

# Active System Manager Version 1.0.1

## User Guide



# Notes, Cautions, and Warnings



**NOTE:** A NOTE indicates important information that helps you make better use of your computer.



**CAUTION:** A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.



**WARNING:** A WARNING indicates a potential for property damage, personal injury, or death.

## © 2013 Dell Inc.

Trademarks used in this text: Dell™, the Dell logo, Dell Boom™, Dell Precision™, OptiPlex™, Latitude™, PowerEdge™, PowerVault™, PowerConnect™, OpenManage™, EqualLogic™, Compellent™, KACE™, FlexAddress™, Force10™ and Vostro™ are trademarks of Dell Inc. Intel®, Pentium®, Xeon®, Core® and Celeron® are registered trademarks of Intel Corporation in the U.S. and other countries. AMD® is a registered trademark and AMD Opteron™, AMD Phenom™ and AMD Sempron™ are trademarks of Advanced Micro Devices, Inc. Microsoft®, Windows®, Windows Server®, Internet Explorer®, MS-DOS®, Windows Vista® and Active Directory® are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. Red Hat® and Red Hat® Enterprise Linux® are registered trademarks of Red Hat, Inc. in the United States and/or other countries. Novell® and SUSE® are registered trademarks of Novell Inc. in the United States and other countries. Oracle® is a registered trademark of Oracle Corporation and/or its affiliates. Citrix®, Xen®, XenServer® and XenMotion® are either registered trademarks or trademarks of Citrix Systems, Inc. in the United States and/or other countries. VMware®, Virtual SMP®, vMotion®, vCenter® and vSphere® are registered trademarks or trademarks of VMware, Inc. in the United States or other countries. IBM® is a registered trademark of International Business Machines Corporation.

2013 - 01

Rev. A00

# Contents

<b>Notes, Cautions, and Warnings.....</b>	<b>2</b>
<b>1 About Active System Manager.....</b>	<b>9</b>
Key Features.....	9
Architecture Overview.....	10
Port Configuration.....	10
Refreshing a Screen.....	11
<b>2 Initial Setup.....</b>	<b>13</b>
Licensing.....	13
Time and Location.....	13
Proxy Settings.....	14
<b>3 Getting Started.....</b>	<b>15</b>
Device Requirements.....	15
Getting Started Tab.....	16
Dashboard Tab.....	16
<b>4 Devices.....</b>	<b>19</b>
Chassis.....	19
Discovering a Chassis.....	20
Configuring a Chassis.....	22
Running a Chassis Inventory Job.....	24
Checking Template Compliance for a Chassis.....	25
Reapplying a Template to a Non-Compliant Chassis.....	25
Removing a Chassis.....	25
Servers.....	25
Powering On a Server.....	26
Powering Off a Server.....	27
Running a Server Inventory.....	27
Checking Template Compliance for Servers.....	27
Reapplying a Template to a Non-Compliant Server.....	27
Removing a Server.....	28
Opening the iDRAC Remote Console.....	28
Server Port View.....	29
I/O Modules.....	30
Running an I/O Module Inventory.....	31

Checking Template Compliance for I/O Modules.....	32
Reapplying a Template to a Non-Compliant I/O Module.....	32
Removing an I/O Module.....	32
Resetting the SSL Certificate for a Device.....	32
Switching to Topology View.....	33
<b>5 Templates.....</b>	<b>35</b>
Management Template.....	35
Creating a Management Template.....	36
Copying a Template.....	40
Editing a Management Template.....	41
Deleting a Management Template.....	41
Deployment Templates.....	41
Creating a Deployment Template.....	42
Creating a Deployment Template from a Reference Server.....	47
Copying a Template.....	47
Editing a Deployment Template.....	47
Enabling a Deployment Template.....	48
Disabling a Deployment Template.....	48
Deleting a Deployment Template.....	48
<b>6 Deployments.....</b>	<b>49</b>
Creating a Deployment.....	50
Migrating a Deployment.....	50
Attaching a Deployment.....	51
Detaching a Deployment.....	51
Deleting a Deployment.....	52
<b>7 Networking.....</b>	<b>53</b>
Networks.....	53
Network Types.....	54
Adding or Editing a Network.....	54
Deleting a Network.....	55
Editing an IP Address Range.....	55
Deleting an IP Address Range.....	56
Pools.....	56
Creating an Identity Pool.....	56
Deleting an Identity Pool.....	57
Network Identities.....	57
Virtual MAC Identities.....	57
Virtual iSCSI Identities.....	58
Virtual FCoE Identities.....	59

<b>8 Jobs.....</b>	<b>61</b>
Exporting All Job Details.....	61
Purging the Job Queue.....	61
Retry a Job on a Device or Deployment in Error State.....	62
Force an Action on a Device or Deployment in Error State.....	62
<b>9 Settings.....</b>	<b>63</b>
Users.....	63
Creating a User.....	63
Deleting a User.....	64
Editing a User.....	64
Enabling or Disabling a User.....	64
About Roles.....	64
Environment.....	65
Editing Default Environment Monitoring Settings.....	65
Editing Default NTP Settings.....	66
Credentials.....	66
Creating a New Credential.....	66
Editing a Credential.....	67
Deleting a Credential.....	67
Logs.....	67
Exporting All Log Entries.....	68
Purging Log Entries.....	68
Appliance Management.....	69
Updating the Virtual Appliance.....	69
Editing the Update Repository Path.....	69
Generating a Troubleshooting Bundle.....	70
Proxy Settings.....	70
SSL Certificates.....	70
License Management.....	71
Backup and Restore.....	72
Backup Details.....	72
Editing Backup Settings And Details.....	73
Editing Automatically Scheduled Backups.....	73
Backup Now.....	73
Restore Now.....	74
Polling Intervals.....	75
Editing Automatically Scheduled Chassis Inventory Jobs.....	75
Setting Status Polling Interval.....	75
<b>10 Use Cases.....</b>	<b>77</b>

ESXi Using FCoE Datastores and Networking on Converged Fabric with Initial iDRAC Boot.....	77
Prerequisites.....	77
Configuring the Management Template.....	78
Configuring the Chassis.....	78
Configuring the Deployment Template.....	79
Deploying Servers.....	80
ESXi Using FCoE Datastores and Networking on Converged Fabric with Initial PXE Boot.....	80
Prerequisites.....	81
Configuring the Management Template.....	81
Configuring the Chassis.....	81
Configuring the Deployment Template.....	82
Deploying Servers.....	83
ESXi Using iSCSI Datastores and Networking on Separate Fabric with Initial iSCSI Boot.....	83
Prerequisites.....	84
Configuring the Management Template.....	84
Configuring The Chassis.....	84
Configuring the Deployment Template.....	85
Deploying Servers.....	86
ESXi Using FCoE Datastores and Networking on Separate Fabric with FCoE Boot.....	87
Prerequisites.....	87
Configuring the Management Template.....	87
Configuring the Chassis.....	88
Configuring the Deployment Template.....	88
Deploying Servers.....	89
Red Hat Enterprise Linux Using iSCSI Datastores and Networking on Converged Fabric.....	90
Prerequisites.....	90
Configuring the Management Template.....	91
Configuring the Chassis.....	91
Configuring the Deployment Template.....	91
Deploying Servers.....	92
Windows Server 2008 R2 Using FCoE Datastores and Networking on Converged Fabric.....	92
Prerequisites.....	93
Configuring the Management Template.....	93
Configure the Chassis.....	93
Configuring the Deployment Template.....	94
Deploying Servers.....	95
<b>11 Troubleshooting.....</b>	<b>97</b>
Browser Errors.....	97
Cannot Enable Or Disable DCB on Broadcom 57810 NIC.....	97
I/O Module Is Down On Active Deployment.....	97
Deployment in an Error State.....	97

Errors with QLogic Cards.....	98
Failed to Configure Server with Deployment Template.....	98
Failed to Connect to I/O Module Services.....	98
Failed to Create Virtual Disk.....	98
FlexAddress Not Available on a Server.....	98
I/O Module Unit Number Not Zero.....	99
Migrating Deployments.....	99
Operating System Security Patches for the Virtual Appliance.....	99
Scheduled Inventory Jobs Failing.....	99
Server Not Found in Deploy Wizard.....	100
UEFI Mode Not Working As Expected.....	100
Deploy Wizard Does Not Display Desired Chassis.....	100
Unresponsive User Interface in Internet Explorer 9.....	100
Updated Virtual Appliance Does Not Display Changes.....	100
Web Interface Time Out Causes Source Identity Information Conflict.....	100

<b>A COPYRIGHT AND PERMISSION NOTICE.....</b>	<b>101</b>
---	------------





# About Active System Manager

Active System Manager is an infrastructure management solution that speeds and simplifies the actions required to set up a Dell PowerEdge M1000e blade enclosure (chassis) environment, and enables administrators to easily configure hardware to support workload-specific needs. After infrastructure is up and running, Active System Manager helps to monitor and manage infrastructure changes within the environment.

The first part of this guide describes how to use specific Active System Manager features to create [templates](#), configure [devices](#) and [networking, deploy](#) servers, see active and pending [jobs](#), and change Active System Manager [settings](#).

At the end of the guide, you'll find a chapter that includes [use cases](#) for creating specific deployment types, and a chapter that is devoted to [troubleshooting](#) issues.

To learn about installing Active System Manager in your environment and configuring the virtual appliance that hosts the solution, see the *Active System Manager Version 1.0.1 Quick Installation Guide*.



**NOTE:** For the latest versions of all Active System Manager documentation, visit [www.dell.com/support/manuals](http://www.dell.com/support/manuals), and select **Choose from a list of all Dell products**. Then, click **Software, Electronics & Peripherals** → **Software** → **Enterprise System Management** → **Active System Manager v 1.0**.

## Key Features

Simplified infrastructure management:

- Manage infrastructure from anywhere using a web-based console
- Get started quickly with wizard-based configuration
- Switch between tabular and topology infrastructure views
- Add users in administrator and operator roles
- Troubleshoot data center issues efficiently from a graphical port view that maps virtual interfaces (including partitions) to networks

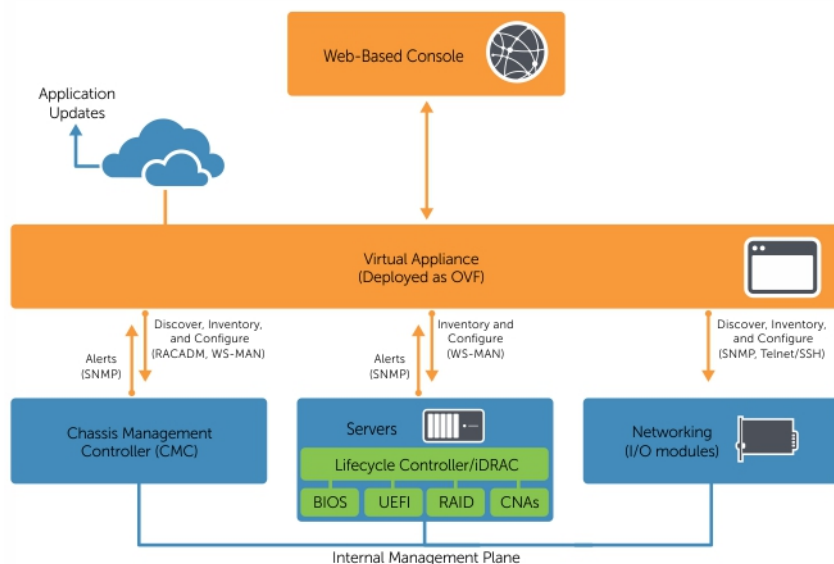
Automated hardware discovery:

- Discover multiple blade chassis using just the chassis IP address and credentials
- Automatically inventory chassis to detect server and I/O module details (firmware, CMC/iKVM, SNMP, and so on)
- Support up to 10 chassis and 320 blade servers

Template-based hardware configuration:

- Create one Management Template to configure multiple chassis, blade servers, and I/O modules
- Specify workload-driven requirements in Deployment Templates
- Easily migrate server deployments in cases of hardware failure
- Capture configuration details of existing servers

## Architecture Overview




## Port Configuration

**Table 1. Active System Manager virtual appliance port configuration**

Port(s)	Protocols	Port Type	Direction	Use
20, 21	FTP	TCP	Outbound	FTP command client
22	SSH	TCP	Outbound	I/O module
23	Telnet	TCP	Outbound	I/O module
53	DNS	TCP	Outbound	DNS server
67, 68	DHCP	UDP	Outbound	DHCP server
69	TFTP	UDP	Inbound	Firmware updates
80	HTTP	TCP	Outbound	HTTP server
123	NTP	UDP	Outbound	Time synchronization
162, 11620	SNMP	UDP	Inbound	SNMP communication for devices
443	HTTPS	TCP	Inbound	Web interface
443, 4433	WS-MAN	TCP	Outbound	iDRAC and CMC communication
445	CIFS	TCP	Outbound	Back up program data to CIFS share
2049, 111, 4001 - 4004	NFS	TCP, UDP	Inbound	Firmware updates
2049	NFS	TCP	Outbound	Back up program data to NFS share

Port(s)	Protocols	Port Type	Direction	Use
5432	PostgreSQL	TCP	Inbound	Database

## Refreshing a Screen

To refresh information listed on detail screens, click the **Reload Grid** icon (  ). Otherwise, Active System Manager automatically refreshes the screen with updated information every 20 seconds.



