider component that is needed for Linux deployments.

Bare Metal Profile

A Bare Metal profile combines an image to a set of additional user-defined properties that allow a successful deployment on bare metal targets. A Bare metal profile contains the required data to deploy an operating system (such as product key, owner, and organization), an optional password to protect the profile to prevent unauthorized deployment, and an optional timeout to allow automatic deployment when the timeout expires. Bare Metal profiles are derived from images and are sent to specific Bare Metal servers in the endpoint management infrastructure.

Bare Metal Target

A Bare Metal target is any computer in your environment that boots from the network or from deployment media that emulates the PXE boot process. Through a binding menu, the target selects bare metal profiles for installation. Profiles can also be automatically deployed without target intervention.

Bare Metal targets can also be managed from the IBM Endpoint Manager infrastructure, through the Management Extender for Bare Metal Targets component.

Console

The IBM Endpoint Manager console (referred to as console) acts as a single point of management and control for all activities in the network. If you are an operator with the required privileges, from the console you can quickly monitor and trigger specific actions to selected targets. In an OS deployment network, the Console operator can complete all the OS deployment preparation and deployment actions from the OS deployment and Bare Metal Imaging site.

Deployment Media

Deployment media are CD/DVDs or USB keys that you prepare for use on targets that are not using PXE for these purposes:

- to emulate the PXE boot process and start the Bare Metal deployment process

- to perform an offline OS deployment

Drivers

Drivers are needed to adapt an image to specific hardware. Both WinPE and Windows operating systems require drivers, for both the pre-installation phase and when the operating system is deployed. In the OS Deployment environment, drivers are stored in the driver library and are separate from the images. The appropriate drivers are selected at capture and deployment time. OS Deployment automatically selects the drivers that are most appropriate for the operating system to be deployed and for the devices that are installed on the target hardware. However, users can customize driver selection and bindings to cover specific situations that might cause automatic driver selection to fail.

Image

An image is a "copy" of an operating system. An image can be created by capturing a reference machine or from an installation media (ISO Image). The image can include one or more disk partitions in a single file.

Image Provider

The Image Provider is a machine that hosts the Linux images (LIM) that are to be deployed to Linux targets. It is a component of OS Deployment that must be installed on those relays that serve the Linux targets that you want to reimage. The relays that have the Bare Metal Server component installed already act as image providers to their connected targets, so this component is not needed.

Management Extender for Bare Metal targets

The Management Extender for Bare Metal Targets is a plug-in that you install on the Bare Metal OS Deployment Server. It collects information about the Bare Metal Targets that completed a PXE boot operation on the Bare Metal Server and reports this information to the IBM Endpoint Management Server. You can then manage the reported Bare Metal targets through the Endpoint Manager infrastructure. The Management Extender for Bare Metal targets requires the Proxy Agent component of the Endpoint Manager Platform.

MDT Bundle

An MDT bundle is a collection of Windows Pre-installation Environment (WinPE) files, a Deployment engine (MDT), and OS resources that are needed for the installation of a Windows operating system. MDT is a tool that allows the definition of a sequence of steps that are required to deploy the operating system. The tools runs within WinPE. The OS resources are packaged starting from an operating system installation CD. The MDT Bundle is created on the MDT Bundle Creator machine and uploaded into the OS Deployment environment. Typically, you need to create a bundle only once.

MDT Bundle Creator

The MDT Bundle creator is a system that is used for creating deployment packages for Windows OS deployments to be uploaded to the server when ready. The bundles contain the tools, resources, and instructions necessary for successful image deployments. OS Deployment automatically installs the necessary tools on your designated MDT Bundle Creator system. Depending on the types of Windows operating systems, you want to

install, the MDT Bundle creator machine might require access to the internet to download the necessary tools.

Network shares

In an OS Deployment context, a network share is a network path that serves as repository for the Windows images (WIM) stored after a capture before they are imported into the Image Library. Network shares are also used to store user data before reimaging a target.

Proxy Agent

The Proxy Agent is an enabling service that is used by Management Extenders to provide a connection to the Endpoint Manager system for devices that do not run a native agent.

RAD profile

A RAD profile is an image that is imported into the Image Library that was prepared with Tivoli Provisioning Manager for OS Deployment, and then exported in RAD file format. RAD profiles are sent to the Bare Metal servers ready to be deployed.

Relay

An IBM Endpoint Manager Relay (henceforth referred to as relay) is a client that is enhanced with a relay service. Relays help manage distributed devices by delivering content and software to child clients and relays. Instead of requiring every networked computer to directly access the server, relays are used to scale much of the workload. Promoting an agent to a relay takes minutes and does not require dedicated hardware or network configuration changes. In an OS Deployment environment, relays take the role of Image Providers for deployments on Linux targets, and become OS Deployment Servers for bare metal provisioning on both Windows and Linux targets.

Server

The IBM Endpoint Manager Server is the main component of the IEM infrastructure. It manages policy-based content, coordinates the flow of information to and from the individual clients, and stores the results in the database. All content is delivered in the network through messages called Fixlets. From an OS Deployment perspective, the IEM Server manages all deployment activities to targets and communicates with relays that act as Image Providers or as Bare Metal Servers. The server stores images, profiles, and all necessary OS resources and tools that are needed for deployments to targets.

Windows Assessment and Deployment Kit (WADK) and Windows Automated Installation Kit (WAIC):

WADK and WAIC are a collection of tools that are used to customize, assess, and deploy Windows operating systems.

Windows Pre-installation Environment (WinPE)

It is a minimal operating system that is used to prepare a computer for a Windows installation. Different versions of WinPE are available for the various Windows Operating system versions. OS Deployment uses WinPE during reimaging and bare metal provisioning.

Provisioning Use Cases

Capturing Windows Images

A Capture process is the creation of a reference image from an installed machine (referred to as reference machine), removing unique identifiers from the image so that it can be "cloned" on new systems. You might also want to capture a newly installed critical machine to create a "golden image" that can be easily restored in case of failure. The capture process relies on Microsoft tools and requires an MDT Bundle.

You can capture systems using the Capture dashboard. You must specify a set of parameters that are needed for the capture process. During the capture process on Windows systems, the selected MDT Bundle is downloaded with the corresponding WinPE and the needed network and disk drivers are downloaded for use with WinPE. The output of the capture process is a Windows image (.WIM) which is stored on a network share and contains one or all of the partitions. An ".imageinfo" file that includes the description of the image, and the ".driverinfo" file that contains the PCI IDs of the devices that are managed by the drivers that are built in the captured OS.

Reimaging Windows targets

Reimaging involves redeploying an operating system image on a target where the old operating system is still running. It involves capturing and restoring the user data when the image is applied to the target. Reimaging allows you to deploy a golden image to one or more targets and to perform operating system upgrades. The image and any applicable drivers are loaded on the target.

During the reimaging process, you can provide additional customization parameters for migrating specific user files. You can modify the mapping of the partitions present in the image (.WIM) with the existing partitions on the target machine. Network shares can be used to store the saved user state and the deployment logs. As part of the customization steps you can automatically join a target machine to a workgroup or specific domain after the reimaging completes.

Reimaging Linux targets

Reimaging involves redeploying an operating system image on a target where the old operating system is still running. Reimaging allows you to deploy an image that is created from an installation media to one or more targets and to perform operating system upgrades.

The Image Provider component (or the Bare Metal Server that embeds an Image Provider) is required on the relay where the targets are connected to; it acts as an HTTP server that hosts the selected LIM image to be provisioned. During the reimaging process, you can provide more customization parameters by editing the configuration file that is used by the Linux Installer.

Bare Metal Target provisioning

Bare Metal Provisioning involves the installation of an operating system on a new machine (bare metal machine). It requires a PXE server or Deployment Media because the target must boot from a bootable device that is not its own disk. A Bare metal profile is created from an image that already includes the correct software stack. You can customize more properties to be used during the deployment. As part of the process, the appropriate drivers are downloaded on the target. You can also repartition the disks on the target during a bare metal deployment.

Bare Metal provisioning can be initiated from the binding menu that is displayed on the Bare Metal target machine after it performs a PXE boot to its Bare Metal OS Deployment Server, or it can be initiated from the IBM Endpoint Manager console, when the Management Extender for Bare Metal Targets plug-in is installed on the Bare Metal Server. With this component you can manage Bare Metal Targets from the Endpoint Manager infrastructure. Typical use cases are:

- When a system is to be reprovisioned to a new user, a best practice is to wipe the disk content entirely. The new machine owner is requested to perform a PXE boot operation, so that the system can be managed from the IBM Endpoint Manager console where an administrator sends a disk wipe task to the target. When the disk wipe operation is complete, the administrator sends a Bare Metal profile deployment task to the target to deploy the wanted operating system image.
- A new server needs to be configured and deployed. The deployment requires configuring the system RAID controller before the operating system is installed. This operation requires an update to the RAID controller firmware. The hardware configuration instructions are prepared using vendor-specific tools available on the vendor's website. Then, the hardware configuration instructions are imported into the Endpoint Manager infrastructure ready to be deployed. When the operator performs a PXE boot operation, the new server becomes manageable from the IBM Endpoint Manager console. A Hardware Configuration Task is then sent to the target to perform the necessary changes.

What's new in version 3.6

Become familiar with the new features of this release.

OS Deployment version 3.6 includes the following new features:

Bare Metal target management from the IBM Endpoint Manager console

This version introduces the Management Extender for Bare Metal Targets Plug-in that discovers and registers Bare Metal targets to the Endpoint Management Server. When targets PXE boot to the Bare Metal OS Deployment server, you can manage them from the console. You can:

- View inventory information for the targets
- Perform deployment tasks
- Define custom variables and associate them to bare metal targets so that tasks can be triggered on these targets after a deployment
- Wipe the disk contents of bare metal targets

The Wipe Disk functionality is typically used when the hardware needs to be dismissed or re-provisioned and allows you to erase the system disk content in a secure manner, so that the data originally stored on the hard disk can no longer be retrieved.

Deploy a scripting environment on a bare metal target

You can leverage vendor scripting toolkits to implement configuration tasks on your bare metal targets. Through a dedicated dashboard, you can import scripting environments and deploy them to your Bare Metal Targets. The product can deploy configurations created with hardware-specific scripting toolkits from IBM, Dell, and HP.

Copy image settings from an existing image to an image that has no objects associated to it.

From the image library, you can copy the following settings from a reference image: bare metal profiles, targeting rules, associations to the bare metal server where the profile is stored, and binding rules. When you copy the bare metal profiles from the selected image, you can specify a prefix or suffix for these profiles in the target image.

Create offline deployment media for Windows targets

You can create CD/DVD or USB media for offline deployments on targets that are not connected to the network.

Features added in previous versions

The following features were added with OS Deployment Version 3.5

Linux Enterprise Support for image creation from installation media (ISO), re-imaging and Bare Metal deployments

This version introduces support for the following Linux Enterprise Versions:

- RedHat Enterprise Linux Versions 5, 6 , and 7
- SuSE Linux Enterprise Server Version 11

You can import images from ISO for Linux re-imaging and Bare Metal deployments. You can re-image Linux systems both as an upgrade or as a fresh installation. You can perform Bare Metal deployments on Linux targets.

New image creation from installation media (ISO) for Windows Deployments

You can create and import images directly from ISO (Setup Images). From the Image Library dashboard you can:

- Import images for Windows deployments from ISO installation media:
 - in archived format by specifying the file name (.iso)
 - by selecting an ISO folder containing the uncompressed image files.

The new import from ISO feature enhances the re-imaging capabilities for Windows platforms. You can now perform re-imaging and Bare Metal deployments choosing between two different sources: from a captured image of a reference machine, or by deploying an image created from ISO. In the latter case, you can choose between different flavors of the operating system (if available) from the ISO image that you imported.

Windows OS Resource creation directly from the Image Library

You can create and upload OS resources (from ISO installation media) for Windows deployments directly from the Image Library, concurrently with the import of the ISO image. Previously, you could create OS resources only from the MDT Bundle Creator machine.

The following features were added with OS Deployment Version 3.4:

New Bundle and Media Manager Dashboard

A new dashboard was implemented to perform the following tasks:

- Install the MDT Bundle Creator and all its prerequisite software.
- Create a MDT Bundle with or without OS resources.
- Create OS resources only

- Create CD, DVD, or USB bootable media for deployments to targets when PXE-boot through the network is unavailable.

The new Bundle and Media Manager dashboard simplifies the bundle creator installation and the bundle creation process by checking for installed prerequisites and helping you to make the correct choices for the operating systems you plan to deploy. The version of the User State Migration Tool (USMT) included in the bundle is displayed on the dashboard.

Join Domain usability improvements during re-imaging

The following usability enhancements were added:

- Information was added to the Image library dashboard to help you to provide the correct Domain Credentials when you are creating a Bare Metal Profile, and when you are deploying an image.
- Improved documentation to explain the Domain and Organizational unit fields.

Support of Microsoft Windows 2012 R2 for capturing, imaging, and bare metal deployments.

You can capture, re-image, or perform bare metal deployments on Windows 2012 R2 targets. You can also install a Bare Metal Server on this operating system. Deployment of Windows 2012 R2 requires a new version of the Microsoft Deployment Toolkit (MDT 2013) and of the Windows Assessment and Deployment Kit (WADK) 8.1, which includes Windows PE 5. These new versions can also be used for earlier supported operating systems.

The following features were added with OS Deployment Version 3.3:

Secure Hash Algorithm (SHA-256) enhanced security support for deployment objects (with IBM Endpoint Manager 9.1 Platform)

The IBM Endpoint Manager platform Version 9.1 supports the NIST security standards and provides an enhanced security option. This setting enables SHA-256 as the hashing algorithm for digital signatures and content verification. SHA-1 and SHA-256 values for deployment objects (MDT Bundles, images, drivers) are calculated and assigned at creation time. Objects that were created with platform versions earlier than 9.1 only have SHA-1 hashing values. Objects created with version 9.1 or later have both SHA-1 and SHA-256 hashing values. OS Deployment version 3.3 supports deployment operations in a mixed environment for compatibility with previous versions. If you decide to set the enhanced security option for your environment, all objects must have been updated with SHA-256 hashing information. A new health check is provided to display non-compliant files and from which you can start a remediation action to update the affected objects.

Bare Metal and re-imaging usability and customization enhancements

- You can define a timeout when you are creating or editing a bare metal profile. This value defines the maximum time the LiteTouch script that installs the WIM image is allowed to run.
- You can set a time limit for the caching of an image on the relay (Bare Metal Server) during a deployment.
- You can start, stop, restart, or view the status of Bare Metal server services.
- You can view if errors were recorded on server logs.

- For any given image linked to a system profile, you can view whether the corresponding WIM image is cached on the relay.
- You can customize the boot partition in the partition mapping for re-imaging and bare metal deployments

Support of Microsoft Windows 8.1 for capturing, imaging, and bare metal, and corresponding Microsoft tools

You can capture, re-image, or perform bare metal deployments on Windows 8.1 targets. You can also install a Bare Metal Server on this operating system. Deployment of Windows 8.1 requires a new version of the Microsoft Deployment Toolkit (MDT 2013) and of the Windows Assessment and Deployment Kit (WADK) 8.1, which includes Windows PE 5. These new versions can also be used for earlier supported operating systems. When you create a new MDT Bundle, you can choose the version of the tools that best suits your needs. A matrix of supported combinations is available.

MDT Bundle usability improvement

In the Upload MDT Bundle dashboard, you can view information about the WinPE version included in each bundle and its corresponding MDT version.

The following features were added in OS Deployment version 3.2:

- Support of Microsoft Windows Server classes, (2003, 2008, 2008 R2, 2012)
- Enhanced Bare Metal profile deployment, by defining rules for target selection based on computer properties.
- Support of UEFI (x64) for capture, re-image and bare metal deployments
- Optional creation of baselines for future use from the **Deploy Image to Computer** wizard.
- Possibility of specifying a computer name during bare metal profile creation and deployment.

The following features were added in OS Deployment version 3.1:

- Support of Microsoft Windows 8 and MDT 2012 Update 1.
- Ability to upload multiple MDT Bundles and specify which to use during capture and deployment.
- Multiple partitions support when capturing, editing, and deploying an image.
- Ability to manage driver bindings at a global level before deployment.
- Improved driver binding grid editor in the Activity Dashboard.
- Improved options for encrypting actions with passwords using the V9.0 platform.

The following features were added in OS Deployment version 3.0:

- Seamless bare metal provisioning through integration with Tivoli Provisioning Manager for OS Deployment
- Dashboard content to configure and manage Tivoli Provisioning Manager for OS Deployment servers for bare metal provisioning
- Activity dashboard to monitor of re-image, capture, and bare metal deployment tasks
- Image Library dashboard expanded to support re-image task and bare metal profile creation
- Enhanced templating features

- Ability to edit CustomSettings.ini directly from the **Deploy Image to Computer** wizard

The following features were added in OS Deployment version 2.2:

- New Driver Library dashboard that manages drivers and assigns where they are used during the reimage process
- New MDT Media Creator tool for generating bootable media

The following features were added in OS Deployment version 2.1:

- MDT Bundle Creation Fixlets that assist with downloading the bundle creator and installation of bundle creator prerequisites
- SSL Encryption of Domain Credentials that reconnect to a domain after imaging
- Save as Template feature in Re-image Options that saves a specific re-image configuration for future use
- Health Checks Dashboard that shows a summary of the overall health of your deployment
- Image Library that integrates the Activate Image and Manage Image dashboards with pre-cache images and modification of image information
- SMB shares are no longer required for OS re-imaging
- Re-Image History Dashboard that displays in-progress or completed re-image jobs
- Images are now stored in any share location and no longer require repositories
- Simplified UI using Take Action Dialogs instead of dashboard UI for initiating tasks
- Support of capture and deployment of Windows Vista

System requirements

To enable and use OS deployment in your environment, ensure that you have the required software prerequisites.

IBM Endpoint Manager Platform prerequisites:

OS Deployment requires version 8.2 , 9.0, 9.1 or 9.2 of both the IBM Endpoint Manager platform and clients.

OS Deployment supports capturing, imaging, and bare metal OS provisioning of the following operating systems:

Windows:

- Microsoft Windows 8.1 (x86, x64)¹
- Microsoft Windows 8 (x86, x64)¹
- Microsoft Windows 7 (x86, x64)¹
- Microsoft Windows Vista (x86, x64^{1, 3})
- Microsoft Windows XP Professional (x86, x64)⁴
- Microsoft Windows Server 2012 (x64)¹
- Microsoft Windows Server 2012 R2 (x64)¹
- Microsoft Windows Server 2012 (x64) with Hyper-V role¹
- Microsoft Windows Server 2012 R2 (x64) with Hyper-V role¹
- Microsoft Hyper-V Server 2012 (x64)¹
- Microsoft Hyper-V Server 2012 R2 (x64)¹
- Microsoft Windows Server 2008 R2 (x64)¹

- Microsoft Windows Server 2008 (x86, x64¹)
- Microsoft Windows Server 2003 R2 SP2 (x86, x64)⁴
- Microsoft Windows Server 2003 SP2 (x86, x64)^{2, 4}

Note:

1. These operating systems are supported both in BIOS and UEFI firmware. All other operating systems in BIOS only.
2. For this operating system, any 2003 OS resource can be used for both capture and deployment of a 2003 WIM image.
3. On UEFI firmware, SP2 is required.
4. Image import from installation media (ISO) is not supported

The Endpoint Manager Client computer on which you build the MDT bundle requires the following software:

- MDT 2010 Update 1
- MDT 2012 Update 1 or MDT 2013
- Windows Assessment and Deployment Kit (WADK).

These prerequisites are installed using the **Bundle and Media Manager** dashboard, as described in Chapter 3, “Managing MDT Bundles and Deployment Media for Windows targets,” on page 29.

Linux:

OS Deployment supports imaging and bare metal provisioning of the following operating systems:

- RedHat Enterprise Linux (RHEL) Versions 5, 6 (x86, x64¹)
- RedHat Enterprise Linux (RHEL) Version 7 (x64¹)
- SuSE Linux Enterprise Server (SLES) Version 10² and 11 (x86, x64¹)

Note:

1. For x64 architectures, these operating systems are supported for both BIOS and UEFI firmware. For x86 architectures, only BIOS is supported.
2. SuSE Version 10 is supported only as a source operating system for re-imaging.

The following system requirements apply to the installation of Tivoli Provisioning Manager for OS Deployment Bare Metal servers, Image Provider, and Management Extender for Bare Metal Targets component:

- Windows Server 2003 and Windows Server 2003 R2 (x86, x64)
- Windows Server 2008 (x86, x64)
- Windows Server 2008 R2 (x64)
- Windows Server 2012 (x64)
- Windows Server 2012 R2 (x64)
- Microsoft Windows XP Professional (x86, x64)
- Windows 7 (x86, x64)
- Windows 8 (x86, x64)
- Windows 8.1 (x86, x64)

Note: To manage Bare Metal Targets from the Endpoint Manager infrastructure, you must install Tivoli Provisioning Manager for OS Deployment Version 7.1.1.17 or later on the Bare Metal servers in your network.

Process overview

Preparing your environment for deployments of Windows and Linux operating systems involves a set of steps you must complete in your environment.

For deployments on Linux systems, you must create and import images from installation media. You can then deploy the images to selected targets or create and deploy profiles for Bare Metal deployments.

For deployments on Windows systems, the IBM Endpoint Manager OS Deployment solution uses the Microsoft Deployment Toolkit (MDT) to provide system preparation, image capture, driver insertion, and image deployment services. To prepare your environment for deployments, the administrator must use an accompanying tool, the MDT Bundle Creator to produce a bundle of tools and resources that are called the MDT Deployment Bundle.

To set up and deploy images to workstations in your Endpoint Management environment, you must complete the following steps:

1. Subscribe to the **OS Deployment and Bare Metal Imaging** site. You can enable the site from the License Overview dashboard in the BigFix Management Domain. Change the site subscription to include both the IBM Endpoint Manager Server as well as all computers on which you complete OS Deployment tasks.
2. Run the tasks that are listed in the Setup node of the navigation tree, and activate all listed analyses.
3. If you are provisioning Linux targets, install the Linux Image Provider component on one or more relays that are not Bare Metal Servers. If your Linux targets are connected to a relay that is a Bare Metal server, the Linux Image Provider component is already embedded.
4. Verify in the Health Checks Dashboard that all setup steps completed successfully.
5. If you are provisioning Windows systems:
 - build and upload the MDT bundle with the MDT Bundle Creator tool
 - import drivers from the Driver Library
 - capture images from reference machines using the Capture Images Wizard or create images from installation media (ISO images)
 - import images from the Image library dashboard
6. If you are provisioning Linux systems:
 - create images from installation media (ISO images) and import them from the Image Library dashboard.
7. Deploy images to Windows and Linux targets from the Image Library.

You can also install images on bare metal workstations by completing the following steps:

1. Install a bare metal OS Deployment server on an Endpoint Manager relay in your network.
2. Create bare metal profiles for Windows and Linux deployments and upload them to the OS Deployment server
3. Deploy the bare metal profiles to targets.

For more information, see Chapter 6, “Bare Metal deployments,” on page 89.

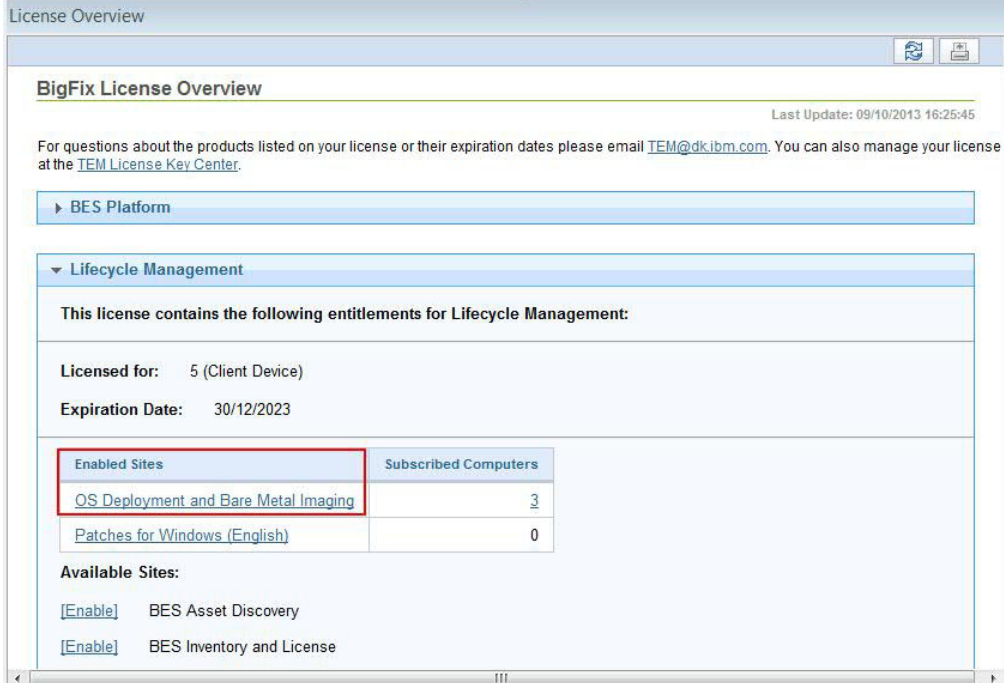
If you want to manage Bare Metal targets from the Endpoint Manager Console, you must install the Management Extender for Bare Metal Targets component on the Bare Metal OS Deployment servers that manage these targets. For information about installing this component, see “Deploying the Management Extender for Bare Metal Targets” on page 21.

Enable OS Deployment and Bare Metal Imaging site

To start working with IBM Endpoint Manager for OS Deployment, you must enable the **OS Deployment and Bare Metal Imaging** site.

From the License Overview dashboard in the **BigFix Management** domain, click **Enable**.

You must also subscribe all computers on which you perform OS Deployment tasks to this site. The site is displayed in the **Systems Lifecycle** domain together with earlier versions of OS Deployment. Earlier OS Deployment sites are appropriately hidden or marked as deprecated after you enable the new site.



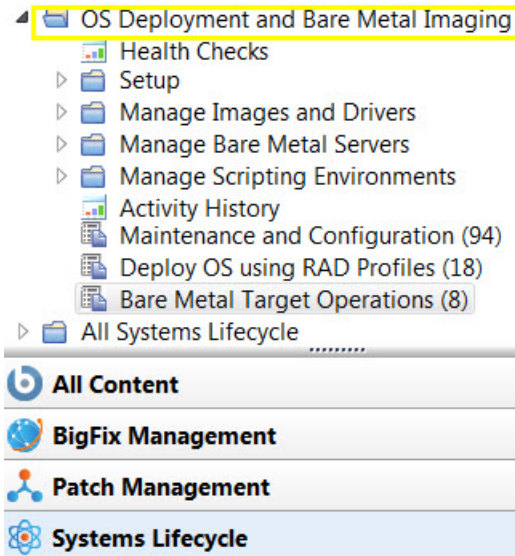
The screenshot shows the 'License Overview' page in the BigFix console. The page title is 'BigFix License Overview' with a last update timestamp of '09/10/2013 16:25:45'. Below the title, there is a link to 'TEM License Key Center'. The main content area is divided into sections: 'BES Platform', 'Lifecycle Management', and 'Available Sites'. Under 'Lifecycle Management', it states 'This license contains the following entitlements for Lifecycle Management:' followed by 'Licensed for: 5 (Client Device)' and 'Expiration Date: 30/12/2023'. A table lists 'Enabled Sites' and 'Subscribed Computers':

Enabled Sites	Subscribed Computers
OS Deployment and Bare Metal Imaging	3
Patches for Windows (English)	0

Below the table, the 'Available Sites' section lists two items: '[Enable] BES Asset Discovery' and '[Enable] BES Inventory and License'.

Navigation tree overview

The OS Deployment and Bare Metal Imaging navigation tree, which is accessed from the IBM Endpoint Manager console, is your primary tool for capturing and deploying OS images. This navigation tree becomes available when you enable the site from the License Overview dashboard in the BigFix Management domain. To access the navigation tree, open the IBM Endpoint Manager console and click the *Systems Lifecycle* domain at the bottom of the domain panel.



Click *OS Deployment and Bare Metal Imaging* to expand the content, which is organized into nodes, dashboards, Fixlets, and tasks that you use to prepare and perform OS deployments in your environment:

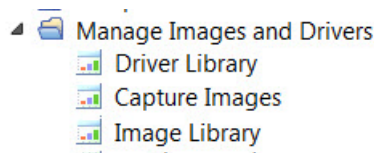
Health Checks

The OS Deployment Health Checks Dashboard provides troubleshooting and optimization checks for OS Deployment. You can drill down into individual health checks to see their results and a resolution path for failing checks. See “Health Checks Dashboard” on page 26.

Setup From this node you perform the installation and configuration steps needed to successfully prepare and upload MDT bundles, to upload images to the Endpoint Management server, and to deploy these images on computers in your environment. The Setup node expands to display the dashboards, Fixlets, tasks, and analyses available for this purpose. Each configuration task is described in detail in Chapter 2, “Configuring the OS Deployment Environment,” on page 17 and Chapter 3, “Managing MDT Bundles and Deployment Media for Windows targets,” on page 29.

Manage Images and Drivers

The Manage Images and Drivers node includes wizards and dashboards for managing your driver and image libraries, as well as for capturing images. For more information about images and drivers, see Chapter 4, “Managing Images and Drivers,” on page 49.



Manage Bare Metal Servers

Expanding this node, you access the Server Management dashboard. From this dashboard you can manage bare metal OS Deployment servers. You can install, uninstall, or upgrade Tivoli Provisioning Manager for OS Deployment Servers by uploading the appropriate installers.

After you install, you can create bare metal profiles containing images that are stored on the server and made available to target computers that PXE boot to that server. When a target selects a profile from the binding menu, the image, the MDT bundle, and all necessary drivers are downloaded through the endpoint management infrastructure and the imaging process begins.

For information about installing a bare metal server and creating profiles on your IBM Endpoint Manager relay, see “Managing Bare Metal OS Deployment Servers” on page 89.

Manage Scripting Environments

Expanding this node, you access the Scripting Environment Library. From this dashboard you can import scripting environments that you have previously created with vendor-specific tools, and deploy them to your Bare Metal targets. The Bare Metal Server that manages the targets must have the Management Extender for Bare Metal targets component installed.

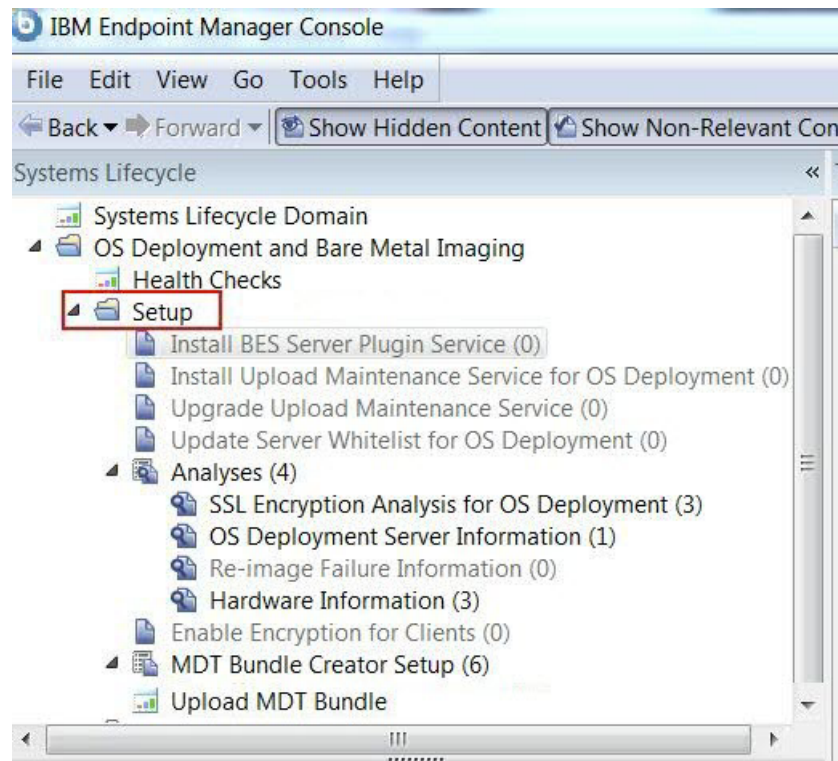
Deploy OS using RAD Profiles

This menu lists a set of Fixlets you can run to perform bare metal deployments using imported RAD profiles. For further information, see Appendix B, “Bare Metal OS Provisioning using RAD Profiles,” on page 133.

Chapter 2. Configuring the OS Deployment Environment

To start working with OS Deployment, run the configuration Fixlets and tasks listed in the Setup Node.

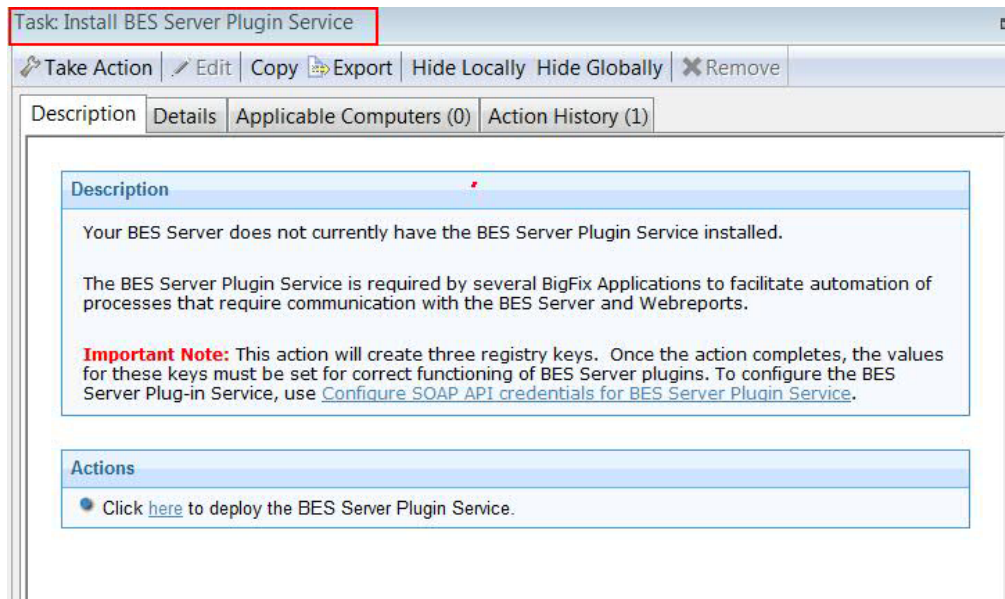
In the *Setup* node in the navigation tree, you can access reports, dashboards, and wizards that you use to manage repositories and images and set parameters for their future use within your deployment.



