BigFix

OS Deployment V3.12.1 User Guide

Special notice

Before using this information and the product it supports, read the information in Notices *(on page cclxvi)*.

Edition notice

This edition applies to BigFix version 10 and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

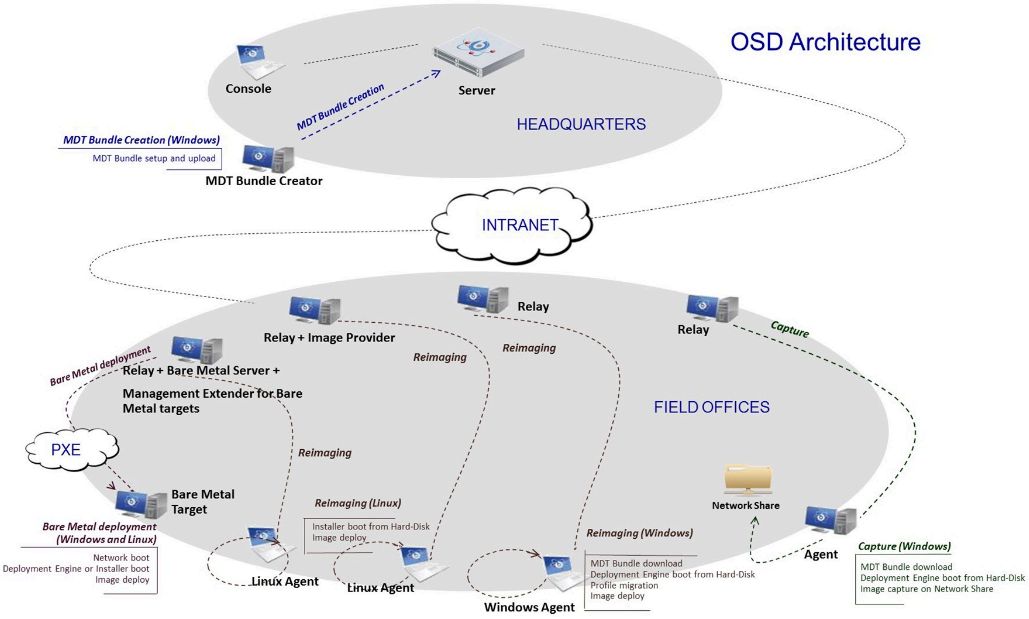
Chapter 1. Product overview

BigFix Bare Metal Server, which is part of the Lifecycle Management suite, provides a consolidated, comprehensive solution to quickly deploy new workstations and servers throughout a network from a single, centralized location. This solution saves time and money, enforces a standardized and approved image, and reduces risks associated with non-compliant or insecure configurations.

The solution provides complete OS provisioning and system reimaging capabilities for Windows and Linux targets. You can deploy a fully-configured operating system to multiple computers across an enterprise.

You can deploy, configure, and manage BigFix Bare Metal Server from the BigFix infrastructure. After you set up the Bare Metal 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 BigFix OS Deployment components and terminology

OS Deployment is a platform-based application. Before you begin working with OS Deployment in your environment, become familiar with the key product components and concepts.

Agent

An BigFix 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 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 BigFix agent installed is referred to as a client. In an OS Deployment network, clients are recipients of deployment actions. They can receive OS upgrades, and can be reimaged by retaining existing user data. A client 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.

You can deploy bare metal profiles and reimaging profiles using multicast communication, if your network infrastructure supports this protocol.

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 BigFix 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 BigFix infrastructure, through the Management Extender for Bare Metal Targets component.

Console

The BigFix 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. Windows Preinstallation Environment (WinPE) and Windows operating systems require drivers, for both the preinstallation 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. In earlier versions of OS Deployment, drivers were selected at deployment time, based on best match criteria for the operating system to be deployed and the devices installed on the target hardware. From version 3.7, driver management is simpler and more efficient. You can explicitly bind drivers to specific machine models for the images you plan to deploy at driver import time. At run time, these bindings take precedence over the automatic binding mechanism.

You can also check which drivers are missing before deploying an image, and import them selectively.

Image

An image is a "copy" of an operating system. An image can be created by capturing a reference machine or created from 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 theBigFix Server. You can then manage the reported Bare Metal targets through theBigFix infrastructure. The Management Extender for Bare Metal targets requires the Proxy Agent component ofBigFix.

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 tool 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.

Note: This component is deprecated. The new component that replaces it is the Windows Bundle.

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 that you want to deploy, the MDT Bundle Creator machine might require access to the internet to download the necessary tools.

Note: This component is deprecated. The new component that replaces it is the Windows Bundle Creator.

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 BigFix infrastructure for devices that do not run a native agent.

Reimage Profile

A Reimage profile is used to reimage Windows targets using multicast communication. To deploy an image using multicast, the Bare Metal Server must be installed on the relays managing these targets. You must create a reimage profile and precache it on the Bare Metal Server before you can deploy it on the target. The reimage profile contains a set of customizable parameters that affect how the multicast distribution will be completed.

Relay

An BigFix 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

BigFix 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 BigFix 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 (WAIK):

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

Windows Bundle

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

Windows Bundle Creator

The Windows 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 Windows Bundle Creator system. The Windows Bundle Creator machine requires access to the internet to download the necessary tools, if not preinstalled.

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 a Windows 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 Windows 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. Targets can be reimaged in multicast.

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 BigFix 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 BigFix 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 BigFix 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 chosen 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 BigFix infrastructure ready to be deployed. When the operator performs a PXE boot operation, the new server becomes manageable from the BigFix console. A Hardware Configuration Task is then sent to the target to perform the necessary changes.

Deployments using multicast communication

For reimaging and Bare Metal deployments of Windows targets, users can take advantage of the multicast protocol if their network infrastructure supports this type of communication. Multicast communication requires the Bare Metal server. Deployments using multicast have a significant reduction in bandwidth use but may increase overall deployment time. When multicast is used, every target starts downloading images as soon as it is ready, and continues with the deployment when it has downloaded all the required files. When two or more targets are downloading files in parallel, they share the same bandwidth.

What is new in OS Deployment and Bare Metal Imaging site 116 (OSD 3.12.1)

Become familiar with the new and changed features of this release.

Added support

Windows 11 25H2 (deploy to and deploy from)

New Windows tool

Windows Bundle 3.12 to support Windows deployment/capture tasks (supersedes MDT Bundle)

Features added in previous versions

In this section, you can find the feature updates from the previous versions.

The following updates were released with OSD 3.11 site 115

Added support (deploy from)

Windows Server 2025

Added support (deploy to)

Red Hat Enterprise Linux 9.5

New feature

Windows OS capture images offline patching

Database support

Microsoft SQL Server 2022 Express is now the default database server for the Bare Metal OS Deployment Server on Windows OS version 10

The following updates were released with OSD 3.11 site 114

Added support (deploy to)

Windows Server 2025

The following updates were released with OSD 3.11 site 113

Added support (deploy to)

Windows 11 Version 24H2

SUSE Linux Enterprise (SLE) 15 SP6

Red Hat Enterprise Linux 8.10

Ubuntu 24.04

Added support (deploy from)

Windows 11 Version 24H2

Windows tools update

WADK for Windows 11 version 24H2 (build 26100) support in MDT Bundle

New feature

In-place upgrade for Red Hat Enterprise Linux (major version upgrade)

The following updates were released with OSD 3.11 site 112

New Operating System support

Red Hat Enterprise Linux 9 support (deploy to) upto 9.4

Added support

Red Hat Enterprise Linux 8.9 support (deploy to)

New feature

In-place upgrade for Windows Server

The following updates were released with OSD 3.11 site 111

New OS support

Ubuntu 22.04 (Capture & deploy the Capture image)

Added support

Windows 11 version 23H2

Red Hat Enterprise Linux 8.8

SUSE Linux Enterprise Desktop (SLED) 15 SP5

SUSE Linux Enterprise Desktop (SLES) 15 SP5

Security improvement

TLS 1.3 protocol is now supported for Bare Metal Server TLS connections

Linux OS Resource improvement

Ubuntu resources now exploit grub2 as UEFI image loader

The following updates were released with OSD 3.11 site 110

New OS support

Ubuntu 22.04 (Capture & deploy the Capture image)

Added support

Windows 11 version 23H2

Red Hat Enterprise Linux 8.8

SUSE Linux Enterprise Desktop (SLED) 15 SP5

SUSE Linux Enterprise Desktop (SLES) 15 SP5

Security improvement

TLS 1.3 protocol is now supported for Bare Metal Server TLS connections

Linux OS Resource improvement

Ubuntu resources now exploit grub2 as UEFI image loader

The following updates were released with OSD 3.11 site 109

Added support

Windows 11 version 22H2

Windows 10 version 22H2

Red Hat Enterprise Linux 8.7

Windows tools update

WADK for Windows 11 version 22H2 (build 22621) support in MDT Bundle

The following updates were released with OSD 3.11 site 105

New Feature

Decentralized Image Library: You can now upload an OS image to a different repository other than the BigFix Root server. For more information, see Upload Mode *(on page 128)*.

Added support

Red Hat Enterprise Linux 8.5

Red Hat Enterprise Linux 8.6

SUSE Linux Enterprise Desktop (SLED) 15 SP3

SUSE Linux Enterprise Desktop (SLED) 15 SP4

SUSE Linux Enterprise Server (SLES) 15 SP3

SUSE Linux Enterprise Server (SLES) 15 SP4

Added certification

Nutanix virtualization environment is now certified for Windows images.

Linux OS Resource improvement

SLES/SLED resources now exploit grub2 as UEFI image loader.

Removed Content

Fixlet 135 - Deploy MDT 2013 or MDT 2013 Update 1 already superseded is now removed from the OSD site.

The following updates were released with OSD 3.11 site 103

New Operating System support

- Ubuntu 20.04 (deploy to)

Added support

Red Hat Enterprise Linux 8.4 support (deploy to)

Red Hat Enterprise Linux 8.3 support (deploy to)

Red Hat Enterprise Linux 7.9 support (deploy to)

The following updates were released with OSD 3.10 site 102

New Operating System support

- Windows 11 (deploy to and deploy from)
- Windows Server 2022 (deploy to and deploy from)

Added support

Windows 10 version 21H1

Windows tools update

WADK for Windows 11 (build 22000) support in MDT Bundle

Flash removal

All the Flash dashboards (already deprecated) are now removed from the OS Deployment and Bare Metal Imaging site.

The following updates were released with OSD 3.10 site 99

New Operating System support

- SUSE Linux Enterprise Server (SLES) version 15 up to SP2
- SUSE Linux Enterprise Desktop (SLED) version 15 up to SP2

The following updates were released with OSD 3.10 site 96

Flash removal from BigFix OS Deployment dashboards

All OSD dashboards are now fully Flash free.

Note: The old Adobe Flash based dashboards are still available, but they are deprecated. They will be removed in a future release.

The following updates were released with OSD 3.10 site 92

Flash removal from BigFix OS Deployment dashboards

Following OS Deployment dashboards are now Adobe Flash free with some limitations:

- Bare Metal Server Manager
- Image Library
- Health Checks
- Bundle and Media Manager

Note: The old Adobe Flash based dashboards are still available and are fully functional.

The following update were released with OSD 3.10 site 90

Added support

Windows 10 Release ID 20H2 (displayed as 2009) support (deploy to).

Flash removal

The Capture and Activity Dashboard are now JavaScript based. The old Flash supported wizards are still available as deprecated content.

Reorganized content

The **Modify Associated Driver Binding Grid** tab is removed from the Activity Dashboard. This feature is already available in the Driver Library.

The following update were released with OSD 3.10 site 89

Updated link

Fixlet 137: Deploy MDT build 8456

The following updates were released with OSD 3.10 site 88

Added support

- Windows 10 Release ID 2004 support (deploy to)
- Red Hat Enterprise Linux 8.2 support (deploy to)
- Red Hat Enterprise Linux 7.8 support (deploy to)
- CentOS Linux 7.8 support (deploy to)
- SUSE Linux Enterprise Server (SLES) version 12 up to SP5
- SUSE Linux Enterprise Desktop (SLED) version 12 SP4

New Windows tool support

This release supports WADK 10 Release ID 2004 to use with MDT 8456

New File System support

btrfs file system is now supported for capture/deploy-of-the-capture-image of SLES/SLED 12

Linux OS Resource improvement

- The OS resource of Setup images is now visible on dashboard and shared with other Linux tasks. It is uploaded with ISO, if missing, and can be updated.
- RHEL/CentOS resources now exploit grub2 as UEFI image loader. This solves issues with some machines with new hardware.

The following updates were released with OSD 3.10 site 87

New Operating System support

CentOS Linux 8 support up to update 1 (deploy to)

Added support

Red Hat Enterprise Linux 8.1 support (deploy to)

Added support

ESXi 6.0 support up to update 3 (deploy to)

Added support

ESXi 6.5 support up to update 3 (deploy to)

Added support

ESXi 6.7 support (deploy to)

New feature

Reset the status of a bare metal target via new Task 303

New feature

SELinux support for RHEL and CentOS deployments

Database support

Microsoft SQL Server 2017 Express is now the default database server for the Bare Metal OS Deployment Server on 64-bit architectures

Database support

Added support to preinstalled Microsoft SQL Server 2019 Express for Bare Metal Server

The following updates were released with OSD 3.10 site 86

New Operating System support

Red Hat Enterprise Linux 8.0 support (deploy to)

New Operating System support

CentOS Linux 7 support up to SP 7 (deploy to)

Added support

Windows 10 Release ID 1909 support (deploy to)

Added support

Red Hat Enterprise Linux 7.7 support (deploy to)

Added support

Ubuntu Desktop 18.04 and 19.04 (Capture and Deploy the Capture Image)

New feature

Allow the user to manage DHCP proxy feature of Bare Metal Server from BigFix console

New feature

Allow the user to manage the TLS protocols for Bare Metal Server Web Interface

New feature

Allow custom certificate for Bare Metal Server Web Interface

Usability improvement

Environment support in RHEL 7/8 and CentOS 7 setup image deployment

Usability improvement

Added the option to ignore warnings in Windows In-place Upgrade fixlet wizard

The following updates were released with OSD 3.10 site 85

Added support

Windows 10 Release ID 1903 support (deploy to)

Added support

Windows Server 2019 support (deploy from)

Windows tools update

WADK 10 for Windows 10 Release ID 1903 support in MDT Bundle

Database support

Preinstalled MSSQL Express 2017 support for Bare Metal Server

Usability improvement

Display multicast session information on the target computer

New feature

Bitlocker configuration in the bare metal profile wizard

New feature

Allow high-performance deployments with target computer lid closed

The following updates were released with OSD 3.10 site 83

Added support

Windows 10 Release ID 1809 and Windows Server 2019 support (deploy to)

Added support

Red Hat Enterprise Linux 7.5 and Red Hat Enterprise Linux 7.6 support (deploy to)

Added support

MDT 8456 support

The following updates were released with OSD 3.10 site 82

Linux deployment

NVM Express controller support

Windows tools update

WADK 10 for Windows 10 Release ID 1809 support.

The following updates were released with OSD 3.10 site 81

Added support of Red Hat Enterprise Linux (RHEL) 6.10

Red Hat Enterprise Linux (RHEL) 6.10 is supported for capture, reimage, and bare metal deployments.

Added support of Windows 10 Release ID 1803

You can capture, reimage and complete in-place upgrades and bare metal deployments of Windows 10 Release ID 1803.

Added support of Windows Server 2016 Release ID 1803

You can capture, reimage and complete bare metal deployments of Windows Server 2016 Release ID 1803.

New Windows tools

This release supports WADK 10 Release ID 1803 for use with MDT 8450.

The following updates were released with OSD 3.10 site 78

SUSE Linux Enterprise Server (SLES) and Desktop (SLED) Version 12 (x64) up to SP3

Extended support of SUSE Linux Enterprise Server (SLES) and Desktop (SLED) Version 12 up to SP3.

Red Hat Enterprise Linux (RHEL) Version 7 up to update 4 (x64)

Extended support of Red Hat Enterprise Linux (RHEL) Version 7 up to update 4 (x64).

ESXi 6.5

Support of ESXi 6.5 hypervisor.

Windows tools update

In this release we have certified MDT 8450 for use with WADK 10 Release ID 1709.

The following updates were released with OSD 3.10 site 77

Added support of Windows 10 Release ID 1709

You can capture, reimage and complete in-place upgrades and bare metal deployments of Windows 10 Release ID 1709.

Added support of Windows Server 2016 Release ID 1709

You can capture, reimage and complete bare metal deployments of Windows Server 2016 Release ID 1709.

New Windows tools

This release supports WADK 10 Release ID 1709 for use with MDT 8443.

The following features were added in OSD Version 3.10

Added Support of Ubuntu Desktop 16.04 and 17.04 for Capture and Bare Metal deployments

To capture and deploy Ubuntu, you create OS Resources via Fixlet or manually and import them into the Bundle and Media Manager dashboard. You can then capture Ubuntu images for bare metal deployments.

Added Support of Windows 10 Release ID 1703

You can capture, reimage and complete in-place upgrades and bare metal deployments of Windows 10 Release ID 1703.

New Windows tools

This release supports WADK 10 Release ID 1703 for use with MDT 8443.

The following update was released with OS Deployment 3.9 site 71

Added support for BigFix Platform version 9.5 Patch 5

OS Deployment now runs on BigFix Platform 9.5.5. You can capture and reimage computers with BigFix client version 9.5.5.

Added support of Windows Server 2016:

You can install the Bare Metal OS Deployment Server on a system with Windows Server 2016.

You can capture, reimage and perform bare metal deployments on Windows Server 2016.

Added support of Red Hat Enterprise Linux (RHEL) 6.8

RHEL 6.8 is supported for capture, reimage, and bare metal deployments

Added support of new Microsoft Tools (MDT and WADK)

OS Deployment now supports Microsoft Deployment Toolkit (MDT) 8443 and WADK 10 Release ID 1607

New direct boot feature for Windows deployments on UEFI targets with Secure Boot option enabled

You can capture, reimage, and perform bare metal deployments on UEFI targets that are Secure boot enabled. You can also create network boot and offline deployment media for these targets.

You can customize log settings for the Bare Metal OS Deployment Server

From the Bare Metal Server manager dashboard, you can customize the number of log files to use for circular logging and the maximum log file size.

The following update was released with OS Deployment 3.9 (and subsequent site updates up to site 70)

Added support for BigFix platform versions 9.1 Patch 8 and 9.2 Patch 8

Support of Windows 10 for the Bare Metal OS Deployment Server

You can install the Bare Metal OS Deployment Server on a system with Windows 10.

Use permanent caching in Unicast deployments

When deploying images in unicast mode, images are stored in the permanent cache on the Bare Metal Server.

Support of ESD image formats for Windows 10 setup images

Support for images in ESD format was added for Windows 10

Enhancements for Windows 10 in-place upgrades:

Improved Usability and Serviceability

Support of Windows 10 to Windows 10 in-place upgrade deployments

Multicast support for in-place upgrade deployments

Added support for Microsoft SQL Server 2014 SP1 as database for the Bare Metal OS Deployment Server on 64-bit architectures.

If an already installed and configured database is not found, Microsoft SQL Server Express 2014 SP1 is downloaded and installed on the Bare Metal Server.

You can specify custom client settings during Bare Metal deployments of Linux captured images

During a Bare Metal deployment of a captured Linux image, you can optionally specify custom settings for targets.

You can assign relays during Bare Metal deployments of Linux captured images

When deploying a captured Linux image, you can optionally assign a relay to the target of the bare metal deployment.

You can specify target network configuration settings for bare metal deployments

You can specify both static and dynamic network configuration settings for targets in three different ways:

- In the bare metal profile.
- With the corresponding task (354).
- At the target computer with a dedicated user interface.

You can also specify a hostname rule for the targets of the deployment.

You can install or upgrade a Bare Metal server from the network, without previously uploading the corresponding installers manually.

In this release, you can automatically install the latest available version of the Bare Metal OS Deployment server directly from the network

New features for Linux deployments:

You can specify custom client settings during Linux Reimage and Bare Metal deployments

You can define custom client settings that can be used for running other tasks when deploying Linux targets.

Linux Partition editor in the Bare Metal Profile creation wizard simplifies partitioning.

You can specify partitions and logical volume layout (LVM) for Linux deployments for both BIOS and UEFI targets.

You can capture a Linux reference image for bare metal deployments

A new task is available to capture Linux images that you can use for bare metal deployments.

Linux Boot media

You can create Linux network boot media for targets that do not use PXE.

Multicast deployments

You can deploy Linux bare metal profiles using multicast for both captured and setup images.

New features for Windows Deployments

Windows 10 in-place upgrade

You can complete an in-place upgrade to Windows 10 of your existing Windows 7, Windows 8 and Windows 8.1 Update your clients by using the corresponding task (202).

You can choose a BigFix Client version to be installed during a Bare Metal deployment of a manually captured Windows Image

If you are deploying a manually captured Windows image that does not contain a BigFix client, you can choose which version to install from the Wizard tab of the Bare Metal Profile. If the captured image already contains a BigFix client, the dashboard selection is ignored.

New tasks to capture and restore user state (USMT) on Windows targets, independently of deployments

Depending on the operating systems in your environment, two pairs of tasks are available. Captured data is stored on a network share. The tasks can be customized to include additional file extensions and content to be captured and restored on the target system.

❗ **Important:** To use the features available in release 3.9 or later, you must upgrade your Bare Metal OS Deployment Server to version 7.1.1.20. This upgrade is also needed to run task 350 which was modified to include partition resizing.

The following features were added with OS Deployment Version 3.8

Multicast support for Reimaging and Bare Metal Deployments on Windows targets

This release adds the support for deployments using multicast communication.

- You can customize Bare Metal Profiles for multicast deployments
- You can create reimaging profiles for both captured and Setup (ISO) images for multicast deployments

All profiles that are deployed using multicast communication must be pre-cached on the Bare Metal OS Deployment servers.

Driver management enhancements

New Check Drivers Tab in the Driver Library

You can select an image and computer model, or all images and all computer models in your environment and check if all the needed device drivers are available before you begin deployment. Based on the resulting table, you can import the missing drivers selectively and bind them to the computer models and images that you plan to deploy.

Non_PCI drivers can be bound to WinPE engines

You can now bind non-PCI drivers to WinPE engines from the Bindings tab.

Windows Bare Metal Deployment final action

After a Bare Metal deployment, you can specify a final action that will be completed on the target computer.

Assigning the Primary and Secondary Relay to targets Bare Metal Profiles

When you create a Bare Metal Profile for Windows images, you can choose to assign the Primary and Secondary relays for the targets to the Bare Metal Server and to the BigFix server respectively.

New Operating System support:

VMware

This release adds the support of VMware ESXi 6 for Bare Metal deployments.

Windows 10 support for capturing, imaging, and Bare Metal deployments (Version 3.8.1)

OS Deployment 3.8.1 adds the support of Windows 10 and related tools (WADK 10 and MDT 2013 Update 1). To deploy Windows 10, you must create an MDT Bundle using the new tools.

The following features were added with OS Deployment Version 3.7

Extended Linux support (SUSE) for targets

This release adds the support of the following Linux operating systems:

- SUSE Linux Enterprise Server (SLES) Version 12
- SUSE Linux Enterprise Desktop (SLED) Version 12

For Reimaging (install mode only) and Bare Metal deployments.

Support of VMware

This release adds the support of VMware ESXi 5 and later for Bare Metal Deployments.

Device Driver Management Enhancements

The Windows Driver Library dashboard was enhanced with several new features:

- Increased efficiency when importing driver packages provided by hardware vendors.
- During driver import, you can associate the imported drivers to one or more computer models that are known in your network.
- You can assign labels to imported drivers so that they can be easily retrieved within the driver library, and managed as a single unit.
- You can edit existing drivers by adding or removing associated models and labels.
- Support of non-PCI drivers with the possibility to import them and manually associate them to a Windows image (WIM).
- Improved usability:
    - New and enhanced driver import wizard
    - New dashboard layouts
    - New search capabilities

Serviceability Improvements for Bare Metal Deployments

From the Deployment Activity Dashboard you can

- Upload the Bare Metal deployment logs from the Bare Metal Server to the BigFix server for Linux and Windows deployments
- For Windows, LiteTouch and Windows deployment logs are uploaded from the target to the Bare Metal Server at the end of the deployment for both successful and failed deployments.
- You can view the deployment activity end time in the activity details
- During the reimage of a Windows target you can enable real time logging of the LiteTouch phase on a user-defined network share for debugging purposes
- BigFix client installation during a Bare Metal Deployment is completed through the network instead of from stored setup files in the MDT Bundle.

The following features were added with OS Deployment Version 3.6

Bare Metal target management from the BigFix console

This version introduces the Management Extender for Bare Metal Targets Plug-in that discovers and registers Bare Metal targets to theBigFix server 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.

The following features were added with OS Deployment Version 3.5

Linux Enterprise Support for image creation from installation media (ISO), reimaging 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 reimaging and Bare Metal deployments. You can reimage 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 reimaging capabilities for Windows platforms. You can now perform reimaging 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 reimaging

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, reimage, 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 BigFix 9.1 Platform)

The BigFix 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 reimaging 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 reimaging and bare metal deployments

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

You can capture, reimage, 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, reimage 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 reimage, capture, and bare metal deployment tasks
- Image Library dashboard expanded to support reimage task and bare metal profile creation
- Enhanced templating features
- Ability to edit `CustomSettings.ini` directly from the **Deploy Image to Computer** wizard.

System requirements

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

BigFix prerequisites:

- OS Deployment runs on BigFix versions 9.5, 10.0, and 11.0.

OS Deployment supports a subset of the operating systems supported by BigFix. For a complete list of supported operating systems for BigFix components, see System requirements. When new Operating System versions and updates are supported by BigFix components, OS Deployment begins testing on them. This means that operating system support in OS Deployment is not always concurrent to the support announced for BigFix Platform components.

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

Windows:

- Microsoft™ Windows™ 11 (x64) Education, Pro, and Enterprise editions up to version 25H2
- Microsoft™ Windows™ 10 (x86, x64) Education, Pro, and Enterprise editions up to version 22H2
- Microsoft™ Windows™ 8.1 (x86, x64)
- Microsoft™ Windows™ 8 (x86, x64)
- Microsoft™ Windows™ 7 (x86, x64)
- Microsoft™ Windows™ Server 2016/2019/2022/2025 (x64)[1], Essentials[2], Standard, and Data Center editions
- Microsoft™ Windows™ Server 2016/2019 (x64) with Hyper-V role[1]
- Microsoft™ Windows™ Server 2012 (x64)
- Microsoft™ Windows™ Server 2012 R2 (x64)
- Microsoft™ Windows™ Server 2012 (x64) with Hyper-V role
- Microsoft™ Windows™ Server 2012 R2 (x64) with Hyper-V role
- Microsoft™ Hyper-V Server 2012 (x64)
- Microsoft™ Hyper-V Server 2012 R2 (x64)
- Microsoft™ Windows™ Server 2008 R2 (x64)
- Microsoft™ Windows™ Server 2008 (x86, x64)

For 64-bit (x64) architectures, these operating systems are supported for both BIOS and UEFI firmware. For 32-bit (x86) architectures, only BIOS is supported.

Note:

1. Reimaging to Windows Server 2016/2019/2022/2025 requires that the BigFix client version 9.5.3 or later is installed on the source operating system before you start the reimage process.
2. Essentials edition is not available in Windows Server 2022 and later.
3. Reimaging to Windows Server 2025 requires that the BigFix client version 11.0.3 or later is installed on the source operating system before starting the reimage process.

For further information about the tool versions required for Windows deployments, see Installing Windows Bundle Creators *(on page 68)*.

You can capture, reimage, and complete Bare Metal deployments on UEFI targets with the Secure Boot firmware option enabled. You can also create deployment media for these targets. Depending on the deployment scenario, check the specific requirements in the relevant topics.

The prerequisites for the BigFix client computer on which you build the Windows Bundle are described in Installing Windows Bundle Creators *(on page 68)*. You can install all prerequisites using the **Bundle and Media Manager** dashboard.

Linux:

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

- RedHat Enterprise Linux (RHEL) Version 6 up to update 10 (x86, x64)
- RedHat Enterprise Linux (RHEL) Version 7 up to update 9 (x64)
- RedHat Enterprise Linux (RHEL) Version 8 up to update 10 (x64)
- RedHat Enterprise Linux (RHEL) Version 9 up to update 5 (x64)
- CentOS Linux Version 7 up to update 8 (x64)
- CentOS Linux Version 8 up to update 1 (x64)
- SUSE Linux Enterprise Server (SLES) Version 11[2] up to SP 4 (x86, x64)
- SUSE Linux Enterprise Server (SLES) Version 12 (x64) up to SP5
- SUSE Linux Enterprise Desktop (SLED) Version 12 (x64) up to SP4
- SUSE Linux Enterprise (SLE) Version 15 up to SP6[1]
- Linux Ubuntu 16.04 Desktop [3]
- Linux Ubuntu 18.04 Desktop [3]
- Linux Ubuntu 20.04 Desktop [3]
- Linux Ubuntu 22.04 Desktop [3]
- Linux Ubuntu 24.04 Desktop [3]

For x64 architectures, these operating systems are supported for both BIOS and UEFI firmware. For x86 architectures, only BIOS is supported.

Note:

1. SLE15 is supported only for Server (SLES15) and Desktop (SLED15) products.
2. Capture of SLES/SLED Version 11 systems is not supported.
3. Linux Ubuntu is supported only for capture and bare metal deployments of captured images (XFS and ZFS file systems are not supported). All other provisioning scenarios are not supported. To deploy Ubuntu Desktop, you must first create and upload a corresponding OS Resource.

VMware:

The following OS versions are supported for bare metal provisioning on targets:

- VMware ESXi 5.x, up to 5.5 Update 3
- VMware ESXi 6.0 up to Update 3
- VMware ESXi 6.5 up to Update 3
- VMware ESXi 6.7

Note: This platform is supported on BIOS firmware only.

Bare Metal OS Deployment Server requirements

BigFix Bare Metal Server, Image Provider, and Management Extender for Bare Metal Targets component can be installed on BigFix relays with the following Windows operating systems:

- Windows™ Server 2008 (x86, x64)
- Windows™ Server 2008 R2 (x64)[1]
- Windows™ Server 2012 (x64)
- Windows™ Server 2012 R2 (x64)
- Windows™ Server 2016/2019/2022/2025 (x64), Essentials, Standard, and Data Center editions[2]
- Windows™ 7 (x86, x64)
- Windows™ 8 (x86, x64)
- Windows™ 8.1 (x86, x64)
- Microsoft™ Windows™ 10 (x86, x64) Education, Pro, and Enterprise editions
- Microsoft™ Windows™ 11 (x64) Education, Pro, and Enterprise editions

Note:

1. Service Pack 1 is required.
2. You must install it on a BigFix relay version 9.5.4 or later. Essentials edition is not available in Windows Server 2022.

Non-Master Operators requirements

Permission requirements for non-master operators working on BigFix OS Deployment.

Non Master Operators must be allowed to use the REST API (set the **Can use REST API** permission to *Yes*) to import/ delete images, drivers, OS resources, Windows Bundle, and handle driver binding grids.

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 BigFix OS Deployment uses an accompanying tool, the Windows™ Bundle Creator, to produce a bundle of tools and resources that are called the Windows Bundle to provide system preparation, image capture, driver insertion, and image deployment services. In the deprecated solution, the tool MDT Bundle Creator uses the Microsoft™ Deployment Toolkit (MDT) to produce a bundle called MDT Bundle that provides the same tasks.

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 BigFix 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 Windows Bundle with the Windows 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.
    - import images from the Image library dashboard
6. If you are provisioning Linux systems:

    - create images from installation media, or capture images using the corresponding task and import them into the Image Library.
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 a BigFix relay in your network.
2. Create bare metal profiles for Windows, Linux, and VMware ESXi deployments and upload them to the OS Deployment server
3. Deploy the bare metal profiles to targets.

For more information, see Bare Metal deployments *(on page 184)*.

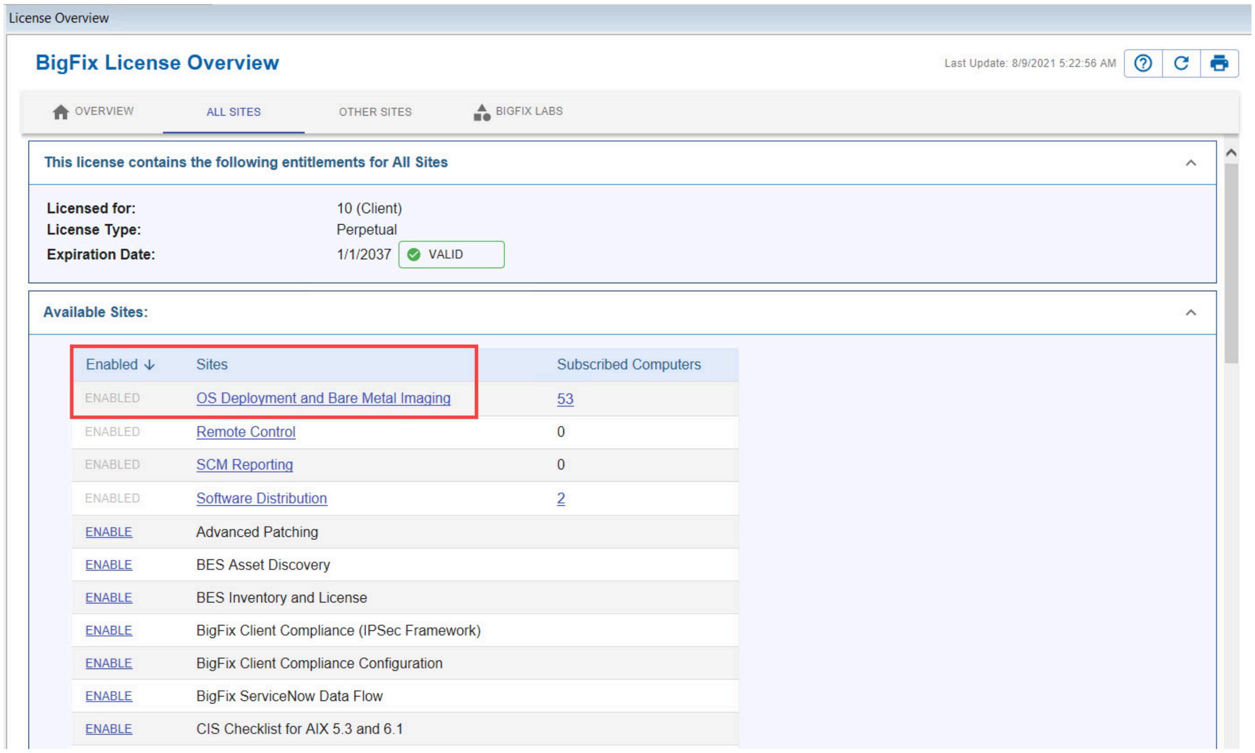
If you want to manage Bare Metal targets from the BigFix Console, you must install the Management Extender for Bare Metal Targets component on the Bare Metal OS Deployment servers that manage these targets. For information about installing this component, see Deploying the Management Extender for Bare Metal Targets *(on page 58)*.

Enable OS Deployment and Bare Metal Imaging site

To start working with BigFix 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 **ALL SITES** at the top of the console window or **All Sites** in the License overview tile and then 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.



BigFix License Overview

Last Update: 8/9/2021 5:22:56 AM

This license contains the following entitlements for All Sites

Licensed for: 10 (Client)
License Type: Perpetual
Expiration Date: 1/1/2037 ✓ VALID

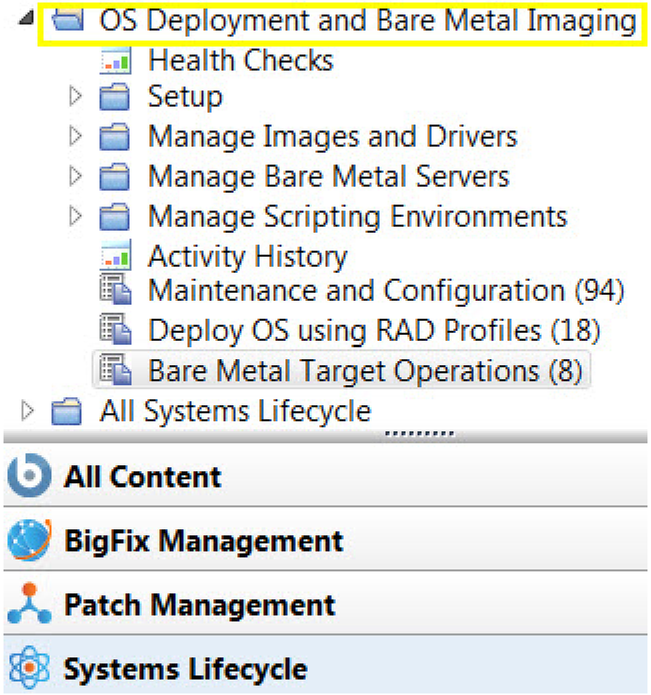
Available Sites:

Enabled ↓	Sites	Subscribed Computers
ENABLED	OS Deployment and Bare Metal Imaging	53
ENABLED	Remote Control	0
ENABLED	SCM Reporting	0
ENABLED	Software Distribution	2
ENABLE	Advanced Patching	
ENABLE	BES Asset Discovery	
ENABLE	BES Inventory and License	
ENABLE	BigFix Client Compliance (IPSec Framework)	
ENABLE	BigFix Client Compliance Configuration	
ENABLE	BigFix ServiceNow Data Flow	
ENABLE	CIS Checklist for AIX 5.3 and 6.1	

Navigation tree overview

This topic gives you an overview of using the Navigation tree.

The OS Deployment and Bare Metal Imaging navigation tree, which is accessed from the BigFix 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 BigFix console and click the *Systems Lifecycle* domain at the bottom of the domain panel.


OS Deployment and Bare Metal Imaging
Health Checks
Setup
Manage Images and Drivers
Manage Bare Metal Servers
Manage Scripting Environments
Activity History
Maintenance and Configuration (94)
Deploy OS using RAD Profiles (18)
Bare Metal Target Operations (8)
All Systems Lifecycle
All Content
BigFix Management
Patch Management
Systems Lifecycle

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

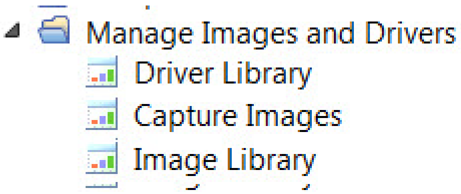
The OS Deployment Health Checks Dashboard provides troubleshooting and optimization checks for OS Deployment. You can drill down into individual health checks to see their results and a resolution path for failing checks. See Health Checks Dashboard *(on page 63)*.

Setup

From this node you perform the installation and configuration steps needed to successfully prepare and upload Windows 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 Configuring the OS Deployment Environment *(on page 39)* and Managing Windows Bundles and Deployment Media for Windows targets *(on page 67)*.

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 Managing Images *(on page 111)*.



.

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 BigFix Bare Metal Server 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 Windows 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 BigFix relay, see Managing Bare Metal OS Deployment Servers *(on page 41)*.

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.

Maintenance and Configuration Tasks

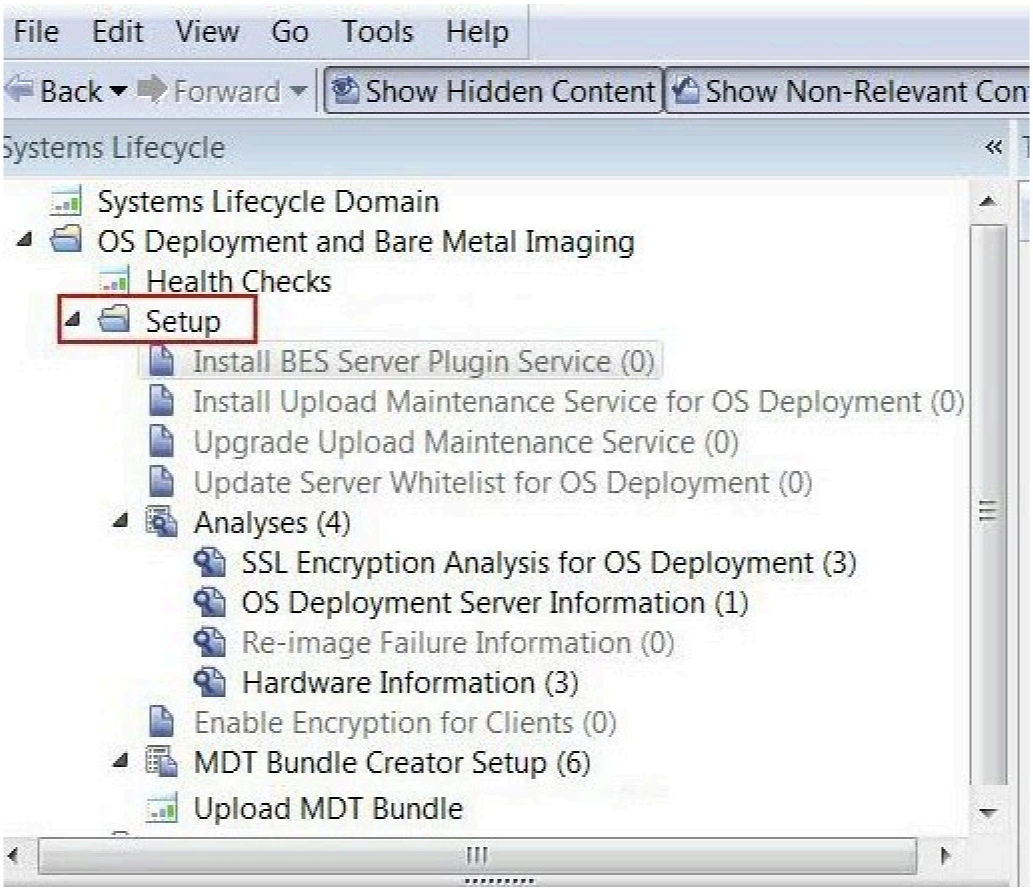
This menu contains Fixlets and tasks that are needed for maintenance of your OS Deployment environment. See Maintenance and troubleshooting *(on page 241)*.

Bare Metal Target Operations

This menu contains tasks and Fixlets to manage Bare Metal targets in your environment. See Managing Bare Metal Targets *(on page 233)*.

Chapter 2. Configuring the OS Deployment Environment

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



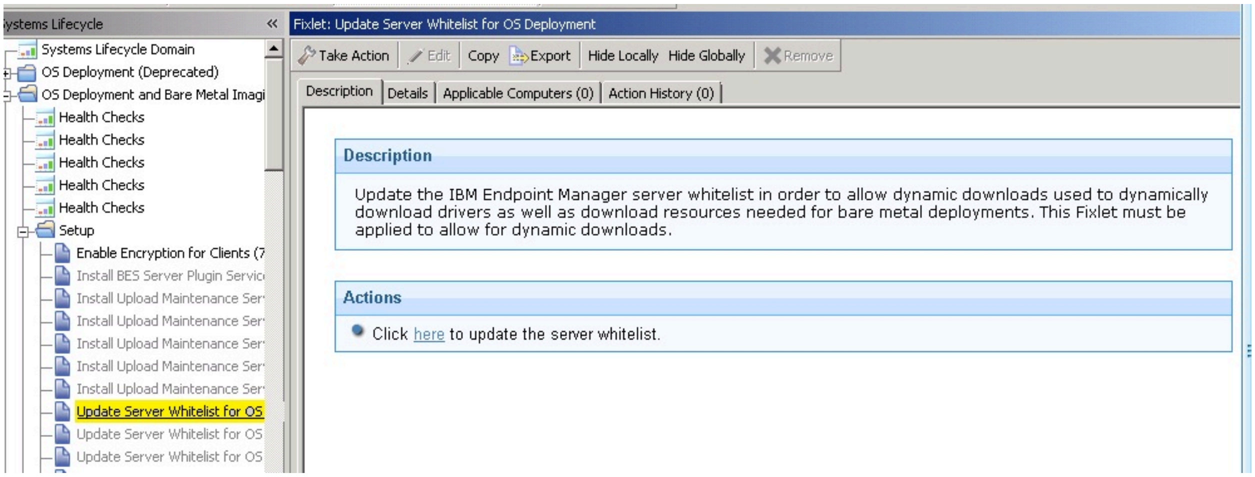
ystems Lifecycle

Systems Lifecycle Domain
OS Deployment and Bare Metal Imaging
Health Checks
Setup
Install BES Server Plugin Service (0)
Install Upload Maintenance Service for OS Deployment (0)
Upgrade Upload Maintenance Service (0)
Update Server Whitelist for OS Deployment (0)
Analyses (4)
SSL Encryption Analysis for OS Deployment (3)
OS Deployment Server Information (1)
Re-image Failure Information (0)
Hardware Information (3)
Enable Encryption for Clients (0)
MDT Bundle Creator Setup (6)
Upload MDT Bundle

The following topics describe the tasks needed to set up your OS Deployment environment.

Update Server Whitelist for OS Deployment

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


ystems Lifecycle
Systems Lifecycle Domain
OS Deployment (Deprecated)
OS Deployment and Bare Metal Imagi
Health Checks
Health Checks
Health Checks
Health Checks
Health Checks
Setup
Enable Encryption for Clients (7
Install BES Server Plugin Servic
Install Upload Maintenance Ser
Install Upload Maintenance Ser
Install Upload Maintenance Ser
Install Upload Maintenance Ser
Install Upload Maintenance Ser
Update Server Whitelist for OS
Update Server Whitelist for OS
Update Server Whitelist for OS
Fixlet: Update Server Whitelist for OS Deployment
Take Action
Edit
Copy
Export
Hide Locally
Hide Globally
Remove
Description
Details
Applicable Computers (0)
Action History (0)

Description

Update the IBM Endpoint Manager server whitelist in order to allow dynamic downloads used to dynamically download drivers as well as download resources needed for bare metal deployments. This Fixlet must be applied to allow for dynamic downloads.

Actions

- Click here to update the server whitelist.

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 reimaging Linux systems in your environment and it can be installed on Windows computers only.

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. You must send at least one Linux bare metal profile to the Bare Metal OS Deployment server for the image provider to be active.

If your targets are connected directly to an BigFix server, you must install this component on the server.

Before you deploy Linux systems, you must update the BigFix 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.

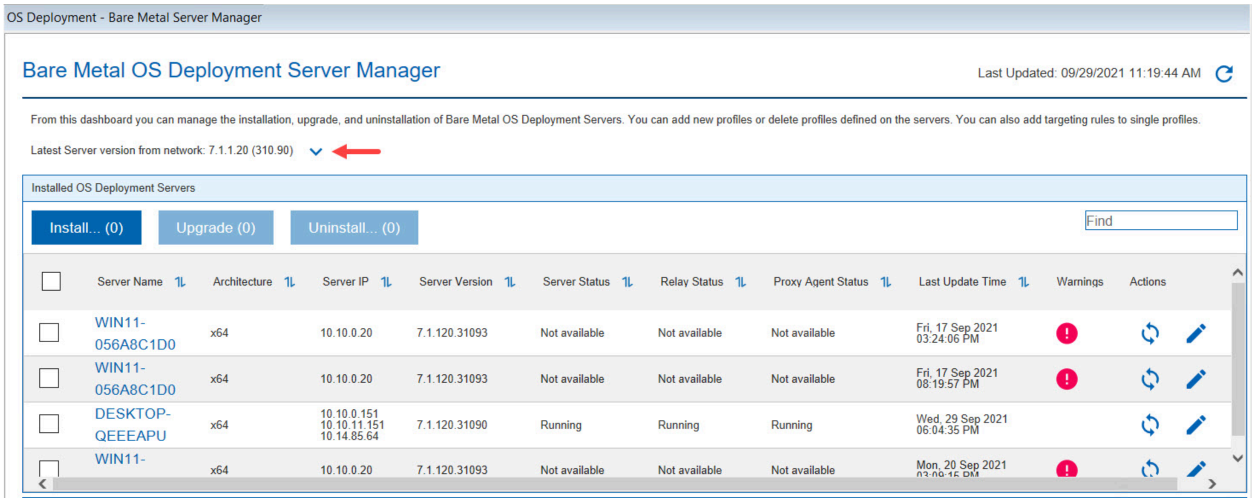
Uninstalling the Linux Image Provider

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

Managing Bare Metal OS Deployment Servers

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

The list of all Bare Metal OS Deployment servers that are subscribed to the site is displayed in the dashboard. You can install the latest OS Deployment server directly from the network in a single step, or you can upload an older installer in the Upload section by clicking the dropdown button. If at least one installer is already present, the Upload section is always displayed.



Bare Metal OS Deployment Server Manager

Last Updated: 09/29/2021 11:19:44 AM

From this dashboard you can manage the installation, upgrade, and uninstallation of Bare Metal OS Deployment Servers. You can add new profiles or delete profiles defined on the servers. You can also add targeting rules to single profiles.

Latest Server version from network: 7.1.1.20 (310.90)

Installed OS Deployment Servers

□	Server Name	Architecture	Server IP	Server Version	Server Status	Relay Status	Proxy Agent Status	Last Update Time	Warnings	Actions
□	WIN11-056A8C1D0	x64	10.10.0.20	7.1.120.31093	Not available	Not available	Not available	Fri, 17 Sep 2021 03:24:06 PM	!	↻ ✎
□	WIN11-056A8C1D0	x64	10.10.0.20	7.1.120.31093	Not available	Not available	Not available	Fri, 17 Sep 2021 08:19:57 PM	!	↻ ✎
□	DESKTOP-QEEEAPU	x64	10.10.0.151 10.10.11.151 10.14.85.64	7.1.120.31090	Running	Running	Running	Wed, 29 Sep 2021 06:04:35 PM		↻ ✎
□	WIN11-	x64	10.10.0.20	7.1.120.31093	Not available	Not available	Not available	Mon, 20 Sep 2021	!	↻ ✎

The latest version of the OS Deployment server installer available from the network is displayed at the top left corner of the page. Run the installation by clicking **Install** and select one or more available relays. Ensure that the relays you select are subscribed to the OS Deployment and Bare Metal Imaging site. Network installers are available for BigFix 9.2 or later.

If you want to install or upgrade your OS Deployment Servers from the network but you already have an installer of an earlier release that you uploaded from Fix Central, you must first delete the existing installer because uploaded installers have precedence over network installations.

If you are upgrading from a previous release, select one or more Bare Metal OS Deployment servers, and click **Upgrade**.

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 OS Deployment Server.
- Authentication must be disabled for the relay on the Bare Metal Server computer.
- If you are upgrading your Bare Metal Server from version 7.1.1.20.311.12 or lower to a version newer than 7.1.1.20.311.12, this upgrade includes an improvement on password security and you will be required to provide the login password to set on your Bare Metal Server. You can also reuse the current password.
- If you are installing your Bare Metal Server on Windows 2012 R2, you need to update your operating system with KB2919355 before you start the installation.

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.

The Bare Metal Server installation task downloads and installs Microsoft SQL Server Express 2017 or Microsoft SQL Server 2022 Express (depends on the OS version) on the selected relay, if a database is not already installed.

On 64-bit architectures, you can install a Bare Metal Server on a relay that already has an installed database, and use the existing installation. The following databases are supported:

- DB2 Enterprise 9.1 FP4a, 9.5 FP3b, 9.7, and 10.1
- Microsoft SQL Server 2005 SP2 and 2008 R2
- Microsoft SQL Server 2012
- Microsoft SQL Server 2014
- Microsoft SQL Server 2017 Express Edition
- Microsoft SQL Server 2019 Express Edition
- Microsoft SQL Server 2022 Express Edition

Before you install the Bare Metal OS Deployment server, complete the following steps on the existing database installation:

1. Create a database with a name of your choice.
2. Run this step only if you have one of the Microsoft SQL Server versions listed above.

   Add the necessary roles to the user named NT AUTHORITY\SYSTEM for the database you created in the previous step. For example, using Management studio: **Security > Logins > NT AUTHORITY\SYSTEM > User Mapping**, then select the database to add the following roles:
   - db_datawriter
   - db_datareader
   - db_ddladmin
   - public
3. Create a Data Source named AutoDeploy using 64-bit ODBC drivers for your database.
4. Verify that the ODBC connection can be established correctly to the database you created in the first step.
5. Proceed with the installation of the Bare Metal Server.

Important:

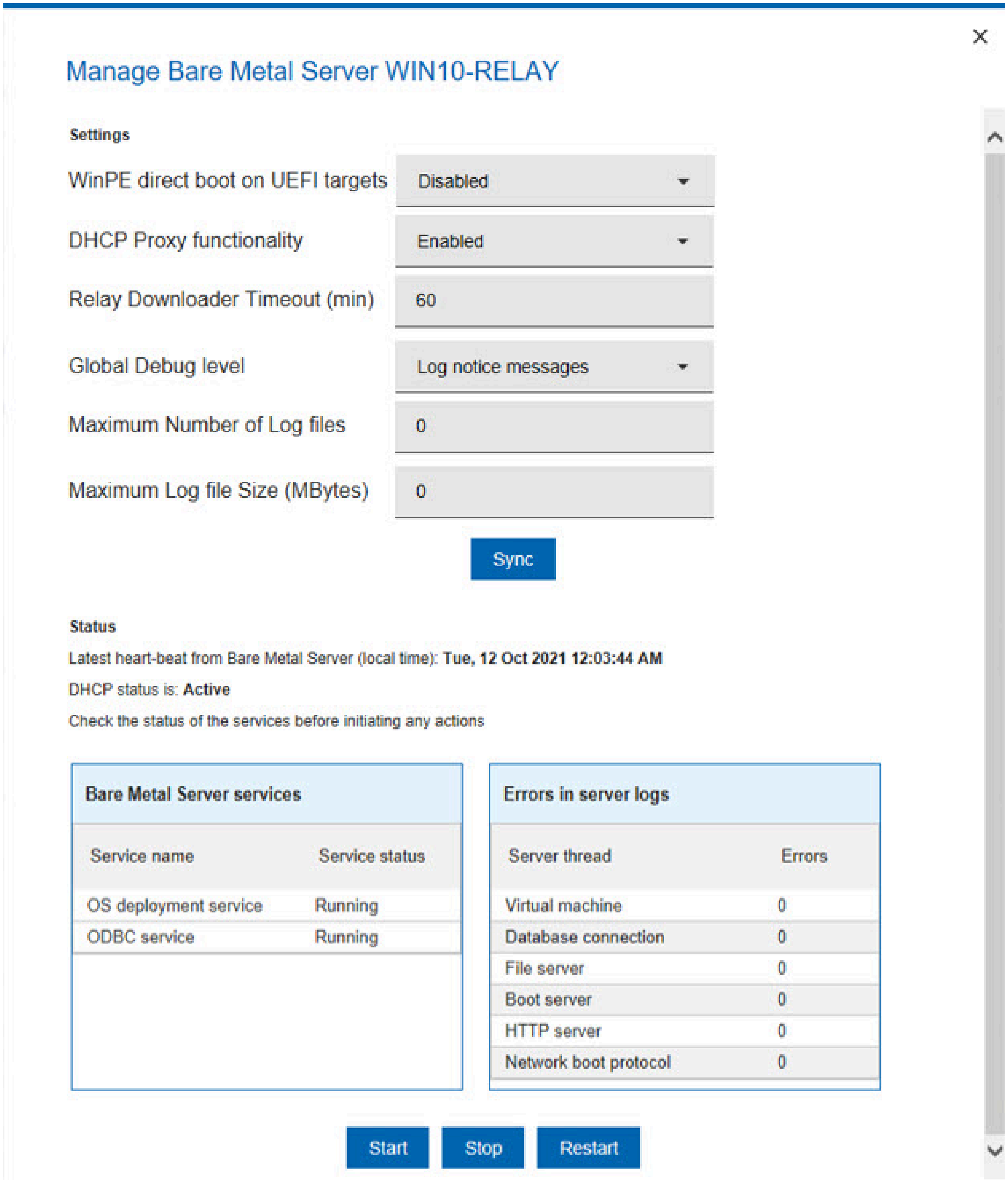
- The installation task ignores the user provided Data Location if data from a previous installation is present and the data directory is set to the existent one. If you want a different folder, get a clean environment by running Task 134.
- If you are installing a Bare Metal Server on a Windows 2008 R2 relay, ensure that it is at Service Pack 1 (SP1) level, or the installation will not complete successfully.
- After you install OS Deployment servers from the Bare Metal Server manager dashboard, you must create and manage profiles and bare metal deployments from the BigFix Console only, using the BigFix infrastructure. You cannot manage the server or any deployment objects on it from Tivoli Provisioning Manager for OS Deployment interfaces.
- If you are installing the Bare Metal Server from a BigFix console running on Windows 2012 R2, the version of Adobe embedded in this operating system may cause bare metal server synchronization problems. To avoid this issue, before you install the Bare Metal Server, ensure that you have installed all the latest Microsoft patch updates.
- Some functions of the dashboard might be 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 Windows Bundle, importing or modifying drivers, an action is automatically generated to update the servers.
- The BigFix Web Interface Extension service is set as disabled among Windows services. Do not change this setting, as this service must not be running. However, its process is automatically started when needed.

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

Two types of synchronization are possible. The Delta sync is available only if some Bare Metal Server resources (like profiles, deployment engines, drivers, etc.) are out of sync. With Delta sync, you can synchronize only the out of sync resources. However, if you want to force the synchronization of all your Bare Metal Server resources, you can launch a Full sync. The Full sync is always possible on a Bare Metal Server. Launch the Full sync if the Delta sync is failing or if you want to reset all your Bare Metal Server resources because the server is not working correctly.

The **Bare Metal Profiles** section of the dashboard lists the available profiles on the Bare Metal Server. Depending on the options specified in the profile, the **cached** column displays whether the image associated to the selected profile is cached on the relay, or, if multicast was enabled, it displays whether the selected profile files are permanently cached on the Bare Metal Server. A green check mark indicates that files were successfully cached. For profiles with multicast enabled, a red warning with an "x" indicates that you must initiate a synchronization action on the Bare Metal Server. A yellow border triangle warning 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 or to modify specific settings on an installed Bare Metal Server, select the server from the list and click ✏.



Manage Bare Metal Server WIN10-RELAY

Settings

WinPE direct boot on UEFI targets	Disabled
DHCP Proxy functionality	Enabled
Relay Downloader Timeout (min)	60
Global Debug level	Log notice messages
Maximum Number of Log files	0
Maximum Log file Size (MBytes)	0

Status

Latest heart-beat from Bare Metal Server (local time): **Tue, 12 Oct 2021 12:03:44 AM**

DHCP status is: **Active**

Check the status of the services before initiating any actions

Bare Metal Server services

Service name	Service status
OS deployment service	Running
ODBC service	Running

Errors in server logs

Server thread	Errors
Virtual machine	0
Database connection	0
File server	0
Boot server	0
HTTP server	0
Network boot protocol	0

You can start, stop or restart the Bare Metal Server, and view if any errors were logged. The information displayed in this window is retrieved by Analysis 50. If the analysis fails to retrieve the current Bare Metal server settings, a warning message is displayed on the dashboard. To troubleshoot the problem, see Troubleshooting problems in retrieving Bare Metal Server Settings (Analysis 50 or Task 361) *(on page 245)*. You can change any settings even if the retrieval of the current settings was not successful.

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.trc` file. You can change this value in the **Relay Downloader Timeout** field. Specify the maximum time (in minutes) 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.

From the edit pane you can also change or enable the following settings:

Global Debug Level

You can select the level of detail for the messages that are logged on the Server log files. Choose on e of the following levels:

- 0: No output
- 1: Log errors only
- 2: Log errors and warnings
- 3: Log significant information (default)
- 4: Log notice messages
- 5: Log debugging messages
- 6: Log every possible detail

Note: Level 5 and Level 6 produce very large amounts of debugging information which might overload the Server. Use these levels with caution.

Maximum number of log files

Specify the maximum number of log files that will be kept on the server. The default value is zero (0) which means that this parameter is not set.

Maximum Log File size (in Megabytes)

Specify the maximum size of the log files generated by the Bare Metal Server. The default value is zero (0), which means that circular logging is not enabled and any value specified for the number of log files is ignored. In this case, a single log file with no limit in size is created. If the value you specify is greater than zero, circular logging is enabled and a minimum of two log files are created and used, even if the log file number is set to zero. For example, if you specify 3 log files with a maximum size of 50 Megabytes, a first log file is created. When the first file reaches the specified limit, a second file is created, and again, a third. when all three files have reached the maximum size of 50 megabytes, the first one is overwritten.

WinPE Direct Boot on Windows UEFI targets

You can boot WinPE directly on UEFI targets that PXE boot during Windows bare metal deployments. This allows computers with the Secure Boot firmware option enabled to run bare metal deployments. By default, the direct boot feature is disabled on the Bare Metal Servers. Select **enabled** to allow Direct Boot of WinPE on Windows UEFI targets during bare metal deployments.

Note: In a WinPE Direct Boot enabled bare metal server, the needed drivers must be explicitly bound in the deployment engine binding matrix ("Current Manual Binding" column) in the Driver Bindings.

You can also change the Bare Metal Server settings by running Fixlet 361 on one or more Bare Metal Servers. Complete the form in the task and click **Take Action**.

Customizing cipher suites and protocols for TLS connections

According to OpenSSL syntax, the TLS 1.2 and TLS 1.3 protocols are enabled with cipher suites set `DEFAULT:!DH:!RC4:!EXP:!RC4-MD5:!RC4-SHA:-RSA:-SHA` by default in an encryption negotiation process for SSL connections. For more information, visit https://www.openssl.org/docs/man3.1/man1/openssl-ciphers.html.

You can customize the cipher suites and protocols by using environment variables `RBO_CIPHERS`, `RBO_EXCLUDE_PROTOCOLS`, and `RBO_FIPS_MODE`.

- Set the environment variable `RBO_CIPHERS` to select or exclude one or more cipher suites that the Bare Metal Server uses. For a complete list of allowed values and other information, see the supported syntax at above link.

  For example, to exclude `DES` and `3DES`, set `RBO_CIPHERS=DEFAULT:!DES:!3DES`.
- Set the environment variable `RBO_EXCLUDE_PROTOCOLS` to exclude/enable protocols from the Bare Metal Server availability. The allowed values for RBO_EXCLUDE_PROTOCOLS are: TLSv1.0, TLSv1.1, TLSv1.2, and TLSv1.3. The only allowed separator is ":". SSLv2 and SSLv3 cannot be enabled.

  For example:
    - To allow only TLSv1.3 protocol, set `RBO_EXCLUDE_PROTOCOLS=TLSv1.0:TLSv1.1:TLSv1.2`.
    - To enable all TLS protocols (that is TLS 1.0, TLS 1.1, TLS 1.2, and TLS 1.3), set `RBO_EXCLUDE_PROTOCOLS=NONE`.
- From Bare Metal Server 7.1.120.31128, its possible to enable FIPS enforcement for TLS connections by defining the environment variable `RBO_FIPS_MODE=true`

Bare Metal Server database connection in a TLS 1.2 environment

For the 64-bit bare metal server running on SQL Express 2014 to work in a TLS 1.2 environment, enable the connection to the database by performing these steps:

1. Open the local policy settings. Run `secpol.msc` from an administrator command prompt.
2. Click **Local Policies > Security Options > System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing > Enabled > OK**.
3. Run the `gpupdate /Force` command from an administrator command prompt.
4. Restart the computer for the changes to take effect.

Note: This is not required, if the 64-bit bare metal server is running on SQL Express 2017 or later.

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.

Bare Metal Server Web Interface

The Bare Metal Server features a web interface that you can access through a browser using the server's IP address or hostname. This interface is intended for the OSD team's troubleshooting purposes and is not recommended for regular use. Firefox is the recommended browser for this interface. This is due to a bug in Chromium-based browsers (like Edge, Chrome, and so on) that can occur when using self-signed certificates, which may require the page to be refreshed multiple times to view certain HTML pages correctly.

Bare Metal Server SSL Certificates

Bare Metal Server for the SSL communication uses a self-signed certificate that is automatically generated by default at the first start of its process.

If you want to replace this default certificate with a custom one or delete the current certificate, do the following steps:

1. Stop BigFix Bare Metal Server service.
2. Open a command line shell and change the directory to the BigFix Bare Metal Server binaries directory. For example: C:\Program Files\BigFix OSD.
3. Run the following commands:
    - To import a new certificate and its private key:

      ```
      rembo.exe -d -v 4 -cert “<certificate filename with fullpath>” “<private key filename with
       fullpath>” <private key passphrase> -exit
      ```

      where the certificate is a `.crt` file and its private key is a `.key` file, the following string represents a certificate and private key:

Certificate

```
-----BEGIN CERTIFICATE-----
<<base64 string>>
-----END CERTIFICATE-----
```

Private key

```
-----BEGIN PRIVATE KEY-----
<<base64 string>>
-----END PRIVATE KEY-----
```

- To delete the current certificate and its private key, either the previously imported custom certificate or the default self-signed certificate:

```
rembo.exe -d -v 4 -delcerts
```

4. Restart BigFix Bare Metal Server service.

Note: If the Bare Metal Server has no certificate at its start, it generates a new self-signed certificate.

Antivirus Exclusions

If an antivirus or a live scan software is running on the Bare Metal Server computer then to avoid concurrency and conflict in file access, it's recommended to add to the exclusion list of this software to the following folders:

- executable folder : `C:\Program Files\BigFix OSD`.
- data folder (which by default is) : `C:\BFOSD Files`. But note that this path can be customized at installation time.

Ports used by the Bare Metal OS Deployment Server

To ensure correct communication, check the ports used for the different deployment scenarios.

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 for OS Deployment tasks and media creation

The following ports are used each time a computer connects to a Bare Metal Server. typical scenarios are:

Bare Metal deployments
Media creation
Reimaging deployments using multicast communication.

Reimaging in unicast mode does not require the Bare Metal Server component.

Bare Metal Server:

- *NBP* : port 4012 *UDP*
- *FILE*: port 4013 *UDP & TCP*
- *MCAST*: ports 10000-10500 *UDP*
- *HTTP*: port 8080 *TCP* (used for upgraded Bare Metal Servers from an earlier installation)
- *HTTP*: port 8081 *TCP* (used for new Bare Metal Server installations)
- *HTTP*: port 8088 *TCP* - Image Provider component used during Linux deployments
- Database gateway: port 2020 *TCP*
- *HTTP*: port 52311 *TCP* - Relay Downloader

Important:

- For new Bare Metal Server installations, the default HTTP port is 8081. The default HTTP port 8080 is maintained only for servers that are upgraded from earlier versions.
- The MCAST ports are not needed for unicast (default) deployments.

Bare Metal and reimaging targets:

- *NBP* : port 4014 *UDP*
- *MCAST* : port 450 *UDP*
- *MCAST* : port 451 *UDP*
- *MCAST* : port 9999 *UDP*

Ports for BigFix Bare Metal Server Web UI access (legacy)

Bare Metal Server:

- *HTTP*: port 8080 *TCP* (for Servers that are upgraded from older installations)
- *HTTP*: port 8081 *TCP* (used for new Bare Metal Server installations)
- *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 the characteristics of 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 BigFix Bare Metal Server can require changes to your DHCP configuration. These changes can typically be performed automatically by the BigFix Bare Metal Server installer. However, in some cases, you might want to perform the changes manually, or to verify them.

Important: If your DHCP Server is configured to use option 210 `pxelinux.pathprefix()`, this option causes the PXE boot to fail on bare metal targets. This option must not be configured for bare metal deployments.

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

- The DHCP server and the BigFix Bare Metal Server *are not* running on the same host
- The DHCP server and the BigFix Bare Metal 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 BigFix Bare Metal Server 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 and 60 for the hosts on which you want to run BigFix Bare Metal Server and follow the instructions given in this section (if you are running on the BigFix Bare Metal Server same host as the DHCP server, you need to set option 60 again).
- There are also cases where you must set both DHCP options 43 and 60, including when you have two different OS Deployment Servers in your environment.

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 more details about these options, see:

- Setting DHCP Option 43 *(on page 52)*
- Setting DHCP Option 60 *(on page 56)*
- Setting DHCP Option 66 and 67 *(on page 57)*

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 Setting DHCP Option 60 *(on page 56)*.

Setting DHCP Option 43

Option 43 (Class identifier) allows you to inform the target that the location of the PXE server is known.

Option 43 is a binary buffer, containing a list of sub-options. Sub-options are packed in the binary buffer in no specific order. Most sub-options are optional.

An exhaustive list of sub-options can be found in the PXE specifications. Only sub-options of interest to specify the IP address of the PXE server are described here. Other configurations, like multicast discovery, multiple unicast servers, or multiple choices, are not explained in this section.

`PXE option 6: PXE_DISCOVERY_CONTROL`

This option specifies how the PXE client contacts PXE servers, using either unicast, multicast or broadcast. The format of this option is one byte.

`PXE option 8: PXE_BOOT_SERVERS`

A list of IP addresses, each address corresponding to one PXE server (when `discovery_control` is unicast). A PXE server is identified by a number (the standard value for BigFix Bare Metal Server is 15) and its IP address. The format of this option is two bytes for the server type, one byte for the number of servers to list (1 in our example), and four bytes per server address.

`PXE option 9: PXE_BOOT_MENU`

This option contains a list of choices to prompt on the screen at boot time. You need to have a PXE boot menu even if it is not used. The format of this option is two bytes for the server type, one byte for the length of the string to display, and the string to display on screen. The total length of this option is 5 bytes.

`PXE option 10 (0A): PXE_BOOT_TIMEOUT`

This option is required to specify how long (in seconds) the boot menu is displayed, and the text of a prompt that is displayed during waiting time. The format of this option is one byte for the timeout value, followed by the prompt text.

`PXE option 255 (FF): PXE_END`

To be valid, the binary buffer of DHCP option 43 must end with `FF`.

Setting DHCP Option 43

If your DHCP server is running on Windows, you can enter the suboption values one at a time in option 43, by selecting hexadecimal input.

If your DHCP server is ISC DHCP (version 2.x), then you can enter the suboption values as provided in the examples (bytes separated with colons) for parameter `vendor-encapsulated-options` (the exact name depends on the version you are using).

If your DHCP server is ISC DHCP (version 3.x or 4.x), then you can use the explicit syntax to describe the PXE options as follows:

```
# In the global section:
   option space PXE;
   option PXE.discovery-control code 6 = unsigned integer 8;
   option PXE.boot-server code 8 = { unsigned integer 16,
                                     unsigned integer 8,
                                     ip-address };
   option PXE.boot-menu code 9 = { unsigned integer 16,
                                   unsigned integer 8,
                                   text};
   option PXE.menu-prompt code 10 = { unsigned integer 8, text };
```

```
# In the scope/host section:
   option dhcp-parameter-request-list = concat(option dhcp-parameter-request-list,60,43);
   option vendor-class-identifier "PXEClient";
   vendor-option-space PXE;
   option PXE.discovery-control 7;
   option PXE.boot-server 15 1 <ip address of the PXE server>;
   option PXE.boot-menu 15 5 "Rembo";
   option PXE.menu-prompt 0 "Rembo";
```

Note: Where <ip address of the PXE server> is the IP address of the bare metal server where your target will connect. For example, option PXE.boot-server 15 1 10.10.10.10.

Example: Option 43 for PXE servers on different subnets

In this example, you want to have targets `A` and `B` boot on server `192.10.10.10`, and targets `C` and `D` boot on server `192.10.11.10`, which is on a different subnet (a valid gateway must be setup for `C` and `D` in order to locate the PXE server on a different subnet).

Note: Server type 15 is translated into 00:0F in hexadecimal. IP address 192.10.10.10 is translated into C0:0A:0A:0A, and 192.10.10.11 is translated into C0:0A:0B:0A. Letters R and B are translated into 52 and 42.

Here are the options that one must insert in the binary buffer and their values:

PXE option 6, length 1, value=`07`

Value `7` means `use PXE_BOOT_SERVERS list, disable multicast and broadcast discovery`

PXE option 8, length 7, value = `00:0F:01:C0:0A:0A:0A`

(targets A and B) Only one IP address is used, the address of the PXE server for the target which receives these DHCP options.

PXE option 8, length 7, value = `00:0F:01:C0:0A:0B:0A`

(targets C and D) Only one IP address is used, the address of the PXE server for the target which receives these DHCP options.

PXE option 9, length 5, value = `00:0F:02:52:42`

There is only one line, displaying `RB`, and which goes to server type 15 (BigFix Bare Metal Server).

PXE option A, length 2, value=`00:52`

The timeout is set to 0 seconds, meaning that one wants to boot using the first line of the boot menu ,and the prompt is set to `R`. Because the timeout is 0, the prompt text is not displayed, but it must be at least one character long.

PXE option FF

This closes the buffer

The format of the binary buffer is similar to what is used for the DHCP packet itself. The buffer is a list of options, each option starting with its option number (one byte), followed by its length (one byte), and its value (a list of bytes).

Here is the transcription of the above example, for targets `A` and `B`:

```
Option 43 =
06:01:07:08:07:00:0F:01:C0:0A:0A:0A:09:05:00:0F:02:52:42:0A:02:00:52:FF
```

And for targets `C` and `D`:

```
Option 43 =
06:01:07:08:07:00:0F:01:C0:0A:0B:0A:09:05:00:0F:02:52:42:0A:02:00:52:FF
```

Example: Option 43 to create a PXE boot menu

The administrator wants to display two lines in the PXE boot menu, pointing to two separate OS deployment servers. The two servers must use different PXE server type numbers or they will be seen as only one server by the PXE network card.

In addition to the standard PXE server type 15, OS deployment server accepts any number between 33008 (`80F0` in hexadecimal) and 33280 (`8200` in hexadecimal). These new PXE server type numbers are used to differentiate multiple OS deployment servers in the `BOOT_SERVERS` sub-option of DHCP option 43.

In this example, the first server has the address `192.168.1.4` (`C0:A8:01:04` in hexadecimal), and the second server, `192.168.1.5` (`C0:A8:01:05` in hexadecimal).

1. Assign an OS deployment server type to each of the servers. OS deployment servers accept server type 15, and server types from 33008 to 33280. For this example, 33008 (`80F0`) is used for the first server, and 33009 (`80F1`) for the second server.
2. The sub-options of DHCP option 43 must then be configured as follows:

   PXE option 6, length 1,value = 07

   Value `7` means `use PXE_BOOT_SERVERS list, disable multicast and broadcast discovery`

   PXE option 8, length 14 (0E), value = `80:F0:01:C0:A8:01:04:80:F1:01:C0:A8:01:05`

   Option 8 defines the two PXE servers. The first server is defined by the first 7 bytes, starting with the OS deployment server type (`80:F0`, 33008), followed by one IP address: `C0:A8:01:05` (192.168.1.4). The second server is defined in the following manner, using OS deployment server type `80:F1` (33009).