# Initial Setup

The Initial Setup wizard configures basic settings required to begin using Active System Manager. Until Initial Setup is complete, Active System Manager will automatically display the wizard every time you log in.

Before you begin, it is recommended to gather the following information:

- Local network share where the Active System Manager [license](#) is stored
- (Optional) [Time and location](#) information, including the time zone where the virtual appliance that hosts Active System Manager is installed and IP addresses of up to two NTP servers
- (Optional) [Proxy server](#) information, such as IP address, port, and credentials

Clicking **Finish** on the final page of the Initial Setup wizard applies the settings you entered and restarts the Active System Manager virtual appliance. To change basic configuration settings after Initial Setup is complete, click the [Settings](#) links in the left pane.



**NOTE:** After completing Initial Setup, it is recommended to [generate](#) and [upload](#) an SSL certificate to prevent users from experiencing browser security errors.

## Licensing

Active System Manager licensing is based on the total number of managed servers. There are two valid license types:

- Standard – Full-access license with no expiration date
- Trial – Limited license that expires after a specified number of days

For both license types, you will receive an email from customer service with instructions on how to download the license file to a local network share. The first time you use Active System Manager, you must upload the license file through the Initial Setup wizard; however, you can upload subsequent licenses on the [Appliance Management](#) screen.

1. On the **Licensing** page of the Initial Setup wizard, click **Browse**, select a valid license file, and then click **Open**.
2. Click **Upload** to load the license file into Active System Manager and display its details.
3. Click **Save and Continue** to immediately activate the license.

## Time and Location

The **Time & Location** page of the Initial Setup wizard sets the time zone in which the Active System Manager virtual appliance operates, and configures optional Network Time Protocol (NTP) servers used for time synchronization.

NTP is a protocol that synchronizes the clocks of networked devices, so that network artifacts are stamped with the same date and time. This consistency is essential to troubleshooting communication problems between devices.

After Initial Setup is complete, you can [change NTP server information](#) from the **Settings** link in the left pane.

1. On the **Time and Location** page of the Initial Setup wizard, select the **Time Zone** in which the virtual appliance operates.



**NOTE:** Clicking **Finish** on the final page of the Initial Setup wizard configures time zone settings on the virtual appliance. Until then, dates and times displayed for various components (for example, logs and job entries) may be incorrect.

2. Optionally, to use an NTP server for time synchronization, select **Enable NTP Server** and enter the IP address or Fully-Qualified Domain Name (FQDN) of a **Preferred NTP Server** and **Secondary NTP Server** (optional). If unselected, the virtual appliance will synchronize time with the hypervisor.
3. Click **Save and Continue**.

## Proxy Settings

If the target environment uses a proxy server to communicate with external services, then you must provide that information to Active System Manager. Alternatively, if the environment does not require a proxy server for external communication, select **Do not use a proxy server**.

After Initial Setup is complete, you can [change the proxy settings](#) from the **Settings** link in the left pane.

To enable communication through a proxy server:

1. On the **Proxy Settings** page of the Initial Setup wizard, select **Use these proxy server settings**.
2. Enter a **Server Address** (IP address or host name) for the proxy server.
3. Enter a **Port** for the proxy server.
4. If the proxy server requires credentials to log in, select **Use proxy credentials** and then enter the **User Name** and **Password**.
5. Click **Test Proxy Connection** to validate the settings entered on this page.
6. Click **Save and Continue**.

# Getting Started

After completing the [Initial Setup](#) wizard, you are ready to configure the Active System Manager environment.

By default, until the basic steps to configure hardware and networking are complete, Active System Manager opens on the [Getting Started](#) tab of the **Home** screen. This screen provides step-by-step links to the recommended workflow for getting started with Active System Manager.

After basic steps for configuring hardware and networking are complete, the **Home** screen opens on the [Dashboard](#) tab.

## Device Requirements

Active System Manager requires the managed infrastructure environment to include specific devices configured with minimum firmware levels:

**Chassis** – One or more PowerEdge M1000e (with K-model switch) blade enclosures configured with:

- Midplane version 1.1 with end-to-end 10 GbE
- Dual Chassis Management Controller (CMC) with the most recent available firmware version
- Connectivity to 1 Gb out-of-band (OOB) management network
- Up to six power supplies
- FlexAddress turned off

**Blade servers** – Dell PowerEdge 12th generation servers (M820, M620, and/or M420) configured with:

- iDRAC7 Express or iDRAC7 Enterprise with firmware version 1.30.30
- Lifecycle Controller 2 with firmware version 1.1.0.1108
- Network Interface Card (NIC) with 10GBASE-KR and minimum Fabric A support
  - Broadcom – 57810-k Network Daughter Card (NDC) or mezzanine card with firmware version 7.4.8
- If using a RAID configuration:
  - PowerEdge H310 – firmware version 20.11.0-0002
  - PowerEdge H710 and H710P – firmware version 21.1.0-0007
  - PowerEdge S110 Software RAID – Windows Server 2008 (32-bit, 64-bit, and R2) firmware version 3.0.0.0134; PERC firmware version 3.0.0.0139

### I/O Module

- PowerEdge M I/O aggregator with firmware version 8.3.17.2

**Top-of-Rack (ToR) Switch** – Minimum of two


- Dell Force10 S4810 with firmware version 8.3.12.0
- Cisco Nexus 5020 with firmware version 5.1(3)N2(1a)

## External Storage

- EqualLogic PS6110 (iSCSI only) with firmware version 6.0.1
- EqualLogic PS6510 (iSCSI only) with firmware version 6.0.1
- Compellent SC8000 (iSCSI and FCoE) with firmware version 6.0 or higher

## Getting Started Tab

The **Getting Started** tab of the **Home** screen displays the end-to-end steps required to configure hardware and networking infrastructure. After completing these steps, deployed servers are ready for operating system installation.

- **Step 1: Discover Chassis** – [Discover](#) one or more Dell PowerEdge m1000e chassis to configure. Active System Manager will connect to the chassis, confirm that the Chassis Management Controller (CMC) meets minimum firmware requirements, perform an inventory of devices within the chassis, and then store inventory results.  
 **NOTE:** Chassis discovery requires a minimum Chassis Management Controller (CMC) firmware version of 4.0. To discover a chassis with firmware below the supported minimum, you must manually upgrade the firmware to at least 4.0 (see the *Dell Chassis Management Controller User Guide* for more information). During chassis configuration, Active System Manager will automatically upgrade firmware to the latest supported version.
- **Step 2: Configure Chassis** – Define and set device management properties for Chassis Management Controllers (CMCs), Integrated Dell Remote Access Controllers (iDRACs), and I/O modules. You can define these properties once within a [Management Template](#), and then apply the template to multiple devices.
  - a. [Create a Management Template](#) that includes chassis configuration default values
  - b. [Configure a chassis](#) and its servers and I/O modules by applying a Management Template
- **Step 3: Deploy Servers** – Define and set device properties related to the workload that runs on a blade server, such as BIOS settings and boot order. You can define these properties once within a [Deployment Template](#), and then apply the template to deploy multiple servers.
  - a. [Create a Deployment Template](#)
  - b. [Deploy one or more servers](#)

Additionally, on this screen you can see details for chassis discovery, configuration, and templates created under your account. You can also see jobs started by your account within the last 24 hours.

## Dashboard Tab

The **Dashboard** tab of the **Home** screen displays consolidated data about the Active System Manager environment, including:

- Status of all active deployments (Critical, Warning, Unknown, OK) organized by the Deployment Templates from which they were instantiated
- Health of all devices (Critical, Warning, Unknown, OK)
- Total number of servers deployed and available for deployment
- Dates of the last compliance and inventory scans
- Licensing information such as license type, number of licenses available and used, and total licences
- Recent activities performed by users



Click **Change Polling Intervals** to [modify](#) the dates and times when Active System Manager runs inventory jobs on all discovered chassis and updates device status.



# Devices

The **Devices** screen displays information about the chassis, servers, and I/O modules discovered by Active System Manager, including:

- Number and [health](#)
- Number of servers available and in deployment
- Time since last compliance scan
- Time since last inventory scan

From this screen, you can:

- Open the [server](#), [chassis](#), or [I/O module](#) details pages
- [Discover](#) a new chassis
- Change the [polling intervals](#) at which Active System Manager runs inventory jobs on all discovered chassis and updates device status

## Chassis

The **Devices** → **Chassis** screen displays information about chassis discovered by Active System Manager. By default, the page displays in a tabular view, with details that include:


- [Health](#)
- IP Address (click to open the Chassis Management Controller (CMC) console)
- Service Tag
- Blades (total number of blade servers within the chassis)
- Management Template (the last Management Template applied to the chassis)
- Compliance (device settings are compliant with the latest template applied to the device)
- [State](#)

From this screen, you can:

- [Switch to a topology view](#) (only available if devices are currently listed)
- [Run an inventory job](#) to discover chassis details
- [Discover](#) one or more chassis
- [Configure](#) chassis
- [Check template compliance](#) to compare the current chassis configuration to the Management Template
- [Reapply](#) a Management Template to a chassis in a *Not Compliant* state
- [Remove](#) a chassis
- [Reset](#) the security certificate for a chassis


Additionally, you can click a chassis to see its details, including:

- Summary
- Blades
- I/O Modules
- Chassis Controllers
- iKVM
- Power Supplies

 **NOTE:** You can modify how the screen displays by clicking a column name to sort displayed items by that column. You can also [refresh](#) the information on the screen.

## Discovering a Chassis

Use the Chassis Discovery wizard to discover one or more chassis that are configured with the same [credentials](#). You can discover new chassis, or discover existing chassis that are already configured within your environment.

 **NOTE:** Chassis discovery requires a minimum Chassis Management Controller (CMC) firmware version of 4.0. To discover a chassis with firmware below the supported minimum, you must manually upgrade the firmware to at least 4.0 (see the *Dell Chassis Management Controller User Guide* for more information). During chassis configuration, Active System Manager will automatically upgrade firmware to the latest supported version.


When Active System Manager discovers a chassis, it also discovers all servers and I/O modules within the chassis. After discovery, you can [configure the chassis](#) by applying a Management Template. For existing chassis, settings in the Management Template will override any configuration values that were previously set.

Before you begin, it is recommended to gather the following information:


- Chassis IP addresses
- Chassis credentials

Additionally, make sure the chassis is connected to the network, the Active System Manager virtual appliance has network connectivity, and the I/O modules in the chassis are wired to the network.

1. Click **Devices** → **Chassis** in the left pane.
2. Click **Discover Chassis**.
3. On the **Welcome** page of the Chassis Discovery wizard, click **Next**.
4. On the **Chassis Connection** page, [enter the chassis connection information](#). Click **Next**.
5. On the **Chassis Selection** page, select one or more chassis to be inventoried and managed by Active System Manager. Click **Next**.

 **NOTE:** You may have to wait while Active System Manager locates and displays all chassis that are connected to managed networks.

6. On the **Summary** page, click **Finish** to inventory the chassis, servers, and I/O modules and update the firmware on the non-compliant Chassis Management Controllers.

 **NOTE:** You must configure a link aggregation group (LAG) on each Top-of-Rack (ToR) switch to enable the server-facing ports on I/O modules. For more information on configuring a LAG, see the white paper *Dell PowerEdge M I/O Aggregator Configuration Quick Reference*.

## Entering Chassis Connection Information for Discovery

1. On the **Chassis Connection** page of the Chassis Discovery wizard, enter one or more **Chassis IP Addresses** of the chassis to discover. You must separate IP addresses with commas, or enter each IP address on a separate line.
2. Select an existing **Chassis Credential** that includes the user name and password required to access the chassis, or click **New** to create a new chassis credential.



**NOTE:** You can also [create](#) new credentials on the **Settings** → **Credentials** screen.

3. Click **Save and Continue**.



**NOTE:** To discover chassis with different credentials, run the Chassis Discovery Wizard again and select different credentials.

## Operational State

After initiating chassis discovery, Active System Manager assigns one or more of the following states to the chassis and each of its devices. These operational states display in the **Compliance** and **State** columns of the device overview screens.

- Compliant – Settings in the applied Deployment Template match the device configuration
- Non-compliant – Settings in the applied Deployment Template do not match the device configuration
- Ready – Ready to be used
- In Use – Currently deployed
- Pending Discovery – Discovering device to add to Active System Manager
- Pending Inventory – Determining device details
- Pending Compliance Check – Validating support for device details such as firmware version
- Pending Applying Template – Applying Deployment Template to the device
- Pending Firmware Update – Updating firmware
- Pending Delete – Removing device from Active System Manager
- Connectivity Error – Active System Manager cannot communicate with the device
- Not supported – Active System Manager does not support devices of this type, configuration, make, and/or model
- Error – Error encountered while executing the last job on the device (click the link for details)
- Not licensed – The device is not covered by a Active System Manager license
- Offline – The device is not physically detected within the chassis

## Health Status

Every device managed by Active System Manager is assigned one of the following health statuses.