Perform each task in the Setup Node. Each task is described in detail.

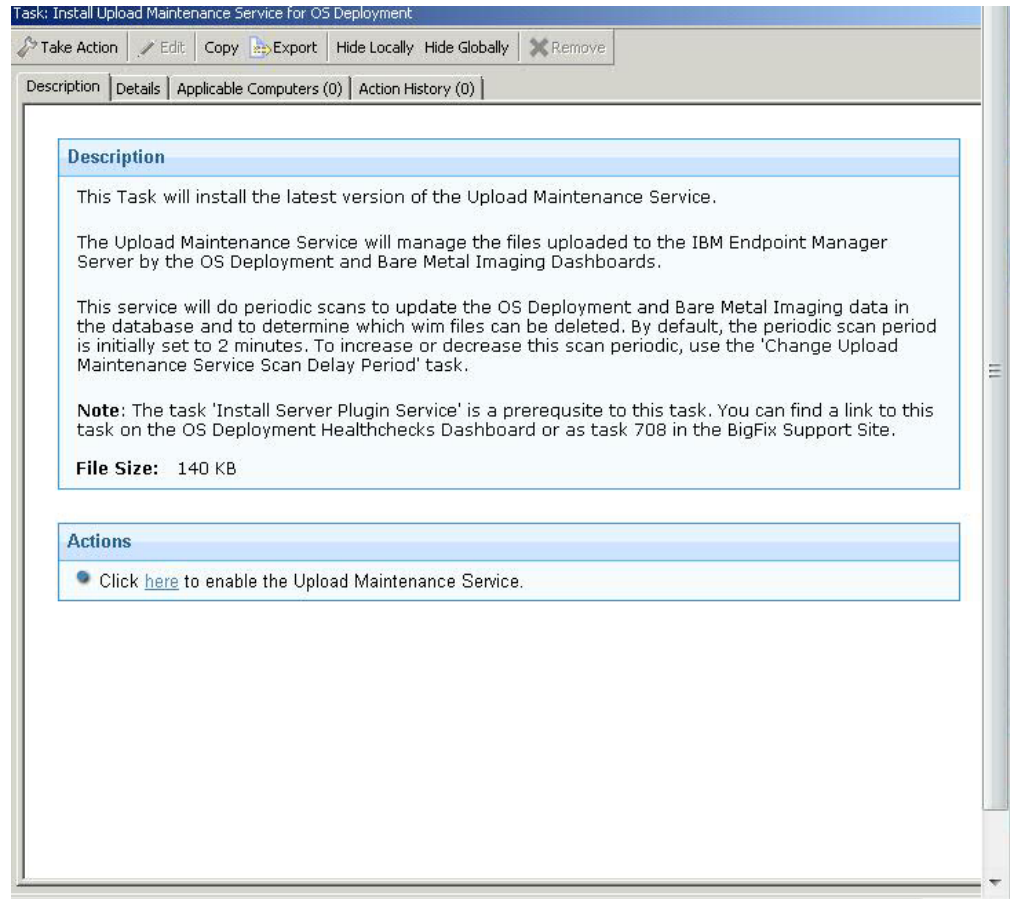
Install BES Server Plugin Service

The *BES Server Plugin Service* task enables the Upload Maintenance Service. From the navigation tree, click the task and, when the Fixlet window opens, click in the Actions box to deploy the plug-in.



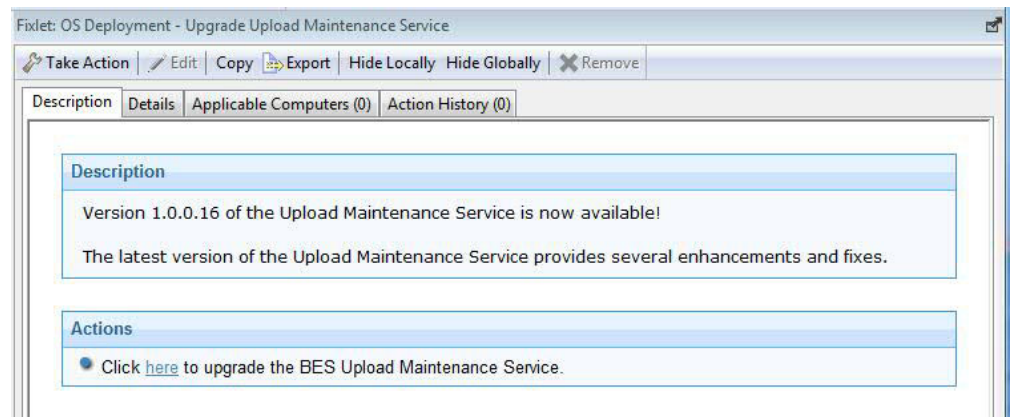
Install Upload Maintenance Service

The Upload Maintenance Service manages files uploaded to the server. This service performs periodic scans to update the OS Deployment and Bare Metal Imaging data in the database. To enable the Upload Maintenance Service, click the link in the Actions box.



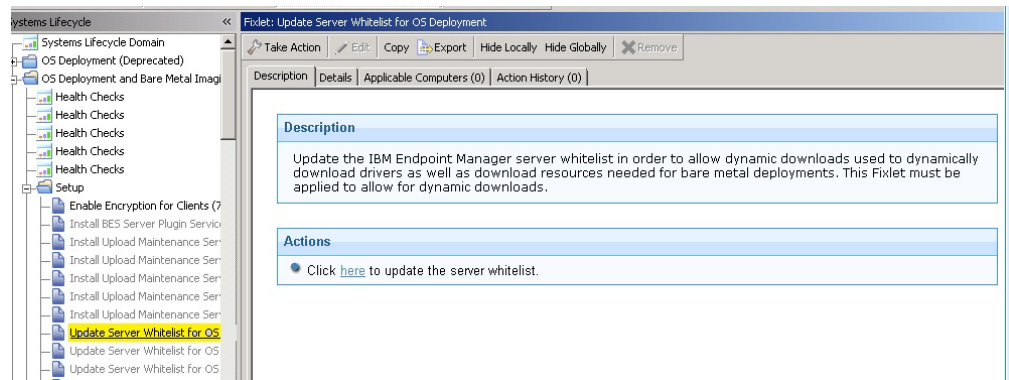
Upgrade Upload Maintenance Service

Click the Upgrade Upload Maintenance Service node in the navigation tree to use the latest content enhancements and fixes. To upgrade the Upload Maintenance Service, click the link in the Actions box.



Update Server Whitelist for OS Deployment

The Update Server Whitelist for OS Deployment Fixlet enables agents to dynamically download the necessary driver files.



Click the link in the Actions box to update the server whitelist.

Managing the Linux Image provider

The Linux Image provider component is needed for re-imaging Linux systems in your environment

To deploy images on Linux targets in your network, you must install the Linux image provider component on the relays to which your Linux targets are connected. You cannot install the Image Provider component on relays that are Bare Metal OS Deployment servers, because this component is already embedded. If your targets are connected directly to an IBM Endpoint Manager server, you must install this component on the server.

Before you deploy Linux systems, you must update the IBM Endpoint Manager Server whitelist to enable the Linux Image Provider to dynamically download the necessary files.

Installing the Linux Image Provider

From the **OS Deployment and Bare Metal Imaging** site, click **Maintenance and Configuration**. Select the corresponding task. When you deploy the action, the list of applicable relays is displayed in the Take Action menu. Select one or more relays from the list and click **OK** to begin installation.

This component is installed in C:\Program Files\OSdImageProvider. When the installation ends, the component is started automatically. The log file `rbagent.log` and trace file `rbagent.trc` are stored in the installation directory

Useful commands

You can start the Linux Image provider by running the "Start Linux Image Provider" Fixlet, which you can also include in your Server Automation Plans.

You can also run the following batch files to start or stop the Image Provider:

- To start the Image provider process:

StartImageProvider.bat

- To stop the Image provider process:
StopImageProvider.bat

To increase the log level for problem determination purposes, you can edit the StartImageProvider.bat file. For example:

```
osdimageprovider.exe -d -v 4 -o rad -startimageprovider
```

raises the log level to 4 from the default level of 3.

Uninstalling the Linux Image Provider

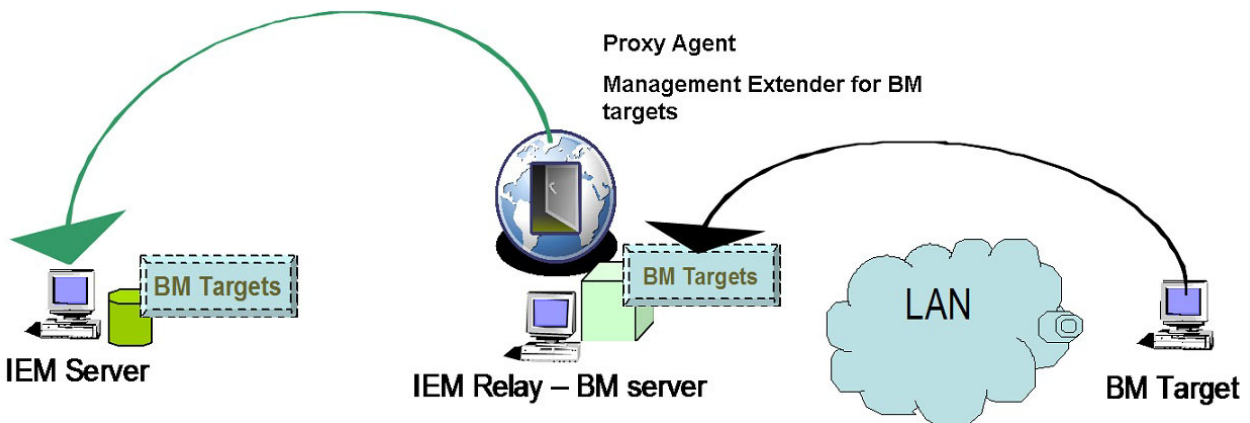
To remove the Linux Image Provider from a relay in your environment, run the "Uninstall Linux Image Provider " task on the relevant relays.

Deploying the Management Extender for Bare Metal Targets

You can manage Bare Metal Targets from the Endpoint Manager infrastructure by installing and using the Management Extender for Bare Metal targets.

With this component, you can manage targets that are not part of the Endpoint Manager infrastructure because they do not have the IBM Endpoint Manager client installed.

The Management Extender for Bare Metal Targets is a plug-in that runs locally on one or more Bare Metal Servers in your environment. When a target PXE-boots to the server, the plug-in queries the PXE server and extracts information on the known bare metal targets. The targets are then reported to the IBM Endpoint Manager Server database, and you can manage them through the IBM Endpoint Manager console. From the console, the tasks that are directed to these targets are forwarded to the local Bare Metal Server to which they belong.



The targets that have completed a PXE boot in the last 48 hours are reported in the IBM Endpoint Manager infrastructure. This means that any target that did not connect to the bare metal Server within this time frame is not reported to the Endpoint Manager Server. You can change this threshold to suit your needs. See "Configuring the behavior of the plug-in " on page 22.

The available target information is refreshed every 10 minutes. You can modify the refresh interval by editing the `settings.jsonfile`. See “Changing the plug-in settings .”

Installing the plug-in

The Management Extender for Bare Metal targets requires the installation of the Proxy Agent as a prerequisite. To install and run the correct proxy agent, complete the following steps on the relay in your environment, which is also the Bare Metal Server:

- If your relay is at IBM Endpoint Manager Platform Version 8.2 or 9.0:
 1. From the Systems Lifecycle Domain, expand **All Systems Lifecycle > Fixlets and Tasks**. Select the **Deploy Proxy Agent 9.0.40099 on 8.2 or 9.0 Relay** task (152).
 2. When you deploy the action, the list of applicable relays is displayed in the **Take Action** menu. Select one or more relays from the list and click **OK** to complete the installation.
 3. Run the task **Deploy Management Extender for Bare Metal Targets** (ID 150)
- If your relay is at IBM Endpoint Manager Platform Version 9.1 or later:
 1. From the BES Support site, search and run fixlet **Install IBM Endpoint Manager Proxy Agent (Version 9.1.1117.0) (1816)** or **Install IBM Endpoint Manager Proxy Agent (Version 9.2.0) (1836)**, depending on your platform version.
 2. When you deploy the action, the list of applicable relays is displayed in the **Take Action** menu. Select one or more relays from the list and click **OK** to complete the installation.
 3. Run the task **Deploy Management Extender for Bare Metal Targets** (ID 150)

The plug-in is installed in the path `C:\Program Files(x86)\BigFix Enterprise\Management Extender`. The service is started automatically.

After the Bare Metal targets PXE-boot, you can view and manage them from the console. A set of tasks are available to manage these targets. For more information, see “Managing Bare Metal Targets” on page 105.

Configuring the behavior of the plug-in

You can change the behavior of the plug-in by configuring parameters in the `BareMetalExtender.ini` file

To change the reporting threshold for the bare metal targets, switch to `C:\Program Files\Common files\IBM Tivoli`. Edit the `BareMetalExtender.ini` and modify the following setting:

```
LastReportTimeThreshold=48
```

Changing the plug-in settings

You can customize parameters in the `settings.json` file.

To increase the logging level for troubleshooting purposes, edit the `C:\Program Files (x86)\Bigfix Enterprise\Management Extender\Plugins\Bare Metal Extender\settings.json` file. For example, to change the logging level from 3 to 4: `"ConfigurationOptions" -d v 4`

If you want to change the default refresh interval for retrieving bare metal target information from 10 to 15 minutes, overwrite the default value:

```
"DeviceReportRefreshIntervalMinutes": 15,
```

To change the circular logging default values, edit the `-m X:Y` setting, where `X` is the maximum file size in Megabytes, and `Y` is the maximum number of log/trace files. The default value is `-m 10:10`. For example, to change the maximum number of trace files from a value of 10 to a value of 5:

```
"ConfigurationOptions": "-d -v 3 -l \\\"C:\\Program Files\\Common Files\\IBM Tivoli\\BareMetalExtender.trc\\\" -m 10:5",
```

After you make changes to the settings in this file, you must restart the Proxy Agent service to have the modifications take effect.

Starting the service

You can start the Proxy Agent service by running the **Start Proxy Agent** Fixlet (75).

Uninstalling the plug-in

To remove the Management Extender for Bare Metal Targets, complete the following steps:

1. Run the **Remove Management Extender for Bare Metal Targets** fixlet (ID 151).
2. Remove the Proxy Agent:
 - If your relay is at IBM Endpoint Manager Platform Version 8.2 or 9.0:
 - Run the remove action of the **Deploy Proxy Agent 9.0.40099 on 8.2 or 9.0 Relay** fixlet (ID 152)
 - If your relay is at IBM Endpoint Manager Platform Version 9.1 or later:
 - From the BES Support site, run the task **TROUBLESHOOTING: Uninstall IBM Endpoint Manager Proxy Agent** (ID 1795)

Troubleshooting

Logs for troubleshooting are on each Bare Metal Server in `%CommonProgramFiles%\IBM Tivoli\BareMetalExtender.trc`. The default logging level is 3. You can change circular logging options in the `settings.json` file. See “Changing the plug-in settings ” on page 22.

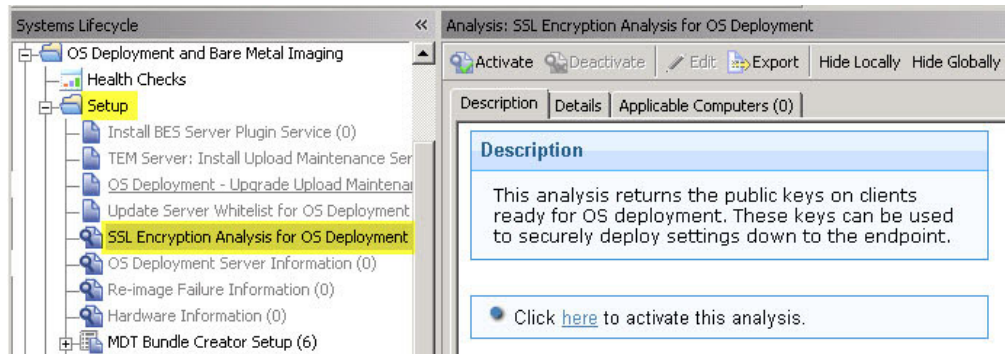
Activating Analyses

To start using OS Deployment, activate the analyses shown in the Setup node in the navigation tree. Click each analysis from the navigation tree, and then click the link provided in the analysis window to activate it.

SSL Encryption Analysis for OS Deployment

The SSL Encryption Analysis for OS Deployment is used to return the public keys on clients ready for OS deployment. These keys can be used to securely deploy settings to the endpoint.

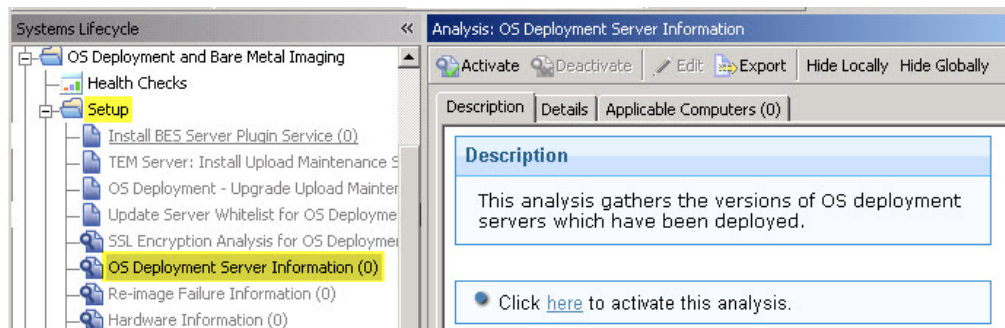
The SSL Encryption Analysis is needed only for encrypting actions to Endpoint Manager clients version 8.2, not for version 9.0 clients or later. If all clients are at version 9.0 or later, this is unnecessary.



Click the link in the Actions box to activate this analysis.

OS Deployment Server Information

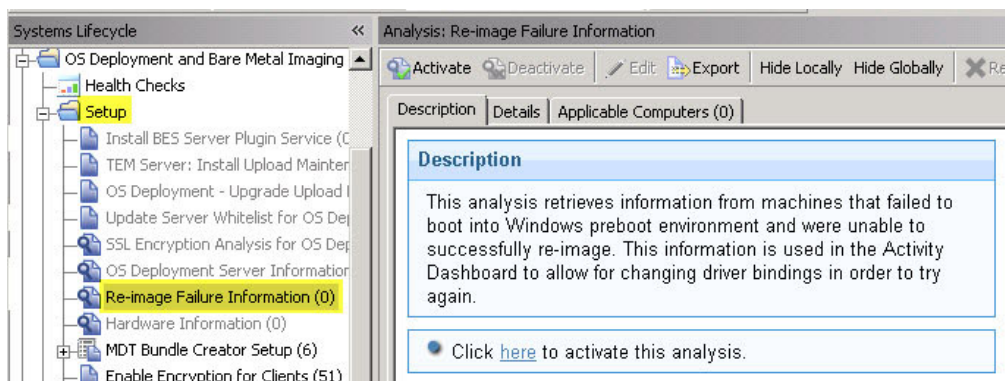
The OS Deployment Server Information is used to gather the versions of OS deployment servers that have been deployed.



Click the link in the Actions box to activate this analysis. To install an OS Deployment server, see “Managing Bare Metal OS Deployment Servers” on page 89.

Re-image Failure Information

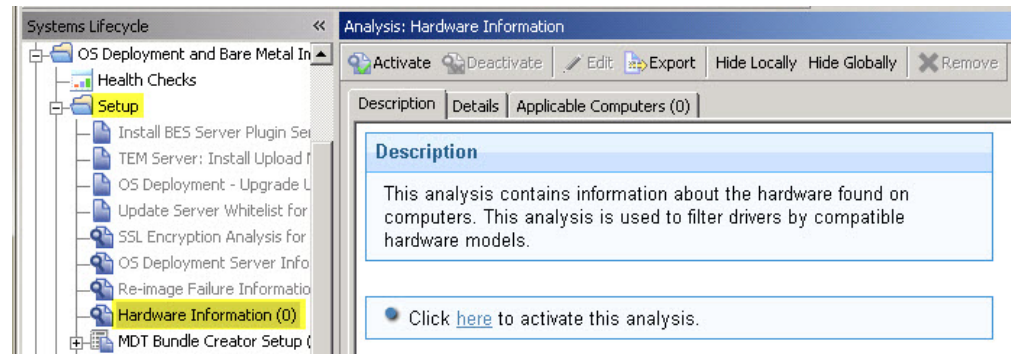
The Re-image Failure Information is used to retrieve information from machines that failed to boot into the Windows preboot environment and were unable to successfully re-image. This information is used in the Activity Dashboard to change the driver bindings and try the boot again.



Click the link in the Actions box to activate this analysis.

Hardware Information

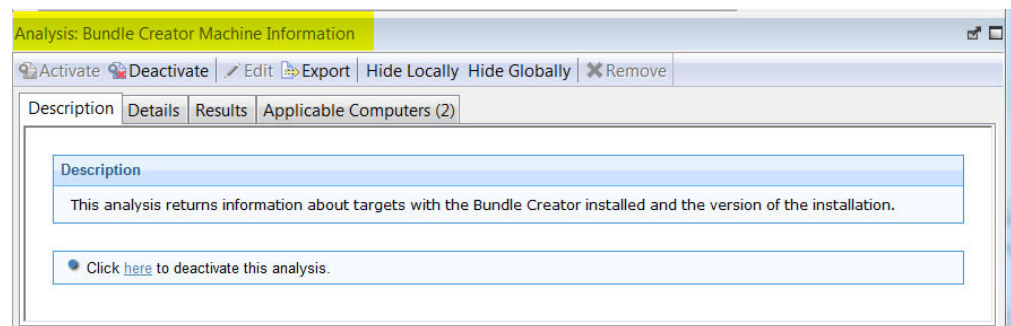
The Hardware Information analysis is used to filter drivers by compatible hardware models and to calculate which drivers are used during a deployment.



Click the link in the Actions box to activate this analysis.

Bundle Creator Machine Information

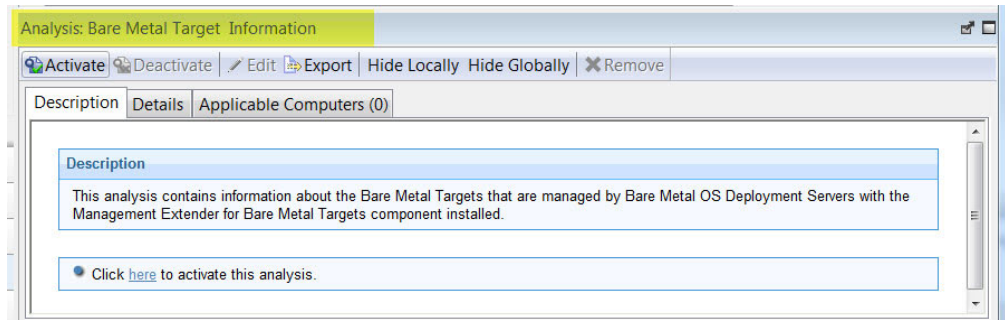
The Bundle Creator Machine Information analysis returns information about targets with the Bundle Creator installed and the version of the installation.



Click the link in the Actions box to activate this analysis.

Bare Metal Target information

This analysis contains information about the Bare Metal Targets managed by Bare Metal OS Deployment Servers with the Management Extender for Bare Metal Targets component installed.



Click the link in the Actions box to activate this analysis.

Health Checks Dashboard

The OS Deployment Health Checks Dashboard provides troubleshooting and optimization checks for OS Deployment. For both the **General** and **Bare Metal** panels, you can drill down into individual health checks to see the results and a resolution path for failing checks.

Use the Health Checks - General dashboard to see the current health status of the IBM Endpoint Manager infrastructure.

General		Overall Status: Fail
Name	Status	Severity
+ OS Deployment Site has Server Subscribed	Pass	High
+ OS Deployment Analyses Activated	Pass	High
+ BES Server Plugin Service Installed on Server	Pass	High
+ BES Server Plugin Service Running on Servers and Relays	Pass	High
+ Upload Maintenance Service (UMS) Installed on Server	Pass	High
+ Upload Maintenance Service (UMS) Updated on Server	Pass	Low
+ Server whitelist updated	Fail	High
+ Server and Relay Cache Size	Fail	High
+ MDT Bundle uploaded and up to date	Pass	Medium
+ WIM information complete	Pass	Low
+ WIM Images have compatible OS Resource	Fail	Low
+ At least one operating system image uploaded	Pass	Medium
+ At least one Windows Driver Uploaded	Pass	Medium
+ Image Provider is installed on Relays	Pass	Medium
+ Relay versions are 9.0 or greater	Pass	Medium
+ Client versions are 9.0 or greater	Pass	Low
+ OS Deployment environment is SHA256-compliant	Pass	Medium

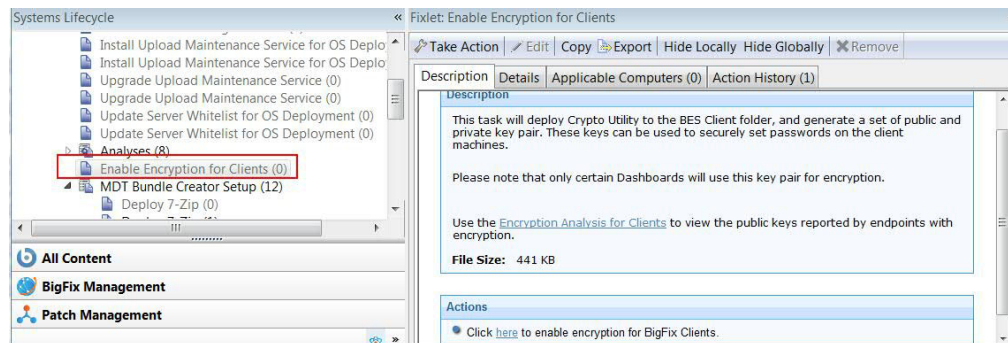
Use the Health Checks - Bare Metal dashboard to see the current health status of the IBM Endpoint Manager infrastructure if you want to install additional components for bare metal deployment.

Bare Metal		Overall Status: Fail
Name	Status	Severity
+ Servers are out of date	Pass	High
+ Servers are encrypted	Pass	High
+ Servers are relays	Pass	High
+ OS Deployment Server Services is running	Pass	High
+ BES Relay Service is running	Pass	High
+ Authentication is disabled on servers	Pass	High
+ Servers are in sync	Pass	High
- Server profiles warnings	Fail	High
Profiles on some servers may be invalid when they become out of sync.		
Results:		
Servers with profile warnings: 1		
Resolution:		
Go to the Bare Metal Server Manager dashboard to view specific details of profile warnings		
+ Server Executables Uploaded and Up to Date.	Pass	High
+ Servers have the Management Extender for Bare Metal Targets installed	Pass	Medium

If the deployment was set up correctly, all the results are shown as *Pass*. If the result of any check is *Fail*, expand the node and take the recommended action.

Enable Encryption for Clients

The Enable Encryption for clients Fixlet deploys the Crypto Utility to the BES Client folder and generates a set of public and private keys. This Fixlet is a prerequisite for the installation of Tivoli Provisioning Manager for OS Deployment Server to manage bare metal deployments in V8.2 environments. It is mandatory only if the relay on which you are installing your Bare Metal Server is Endpoint Manager version 8.2 or you have V8.2 clients in your environment. Run this Fixlet on your designated relay before installing the Bare Metal Server.



Click the link in the Actions box to enable encryption for clients.

Verifying Secure Hash Algorithm (SHA-256) readiness

IBM Endpoint Manager version 9.1 uses the SHA-256 hashing algorithm to increase file exchange security. OS Deployment manages file exchange within the application flows using SHA-256.

In Endpoint Manager V9.1, all application-specific files are managed with SHA-256. All new files uploaded by the user (images, drivers, MDT bundles etc.) and generated by the system after the installation of IBM Endpoint Manager version 9.1 are created with the SHA-256 hashing information included, and are managed accordingly. The files that were uploaded and created on earlier Endpoint Manager versions, do not have the SHA-256 information. You can continue to use these files, but file exchange will not benefit from the improved security provided by SHA-256.

If the IBM Endpoint Manager V9.1 Server is configured to allow exchange of files in SHA-256 mode only, then it will no longer be possible to use files created with earlier versions of Endpoint Manager.

To verify SHA-256 readiness, the health check named "OS deployment Environment is SHA-256 compliant" scans for files that do not have SHA-256 information. The outcome of this check can result in a warning message indicating that some files are not SHA-256 compliant. You can start an action to calculate the missing SHA-256 information and to automatically update the affected files from the Resolution section of the health check. If the action does not update one or more files, you can display the file names for further problem determination. When the action completes successfully, the status changes to "Pass". In this case, a synchronization action is automatically started to update the hashing information on Bare Metal servers in the network.

If the IBM Endpoint Management Server is configured to allow the exchange of files in SHA-256 mode only, a warning banner is also displayed in the OS Deployment dashboards, with an indication for the user if the SHA256 compliance health check status is not "Pass". Clicking on the banner opens the Health Checks dashboard from where you can start a remediation action.

Chapter 3. Managing MDT Bundles and Deployment Media for Windows targets

To perform OS Deployment of Windows operating systems, you prepare your deployment environment and resources using the Bundle and Media Manager Dashboard.

From the **Bundle and Media Manager** dashboard, you can:

- Install MDT Bundle Creators
- Create MDT Bundles
- Create Deployment Media

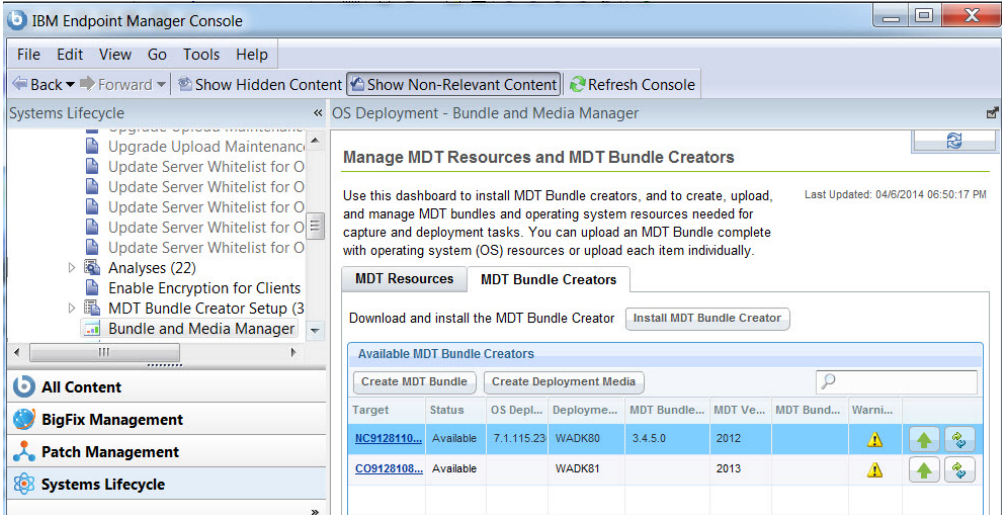
The tasks available from this dashboard provide a simplified approach to setting up your environment for Windows operating system deployments. You can download MDT Bundle Creators and their prerequisites, and create MDT Bundles in a simple, guided manner, eliminating the need to manually install the required software stack or edit the configuration parameters. You can create bundles with or without OS resources, or OS resources only. You can also create bootable CD, DVD or USB devices, to be used for offline deployments. Colored icons in the warnings column provide information about any missing prerequisites or about deprecated components.

Each task is available in a separate wizard. Each wizard is described in detail in the following sections.

Bundle and Media Manager Dashboard

You can install MDT Bundle Creators, and create MDT Bundles and Deployment Media using the Bundle and Media Manager dashboard.

To use this dashboard, you must first activate the **Bundle Creator Machine information** analysis.



The screenshot displays the IBM Endpoint Manager Console interface. The main content area is titled "Manage MDT Resources and MDT Bundle Creators" and includes instructions on how to use the dashboard. Below the instructions, there are tabs for "MDT Resources" and "MDT Bundle Creators". A button labeled "Install MDT Bundle Creator" is visible. A table titled "Available MDT Bundle Creators" is shown, with columns for Target, Status, OS Depl..., Deploye..., MDT Bundle..., MDT Ve..., MDT Bund..., and Warni... The table contains two rows of data:

Target	Status	OS Depl...	Deploye...	MDT Bundle...	MDT Ve...	MDT Bund...	Warni...
NC9128110...	Available	7.1.115.23	WADK80	3.4.5.0	2012		Warning icon
CO9128108...	Available		WADK81		2013		Warning icon

Use the **Install MDT Bundle Creator** wizard in the **MDT Bundle Creators** to select the tool combination that best suits your deployment patterns. When you select the tools, the corresponding set of supported operating systems is highlighted.

An MDT Bundle is a collection of scripts, OS resource files, and folders that are required for re-image, capture, and bare metal deployments. When you create an MDT bundle, these resources must be specified for each operating system, architecture, and Service Pack combination that you plan to deploy in your environment.

The **Create MDT Bundle** wizard detects the software stack available on the selected Bundle Creator machine. Based on the installed software, it guides you in selecting the correct resources for the creation of the MDT Bundle. The target on which the bundle is created must have either Windows Automated Installation Kit (WAIK) or Windows Assessment and Deployment Kit (WADK).

Use the **Create Deployment Media** to create network boot and offline deployment media needed to boot systems when a PXE Server is not available, and to deploy profiles to targets that are disconnected from the network. The supported media types are USB, CD, and DVD devices.

For each target , the table displays information about the following:

- which OS Deployment server is installed
- which MDT Bundle version is installed
- which Deployment kit is installed

The **Warnings** column indicates whether some prerequisites are missing, or if components are not at the required version or level for the available tasks.

You can install the MDT Bundle Creator manually, by using the **MDT Bundle Creator Setup** node. If the creators you installed manually are Endpoint Manager clients, they are displayed in the list of available MDT Bundle creators. You can also create MDT Bundles manually by customizing the required parameters in the `parameters.ini` file, and launching the MDT Bundle Creator executable. For information about manual installation and configuration, see “Creating and managing MDT bundles manually” on page 37.