PXE option 9, length 22 (16), value = `80:F0:08:53:65:72:76:65:82:20:41:80:F1:08:53:65:72:76:65:82:20:42`

Option 9 defines the boot menu that is displayed at boot time. The first 11 bytes correspond to the first line, for the first server. It shows the string `Server A`, associated with type `80:F0` (first server). The second line shows the string `Server B`, associated with type `80:F1` (second server).

PXE option A, length 6, value =`0F:53:65:6C:65:63:74`

Option 10 (`0A`) specifies a 15 second timeout and shows the string `Select` as the boot menu prompt.

PXE option FF

To close the buffer.

The full option 43 reads as follows:

```
06:01:07:08:0E:80:F0:01:C0:A8:01:04:80:F1:01:C0:A8:01:05:
09:16:80:F0:08:53:65:72:76:65:82:20:41:80:F1:08:53:65:72:76:65:82:20:42:
0A:06:0F:53:65:6C:65:63:74:FF
```

When your boot menu is displayed on your target screen, press F8 to make your selection.

Setting DHCP Option 60

Option 60 (Class identifier) allows you to inform the target that the location of the PXE server is known.

Adding DHCP option 60 to Windows DHCP server

By default, option 60 is not set on Windows. If the OS deployment server is running on the same host as the DHCP server, you have to add this option and set its value to `PXEClient` in order to tell PXE clients where to find the OS deployment server.

Follow these steps to add option 60 on Windows:

1. Open a command window (select **Start > Run > cmd**)
2. Type `netsh`
3. Type `dhcp`
4. Type `server \\<servername>` or `server <ip_address>`
5. You then see a command prompt that says: `dhcp server>`
6. Type `add optiondef 60 PXEClient STRING 0 comment=option added for PXE support`
7. Type `set optionvalue 60 STRING PXEClient`
8. To confirm that everything has been set correctly, type `show optionvalue all`

Adding DHCP option 60 to a host with ISC DHCP server

If you are using the ISC DHCP server 2.0, you can add the DHCP option 60 to a group of targets or to a single target by adding the statement `option dhcp-class-identifier "PXEClient";` to a section of the configuration file. If you were using option 43 (vendor-encapsulated-options) for another PXE application, remove it for BigFix for OS Deployment targets.

The modifications to perform on a ISC DHCP server 3.0 are the same as for a 2.0 server, but the names differ:

- Add `vendor-class-identifier "PXEClient";` for the targets running BigFix for OS Deployment
- Remove any occurrences of `option space PXE;` if you were running another PXE application.

Note: The OS deployment server responds to all requests, including requests originating from unknown targets.

Note: If the flag **Completely ignore unknown targets** is set for the server, it only responds to discovery requests originating from known targets. You can specify either the IP address or the Ethernet address in the target list. At this stage, the IP address of the remote-boot target is known.

Setting DHCP Option 66 and 67

You must set option 66, Boot Server Host Name, and 67, Boot File Name, for each specific UEFI target that cannot process option 43.

Adding DHCP option 66 and 67 to Windows DHCP server

To set options 66 and 67 it is necessary to reserve an IP address for the target. Select a free IP address from the range assigned by your DHCP server. This address is referenced in the following procedure as the target IP address. Keep a record of the MAC address of the target machine network card. It is referenced in the following procedure as the target MAC address.

Follow these steps to add option 66 and 67 on Windows:

1. Open a command window (select **Start > Run > cmd**)
2. Type `netsh`
3. Type `dhcp`
4. Type `server \\<servername>` or `server <server_ip_address>`
5. You see a command prompt that says: `<dhcp server>`
6. Type `scope <scopename>`
7. You see a command prompt that says: `<dhcp server scope>`
8. Type `add reservedip <target_ip_address> <target_mac_address>`
9. Type `set reservedoptionvalue <target_ip_address> 66 STRING <boot_server_ip_address>`
10. Type `set reservedoptionvalue <target_ip_address> 67 STRING Rembo-x64UEFI`
11. To confirm that everything was set correctly, type `show reservedoptionvalue <target_ip_address>`

Adding DHCP option 66 and 67 to a host with ISC DHCP server

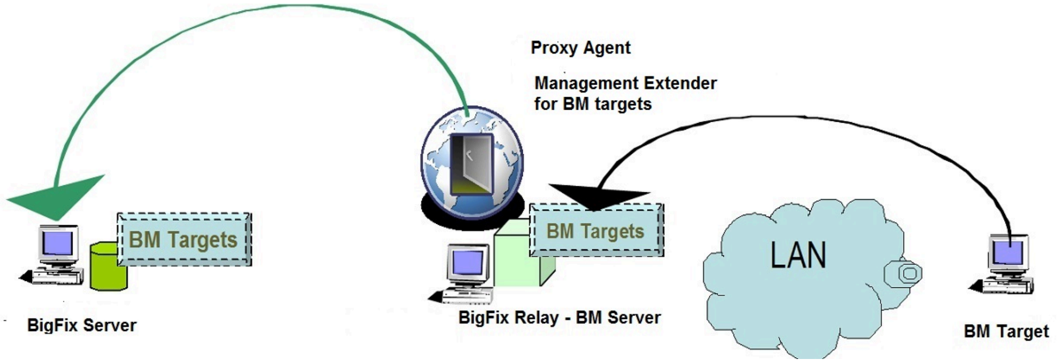
If you are using the ISC DHCP server, you can add the DHCP option 66 and 67 to a group of UEFI targets or to a single UEFI target by adding, respectively, the statement `options tftp-server-name <server_ip_address>` and option `bootfile-name "Rembo-x64UEFI"` to a section of the configuration file.

Deploying the Management Extender for Bare Metal Targets

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

With this component, you can manage targets that do not have the BigFix 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 BigFix server database, and you can manage them through the BigFix 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 BigFix infrastructure. This means that any target that did not connect to the bare metal Server within this time frame is not reported to the BigFix server, and is not visible from the Console. You can change this threshold to suit your needs. See Configuring the plug-in behavior in the BareMetalExtender.ini file *(on page 59)*.

The available target information is refreshed every 10 minutes. You can modify the refresh interval by editing the `settings.json` file. See Changing the plug-in settings *(on page 59)*.

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:

1. From the BES Support site, search and run Fixlet **Install BigFix Proxy Agent (Version 10.0.x)** or **Install IBM BigFix Proxy Agent (Version 9.x.x)**, depending on your relay 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)

If your relay is BigFix version 8.2 or 9.0, see Deprecated and Superseded functionalities *(on page 259)*

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 233)*.

Configuring the plug-in behavior in the BareMetalExtender.ini file

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

The `LastReportTimeThreshold` parameter defines the time window that is taken into account to determine if the bare metal target that completed a PXE boot is still active. The default is set to 48 hours. You can configure this threshold to suit your specific needs and environment.

To change the reporting threshold for the bare metal targets, switch to `C:\Program Files\BigFix OSD`. Edit the `BareMetalExtender.ini`, and modify the value of the corresponding parameter:

```
LastReportTimeThreshold=48
```

Changing the plug-in settings

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

You can decide the logging detail by modifying the configuration options. 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
```

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\\BigFix OSD\\BareMetalExtender.log\\\" -t \\\"C:\\Program Files\\BigFix
 OSD\\BareMetalExtender.trc\\\" -m 10:5",
```

The target information is retrieved and refreshed on the server every 10 minutes. If you want to modify the default refresh interval for retrieving this information from 10 to 15 minutes, overwrite the default value, as shown in the following example:

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

The `DeviceReportExpirationIntervalHours` parameter defines the expiration period after which a bare metal target is considered inactive and can be erased. After this period has expired, the plug-in will stop tracking information for the target. The default value for this interval is 168 hours. You can modify the expiration period by locating the corresponding string:

```
"DeviceReportExpirationIntervalHours": 168,
```

After this interval has elapsed, the entry for the target in the Subscribed Computers can be erased. For information about deleting bare metal target entries, see Deleting bare metal target entries *(on page 234)*.

After you make changes to the settings in this file, the Proxy Agent service must be restarted for the modifications to 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** Task (ID 151).
2. Remove the Proxy Agent from the BES Support site, run the task **TROUBLESHOOTING: Uninstall BigFix Proxy Agent** (ID 1795)

   If your relay is BigFix version 8.2 or 9.0, see Deprecated and Superseded functionalities *(on page 259)*

Troubleshooting

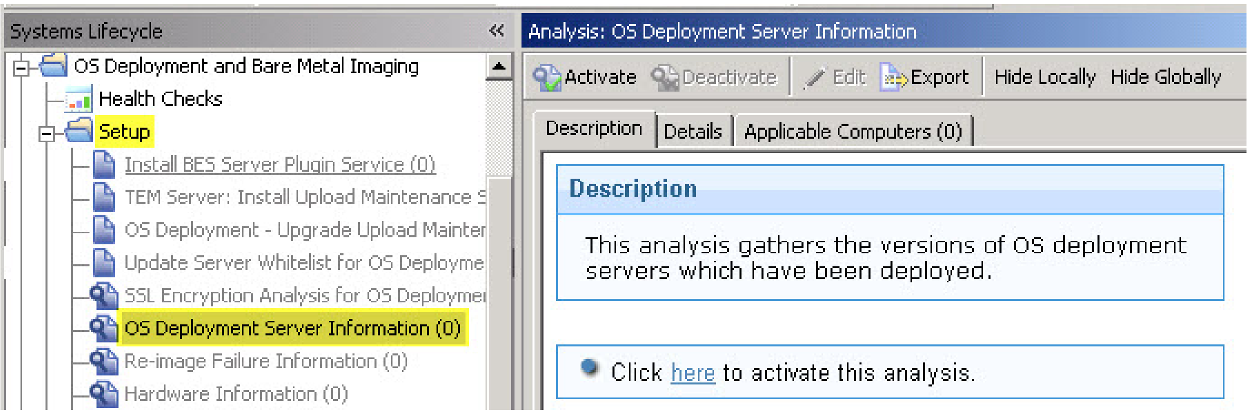
Logs for troubleshooting are on each Bare Metal Server in `%ProgramFiles%\BigFix OSD\BareMetalExtender.trc`. The default logging level is 3. You can change circular logging options in the `settings.json` file. See Changing the plug-in settings *(on page 59)*.

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.

OS Deployment Server Information

The OS Deployment Server Information is used to gather the versions of OS deployment servers that have been deployed and also retrieves information about the status and settings.


Systems Lifecycle
OS Deployment and Bare Metal Imaging
Health Checks
Setup
Install BES Server Plugin Service (0)
TEM Server: Install Upload Maintenance S
OS Deployment - Upgrade Upload Mainter
Update Server Whitelist for OS Deployme
SSL Encryption Analysis for OS Deploymer
OS Deployment Server Information (0)
Re-image Failure Information (0)
Hardware Information (0)
Analysis: OS Deployment Server Information
Activate
Deactivate
Edit
Export
Hide Locally
Hide Globally
Description
Details
Applicable Computers (0)

Description

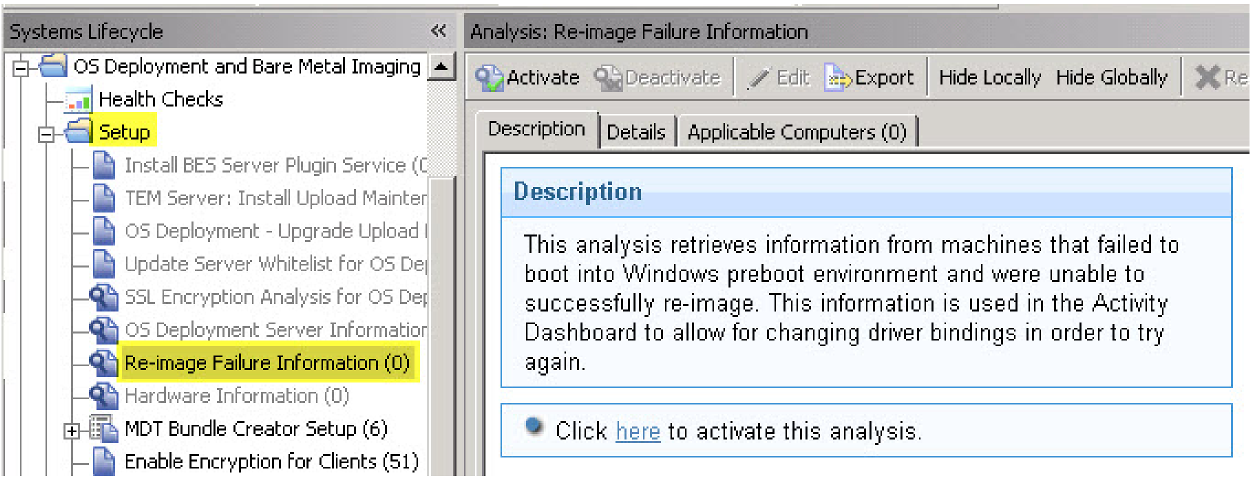
This analysis gathers the versions of OS deployment servers which have been deployed.

Click here to activate this analysis.

Click the link in the Actions box to activate this analysis. To install an OS Deployment server and to view or change information about installed servers, see Managing Bare Metal OS Deployment Servers *(on page 41)*.

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.


Systems Lifecycle
OS Deployment and Bare Metal Imaging
Health Checks
Setup
Install BES Server Plugin Service (C
TEM Server: Install Upload Mainter
OS Deployment - Upgrade Upload I
Update Server Whitelist for OS Dep
SSL Encryption Analysis for OS Dep
OS Deployment Server Informatior
Re-image Failure Information (0)
Hardware Information (0)
MDT Bundle Creator Setup (6)
Enable Encryption for Clients (51)
Analysis: Re-image Failure Information
Activate
Deactivate
Edit
Export
Hide Locally
Hide Globally
Re
Description
Details
Applicable Computers (0)

Description

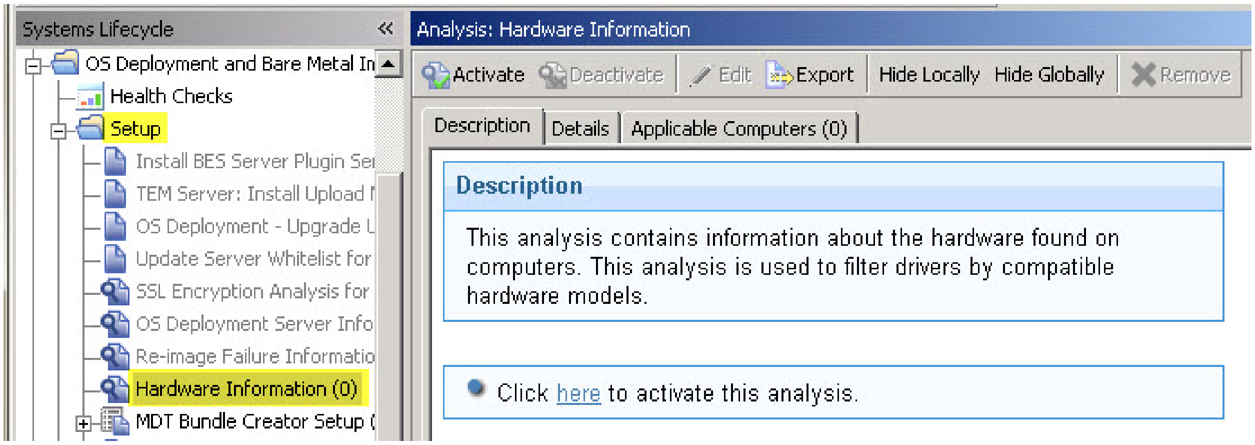
This analysis retrieves information from machines that failed to boot into Windows preboot environment and were unable to successfully re-image. This information is used in the Activity Dashboard to allow for changing driver bindings in order to try again.

Click here to activate this analysis.

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.


Systems Lifecycle
OS Deployment and Bare Metal In
Health Checks
Setup
Install BES Server Plugin Se
TEM Server: Install Upload
OS Deployment - Upgrade L
Update Server Whitelist for
SSL Encryption Analysis for
OS Deployment Server Info
Re-image Failure Informatio
Hardware Information (0)
MDT Bundle Creator Setup (
Analysis: Hardware Information
Activate
Deactivate
Edit
Export
Hide Locally
Hide Globally
Remove
Description
Details
Applicable Computers (0)

Description

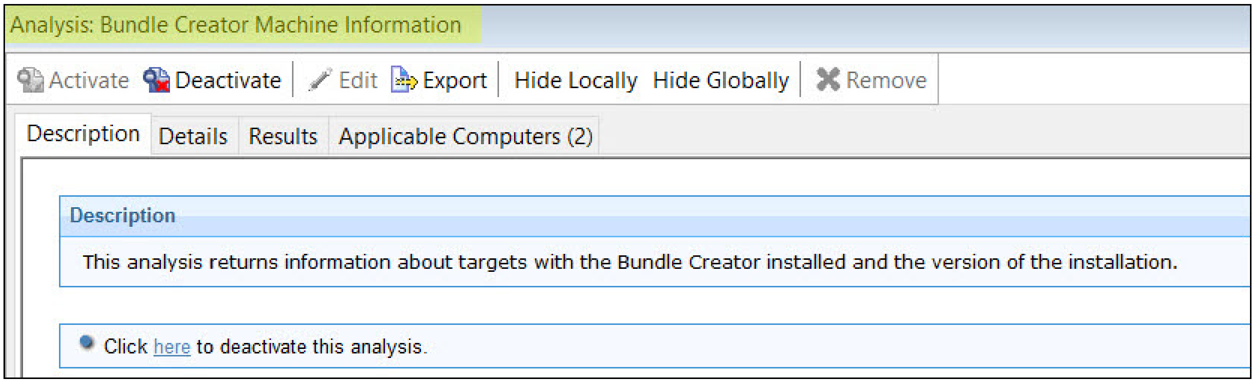
This analysis contains information about the hardware found on computers. This analysis is used to filter drivers by compatible hardware models.

Click here to activate this analysis.

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.



Description

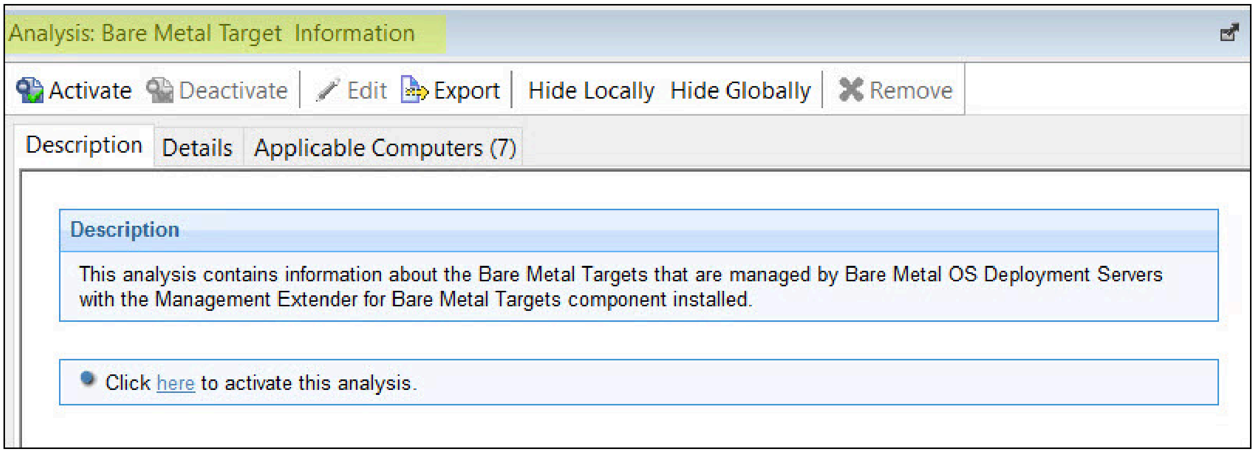
This analysis returns information about targets with the Bundle Creator installed and the version of the installation.

Click here to deactivate this analysis.

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.



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

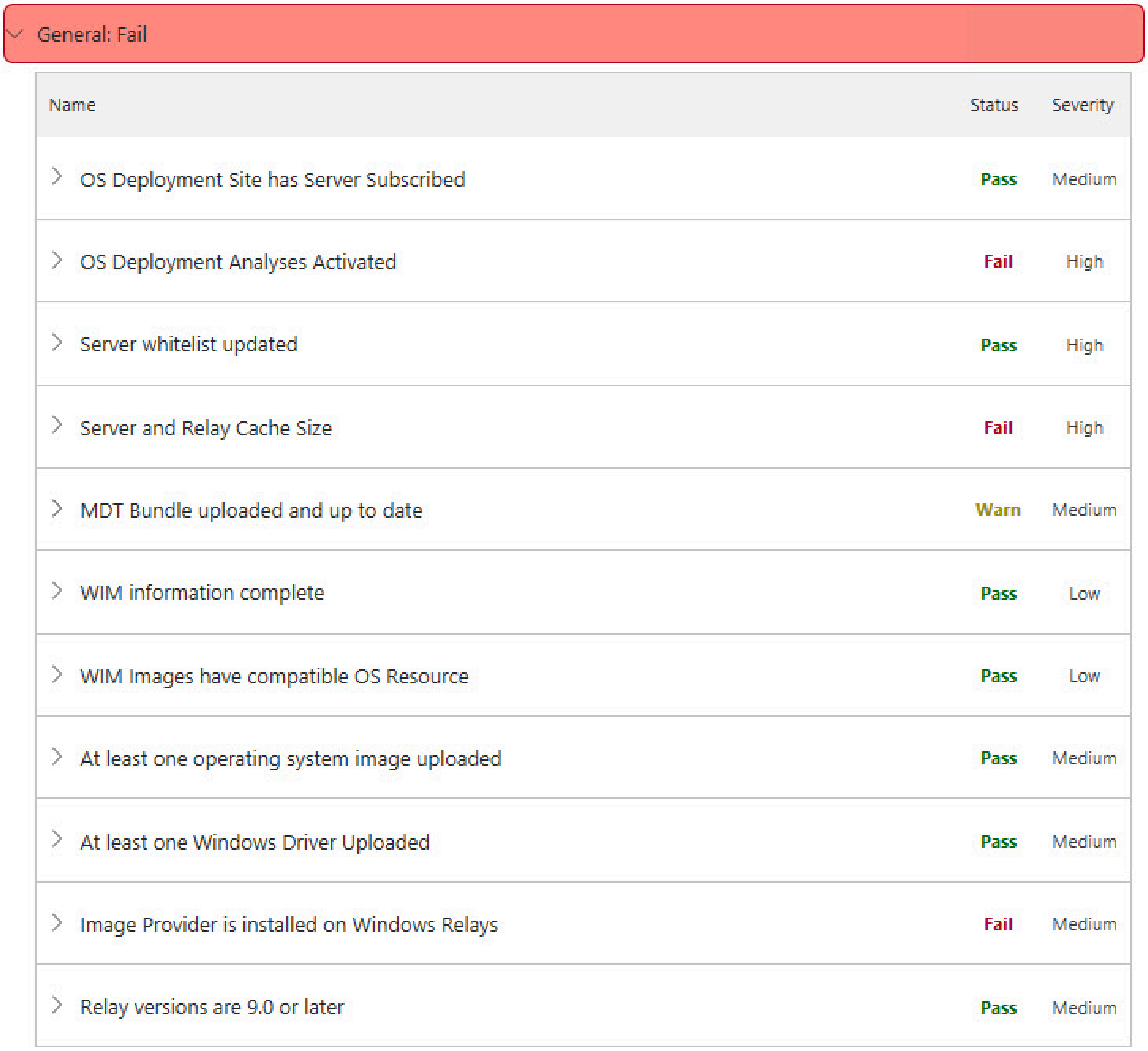
- Click here to activate this analysis.

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.

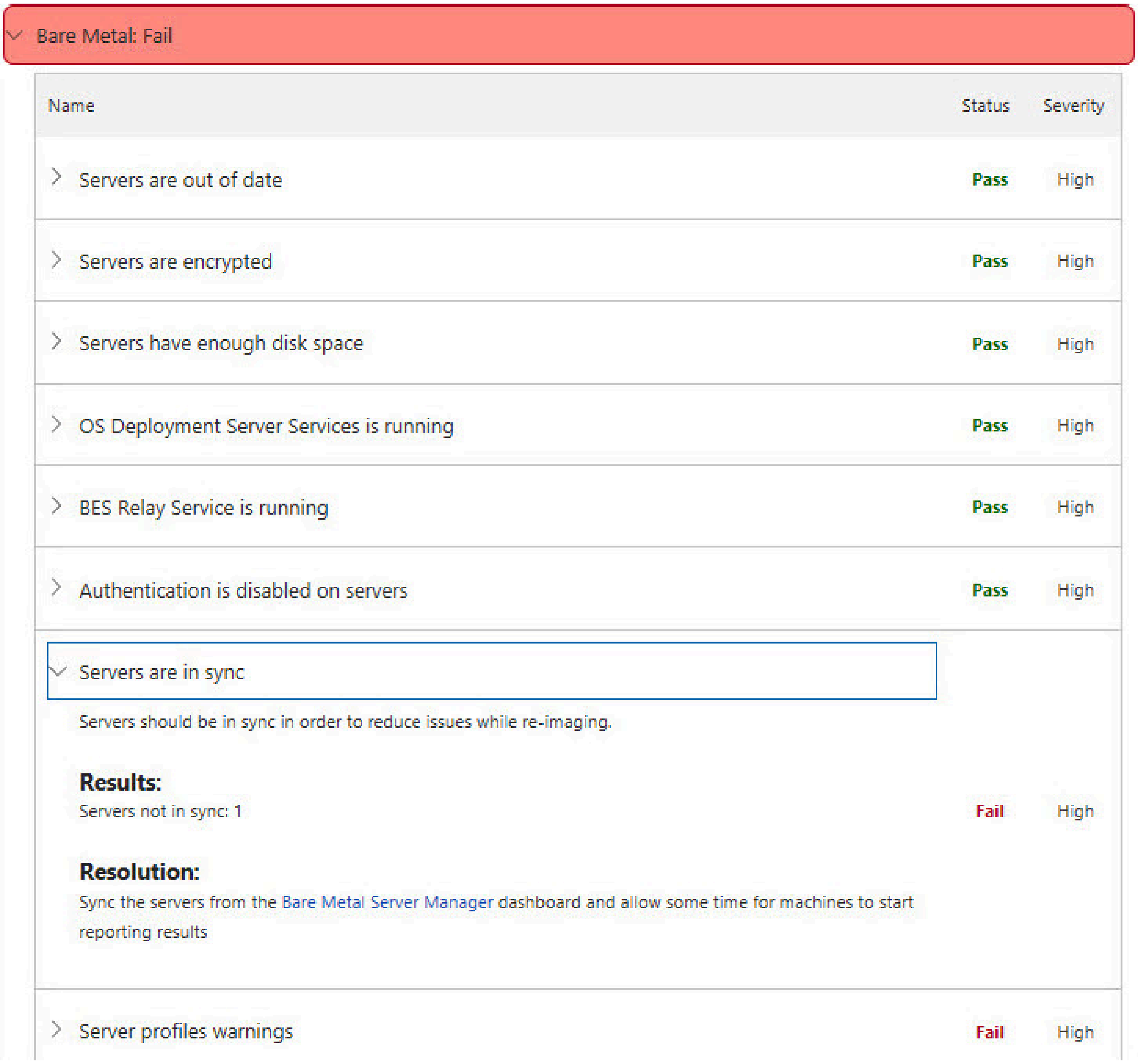
Use the Health Checks - General dashboard to see the current health status of the BigFix infrastructure.



General: Fail

Name	Status	Severity
OS Deployment Site has Server Subscribed	Pass	Medium
OS Deployment Analyses Activated	Fail	High
Server whitelist updated	Pass	High
Server and Relay Cache Size	Fail	High
MDT Bundle uploaded and up to date	Warn	Medium
WIM information complete	Pass	Low
WIM Images have compatible OS Resource	Pass	Low
At least one operating system image uploaded	Pass	Medium
At least one Windows Driver Uploaded	Pass	Medium
Image Provider is installed on Windows Relays	Fail	Medium
Relay versions are 9.0 or later	Pass	Medium

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



Bare Metal: Fail

Name	Status	Severity
Servers are out of date	Pass	High
Servers are encrypted	Pass	High
Servers have enough disk space	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 Servers should be in sync in order to reduce issues while re-imaging. **Results:** Servers not in sync: 1 **Resolution:** Sync the servers from the Bare Metal Server Manager dashboard and allow some time for machines to start reporting results	Fail	High
Server profiles warnings	Fail	High

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.

Verifying Secure Hash Algorithm (SHA-256) readiness

BigFix 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.

From BigFix Version 9.1, all application-specific files are managed with SHA-256. All new files uploaded by the user (images, drivers, Windows Bundles etc.) and generated by the system after the installation of BigFix 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 BigFix 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 BigFix 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 BigFix.

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 BigFix 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 Windows 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 Windows Bundle Creators
- Create Windows Bundles
- Create Deployment Media

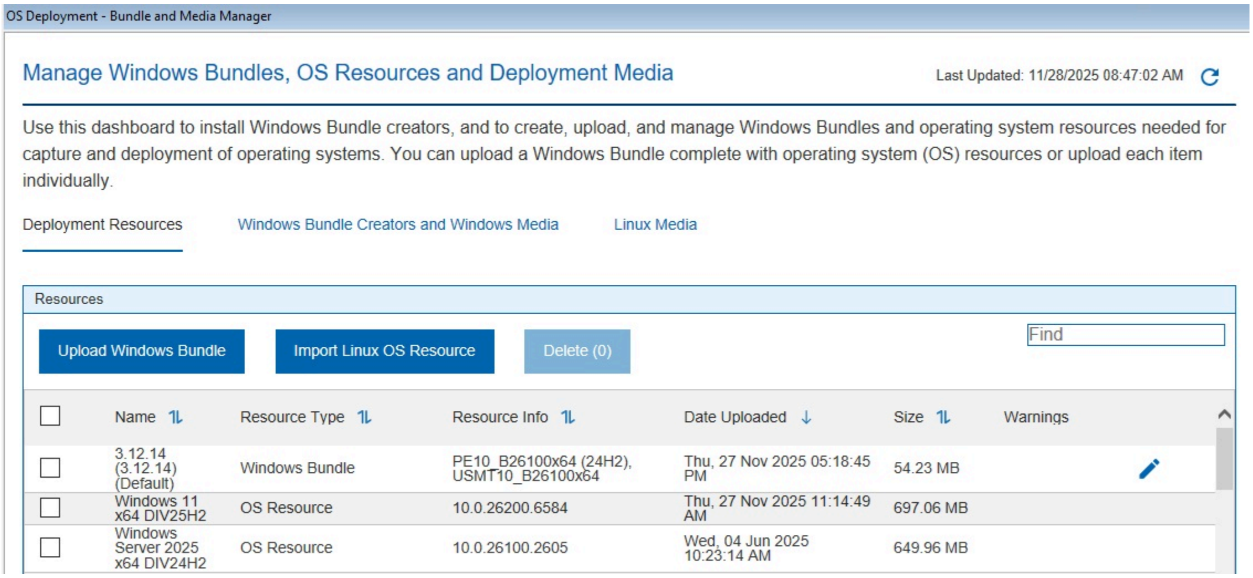
The tasks available from this dashboard provide a simplified approach to setting up your environment for Windows operating system deployments. You can download Windows Bundle Creators and their prerequisites, and create Windows Bundles in a simple, guided manner, eliminating the need to manually install 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 Windows Bundle Creators, and create Windows 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.


OS Deployment - Bundle and Media Manager
Last Updated: 11/28/2025 08:47:02 AM
Deployment Resources
Windows Bundle Creators and Windows Media
Linux Media
Resources
Upload Windows Bundle
Import Linux OS Resource
Delete (0)
Find

Manage Windows Bundles, OS Resources and Deployment Media

Use this dashboard to install Windows Bundle creators, and to create, upload, and manage Windows Bundles and operating system resources needed for capture and deployment of operating systems. You can upload a Windows Bundle complete with operating system (OS) resources or upload each item individually.

□	Name	Resource Type	Resource Info	Date Uploaded	Size	Warnings
□	3.12.14 (3.12.14) (Default)	Windows Bundle	PE10_B26100x64 (24H2), USMT10_B26100x64	Thu, 27 Nov 2025 05:18:45 PM	54.23 MB	
□	Windows 11 x64 DIV25H2	OS Resource	10.0.26200.6584	Thu, 27 Nov 2025 11:14:49 AM	697.06 MB	
□	Windows Server 2025 x64 DIV24H2	OS Resource	10.0.26100.2605	Wed, 04 Jun 2025 10:23:14 AM	649.96 MB	

From this dashboard you can:

- Install Windows Bundle Creators from the **Windows Bundle Creators and Windows Media** tab, by clicking **Install Windows Bundle Creator** . In the wizard, select the tool combination that best suits your deployment patterns. When you select the tools, the corresponding set of supported operating systems is highlighted.
- Create Windows Bundles for the operating systems you plan to deploy. An Windows Bundle is a collection of scripts, OS resource files, and folders that are required for reimage, capture, and bare metal deployments. When you create an Windows 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 Windows 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 Windows Bundle. The target on which the bundle is created must have either Windows Automated Installation Kit (WAIK) or Windows Assessment and Deployment Kit (WADK).
- Create network boot and offline deployment media from the **Create Deployment Media** wizard, 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.
- Import Linux OS Resources
- Create Linux Deployment media from the **Linux Media** tab.

For each target in the **Windows Bundle Creators and Windows Media** tab, the table displays information about the following:

- the version of the installed OS Deployment server
- which Windows Bundle Creator 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.

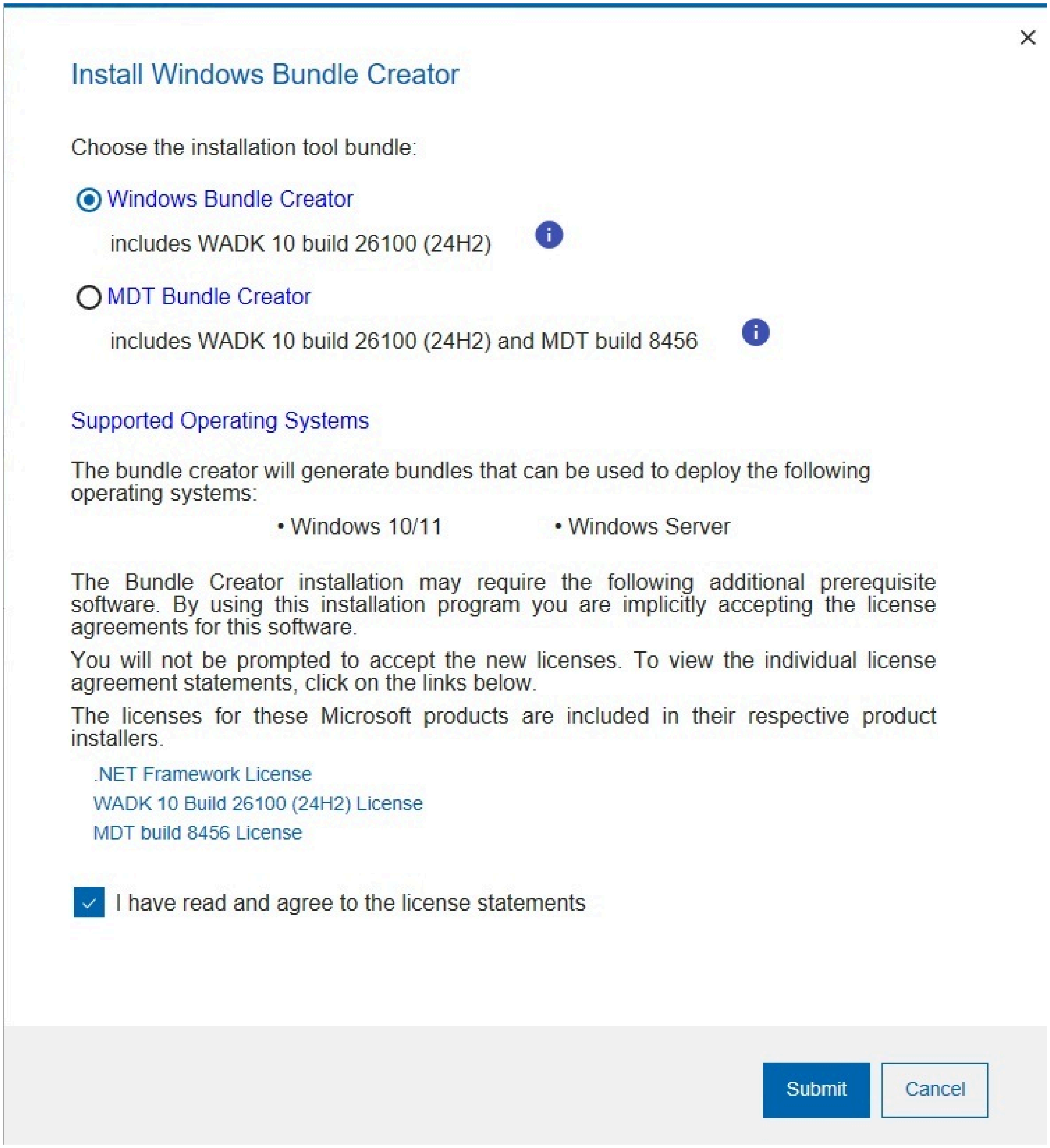
You can install the Windows Bundle Creator on a computer manually from the **Windows Bundle Creator Setup** node. If the creators you install manually are on systems that have a BigFix client installed, they are displayed in the list of available Windows Bundle Creators. You can also create Windows Bundles manually by customizing the required parameters in the `parameters.ini` file, and by launching the Windows Bundle Creator executable. For information about manual installation and configuration, see Creating and managing Windows Bundles manually *(on page 81)*.

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

Installing Windows Bundle Creators

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

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



Install Windows Bundle Creator

Choose the installation tool bundle:

● Windows Bundle Creator

includes WADK 10 build 26100 (24H2)

○ MDT Bundle Creator

includes WADK 10 build 26100 (24H2) and MDT build 8456

Supported Operating Systems

The bundle creator will generate bundles that can be used to deploy the following operating systems:

- Windows 10/11
- Windows Server

The Bundle Creator installation may require the following additional prerequisite software. By using this installation program you are implicitly accepting the license agreements for this software.

You will not be prompted to accept the new licenses. To view the individual license agreement statements, click on the links below.

The licenses for these Microsoft products are included in their respective product installers.

.NET Framework License
WADK 10 Build 26100 (24H2) License
MDT build 8456 License

☑ I have read and agree to the license statements

Here you can select the type of Bundle Creator you want to install (Windows Bundle Creator or MDT Bundle Creator), see the tools that they include, and the list of operating systems that can be deployed. MDT Bundle Creator is deprecated.

Depending on the target you select for the installation, 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.

Important:

- The computers on which you install the Windows Bundle Creators must have direct internet access for the prerequisites to be correctly downloaded and installed through the wizard.
- You don't need to create an Windows Bundle for Windows 10/11 in-place upgrades. For more information, see Installing Windows 10/11 or Windows Server using in-place upgrade *(on page 179)*.
- If you select to install the Windows Bundle Creator on a target machine that already has deprecated deployment tools, the existing tools are not replaced. To ensure that the tools you select are downloaded on the target, check it beforehand and manually remove the preexisting tools if necessary. The deprecated tool combinations are listed in Deprecated Component Combinations for MDT Bundle Creator *(on page 259)*.
- The Windows Bundle Creator computer requires 7-Zip. Install your preferred version beforehand, or the version defined in the Fixlet 40 of OSD site (Deploy 7-zip) will be installed when running the task. You can then upgrade it manually later if needed.

Windows Bundle Creators

The following table lists the valid components using the Windows Bundle Creator Tool 3.12.15 (the final version is to be updated). For each component, here is a corresponding list of operating systems that you can deploy.

Table 1. Valid component combinations for capture, reimage, and bare metal deployments

This table lists the component combination supported for capture, reimage, and bare metal deployment scenarios on Windows targets

Operating System	Windows Bundle Creator [1]	WIM Toolkit
Windows 11	3.12.15	WADK for Windows 11 24H2 (build 26100)
Windows 10	3.12.15	WADK for Windows 11 24H2 (build 26100)
Windows Server 2025	3.12.15	WADK for Windows 11 24H2 (build 26100)
Windows Server 2022	3.12.15	WADK for Windows 11 24H2 (build 26100)
Windows Server 2019	3.12.15	WADK for Windows 11 24H2 (build 26100)
Windows Server 2016	3.12.15	WADK for Windows 11 24H2 (build 26100)

Notes

1. Windows Bundle Creator 3.12.15 supersedes all earlier versions.

The following table lists the valid combinations for components using the deprecated MDT Bundle Creator Tool 3.11.141. For each combination, here is a corresponding list of operating systems that you can deploy.

Table 2. Valid component combinations for capture, reimage, and bare metal deployments

This table lists the component combination supported for capture, reimage, and bare metal deployment scenarios on Windows targets

Operating System	MDT Bundle Creator	Microsoft Deployment Toolkit	WIM Toolkit
Windows 11	3.11.14	MDT build 8456	WADK for Windows 11 24H2 (build 26100)
Windows 10[2]	3.11.14	MDT build 8456	WADK for Windows 11 24H2 (build 26100)
Windows Server 2025	3.11.14	MDT build 8456	WADK for Windows 11 24H2 (build 26100)
Windows Server 2022	3.11.14	MDT build 8456	WADK for Windows 11 24H2 (build 26100)
Windows Server 2019	3.11.14	MDT build 8456	WADK for Windows 11 24H2 (build 26100)
Windows Server 2016	3.11.14	MDT build 8456	WADK for Windows 11 24H2 (build 26100)
Windows Server 2012 R2	3.11.14	MDT build 8456	WADK for Windows 11 24H2 (build 26100)
Windows Server 2012	3.11.14	MDT build 8456	WADK for Windows 11 24H2 (build 26100)

Notes

1. For windows 10 x86, the last supported WADK is WADK 10 2004, refer to https://learn.microsoft.com/en-us/windows-hardware/get-started/adk-install.

For the list of other deprecated component combinations for MDT Bundle Creator, see Deprecated Component Combinations for MDT Bundle Creator *(on page 259)*.

For a complete list of WADK(WinPE) versions and Operating System support, refer to the Microsoft Technet website.

Note: WADK 10.1.25398.1 (September 2023) is not supported for MDT Bundle creation.

Creating and uploading Windows Bundles and OS resources

Using the wizard, you create Windows Bundles and OS resources for your Windows deployments. The bundle tool that will be created (Windows Bundle or MDT Bundle) depends on the choice that has been made when preparing the Creator machine with the "Install Windows Bundle Creator" task.

From the Windows Bundle Creators and Windows Media Tab, select a target and click **Create Windows 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 Windows Bundle and OS resources
- Create a new Windows Bundle only
- Create new OS resources only

Depending on the tool combinations installed on your target, the wizard displays the set of parameters that are available to you.

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.

OS resources are created from Windows™ installation media by the Windows Bundle Creator. The resources can be left in the output of the Windows 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 OS resource is required for each operating system, architecture, or Service Pack/Release ID combination that you plan to manage with OS Deployment. Single resources can be uploaded by specifying an individual resource folder such as `W7X86SP0` or `W10X64RID1607`.

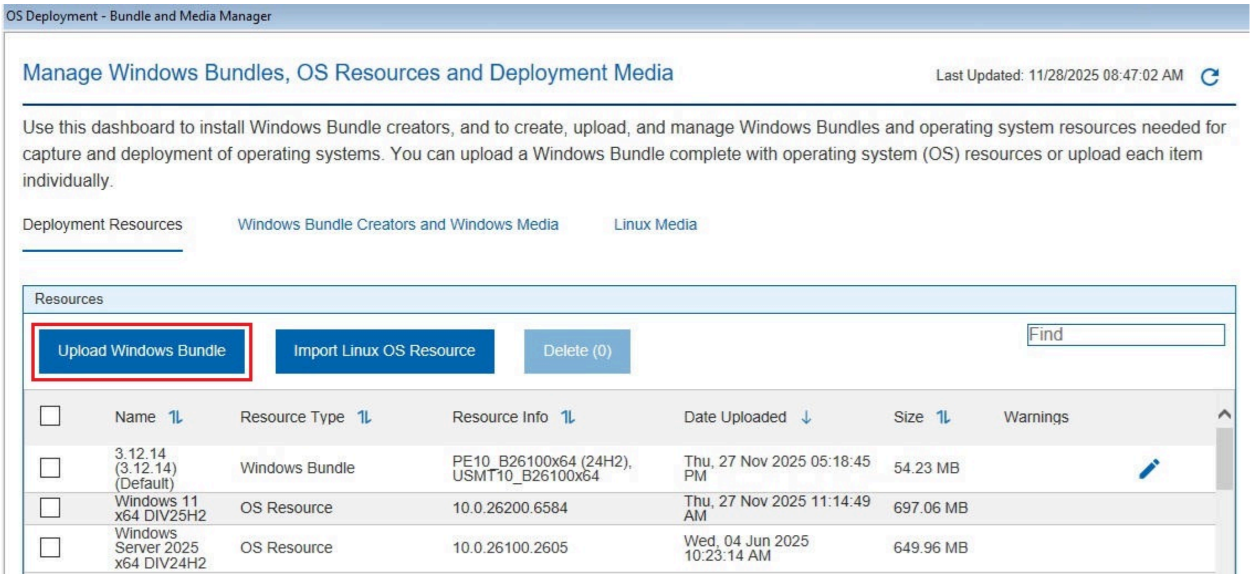
Note: Individual OS Resources must have been created in previous runs of the Windows Bundle Creator and can be found in the generated Deploy folder under `WindowsBundle\Deploy\Operating Systems`.

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

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 Windows Bundle.

When you have created your Windows Bundles, you can upload them to the BigFix Server from the **Deployment Resources** tab of the Bundle and Media Manager dashboard. Browse to the directory where your Windows Bundle is stored, and upload only the WindowsBundle\Deploy directory from this location. Click **Upload Windows Bundle** to load the directory onto the BigFix server and complete the upload process from the console.

You can upload multiple Windows Bundles. When you create or edit an Windows Bundle, you can make it your default Bundle by selecting the corresponding option.



OS Deployment - Bundle and Media Manager

Manage Windows Bundles, OS Resources and Deployment Media

Last Updated: 11/28/2025 08:47:02 AM

Use this dashboard to install Windows Bundle creators, and to create, upload, and manage Windows Bundles and operating system resources needed for capture and deployment of operating systems. You can upload a Windows Bundle complete with operating system (OS) resources or upload each item individually.

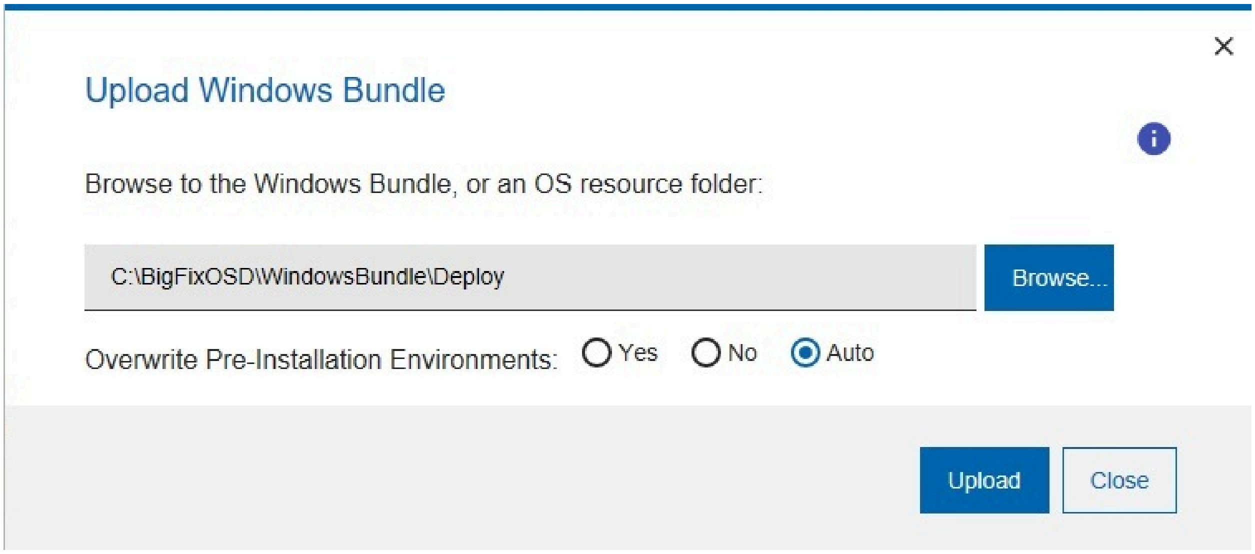
□	Name	Resource Type	Resource Info	Date Uploaded	Size	Warnings
□	3.12.14 (3.12.14) (Default)	Windows Bundle	PE10_B26100x64 (24H2), USMT10_B26100x64	Thu, 27 Nov 2025 05:18:45 PM	54.23 MB	
□	Windows 11 x64 DIV25H2	OS Resource	10.0.26200.6584	Thu, 27 Nov 2025 11:14:49 AM	697.06 MB	
□	Windows Server 2025 x64 DIV24H2	OS Resource	10.0.26100.2605	Wed, 04 Jun 2025 10:23:14 AM	649.96 MB	

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

For WinPE 10, the Release ID that uniquely identifies the current PE version loaded on the BigFix server is displayed in parentheses. This version could be different from the PE version used to create the Windows Bundle.

When you upload the Windows Bundle, you can set the **Overwrite Preinstallation Environments** option by expanding the Preferences section. 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.

When uploading an Windows Bundle with WinPE 10 of a later release ID than the one currently stored on the BigFix server, if you select to not overwrite the existing preinstallation environments, the earlier release is kept and displayed in the Resource Info column of the dashboard.



Upload Windows Bundle

Browse to the Windows Bundle, or an OS resource folder:

C:\BigFixOSD\WindowsBundle\Deploy

Overwrite Pre-Installation Environments: ○ Yes ○ No ● Auto

You can upload both a Windows Bundle and an MDT Bundle. The upload path is pre-filled with the default upload path for a Windows Bundle. If you want to upload an MDT, change the path to the correct one. The default path for MDT Bundle is `C:\BigFixOSD\MDTBundle\Content\Deploy`. If you are importing a Windows Bundle for the first time in your environment, all the bare metal server must be at version 7.1.1.20.312.02 or newer and you cannot select the option to not overwrite the existing preinstallation environments.

Important: If you want to deploy on UEFI targets with the Secure Boot firmware option enabled, your Windows Bundle must be at level 3.9.06 or later, and you must select **Yes** to overwrite preinstallation environments when you upload it.

Creating Windows Deployment Media

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

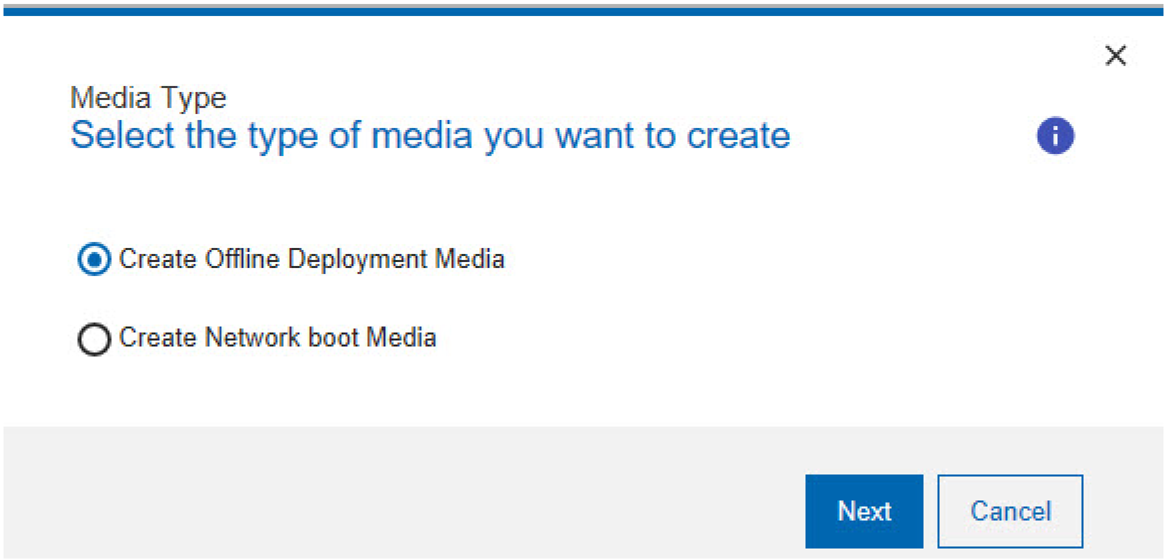
From the Windows Bundle Creators and Windows Media tab, select **Create Deployment Media** to complete one of the following tasks:

- 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 server (PXE server) to receive the binding menu.
- **WinPE and one or more bootable images (offline deployment)**: In this case, when the boot operation completes on the target, the binding menu is displayed. The user at the target can select the profile to deploy from the media.

Based on the Windows Deployment Kit installed on the selected computer, the correct version of Windows Preinstallation environment (WinPE) is downloaded from the specified Bare Metal OS deployment server and included in the media.



Media Type

Select the type of media you want to create

● Create Offline Deployment Media

○ Create Network boot Media

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

During the media creation process, files are stored in a temporary folder on the selected Bare Metal OS deployment server. By default, the temporary folder is created in the system `TEMP` folder. When the process completes, the folder is erased. To specify a different path for the temporary folder, complete the following steps before you create the media:

1. From the subscribed computers list, locate the Bare Metal OS deployment server and edit the computer settings.
2. Add the custom setting **BAREMETAL_CURRENT_MEDIATMP** and specify the new path in the value field. This path must already exist on the selected server. If the specified path is not found, the temporary folder is created in the default path.
3. After the task completes successfully, create the media.

Important: When you create network boot or offline deployment media for UEFI targets that have the Secure Boot firmware option enabled, you must use an Windows Bundle with WinPE 4 or later and you must disable enhanced error detection in the profiles that you deploy to these targets.

Note: To deploy from a deployment media, the needed drivers must be explicitly bound in the deployment engine binding matrix ("Current Manual Binding" column) in the Driver Bindings.

Note: If the Bare Metal Server providing the deployment media files is not local onto the creator machine, and the creator machine client version is 10.0.8 or later, an additional step for allowing the creator machine to download via https from the Bare Metal Server computer is needed before launching the creation task. Any one of the following alternative steps should be in place before launching the deployment media creation:

- Import on the Bare Metal Server web interface, a certificate signed by a Public CA. See Managing Bare Metal OS Deployment Servers *(on page 41)*.

  or

- Export from a browser connected to the Bare Metal Server web interface, the self signed certificate the server uses for https communications (the *.crt file) and copy it to the folder <bigfix client folder>\TrustedDownloadCerts (by default it's "C:\Program Files (x86)\BES Client\TrustedDownloadCerts) in the creator machine.

  or

- Add to the client running on the creator machine the setting **_BESClient_Download_UntrustedSites** with value as 1.

Creating network boot media

The use of network boot media is useful in situations where a DHCP server is not available, or when there is a firewall that is preventing PXE traffic.

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

1. On the **Media Type** pane 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 are downloaded, and click **Next**.
3. Depending on the deployment kit that is installed on the selected target, the **Create Deployment Media** page displays the version of WinPE that is included in the media. You can specify, select, or change the following settings:
   a. The OS architecture .
   b. Optionally, you can choose to include all available WinPE drivers in the media. This option is useful only when you have a new computer model which is not listed among the available models in the Driver Library, and a binding grid cannot be generated to associate the correct drivers for the devices. A preferable alternative is to add the new computer model to your BigFix environment in one of the following two ways:

        - Install an operating system on the computer of that model and connect it to the BigFix infrastructure through a BES client.

          or

        - PXE boot a computer of that model to a Bare Metal server where the Management Extender for Bare Metal targets is installed and running.

    c. 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 might apply. See Network boot media limitations *(on page 77)*.
    d. Specify 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.
    e. Select the type of network configuration settings that are assigned to the client at boot time. By default, a dynamic IP address is assigned (DHCP). Alternatively, you can specify a static IP address, network mask, and gateway address. If you specify static network settings, you can overwrite them at boot time by checking the corresponding option.
    f. 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.
    g. If the network boot media must connect to a bare metal server of version 7.1.1.20.311.12 or lower, you must select the specific option.

4. When you have completed your selections, click **OK**. The information that you provided is validated before the media creation task begins.

Network boot media requirements and 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 should first format the key with a single bootable FAT32 partition of at least 512 Megabytes.

Important:

- When a target connects to a bare metal server using a network boot CD, a binding menu with all available profiles on that server is displayed. However, because the WinPE that is included in the boot media is downloaded and started on the target, only profiles with an Windows Bundle with the same WinPE version can be deployed successfully.

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 that are disconnected from an internal network, or notebook 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.

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

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

1. On the **Media Type** window, select the target, then select **Create Offline Deployment Media**, and click **Next**.
2. In the **OS Deployment Server and Bare Metal Profiles** pane, select theOS deployment serverto which the files used to build the media are downloaded.
3. The Bare Metal Profiles available at the selected OS deployment server are displayed. The profiles that you can choose from are filtered and meet the following requirements:
    - contain Windows 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**.

   Note: If the profiles you select have a hostname rule containing variables for IP or MAC addresses, their values are substituted with zero (0) at runtime. For example, Win10-[IP] becomes Win10-[0000] on the target.

   Important: If you are creating deployment media for UEFI targets that have the Secure Boot firmware option enabled, the profiles you select to include in the media must not have enhanced error detection enabled. Ensure that the profiles you include meet this criterion, or edit them to disable enhanced error detection before you create the media.

   Note: When you select more than one profile of OS images with different architecture (32-bit and 64-bit), the WinPE 64-bit will be included in the media, and it will not be possible to successfully deploy 32-bit OS image. When you are adding more that one profile of OS images, the OS images must be of the same architecture.

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

    - You can optionally choose to inject available drivers in WinPE
    - You must specify the password of the administrative user on the OS Deployment server that you selected in the previous window. 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 might apply. See Offline deployment media limitations *(on page 79)*
    - 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 completed your selections, click **OK**. The information that you provided is validated before the media creation task begins.

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

- If your media type is a mounted USB key:
    - If you select the **Format the USB key** option, the USB media must 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 first format the key with two partitions, of which the first must be a bootable FAT32 partition of at least 1024 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 your USB key is a fixed disk, and you want to format it with two partitions, you can either format it with the formatUSB.cmd script or manually. If you want to format the key manually, the first partition must be a bootable FAT32 partition of at least 1024 Megabytes, and the second partition a non-bootable NTFS partition, large enough to store the selected images.
    - If the USB key is removable and you want format it with a single partition for deployment on both BIOS and UEFI targets, you must format it manually as a FAT32 bootable partition, then run the makeUSB.cmd script. Furthermore, the image included in the Bare Metal profile must not be larger than 4 GB.
    - For deployment on BIOS targets only, if the USB key is removable, you must format it manually with a single NTFS partition and then run 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 that are 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 that are 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 that is assigned to it, an extra drive letter that 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. Ensure that the key was previously formatted with a bootable FAT32 partition and an extra 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:

   ```
   formatUSB.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. Ensure that the USB key was 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, make sure that you specify the correct disk number and drive letter. Failure to do so might cause unrecoverable damage to your computer. All partitions on the USB key are erased.

Creating and managing Windows Bundles manually

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

You can download and run the Windows Bundle Creator tool on an BigFix 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 Windows Bundle Creator tool manually and install the needed prerequisites , by following the process described in Windows Bundle creation process *(on page 83)*.

If you are setting up the Windows Bundle on an BigFix client, from the **Setup** node, expand **Windows Bundle Creator Setup** to display the required Fixlets and tasks.

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

Note that some Fixlets might not be relevant if the selected client already has the corresponding prerequisites at the required level. The computer on which you run the WADK installation Fixlets must be connected to the external network.

Important: At least Powershell 2.0 is required as a prerequisite to install the Windows Bundle Creator tool.

1. **Deploy 7-Zip - Fixlet 40**

   Downloads the 7-zip compression and decompression tool to the selected computer.
2. **Deploy Windows Assessment and Deployment Kit 10 - Fixlet 62**

   To download and install one of the following on the selected computer:
   - WADK for Windows 11 24H2 (build 26100) for Windows Bundle or to use with MDT build 8456 for MDT Bundle
   - WADK for Windows 11 22H2 (build 22621) to use with MDT build 8456
   - WADK for Windows 11 (build 22000) to use with MDT build 8456
   - WADK 10 release id 2004 to use with MDT build 8456
   - WADK 10 release id 1903 to use with MDT build 8456
   - WADK 10 release id 1809 to use with MDT build 8450 or build 8456
   - WADK 10 release id 1803 to use with MDT build 8450
   - WADK 10 release id 1709 to use with MDT build 8443 or build 8450
   - WADK 10 release id 1703 to use with MDT build 8443
   - WADK 10 release id 1607 to use with MDT build 8443

   Important:
   - WADK for Windows 11 (build 26100) supersedes all previous x64 versions.
   - WADK for Windows 10 2004 supersedes all previous x86 versions.
   - Using WADK 10 release id 1703 or later, when you create an MDT Bundle with a parameters.ini file pointing to an .iso containing `install.esd` or to a folder containing an `install.esd` image, and not `install.wim`, the creation of the bundle is successful.
   - On Windows 7, Windows 2008, or Windows 2008 R2 systems, Microsoft .NET Framework 4.5 must already be installed before you run this Fixlet.

Note: The choice of which kit to download depends on the operating systems you are planning to deploy. See Windows Bundle Creators *(on page 70)*. WAIK and WADK cannot coexist on the same computer.

3. **Deploy MDT build 8456 - Fixlet 137**

   Run this Fixlet on the selected computer if you installed WADK 10 version 1809, version 1903, version 2004, version 21H2 (build 22000), version 22H2 (build 22621), version 24H2 (build 26100) in the previous step if you want to create an MDT Bundle.

   This is not needed if you want to create a Windows Bundle.

   Note: MDT build 8443 and build 8450 are no longer available.

4. **Deploy Windows Bundle Creator - Task 46**

   When you run the Windows Bundle Creator task from the OS Deployment and Bare Metal Imaging site, a folder containing all the Windows Bundle Creator tool program is created. The folder is located in the path `<Drive of BigFix Client>\OSDSETUP`. You can also download the Windows Bundle tool manually to your computer. In this case, a compressed file is downloaded to the specified path and you must extract its contents.
5. Follow the steps described in Windows Bundle creation process *(on page 83)* to launch the Windows Bundle Creator tool on the selected computer.
6. Upload the Windows Bundle to the BigFix server from the Deployment Resources tab of the Bundle and Media Manager Dashboard.

You can find further Fixlets to deploy the old tools at Superseded and Deprecated Fixlets *(on page 260)*.

Windows Bundle creation process

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

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

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

Depending on what you are creating with the Windows 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 Windows 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 84)*.
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 Windows Bundle creation options *(on page 86)*. The only mandatory parameters are listed in the General section of the file.
4. Run the appropriate Windows Bundle Creator for your architecture from within the extracted directory as an Administrator. Run `WindowsBundleCreator.exe` or `WindowsBundleCreator64.exe` depending on your architecture. A `setup.log` file is created in this directory.

   Important: If an Antivirus program is running simultaneously with the Windows 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 `WindowsBundle` folder beneath the directory specified as the target in `parameters.ini` configuration file.
5. Upload the Windows Bundle on the BigFix server. See Creating and uploading Windows Bundles and OS resources *(on page 72)*.

Prerequisites

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

If you choose to create your Windows Bundles on an Endpoint Management client, you can download prerequisites by running the Fixlets described in Creating and managing Windows Bundles manually *(on page 81)* If you download the Windows 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 Windows Bundle Creator tool:

- Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016/2019/2022/2025, Windows Vista Service Pack 2, Windows Server 2008 Service Pack 2.
- MSXML 6.0.

Additionally, you use PowerShell to automate the sequence creation steps. PowerShell is available with Windows Server 2008 and later operating systems 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 download

Note: The license for 7-zip is LGPL and can be found here.

When all prerequisites are satisfied, download and install the following components from the Microsoft sites, depending on the operating systems you are planning to deploy. You can also run the corresponding Fixlets to download them to your Windows Bundle Creator machine. For further information, see Windows Bundle Creators *(on page 70)*.

Table 3. Deployment Toolkits

Deployment Toolkits	Fixlets
Microsoft Deployment Toolkit (Windows) build 8456	Fixlet 137
Windows Assessment and Deployment Kit (WADK) for Windows 8 and 8.1 (Superseded)	Fixlet 60
Windows Assessment and Deployment Kit (WADK) 10	Fixlet 62

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™ 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™ 10 32-bit
- Windows™ 10 64-bit
- Windows™ 11 64-bit
- Windows™ Server 2008 (x86, x64)
- Windows™ Server 2008 R2 (x64)

- Windows™ Server 2012 (x64)
- Windows™ Server 2012 R2 (x64)
- Windows™ Server 2016/2019/2022/2025 (x64)

Windows Bundle creation options

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

The following sections include parameters that you specify to create and customize your Windows 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 `WindowsBundle` 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 (Windows Bundle)

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

WADK10

To use Windows Assessment and Deployment Kit for Windows 10 or Windows Assessment and Deployment Kit for Windows 11.

wimtoolkit (MDT Bundle)

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 for Windows 8.0.

WADK81

To use Windows Assessment and Deployment Kit for Windows 8.1.

WADK10

To use Windows Assessment and Deployment Kit for Windows 10 or Windows Assessment and Deployment Kit for Windows 11.

WADK10_1607

To use Windows Assessment and Deployment Kit for Windows 10 Version 1607.

WADK10_1703

To use Windows Assessment and Deployment Kit for Windows 10 Version 1703.

WAIK

To use Windows Automated Installation Kit.

usmt4x86location (MDT Bundle)

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 (MDT Bundle)

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 (MDT Bundle)

Specifies the path of USMT Version 3 (32-bit). This parameter is optional.

usmt301x64location (MDT Bundle)

Specifies the path of USMT Version 3 (64-bit). This parameter is optional.

Note: Ensure that you have USMT versions 4 or 5 or 10 available prior to deployment. USMT 5 and USMT 10 are included in the Windows ADK installation, USMT 4 must be specified to reimage to Windows Vista.

isosources (Windows Bundle) or mdtsources (MDT Bundle)

This section specifies the locations of the OS resources (ISO files) that are used to create the Windows Bundle. 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 Windows Bundle.

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.

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 Windows 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
```

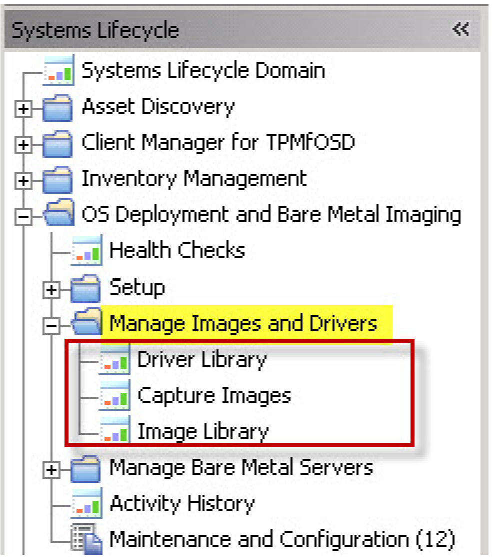
These example parameters copy all the files from `C:\customContent` so that Windows PE will have them under `X:\customScript.`

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

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

Chapter 4. Managing Drivers for Windows Deployments

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



To successfully deploy Windows operating system images on a variety of different computer models, you must import the drivers that are required for both the pre-installation phase (WinPE) and for the Windows Setup phase, when the actual operating system deployment occurs. Drivers are needed to manage the devices on the target hardware models in your network.

You can import single drivers or driver packages and associate them to the hardware models in your network for the operating systems you plan to deploy. At run time, these associations have precedence over the automatic binding mechanism. You can tag and group drivers to make them easily searchable. You can also import and manage non-PCI drivers.

Driver management use cases

To understand how to optimize driver management for your Windows deployments, read the following use cases:

Deployment scenario 1: Provisioning of a new computer model using the BigFix (BES) Client

If you are deploying a new computer model in your environment that already has a pre-installed operating system:

1. Install the BigFix client on the new computer model.
2. Activate the *Hardware Information* analysis (34) to retrieve information about the client
3. Search the hardware vendor sites for the drivers needed for the computer model and operating system that you plan to deploy.

4. Import the drivers and bind them to the new computer model. Generate a binding grid to check which drivers are selected during deployment for the devices found on the computer model, and make any necessary adjustments.
5. Begin deployment.

Deployment Scenario 2: Provisioning of a new computer model using Bare Metal Targets (with the Management Extender for Bare Metal Targets component)

If you are deploying a new hardware model in your environment that has no operating system:

1. Install the Proxy Agent and Management Extender for Bare Metal Targets components on the Bare Metal server. This server must have BigFix Bare Metal Server Version 7.1.1 Fix Pack 18 or later installed.
2. Have the target perform a PXE boot to the Bare Metal Server
3. Activate the *Bare Metal Target Information* analysis (352)
4. Search the hardware vendor sites for the drivers needed for the computer model and operating system that you plan to deploy.
5. Import the drivers and bind them to the new computer model. Generate a binding grid to check which drivers are selected during deployment for the devices found on the computer model, and make any necessary adjustments.
6. Begin Bare Metal deployment.

Deployment Scenario 3: Provisioning of a new computer model using Bare Metal Targets

1. When The target PXE boots to the server and chooses a profile from the Binding Menu , deployment begins.
2. Verify the deployment results in the Activity Dashboard.
3. Import any required drivers and use either the Activity Dashboard or the Binding Tab in the Driver Library dashboard to manually bind the required drivers for the deployment.

You can also import drivers for models that are not yet available in your network. You can tag them with one or more labels to easily identify them at a later date and bind them to the new computer models as they are deployed in your environment.

Click **Driver Library** to import and work with drivers for your deployments on Windows targets.

Before you begin deployments on your Windows targets, complete the following tasks:

- Preparing drivers for Windows deployments *(on page 91)*.
- Importing and managing drivers for Windows deployments *(on page 91)*.
- Managing Windows driver bindings *(on page 99)*

You can also check if critical device drivers are missing or not bound to the target hardware before you deploy images to Windows targets. From the **Check Drivers** tab, select an image and a computer model , and run the driver check.

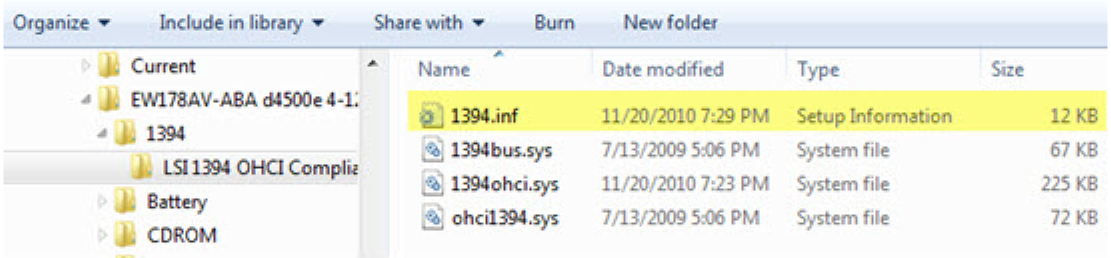
Based on the outcome, you can import any missing driver and bind it to the selected model. See Checking driver availability *(on page 102)*.

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:



Name	Date modified	Type	Size
1394.inf	11/20/2010 7:29 PM	Setup Information	12 KB
1394bus.sys	7/13/2009 5:06 PM	System file	67 KB
1394ohci.sys	11/20/2010 7:23 PM	System file	225 KB
ohci1394.sys	7/13/2009 5:06 PM	System file	72 KB

Importing and managing drivers for Windows deployments

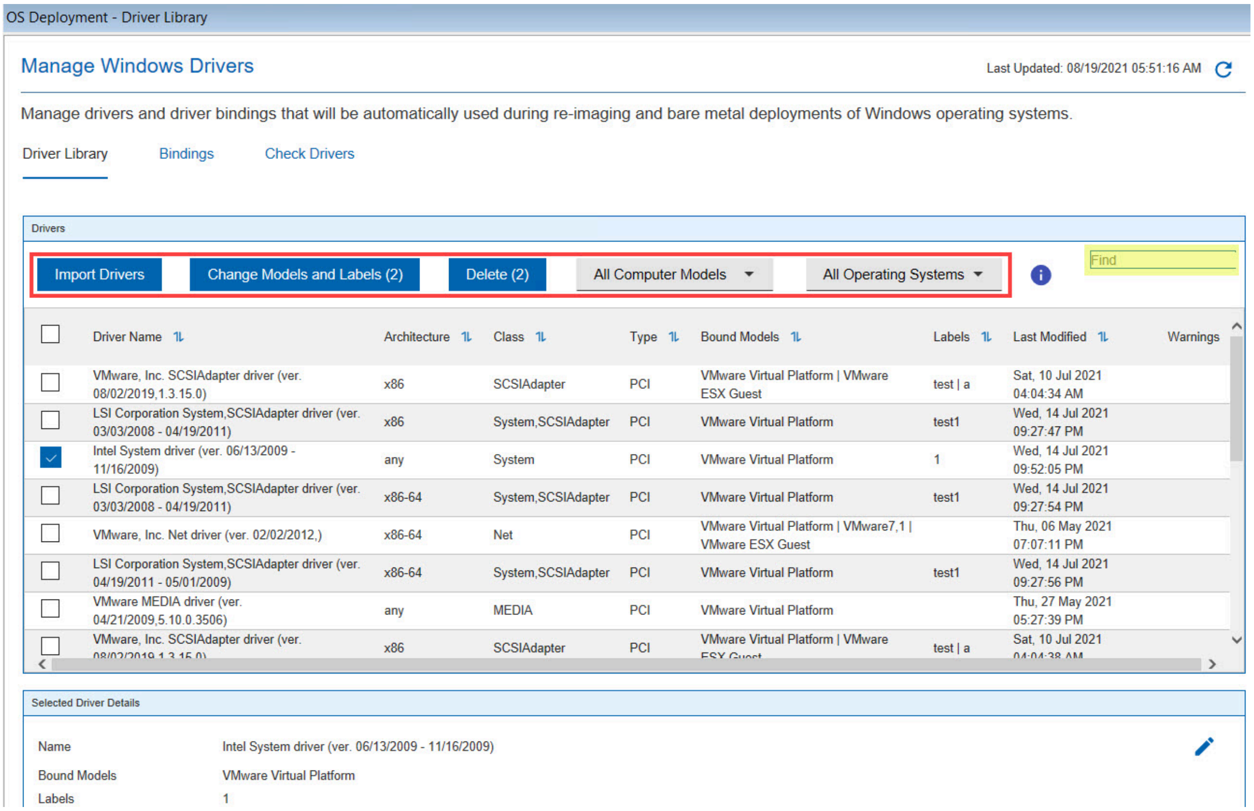
The **Driver Library** dashboard is divided into tabs, from which you can easily manage all device drivers needed for your deployments.