– OK



– Warning



– Critical error



**NOTE:** A critical error indicates a hardware issue. For detailed information, click the device IP address to launch the Chassis Management Controller (CMC) or Integrated Dell Remote Access Controller (iDRAC) console.



– Under maintenance




– Not in use

## Configuring a Chassis

Use this wizard to configure one or more chassis and associated servers and I/O modules by applying a Management Template. Any settings configured on the chassis that are not handled by Active System Manager—for example, Microsoft Active Directory integration on a Chassis Management Controller (CMC)—will not change when the Management Template is applied. The wizard also configures fabric connectivity and identity information, and updates firmware that is not at the required level.

Except for identity information, the same configuration will apply to all selected chassis. When configuring multiple chassis, fabric connectivity settings correspond to the first selected chassis.

During configuration, Active System Manager powers on every blade in the chassis, and waits for Collect System Inventory On Restart (CSIOR) to complete. For this reason, some servers may take up to 15 minutes to move into a *Ready* state after configuration.


 **NOTE:** Configuring a chassis by applying a Management Template affects physical infrastructure, which may cause server fans to power on or increase in speed. This is standard behavior, to help ensure that hardware remains at the appropriate temperature.

Before you begin, it is recommended to gather the following information:

- Fabric and connectivity information
- Management Template
- Chassis, server, and I/O module identity information

1. Click **Devices** → **Chassis** in the left pane.
2. Select the chassis to configure, and click **Configure**.
3. On the **Welcome** page of the Configure Chassis wizard, click **Next**.
4. On the **Firmware** page, check the box to allow Active System Manager to update any firmware that is not at the required level. Click **Next**.


 **NOTE:** The **Firmware Version** indicates the version to which Active System Manager will upgrade.

 **NOTE:** Selecting this option is required to continue configuring the chassis.


5. On the **Connectivity** pages, [configure the fabrics](#) for the chassis. Click **Next**.

 **NOTE:** You must select the **Fabric Purpose** for at least one fabric.


6. On the **Templates** page, select the **Management Template** to apply to the chassis and the devices within the chassis. If a blade is inserted after the chassis is configured, this Management Template will still be applied. Click **Next**.
7. Optionally, on the **Device Identification** → **Chassis** page, enter configuration information for each chassis. Click **Next**.

 **NOTE:** Active System Manager will automatically register the chassis on the domain name server (DNS) with its **DNS Name**. This enables users to access the Chassis Management Controller (CMC) with a user-friendly name instead of an IP address, if that option is [enabled](#) in the Management Template. The maximum number of characters is 63. The first character must be an alphanumeric character (a-z, A-Z, 0-9), followed by alphanumeric characters or a hyphen (-).

8. Optionally, on the **Device Identification** → **Servers** page, enter an **iDRAC DNS Name** for each server in the selected chassis. Click **Next**.

 **NOTE:** Active System Manager will automatically register the server on the domain name server (DNS) with its **iDRAC DNS Name**. This enables users to access the server's Integrated Dell Remote Access Controller (iDRAC) with a user-friendly name instead of an IP address, if that option is [enabled](#) in the Management Template.


9. Optionally, on the **Device Identification** → **I/O Modules** page, enter a **Host Name** for each I/O module on each chassis. This is name that will display when connecting to the I/O module. Click **Next**.

 **NOTE:** To access the I/O module with a user-friendly name, register the device directly on the DNS.


10. On the **Summary** page, click **Finish** to configure the chassis.


## Configuring Fabrics

1. Select the **Fabric Purpose** to identify the type of traffic the fabric will carry and to perform automatic protocol configuration, if needed.
2. For LAN and SAN networks, check **Enable DCB** to enable [Data Center Bridging \(DCB\)](#), if needed. This option is automatically configured on FCoE and Converged networks.

 **NOTE:** DCB provides the control needed to converge LAN and SAN (iSCSI/FCoE) traffic types in the same network and ensure lossless performance for critical SAN traffic.

3. To manually add networks to this fabric, select **Customize networks for this fabric**, and then select from the available networks that display. This list is filtered based on the **Fabric Purpose**. To add a network to the list, click **New Network**, and enter required information.

 **NOTE:** Chassis with customized fabrics will not automatically display on the **Server Selection** page of the [Deploy](#) wizard, if the Deployment Template includes a [virtual NIC configuration](#). To resolve this issue, add the network(s) associated with the virtual NIC configuration to the fabric following the steps above.

 **NOTE:** If the server's NIC has been replaced since the server was discovered, then it is recommended to [run a manual inventory job](#) before deploying the server.

4. Click **Next**.

### *Fabric Purpose*

**Fabric Purpose** indicates the type of traffic a network fabric will carry. Selecting a fabric purpose on one of the **Connectivity** pages of the **Configure Chassis** wizard serves these purposes:

- Automatically configures the fabric with specific network protocols, if needed—for example, configures data center bridging (DCB) on FCoE and converged network types.
- Determines which converged network adapters (CNAs) to use for a virtual NIC—for example, if Fabric A has a LAN purpose and Fabric B has a SAN purpose, then Active System Manager places the virtual NIC that requires access to LANs on the network daughter card that is connected to Fabric A. Similarly, if a virtual NIC requires access to SAN networks, then Active System Manager assigns it to the Mezzazine NIC that is connected to Fabric B.
- When **Customize network VLANs for this fabric** is selected, only displays VLANs of the selected type.

Options include:

- LAN – Displays all public, private, and hypervisor management networks.
- Public LAN – Displays all public LAN and hypervisor management networks.
- Private LAN – Displays all private LAN networks.
- SAN – Displays all SAN (iSCSI) and SAN (FCoE) networks.
- SAN (iSCSI) – Displays all SAN (iSCSI) networks.

- SAN (FCoE) – Displays all SAN (FCoE) networks.
- Converged – Displays all networks (LAN, SAN, and FCoE).
- None – Leaves the VLAN with an undefined purpose. In this scenario, Active System Manager will not manage the fabric or its corresponding server converged network adapters (CNAs) or partitions.

By default, if a fabric has a supported I/O module, then Active System Manager will configure its server-facing ports for the defined fabric purpose. If a fabric has an unsupported I/O module and a defined fabric purpose, then Active System Manager will read the fabric purpose to determine how to configure the server CNAs or partitions.

### ***Data Center Bridging (DCB)***

Data Center Bridging (DCB) provides the control needed to converge LAN and SAN (iSCSI/FCoE) traffic types on the same network without losing critical SAN traffic.

In the past, it was common to separate SAN and LAN traffic onto different networks, because of the very different characteristics and reliability requirements of each traffic type. While most LANs can track packets and simply request retransmission when they are lost, SANs usually require a high level of consistency in packet transmission—especially when booting a physical or virtual operating system that is sensitive to failure when data is lost or delayed. DCB is useful, because it provides a mechanism to allow SAN and LAN traffic to share the same network, while still meeting the specific needs of highly-sensitive SAN traffic.

When enabling DCB on a network, best practices recommend supporting the feature on all devices. Otherwise, flow control is lost at the disabled device, resulting in dropped packets and poor performance.

DCB involves the following protocols:

- Priority Flow Control (PFC) provides the ability to execute granular flow control pause frames based on traffic type. PFC pause frames temporarily stop data flow from low-priority queues, while continuing to transmit and receive packets from higher-priority queues. This prioritization ensures that latency-sensitive storage is protected from unwanted pauses.
- Enhanced Transmission Selection (ETS) provides, among other things, guaranteed bandwidth to high-priority traffic, while still guaranteeing a minimum amount of bandwidth to lower-priority traffic. This helps to prevent one type of traffic from monopolizing all available bandwidth.
- Data Center Bridging Exchange Protocol (DCBx)—an extension of Link Layer Discovery Protocol (LLDP)—is a discovery and exchange protocol for communicating configuration and capability information between directly-connected devices to ensure consistency throughout a network.

## **Running a Chassis Inventory Job**

If scheduled, Active System Manager automatically runs inventory jobs to track chassis details. However, if changes to the device occur outside of Active System Manager after a scheduled inventory job runs—for example, servers or I/O modules are removed from or replaced in the chassis—then it may be necessary to manually run an inventory job to update Active System Manager.

1. Click **Devices** → **Chassis** in the left pane.
2. Select one or more compliant chassis.
3. Click **Run Inventory**.
4. Click **OK**.

An inventory job is scheduled, and the chassis state changes to *Pending Inventory*.

When the inventory is complete, the chassis state changes to *Ready* and its details display in the Summary tab.



## Checking Template Compliance for a Chassis

Checking template compliance for a chassis determines whether any device settings have changed since the last Management Template was applied.

1. Click **Devices** → **Chassis** in the left pane.
2. Select one or more chassis.
3. Select **Check Template Compliance** from the **Other Tasks** drop-down list.  
A compliance job is submitted, and the chassis state changes to *Pending Compliance Check*.
4. If a chassis is found to be non-compliant, click *Non-Compliant* in the **Compliance** column for a list of the non-compliant settings. [Reapply](#) the template to return the chassis to a *Ready* state.

## Reapplying a Template to a Non-Compliant Chassis

Reapply a template to reset the configuration of a chassis according to a Management Template.

1. Click **Devices** → **Chassis** in the left pane.
2. Select a non-compliant chassis.
3. Do one of the following:
  - Select **Reapply Template** from the **Other Tasks** drop-down list.
  - Click *Non-Compliant* in the **Compliance** column, and on the **Compliance Check** screen, click **Reapply Template**.

A reapply template job is submitted, and the chassis state changes to *Pending Apply Template*. When the reapply job is complete the state changes to *Ready*.

## Removing a Chassis

1. Click **Devices** → **Chassis** in the left pane.
2. Select one or more chassis, and click **Remove**.
3. On the confirmation screen, click **Yes**.  
The chassis state changes to *Pending Remove*.

After removal completes, the chassis and any servers and I/O modules it contains are removed from Active System Manager. The removal process shuts down the servers and erases identity information to prevent potential corruption, and identity information returns to the associated pool. Associated targets (for example, storage volume) are not affected.



**NOTE:** You cannot remove a chassis that is in any *Pending* state.

## Servers

The **Devices** → **Servers** screen displays information about servers that have been discovered or are pending discovery by Active System Manager. By default, the page displays in a tabular view, with details that include:

- [Health](#)
- IP Address

- Service Tag
- System Model
- CPUs
- Memory (GB)
- Deployment Name (name of the deployment associated with the server)
- Management Template (the last Management Template applied to the chassis)
- Compliance (device settings are compliant with the latest template applied to the device)
- [State](#)

From this screen, you can:

- [Switch to a topology view](#) (only available if devices are currently listed)
- [Run inventory](#) to discover server details
- [Power on](#) a server
- [Power off](#) a server
- [Check template compliance](#) to compare a server's current configuration to the last applied Management Template or Deployment Template
- [Reapply](#) the last applied Management Template or Deployment Template to a server in a *Not Compliant* state
- [Remove](#) a server
- [Reset](#) the security certificate for a server
- Open the [remote console](#) for a server's Integrated Dell Remote Access Controller (iDRAC)

Additionally, you can click a server to see its details, including:

- Summary
- Network Interfaces
- Firmware Revisions
- CPUs
- [Port View](#)



**NOTE:** You can modify how the screen displays by clicking a column name to sort displayed items by that column. You can also [refresh](#) the information on the screen.

## Powering On a Server

1. Do one of the following:
  - Click **Devices** → **Servers** in the left pane.
  - Click **Deployments** in the left pane.
2. Select one or more servers.
3. Click **Power On**.
4. On the confirmation screen, click **Yes**.

The server state changes to *Pending Power On*. When the server is powered on, if a deployment is currently applied to it, then its state transitions to *Activated* on the **Deployments** screen.

## Powering Off a Server

1. Do one of the following:
  - Click **Devices** → **Servers** in the left pane.
  - Click **Deployments** in the left pane.
2. Select one or more servers.
3. Click **Power Off**.
4. On the confirmation screen, click **Yes**.

The server state changes to *Pending Power Off*. When the server is powered on, if a deployment is currently applied to it, then its state transitions to *Deactivated* on the **Deployments** screen.

## Running a Server Inventory

If scheduled, Active System Manager automatically runs inventory jobs to track server details. However, if changes to the device occur outside of Active System Manager after a scheduled inventory job runs, then it may be necessary to manually run an inventory job to update Active System Manager.

1. Click **Devices** → **Servers** in the left pane.
2. Select one or more servers.
3. Click **Run Inventory**.
4. Click **OK**.

An inventory job is scheduled, and the server state changes to *Pending Inventory*.

When the inventory is complete, the server state changes to *Ready* and its details display in the Summary tab.

## Checking Template Compliance for Servers

Checking template compliance for a server determines whether device settings have changed since the last template was applied (Management Template or Deployment Template).