Note: If you have installed MDT Bundle Creators with versions earlier than 3.4, these computers are visible in the dashboard, but the **Create MDT Bundle** wizard is disabled for these targets.

Installing MDT Bundle Creators

From the Bundle and Media Manager dashboard, you can install MDT Bundle Creators on selected targets.

In the **Bundle and Media Manager** dashboard, select the MDT Bundle Creators tab and click **Install MDT Bundle Creator** to start the wizard.

Install MDT Bundle Creator

Select the combination of tools that best suits your deployment needs

MDT Bundle Creator

WADK 8 and MDT 2012 Update 1

This combination produces WinPE 4 based bundles. This option provides the broaden platform support and it is the default choice

WADK 8.1 and MDT 2013

This combination produces WinPE 5 based bundles. Use this option if you need to deploy Windows 8.1 or Windows 2012 R2

WAIK and MDT 2012 Update 1

This combination produces WinPE 3 based bundles. Use this option if your hardware does not support WinPE 4 or later

Supported Operating Systems

The bundle creator you selected will generate bundles that can run on the following systems:

Windows XP Windows 2003

Windows Vista Windows 2008

Windows 7 Windows 2008 R2

Windows 8 Windows 2012

Windows 8.1 Windows 2012 R2

Next **Cancel**

Choose the combination of tools that best matches your deployment needs. For each choice, the list of operating systems that can be deployed is automatically selected. Click **Next**. Depending on the target you selected, additional prerequisite software can be automatically downloaded and installed. You are asked to agree to the license statements regarding this software. Click **Submit** to take action, and select one or more targets where the Bundle Creator will be downloaded.

Note: The computers on which you install the MDT Bundle creators must have direct internet access for the prerequisites to be correctly downloaded and installed with the wizard.

Creating MDT Bundles

Using this wizard, you create MDT Bundles and OS resources for your Windows deployments.

From the MDT Bundle Creators Tab, select a target and click **Create MDT Bundle**. This option is disabled if the target you selected does not have Windows Automated Installation Kit (WAIK) or Windows Assessment and Deployment Kit (WADK) installed.

From the wizard, you can choose one of the following tasks:

- Create both an MDT bundle and OS resources
- Create a new MDT bundle only
- Create new OS resources only

Depending on the tool combinations installed on your target, the wizard displays the set of parameters that you can choose from.

If you are creating OS resources, you can choose to include ISO images from a specific directory on the target, or include specific ISO image files by specifying the file names, or both. The folder you specify can be either local to the target, or a mapped drive on the target system. In the latter case, you must specify the IP address and the credentials needed to mount the drive.

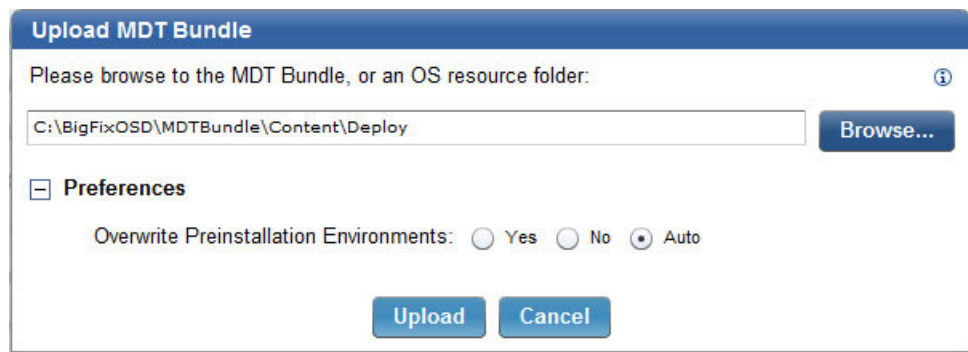
You can also create OS resources from the Image Library when you import the ISO images directly from installation media.

If you plan to re-image to Windows XP, select the corresponding option. USMT3 is required for re-imaging to XP, and you are asked to specify the path of the USMT3 installation.

Note: The **Manual** tab displays the parameters.ini file, where all specified options are stored. Editing this section incorrectly could result in failures during the upload of the MDT bundle.

When you have created your MDT Bundles, you can upload them to the Endpoint Manager Server from the **MDT Resources** tab. To upload an MDT Bundle, click **Upload MDT Bundle**.

When you upload the MDT bundle, if you expand the Preferences section, you can set the **Overwrite Preinstallation Environments** option. Select **Yes**, to overwrite Preinstallation Environments previously loaded on the server. The default setting is **Auto**. With the default setting, the Preinstallation Environments are overwritten only if the version you are uploading is the same or later than the currently saved versions.



Creating Windows Deployment Media

You can generate network boot and offline deployment media for Windows OS deployments from the Bundle and Media Manager Dashboard.

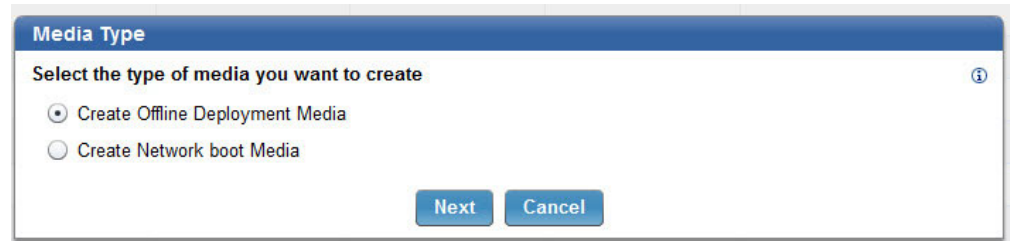
You can:

- Generate an iso file to burn a CD/DVD media
- Create a USB deployment media on a mounted USB key which can be formatted before creation.
- Generate USB key content for later creation of USB deployment media.

Depending on your selection, the CD, DVD, or USB media can include:

- **WinPE only (network boot):** In this case, when WinPE starts from the media, the target boots and connects to the Bare Metal OS Deployment (PXE) server to receive the binding menu.
- **WinPE and one or more bootable images (offline deployment):** In this case, once the boot operation has completed on the target, the binding menu is displayed. The user at the target can select the profile to deploy from the media.

Depending on the Windows Deployment Kit installed on the target you select, the correct version of Windows Preinstallation environment (WinPE) is downloaded from the specified Bare Metal OS Deployment Server and included in the media.



Note: The OS Deployment Server from which you download the files needed for creating the media must be at Version 7.1.1.17 or later.

Creating network boot media

In situations where a DHCP server is not available, or when there is a firewall preventing PXE traffic, the use of network boot media is particularly useful.

To create a network boot CD/DVD or USB media complete the following steps:

1. On the Media Type panel, select the target, then select **Create Network Boot Media**, and click **Next**.
2. Select the OS Deployment server from which the files used to create the media will be downloaded, and click **Next**.
3. Depending on the deployment kit that is installed on the selected target, the **Create Deployment Media** panel displays the version of WinPE that will be included in the media. You can specify, select, or change the following settings:
 - The OS architecture, and if you want all available WinPE drivers to be included in the media
 - You must specify the password of the administrative user on the OS Deployment Server you selected in the previous panel. This is the Server from which the WinPE is downloaded.
 - The type of media : CD/DVD, mounted USB key, or USB key content. You can optionally select to format the USB mounted media. For the USB content, you must specify a target directory. Two scripts are downloaded in the specified target directory, **formatUSB.cmd** and **MakeUSB.cmd** Depending on your selections, some restrictions may apply. See Network boot media limitations.
 - The connection details for the target PXE boot. By default, the OS Deployment server that the target contacts when the PXE boot operation is complete is automatically discovered. You can specify the connection parameters either explicitly or at boot time. You must always specify the password of the administrative user on the OS Deployment Server.

- You can optionally specify to have the user start the boot sequence on the target. In this case, a prompt is displayed on the target and the boot sequence begins only when the user responds to the prompt.
4. When you have completed your selections, click **OK**. The information you provided is validated before the media creation task begins.

Network boot media limitations: The following restrictions apply to network boot media:

- If you select the USB Key content media type, you must format the USB key with a single bootable FAT32 partition of at least 512 Megabytes. To format the USB key, you can use the **formatUSB.cmd** script. USB keys that are formatted as NTFS file systems are not supported on UEFI targets.
- If you select mounted USB key and no formatting option, for the key to work on UEFI targets, you must have previously formatted the key with a single bootable FAT32 partition of at least 512 Megabytes.

Creating offline deployment media

Offline deployment media can be used when the target has no connection to the OS Deployment Server or when the network connection is slow. Some typical situations are small branch offices with slow links and no local deployment server, isolated computers disconnected from an internal network, or laptop users that cannot connect to the Local Area Network or are using a modem. When you create offline deployment media, all necessary files for the deployment are downloaded.

Note: Offline Deployment media is not supported for Windows XP targets.

From the **Bundle and Media Manager** dashboard, click the **MDT Bundle Creators** tab, select a target from the list and click **Create Deployment Media**. The Media Type panel is displayed:

To create an offline deployment CD/DVD or USB media complete the following steps:

1. On the Media Type panel, select the target, then select **Create Offline Deployment Media**, and click **Next**.
2. In the **OS Deployment Server and Bare Metal Profile** pane, select the OS Deployment Server from which the files used to build the media will be downloaded.
3. The Bare Metal Profiles available at the selected OS deployment server are displayed. The profiles that you can choose from are those that meet the following requirements:
 - contain MDT Bundle Version 3.6 or later with the level of WinPE compatible with the deployment kit installed on the target where you are creating the media.
 - contain OS images that are compatible with the deployment kit installed on the target where you are creating the media.

Profiles that do not meet these criteria are not displayed. Select one or more profiles to include in the media you are creating . Click **Next**.

4. In the **Create Deployment Media** panel, some selections are already made, based on your input in the previous panel.

- You must specify the password of the administrative user on the OS Deployment server that you selected in the previous panel. The password is needed only if the target used for creating the media is not an OS Deployment server.
 - Select the type of media you want to create. If you select the USB Key content, you must specify an output directory. Two scripts are downloaded in the specified directory, **formatUSB.cmd** and **MakeUSB.cmd**. Depending on the selected media type, some restrictions may apply. See Offline deployment media limitations
 - You can optionally specify to have the user start the boot sequence on the target. In this case, a prompt is displayed on the target and the boot sequence begins only when the user responds to the prompt.
5. When you have completed your selections, click **OK**. The information you provided is validated before the media creation task begins.

Offline deployment media limitations: The following restrictions apply to offline deployment media:

- CD/DVD media types are not supported for deployment on UEFI targets.
- If your media type is a mounted USB key:
 - if you select the **Format the USB key** option, there is a restriction requiring that USB media be seen as a fixed disk and not as removable. Typically, Flash Drive USB cards are seen as fixed disks and can be used.
 - If you do not choose the formatting option, you must have previously formatted the key with two partitions, of which the first must be a bootable FAT32 partition of at least 512 Megabytes, and the second partition a non-bootable NTFS partition, large enough to store the selected images. The USB media must be seen as a fixed disk and not as removable.
- If your media type is USB Key Content:
 - If you want to use the key for deployments on UEFI targets, you must format the USB key with two partitions, of which the first must be a bootable FAT32 partition of at least 512 Megabytes, and the second partition a non-bootable NTFS partition, large enough to store the selected images. The USB key can also be formatted with a single partition. In this case, if you want to use it on UEFI targets, the partition must be FAT32 and not NTFS. To format the key you can use the **formatUSB.cmd** script, and you can populate the contents using the **makeUSB.cmd** script.

Note: To complete the operating system deployment successfully on the target, ensure that the hard disk device on your target is configured before the CD/DVD or USB media device in the boot sequence. Then force the boot from the media device to start the deployment. Alternatively, only for CD/DVD media, select the **Boot at User Request** option during the creation of the media.

Formatting and loading USB key content

When you are creating network boot or offline deployment USB key content, all files needed for booting from the network or for offline deployments of operating systems on targets are stored in the specified folder on the selected target. In this path, two scripts named **formatUSB.cmd** and **makeUSB.cmd** are downloaded. You can run these scripts to format and load the folder content on the USB key. To run the scripts, open a Windows shell with administrative privileges.

Offline deployment media preparation:

formatUSB.cmd

Use this script to format your offline deployment USB key with a bootable FAT32 partition and a non-bootable NTFS partition.

Complete the following steps:

1. Insert the USB key. The USB key must be empty, and identified as a local disk.
2. Run the script from a shell with administrative privileges by specifying the drive letter assigned to it, an additional drive letter which is not currently assigned to another disk, and the disk number. For example:

```
formatUSB.cmd F G 1
```
3. When the formatting step completes, use the **makeUSB.cmd** script to complete the USB key preparation.

Run the script without arguments to view the disk configuration. The disk numbers are displayed in the first list. The drive letter is displayed in the second list. The letter must be identified as type 'Partition'.

makeUSB.cmd

Use this script to populate your bootable offline deployment USB key:

1. Insert the USB key. The key must have been previously formatted with a bootable FAT32 partition and an additional NTFS partition. You can use **formatUSB.cmd** to format the key.
2. Run the script from a shell with administrative privileges, by specifying the USB key drive letters. The first letter must be the FAT32 partition. For example:

```
makeUSB.cmd F G
```

You can use a USB key with a single partition. For the key to work on UEFI targets it must be formatted FAT32 , not NTFS. For example:

```
makeUSB.cmd F
```

Network boot media preparation:

formatUSB.cmd

Use this script to format your network boot USB key with a single bootable FAT32 partition:

1. Insert the USB key. the key must be empty.
2. Run the script from a shell with administrative privileges, by specifying the drive letter that is assigned to the USB key, and the disk number. For example:

```
makeUSB.cmd F 1
```
3. When the formatting step completes, use the **makeUSB.cmd** script to complete the USB key preparation.

Run the script without arguments to view the disk configuration. The disk numbers are displayed in the first list. The drive letter is displayed in the second list. The letter must be identified as type 'Partition'.

makeUSB.cmd

Use this script to populate your network boot USB key:

1. Insert the USB key.
2. The USB key must have been previously formatted with a single bootable FAT32 partition. You can use **formatUSB.cmd** script to format the key.
3. Run the script from a shell with administrative privileges, by specifying the USB drive letter. For example:

```
makeUSB.cmd F
```

Important: When you run **formatUSB.cmd**, ensure that you specify the correct disk number and drive letter. Failure to do so may cause unrecoverable damage to your computer. All partitions on the USB key will be erased.

Creating and managing MDT bundles manually

Use the Fixlets and tasks in the MDT Bundle Creator Setup node to manually prepare your environment for creating MDT bundles.

You can download and run the MDT Bundle Creator tool on an Endpoint Manager client, or on any other computer of your choice, providing it connects to the external network, and meets specific system requirements and prerequisites. If you run the tool on a client, there are Fixlets and tasks that install the required prerequisites and components for you.

If your designated computer is not an Endpoint Management client, then you must download the MDT Bundle creator tool manually and install the needed prerequisites, by following the process described in “MDT Bundle creation process” on page 38.

If you are setting up the MDT Bundle on an Endpoint Manager client, from the **Setup** node, expand **MDT Bundle Creator Setup** to display the required fixlets and tasks.

To prepare your client system to run the MDT Bundle Creator Tool, run the required Fixlets and tasks in the order shown, then launch the MDT Bundle creator tool to create your MDT bundle, and finally upload the bundle to the IBM Endpoint Management server.

Note that some fixlets might not be relevant if the selected client already has the corresponding prerequisites at the required level.

1. **Deploy 7-Zip**

Downloads the 7-zip compression and decompression tool to the selected computer.

2. **Deploy Microsoft .NET Framework**

Installs Microsoft .NET framework on the selected computer. It is a prerequisite to the installation of PowerShell.

3. **Deploy PowerShell**

Installs PowerShell on the selected computer. It is needed to automate the sequence of creation steps.

4. **Deploy Windows Automated Installation Kit (WAIK)**

downloads and installs the Windows Automated Installation Kit (for use with MDT 2012 Update 1) on the selected computer.

or

Deploy Windows Assessment and Deployment Kit (WADK)

Downloads and installs either WADK8 (for use with MDT 2012 Update 1) or WADK 8.1 (for use with MDT 2013) on the selected computer.

Note: The choice of which kit to download depends on the operating systems you are planning to deploy. See “MDT bundles and possible component combinations” on page 40. WAIK and WADK cannot coexist on the same computer.

5. Deploy MDT 2012 Update 1

Run this Fixlet on the selected computer if you installed WAIK or WADK 8 in the previous step.

or

Deploy MDT 2013

Run this Fixlet on the selected computer if you installed WADK 8.1 in the previous step.

6. Deploy MDT Bundle Creator.

When you run the MDT Bundle Creator task from the OS Deployment and Bare Metal Imaging site, a folder containing all the MDT bundle creator tool executables and documentation is created. The folder is located in the path %Drive of TEM Client%\OSDSETUP. You can also download the MDT Bundle tool manually to your computer. In this case, a compressed file is downloaded to the specified path and you must extract its contents.

7. Follow the steps described in “MDT Bundle creation process” to launch the MDT bundle creator tool on the selected computer.

If you are using XP mass storage drivers, see “Prepare and add XP mass storage drivers” on page 50 before you run the tool.

8. Upload the MDT Bundle to the IBM Endpoint Management Server from the Upload MDT Bundle Dashboard.

MDT Bundle creation process

To create your deployment bundle using the MDT Bundle creator, you must customize a parameter file with the required options.

You use the MDT Bundle Creator tool to create any of the following:

- An MDT Bundle that does not include any OS resource.
- An MDT Bundle that includes one or more OS resources.
- One or more OS resources only.

Depending on what you are creating with the MDT Bundle creator tool, you must specify the corresponding parameters in the parameters.ini file, before you run it. The process is described in the following steps:

1. Download the appropriate version of the MDT Bundle Creator. If you download the tool manually, extract the file into a clean directory.
2. Check that you have all the required prerequisites, as detailed in “Prerequisites” on page 39.
3. Edit the parameters.ini configuration file. The parameters.ini file is used to specify a target output directory and the locations of prerequisites and OS resources. All available configuration options are in “MDT Bundle Creation Options” on page 42. The only mandatory parameters are listed in the General section of the file.

4. Run the appropriate MDT Bundle Creator for your architecture from within the extracted directory as an Administrator. Run `MDTBundlCreator.exe` or `MDTBundlCreator64.exe` depending on your architecture. A `setup.log` file is created in this directory.

Important: If an Antivirus program is running simultaneously with the MDT Bundle Creator, the resulting bundle might be corrupted, causing the upload step to fail. You must stop or temporarily disable the Antivirus program before running the tool and for the time needed to complete the bundle creation process.

The bundle creation process takes about 30 to 60 minutes to complete and results in the creation of the `MDTBundl` folder beneath the directory specified as the target in `parameters.ini` configuration file.

5. Upload the MDT bundle on the Endpoint Management Server. See “Upload MDT Bundle Dashboard” on page 45.

Prerequisites

If you have downloaded the MDT Bundle creator tool manually, make sure you have installed all the correct prerequisites before you run the tool.

If you choose to create your MDT bundles on an Endpoint Management client, you can download prerequisites by running the Fixlets described in “Creating and managing MDT bundles manually” on page 37. If you download the MDT Bundle Creator on a computer which is not part of your Endpoint Management network, you must ensure that the following prerequisites are installed before you run the tool.

The following list includes system requirements and prerequisites for using the MDT Bundle Creator tool:

- Windows 7, Windows 8, Windows 8.1, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows Vista Service Pack 2, Windows Server 2008 Service Pack 2, Windows Server 2003 R2.
- MMC 3.0 is required to run the Workbench and view the documentation on Windows XP. MMC 3.0 is included in Windows Vista and later.
- MSXML 6.0.

Additionally, you use PowerShell to automate the sequence creation steps. PowerShell is available with Windows Server 2008, but must be installed on Windows Server 2003. (.Net is required by PowerShell.)

- Powershell can be downloaded from the following url: <http://support.microsoft.com/kb/926140>.

Finally, 7zip is required:

- 7zip can be downloaded from the following url: <http://www.7-zip.org/download.html>.

Note: The license for 7-zip is LGPL and can be found at the following url: <http://www.7-zip.org/license.txt>.

When all prerequisites are satisfied, download and install the following components:

- Microsoft Deployment toolkit 2012 Update 1 from the following url: <http://www.microsoft.com/en-us/download/details.aspx?id=25175> or Microsoft Deployment Toolkit 2013 from the following url: <http://www.microsoft.com/en-us/download/details.aspx?id=40796>.
- Windows Assessment and Deployment Kit (ADK) for Windows 8 from the following url: <http://www.microsoft.com/en-us/download/details.aspx?id=30652>. or Windows Assessment and Deployment Kit (ADK) for Windows 8.1 from the following url: <http://www.microsoft.com/en-us/download/details.aspx?id=39982>.

Important: Prior to installing Windows ADK, ensure that WAIK is not installed.

You must include the following required Windows ADK components:

- Windows Preinstallation Environment (Windows PE)
- Deployment Tools
- User State Migration Tool (USMT).

You will also need an ISO file of the installation source for the operating systems you plan to deploy. The supported Microsoft operating systems are:

- Windows XP Professional 32-bit
- Windows XP Professional 64-bit
- Windows Vista 32-bit
- Windows Vista 64-bit
- Windows 7 32-bit
- Windows 7 64-bit
- Windows 8 32-bit
- Windows 8 64-bit
- Windows 8.1 32-bit
- Windows 8.1 64-bit
- Windows Server 2003 SP2 (x86, x64)
- Windows Server 2003 R2 SP2 (x86, x64)
- Windows Server 2008 (x86, x64)
- Windows Server 2008 R2 (x64)
- Windows Server 2012 (x64)
- Windows Server 2012 R2 (x64)

MDT bundles and possible component combinations

The following table lists the valid combinations for components using the MDT Bundle Creator Tool 3.6, and Tivoli Provisioning Manager for OS Deployment Version 7.1.1.17. For each combination, there is a corresponding list of operating systems that you can deploy.

Table 1. Valid component combinations for MDT Bundle Creator

MDT Bundle Creator	Microsoft Deployment Toolkit	WIM Toolkit	Operating Systems
MDT Bundle Creator 3.6 ¹	2013	WADK 8.1(WinPE 5)	<ul style="list-style-type: none"> • Windows 8.1 • Windows 8 • Windows 7 • • Windows Server 2012 R2 ² • Windows Server 2012 • Windows Server 2008 R2
	2012	WADK 8(WinPE 4)	<ul style="list-style-type: none"> • Windows 8 • Windows 7 • Windows Vista • Windows XP • Windows Server 2012 • Windows Server 2008 R2 • Windows Server 2008 • Windows Server 2003
	2012	WAIK (WinPE 3)	<ul style="list-style-type: none"> • Windows 7 • Windows Vista • Windows XP

Notes:

1. MDT Bundle Creator 3.6 supersedes all previous versions
2. Windows 2012 R2 is supported only with MDT Bundle Creator 3.4 or later.

Target operating systems for re-imaging and bare metal provisioning

The following table lists, for each supported operating system, the component combinations you can use for re-imaging and bare metal deployments.

Table 2. Target operating systems and component combinations for re-imaging and bare metal provisioning

Operating System	MDT Bundle Creator ¹	Microsoft Deployment Toolkit	WIM Toolkit
Windows 8.1 ²	3.6	2013	WADK 8.1 (WinPE 5)
Windows 8	3.6	2013	WADK 8.1 (WinPE 5)
	3.6	2012	WADK 8 (WinPE 4)

Table 2. Target operating systems and component combinations for re-imaging and bare metal provisioning (continued)

Operating System	MDT Bundle Creator ¹	Microsoft Deployment Toolkit	WIM Toolkit
Windows 7 ³	3.6	2013	WADK 8.1 (WinPE 5)
	3.6	2012	WADK 8 (WinPE 4)
	3.6	2012	WAIK (WinPE 3)
Windows Vista	3.6	2012	WADK 8 (WinPE 4)
	3.6	2012	WAIK (WinPE 3)
Windows XP	3.6	2012	WADK 8 (WinPE 4)
	3.6	2012	WAIK (WinPE 3)
Windows Server 2012 R2	3.6	2013	WADK 8.1 (WinPE 5)
Windows Server 2012	3.6	2013	WADK 8.1 (WinPE 5)
	3.6	2012	WADK 8 (WinPE 4)
Windows Server 2008 R2	3.6	2013	WADK 8.1 (WinPE 5)
	3.6	2012	WADK 8 (WinPE 4)
Windows Server 2008	3.6	2012	WADK 8 (WinPE 4)
Windows Server 2003	3.6	2012	WADK 8 (WinPE 4)

Notes

1. MDT Bundle Creator 3.6 supersedes 3.5 and earlier versions.
2. Direct re-imaging from Windows XP or Windows Vista to Windows 8.1 is not supported. It must be done as a two-step process. You must first re-image the target to Windows 7 or Windows 8, and subsequently re-image to Windows 8.1.
3. When re-imaging from Windows XP to Windows 7, WinPE5 is not supported.

Note: MDT 2013 requires WADK 8.1

For a complete list of WinPE versions and Operating System support, see the information provided at this url: <http://technet.microsoft.com/en-us/library/dn293271.aspx>

MDT Bundle Creation Options

You must customize your MDT deployment bundle by specifying the required options in the `parameters.ini` configuration file.

The following sections include parameters that you specify to set up and customize your MDT Bundle.

Note: All section and option names are case-sensitive.

General

This section of the `parameters.ini` file contains the general options. These are mandatory, unless otherwise specified.

target Specifies a directory under which the MDTBundle and DeploymentShare directories are created. If this directory does not exist, it is created. For example, C:\BigFix OSD.

debug Set to 0 to turn off debugging, 1 to turn on light debugging, 2 to turn on high debugging (requires some user interaction).

wimtoolkit

Specify the Windows Kit to use for the creation of the MDT bundle. The kit that you specify must exist on the system where you are running the tool. Possible values are:

WADK80

To use Windows Assessment and Deployment Kit Version 8.0.

WADK81

To use Windows Assessment and Deployment Kit Version 8.1.

WAIK To use Windows Automated Installation Kit.

usmt4x86location

Specify the path of USMT Version 4 (32-bit). These files are necessary to migrate user data from Vista computers - and refer to a previous installation of Windows AIK

usmt4x64location

Specify the path of USMT Version 4 (64-bit). These files are necessary to migrate user data from Vista computers - and refer to a previous installation of Windows AIK.

usmt301x86location

Specifies the path of USMT Version 3 (32-bit). This parameter must be specified only if you are re-imaging to Windows XP. It is optional in all other cases.

usmt301x64location

Specifies the path of USMT Version 3 (64-bit). This parameter must be specified only if you are re-imaging to Windows XP. It is optional in all other cases.

Note: Ensure that you have USMT versions 4 and 5 available prior to deployment. USMT 5 is included in the Windows ADK installation, USMT 4 must be specified to re-image to Windows Vista. USMT 3 is mandatory only if you are re-imaging to Windows XP.

MDTsources

This section specifies the locations of the OS resources (ISO files) that are used to create the DeploymentShare and MDTBundle. You can add an arbitrary number of media, but only a maximum of one per OS, architecture, and operating system service pack will be included in the resulting MDT Bundle. Windows XP resources are language-specific.

media1

Specifies an install media path for the OS resources. See the examples and explanations in the parameters.ini file. For additional media paths, use media2, media3, and so on.

media1_locale

For Windows server 2003 only. Specifies the language code for the Windows Server 2003 install media, indicated by the "media1" key. You

can find language codes at the following web address:
[http://msdn.microsoft.com/en-us/library/ms533052\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/ms533052(v=vs.85).aspx).

mediaisodir

Specifies the full local path to the directory containing the ISO images.

createmediaonly=yes

Specifies whether only OS resources are to be generated for the specified media items. This parameter places the OS resources in the target directory and does not create an MDT bundle.

WinPECustom

The WinPECustom section allows for the advanced customization of the preinstallation environment that is generated by this tool. You can place custom content into WinPE and have commands run at the beginning and end of the WinPE sequence. You can specify the following parameters:

sourcePath

path that is copied into the Windows PE.

destinationFolder

Windows PE root folder that contains the custom content.

preCommand

optional command that runs before starting the WinPE sequence.

postCommand

Optional command to run before rebooting.

```
sourcePath=C:\customContent  
destinationFolder=customScript  
preCommand=call X:\customScript\prerun.bat  
postCommand=call X:\customScript\postrun.bat
```

These example parameters copy all the files from C:\customContent so that Windows PE will have them under X:\customScript.

call X:\customScript\prerun.bat is started before task execution.

call X:\customScript\postrun.bat is started after task execution.

xpMassStoragex86

This section allows Windows XP x86 mass storage drivers to be specified. To deploy Windows XP images onto computers that require mass storage drivers that do not come standard in Windows XP, you must add these drivers to the image at capture time. The drivers specified in this section are automatically installed on Windows XP x86 computers before capturing.

location

A directory containing XP Mass Storage Drivers for x86. Only device IDs applicable to x86 are added. Any others are silently skipped.

force Forces x64 device IDs to also be added.

xpMassStoragex64

This section allows Windows XP x64 mass storage drivers to be specified. To deploy Windows XP images onto computers that require mass storage drivers that do not come standard in Windows XP, you must add these drivers to the image at

capture time. The drivers specified in this section are automatically installed on Windows XP x64 computers before capturing.

location

A directory containing XP Mass Storage Drivers for x64. Only device IDs applicable to x64 are added. Any others are silently skipped.

force Forces x86 device IDs to also be added.

Upload MDT Bundle Dashboard

From this dashboard you upload the MDT resource bundle and any operating system resources needed for your deployments.

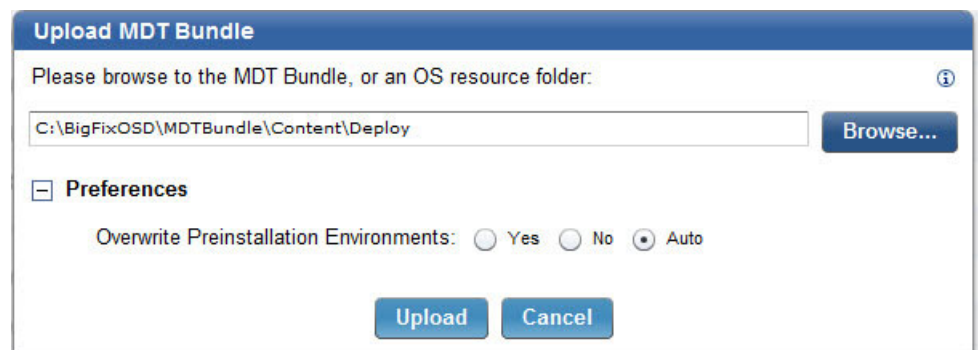
Upload previously created MDT resource bundles using the Upload MDT Bundle dashboard. After you create the deployment bundle, browse to that directory on your computer. Upload only the **MDTBundle\Content\Deploy** directory from this location. Click **Upload MDT Bundle** to load the directory onto the IBM Endpoint Manager server and complete the upload process using the console.

Operating system resources are created from Windows installation media by the MDT Bundle Creator. The resources can be left in the output of the MDT Bundle Creator and uploaded at the same time, or they can be moved elsewhere and uploaded separately. The OS resources loaded separately are identified by **Resource Type** "OS Resource" in the dashboard.

An operating system resource is required for each operating system, architecture, or Service Pack combination that you plan to manage with OS Deployment. Single resources can be uploaded by specifying an individual resource folder such as W7X86SP0 or XPX64SP2.

Note: Individual OS Resources must have been created in previous runs of the MDT Bundle Creator and can be found in the generated Deploy folder under MDTBundle\Content\Deploy\Operating Systems.

When you upload the MDT bundle, if you expand the Preferences section, you can set the **Overwrite Preinstallation Environments** option. Select **Yes**, to overwrite Preinstallation Environments previously loaded on the server. The default setting is **Auto**. With the default setting, the Preinstallation Environments are overwritten only if the version you are uploading is the same or later than the currently saved versions.



Manage MDT Bundle

This dashboard helps upload and manage the MDT resource bundle and operating system resources needed for deployment and capture tasks. You can choose to upload a MDT bundle complete with operating system resources or upload each item individually.

Last Updated: 01/21/2014 04:13:47 PM

Resources						
+ Upload MDT Bundle Delete (0)						
<input type="checkbox"/>	Name	Resource Type	Resource Info	Date Uploaded	Size	Warnings
<input checked="" type="checkbox"/>	MDT_wadk81 (3.3.04)	MDT Bundle	PE 5.0, MDT 2013	Mon, 16 Dec 2013 02:27:38 PM	106.93 MB	
<input type="checkbox"/>	MDT_waik (3.3.01)	MDT Bundle	PE 3.0, MDT 2012	Fri, 15 Nov 2013 04:26:47 PM	81.01 MB	
<input type="checkbox"/>	Sab03 (3.2.20)	MDT Bundle	PE 4.0, MDT 2012	Tue, 05 Nov 2013 03:10:25 PM	93.24 MB	
<input type="checkbox"/>	w7x64(3.3.01) (3.3.01)	MDT Bundle	PE 3.0, MDT 2012	Wed, 11 Dec 2013 05:18:32 PM	81.41 MB	
<input type="checkbox"/>	w7x86 (3.3.01)	MDT Bundle	PE 3.0, MDT 2012	Tue, 19 Nov 2013 02:16:14 PM	81.41 MB	
<input type="checkbox"/>	w8x86 (3.2.20)	MDT Bundle	PE 4.0, MDT 2012	Thu, 28 Nov 2013 04:57:07 PM	93.25 MB	
<input type="checkbox"/>	w8x86_OSres (3.2.20)	MDT Bundle	PE 4.0, MDT 2012	Mon, 02 Dec 2013 02:33:40 PM	93.25 MB	
<input type="checkbox"/>	Windows Vista x64 SP2	OS Resource		Thu, 05 Dec 2013 04:10:13 PM	229.75 MB	
<input type="checkbox"/>	Windows 7 x64 SP1	OS Resource		Wed, 11 Dec 2013 05:23:20 PM	245.90 MB	
<input type="checkbox"/>	Windows 7 x86 SP1	OS Resource		Tue, 19 Nov 2013 02:20:32 PM	217.98 MB	
<input type="checkbox"/>	Windows 8.1 x64 SP0	OS Resource		Fri, 17 Jan 2014 12:09:19 PM	399.15 MB	
<input type="checkbox"/>	Windows 8 x64 SP0	OS Resource		Mon, 16 Dec 2013 02:34:46 PM	340.59 MB	

For each resource of **Resource Type** "MDT Bundle", the **Resource Info** column displays the Windows PE version included in the bundle.