From the **Driver Library** tab you can import new drivers, and manually associate them to specific computer models and operating systems in your environment. You can add labels and model bindings to existing drivers, delete unused drivers, and modify a driver's operating system, model, and architecture compatibility. You can also filter and search drivers with specific characteristics.

From the **Bindings** tab, you can simulate the driver selection that is automatically used for the deployment of a given image on a computer model, by generating a binding grid. You can preview driver assignments in advance, and you can add manual driver bindings for a given image.

From the **Check Drivers** tab, you can verify that all critical drivers needed to deploy one or more images on one or more computer models are available. If drivers are missing, you can import missing drivers selectively.

In the Windows Driver Library, a set of action and filter buttons are available at the top of the list. When you highlight a driver in the list, the details for that driver are displayed in the bottom part.



OS Deployment - Driver Library

Manage Windows Drivers

Last Updated: 08/19/2021 05:51:16 AM

Manage drivers and driver bindings that will be automatically used during re-imaging and bare metal deployments of Windows operating systems.

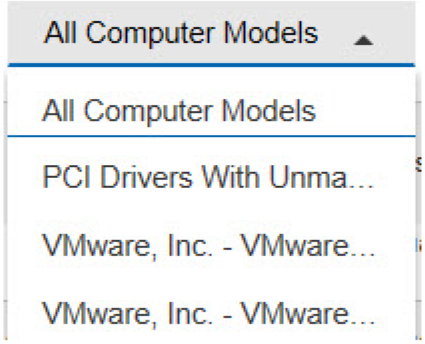
□	Driver Name	Architecture	Class	Type	Bound Models	Labels	Last Modified	Warnings
□	VMware, Inc. SCSIAdapter driver (ver. 08/02/2019,1.3.15.0)	x86	SCSIAdapter	PCI	VMware Virtual Platform | VMware ESX Guest	test | a	Sat, 10 Jul 2021 04:04:34 AM	
□	LSI Corporation System,SCSIAdapter driver (ver. 03/03/2008 - 04/19/2011)	x86	System,SCSIAdapter	PCI	VMware Virtual Platform	test1	Wed, 14 Jul 2021 09:27:47 PM	
☑	Intel System driver (ver. 06/13/2009 - 11/16/2009)	any	System	PCI	VMware Virtual Platform	1	Wed, 14 Jul 2021 09:52:05 PM	
□	LSI Corporation System,SCSIAdapter driver (ver. 03/03/2008 - 04/19/2011)	x86-64	System,SCSIAdapter	PCI	VMware Virtual Platform	test1	Wed, 14 Jul 2021 09:27:54 PM	
□	VMware, Inc. Net driver (ver. 02/02/2012,)	x86-64	Net	PCI	VMware Virtual Platform | VMware7,1 | VMware ESX Guest		Thu, 06 May 2021 07:07:11 PM	
□	LSI Corporation System,SCSIAdapter driver (ver. 04/19/2011 - 05/01/2009)	x86-64	System,SCSIAdapter	PCI	VMware Virtual Platform	test1	Wed, 14 Jul 2021 09:27:56 PM	
□	VMware MEDIA driver (ver. 04/21/2009,5.10.0.3506)	any	MEDIA	PCI	VMware Virtual Platform		Thu, 27 May 2021 05:27:39 PM	
□	VMware, Inc. SCSIAdapter driver (ver. 08/02/2019,1.3.15.0)	x86	SCSIAdapter	PCI	VMware Virtual Platform | VMware ESX Guest	test | a	Sat, 10 Jul 2021 04:04:38 AM	

Selected Driver Details

Name	Intel System driver (ver. 06/13/2009 - 11/16/2009)
Bound Models	VMware Virtual Platform
Labels	1

Drivers are organized by name, architecture, class, and type. The type column lists the device BUS type which is retrieved from the `.inf` file. Depending on the choices you make when importing drivers, or if you modify the current associations of drivers to computer models, additional information is displayed. See Importing drivers *(on page 94)*.

You can filter the list of drivers to display those drivers that are compatible with the devices found for the selected computer model. Click **All Computer Models**, and select a computer model among those available in your environment. The list of available computer models that you can choose from is determined by the analysis *Hardware Information* (34) for the Endpoint Manager clients, and by the analysis *Bare Metal Target Information* (352) for the Bare Metal targets that have completed a PXE boot to Bare Metal Servers with the Management Extender for Bare Metal Targets component installed. The models are listed in the format `Vendor - Computer Model`. For models reported by analysis 352 the format is `*- Computer Model`.



For Bare Metal targets, the devices listed for the discovered computer models are a minimal set of those present on the computer. If a computer model is detected for both a Bare Metal target and an BigFix (BES) client, the model relevant to the BES client takes precedence and is listed.

You can also filter driver compatibility by Operating System. Click **All Operating Systems** and make your selection. The filtered list displays the drivers that are compatible with the selected operating system. Using both filters narrows the list further to display only the drivers that are compatible with the selected Computer model and Operating system combination.

Use the advanced search option by typing in the corresponding search box to filter for specific drivers. You can specify the following:

- Driver Name (including the driver version)
- Class
- Model bind ("Bound Models" column in the Driver Library tab)
- Labels (Labels column in the Driver Library tab)
- Hardware IDs, which identify the specific device and are displayed in the driver details
- Any specific file that is part of the imported driver, including the path that was specified in the wizard ("Imported From" column in the Driver Library tab).

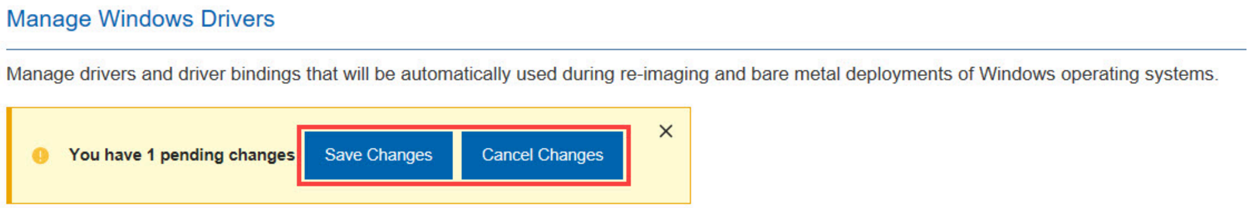
To change model bindings or labels for a driver, select the driver and click **Change Models and Labels**. You can:

- Add one or more labels or delete all labels.
- Add other model bindings or delete all current model bindings.

Click **OK** and save your changes.

To add or modify operating system associations for a driver, click ✏ in the corresponding row. The details for the selected driver are displayed in the bottom section of the dashboard. Modify the current associations, and save your changes.

If you modify the driver model or operating system bindings or if you delete a driver, a *"pending changes"* message displays at the top of the dashboard. You can commit and finalize these changes by clicking **Save Changes** or **Cancel Changes**. An action is created to automatically update any bare metal server with the changes you have saved.



Manage Windows Drivers

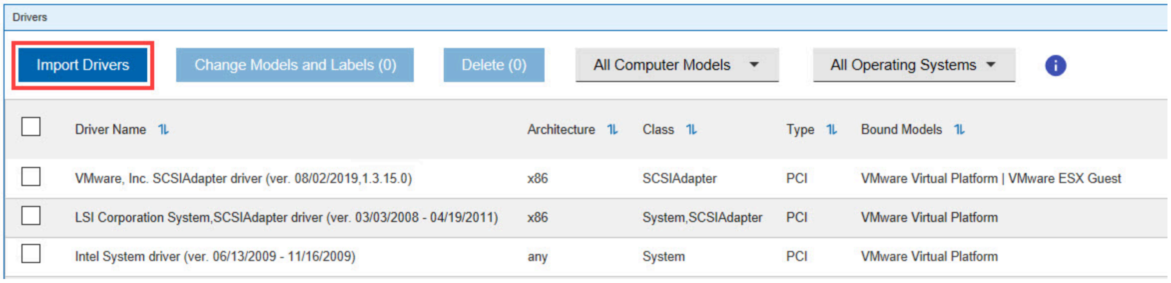
Manage drivers and driver bindings that will be automatically used during re-imaging and bare metal deployments of Windows operating systems.

You have 1 pending changes

Importing drivers

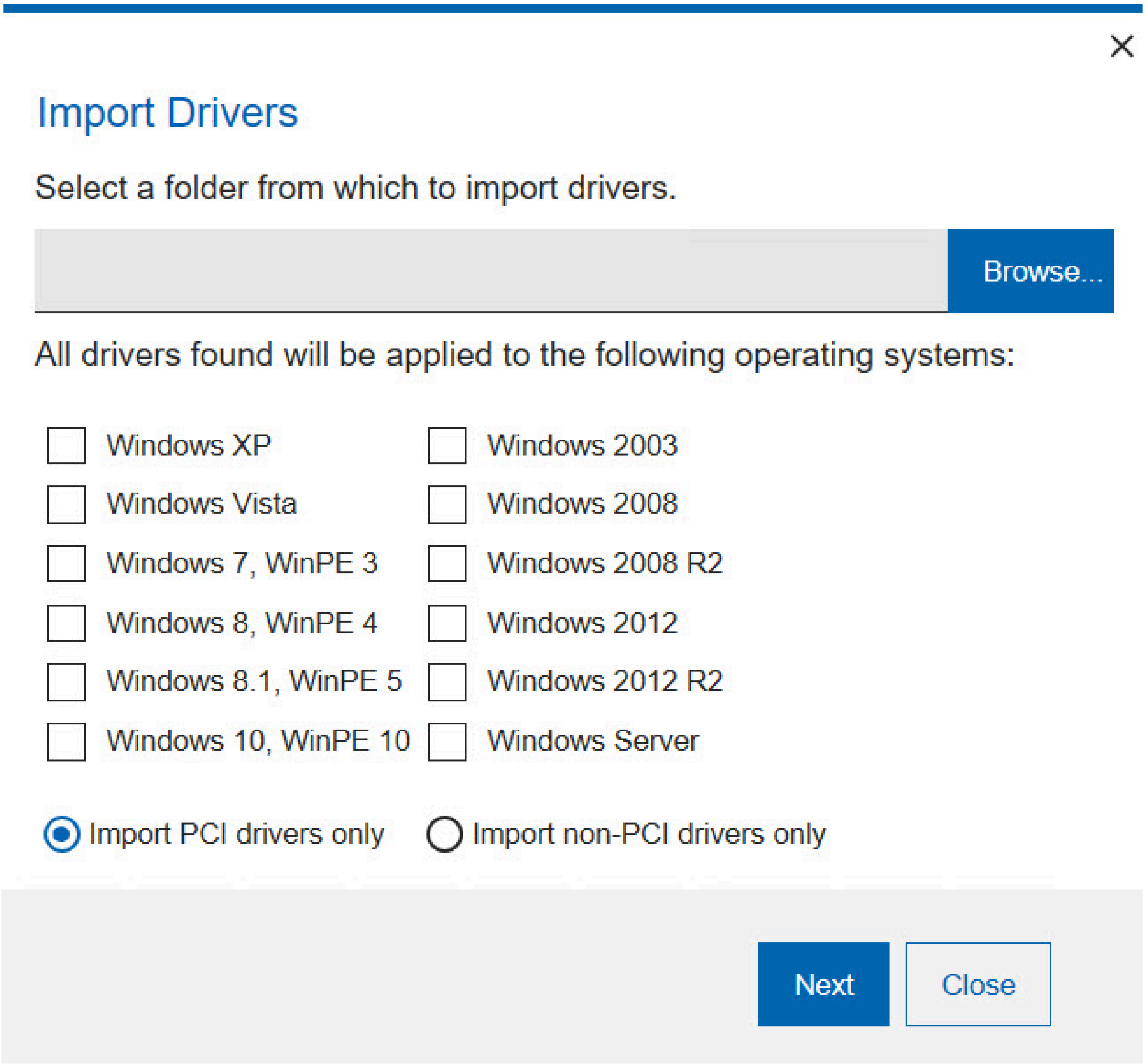
To import new drivers, complete the following steps:

1. Click **Import Drivers**.



□	Driver Name	Architecture	Class	Type	Bound Models
□	VMware, Inc. SCSIAdapter driver (ver. 08/02/2019,1.3.15.0)	x86	SCSIAdapter	PCI	VMware Virtual Platform | VMware ESX Guest
□	LSI Corporation System,SCSIAdapter driver (ver. 03/03/2008 - 04/19/2011)	x86	System,SCSIAdapter	PCI	VMware Virtual Platform
□	Intel System driver (ver. 06/13/2009 - 11/16/2009)	any	System	PCI	VMware Virtual Platform

2. In the Import Drivers dialog, browse to select a folder from which to import drivers. Then select the compatible operating systems for which the imported drivers are to be used. By default, only PCI drivers are imported from the specified folder. If you want to import only non-PCI drivers, select the corresponding option. Click **Next**. The application examines the specified path to identify and analyze the available drivers.



Import Drivers

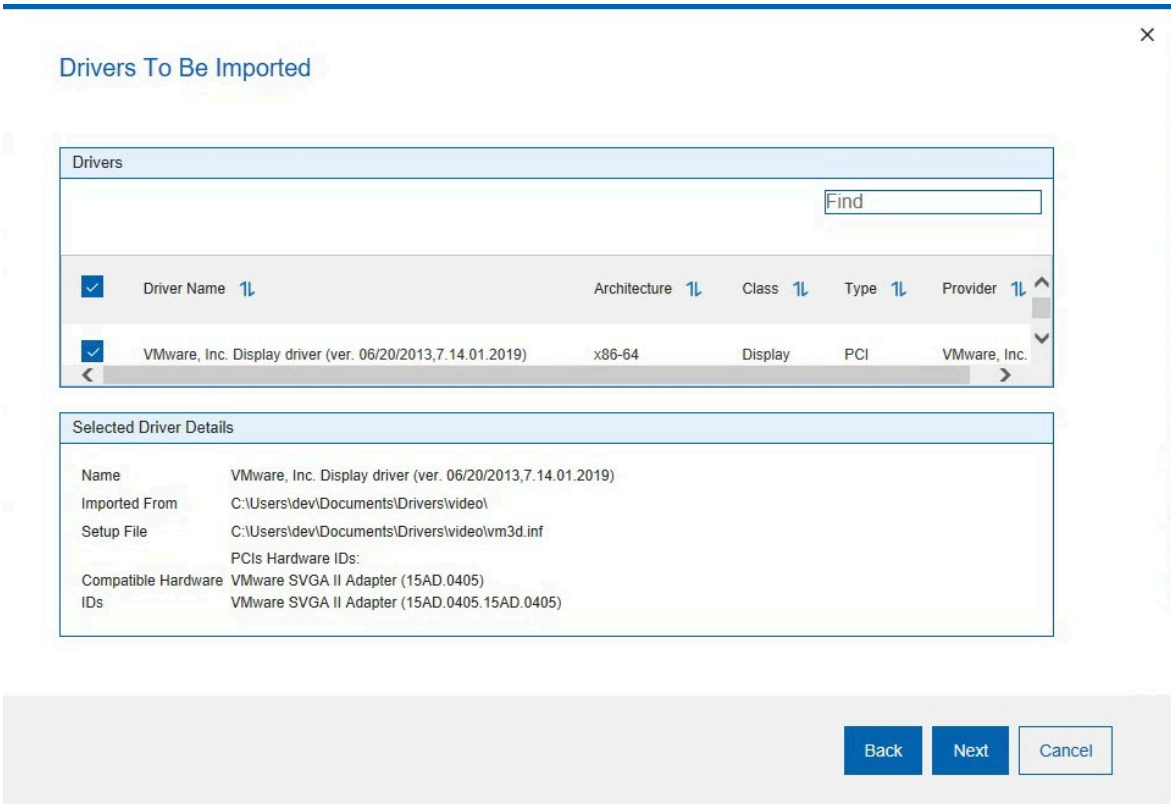
Select a folder from which to import drivers.

All drivers found will be applied to the following operating systems:

□ Windows XP
□ Windows Vista
□ Windows 7, WinPE 3
□ Windows 8, WinPE 4
□ Windows 8.1, WinPE 5
□ Windows 10, WinPE 10
□ Windows 2003
□ Windows 2008
□ Windows 2008 R2
□ Windows 2012
□ Windows 2012 R2
□ Windows Server

● Import PCI drivers only ○ Import non-PCI drivers only

3. The drivers found in the specified path are displayed:



Drivers To Be Imported

Drivers

Find

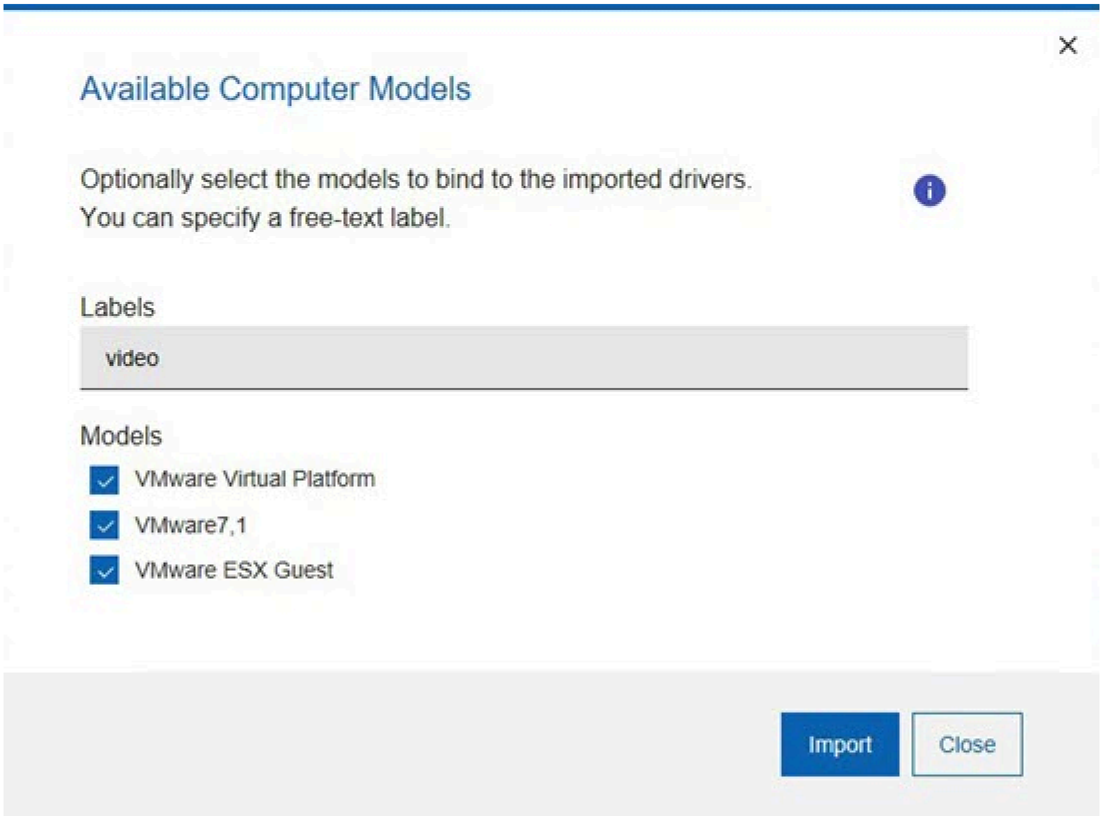
☑	Driver Name	Architecture	Class	Type	Provider
☑	VMware, Inc. Display driver (ver. 06/20/2013,7.14.01.2019)	x86-64	Display	PCI	VMware, Inc.

Selected Driver Details

Name	VMware, Inc. Display driver (ver. 06/20/2013,7.14.01.2019)
Imported From	C:\Users\dev\Documents\Drivers\video\
Setup File	C:\Users\dev\Documents\Drivers\video\vm3d.inf
Compatible Hardware IDs	PCIs Hardware IDs: VMware SVGA II Adapter (15AD.0405) VMware SVGA II Adapter (15AD.0405.15AD.0405)

From this panel you can simply verify if the drivers you want are included in the specified directory. In this case, after viewing the drivers click **Cancel** to exit the wizard. To proceed with the import operation, select one or more drivers from the list and click **Next**.

4. You can optionally select hardware models to bind to the imported drivers. If you do not bind the drivers to any specific models, they are imported and managed using "best match" criteria, after the other drivers that you have bound to specific models. You can optionally assign one or more free text labels to make the drivers you are importing easily identifiable and to simplify driver search. The labels and models that you specify are displayed in the corresponding columns in the Driver Library. Both are optional. If you specify more than one label, each label must be separated by the *"|"* (vertical bar) character. Labels are viewed in the corresponding column of the dashboard, with the vertical bar separating each label. Using labels can be useful if you are importing drivers for models that are not yet deployed in your network. You can tag these drivers and easily retrieve them to bind them to your new computer models when they are available in your network. When you are done, click **Import**.



Available Computer Models

Optionally select the models to bind to the imported drivers.
You can specify a free-text label.

Labels: video

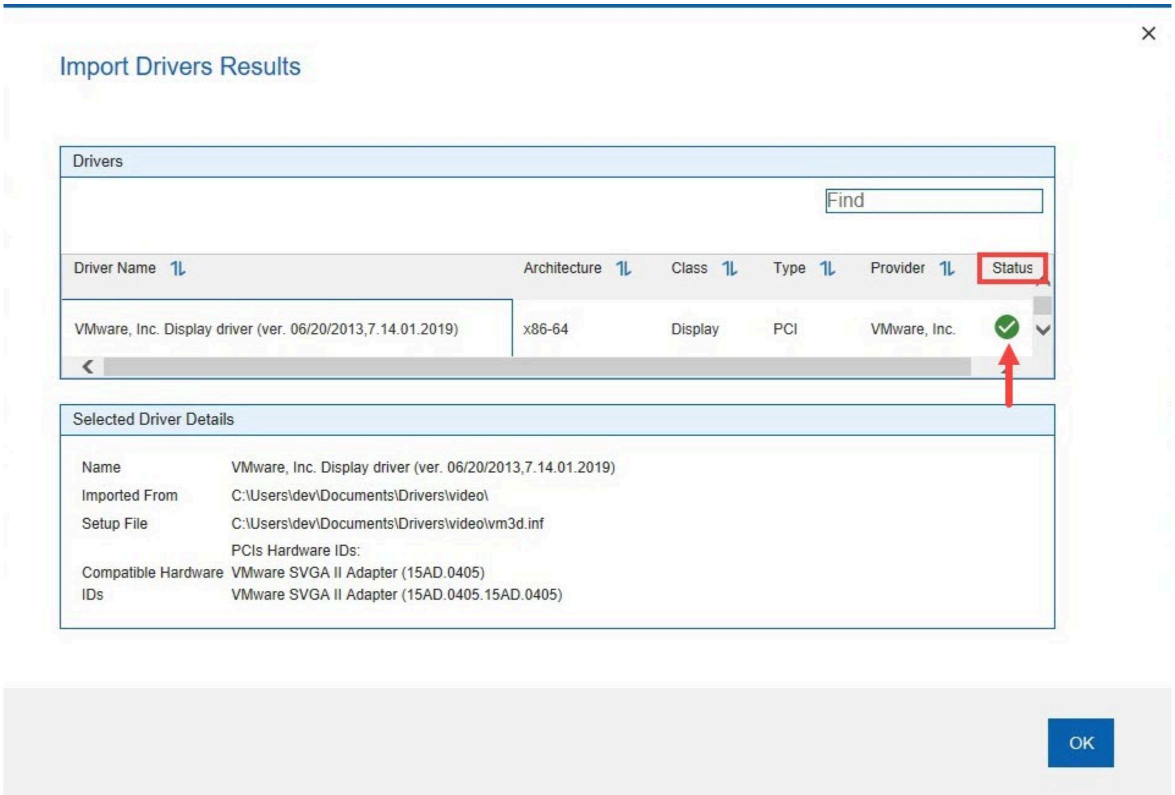
Models

☑ VMware Virtual Platform

☑ VMware7,1

☑ VMware ESX Guest

5. The import results are displayed for each driver you selected, as well as the details.



Import Drivers Results

Drivers

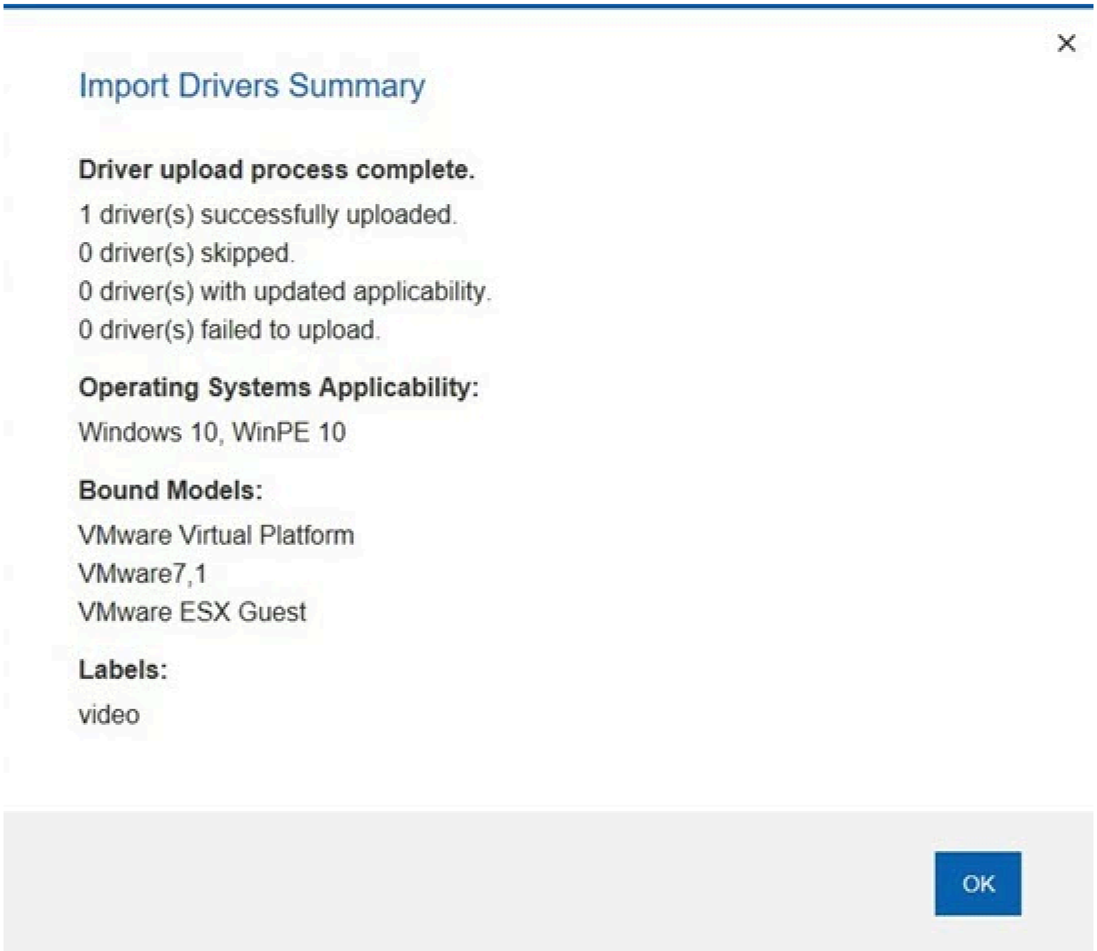
Driver Name	Architecture	Class	Type	Provider	Status
VMware, Inc. Display driver (ver. 06/20/2013,7.14.01.2019)	x86-64	Display	PCI	VMware, Inc.	✓

Selected Driver Details

Name	VMware, Inc. Display driver (ver. 06/20/2013,7.14.01.2019)
Imported From	C:\Users\dev\Documents\Drivers\video\
Setup File	C:\Users\dev\Documents\Drivers\video\vm3d.inf
Compatible Hardware IDs	PCIs Hardware IDs: VMware SVGA II Adapter (15AD.0405) VMware SVGA II Adapter (15AD.0405.15AD.0405)

Click **OK**

6. The Import Drivers Summary is displayed. You can view how many drivers were uploaded. If a driver was already found, its applicability is updated with the information you supplied.



Import Drivers Summary

Driver upload process complete.

1 driver(s) successfully uploaded.
0 driver(s) skipped.
0 driver(s) with updated applicability.
0 driver(s) failed to upload.

Operating Systems Applicability:

Windows 10, WinPE 10

Bound Models:

VMware Virtual Platform
VMware7,1
VMware ESX Guest

Labels:

video

Note:

- As a best practice, import smaller folders of drivers all at the same time. This allows for easier assigning of manual OS and model compatibility and also avoids importing unnecessary drivers. The memory limit for importing drivers requires that the size of the folder to be imported does not exceed the available system memory.
- Drivers that were imported with OS Deployment Version 3.6 or earlier do not have any model bindings defined. These drivers are bound at run time using a best match criteria. You can add these associations manually by using **Change Models and Labels**. If you have one or more driver packages that were imported with earlier versions, you can reimport the same driver packages (without deleting the existing ones) specifying the models that you want to bind at import time. The driver applicability will be updated and the new model binding mechanism is used during deployment.

When drivers are imported, the action **Update Driver Manifests on Bare Metal Servers** is automatically created and run to update the driver manifests on any bare metal server with any changes. The drivers are imported when the action completes.

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

Non-PCI driver management

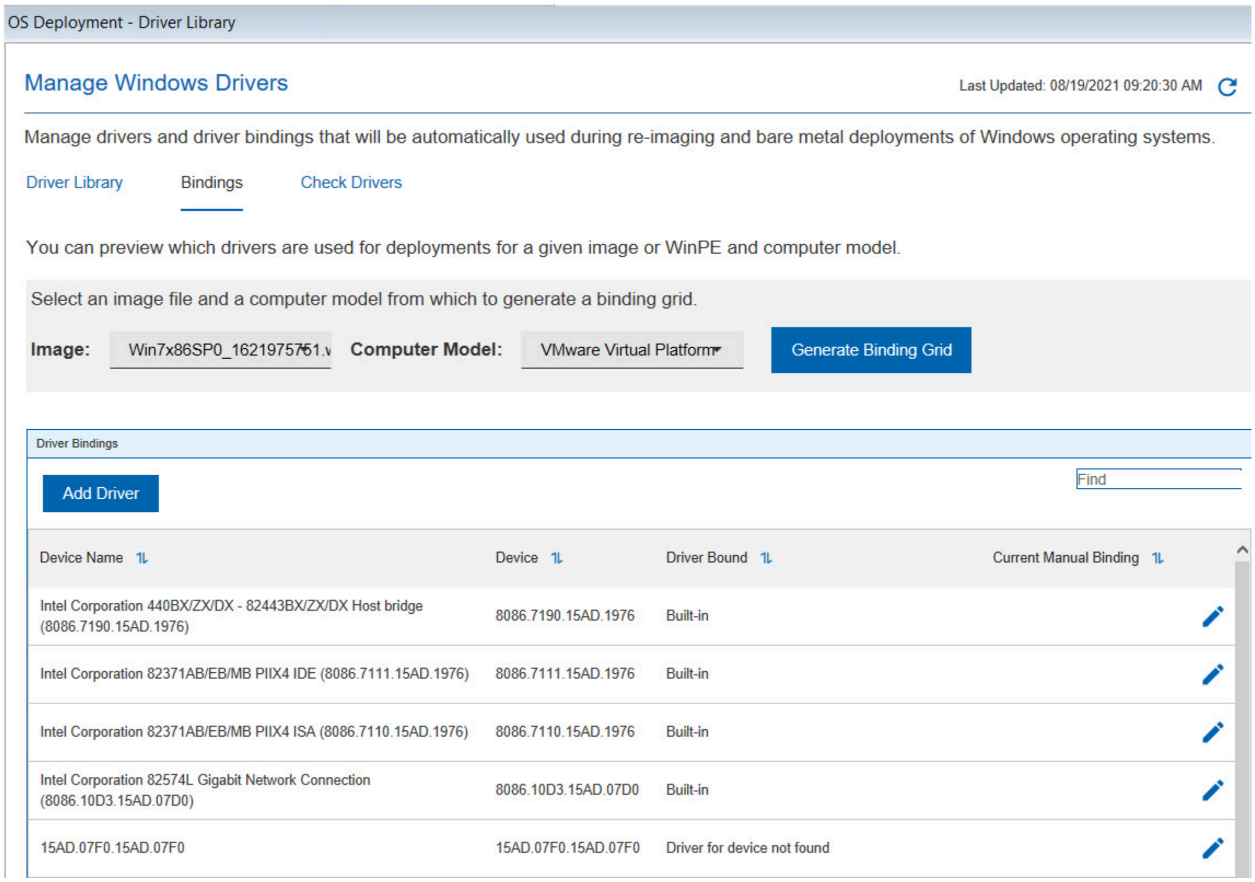
You can manage non-PCI "Server-Site Installation" drivers. From the Driver Library, you can import non-PCI drivers. You can also tag non-PCI drivers by binding them to specific computer models. However, these model bindings are not used at run time during deployments. To use non-PCI drivers during a deployment, you must manually bind the drivers to the image that you want to deploy from the **Bindings** tab. If you do not manually bind them, they are not used during deployments.

Managing Windows driver bindings

Before you deploy an image to a computer, you must ensure that the correct drivers for the devices on the computer are downloaded during the deployment.

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 to be deployed and a computer model on which you want to deploy the image, and click **Generate Binding Grid**. A binding grid is created and displayed in the **Driver Bindings** table. You can view the drivers that are bound. For each device pertaining to the selected model and image. You can also generate a binding grid for Windows Preinstallation Environments (WinPE) images by selecting the WinPE version and computer model from the menu.



Manage Windows Drivers

Last Updated: 08/19/2021 09:20:30 AM

Manage drivers and driver bindings that will be automatically used during re-imaging and bare metal deployments of Windows operating systems.

You can preview which drivers are used for deployments for a given image or WinPE and computer model.

Select an image file and a computer model from which to generate a binding grid.

Image: Win7x86SP0_1621975761.v **Computer Model:** VMware Virtual Platform

Driver Bindings

Device Name	Device	Driver Bound	Current Manual Binding
Intel Corporation 440BX/ZX/DX - 82443BX/ZX/DX Host bridge (8086.7190.15AD.1976)	8086.7190.15AD.1976	Built-in	
Intel Corporation 82371AB/EB/MB PIIX4 IDE (8086.7111.15AD.1976)	8086.7111.15AD.1976	Built-in	
Intel Corporation 82371AB/EB/MB PIIX4 ISA (8086.7110.15AD.1976)	8086.7110.15AD.1976	Built-in	
Intel Corporation 82574L Gigabit Network Connection (8086.10D3.15AD.07D0)	8086.10D3.15AD.07D0	Built-in	
15AD.07F0.15AD.07F0	15AD.07F0.15AD.07F0	Driver for device not found	

The binding grid displays for each device name the following information:

In the **Driver Bound** column, the possible values for the 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.

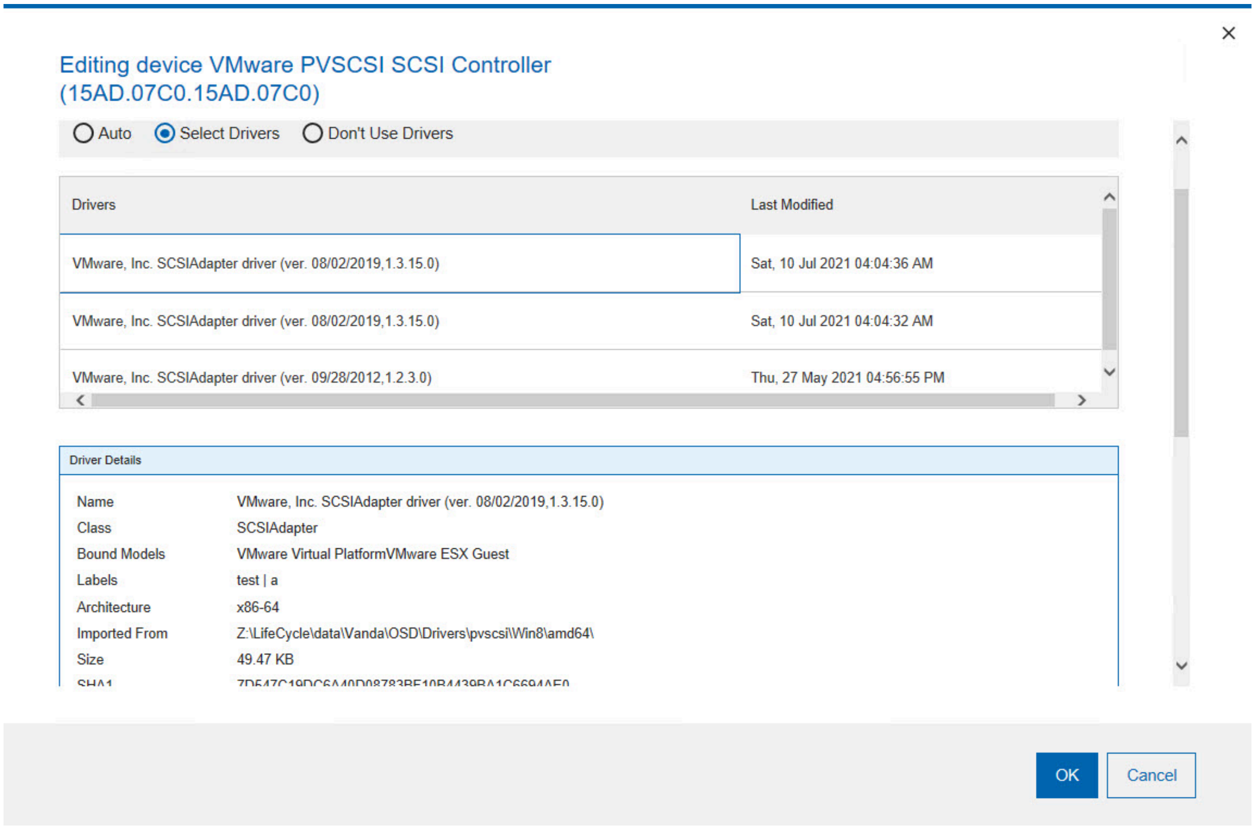
No applicable drivers found

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 **Current Manual Binding** column displays any drivers that were manually selected by editing a device in the binding grid.

At run time, OS Deployment selects the drivers that are the best match for the selected image/model combination. However, if you have bound a driver at import time to a computer model, this binding has precedence over the default best match (auto) mechanism.

You can edit the driver bindings for a specific device by clicking ✏.



Editing device VMware PVSCSI SCSI Controller (15AD.07C0.15AD.07C0)

○ Auto ● Select Drivers ○ Don't Use Drivers

Drivers	Last Modified
VMware, Inc. SCSIAdapter driver (ver. 08/02/2019,1.3.15.0)	Sat, 10 Jul 2021 04:04:36 AM
VMware, Inc. SCSIAdapter driver (ver. 08/02/2019,1.3.15.0)	Sat, 10 Jul 2021 04:04:32 AM
VMware, Inc. SCSIAdapter driver (ver. 09/28/2012,1.2.3.0)	Thu, 27 May 2021 04:56:55 PM

Driver Details

Name	VMware, Inc. SCSIAdapter driver (ver. 08/02/2019,1.3.15.0)
Class	SCSIAdapter
Bound Models	VMware Virtual PlatformVMware ESX Guest
Labels	test | a
Architecture	x86-64
Imported From	Z:\LifeCycle\data\Vanda\OSD\Drivers\pvscsi\Win8\amd64\
Size	49.47 KB
SHA1	7D547C19DC6A40D08783BE10B4439BA1C6694AE0

You can change the following options.

Auto

Automatically selects the driver (best match) and is the default option.

Select Drivers

Allows you to select the drivers that you want to include in the deployment from a list of compatible drivers for the specific device. The drivers you select are displayed in the "Current Manual Binding" column of the binding grid.

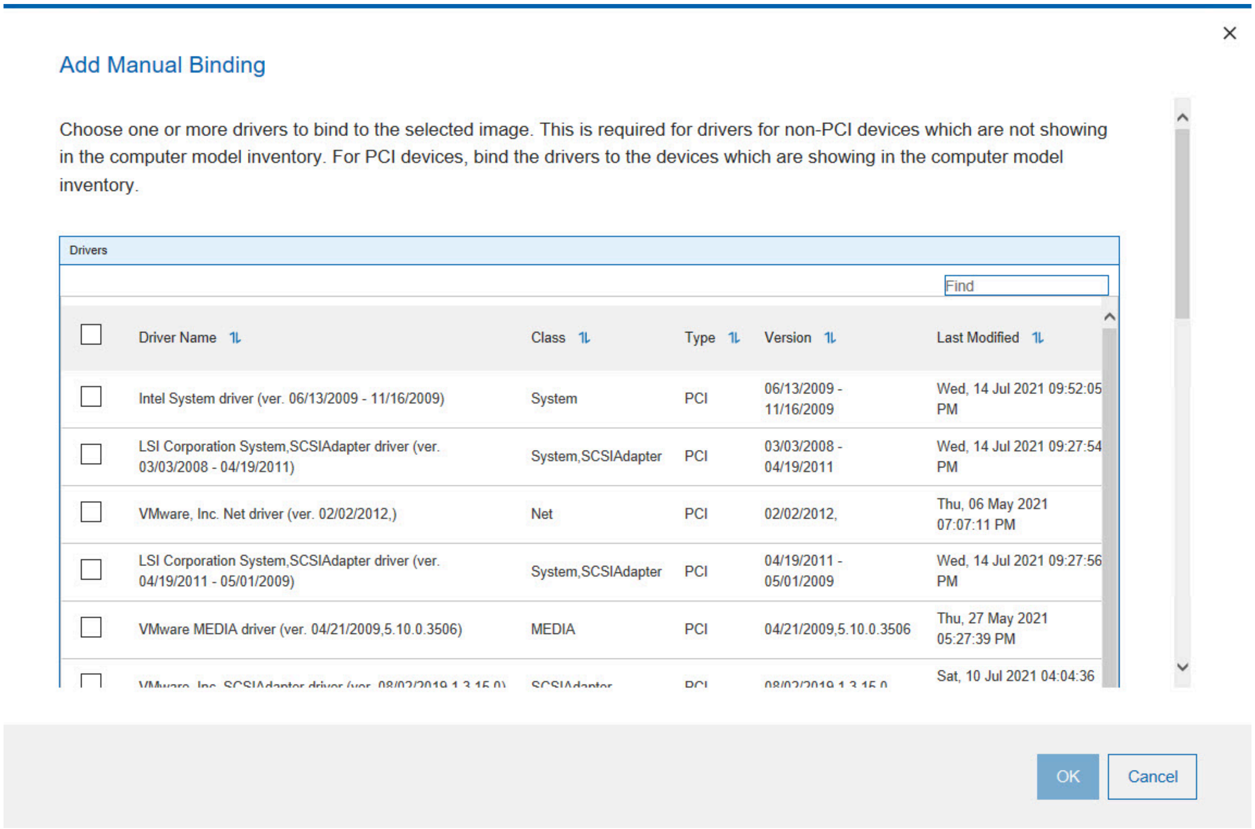
Don't Use Drivers

Allows you not to associate any driver to the device.

You can refresh the generated binding grid to include the changes that you have made by clicking the corresponding button.

Click **Add Driver** 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. If you add a driver, it takes precedence over the model binding that you specified at driver import time.

You can bind drivers to WinPE images if your Windows Bundle is at version 3.8 or later and you have selected to overwrite existing WinPEs when you upload the Windows Bundle. The Bare Metal OS Deployment server must be at version 7.1.1.19 or later.



Add Manual Binding

Choose one or more drivers to bind to the selected image. This is required for drivers for non-PCI devices which are not showing in the computer model inventory. For PCI devices, bind the drivers to the devices which are showing in the computer model inventory.

Drivers

□	Driver Name ⇅	Class ⇅	Type ⇅	Version ⇅	Last Modified ⇅
□	Intel System driver (ver. 06/13/2009 - 11/16/2009)	System	PCI	06/13/2009 - 11/16/2009	Wed, 14 Jul 2021 09:52:05 PM
□	LSI Corporation System,SCSIAdapter driver (ver. 03/03/2008 - 04/19/2011)	System,SCSIAdapter	PCI	03/03/2008 - 04/19/2011	Wed, 14 Jul 2021 09:27:54 PM
□	VMware, Inc. Net driver (ver. 02/02/2012,)	Net	PCI	02/02/2012,	Thu, 06 May 2021 07:07:11 PM
□	LSI Corporation System,SCSIAdapter driver (ver. 04/19/2011 - 05/01/2009)	System,SCSIAdapter	PCI	04/19/2011 - 05/01/2009	Wed, 14 Jul 2021 09:27:56 PM
□	VMware MEDIA driver (ver. 04/21/2009,5.10.0.3506)	MEDIA	PCI	04/21/2009,5.10.0.3506	Thu, 27 May 2021 05:27:39 PM
□	VMware, Inc. SCSIAdapter driver (ver. 08/02/2019,1.3.15.0)	SCSIAdapter	PCI	08/02/2019,1.3.15.0	Sat, 10 Jul 2021 04:04:36

At run time, OS Deployment selects the drivers that are the best match for the selected image/model combination. However, if you have bound a driver at import time to a computer model, this binding has precedence over the default best match (auto) mechanism.

Note: In a WinPE Direct Boot enabled bare metal server, the needed drivers must be explicitly bound in the deployment engine binding matrix ("Current Manual Binding" column) in the Driver Bindings.

Checking driver availability

Before you deploy images to computers in your network, you can verify that the drivers you need for the installed devices are available, and, if necessary import missing drivers selectively.

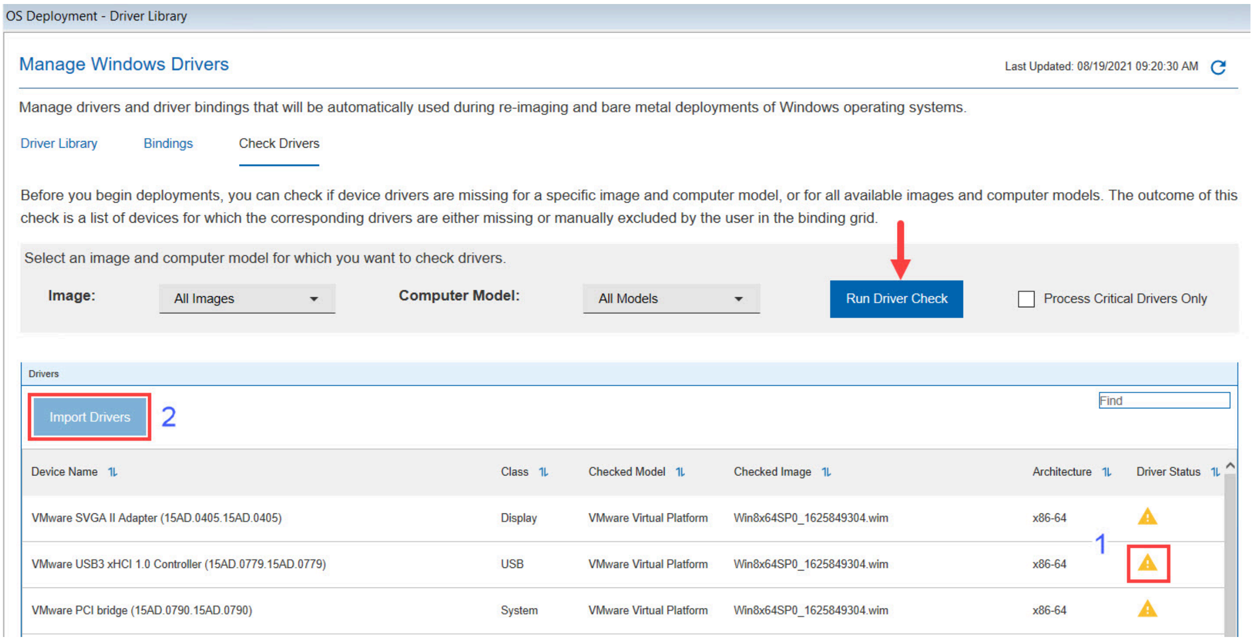
From the **Check Drivers** tab of the **Driver Library** dashboard, you can check driver availability for any single image and computer model in your environment or for all images and computer models. If specific device drivers are missing, you can import them directly. Only PCI drivers are checked.

Select an image and a computer model from the list, or all images and computer models. and click **Run Driver Check**.

By default, the check is processed on critical drivers only. Deselect this option to also include non-critical drivers. Depending on the size and diversity of the hardware models and operating system images in your network, the process of checking all images and models can take a few minutes to complete.

The result of this check is a list of devices for which the related drivers are either not available or were explicitly excluded from deployment when you generated the binding grid. In the **Driver Status** column, different icons display the status of the driver for each of the listed devices:

- ❗ The driver is missing for a critical device (typically network or disk drivers).
- ⚠ The driver is missing, but the device is not a critical device.
- ℹ The driver for this device exists, but the user manually excluded the driver from the binding grid.



OS Deployment - Driver Library

Manage Windows Drivers

Last Updated: 08/19/2021 09:20:30 AM

Manage drivers and driver bindings that will be automatically used during re-imaging and bare metal deployments of Windows operating systems.

Before you begin deployments, you can check if device drivers are missing for a specific image and computer model, or for all available images and computer models. The outcome of this check is a list of devices for which the corresponding drivers are either missing or manually excluded by the user in the binding grid.

Select an image and computer model for which you want to check drivers.

Image: All Images **Computer Model:** All Models

□ Process Critical Drivers Only

Device Name	Class	Checked Model	Checked Image	Architecture	Driver Status
VMware SVGA II Adapter (15AD.0405.15AD.0405)	Display	VMware Virtual Platform	Win8x64SP0_1625849304.wim	x86-64	⚠
VMware USB3 xHCI 1.0 Controller (15AD.0779.15AD.0779)	USB	VMware Virtual Platform	Win8x64SP0_1625849304.wim	x86-64	⚠
VMware PCI bridge (15AD.0790.15AD.0790)	System	VMware Virtual Platform	Win8x64SP0_1625849304.wim	x86-64	⚠

For each device listed you can complete a remediation action. To import a missing driver, select a device from the list and click **Import Drivers**. In the import wizard, specify the folder from which to import the driver. The import process selectively searches and displays only the driver or drivers that are compatible for the chosen device, image, model and architecture. You can also double click the device to open the import wizard.

If the driver for the listed device exists but the binding was disabled by the user, click the **Bindings** tab, select the image and computer model to generate the binding grid, and manually bind the driver to include it in the deployment.

Chapter 5. Managing Linux OS Resources and Deployment Media

You can import Linux OS Resources needed to create network boot media and to capture and deploy Linux images

Importing Linux OS Resources for RHEL, SLES and CentOS deployments

Linux OS Resources are required to capture Linux reference machines, to create network boot media for Linux deployments and to install Linux OS.

To create it from the **Bundle and Media Manager** dashboard, click the corresponding button in the **Deployment Resources** tab. Browse to the fully qualified path of the Linux ISO file from which the OS Resource will be imported, and click **OK**. When the action completes, the Linux OS Resource is displayed in the list. To delete a Linux OS Resource entry, select it and click **Delete**.

A Linux OS Resource for the same OS level is also created when its setup image is imported from the **Image Library** dashboard.

For a Linux resource, the specific grub2 bootloader for UEFI targets is also included in it. You can check if the grub2 bootloader for UEFI targets is included in the OS Resource by checking the **Resource Info** column, where grub.efi or grubx64.efi is reported if it is included. If it is not included, the Linux deployment on UEFI target uses the external grub2 bootloader if present, as described in Creating Bare Metal Profiles for Linux Images *(on page 200)*; otherwise, the embedded elilo.efi bootloader is used.

To use the grub2 bootloader for Linux deployment on UEFI target, the DHCP server must provide the option "next-server" with the value of the bare metal server IP address. On some DHCP servers, this options is provided together with the option 66.

Importing Linux OS Resources for RHEL in-place upgrade

RHEL in-place upgrade OS resource is needed to run the in-place upgrade from RHEL 6 to RHEL 7, from RHEL 7 to RHEL 8 and from RHEL 8 to RHEL 9. The resource will be applied to the initial OS and most files needed to create it can be found in the installation media of the initial OS. The files that cannot be found on the installation media must be downloaded from the RHEL web site, after authenticating with a user authorized for rpm download.

You can create RHEL in-place upgrade OS resource for RHEL 6.10 to upgrade to RHEL 7.9, for RHEL 7.9 to upgrade to RHEL 8.8 and 8.10, for RHEL 8.8 to upgrade to RHEL 9.2, for RHEL 8.9 to upgrade to RHEL 9.3, for RHEL 8.10 to upgrade to RHEL 9.4 or later.

To create it from the **Bundle and Media Manager** dashboard, click the corresponding button in the **Deployment Resources** tab. Browse to the dedicated folder where the files needed for the initial OS of your in-place upgrade task are and click **OK**. When the action completes, the Linux in-place OS Resource is displayed in the list. To delete a Linux OS Resource entry, select it and click **Delete**.

To create the in-place upgrade Linux OS resource needed to upgrade RHEL 6.10 to 7.9, the needed rpm files are listed below:

- **FOR RHEL 6.10**:
  - `fakeroot-1.12.2-22.2.el6.x86_64.rpm`
  - `fakeroot-libs-1.12.2-22.2.el6.x86_64.rpm`
  - `gdb-7.2-92.el6.x86_64.rpm`
  - `openscap-1.2.13-2.el6.x86_64.rpm`
  - `openscap-engine-sce-1.2.13-2.el6.x86_64.rpm`
  - `openscap-scanner-1.2.13-2.el6.x86_64.rpm`
  - `openscap-utils-1.2.13-2.el6.x86_64.rpm`
  - `preupgrade-assistant-2.6.2-1.el6.noarch.rpm`
  - `preupgrade-assistant-el6toel7-0.8.0-3.el6.noarch.rpm`
  - `preupgrade-assistant-el6toel7-data-0.20200704-1.el6.noarch.rpm`
  - `pykickstart-1.74.22-1.el6.noarch.rpm`
  - `redhat-rpm-config-9.0.3-51.el6.noarch.rpm`
  - `redhat-upgrade-tool-0.8.0-9.el6.noarch.rpm`
  - `rpm-build-4.8.0-59.el6.x86_64.rpm`
  - `rpmdevtools-7.5-2.el6.noarch.rpm`
  - `yum-utils-1.1.30-42.el6_10.noarch.rpm`

  The files that cannot be found on RHEL 6.10 installation media can be found at the link https://access.redhat.com/downloads/content/69/ver=/rhel---6/6.10/x86_64/packages

To create the in-place upgrade Linux OS resource needed to upgrade RHEL 7.9 to 8.8 or to 8.10, the needed rpm files are listed below:

- **For RHEL 7.9**:
  - `audit-2.8.5-4.el7.x86_64.rpm`
  - `audit-libs-2.8.5-4.el7.x86_64.rpm`
  - `audit-libs-python-2.8.5-4.el7.x86_64.rpm`
  - `checkpolicy-2.5-8.el7.x86_64.rpm`
  - `dnf-4.0.9.2-2.el7_9.noarch.rpm`
  - `dnf-data-4.0.9.2-2.el7_9.noarch.rpm`
  - `json-glib-1.4.2-2.el7.x86_64.rpm`
  - `leapp-deps-0.17.0-1.el7_9.noarch.rpm`
  - `leapp-upgrade-el7toel8-0.20.0-2.el7_9.noarch.rpm`
  - `leapp-upgrade-el7toel8-deps-0.20.0-2.el7_9.noarch.rpm`
  - `libcgroup-0.41-21.el7.x86_64.rpm`
  - `libcomps-0.1.8-14.el7.x86_64.rpm`
  - `libdnf-0.22.5-2.el7_9.x86_64.rpm`
  - `libmodulemd-1.6.3-1.el7.x86_64.rpm`
  - `librepo-1.8.1-8.el7_9.x86_64.rpm`
  - `libreport-filesystem-2.1.11-53.el7.x86_64.rpm`
  - `librhsm-0.0.3-3.el7_9.x86_64.rpm`
  - `libsemanage-python-2.5-14.el7.x86_64.rpm`

    - `libsolv-0.6.34-4.el7.x86_64.rpm`
    - `libyaml-0.1.4-11.el7_0.x86_64.rpm`
    - `pciutils-3.5.1-3.el7.x86_64.rpm`
    - `policycoreutils-2.5-34.el7.x86_64.rpm`
    - `policycoreutils-python-2.5-34.el7.x86_64.rpm`
    - `python-chardet-2.2.1-3.el7.noarch.rpm`
    - `python-enum34-1.0.4-1.el7.noarch.rpm`
    - `python-IPy-0.75-6.el7.noarch.rpm`
    - `python-requests-2.6.0-10.el7.noarch.rpm`
    - `python-urllib3-1.10.2-7.el7.noarch.rpm`
    - `python2-dnf-4.0.9.2-2.el7_9.noarch.rpm`
    - `python2-hawkey-0.22.5-2.el7_9.x86_64.rpm`
    - `python2-leapp-0.17.0-1.el7_9.noarch.rpm`
    - `python2-libcomps-0.1.8-14.el7.x86_64.rpm`
    - `python2-libdnf-0.22.5-2.el7_9.x86_64.rpm`
    - `setools-libs-3.3.8-4.el7.x86_64.rpm`

  The files that cannot be found on RHEL 7.9 installation media can be found at the link https://access.redhat.com/downloads/content/69/ver=/rhel—7/7.9/x86_64/packages

- **For RHEL 8.8**:
    - `leapp-0.15.1-1.el8.noarch.rpm`
    - `leapp-deps-0.15.1-1.el8.noarch.rpm`
    - `leapp-upgrade-el8toel9-0.18.0-1.el8_8.2.noarch.rpm`
    - `leapp-upgrade-el8toel9-deps-0.18.0-1.el8.noarch.rpm`
    - `python3-leapp-0.15.1-1.el8.noarch.rpm`
    - `python3-pip-9.0.3-22.el8.noarch.rpm`
    - `python3-setuptools-39.2.0-7.el8.noarch.rpm`
    - `python36-3.6.8-38.module+el8.5.0+12207+5c5719bc.x86_64.rpm`
    - `systemd-container-239-74.el8_8.x86_64.rpm`

  All the files can be found on the installation ISO apart from `leapp-upgrade-el8toel9-0.18.0-1.el8_8.2.noarch.rpm` that can be downloaded from the link https://access.cdn.redhat.com/content/origin/rpms/leapp-upgrade-el8toel9/0.18.0/1.el8_8.2/fd431d51/leapp-upgrade-el8toel9-0.18.0-1.el8_8.2.noarch.rpm

- **For RHEL 8.9**:
    - `leapp-0.16.0-2.el8.noarch.rpm`
    - `leapp-deps-0.16.0-2.el8.noarch.rpm`
    - `leapp-upgrade-el8toel9-0.19.0-1.el8.noarch.rpm`
    - `leapp-upgrade-el8toel9-deps-0.19.0-1.el8.noarch.rpm`
    - `python3-leapp-0.16.0-2.el8.noarch.rpm`
    - `python3-pip-9.0.3-23.el8.noarch.rpm`
    - `python3-setuptools-39.2.0-7.el8.noarch.rpm`

    - `python36-3.6.8-38.module+el8.5.0+12207+5c5719bc.x86_64.rpm`
    - `systemd-container-239-78.el8.x86_64.rpm`

  All the files can be found on the installation media.

- **For RHEL 8.10**:
    - `leapp-0.18.0-1.el8.noarch.rpm`
    - `leapp-deps-0.18.0-1.el8.noarch.rpm`
    - `leapp-upgrade-el8toel9-0.21.0-2.el8_10.noarch.rpm`
    - `leapp-upgrade-el8toel9-deps-0.21.0-2.el8_10.noarch.rpm`
    - `python3-leapp-0.18.0-1.el8_10.noarch.rpm`
    - `python3-pip-9.0.3-24.el8.noarch.rpm`
    - `python3-setuptools-39.2.0-7.el8.noarch.rpm`
    - `python36-3.6.8-39.module+el8.10.0+20784+edafcd43.x86_64.rpm`
    - `systemd-container-239-82.el8.x86_64.rpm`

  The files that cannot be found on RHEL 8.10 installation media can be found at the link https://access.redhat.com/downloads/content/479/ver=/rhel---8/8.10/x86_64/packages

Creating and importing OS Resources for Ubuntu deployments

Linux Ubuntu, deployments require that you create and import a corresponding OS resource. To create and import OS Resources for Ubuntu deployments, see Create and Import OS Resources for Linux Ubuntu Deployments *(on page 108)*.

Creating network boot media for Linux RHEL, SLES, and CentOS targets

To create Linux network boot media, complete the following steps:

1. From the **Bundle and Media Manager** dashboard, import a Linux OS Resource by clicking the corresponding button. Select the fully qualified path to the ISO file. The supported ISO files are RedHat Enterprise Linux (RHEL) Release 6, 7, 8, 9, CentOS Linux Release 7, 8 or SUSE Linux Version 12 or 15. If you have already imported Linux OS Resources for these platforms skip this step.
2. From the **Linux Media** tab, click **Create Deployment Media**. The Media creation wizard is displayed. Select the OS Deployment Server where the media will be created, and click **Next**.
3. Select or specify the following:
    a. The Linux OS Resource to be included in the media. You must have previously imported the resource.
    b. Specify the fully qualified path on the OS Deployment Server where the ISO file for the media will be created
    c. In the Server Settings section, specify the IP address and the administrative user password of the OS Deployment Server to which the target connects at boot time. This server can be the same or a different OS Deployment server from the one you are creating the media on. Alternatively, you can specify the connection parameters at boot time, by checking the corresponding option.
    d. Select the type of network configuration settings that are assigned to the client at boot time. By default, a dynamic IP address is assigned (DHCP). Alternatively, you can specify a static IP address,

network mask, and gateway address. If you specify static network settings, you can overwrite them at boot time by checking the corresponding option.

e. 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.

f. If the network boot media must connect to a bare metal server of version 7.1.1.20.311.12 or lower, you must select the specific option.

4. When you have completed your selections, click **OK**. The information that you provided is validated before the media creation task begins.

! **Important:**

- If you want to deploy a Linux setup image in multicast from network boot media, the Linux OS resource that you include in the media must be of the same major version of the image that you are deploying. For example, you can use a RedHat Enterprise Linux (RHEL) Versions 7 Update 8 resource to deploy all Red Hat Enterprise Linux (RHEL) Version 7 setup images using multicast communication.

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

- Only CD/DVD media are supported.
- Deployment of the media on UEFI targets is not supported.
- Media creation and deployment on Ubuntu Linux is not supported.

Create and Import OS Resources for Linux Ubuntu Deployments

To capture and deploy Linux Ubuntu Desktop images, you must create and upload the required OS resources.

OS Deployment 3.10 introduces the support of Ubuntu Desktop for Bare Metal Deployments of captured images. To deploy Ubuntu, you must create a corresponding OS Resource, by downloading a Server .ISO used for resource creation, and by running Task 68, as described in the following steps.

! **Important:**

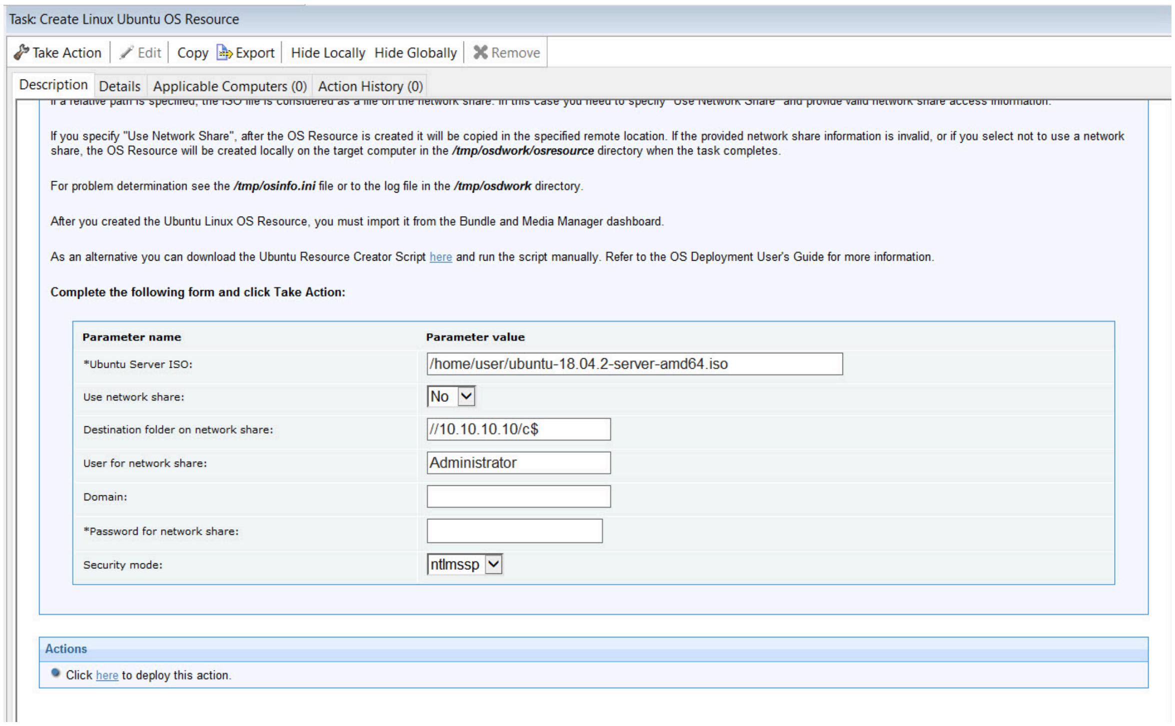
- Ubuntu 16.04, 18.04, and 20.04 require the Legacy Server ISO. You can download the Ubuntu Server ISO from the alternative downloads of the official Ubuntu webpage (for Ubuntu 20.04 visit http://cdimage.ubuntu.com/ubuntu-legacy-server/releases/20.04/release).

- Ubuntu 22.04 requires the Live Server ISO.

Creating OS Resources for Ubuntu deployments

To create an OS Resource for Ubuntu deployments, perform the following steps on an Ubuntu machine of the same release of the Server ISO that you are downloading. The Ubuntu machine can be either Ubuntu Desktop or Ubuntu Server but they may require some additional packages to be installed.[1]

1. Download from the internet the Ubuntu server .ISO file[2] in your environment to an existing Ubuntu machine.
2. From the Bigfix Console, run the Create Linux Ubuntu OS Resource Task (ID 68):



Task: Create Linux Ubuntu OS Resource
Take Action | Edit | Copy | Export | Hide Locally | Hide Globally | Remove
Description | Details | Applicable Computers (0) | Action History (0)

If a relative path is specified, the ISO file is considered as a file on the network share. In this case you need to specify "Use Network Share" and provide valid network share access information.

If you specify "Use Network Share", after the OS Resource is created it will be copied in the specified remote location. If the provided network share information is invalid, or if you select not to use a network share, the OS Resource will be created locally on the target computer in the ***/tmp/osdwork/osresource*** directory when the task completes.

For problem determination see the ***/tmp/osinfo.ini*** file or to the log file in the ***/tmp/osdwork*** directory.

After you created the Ubuntu Linux OS Resource, you must import it from the Bundle and Media Manager dashboard.

As an alternative you can download the Ubuntu Resource Creator Script here and run the script manually. Refer to the OS Deployment User's Guide for more information.

Complete the following form and click Take Action:

Parameter name	Parameter value
*Ubuntu Server ISO:	/home/user/ubuntu-18.04.2-server-amd64.iso
Use network share:	No
Destination folder on network share:	//10.10.10.10/c$
User for network share:	Administrator
Domain:	
*Password for network share:	
Security mode:	ntlmssp

Actions

- Click here to deploy this action.

Fill in the fields as explained in the Task description. You must provide the Ubuntu Server ISO file that you downloaded previously. Deploy the action to the Ubuntu machine that you used to download the .ISO file in the first step.

Note:

- [1] Installed genisoimage package is needed to create the Ubuntu resource.
- [2] The Ubuntu Server .iso file specified in the command must be the same point release version of the Ubuntu workstation that you want to provision.

You can also create the Ubuntu Resources manually by downloading and running the resource tool script, as described in Create Ubuntu OS Resources manually *(on page 263)*.

After creating the Ubuntu OS Resource you must import it from the Bundle and Media Manager Dashboard.

Importing Ubuntu OS Resources

From the Bundle and Media Manager dashboard, click **Import Linux OS Resource** in the Deployment Resources tab. Browse to the fully qualified path of the Ubuntu ISO file of the resource you have just created (for example, `OS_Resource_Ubuntu_Server_16.04.2_amd64.iso`) and click **OK**. When the action completes, the Ubuntu Linux OS Resource is displayed in the list. To delete the OS Resource entry, select it and click **Delete**.

Chapter 6. Managing Images

The Manage Images and Drivers node includes tasks to capture, import and manage images for deployment to targets.

You can capture images for Windows and Linux targets, and import images for Windows, Linux and VMware deployments. The topics in the following sections describe how to complete these steps for the operating systems that you plan to deploy.

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.

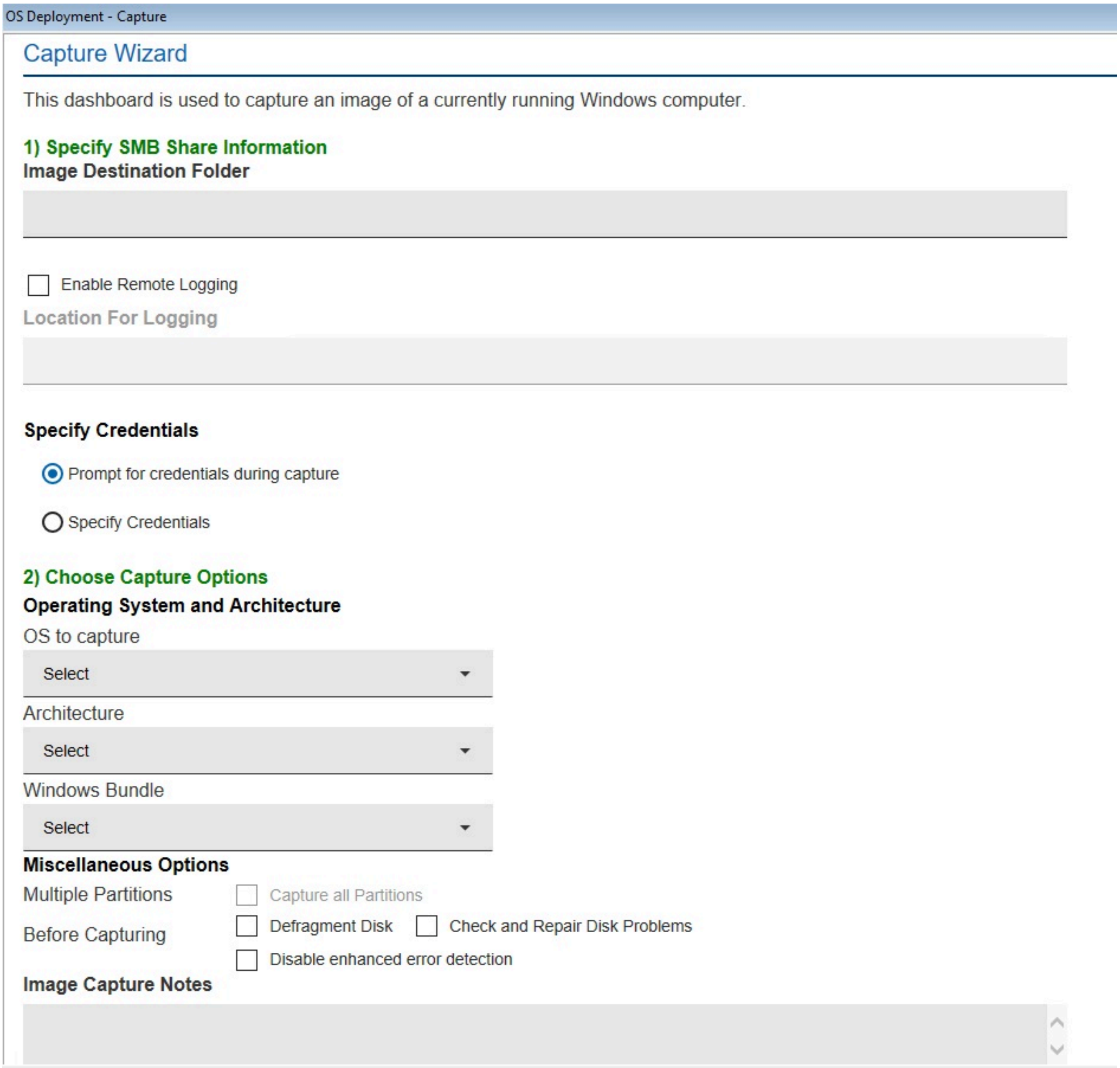
The captured image is stored on a network share, ready to be uploaded to the server into the Image Library.

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

From the **Capture** dashboard wizard, you can specify SMB share information and choose capture options.

The Capture wizard is organized into two sections:

- Specify SMB Share information
- Choose Capture Options



OS Deployment - Capture

Capture Wizard

This dashboard is used to capture an image of a currently running Windows 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: Select

Architecture: Select

Windows Bundle: Select

Miscellaneous Options

Multiple Partitions: □ Capture all Partitions

Before Capturing: □ Defragment Disk □ Check and Repair Disk Problems

□ Disable enhanced error detection

Image Capture Notes

To select the correct Windows Bundle for the Windows version you plan to capture, see Installing Windows Bundle Creators *(on page 68)*.