1. Click **Devices** → **Servers** in the left pane.
2. Select one or more servers.
3. Select **Check Template Compliance** from the **Other Tasks** drop-down list.

A compliance job is submitted, and the server state changes to *Pending Compliance Check*.
4. If a server is found to be non-compliant, click *Non-Compliant* in the **Compliance** column for a list of the non-compliant settings. [Reapply](#) the templates to return the chassis to a *Ready* state.

## Reapplying a Template to a Non-Compliant Server

Reapply a template to reset the configuration of a server to the last template applied (Management Template or Deployment Template).

1. Click **Devices** → **Servers** in the left pane.
2. Select a non-compliant server.
3. Do one of the following:


- Select **Reapply Template** from the **Other Tasks** drop-down list.
- Click *Non-Compliant* in the **Compliance** column, and on the **Compliance Check** screen, click **Reapply Template**.

A reapply template job is submitted, and the server state changes to *Pending Apply Template*. When the reapply job is complete, the state changes to *Ready*.

## Removing a Server

When a server is no longer needed, you can remove it from Active System Manager. This returns the server to a configured (but not deployed) state, deletes the associated deployment, and releases any resources consumed by the deployment.

1. Click **Devices** → **Servers** in the left pane.
2. Select one or more servers that are in an *Offline* state, and click **Remove**.


 **NOTE:** To move a server into an *Offline* state, [physically remove](#) it from the chassis.

3. On the confirmation screen, click **Yes**.

The server state changes to *Pending Remove*. The server powers off, Active System Manager erases network identity information from the server to prevent potential corruption, and network identity information returns to the associated pool.


## Physically Removing a Server


At times, you may need to physically remove a server from a chassis to add additional memory, replace the NIC, or perform other maintenance. After removing the server from a chassis, it moves into an *Offline* state in Active System Manager.

 **NOTE:** If the server is currently attached to a deployment, it is recommended to [detach the deployment](#) before starting the removal process to prevent network identity conflicts.

Reinserting the server into a managed chassis will cause Active System Manager to automatically:

- [Perform a compliance check](#)
- Reapply the [Management Template](#)
- Reapply the [Deployment Template](#), if the server was deployed when it was removed
- Move the server back into an *In Use* state

 **NOTE:** If the deployment was detached, as recommended above, reinserting the server will not reattach the deployment, since at time of insertion the deployment is not associated with any server.

 **NOTE:** Inserting the server into a chassis with a different wiring scheme than the original chassis may cause the deployment to fail.

## Opening the iDRAC Remote Console

To simplify routine server maintenance, you can open a remote console to the server's Integrated Dell Remote Access Controller (iDRAC) directly from Active System Manager:

 **NOTE:** For more information, see the *Integrated Dell Remote Access Controller User Guide*.

1. Click **Devices** → **Servers** in the left pane.
2. Do one of the following:

- a) Click the **IP Address** for the server.
- b) Select one server.
- c) In the **Other Tasks** drop-down list, select **Remote Console**.

## Server Port View



**NOTE:** To enable all fields in the port view topology, you must first [configure](#) the top-of-rack (ToR) switch. Additionally, the server must be [deployed](#).

On the **Devices** → **Servers** screen, click a server and then click the **Port View** tab to see a topology of how server ports are configured. Information includes:

- **NIC Partitions** – If the Network Interface Card (NIC) is configured to dynamically allocate bandwidth to applications, then the port view displays each partition and its details, including:
  - Max Bandwidth – Maximum amount of bandwidth in GB that will be dynamically allocated
  - Min Bandwidth – Minimum percentage of overall bandwidth that will be dynamically allocated
  - Network Mode – LAN, FCoE, and/or iSCSI
  - LAN identities
    - \* Virtual MAC address
    - \* Permanent MAC address
  - iSCSI identities
    - \* Virtual iSCSI MAC address
    - \* Permanent iSCSI MAC address
    - \* Initiator IQN
    - \* Initiator IP address
  - FCoE identities
    - \* Virtual FIP MAC address
    - \* Permanent FIP MAC address
    - \* Virtual WWPN
    - \* Permanent WWPN
    - \* Virtual WWNN
    - \* Permanent WWNN
  - iSCSI boot
    - \* Target IP address
    - \* Target IQN
    - \* Boot LUN
  - FCoE boot
    - \* Target WWPN
    - \* Boot LUN
- **Blade/Ports**
  - Fully Qualified Device Descriptor (FQDD) – Last three digits indicate slot/port number/partition number
  - Vendor
  - Product Name

- **I/O Modules**
  - Current health (green is OK, yellow is warning, red is critical)
  - IP address
  - Fabric associated with the port
  - Service tag
  - System model
  - Total number of ports
  - Last Management Template applied to the chassis associated with the I/O module
  - State
  - Uplinks – Total number of uplink Ethernet ports
  - Bandwidth – Total bandwidth of all uplinks
- **ToR Switches** — Top-of-rack (ToR) switch associated with the port, including:
  - MAC Address
  - Name
  - Description
- **VLAN – Networks** – Networks currently associated with the NIC partition
  - VLAN ID
  - Name

## Configuring ToR Switches for Port View Topology

To enable all fields in the port view topology, you must perform specific configuration steps on the top-of-rack (ToR) switch.



**NOTE:** These steps describe how to configure a Force10 S4810 switch; however, other switches also require similar configuration. For more information, see the User Guide for the specific switch model.

1. Log into the ToR switch.
2. Enter these commands to power on ToR ports that are connected to the I/O module.

```
Force10-1#configure
Force10-1(conf)#interface tengigabitethernet 0/34
Force10-1(conf-if-te-0/34)#no shutdown
Force10-1(conf-if-te-0/34)#exit
Force10-1(conf)#exit
Force10-1#
```

3. Enter these commands to publish ToR attributes.

```
Force10-2#configure
Force10-2(conf)#protocol lldp
Force10-2(conf-lldp)#no disable
Force10-2(conf-lldp)#advertise management-tlv system-name
Force10-2(conf-lldp)#advertise management-tlv system-description
Force10-2(conf-lldp)#exit
Force10-2(conf)#exit
```

4. Rediscover and configure any I/O modules that already exist in Active System Manager.

## I/O Modules

The **Devices** → **I/O Modules** screen displays information about Input/Output (I/O) modules that have been discovered or are pending discovery by Active System Manager.



**NOTE:** You must configure a link aggregation group (LAG) on each Top-of-Rack (ToR) switch to enable the server-facing ports on I/O modules. For more information on configuring a LAG, see the white paper *Dell PowerEdge M I/O Aggregator Configuration Quick Reference*.

By default, the page displays in a tabular view, with details that include:

- [Health](#)
- IP Address
- Service Tag
- System Model
- Ports
- Management Template (the last Management Template applied to the chassis)
- Compliance (device settings are compliant with the latest template applied to the device)
- [State](#)

From this screen, you can:

- [Switch to a topology view](#) (only available if devices are currently listed)
- [Run Inventory](#) to update the list of I/O modules
- [Check template compliance](#) to compare an I/O module's current configuration to its Management Template
- [Reapply](#) a Management Template to an I/O module in a *Not Compliant* state
- [Remove](#) an I/O module

Additionally, you can click an I/O module to see a summary of its details.



**NOTE:** The Template Applied, Last Inventory, Last Compliance Check, and Discovered On times are based on the Active System Manager virtual appliance, not the client system running the Active System Manager web interface.



**NOTE:** You can modify how the screen displays by clicking a column name to sort displayed items by that column. You can also [refresh](#) the information on the screen.

## Running an I/O Module Inventory

If scheduled, Active System Manager automatically runs inventory jobs to track I/O module details. However, if changes to the device occur outside of Active System Manager after a scheduled inventory job runs, then it may be necessary to manually run an inventory job to update Active System Manager.

1. Click **Devices** → **I/O Module** in the left pane.
2. Select one or more compliant I/O modules.
3. Click **Run Inventory**.
4. Click **OK**.

An inventory job is scheduled, and the I/O module state changes to *Pending Inventory*.

When the inventory is complete, the I/O module state changes to *Ready* and its details display in the Summary tab.

## Checking Template Compliance for I/O Modules

Checking template compliance for an I/O module determines whether device settings have changed from the last Management Template that was applied. This check does not include chassis identity information set in the [Configure Chassis](#) wizard.

1. Click **Devices** → **I/O Modules** in the left pane.
2. Select one or more I/O modules.
3. Click **Check Template Compliance**.  
A compliance job is submitted, and the I/O module state changes to *Pending Compliance Check*.
4. If an I/O module is non-compliant, click *Non-Compliant* in the **Compliance** column for a list of the non-compliant settings. [Reapply](#) the template to return the chassis to a *Ready* state.

## Reapplying a Template to a Non-Compliant I/O Module

Reapply a template to reset the configuration of an I/O module according to a Management Template.

1. Click **Devices** → **I/O Modules** in the left pane.
2. Select a non-compliant I/O module.
3. Do one of the following:
  - Select **Reapply Template**.
  - Click *Non-Compliant* in the **Compliance** column, and on the **Compliance Check** screen, click **Reapply Template**.

A reapply template job is submitted, and the I/O module state changes to *Pending Apply Template*. When the reapply job is complete, the state changes to *Ready*.

## Removing an I/O Module

When you physically remove an I/O module from a chassis, it remains in Active System Manager in an *Offline* state. To remove an I/O module from Active System Manager, it must be in an *Offline* state and it cannot be associated with a chassis.

1. Click **Devices** → **I/O Modules** in the left pane.
2. Select one or more I/O modules, and click **Remove**.
3. On the confirmation screen, click **Yes**.  
The I/O module state changes to *Pending Remove*.

## Resetting the SSL Certificate for a Device

If the **Enable Certificate Check** option is selected in a device's [credentials](#), then Active System Manager stores a copy of the device's SSL certificate. When Active System Manager communicates with the device, it compares the stored certificate to the certificate currently present on the device to ensure secure communication.

If security certificate errors display in Active System Manager when communicating with a device, then the stored certificate does not match the device certificate. Reset the certificate to delete the stored copy and upload the certificate that is currently on the device into Active System Manager.




1. Do one of the following:
  - To reset the certificate on a chassis, click **Devices** → **Chassis** in the left pane.
  - To reset the certificate on a server, click **Devices** → **Servers** in the left pane.
2. Select one or more devices.
3. Select **Reset Certificate** from the **Other Tasks** drop-down list.
4. On the confirmation screen, click **Yes**.

The SSL certificate for the selected device is deleted from the certificate store in Active System Manager. When Active System Manager next communicates with the device, it downloads and stores the new certificate.

## Switching to Topology View

By default, **Device** screens display in a tabular view; however, you can switch to a topology view that provides a graphical representation of a selected chassis and its associated servers and I/O modules.

1. Click **Devices** in the left pane, and then click **Servers, Chassis, or I/O Modules**.
2. Click a device.  
 **NOTE:** You can view the topology for one chassis at a time. If you select a server or I/O module, the topology view will default to the associated chassis and highlight the selected device.
3. In the upper-right corner of the screen, click **Switch to Topology View**. A topology displays that highlights the device from which you launched the view, and indicates the service tag, status, and IP address of the selected chassis and its associated devices. Additionally, it displays the fabric associated with each I/O module.
4. To display additional details for a specific device, hover the cursor over its icon. Hovering over an I/O module displays details about the associated fabric.



# Templates

In Active System Manager, a template defines the basic configuration of a device. You can create the following template types:

- [Management Templates](#) for configuring chassis
- [Deployment Templates](#) for configuring servers for deployment

The **Templates** screen displays the following data for Management Templates and Deployment Templates:

- **Total** – Number of templates that currently exist (includes both *Draft* and *Ready* states)
- **Ready** – Number of templates that are complete and available to apply to a device
- **Draft** – Number of templates that require additional information before they can be applied to a device

## Management Template

A Management Template contains basic configuration settings for a chassis and the servers and I/O modules within that chassis.

Creating a Management Templates saves time by enabling you to specify configuration settings once within the template. Then, you can apply that template to multiple chassis from the [Chassis Configuration](#) wizard. All chassis configured with the same Management Template must use identical device credentials.

The **Templates** → **Management Templates** screen displays the basic details of all existing Management Templates, including:


- Name
- Description
- Last Updated By
- [State](#)
- Usage (the number of chassis to which the template is currently applied)

From this screen, you can:

- [Edit](#) a Management Template
- [Create](#) a Management Template
- [Copy](#) a Management Template
- [Delete](#) a Management Template

Additionally, you can select a Management Template to see more details, including:

- **Summary** – Template information, device access, chassis power configuration, networking, environment configuration, and users
- **Chassis** – A list of chassis that are currently configured with this template

 **NOTE:** You can modify how the screen displays by clicking a column name to sort displayed items by that column. You can also [refresh](#) the information on the screen.