You can upload multiple MDT bundles. When you upload a bundle, you can specify a name and set it as a default MDT bundle. You can also edit these settings after creating the MDT Bundle.

Edit MDT Bundle: MDT_3307_WADK81

Please name the MDT Bundle to be uploaded.

Name

Make this MDT Bundle the default

Troubleshooting MDT Bundle errors

This topic describes how to troubleshoot errors in the MDT bundle creation process, describing a solution or workaround, if available.

Upload MDT Bundle fails when an antivirus program is running

If an antivirus program is running on the computer during the MDT bundle creation, the upload MDT Bundle task fails with the following error messages in `rbagent.trc`:

```
2013/10/30 00:19:40] A <ERR>; Command ["C:\Program Files\Windows Kits\8.0\Assessment and Deployment Kit\Deployment Tools\x86\DISM\dism.exe" /Image:"C:\Users\AALORE 1\AppData\Local\Temp\tpm_2ACAF972294C2089_1" /Add-Package/PackagePath:"C:\Program Files\Windows Kits\8.0\Assessment and Deployment Kit\Windows Preinstallation Environment\x86\WinPE_OCs\winpe-setup.cab" /PackagePath:"C:\Program Files\Windows Kits\8.0\Assessment and Deployment Kit\WindowsPreinstallation Environment\x86\WinPE_OCs\winpe-setup-client.cab" /PackagePath:"C:\Program Files\Windows Kits\8.0\Assessment and Deployment Kit\Windows Preinstallation Environment\x86\WinPE_OCs\winpe-setup-server.cab" /PackagePath:"C:\Program Files\Windows Kits\8.0\Assessment and Deployment Kit\WindowsPreinstallation Environment\x86\WinPE_OCs\winpe-legacysetup.cab" /PackagePath:"C:\Program Files\Windows Kits\8.0\Assessment and Deployment Kit\Windows Preinstallation Environment\x86\WinPE_OCs\winpe-wmi.cab" /English] failed with exit code 5 in 32.39 seconds
2013/10/30 00:19:40] A <ERR>; Command error: Unknown error, Error when installing some packages in WinPE: Error code (5)
2013/10/2013/10/30 00:19:40 A <ERR>;Error raised by AddPackages in load.rbc, line 3618 [:0]
2013/10/2013/10/30 00:19:40 A <ERR>;Unknown error (Error when installing some packages in WinPE: Error code (5))
2013/10/2013/10/30 00:19:40 A <WRN>;(called from MakeWPESoftware (load.rbc:3626))
2013/10/2013/10/30 00:19:40 A <WRN>;(called from MakeWPE (load.rbc:3969))
```

```
2013/10/2013/10/30 00:19:40 A <WRN>;(called from RAD_temmakewpe (load.rbc:4038))
2013/10/2013/10/30 00:19:40 A <WRN>;(called from AgentDispatch (rbagent.rbc:4079))
2013/10/2013/10/30 00:19:40 A <WRN>;(called from --toplevel-- (rbagent.rbc:4317))
2013/10/2013/10/30 00:19:40 A <ERR>;RbAgent command rad-temmakewpe has failed [AGT:4086]
```

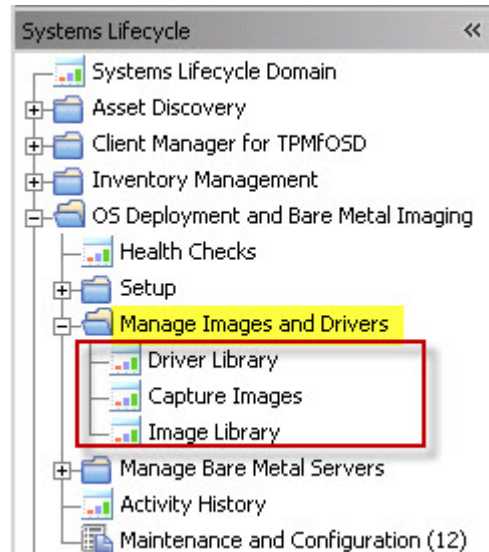
Workaround:

On the machine where you run the MDT Bundle creator tool: you can either temporarily disable the antivirus program for the time necessary to create the bundle, or you can configure the antivirus program to allow the WAIK or WADK (dism.exe) program to run.

Chapter 4. Managing Images and Drivers

The Manage Images and Drivers node includes tasks to prepare drivers and images for deployment to targets.

The **Manage Images and Drivers** node in the navigation tree includes dashboards for managing your drivers, capturing Windows images, and importing and deploying Linux or Windows images to selected targets.



To successfully deploy images to your targets, you must complete some or all of the following tasks, depending on whether you are re-imaging Windows or Linux targets:

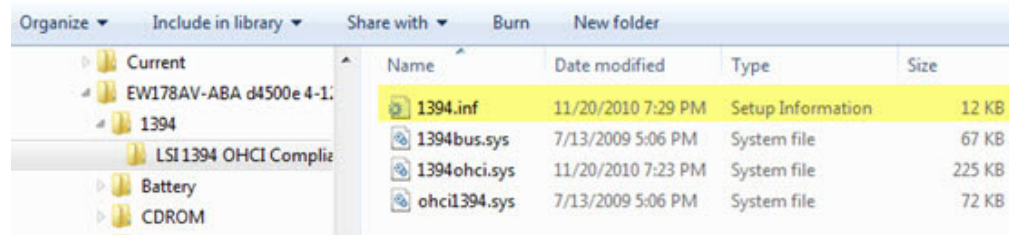
- Prepare drivers for Windows deployments, see “Preparing drivers for Windows deployments.”
- Import and manage drivers for Windows Deployments, see “Importing and managing drivers for Windows deployments” on page 50.
- Manage driver bindings for Windows deployments, see “Managing Windows driver bindings” on page 54
- Capture Windows images from a reference machine, see “Capturing Windows Images” on page 56
- Import images for Windows and Linux deployments, see “Importing Windows and Linux images” on page 60

Preparing drivers for Windows deployments

To prepare your drivers for import, you must gather them and then extract them into the correct format.

First, gather the drivers for the models in your deployment. Each driver must be in an uncompressed format. You might be required to extract a driver package if it is in an archived form (cab or zip) or if it is an executable file. Each driver must have an INF file and be in its own folder.

Regardless of how you extract the driver, a sample folder hierarchy of drivers might be as the following:



Prepare and add XP mass storage drivers

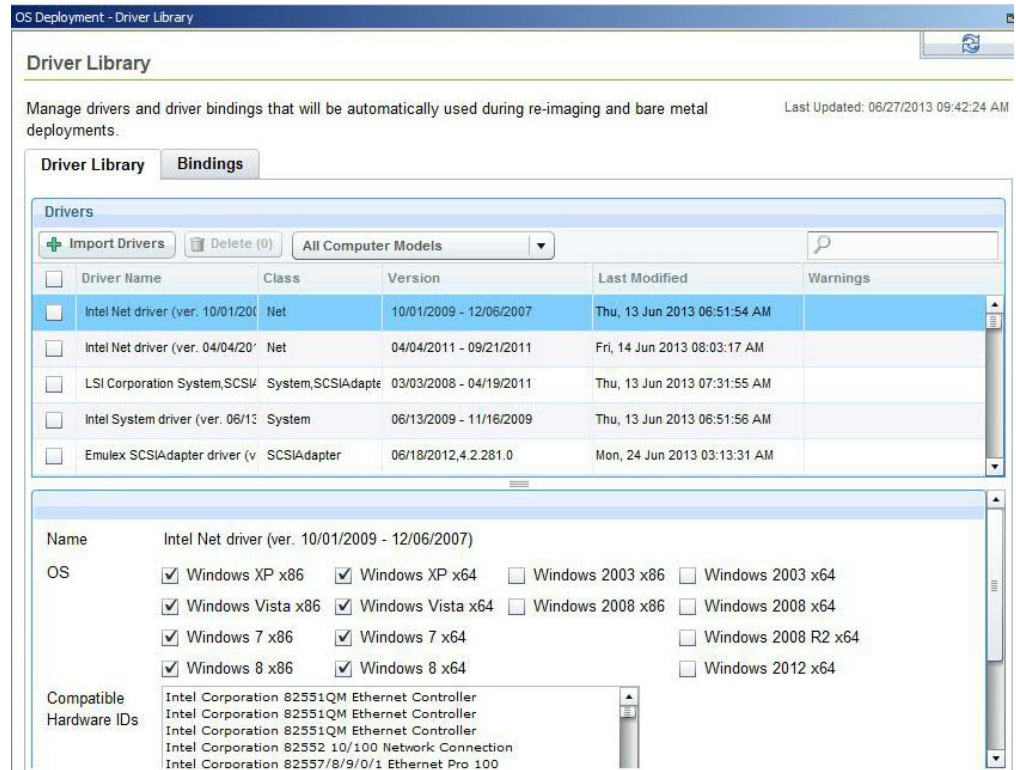
XP mass storage drivers must be handled differently from all other drivers because they must be included in the WIM files that are captured, at capture time. These drivers cannot be added manually later. XP mass storage drivers can be added only through the bundle creation process, which is specified in the parameters.ini file under the INI sections [xpMassStoragex86] and [xpMassStoragex64]. Whenever you want to add new XP mass storage drivers, you must repeat this process, recreate, and upload the MDT bundle.

Importing and managing drivers for Windows deployments

You manage drivers using the **Driver Library** dashboard. The Driver Library displays a list of available drivers based on compatible computer models. You can search for specific drivers, delete listed drivers, modify a driver's operating system and architecture compatibility, and import new drivers. Only PCI device drivers are supported.

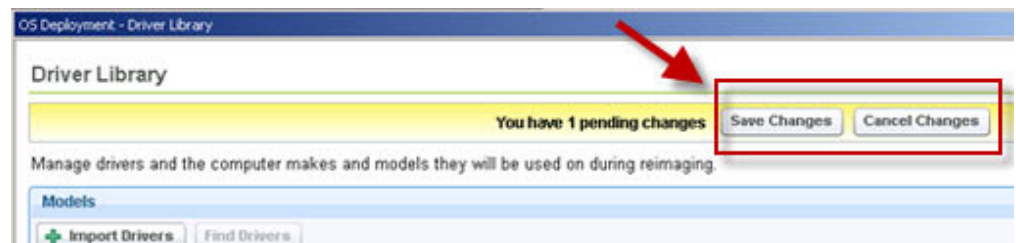
Drivers are used in the deployment process for inclusion in the Windows Preboot Environment, as well as being provided to Windows setup.

The Driver Library dashboard is divided into two sections, **Drivers**, which lists the available drivers, and the bottom section that displays details for the highlighted driver.

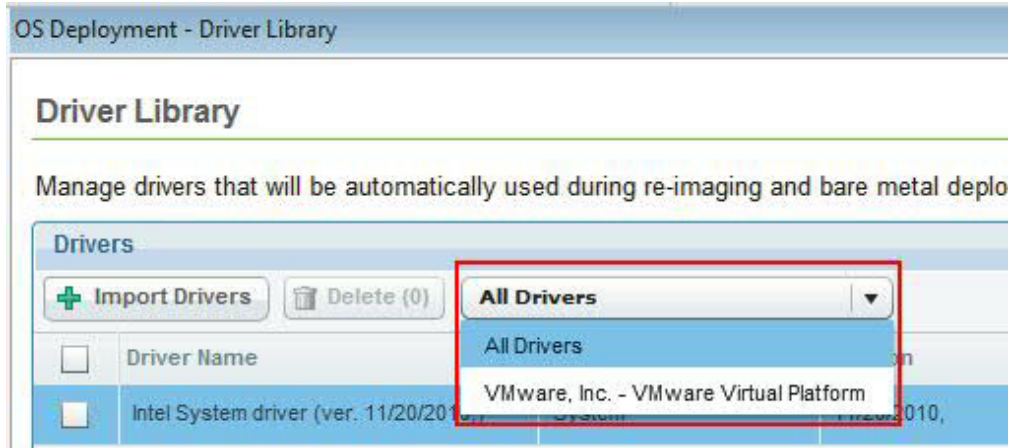


In the *Drivers* section, you can find or import drivers into your driver library. Drivers in your library are organized by driver name, class, and version.

If you modify the driver compatibility, operating system, or delete a driver, a Pending Changes message displays at the top of the Driver Library dashboard. You can commit or finalize these changes by clicking **Save Changes** or **Cancel Changes** and an automatic action is created to update any bare metal server with the change in the drivers.



At the top of the Drivers section, you can filter the hardware models that are found in the deployment to show only drivers compatible with that hardware model.

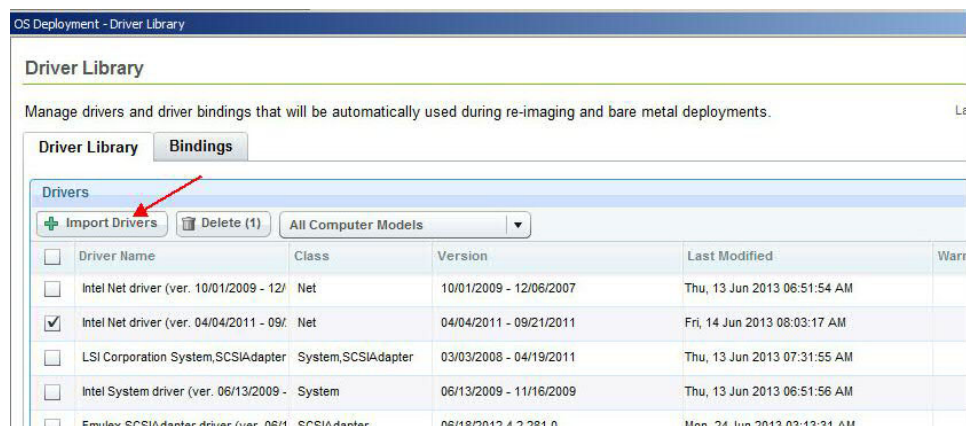


If the filter is empty, the analysis **Hardware Information** must be activated.

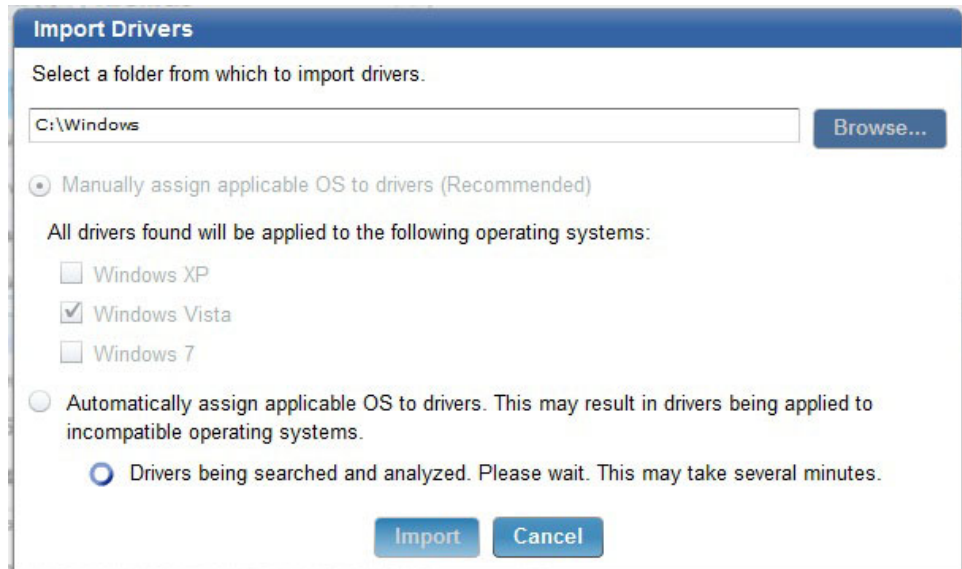
Importing drivers

To import drivers, perform the following steps:

1. Click **Import Drivers** in the Driver Library dashboard.



2. In the Import Drivers dialog, browse to select a folder from which to import drivers. When importing drivers, you can determine the operating system compatibility for the drivers in the specified folder either manually by specifying the compatible operating systems, or automatically by allowing the application to determine the compatible operating systems.



After you select the manual or automatic way to assign the drivers to the operating systems, click **Import** to search and analyze the drivers. The process can take several minutes or longer depending on the number of drivers. When the import process is complete, a status page is displayed with the driver import results.

Import Drivers Results

Driver upload process complete.

2 driver(s) successfully uploaded.

0 driver(s) skipped.

0 driver(s) with operating system applicability updated.

Successfully imported drivers:

C:\Drivers\win7\Acconwin\WLANINT\Win7\S32\Drivers\NETwNs32.INF
C:\Drivers\win7\Acconwin\WLANINT\Win7\S64\Drivers\NETwNs64.INF

Drivers Skipped:

Drivers with operating system applicability updated:

Note:

Import drivers with operating system compatibility manually specified. Due to the nature in which drivers are created, automatic determination can lead to drivers being listed as compatible for the wrong operating systems.

Import smaller folders of drivers all at the same time. This allows for easier assigning of manual OS compatibility as well as encourages the importing of only necessary drivers. Importing unnecessary drivers might lead to issues during the deployment process. The memory limit for importing drivers requires that the size of the folder to be imported does not exceed the available system memory.

Only PCI device drivers are supported.

After importing a driver, click the driver to see more detailed information about it. You can also change the operating system compatibility, even if the driver has been imported automatically.

When drivers are imported, an automatic action is created to update any bare metal server with the change in drivers.

The drivers are imported as soon as the following action, Update Driver Manifests on Bare Metal Servers, completes:

All Actions			
Time Issued	State	% Complete	Name
13/11/2012 17:03:06	Open	100,00% (2/2)	Update Driver Manifests on Bare Metal Servers

Note: Importing drivers from a share can take longer than importing them from a local folder.

Managing Windows driver bindings

In the **Bindings** tab of the **Driver Library** dashboard, you can view the device drivers that are used when the selected image is deployed on the selected computer model. This is useful to evaluate in advance which device drivers are missing and prevent image deployment failures.

From the menu, choose an image file to be deployed and a hardware model on which to deploy. Then, you automatically see the **Driver Bindings** table with a list of all the drivers that are associated to the specific devices.

You can perform the same operation to check the drivers for WinPE by selecting **WinPE** from the menu.

The screenshot shows the 'Driver Library' interface with the 'Bindings' tab selected. It includes a search bar, a table of driver bindings, and a '+ Add Manual Binding' button. The table lists device names, their hardware IDs, and the driver bound to them.

Device Name	Device	Driver Bound	
Intel Corporation 82371AB/EB/AM	8086.7111.15AD.1976	Intel hdc,System,USB driver (ver. 02/08/2010 - 11/20/2010)	
Intel Corporation 82545EM Gigab	8086.100F.15AD.0750	No applicable drivers found	
VMware VMXNET3 Ethernet Cor	15AD.07B0.15AD.07B0	Built-in	
VMware SVGA II Adapter	15AD.0405.15AD.0405	Built-in	
LSI Logic / Symbios Logic SAS1	1000.0054.15AD.1976	Built-in	
LSI Logic / Symbios Logic 53c10	1000.0030.15AD.1976	Built-in	

The possible values for the **Driver Bound** status are:

Built-in

Indicates that the support for the device is already included in the image by default.

A driver is listed

Indicates that this type of driver is used.

No applicable drivers found

Indicates that there is no driver available. In this case, ensure that you import the appropriate drivers for your device from the **Driver Library** tab.

The driver bindings displayed by the **Driver Bindings** table can be edited. You can set specific rules for a device by selecting one of the following options:

Auto Automatically selects the driver and is the default option.

Select Drivers

Allows you to select the appropriate drivers from the list.

Don't Use Drivers

Allows you not to associate any driver to the device.

The screenshot shows a dialog box titled "Editing device: Advanced Micro Devices [AMD] 79c970 [PCnet32 LANCE]". The main text says: "Select a rule for device ID 1022.2000.1022.2000 from the radio buttons below. You can hover your mouse over each radio button for more information." Below this are three radio buttons: "Auto", "Select Drivers" (which is selected), and "Don't Use Drivers". There is also a "Built-in" checkbox. Below the radio buttons is a table with two columns: "Drivers" and "Last Modified".

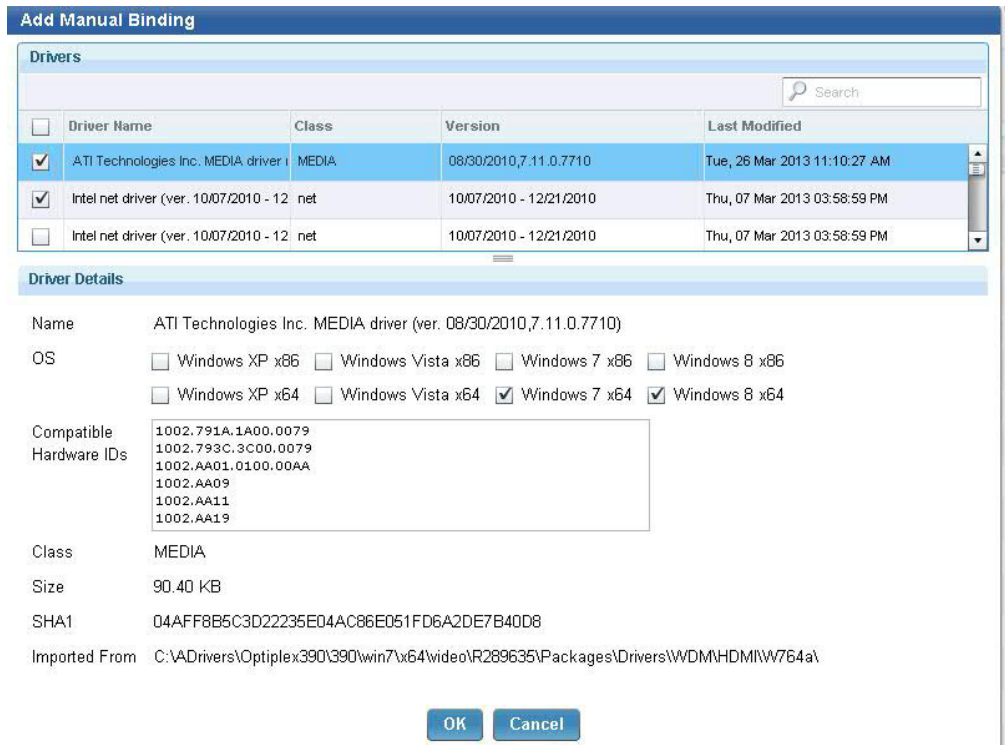
Drivers	Last Modified
VMware, Inc. Net driver (ver. 02/19/2010,)	Sun, 10 Mar 2013 12:49:34 PM

Below the table is a "Driver Details" section with the following fields:

- Name
- OS: Windows XP x86 Windows Vista x86 Windows 7 x86 Windows 8 x86
 Windows XP x64 Windows Vista x64 Windows 7 x64 Windows 8 x64
- Compatible Hardware IDs: [Empty text box]
- Class
- Size
- SHA1
- Imported From

At the bottom are "OK" and "Cancel" buttons.

Click **Add Manual Binding** to select additional drivers for those devices that do not provide a Device ID. The manually added device drivers are provided to the OS Installer when installing the operating system. This option has no effect on WinPE images.



Capturing Windows Images

When you capture an image, you are creating an image that can be customized and applied to other computers in your network.

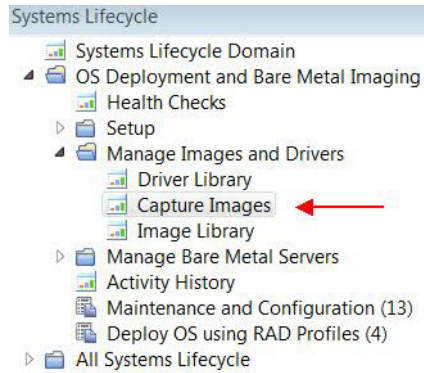
Capturing an image involves a set of tasks that result in the creation of a generic image that can be applied on any computer. The process of capturing an image can affect the product activation of the captured system. To avoid this problem, you must capture an image from a virtual machine with snapshot restoration capability.

During the capture phase, the machine you are capturing must be a member of a workgroup and cannot be in a domain, because the Sysprep tool runs only on machines in a workgroup.

The captured image is stored on a network share, ready to be uploaded to the server into the Image Library.

Because captured images are firmware independent, you can deploy (for re-imaging or Bare Metal), images that are captured from BIOS machines to UEFI machines and vice versa.

From the *Capture Image* wizard, you can specify SMB share information and choose capture options. Access the wizard from the *Manage Images and Drivers* node in the navigation tree.



The Capture wizard is organized into two sections:

- Specify SMB Share information
- Choose Capture Options

Capture Wizard Last Updated: 04/6/2014 06:24:45 PM

This dashboard is used to capture an image of a currently running computer.

1) Specify SMB Share Information

Image Destination Folder

Enable Remote Logging

Location For Logging

Specify Credentials

Prompt for credentials during capture

Specify Credentials

2) Choose Capture Options

Operating System and Architecture

OS to capture

Architecture

MDT Bundle

Miscellaneous Options

Multiple Partitions Capture all Partitions

Before Capturing Defragment Disk Check and Repair Disk Problems

Disable enhanced error detection

Image Capture Notes

Note:

If you are capturing an XP operating system, you must verify that you included the appropriate mass storage drivers during the MDT Bundle Creation process. These mass storage drivers must be compatible with the mass storage devices on the machines on which the captured WIM is deployed. Without correct mass

storage drivers, imaging tasks with this captured WIM are likely to fail, particularly during a PXE imaging task. See “Prepare and add XP mass storage drivers” on page 50.

After you capture an image of a Windows 2008 R2 or later with multiple disks, the reference machine reboots and the second disk goes offline. Bring the second disk online again to see the data on it.

Dedicated boot partitions (also known as System Reserved on BIOS machines and ESP on UEFI machines) are captured but are not restored on the deployed machine. These partitions are instead re-created on the deployed machine to allow any combination of firmware architectures between source and target machines (BIOS to BIOS, BIOS to UEFI, UEFI to BIOS, UEFI to UEFI).

If the image you are capturing has a recovery partition, as, for example, in the case of Windows 8 or Windows 8.1 UEFI machines, this partition is recognized and marked as such in the partition mappings menu for the re-image or bare metal deployments.

Capturing an image on a system with an encrypted disk is not supported. You must decrypt the disk prior to capturing.

Specify SMB Share Information

From this section of the Capture Image wizard, you can set image destination, enable remote logging, and specify the credentials to use to access the share location.

1) Specify SMB Share Information

Image Destination Folder

Enable Remote Logging

Location For Logging

Specify Credentials

Prompt for credentials during capture

Specify Credentials

The **Prompt for credentials during capture** option is selected by default, and causes a prompt, to be shown on the endpoint, requesting credentials. This occurs just before the .wim file is saved. You can also select the **Specify Credentials** option to identify the appropriate credentials required to access the Image Destination Folder and, if applicable, the Remote Logging location.

If you specify both **Image Destination Folder** and **Enable Remote Logging**, the credentials must be the same.

Note: If you are using Endpoint Manager version 9.0 platform and you select **Enable 9.0 Encryption**, the computers listed in the **Take Action** dialog are filtered by the V9.0 clients.

Choosing Capture Options

You can specify different options when you are capturing computer images

From this section of the Capture Images wizard, you can select an operating system and architecture for your capture, locate Windows PE drivers, defragment or check disks prior to capturing, and record specific capture notes.

2) Choose Capture Options

Operating System and Architecture

OS to capture **Windows 8.1** ▼

Architecture **x64** ▼

MDT Bundle **MDT_3304_WADK81 (3.3.04)** ▼

Miscellaneous Options

Multiple Partitions Capture all Partitions

Before Capturing Defragment Disk Check and Repair Disk Problems

Disable enhanced error detection

Image Capture Notes

Start by selecting the operating system and architecture of the computer you want to capture. For Windows XP you must also specify the service pack that you require.

Choose the MDT Bundle to be used during the capture process. MDT Bundles are filtered based on which bundles are compatible with the chosen operating system.

You can capture multiple partitions in a single .WIM file, to enable the support of multi-partition master images. An MDT Bundle 3.1 or later is required to capture multiple partitions.

In the **Miscellaneous Options** section, you can:

- Choose to capture multiple partitions by checking **Capture all Partitions**.
- Choose to defragment or check and repair disk problems before capturing by selecting the corresponding option.
- Choose to prevent modifications to the target boot sequence during the capture process by selecting **Disable enhanced error detection**. For more information about this option, see “Error detection” on page 75.
- Include capture notes in the available field.

After selecting all capture options, click **Capture Image**. In the Take Action dialog, target the computer to be captured. When the action is complete, the capture begins.

Note: This process can affect the product activation of the captured system, making it unable to reactivate. You must capture an image from a virtual machine with snapshot restoration capability.

Importing Windows and Linux images

The **Image Library** Dashboard allows you to manage images by importing, pre-caching, deleting, modifying the metadata of your existing images.

From the **Image Library**, you can upload images that have been previously captured with the Capture dashboard (.wim) for Windows deployments, or import images directly from installation media for both Windows and Linux deployments. You cannot import images from installation media (ISO) for Windows XP or Windows 2003 platforms.

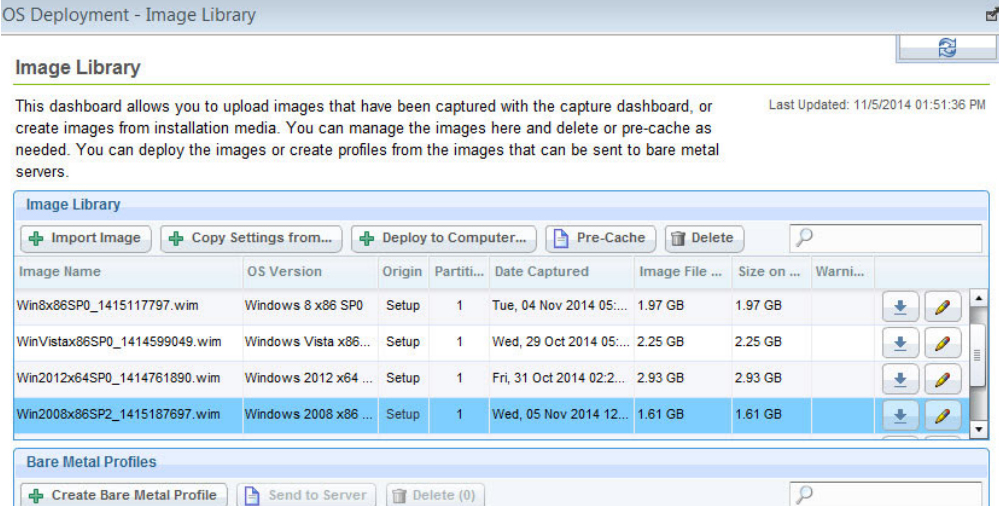
You can also import images in RAD format. Unlike Windows and Linux images, RAD images cannot be deployed to targets through the binding menu. You cannot create Bare Metal profiles based on RAD images from the Image Library dashboard. From these images you create RAD profiles for deployments using Server Automation plans. For more information, see Appendix B, “Bare Metal OS Provisioning using RAD Profiles,” on page 133.

For Windows images only, you can copy configuration settings from an existing image to a newly imported image, providing they are compatible. For example, if you have uploaded a new image for an Operating System update, you can associate to it any Bare Metal Profiles, driver bindings, and templates that were defined in an existing image of an earlier service pack of the same Operating System. See “Copying configuration settings from a Windows reference image” on page 62.

From the Image Library, you can then deploy these images to selected targets, or create profiles to be sent to Bare Metal OS Deployment Servers for deployments on Windows and Linux targets.

The Origin column displays whether the image was captured or imported from installation media (setup). Linux images are identified by the extension .l1m.

To import a new image, click **Import Image**. Use the icons on the right to either download or edit an existing image in the library.



OS Deployment - Image Library

Image Library

This dashboard allows you to upload images that have been captured with the capture dashboard, or create images from installation media. You can manage the images here and delete or pre-cache as needed. You can deploy the images or create profiles from the images that can be sent to bare metal servers. Last Updated: 11/5/2014 01:51:36 PM

Image Name	OS Version	Origin	Partiti...	Date Captured	Image File ...	Size on ...	Warni...
Win8x86SP0_1415117797.wim	Windows 8 x86 SP0	Setup	1	Tue, 04 Nov 2014 05:...	1.97 GB	1.97 GB	
WinVistax86SP0_1414599049.wim	Windows Vista x86...	Setup	1	Wed, 29 Oct 2014 05:...	2.25 GB	2.25 GB	
Win2012x64SP0_1414761890.wim	Windows 2012 x64 ...	Setup	1	Fri, 31 Oct 2014 02:2...	2.93 GB	2.93 GB	
Win2008x86SP2_1415187697.wim	Windows 2008 x86 ...	Setup	1	Wed, 05 Nov 2014 12:...	1.61 GB	1.61 GB	

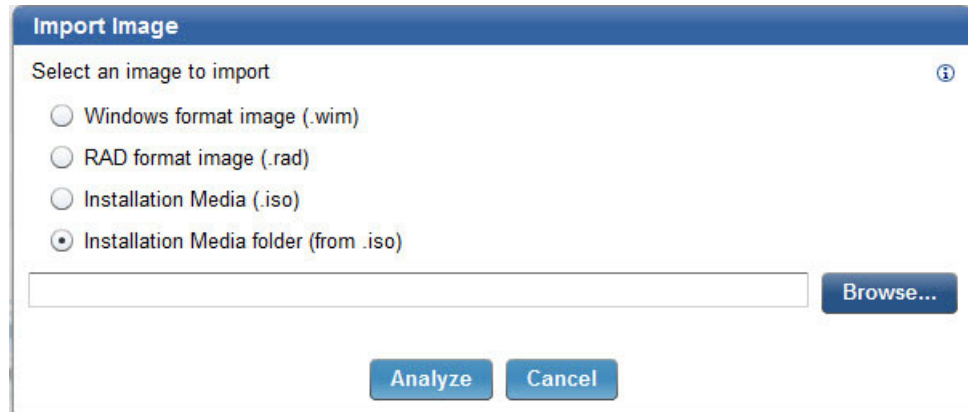
Bare Metal Profiles

Create Bare Metal Profile Send to Server Delete (0)

In the import image menu, select the type of image you want to import. You can import .wim images resulting from a capture of a Windows reference machine, a

RAD format image, or an ISO image. ISO images can be imported in archive format (.iso) or from a folder or drive which contains the uncompressed ISO image files.