Capture requirements and restrictions

Check the following requirements and restrictions before you capture an image:

- 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. You must 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 reimage or bare metal deployments.
- Capturing an image on a system with an encrypted disk is not supported. You must decrypt the disk before you begin the capture process.

  Note: Due to default BitLocker pre-provisioning on Windows 11 UEFI devices (TPM/Secure Boot), the drive may report as "Fully Encrypted" even if protection is suspended. To ensure a successful capture, run the following PowerShell command in an elevated session to disable BitLocker on all protected volumes before proceeding: Get-BitLockerVolume | Disable-BitLocker.

- To capture Windows 10 release ID 2004, Windows Bundle 3.10.33 or later is required.
- You need an Windows Bundle originally created using a WinPE 10 2004 or earlier to re-image an x86 operating system.
- Capture of a Windows 10 or Windows 11 image might fail (sysprep error while generalizing the image) if the system has Microsoft Store-based applications (Appx) installed. If one or more of these applications were updated, the capture process might fail to generalize the image. The error log displays which applications are causing the problem. One or more messages similar to the following are logged:

  ```
  Error SYSPRP Package <Package_name> was installed for a user but not provisioned for all users.
  This package will not function properly in the sysprep image.
  ```

  Where *Package_name* is the name of the application that caused the problem. These applications must be uninstalled before you begin the capture process.

  You can list Microsoft Store-based applications by running the following command from a powershell prompt:

  ```
  Get-AppxPackage -AllUsers
  ```

  You can choose to manually uninstall each of the applications that makes the sysprep fail with the following command:

  ```
  Remove-AppxPackage <package name> -AllUsers
  ```

  You can find more details at:

  Sysprep fails after you remove or update Microsoft Store apps that include built-in Windows images

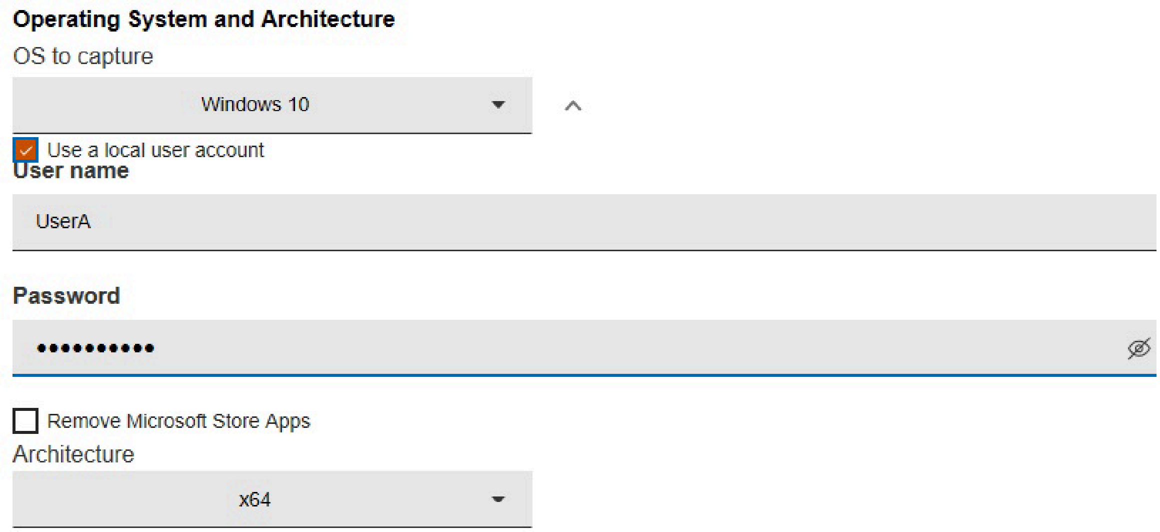
  Alternatively you can run the capture task with the same local user that ran the Microsoft Store-based applications updates. Nevertheless, some of them might need to be uninstalled before successfully capturing the image. You can optionally select the check box to remove the Microsoft Store-based applications during the capture task. For Windows 10, Windows Bundle later than 3.10.21 is required and for Windows 11, you need at least Windows Bundle 3.10.41.

Note: Also the following error might occur if the system has Microsoft Store-based applications (Appx) installed.

```
Error SYSPRP Failed while deleting repository files under
 C:\ProgramData\Microsoft\Windows\AppRepository
```

If this error occurs, run the capture task with the same local user that applied some changes to the AppRepository.

To do this, click the expand icon next to OS to capture when Windows 10/11 is selected, to display the section that allows you to make the choice.



Operating System and Architecture

OS to capture

Windows 10

☑ Use a local user account

User name

UserA

Password

•••••••••••

☐ Remove Microsoft Store Apps

Architecture

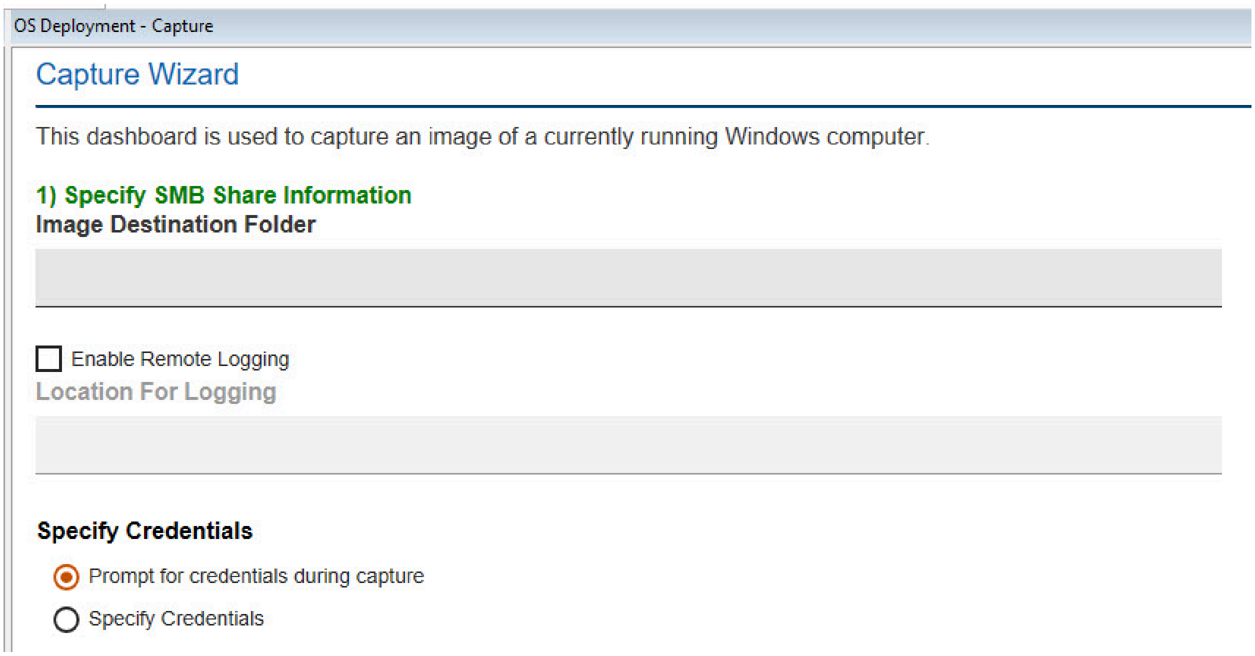
x64

If you select the check box to run the capture with a local user account, you must provide its credentials and the local user must be logged on to the target computer when the capture task is running.

- To capture a Windows Hyper-V *"Generation 1"* virtual machine successfully, you must select the **Disable enhanced error detection** option.
- To capture an image on a UEFI client with the Secure Boot firmware option enabled, you must select the **Disable enhanced error detection** option, and you must use an Windows Bundle with WinPE 4 or later.

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.



OS Deployment - Capture

Capture Wizard

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

1) Specify SMB Share Information

Image Destination Folder

□ Enable Remote Logging

Location For Logging

Specify Credentials

● Prompt for credentials during capture

○ Specify Credentials

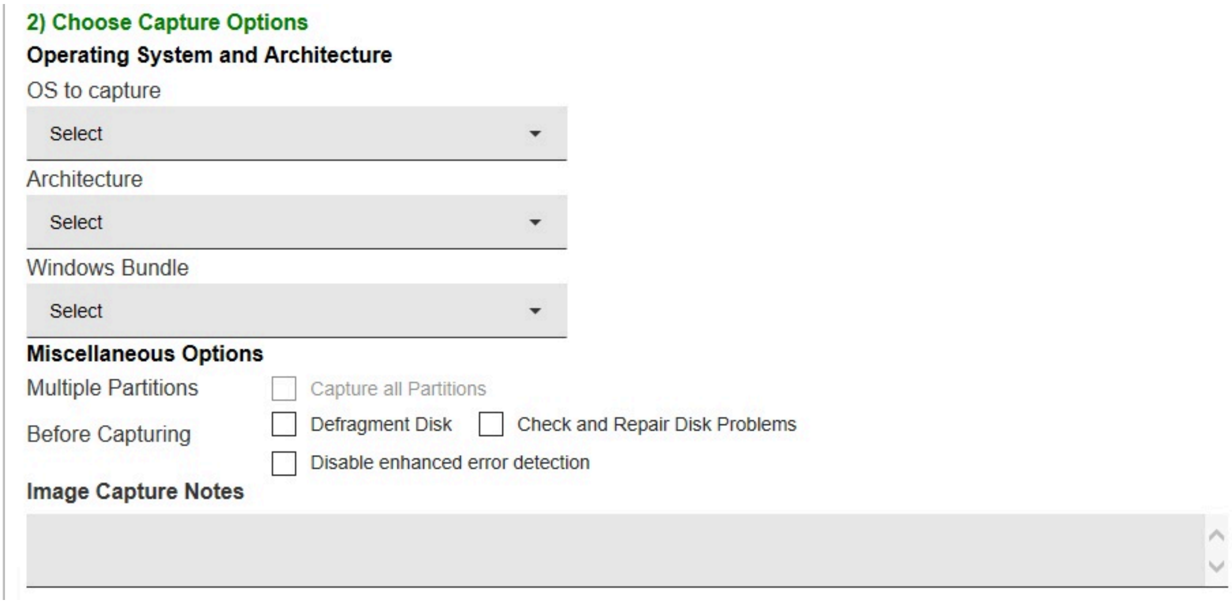
The **Prompt for credentials during capture** option is selected by default, and causes a prompt, to be shown on the endpoint, requesting credentials. This occurs just before the `.wim` file is saved. You can also select the **Specify Credentials** option to identify the appropriate credentials required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

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: Select

Architecture: Select

Windows Bundle: Select

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.

Choose the Windows Bundle to be used during the capture process. Windows 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 Windows 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 Enhanced error detection *(on page 154)*.
- 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.

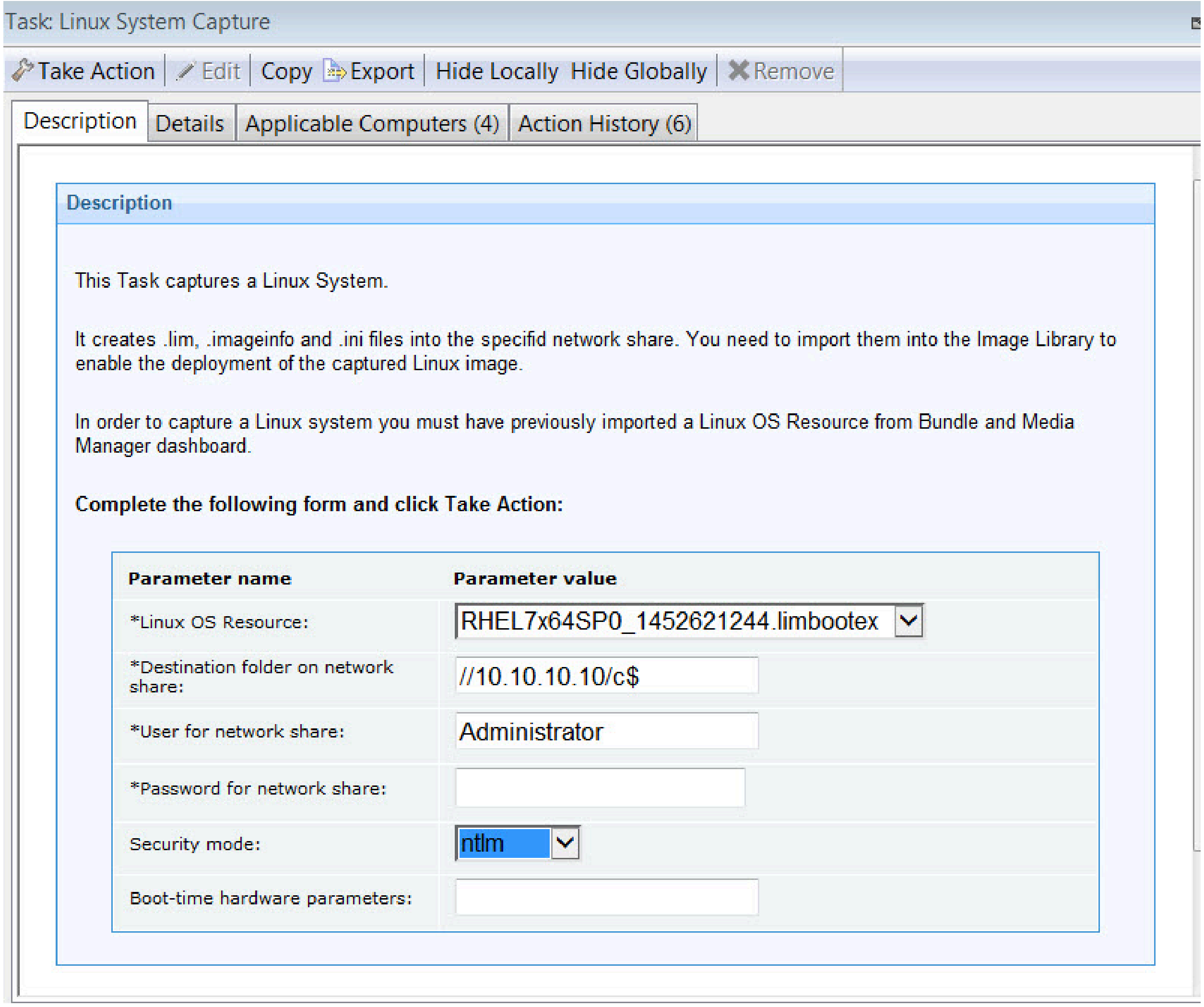
Important:

- To capture an image on a UEFI client with the Secure Boot firmware option enabled, you must select **Disable enhanced error detection** .
- The capture 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.

Capturing Linux images

You can capture a Linux system to create a reference image that can be deployed to bare metal targets.

To capture a Linux system use the **Linux System capture** task (ID 201).



Description

This Task captures a Linux System.

It creates .lim, .imageinfo and .ini files into the specifid network share. You need to import them into the Image Library to enable the deployment of the captured Linux image.

In order to capture a Linux system you must have previously imported a Linux OS Resource from Bundle and Media Manager dashboard.

Complete the following form and click Take Action:

Parameter name	Parameter value
*Linux OS Resource:	RHEL7x64SP0_1452621244.limbootex
*Destination folder on network share:	//10.10.10.10/c$
*User for network share:	Administrator
*Password for network share:	
Security mode:	ntlm
Boot-time hardware parameters:	

The capture task is supported for the following operating systems:

- RedHat Enterprise Linux Versions 6, 7, and 8.
- CentOS Linux Versions 7 and 8.
- SUSE Linux Enterprise Server (SLES) and SUSE Linux Enterprise Desktop (SLED) Versions 12 and 15.
- Linux Ubuntu Desktop Versions 16.04, 18.04, 20.04, and 22.04.

Complete the required fields in the form and take action:

Linux OS Resource

You must have previously imported a Linux OS Resource. If you are capturing a Red Hat Enterprise Linux system, the OS resource must be RHEL Version 7, 8, or 9, even if you are capturing a version 6 system. For SUSE Enterprise Linux systems, you must specify a SLES Version 12 or 15 OS resource. To import a Linux OS Resource, see Managing Linux OS Resources and Deployment Media *(on page 104)*.

To capture a Linux Ubuntu system, you must have previously created and imported an Ubuntu Linux OS Resource. To create and import an Ubuntu resource see Create and Import OS Resources for Linux Ubuntu Deployments *(on page 108)*.

Destination folder on network share

Specify the folder on the network share where the files created by the capture task are stored. The network share folder must be specified in the form `//<IP Address>/<drive_name>`, for example `//192.168.1.232/shared`. The task creates the following files:

- The image files from the captured system (`.lim`)
- The file containing information about the captured image (`.imageinfo`), such as operating system, service pack number, and locale, among others.
- The partition information of the captured system (`.ini`). This information is displayed in the Partition editor section of the bare metal profile,

User for Network Share

Specify the user to access the network share

Password for Network share

Specify the password to access the network share

Security mode

Select the authentication protocol that must be used to access the network share. The default is `ntlm`.

Boot time hardware parameters

Specify any boot time parameters to be provided to the installer.

Important:

- When you prepare your reference machine for the capture task, you must ensure that one of the primary partitions is flagged as bootable.
- You cannot deploy images captured on computers booted in UEFI mode to computers booted in BIOS mode and vice-versa.

After you have successfully captured your Linux system, you must import the image into the Image Library, and create a bare metal profile to deploy the captured image. For further details, see Importing images *(on page 119)*, and Creating Bare Metal Profiles for Linux Images *(on page 200)*.

Requirements and limitations

The following limitations apply to the Linux capture task:

- btrfs file system for capture and deployment of captured images is supported only on SLES/SLED operating systems starting from version 12. For deployment of version 12 up to service pack 4, OS resource version 12 service pack 4 must be used in the bare metal profile.
- Capturing an image on a system with an encrypted disk is not supported.
- XFS and ZFS file systems are not supported for Ubuntu images.
- LVM thin provisioning is not supported.
- If you are capturing a RHEL 8.0 (CentOS 8.0) system with LVM partitions, RHEL 8 (CentOS 8) version 1 resource is required instead of RHEL 8 (CentOS 8) version 0.
- If you are capturing a SUSE Linux Enterprise (SLES) 12 system,
    - it must have at least 200 MB free space in a non-LVM partition and
    - boot directory (/boot) must be on a non-LVM partition.
- If you are capturing an Ubuntu system, a gateway (even fictitious) must be provided to the network. If not, a message will be prompted and you must manually confirm to continue.
- 32-bit physical machines are not supported.
- You can capture 32-bit operating system images running on 64-bit physical machines, but you must use a 64-bit OS resource.
- Capture of LVM volume groups (VG) on multiple physical disks is not supported. If you deploy the resultant image of such capture, there can be issues in the partition sizes as the whole VG is put in a single physical disk.
- Capture of systems with multiple physical disks with different layouts of the partition tables (some MBR and GPT) is not supported.
- MBR partition table on UEFI booted targets is not supported.

Importing images

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

From the **Image Library**, you can upload the following images:

- Windows images that have been previously captured with either the Capture dashboard or manually. (`.wim`), or images uploaded directly from installation media. You cannot import images from installation media (ISO) for Windows 2003 platforms.
- Linux images that you have captured using task 201, or created from installation media (setup).
- VMware ESXi images created from installation media.

Linux and VMware images are identified by the extension `.lim`.

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 124)*.

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

The Origin column displays whether the image was captured (Capture) or imported from installation media (Setup).

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.

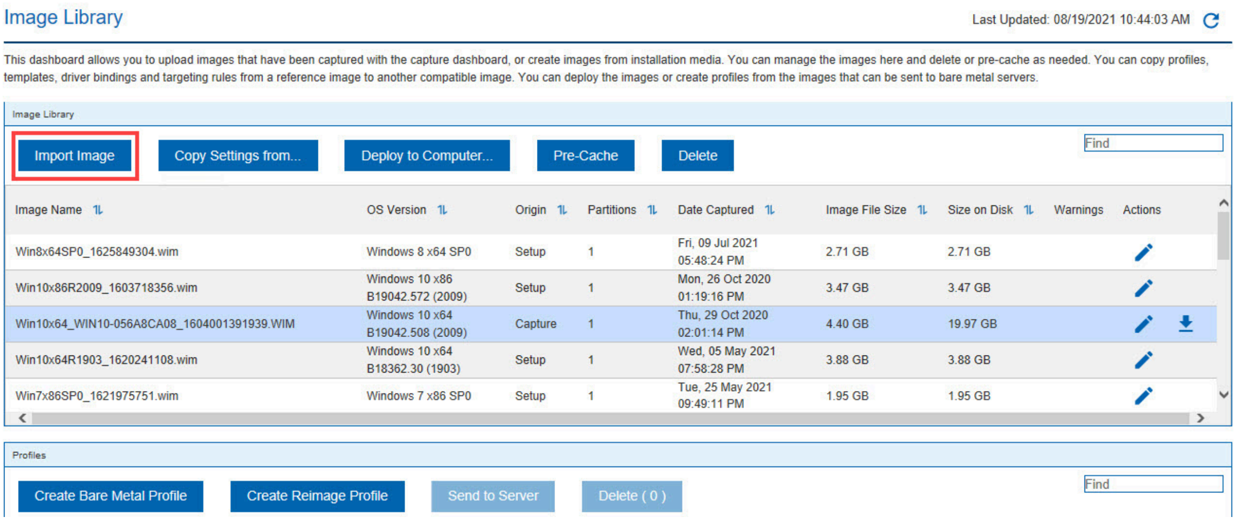


Image Library

Last Updated: 08/19/2021 10:44:03 AM

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 copy profiles, templates, driver bindings and targeting rules from a reference image to another compatible image. You can deploy the images or create profiles from the images that can be sent to bare metal servers.

Image Name	OS Version	Origin	Partitions	Date Captured	Image File Size	Size on Disk	Warnings	Actions
Win8x64SP0_1625849304.wim	Windows 8 x64 SP0	Setup	1	Fri, 09 Jul 2021 05:48:24 PM	2.71 GB	2.71 GB		✎
Win10x86R2009_1603718356.wim	Windows 10 x86 B19042.572 (2009)	Setup	1	Mon, 26 Oct 2020 01:19:16 PM	3.47 GB	3.47 GB		✎
Win10x64_WIN10-056A8CA08_1604001391939.WIM	Windows 10 x64 B19042.508 (2009)	Capture	1	Thu, 29 Oct 2020 02:01:14 PM	4.40 GB	19.97 GB		✎ ⬇
Win10x64R1903_1620241108.wim	Windows 10 x64 B18362.30 (1903)	Setup	1	Wed, 05 May 2021 07:58:28 PM	3.88 GB	3.88 GB		✎
Win7x86SP0_1621975751.wim	Windows 7 x86 SP0	Setup	1	Tue, 25 May 2021 09:49:11 PM	1.95 GB	1.95 GB		✎

In the import image menu, select the type of image you want to import. You can import images captured from a Windows (`.wim`) or Linux (`.lim`) reference machine, or images from installation media (ISO).

Important: Reimaging is not supported on WMware ESXi targets.

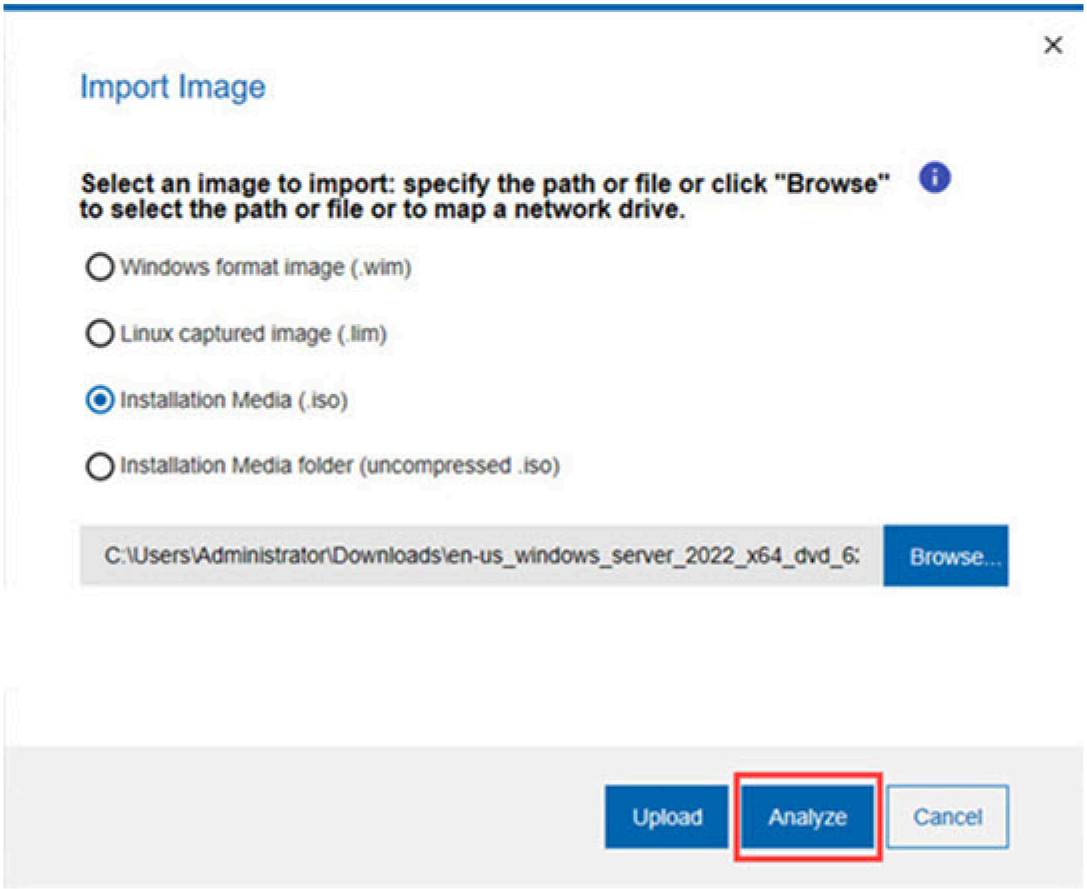
Importing images from installation media

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

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 pop-up.

Note: For SLE15 SP0 and SP1, ensure that you merge the Installer ISO with Package ISO. For information on the procedure, see SUSE official documentation at https://documentation.suse.com/sbp/all/single-html/SBP-SLE15-Custom-Installation-Medium/.

To import an image, browse to locate the image file or folder on your computer and click **Analyze**.



Import Image

Select an image to import: specify the path or file or click "Browse" to select the path or file or to map a network drive.

○ Windows format image (.wim)

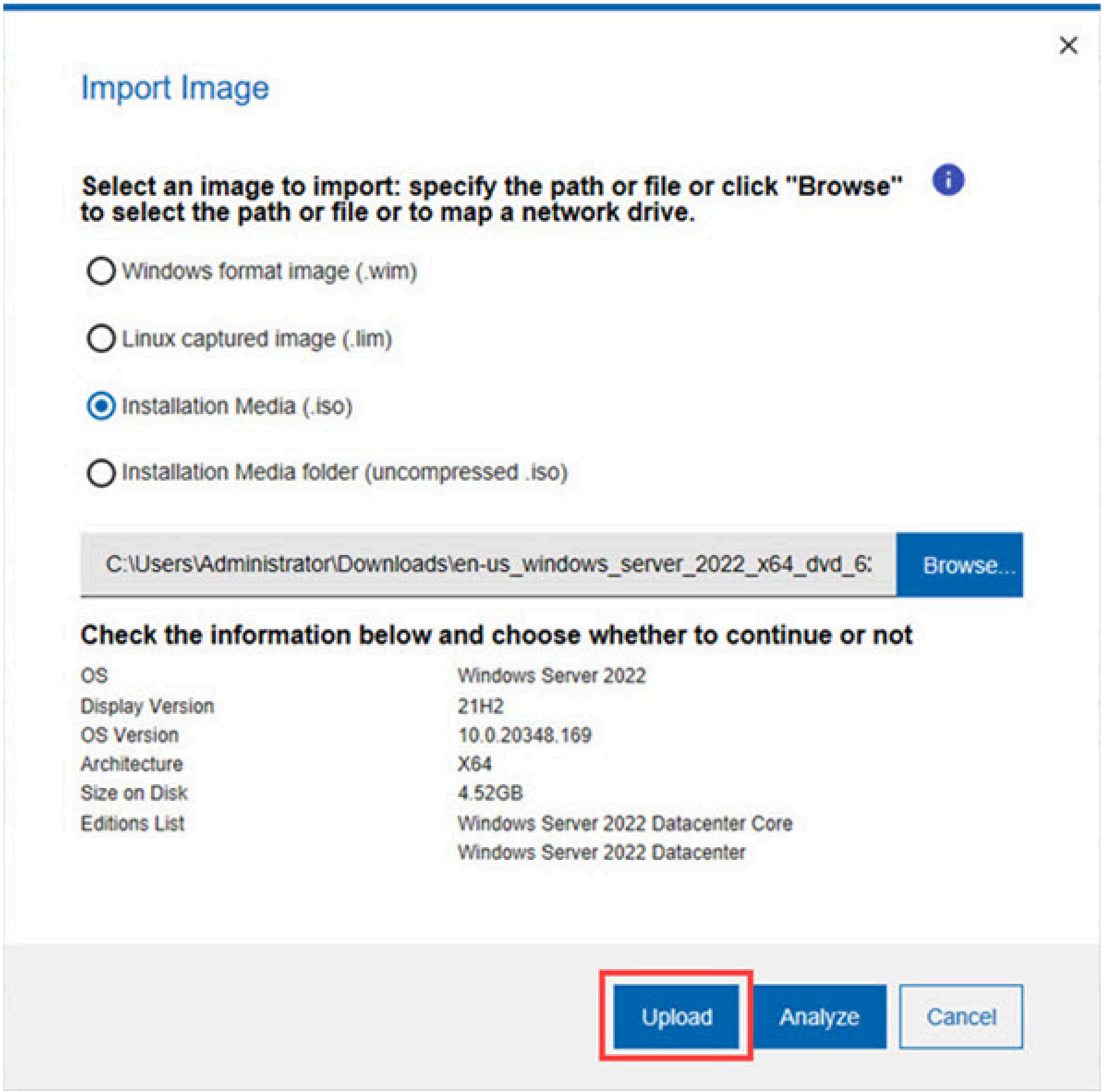
○ Linux captured image (.lim)

● Installation Media (.iso)

○ Installation Media folder (uncompressed .iso)

C:\Users\Administrator\Downloads\en-us_windows_server_2022_x64_dvd_6:

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. OS resources contained in the image are automatically uploaded, if not already present.



Import Image

Select an image to import: specify the path or file or click "Browse" to select the path or file or to map a network drive.

○ Windows format image (.wim)

○ Linux captured image (.lim)

● Installation Media (.iso)

○ Installation Media folder (uncompressed .iso)

C:\Users\Administrator\Downloads\en-us_windows_server_2022_x64_dvd_6:

Check the information below and choose whether to continue or not

OS	Windows Server 2022
Display Version	21H2
OS Version	10.0.20348.169
Architecture	X64
Size on Disk	4.52GB
Editions List	Windows Server 2022 Datacenter Core Windows Server 2022 Datacenter

Note: For `.wim` and `.lim` files, clicking **Analyze** analyzes and uploads the images without any addition input.

Check the information and click **Upload** to begin importing the image, or **Cancel** to quit.

A message will be displayed at the top of the Import Image window stating that "The image is now uploading in the background". Once the image is successfully uploaded the procedure is completed.

Important:

- If you are importing a Windows 10 image from installation media in `.esd` format generated with the Microsoft Media Creation Tool, the image must contain a single architecture (x86 or x64), not both, else the import operation fails.
- Simple bootable Linux iso images that have the behavior of a network installation when deployed cannot be imported as setup images in the Image Library. For example, the Red Hat *"`boot.iso`"* images, such as RHEL-6.8-20160414.0-Server-x86_64-boot ISO, and SUSE *"`mini-iso` "* images, such as SLE-12-Server-MINI-ISO-x86_64-GM-DVD.iso cannot be used to create Setup images in the Image Library Dashboard.

Requirements for importing Windows 10 and Windows 11 images

You can import Windows 10/11 `.iso` files that contain compressed images in the `.esd` file format, if you have the correct level of deployment tools for the operating system on which the BigFix Console runs. The following BigFix Console requirements apply:

- Console running on a Windows 8.1 or Windows 2012 R2 system or later, with any WADK 10.
- Console running on a Windows system with WADK 10.
- Console running on a Windows 10/11 or Windows 2016/2019 system.

To successfully import Windows 10/11 (non `.esd`) images, the following BigFix console requirements apply:

- Console running on a system with Windows 7 or later.
- Console running on any Windows system where WADK 10 is installed. If the installed WADK 10 version is 1709 or later, the Console must be on a system with Windows 8.1 or later.
- Console running on a Windows 10/11 or Windows 2016/2019 system.

Importing captured Windows images

You can import images that you have previously captured using the Capture dashboard or that you have captured manually. 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 driver descriptor file and/or the image descriptor file is missing, the import process automatically creates it.

Important: If you import a manually captured image containing multiple partitions, ensure you have run the Sysprep command with the generalize option.

Importing captured Linux images

To import a Linux image that you have previously captured using task 201, click **Import image**, select **Linux captured image (.lim)** and specify the fully qualified path to the captured image. Click **Analyze** . When the analysis completes, the import process begins. Click **OK**.

Copying configuration settings from a Windows reference image

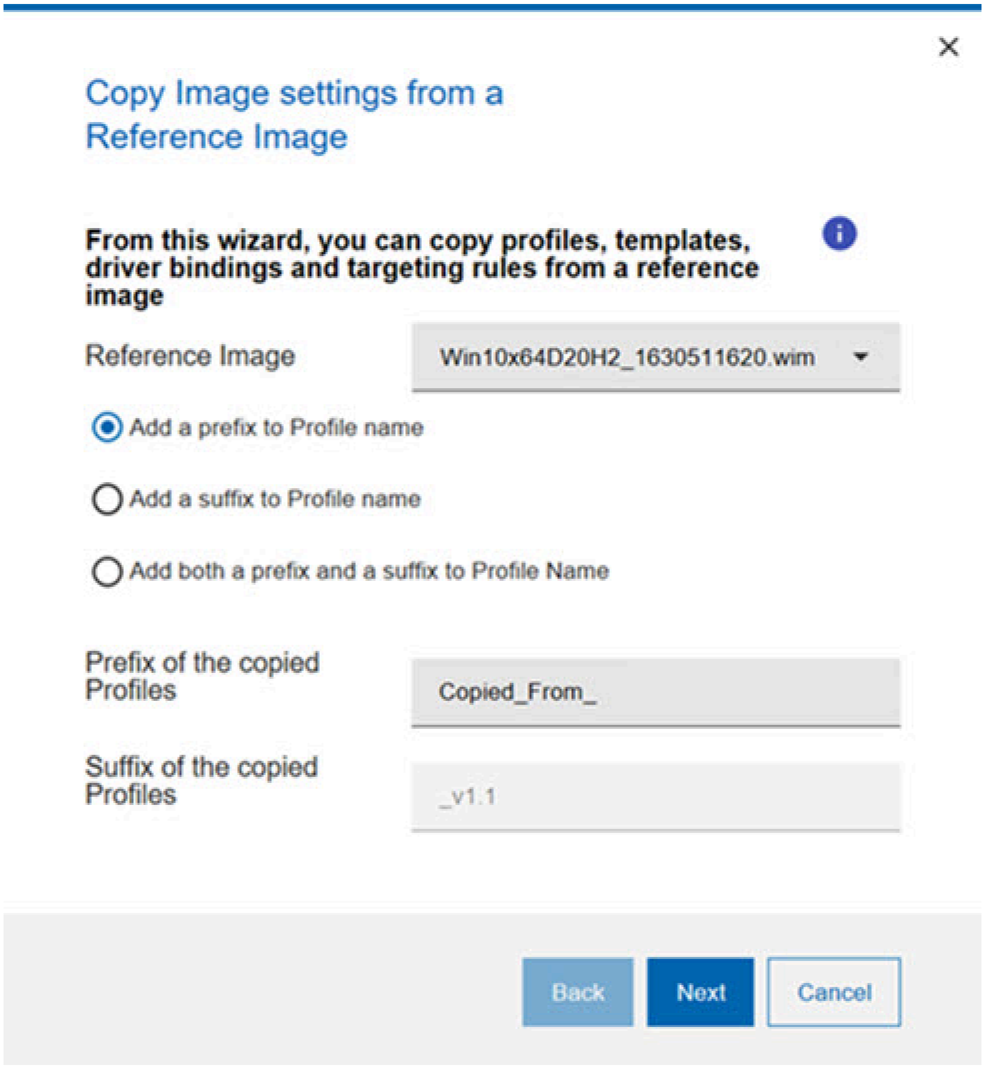
For Windows images, you can copy configuration settings such as Bare Metal Profiles, templates, and driver binding grids, from an existing image to another compatible image. The configuration settings are copied only if the following compatibility conditions are met:

- 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, a suffix, or both for the profile names to be used when they are copied on the target image.



Copy Image settings from a Reference Image

From this wizard, you can copy profiles, templates, driver bindings and targeting rules from a reference image

Reference Image: Win10x64D20H2_1630511620.wim

● Add a prefix to Profile name

○ Add a suffix to Profile name

○ Add both a prefix and a suffix to Profile Name

Prefix of the copied Profiles: Copied_From_

Suffix of the copied Profiles: _v1.1

Note: If you have specified either a prefix, suffix, or both, and the resulting profile name exceeds 70 alphanumeric characters, the name is shortened to the maximum allowed length.

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.

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 249)*.

Patching Windows Capture Images

The Image Library Dashboard enables patching of Windows capture images using cumulative updates from the Microsoft Update Catalog (.msu files). A band-aid button in the Actions column initiates the patching process, creating a new image while preserving the original. If a new servicing stack is required, it must be applied first, and users can copy settings from compatible reference images to maintain profiles and templates.

The **Image Library** Dashboard allows you to patch a Windows capture image that has already been imported with an applicable cumulative update from **Microsoft Update Catalog** (`.msu files`).

For the Windows capture image, a band-aid button is available in the **Actions** column.

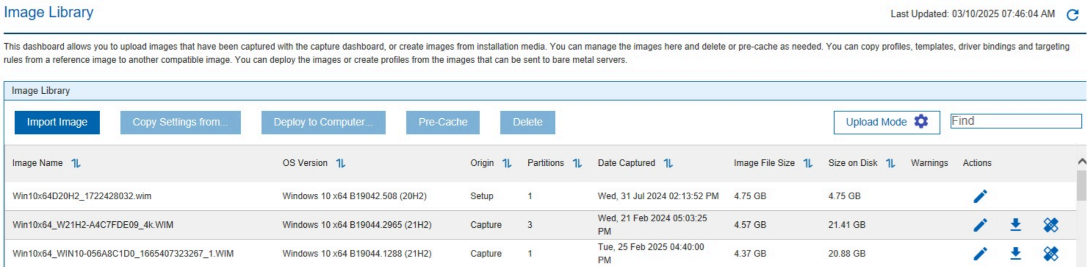


Image Library

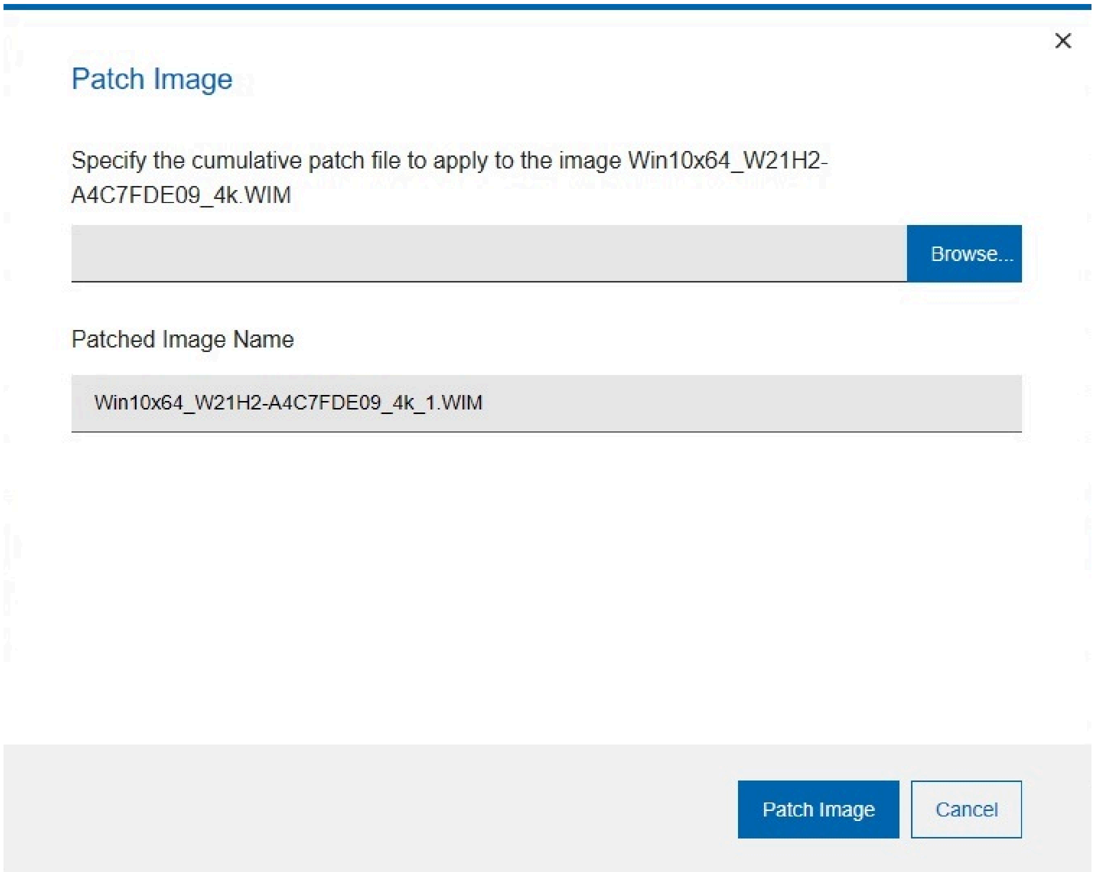
Last Updated: 03/10/2025 07:46:04 AM

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 copy profiles, templates, driver bindings and targeting rules from a reference image to another compatible image. You can deploy the images or create profiles from the images that can be sent to bare metal servers.

Image Library

Image Name	OS Version	Origin	Partitions	Date Captured	Image File Size	Size on Disk	Warnings	Actions
Win10x64D20H2_1722428032.wim	Windows 10 x64 B19042.508 (20H2)	Setup	1	Wed, 31 Jul 2024 02:13:52 PM	4.75 GB	4.75 GB		
Win10x64_W21H2-A4C7FDE09_4k.WIM	Windows 10 x64 B19044.2965 (21H2)	Capture	3	Wed, 21 Feb 2024 05:03:25 PM	4.57 GB	21.41 GB		
Win10x64_WIN10-056A8C1D0_1665407323267_1.WIM	Windows 10 x64 B19044.1288 (21H2)	Capture	1	Tue, 25 Feb 2025 04:40:00 PM	4.37 GB	20.88 GB		

It will start a panel where you can provide the file to use to apply a cumulative update downloaded from **Microsoft Update Catalog** (`.msu files`) to your capture image and the name of the image that will be created.



Patch Image

Specify the cumulative patch file to apply to the image Win10x64_W21H2-A4C7FDE09_4k.WIM

Patched Image Name

Win10x64_W21H2-A4C7FDE09_4k_1.WIM

At the end of the patch activity, a new entry will be added to the image library referring to the new image while the original image will not be modified.

If the image to patch requires a new servicing stack to be applied before being able to apply the patch content, and the servicing stack is not included in the same cumulative patch, you must apply to servicing stack as first, a new image will be added to the image library containing the new servicing stack, and the cumulative patch can be applied on it.

The new image will not have any bare metal profile, reimage profile, and template on it but you can use the **Copy Settings from...** feature (see Copying configuration settings from a Windows reference image *(on page 124)*) to copy all the bare metal profiles, reimage profiles and templates from a compatible reference image, including the image it has been created from.

Chapter 7. Upload Mode

By default, the OS images are permanently stored in the BigFix root server.

In some environment, where the BigFix root server is in remote (for example, in a cloud environment or it has a slow connection with the network where the OS images are imported and deployed) this would require a significant time to complete their upload process at the time of import and their download at the time of deployment. This also results in a significant usage of network between BigFix root server and the local network, where the image are coming from and finally dispatched to.

In this case, it is possible to configure the **Upload Mode** to store the OS images in a local network permanently instead of BigFix root server. Using a primary local repository to store the master copies of the OS images and the local caches of some specified local relays that are at the top of the network areas, where these relays will be used as a local repositories.

Note:

1. Files other than OS images (for example, Windows drivers or OS resources) will be handled in a **Standard Mode**, using the BigFix root server as a permanent file repository.
2. With the local repositories, you have the maximum advantage of reduced network usage and time when uploading or downloading images when the console is running in the local network. Also, when the console is running in the remote network, you have an advantage using the local relay repositories with a direct connection to the primary local repository.

Configuring Local Repositories Upload Mode

This topic helps you to configure and switch to Local Repositories Upload Mode.

To configure and switch to the Local Repositories Upload Mode, on the Image Library dashboard, click **Upload Mode**.

Figure 1. Image Library dashboard

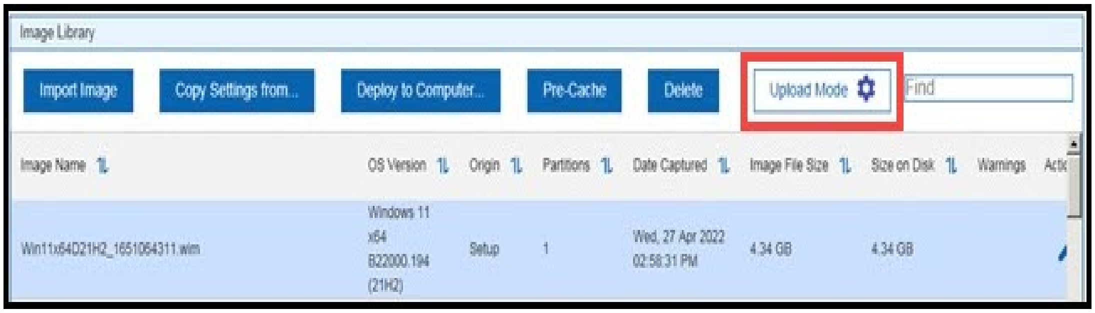
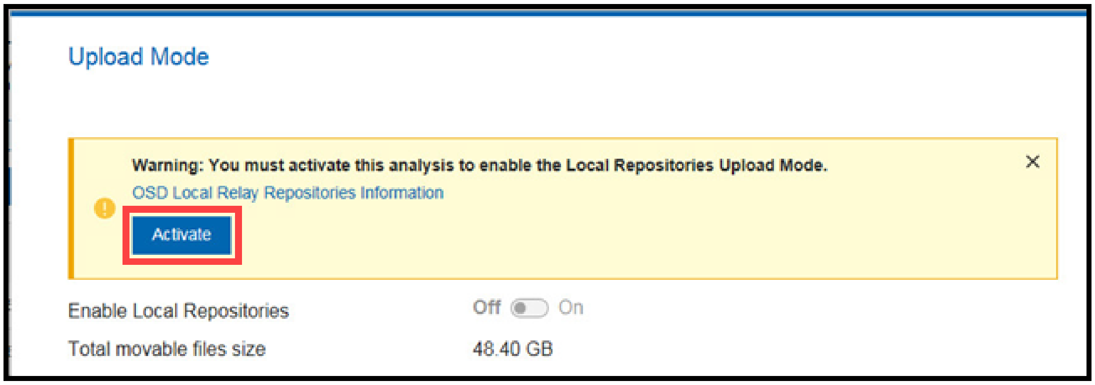


Image Name	OS Version	Origin	Partitions	Date Captured	Image File Size	Size on Disk	Warnings	Actic
Win11x64D21H2_1651064311.wim	Windows 11 x64 B22000.194 (21H2)	Setup	1	Wed, 27 Apr 2022 02:58:31 PM	4.34 GB	4.34 GB		

Important: The analysis `“OSD Local Relay Repositories Information” (55)` must be enabled to use Upload Mode wizard.

If the analysis is not activated, a warning notification is displayed to activate the analysis. To enable the analysis, click **Activate**.

Figure 2. Activate analysis warning



Upload Mode

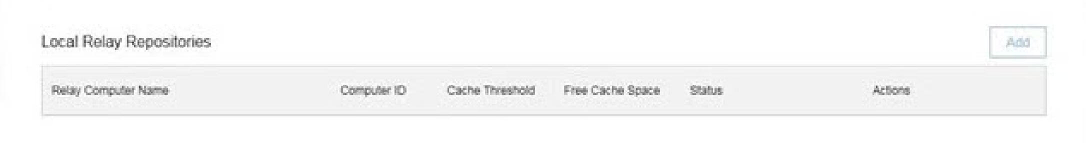
Warning: You must activate this analysis to enable the Local Repositories Upload Mode.
OSD Local Relay Repositories Information

Enable Local Repositories: Off ○ On

Total movable files size: 48.40 GB

When the analysis **"OSD Local Relay Repositories Information" (55)** is activated, you can configure the Local Repositories Upload Mode.

Figure 3. Local Repositories Upload Mode configuration environment.



Local Relay Repositories

Relay Computer Name	Computer ID	Cache Threshold	Free Cache Space	Status	Actions

Note: When the Local Repositories Upload Mode is enabled, the total size of the OS image that have been already imported in your Image Library is reported in the wizard and it will be moved to the local repositories.

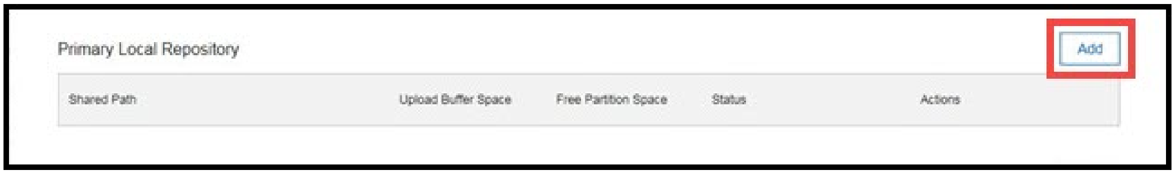
Note: You must use a dedicated folder for the primary repository of the local repositories upload mode and it must not contain any external file or folder.

Adding a primary local repository

You can start the configuration by adding the Primary Local Repository. You can possibly define some relays to work as local repositories for the OS images at deployment time for the target computers that are below them in the download chain.

Complete the following steps to add a primary local repository:

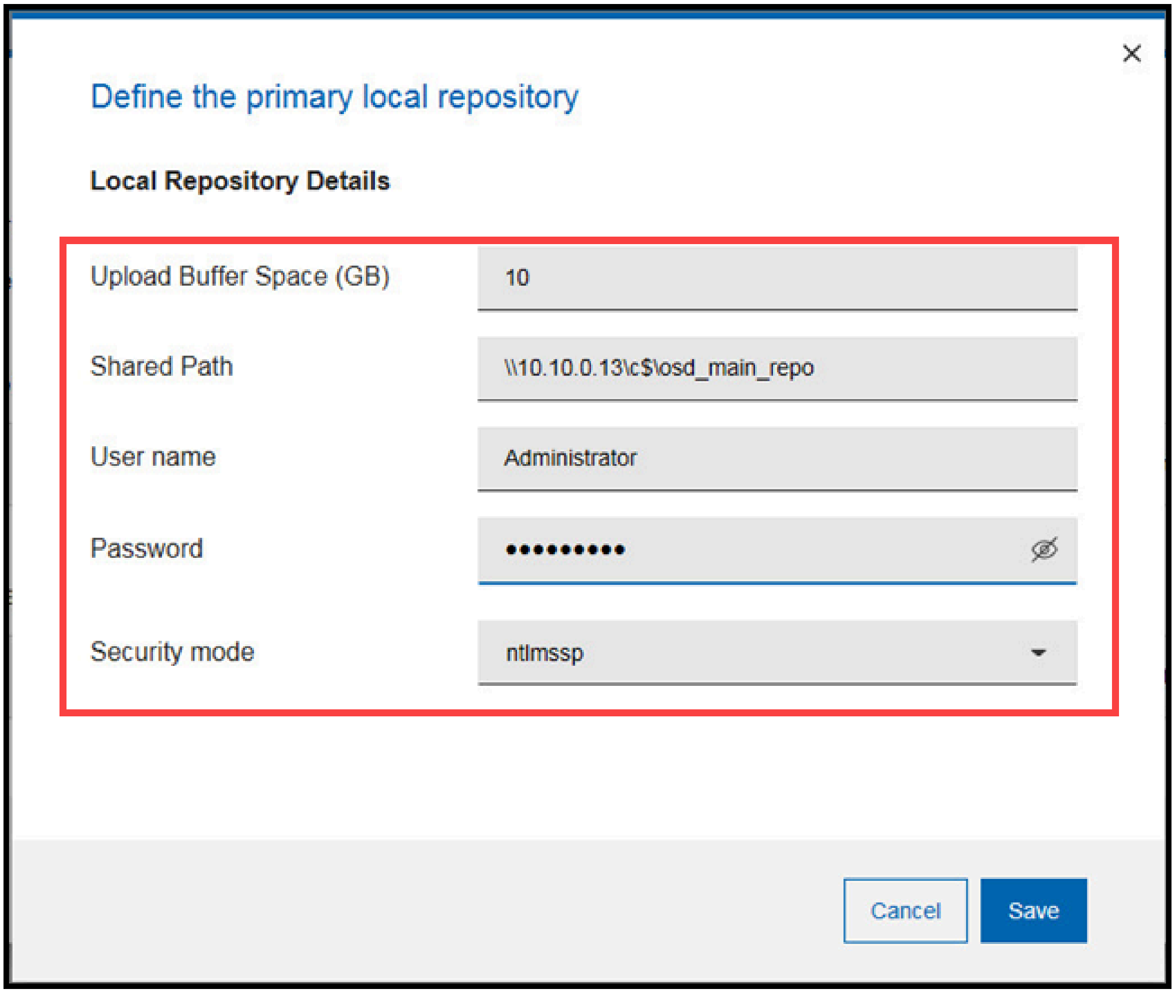
1. Click **Add** button on the Primary Local Repository section.



Primary Local Repository

Shared Path	Upload Buffer Space	Free Partition Space	Status	Actions

2. Define the following Primary local repository parameters:



Define the primary local repository

Local Repository Details

Upload Buffer Space (GB)	10
Shared Path	\\10.10.0.13\c$\osd_main_repo
User name	Administrator
Password	••••••••••
Security mode	ntlmssp

Upload Buffer Space (GB)

The minimum buffer space size in GB on primary local repository partition and on relay repository caches to allow the upload of a new OS image. By default, it is 10 GB.

Shared Path

The writable samba shared network folder that works as primary local repository. It must be reachable from the console computer where the Local Repository Upload Mode is being configured.

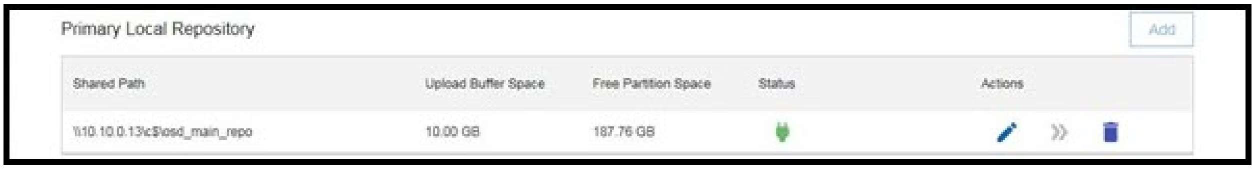
User name and Password

The user credentials to connect to the shared path.

Security mode

Applicable only in the case of Linux local relay repositories with direct connection to the primary local repository share. This security mode is used to mount it via samba client.

When a Primary Local Repository definition is saved, the connection with the provided details is tested and the status of the test is reported in the **Status** column.



Primary Local Repository

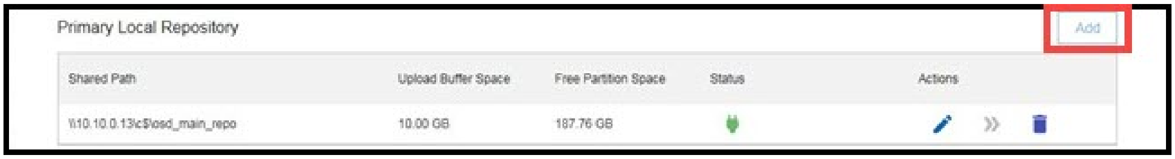
Shared Path	Upload Buffer Space	Free Partition Space	Status	Actions
\\10.10.0.13\c$\osd_main_repo	10.00 GB	187.76 GB	🔌	✎ » 🗑

When the primary local repository is configured, if its connection has been successfully tested, a green icon 🔌 is displayed in the Status column. The local repositories upload mode can be enabled, if this has enough space to contain the OS images already imported in the environment.

Adding the Local relay repositories

You can optionally configure the local relay repositories before enabling the Local Repository Upload Mode or define them later. To deploy the OS image on the target computer, a relay cache must contain the OS image in its download chain.

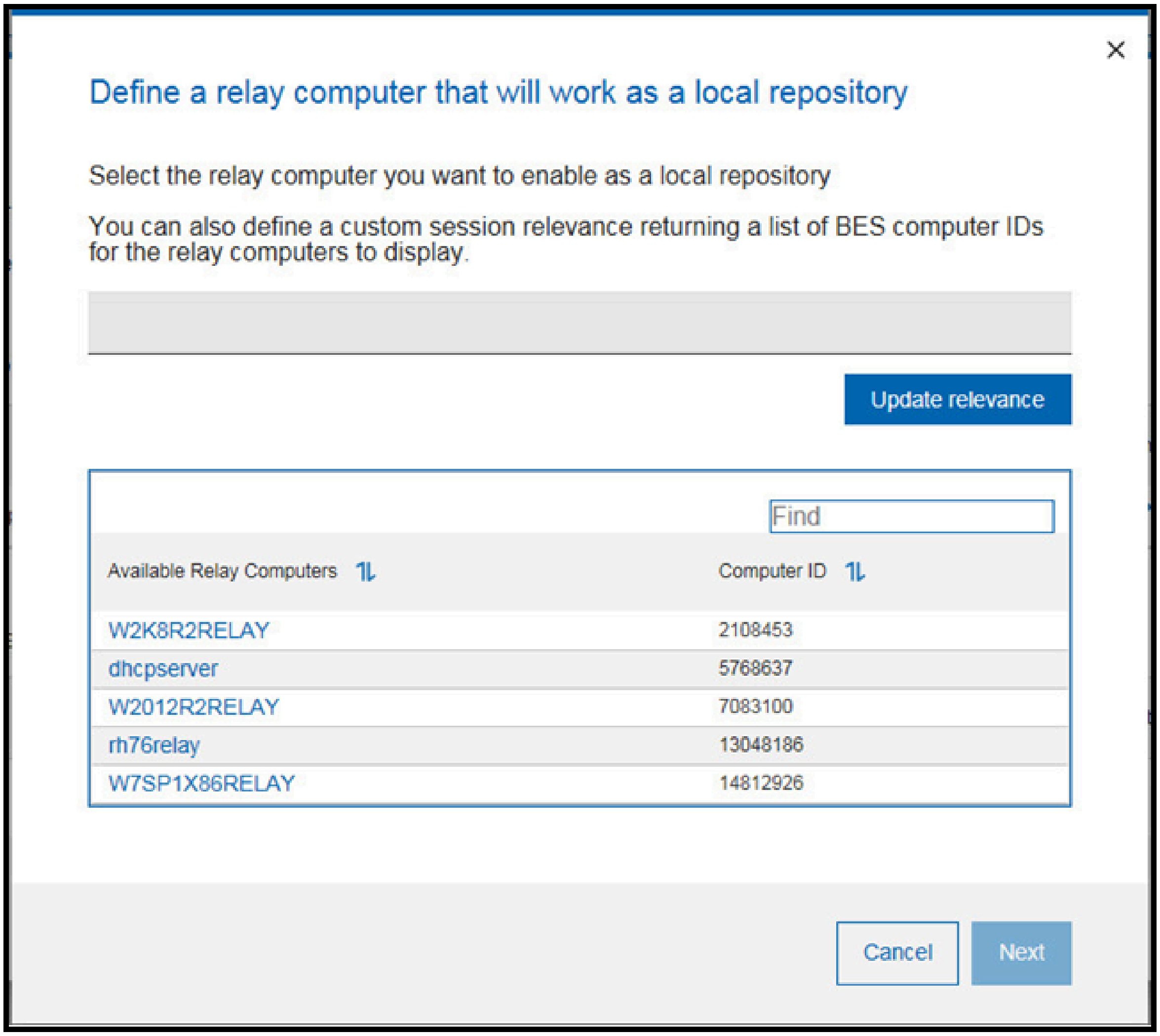
1. Click **Add** on the Local Relay Repositories section.



Primary Local Repository

Shared Path	Upload Buffer Space	Free Partition Space	Status	Actions
\\10.10.0.13\c$\osd_main_repo	10.00 GB	187.76 GB	🔌	✎ » 🗑

A wizard opens and displays all the relay computers that are subscribed to the OS Deployment and Bare Metal Imaging site. Select the desired relay computer to define it as the local repository.



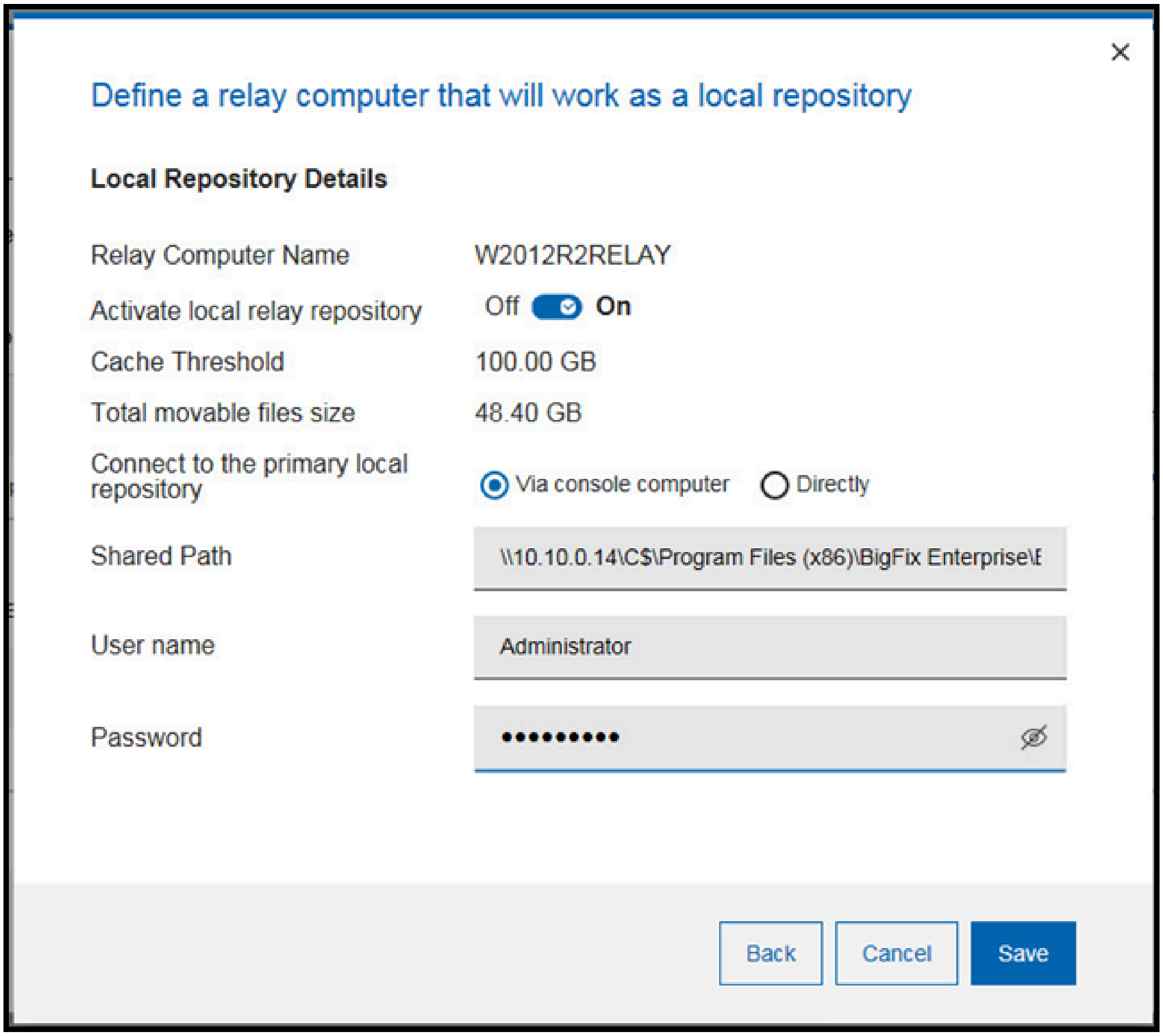
Define a relay computer that will work as a local repository

Select the relay computer you want to enable as a local repository

You can also define a custom session relevance returning a list of BES computer IDs for the relay computers to display.

Available Relay Computers	Computer ID
W2K8R2RELAY	2108453
dhcpserver	5768637
W2012R2RELAY	7083100
rh76relay	13048186
W7SP1X86RELAY	14812926

2. You can optionally define a custom session relevance to filter them. You can select a relay computer and click on **Next**.
3. Use On/Off toggle switch to enable or disable the local relay repository.



Define a relay computer that will work as a local repository

Local Repository Details

Relay Computer Name	W2012R2RELAY
Activate local relay repository	Off ● On
Cache Threshold	100.00 GB
Total movable files size	48.40 GB
Connect to the primary local repository	● Via console computer ○ Directly
Shared Path	\\10.10.0.14\C$\Program Files (x86)\BigFix Enterprise\E
User name	Administrator
Password	••••••••••

An active local relay repository is automatically synchronized with the OS images on the primary local repository during the following scenarios:

- when enabling the Local Repositories Upload Mode.
- when a new OS image is uploaded when the Local Repositories Upload Mode is enabled.

A local relay repository can work with two different types of connection to the primary local repository:

Via console computer

The samba connection to the local relay repository cache will be carried out from the console computer to copy/delete/synchronize OS images from primary local repository and to check the following factors:

a. If the connection can be established
b. Cache free space
c. OS images present

Provide the Shared Path, User name, and Password to access the relay http server root (wwwrootbes) directory. Ensure it is a writable samba shared network folder. It must be reachable from the console computer where the Local Repository Upload Mode is being configured.

The Shared Path field is pre-filled with a default string, but it must be checked and eventually changed to the correct one.

When the Local Relay Repository definition is saved, the connection with the provided information is tested and its status is reported in real time in the Status column.

Direct

The connection to the primary local repository will be established directly from the relay computer through a BigFix client action to copy/delete/synchronize OS images from the primary local repository when these tasks are run. The information on free space and OS images cached is displayed when the result of the `analysis 55` is reported. The Shared Path, User name and Password fields are disabled and not needed for this type of connection.

Upload Mode status and actions

Read this topic to understand the status and actions of Primary Local Repositories and Local Relay Repositories in Upload Mode.

The following screenshot contains two local relay repositories:

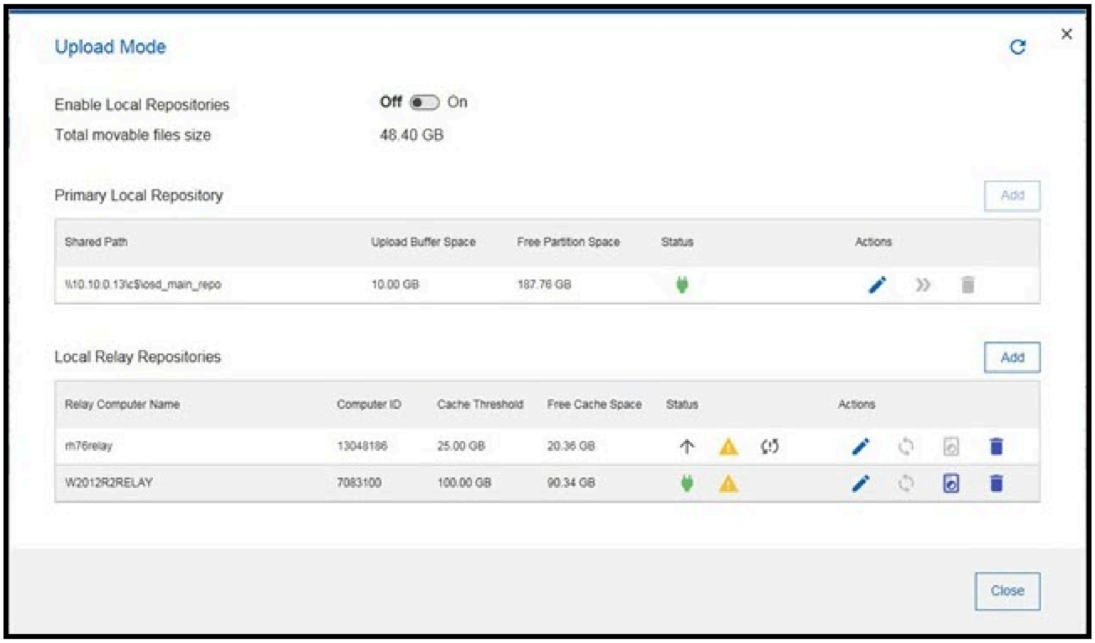
- one with direct connection ↑ and
- one with connection via console computer whose status has been successfully tested 🔌

The relay repository with connection via console has been also activated, while the relay repository with direct connection is not active (!). Both the relay repositories report that they do not have all the OS images in their cache ⚠.

The check on the OS images present in the relay cache is done even when the Local Repositories Upload Mode is not enabled. If all the OS images are present a green check is displayed ✓. This means that if a target computer needs to download any of the OS image files from that relay computer or from any relay computer in its download chain below, this relay will provide that file without making a download request to its download chain above.

Note: An error will be displayed in the Downloads section of the actions containing the prefetch of an image stored in local repositories, reporting a download error (404: Not Found). This happens because the BigFix root server cannot retrieve that file locally. By the way, the action will be completed and the image will be available for download to the target computers that have a local relay repository that stores that image in their download chain.

Figure 4. Status in Upload Mode



Enable Local Repositories: Off ○ On

Total movable files size: 48.40 GB

Primary Local Repository

Shared Path	Upload Buffer Space	Free Partition Space	Status	Actions
\\10.10.0.13\c$\osd_main_repo	10.00 GB	187.76 GB	🔌	✎ » 🗑

Local Relay Repositories

Relay Computer Name	Computer ID	Cache Threshold	Free Cache Space	Status	Actions
rh76relay	13048186	25.00 GB	20.36 GB	↑ ⚠ ⟳	✎ ⟳ 🗑
W2012R2RELAY	7083100	100.00 GB	90.34 GB	🔌 ⚠	✎ ⟳ 🗑

These are possible statuses reported for the repositories, move your cursor on the status icon for more information.

Connection status

- 🔌 : the local relay repository uses the connection to the primary local repository via console computer and it has been successfully established using the credentials provided in its details (light green).
- 🔌: the local relay repository uses the connection to the primary local repository via console computer, it has been found already established and has been successfully validated (dark green).
- 🔌: the local relay repository uses the connection to the primary local repository via console computer and it has been successfully validated but there's a warning.
- 🔌: the local relay repository uses the connection to the primary local repository via console computer but there's an error trying to verify it.
- ↑ : the local relay repositories use the direct connection to the primary local repository.

Files check status

- ✓: All the files of OS images in the Image Library have been found in the local relay repository cache.
- ⚠ : Not all the files of OS images in the Image Library have been found in the local relay repository cache or the information is not available.

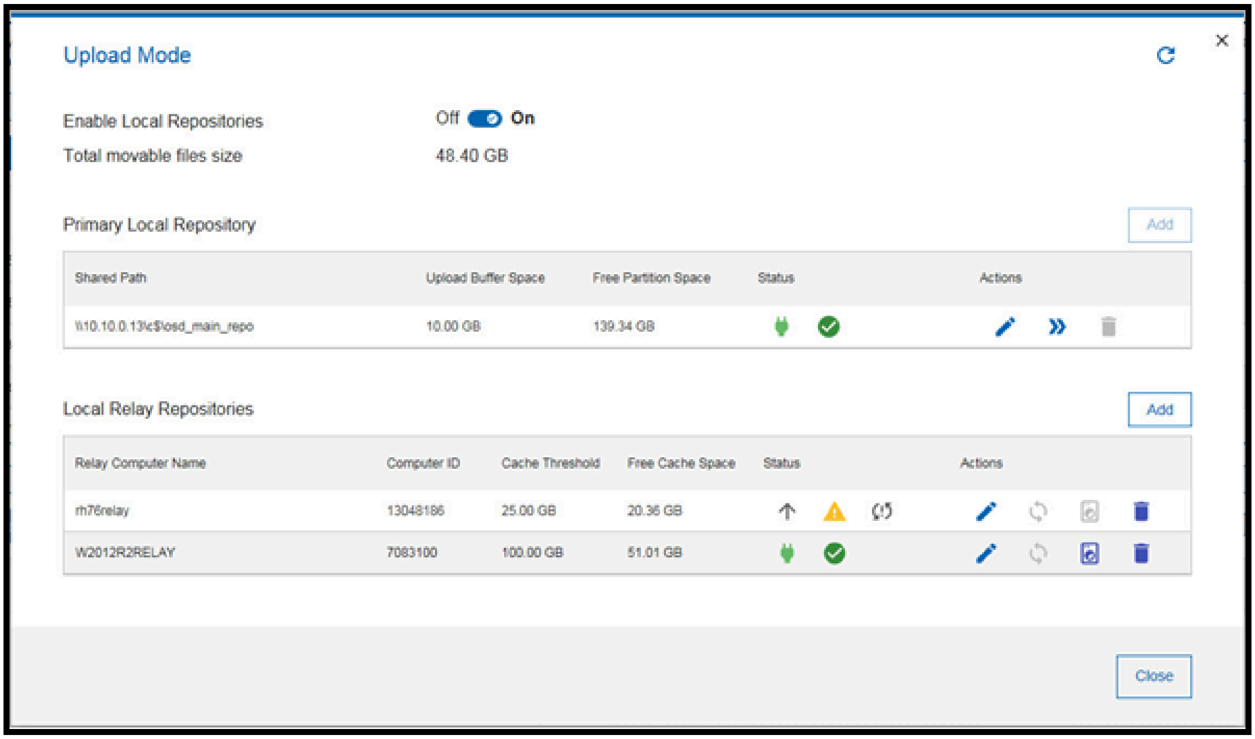
Activation status

- ⟲! : The local relay repository is not active for automatic cache files synchronization, when the Local Repositories Upload Mode is enabled or a new OS image is uploaded.
- No icon is displayed if the local relay repository is active.