## Creating a Management Template


Before you begin, it is recommended to gather the following information:

- How to assign IP addresses to devices:
  - Use the device's existing IP address
  - Use DHCP to automatically allocate an IP address
  - Assign a static IP address from the pool of IP addresses in a management network
- User names and passwords of accounts that can access the devices to which the template is applied
- Optionally, IP addresses for alert destinations
- Optionally, SMTP server and email address for an account to receive alerts
- Optionally, NTP server IP addresses
- (Optional) Chassis Management Controller (CMC) and Integrated Dell Remote Access Controller (iDRAC) VLAN IDs

 **CAUTION:** Before enabling the chassis controller or iDRAC VLAN IDs, make sure you [understand](#) the steps you must take in your environment to prevent a loss of network connectivity to the chassis or server.


1. Click **Templates** → **Management Templates** in the left pane.
2. Click **Create**.
3. On the **Welcome** page of the Create Management Template wizard, click **Next**.
4. On the **Template Information** page, enter a unique **Name** and **Description** to help identify this template for future use. Click **Save and Continue**.

 **NOTE:** Valid characters include uppercase and lowercase letters, numbers, and spaces. The following special characters are also allowed: . \_ -()
5. On the **IP Addressing** page, [select the method of assigning IP addresses](#) to the chassis, servers, and I/O modules based on this template. Click **Save and Continue**.
6. On the **Credentials** page, select credentials for accessing chassis, servers, and I/O modules based on this template. Click **New** to create a new credential configuration, or select an existing credential that you created on the **Settings** → **Credentials Mgmt** screen. When this template is used to configure a chassis, the selected credentials are configured on the associated devices. Click **Save and Continue**.
7. Optionally, on the **Users** page, configure additional CMC and iDRAC local users, and then click **Save and Continue**.
  - To [add a new Chassis Management Controller \(CMC\) user](#), click **Add User** in the **Chassis Management Controller (CMC) Users** area, and complete the **New User** screen.
  - To [add a new Integrated Dell Remote Access Controller \(iDRAC\) user](#), click **Add User** in the **Integrated Dell Remote Access Controller (iDRAC) Users** area, and complete the **New User** screen.
  - To modify an existing user, click **Edit** next to that user.
  - To remove an existing user, click **Remove** next to that user.
8. Optionally, on the **Monitoring** page, [add monitoring settings](#). Click **Save and Continue**.

 **NOTE:** Monitoring settings are pre-populated with values from the **Settings** → **Environment** screen.
9. On the **NTP** page, [select the time zone and add NTP servers](#) to use for time synchronization. Click **Save and Continue**.


10. On the **Power** page, [configure power budget and redundancy attributes](#). Click **Save and Continue**.
11. On the **Networking** page, [add networking settings](#) for devices based on this template. Click **Save and Continue**.
12. On the **Summary** page, review the information you entered, and click **Finish** to activate the template.

### Adding IP Addresses to Devices

1. On the **Device Access** → **IP Addressing** page of the Create/Edit Management Template wizards, select the method of obtaining IP addresses for the chassis and its respective servers and I/O modules:
  - **Use Existing <Device> IP Address** – Active System Manager does not change the IP address of the device.  
 **NOTE:** This option is valid only for devices that have been previously configured and deployed inside or outside of Active System Manager. Do not choose this option for new devices.
  - **Assign IP address via DHCP** – Use DHCP to automatically allocate an IP address. This option is not valid for chassis.
  - **Assign IP address from this network** – Assign a static IP address from the pool of IP addresses in a management network. To add a network, click **Create New Network** and complete the **Add New Network** screen.
2. Click **Save and Continue**.


### Adding Or Editing A Chassis Management Controller (CMC) User

You can add up to 15 user accounts with permission to access the Chassis Management Controller (CMC). The total number of allowed CMC users is 16; however, that number includes the root account created on the [credentials](#) screen and assigned in the Management Template.


1. On the **New User** screen (from the **Users** page of the Create/Edit Management Template wizards), enter the **User Name** of an account to add to this template.
2. Enter a **Password** that will be required for the user to log into the CMC. Confirm the password.
3. Select the **Role** to assign to the account.  
 **NOTE:** For more information, see the *Dell Chassis Management Controller User Guide*.
4. Select **Enabled** to enable this user account. If deselected, the account is added in a disabled state.
5. Click **Save**.

### Adding Or Editing An Integrated Dell Remote Access Controller (iDRAC) User

You can add up to 15 user accounts with permission to access the Integrated Dell Remote Access Controller (iDRAC). The total number of allowed iDRAC users is 16; however, that number includes the root account created on the [credentials](#) screen and assigned in the Management Template.

1. On the **New User** screen (from the **Users** page of the Create/Edit Management Template wizards), enter the **User Name** of an account to add to this template.
2. Enter a **Password** that will be required for the user to log into the iDRAC. Confirm the password.
3. Select **Enable User** to enable this user account. If deselected, the account is added in a disabled state.
4. Select the iDRAC **Role** to assign to the account.  
 **NOTE:** For more information, see the *Integrated Dell Remote Access Controller (iDRAC) User Guide*.
5. Select the **LAN** role to assign to the account: *Administrator* (full read-write access), *Operator* (limited read-write access), *User*, or *No Access* (no assigned permissions for the iDRAC LAN).
6. Optionally, select **Enable Serial Over LAN** to enable this account to access the server through a serial port.
7. Click **Save**.


## Configuring Monitoring Settings for a Management Template

 **NOTE:** You can change the default monitoring settings that apply to Management Templates on the **Settings** → **Environment** screen.

1. Optionally, on the **Environment** → **Monitoring** page of the Create/Edit Management Template wizards, add an SNMP trap alert destination for chassis:
  - a) Click **Add Trap Setting**.
  - b) Enter a valid **Destination IP Address**. Use the quad-dot IPv4 format (for example, 10.10.10.10) or Fully-Qualified Domain Name (for example, dell.com).


 **NOTE:** By default, the trap destination is set to the Active System Manager virtual appliance IP address.

- c) Enter the **Community String** to which the destination management station belongs.
  - d) Click **Save**.
2. To configure the Chassis Management Controller (CMC) to send email alerts to one or more email addresses:
    - a) Enter the IP address or host name of an **SMTP server** that will receive email alerts.
    - b) Enter the **Source Email Name** from which the email alerts will be sent.
    - c) [Add](#) one or more destination email addresses.

 **NOTE:** You must configure the SMTP e-mail server to accept relayed emails from the CMC IP address. This feature is normally disabled due to security concerns. For instructions on securely enabling this feature, refer to the documentation that came with your SMTP server.

3. To send I/O module log messages to a **Syslog Destination**, enter the IP address of the syslog server.
4. Click **Save and Continue**.

### *Adding a Destination Email for Alerts*

 **NOTE:** You can change the default monitoring settings that apply to Management Templates on the **Settings** → **Environment** screen.

1. On the **Environment** → **Monitoring** page of the Create/Edit Management Template wizards, click **Add Destination Email**.
2. Enter a **Destination Email Address** (the e-mail address that will receive the alerts).
3. Enter the **Name** of the recipient.
4. Click **Save**.

## Adding Time Settings to a Management Template

1. On the **Environment** → **NTP** page of the Create/Edit Management Template wizards, select the **Time Zone** in which the chassis is located.
2. Optionally, to synchronize the chassis clock with an NTP server, select **Enable NTP Server** and enter up to two NTP server names (host names or IP addresses).
3. Click **Save and Continue**.

## Adding Power Settings to a Management Template

1. On the **Power** page of the Create/Edit Management Template wizards, select the power **Redundancy Policy** that applies to chassis configured with this template:
  - *No Redundancy*– The chassis is not configured with power redundancy.

- *AC Redundancy*– All PSUs are active. The PSUs on the left must connect to one AC power grid, while the PSUs on the right connect to another AC power grid. If one AC grid fails, the PSUs on the functioning AC grid take over without interrupting the servers or infrastructure.



**CAUTION:** To avoid a system failure and for AC Redundancy to work effectively, there must be a balanced set of PSUs properly cabled to separate AC grids.

- *Power Supply Redundancy*– A PSU in the chassis is kept as a spare, ensuring that the failure of any one PSU does not cause the servers or chassis to power down.




**NOTE:** For more information on chassis power redundancy policies, see the *Dell Chassis Management Controller User Guide*.


2. Optionally, select **Server Performance Over Power Redundancy** to favor server performance and power up over maintaining power redundancy.
3. Optionally, select **Enable Dynamic Power Supply Engagement** to allow the chassis controller to put under-utilized PSUs into standby mode based on the redundancy policy and system power requirements.
4. Click **Save and Continue**.


## Adding Networking Settings to a Management Template


On the **Networking** page of the Create/Edit Management Template wizards:

1. Optionally, select **Register Chassis Controller on DNS** to enable users to access the Chassis Management Controller (CMC) with a user-friendly name, instead of an IP address. When the Management Template is applied to the chassis in the [Configure Chassis](#) wizard, Active System Manager will register one of the following names on the domain name server (DNS):
  - If a **DNS Name** is entered on the **Device Identification** → **Chassis** screen, then Active System Manager will register this as the name.
  - If a DNS Name is not specified, then Active System Manager will register the default name. The default CMC name is *CMC-service\_tag*, where *service\_tag* is the service tag of the chassis.
2. Optionally, select **Register iDRAC on DNS** to enable users to access the Integrated Dell Remote Access Controller (iDRAC) with a user-friendly name, instead of an IP address. When the Management Template is applied to servers in the [Configure Chassis](#) wizard, Active System Manager will register one of the following names on the domain name server (DNS):
  - If an **iDRAC DNS Name** is entered on the **Device Identification** → **Servers** screen, then Active System Manager will register this as the name.
  - If an iDRAC DNS Name is not specified, then Active System Manager will register the default name. The default name is *idrac-service\_tag*, where *service\_tag* is the service tag of the server.
3. Optionally, select **Enable Chassis Controller VLAN ID**, and enter a **Chassis Controller VLAN ID**. Enabling this option configures the CMC to require all incoming traffic to be tagged with the indicated VLAN ID. This requires a specific [IP configuration](#).
 

 **NOTE:** Valid VLAN IDs are between 1 to 4000 and 4021 to 4094. The default VLAN ID is 1.

 **CAUTION:** Before enabling the chassis controller or iDRAC VLAN IDs, make sure you [understand](#) the steps you must take in your environment to prevent a loss of network connectivity to the chassis or server.
4. Optionally, select **Enable iDRAC VLAN ID** to enable VLANs on the iDRAC, and enter an **iDRAC VLAN ID**.
 


 **NOTE:** Valid VLAN IDs are between 1 to 4000 and 4021 to 4094. The default VLAN ID is 1.

 **CAUTION:** Before enabling the chassis controller or iDRAC VLAN IDs, make sure you [understand](#) the steps you must take in your environment to prevent a loss of network connectivity to the chassis or server.
5. Optionally, select **Enable Telnet** to allow telnet access to the CMC.

6. Optionally, select **Enable SSH** to allow remote SSH access to the CMC.
7. Click **Save and Continue**.


### Enabling the VLAN ID

Chassis Management Controllers (CMCs) and Integrated Dell Remote Access Controllers (iDRACs) both support VLAN tagging; however, they share a port with the I/O aggregator switch, which does not support VLAN tagging. For this reason, before enabling VLAN tagging for the CMC and iDRAC, you must take certain steps to make sure that all traffic (tagged and untagged) passes through the network and the out-of-band switch port to the CMC without being dropped.

 **CAUTION:** To avoid losing device connectivity, it is critical to use extreme caution when enabling VLAN tagging. If tagging is not enabled correctly on the switch port, then traffic from the CMC and iDRAC is likely to be lost. Additionally, because the I/O aggregator does not support VLAN tagging, you must also configure the switch port to allow untagged traffic. To ensure Active System Manager can communicate between all tagged and untagged devices, your external network must route between these tagged and untagged VLANs.

To prevent dropped traffic, configure your network as follows:

- Use VLANs to carry both tagged and untagged traffic.
- Configure routing for the affected subnets and VLANs.
- Configure IP addresses so that, when a CMC or iDRAC moves to a private VLAN, its IP address also moves to a different subnet than untagged traffic.

 **NOTE:** Failing to move the IP address will cause the router to assume the CMC or iDRAC is on the same network as untagged packets. Routing will not work, and packets won't forward correctly between subnets and VLANs. This can cause communication loss with some or all devices.

The following table shows a sample IP configuration that prompts the router to forward packets after the VLAN is configured. Notice that the initial IP addresses of the CMC, iDRAC, I/O aggregator, and Active System Manager virtual appliance are all on the same subnet, and (because VLANs are not used) all traffic is untagged. The final IP addresses of the CMC and iDRAC do use VLAN tagging, and are on a different subnet than untagged traffic.


**Table 2. IP Configuration For Forwarding Packets**

	Initial IP Address / Subnet Mask / VLAN	Final IP Address / Subnet Mask / VLAN
CMC	172.6.53.4 / 255.255.0.0 / None	172.5.53.4 / 255.255.0.0 / 5
I/O Module	172.6.53.4 / 255.255.0.0 / None	172.6.53.4 / 255.255.0.0 / None
Active System Manager	172.6.53.4 / 255.255.0.0 / None	172.6.53.4 / 255.255.0.0 / None
iDRAC	172.6.53.4 / 255.255.0.0 / None	172.7.53.4 / 255.255.0.0 / 7

## Copying a Template

Copying a template creates an exact duplicate of an existing template.