If the image you are importing is provided in more than one installation media file, for example in SLES-DVD1.iso and SLES-DVD2.iso, you must uncompress the files into a single folder, and specify that folder in the Import image popup.



If you are importing Windows images in ISO archive format (.iso), you must have previously downloaded and installed the 7-zip compression/decompression tool on the system where the Console is installed.

Browse to locate the image file or folder on your computer and click **Analyze**.

Showing information for Image: Win2012R2x64SP0_1403536206

Check the information below and choose whether to continue or not.

OS	Windows 2012 R2
Service Pack	0
Architecture	x64
Size on Disk	3.67GB
Editions List	Windows Server 2012 R2 Standard Core Windows Server 2012 R2 Standard Windows Server 2012 R2 Datacenter Core Windows Server 2012 R2 Datacenter

OK **Cancel**

The analysis typically takes several minutes to complete. During this time, if you are importing an ISO image, the contents of the specified ISO file or folder are checked and the information retrieved from the image is displayed. In the Editions

List, you can view the editions you can deploy. Check the information and click **OK** to begin importing the image, or **Cancel** to quit.

When you import Windows images from ISO, you can choose to upload any available OS resources automatically during the image creation process, if these resources are not already available on the server. If you deselect **Upload OS resources**, you must upload the necessary OS resources by using the **Bundle and Media Manager** dashboard.

When the analysis completes, your newly imported image is displayed in the Image Library list.

During the import of a captured .wim image file, the corresponding driver descriptor file (.driverinfo) and image descriptor file (.imageinfo) that were created during the capture phase, must exist in the same path. If the driver descriptor file is missing, the import process automatically creates it. If the image descriptor file is missing, you are prompted to specify the required fields.

Note: If a captured .wim file does not contain an IBM Endpoint Manager client, one is installed during the re-image process.

Copying configuration settings from a Windows reference image

For Windows images, you can copy configuration settings such as Bare Metal Profiles, templates, and driver binding grids, from an existing image to another compatible image. The configuration settings are copied only if the following compatibility conditions are met:

- Both images must:
 - be of the same Operating System
 - have the same architecture (32-bit or 64-bit)
 - have the same origin (both must be either captured images or created from installation media).
- The image that inherits the settings must not already have configuration settings associated to it.

If one or more of the conditions above are not satisfied, an error message is issued.

From the **Image Library** dashboard, select the target image on which you want to copy the configuration settings and click **Copy Settings from...**

Choose the reference image from the list of compatible images. If the reference image has Bare Metal profiles associated to it, you can optionally specify a prefix or a suffix for the profile names to be used when they are copied on the target image. If the reference image has templates and driver bindings associated to it, these are also copied to the new image. You can change profile names in the new image.

A summary panel displays all objects that are copied. You can optionally select **Send All New Bare Metal Profiles to Server**, to send the copied profiles to the same Bare Metal Servers where the profiles of the reference image reside. Similarly, you can pre-cache the images on the server. Click **OK** to take action.

You can also send only one or some of the copied profiles to a Bare Metal Server of your choice.

Important: If there are rules associated to the Bare Metal Profiles in the reference image, these rules are copied to the new image but they are disabled, so as to avoid conflicts with the old profiles. To reactivate them in the copied Bare Metal profiles, use **Activate Rule**. After the copy has completed, the reference image and configurations are not erased.

Note: In some cases, you might receive an error message even if the target image does not have any previously defined settings. For more information, see “Copy image settings error on manual driver bindings” on page 126.

Chapter 5. Re-imaging

Re-imaging is the process of saving the user state on a computer, installing a new image on it, and then restoring the user state.

You can re-image Windows or Linux systems by choosing previously uploaded images from the **Image Library**.

The re-imaging process on Windows systems does not re-partition the disk on the target system. To re-image a computer successfully, ensure that on the target machine the available free disk space is at least equal to or greater than the **Size on disk** of the image you are deploying.

Re-imaging a Linux system means refreshing the Operating System on a computer with an active IBM Endpoint Manager Client. The machine identity is preserved during the migration.

On Linux systems, re-imaging involves the Linux Image provider component which you must install on those relays that manage the targets that you want to re-image. If the Linux targets are connected to a relay that is a Bare Metal Server, this component is not needed. To install and use this component, see “Managing the Linux Image provider” on page 20.

When you re-image a computer you can upgrade the operating system or install a later service pack, but you cannot downgrade architectures or operating systems (you cannot deploy a 64-bit image on a 32-bit target or re-image from Windows 7 to Windows XP). However, you can deploy a 32-bit image on a 64-bit target if the hardware supports it.

From the Image Library Dashboard, choose a source image and click **Deploy to Computer**.

In the dialog, you can customize a variety of settings and options and create deployment actions that re-image a computer with the specified settings. You can save the customized options as a template that you can use again in the future. The re-imaging process on a Endpoint Management client creates multiple actions to download and customize all files needed. When the download is complete, re-imaging begins. The status on the Endpoint Management Console is visible at the end of the re-image process, when the new operating system is successfully started.

Image Library

This dashboard allows you to upload images that have been captured with the capture dashboard, or create images from installation media. You can manage the images here and delete or pre-cache as needed. You can deploy the images or create profiles from the images that can be sent to bare metal servers. Last Updated: 07/7/2014 02:34:21 PM

Image Library

+ Import Image
+ Deploy to Computer...
Pre-Cache
Delete
🔍

Image Name	OS	S...	Arch...	Origin	Size on ...	P...	Date Captu...	Image Fi...	Impor...	Warnings	
WinVistax86SP0_1404314964.wim	Vista	0	x86	Setup	2.25 GB	1	Wed, 02 Jul 2...	2.25 GB			⬇️ ✎
Win2012x64SP0_1404137877.wim	Win2012	0	x64	Setup	2.93 GB	1	Mon, 30 Jun ...	2.93 GB			⬇️ ✎
WinVistax64SP2_1404478819.wim	Vista	2	x64	Setup	2.67 GB	1	Fri, 04 Jul 20...	2.67 GB			⬇️ ✎
RHEL6-5x64SP0_1403863846.lim	RHEL6.5	0	x64	Setup	0.00 GB	-	Fri, 27 Jun 20...	3.58 GB			✎

Depending on whether you are re-imaging Windows or Linux, the options you can customize are described in “Re-imaging Windows Systems” or in “Re-imaging Linux Systems” on page 81.

Re-imaging Windows Systems


You can specify different options which will affect the re-imaging process on the target.

To re-image a Windows system from the Image Library, you have these options:

- Edit an image that was previously imported .
- Deploy an image that you previously captured from a reference machine. In this case, if you have saved the user state on the captured system, you can restore it on the system you are re-imaging.
- Deploy an image that was created from installation media (ISO image).

You can use the *Search* box to search by a specific image name. Select an image by clicking the appropriate row in the table.

Editing an image

You can also edit an image by selecting it and clicking  . In the Edit Image window, you can change the image information.

Edit Image: Win8.1x86_WIN8132BIT_1386249071648.WIM

Fill out the required information below.

Required Fields

OS:

Service Pack:

Architecture:

Image Locale:

Image Keyboard Locale:

Size on Disk:

Date Captured:

Optional Fields

Product Key:

IEM Client Version:

Manufacturer:

Model:

Notes:

Partitions

Letter	Is Bootable?	Is System?	Info	Size on Disk
	yes	no		50.79 MB
C	no	yes		7.87 GB
E	no	no		99.48 MB

Note: Some fields cannot be modified if there are one or more bare metal profiles created from or associated to the image.

If you expand the **Partition Mappings** subsection, which is closed by default, the following information is displayed:

- The drive letter of the partition.
- If the partition is bootable.
- If the partition is a system partition.
- Additional information about the partition, for example if it is a recovery partition.
- The size of the partition.

In this subsection, you can edit partition mappings for the computers to which the selected WIM image is to be applied.

Note: Both disk and partition numbers are 0-indexed in this view.

Managing multiple partitions for captured images

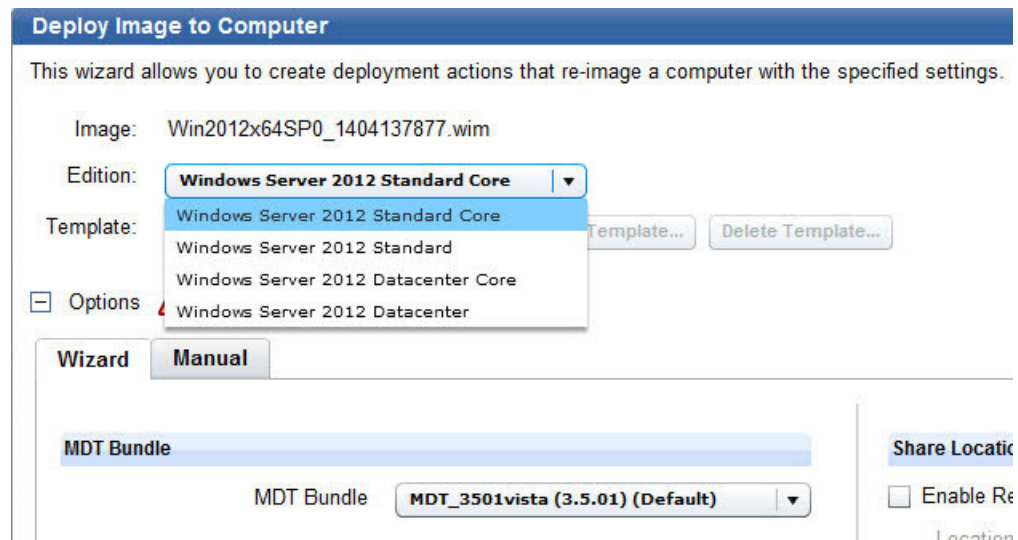
If your source image is multiple-partitioned, you can:

- Capture multiple partitions in a single .WIM file to enable the support of multi-partition master images.
- During a re-image, map the captured partitions into existing partitions and decide which target partitions to overwrite and which ones to keep.
- During a bare metal deployment, decide how many partitions to create and how to map them into partitions of the reference image.
- During a bare metal deployment, allow the administrator to decide if the disk must be cleaned and repartitioned or simply if some partitions must be reformatted, while others must be kept, (for example data partitions).

Choosing a source image

Select a Windows image from the Image Name list and click **Deploy to computer** to open the wizard.

If you choose an image that was created from installation media (ISO images), you can also select the operating system type that you want to deploy, if more than one is available in the image. Expand **Edition**, and make your selection.



In addition to the wizard, you can also use the **Manual** tab to edit the CustomSettings.ini file to be used for the re-imaging.

Deploy Image to Computer

To re-image your target computer, use this wizard to customize deployment parameters and user settings.

The **Deploy Image to Computer** wizard sets specific parameters, including migration settings, miscellaneous options, and credentials. You can deploy an image to a computer either using the wizard or manually.

To proceed manually, select the **Manual** tab to manually edit the customsettings.ini file that is generated from fields specified in the **Wizard** tab.

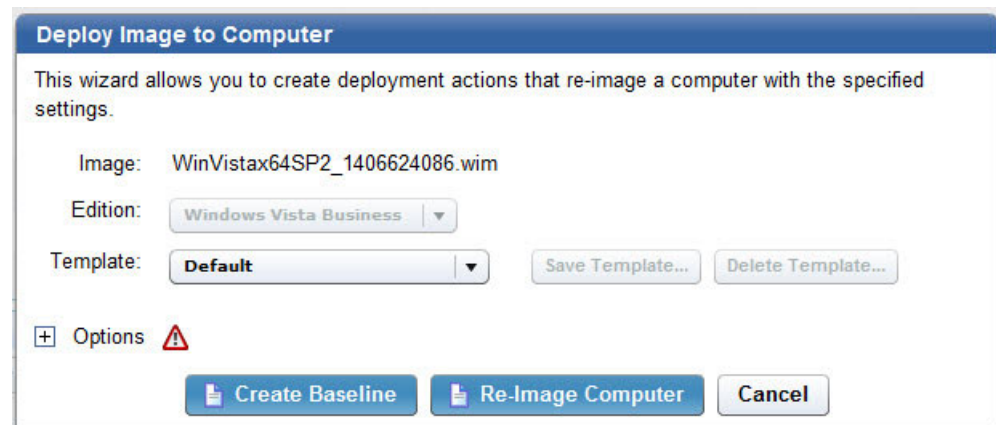
Changes made in the file make fields in the **Wizard** tab non-editable and manual changes must be undone to be able to make changes in the **Wizard** tab again.

Editing the customsettings.ini file incorrectly might cause failure during the imaging process. Some settings of this file are not present in this tab because they are handled separately by encryption. Specifically, these settings are:

- **DomainAdmin**
- **JoinDomain**
- **DomainAdminDomain**
- **DomainAdminPassword**
- **MachineObjectOU**

For these values, the settings in the **Wizard** tab take precedence over the settings found in the **Manual** tab.

From the wizard, you can optionally create a baseline that can be reused for subsequent re-image deployments:

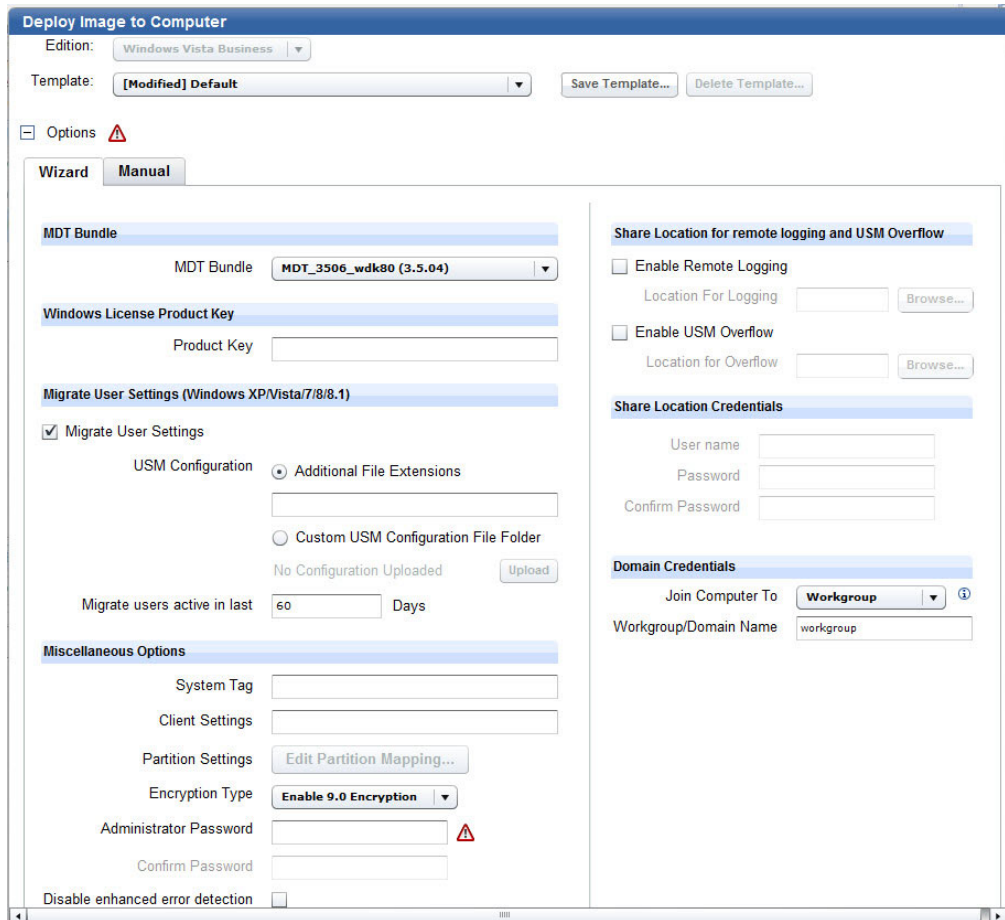


When you take action from the baseline, and provide the necessary credentials, multiple action groups are created and the activity dashboard is updated with new entries.

Expand **Options** to edit the settings for the re-image. When you have made the required changes, you can save the template, and either create a Re-image action by clicking **Re-image computer** or create a reusable baseline by clicking **Create Baseline**.

Important: You cannot re-image a system with an encrypted disk. You must decrypt the disk before deploying the image on the target system, or the re-imaging fails.

The following sections provide specific details about each component of the **Wizard** tab.



Windows License Product Key

Enter a valid Windows license product key in this field. To deploy multiple copies of Windows, you must have a volume key.

Note: If you fail to specify a correct product key, this might result in a failed re-image job and put the computer in an unrecoverable state.

Migrate User Settings

You can capture the user profiles and settings of a system before the re-imaging process begins.

The *Migrate User Settings* capability captures multiple user profile directories from a system about to be re-imaged. In most cases, the profile data stays on the migrated system. However, if the migration is from Windows XP to Windows XP and the system does not have sufficient disk space to duplicate the migrated profiles, the data might overflow to a "USM Overflow Location" (SMB) and be restored to the system after the image task is complete. To avoid filling up your available storage on the specified USM Overflow location, perform multiple migrations.

The users defined on the computer that you are re-imaging and that do not already exist in the image that you are deploying, are migrated and set to disabled on the re-imaged computer. You must enable them again by using the "Computer

Management” option of the Administrative tools. Alternatively, if you want the migrated users to be enabled during the deployment process, follow these steps:

1. In the Image Library, select the image you want to deploy and click **Deploy to Computer**
2. In the **Deploy Image to Computer** pane expand the Options section
3. Select the **Manual** tab and scroll to USM Settings
4. Modify the value of the **LoadStateArgs** parameter as follows:

LoadStateArgs=/lac /lae

The restored users will have an empty password which must be changed at first logon.

Note that by adding these values in the **LoadStateArgs** parameter, the restored users that were disabled in the source operating system (and that do not already exist in the image you are deploying) will be enabled in the final operating system. For more information about editing parameter values for capturing (**ScanStateArgs**) and restoring (**LoadStateArgs**) user settings in the **Manual** tab, see the documentation at the following links: <http://technet.microsoft.com/en-us/library/cc749015%28v=ws.10%29.aspx> (ScanState) and <http://technet.microsoft.com/en-us/library/cc766226%28v=ws.10%29.aspx> (LoadState).

Note:

You cannot migrate user settings for server class computers. When you re-image these computers, this option is disabled.

User State Migration behavior and capabilities might vary based on the original operating system, new operating system, or amount of storage space.

From / To	Windows XP	Windows Vista	Windows 7	Windows 8	Windows 8.1
Windows XP	Uses local storage space to copy profile Potential disk impact Use local relay for compressed storage if computer has insufficient space (at cost of network impact)	Uses “hard link” to migrate profile locally No disk or network impact	Uses “hard link” to migrate the profile locally No disk or network impact	Uses “hard link” to migrate the profile locally No disk or network impact	Not supported
Windows Vista	Not supported	Uses “hard link” to migrate profile locally No disk or network impact	Uses “hard link” to migrate the profile locally No disk or network impact	Uses “hard link” to migrate the profile locally No disk or network impact	Not supported

From / To	Windows XP	Windows Vista	Windows 7	Windows 8	Windows 8.1
Windows 7	Not Supported	Not Supported	Uses "hard link" to migrate the profile locally No disk or network impact	Uses "hard link" to migrate the profile locally No disk or network impact	Uses "hard link" to migrate the profile locally No disk or network impact
Windows 8	Not Supported	Not Supported	Not Supported	Uses "hard link" to migrate the profile locally No disk or network impact	Uses "hard link" to migrate the profile locally No disk or network impact
Windows 8.1	Not Supported	Not Supported	Not Supported	Not Supported	Uses "hard link" to migrate the profile locally No disk or network impact

Miscellaneous Options

In the Deploy Image to Computer dashboard, you can specify a set of options to customize the deployment for your specific environment.

Use the **Miscellaneous Options** section of the dashboard to specify environment-specific options to be used for the deployment.


Miscellaneous Options

System Tag

Client Settings

Partition Settings

Encryption Type

Administrator Password 

Confirm Password

Disable enhanced error detection

Use the **System Tag** field to set a string in the registry file to highlight something specific for that system to the IBM Endpoint Manager platform. For example, it could indicate that this system has been newly imaged. A registry entry with name SystemTag and the specified value is created under the key

HKEY_LOCAL_MACHINE\SOFTWARE\BigFix\EnterpriseClient\ImageInfo

or

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\BigFix\EnterpriseClient\ImageInfo

depending on the architecture of the machine. You can then create an action using the SystemTag registry key and its value as relevance to apply your action and reset that key as the first step of your action to prevent it from being run twice.

Note: This field is deprecated and is kept for backward compatibility only. If you want to identify computers or groups of computers in your network by assigning variables, use the **Client Settings** field.

Use the **Client Settings** field to list named variables that can be assigned to the deployed computer. This is a useful technique for organizing a network of computers, and can help to identify individual computers as well as groups. The values you assign can be used either as "labels" to identify computers with specific roles or as filters in the Fixlet actions and in the Fixlet relevance to exclude an action. After a deployment, you can display these values in the IBM Endpoint Manager console by selecting the specified computer, and clicking "Edit Computer Settings". The settings are listed under "Custom Settings."

For example:

If you specify depts:humanresources, an entry with name "depts" and the specified value (humanresources) is created in the registry file under the key: HKEY_LOCAL_MACHINE\SOFTWARE\BigFix\EnterpriseClient\Settings\Client or HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\BigFix\EnterpriseClient\Settings\Client, depending on the architecture of the machine.

You could then write an action against targets with this setting, as in the following example:

```
// "depts:humanresources"  
if {value of setting "depts" of client = "humanresources"}  
    .... action to perform ....  
endif
```

You can tag a system with role-specific baselines, for example, *Emeryville Office* or *Accounting Department*. You can install specific software applications relevant to those baselines, such as VPN for remote users or finance software for accounting personnel.

Note: During a system migration, preexisting client settings are restored in the new operating system. Using this feature, you can extend with new client settings.

OS Deployment supports role-specific baselines that allow administrators to target deployments based on user-defined tags. You can set a baseline to use these tags. For example, if the newly-imaged system is tagged with "Emeryville=1" and "Accounting=1", then the baseline to support the accounting group in the Emeryville office uses the following relevance:

```
value of setting "Location" of client = "Emeryville"  
AND  
value of setting "Group" of client = "Accounting"
```

When systems are migrated from one operating system to another, OS Deployment retains the client settings that were set in the previous operating system.

Select **Enable Administrator Account** to enable the Administrator account on the target system during the deployment process of captured images.

Miscellaneous Options

System Tag

Client Settings

Partition Settings [Edit Partition Mapping...](#)

Enable Administrator Account

Disable enhanced error detection

When you deploy images created from installation media (ISO), the Administrator user is always enabled and you must always supply the corresponding password. For further information about enabling users, see “Migrate User Settings” on page 70.

Setting Secure Password Transfer

If you are using Endpoint Manager version 9.0 or later on the server and clients, You can enable the encryption method by selecting **Enable 9.0 Encryption** in the Encryption type field. This selection requires no further actions, but the take action dialog will be filtered by the V9.0 clients, an SSL encryption which requires public and private keys to be generated, or no encryption of passwords.

If you choose to use SSL encryption and you have Endpoint Manager version 8.2, you must perform the following steps:

Select **Enable SSL Encryption**. If your Endpoint Manager server is at version 9.0 or later, this option does not apply.

Miscellaneous Options

System Tag

Client Settings

Partition Settings [Edit Partition Mapping...](#)

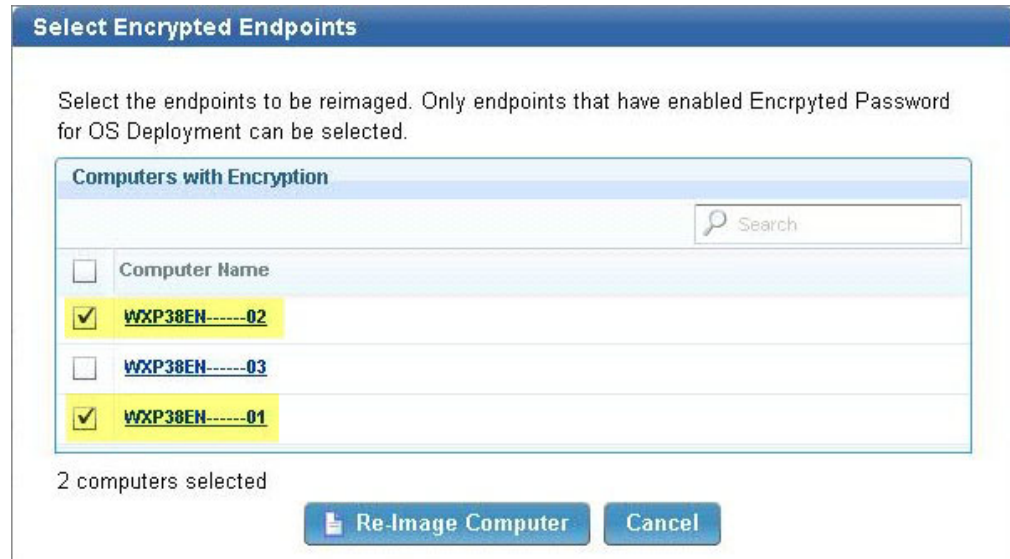
Encryption Type **Enable SSL Encryption** ▼ ⚠

Administrator Password ⚠

Confirm Password

Disable enhanced error detection

1. Activate the *SSL Encryption Analysis*, which is located in the Setup node in the navigation tree. The *SSL Encryption Analysis* is needed only for encrypting actions to Endpoint Manager clients version 8.2, not for version 9.0 clients. If all clients are at version 9.0 or later, this is not necessary.
2. Run the *Enable Encrypted Passwords* task on the machines that you want to re-image using a secure password. This Fixlet can be found in the Maintenance and Configuration node of the navigation tree.
3. After you enable SSL encryption and choose computers to re-image, the Select Encrypted Endpoints dialog displays. In the list check the computers that you want to securely re-image, and then click **Re-Image Computer**.



Error detection

OS Deployment modifies the boot sequence of target machines to monitor and track operations performed during capture, re-image, and bare metal deployments. This is done by hooking the master boot record (MBR) to detect and handle boot errors and other exceptions such as system crashes, startup failures, and infinite loops.

You can choose to prevent the modification of the boot sequence during these operations by checking **Disable enhanced error detection**.

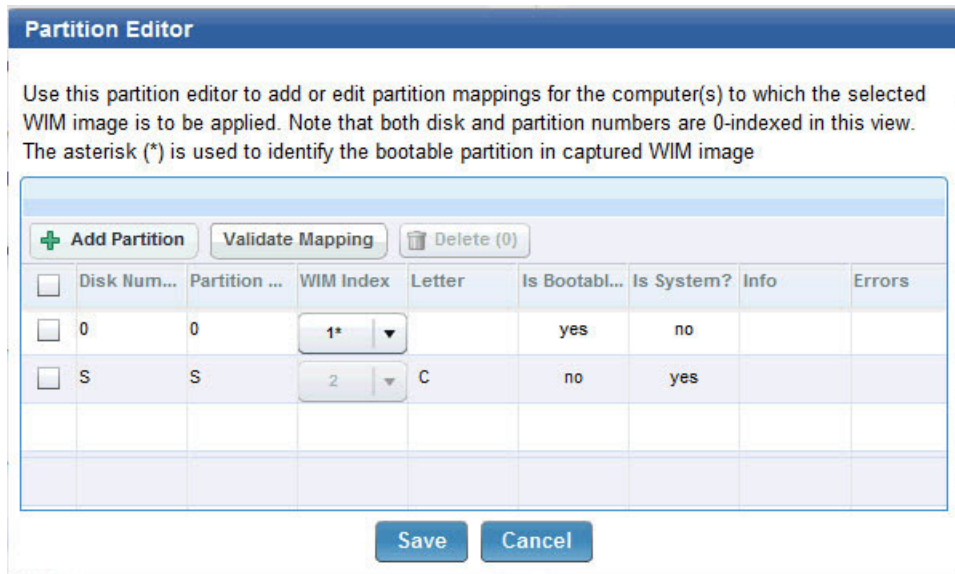
Disabling error detection inhibits changes to the boot sequence to avoid interference with specific target settings or company policies. Checking this option does not affect the deployment process flow and result.

Mapping partitions

Click **Edit Partition Mapping** to choose the partition layout for the deployment depending on your needs.

In the **Partition Editor**, the partitions contained in the WIM image are associated with the partitions that are present on the target computer. You map the captured partitions into existing partitions and decide which target partitions to overwrite and which ones to keep.

You can maintain partitions previously created on the physical disk. These are kept even after creating the new associations.

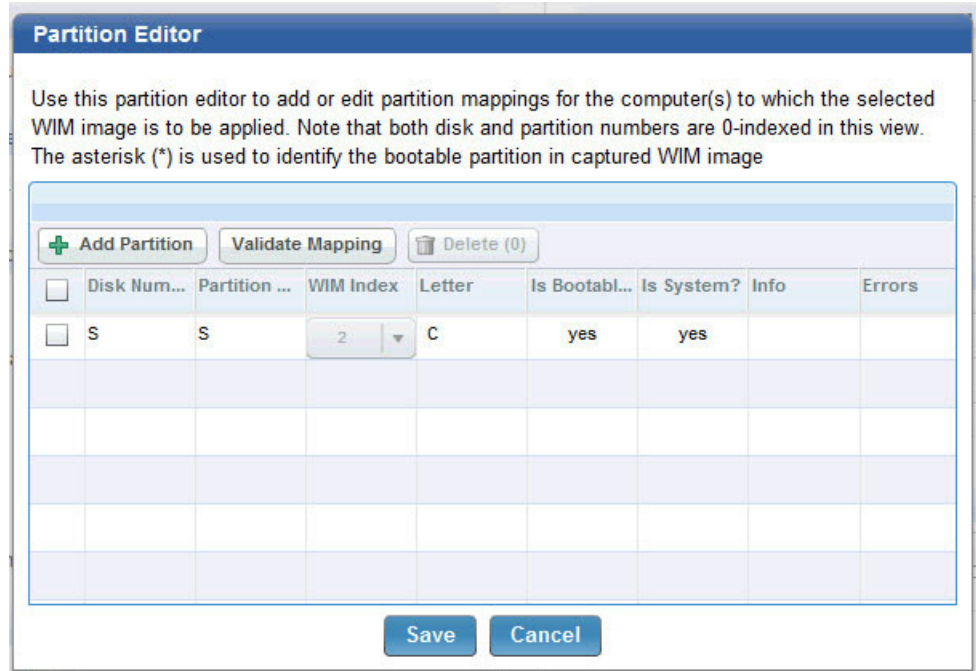


The **WIM Index** column identifies the partitions of the captured image, that you map to the partitions of the target machine, which are identified by **Disk number** and **Partition Number** in the corresponding columns.

The **Info** column displays additional information on the partition, for example, whether it is a recovery partition.

The asterisk (*) in the WIM index column indicates that this partition in the captured image was marked as bootable at capture time. If you delete this partition, the system partition is automatically set as bootable.

For example, when re-imaging a target from Windows XP (default installation with single-partition), to Windows 7 (which has separate boot and system partitions), you must delete the boot partition from your captured Windows 7 image. The system partition is then automatically marked as bootable.

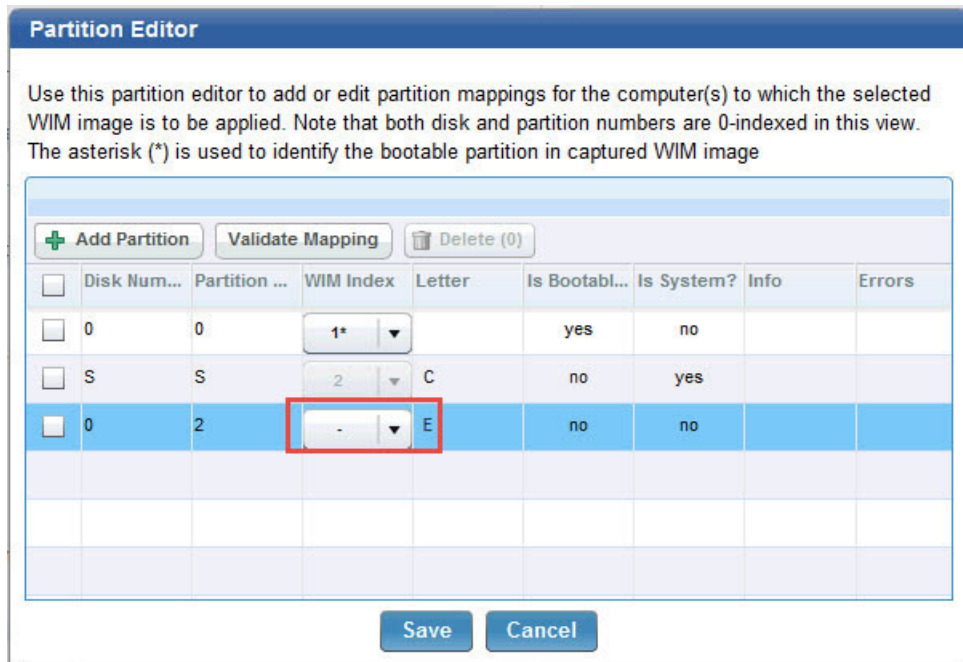


During the re-imaging process, regardless of how you map the system and boot partitions, if the number of partitions in the captured image is greater than the partitions present on the target machine, the validation fails. Because the re-image process does not re-partition the target machine, you must ensure that the number of mapped partitions is not greater than the partitions defined on the target, or both the validation step and the re-imaging process fail.

If the number of partitions you send to the target is less than the number of partitions present on the target, the results of the validation depend on how the partitions in the image are mapped to the target disk and partition.

It is strongly recommended to re-image ensuring that the number of partitions mapped from the captured image are equal to the number of actual partitions on the target.

You can also select the dash character (-) in the WIM Index column, to avoid overwriting the target partition with the specified partition of the WIM. For example, if on a Windows XP target machine you have a data partition that you want to prevent from being overwritten, you must modify the partition mapping by selecting the dash (-) character in the WIM Index column, so that on the corresponding target partition, no partition of the WIM image is transferred, as displayed in the following panel:



If the target of a re-image is a UEFI machine, a separate boot partition is always available at run time, regardless of how the bootable and system partitions are mapped in the WIM.