General status:

❗ : There is an error on the local repository.

Some actions are available for both primary and relay repositories. This is how Upload Mode wizard appears after enabling the Local Repositories Upload Mode in the same previous environment with two local relay repositories, where only one of them is active.



Upload Mode

Enable Local Repositories: Off / On

Total movable files size: 48.40 GB

Primary Local Repository

Shared Path	Upload Buffer Space	Free Partition Space	Status	Actions
\\10.10.0.13\c$\osd_main_repo	10.00 GB	139.34 GB	✓	

Local Relay Repositories

Relay Computer Name	Computer ID	Cache Threshold	Free Cache Space	Status	Actions
rh76relay	13048186	25.00 GB	20.36 GB	↑ ⚠ ⟲!	
W2012R2RELAY	7083100	100.00 GB	51.01 GB	✓	

Primary Local repository

- ✎ : Edit the primary local repository definition.
- » : Move the primary local repository to a different shared path, moving all the files (next paragraph).
- 🗑 : Delete the primary local repository definition. It can be deleted only if no local relay repositories are defined and local repositories upload mode is not enabled.

Local relay repository

- ✎: Edit the local relay repository definition.
- 🔄: Synchronize the local relay repository cache files with the primary local repository. This button is enabled if the local relay repository misses any of the files in the primary local repository. This can happen if the relay repository is not active or not reachable when a new image is imported or when the Local Relay Repository Upload Mode is enabled, or if the relay cache logic deletes some of the OS image files.
- ▣: Clean the relay cache. This button is enabled if some file in the relay cache is not identified as related to bare metal profiles that have been send to bare metal server or saved reimage templates. If you run clean, those files are deleted from the relay cache to reduce the possibility that the relay cache threshold is reached and then the relay cache logic deletes some file. Clean option can be used only by a Master operator.
- 🗑: Delete the local relay repository definition.

A check on the local repositories is done when you open the Upload Mode wizard or add or edit one of the local repositories. You can also run a new check clicking on the refresh icon ↻.

Moving Primary Local Repository

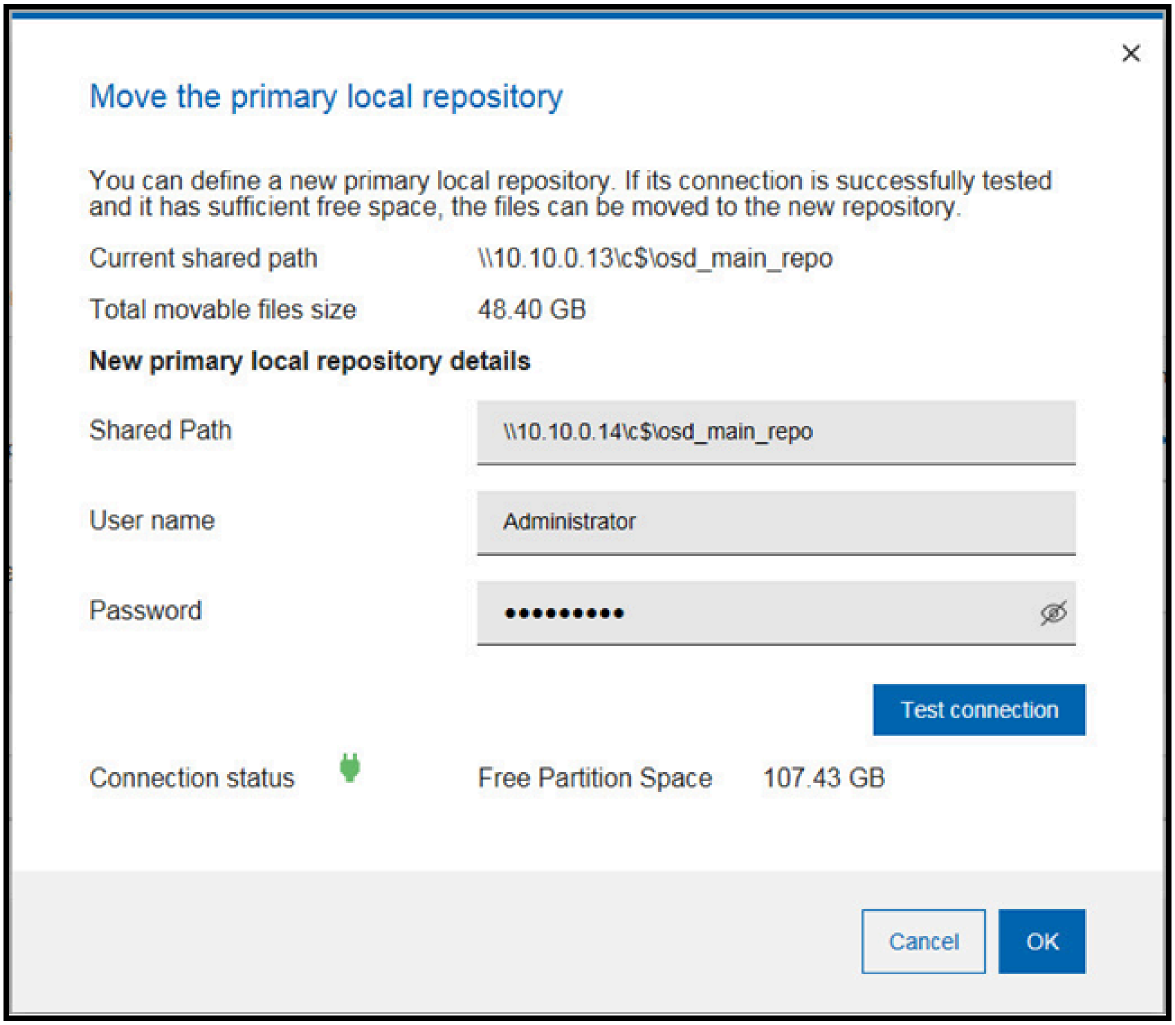
The Upload Mode wizard allows you to move the Primary Local Repository to a different shared path.

Perform the following to move the primary local repository to a different shared path:

- Manually move the files from the primary local repository location to a new location and then **Edit** ✎ the primary local repository definition to update it.

Or

- Use the **Action** feature to move the files. By clicking the » icon a wizard is prompted. Fill the **Shared Path**, **User name**, and **Password** with the details of the new primary local repository and click **Test Connection**.



Move the primary local repository

You can define a new primary local repository. If its connection is successfully tested and it has sufficient free space, the files can be moved to the new repository.

Current shared path \\10.10.0.13\c$\osd_main_repo

Total movable files size 48.40 GB

New primary local repository details

Shared Path \\10.10.0.14\c$\osd_main_repo

User name Administrator

Password ●●●●●●●●●

Connection status 🔌 Free Partition Space 107.43 GB

If the Connection status is successfully tested 🔌 and the free partition space is at least as the total movable files size, you can start moving the files by clicking **OK**.

Importing, deleting, and downloading images

You can perform various action such as import, delete and download from the image library dashboard.

If the Local Repositories Upload Mode is enabled, you can import, delete, or download an image from the console only if the check is successful. Otherwise, your Local Repositories must be verified in the Upload Mode wizard.

Figure 5. Image Library dashboard

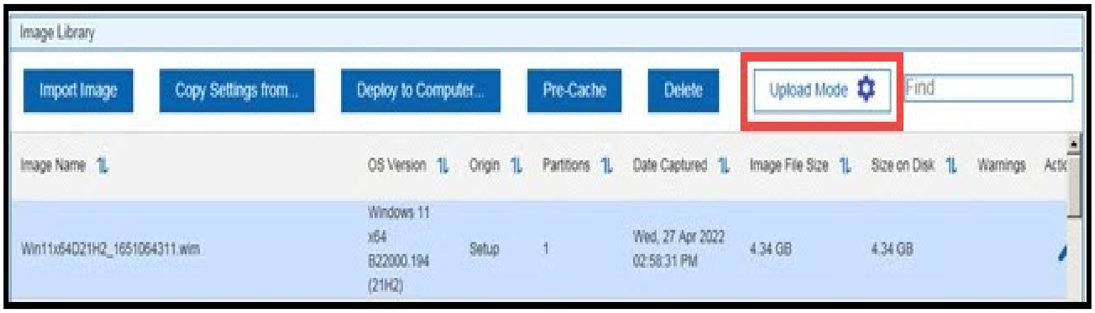


Image Name	OS Version	Origin	Partitions	Date Captured	Image File Size	Size on Disk	Warnings	Actic
Win11x64D21H2_1651064311.wim	Windows 11 x64 B22000.194 (21H2)	Setup	1	Wed, 27 Apr 2022 02:58:31 PM	4.34 GB	4.34 GB		

Chapter 8. Reimaging

Reimaging 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 reimage Windows or Linux systems by choosing previously uploaded images from the **Image Library**.

When you reimage a computer you can upgrade the operating system or install a later service pack, but you cannot downgrade architectures or operating systems. For example, you cannot reimage from Windows 8 to Windows 7 (independently of the architecture), and you cannot deploy a 32-bit image on a target running a 64-bit operating system.

On Windows systems, you cannot reimage a server class operating system to a client class operating system and vice-versa.

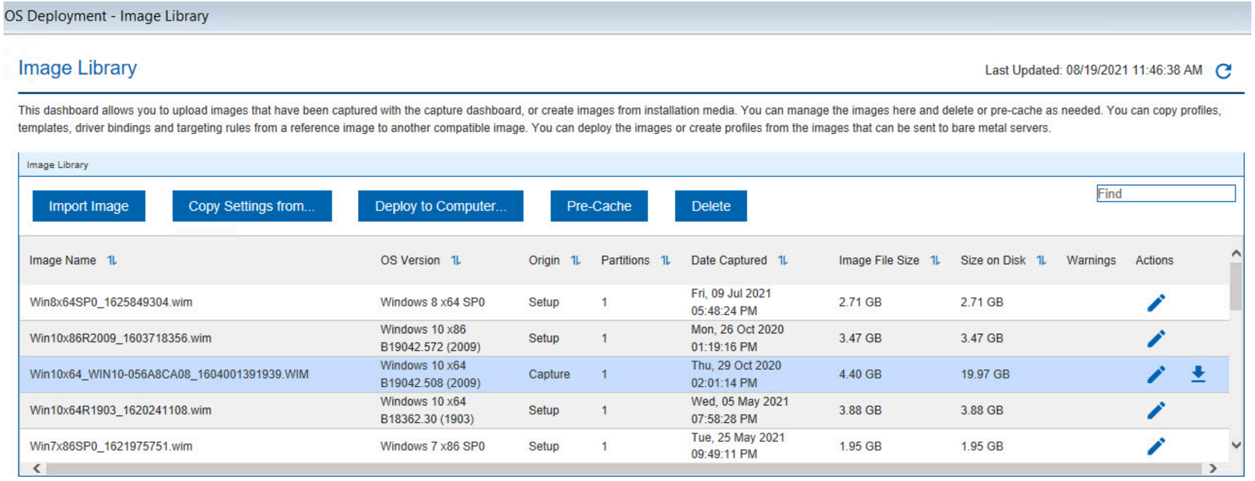
On Windows systems, reimaging can be completed using multicast distribution if your network infrastructure supports it. To reimage in multicast, the targets must be connected to relays that are also Bare Metal Servers, and at least one reimage profile must be available for the image you want to deploy.

Reimaging a Linux system means refreshing the Operating System on a computer with an active BigFix Client. The machine identity is preserved during the migration.

On Linux systems, reimaging requires the Linux Image provider component which you must install on those relays that manage the targets that you want to reimage. 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 40)*.

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



Last Updated: 08/19/2021 11:46:38 AM

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 copy profiles, templates, driver bindings and targeting rules from a reference image to another compatible image. You can deploy the images or create profiles from the images that can be sent to bare metal servers.

Image Name	OS Version	Origin	Partitions	Date Captured	Image File Size	Size on Disk	Warnings	Actions
Win8x64SP0_1625849304.wim	Windows 8 x64 SP0	Setup	1	Fri, 09 Jul 2021 05:48:24 PM	2.71 GB	2.71 GB		
Win10x86R2009_1603718356.wim	Windows 10 x86 B19042.572 (2009)	Setup	1	Mon, 26 Oct 2020 01:19:16 PM	3.47 GB	3.47 GB		
Win10x64_WIN10-056A8CA08_1604001391939.WIM	Windows 10 x64 B19042.508 (2009)	Capture	1	Thu, 29 Oct 2020 02:01:14 PM	4.40 GB	19.97 GB		
Win10x64R1903_1620241108.wim	Windows 10 x64 B18362.30 (1903)	Setup	1	Wed, 05 May 2021 07:58:28 PM	3.88 GB	3.88 GB		
Win7x86SP0_1621975751.wim	Windows 7 x86 SP0	Setup	1	Tue, 25 May 2021 09:49:11 PM	1.95 GB	1.95 GB		

Depending on whether you are reimaging Windows or Linux, the options you can customize are described in Reimaging Windows Systems *(on page 141)*, Reimaging Windows Systems in multicast *(on page 160)*, and Reimaging Linux Systems *(on page 166)*.

Reimaging Windows Systems

You can specify different options which will affect the reimaging process on the target.

The reimaging process on Windows systems does not re-partition the disk on the target system. To reimage 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.

Before deploying Windows 11, check the system requirements at https://www.microsoft.com/en-us/windows/windows-11-specifications.

You can reimage Windows targets in multicast, using either captured images or ISO images. To complete this task see Reimaging Windows Systems in multicast *(on page 160)*.

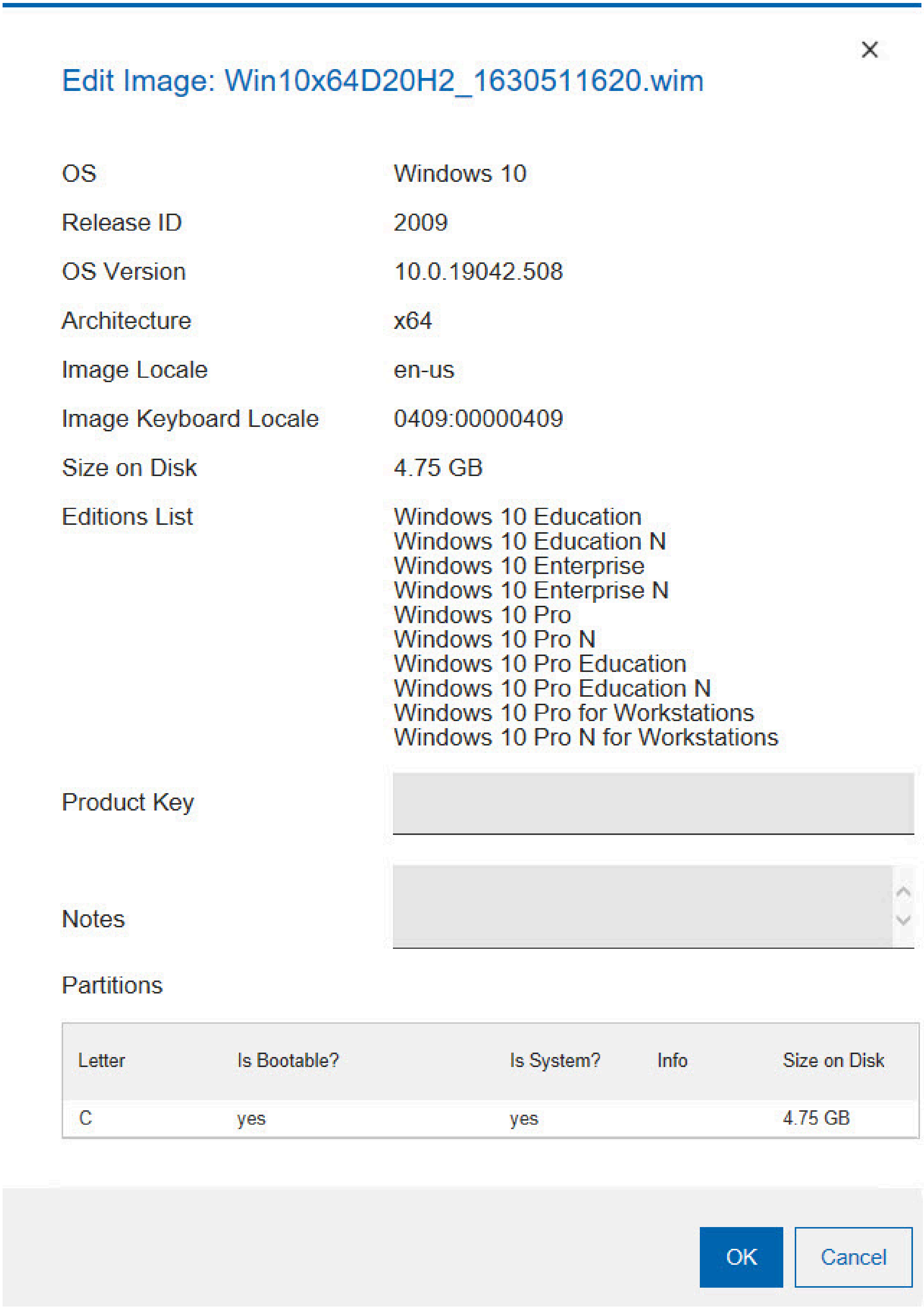
To reimage a Windows system from the Image Library, you have these options:

- Edit an image that was previously imported, and deploy it to one or more targets.
- 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 reimaging.
- 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 Product Key and Notes.



Edit Image: Win10x64D20H2_1630511620.wim

OS	Windows 10
Release ID	2009
OS Version	10.0.19042.508
Architecture	x64
Image Locale	en-us
Image Keyboard Locale	0409:00000409
Size on Disk	4.75 GB
Editions List	Windows 10 Education Windows 10 Education N Windows 10 Enterprise Windows 10 Enterprise N Windows 10 Pro Windows 10 Pro N Windows 10 Pro Education Windows 10 Pro Education N Windows 10 Pro for Workstations Windows 10 Pro N for Workstations
Product Key	
Notes	

Partitions

Letter	Is Bootable?	Is System?	Info	Size on Disk
C	yes	yes		4.75 GB

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

The following **Partition** 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 zero-indexed in this view.

Managing multiple partitions for captured images

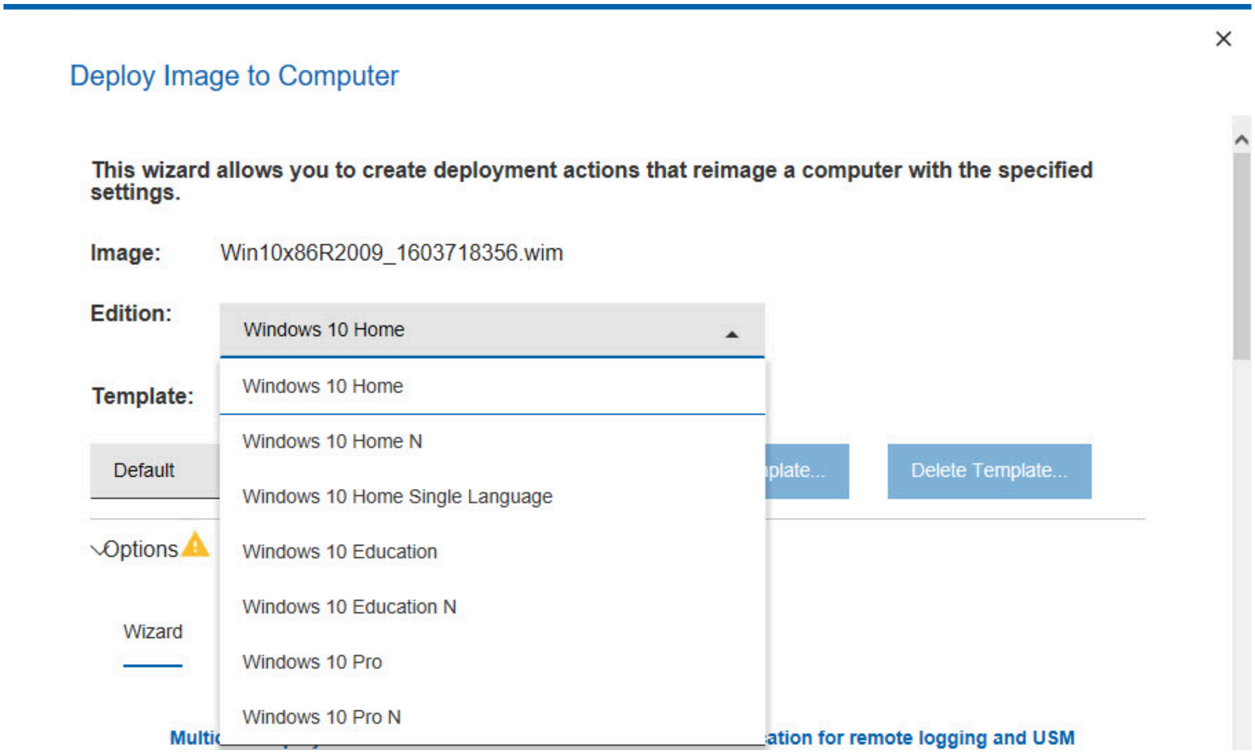
If your source image is multiple-partitioned, you can:

- Capture multiple partitions in a single .WIM file to enable the support of multi-partition master images.
- During a reimage, 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.



Deploy Image to Computer

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

Image: Win10x86R2009_1603718356.wim

Edition: Windows 10 Home

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

Note: When you reimage a computer whose disk is encrypted with Bitlocker protection, the Bitlocker protection is suspended to run the deployment task. After the reimage deployment task completes, you must manually resume the BitLocker protection or restart the computer to automatically resume it.

Deploying an image to a target computer

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

The **Deploy Image to Computer** wizard sets specific parameters, including multicast options, migration settings, miscellaneous options, and credentials. You can deploy an image to a computer either using the wizard or manually. To reimage a computer in multicast, you must create a reimage profile as described in Reimaging Windows Systems in multicast *(on page 160)*.

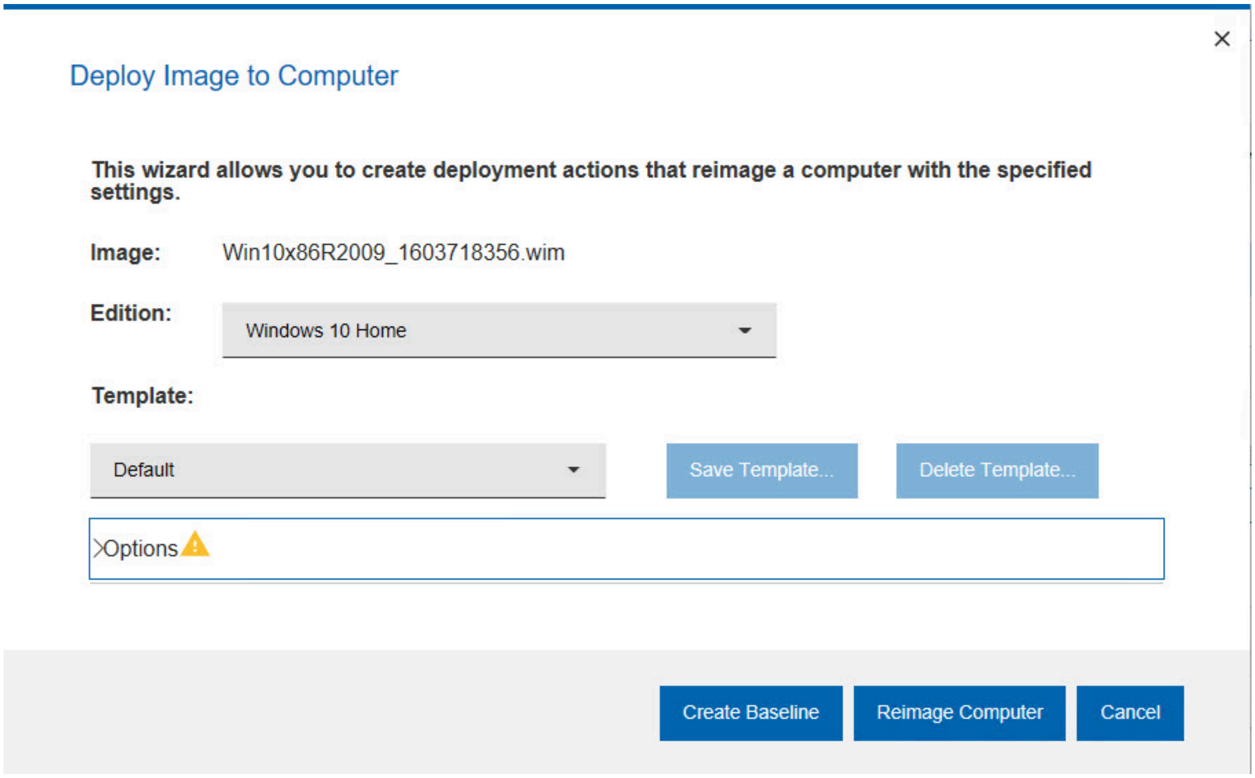
To proceed manually, select the **Manual** tab to manually edit the `customsettings.ini` file that is generated from fields specified in the **Wizard** tab. Changes made in the file make fields in the **Wizard** tab non-editable and manual changes must be undone to be able to make changes in the **Wizard** 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 reimage deployments:



Deploy Image to Computer

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

Image: Win10x86R2009_1603718356.wim

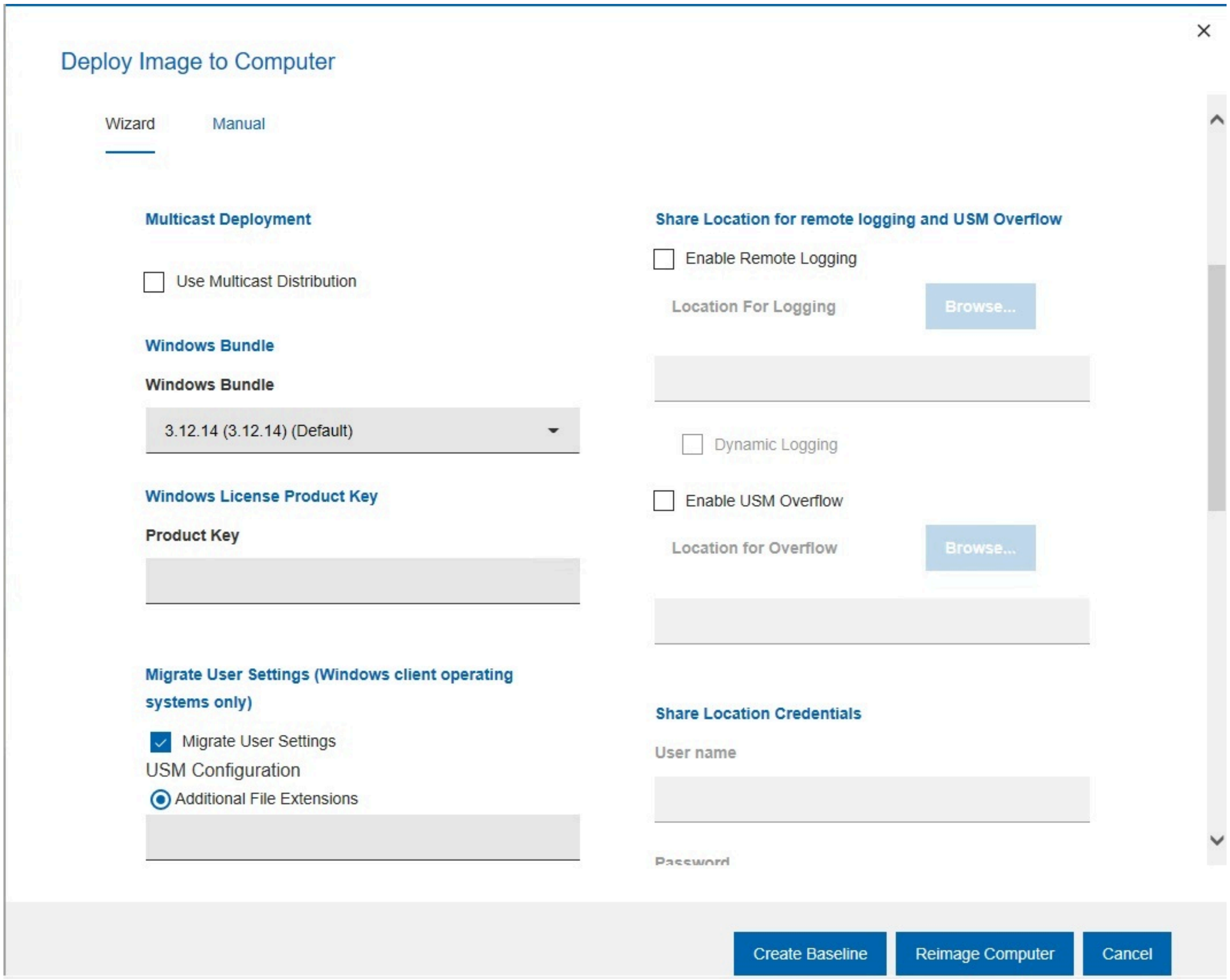
Edition: Windows 10 Home

Template: Default

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 reimage. When you have made the required changes, you can save the template, and either create a reimage action by clicking **Reimage computer** or create a reusable baseline by clicking **Create Baseline**.

Each component of the **Wizard** tab is explained in the following sections.



Deploy Image to Computer

Wizard Manual

Multicast Deployment

□ Use Multicast Distribution

Windows Bundle

Windows Bundle: 3.12.14 (3.12.14) (Default)

Windows License Product Key

Product Key:

Migrate User Settings (Windows client operating systems only)

☑ Migrate User Settings

USM Configuration

● Additional File Extensions

Share Location for remote logging and USM Overflow

□ Enable Remote Logging

Location For Logging

□ Dynamic Logging

□ Enable USM Overflow

Location for Overflow

Share Location Credentials

User name

Password

Requirements and limitations

The reimaging process is influenced by different components, such as source and destination operating systems, the Windows Bundle used, and by user and domain settings. One or more of the following requirements or restrictions may apply, depending on your specific selection:

1. You cannot reimage a system with an encrypted disk. You must decrypt the disk before deploying the image on the target system, or else the reimaging fails.
2. When you deploy a captured image, if the BES client version installed on the target computer is earlier than the version contained in the image, the reimaging completes successfully. However, if you upgrade the BES client on the target computer at a later time using the upgrade Fixlet, this operation might fail. To solve the problem, manually upgrade the client on the target where the upgrade has failed by using the *Repair* option.
3. You cannot reimage a Server class operating system on a client class operating system or vice-versa.
4. Reimaging to Windows 10 requires that the source operating system must have BigFix client version 9.2.5 or later installed before you start the reimaging process.
5. Reimaging from Windows 10 release ID 2004 requires Windows Bundle 3.10.33 or later.

6. Reimaging to Windows Server 2016, 2019 or 2022 requires that the source operating system must have BigFix client version 9.5.3 or later.
7. If you are reimaging a Windows Hyper-V "Generation 1" virtual machine, you must disable enhanced error detection for the task to complete successfully.
8. To reimage a UEFI client with the Secure Boot firmware option enabled, you must disable enhanced error detection in the Miscellaneous Options section of the wizard . WinPE 4 or later is required in the Windows Bundle.
9. You need an Windows Bundle originally created using a WinPE 10 2004 or earlier to re-image an x86 operating system.
10. Reimaging to Windows Server 2025 requires that the source operating system must have BigFix client version 11.0.3 or later.

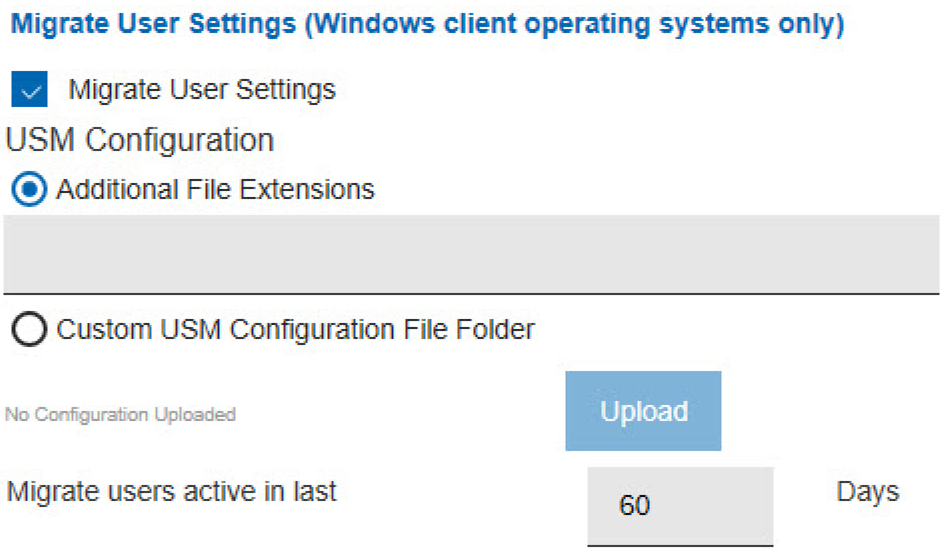
Windows License Product Key

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 reimaging process begins.



Migrate User Settings (Windows client operating systems only)

☑ Migrate User Settings

USM Configuration

● Additional File Extensions

○ Custom USM Configuration File Folder

No Configuration Uploaded

Migrate users active in last 60 Days

The *Migrate User Settings* capability captures multiple user profile directories from a system about to be reimaged. In most cases, the profile data stays on the migrated system. However, if 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 reimaging and that do not already exist in the image that you are deploying, are migrated and set to disabled on the reimaged 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 operating systems. When you select server class operating systems, 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.

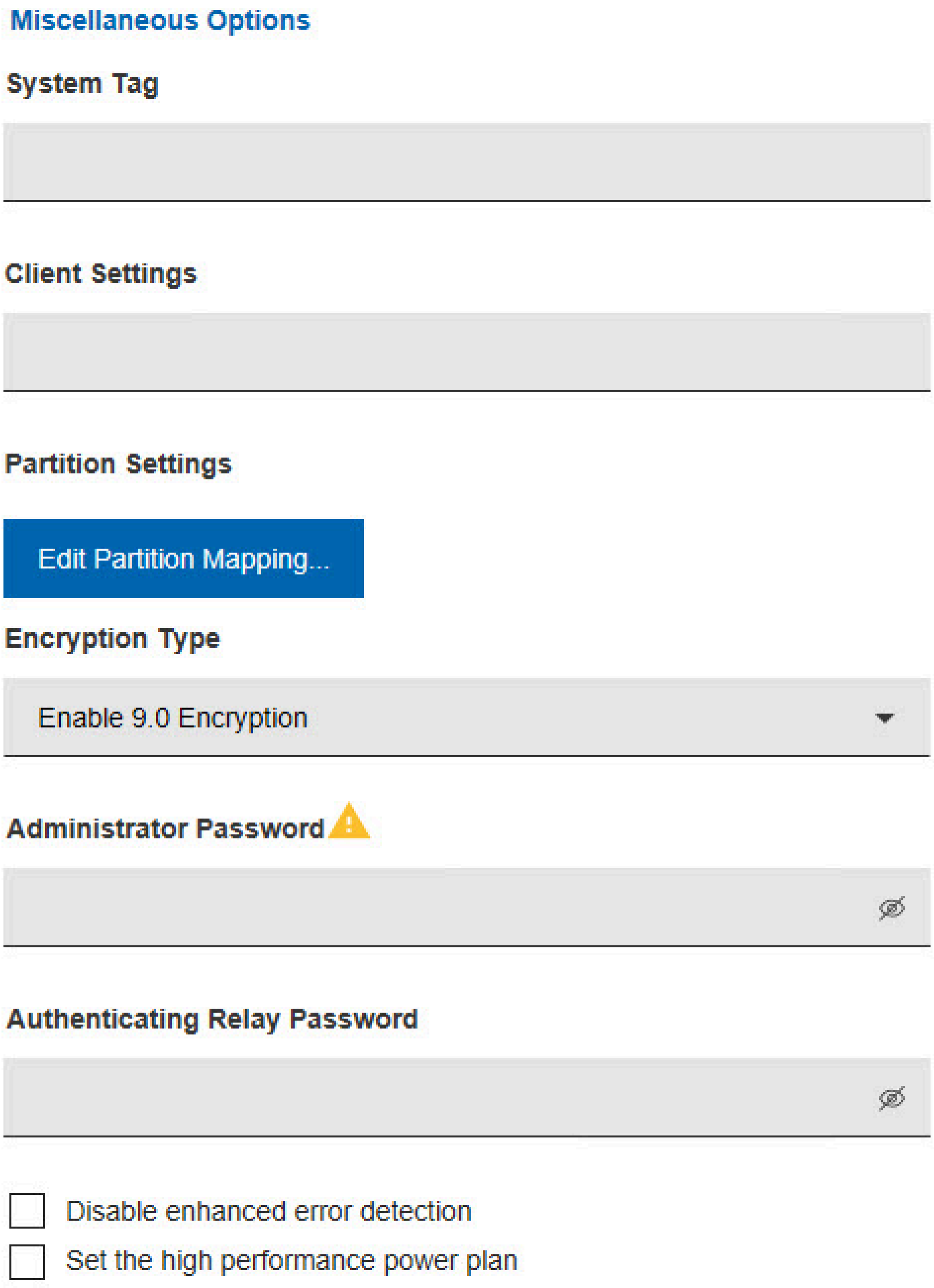
From / To	Windows 7	Windows 8	Windows 8.1	Windows 10	Windows 11
Windows 7	Uses 'hard link' to migrate the profile locally No disk or network impact	Uses 'hard link' to migrate the profile locally No disk or network impact	Uses 'hard link' to migrate the profile locally No disk or network impact	Uses '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	Uses 'hard link' to migrate the profile locally	Uses 'hard link' to migrate the profile locally	Uses 'hard link' to migrate the profile locally	Uses 'hard link' to migrate the profile locally

From / To	Windows 7	Windows 8	Windows 8.1	Windows 10	Windows 11
		No disk or network impact	No disk or network impact	No disk or network impact	No disk or network impact
Windows 8.1	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 10	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 11	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

Enable 9.0 Encryption

Administrator Password

Authenticating Relay Password

□ Disable enhanced error detection

□ Set the high performance power plan

Use the **System Tag** field to set a string in the registry file to highlight something specific for that system to the BigFix 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.

You can specify **Client Settings** to list named variables that are assigned to the deployed computer. 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. You must specify the variables in a `NAME:VALUE` format. If you specify multiple variables, each one must be separated by a vertical bar *“”*`|`.

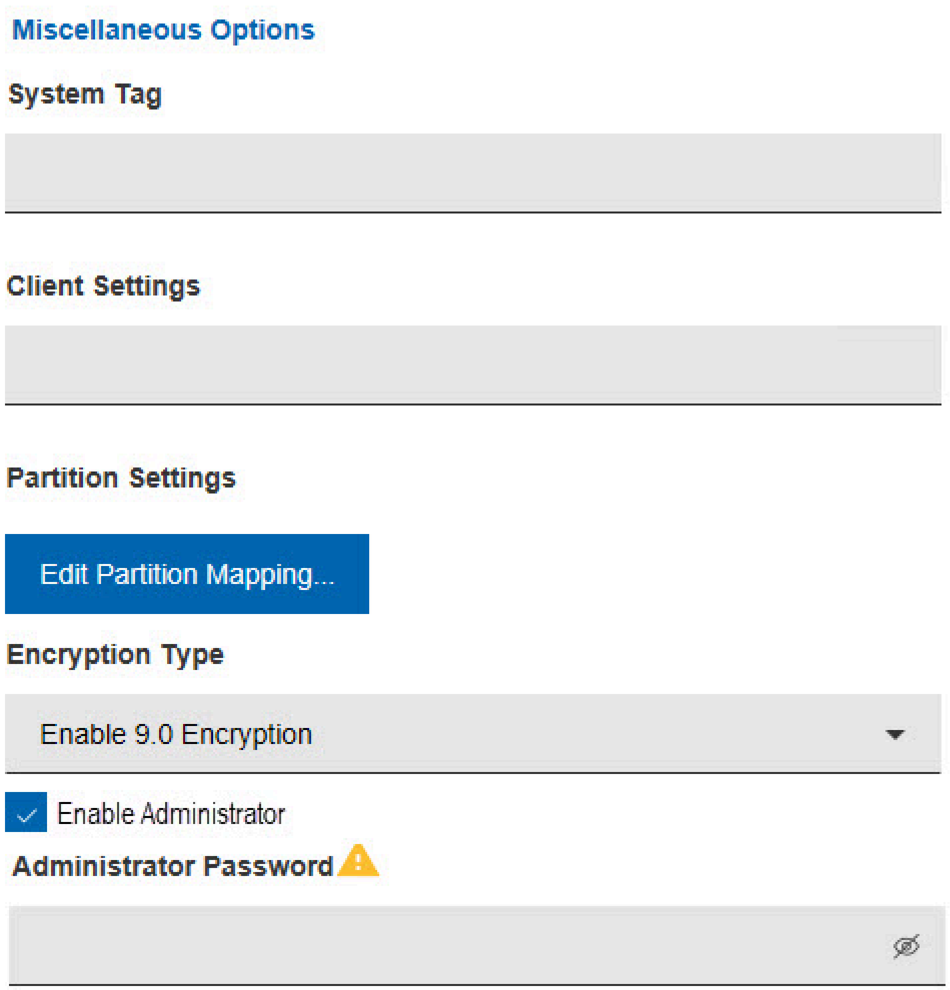
After a deployment, you can display these values in the BigFix console by selecting the specified computer, and clicking *“Edit Computer Settings”*. The settings are listed under *“Custom Settings.”*

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

Examples of how you can use the client settings field to configure the target after a deployment are available on the BigFix wiki.

A complete list of available client configuration (custom) settings, and a description of how to use them is available at this link: Configuration Settings.

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



Miscellaneous Options

System Tag

Client Settings

Partition Settings

Encryption Type: Enable 9.0 Encryption

☑ Enable Administrator

Administrator Password ⚠

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 148)*.

Setting Secure Password Transfer

If you are using BigFix 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.

Relay Password

This password is used to connect the BigFix clients to their authenticating relays in the new operating system. You can leave it empty, if the BigFix clients are not connected to authenticating relays.

If the BigFix client is connected to an authenticated relay but its password is not provided, it cannot reconnect to its relay in the new operating system.

Enhanced error detection

OS Deployment modifies the boot sequence of target machines to monitor and track operations performed during capture, reimage, 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 prevents 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. You must select this option when you deploy images to UEFI targets with the Secure Boot option enabled.

High performance power plan

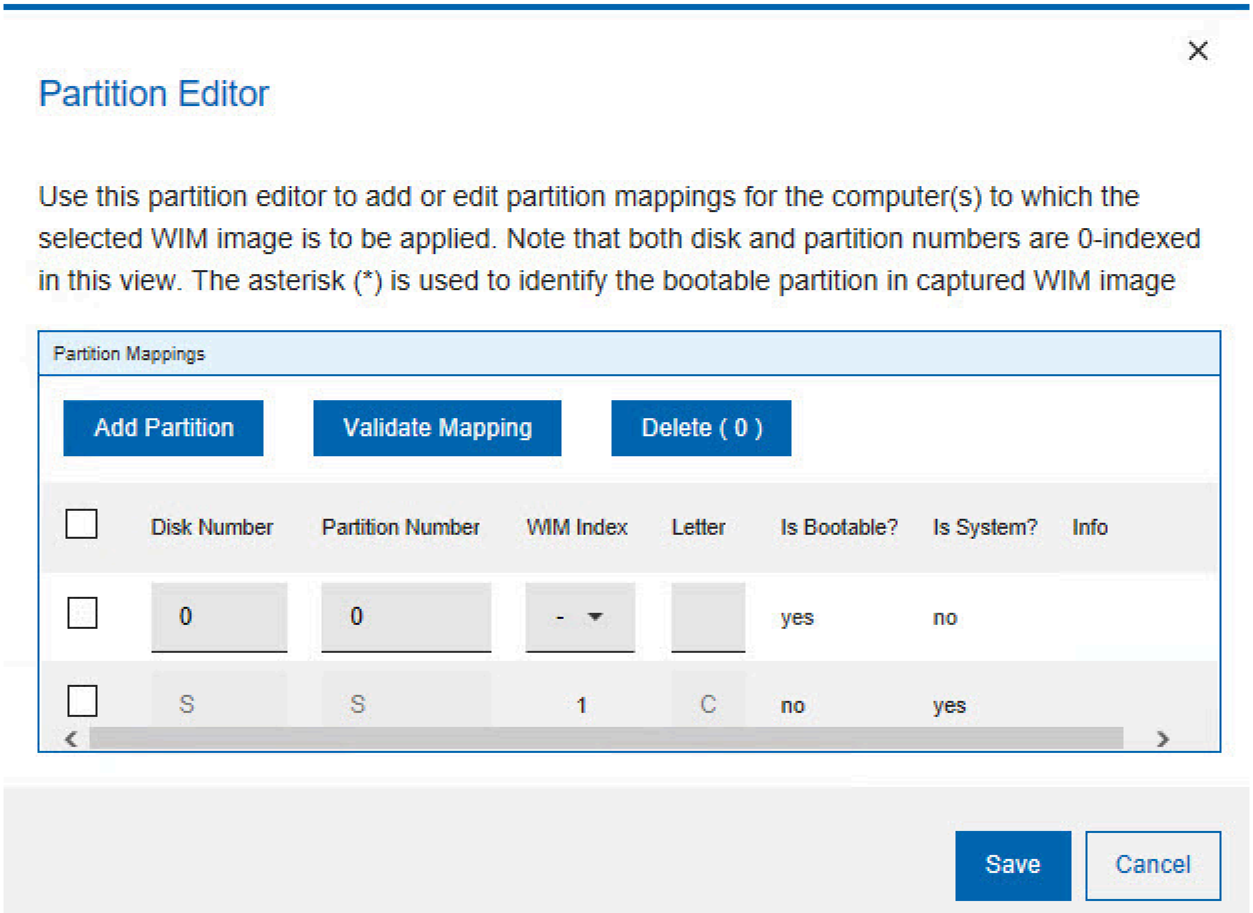
This option is available only for Windows 10/11 and, if selected, sets the high performance power plan on the target computer. This will also prevent the standby during the deployment on laptops when the lid is closed on AC. Windows Bundle later than Version 3.10.16 is required.

Mapping partitions

Click **Edit Partition Mapping** to choose the partition layout for the deployment. This option is enabled only for captured images with more than one partition.

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.



Partition Editor

Use this partition editor to add or edit partition mappings for the computer(s) to which the selected WIM image is to be applied. Note that both disk and partition numbers are 0-indexed in this view. The asterisk (*) is used to identify the bootable partition in captured WIM image

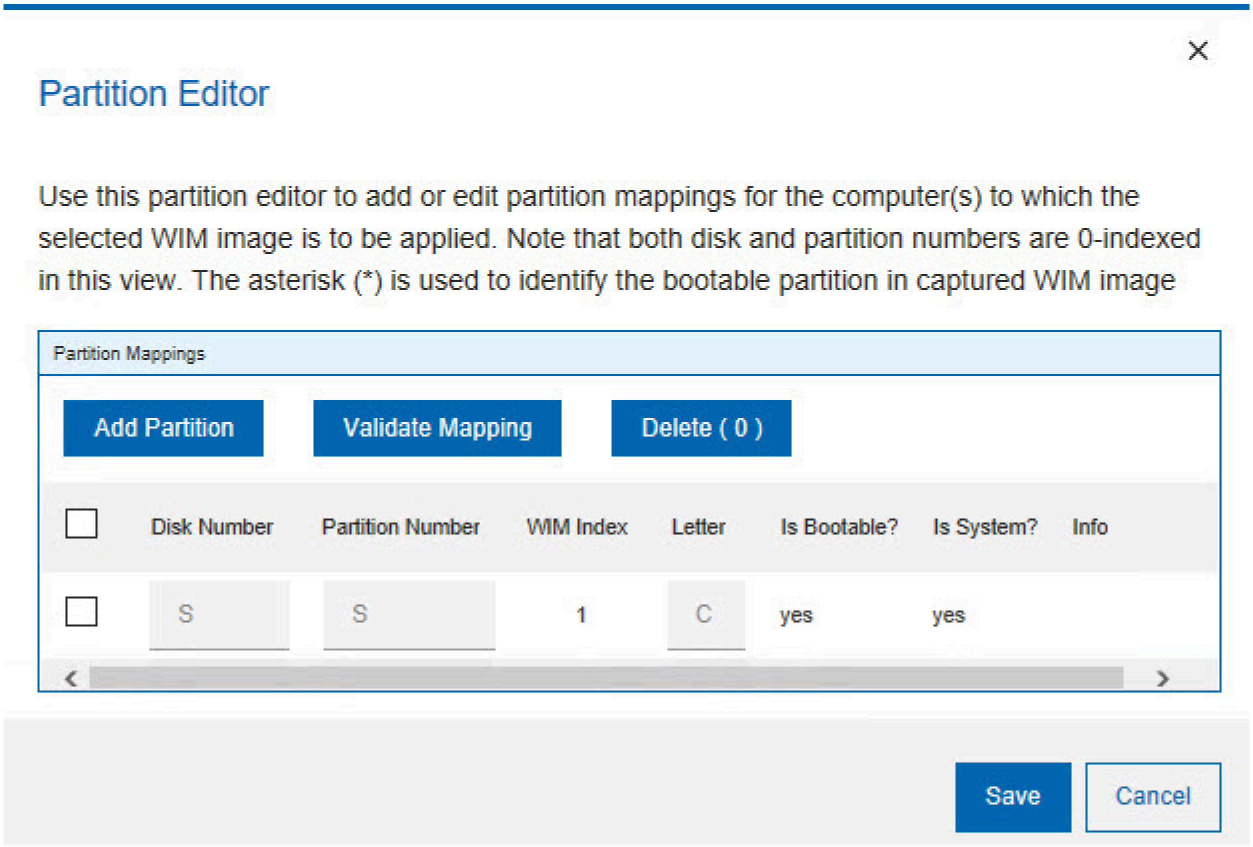
Partition Mappings

□	Disk Number	Partition Number	WIM Index	Letter	Is Bootable?	Is System?	Info
□	0	0	- ▾		yes	no	
□	S	S	1	C	no	yes	

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.



Partition Editor

Use this partition editor to add or edit partition mappings for the computer(s) to which the selected WIM image is to be applied. Note that both disk and partition numbers are 0-indexed in this view. The asterisk (*) is used to identify the bootable partition in captured WIM image

Partition Mappings

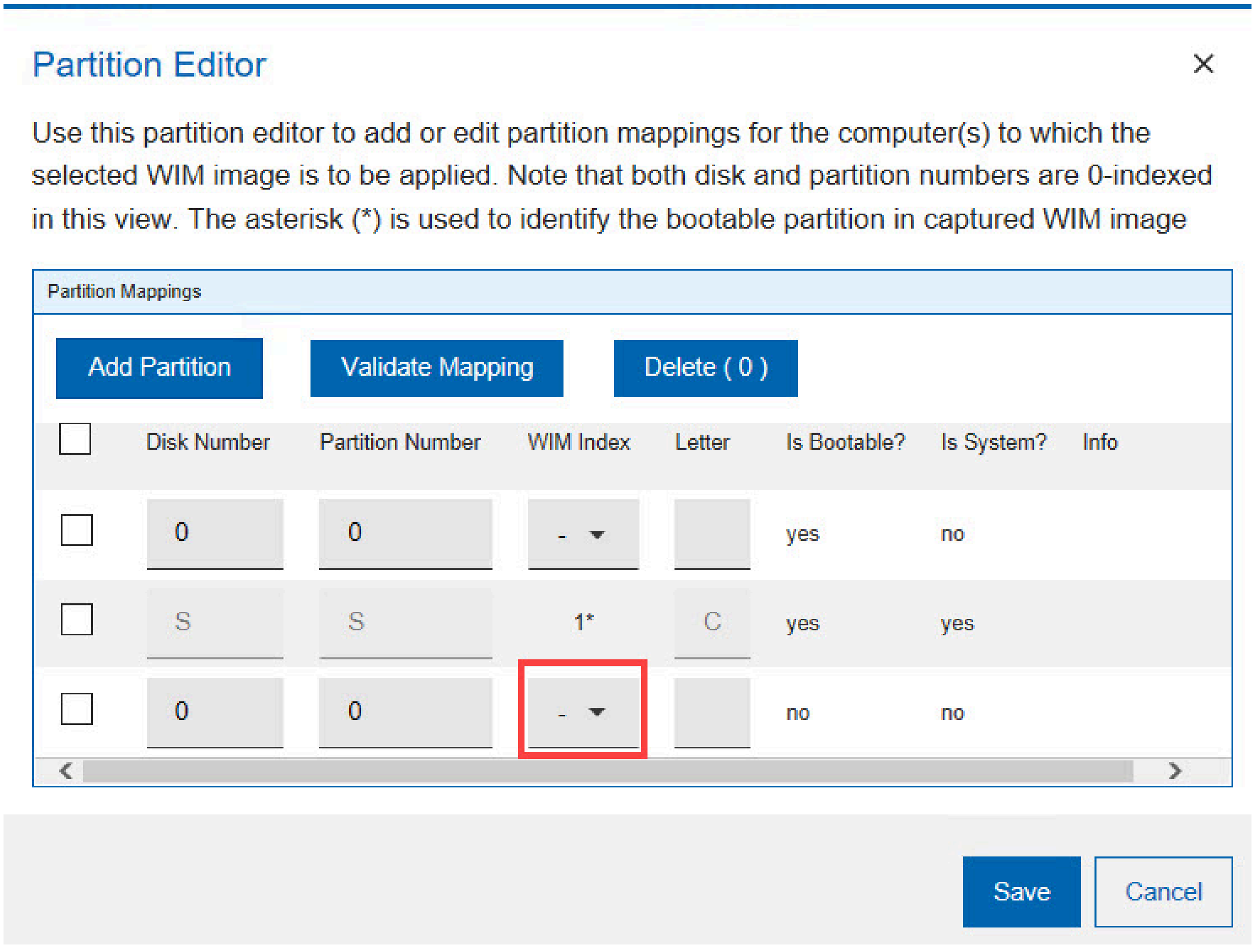
□	Disk Number	Partition Number	WIM Index	Letter	Is Bootable?	Is System?	Info
□	S	S	1	C	yes	yes	

During the reimaging 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 reimage 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 reimaging process fail.

If the number of partitions you configure for the target is less than the actual 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 reimage 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 8 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:



Partition Editor

Use this partition editor to add or edit partition mappings for the computer(s) to which the selected WIM image is to be applied. Note that both disk and partition numbers are 0-indexed in this view. The asterisk (*) is used to identify the bootable partition in captured WIM image

Partition Mappings

□	Disk Number	Partition Number	WIM Index	Letter	Is Bootable?	Is System?	Info
□	0	0	- ▾		yes	no	
□	S	S	1*	C	yes	yes	
□	0	0	- ▾		no	no	

If the target of a reimage 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 for remote logging and USM Overflow

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.

If you enabled remote logging you can also select **Dynamic Logging** to enable real time logging for debugging purposes. Logs are created dynamically and stored in the specified network location.

Enable USM Overflow specifies a network location where user files are to be migrated if there is insufficient space on the endpoint. 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 4. 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`

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

Table 5. 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.

Table 5. Join Domain Properties in the CustomSettings.ini file (continued)

Property in CustomSettings.ini file	Description
`MachineObjectOU`	The Organizational Unit (OU) in the target domain in which the account for the target computer is created.

Reimaging Windows Systems in multicast

You can reimage your targets by using multicast communication, if your network infrastructure supports it.

To reimage Windows targets using multicast, the following requirements must be met:

- Your Bare Metal Server component must be at version 7.1.1.19 or later, and must be installed and running on the relays to which the targets are connected. To use a different relay from the one to which the target is connected, you can add a custom client setting as described in Adding a custom setting to connect a target to a specific relay *(on page 165)*. During the reimaging deployment, the target dynamically connects to the relay specified in the setting.
- You must create at least one reimage profile for each image that you want to deploy in multicast and precache it on one or more Bare Metal servers that manage the multicast deployment.

Multicast is implemented as a group-based deployment so that computers can be installed in batches. The Bare Metal Server splits the profiles into blocks that are sent to all targets that belong to the same multicast group. Before sending each block, the server sends a packet called TOC, that describes the content of the block.

To create a reimage profile, complete the following steps:

1. From the **Image Library** select a Windows image that you want to deploy in multicast.
2. Click **Create Reimage Profile**.

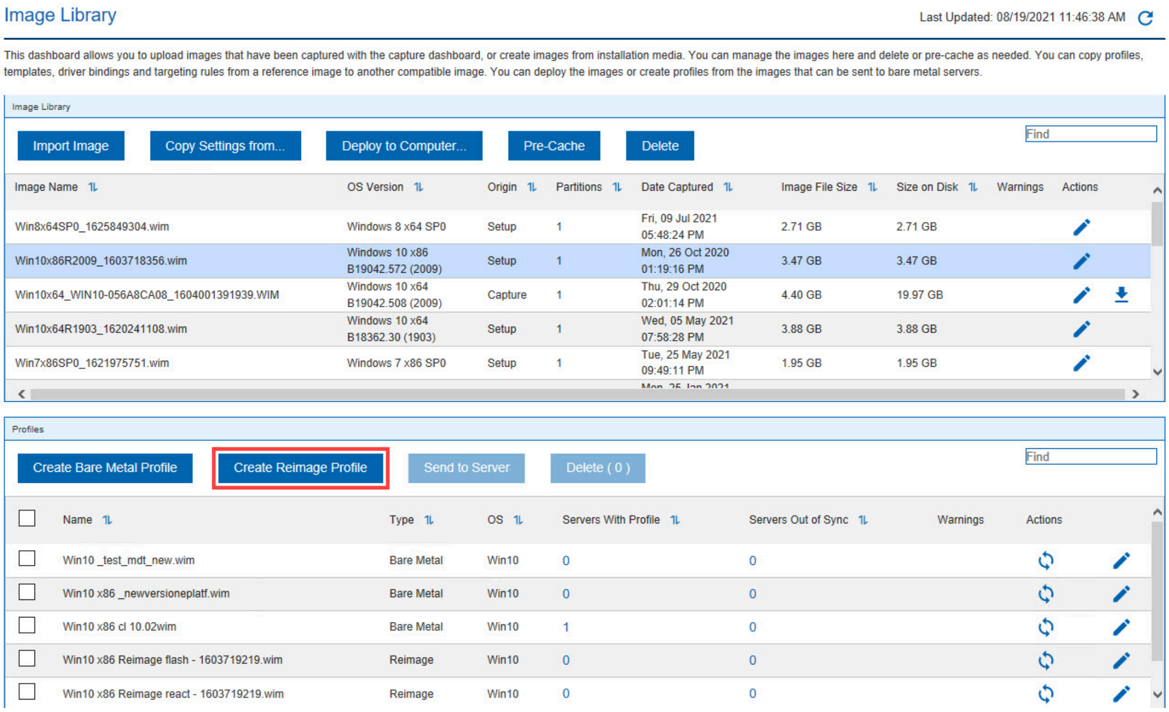


Image Library

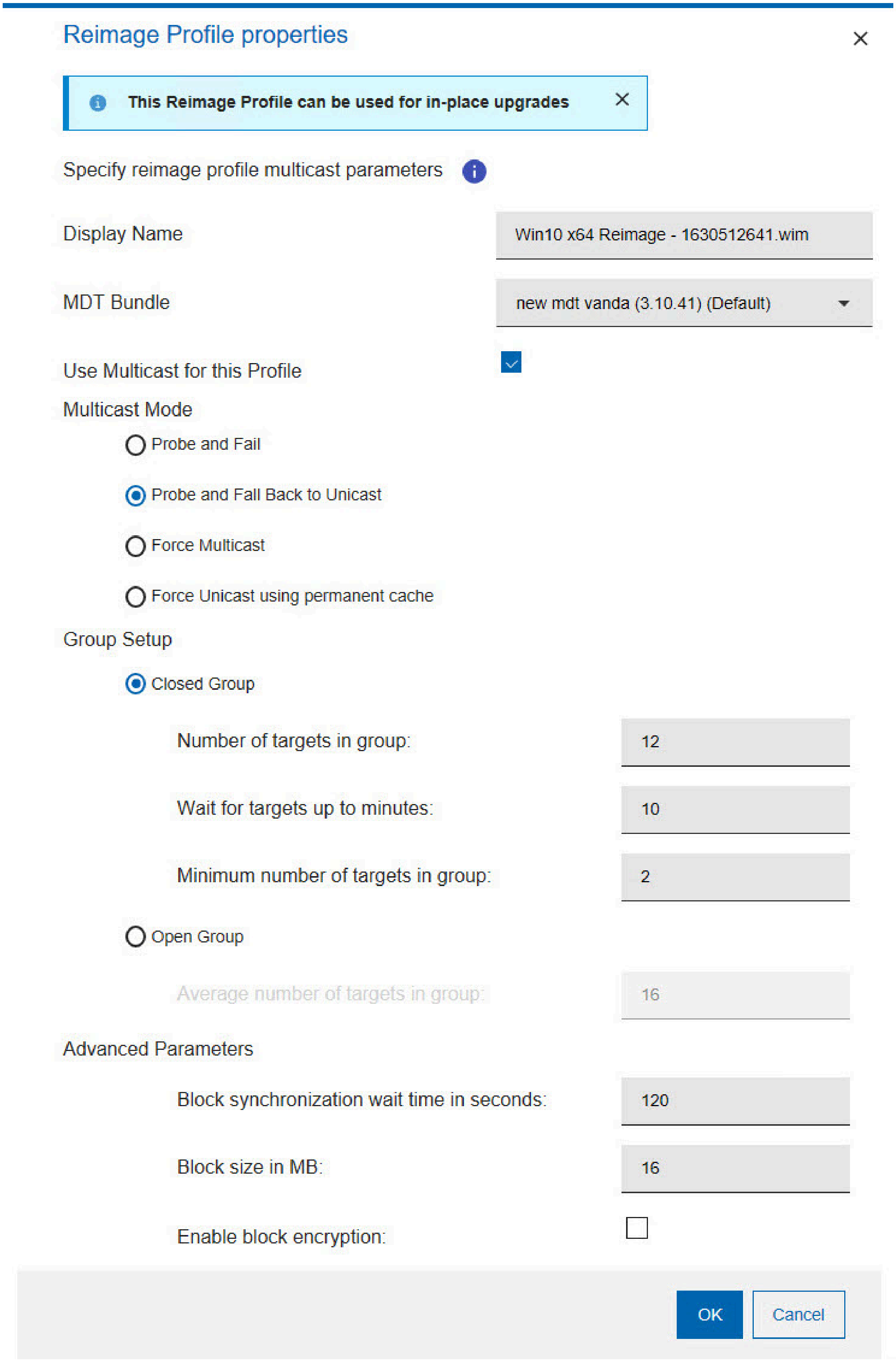
Last Updated: 08/19/2021 11:46:38 AM

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 copy profiles, templates, driver bindings and targeting rules from a reference image to another compatible image. You can deploy the images or create profiles from the images that can be sent to bare metal servers.

Image Name	OS Version	Origin	Partitions	Date Captured	Image File Size	Size on Disk	Warnings	Actions
Win8x64SP0_1625849304.wim	Windows 8 x64 SP0	Setup	1	Fri, 09 Jul 2021 05:48:24 PM	2.71 GB	2.71 GB		
Win10x86R2009_1603718356.wim	Windows 10 x86 B19042.572 (2009)	Setup	1	Mon, 26 Oct 2020 01:19:16 PM	3.47 GB	3.47 GB		
Win10x64_WIN10-056A8CA08_1604001391939.WIM	Windows 10 x64 B19042.508 (2009)	Capture	1	Thu, 29 Oct 2020 02:01:14 PM	4.40 GB	19.97 GB		
Win10x64R1903_1620241108.wim	Windows 10 x64 B18362.30 (1903)	Setup	1	Wed, 05 May 2021 07:58:28 PM	3.88 GB	3.88 GB		
Win7x86SP0_1621975751.wim	Windows 7 x86 SP0	Setup	1	Tue, 25 May 2021 09:49:11 PM	1.95 GB	1.95 GB		

☐	Name	Type	OS	Servers With Profile	Servers Out of Sync	Warnings	Actions
☐	Win10 _test_mdt_new.wim	Bare Metal	Win10	0	0		
☐	Win10 x86 _newversioneplatf.wim	Bare Metal	Win10	0	0		
☐	Win10 x86 cl 10.02wim	Bare Metal	Win10	1	0		
☐	Win10 x86 Reimage flash - 1603719219.wim	Reimage	Win10	0	0		
☐	Win10 x86 Reimage react - 1603719219.wim	Reimage	Win10	0	0		

3. The **Reimage Profile properties** window is displayed.



Reimage Profile properties

This Reimage Profile can be used for in-place upgrades

Specify reimage profile multicast parameters

Display Name: Win10 x64 Reimage - 1630512641.wim

MDT Bundle: new mdt vanda (3.10.41) (Default)

Use Multicast for this Profile ☑

Multicast Mode

- ○ Probe and Fail
- ● Probe and Fall Back to Unicast
- ○ Force Multicast
- ○ Force Unicast using permanent cache

Group Setup

- ● Closed Group
  - Number of targets in group: 12
  - Wait for targets up to minutes: 10
  - Minimum number of targets in group: 2
- ○ Open Group
  - Average number of targets in group: 16

Advanced Parameters

- Block synchronization wait time in seconds: 120
- Block size in MB: 16
- Enable block encryption: □

To enable multicast for the profile, select the corresponding option. Default values for multicast deployment are provided. You can accept or change them, depending on the characteristics of your network:

Display Name

The name of the profile. By default, the name is derived from the associated image and the type of profile (in this case, Reimage). You can specify a different name, with a maximum length of 70 alphanumeric characters.

Windows Bundle

The Windows Bundle to be used for the deployment. You can choose a different one from the list of compatible bundles for the selected image.

Multicast Mode

Defines how the multicast distribution is managed on the targets at deployment time for the profile:

Probe and Fail

If the probe on the target fails, the deployment task also fails.

Probe and Fall back to Unicast

If the probe on the target is successful, deployment occurs in multicast. If the probe fails, deployment of the profile occurs in unicast, using the Bare Metal Server cache, instead of the relay cache.

Force Multicast

Deployment on the target is forced to multicast regardless of probe results.

Force Unicast using permanent cache

Deployment on the target is completed in unicast using the Bare Metal Server cache. This option is useful when you want to ensure that all necessary files are available at deployment time.

Important: If the image you selected is larger than 16 gigabytes in size, and you have enabled multicast, the options "Probe and Fall Back to Unicast and "Force Unicast using permanent cache" are disabled.

Group Setup

Select the type of multicast group that is used for the deployment. You can accept or change the associated parameters.

Closed Group

Targets join the group as they are ready. When the following criteria are satisfied, the group is closed and distribution begins. This is the default.

Number of targets in group

Specify the maximum number of targets allowed in the group. The default value is 12.

Wait for targets up to minutes

Specify the maximum number of minutes to wait for targets before starting the multicast deployment. The default value is 10 minutes.

Minimum number of targets in group

Specify the minimum number of targets that must join for a multicast deployment. If the specified value is not reached, deployment is completed in unicast. The default value is 2.

Open Group

Targets can join the group as they are ready, at any time during deployment. You can change the associated parameter.

Average number of targets in group

Specify the average number of targets expected in the group. This value is used to optimize block synchronization. The closer the number of actual targets is to this value, the more efficient the multicast deployment. The default value is 16.

Advanced Parameters

Multicast advanced customization and tuning options that apply to both multicast group types.

Block synchronization wait time in seconds

Specify how many seconds the server must wait before sending the next block. This value is preset to 120 seconds. If you specify a value less than 5 seconds, the block synchronization wait time is forced to 5.

Block size in MB

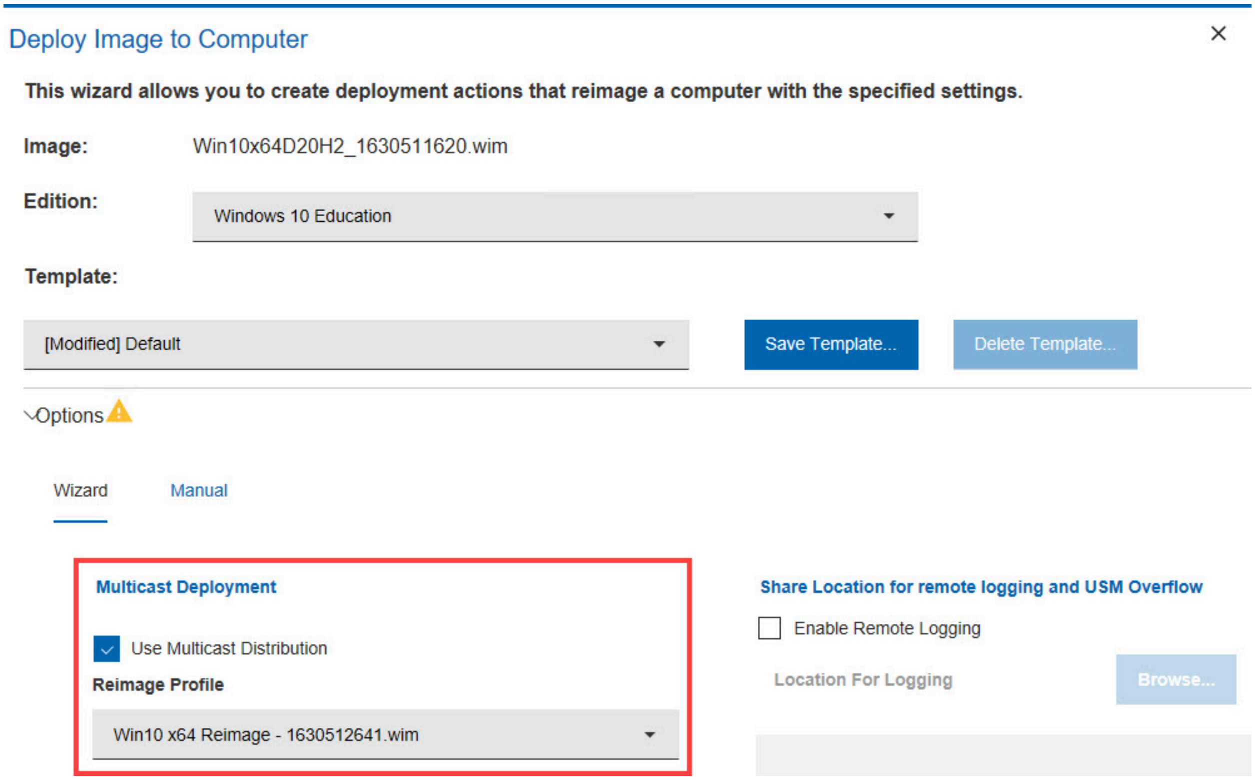
The image is divided into blocks that are sent to the targets. This parameter sets the maximum size of the data blocks (in megabytes) sent in each transmission packet. The default value is 16 Megabytes.

Enable block encryption

Specify if the blocks must be encrypted during transmission.

4. Click **OK** to save the profile.
5. Select the profile from the list, and click **Send to Server**. If you select multiple profiles and more than one server, the send operation might take some time.

To deploy an image in multicast, select it from the list and click **Deploy to Computer**.



Deploy Image to Computer

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

Image: Win10x64D20H2_1630511620.wim

Edition: Windows 10 Education

Template: [Modified] Default

Multicast Deployment

☑ Use Multicast Distribution

Reimage Profile: Win10 x64 Reimage - 1630512641.wim

Share Location for remote logging and USM Overflow

□ Enable Remote Logging

Location For Logging

Check the multicast distribution option and select the reimage profile. Specify the other parameters as needed. For a detailed explanation of the parameters see Deploying an image to a target computer *(on page 145)*.

Probing targets before a multicast deployment

Before deploying images in multicast, you can check if targets in your network can receive multicast deployments by running the **Probe Clients for Multicast Deployment** task (80). The task checks that the client can accept incoming multicast packets. The probe uses an incremental TTL (Time to Live) value up to a maximum default of 5. If you want to change the maximum TTL value that the Bare Metal server uses to check if the target is able to receive multicast packets, edit the computer settings of the Bare Metal server and create a new client setting `OSD_MaximumTTL_MCastProbe`.

To successfully deploy images in multicast, you must ensure that the needed ports are available on the Bare Metal Server and on the targets connected to them. For more information about the ports that are used for multicast distribution, see Listening ports used for OS Deployment tasks, media creation and reimaging deployments in multicast. *(on page 50)*.

Adding a custom setting to connect a target to a specific relay

From the **Subscribed computers** view, highlight the target computer and click **Edit Settings**. Click **Add** to define the new setting with name `BMServerOverride`. Set the value to the hostname or IP address of the relay with the Bare Metal Server component to which the target must connect for the reimaging deployment, then click **OK** to save.

Reimaging Linux Systems

You can reimage Linux systems by deploying images that you previously imported from installation media.

When you reimage a Linux target system, you are installing an image file (`.LIM`) previously created from an ISO image and stored in the Image Library. The images that you can deploy are of type **Setup** and are identified by the Origin field of the Image Library dashboard.

Depending on the reimaging mode, (Upgrade or Install), you are required to specify parameters that are needed for the target deployment. The parameters that you specify must be saved to a template before starting the reimage task. For more information, see Managing templates *(on page 177)*.

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 49)*.

You can reimage 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 that is 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 copied to the reimaged system:

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

Note: In some cases, the BigFix client identity is not preserved. For more information, see Duplicate client computer entry in the Server database after a Linux reimage *(on page 248)*.