1. Under **Templates** in the left pane, click **Deployment Templates** or **Management Templates**.
2. Select the template to duplicate.
3. For a Management Template, click **Copy**. For a Deployment Template, select **Copy** in the **Other Tasks** drop-down list.
4. Enter a unique **Name** and **Description** to help identify this template for future use.


 **NOTE:** Valid characters for the template name include uppercase and lowercase letters, numbers, and spaces. The following special characters are also allowed: \_-()

5. Click **Create Copy**.




6. Click **OK**.

## Editing a Management Template

 **NOTE:** Changes will not automatically apply to devices currently using this template. To apply changes, [check device compliance](#), and then reapply the template.

1. Click **Templates** → **Management Templates** in the left pane.
2. Select a template, and click **Edit**.
3. In the Management Template wizard, click the page to edit, and modify the appropriate information.
4. Click **Save**.
5. Close the wizard, or select another page to continue making changes.

## Deleting a Management Template

 **NOTE:** You cannot delete a Management Template that is associated with a managed device or used in a Deployment Template.

1. Click **Templates** → **Management Templates** in the left pane.
2. Select one or more templates, and click **Delete**.
3. Click **Yes**.

## Deployment Templates

A Deployment Template defines the basic configuration of a deployed physical server, including number of CPUs, memory, BIOS settings, RAID settings, boot mode and sequence, networks, and operating system (OS) boot type.

Creating a Deployment Template saves time by enabling you to specify configuration settings once within the template. Then, you can apply that template to multiple servers from the [Deploy](#) wizard.

The **Templates** → **Deployment Templates** screen displays the basic details of all existing Deployment Templates, including:

- Name
- Description
- Last Updated By
- [State](#)

From this screen, you can:

- [Edit](#) a Deployment Template
- [Deploy](#) a server by applying a Deployment Template
- [Create](#) a Deployment Template
- [Create](#) a Deployment Template from a reference server
- [Copy](#) a Deployment Template
- [Enable](#) a Deployment Template
- [Disable](#) a Deployment Template
- [Delete](#) a Deployment Template

Additionally, you can select a Deployment Template to see more details, including:

- Summary – Template, server, boot, and network information
- Deployments – A list of deployments instantiated from this template



**NOTE:** You can modify how the screen displays by clicking a column name to sort displayed items by that column. You can also [refresh](#) the information on the screen.

## Creating a Deployment Template

Before you begin, it is recommended to gather the following information:

- Recommended number of CPUs and amount of memory for servers based on this template (exact number or minimum)
- Desired BIOS and RAID settings
- Boot mode and sequence
- Virtual NIC configuration(s) for servers deployed with this template
- Operating system boot type

1. Click **Templates** → **Deployment Templates** in the left pane.
2. Click **Create**.
3. On the **Welcome** page of the Create Deployment Template wizard, click **Next**.
4. On the **Template Information** page, enter a unique **Name** and **Description** to help identify this template for future use. Click **Save and Continue**.




**NOTE:** It is recommended to choose a name that reflects the template's purpose—for example, *WebServer\_Datacenter1*. Valid characters include uppercase and lowercase letters, numbers, and spaces. The following special characters are also allowed: `._-()`

5. On the **Server Information** page, enter the **Number of CPUs** and amount of **Memory GB** (*Exactly or At Least*) recommended to ensure good performance for servers based on this template. When the template is deployed, Active System Manager will recommend servers that meet these specifications.
6. On the **BIOS** page, [configure the BIOS settings](#) that will be applied to servers based on this template. Alternately, to exclude BIOS information from this template, deselect **Include BIOS configuration in this template**. Click **Save and Continue**.
7. On the **RAID** page, [select the RAID level](#) that will be applied to servers based on this template. Alternately, to exclude RAID configuration from this template, deselect **Include RAID configuration in this template**. Click **Save and Continue**.
8. On the **Networks** page, [configure the virtual NICs](#) available to servers deployed with this template. Click **Save and Continue**.
9. On the **Boot Information** page, [select the operating system \(OS\)](#) boot type that servers based on this template will use at startup. Click **Save and Continue**.
10. On the **Boot Sequence** page, [configure the boot sequence](#) that will be applied to servers based on this template. Alternately, to exclude RAID boot sequence from this template, deselect **Include boot sequence configuration in this template**. Click **Save and Continue**.
11. On the **Summary** page, if the summary information is correct, and click **Finish** to activate the template.

### Adding BIOS Information to a Deployment Template

To exclude BIOS information from this template, deselect **Include BIOS configuration in this template**. Alternately, to configure BIOS settings that will be applied to servers based on this template:

1. On the **BIOS** page of the Create/Edit Deployment Template wizards, select a [System Profile](#) to apply for power management.
2. Optionally, select **Processor Virtualization Technology** to permit virtualization software to use Virtualization Technology functions incorporated in the processor design. This feature can only be used by software that supports Virtualization Technology; for example, you can enable this feature for ESXi servers.
3. Optionally, select **Logical Processor** to monitor both logical processors on servers that support Simultaneous Multi-Threading (SMT) technology. If disabled, only the first logical processor of each processor installed in the system is used by the operating system.
4. Optionally, select **Memory Node Interleaving** to enable memory interleaving on servers with a symmetric memory configuration. If disabled, the system supports Non-Uniform Memory Architecture (NUMA) (asymmetric) memory configurations. Enabling this setting can decrease performance.
5. Select the configuration for **User Accessible USB Ports** to turn on or off all of the user accessible USB ports.
6. Optionally, select **Integrated RAID Controller**, if supported by the server configuration. Selecting this option also selects the **Include RAID configuration in this template** option on the [RAID](#) page.
7. Optionally, select **Execute Disable** to enable Data Execution Prevention (DEP) memory protection technology. DEP is a set of hardware and software technologies that perform additional checks on memory to help protect against malicious code exploits.
8. Optionally, select **Single Root I/O Virtualization** to enable BIOS configuration of Single Root I/O Virtualization (SR-IOV) devices. SR-IOV enables a single PCI Express (PCIe) based I/O device to provide up to 64 virtual functions per 10-Gigabit Ethernet (10GbE) port.
9. Select the **Number of Cores Per Processor**. If set to *All*, the maximum number of cores in each processor is enabled.
10. Click **Save and Continue**.

 **NOTE:** For more information on these options, see the *Dell PowerEdge Systems Hardware Owner's Manual*.

### ***Choosing a System Profile for Power Management***

The system profile sets the power management configuration for a server. Profile options include:

- **Active Power Controller** – Enables Demand-Based Power Management (DBPM) to optimize for performance per watt. All processor performance information is passed from the system BIOS to the operating system for control. The operating system sets processor performance based on processor utilization. Memory frequency is set to *Maximum Performance*, and the fan is set to *Minimum Power*.
- **Max Performance** – Disables DBPM. The BIOS sets the processor P-state to the highest supported level.
- **OS Control** – Enables DBPM. All supported processor P-states are available to the operating system in the ACPI table.
- **Dense Configuration Optimized** – Optimizes power settings for reliability in systems with a large number of DIMMs. CPU power management is set to Dell Advanced Power Control (DAPC), memory frequency is reduced to the minimum level, turbo boost is disabled, the patrol scrub rate is extended, and memory operating voltage is set to 1.5V to increase memory margins.

 **NOTE:** For more information, see the *Dell PowerEdge Systems Hardware Owner's Manual*.

### **Adding RAID Information to a Deployment Template**

To leave RAID configuration unchanged on the server, deselect **Include RAID configuration in this template**. If you select this option, the **Integrated RAID Controller** on the [BIOS](#) page is also selected.

To specify the RAID configuration that will be applied to servers based on this template:

1. On the **RAID** page of the Create/Edit Deployment Template wizards, select **Basic RAID Configuration**, and then select a RAID level.

When this Deployment Template is selected in the [Deploy](#) wizard, only servers with the following hardware configurations will display on the **Server Selection** page.

- RAID 0 – Servers with at least one disk
- RAID 1 – Servers with at least two disks
- RAID 5 – Servers with at least three disks

In RAID modes 1 and 5, Active System Manager creates a hot spare if an additional disk is available. You will receive a message after creating a deployment based on this Deployment Template to indicate whether or not a hot spare was created.

- RAID 1 – Attempts to create one hot spare if more than two disks are available to the server
- RAID 5 – Attempts to create one hot spare if more than three disks are available to the server

For example, for a Dell PowerEdge M820 with four disks installed, if the Deployment Template specified RAID 5, three disks would be used to create RAID 5 and one would be configured as a hot spare.

Alternately, select **Clone RAID Configuration** to use an existing configuration imported from a controller.

2. Click **Save and Continue**.

### **Adding Networks to a Deployment Template**


On the **Networks** page of the **Deployment Template** wizard, you can create, edit, and delete the virtual NICs available to servers deployed with this template. A virtual NIC configures the adapter port or port partition on a network adapter. If more than one virtual NIC configuration exists, you can change the sequence with which they are assigned by clicking the up and down arrows. The virtual NIC settings are used to filter the available servers that display when applying the template.

1. Select [Enable Bandwidth Over-subscription](#) to allow you to set a higher maximum bandwidth for each of the virtual NICs on a server, so that their total exceeds 100% of the network bandwidth available to the NIC port to which the virtual NIC is assigned.
2. Select the [Virtual NIC Mapping Order](#) (*Physical Partition* or *PCI Function*).
3. If more than one virtual NIC configuration exists, you can change the sequence with which they are assigned by clicking the up and down arrows.
4. Click **New** to [create one or more new virtual NIC configurations](#). Click **Edit** to change an existing configuration, or **Remove** to delete the configuration from the template.
5. Click **Save and Continue**.

### **Enabling Bandwidth Oversubscription**

Enable bandwidth oversubscription allows you to set a higher Max Bandwidth for each of the virtual NICs on a server, so that their total exceeds 100% of the network bandwidth available to the NIC port to which the virtual NIC is assigned.

This enables the various virtual NICs to use as much bandwidth as possible, as their individual traffic flows change. For example, if bandwidth oversubscription is enabled on a server with four virtual NICs and a total available bandwidth of 10 GB, then you can assign a Max Bandwidth as high as 10 GB for each virtual NIC. In this case, if traffic flow is high on one virtual NIC and low on another, then the virtual NIC with high traffic flow will consume the excess bandwidth of the low-traffic virtual NIC. However, if bandwidth oversubscription is disabled, then the total bandwidth of the virtual NICs assigned to a 10GB port is less than or equal to 10GB.

 **NOTE:** In most environments, it is recommended to enable bandwidth oversubscription.

### **Adding or Editing a Virtual NIC Configuration**

Adding a virtual NIC configuration to a Deployment Template enables [NIC partitioning](#) on servers to which the template is applied. The virtual NIC configuration includes settings such as Network Type, Native VLAN, Maximum Bandwidth,

Minimum Bandwidth, and Redundancy that Active System Manager uses to filter the available servers that display when [creating a new deployment](#).

To access the virtual NIC configuration screen, click **Create** or **Edit** on the **Templates** → **Deployment Templates** screen. Then, click **New** or **Edit** on the **Networks** page of the wizard.



**NOTE:** The virtual MAC identity that Active System Manager assigns to the NIC depends on the **Network Type** selected when [adding](#) a network. For a LAN network type, a virtual MAC address is assigned to the server. For an iSCSI network type, a virtual iSCSI MAC address is assigned to the server. For an FCoE network type, a virtual FIP MAC address is assigned to the server.

1. Enter a **Name** for the virtual NIC configuration.
2. Select a **Connection Type** of *LAN*, *SAN (iSCSI)*, or *SAN (FCoE)* to display existing networks of that type.
3. Select the **Native VLAN** on which all untagged traffic will be placed. This option is required for FCoE and boot-to-network configurations (for example, boot to SAN or PXE).
4. Enter the **Maximum Bandwidth** in GB (maximum of 10 GB). This is the maximum bandwidth the virtual NIC can consume at any time, even if [bandwidth oversubscription](#) is enabled.
5. Enter the **Minimum Bandwidth** in GB (maximum of 10 GB). This is the minimum bandwidth the virtual NIC will be guaranteed. If needed, the virtual NIC will consume up to the maximum bandwidth but not over.
6. Optionally, select **Redundancy** to configure a secondary virtual NIC on the server that provides a redundant network path through the fabric.
7. Select a [Virtual Identity Pool](#).
8. Select the network(s) to associate with this configuration. You can select one or more networks for a LAN connection type, but only one network for SAN (iSCSI) or SAN (FCoE) connection types.
9. Click **Save**.

#### *NIC Partitioning*

Dell PowerEdge blade servers offer the ability to divide each 10GbE adapter port into as many as four logical NIC partitions. Each partition functions as an independent NIC port, appearing to system memory and the operating system as a distinct physical NIC with its own driver software.