When you are done, click **Validate Mapping** to validate your associations.

Note: On BIOS machines only, a maximum of four partitions (primary) are supported on the same disk. Because images are firmware independent, you can define more than four partitions on the same disk but the deployment of such an image fails on BIOS machines. This limitation does not apply to UEFI machines.

Share Location

Remote Logging specifies a network location to which your log files are copied after capture or re-image. To use this feature, click the *Enable* box and browse to assign a logging location.

USM Overflow specifies a network location where user files are to be migrated if there is insufficient space on the endpoint. This occurs only during Windows XP to Windows XP migrations. To use this feature, click the *Enable* box and browse to assign an overflow location.

Share Location Credentials

Enter user name and password credentials for users to access the shared location. If using both Remote Logging and USM Overflow, the credentials must be the same.

Domain Credentials

After a deployment, a computer can be joined to a workgroup or to a new or existing domain.

Workgroup

To join a computer to a workgroup, specify the name of the workgroup.

Specify Domain

To join a computer to a domain, specify the name of the domain and credentials with domain-joining privileges. The domain name can contain all alphanumeric characters, but none of the following:

- backslash (\)
- slash mark (/)
- colon (:)
- asterisk (*)
- question mark (?)
- quotation mark (")
- less than sign (<)
- greater than sign (>)
- vertical bar (|)

Names can contain a period (.), but cannot start with a period. You should not use periods in Active Directory domains. If you are upgrading a domain whose NetBIOS name contains a period, change the name by migrating the domain to a new domain structure and do not use periods in the new domain names. You can also specify the DNS domain name, for example, MyDom or MyDom.MyCompany.com.

Existing Domain

To migrate domain settings from the previous operating system, enter the appropriate domain-joining credentials.

Specify OU

To join a computer to an active directory organizational unit, specify the full Active Directory path name of the OU to join. Specify the user credentials with domain-joining privileges.

For example:

```
OU=MyOu,DC=MyDom,DC=MyCompany,DC=com
```

All characters are allowed, including extended characters. As a best practice, use Organizational Unit (OU) names that describe the purpose of the OU and that are short enough to be easily managed.

Note: OU settings cannot be specified for a workgroup or domain name. Domain-joining credentials can be specified as a domain name or as a DNS domain name, as described previously. If the domain is not specified as part of the user name, the name of the domain to which you are joining is used. Formats such as Administrator@server1.mydept.us.myco.com are not allowed.

The values you specify in the wizard are stored in the CustomSettings.ini file and are mapped as follows:

Table 3. Domain Credentials value mapping in the CustomSettings.ini file

Field in the wizard	Corresponding property in CustomSettings.ini file
Workgroup/Domain Name	JoinDomain
Organizational Unit to join (OU)	MachineObjectOU
User name (Domain\user login name)	DomainAdminDomain and DomainAdmin
Password	DomainAdminPassword

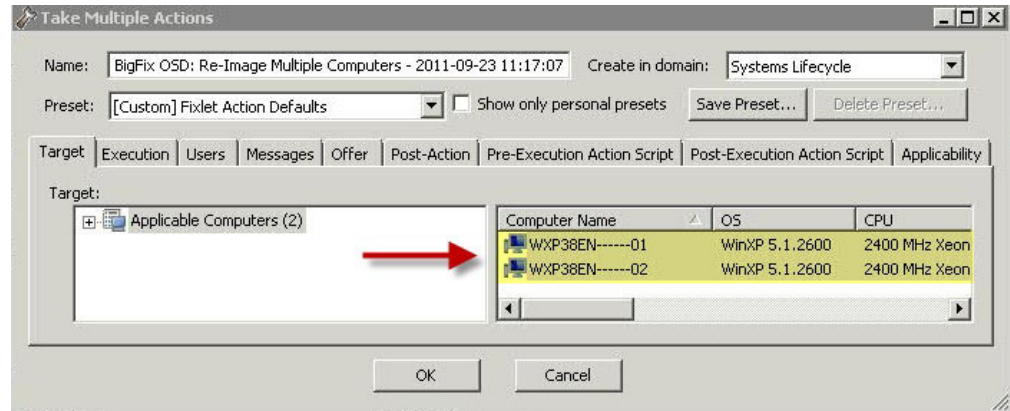
IBM Endpoint Manager performs the Join Domain using the Microsoft Deployment Toolkit (MDT). Lite Touch Installation (LTI) is used for deployments. LTI uses a common set of scripts and configuration files (CustomSettings.ini) to deploy the target computers. IBM Endpoint Manager automates the domain-join process by modifying the CustomSettings.ini file used for the MDT deployment process. The settings that you specify and that are stored in the file, are then parsed by the Windows Setup program, and the system attempts to join to the domain early in the deployment process.

You can modify the following properties in the CustomSettings.ini file by selecting the **Manual** tab.

Table 4. Join Domain Properties in the CustomSettings.ini file

Property in CustomSettings.ini file	Description
DomainAdmin	The user account credentials used to join the target computer to the domain specified in JoinDomain. Specify as domain\user_name or user_name@domain.com
DomainAdminDomain	The domain in which the user's credentials specified in DomainAdmin are defined.
DomainAdminPassword	The password of the domain Administrator account specified in the DomainAdmin property and used to join the computer to the domain
JoinDomain	The domain that the target computer joins after the operating system deployment is complete. This is the domain in which the computer account for the target computer is created. This field can contain alphanumeric characters, hyphens [-], and underscores [_]. Blanks or spaces are not allowed.
MachineObjectOU	The Organizational Unit (OU) in the target domain in which the account for the target computer is created.

To enable an SSL encryption of domain credentials, select **Enable SSL Encryption** and check computers in the dialog. The dialog is filtered by computers that have had encryption enabled on them with the **Enable Encryption for Clients** Fixlet in BES Support. Click *Re-Image*. The Take Action dialog is pre-populated with the computers that you selected on the previous dialog. You must run the action on all the selected computers.



Re-imaging Linux Systems

You can re-image Linux systems by deploying images previously created from deployment media.

When you re-image a Linux target system, you are installing an image file (.LIM) previously created from an ISO image and stored in the Image Library. Depending on the re-imaging mode you select (Upgrade or Install), you are required to specify parameters needed for the target deployment. The parameters you specify must be saved to a template before launching the re-image task. For more information, see “Managing templates” on page 86.

Note: HTTP Access is needed to the Image Provider component, which listens on port 8088. For more information, see “Ports used by the Bare Metal OS Deployment Server” on page 92.

You can re-image Linux systems in two different modes:

Upgrade

If you select this mode, the operating system RPM Package Manager files (.rpm) on the target are updated at the required level. Optionally, you can choose to upgrade the Endpoint Manager Client installed on the target.

Install

If you select this mode, the selected image is installed on the target system. The data on the current system is overwritten by the new installation. The disks on the target are re-partitioned by default. The following existing settings on the target are preserved and migrated to the re-imaged system:

- Machine identity (language, keyboard, timezone, network settings)
- Endpoint Manager client identity

Note: In some cases, the Endpoint Manager client identity is not preserved. For more information, see “Duplicate client computer entry in the Server database after a Linux re-image” on page 125

Important:

- Re-imaging to targets that are managed by a proxy server is not supported.
- If your server is IBM Endpoint Manager Version 8.2, you cannot re-image Linux targets from the dashboard. You must use the Linux re-image task. See “Using the Linux System Re-image task” on page 85.

From the Image Library Dashboard, select the Linux source image you want to deploy and click **Deploy to Computer**.

Linux configuration options

For the re-imaging process, a configuration file is used at deployment time for both re-imaging modes. The default configuration file is displayed in the corresponding field of the **Deploy Image to Computer** dialog. This file includes a base system configuration for the installation of the most common packages, and, for the install mode only, a standard partition layout.

The configuration file is updated on the target system during the re-imaging task to migrate the machine identity on the destination image. The language, keyboard, timezone, and network settings are added at run time for this purpose. To override this behavior, edit the configuration file by providing your values for these settings. The values you provide are used on the target instead of the default ones.

For more information about customizing the configuration files for the supported Linux operating systems, refer to the specific Linux vendor documentation. For example, you can view information about the RedHat Enterprise Linux Kickstart configuration file options for Version 6, at this link: https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/6/html/Installation_Guide/ch-kickstart2.html, and information about the SUSE Linux Enterprise Server Control file for Version 11 SP3, at this link: <http://doc.opensuse.org/projects/autoyast/index.html>.

Valid re-imaging combinations

The following table lists the valid re-imaging combinations for both modes:

Table 5. Linux re-imaging combinations

Re-image mode	Architecture (From/To)	Distribution	Final Release/SP level	OS Combinations (From/To)
Upgrade	<ul style="list-style-type: none"> 32 bit to 32 bit 64 bit to 64 bit 			<ul style="list-style-type: none"> RHEL 5.x to RHEL 5.x, 6.x, 7.0¹
Install	<ul style="list-style-type: none"> 32-bit to 32-bit 32-bit to 64-bit 64-bit to 64-bit 	<ul style="list-style-type: none"> RHEL to RHEL SLES to SLES 	equal or higher	<ul style="list-style-type: none"> RHEL 6.x to RHEL 6.x, 7.0¹ RHEL 7.0 to RHEL 7.0¹ SLES 10.x to SLES 11.x SLES 11.x to SLES 11.x

Note:

1. RedHat Enterprise Linux Version 7 (RHEL 7) is supported only in Install mode.

Important:

- SUSE Linux Enterprise Server (SLES) 10 is supported only as a source operating system. Re-imaging to SLES 10 is not supported.
- For 64-bit architectures, both BIOS and UEFI targets are supported.

Re-imaging in Upgrade mode

In the Deploy Image to Computer dialog, select **Upgrade**.

This wizard allows you to create deployment actions that re-image a computer with the specified settings.

Image: SLES11x64SP2_1405677967.lim

Mode: Upgrade Install

Template: **Default**

Options

Encryption Type: **Enable 9.0 Encryption**

Root Password:

Confirm Password:

Force upgrade:

Upgrade client:

Kernel parameters:

Configuration file:

```
<?xml version="1.0"?>
<!DOCTYPE profile>
<profile xmlns="http://www.suse.com/1.0/yast2ns"
xmlns:config="http://www.suse.com/1.0/configs" >
<general>
<signature-handling>
<accept_unsigned_file
config:type="boolean">true</accept_unsigned_file>
<accept_file_without_checksum
config:type="boolean">true</accept_file_without_checksum>
<accept_verification_failed
config:type="boolean">true</accept_verification_failed>
```

This mode is intended for upgrading to later service packs for the same major release. However, if you check **Force upgrade** the upgrade to a major release is forced, which could lead to an unsuccessful deployment.

There are no required parameters for the Upgrade mode. Optionally, you can select to upgrade the IBM Endpoint Manager client, by checking the corresponding option. You are then prompted to select the client package version. All selections you make must be saved to a template. You can save to the Default template, choose to save your selections to a new template, or populate the dialog with settings from a previously saved template. The default configuration parameters stored in the installer response file and used for the upgrade are displayed. You can modify these parameters to suit your re-imaging needs. Optionally, you can specify additional kernel parameters that the Linux installer uses during installation.

Re-imaging in Install mode

In the **Deploy Image to Computer** dialog, select **Install** .

Deploy Image to Computer

This wizard allows you to create deployment actions that re-image a computer with the specified settings.

Image: RHEL6-5x64SP0_1403863846.lim

Mode: Upgrade Install

Template: **RHEL_Install_Tpmfosd10** | Save Template... | Delete Template...

Options

Encryption Type: **Enable 9.0 Encryption**

Root Password: [masked]

Confirm Password: [masked]

Client version: **9.1.1082.0**

Kernel parameters: [empty]

Allow client traffic:

Configuration file

```
install
# System keyboard
# keyboard us
# System language
# lang en_US.UTF-8
# Network information
# network --bootproto=dhcp --device=eth0
# Use graphical install
graphical
# System timezone
# timezone Europe/London
# Firewall configuration
```

Undo Changes

Re-Image Computer | Cancel

Select a previously saved template, create a new template to save the current settings, or save your selections to the Default template. When you re-image in Install mode, the IBM Endpoint Manager client is installed. The default version is the same version as the IBM Endpoint Manager server. You can select a different version by expanding **Client Version**. You must specify the root password of the target, or select a previously saved template that contains the correct root password.

The **Allow client traffic** option is selected by default. If your targets have the operating system firewall enabled, this option allows inbound udp traffic from the server to be correctly received. If you clear this option, you must allow inbound traffic by using Fixlets 678 or 682, depending on the type of operating system, as detailed in “Firewall considerations” on page 86

The default deployment configuration parameters stored in the installer response file and used for the installation are displayed. You can modify these parameters to

suit your re-imaging needs. Optionally, you can specify additional kernel parameters that the Linux installer uses during installation.

Using the Linux System Re-image task

You can re-image Linux targets using the Linux System Re-image task. Select the image and the associated configuration template containing the settings to be used for the re-imaging process that you have previously created and saved in the Image Library. Specify the root password for the target system if you are re-imaging in Install mode. The password you specify can be either in clear text or encrypted. If your server is at IBM Endpoint Manager Version 8.2 level, the password you specify must be encrypted. In either case, the password is always encrypted during the deployment process.

The re-image task does not install the Endpoint Manager client. For re-imaging to run successfully on the selected targets, the Image Provider component must be running on the relays to which these targets are connected.

Complete the following form and click Take Action:

Parameter name	Parameter value
*Name of the image:	RHEL6-1x86SP0_1404198971.lim ▼
*Select the configuration template:	(Default) RHEL_Install ▼
*Root password (Install only):	<input type="text"/>
Kernel boot-time hardware parameters for the installer:	<input type="text"/>

Activate

During task execution, the Linux installer boot files are saved in `/boot/OSD_XX` (if the target is BIOS) or `/boot/efi/OSD_XX` (if the target is UEFI), where `XX` is a randomly generated number.

During the final steps of the task, the original boot loader sequence is modified to start the Linux installer after the target reboots. The original boot loader configuration file is saved in `/tmp/BOOTLOADER.rbobkp`, where `BOOTLOADER` is either `grub.conf` or `elilo.conf`, depending on the boot loader on the target.

Password encryption

The root password you supply for re-imaging can be either in clear text or encrypted using any of the encryption methods supported by the corresponding Linux installers.

You can generate encrypted passwords using a "salt" string value, with a format: `idmysalt$mypassword`

where `mysalt` is a character string preceded by the characters `"id"` where the value in `id` identifies the encryption method used, ending with `"$"` and followed by the actual password string. The salt string can be up to 16 characters.

The following methods (allowed values for `id`) are generally supported:

Table 6. Generally supported encryption methods and corresponding IDs

ID	Method
1	MD5
2a	Blowfish algorithm
5	SHA-256
6	SHA-512

Example 1:

Encryption using MD5:

```
# openssl passwd -1 -salt my_key
Password: mypassword

$1$my_key$jVY4Txf5wMoEsJX3ieQaR0
```

Example 2:

Encryption using SHA-512:

```
# python -c 'import crypt; print crypt.crypt("mypassword", "$6$my_key")'

$6$my_key$2Wz7.0skHT/FQI3yy9TbjPtLjjRq9cmU.TjnPGHWu4WUjemTR/.TdaK68y2E63cxdxVaD58i64dyQIpnabUjz/
```

Firewall considerations

When a re-image action is run from the IBM Endpoint Manager server, to a target with a firewall enabled on the operating system, the target does not receive the action immediately because inbound udp traffic is blocked. Targets do not receive notification packets until they gather the new actionsite, which typically occurs once a day. To ensure that the action is received on the target in a timely manner, you can change the firewall settings to allow inbound udp traffic from the server by using the following Fixlets in the BES Support site:

- RedHat Firewall is Blocking BES Traffic - BES Client (678)
- SuSE Firewall is Blocking BES Traffic - BES Client (682)

Running Fixlets 678 or 682 has the same effect as the **Allow Client Traffic** checkbox in the wizard, and they can also be included in a Server Automation plan.

Managing templates

When you save a template, all input fields and options selected are stored for future use.

You can manage templates by selecting an image in the Image Library and clicking **Deploy to Computer**. When you have specified all required parameters you save the template by specifying a name or by updating the Default template.

Save Template As...

Saving a template will store all inputted fields and options selected for future use. Any passwords saved in this way will be obfuscated, and then saved in the database. If no password is specified, the user will be prompted to provide a password when a template is deployed.

Name

Privacy Shared Private

Save

Cancel

Templates that are saved with **Shared** privacy are visible and usable by all IBM Endpoint Manager console operators. Templates that are saved with **Private** privacy are only visible to the operator that created them. If you save a template and you use the default template name, the default template is overwritten. Deleting this template restores the original default template.

Chapter 6. Bare Metal deployments

You can manage Tivoli Provisioning Manager for OS Deployment PXE servers and bare metal profiles that exist on those servers.

Bare Metal deployments are installations of operating systems to targets that either have no operating system installed, or must be re-installed without preserving any existing data or settings.

A Bare Metal deployment normally requires the use of a PXE server. The targets that PXE boot to these servers see a menu with profiles available for deployment. For this purpose, Tivoli Provisioning Manager for OS Deployment must be installed on relays in your Endpoint Management environment. The installers can be uploaded to the **Bare Metal Server Management** dashboard. You must install the latest version available. After the install process completes, you are ready to create the profiles used for bare metal deployments.

You can create bare metal profiles from the Image Library dashboard. These profiles are then sent and stored on the OS Deployment PXE server. After you upload the profiles, they are ready to be deployed to targets. Any computer that PXE boots and connects to a managed OS Deployment PXE server can select the profile from the binding menu. That profile is deployed, downloading necessary files through the IBM Endpoint Manager infrastructure.

You can also deploy bare metal profiles to Windows targets that do not have a connection to a PXE Server by creating a network boot CD, DVD, or USB drive. These targets can boot and connect to the server directly through the boot media. For more information, see “Creating Windows Deployment Media” on page 32.

Managing Bare Metal OS Deployment Servers

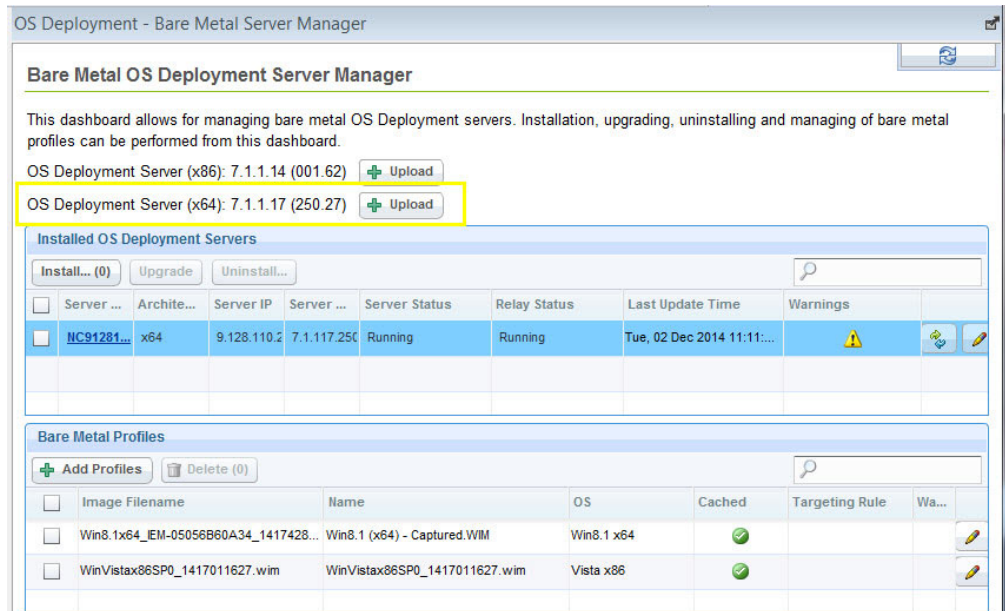
The **Bare Metal Server Manager** dashboard manages the installation, upgrade, and uninstallation of Tivoli Provisioning Manager for OS Deployment servers.

For more information about Tivoli Provisioning Manager for OS Deployment product, see the documentation at the following url:<http://www-01.ibm.com/support/knowledgecenter/SS3HLM/welcome>.

In the dashboard, a list of all Tivoli Provisioning Manager for OS Deployment servers that are subscribed to the site is displayed. To install the bare metal servers, you must upload the bare metal installer of the OS Deployment Server for each architecture.

Upload the latest release of the server installer available from Fix Central at this url: <http://www-933.ibm.com/support/fixcentral/> or from the Tivoli Provisioning Manager for OS Deployment portal.

After you upload the installer, you can run the installation on one or more of the available relays by clicking **Install**. Ensure that these relays are subscribed to the OS Deployment and Bare Metal Imaging site.



Note: If the relays you select already have the Image Provider component installed, you must remove it by using the "Uninstall Linux Image Provider Task" before you install the Bare Metal Server.


If you are using Endpoint Manager version 9.0 or later, the available computers do not require SSL Encryption.

If you are using the Endpoint Manager version 8.2 platform, the available computers to install on are those relays that have **SSL Encryption** enabled.

Accept the license and specify where to install the OS Deployment Server. Before you install, you must enter the user name and password for the login on the OS Deployment Server.

Note: Some functions of the dashboard are limited if the Bare Metal servers are not at a minimum required version. When you change a resource on a Bare Metal server, such as importing a new MDT Bundle, importing or modifying drivers, an action is automatically generated to update the servers.



If any of the resources are out of date, a warning is displayed. Click  to synchronize the server resources.

Important: After you install Tivoli Provisioning Manager for OS Deployment servers from the Bare Metal Server manager dashboard, you can choose to create and manage profiles and bare metal deployments from the IBM Endpoint Manager Console, using the IBM Endpoint Manager infrastructure. Alternatively, you can use the Tivoli Provisioning Manager for OS Deployment stand-alone product, but you cannot use both to manage the same deployment objects.

The **Bare Metal Profiles** section of the dashboard lists the available profiles on the Bare Metal Server. The **cached** column displays whether the image associated to the selected profile is cached on the relay. A green check mark indicates that the corresponding image is currently cached at the relay. A yellow warning icon

indicates that the corresponding image is not cached at the relay and will be copied when the profile is deployed for the first time. A red border triangle indicates that the caching status of the image cannot be determined.

To view the status of the services on an installed OS Deployment Server, select the



server from the list and click to view or modify the current settings:

Manage bare metal server NC9128110229

Settings
Relay Downloader Timeout (min)
Sync

Status
Latest heart-beat from Bare Metal Server (local time): Invalid Date
Check the status of the services before initiating any actions

Bare Metal Server services		Errors in server logs	
Service name	Service status	Server thread	Errors
OS deployment service	Running	Virtual machine	0
ODBC service	Running	Database connection	0
		File server	0
		Boot server	0
		HTTP server	0
		Network boot protocol	0

Start **Stop** **Restart**

You can start, stop or restart the Bare Metal Server, and view if any errors were logged.

When you deploy a Bare Metal Profile for the first time, the images linked to the profile are cached (copied) on the relay. If network traffic is slow, the caching might take a long time and cause the deployment of the Bare Metal Profile to fail. The default timeout value is written in the bom.trcfile. You can change this value in the **Relay Downloader Timeout** field. Specify the maximum time (in seconds) allowed to download an image from the Endpoint Management server to the relay if the image is not cached. Click **Sync** to update this value on the Bare Metal Server.

Cleaning up after a failed installation or uninstallation

If the installation or uninstallation of the OS Deployment Server on your relay fails, you can run the Bare Metal Server Clean Up Post-Uninstall or Install failure task (ID 134) from the Systems Lifecycle domain. Use this task only when you want to avoid system inconsistencies that might occur after a failure or when the installation or uninstallation task processing is incomplete.

Note:

This task removes SQL Express database from the target system. Do not run this task if there are other applications using this database. Do not run this task on OS Deployment Servers that are listed as installed in the Bare Metal OS Deployment Server Manager dashboard. On these servers, you must first run an uninstall action.

Ports used by the Bare Metal OS Deployment Server

To ensure correct communication, check the ports used for bare metal deployments

Listening ports used during client network boot (PXE/TFTP protocols):

By default, Bare Metal OS Deployment Servers and targets use the following ports for communication:

Bare Metal Server:

- *DHCP* : port 67 *UDP*
- *PXE BINL* : port 4011 *UDP*
- *TFTP* : port 69 *UDP*

Bare Metal Target:

- *DHCP* : port 68 *UDP*
- *PXE BINL* : port 4011 *UDP*

Note: PXE and TFTP ports are not needed when using network boot media.

Listening ports used during OS Deployment tasks and deployment media creation

Bare Metal Server:

- *NBP* : port 4012 *UDP*
- *FILE* : port 4013 *UDP & TCP*
- *HTTP*: port 8080 *TCP*
- *HTTP*: port 8088 *TCP* - Image Provider component used during Linux deployments
- *Database gateway* : port 2020 *TCP*

Bare Metal Target:

- *NBP* : port 4014 *UDP*

Ports for direct Web UI access (optional)

Bare Metal Server:

- *HTTP*: port 8080 *TCP*
- *HTTPS* : port 443 *TCP*

Configuring the DHCP server

To connect targets to the OS Deployment server, you might need to configure the DHCP server based on your network.

The DHCP server is used by the PXE bootrom to get its IP address and other basic networking information (including subnet mask, and default gateway). Using Endpoint Manager for OS Deployment can require changes to your DHCP configuration. These changes can typically be performed automatically by the Tivoli Provisioning Manager for OS Deployment installer. However, in some cases, you might want to perform the changes manually, or to verify them.

You can configure your DHCP server for one of the three following situations:

- The DHCP server and the OS deployment server *are not* running on the same host
- The DHCP server and the OS deployment server *are* running on the same host
- You already have a PXE 2.0 infrastructure with PXE Boot Server discovery installed and you want to add Endpoint Manager for OS Deployment to the list of servers to discover

Note: If you have previously configured your DHCP server for another PXE bootstrap, do not reuse your existing DHCP configuration. Remove DHCP options 43 & 60 for the hosts on which you want to run Endpoint Manager for OS Deployment and follow the instructions given in this section (if you are running Endpoint Manager for OS Deployment on the same host as the DHCP server, you need to set option 60 again).

Note: There are also cases where you must set both DHCP options 43 & 60, including when you have two different OS deployment servers.

DHCP server and OS deployment server on different targets, without information on PXE server location

Actions to perform:

- If DHCP options 43 and 60 are set, remove them.
- If the DHCP server *is not* running on the same computer as the OS deployment server, the DHCP configuration does not change. The OS deployment server detects DHCP packets sent over the network by PXE bootroms and offers PXE parameters without disturbing standard DHCP negotiation process. This behavior is called DHCPProxy.

Note: This configuration is not allowed if more than one OS deployment server is defined in the same environment. In the OS deployment server WebUI ensure that the DHCP proxy functionality is disabled: **Server parameters > Server configuration > Disable the DHCP proxy functionality = NO** (default value).

DHCP server and OS deployment server on different targets, with information on PXE server location

Actions to perform:

- Set option 60 (Class identifier) to "PXEClient" to inform the target that the location of the PXE server is known.
- Set option 43 to indicate that the PXE server does not reside on the same computer as the DHCP server and to precise the location of the PXE server.

Note: This configuration is mandatory if more than one OS deployment server is defined in the same environment.

Note: Some UEFI targets are not able to correctly process option 43. For those targets it is necessary to set option 66 and 67.

For detailed information about setting options, 43, 60, 66 and 67, see Tivoli Provisioning Manager for OS Deployment Installation Guide, Chapter 4: *DHCP server configuration*.

DHCP server and OS deployment server on the same target

Set your DHCP server to send DHCP option 60 (Class identifier) to the target. When option 60 is set to PXEClient the DHCP server knows where the PXE server is. If option 43 is not set, the PXE server has the same IP address as the DHCP server.

For detailed information about setting option 60, see Tivoli Provisioning Manager for OS Deployment Installation Guide, Chapter 4: *DHCP server configuration*.

Creating bare metal profiles

Create Bare Metal profiles from the Image Library dashboard, which you can then upload to the server.

To deploy images to Windows or Linux Bare Metal targets, you create bare metal profiles from the Image Library. You then upload the profiles to the Server so that it can be deployed on the selected targets.

Select an image for which to create a bare metal profile and click **Create Bare Metal Profile**.

The screenshot shows the 'Image Library' dashboard. At the top, there is a header 'Image Library' and a sub-header 'Bare Metal Profiles'. The 'Image Library' section contains a table with columns: Image Name, OS, S., Ar..., Origin, Size, P., Date C..., Imag..., Im..., and Wa... Two images are listed: 'Win2012x64SP0_140413787...' and 'RHEL6-5x64SP0_140386384...'. The 'Bare Metal Profiles' section contains a table with columns: Name, OS, Servers With Profile, Servers Out of Sync, and Warnin... One profile is listed: 'Win2012...' with OS 'Win2012 x64', 1 server with profile, and 0 servers out of sync. The 'Create Bare Metal Profile' button is highlighted in yellow.

Image Name	OS	S.	Ar...	Origin	Size	P.	Date C...	Imag...	Im...	Wa...
Win2012x64SP0_140413787...	Win2012	0	x64	Setup	2.93 GB	1	Mon, 30 ...	2.93 GB		
RHEL6-5x64SP0_140386384...	RHEL6.5	0	x64	Setup	0.00 GB	-	Fri, 27 Ju...	3.58 GB		

Name	OS	Servers With Profile	Servers Out of Sync	Warnin...
Win2012...	Win2012 x64	1	0	

A wizard with the information retrieved from the image is displayed. Depending on whether the type of image you select is a Linux image (.LIM), or a Windows image (.WIM), the fields you are required to specify differ.

Creating Bare Metal Profiles for Windows Images

Create Bare Metal profiles from the Image Library dashboard, to perform bare metal deployments on Windows targets.

Select a Windows image and click **Create Bare Metal Profile**.

A wizard with the information retrieved from the image is displayed. Depending on whether the type of WIM image you select is captured or created from installation media (ISO), some of the required and optional fields are different. Values for some of these fields are already set but you can change them as appropriate.

Common bare metal profile fields (both ISO and captured images)

Required fields:

Display Name

The name of the bare metal profile created from the image that you selected. By default, the name is the same as the image name.

Registered Owner

Specify the name of the person registered to use the operating system

Registered Organization

Specify the full name of the organization to which the registered owner belongs.

Image Locale

Choose the image locale for the operating system if different from the preset one.

Image Keyboard Locale

The keyboard locale is automatically set to match the image locale.

Time Zone

Select the time zone of the target operating system

New Computer Prefix

Specify the string that will be used to build the hostname, computer name, and full computer name of the target. You can specify a maximum of 8 characters for this field.

Note: The value specified for this field is ignored if "Prompt end user for hostname" is selected, and a hostname is specified at the target, when prompted.

MDT Bundle

Select the MDT Bundle to be used for the deployment of the bare metal profile. The MDT Bundle is preset based on the operating system that you want to deploy.

Administrator Password

Specify the password of the Administrator account on the target system. You are asked to enter the password twice for confirmation. This field is mandatory only for images created from installation media (ISO). It is optional for captured images.

Required Domain Credentials

Specify the required Domain Credentials. For a description of the field values, see "Domain Credentials" on page 78.

Optional fields:

Product Key

Specify a valid Windows Product Key.

Client Settings

Use this field to set named variables that can be assigned to the deployed computer. This is a useful technique for organizing a network of computers and helps to identify single computers as well as groups. The values you assign can be used either as labels to identify computers with specific roles or as filters in Fixlet actions and in Fixlet relevance to exclude an action on a target. After a deployment, you can display these values in the IBM Endpoint Manager console by selecting the specified computer, and clicking "Edit Computer Settings". The settings are listed under "Custom Settings."

When you specify client settings during a bare metal deployment, you can then complete further actions on the bare metal targets using other IBM Endpoint Manager applications. For example, you can trigger a software distribution task to automatically install the "7-zip" application on those targets with a client setting of :

```
7zip=Install
```

For more examples, see the Client Settings field description in "Miscellaneous Options" on page 72. For a sample Software distribution task using this field, see the wiki page at this link <https://www.ibm.com/developerworks/community/wikis/home?lang=en#!/wiki/Tivoli%20Endpoint%20Manager/page/How%20to%20trigger%20an%20application%20distribution%20after%20a%20Bare%20Metal%20deployment>.

Prompt end user for hostname

You can optionally select to assign a host name of your choice to the target of the bare metal profile deployment. The host name you specify can have a maximum of 15 alphanumeric characters. When the Windows Preinstallation Environment starts on the target, the user is prompted to enter a host name. If the user leaves this field blank when prompted, the value specified in "New Computer prefix" during the profile creation is used. If neither prefix nor hostname values are found, a default value is assigned to the hostname.

Deployment Password

Providing a deployment password protects the profile during deployment. Protected profiles are installed only after you provide the correct password at the target when prompted

Auto Deploy Timeout

If you specify a value in seconds, a counter is started during the PXE boot on the target machine, and when the specified time expires, the profile is automatically installed on the target.

Image Setup Timeout

If you specify a timeout value in seconds, the setup of the WIM image is interrupted when the specified time expires. This option is available only for Tivoli Provisioning Manager for OS Deployment Servers version 7.1.1.14 or later.

Repartition the disks

This check box is selected by default. Clear it to avoid re-partitioning the disks on the target machine. In this case, only the specified partitions are deployed on the existing partition layout.

Disable enhanced error detection

Select this option to prevent modifications to the boot sequence during the bare metal deployment. For more information, see “Error detection” on page 75.

Unique fields for creating a Bare Metal profile for an ISO image:

Required fields:

Edition

The operating system edition you want to deploy. Expand the list to select a different edition.

Same Client Version as server

This checkbox is selected by default indicating that the Endpoint Manager Client version that will be installed on the target system is the same version as the server. You can select a different version, by clearing the checkbox, and selecting the version you want.

Note: The list of available client versions depends on the selected MDT Bundle. For example, if you upgraded your Endpoint Manager Server from version 9.1 to version 9.2, the 9.2 client will not be listed among the available client versions. If you want to select the latest client version, you must recreate the MDT bundle with OS Deployment version 3.6.

Bare Metal Profile properties

Wizard Manual

Passwords entered here will be obfuscated in the datastore. If left blank, the user will be prompted for the password when sending the profile to a bare metal server.