Important:

- Reimaging to targets that are managed by a proxy server is not supported.
- Reimaging to targets that are connected to an authenticating relay is not supported.
- Reimaging of captured images is not supported.
- Reimaging of Ubuntu systems is not supported.
- It is good practice to backup your system before upgrading.

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

Linux configuration options

For the reimaging process, a configuration file is used at deployment time for both reimaging 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 reimaging task to copy 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 reimaging combinations

The following table lists the valid reimaging combinations for the **Install** mode:

Table 6. Linux reimaging combinations - Install Mode

Allowed combinations for reimaging in Install mode

Architecture (From/To)	Distribution	OS Combinations (From/To)
• 32-bit to 32- bit • 32-bit to 64-bit • 64-bit to 64-bit	• RHEL to RHEL • CentOS to CentOS • SLES/SLED to SLES/SLED	• RHEL 6.x to RHEL 6.x, 7.x • RHEL 7.x to RHEL 7.x, 8.x • RHEL 8.x to RHEL 8.x, 9.x • RHEL 9.x to RHEL 9.x • CentOS 7.x to CentOS 7.x, 8.x • CentOS 8.x to CentOS 8.x • SLES 11.x to SLES 11.x • SLED 11.x to SLED 11.x • SLES 12.x to SLES 12.x • SLED 12.x to SLED 12.x • SLES 11.x to SLE 15.x • SLES/SLED 12.x to SLE 15.x • SLE 15.x to SLE 15.x

The following table lists the valid reimaging combinations for the **Upgrade** mode:

Table 7. Linux reimaging combinations - Upgrade Mode

Architecture (From/To)	Distribution	OS/SP Combinations (From/To)
• 32-bit to 32-bit • 64-bit to 64-bit	• RHEL to RHEL	Version 6.x to 6.x+n
		Version 6.10 to 7.9
		Version 7.x to 7.x+n
		Version 8.x to 8.x+n
		Version 8.8 to 9.2
		Version 8.9 to 9.3
		Version 8.10 to 9.4 or later
		Version 9.x to 9.x+n
		Server 6.10 to Server 7.9
		Server 7.9 to Server 8.8 & 8.10
• 64-bit to 64-bit	• CentOS to CentOS	Version 7.x to 7.x+n
		Version 8.x to 8.x+n
• 32-bit to 32-bit • 64-bit to 64-bit	• SLES to SLES • SLED to SLED	Version 11.x to 11.x+1
		Version 11.3 or later to 12.x
		Version 12.x to 12.x+n[1]
		Version 12.x to 15.x[1]
		Version 15.x to 15.x+n[1]

Note:

1. Select **Force upgrade** to run the action, if the selected OS combination is not recommended by the manufacturer.

Important:

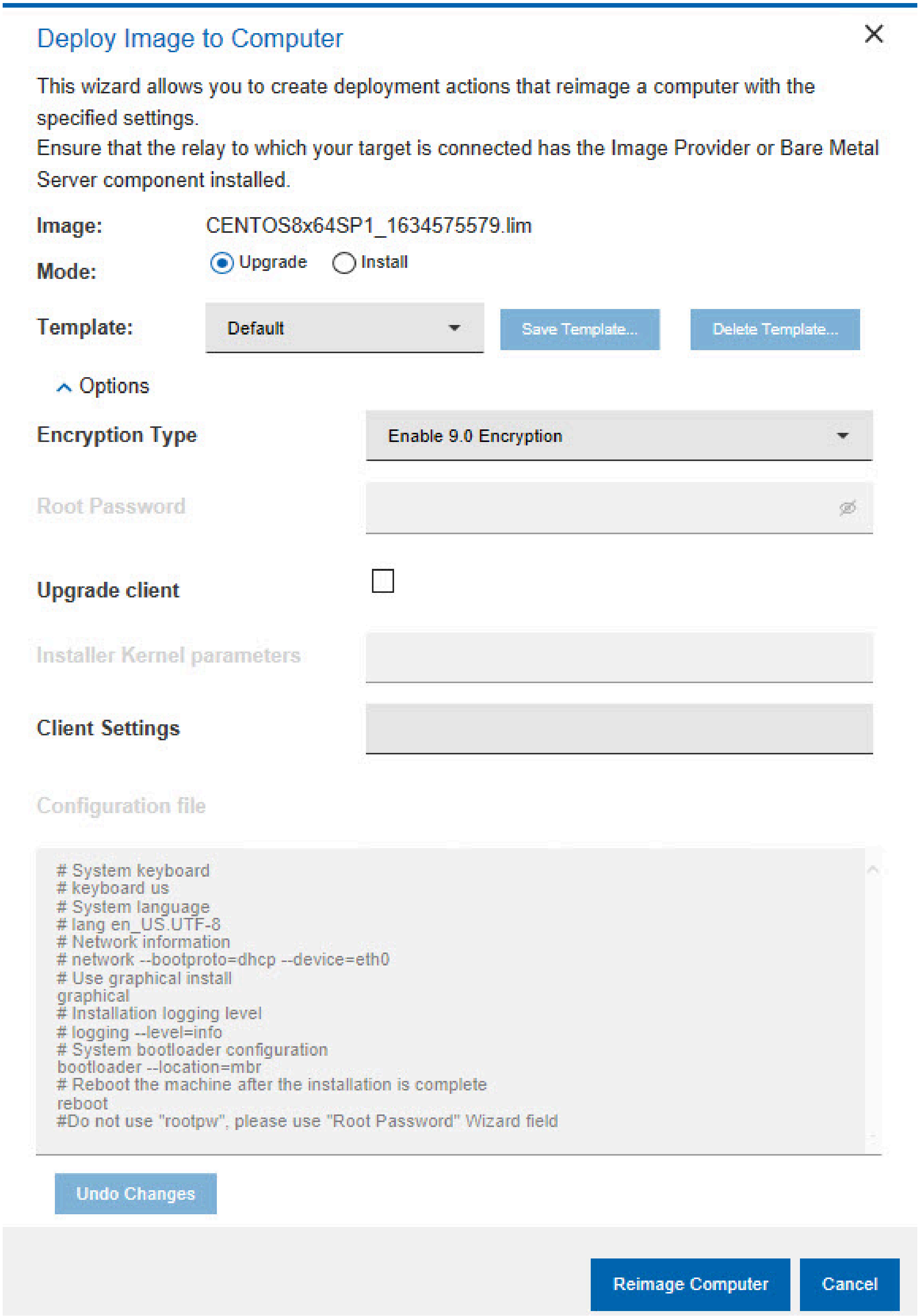
- Upgrading from CentOS 7.x to CentOS 8.x is not supported.
- For 64-bit architectures, both BIOS and UEFI targets are supported.

To upgrade to SLE15, you must edit the configuration file of the reimage template correctly by selecting all the required modules and repositories. On a running SLE15 target, a list of modules can be found in `/etc/zypp/repos.d`. But this does not include packages installed after OS installation.

As a guideline, the configuration file reports a commented list of all available modules. BaseSystem Module is uncommented, as it is required. You must uncomment the other modules, as required for your system.

Reimaging in Upgrade mode

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



Deploy Image to Computer

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

Ensure that the relay to which your target is connected has the Image Provider or Bare Metal Server component installed.

Image: CENTOS8x64SP1_1634575579.lim

Mode: ● Upgrade ○ Install

Template: Default

Encryption Type: Enable 9.0 Encryption

Root Password

Upgrade client □

Installer Kernel parameters

Client Settings

Configuration file

```
# System keyboard
# keyboard us
# System language
# lang en_US.UTF-8
# Network information
# network --bootproto=dhcp --device=eth0
# Use graphical install
graphical
# Installation logging level
# logging --level=info
# System bootloader configuration
bootloader --location=mbr
# Reboot the machine after the installation is complete
reboot
#Do not use "rootpw", please use "Root Password" Wizard field
```

Apart from specific upgrade paths for RHEL (RHEL in-place upgrade, that is described in the next section), this mode is intended for upgrading to later service packs for the same major release. However, if you check **Force upgrade**, when it's available, the upgrade to a major release is forced, which could lead to an unsuccessful deployment. If you plan to change major release, you should use the install mode.

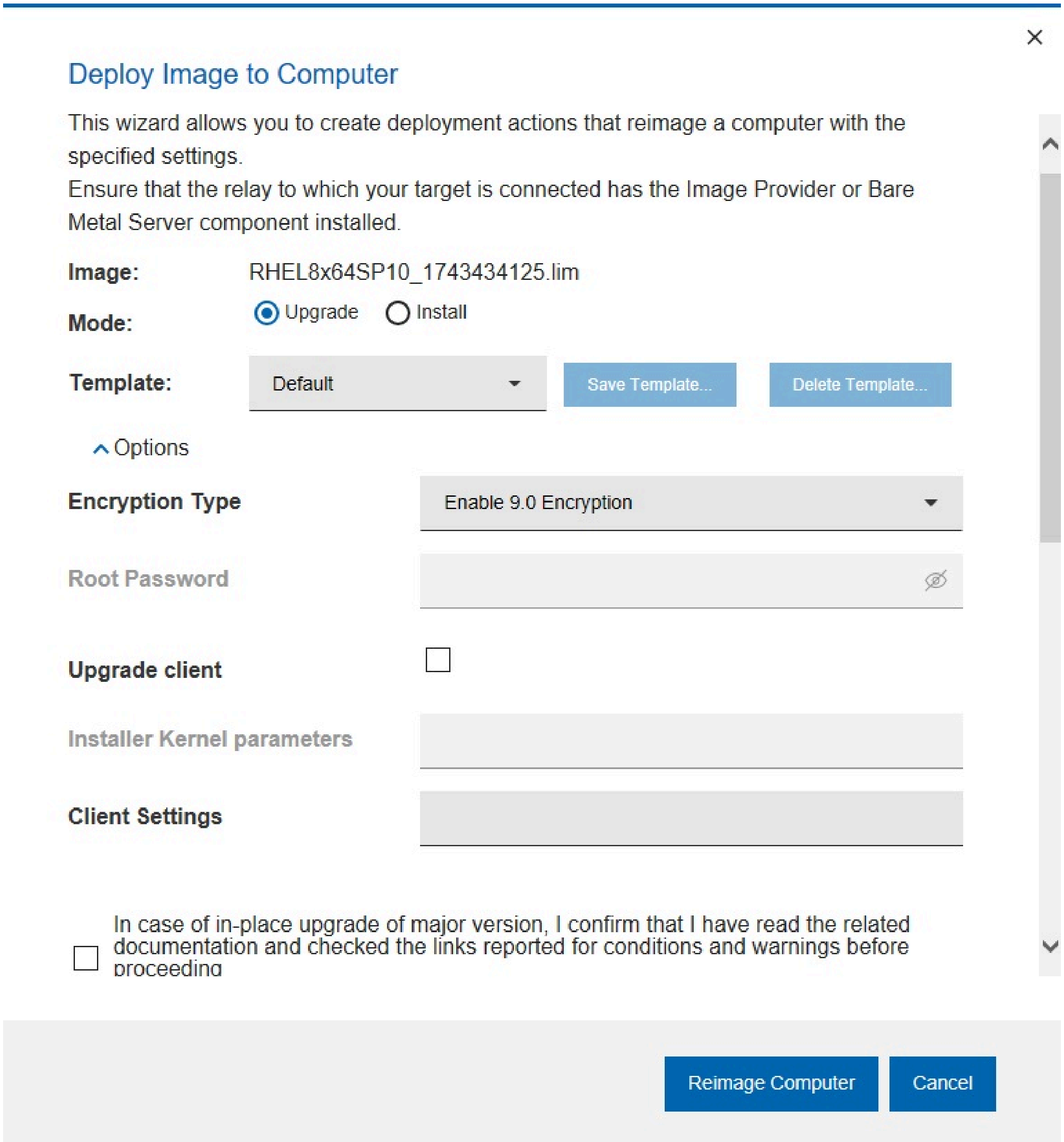
There are no required parameters for the **Upgrade** mode if it's not a RHEL in-place upgrade. Optionally, you can select to upgrade the BigFix client, by checking the corresponding option. You are then prompted to select the client package version. All selections that you make must be saved to a template. 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 that are stored in the installer response file and used for the upgrade are displayed. You can modify these parameters to suit your reimaging needs. Optionally, you can specify additional kernel parameters that the Linux installer uses during installation, and any client settings for the targets.

RHEL in-place Upgrade

Reimaging in **Upgrade** mode can be used on RHEL, for some specific paths, to upgrade to major release. The supported upgrade paths for RHEL in-place upgrade are from RHEL Server version 6.10 to 7.9, from RHEL Server version 7.9 to 8.8 and 8.10, from RHEL version 8.8 to 9.2, from RHEL version 8.9 to 9.3, and from RHEL version 8.10 to 9.4 or later. Before proceeding with the in-place upgrade, you need to verify the conditions and warnings at the following links for the respective in-place upgrades:

- for RHEL version 6 to 7 in-place upgrade - https://docs.redhat.com/en/documentation/red_hat_enterprise_linux/7/html-single/upgrading_from_rhel_6_to_rhel_7/index.
- for RHEL version 7 to 8 in-place upgrade - https://docs.redhat.com/en/documentation/red_hat_enterprise_linux/8/html-single/upgrading_from_rhel_7_to_rhel_8/index.
- for RHEL version 8 to 9 in-place upgrade - https://docs.redhat.com/en/documentation/red_hat_enterprise_linux/9/html/upgrading_from_rhel_8_to_rhel_9/planning-an-upgrade-to-rhel-9_upgrading-from-rhel-8-to-rhel-9.

The creation of an in-place upgrade OS resource for the specific initial OS is needed before proceeding with the task. More details are available at this link - https://help.hcl-software.com/bigfix/10.0/lifecycle/Lifecycle/OSD_Users_Guide/c_manage_linux_dep_media.html. You must accept the disclaimer that you consulted this documentation and the Red Hat documentation for instructions and warnings for the in-place upgrade in order to unblock the in-place upgrade task (assessment only or actual upgrade).



Deploy Image to Computer

This wizard allows you to create deployment actions that reimage a computer with the specified settings.
Ensure that the relay to which your target is connected has the Image Provider or Bare Metal Server component installed.

Image: RHEL8x64SP10_1743434125.lim

Mode: ● Upgrade ○ Install

Template: Default

Encryption Type: Enable 9.0 Encryption

Root Password

Upgrade client □

Installer Kernel parameters

Client Settings

□ In case of in-place upgrade of major version, I confirm that I have read the related documentation and checked the links reported for conditions and warnings before proceeding

After accepting the disclaimer, you have the following different options that can be selected:

- For the in-place upgrade from RHEL version 6 to 7: You can select either to run the assessment only or the actual upgrade.
    - **Assessment only**: Select this option to run only the assessment on your computer. Note that even with this option, some changes can be done on the computer to prepare it for the actual upgrade. When you run this option, the task will be successful if the computer is ready to run the actual upgrade, but the

upgrade will not start. However, if you don't select this option, the assessment will be anyway done on the computer and, if successful, the actual upgrade will start.

- **Allow extreme risk**: Select this option to accept the extreme level risks of the assessment to be considered successful and to start the actual upgrade if the **Assessment only** option is not selected.

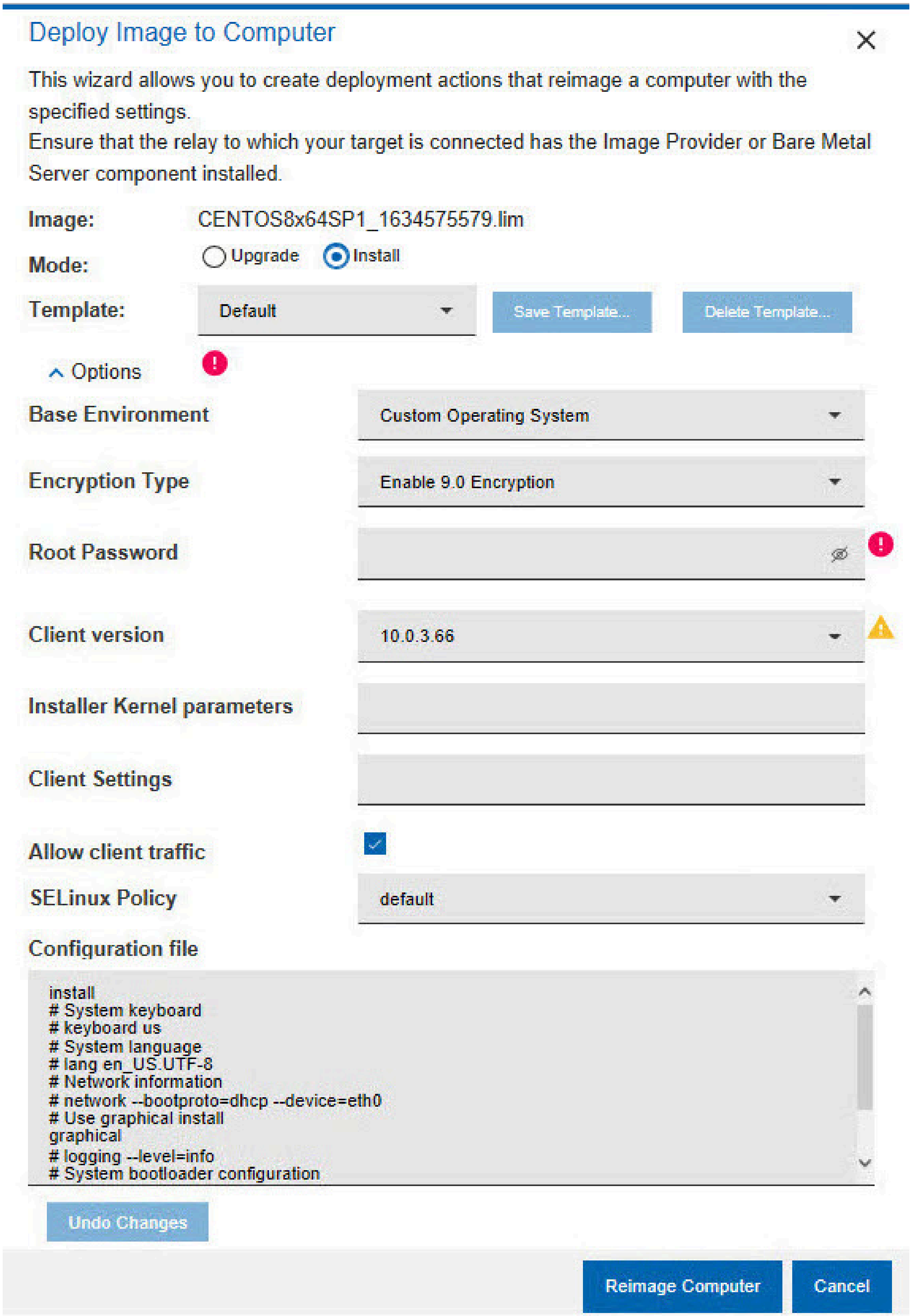
Note: Even when you don't allow extreme risks, if you do not select the **Assessment only** option, the upgrade will run in presence of high level risks. If you want to consult the report before allowing the extreme risks or if you want to check which risks are present and their levels, you can run the assessement without allowing extreme risks and consult the report. The text report file is `<bigfix client logs directory>/DeploymentLogs/preyumupgrad.log` and can be accessed after running the task.

- For the in-place upgrade from RHEL version 7 to 8 and from RHEL version 8 to 9:
    - **Assessment only**: Same as for in-place upgrade from RHEL version 6 to 7.
    - **Fix known inhibitors**: Select this option to remediate some known inhibitors that could block the in-place upgrade. Other inhibitors could still block the in-place upgrade and must be manually fixed before restarting the task. The inhibitors that the fixlet will remediate to are:
        - For the in-place upgrade from RHEL version 7 to 8:
            1. Remove `floppy` and `pata_acpi` modules.
            2. Confirm to accept the removal of `pam_pkcs11` module during the upgrade.
        - For the in-place upgrade from RHEL version 8 to 9:
            1. Change the Red Hat default firewall configuration with the setting **AllowZoneDrifting=no**
            2. Disable root user login in `ssh daemon configuration` (setting **PermitRootLogin no**)
            3. Confirm that no VDO devices are present on the system or all VDO devices have been successfully converted to LVM management.

        Refer to Red Hat documentation for more details. Do not select the option to **Fix known inhibitors** if you don't agree on what is to be done. If some inhibitors have been manually remediated, selecting this option to fix known inhibitors could overwrite the manual remediation so ensure it is not selected after manual remediation.

Reimaging 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 reimage a computer with the specified settings.
Ensure that the relay to which your target is connected has the Image Provider or Bare Metal Server component installed.

Image: CENTOS8x64SP1_1634575579.lim

Mode: ○ Upgrade ● Install

Template: Default

Options

Base Environment: Custom Operating System

Encryption Type: Enable 9.0 Encryption

Root Password:

Client version: 10.0.3.66

Installer Kernel parameters:

Client Settings:

Allow client traffic: ☑

SELinux Policy: default

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
# logging --level=info
# System bootloader configuration
```

Select a previously saved template, create a new template to save the current settings, or save your selections to the Default template. When you reimage in Install mode, the BigFix client is installed. The default version is the same version as the BigFix 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 Changing Firewall settings *(on page 177)*.

SELinux Policy

This field is available only for RHEL and CentOS. The SELinux Policy option allows to select the selinux policy to apply. The values are:

- **default**: Lets the operating system apply its default policy by not specifying any policy.
- **disabled**: Configures selinux policy as disabled.
- **permissive**: Configures selinux policy as permissive.
- **enforcing**: Configures selinux policy as enforcing. If you select this selinux policy, the configured type will be automatically set as "Targeted".

Note: With the SELinux support, if policy is not specified, it will be the default of the OS level being deployed. If you want to continue to have the SELinux policy disabled, edit the reimage template and set the value as disabled.

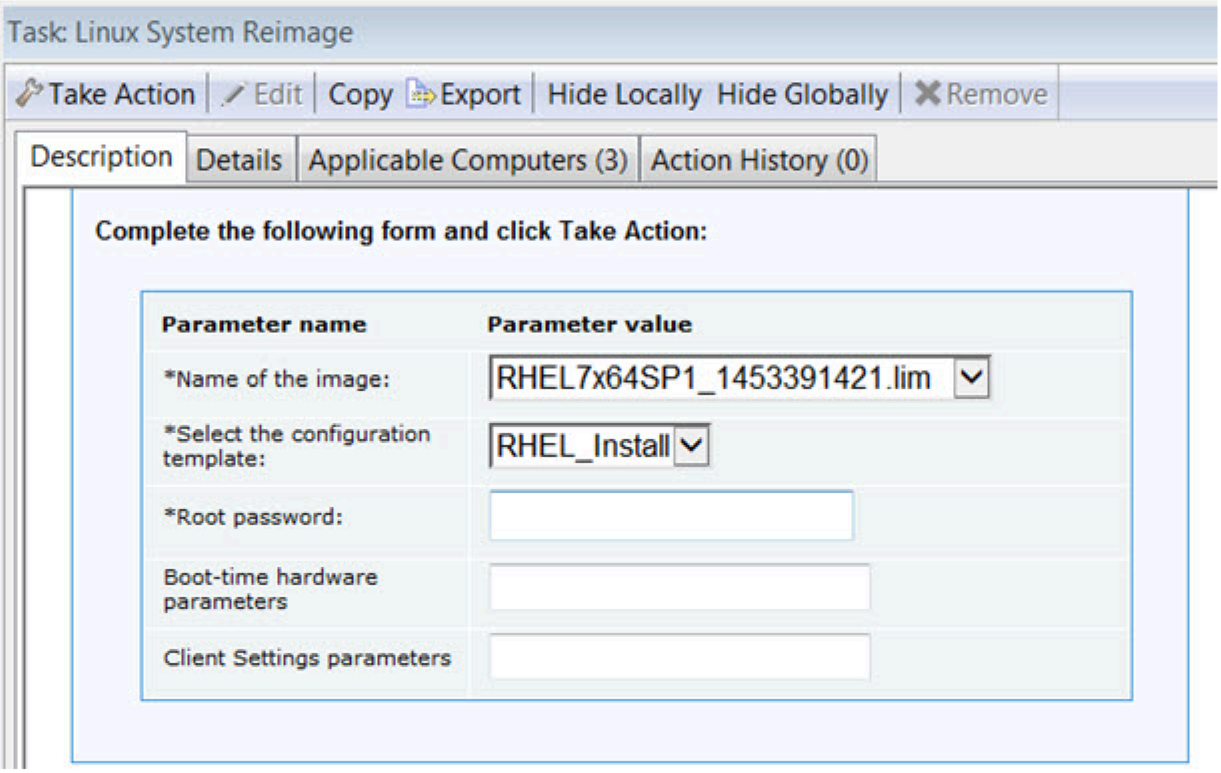
The default deployment configuration parameters stored in the installer response file and used for the installation are displayed. You can modify these parameters to suit your reimaging needs. Optionally, you can specify additional kernel parameters that the Linux installer uses during installation, and any client settings for the targets.

Using the Linux System Reimage task

You can reimage Linux targets using the Linux System Reimage task. Select the image and the associated configuration template containing the settings to be used for the reimaging process that you have previously created and saved in the Image Library. Specify the root password for the target system if you are reimaging in Install mode. The password that you specify can be either in clear text or encrypted. In either case, the password is always encrypted during the deployment process.

You can optionally specify boot-time kernel parameters for the installer, and client settings.

For reimaging 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:	RHEL7x64SP1_1453391421.lim
*Select the configuration template:	RHEL_Install
*Root password:	
Boot-time hardware parameters	
Client Settings parameters	

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 that you supply for reimaging 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:

```
$id$mysalt$mypassword
```

where *mysalt* is a character string that is 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 supported:

Table 8. 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/
```

Changing Firewall settings

When a reimage action is run from the BigFix 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:

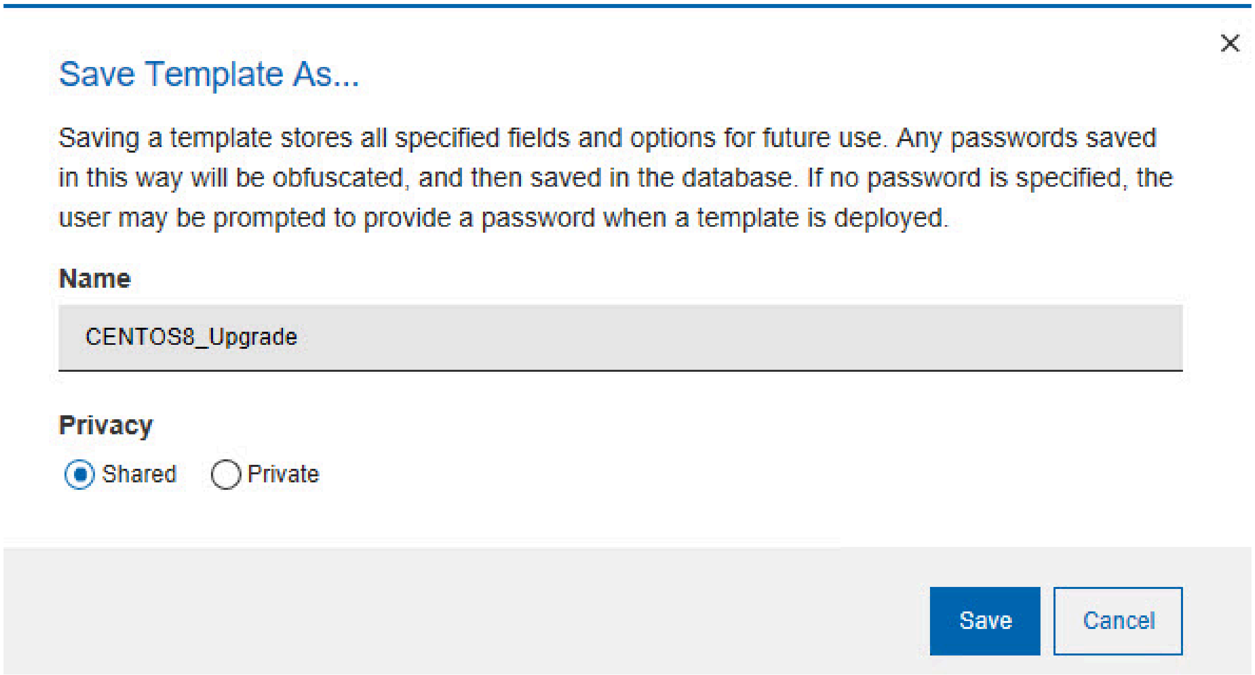
- RedHat Firewall is Blocking BES Traffic - BES Client (678)
- SuSE Firewall is Blocking BES Traffic - BES Client (682)

Running Fixlets 678 or 682 has the same effect as the **Allow Client Traffic** check box 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 stores all specified fields and options 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 may be prompted to provide a password when a template is deployed.

Name

CENTOS8_Upgrade

Privacy

● Shared ○ Private

Templates that are saved with **Shared** privacy are visible and usable by all BigFix 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 9. Installing Windows 10/11 or Windows Server using in-place upgrade

To upgrade your existing Windows systems to Windows 10/11 or Windows Server you can use the in-place upgrade fixlets.

For Windows client class, BigFix OS Deployment supports in-place upgrade installations to Windows 10 from Windows 7 Service Pack 1, Windows 8, Windows 8.1 update, and from Windows 10 to a later build and to Windows 11 from Windows 8, Windows 8.1 update and from Windows 10.

For Windows server class, BigFix OS Deployment supports in-place upgrade installations to Windows Server 2016 from Windows Server 2012 and Windows Server 2012 R2, to Windows Server 2019 from Windows Server 2012 R2 and Windows Server 2016, to Windows Server 2022 from Windows Server 2016 and Windows Server 2019, and to Windows Server 2025 from Windows Server 2012 R2, Windows Server 2016, Windows Server 2019 and Windows Server 2022.

The clients that you upgrade must be at BigFix version 11.0.3 or later if upgrading to Windows Server 2025 or later, or at BigFix version 9.2.5 or later if upgrading to all other Windows versions. In-place upgrade installs Windows 10/11 or Windows Server without previously removing the older version of the operating system on the client computer. The process automatically maintains existing settings, programs, and data. Only setup images are supported for the in-place upgrade. Before you begin the in-place upgrade, it is best practice to back up your systems.

Important:

- By using the following Tasks you are accepting the Microsoft end user license agreement for the final operating system.
- Before you upgrade to Windows 11, check the system requirements at Windows 11 specifications.
- If the execution settings of the action launched by the in-place upgrade fixlets are modified, it could lead to unexpected results including failures.

Consider the following use cases:

I am importing Windows 10/11 or Windows Server setup images for the first time in my BigFix OS Deployment environment.

To complete an in-place upgrade to Windows 10/11 or Windows Server, you must import the corresponding image from installation media. The system that you plan to upgrade must have a valid Windows license for the process to complete successfully, or you must specify it in the image product key field in the upgrade task.

Complete the following steps:

1. From the **Image Library** dashboard, import the Windows 10/11 or Windows Server images for the editions that you want to deploy.
2. Run the in-place upgrade using one or more of the available tasks for the selected image. Specify the image product key if required. Specify the Image Index if more than one index in the image can be applied to the edition to upgrade.

You do not need to create a new Windows Bundle for Windows in-place upgrades. If you want to complete bare metal and reimaging deployments of Windows 10/11 or Windows Server, you must create an Windows Bundle with the required tools. For more information, see Managing Windows Bundles and Deployment Media for Windows targets *(on page 67)*.

I already have one or more Windows 10 setup images in my BigFix OS Deployment environment.

If you already have Windows 10 setup images in the Image Library, complete the following steps:

1. If you plan to use Windows 10 setup images that you had already imported with OS Deployment Version 3.8, you must import them again to enable them for the in-place upgrade.
2. Run the in-place upgrade using one or more of the available tasks for the selected image. Specify the image product key if required.

You can use four different tasks to prepare and complete an in-place upgrade of your targets to Windows 10/11:

Task 202: Windows in-place upgrade

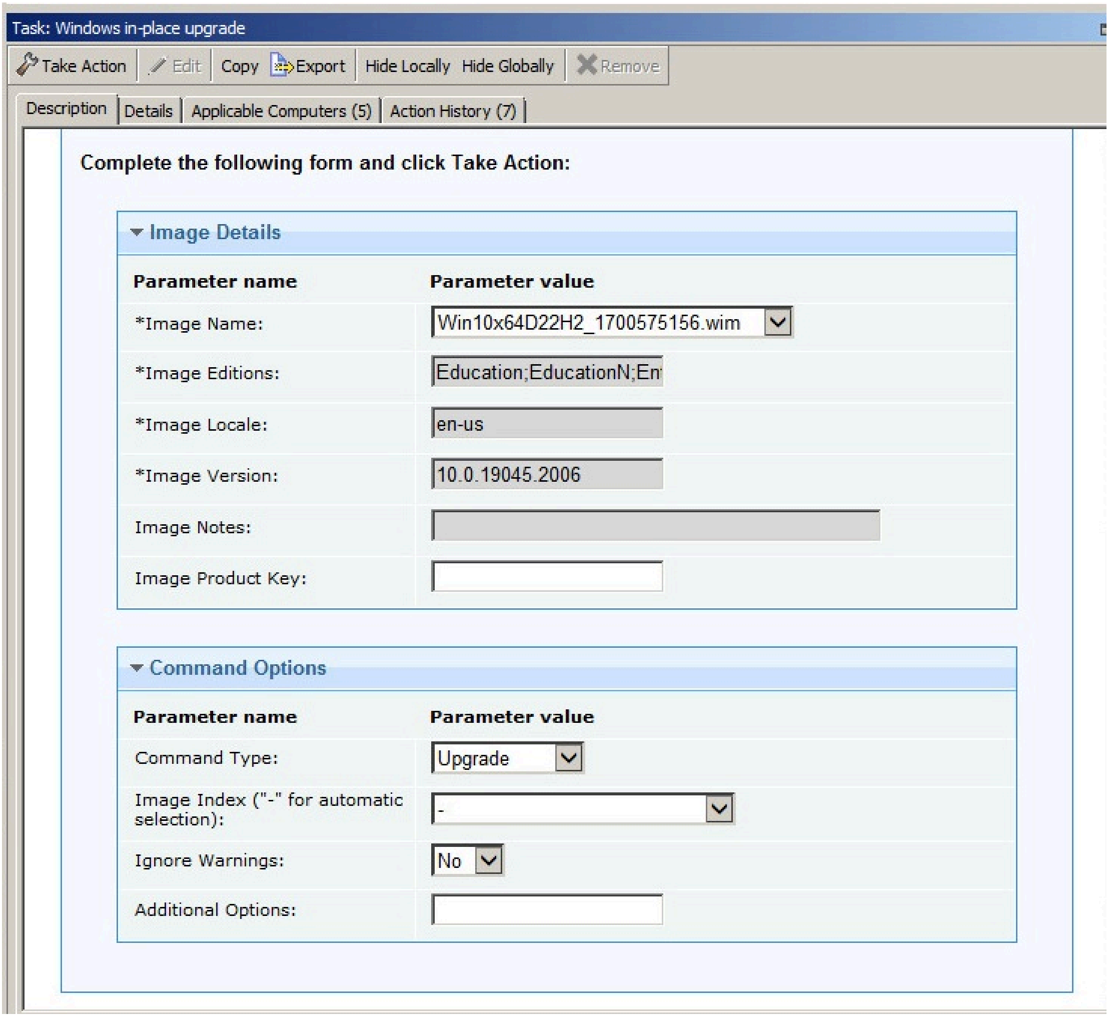
Command Type: Under the Command Options section, select a command type from the following processing options:

- `Upgrade` – Runs the upgrade process on the selected targets.
- `Check only` – Downloads the required binaries and starts the upgrade process in preview mode to detect any potential issues, without actually completing the upgrade. You can then run task 204 to complete the upgrade.
- `Prepare only` – Downloads the required binaries and prepares for the upgrade, without actually completing the upgrade. You can then run task 204 to complete the upgrade.

Ignore Warnings: Select "Yes" for the in-place upgrade to ignore any dismissible compatibility messages.

Image Index: Specify the index of the edition to apply if multiple editions in the image are applicable.

Additional Options: Specify any additional options that are used during the setup phase. Refer to the operating system manufacturer site for a list of commands you can specify for the setup phase.



Complete the following form and click Take Action:

Image Details

Parameter name	Parameter value
*Image Name:	Win10x64D22H2_1700575156.wim
*Image Editions:	Education;EducationN;En
*Image Locale:	en-us
*Image Version:	10.0.19045.2006
Image Notes:	
Image Product Key:	

Command Options

Parameter name	Parameter value
Command Type:	Upgrade
Image Index ("-" for automatic selection):	-
Ignore Warnings:	No
Additional Options:	

Task 203: Windows in-place upgrade - target validation

This task is useful to determine if the in-place upgrade can be completed successfully for the selected image on the selected targets. The task runs a set of validation steps and downloads the necessary files for the upgrade. The actual upgrade can be completed using task 202 if the validation is successful. If the task fails, investigate the reason of failure before running the actual upgrade. You can optionally specify the following target preparation options:

Increase Client PreCacheStageDiskLimit

The default client PreCacheStageDiskLimit value might be too small to accommodate the Windows 10/11 or Windows Server image for the upgrade. You can select to increase this limit to 7 gigabytes.

Increase Client CPU Usage:

You can reduce download and upgrade processing duration by increasing the client CPU usage.

Task 204: Windows in-place upgrade - run upgrade only

This task initiates the in-place upgrade process on the selected targets without performing any validation. You can run this task after running task 202 with the **Check Only** or **Prepare Only** processing options.

Important:

- The system language of the base operating system that is currently installed on the client system is the one that will be upgraded. If additional language packs were installed on the client, these are uninstalled during the upgrade.
- In-place upgrade of targets that have BitLocker disk encryption enabled is supported. The BitLocker will be temporarily disabled during the upgrade process and automatically enabled when the upgrade is complete.

Task 205: Windows in-place upgrade - multicast

This task offers the same processing options as task 202, but the image is deployed in multicast. To use this task, you must create a reimage profile for the image you want to deploy, and send it to the Bare Metal Server that manages the selected target. See Reimaging Windows Systems in multicast *(on page 160)*. You must select a Windows 10/11 or Windows Server setup image that you have imported using OS Deployment 3.9 or later. The target of your in-place upgrade must be connected to a Bare Metal Server at Version 7.1.1.20 at the latest available build level.

Important: If the image you selected is larger than 16 gigabytes in size, and you have enabled multicast, the options "Probe and Fall Back to Unicast and "Force Unicast using permanent cache" are disabled.

Note: When the upgrade is successful, the global status of the action is "Completed" but its step

```
pause while {pending restart}
```

will be shown as “Failed”, since the computer is restarted during this action to configure the new OS. But this does not invalidate the successful status of the upgrade.

Requirements and Limitations

The following requirements and limitations apply:

- If you upgrade to Windows 10, the client source operating system must be of the same architecture of the final OS (x86 or x64).
- If you upgrade to Windows 11, the client source operating system must be of x64 architecture.
- You cannot deploy an image of a base language different from base language of the client to be upgraded.

- The operating system edition and language of the image you are upgrading must match the language and edition of the base operating system. The upgrade process checks the edition that is currently installed on the client and upgrades it.
- You cannot capture (sysprep) a computer that was upgraded with an in-place installation.
- The upgrade process disables the built-in Administrator account on the client.
- You must disable any firewall or antivirus program on the target, before the deployment.

For troubleshooting information about in-place upgrades, see the BigFix Wiki page.

Chapter 10. Bare Metal deployments

You can install and manage BigFix for OS Deployment servers and create profiles for bare metal deployments.

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, BigFix Bare Metal Server must be installed on relays in your Endpoint Management environment. The installers can be uploaded to the **Bare Metal Server Manager** 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 Bare Metal 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 BigFix infrastructure.

Important:

- Before deploying Windows 11, check the system requirements at https://www.microsoft.com/en-us/windows/windows-11-specifications.
- Linux Bare Metal Deployments are not supported on UEFI targets that have the Secure Boot firmware option enabled. To complete the deployment successfully, you must disable this option on the target and also check that the Direct Boot option is disabled on the Bare Metal Server.
- Bare Metal deployments on Nutanix virtualization environment are supported only on virtual machines with UEFI firmware.
- Bare Metal deployments on Hyper-V guests are supported only on virtual machines created as "Generation 2".
- The PXE boot process of BigFix OSD bare metal server supports BIOS (Legacy) booted computers that are equipped with a PXE-compliant bootrom version 2.1.

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 74)*.

Bare Metal Deployment behavior of VMware ESXi

You can complete bare metal deployments of VMware ESXi Version 5 and later on BIOS targets. Unlike Windows and Linux targets, when the bare metal deployment completes successfully, VMware targets are automatically powered off. You must power them on manually. The BigFix Client is not installed during the deployment.

Windows Bare Metal Deployments on UEFI targets with the Secure Boot firmware option

If you are completing a Windows Bare Metal deployment on UEFI targets with the Secure Boot option, check the following requirements and limitations:

- If you did not enable the Windows Direct Boot environment, to complete a PXE boot successfully on UEFI targets, the Secure Boot firmware option must be disabled. For more information about enabling this feature, see Managing Bare Metal OS Deployment Servers *(on page 41)*
- For Bare Metal deployments on UEFI targets that have the Secure Boot firmware option enabled, The WinPE Direct Boot feature requires an Windows Bundle 3.9.06 or later created with WinPE 10.
- When you deploy on a new hardware model, the Direct boot feature adds the model to the driver library (binding grid) only if the WinPE contains the driver for the network card. If the network card driver is missing, the new model is not added to the driver library. To add the new computer model to the list you can choose one of the following options:
    - Complete a PXE boot from the UEFI target of the new model, without enabling the Direct Boot feature, and with the Secure Boot firmware option disabled on the target. You can enable both Secure Boot on the target and select the Direct boot option after the model has been added to the driver library. You must have the Bare Metal Extender component installed on the Bare Metal Server to use this option.

      Or
    - By using a BigFix client running on an installed computer of the same hardware model, connected to a BigFix environment.

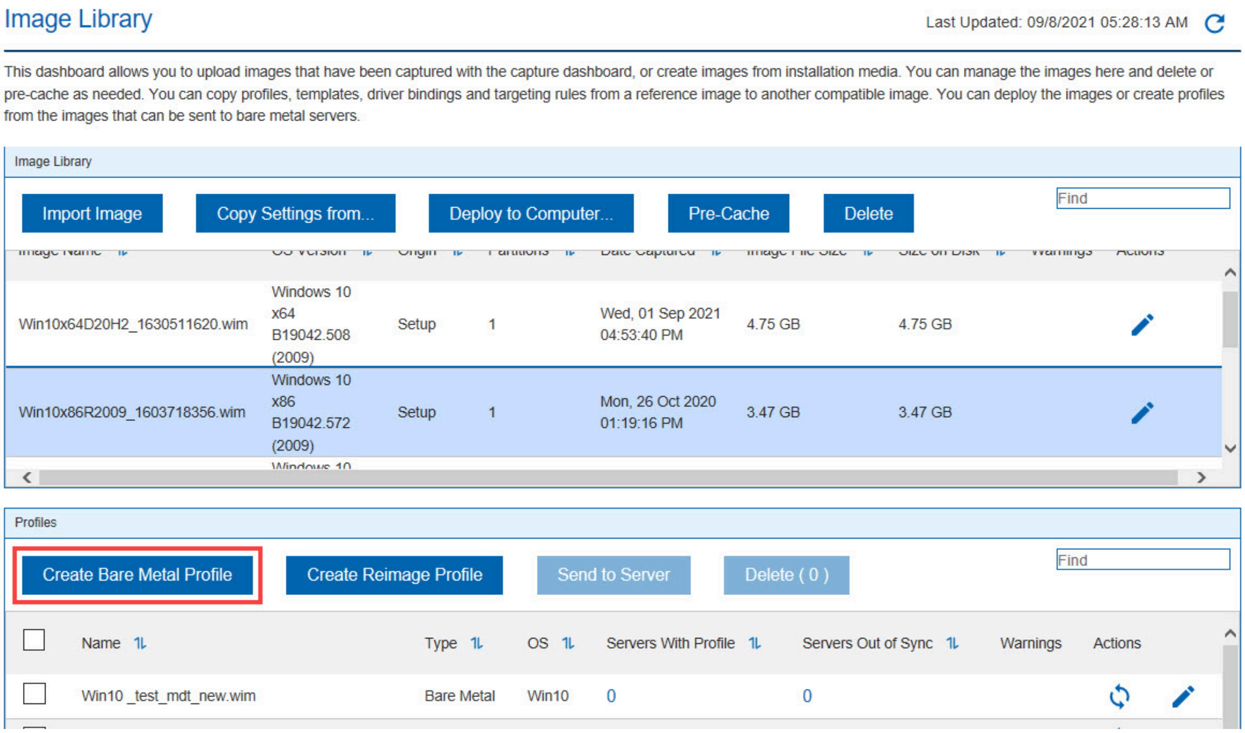
The drivers must be explicitly bound in the deployment engine binding matrix ("Current Manual Binding" column) in the Driver Bindings.

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, Linux and VMware Bare Metal targets, you create bare metal profiles from the Image Library. You then upload the profiles to the Server so that they can be deployed on the selected targets.

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



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 copy profiles, templates, driver bindings and targeting rules from a reference image to another compatible image. You can deploy the images or create profiles from the images that can be sent to bare metal servers.

Image Name	OS Version	Origin	Partitions	Date Captured	Image File Size	Size on Disk	Warnings	Actions
Win10x64D20H2_1630511620.wim	Windows 10 x64 B19042.508 (2009)	Setup	1	Wed, 01 Sep 2021 04:53:40 PM	4.75 GB	4.75 GB		✎
Win10x86R2009_1603718356.wim	Windows 10 x86 B19042.572 (2009)	Setup	1	Mon, 26 Oct 2020 01:19:16 PM	3.47 GB	3.47 GB		✎

□	Name	Type	OS	Servers With Profile	Servers Out of Sync	Warnings	Actions
□	Win10 _test_mdt_new.wim	Bare Metal	Win10	0	0		↻ ✎

A wizard with the information retrieved from the image is displayed. Depending on whether the type of image you select is a Linux or VMware 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 fields are already set but you can change them as appropriate.

If you have profiles that were created with earlier versions of OS Deployment, when you edit them, some fields might be preset to values that cannot be changed to ensure compatibility.

If your network supports multicast communication, and you want to deploy bare metal profiles using multicast, you can specify multicast parameters in the **Multicast** tab.

You can specify network configuration parameters for the targets receiving the profile by using the **Network** tab. The default network configuration is DHCP. If your targets have multiple interface cards (NICs) use the **Change Bare Metal Target Network Configuration** task (354) to configure them.

Note: If you specify a value enclosed by {} (curly brackets) for a field in the wizard or for a parameter value in the Manual tab, the enclosed value is considered as a relevance that will be evaluated. You must ensure that the syntax of the values enclosed by the curly brackets is correct. If you want to use the curly bracket as part of the field value without a relevance substitution, you must specify it with a double curly bracket at the beginning, for example:

```
{{yes}
```

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 derived from the image name and the type of profile (in this case Bare Metal). You can specify a maximum of 70 alphanumeric characters.

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

Hostname Rule

Specify the hostname rule that will be used to build the hostname, computer name, and full computer name of the target. You can specify values in the following forms:

- A prefix.
- A prefix and one or more variables.
- One or more variables.

There is a limit of 8 alphanumeric characters if you specify a prefix only. If you specify an asterisk (*) as prefix, the target hostname is set to a string formed by the characters `OSDOSD-` followed by a string assigned by Windows. Variables must be specified in the form `[variable]` enclosed by square brackets. You can concatenate variables. Allowed variables are:

- [IP] - IP Address of the primary interface that has performed a PXE boot
- [MAC] - Hardware Address of the primary interface that has performed PXE boot)

- [UUID] - System UUID as found in DMI (SMBIOS)
- [SN] - Serial number as found in DMI (SMBIOS)
- [AT] - Asset TAG as found in DMI (SMBIOS)
- [BBSN] - Base Board Serial Number as found in DMI (SMBIOS)

Every variable keyword supports a range extension, and you can decide to include only part of the information. The range starts at value zero. The value [IP3] corresponds to the last byte of the IP address. In IP addresses bytes are separated by dots. For example, if you specify a hostname rule of `pc-[IP3]` and the IP address of the target is `192.168.0.232`, the hostname becomes `pc-232`. If you specify `[IP0-2]`, the first three bytes of the IP address are included. For SN, UUID, AT, and BBSN values, the range corresponds to a substring. You can also add `R` at the end of the range to start it from the last character specified. Dots are always removed from the IP address in the final string.

Note: If the deployment is started from network boot media, the IP address used in the hostname rule is the one assigned during the network boot.

Windows Bundle

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

Deployment Final Action

Select a final action to complete on the target at the end of the deployment.

Restart

The target computer is restarted. This is the default action for all new profiles.

Shutdown

The target computer is shut down.

Log off

The target computer is logged off.

No action

The current user stays logged in. This is the default action for all profiles that were created with OS Deployment versions earlier than 3.8.

Note: If you are joining the target computer to a domain, only *"Restart "* or *" Shutdown"* are allowed. If you are editing a profile created with earlier versions of OS deployment and you select an Windows Bundle Version 3.8 or later, the default action is forced to *"Restart "*.

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 possible values, see Domain Credentials *(on page 158)*.

Optional fields:*""*

Product Key

Specify a valid Windows Product Key.

Assign relays

Select this option to disable automatic relay selection on the target system, and to set the Bare Metal server to which the target connects as Primary Relay, and the BigFix server as Secondary Relay. The following client settings for the target are updated at deployment time:

- `__RelaySelect_Automatic = 0`, to disable automatic relay selection
- `__RelayServer1`, which is set to the relay with the Bare Metal Server to which the target connects
- `__RelayServer2`, which is set to the BigFix server

To use this option, the Windows Bundle must be version 3.7 or later.

Client Settings

Use this field to set named variables that are assigned to the deployed computer. 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. You must specify the variables in a `NAME:VALUE` format. If you specify multiple variables, each one must be separated by a vertical bar `|`. After a deployment, you can display these values in the BigFix console by selecting the specified computer, and clicking *"Edit Computer Settings"*. The settings are listed under *"Custom Settings."* Examples of how to use client settings to configure the target after a deployment are available on the Endpoint Manager wiki at this link: Using the Client Settings field to configure targets during deployments.

A complete list of available client configuration settings, and a description of how to use them is available on the BigFix wiki at this link: Configuration Settings.

Prompt end user for properties

You can optionally select this option to prompt the user at the target computer for a hostname and network parameters. When the deployment starts on the target, a user interface is displayed and the user can configure the hostname and network settings for one or more network interfaces (NICs) available on the target system. This option is useful to view and check the network parameters that will be applied to the target at deployment time, and to change them if needed. For more information about the properties you can specify, see Specifying target network parameters at deployment time *(on page 199)*.

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 BigFix Bare Metal Server 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. If you are deploying the profile to UEFI targets with the Secure Boot option enabled you must select this option. For more information, see Enhanced error detection *(on page 154)*.

Bitlocker Method

Use this option to specify if you want Bitlocker on the target computer and which method to use. Bitlocker might not be supported on some editions of the operating system. The available choices are:

No Bitlocker

No Bitlocker will be enabled on the target computer.

On TPM

Bitlocker will be enabled and the computer will be protected with TPM only.

On TPM and use PIN

Bitlocker will be enabled and the computer will be protected with TPM and a pin. The pin must be specified in the field "Bitlocker PIN" which is a numeric field between 6 and 20 digits long.

On TPM and key

Bitlocker will be enabled and the computer will be protected with TPM and a startup key. The startup key will be created and saved on a USB Flash Drive. The startup key must be connected each time the computer starts. You can specify the drive letter of a removable disk where to save it in the field "Bitlocker key location". If not specified, the first available removable drive will be used.

On key

Bitlocker will be enabled and the computer will be protected with TPM and a startup key.

You can additionally create a recovery password for Bitlocker by selecting the option "Create Bitlocker recovery password". The file containing the password is saved in the same location of the Bitlocker key. If you are not using a Bitlocker key, the file is saved on the first available applicable device.

Note: When you enable Bitlocker, the "Disable enhanced error detection" option is automatically selected and cannot be unselected.

Note: For Bitlocker on server operating systems (such as Windows Server 2019), Windows Bundle Version 3.10.21 or later is required.

Set the high performance power plan

This option is available only for Windows 10/11 and, if selected, sets the high performance power plan on the target computer. This will also prevent the standby during the deployment on laptops when the lid is closed on AC. Windows Bundle later than Version 3.10.16 is required.

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

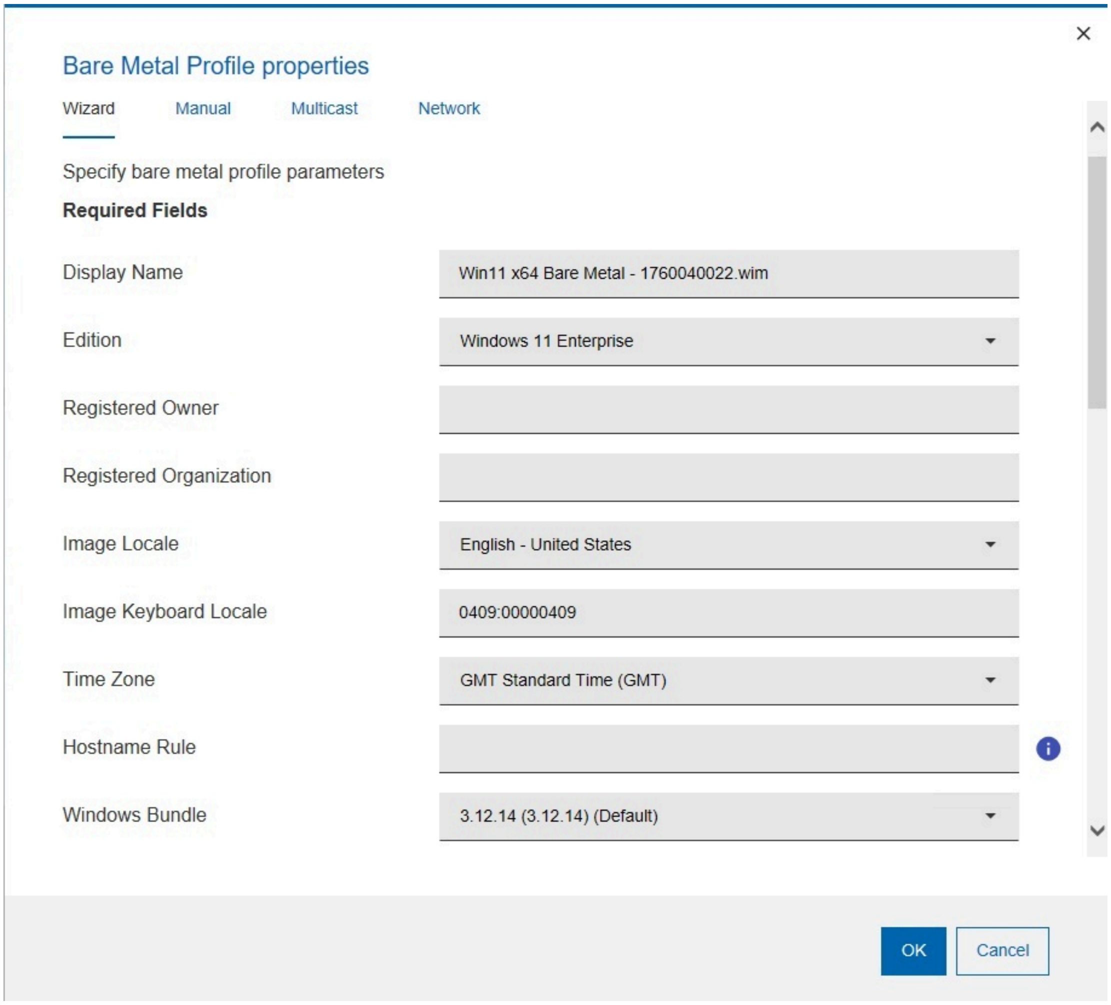
Required fields:

Edition

The operating system edition you are deploying. Expand the list to select a different edition.

Client Version

The displayed version depends on the Windows Bundle that is used. For Windows Bundles earlier than version 3.7, the best match is displayed. For Windows Bundle versions 3.7 or later, all client versions are supported. To select a Client version your Bare Metal OS Deployment server must be at version 7.1.1.18 or later.



Bare Metal Profile properties

Specify bare metal profile parameters

Required Fields

Display Name	Win11 x64 Bare Metal - 1760040022.wim
Edition	Windows 11 Enterprise
Registered Owner	
Registered Organization	
Image Locale	English - United States
Image Keyboard Locale	0409:00000409
Time Zone	GMT Standard Time (GMT)
Hostname Rule	
Windows Bundle	3.12.14 (3.12.14) (Default)

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

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 to confirm.

When you create bare metal profiles, you can specify the partition layout. The **Partition Mappings** section is the same as in Mapping partitions *(on page 154)* 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.

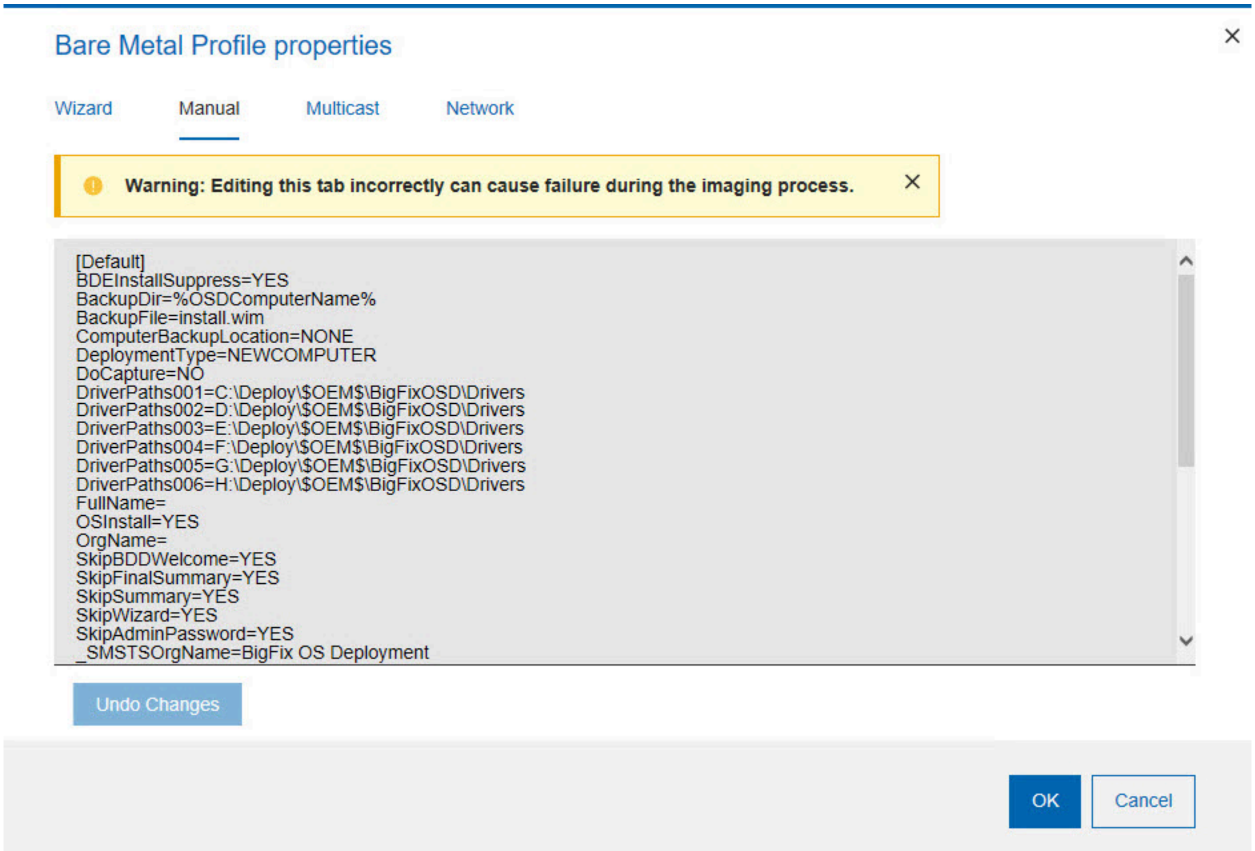
Note: You cannot edit boot partitions because the size of these partitions is fixed.

If you decide to repartition the disks on the target machine, the disks are formatted and the partitions are recreated on the target machine as you mapped them in the WIM. If you do not repartition the disks on the target machine, the same rules that are described for the number of partitions for reimaging 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.)

Use the **Manual** tab to manually specify customization options in the `CustomSettings.ini` file.


Bare Metal Profile properties
×
Wizard
Manual
Multicast
Network
Warning: Editing this tab incorrectly can cause failure during the imaging process.
×
Undo Changes
OK
Cancel

```
[Default]
BDEInstallSuppress=YES
BackupDir=%OSDComputerName%
BackupFile=install.wim
ComputerBackupLocation=NONE
DeploymentType=NEWCOMPUTER
DoCapture=NO
DriverPaths001=C:\Deploy\$OEM$\BigFixOSD\Drivers
DriverPaths002=D:\Deploy\$OEM$\BigFixOSD\Drivers
DriverPaths003=E:\Deploy\$OEM$\BigFixOSD\Drivers
DriverPaths004=F:\Deploy\$OEM$\BigFixOSD\Drivers
DriverPaths005=G:\Deploy\$OEM$\BigFixOSD\Drivers
DriverPaths006=H:\Deploy\$OEM$\BigFixOSD\Drivers
FullName=
OSInstall=YES
OrgName=
SkipBDDWelcome=YES
SkipFinalSummary=YES
SkipSummary=YES
SkipWizard=YES
SkipAdminPassword=YES
_SMSTSOrgName=BigFix OS Deployment
```

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 unexpected effects if not appropriately tested and verified.

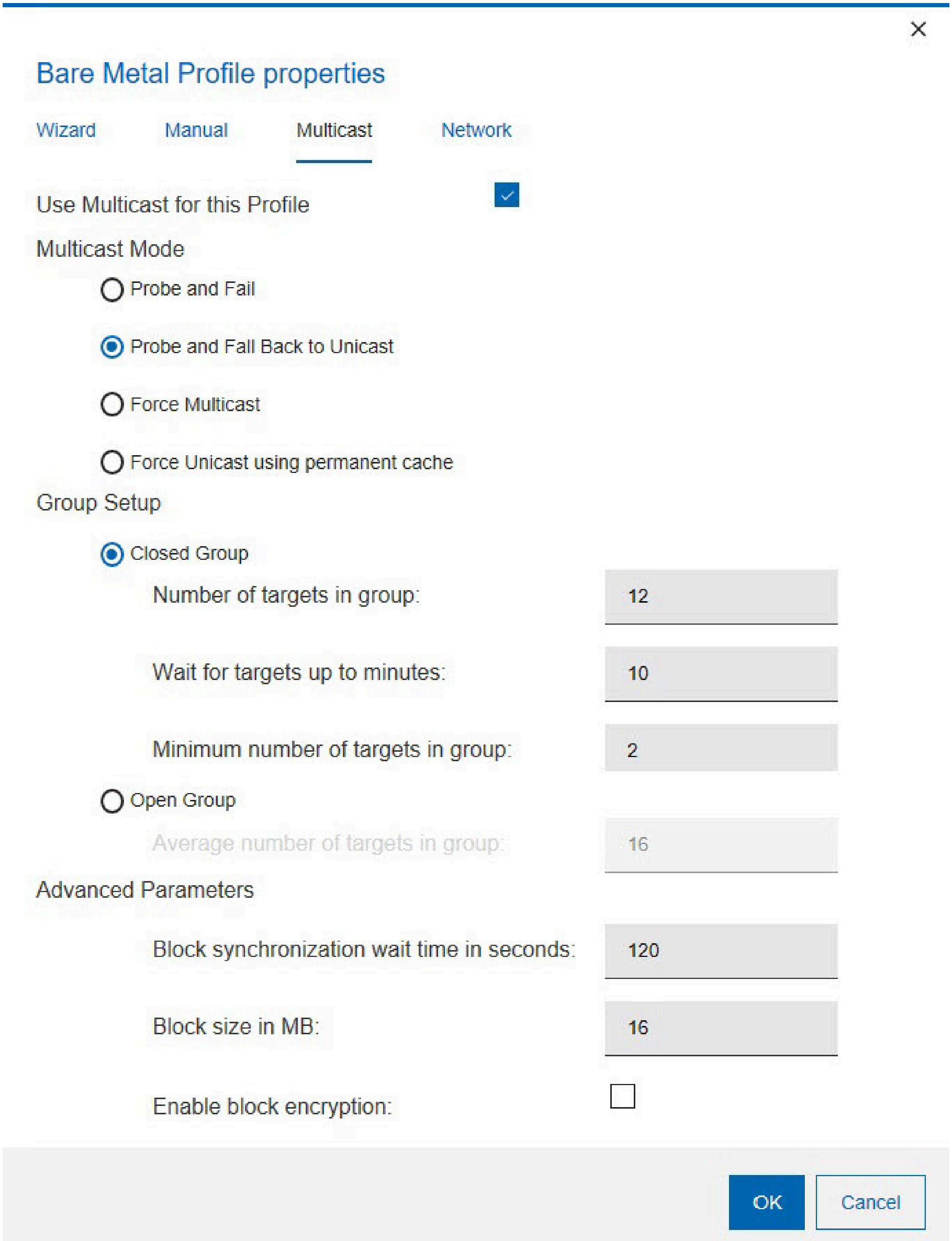
Requirements and limitations

For the Windows Bundle requirements needed to deploy Windows 10/11 and Windows Server 2016/2019/2022/2025 bare metal profiles, see Installing Windows Bundle Creators *(on page 68)*.

If you are deploying to a UEFI target with the Secure Boot firmware option enabled, your Windows Bundle must be Version 3.9.0.6 or later, and must have been imported with the option to overwrite the preinstallation environments (using "Yes" or "Auto" options when importing the bundle).

Deploying bare metal profiles in multicast

If you want to deploy a Bare Metal profile using multicast, you must specify the corresponding parameters in the **Multicast** tab:



Bare Metal Profile properties

Use Multicast for this Profile ☑

Multicast Mode

- ○ Probe and Fail
- ● Probe and Fall Back to Unicast
- ○ Force Multicast
- ○ Force Unicast using permanent cache

Group Setup

- ● Closed Group
  - Number of targets in group: 12
  - Wait for targets up to minutes: 10
  - Minimum number of targets in group: 2
- ○ Open Group
  - Average number of targets in group: 16

Advanced Parameters

- Block synchronization wait time in seconds: 120
- Block size in MB: 16
- Enable block encryption: □

To enable multicast for the profile, select the corresponding option. Default values for multicast deployment are provided. You can accept or change them, depending on the characteristics of your network:

Multicast Mode

Defines how the multicast distribution is managed on the targets at deployment time for the profile:

Probe and Fail

If the probe on the target fails, the deployment task also fails.

Probe and Fall Back to Unicast

If the probe on the target is successful, deployment occurs in multicast. If the probe fails, deployment of the profile occurs in unicast, using the Bare Metal Server cache, instead of the relay cache.

Force Multicast

Deployment on the target is forced to multicast regardless of probe results.

Force Unicast using permanent cache

Deployment on the target is completed in unicast using the Bare Metal Server cache. This option is useful when you want to ensure that all necessary files are available at deployment time.

Group Setup

Select the type of multicast group that is used for the deployment. You can accept or change the associated parameters.

Closed Group

Targets join the group as they are ready. When the following criteria are satisfied, the group is closed and distribution begins. This is the default.

Number of targets in group

Specify the maximum number of targets allowed in the group. The default value is 12.

Wait for targets up to minutes

Specify the maximum number of minutes to wait for targets before starting the multicast deployment. The default value is 10 minutes.

Minimum number of targets in group

Specify the minimum number of targets that must join for a multicast deployment. If the specified value is not reached, deployment is completed in unicast. The default value is 2.

Open Group

Targets can join the group as they are ready, at any time during deployment. You can change the associated parameter.

Average number of targets in group

Specify the average number of targets expected in the group. This value is used to optimize block synchronization. The closer the number of actual targets is to this value, the more efficient the multicast deployment. The default value is 16.

Advanced Parameters

Multicast advanced customization and tuning options that apply to both multicast group types.

Block synchronization wait time in seconds

Specify how many seconds the server must wait before sending the next block. This value is preset to 120 seconds. If you specify a value less than 5 seconds, the block synchronization wait time is forced to 5.

Block size in MB

The image is divided into blocks that are sent to the targets. This parameter sets the maximum size of the data blocks (in megabytes) sent in each transmission packet. The default value is 16 Megabytes.

Enable block encryption

Specify if the blocks must be encrypted during transmission.

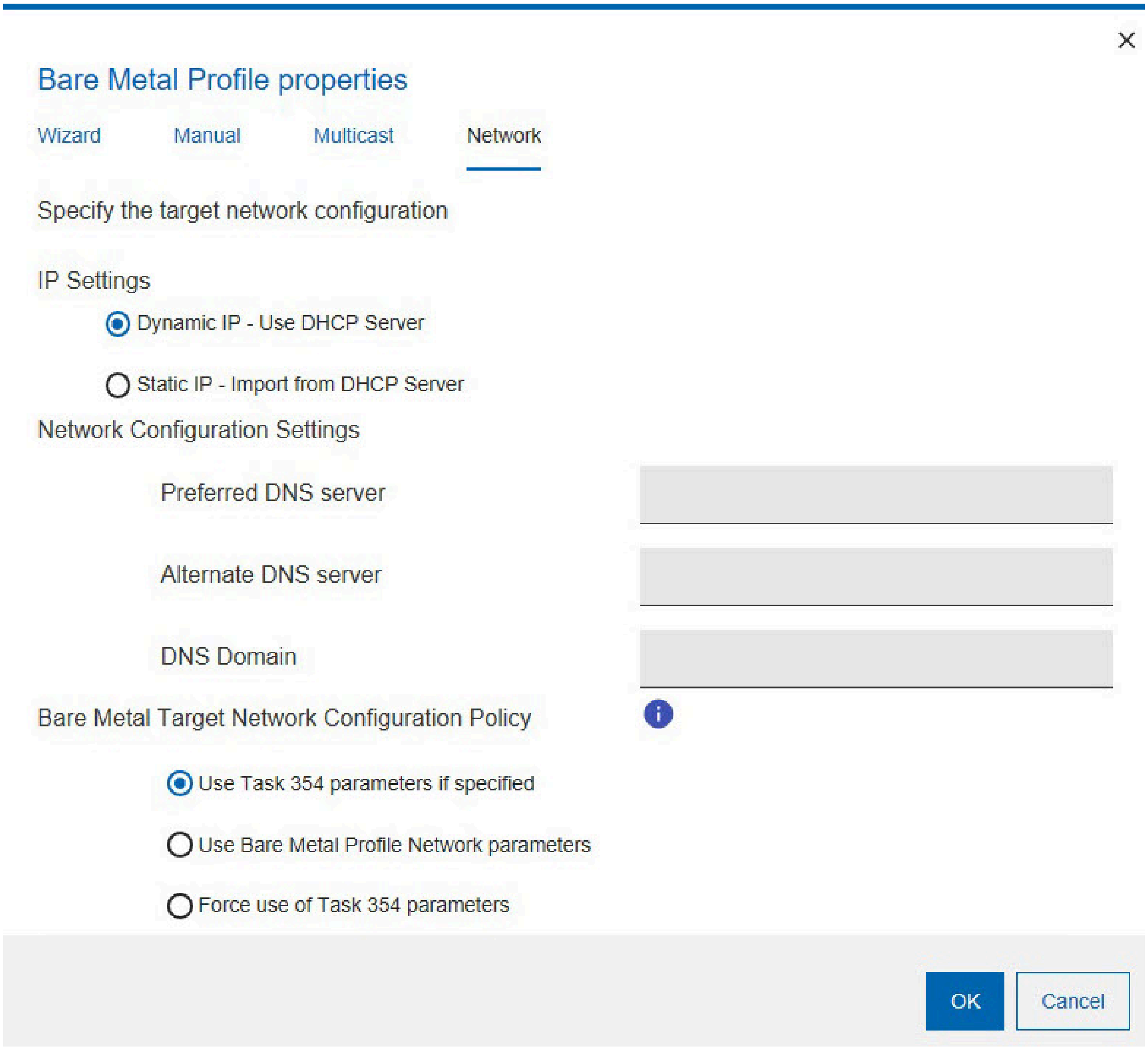
Before deploying bare metal profiles in multicast, you can check if multicast is enabled in the subnet that is used for Bare Metal deployments by running the **Probe Clients for Multicast Deployment** task (80) against a target in the same network. The BigFix client must be running on the target.

Important: If the image you selected is larger than 16 gigabytes in size, and you have enabled multicast, the options "Probe and Fall Back to Unicast and "Force Unicast using permanent cache" are disabled.

Specifying target network parameters

You can define bare metal target network configuration settings with Task 354, by specifying them in the bare metal profile in the **Network** tab, or using a combination of both.

The actual network configuration settings used by the targets receiving the profile is determined by the type of configuration (Static or Dynamic), by the selected configuration policy, and by the **Change Bare Bare Metal Target Network Configuration Settings** task (354), if you have run it on targets before deploying this profile.



Specify the target network configuration

IP Settings

● Dynamic IP - Use DHCP Server

○ Static IP - Import from DHCP Server

Network Configuration Settings

Preferred DNS server

Alternate DNS server

DNS Domain

Bare Metal Target Network Configuration Policy

● Use Task 354 parameters if specified

○ Use Bare Metal Profile Network parameters

○ Force use of Task 354 parameters

You can specify the following information:

IP Settings

Specify the type of configuration for the targets:

Dynamic IP - Use DHCP Server

Ths is the default selection. A dynamic IP address is assigned by the DHCP Server

Static IP - Import from DHCP Server

IP address, gateway, and network mask are imported from the DHCP Server

Network Configuration Settings

Optional. These parameters are used only if you select a static IP configuration. If your policy is to use the bare metal target configuration parameters previously defined with task 354, the parameters that were not already set with the task and specified in this section are considered. If there are parameters in common, the ones specified in the task take precedence. The parameters specified in this section are also used if you select a static IP configuration and you select to ignore any parameter defined with task 354. The configuration settings in this section are disabled if you are configuring a dynamic IP and you have selected to ignore any previously defined target network configuration using task 354).