NIC partitioning (NPAR) improves network efficiency by isolating and dividing networking and storage resources, so that a single port provides bandwidth for multiple concurrent workloads. For example, in a PowerEdge M620 server, you can quadruple the total logical NIC count from six (three NICs with two ports each) to twenty-four (three NICs/two ports/four partitions per port). Additionally, NPAR provides the ability to [enable bandwidth oversubscription](#) to dynamically allocate resources based on current workload needs.

For more information, see the white paper *Enhancing Scalability Through Network Interface Card Partitioning*.

#### *Virtual NIC Mapping Order*

The Virtual NIC Mapping Order determines how virtual NICs are mapped to the partitions on each port of an adapter:


- **Physical Partition** – Consecutively assigns virtual NICs to partitions (for example, Port1/Partition0, then Port1/Partition1, and so on).
- **PCI Function** – Assigns virtual NICs by PCI function order—for example, on a two-port network daughter card (NDC), the PCI function number for port 1 is 0/2/4/6, and the PCI function number for port 2 is 1/3/5/7.


Different operating systems have different mapping order requirements—for example, RHEL 6.2 and ESX 5.0 both use PCI function to enumerate partitions. For more information, see the “Mapping Order” section of the *Active System Manager Network Configuration for Deployment Templates* white paper.


### **Adding Boot Information to a Deployment Template**


The information entered on this page is used to filter the servers that will be displayed on the **Server Selection** page of the **Deploy** wizard. Only servers that match the criteria can host deployments created with this Deployment Template.

1. On the **Boot Information** page of the Create/Edit Deployment Template wizards, select an **OS Boot Type** of Local HD (hard drive), SD Card, PXE (permanent), PXE (one time), iDRAC image boot (one time), SAN (iSCSI), or SAN (FCoE).
2. Depending on the OS boot type, enter additional information:
  - If PXE (permanent) or PXE (one time), select a **Virtual Boot NIC** of network type LAN.
 

 **NOTE:** This list is populated with virtual NICs [added](#) on the **Networking** → **Networks** screen. The virtual NIC must have a native VLAN selected.
  - If iDRAC image boot, select a **Network Share Type** (NFS or CIFS), and enter the **Network Share File Path** where the ISO is located in the format **host\share\<ISO\_filename>** for NFS or **//host/share/<ISO\_filename>** for CIFS. Also, enter the **User Name** and **Password** required to access the share.
 

 **NOTE:** iDRAC image boot is a one-time boot for a set number of hours, after which the ISO is unmounted and the server returns to the boot sequence configured in the operating system.
  - If SAN (iSCSI):
    1. Select a **Virtual Boot NIC** of SAN (iSCSI).
 

 **NOTE:** This list is populated with networks [added](#) on the **Networking** → **Networks** screen.
    2. Select an **Initiator IP Address** (*Static* or *DHCP*).
    3. Select an existing **Storage Device** or click **New** to [add](#) a new storage device.
  - If SAN (FCoE), select a **Virtual Boot NIC** of SAN (FCoE).
 

 **NOTE:** This list is populated with networks [added](#) on the **Networking** → **Networks** screen.
3. Click **Save and Continue**.

### ***Adding a Storage Device***

Adding a storage device is available only for SAN (iSCSI) virtual NIC configuration with a native iSCSI VLAN.

1. On the **Add Storage Device** screen (from the **Boot Information** page of the Create/Edit Deployment Template wizards), enter a **Name** used to identify the device.
2. Enter the **Storage IP Address** associated with the device.
3. Optionally, enter a **Port Number** between 1 - 65535. Default is 3260.
4. Optionally, select **Enable Authentication** to enable CHAP (Challenge and Handshake Authentication Protocol). Then, select existing **Credentials** or click **New** to add new credentials.
5. Click **Save**.


### ***Editing or Removing a Storage Device***

1. On the **Templates** → **Deployment Templates** screen, select the Deployment Template on which the storage device is configured.
2. Click **Edit**.
3. On the **Boot Information** screen, click **Edit** or **Remove**.

### **Adding Server Boot Sequence to a Deployment Template**

To leave boot sequence unchanged on the server, deselect **Include boot sequence configurations in this update**. Alternately, to configure the boot order for this server:

1. On the **Boot Sequence** page of the Create or Edit Deployment Template wizard, select a **Boot Mode** (BIOS or UEFI).
 

 **NOTE:** Boot to iSCSI and FCoE are not supported in UEFI mode.
2. Optionally, select **Enable Boot Sequence Retry** to automatically retry if the boot sequence fails.
3. Optionally, reorder the boot devices by clicking on the up or down arrows and select whether they are enabled or disabled.

4. Click **Save and Continue**.

## Creating a Deployment Template from a Reference Server

You can create a Deployment Template based on a server in your network, even if the server is not managed by Active System Manager. All deployments created using this Deployment Template will have the same BIOS, RAID, and boot order configuration as the reference server.

Before you begin, it is recommended to gather the following information:

- The IP address of the reference server
- Credentials for the reference server

1. Click **Templates** → **Deployment Templates** in the left pane.
2. Click **Create From Reference Server**.
3. On the **Welcome** page of the Create From Reference Server wizard, click **Next**.
4. On the **Template Information** page, enter a unique **Name** and **Description** to help identify this template for future use. Click **Next**.



**NOTE:** It is recommended to choose a name that reflects the template's purpose—for example, *WebServer\_Datacenter1*. Valid characters include uppercase and lowercase letters, numbers, and spaces. The following special characters are also allowed: . \_ - ( )

5. On the **Server Selection** page, enter the **IP Address** of the reference server and select the **Credential**. You can select existing credentials that were created on the **Settings** → **Credentials Mgmt** screen, or click **New** to configure new credentials. Click **Next**.
6. On the **Summary** page, if the summary information is correct and the connection is successful, and click **Finish** to activate the template.

## Copying a Template

Copying a template creates an exact duplicate of an existing template.

1. Under **Templates** in the left pane, click **Deployment Templates** or **Management Templates**.
2. Select the template to duplicate.
3. For a Management Template, click **Copy**. For a Deployment Template, select **Copy** in the **Other Tasks** drop-down list.
4. Enter a unique **Name** and **Description** to help identify this template for future use.



**NOTE:** Valid characters for the template name include uppercase and lowercase letters, numbers, and spaces. The following special characters are also allowed: . \_ - ( )

5. Click **Create Copy**.
6. Click **OK**.

## Editing a Deployment Template

If a Deployment Template is currently in use, then certain attributes—for example, connection type, virtual identity pool, redundancy, and OS boot type—cannot be edited.

1. Click **Templates** → **Deployment Templates** in the left pane.
2. Select the template, and click **Edit**.

3. Click the page to edit, and modify the appropriate information.
4. Click **Save**.
5. Close the wizard, or select another page and continue making changes.



**NOTE:** Editing a Deployment Template applies changes to future deployments; however, changes are *not* applied to active deployments that use the template.

## Enabling a Deployment Template

1. Click **Templates** → **Deployment Templates** in the left pane.
2. Select one or more disabled templates to enable.
3. In the **Other Tasks** drop-down menu, select **Enable**.
4. Click **Yes** to enable the Deployment Template(s).

The template state changes to *Ready*. You can apply a ready Deployment Template to a server in the [Deploy wizard](#).

## Disabling a Deployment Template

1. Click **Templates** → **Deployment Templates** in the left pane.
2. Select one or more enabled templates to disable.
3. In the **Other Tasks** drop-down menu, select **Disable**.
4. Click **Yes** to disable the Deployment Template(s).

The template state changes to *Disabled*. You can only disable a template that is in a *Ready* state.

## Deleting a Deployment Template

1. Click **Templates** → **Deployment Templates** in the left pane.
2. Select a template, and select **Delete** from the **Other Tasks** drop-down list.
3. Click **Yes** to delete the template.



**NOTE:** You cannot delete a Deployment Template that is associated with an active deployment.



# Deployments

In Active System Manager, a deployment is a single instantiation of a [Deployment Template](#) that you can apply to a server to prepare it for operating system installation.

Every deployment instance is distinct from the servers to which it is applied. You can freely attach the deployment to a server, detach it from a server, and migrate it between servers.

After a deployment instance is created, any future changes made to the template do not affect the instance. To determine whether the template that is applied to a device matches the current version, check the template compliance.

Active System Manager provides several ways to deploy a server with a deployment instance:

- [Deploy](#) a server while creating a deployment instance
- [Migrate](#) a deployment instance from one managed server to another managed server
- [Attach](#) a detached or delayed deployment to a managed server

The **Deployments** screen displays information about deployment instances, including:

- Name
- Template Name
- Server IP Address
- [State](#)
- Instantiated By

From this screen, you can:

- [Migrate](#) a deployment instance
- [Power On](#) a deployed server
- [Power Off](#) a deployed server
- [Deploy](#) a server
- [Attach](#) a deployment instance to a server
- [Detach](#) a deployment instance from a server
- [Delete](#) a deployment instance

Additionally, you can click a deployment instance to see its details, including:

- Summary
- [Network Identity](#)



**NOTE:** You can modify how the screen displays by clicking a column name to sort displayed items by that column. You can also [refresh](#) the information on the screen.

# Creating a Deployment

The Deploy wizard enables you to create one or more deployment instances based on a Deployment Template, and either immediately apply the instances to servers or defer the instances to attach them at a later time.

Before you begin, it is recommended to do the following:


- Determine what type of server configuration should host the deployment
- If booting from iSCSI or FCoE, know the storage target identity (iSCSI Qualified Name or WWPN) and boot LUN for the deployment
- If the number of CPUs, amount of memory, or RAID configuration has changed since the server was discovered, then [manually run an inventory job](#)

1. Do one of the following:

- Click **Deployments**, and then select **Deploy** from the **Other Tasks** drop-down list.
- Click **Templates** → **Deployment Templates** in the left pane. Then, select a [Deployment Template](#), and click **Deploy**.

2. On the **Welcome** page of the Deploy wizard, click **Next**.


3. On the **Deployment Information** page, select a **Deployment Template** (if not already selected), and enter a unique **Deployment Name** and **Deployment Description** to help identify this deployment for future use. Click **Next**.

 **NOTE:** It is recommended to choose a name that reflects the deployment's purpose—for example, *WebServer\_Datacenter1*. Valid characters include uppercase and lowercase letters, numbers, and spaces. The following special characters are also allowed: . \_ -()

4. On the **Server Selection** page, select the servers to which the selected Deployment Template will be applied:


- **Manual Server Selection** — Select one or more servers that match your deployment requirements. This list is filtered by the server information, RAID configuration, networks, and boot information specified in the Deployment Template.
- **Deferred Placement** — Creates a deployment that is not attached to a specific physical server (can be [attached](#) to a server at a later time). Enter the **Number of deployments to create**.

Click **Next**.

 **NOTE:** This page displays only the servers that match the criteria specified on the [Boot Information](#) page of the selected Deployment Template.

5. On the **Deployment Settings** page, if the deployment will boot from iSCSI or FCoE, enter the **Target Identity** in the format of an iSCSI Qualified Name (IQN) or World Wide Port Name (WWPN) and the **Boot LUN**. Target identity and boot LUN values are available from your Storage Administrator. Click **Next**.

6. On the **Summary** page, review the information you entered, and then click **Finish** to deploy the server.

 **NOTE:** Configuring a server by applying a Deployment Template affects physical infrastructure, which may cause chassis fans to power on or increase in speed. This is standard behavior, to help ensure that hardware remains at the appropriate temperature.

After the server is deployed and in an *In Use* state, it is ready to host applications.

## Migrating a Deployment

Migrating a deployment [detaches](#) the deployment instance from one server, and [attaches](#) it to another server in one step. You can migrate a deployment between the servers in different chassis, between servers with network interface

cards (NICs) from different vendors, and even between servers with different configurations of memory and processors, as long as the servers meet the deployment criteria.

Deployment information (including the target identity, boot LUN, initiator IP address, and [virtual identity](#)) migrates to the new server; however, the server IP address does not migrate. After migration completes, the server from which the deployment migrated returns to the pool of available servers.

1. Click **Deployments** in the left pane.
2. Select a deployment that is currently attached to a server, and then click **Migrate**.
3. On the **Migrate Deployment** screen, select the server to which the deployment will be migrated. Only servers that fit your deployment requirements display in this list.
4. Click **Submit**.

The deployment state changes to *Pending Detach* first, and later transitions to *Pending Deploy*. When the migrate deployment job completes, the state of the deployment that was migrated changes to *Activated*. The state of the server that was migrated from changes to *Ready*, and the server is powered off.

## Attaching a Deployment

You can deploy a server by attaching a delayed or detached deployment instance:

- Delayed Deployment – Not associated with a specific server at the time the deployment is [created](#).
- Detached Deployment – After a server is deployed, you can [detach](#) its deployment instance, and attach it to a different server.

1. Click **Deployments** in the left pane.
2. Select a detached or delayed deployment, and click **Attach** in the **Other Actions** drop-down list.
3. On the **Attach Deployment** screen, select the server to which the deployment will be attached. Only servers that fit your deployment requirements display in this list.
4. Click **Submit**.