Required Fields

Display Name: Vista (x64) - WinVistax64SP2_1406624086.wim

Edition: Windows Vista Business

Registered Owner: [Empty]

Registered Organization: [Empty]


Image Locale: English - United States

Image Keyboard Locale: 0409:00000409

Time Zone: GMT Standard Time (GMT)

New Computer Prefix: [Empty]

MDT Bundle: MDT_3506_wdk80 (3.5.04)


Administrator Password: [Empty] 

Confirm Password: [Empty]

Same client version as server:

Client version: 9.1.1082.0

Required Domain Credentials

Join Computer To: Workgroup 

Workgroup/Domain Name: workgroup

Unique fields for creating a Bare Metal Profile for a captured image:

Optional fields:

Enable Administrator

You can choose to enable the Administrator account on the target system. If you select this option, you must also specify the password.

Administrator password

Specify the password of the Administrator on the target system. You are asked to enter the password twice for confirmation.

Create Bare Metal Profile

Wizard **Manual**

The domain password and administrator password will be obfuscated in the datastore if entered here. If left blank, the user will be prompted for the password when sending the profile to a bare metal server.

Required Fields

Display Name: Win2008 (x86) - Win2008x86_228.WIM

Registered Owner:

Registered Organization:

Time Zone: GMT Standard Time (GMT)

New Computer Prefix:

MDT Bundle: MDT_3301_WAIK (3.3.01)

Required Domain Credentials

Join Computer To: Specify Domain

Workgroup/Domain Name:

User name:

Password:

Confirm Password:

Optional Fields

Product Key:

Prompt end user for hostname:

Deployment Password:


Auto Deploy Timeout (sec): 

Image Setup Timeout (sec):

Enable Administrator Password

Administrator Password:

Confirm Password:

OK Cancel

When you create bare metal profiles, you can specify the partition layout. The **Partition Mappings** section is the same as in “Miscellaneous Options” on page 72 but the behavior is different in bare metal deployments. When you add partitions, the size of the partitions can be specified using percentages. If you did not select to re-partition the disks, you must adapt the partitions of the source image to match the physical partitions of the target.

Note: You cannot edit boot partitions because the size of these partitions is fixed.

If you decide to repartition the disks on the target machine, the disks are formatted and the partitions are re-created on the target machine as you mapped them in the WIM. If you decide not to repartition the disks on the target machine, the same rules that are described for the number of partitions for re-imaging apply.

If the number of partitions you send to the target is less than the number of partitions that exist on the target, the results of the validation depend on how you

mapped the partitions. For example, a target has Windows 7 with a bootable partition and a system partition. If you deploy a Windows 7 customized bare metal profile with only the system partition and you map this partition to the first partition of the target, the deployment fails. If you map the partition in your profile to the second partition of the target, the deployment is successful.

If you are deploying a bare metal profile on a UEFI target, a dedicated boot partition (ESP) is always created on the target, regardless of how these partitions were mapped in the WIM (system and boot partitions are mapped on the same target partition in the partition editor.)



By using the **Manual** tab, customize the CustomSettings.ini file. Some portions of this file are not present in this tab because they are handled separately by encryption.



The following settings are not present in the **Manual** tab because they are handled separately by encryption: AdminPassword, DomainAdmin, JoinDomain, DomainAdminDomain, DomainAdminPassword, and MachineObjectOU. The settings in the **Wizard** tab take precedence over the settings that are found in **Manual** tab for these values.

Note: Making modifications in this tab can have negative effects if not appropriately tested and verified.

Creating Bare Metal Profiles for Linux Images

Create Bare Metal profiles from the Image Library dashboard, to perform bare metal deployments on Linux targets.

Select a Linux image (.LIM) and click **Create Bare Metal Profile**.

A wizard with the information retrieved from the selected Linux image is displayed.

Bare Metal Profile properties

Wizard Manual

Passwords entered here will be obfuscated in the datastore. If left blank, the user will be prompted for the password when sending the profile to a bare metal server.

Required Fields

Display Name: SLES11 (x64) - SLES11x64SP1_1406631385.lim

Image Locale: English - United States

Time Zone: GMT Standard Time (GMT)

New Computer Prefix: [Empty]

Root Password: [Empty] ⚠

Confirm Password: [Empty]

Same client version as server:

Client version: 9.1.1117.0

Optional Fields

Kernel parameters: [Empty]

Allow client traffic:

Deployment Password: [Empty]

Auto Deploy Timeout (sec): [Empty] ⚠

OK Cancel

Required fields:

Display name

The name of the bare metal profile created from ISO image that you selected. by default it is the same name as the image.

Image Locale

Choose the image locale for the operating system if different form the preset one.

Time Zone

Select the time zone of the target operating system

New Computer Prefix

Specify the string that will be used to build the hostname, computer name, and full computer name of the target.

Root Password

Specify the root password for the target system. You are asked to specify it twice for confirmation.

Same Client Version as Server

This checkbox is selected by default and indicates that the version of the IBM Endpoint Manager Client installed on the target is the same version as the server. Clear this option to select a different client version.

Optional fields:

Kernel parameters

Specify optional kernel parameters for the Linux installer

Allow client traffic

This option is selected by default. It is needed if the selected target has the operating system firewall enabled, to allow inbound udp traffic from the Server. You can also allow inbound traffic on the target by running fixlets 678 or 682. For more information, see “Firewall considerations” on page 86.

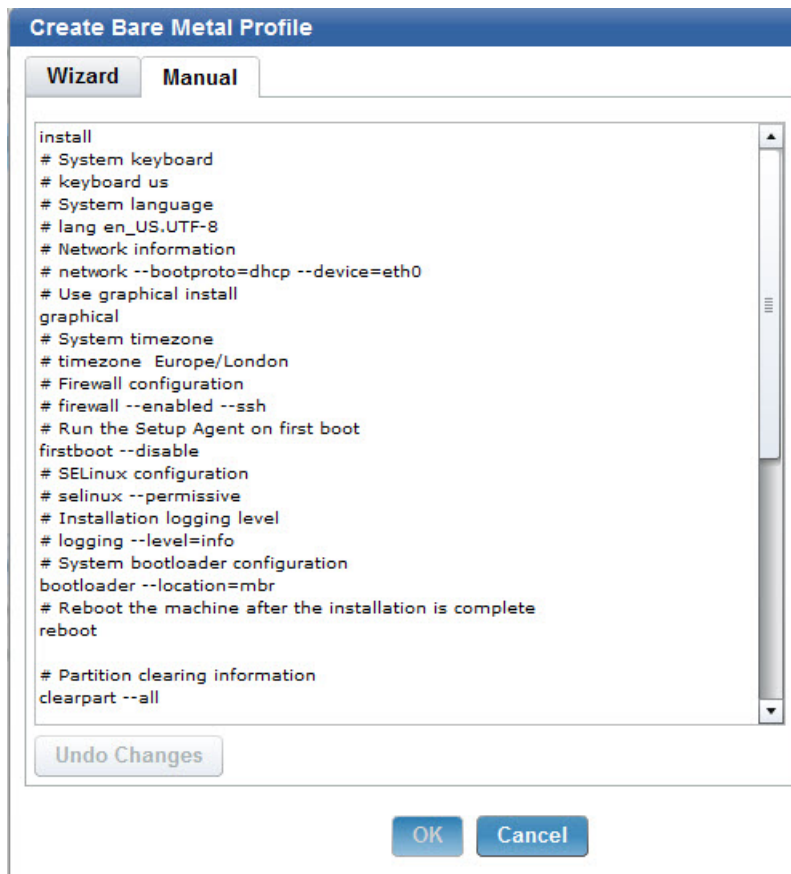
Deployment password

Providing a deployment password protects the profile during deployment. Protected profiles are installed only after you provide the correct password at the target when prompted.

Auto Deploy Timeout (sec)

If you specify a value in seconds, a counter is started during the PXE boot on the target machine, and when the specified time expires, the profile is automatically installed on the target.


By using the **Manual** tab, you can customize the installation with specific settings that are not available in the wizard. Uncomment the settings you want to customize and include in your deployment. For more information about the customization of the configuration files, see “Linux configuration options” on page 82 or refer to the specific Linux vendor documentation.



Working with Bare Metal Profiles

After a profile is created, it is displayed in the **Bare Metal Profiles** table at the bottom of the dashboard. If you select an image, all bare metal profiles that are created from that image are displayed.

Bare Metal Profiles						
<input type="checkbox"/> Create Bare Metal Profile <input type="button" value="Send to Server"/> <input type="button" value="Delete (0)"/> <input type="text" value="Search"/>						
<input type="checkbox"/>	Name	OS	Computers With Profile	Computers Out of Sync	Warnings	
<input type="checkbox"/>	XP (x8...	XP x86	0	0		
<input type="checkbox"/>	XP (x8...	XP x86	1	1		
<input type="checkbox"/>	XP (x8...	XP x86	1	1		

You can edit the profile also by using the  icon. After the changes are saved, an action is automatically generated to update the profile on any servers that have that profile. If there are any servers with the profile, but that are out of sync with the profile available in the console, a warning is shown and you can use

this icon , to resynchronize.

You can send the profile to the server by clicking **Send to Server**.



This generates an action for any valid bare metal servers.

Note:

Bare metal servers might be invalid because they are an old version or do not have encryption enabled.

It is recommended that images are pre-cached to bare metal servers where profiles are created. This way large files are immediately available when first attempting to deploy a profile.

From the Bare Metal Profile table in the Image Library, you can see on which servers the profile exists by clicking the **Servers with Profile** link.



You can delete a profile on the server by selecting it and then clicking **Delete**; the profile is removed also from all servers. An image cannot be deleted if there are profiles that are created from it.

Managing Bare Metal Targets

If you install the Management Extender for Bare Metal targets on your OS Deployment Server, you can manage your targets through the IBM Endpoint Manager console when the targets PXE boot to their local server. You can run the following tasks:

- Change Bare Metal target settings before a deployment
- Schedule the deployment of profiles on Bare Metal targets. For more information, see “Deploying a bare metal profile from the IBM Endpoint Manager console” on page 111.
- Wipe Bare Metal target disks. For more information, see “Wiping target disks” on page 112.

You can run these tasks from the **Bare Metal Target Operations** tasks list.

Target inventory

To retrieve information on the bare metal targets, you must activate the **Bare Metal Target Information** analysis. For each target, you can view:

- Computer model
- Computer serial number
- Computer Status (ok, error, or empty if the target is new)
- Hostname (this property is set with the **Change Bare Metal Target Settings** described in the following topic.
- Universal Unique Identifier (UUID).

Note:

In the **Subscribed Computers** view, targets that successfully completed a PXE boot are identified by the **agent type** attribute set to "Bare Metal Extender." For each target, the listed agent version refers to the agent installed on its local Bare Metal Server.

Changing target settings before deployments

Run the **Change Bare Metal Target Settings** task (350) to set or remove target settings. The settings that you change here are used by the **Deploy Profile on Bare Metal Targets** task (301). If you are setting the hostname for a deployment on a Windows target, you must specify a maximum of 15 characters or else the deployment fails.

Forcing network boot on targets

To boot bare metal targets from the network, run the **Force Network Boot** Fixlet (132). This action changes the boot order of the target so that it boots from the network and not from the operating system. This action is performed only once.

Booting Windows targets without using PXE

If you are not using PXE, you can create network boot media for your targets.

For both BIOS and UEFI targets, if you do not want to use PXE on your network, you can deploy images by creating a network boot CD, DVD, or USB drive. You create network boot media for bare metal deployments using the **Bundle and Media Manager** dashboard.

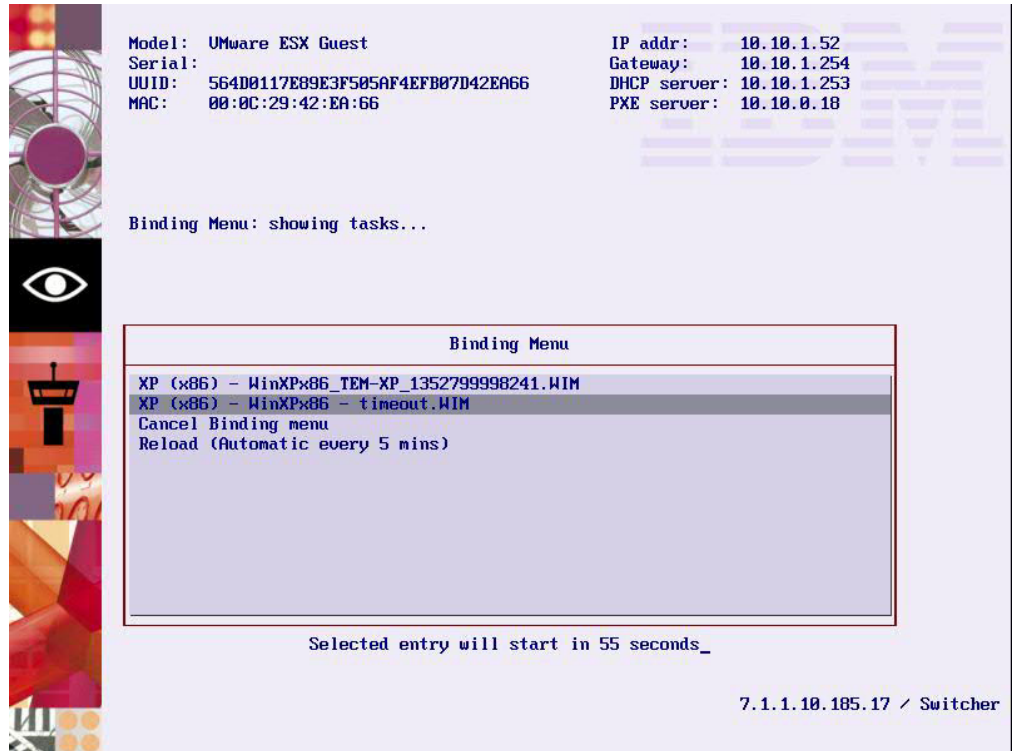
With network boot media, your target can boot and connect to the server in a PXE-less environment. Use this kind of deployment when it is not possible to use PXE to boot the target. For more information, see "Creating Windows Deployment Media" on page 32.

Deploying a bare metal profile from the target binding menu

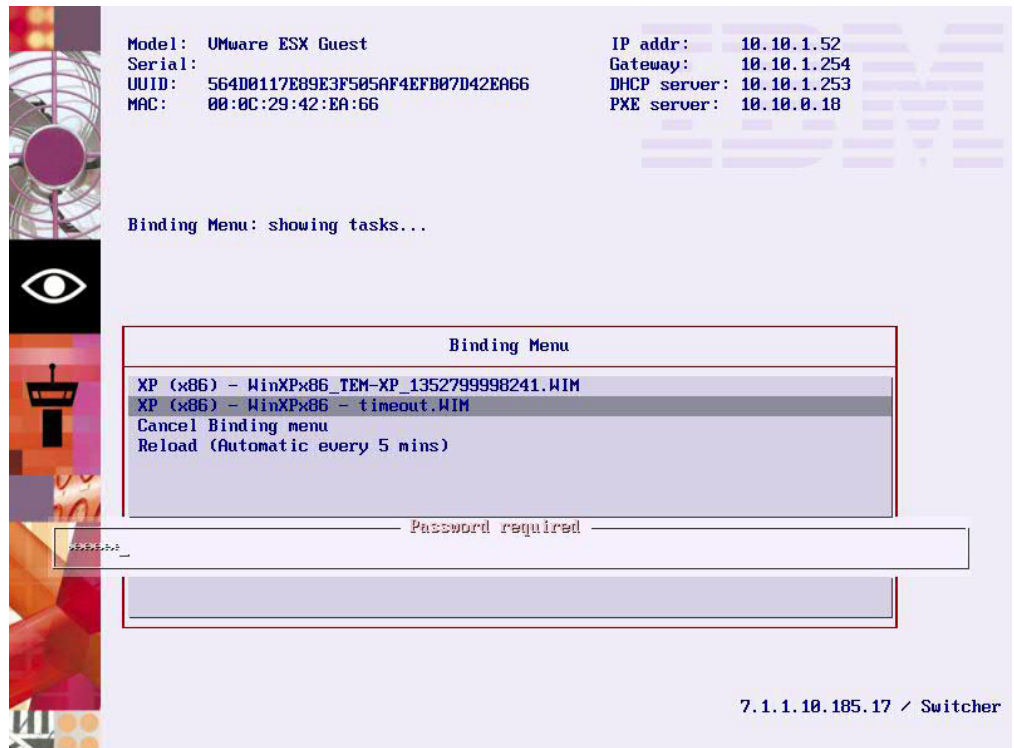
To deploy a bare metal profile on your target, you must reboot the target from the network by pressing a hot key, for example, F1 or F12. For information about which hot key to use, see your computer manual. Before you run the reboot from the network, ensure that the DHCP server is configured.

Important: If you are deploying a bare metal profile on a UEFI target, you must place the hard disk before the EFI shell in the boot sequence, otherwise the deployment does not complete successfully.

During the target reboot, the following window is displayed to download and install a Windows operating system according to the information of the bare metal profile that is created from the IBM Endpoint Manager Console:



In the displayed menu, you can choose to install any of the available profiles. If an auto-deploy profile is displayed in the list, a countdown is started and the profile is automatically installed. To install a profile different from the one with the timeout, you must select it and press enter. Any protected profile is installed only after you enter the required password.



If you click **Cancel Binding Menu** and reboot the target, the menu is refreshed with the updated list of profiles available on the server. Use this option and reboot your target if no bare metal profile is displayed in the binding menu list.

Note: All profiles available on the bare metal server are displayed in the binding menu, regardless of whether they are compatible with the target machine. Deployment tasks of images that are not compatible end in error (for example, deployment of a 64-bit image on 32-bit hardware, or deployment on a UEFI target of an OS image that is not supported on UEFI machines).

If you click **Reload (Automatic every 5 mins)**, you check whether there are pending activities on the server for that target. If there are no activities, the same binding menu is displayed again. If you clear a profile ready to be installed because of a timeout, even if you stop its installation by clearing it, after 5 minutes a task to install this profile is reloaded.

Deploying bare metal profiles based on target properties

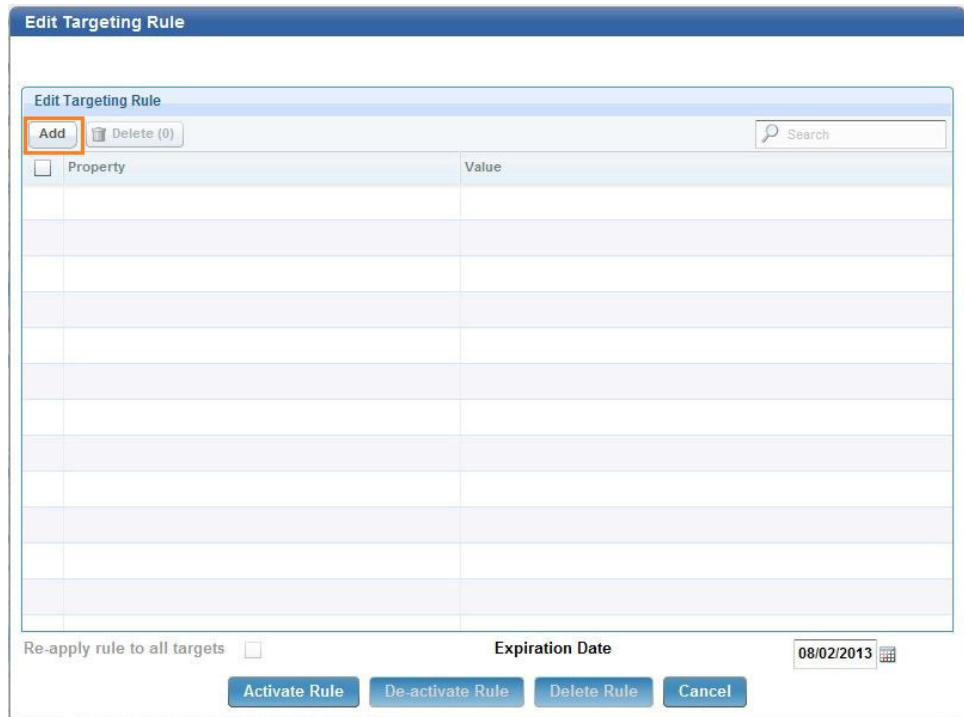
When you deploy a bare metal profile, you can optionally choose to define a set of properties that determine which targets are dynamically selected for deployment. You can specify properties such as IP address list, IP address range, MAC address list, Serial Number list, UUID list, and Model list by defining them as conditions in a rule that is associated to the profile for the selected OS Deployment Server. You can associate only one rule to a profile.

When you save the rule, it is uploaded on the deployment server. When targets perform a PXE boot, the target properties are evaluated against the rule. If a match is found, a deployment task is created for the target. If no match is found, the binding menu is displayed. The target becomes eligible for deployment if at least one of the conditions in the rule is true. You can also specify an expiry date for the rule. After this date, the rule is no longer effective, and targets are not evaluated against this rule.

For each profile, you can see if there are any associated rules and if the status of the rule is active or inactive.

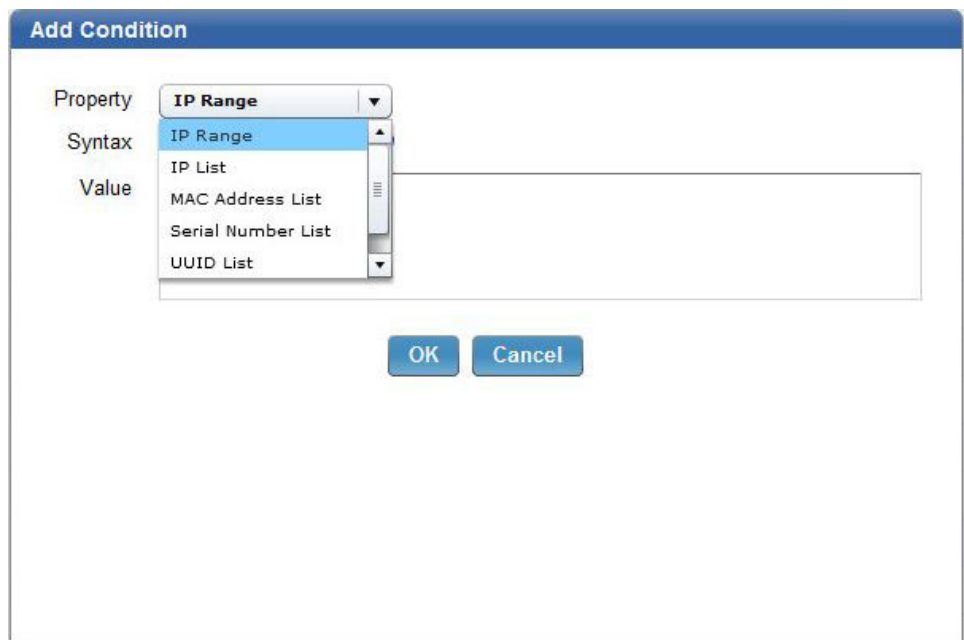
To create a rule, complete the following steps from the **Bare Metal Server Manager** dashboard:

1. Select a bare metal profile and click  to create a rule for the profile. The **Edit Targeting Rule** window is displayed.



Click **Add** to create a new condition in the rule.

- From the **Property** list, select the property that must be verified on the target.



- Specify a value for the target property.

Add Condition

Property: IP Range

Syntax: IPAddress-IPAddress, ...

Value: 10.10.5.20-10.10.5.96

OK Cancel

Click **OK** to save the condition. To add other conditions, click **Add**, and select another property.

4. You can optionally specify an expiration date for the rule, different from the default date. When you select list target properties, such as MODEL LIST, you can use the asterisk (*) as wildcard.

Edit Targeting Rule

Add Delete (0) Search

Property	Value
<input type="checkbox"/> IPRANGE	10.10.5.10-10.10.5.96
<input type="checkbox"/> MODELLIST	*guest

Re-apply rule to all targets

Expiration Date 08/02/2013

Activate Rule De-activate Rule Delete Rule Cancel

You can also specify a question mark (?) as wildcard to represent a single alphanumeric character.

Possible values:

IP Range

The IP address range for the targets. Specify the address range intervals, separating them with a hyphen (-).

IP List, MAC Address List, Serial Number List, UUID List, Model List

One or more elements, separating each element with a comma.

For example, to specify a UUID list:

```
564D9938F62C241D43324B5B24A68A0B,564D9938F62C241D43324B5B24A68A0B
```

To specify a list of models, using wildcards:

```
*guest, HP*
```

When you have finished, click **Activate Rule** to upload the rule on the server.

You can also edit an existing rule to add new conditions or modify the existing ones. To add a new condition, click **Add**. To modify an existing condition, select the condition and click **Edit**.

Targets are evaluated only once against a rule. When you modify a rule, if you want all targets to be evaluated against the changed rule, select **Re-apply rule to all targets**. Click **Activate Rule** to upload the changes on the server.

You can choose to deactivate a rule by clicking **De-activate Rule**. When a rule is deactivated, it still exists but targets are not evaluated against it. You can activate it again later. If you want to delete the rule permanently, click **Delete Rule**.

You can synchronize rule changes either immediately during the rule update, deletion, or deactivation on all the servers that are out of sync with the profile available in the console, or later only on the resources for which a warning is

displayed, by using this icon  to resynchronize.

Deploying a bare metal profile from the IBM Endpoint Manager console

You can deploy bare metal profiles to targets that are connected to Bare Metal Servers that have the Management Extender for Bare Metal Targets plug-in installed.

To deploy a bare metal profile from the console, you must use the **Deploy Profile on Bare Metal Targets** task (ID 301). You can run this task on all Bare Metal Targets that have completed a PXE boot operation. If specific settings were changed on the target, these will be used for the target configuration. For more information about changing target parameters before a deployment, see “Changing target settings before deployments” on page 106. Specify the following information:

- Select the image you want to deploy from the list
- Select the Bare Metal profile you want to deploy. this Profile must exist on the Bare Metal Server.
- Specify whether you want to use Wake-On LAN on the target, if the hardware supports it.

When you are done, deploy the action.

Wiping target disks

You can permanently wipe disks on selected Bare Metal targets, to comply with specific company policies and industry regulations.

Run the **Wipe Disk on Bare Metal Targets** task (ID 300), to perform secure disk wiping on Bare Metal targets that have PXE-booted, and are registered to the IBM Endpoint Manager server through the Bare Metal Extender Plug-in. The task destroys disk content on the target system. You can choose between 5 types of destroy methods, which involve different levels of wiping of the master boot record and disk partitions. If you select the **Arbitrary Overwrite** method, you can also specify the number of overwrite rounds (number of passes) to be completed on the target disk.

WinPE is required for the disk wipe operation, and you can select it from the list of the available versions on the Bare Metal server. For the available WinPE versions to be displayed, you must have previously uploaded at least one MDT Bundle on the IBM Endpoint Manager server.

When you have made your choices, click **Take Action** to select the targets for this task. When the action completes, the disk wipe operation has been queued for execution on the Bare Metal Server. To see the result of the disk wipe operation on the selected targets, check the **Deployment Activity** dashboard.

Note: The disk wipe operation could fail if some drivers are missing from the selected WinPE. In this case, the product attempts to inject the missing drivers and the target may be rebooted several times before the operation completes unsuccessfully.

Chapter 7. Creating and deploying scripting environments

You can automate the execution of configuration tasks on Bare Metal targets by deploying scripting environments.

The Scripting toolkits provided by hardware vendors like IBM, HP, and Dell, include a set of tools to configure and deploy servers in a customized and unattended way. Scripting toolkits create a customized preinstallation environment (WinPE) containing the required drivers and utilities to automate the unattended configuration of servers, and to deploy operating systems based on scripts.

You can deploy vendor-specific hardware configurations to your Bare Metal targets, for example to update the firmware or to configure RAID volumes. For this purpose, you create a scripting environment with the tools provided by the specific hardware vendor and package it in a format that can be managed by the Endpoint Manager infrastructure. Then, through a dedicated dashboard, you import the configurations in your Endpoint Manager environment and deploy them to selected Bare Metal targets.

To use this feature, you must install the Management Extender for Bare Metal Targets on the Bare Metal OS Deployment Servers that manage these targets. When the targets PXE boot to their servers, the scripting environments can be deployed to them.

For information about installing the Management Extender for Bare Metal Targets, see “Deploying the Management Extender for Bare Metal Targets” on page 21.

To automate the configuration and deployment of your targets, you must use the appropriate scripting toolkits provided by the hardware vendor. IT administrators use these toolkits to create the hardware environment that contains Windows Pre-Installation Environment (WinPE), and drivers that are specific to the given hardware models, as well as vendor-specific tools and scripts that perform the actual configuration tasks on the targets. You can also create your own customized WinPE without using a vendor toolkit, and import it into your OS Deployment environment.

Some examples of configurations you can complete on targets are:

- RAID configuration
- Firmware update (BIOS and UEFI)
- Firmware settings (BIOS and UEFI)
- Hardware custom configuration, that is, any kind of tool that you can load into the environment and run from a command line.

As an IT Administrator in your organization, the process you must complete to deploy a scripting environment consists of the following steps:

1. Use the vendor scripting toolkit on a dedicated machine to prepare the scripting environments that you want to deploy to the targets.
2. Download the Scripting Environment Creator tool **ScriptingEnvironmentCreator.zip** on the machine where the vendor scripting toolkit is installed, and use it to package the vendor deployment artifacts into a format (.rad) that can be imported and used by OS Deployment.

3. Import the .rad file containing the scripting environment into the Endpoint Manager infrastructure by using the **Scripting Environment Library** dashboard.
4. Send the Scripting environment to the OS Deployment Bare Metal Servers that manage the targets on which you want to deploy the scripting environments. These Servers must have Tivoli Provisioning Manager for OS Deployment version 7.1.1.17 installed.
5. Trigger the deployment task by running the **Deploy Scripting Environment on Bare Metal Target** Fixlet.

The topics in this section describe how to create a scripting environment that you can import and deploy from IBM Endpoint Manager.

Prerequisites

To prepare, package, and deploy the scripting environment you created, you must have a dedicated machine with the vendor-specific scripting toolkit installed.

The supported vendor scripting toolkits are:

- IBM ServerGuide Scripting Toolkit Version 9.63 (WinPE 3.x based)
- Dell OpenManage Deployment Toolkit Version 4.4 (WinPE 3.x, 4.x, or 5.x based)
- HP Scripting Toolkit Version 9.60 (WinPe 3.x based). .

Note: The supported vendor toolkits refer to the latest available versions on the vendor sites at the time of this OS Deployment release.

Every environment is specific to its vendor, and is prepared with the suitable drivers and scripting toolkit tools. Depending on the toolkit, Windows Automated Installation Kit (WAIK) and/or Windows Assessment and Deployment Kit (WADK) 8.0 or 8.1 are required. Refer to the specific vendor sites and documentation for information about installing and using the toolkits.

On the Bare Metal OS Deployment Server, the following prerequisites must be installed:

- Tivoli Provisioning Manager for OS Deployment Version 7.1.1.17 or later.
- The Management Extender for Bare Metal Targets plug-in. See “Deploying the Management Extender for Bare Metal Targets” on page 21.

Note: You must not create scripting environments as ISO image files, because this format is not supported.

When you have completed the scripting environment with the appropriate tools, you can package this environment and import it into the Endpoint Manager infrastructure for deployment on targets, as explained in “Creating a scripting environment.” When a scripting environment task is run, the configuration is performed on the target.

Creating a scripting environment

The scripting environment creator allows you to package the vendor-specific environment and configurations in a format that can be managed by OS Deployment.

Before you can deploy a scripting environment on a Bare Metal Target you must convert the vendor-specific scripting environment that you created using the

supported toolkits, into a format that can be imported into the Endpoint Manager environment by using the Scripting Environment Creator tool.

You can also build and import a customized Windows Preinstallation Environment (WinPE) without using a scripting toolkit of a specific vendor. For this purpose, you can specify the *vendorName=Other* option when you run the Scripting Environment Creator tool. You can then import and deploy it as any other scripting environment.

1. Download the Scripting Environment Creator from this link:
<http://software.bigfix.com/download/osd/ScriptingEnvironmentCreator.zip>.
2. Extract the zip file on the same machine where the vendor scripting toolkit is installed.
3. Run the Scripting Environment Creator as follows:

```
rbagent[64].exe -o rad-makescriptingenv scriptingEnvName=scripting_env_name  
exportdir=export_directory [ osdtoolsdir=osdtools_dir ]  
scriptingEnvPath=scripting_env_path vendorName=vendor_name  
[toolsPath=tools_path]
```

Where:

- *scripting_env_name*: is the name of the scripting environment you are creating. The name must be unique in your Endpoint Manager environment.
- *export_directory*: is the path where the Scripting environment is created.
- *osdtools_dir*: is the path where the OSd tools are located. Typically this is the path where you extracted the Scripting Environment creator. This parameter is optional. If not specified, it is the current directory.
- *scripting_env_path*: is the path where you created the vendor scripting environment.
- *vendor_name*: is the name of the vendor. The allowed values are HP, Dell, IBM, or Other.
- *tools_path*: is the vendor tools directory that must be injected into the Scripting Environment. This parameter is optional. This path does not apply when the vendor is IBM.

For example:

```
C:\ScriptingEnvironmentCreator> rbagent -o rad-makescriptingenv  
scriptingEnvName=IBM_Toolkit_env exportdir="C:\scripting_env_IBM"  
scriptingEnvPath="D:\IBM_Toolkit\ibm_utl_sgtkwin_9.63_windows_32-64\sgdeploy\  
WinPE_ScenarioOutput\Local_Asu_Config_Only_x64_BootOrder\ISO" vendorName="IBM"
```

Depending on the Microsoft deployment toolkit (WAIK or WADK 8.0 or 8.1) that is installed on the machine where you have run the vendor scripting toolkit, the output is created in a different directory. You must specify the full path to the scripting environment in the *scriptingEnvPath* input parameter of the scripting environment creator (*rad-makescriptingenv*):

- *<toolkit_output>\ISO* if the toolkit is WAIK (WinPE 3.x)
- *<toolkit_output>\media* if the toolkit is WADK (WinPE 4.x or WinPE 5.x)

Example 1: an IBM toolkit on a machine with WAIK (WinPE 3.x):

```
scriptingEnvPath="f:\sgdeploy\WinPE_ScenarioOutput\Local_Raid_Config_Only_x86\ISO"
```

Example 2: a Dell toolkit on a machine with WADK (WinPE 5.x):

```
scriptingEnvPath="C:\DELL-DTK\WinPE5.x_Out_x64\media"
```

4. When the command completes, the output is a bundle that includes the following files:
 - a RAD file containing WinPE version 3, 4, or 5 depending on the vendor toolkit used, and vendor tools (if specified).