Preferred DNS Server

Specify the IP address of the Preferred DNS server in your network

Alternate DNS Server

Specify the IP address of the Alternate DNS server in your network

DNS Domain

Specify The Domain Name Server name

Bare Metal Target Network Configuration Policy

Choose the configuration policy that must be applied to the selected targets for this profile.

Use Task 354 parameters if specified

If you have run the **Change Bare Metal Target Network Configuration Settings** task 354 to configure network parameters on targets of this profile, and you have selected this option, the parameters you specified in the task will have precedence over the same parameters specified in the profile. A field by field check is performed, and the profile parameters that were not specified in the task are also used.

Use Bare Metal Profile Network Parameters

Select this option if you want to ignore any previously defined target network parameters with task 354. Only the parameters specified in the profile are used.

Force use of Task 354 parameters

Select this option if you want to use only network parameters defined with Task 354. If you have not previously run task 354 on the targets of this profile, the deployment fails.

To set or change bare metal target network configuration settings using the corresponding task (ID 354), see Changing Bare Metal Target Network Configuration Settings *(on page 235)*.

Specifying target network parameters at deployment time

If you have selected the **Prompt end user for properties** option in the bare metal profile properties wizard, a user interface is displayed on the target system at deployment time. From this interface you can view and change the network interface settings, the hostname, and the partition mapping information that will be applied to the target. You can accept the displayed settings or change them as needed:

Network interface card (NIC)

All settings defined with task 354 or specified in the **Network** tab of the bare metal profile properties wizard are displayed. If the target has more than one network interface card (NIC), a separate configuration window is displayed for each one. Each interface is identified by the corresponding MAC address.

Hostname

Displays the hostname previously set with task 350 if used, or the final hostname value resulting from the application of the hostname rule you specified in the bare metal profile.

Note: If you set the hostname for a target at deployment time, this value is maintained for any subsequent bare metal deployments, independently of the hostname rule specified in the bare metal profile. To change the hostname, you can either use task 350 or deploy a new profile selecting the "Prompt end user for properties" option.

Partition mapping

Displays the partition mapping information that was specified using task 350. You can resize the partitions or accept the current mapping. If this information is not available, the related page is not displayed at the target.

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. Some field values are already set but you can change them as appropriate. The fields apply depending on whether the selected image is captured or created from installation media.

Important:

- If the relay component on your Bare Metal Server computer works only in https, you must select its Bare Metal Profile OS resource of the corresponding 64-bit version to deploy a 32-bit capture image. For Ubuntu 64-bit OS, the minimum OS resource level to work in https is 1804.
- Bare metal deployments of Linux Ubuntu Desktop are supported only for captured images. Setup images are not supported.
- The boot mode of the captured image must match the boot mode of the computer where the image is deployed. For example, if you select an image that was captured on a machine booted in UEFI mode, it must be deployed to a target that booted in UEFI mode.
- If you deploy a RHEL 8.0 (CentOS 8.0) capture image with LVM partitions, RHEL 8 (CentOS 8) version 1 resource is required instead of RHEL 8 (CentOS 8) version 0.
- If you deploy a SLES/SLED 12 capture image, patch level 3 resource is recommended for the operating systems SLES/SLED 12 patch level 3 or lower.

- If you deploy an Ubuntu capture image, a gateway (even fictitious) must be provided to the network. If not, a message will be prompted and you must manually confirm to continue.
- During the Ubuntu 22.04 Capture Image deployment, an "unable to locate any package file" message may appear after downloading the OS resource. This message will disappear shortly afterwards and the deployment task will continue without displaying any other error messages.

You can deploy your bare metal profiles in multicast, if your network supports it, by specifying the required parameters in the **Multicast** tab.

The default network configuration for targets is DHCP. You can specify different network configuration parameters for the targets receiving the profile by using the **Network** tab. If your targets have multiple network interface cards, use the **Change Bare Metal Target Network Configuration** task (354) to configure them.

Note: If you specify a value enclosed by {} (curly brackets) for a field in the wizard or for a parameter value in the Manual tab, the enclosed value is considered as a relevance that will be evaluated. You must ensure that the syntax of the values enclosed by the curly brackets is correct. If you want to use the curly bracket as part of the field value without a relevance substitution, you must specify it with a double curly bracket at the beginning, for example:

```
{{yes}
```

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

Required fields:

Display name

The name of the bare metal profile created from the 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.

Note: All locales are listed. Before choosing a locale, ensure that the locale is available in the image you are creating the bare metal profile for.

Time Zone

Select the time zone of the target operating system

Hostname Rule

Specify the hostname rule that will be used to build the hostname, computer name, and full computer name of the target. You can specify values in the following forms:

- A prefix.
- A prefix and one or more variables.
- One or more variables.

There is a limit of 8 alphanumeric characters if you specify a prefix only. If you specify an asterisk (*) as prefix, the target hostname is set to a string formed by the characters `OSDOSD-` followed by a string assigned by the operating system. Variables must be specified in the form `[variable]` enclosed by square brackets. You can concatenate variables. Allowed variables are:

- [IP] - IP Address of the primary interface that has completed a PXE boot
- [MAC] - Hardware Address of the primary interface that has completed the PXE boot)
- [UUID] - System UUID as found in DMI (SMBIOS)
- [SN] - Serial number as found in DMI (SMBIOS)
- [AT] - Asset TAG as found in DMI (SMBIOS)
- [BBSN] - Base Board Serial Number as found in DMI (SMBIOS)

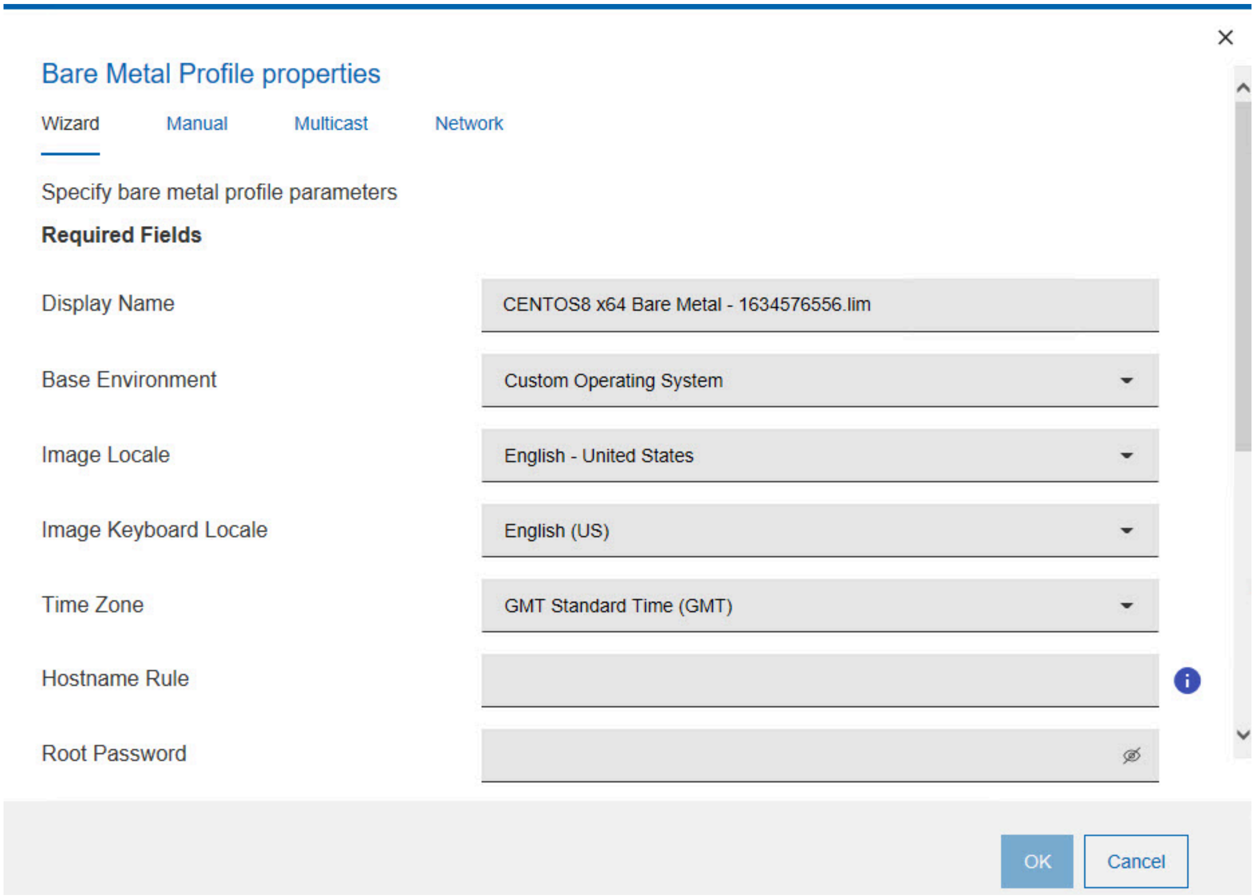
Every variable keyword supports a range extension, and you can decide to include only part of the information. The range starts at value zero. The value [IP3] corresponds to the last byte of the IP address. In IP addresses bytes are separated by dots. For example, if you specify a hostname rule of `pc-[IP3]` and the IP address of the target is `192.168.0.232`, the hostname becomes `pc-232`. If you specify `[IP0-2]`, the first three bytes of the IP address are included. For SN, UUID, AT, and BBSN values, the range corresponds to a substring. You can also add `R` at the end of the range to start it from the last character specified. Dots are always removed from the IP address in the final string.

Note: If the deployment is started from network boot media, the IP address used in the hostname rule is the one assigned during the network boot.

Root Password

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

The following figure displays a bare metal profile for an image created from installation media (Setup).



Bare Metal Profile properties

Specify bare metal profile parameters

Required Fields

Display Name	CENTOS8 x64 Bare Metal - 1634576556.lim
Base Environment	Custom Operating System
Image Locale	English - United States
Image Keyboard Locale	English (US)
Time Zone	GMT Standard Time (GMT)
Hostname Rule	
Root Password	

Optional fields

""

Prompt end user for properties

Select this option to prompt the user at the target computer for a hostname and network parameters. When the deployment starts on the target, a user interface is displayed and the user can configure the hostname and network settings for one or more network interfaces (NICs) available on the target system. For more information about the properties displayed at the target, see Specifying target network parameters at deployment time, and Changing Bare Metal Target Network Configuration Settings *(on page 235)*.

Installer Kernel parameters

Specify one or more optional kernel parameters for the Linux installer, and the corresponding values if required.

Kernel parameters

Specify one or more optional kernel parameters for the installed Linux operating system.

Kernel parameters have the following syntax:

```
#<model>#<parameter>#
```

Where the model refers to the computer model of the target to which the parameter is applied, and the parameter can be a single keyword or in the form `key=value`. Each model/parameter pair must be separated by a blank character. You can use the asterisk as a wildcard character. For example, `#vm*#<parameter>#` applies the specified parameter to all models with names beginning with *"vm"*. The model field is not case-sensitive.

You can also replace existing values for parameters. For example, if you want to set a lower screen resolution on all VMware virtual machines while defining a higher screen resolution for all other available models, write the following:

```
#vm*#video=800x600-24#video=1024x800-32#
```

Assign Relays

Select this option to disable automatic relay selection on the target system, and to set the Bare Metal server to which the target connects as Primary Relay, and the BigFix server as Secondary Relay. The following client settings for the target are updated at deployment time:

- `__RelaySelect_Automatic = 0`, to disable automatic relay selection
- `__RelayServer1`, which is set to the relay with the Bare Metal Server to which the target connects
- `__RelayServer2`, which is set to the BigFix server

Client Settings

Use this field to set named variables that are assigned to the deployed computer. 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. You must specify the variables in a `NAME:VALUE` format. If you specify multiple variables, each one must be separated by a vertical bar `|`. After a deployment, you can display these values in the BigFix console by selecting the specified computer, and clicking *"Edit Computer Settings"*. The settings are listed under *"Custom Settings."* Examples of how to use client settings to configure the target after a deployment are available on the Endpoint Manager wiki at this link: Using the Client Settings field to configure targets during deployments.

For a complete list of available client configuration settings, and a description of how to use them, see BigFix Configuration Settings.

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. When the specified time expires, the profile is automatically installed on the target.

SELinux Policy

This field is available only for RHEL and CentOS. Here you can select a selinux policy to apply. The values are:

- **default**: For setup image. Lets the operating system apply its default policy by not specifying any policy.
- **no change**: For captured image. Preserves the policy configured in the captured image.
- **disabled**: Configures selinux policy as disabled.
- **permissive**: Configures selinux policy as permissive.
- **enforcing**: Configures selinux policy as enforcing. If you select this selinux policy, the configured type will be automatically set as "Targeted".

Note: With the SELinux support, if policy is not specified, it will be the default of the OS level being deployed. If you want to continue to have the SELinux policy disabled, edit the profile and set the value disabled.

Unique fields for images created from installation media (setup)

Required fields

Base Environment

Pre-defined sets of packages with a specific purpose. If you want to manually manage the packages, select "No Environment" from the list. This field is available only for RHEL 7, RHEL 8, RHEL 9, CentOS 7, and CentOS 8.

Client Version

Specify the version of the BigFix client to be installed on the target. The default selection is the same version as the BigFix server.

Optional fields

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 Changing Firewall settings *(on page 177)*.

Unique fields for captured images

Required fields

Linux OS Resource

The OS Resource to be used for the deployment of the selected image. This field displays the OS resource that best matches the selected image.

Optional fields

Reset Captured Client Settings

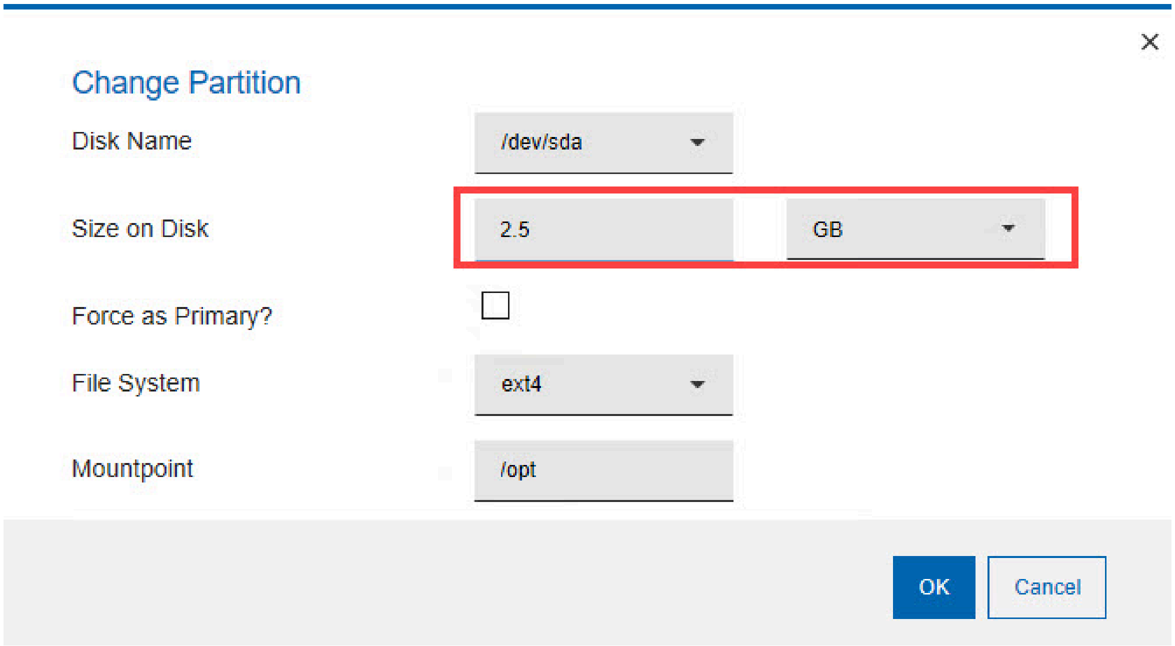
Selecting this option will delete any existing previously defined client settings in the selected captured image.

Important: When you deploy captured images, on the target, the Logical Volume configuration (LVM) is deleted only on the disks of the captured image. If you want to delete the Logical Volume configuration on all disks of the target receiving the Bare Metal Profile, you must specify `rboforcelvmcleanup` in the **Installer Kernel parameter** field of the Optional fields section.

Using the Partition Editor

Depending on the type of image, different partitioning actions are available. To work with partitions, expand the **Partition Editor** section of the wizard tab. If you selected a captured image, the partition editor displays the partition layout of the captured reference machine. You cannot add new partitions to captured images, but you can edit primary partitions and logical volumes to change their sizes. You can complete the following action:

- Resize selected primary partitions and logical volumes. Highlight the partition and click the edit icon to change the size.



Change Partition

Disk Name: /dev/sda

Size on Disk: 2.5 GB

Force as Primary? □

File System: ext4

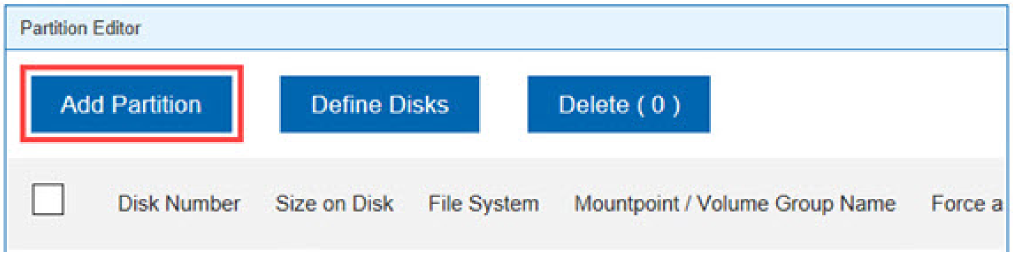
Mountpoint: /opt

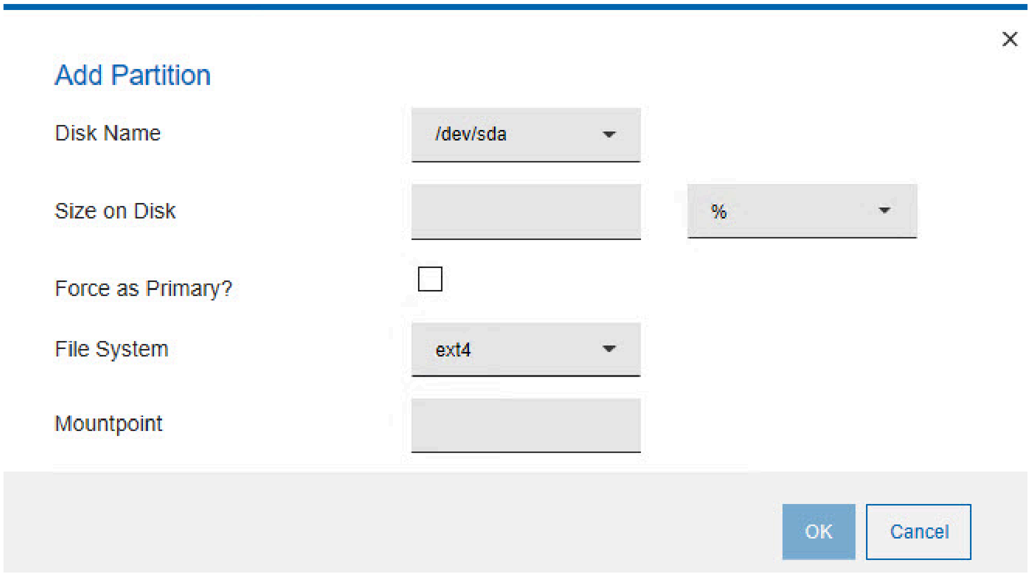
You can specify the size in kilobytes, megabytes, gigabytes, terabytes and percentages. If more than one partition is defined, specifying a value of one hundred percent (100%) for a partition, means that it will occupy all remaining space after the specified sizes have been allocated to the other partitions. You cannot delete captured partitions.

If you are deploying images imported from installation media (`setup`) you do not have to edit partitions. In this case, the default partitioning is applied. If you want to edit partitions, you can specify a partition layout by expanding the **Partition Editor** section of the wizard tab. Consider the following partitioning use cases, depending on the characteristics of your target systems:

I want to define multiple partitions on a single physical disk:

1. Define the partitions on the disk by clicking the corresponding option:





Add Partition

Disk Name: /dev/sda

Size on Disk: %

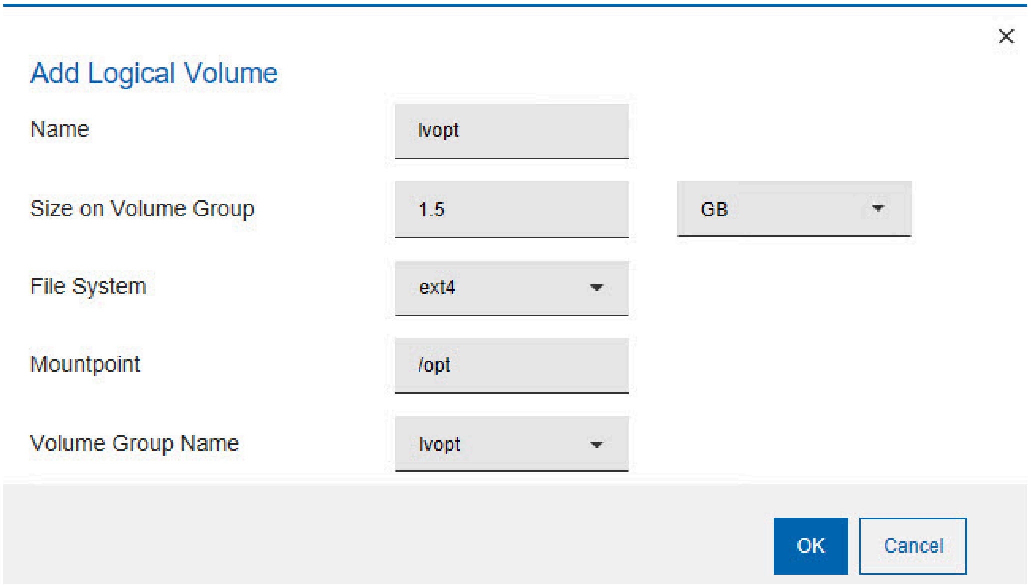
Force as Primary? □

File System: ext4

Mountpoint:

You can add partitions or logical volumes. Specify the required information.

2. If you want to add a logical volume, select `LVM` from the File system list, and specify a Volume Group name. When you click **OK** the **Logical volume Editor** becomes available at the bottom of the section. Click **Add Logical volume** and specify the characteristics of the logical volume.



Add Logical Volume

Name: lvopt

Size on Volume Group: 1.5 GB

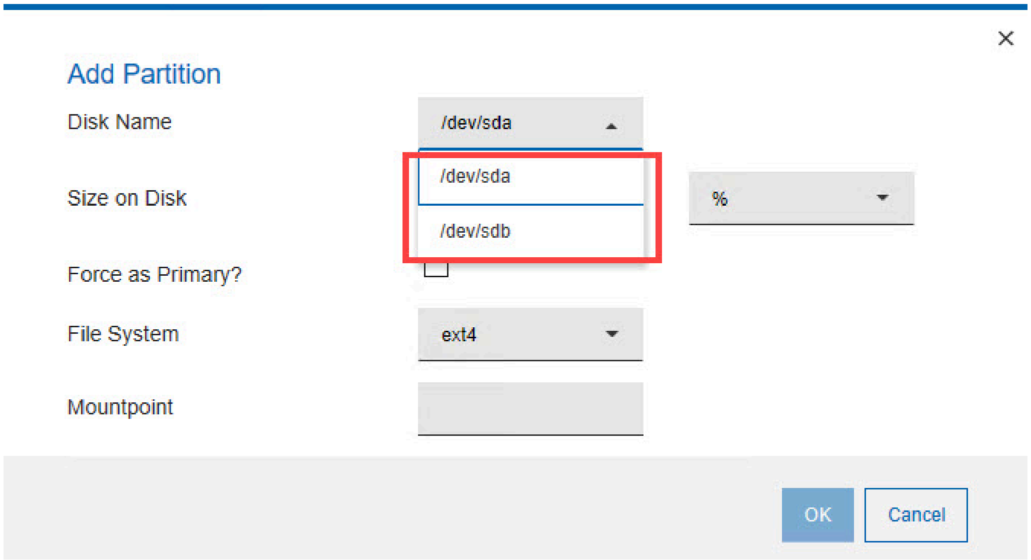
File System: ext4

Mountpoint: /opt

Volume Group Name: lvopt

I want to define multiple partitions on different physical disks

1. Define the physical disks on the machine that receives the profile. Click **Define Disks** The default disk name is `/dev/sda`. To define more physical disks, specify each disk element separated by a semicolon. For example: `/dev/sda;/dev/sdb`. Click **OK** to save your changes.
2. Click **Add Partition** and select a disk that you defined in the previous step to partition it.



Add Partition

Disk Name: /dev/sda

Size on Disk: %

Force as Primary? □

File System: ext4

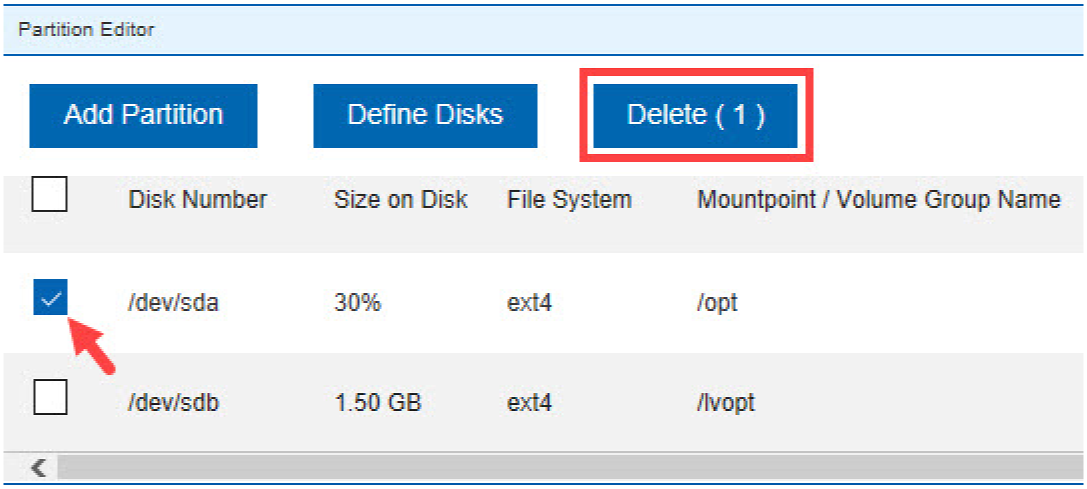
Mountpoint:

Specify the size of the partition, mount point and file system type. You can set the disk as primary. Specify the partition mount point. To add a logical volume, select **LVM** from the File System List, and specify a Logical Volume Group name. When you click **OK** the **Logical volume**

Editor becomes available at the bottom of the section. Click **Add Logical volume** and specify the characteristics of the logical volume.

3. Repeat step 2 for each physical disk that you defined.

You can delete partitions of Linux images imported from installation media (setup) by selecting the partition you want to delete and click the corresponding option.



□	Disk Number	Size on Disk	File System	Mountpoint / Volume Group Name
☑	/dev/sda	30%	ext4	/opt
□	/dev/sdb	1.50 GB	ext4	/lvopt

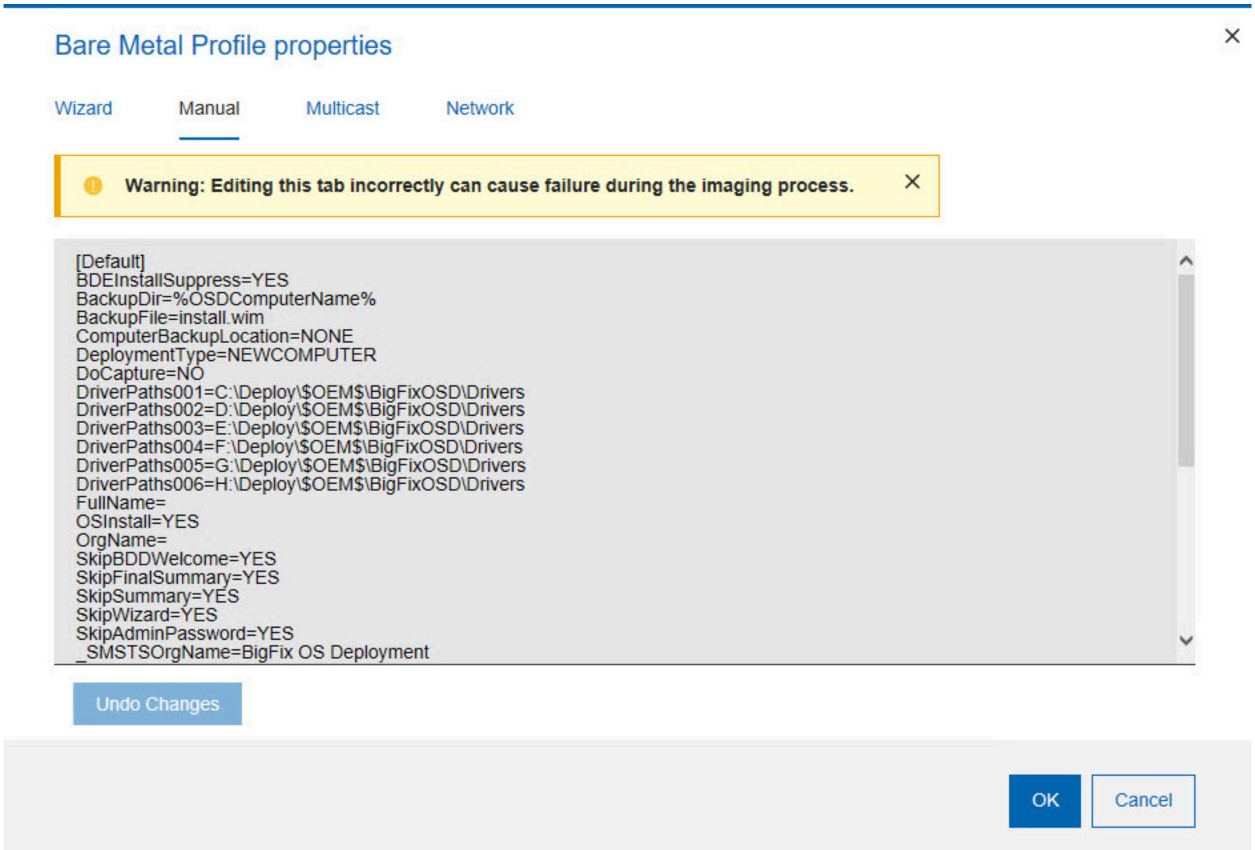
You cannot delete the captured partitions.

Important:

- You can define up to three primary partitions, by selecting the appropriate option. If you want to deploy the profile in multicast to BIOS targets, you can define a maximum of two primary partitions.
- If you are deploying a Linux Setup image in multicast on a target that has existing Windows partitions not on the primary disk, these partitions will not be formatted. This must be considered when defining multiple disks using the partition editor in the profile.
- When you define multiple partitions for a disk, make sure you specify the size of at least one of the partitions using percentage (%) not with a fixed value, so as to optimize disk allocation and avoid disk space errors. This best practice applies to Logical Volumes too. When you define a fixed size for a Volume Group, for example 10 gigabytes, the actual size available to create Logical Volumes is slightly less (usually in the order of a few megabytes). To avoid space allocation problems, when you define Volume Groups you should specify the size of at least one Logical Volume in percentage (%).
- When you edit a profile containing a partition layout, if you change the disk mapping, the current layout is erased. A warning message is issued asking you to confirm or to cancel the operation.
- In RHEL deployment, if you define one or more partitions (not in LVM) in percentage (%), the partitions (in percentage (%)) will cover the entire disk not assigned to the fixed size proportionally to their percentage (%) value, even if the sum does not reach the 100%, so no free space will be left for the missing percentage to reach 100%.

Manual tab settings

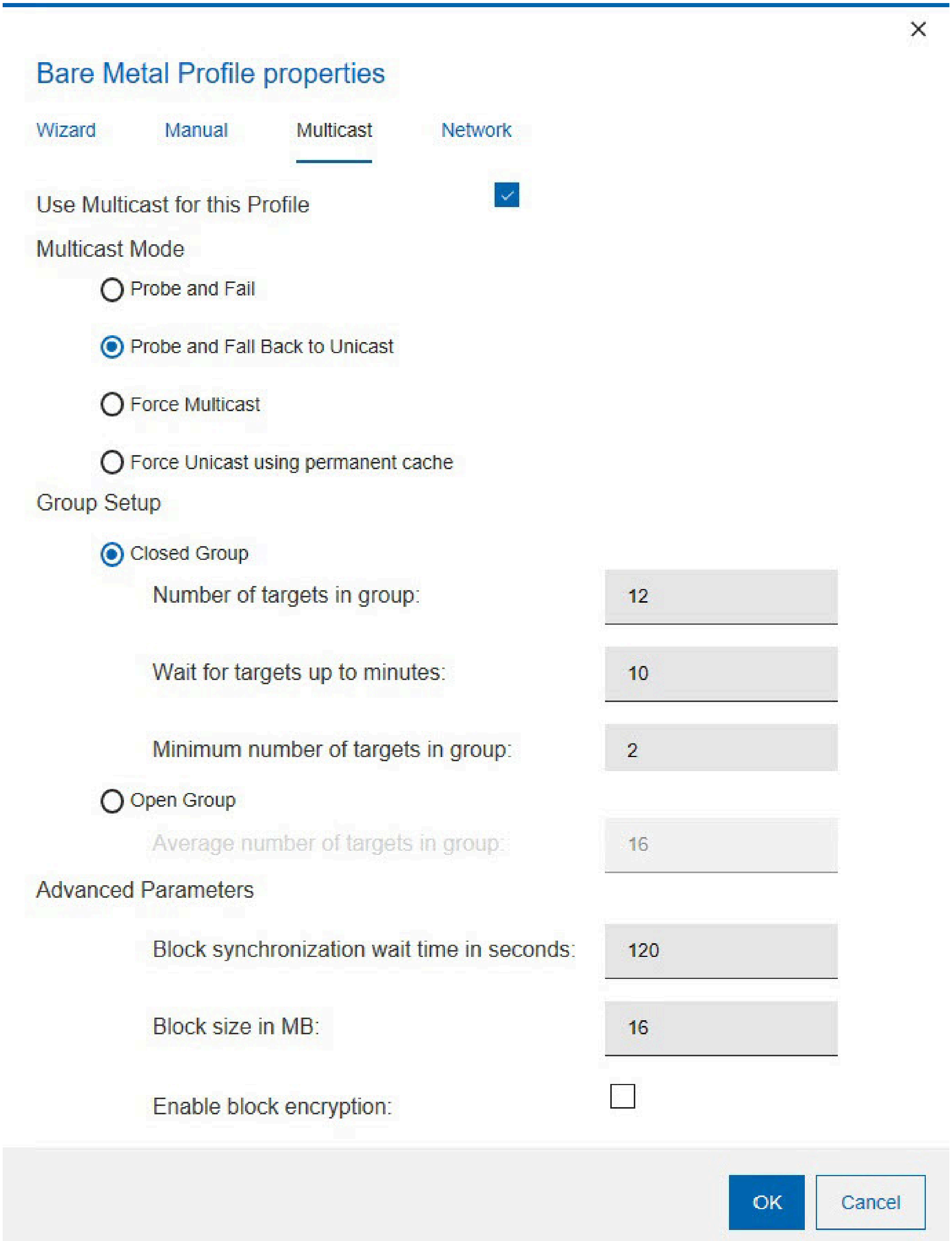
Using the **Manual** tab, you can customize the installation of Linux images imported from installation media (Setup) with specific settings that are not available in the wizard. Uncomment the settings you want to customize and include in your deployment. For more information about the customization of the configuration files, see Linux configuration options *(on page 167)* or refer to the specific Linux vendor documentation.


Bare Metal Profile properties
Wizard
Manual
Multicast
Network
Warning: Editing this tab incorrectly can cause failure during the imaging process.
Undo Changes
OK
Cancel

```
[Default]
BDEInstallSuppress=YES
BackupDir=%OSDComputerName%
BackupFile=install.wim
ComputerBackupLocation=NONE
DeploymentType=NEWCOMPUTER
DoCapture=NO
DriverPaths001=C:\Deploy\$OEM$\BigFixOSD\Drivers
DriverPaths002=D:\Deploy\$OEM$\BigFixOSD\Drivers
DriverPaths003=E:\Deploy\$OEM$\BigFixOSD\Drivers
DriverPaths004=F:\Deploy\$OEM$\BigFixOSD\Drivers
DriverPaths005=G:\Deploy\$OEM$\BigFixOSD\Drivers
DriverPaths006=H:\Deploy\$OEM$\BigFixOSD\Drivers
FullName=
OSInstall=YES
OrgName=
SkipBDDWelcome=YES
SkipFinalSummary=YES
SkipSummary=YES
SkipWizard=YES
SkipAdminPassword=YES
_SMSTSOrgName=BigFix OS Deployment
```

Deploying bare metal profiles in multicast

To deploy bare metal profiles using multicast, specify the parameters in the **Multicast** tab. Multicast deployments are supported for Linux captured images on both BIOS and UEFI targets. Multicast deployments of Linux images imported from installation media (Setup) are limited to Linux RedHat version 6, 7 and 8 and CentOS Linux 7, 8 images on BIOS targets only. If you are deploying a RedHat/CentOS image on a BIOS target, the number of primary partitions you can define for the target is limited to two.



Bare Metal Profile properties

Use Multicast for this Profile ☑

Multicast Mode

○ Probe and Fail

● Probe and Fall Back to Unicast

○ Force Multicast

○ Force Unicast using permanent cache

Group Setup

● Closed Group

Number of targets in group: 12

Wait for targets up to minutes: 10

Minimum number of targets in group: 2

○ Open Group

Average number of targets in group: 16

Advanced Parameters

Block synchronization wait time in seconds: 120

Block size in MB: 16

Enable block encryption: □

Important:

- Multicast deployments of Linux setup images are limited to BIOS only.
- When deploying Linux setup images in multicast, if you define multiple partitions for the first disk (/dev/sda), you must leave some free space that is needed locally to store the image file, or alternatively, specify the size of at least one of the partitions using a percentage value (%). The amount of the minimum required free space is the size of the Image File Size (as reported in the Image Library Dashboard) +1 GB.
- CentOS Linux 7 Minimal ISO does not support multicast.

To enable multicast for the profile, select the corresponding option. Default values for multicast deployment are provided. You can accept or change them, depending on the characteristics of your network:

Multicast Mode

Defines how the multicast distribution is managed on the targets at deployment time for the profile:

Probe and Fail

If the probe on the target fails, the deployment task also fails.

Probe and Fall Back to Unicast

If the probe on the target is successful, deployment occurs in multicast. If the probe fails, deployment of the profile occurs in unicast, using the Bare Metal Server cache, instead of the relay cache.

Force Multicast

Deployment on the target is forced to multicast regardless of probe results.

Force Unicast using permanent cache

Deployment on the target is completed in unicast using the Bare Metal Server cache. This option is useful when you want to ensure that all necessary files are available at deployment time.

Group Setup

Select the type of multicast group that is used for the deployment. You can accept or change the associated parameters.

Closed Group

Targets join the group as they are ready. When the following criteria are satisfied, the group is closed and distribution begins. This is the default.

Number of targets in group

Specify the maximum number of targets allowed in the group. The default value is 12.

Wait for targets up to minutes

Specify the maximum number of minutes to wait for targets before starting the multicast deployment. The default value is 10 minutes.

Minimum number of targets in group

Specify the minimum number of targets that must join for a multicast deployment. If the specified value is not reached, deployment is completed in unicast. The default value is 2.

Open Group

Targets can join the group as they are ready, at any time during deployment. You can change the associated parameter.

Average number of targets in group

Specify the average number of targets expected in the group. This value is used to optimize block synchronization. The closer the number of actual targets is to this value, the more efficient the multicast deployment. The default value is 16.

Advanced Parameters

Multicast advanced customization and tuning options that apply to both multicast group types.

Block synchronization wait time in seconds

Specify how many seconds the server must wait before sending the next block. This value is preset to 120 seconds. If you specify a value less than 5 seconds, the block synchronization wait time is forced to 5.

Block size in MB

The image is divided into blocks that are sent to the targets. This parameter sets the maximum size of the data blocks (in megabytes) sent in each transmission packet. The default value is 16 Megabytes.

Enable block encryption

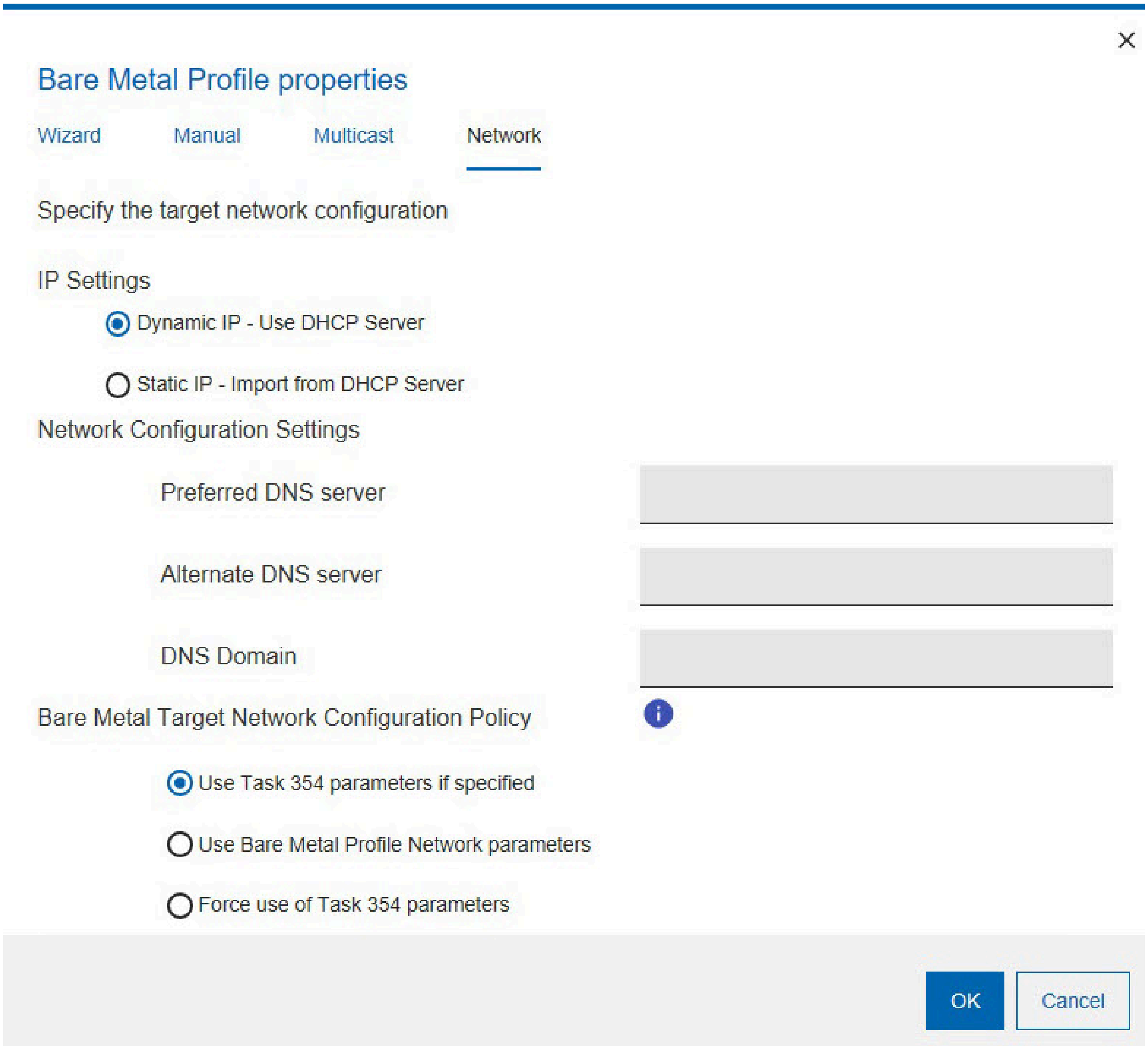
Specify if the blocks must be encrypted during transmission.

Before deploying bare metal profiles in multicast, you can check if multicast is enabled in the subnet that is used for Bare Metal deployments by running the **Probe Clients for Multicast Deployment** task (80) against a target in the same network. The BigFix client must be running on the target.

Specifying target network parameters

You can define bare metal target network configuration settings with Task 354, by specifying them in the bare metal profile in the **Network** tab, or using a combination of both.

The actual network configuration settings used by the targets receiving the profile is determined by the type of configuration (Static or Dynamic), by the selected configuration policy, and by the **Configure Bare Metal Target Network parameters** task (354), if you have run it on targets before deploying this profile.



Bare Metal Profile properties

Wizard Manual Multicast Network

Specify the target network configuration

IP Settings

● Dynamic IP - Use DHCP Server

○ Static IP - Import from DHCP Server

Network Configuration Settings

Preferred DNS server

Alternate DNS server

DNS Domain

Bare Metal Target Network Configuration Policy

● Use Task 354 parameters if specified

○ Use Bare Metal Profile Network parameters

○ Force use of Task 354 parameters

You can specify the following information:

IP Settings

Specify the type of configuration for the targets:

Dynamic IP - Use DHCP Server

Ths is the default selection. A dynamic IP address is assigned by the DHCP Server

Static IP - Import from DHCP Server

IP address, gateway, and network mask are imported from the DHCP Server

Network Configuration Settings

Optional. These parameters are used only if you select a static IP configuration. If your policy is to use the bare metal target configuration parameters previously defined with task 354, the parameters that were not already set with the task and specified in this section are considered. If there are parameters in common, the ones specified in the task take precedence. The parameters specified in this section are also used if you select a static IP configuration and you select to ignore any parameter defined with task 354. The configuration settings in this section are disabled if you are configuring a dynamic IP and you have selected to ignore any previously defined target network configuration using task 354).

Preferred DNS Server

Specify the IP address of the Preferred DNS server in your network

Alternate DNS Server

Specify the IP address of the Alternate DNS server in your network

DNS Domain

Specify The Domain Name Server name

Domain Search order

Specify the domain search order. Each domain name must be separated by blanks.

Bare Metal Target Network Configuration Policy

Choose the configuration policy that must be applied to the selected targets for this profile.

Use Task 354 parameters if specified

If you have run the **Change Bare Metal Target Network Configuration Settings** task 354 to configure network parameters on targets of this profile, and you have selected this option, the parameters you specified in the task will have precedence over the same parameters specified in the profile. A field by field check is performed, and the profile parameters that were not specified in the task are also used.

Use Bare Metal Profile Network Parameters

Select this option if you want to ignore any previously defined target network parameters with task 354. Only the parameters specified in the profile are used.

Force use of Task 354 parameters

Select this option if you want to use only network parameters defined with Task 354. If you have not previously run task 354 on the targets of this profile, the deployment fails.

To set or change bare metal target network configuration settings using the corresponding task (ID 354) , see Changing Bare Metal Target Network Configuration Settings *(on page 235)*.

Specifying target network parameters at deployment time

If you have selected the **Prompt end user for properties** option in the bare metal profile properties wizard, a user interface is displayed on the target system at deployment time. From this interface you can view and change the network interface settings, the hostname, and the partition mapping information that will be applied to the target. You can accept the displayed settings or change them as needed:

Network interface card (NIC)

All settings defined with task 354 or specified in the **Network** tab of the bare metal profile properties wizard are displayed. If the target has more than one network interface card (NIC), a separate configuration window is displayed for each one. Each interface is identified by the corresponding MAC address.

Hostname

Displays the hostname previously set with task 350 if used, or the final hostname value resulting from the application of the hostname rule you specified in the bare metal profile.

Note: If you set the hostname for a target at deployment time, this value is maintained for any subsequent bare metal deployments, independently of the hostname rule specified in the bare metal profile. To change the hostname, you can either use task 350 or deploy a new profile selecting the "Prompt end user for properties" option.

Partition mapping

Displays the partition mapping information that was specified using task 350. You can resize the partitions or accept the current mapping. If this information is not available, the related page is not displayed at the target.

Use grub2 bootloader for Linux deployment on UEFI targets

For UEFI deployment of Linux images (both setup and capture), if the OS resource that is associated to the bare metal profile (the resource selected in the bare metal profile wizard for the captured images, the resource specific for the OS version and update level for setup images) does not include the grub2 bootloader, the default bootloader elilo.efi is used to launch the specific Linux installer. If it does not work on your hardware, you can replace it with grub2 using the following procedure.

Pre-requisites: You need the `shim.efi` file or the `BOOTX64.efi` file (depending on the version of OS you are extracting it from) from the shim package and the `grubx64.efi` file from the grub2-efi package in the ISO image file.

The packages are `shim-x64-<version>.rpm` and `grub2-efi-x64-<version>.rpm`, where the <version> depends on the version of the OS on the dvd that you are extracting it from. For example, `shim-x64-15-2.el7.x86_64.rpm` and `grub2-efi-x64-2.02-0.80.el7.x86_64.rpm`.

Note:

- It is not mandatory to extract the files from the same version of the OS that you are going to deploy.
- The DHCP server must provide the option "next-server" with the value of the bare metal server IP address. On some DHCP servers, this options is provided together with the option 66.

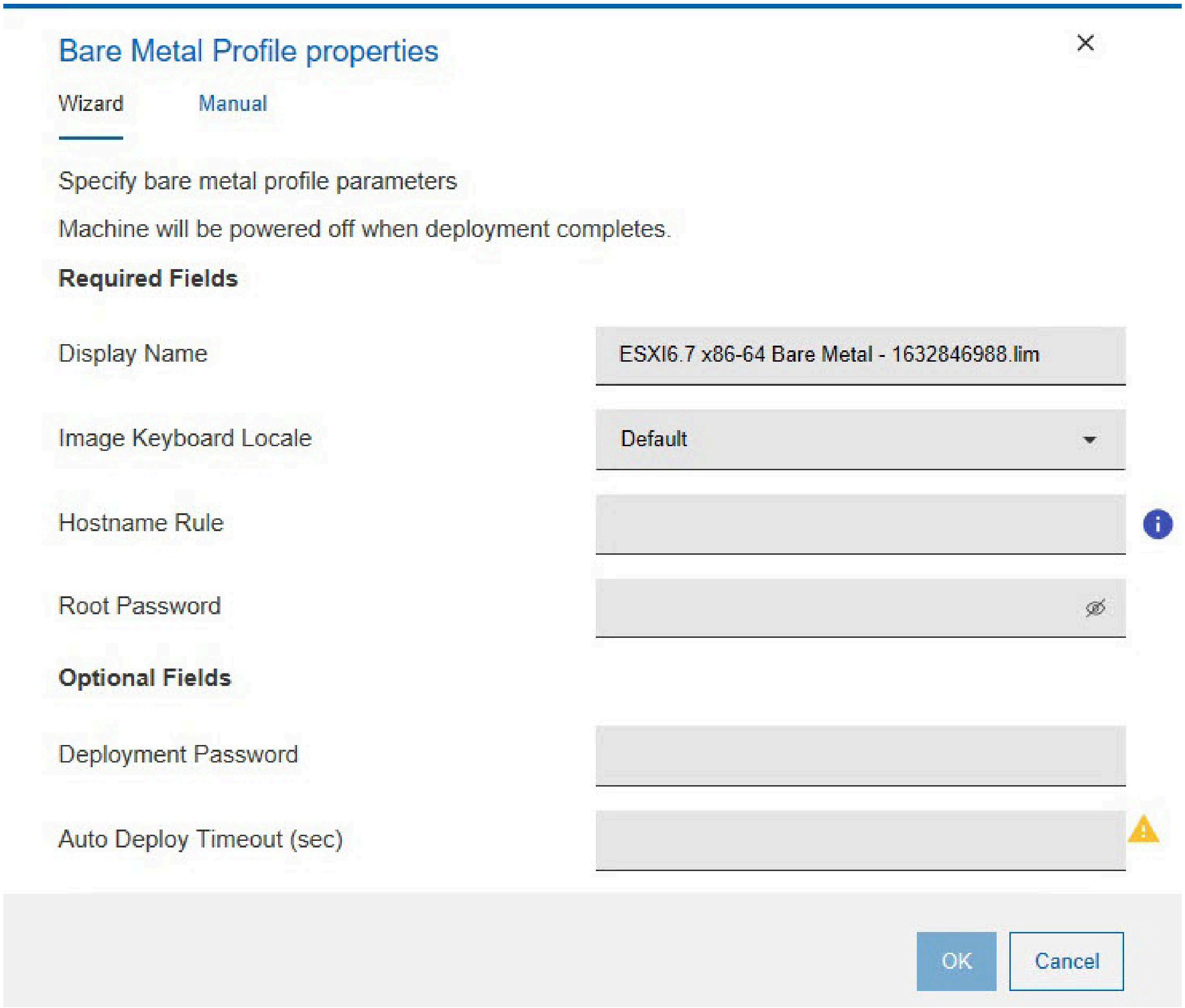
1. Extract the files `shim.efi` and `grubx64.efi` from packages.
    a. To extract them on a Linux computer, run the following commands:
        i. `rpm2cpio shim-x64-<version>.rpm | cpio -dimv`
        ii. `rpm2cpio grub2-efi-x64-<version>.rpm | cpio -dimv`
    b. To extract them on a Windows computer, you can use an utility like 7zip.
2. Copy the EFI boot images (the files `shim.efi` and `grubx64.efi`) on your bare metal server computer to the folder <bare metal server data>\tftp, where the default for <bare metal server data> is `C:\BFOSD Files`.
3. Start a new Linux deployment on UEFI target.

Creating Bare Metal Profiles for VMware ESXi Images

You can create and deploy VMware ESXi Bare Metal profiles on targets.

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

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



Bare Metal Profile properties

Specify bare metal profile parameters

Machine will be powered off when deployment completes.

Required Fields

Display Name	ESXI6.7 x86-64 Bare Metal - 1632846988.lim
Image Keyboard Locale	Default
Hostname Rule	
Root Password	

Optional Fields

Deployment Password	
Auto Deploy Timeout (sec)	

Required fields:

Display name

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

Image Keyboard Locale

Choose the image keyboard locale for the operating system.

Hostname Rule

Specify the hostname rule that will be used to build the hostname, computer name, and full computer name of the target. You can specify values in the following forms:

- A prefix.
- A prefix and one or more variables.
- One or more variables.

There is a limit of 8 alphanumeric characters if you specify a prefix only. If you specify an asterisk (*) as prefix, the target hostname is set to a string formed by the characters `OSDOSD-` followed by a string assigned by the operating system. Variables must be specified in the form `[variable]` enclosed by square brackets. You can concatenate variables. Allowed variables are:

- [IP] - IP Address of the primary interface that has performed a PXE boot
- [MAC] - Hardware Address of the primary interface that has performed PXE boot)
- [UUID] - System UUID as found in DMI (SMBIOS)
- [SN] - Serial number as found in DMI (SMBIOS)
- [AT] - Asset TAG as found in DMI (SMBIOS)
- [BBSN] - Base Board Serial Number as found in DMI (SMBIOS)

Every variable keyword supports a range extension, and you can decide to include only part of the information. The range starts at value zero. The value [IP3] corresponds to the last byte of the IP address. In IP addresses bytes are separated by dots. For example, if you specify a hostname rule of `pc-[IP3]` and the IP address of the target is `192.168.0.232`, the hostname becomes `pc-232`. If you specify `[IP0-2]`, the first three bytes of the IP address are included. For SN, UUID, AT, and BBSN values, the range corresponds to a substring. You can also add `R` at the end of the range to start it from the last character specified. Dots are always removed from the IP address in the final string.

Root Password

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

Optional fields:

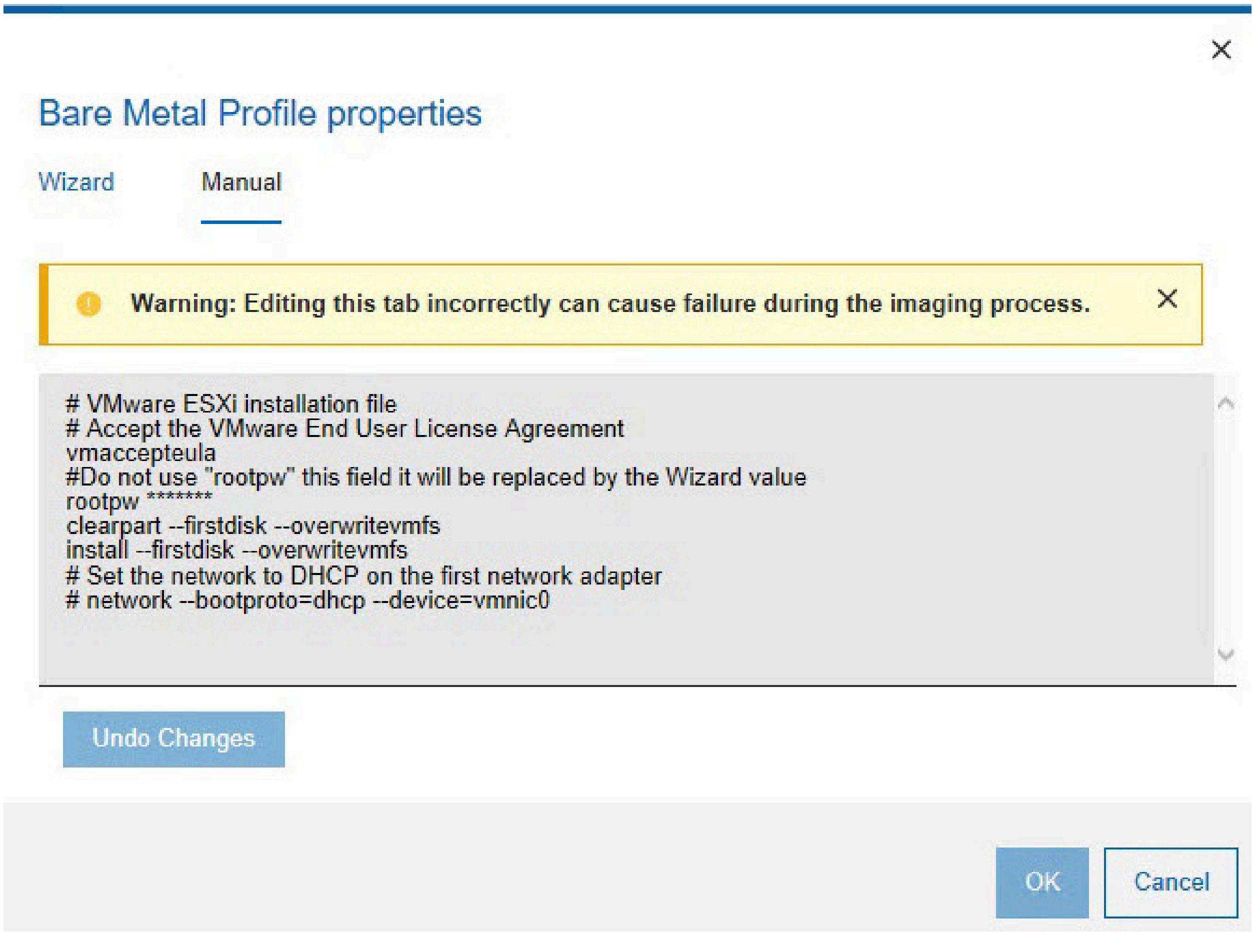
Deployment password

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.



Warning: Editing this tab incorrectly can cause failure during the imaging process.

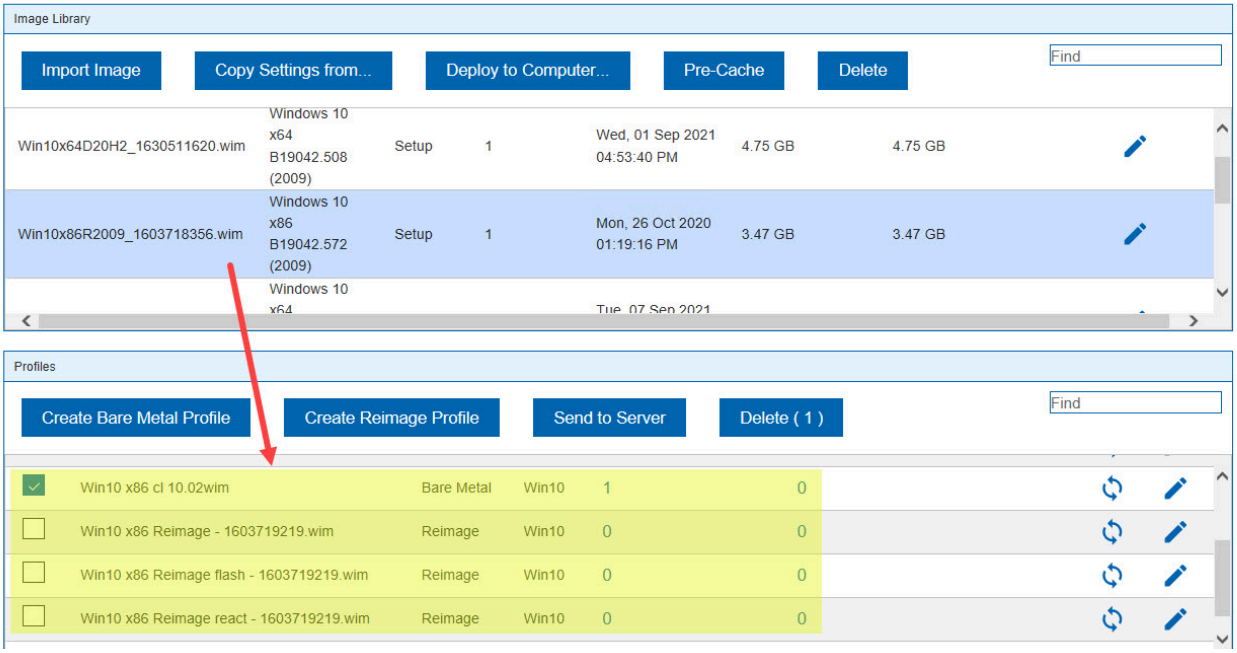
```
# VMware ESXi installation file
# Accept the VMware End User License Agreement
vmaccepteula
#Do not use "rootpw" this field it will be replaced by the Wizard value
rootpw *******
clearpart --firstdisk --overwritevmfs
install --firstdisk --overwritevmfs
# Set the network to DHCP on the first network adapter
# network --bootproto=dhcp --device=vmnic0
```

Important:

- VMware ESXi is supported for deployment on BIOS targets only.
- Any network parameters previously set with task 354 on targets of a VMware ESXi bare metal deployment are ignored.

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.

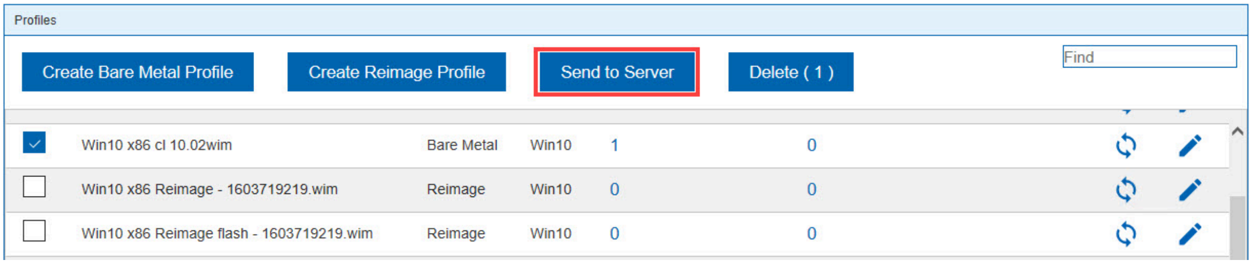


Win10x64D20H2_1630511620.wim	Windows 10 x64 B19042.508 (2009)	Setup	1	Wed, 01 Sep 2021 04:53:40 PM	4.75 GB	4.75 GB	✏
Win10x86R2009_1603718356.wim	Windows 10 x86 B19042.572 (2009)	Setup	1	Mon, 26 Oct 2020 01:19:16 PM	3.47 GB	3.47 GB	✏
	Windows 10 x64			Tue, 07 Sep 2021			

☑	Win10 x86 cl 10.02wim	Bare Metal	Win10	1	0	⟳	✏
□	Win10 x86 Reimage - 1603719219.wim	Reimage	Win10	0	0	⟳	✏
□	Win10 x86 Reimage flash - 1603719219.wim	Reimage	Win10	0	0	⟳	✏
□	Win10 x86 Reimage react - 1603719219.wim	Reimage	Win10	0	0	⟳	✏

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**.



☑	Win10 x86 cl 10.02wim	Bare Metal	Win10	1	0	⟳	✏
□	Win10 x86 Reimage - 1603719219.wim	Reimage	Win10	0	0	⟳	✏
□	Win10 x86 Reimage flash - 1603719219.wim	Reimage	Win10	0	0	⟳	✏

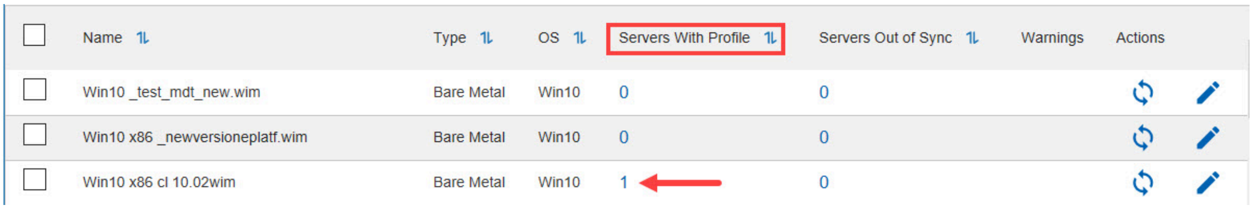
This generates an action for any valid bare metal servers.

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.



□	Name ⇅	Type ⇅	OS ⇅	Servers With Profile ⇅	Servers Out of Sync ⇅	Warnings	Actions
□	Win10 _test_mdt_new.wim	Bare Metal	Win10	0	0		↻ ✎
□	Win10 x86 _newversioneplatf.wim	Bare Metal	Win10	0	0		↻ ✎
□	Win10 x86 cl 10.02wim	Bare Metal	Win10	1	0		↻ ✎

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.

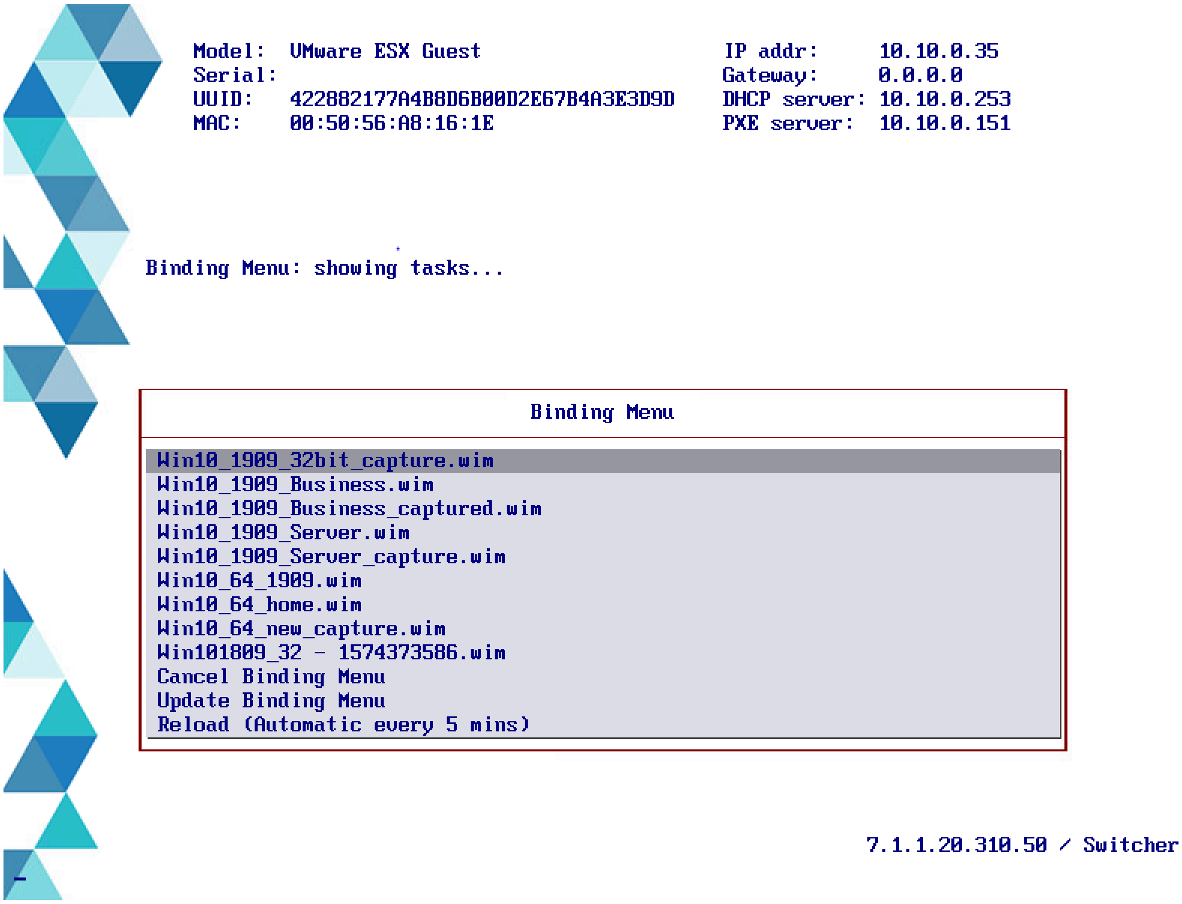
Deploying a bare metal profile from the target binding menu

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.
- On VMware targets, when the deployment completes, the target is powered off. See Bare Metal Deployment behavior of VMware ESXi *(on page 184)*.

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 BigFix Console:



```
Model:  VMware ESX Guest                    IP addr:     10.10.0.35
Serial:                                     Gateway:     0.0.0.0
UUID:   422882177A4B8D6B00D2E67B4A3E3D9D    DHCP server: 10.10.0.253
MAC:    00:50:56:A8:16:1E                   PXE server:  10.10.0.151

Binding Menu: showing tasks...

                     Binding Menu
 Win10_1909_32bit_capture.wim
 Win10_1909_Business.wim
 Win10_1909_Business_captured.wim
 Win10_1909_Server.wim
 Win10_1909_Server_capture.wim
 Win10_64_1909.wim
 Win10_64_home.wim
 Win10_64_new_capture.wim
 Win101809_32 - 1574373586.wim
 Cancel Binding Menu
 Update Binding Menu
 Reload (Automatic every 5 mins)

                                          7.1.1.20.310.50 / Switcher
```

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

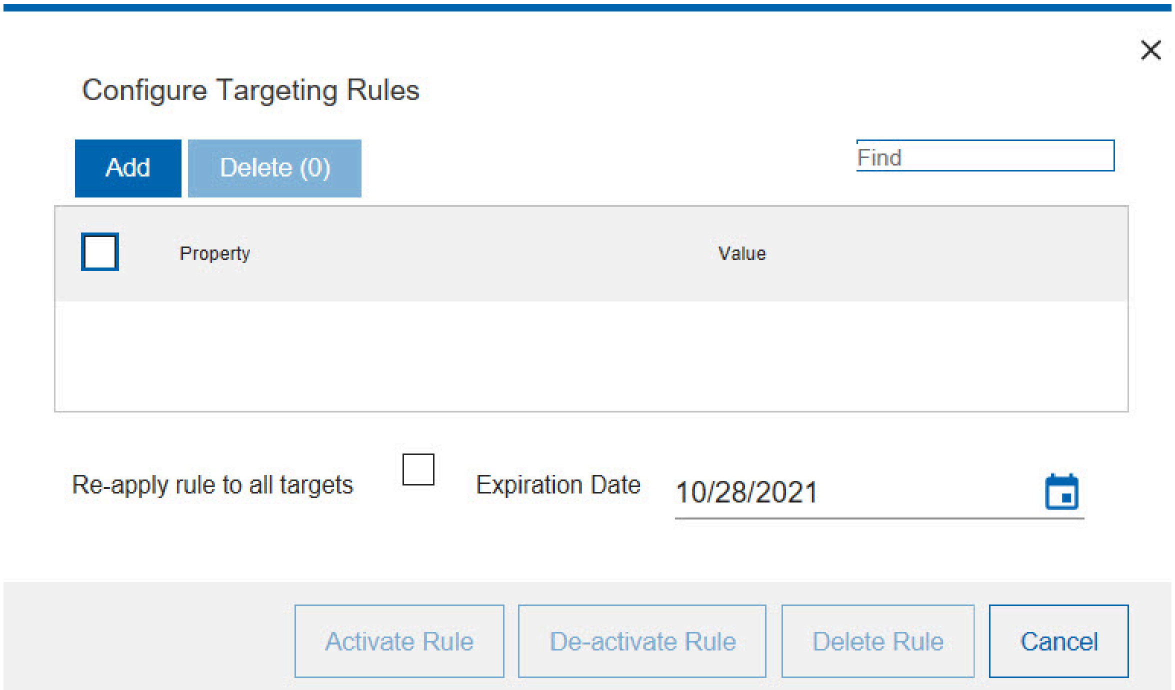
When you deploy a bare metal profile, you can optionally choose to define a set of properties that determine which targets are dynamically selected for deployment. You can specify properties such as IP address list, IP address range, MAC address list, Serial Number list, UUID list, and Model list by 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:

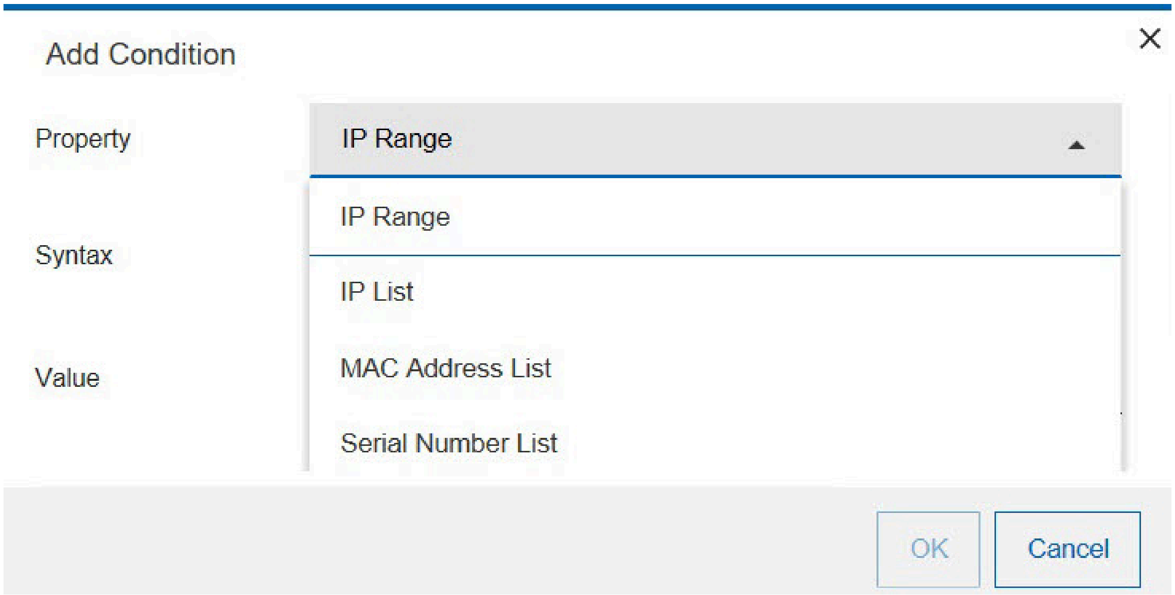
1. Select a bare metal profile and click ✏ to create a rule for the profile. The **Configure Targeting Rule** window is displayed.



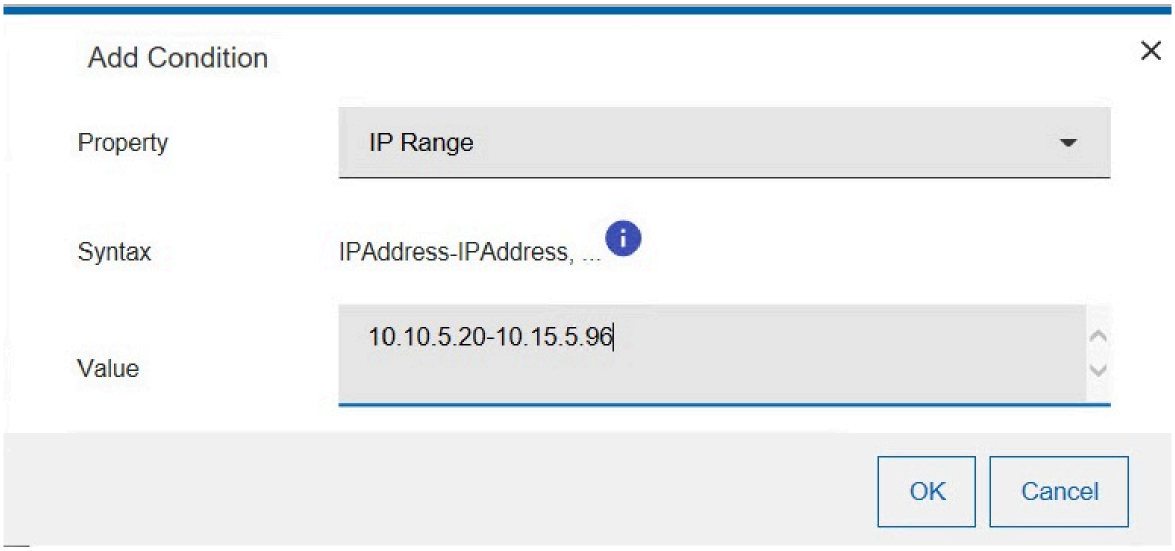
Re-apply rule to all targets □ Expiration Date 10/28/2021

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

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



3. Specify a value for the target property.



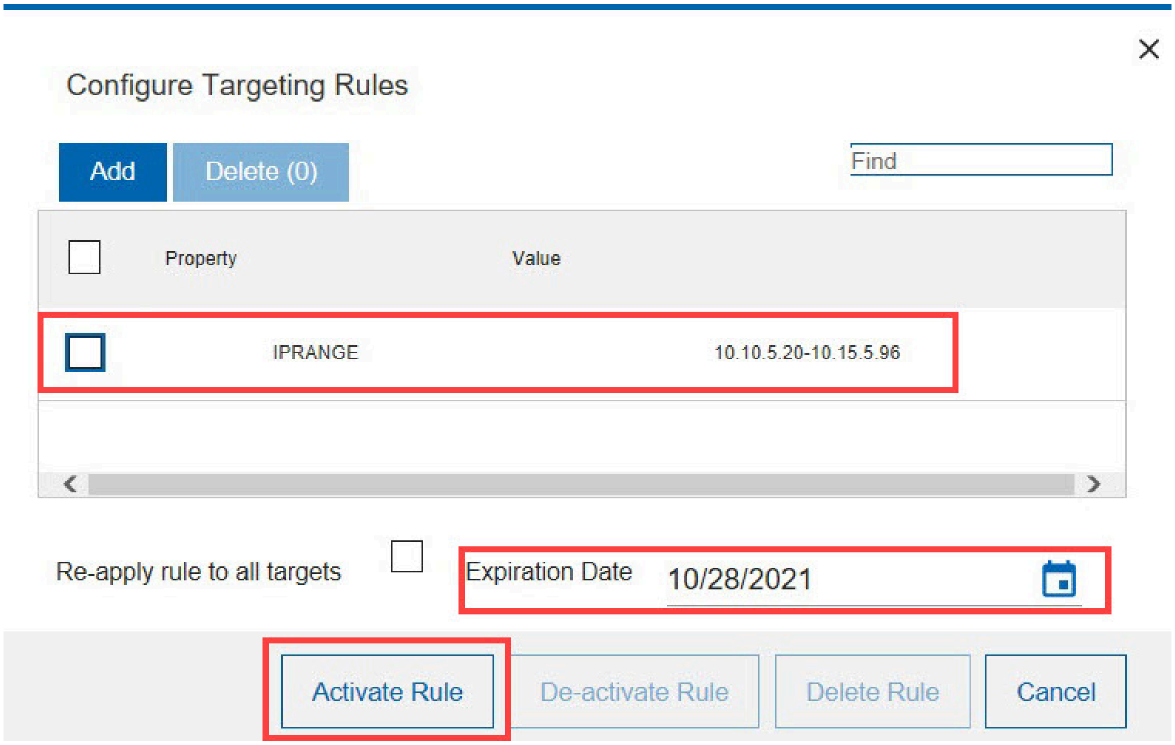
Property: IP Range

Syntax: IPAddress-IPAddress, ...

Value: 10.10.5.20-10.15.5.96

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.



□	Property	Value
□	IPRANGE	10.10.5.20-10.15.5.96

Re-apply rule to all targets □

Expiration Date 10/28/2021

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 BigFix 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 233)*. 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.

Note: If you are deploying on a VMware targets, see Bare Metal Deployment behavior of VMware ESXi *(on page 184)*.

Capturing and restoring user state of Windows targets

When you complete an operating system migration on new hardware, you can restore previously captured user settings on the new system.

When you are deploying new hardware in your organization, you can capture the user state of an initial operating system on the current hardware, perform a bare metal deployment on the new hardware, and then restore the previously captured user state to the new machine. OS Deployment uses Microsoft's USMT ScanState and LoadState commands for this purpose. When you are capturing user state, you can optionally choose to modify the default ScanState arguments, capture additional file extensions, and also provide other ScanState instructions through XML file content using USMT syntax up to a maximum of 4000 characters. Captured data and logs are stored in the destination folder which must be on a network share. If access to the network share is restricted, you are required to supply the credentials at task submission time.

You can capture and restore different user state content on multiple computers with a single task. When you are capturing user state from a single computer or multiple computers, a specific capture folder identified by the computer name is created for each computer. If you are restoring user state for a single computer or multiple computers, you can choose a single restore folder for all computers, or a specific folder for each computer.

Depending on the source and destination operating systems, use one of the following task pairs:

- If you want to capture the user state of Windows 7 computers and restore on Windows 7 or Windows 8 computers, you must have previously created an Windows Bundle with WADK8 (USMT5) and imported it using the Bundle and Media Manager dashboard. Run the following tasks:

  Capture User State on Windows XP, Vista, and 7 computers (USMT5) - Task 170

  Restore User State on Windows 7 and 8 (USMT5) - Task 171

- If you want to capture the user state of Windows 7, 8, 8.1, or 10 computers, and restore on Windows 8, 8.1, and 10, you must have previously created an Windows Bundle with WADK10 (USMT10) and imported it using the Bundle and Media Manager Dashboard. Run the following tasks:

  Capture User State on Windows 7, 8, 8.1, and 10 (USMT10) - Task 175

  Restore User State on Windows 8, 8.1, and 10 computers (USMT10) - Task 176

For the capture tasks you must provide the following information:

- The destination folder on the network share where the captured data must be stored, and the credentials to access the network share, if required. At capture time, a separate subfolder identified by te computer name is created for each target.
- The task contains the following predefined ScanState command arguments:

  ```
  /v:6 /c /localonly /o /uel:60
  ```

  You can optionally add or modify these arguments using the ScanState syntax, but BigFix does not perform any input validation.
- You can also specify additional file extensions to include in the capture, in a comma separated list, and any other optional instructions up to a maximum of 4000 characters that are supplied to the ScanState command in xml file format. For example, if you want to capture all files contained in the path `C:\test files\*`:

  ```
  <?xml version="1.0" encoding="UTF-8"?>
       <migration urlid="http://www.microsoft.com/migration/1.0/migxmlext/cust">
   <!-- Additional pattern to capture-->
       <component type="Documents" context="System">
         <displayName>Component to migrate additional files Sergio</displayName>
         <role role="Data">
           <rules>
  ```

```
          <include>
            <objectSet>
  <pattern type="File">C:\test files\* [*]</pattern>
            </objectSet>
          </include>
        </rules>
      </role>
    </component>
</migration>
```

For the restore tasks, the predefined arguments are:

```
/lac
```

You can optionally add or modify the LoadState arguments but BigFix does not perform any syntax validation.

You must specify the source folder on the network share where the data to be restored resides, and the credentials to access the network share, if required. You can also select to read the user data from a separate subfolder identified by the computer name, for each target, by specifying Yes in the corresponding field.

You can add the capture and restore tasks to a Server Automation plan. For example, you can define the following sequence in a server Automation plan:

1. Capture the source user state on a target by using task 170 or 175
2. Set the hostname of the target where the user state will be restored using task 350
3. Deploy the profile on the target where the user state will be restored using task 301
4. Restore user state on the deployed target using task 171 or 176.

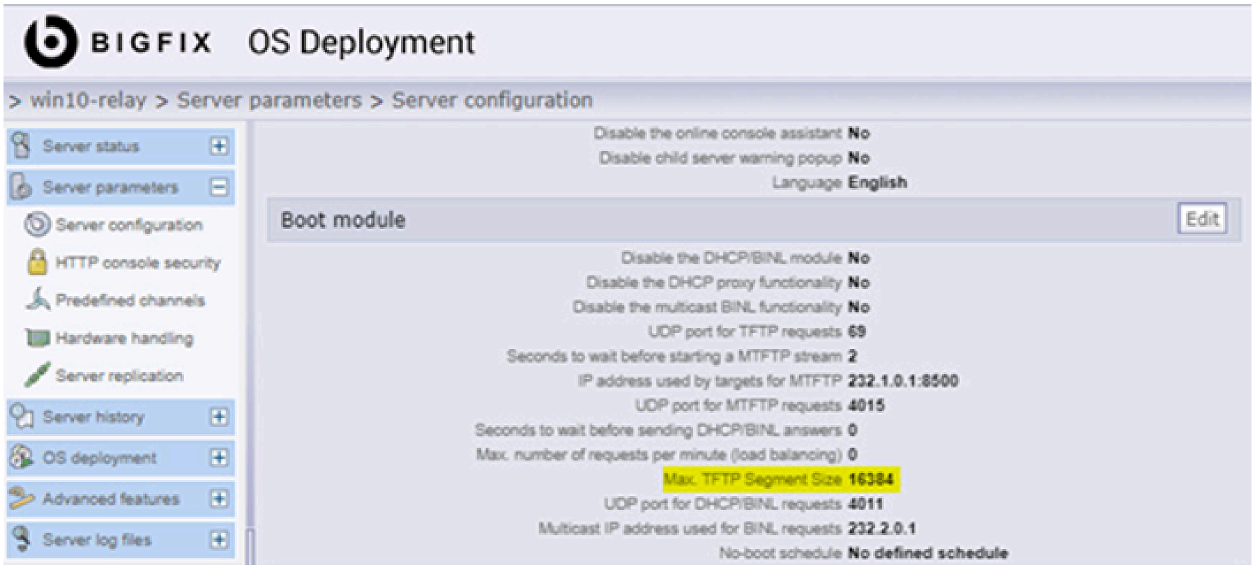
Tuning WinPE TFTP settings for bare metal deployments

You can tune WinPE download speed during Bare Metal deployments by running task 360.

Run the **Bare Metal WinPE TFTP Settings** task (360) to change parameters such as block size or window size, to improve WinPE download speed and performance in bare metal deployment scenarios. The task can be run on Bare Metal Servers that are at build level 290.02 or later. This task simplifies the configuration of these parameters, and should only be used if you are experiencing significant performance and reliability issues in this area. Increasing Block size and Window size can improve download performance if the network conditions allow it.

Before you run this task, to enable flexibility in tuning the TFTP parameters, you must complete a configuration step on the Bare Metal Server once only:

1. From the BigFix Bare Metal Server WebUI, select **Server Parameters > Server configuration**.
2. In the **Max TFTP Segment Size** field substitute the default value of `512` with the maximum value `16384`.
3. Restart the Server.



Disable the online console assistant No
Disable child server warning popup No
Language English

Boot module

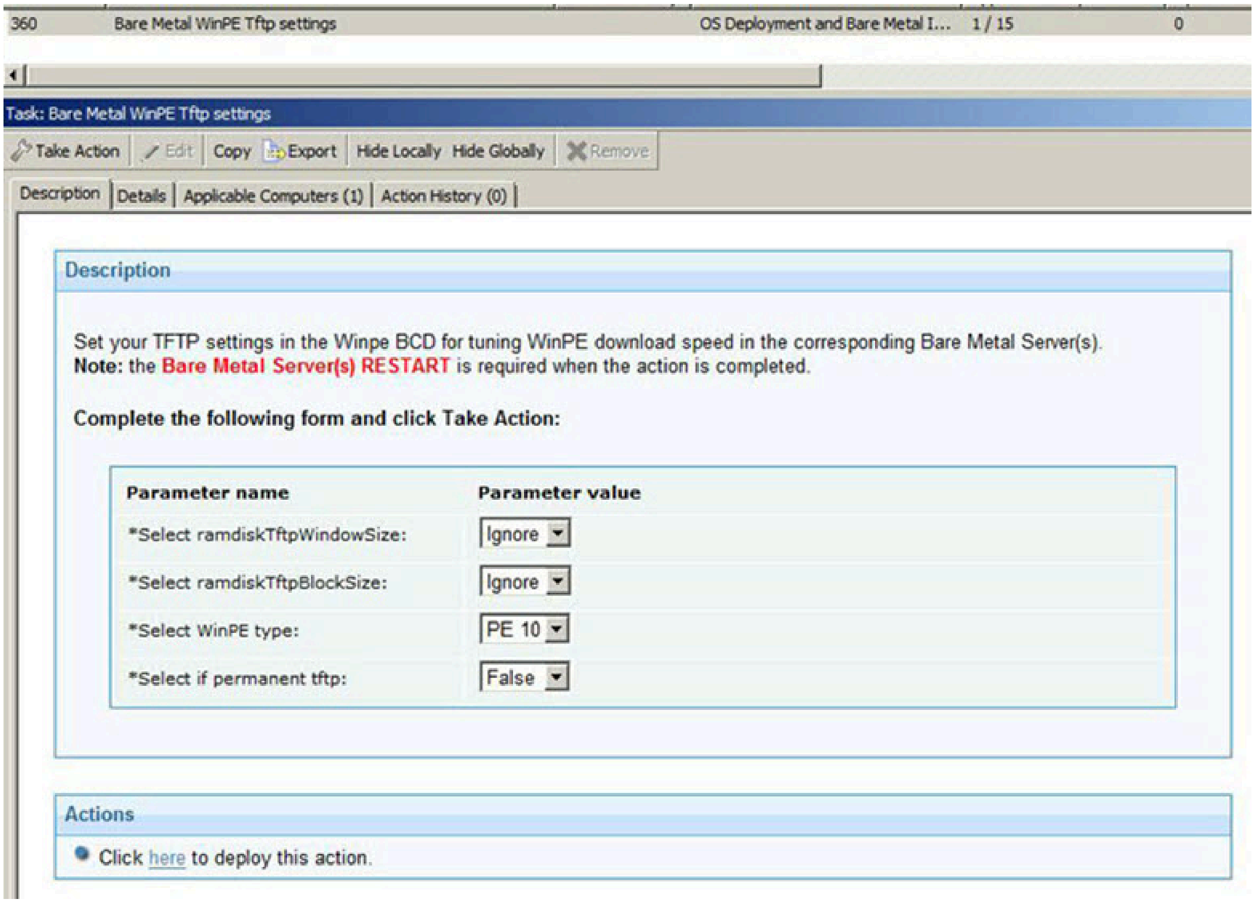
Disable the DHCP/BINL module No
Disable the DHCP proxy functionality No
Disable the multicast BINL functionality No
UDP port for TFTP requests 69
Seconds to wait before starting a MTFTP stream 2
IP address used by targets for MTFTP 232.1.0.1:8500
UDP port for MTFTP requests 4015
Seconds to wait before sending DHCP/BINL answers 0
Max. number of requests per minute (load balancing) 0
Max. TFTP Segment Size 16384
UDP port for DHCP/BINL requests 4011
Multicast IP address used for BINL requests 232.2.0.1
No-boot schedule No defined schedule

Important:

- TFTP settings are affected by the specific environment, in terms of network speed, topology, and bare metal server performance among other things. Changing TFTP parameter settings could lead to unexpected behaviors. As a best practice, you should verify the changes thoroughly in a test environment before you apply them to your production environment. The advised procedure is to gradually increase the block size and window size size in a test environment to determine the optimum.
- These are Microsoft WinPE settings. For additional information, refer to the available Microsoft documentation.

Parameter settings in task 360

Run the **Bare Metal WinPE Tftp settings** task on your Bare Metal Servers to change the following settings.



Description

Set your TFTP settings in the Winpe BCD for tuning WinPE download speed in the corresponding Bare Metal Server(s).
Note: the **Bare Metal Server(s) RESTART** is required when the action is completed.

Complete the following form and click Take Action:

Parameter name	Parameter value
*Select ramdiskTftpWindowSize:	Ignore
*Select ramdiskTftpBlockSize:	Ignore
*Select WinPE type:	PE 10
*Select if permanent tftp:	False

Actions

- Click here to deploy this action.

You must restart the affected Bare Metal Servers when the action completes, to ensure that the settings are applied to the selected WinPE.

There are four mandatory parameters:

ramdiskTftpWindowSize

Select one of the following values:

- 4, 6, 8, 12, 16, 24, 32
- **Ignore**: This setting is not modified
- **Delete**: The current setting is deleted, and the initial behavior is restored.

ramdiskTftpBlockSize

Select one of the following values:

- 1432, 4096, 8192, 16384, 32678
- **Ignore**: This setting is not modified
- **Delete**: The current setting is deleted, and the initial behavior is restored.

Selecting **Delete** always resets the parameters and restores the initial behavior.

WinPE type

The WinPE to which the settings are applied. Possible values are 3, 4, 5, and 10. Only the WinPE types for which an Windows Bundle is available are displayed.

permanent tftp

Possible values are:

True

When a subsequent sync action is completed on the Bare Metal Server, and the WinPE of the specified type is created, the same settings are reapplied to the new WinPE. Selecting this value adds the following three parameters to the Bare Metal server computer settings for each WinPE type:

```
ramdiskftpwindowsize_PE<WinPE type>

ramdiskftpblocksize_PE<WinPE type>

restoreftpparam_PE<WinPE type>
```

You can view the settings from the subscribed computer list by selecting the Bare Metal Server on which the task was run.

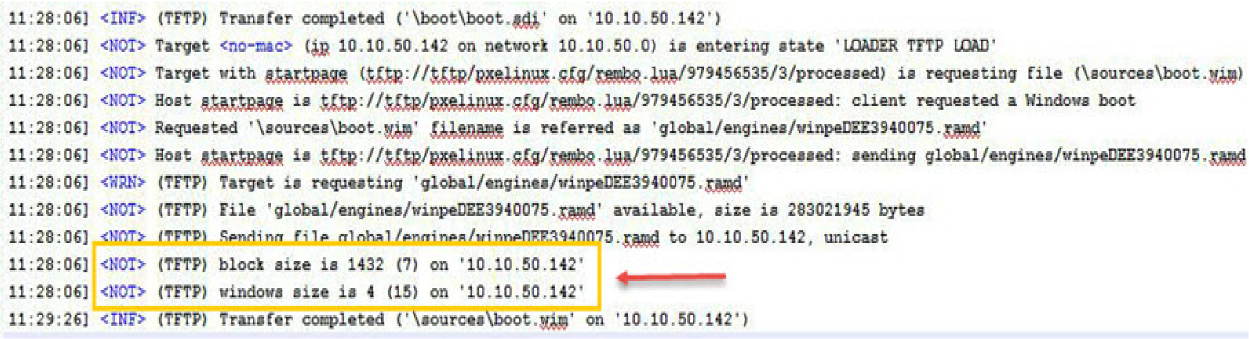
False

This selection deletes any existing computer setting.

Note: The specific combination `ramdiskTftpWindowSize=delete` and `ramdiskTftpBlockSize=delete`, with `permanent tftp=true` results in the settings being applied once; However, permanent=true is ignored, so that when a subsequent sync action is completed, the computer settings are deleted and not reapplied.

Checking TFTP parameter values in the log files

On the Bare Metal Server, in the trace file `boot.trc` with debug level set to 4, you can view information about the block size and window size settings used by the TFTP server to download the selected WinPE. In this example, during download of WinPE `"global/engines/winpe<....>.ramd"`, on the target `10.10.50.142`, you can view the block and window sizes used by the TFTP server to download the WinPE. In this case, the values are 1432 and 4 respectively.



```
11:28:06] <INF> (TFTP) Transfer completed ('\boot\boot.sdi' on '10.10.50.142')
11:28:06] <NOT> Target <no-mac> (ip 10.10.50.142 on network 10.10.50.0) is entering state 'LOADER TFTP LOAD'
11:28:06] <NOT> Target with startpage (tftp://tftp/pxelinux.cfg/rembo.lua/979456535/3/processed) is requesting file (\sources\boot.wim)
11:28:06] <NOT> Host startpage is tftp://tftp/pxelinux.cfg/rembo.lua/979456535/3/processed: client requested a Windows boot
11:28:06] <NOT> Requested '\sources\boot.wim' filename is referred as 'global/engines/winpeDEE3940075.ramd'
11:28:06] <NOT> Host startpage is tftp://tftp/pxelinux.cfg/rembo.lua/979456535/3/processed: sending global/engines/winpeDEE3940075.ramd
11:28:06] <WRN> (TFTP) Target is requesting 'global/engines/winpeDEE3940075.ramd'
11:28:06] <NOT> (TFTP) File 'global/engines/winpeDEE3940075.ramd' available, size is 283021945 bytes
11:28:06] <NOT> (TFTP) Sending file global/engines/winpeDEE3940075.ramd to 10.10.50.142, unicast
11:28:06] <NOT> (TFTP) block size is 1432 (7) on '10.10.50.142'
11:28:06] <NOT> (TFTP) windows size is 4 (15) on '10.10.50.142'
11:29:26] <INF> (TFTP) Transfer completed ('\sources\boot.wim' on '10.10.50.142')
```

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 BigFix console after the targets PXE boot to their local server. You can complete the following actions:

- Change Bare Metal target settings before a deployment using the corresponding task (350). See Changing target settings before deployments *(on page 233)*.
- Set or remove network configuration settings for a target, see Changing Bare Metal Target Network Configuration Settings *(on page 235)*.
- Schedule the deployment of profiles on Bare Metal targets. For more information, see Deploying a bare metal profile from the BigFix console *(on page 227)*.
- Capture and restore user state of Windows targets, see Capturing and restoring user state of Windows targets *(on page 227)*.
- Wipe Bare Metal target disks. For more information, see Wiping target disks *(on page 237)*.
- Reset the status of a bare metal target on the associated bare metal server, see Reset the status of a bare metal target *(on page 237)*

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 the following properties:

- 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** task.
- Universal Unique Identifier (UUID).
- Any network parameters defined with the **Change Bare Metal Target Network Configuration Settings** task.

Note:

In the **Subscribed Computers** view, targets that successfully completed a PXE boot are identified by the **agent type** attribute set to *"Proxy - 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 (ID 350) to set or remove settings for a selected target. The values you specify with this task will affect the partition mappings and hostname rule values specified in the bare metal profile for the selected target.

Important: Before you run this task, ensure that your Bare Metal OS Deployment servers are at Version 7.1.1.20 or later.

Hostname

The value you specify becomes the computer name of the bare metal target on which you run the task. For Windows targets, the name must be a maximum of 15 characters or else the deployment fails. If you have set this property, the value specified in the task overrides the value specified in the Hostname Rule field of the Bare Metal profile.

Partition mapping

You can resize one or more partitions for a specific target. The partitions you resize must exist in the partition mappings section of the bare metal profile that you are deploying to the target. At deployment time, the resizing information is checked against the partitions in the profile, and the partition layout for the target is updated accordingly. If you specify a partition that does not match the partitions found in the profile that you are deploying, the information in this field is ignored, and the partition layout of the target will be the one specified in the profile. The syntax is `[resize <mount point> <size in MB>]`.

For example, to resize the D partition to 1 gigabyte for a Windows target specify `resize D 1024`. To resize /usr and /root for a Linux target, specify `resize /usr 1024 /root 1024`

Note: If you select the **Prompt end user for properties** option in the bare metal profile, the properties specified in this task are displayed at the target at deployment time. You can accept them or change them as required.

Forcing network boot on targets

Run the **Force Network Boot** Task (ID132) on a running target to boot it on the network. 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.

Deleting bare metal target entries

When you deploy a bare metal profile on a target discovered through the Management Extender for Bare Metal targets, a BigFix client is installed on the target during the deployment process and a new computer entry is added in the BigFix database with agent type set to *"Native"* For this reason, duplicate entries are visible in the **Subscribed Computers** list for the same physical computer. The value specified for the `DeviceReportExpirationIntervalHours` in the `settings.json` configuration file of the Management Extender for Bare Metal Targets determines the expiration period for the bare metal target, after which the corresponding entry can be permanently deleted from the database. You can delete the expired bare metal target entries manually from the console or by using the BES computer remover tool. You can download the tool and related documentation from the BigFix wiki at this link: https://bigfix-wiki.hcltechsw.com/wikis/home?lang=en-us#!/wiki/BigFix%20Wiki/page/BES%20Computer%20Remover. To change the Management Extender for Bare Metal Targets Plug-in configuration settings, see Changing the plug-in settings *(on page 59)*.

Booting 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 74)* and Managing Linux OS Resources and Deployment Media *(on page 104)*.

Changing Bare Metal Target Network Configuration Settings

You can define or remove configuration settings for one or more network interface cards on selected targets using task 354.

To set or remove network configuration settings for specific bare metal targets, run the **Change Bare Metal Target Network configuration settings** task (ID 354). The parameters set with this task are used together with what you specify in the bare metal profile that is deployed on the target. The configuration policy that you specify in the **Network** tab of the profile creation wizard determines whether the parameters specified with this task will take precedence over the parameters specified in the profile.

Typically, this task is useful when you are configuring network settings for specific bare metal targets that have more than one network interface, or when your targets must be configured with a static IP. In this scenario, you can define the common subset of network configuration parameters in the bare metal profile, and use this task to configure the unique settings for each target.

Select the required configuration action (Set or Remove) and specify the configuration type (Static or dhcp). You can define the following network configuration parameters for the network interface card (NIC) identified by the specified MAC address:

- IP Address
- Subnet mask
- Default gateway
- Connection name
- Preferred DNS Server
- Alternate DNS Server
- DNS Domain
- Domain Search Order

You can set or remove configurations for multiple network interface cards (NICs) on the same target, by running the task for each interface and specifying the corresponding MAC address. If your targets have a single network interface card, the MAC address is not mandatory.

You can optionally associate a connection name to each NIC. For Windows targets, the connection name becomes the name of the network interface. For Linux targets, if the MAC address is not specified, the connection name is used to identify the network interface that will be configured.

The Remove action deletes all network configuration parameters on a specific target interface. If multiple NICs were configured, the network configuration parameters of the specified MAC address is deleted. If the MAC address is not specified, the settings of the first (oldest) configured interface are removed. To selectively delete one or more network parameters, use the Set action and specify an asterisk (*) in the corresponding parameter value fields. The fields marked with the asterisk are reset for the specified target. The asterisk is ignored if specified in the MAC address field.

Important:

- If you are defining a Connection name, if the target operating system is Linux, the operating system will limit it to nine characters.
- If you are defining a static IP configuration for a specific target, the IP address, Subnet Mask, and default gateway values are mandatory. If you are defining a static IP address for a target with a single interface, the address you specify must be in a network from which the OS Deployment server can be reached, else the deployment task will not complete.
- When you configure multiple NICs, you must always specify the MAC address that uniquely identifies it, otherwise results might be different from what you expect.
- If you are defining a dynamic (DHCP) configuration for the target, the only parameter that can be specified is the MAC address. If the MAC address is omitted, the interface that performed the PXE boot is configured by default.
- The Domain Search order parameter is ignored if the target operating system is Windows.

Example:

A company network has targets with two network interfaces. One must be configured with a dynamic (DHCP) configuration, and the other with a static IP configuration.

1. In the Bare Metal Profile that will be deployed, the following parameters are specified in the **Network**tab. These parameters are common to all targets in the network:
   - Preferred DNS Server: `192.168.100.125`
   - DNS Domain: `company.com`
2. For each target, task 354 is run twice to configure each network interface. For example:

   First run:
   - Configuration action: `Set`
   - Configuration type: `dhcp`
   - MAC Address`<MAC1>` where <MAC1> is the MAC address of the network interface that must have a dynamic IP configuration.

Second run:

- Configuration action: `Set`
- Configuration type: `static`
- MAC Address: `<MAC2>` where <MAC2> is the MAC address of the network interface that must have a static IP configuration.
- IP address: `10.10.6.95`
- Subnet mask: `255.255.255.0`
- Default gateway: `10.10.6.254`

When the profile is deployed, all targets will have the same Preferred DNS Server name and domain, and each individual target will be configured as specified in task 354.

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 completed a PXE-boot and are registered to the BigFix server through the Bare Metal Extender Plug-in. The task destroys disk content on the target system. You can choose between 5 different destruction 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 Windows Bundle on the BigFix 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 is queued for execution on the Bare Metal Server. To see the results of the actual 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.

Reset the status of a bare metal target

You can reset the status of a bare metal target and make it available again for OS deployment tasks.

Run the **Reset the status of a bare metal target** task (ID 303), to reset the status of bare metal targets that are registered to the BigFix server through the Bare Metal Extender plug-in. No user parameters are required.

This action is useful to make the target ready for a new deployment if it seems to be blocked on an old deployment task and/or does not respond correctly.

Note: Task 303 works only on bare metal servers that are upgraded to version 7.1.1.20.310.66 or later.

Chapter 11. Monitoring Deployment Activities

You can track and monitor all deployment activities in your Endpoint Management network.

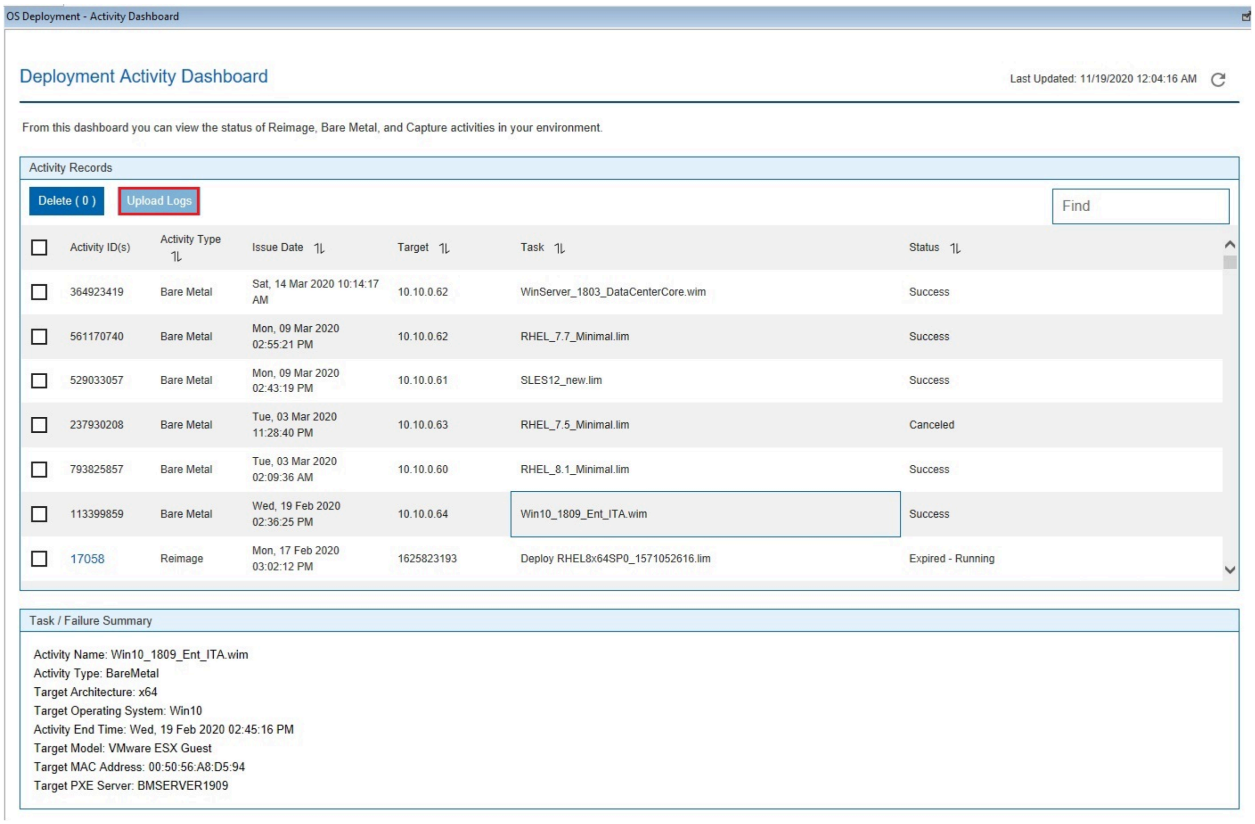
From the **Deployment Activity Dashboard** you can track, monitor, and view the results of capture, reimaging and Bare Metal tasks in your environment.

Deployment Activity Dashboard

In the Deployment Activity Dashboard, you can view the status and result of Reimage, Bare Metal, and Capture tasks 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 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 during certain phases of a deployment task.



Deployment Activity Dashboard

Last Updated: 11/19/2020 12:04:16 AM

From this dashboard you can view the status of Reimage, Bare Metal, and Capture activities in your environment.

Activity Records

□	Activity ID(s)	Activity Type ⇅	Issue Date ⇅	Target ⇅	Task ⇅	Status ⇅
□	364923419	Bare Metal	Sat, 14 Mar 2020 10:14:17 AM	10.10.0.62	WinServer_1803_DataCenterCore.wim	Success
□	561170740	Bare Metal	Mon, 09 Mar 2020 02:55:21 PM	10.10.0.62	RHEL_7.7_Minimal.lim	Success
□	529033057	Bare Metal	Mon, 09 Mar 2020 02:43:19 PM	10.10.0.61	SLES12_new.lim	Success
□	237930208	Bare Metal	Tue, 03 Mar 2020 11:28:40 PM	10.10.0.63	RHEL_7.5_Minimal.lim	Canceled
□	793825857	Bare Metal	Tue, 03 Mar 2020 02:09:36 AM	10.10.0.60	RHEL_8.1_Minimal.lim	Success
□	113399859	Bare Metal	Wed, 19 Feb 2020 02:36:25 PM	10.10.0.64	Win10_1809_Ent_ITA.wim	Success
□	17058	Reimage	Mon, 17 Feb 2020 03:02:12 PM	1625823193	Deploy RHEL8x64SP0_1571052616.lim	Expired - Running

Task / Failure Summary

Activity Name: Win10_1809_Ent_ITA.wim
Activity Type: BareMetal
Target Architecture: x64
Target Operating System: Win10
Activity End Time: Wed, 19 Feb 2020 02:45:16 PM
Target Model: VMware ESX Guest
Target MAC Address: 00:50:56:A8:D5:94
Target PXE Server: BMSERVER1909

Delete a record by selecting the corresponding Activity ID and clicking **Delete**.

Click a record to see more detailed information in the **Task / Failure Summary**. If your Bare Metal OS Deployment Server is at Version 7.1.1 Fix Pack 18 or later, you can view the activity end time for the selected Bare Metal task.

You can upload Bare Metal deployment logs for any bare metal deployment in your environment by selecting the activity and clicking **Upload Logs**. All the logs for the selected activity are compressed and sent in archive format from the Bare Metal Server to the BigFix Server in the following default path:

- Windows:

```
C:\Program Files\BigFix Enterprise\BES Server\UploadManagerData\BufferDir
\sha1\<nn>\<BM_Computer_ID_>\<task_id_string>.zip
```

- Linux:

```
/var/opt/BESServer/UploadManagerData/BufferDir
/sha1/<nn>/<BM_Computer_ID_>/<task_id_string>.zip
```

Where:

- <nn> are the last two digits of the Bare Metal Server Computer ID .
- <BM_Computer_ID_> is the computer ID of the Bare Metal Server.
- <task_id_string> is a string formed by the task ID of the Bare Metal activity.

You can also upload bare metal deployment logs for a specific task by running the "Upload Logs from Bare Metal Server" task (351). You must supply the *TaskID* on the Bare Metal Server as input parameter. To run this task, 7zip is required on the Bare Metal Server that ran the deployment.

For Bare Metal activities on Windows targets, if the deployed Windows profile was created using Windows Bundle Version 3.7 or later, the bare metal deployment logs are uploaded from the target to the Bare Metal Server when the deployment completes, for both successful and failed deployments.

Note: The uploaded archive files are handled by the Archive Manager component of the BigFix Platform. For more information about the specific settings and behavior of this component, see:.

Chapter 12. 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 section 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 63)*.

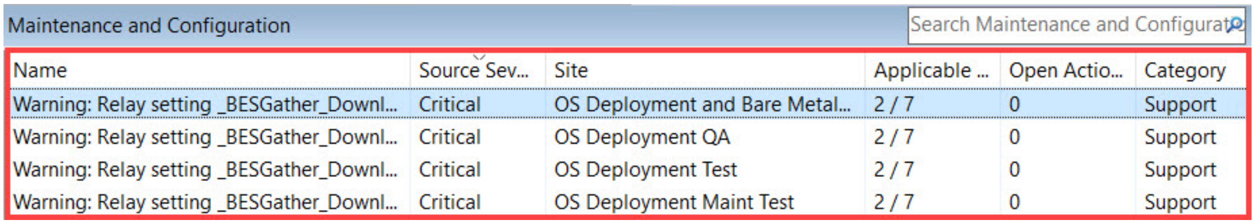
To troubleshoot problems related to the Relay Downloader component, see RelayDownloader Troubleshooting Tips.

Additional troubleshooting information is also available in the OS Deployment Troubleshooting wiki page at this link: OSD Troubleshooting.

Maintenance and Configuration tasks and Fixlets

Maintenance and Configuration tasks and Fixlets 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 Configurati

Name	Source Sev...	Site	Applicable ...	Open Actio...	Category
Warning: Relay setting _BESGather_Downl...	Critical	OS Deployment and Bare Metal...	2 / 7	0	Support
Warning: Relay setting _BESGather_Downl...	Critical	OS Deployment QA	2 / 7	0	Support
Warning: Relay setting _BESGather_Downl...	Critical	OS Deployment Test	2 / 7	0	Support
Warning: Relay setting _BESGather_Downl...	Critical	OS Deployment Maint Test	2 / 7	0	Support

Log and trace files

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 9. Files for deployment failure problem determination

Filename	Path	Scenario
• `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	Reimage was successful but drivers were missing in the new operating system. You can find Windows PE binding grid in the specified location.
• `peresult.ini` • `pegrid.ini.update` • `rbagent.trc` • `osresult.ini` • `osgrid.ini.update`	`C:\Deploy\$OEM$\BigFixOSD\RBAgent` on target workstation for reimaging	`C:\Deploy\$OEM$\BigFixOSD\RBAgent` on target workstation for reimaging
• `bom`*`nn`*`-peresults.ini` • `bom`*`nn`*`-pegrid.ini.update` • `bom`*`nn`*`.trc` • `bom`*`nn`*`-osresult.ini` • `bom`*`nn`*`-osgrid.ini.update`	`C:\BFOSD Files\global\hostactitiestask`*`nnnnn`* 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:\BFOSD Files\logs` on relay server for bare metal	OSD PXE component logs
All deployment files (Windows Bundle scripts, OS Resources, WIM and WinPE)	`C:\mcastdownload` on the target workstation for reimaging.	Reimaging in multicast has failed.
• `mcastdownload.log` • `validateBMserver.log`	`C:\Program Files\BigFix Enterprise\BES Client\__BESData\__Global\Logs\OSDeploymentLogs\McastDownload` on the target workstation after reimaging.	Reimaging in multicast (reimage profile) was successful. These logs contain statistical information about the files downloaded during the deployment and about the validation completed by the relay/Bare Metal Server to which the target is connected. You can also view if the deployment was switched to unicast mode.

Files for problem determination during Windows setup

During the reimaging 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 reimaging process failures, see the BigFix wiki page: Re-Image Process

Files for troubleshooting Console errors while importing files

When you import files using the Console (for example, when you upload an Windows 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 files

If errors occur during deployment media creation, you can check the following files:

- From the BigFix 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 `%ProgramFiles%\BigFix OSD`.

  For Example:

  ```
  C:\Program Files\BigFix OSD
  ```

  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 reimaging 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 allready exists"

Case 2691 Explanation = "Allready joined"
```

More information about error codes can be found at the following link:https://msdn.microsoft.com/en-us/library/ms681381(v=vs.85).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
```

Troubleshooting RelayDownloader errors

The RelayDownloader tool is used to retrieve files from the BigFix server, for example during the creation of deployment media or for Bare Metal Deployments. For tips about troubleshooting RelayDownloader errors, see the BigFix wiki at this link: RelayDownloader Troubleshooting Tips.

Troubleshooting problems in retrieving Bare Metal Server Settings (Analysis 50 or Task 361)

Analysis 50 and Task 361 are used to retrieve current parameter settings for the Bare Metal servers so that they can be viewed and changed either from the Bare Metal Server Manager dashboard or by running Task 361. When there are problems, and the parameters cannot be retrieved, you can check the following files on the Bare Metal Server:

- `\global\tem\baremetalsettings.conf` is the file where the settings are stored.
- `C:\Program Files\BigFix OSD\rbagent.trc` If the configuration file does not exist or is invalid, the `rbagent.trc` file logs any errors to help you troubleshoot the problem.

Troubleshooting Windows Bundle process errors

This topic describes how to troubleshoot errors in the different steps of the Windows Bundle creation process, describing a solution or workaround, if available.

Upload Windows Bundle fails when an antivirus program is running

If an antivirus program is running on the computer during the Windows Bundle creation, the upload Windows 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\Windows Preinstallation 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 Windows 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.

Windows ADK for Windows 10 (WADK 10) installation action fails on Windows 7, Windows 2008, or Windows 2008 R2 targets

If you choose WADK 10 and MDT 2013 Update 1 when you install the MDT Bundle Creator using the **Bundle and Media Manager** dashboard and select a Windows 7, Windows 2008, or Windows 2008 R2 target, the WADK 10 installation action might fail. This problem can also occur when you run the WADK 10 installation Fixlet individually on one of the above operating systems.

Solution/Workaround:

The problem occurs because the required Microsoft .NET Framework version 4.5 is not already installed on these operating systems. The Fixlet invokes the adk installer to install .NET Framework the first time it is run, but exits without completing the ADK installation. To solve the problem, reboot the MDT Bundle Creator machine, and rerun the MDT Bundle Creator installation action sequence from the dashboard. If you launched the Fixlet individually, verify that Microsoft .NET Framework version 4.5 is installed on the selected target , then rerun the Fixlet.

Problems and limitations

You can troubleshoot and gather information about known problems and limitations. A solution or workaround is provided if available.

Update Driver Manifests on Bare Metal Servers action repeatedly fails

Problem description

Update Driver Manifests on Bare Metal Servers action repeatedly fails

Solution/workaround

In a network where the download from the BigFix Root Server to the Bare Metal Server computer takes time (for example, long download chain for long relays hierarchy), the Update Driver Manifests on Bare Metal Servers action could repeatedly fail, during the Bare Metal Server installation or for a Sync Driver action.

This happens because there's a timeout for the Bare Metal Server to download the driver packages to import. If this time is not enough, the action will fail.

To solve this issue, you can add this system variable *TEM_RELAY_DOWNLOADER_TIMEOUT* and set its value in minutes, to give more time to the Bare Metal Server to download the driver packages.

For example, to give 90 minutes, you set the value of this system variable to 90. The Bare Metal Service must be restarted after adding or modifying this variable value.

Adobe Flash removal from BigFix OS Deployment dashboards limitations

Problem description

OS Deployment dashboards can now work without Adobe Flash, however, with some limitations.

Solution/workaround

The following are some of the general limitations for all the OS Deployment dashboards after Adobe Flash dependency removal:

- Adjusting column width in the tables are not supported.
- Changing the column positions in the tables are not supported.
- The table headers are not sticky to the top of the rows when the tables are scrolled down.

Scripting Environment Library dashboard

This dashboard is obsolete and is being deprecated. The Adobe Flash version of this dashboard continues to be available.

CPU usage reaches 100% during installation or upgrade of a Bare Metal Server

Problem description

When installing or upgrading BigFix Bare Metal Server on an BigFix 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 reimage

Problem description

After a reimage 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 reimaging 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 that 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 reimaging from a 32-bit to a 64-bit architecture.

Solution/workaround

When this problem occurs, you can remove the duplicate entry from the BigFix Console by right-clicking on the computer name and selecting **Remove from database**.

Reimage in install mode on RedHat Enterprise Linux (RHEL) 7 stops during boot sequence

Problem description

During a reimage 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.

Failure during "Send to Server" of a Bare Metal profile

Problem description

From the Image Library dashboard, when a "Send to Server" of a profile is started through the corresponding button, the action "Bare Metal Profile Properties" is triggered. If the last statement of the action fails with the following message displayed in the action info:

```
Failed continue if {exists file ((parameter "AGENTFOLDER" of action) &
"\mkgenericsysprof.log") whose (exists lines whose
 (it as string contains "[AGTRC:0]") of it)}
```

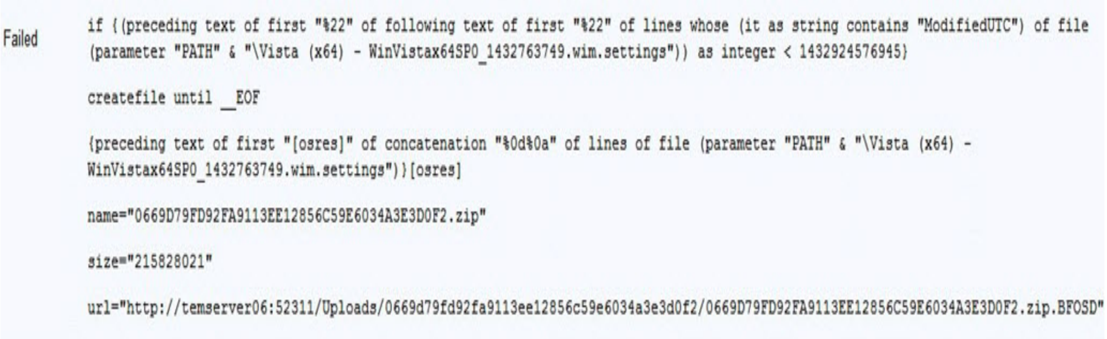
Solution/workaround

To troubleshoot the cause of the failure, on the Bare Metal Server open the file `C:\Program Files \BigFix OSD\mkgenericsysprof.log`. In this file you can find details about the cause of the error. Correct the problem and repeat the "Send to Server" operation.

Update profiles action on Bare Metal Server fails after editing driver bindings for Windows setup image

Problem description

When you modify a binding rule for a selected image and computer model from the Bindings tab of the **Driver Library** dashboard, an action is generated to update all Bare Metal Servers that have profiles linked to that image. If the binding rules for the same image and computer model are modified again at a later time, the "Update Profile on Bare Metal Server" task fails with the following error in the ActionScript Execution detail:



```
Failed    if {(preceding text of first "%22" of following text of first "%22" of lines whose (it as string contains "ModifiedUTC") of file
          (parameter "PATH" & "\Vista (x64) - WinVistax64SP0_1432763749.wim.settings")) as integer < 1432924576945}

          createfile until __EOF

          {preceding text of first "[osres]" of concatenation "%0d%0a" of lines of file (parameter "PATH" & "\Vista (x64) -
          WinVistax64SP0_1432763749.wim.settings")}[osres]

          name="0669D79FD92FA9113EE12856C59E6034A3E3D0F2.zip"

          size="215828021"

          url="http://temserver06:52311/Uploads/0669d79fd92fa9113ee12856c59e6034a3e3d0f2/0669D79FD92FA9113EE12856C59E6034A3E3D0F2.zip.BFOSD"
```

The problem is caused by incorrect handling of the first driver binding rule change for the image.

Solution/workaround

From the Bare Metal Server dashboard, you must manually start a sync action on each Bare Metal Server with profiles that are linked to the image for which the binding rule was changed.

Disk full on IEM server during download of image

Problem description

During a re-image activity, on the server system the WIM file is moved to the downloads directory (download and set up WIM image task). This operation requires the server to have free disk space of at least twice the size of the WIM image. If the disk space on the server is not sufficient, the server retries the download action several times. Even if you free space, the task cannot recover and remains in a waiting state (pending downloads for the main task).

Solution/workaround

Cancel the re-image activity. Check that you have enough free space and start a new re-image task.

Capture fails if network boot is configured before disk in target boot sequence and PXE server is in the same network

Problem description

During a capture scenario for both BIOS and UEFI targets, if the network boot entry preceeds the disk boot entry and there is a PXE Server in the target's network, the capture action fails when the target performs a PXE boot on the network instead of loading WinPE. The action status might remain running or change to complete.

Solution/workaround

Check the boot sequence at the target, and eventually change the configuration so that the target boots from disk instead of performing a network boot with a PXE server.

Deployment from media fails because some files are not read correctly

Problem description

Deployments using offline or netboot media can fail because some files on the media are not read correctly. For example, this error can occur if you are using the media for deployments on older hardware or operating systems that might not support the current UDF format (UDF version 1.02) used to create the media.

Solution/workaround

A possible solution is to create the deployment media using the old ISO9660 format, To use this format, you must add a computer setting on the Bare Metal Server that you selected for the media creation. Locate the Bare Metal Server in the **Subscribed Computers** view, then edit the computer and add the following custom setting:

```
BAREMETAL_USE_ISO9660
```

Set the value to `TRUE`.

This setting forces the creation of the media in the legacy ISO9660 format. Recreate the media and repeat the deployment.

RBO entry causes Linux targets to reboot repeatedly during capture or reimage

Problem description

During a capture or a reimage deployment, a new entry is added to the linux boot loader of the system being captured or reimaged. If the capture or deployment fails, the RBO entry might not be removed on the Linux target. This causes the target to reboot repeatedly. To remove the entry manually, complete the steps described below.

Solution/workaround

- For 32-bit Linux systems:
    1. Download http://software.bigfix.com/download/osd/rbagent.bin.
    2. Make it executable (`chmod +x rbagent.bin`).
    3. Download rbagent.pak http://software.bigfix.com/download/osd/rbagent.pak in the same directory of the rbagent.bin.
    4. Run the following command:

       ```
       rbagent.bin -o rad-setlinuxboot removeconf
       ```
- For 64-bit Linux systems:
    1. Download http://software.bigfix.com/download/osd/rbagent64.bin.
    2. Make it executable (`chmod +x rbagent64.bin`).
    3. Download rbagent.pak http://software.bigfix.com/download/osd/rbagent.pak in the same directory of the rbagent64.bin.
    4. Run the following command:

       ```
       rbagent64.bin -o rad-setlinuxboot removeconf
       ```

Console freezes when importing a captured Windows image (.wim) file

Problem description

When you import in the Image Library a captured image that resides on a remote machine and click "Analyze", this operation might cause the console to freeze for some time, depending on the size of the `.wim` file and the network speed.

Solution/workaround

To avoid this problem, copy the image locally on the machine where your Console is installed and repeat the import operation.

Creation of OS resource fails

Problem description

When creating a Windows Bundle with a parameters.ini file pointing to an .iso containing `install.esd` or to a folder containing an `install.esd` image, and not `install.wim`, the creation of the bundle fails because the creation binary searches for `install.wim`.

Solution/workaround

The code was changed to manage that if `install.wim` is not found, `install.esd` is searched. But this works only with WADK 10 Version 1607.

To avoid this problem, use WADK 10 Version 1607.

Note: It might occur that the `install.wim` file is in fact an ESD file and it is handled as such.

Note: ESD images with more than one architecture are not supported, independently from the WADK level used.

Problem importing a Windows image on Windows 7 or Windows 2008 R2 when disablecompression parameter is set to 1 (true)

Problem description

When you import a Windows image on Windows 7 or Windows 2008 R2 machine, the import fails with an error message like:

```
12:19:58 PM: [2016/07/05 10:18:17] A <INF> Extracting Driver information from WIM image...
16/07/05 10:18:24] Cannot find Windows files in
 local://temp/tpm_BB8EF01E69B2DD1F_1<BR>[2016/07/05 10:18:25]
 A <ERR> Error raised by OSDT_ExtractWIMDrivers inload.rbc, line 2268 [VM:3338][2016/07/05
 10:18:25]
 A<ERR> Index out of range (2)
```

This problem occurs when the disablecompression parameter of Windows is set to 1 (TRUE).

Solution/workaround

To solve the problem, check the setting of this parameter by running the following command from a DOS shell with administrator rights:

```
fsutil behavior query disablecompression
```

.

The query must return the value zero (false). If the value returned is 1 (TRUE), you must change the setting by running the following command:

```
fsutil behavior set disablecompression 0
```

You must restart the computer to enable the new behavior .

Cannot capture/deploy Ubuntu 18.04 from/to VMware Virtual Machine Version 13 or later

Problem description

When you try to capture/deploy Ubuntu 18.04 from/to VMware Virtual Machine Version 13 or later a white screen appears. This issue occurs for both BIOS and UEFI firmware.

Solution/workaround

Using a VMware Virtual Machine Version earlier than 13 is recommended, alternatively the capture/deploy with resource Ubuntu 16.04 is also possible.

RHEL/CentOS versions up to 7.3 prompt for user creation after Bare Metal Deploy

Problem description

After bare metal deployment, on the first start, RHEL/CentOS versions up to 7.3 prompt for the creation of user account and password. This action is mandatory to start the OS. The issue is verified on gnome-based installation. To note, the deploy of the setup completes successfully and the root user is correctly installed.

Solution/workaround

The issue is caused by a service installed by package *gnome-initial-setup*. This service no longer exists in later versions of the package. A possible workaround is to edit the manual tab as follows:

```
%packages
-gnome-initial-setup
%end
%post
yum group mark blacklist gnome-desktop
%end
```

.

This set of instructions blocks the installation of *gnome-initial-setup* during the deploy and "*yum group mark blacklist gnome-desktop"* and prevents future installations after updates.

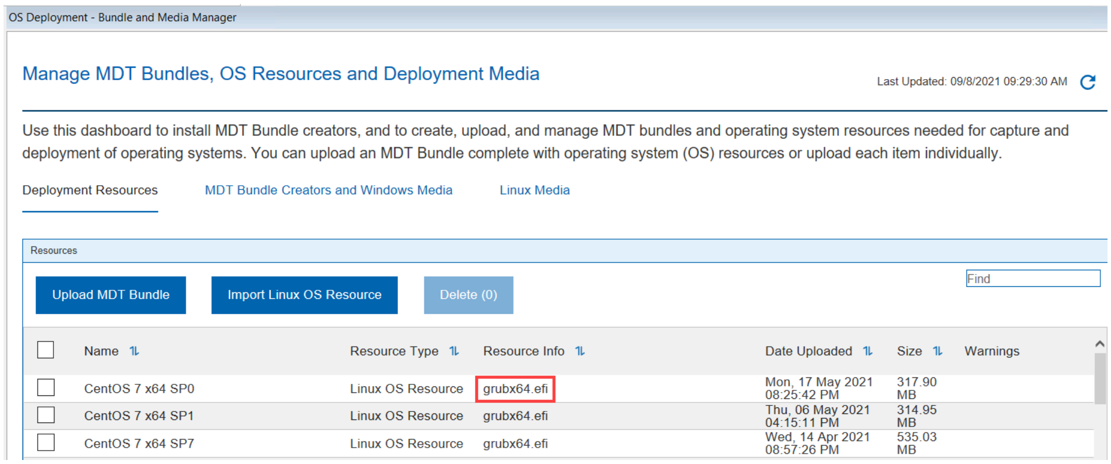
Kernel panic error while deploying Linux images on VM with UEFI firmware

Problem description

When you try to deploy a Linux image on some VMware Virtual Machine versions with UEFI firmware, you might get kernel panic error and the deployment stops. This issue occurs for both setup and capture images deployments.

Solution/workaround

Ensure that the corresponding Linux OS resource has the `grubx64.efi` or `grub.efi` flag as shown in the following figure. If not, you can re-import the Linux OS resource. Otherwise, for all supported Linux operating systems, you can also use the grub2 loader by following the instructions in Use grub2 bootloader for Linux deployment on UEFI targets *(on page 216)*.


OS Deployment - Bundle and Media Manager
Last Updated: 09/8/2021 09:29:30 AM
Deployment Resources
MDT Bundle Creators and Windows Media
Linux Media
Resources
Upload MDT Bundle
Import Linux OS Resource
Delete (0)
Find

Manage MDT Bundles, OS Resources and Deployment Media

Use this dashboard to install MDT Bundle creators, and to create, upload, and manage MDT bundles and operating system resources needed for capture and deployment of operating systems. You can upload an MDT Bundle complete with operating system (OS) resources or upload each item individually.

☐	Name	Resource Type	Resource Info	Date Uploaded	Size	Warnings
☐	CentOS 7 x64 SP0	Linux OS Resource	grubx64.efi	Mon, 17 May 2021 08:25:42 PM	317.90 MB	
☐	CentOS 7 x64 SP1	Linux OS Resource	grubx64.efi	Thu, 06 May 2021 04:15:11 PM	314.95 MB	
☐	CentOS 7 x64 SP7	Linux OS Resource	grubx64.efi	Wed, 14 Apr 2021 08:57:26 PM	535.03 MB	

Warnings on RHEL 9 deployment

Problem description

When installing a RHEL 9 image with BigFix client version lower than 11.0.2, some message may be displayed on the first boot of the operating system. The message will report warnings on initscripts services, that is the service manager of the installed BigFix client. For example -

```
/etc/rc.d/rc.local is not marked as executable, skipping.
```

Solution/workaround

This will not cause any issues and the message won't appear on any subsequent booting(s) of the operating system.

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 BigFix Console is installed as well as on the BigFix 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 Airgap tool 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 BigFix Server.

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 on the Wiki Utilities page at the following link. 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`.

3. Pre-cache additional files on the BigFix server:

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 BigFix 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.exe
- http://software.bigfix.com/download/osd/RelayDownloader-x64.exe
- http://software.bigfix.com/download/osd/RelayDownloader.bin
- http://software.bigfix.com/download/osd/RelayDownloader-x64.bin
- http://software.bigfix.com/download/osd/RelayDownloader-x64_1.0.bin

- http://software.bigfix.com/download/osd/RelayDownloader-x64_1.1.bin
- http://software.bigfix.com/download/osd/getLocaleName.exe
- http://software.bigfix.com/download/osd/unzip-6.0.exe
- http://software.bigfix.com/download/osd/unzip32-6.0.exe
- http://software.bigfix.com/download/osd/unzip64-6.0.exe
- http://software.bigfix.com/download/osd/zip.exe

If you want to install the latest Bare Metal OS Deployment Server version from the network using the corresponding button in the Bare Metal Server Manager dashboard, you must also pre-cache the following;

- http://software.bigfix.com/download/osd/bmserver.zip.

The downloaded files must be renamed with their SHA1 before you copy them to the SHA1 folder.

If you are provisioning a Linux system, and installing an BigFix Client, you must also pre-cache the selected client installation packages.

If you are performing a Bare Metal provisioning of a Windows system with an image of type Setup, and installing an BigFix Client, you must pre-cache the selected client installation packages. For example, if you are provisioning one of the supported Windows versions, and select to install the Client Version 9.1.1229.0, you must pre-cache the following package:

```
<IEMOSAgentImage>

  <CompatibleOS name="MicrosoftWindows" version="5.1" />

  <CompatibleOS name="MicrosoftWindows" version="5.2" />

  <CompatibleOS name="MicrosoftWindows" version="6.0" />

  <CompatibleOS name="MicrosoftWindows" version="6.1" />

  <CompatibleOS name="MicrosoftWindows" version="6.2" />

  <CompatibleOS name="MicrosoftWindows" version="6.3" />

  <ImageName>BigFix-BES-Client-9.1.1229.0.exe</ImageName>

  <ImageSha>ac13e360e122d2079f88628dfa6e89af71c29b599aa45917514938376809e884</ImageSha>

        <ImageSize>12136344</ImageSize>

        <ImageURL>http://software.bigfix.com/download/bes/91/

           BigFix-BES-Client-9.1.1229.0.exe</ImageURL>

 </IEMOSAgentImage>
```

For more information, see the Image catalog file at this link: http://software.bigfix.com/download/bes/util/AgentDeployment/TEMImageCatalog.xml

.

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.

Appendix B. Deprecated and Superseded functionalities

This topic lists the functionalities that are still present in OSD, but are deprecated.

Deprecated Component Combinations for MDT Bundle Creator

The following tool combinations are deprecated. You cannot select these tool combinations when you install the MDT Bundle Creator from the Bundle and Media Manager Dashboard.

- MDT Build 8456 and WADK 10 version 22H2
- MDT Build 8456 and WADK 10 version 21H2
- MDT Build 8456 and WADK 10 version 2004
- MDT Build 8456 and WADK 10 version 1903
- MDT Build 8456 and WADK 10 version 1809
- MDT Build 8450 and WADK 10 version 1809
- MDT Build 8450 and WADK 10 version 1803
- MDT Build 8450 and WADK 10 version 1709
- MDT Build 8443 and WADK 10 version 1709
- MDT Build 8443 and WADK 10 version 1703
- MDT Build 8443 and WADK 10 version 1607
- MDT 2013 Update 1 and WADK 10
- MDT 2013 and WADK 8.1 (WinPE 5)
- MDT 2012 Update 1 WADK 8 (WinPE 4)
- MDT 2012 Update 1 and WAIK (WinPE 3)

If you have MDT Bundles created with the deprecated tools, they are visible from the Bundle and Media Manager dashboard, and you can continue to use them. You can create MDT Bundles with the deprecated tools using the Fixlets available in the manual procedure or others in the Superseded and Deprecated Fixlets *(on page 260)* section.

Note:

1. If you are reimaging Windows 7 to Windows 7, using MDT Bundle 3.8.12 or later, created with WADK 10 and MDT 2013 Update 1, the **Migrate user settings** option is not supported.
2. WADK 10 version 2004 does not show the progress bar for few minutes while the computer is downloading the `boot.wim` for UEFI target.

Proxy Agent

Learn how to install or uninstall the superseded BigFix versions.

Installation steps for superseded BigFix versions

If you are using a relay with BigFix 8.2 or BigFix 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 (Deprecated)** 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)**.

Uninstallation steps for superseded BigFix versions

If your relay is BigFix Version 8.2 or 9.0:

1. Run the **Remove Management Extender for Bare Metal Targets** Fixlet (ID 151).
2. Remove the Proxy Agent: Run the remove action of the **Deploy Proxy Agent 9.0.40099 on 8.2 or 9.0 Relay (Deprecated)** Fixlet (ID 152).
3. 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.
4. Run the task **Deploy Management Extender for Bare Metal Targets (ID 150)**.

Superseded and Deprecated Fixlets

Following is the list of superseded Fixlets.

Upgrade Upload Maintenance Service (Deprecated) - Fixlet 24

This Fixlet upgrades the Upload Maintenance Service to version 1.0.0.17.

Deploy Microsoft .NET Framework (Superseded) - Fixlet 41

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

Deploy PowerShell (Deprecated) - Fixlet 42

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

Deploy WAIK (Superseded) – Fixlet 45

Use this Fixlet to download and install the Windows Automated Installation Kit (to use with MDT 2012 Update 1) on the selected computer.

Deploy Windows Assessment and Deployment Kit 8 and 8.1 (Superseded) - Fixlet 60

Use this Fixlet to download and install the Windows Automated Installation Kit (to use with MDT 2012 Update 1) on the selected computer.

- WADK8 (to use with MDT 2012 Update 1)
- WADK 8.1 (to use with MDT 2013)

Superseded and Deprecated Tasks

Following is the list of superseded and deprecated Tasks.

Install Upload Maintenance Service for OS Deployment (Deprecated) - Task 9

This task installs the latest version of the Upload Maintenance Service on the required platform versions.

Deploy operating system to one or more registered computers (Superseded) – Task 107

This Fixlet deploys a Bare Metal Profile to one or more registered computers. This Fixlet requires RAD image format that are no longer supported to deploy images.

Deploy an operating system to one or more computers (Superseded) – Task 133

This Fixlet deploys a Bare Metal Profile to one or more computers. This Fixlet requires RAD image format that are no longer supported to deploy images.

Deploy Proxy Agent 9.0.40099 on 8.2 or 9.0 Relay (Deprecated) – Task 152

This Fixlet Installs (or Removes) the Proxy Agent on machines already running a Relay version 8.2 or version 9.0. For later Relay versions use the Proxy Agent install Fixlet that is provided in the BES Support site.

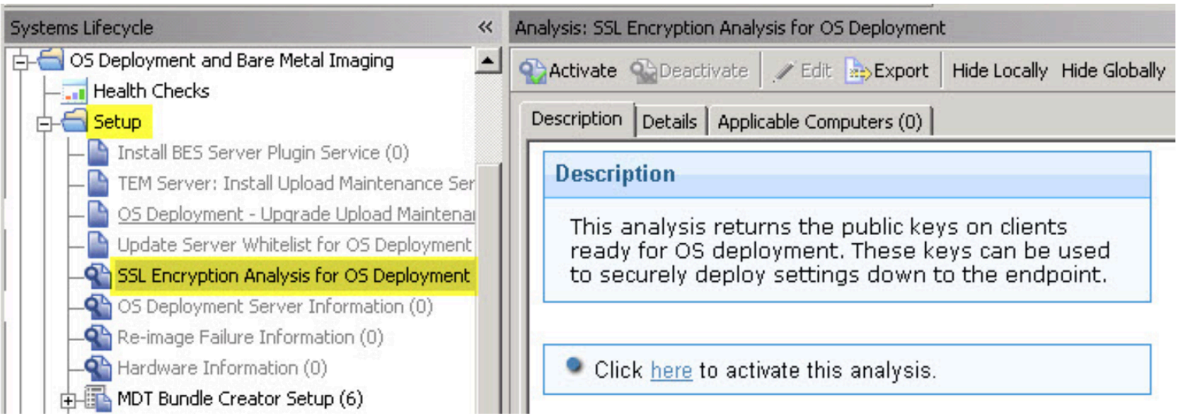
Deprecated Analysis

SSL Encryption Analysis for OS Deployment (Deprecated)–ID 30

The SSL Encryption Analysis is not applicable for BigFix client 9.0 or later. Only BigFix clients 8.2 needs it for encrypting actions. If all the clients are of version 9.0 or later, this is not necessary. Hence, this analysis is marked as deprecated.

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

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



Systems Lifecycle
OS Deployment and Bare Metal Imaging
Health Checks
Setup
Install BES Server Plugin Service (0)
TEM Server: Install Upload Maintenance Ser
OS Deployment - Upgrade Upload Maintenai
Update Server Whitelist for OS Deployment
SSL Encryption Analysis for OS Deployment
OS Deployment Server Information (0)
Re-image Failure Information (0)
Hardware Information (0)
MDT Bundle Creator Setup (6)
Analysis: SSL Encryption Analysis for OS Deployment
Activate
Deactivate
Edit
Export
Hide Locally
Hide Globally
Description
Details
Applicable Computers (0)

Description

This analysis returns the public keys on clients ready for OS deployment. These keys can be used to securely deploy settings down to the endpoint.

Click here to activate this analysis.

Appendix C. Create Ubuntu OS Resources manually

In alternative to Task 68, you can use a script to manually create the Ubuntu Resources needed for your deployments, as described in the following steps. The script requires that you download a Server .ISO file of the same point release of the Ubuntu Desktop that you plan to deploy on your workstations.

Important:

- Ubuntu 16.04, 18.04, and 20.04 require the Legacy Server ISO. You can download the Ubuntu Server ISO from the alternative downloads of the official Ubuntu webpage (for Ubuntu 20.04 visit http://cdimage.ubuntu.com/ubuntu-legacy-server/releases/20.04/release).
- Ubuntu 22.04 and later supported versions require the Live Server ISO.

Creating OS Resources for Ubuntu deployments using the resource creation tool

To create an OS Resource for Ubuntu deployments manually, perform the following steps on an Ubuntu machine (where you have installed the required packages)[1] with the same release as that of the downloaded Server .ISO.

1. Download the Ubuntu Resource Creator Script from the following link: http://software.bigfix.com/download/osd/ubuntu_resource_tool.sh. You can also use the link available in Task 68.
2. Download the Ubuntu server .iso file from the internet depending on the version and architecture required for your deployments.[2]
3. From the directory where you downloaded the Resource Creator script, run it as `root` or `sudo`, using the syntax:

   ```
   ubuntu_resource_tool.sh [-w <working_dir>] [-c <copy_to_folder>][-l
    <logfile_path]{<path_to_server_iso>}
   ```

   Where:

   - `-w <working_dir>` is the working directory used by the OS resource creation process. It is optional. If not specified, the tool uses a temporary directory named `wd` in the current path.
   - `-c <copy_to_folder>` is the directory where the tool stores the generated OS resources. It is optional. If not specified, the OS resource is copied in the current path.
   - `-l <logfile_path>` is the path of the OS Resource creation process log. If not specified, the log file is created in the current path with the default name `prepare.log`
   - `{<path_to_server_iso>}` is the path of the Ubuntu server .iso file that you downloaded in step 2. If only the file name is specified, the current path is assumed.

   Note:

   - [1] Installed genisoimage package is needed to create the Ubuntu resource.
   - [2] The Ubuntu Server .iso file specified in the command must be the same point release version of the Ubuntu workstation that you want to provision.

For example, assuming that the `ubuntu_resource_tool.sh` is available in the current directory and that you downloaded the Ubuntu Server .iso in the `/tmp` folder, you can create the Ubuntu OS Resource with the following command:

```
sudo ./ubuntu_resource_tool.sh -w osdworkdir /tmp/ubuntu-16.04.2-server-amd64.iso
```

The directory specified in `-w` can be a relative or absolute path. The directory is created if it does not exist. If it already exists, all content is erased. In this example the resource file is created in the `osdworkdir` subdirectory.

The script produces an `.iso` file containing the OS resource which you must import from the Bundle and Media Manager dashboard. Depending on the Server version and architecture that you specified in input to the script (Server .iso file), the new OS resource file names are composed by a fixed part `OS_Resource_Ubuntu-Server` followed by the release such as `_16.04.2` and the architecture `_i386.iso` or `_amd64.iso`.

4. Import the Ubuntu resource from the Bundle and Media Manager dashboard, by clicking **Import Linux OS Resource** and specifying the path to the newly created Ubuntu OS Resource.

Appendix D. Support

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

- BigFix Support Portal
- BigFix Developer
- BigFix Playlist on YouTube
- BigFix Tech Advisors channel on YouTube
- BigFix Forum

Notices

This information was developed for products and services offered in the US.

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

HCL 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:

HCL
330 Potrero Ave.
Sunnyvale, CA 94085
USA
Attention: Office of the General Counsel

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

HCL
330 Potrero Ave.
Sunnyvale, CA 94085
USA
Attention: Office of the General Counsel

HCL TECHNOLOGIES LTD. 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 jurisdictions 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. HCL 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-HCL 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 HCL product and use of those websites is at your own risk.

HCL may use or distribute any of the information you provide 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:

HCL
330 Potrero Ave.
Sunnyvale, CA 94085
USA
Attention: Office of the General Counsel

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 HCL under terms of the HCL Customer Agreement, HCL International Program License Agreement or any equivalent agreement between us.

The performance data discussed herein is presented as derived under specific operating conditions. Actual results may vary.

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

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

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 actual people or business enterprises 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 HCL, 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. HCL, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS," without warranty of any kind. HCL 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:
© (your company name) (year).
Portions of this code are derived from HCL Ltd. Sample Programs.

Trademarks

HCL Technologies Ltd. and HCL Technologies Ltd. logo, and hcl.com are trademarks or registered trademarks of HCL Technologies Ltd., registered in many jurisdictions worldwide.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

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

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

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

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

Other product and service names might be trademarks of HCL or other companies.

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 HCL 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 HCL.

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 HCL.

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.

HCL 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 HCL, 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.

HCL 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.