- a descriptor file (.scriptenvinfo) that describes the content of the Scripting Environment.

You are now ready to upload the scripting environment to the **Scripting Environment Library** dashboard.

From the **Scripting Environment Library** dashboard, you can manage the scripting environments you created.

Managing scripting environments

The Scripting Environment Library dashboard allows you to import previously created scripting environments and to delete, download or send them to Bare Metal servers.

Before you import a scripting environment, you must have previously completed the steps described in “Creating a scripting environment” on page 114. The scripting environment files must be accessible by the console.


Importing , downloading, and deleting scripting environments

To import a scripting environment :

1. Expand the **Manage Scripting Environment** node and click **Scripting Environment Library** to open the dashboard.
2. Click **Import Scripting Environment**
3. In the dialog, specify the path to your .rad file. The .scriptenvinfo file must be stored in the same path or the import will fail.
4. Click **Analyze**. When the action completes, the imported scripting environment is displayed in the list.

To delete one or more scripting environments, select them from the list and click **Delete**. The selected environments are deleted from the dashboard and also recursively deleted from all Bare Metal Servers that have received them.

To download a scripting environment to a local path on your computer click

download  and specify a local path where you want to save the scripting environment.

Sending scripting environments to Bare Metal servers

To perform configuration tasks on the Bare Metal targets, you must send the scripting environments to the Bare Metal Servers that manage them. Select a scripting environment from the **Scripting Environment Library**, and click **Send to Server**.

A list of applicable Bare Metal Servers is displayed. Select one or more computers and click **OK**.

Deploying scripting environments to Bare Metal Targets

To deploy the scripting environments to Bare Metal Targets, you must run the **Deploy Scripting Environment on Bare Metal Targets** Fixlet.

You must select the Scripting environment that you want to deploy. After you take action on the Fixlet, open the **OS Deployment Activity** dashboard to check the status of the scripting task on the selected targets.

Ensure that the Bare Metal Server that manages the selected targets has already received the scripting environment through the **Send to server** button in the **Scripting Environment Library**.

Troubleshooting scripting environment problems

For problems or errors occurring during the creation of the scripting environment with the Scripting Environment Creator tool, collect the following files from the directory where you extracted the ScriptingEnvironmentCreator.zip:

- rbagent.log
- rbagent.trc

If there are problems in sending the Scripting Environments to the Bare Metal Server, errors are logged in the following file on the Bare Metal Server:

- c:\Program Files\Common Files\IBM Tivoli\radimportscriptingenv.log.

If there are problems during the deletion of a Scripting Environment from a Bare Metal Server:

- Remove the Scripting Environment from the Bare Metal Server Action Info
- Check for any error message in c:\Program Files\Common Files\IBM Tivoli\raddeletescriptingenv.log

For problems during the submission of the Scripting Environment Task, the Fixlet status will report "Failed". Check the following files in C:\Program Files\Common Files\IBM Tivoli:

- BareMetalExtender.trc
- BareMetalExtender.log

for the cause of the failure.

Chapter 8. Maintenance and troubleshooting

You can monitor deployment activities, correct exceptions and adjust configuration settings specific to your environment through dashboards and tasks available for these purposes.

To monitor and maintain your deployment environment, you use the Health Checks Dashboard, the Deployment Activity Dashboard, and the maintenance and configuration tasks. When exceptions occur, specific error messages are logged. This topic provides an overview of the tools available for troubleshooting configuration and deployment errors, and lists some common exceptions and workarounds. For information about the **Health Checks** dashboard, see “Health Checks Dashboard” on page 26.

Additional troubleshooting information is available in the OS Deployment Troubleshooting wiki page at this link:<https://www.ibm.com/developerworks/community/wikis/home?lang=en#!/wiki/Tivoli%20Endpoint%20Manager/page/OSD%20Troubleshooting>.

Deployment Activity Dashboard

In the Deployment Activity Dashboard, you can see the statuses of Re-Image, Bare Metal, and Capture activities in your environment.

You can also collect information through several analyses. In the Activity Records grid, each individual activity is listed together with important information about the type of activity, the target machine, the task being performed, and the best approximation of the status of the task.

The status given is the best approximation of the current status of the task. Depending on the type of task, an accurate status is not always displayed, and can sometimes be incorrect in certain phases of a deployment task.

OS Deployment - Activity Dashboard

Deployment Activity Dashboard

This dashboard shows the statuses of Re-Image, Bare Metal, and Capture activities in your environment.

Activity Records

Delete (0)

<input type="checkbox"/>	Activity ID(s)	Activity Type	Issue Date	Target	Task	Status
<input type="checkbox"/>	217314747	Bare Metal	Tue, 02 Apr 2013 06:09:13 PM	10.10.0.183	Win7 (x64) - Win7x64_W764PC_1362649409311.WIM	Success
<input type="checkbox"/>	532674205	Bare Metal	Fri, 29 Mar 2013 03:02:36 PM	10.10.0.146	Win7 (x64) - Win7x64_W764PC_1362649409311.WIM	Failed
<input checked="" type="checkbox"/>	5327 / 5325	Re-image	Fri, 29 Mar 2013 02:49:17 PM	VISTA-C29CDDC6B	Deploy Win7x64_W764PC_1362649409311.WIM	Expired - Failed
<input type="checkbox"/>	738845621	Bare Metal	Fri, 29 Mar 2013 02:13:39 PM	10.10.1.120	Win7 (x64) - Win7x64_W764PC_1362649409311.WIM	Success
<input type="checkbox"/>	5308 / 5306	Re-image	Fri, 29 Mar 2013 11:54:56 AM	VISTA-PC	Deploy WinVistax86_VISTA-PC_1363362612298.WIM	Expired - Fixed
<input type="checkbox"/>	227618560	Bare Metal	Fri, 29 Mar 2013 08:05:41 AM	10.10.0.146	Win8 (x64) -3.1.25 Win8x64_UNKNOWIN-VNFED05_1...	Success
<input type="checkbox"/>	594968098	Bare Metal	Fri, 29 Mar 2013 06:37:29 AM	10.10.1.51	Vista (x86) 3.1.25 - WinVistax86_VISTA-PC_136336...	Success
<input type="checkbox"/>	5283 / 5281	Re-image	Thu, 28 Mar 2013 07:21:53 PM	VISTA-PC	Deploy WinVistax86_VISTA-PC_1363362612298.WIM	Expired - Running

Task / Failure Summary **Modify Associated Driver Binding Grid**

Add Failure Info File

Activity Name: Deploy Win7x64_W764PC_1362649409311.WIM
 Activity Type: Re-image
 Target Architecture: x64
 Target Operating System: Win7

Delete a record by selecting the Activity ID and clicking **Delete**.

Click a record to see more detailed information in the **Task / Failure Summary**.

For certain types of failure, a Driver Binding Grid is available. A Driver Binding Grid displays the drivers that are used for each hardware device on the computer being targeted.

OS Deployment - Activity Dashboard

Deployment Activity Dashboard

This dashboard shows the statuses of Re-Image, Bare Metal, and Capture activities in your environment.

Activity Records

Delete (0) Search

Activity ID(s)	Activity Type	Issue Date	Target	Task	Status
217314747	Bare Metal	Tue, 02 Apr 2013 06:09:13 PM	10.10.0.183	Win7 (x64) - Win7x64_W764PC_1362649409311.WMM	Success
532674205	Bare Metal	Fri, 29 Mar 2013 03:02:36 PM	10.10.0.146	Win7 (x64) - Win7x64_W764PC_1362649409311.WMM	Failed
5327 / 5326	Re-image	Fri, 29 Mar 2013 02:49:17 PM	VISTA-C29C0DC6B	Deploy Win7x64_W764PC_1362649409311.WMM	Expired - Failed
738845621	Bare Metal	Fri, 29 Mar 2013 02:13:39 PM	10.10.1.120	Win7 (x64) - Win7x64_W764PC_1362649409311.WMM	Success
5308 / 5306	Re-image	Fri, 29 Mar 2013 11:54:56 AM	VISTA-PC	Deploy WinVistax86_VISTA-PC_1363362612298.WMM	Expired - Fixed
227618560	Bare Metal	Fri, 29 Mar 2013 08:05:41 AM	10.10.0.146	Win8 (x64) - 3.1.25 Win8x64_LINKNOWN-VNFED05_1...	Success
594966098	Bare Metal	Fri, 29 Mar 2013 06:37:29 AM	10.10.1.51	Vista (x86) 3.1.25 - WinVistax86_VISTA-PC_136336...	Success
5283 / 5281	Re-image	Thu, 28 Mar 2013 07:21:53 PM	VISTA-PC	Deploy WinVistax86_VISTA-PC_1363362612298.WMM	Expired - Running

Task / Failure Summary **Modify Associated Driver Binding Grid**

Driver Bindings

Search

Device	Device ID	Driver Bound	Current Driver Binding
VMware SVGA II Adapter	15ad.0405.15ad.0405	No applicable drivers found	
Intel Corporation 82371AB/EB/MB PIX4 IDE	8086.7111.15ad.1976	Built-in	
LSI Logic / Symbios Logic 53c1030 PCI-X Fusion-MPT Dual UI	1000.0030.15ad.1976	Built-in	
VMware Virtual Machine Communication Interface	15ad.0740.15ad.0740	No applicable drivers found	
Intel Corporation 82545EM Gigabit Ethernet Controller (Copper	8086.100f.15ad.0750	Built-in	

In the **Modify Associated Driver Binding Grid**, you can find additional information about all the hardware devices.

In the **Driver Bindings** table, more information is displayed about a device. You can find what occurred for that device, and a list of drivers from which you can choose. If you click a driver, additional details are displayed to help you decide which driver to associate to the hardware device.

Click **Edit** to modify the driver associated to the device.

In some cases, the driver binding grid might not be retrieved automatically. If you have a driver binding grid available, you can manually add it to the Activity Records table by selecting the corresponding activity and then clicking **Add Failure Info File** in the **Task / Failure Summary**.

For Re-Imaging and Capture jobs that have failed, you can find the generated driver binding grid on the endpoint in the file location `C:\Deploy\%OEM%\BigFixOSD\RBAgent\osgrid.ini.update` and `C:\Deploy\%OEM%\BigFixOSD\RBAgent\pegrid.ini.update`.

If re-imaging was successful, but drivers were missing in the new operating system, you can find binding grids in `C:\Program Files\BigFix Enterprise\BES Client\OSDeploymentBindingGrids\` or in the `C:\Program Files\BigFix Enterprise\BES Client__BESData__Global\Logs\OSDeploymentLogs\OSDeploymentBindingGrids` folder in the client logs directory. Depending on where the deployment failed, apply the appropriate grid to the corresponding activity record in the dashboard.

If bare metal jobs have failed, you can find the generated driver binding grid on the relay server in the following path: C:\TPMfOS Files\global\hostactitiestasknnnnn.

Maintenance and Configuration tasks

Maintenance and Configuration tasks indicate actions that you must take to maintain your deployment. If a Fixlet or task in the list is disabled, it is not relevant to any computers in your deployment.

Click *Maintenance and Configuration* from the navigation tree and select a task or Fixlet. For each Fixlet, click the name and then click in the Actions box of the Fixlet window to deploy the appropriate action.

Maintenance and Configuration		Search Maintenance and Configuration	
Name	Source Sev...	Category	Download Size
Deploy MDT Media Creator	<Unspecified>	Setup	11.79 MB
Change Upload Maintenance Service Scan Delay Period	<Unspecified>	Configuration	<no download>
TEM Server: Install Upload Maintenance Service for ...	<Unspecified>	Configuration	100 KB
Uninstall Upload Maintenance Service	<Unspecified>	Maintenance	<no download>
Remove System Restore Points	<Unspecified>	Maintenance	<no download>
Start BES Relay Service	<Unspecified>	Maintenance	<no download>
Start OS Deployment Server Services	<Unspecified>	Maintenance	<no download>
Clean Up Failed Re-Image	Moderate	Maintenance	<no download>
OS Deployment - Upgrade Upload Maintenance Service	Important	Setup	<no download>
Warning: Relay setting _BESGather_Download_Cach...	Critical	Support	<no download>
Warning: TEM Server is Low on Free Disk Space	Critical	Support	<no download>
Update Server Whitelist for OS Deployment	Critical	Setup	<no download>

Troubleshooting

When problems occur, you can determine what went wrong by viewing messages in the appropriate log files which provide information about how to correct errors.

Files for troubleshooting deployment failures on Windows targets

When a deployment fails you can troubleshoot the problem by analyzing the following files depending on the scenario you are running:

Table 7. Files for deployment failure problem determination

Filename	Path	Scenario
<ul style="list-style-type: none"> peresult.ini pegrid.ini.update rbagent.trc osresult.ini osgrid.ini.update 	C:\Program Files\BigFix Enterprise\BES Client__BESData__Global\Logs\OSDeploymentLogs\OSDeploymentBindingGrids on target workstation	Re-image was successful but drivers were missing in the new operating system. You can find Windows PE binding grid in the specified location.
<ul style="list-style-type: none"> peresult.ini pegrid.ini.update rbagent.trc osresult.ini osgrid.ini.update 	C:\Deploy\%OEM%\BigFixOSD\RBAgent on target workstation for re-imaging	C:\Deploy\%OEM%\BigFixOSD\RBAgent on target workstation for re-imaging

Table 7. Files for deployment failure problem determination (continued)

Filename	Path	Scenario
<ul style="list-style-type: none"> • bomnn-peresults.ini • bomnn-pegrid.ini.update • bomnn.trc • bomnn-osresult.ini • bomnn-osgrid.ini.update 	C:\TPMf0S Files\global\ hostactitiestasknnnnn on relay server for bare metal	Bare metal jobs have failed. You can find the generated driver binding grid on the endpoint in the specified location.
OSD log files	C:\TPMf0S Files\logs on relay server for bare metal	OSD PXE component logs

Files for problem determination during Windows setup

During the re-imaging process and during Bare Metal deployments, errors can occur when Windows Setup is installing and configuring the new operating system. To troubleshoot errors occurring during the Windows Setup phase, check the following log files in these locations:

```
C:\Windows\Panther
C:\Windows\Panther\setuperr.log
C:\Windows\Panther\miglog.xml
C:\Windows\Panther\PreGatherPnPList.log
C:\Windows\setupact.log
C:\Windows\setuperr.log
C:\WINDOWS\INF\setupapi.dev.log
C:\WINDOWS\INF\setupapi.app.log
C:\WINDOWS\Performance\Winsat\winsat.log
```

Files for problem determination during Linux deployments

To troubleshoot errors occurring during deployments on Linux systems, check the log files in this location:

```
/var/opt/BESClient/__BESClient/__Global/logs/DeploymentLogs
```

Files:

```
cleanupbesclientcache.log
instpostscript.log
instpostscriptnochroot.log
instprescript.log
limunpack.log
patchlinuxconf.log
prepareimageprovider.log
setlinuxboot.log
testlinuxboot.log
```

Depending on the type of deployment, some of these files may not be available.

For more information about troubleshooting re-imaging process failures, see the IBM Endpoint Manager wiki at this link: <https://www.ibm.com/developerworks/community/wikis/home?lang=en#!/wiki/Tivoli%20Endpoint%20Manager/page/Re-Image%20Process>

Files for troubleshooting Console errors while importing files

When you import files using the Console (for example, when you upload an MDT Bundle, images, or drivers) all temporary files and logs used during the import process are stored in the Console working directory:

%USERPROFILE%\OSDeployment

If any errors occur during the import step, you can troubleshoot the problem by analyzing the general trace file %USERPROFILE%\OSDeployment\rbagent.trc.

All files being uploaded are tracked in the %USERPROFILE%\OSDeployment\UploadManagerFiles folder.

Deployment media creation problem determination

If errors occur during deployment media creation, you can check the following files:

- From the IBM Endpoint Manager Console, check the GenerateDeploymentMedia Action Info that was executed on the selected target.
- If the selected target is an OS Deployment Server look at the rbagent.log and rbagent.trc files under %CommonProgramFiles%\IBM Tivoli.

For Example:

```
C:\Program Files\Common files\IBM Tivoli
```

on the selected target machine.

- If the selected target is not an OS Deployment Server, look at the rbagent.log and rbagent.trc files under <IEM Client>_BESData\actionsite_Download

For example:

```
C:\Program Files\BigFixEnterprise\BESClient>\_BESData\actionsite\_Download
```

on the selected target machine.

Troubleshooting JoinDomain errors during Bare Metal and re-imaging deployments

Failures that occur when joining targets to domains are not unrecoverable errors. The deployment completes successfully. If the target fails to join the domain, you can determine the cause of the problem by looking in the c:\Windows\Temp\Deployment Logs\ZTIDomainJoin.log file and searching for the string "RC="..

The following list provides details on the most frequent JoinDomain errors:

Case 2 Explanation = "Missing OU"

Case 5 Explanation = "Access denied"

Case 53 Explanation = "Network path not found"

Case 87 Explanation = "Parameter incorrect"

Case 254 Explanation = "The specified extended attribute name was invalid."

-> probably the specified OU (organizational Unit) parameter is incorrect or OU doesn't exist

Case 1326 Explanation = "Logon failure, user or pass"

Case 1355 Explanation = "The specified domain either does not exist or could not be contacted."

-> probably there is a DHCP/DNS configuration error

Case 1909 Explanation = "User account locked out"

Case 2224 Explanation = "Computer Account already exists"

Case 2691 Explanation = "Already joined"

More information about error codes can be found at the following link:<http://msdn.microsoft.com/en-us/library/ms681381%28v=vs.85%29.aspx> .

Troubleshooting Client settings problems after a Bare Metal deployment

If client settings that were specified in a Bare Metal Profile deployed on a target are not correctly set, you can check the following file on the target system for the probable cause::

C:\Windows\temp\...\BFCloseBareMetalTask.log

Problems and limitations

You can troubleshoot and gather information about known problems and limitations. A solution or workaround is provided if available.

CPU usage reaches 100% during installation or upgrade of a Bare Metal Server

Problem description

When installing or upgrading Tivoli Provisioning Manager for OS Deployment on an Endpoint Manager relay, the CPU on that system reaches 100% usage for several minutes. This may downgrade system performance considerably and tasks running on the system might become unresponsive.

Solution/workaround

This problem does not affect the outcome of the installation itself. To minimize the impact on system performance, you can plan the installation or upgrade of your Bare Metal Server in a timeframe during which the relay is not processing other time-critical activities.

Duplicate client computer entry in the Server database after a Linux re-image

Problem description

After a re-image of a Linux system in Install mode, the computer definition for that target is duplicated in the Server database and two entries are displayed in the Console. This problem can occur in the following cases:

1. When the re-imaging is performed, the agent is reinstalled and the existing data in the `/var/opt/BESClient` directory is saved and migrated to preserve the agent identity. Although the cache on the target is cleared during the process, if the resulting size of this directory is greater than 100 megabytes, the client identity is duplicated.
2. When the version of the client you select in the Deploy image to Computer dialog is an earlier version than the version currently installed on the target.
3. When you are re-imaging from a 32-bit to a 64-bit architecture.

Solution/workaround

When this problem occurs, you can remove the duplicate entry from the IBM Endpoint Manager Console by right-clicking on the computer name and selecting **Remove from database**.

Re-image install on RedHat Enterprise Linux (RHEL) 7 stops during boot sequence

Problem description

During a re-image in install mode, processing stops during the boot sequence on a RHEL 7 target. The Dracut Emergency shell is started and the following message is displayed:

```
dracut-initqueue[612]: Warning: Could not boot.  
dracut-initqueue[612]: Warning: /dev/root does not exist  
Starting Dracut Emergency shell...  
Warning: /dev/root does not exist
```

```
Generating "/run/initramfs" rdsoreport.txt
```

```
Entering emergency mode. Exit the shell to continue.  
Type "journalctl" to view system logs.
```

Solution/workaround

When this problem occurs, check for any errors in the network configuration on the target and on the DHCP server. Correct the problem and reboot the target. When you reboot the target the installation resumes.

Typically, this error can occur when the DHCP server has assigned an IP address to the target that was already in use on the network.

Login prompt not displayed on RedHat Enterprise Linux (RHEL) 7 after Bare Metal deployment

Problem description

After a Bare Metal deployment on a RedHat Enterprise Linux Server version 7 (RHEL 7), the login prompt is not displayed on the target, and the following message is issued:

```
sda3: WRITE SAME FAILED. Manually zeroing
```

Solution/workaround

Press Enter on the target and the login prompt is displayed. This error can occur on VMWare targets only.

Copy image settings error on manual driver bindings

Problem description

From the **Image Library** dashboard, when you attempt to copy image settings to a target image from which all manual driver bindings were previously removed, the following error message is displayed:

```
Selected image already contains manual driver binding grids.  
The operation cannot be completed
```

Solution/workaround

Sometimes, the data store is not erased even after drivers are manually removed. To avoid this error, complete the following steps for the target image for which the copy settings operation received the error message:

1. Open the **Driver Library** dashboard.
2. Click the **Bindings** tab.
3. Select the target image and the computer model from the list.
4. Select the bound driver and click **Edit**.

5. Select the **Auto** radio button to disable manual driver binding and save your changes.

From the **Image Library**, select the target image again and click **Copy Settings from...** to repeat the operation.

Appendix A. Setting up OS Deployment in an air-gapped network

You can choose to configure your OS Deployment and Bare Metal Imaging site in an air-gapped network.

To setup the OS Deployment and Bare Metal Imaging site in an air-gapped environment, you need to manually download and cache specific files on the machines where the IBM Endpoint Manager Console is installed as well as on the IBM Endpoint Manager Server. To set up your environment, you must perform the following steps.

1. Obtain OS Deployment and Bare Metal Imaging Site content

You must use the Make Mirror Archive utility, available at the following url: <http://software.bigfix.com/download/bes/util/MakeMirrorArchive.zip>, to download the OS Deployment and Bare Metal Imaging external site content from an internet connected machine. This utility requires the external site masthead file and cannot be run on the Endpoint Manager Server.

For details, see the following link in the IBM Endpoint Manager Wiki: <https://www.ibm.com/developerworks/community/wikis/home?lang=en#!/wiki/Tivoli%20Endpoint%20Manager/page/OSD%20in%20an%20Air-gapped%20or%20Download%20Challenged%20Environment>.

2. Pre-cache OS Deployment and Bare Metal Imaging Site downloads

To pre-cache the OS Deployment site files, you must obtain the OS Deployment and Bare Metal Imaging site masthead file, and create a cache folder for the pre-cached SHA1 files on an internet connected machine. Download and run the BES Download Cacher utility available at the following link: <https://www.ibm.com/developerworks/community/wikis/home?lang=en#!/wiki/Tivoli%20Endpoint%20Manager/page/TEM%20Download%20Cacher>. The utility copies files in the cache folder you specified. You must then transfer these files to the SHA1 download cache on the Endpoint Manager Server. The default location of the download cache is: `...\Program files (x86)\BigFix Enterprise\BES Server\wwwrootbes\bfmirror\downloads\sha1`.

More information is available on the IBM Endpoint Manager Wiki at the following link: <https://www.ibm.com/developerworks/community/wikis/home?lang=en#!/wiki/Tivoli%20Endpoint%20Manager/page/OSD%20in%20an%20Air-gapped%20or%20Download%20Challenged%20Environment>.

3. Pre-cache additional files on the IBM Endpoint Manager Server:

Important: The OS deployment and Bare Metal Imaging site requires the Upload Maintenance Service (UMS) on the Endpoint Manager Server. This service must be installed and running to manage and maintain files correctly. You can install this service from the BES Support site, using the "Install BES Server Plugin Service" Fixlet.

You must also pre-cache additional files on the server. The following files must be downloaded from the sites listed below to the SHA1 download cache on the Endpoint Manager Server.

The default location of the download cache is: ...\\Program files (x86)\\BigFix Enterprise\\BES Server\\wwwrootbes\\bfmirror\\downloads\\sha1

- <http://software.bigfix.com/download/osd/rbagent.exe>
- <http://software.bigfix.com/download/osd/rbagent.pak>
- <http://software.bigfix.com/download/osd/rbagent64.exe>
- <http://software.bigfix.com/download/osd/rbagent.bin>
- <http://software.bigfix.com/download/osd/rbagent64.bin>
- <http://software.bigfix.com/download/osd/osdimageprovider.pak>
- <http://software.bigfix.com/download/osd/osdimageprovider.exe>
- <http://software.bigfix.com/download/osd/osdimageprovider64.exe>
- <http://software.bigfix.com/download/osd/RelayDownloader-1.2.exe>
- <http://software.bigfix.com/download/osd/RelayDownloader-1.2-x64.exe>
- <http://software.bigfix.com/download/osd/getLocaleName-2.0.exe>
- <http://software.bigfix.com/download/osd/modifyUnattend.exe>
- <http://software.bigfix.com/download/redis/unzip-6.0.exe>
- <http://software.bigfix.com/download/redis/unzip32-6.0.exe>
- <http://software.bigfix.com/download/redis/unzip64-6.0.exe>

If you are provisioning a Linux system, and installing an IBM Endpoint Manager Client, you must also pre-cache the selected client installation packages. For more information, see the Image catalog file at this link: <http://software.bigfix.com/download/bes/util/AgentDeployment/TEMImageCatalog.xml> . For example, if you are provisioning SuSE Linux Enterprise Server (SLES) 11 and select to install Endpoint Manager Client Version 8.2 (32 bit), you must pre-cache the following package:

```
- <IEMOSAgentImage>
  <CompatibleOS name="Suse" version="11"/>
  <OSArch>i386</OSArch>
  <OSArch>i486</OSArch>
  <OSArch>i586</OSArch>
  <OSArch>i686</OSArch>
  <ImageName>BESAgent-8.2.1372.0-sle11.i586.rpm</ImageName>
- <ImageSha>
  c6bf32a8a1f5818aa4bdadcd87f354b41d3cd80dbcbc4860dd8bea24ef1be7
  </ImageSha>
  <ImageSize>4666367</ImageSize>
- <ImageURL>
  http://software.bigfix.com/download/bes/82/BESAgent-8.2.1372.0-sle11.i586.rpm
  </ImageURL>
</IEMOSAgentImage>
```

Note: You can use the relevance debugger (QnA debugger) to find the sha1 of each of these files by using the following relevance expression:
(name of it, sha1 of it) of files of folder "c:\AirgapOSD"

where **c:\AirgapOSD** is the folder to which you downloaded the files on the internet connected machine.

4. Download additional files to the machines where the Endpoint Manager Console is installed:

The following files must be downloaded from the sites listed below and placed within %USERPROFILE%\OSDeployment on the console machines. This step must be performed also if your console machines are behind a proxy:

- <http://software.bigfix.com/download/osd/rbagent.exe>
- <http://software.bigfix.com/download/osd/rbagent.pak>
- <http://software.bigfix.com/download/osd/rbagent64.exe>
- <http://software.bigfix.com/download/osd/zip.exe>

Appendix B. Bare Metal OS Provisioning using RAD Profiles

You can Deploy operating systems using RAD system profiles that you import into the Image Library

IBM Endpoint Manager for OS Deployment provides a set of fixlets that you can use to perform bare metal deployments using RAD system profiles. You create system profiles using a Tivoli Provisioning Manager for OS Deployment stand-alone installation, and then export them in RAD file format. You can create profiles for the deployment of Windows, Linux, or VMWare operating systems. To these profiles you must associate a deployment scheme and optionally one or more software modules. On the Endpoint Manager side, you import the RAD profiles into the Image library and then copy them to the Bare Metal servers ready to be deployed.

You can also use these fixlets in a Server Automation environment by including them in your Automation Plans.

Note: To ensure that an adequate disk space is available on the Bare Metal Servers to correctly receive the RAD profiles, you must add the following client setting to those Bare Metal Servers in your network that need to receive the RAD profiles. The size value you set must be large enough to contain the RAD images:

```
_BESClient_Download_PreCacheStageDiskLimitMB
```

If the space is not sufficient, the send to server of these profiles fails.

From the OS Deployment and Bare Metal Imaging site, expand **Deploy OS using RAD profiles**. The available fixlets and tasks are displayed:

Deploy an operating system to one or more computers

This fixlet deploys the specified RAD Bare Metal Profile to one or more computers that are not already registered with a Bare Metal Server.

Deploy operating system to one or more registered computers

This fixlet deploys the specified RAD Bare Metal Profile to one or more computers that are already registered with the bare metal server.

Register computer with Bare Metal Server

This fixlet registers new computers with the bare metal server. For each computer you want to register, you specify a MAC address and an associated computer name.

Force network boot

This Fixlet boots the computer on the network to facilitate re-imaging. The boot order of the computer is changed so that it boots from the network and not from the operating system. This is done just once. The last action is a new reboot of the computer. This operation allows Tivoli Provisioning Manager for OS Deployment to capture an image from the computer and to re-image a new operating system. If the target computer is an Endpoint Manager client, it is rebooted through the network and it waits for the Bare Metal server to deploy the RAD profile.

Note: The deployment Fixlets run successfully only on targets that PXE boot through the network.

Depending on the Fixlet you select to run, you need to specify one or more of the following parameters:

MAC Address:

The MAC Address of the computer or computers that you are provisioning. Specify them as a comma separated list.

Computer name:

The name or names for the computers that you are provisioning. Use commas to separate each entry. Do not include spaces.

Name of the Bare Metal Profile:

Select the Bare Metal Profile you created from the imported RAD system profile.

Use Wake-on-LAN

Optionally, select to use Wake-on-LAN to power-on the computers.

For detailed information about creating and exporting system profiles and deployment schemes, see Tivoli® Provisioning Manager for OS Deployment documentation at this link: <http://www-01.ibm.com/support/knowledgecenter/SS3HLM/welcome>.

To set up your environment for Linux and Windows deployments using RAD profiles , see the examples provided in the IBM Endpoint Manager wiki at these links:

- For Linux deployments: <https://www.ibm.com/developerworks/community/wikis/home?lang=en#!/wiki/Tivoli%20Endpoint%20Manager/page/How%20to%20set%20up%20for%20Linux%20OS%20%20Provisioning%20with%20Server%20Automation>
- For Windows deployments: <https://www.ibm.com/developerworks/community/wikis/home?lang=en#!/wiki/Tivoli%20Endpoint%20Manager/page/How%20to%20Set%20up%20for%20Windows%20Server%20OS%20provisioning%20using%20Server%20Automation>.

Files for troubleshooting errors

Problems importing the RAD profiles to the Endpoint Manager Server from the Image Library Dashboard: check %Temp%/OSDeployment/rbagent.trc of the machine where the IBM Endpoint Manager console runs.

Problems sending the image to the Bare Metal Server: check the BES client logs on your relay in <BESCLIENTPATH>/_BESData/_Global/logs, for example: BigFixEnterprise/BES Client/_BESData/_Global/logs.

Error deploying the RAD profiles on the targets: Check the deployment logs in <TPMfOSD path>/global/hostactivities/taskxxxxxxxx, on the Bare Metal targets, where taskxxxxxxxx is the task number that you can view in the Deployment Activity Dashboard.

Appendix C. Frequently asked questions

What is the BES Server Plugin service?

The BES Server Plugin service facilitates communication between the IBM Endpoint Manager server and side utilities such as the BES Upload Maintenance service. For more information about the BES Server Plugin service and detailed setup instructions, see **TEM Server Plugin Service installation and setup**.

What is the Upload Maintenance service and why do dashboards show warnings of "Upload in Progress"?

The Upload Maintenance service is a utility that must be set up on the IBM Endpoint Manager server to manage file uploads. When the server utility is set up, file status is updated on the server automatically. You might need to refresh your console to see the updates.

How can I deploy OS Deployment bare metal servers using some guidelines?

For instructions for deploying OS Deployment bare metal servers, see <http://www-01.ibm.com/support/knowledgecenter/SS3HLM/welcome>

How do I import a custom .wim file?

You can import from the Image Library dashboard under Manage Images in the navigation tree. You can manually input operating system, architecture, and size on disk.

Note: Size on disk in this case indicates the extracted size of the .wim file. This is typically about two and a half times the size of the actual .wim file.

When can PE drivers be used?

PE drivers are injected into the PE .wim file in the operating system before the start of a migration.

Does OS Deployment version support re-imaging systems with multiple partitions?

Yes. Systems with multiple partitions are supported to the extent that the Microsoft Deployment Toolkit is able to support them, although non-standard partition numbering is not currently supported.

Why did my driver fail to upload?

The most common reasons why drivers fail to upload is because they were not correctly written, such as missing required fields, or they are not plug-and-play drivers.

What does Part 1 and Part 2 of the Re-Image Action refer to?

Part 1 of the Re-Image Action is a multiple action group (MAG) that downloads and prepares all of the necessary files and resources for re-imaging. It then starts the re-image process. Part 2 is run after the re-image task has completed and performs any necessary cleanup tasks.

Why does Part 1 of the Re-Image Action report as completed although the Re-Image process is still running or has failed?

The last part of the first multiple action group is to stop the IBM Endpoint Manager client to correctly save the state of the IBM Endpoint Manager client for restoring after the Re-Image process. This means that the IBM Endpoint Manager client no longer reports on the status of the Re-Image until after the Re-Image process is completed and Part 2 has started running. The status of Part 1 is not indicative of the overall success of the Re-Image; it shows only that the process started successfully.

When re-imaging, are there any restrictions on upgrading or downgrading the current operating system?

When you re-image a computer you can upgrade the operating system or install a later service pack, but you cannot downgrade architectures or operating systems (you cannot deploy a 64-bit image on a 32-bit target or re-image from Windows 7 to Windows XP). However, you can deploy a 32-bit image on a 64-bit target if the hardware supports it.

I am upgrading Tivoli Provisioning Manager for OS Deployment servers from a prior version. Is there anything that I need to do?

Targets previously known to Tivoli Provisioning Manager for OS Deployment servers might need to be either deleted or changed to "Kernel Free" and "Autoboot" to correctly see created bare metal profiles when PXE booting.

Does OS Deployment support capturing and re-imaging of Windows systems with encrypted disks?

Re-imaging fails on targets that have encrypted disks. If you are using a full disk encryption product on your targets you must decrypt the disks before capturing or re-imaging these systems.

Appendix D. 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

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.



Printed in USA