**NOTE:** Configuring a server by applying a Deployment Template affects physical infrastructure, which may cause chassis fans to power on or increase in speed. This is standard behavior, to help ensure that hardware remains at the appropriate temperature.

The deployment state changes to *Pending Attach*. When the attach deployment job completes, the deployment state changes to *Activated*. The state of the selected server becomes *In Use*.

## Detaching a Deployment

Detaching a deployment removes identity information from a server (including the including the target identity, boot LUN, initiator IP address, and [virtual identity](#)), but does not return it to the global virtual identity pool. Instead, the deployment instance becomes available to [attach](#) to a different server. The server from which the deployment was detached returns to the pool of available servers.

1. Click **Deployments** in the left pane.
2. Select an activated or deactivated deployment, and select **Detach** in the **Other Actions** drop-down list.
3. Click **Yes**, and then click **OK**.

The deployment state changes to *Pending Detach*. When the detach deployment job completes, the server state changes to *Ready*.

## Deleting a Deployment

If a deployment is no longer needed, then you can delete it to release any resources being consumed by the deployment.

1. Click **Deployments** in the left pane.
2. Select one or more deployments to delete.
3. In the **Other Tasks** drop-down list, click **Delete**.
4. Click **Yes** to delete the deployment(s).

The deployment state changes to *Pending Remove*. Identity information associated with the deployment returns to the global [virtual identity pool](#), and is available for reuse. If the deployment is currently attached to a server, then the server returns to the pool of available servers.

# Networking

Active System Manager manages LAN (private/public/hypervisor management), SAN (iSCSI/FCoE), and out-of-band management networks.

To facilitate network communication, you can [add](#) ranges of static IP addresses that Active System Manager will assign to devices for out-of-band management and iSCSI initiators. You can also create pools of MAC, iSCSI, and FCoE [virtual identities](#) that Active System Manager will assign to [virtual NICs](#). Adding a virtual NIC configuration to a Deployment Template enables [NIC partitioning](#) on servers to which the template is applied.

On the **Networking** screen, you can see graphs of:

- [Networks](#) – The two networks with the fewest static IP addresses currently available for devices
- [Virtual Identities](#) – Total numbers of MAC, iSCSI, and FCoE virtual identities that are currently available and in use

## Networks

The **Networking** → **Networks** screen displays information about networks configured in Active System Manager, including:

- Name
- Description
- [VLAN ID](#)
- [Network Type](#)

From this screen, you can:

- [Edit](#) an existing network
- [Add](#) a network
- [Delete](#) a network

Additionally, you can click a network to see its details, including:


- Summary
- Templates configured to use the network



**NOTE:** You can modify how the screen displays by clicking a column name to sort displayed items by that column. You can also [refresh](#) the information on the screen.

## Network Types


Active System Manager manages these network types:

- **Private LAN** – Used to access network resources for functions such as vMotion traffic or heartbeat communication. If associated with a virtual NIC, the VLAN ID is used to configure the I/O module's server-facing ports. DHCP only.
- **Public LAN** – Used to access network resources for basic networking activities. If associated with a virtual NIC, the VLAN ID is used to configure the I/O module's server-facing ports. DHCP only.  
 **NOTE:** Private and public LANs are functionally identical in Active System Manager. The purpose of offering both labels is to help users categorize LANs based on functional use.
- **SAN (iSCSI)** – Used to manage storage-related traffic on an iSCSI network. If associated with a virtual NIC, the VLAN ID is used to configure the I/O module's server-facing ports. If an IP address pool is associated with the network, then Active System Manager can use it to configure the iSCSI initiator IP address when doing a SAN (iSCSI) boot. Static or DHCP.
- **SAN (FCoE)** – Used to identify storage-related traffic on a Fibre Channel Over Ethernet (FCoE) network. If associated with a virtual NIC, the VLAN ID is used to configure the I/O module's server-facing ports. DHCP only.
- **Management Network** – Used for out-of-band management of hardware infrastructure. After discovery, you can configure hardware by applying Management Templates. DHCP is allowed for servers and I/O modules, but not for chassis. Static addressing is allowed for all hardware types. IP addresses are assigned in the Configure Chassis wizard.
- **Hypervisor Management** – Used to identify the management network for a hypervisor or operating system deployed on a server. The VLAN ID is used to configure the I/O module's server-facing ports. DHCP only.


## Adding or Editing a Network


Adding the details of an existing network enables Active System Manager to automatically configure chassis, servers, and I/O modules that are connected to the network.

1. Click **Networking** → **Networks** in the left pane, and then click **Add** or **Edit**.
2. Enter a unique **Name** for the network.
3. Optionally, enter a **Description** for the network.
4. Select a [Network Type](#).


 **NOTE:** The virtual MAC identity that Active System Manager assigns to the NIC depends on the **Network Type** selected when [adding](#) a network. For a LAN network type, a virtual MAC address is assigned to the server. For an iSCSI network type, a virtual iSCSI MAC address is assigned to the server. For an FCoE network type, a virtual FIP MAC address is assigned to the server.

5. Enter a [VLAN ID](#) between 1 and 4094.


 **NOTE:** Management networks do not require a VLAN ID, because management networks are not configured on I/O modules. Active System Manager uses the VLAN ID specifically to configure I/O modules to enable network traffic to flow from the server to configured networks during deployment.


 **NOTE:** The VLAN ID can be edited only if the network is not currently referenced by a Management Template or Deployment Template.

6. For a SAN (iSCSI) or Management Network, select **Configure static IP address pools** and do the following:

 **NOTE:** This step is optional for SAN (iSCSI) networks, and required for Management Networks. After a network is created, you cannot select or deselect the option to configure static IP address pools.

- a) Enter the default **Gateway** IP address for routing network traffic (optional for SAN (iSCSI); required for a Management Network).
- b) Enter the **Subnet Mask**.
- c) Optionally, enter the IP addresses of the **Primary DNS** (required) and **Secondary DNS** (optional).
- d) Optionally, enter the **DNS Suffix** to append for host name resolution.
- e) Click **Add IP Range**, enter a **Starting IP Address** and **Ending IP Address**, and then click **Save IP Range**. Repeat until all ranges are added.

 **NOTE:** IP address ranges cannot overlap. For example, you cannot create an IP address range of 10.10.10.1–10.10.10.100 and another range of 10.10.10.50–10.10.10.150.

 **NOTE:** The network type can be edited only if the network is not currently referenced by a Management Template or Deployment Template.


7. Click **Save Network**.

## VLAN ID

A VLAN ID is a unique identifier that enables switching and routing of network traffic. Active System Manager uses the VLAN ID specifically to configure I/O modules to enable network traffic to flow from the server to configured networks during deployment.


The VLAN ID must be a number between 1 and 4094. If using a flat network (no VLANs), enter a value of 1.

## Deleting a Network

 **NOTE:** You cannot delete a network that is referenced in a Management Template or a Deployment Template.

1. Click **Networking** → **Networks** in the left pane.
2. Click the network, and then click **Delete**.
3. Click **Yes** to delete the network.

## Editing an IP Address Range

 **NOTE:** You cannot extend an IP address range after it is created. Instead, you must add an additional range. For example, to extend the IP address range 10.10.10.1–10.10.10.50 by ten IP addresses, add an additional range of 10.10.10.51–10.10.10.60. Alternatively, if the IP address range is unused, you can [delete](#) it and add a new range with the desired values.

1. Click **Networking** → **Networks** in the left pane.
2. Click an existing network for a SAN (iSCSI) or management network.
3. Click **Edit**.
4. Click **Edit** next to the IP address range.
5. Make your desired changes.
6. Click **Save IP Range**.
7. Click **Save Network**.

## Deleting an IP Address Range



**NOTE:** Attempting to delete an IP address range that includes addresses currently assigned to a device will cause an error. Additionally, any other changes you make on the Edit Network screen at this time will not be applied.

1. Click **Networking** → **Networks** in the left pane.
2. Click an existing network connection for a SAN (iSCSI) or Management Network.
3. Click **Edit**.
4. Click **Remove** next to the IP address range you want to delete.
5. Click **Save Network**.

## Pools

In Active System Manager, pools provide a conceptual way to categorize the [virtual identities](#) that facilitate network communication.

A pool can include any combination of MAC, iSCSI, and FCoE virtual identities. By default, virtual identities that are not assigned to a pool belong to the *Global* pool.

After [creating a pool](#), you can [add virtual identities](#) to it and then [assign the pool](#) to one or more Deployment Templates. For example, you might create a pool to use for a specific business unit (like Finance or HR) or for a specific application.

The **Pools** screen displays information about identity pools configured in Active System Manager, including:

- Name
- Available (total number of identities available in the pool)
- Assigned (total number of identities currently assigned to devices)
- Reserved (total number of identities currently reserved for future use)
- Deployment Template (total number of Deployment Templates currently using the pool)

From this screen, you can:

- [Create](#) a pool
- [Delete](#) a pool

Additionally, you can click an existing pool to see its details, including:

- Summary of the virtual identities assigned to the pool, including status (available, assigned, reserved)
- Deployment Templates associated with the pool



**NOTE:** You can modify how the screen displays by clicking a column name to sort displayed items by that column. You can also [refresh](#) the information on the screen.

## Creating an Identity Pool

1. Click **Networking** → **Pools** in the left pane.
2. Click **Create**.
3. Enter a **Pool Name** that is less than 100 characters.
4. Click **Save**.



Now, you can add any combination of new [MAC](#), [iSCSI](#), and [FCoE](#) identities to the pool.

## Deleting an Identity Pool



**NOTE:** You cannot delete a pool that is currently associated with a Deployment Template, or that has identities in an *Assigned* or *Reserved* state. Additionally, you cannot delete the *Global* pool.

1. Click **Networking** → **Pools** in the left pane.
2. Select a pool.
3. Click **Delete**.
4. Click **Yes** to confirm the deletion.

The pool and all identities associated with the pool are deleted.

## Network Identities

Active System Manager uses three types of virtual identities to facilitate network communication:

- [Virtual MAC identities](#)
- [Virtual iSCSI identities](#)
- [Virtual FCoE identities](#)

### Virtual MAC Identities

Virtual MAC identities are unique device identifiers that facilitate Ethernet communication in a local area network (LAN). Adding virtual MAC identities enables Active System Manager to automatically assign Ethernet MAC addresses to LAN virtual NICs during deployment.

The **Virtual MAC Identities** screen displays information about existing addresses including:

- MAC Address – In the format *XX:XX:XX:YY:YY:YY*



**NOTE:** The virtual MAC identity that Active System Manager assigns to the NIC depends on the **Network Type** selected when [adding](#) a network. For a LAN network type, a virtual MAC address is assigned to the server. For an iSCSI network type, a virtual iSCSI MAC address is assigned to the server. For an FCoE network type, a virtual FIP MAC address is assigned to the server.

- [Pool](#) to which the identity is assigned
- State
  - *Assigned* if associated with a device
  - *Available* if not associated with a device
  - *Reserved* if pending assignment
- Deployment Name
- Deployment Template
- Server IP Address

From this screen, you can [add](#) new MAC addresses. Additionally, you can click an identity to see its details, including:

- Summary information
- Network configurations



**NOTE:** You can modify how the screen displays by clicking a column name to sort displayed items by that column. You can also [refresh](#) the information on the screen.

### Adding Virtual MAC Identities

You can add as few as one and as many as 1,024 [virtual MAC identities](#) at one time. The maximum number of virtual MAC identities that Active System Manager can manage is 250,000.

1. Click **Networking** → **Virtual Identities** → **LAN** in the left pane.
2. Click **Add**.
3. Enter the total **Number of Virtual MAC Identities** to add (any whole number between 1 – 1,024).
4. Select the **Pool Name** to associate with the identities. The default pool is *Global*.
5. Click **Save**.

### Virtual iSCSI Identities

Virtual iSCSI identities are unique device identifiers that facilitate iSCSI communication. Each iSCSI identity comprises an initiator iSCSI Qualified Name (IQN) and an iSCSI MAC address. Adding virtual iSCSI identities enables Active System Manager to automatically assign identity information to an iSCSI virtual NIC during deployment.

The **Virtual iSCSI Identities** screen displays information about existing IQNs including:

- Initiator Virtual IQN Address – In the format *Prefix.UniqueID*. Customized identities use the following format:
  - *Prefix* is the **IQN Prefix** entered when [adding the IQN address](#)
  - *UniqueID* is a sequential number automatically assigned by Active System Manager based on the **Starting Point** entered when [adding the IQN address](#)
- [Pool](#) to which the identity is assigned
- State
  - *Assigned* if associated with a device
  - *Available* if not associated with a device
  - *Reserved* if pending assignment
- Deployment Name
- Deployment Template
- Server IP Address
- Virtual MAC Address
- Initiator IP Address

From this screen, you can [add](#) new iSCSI identities. Additionally, you can click an identity to see its details, including:

- Summary information
- Network configurations





**NOTE:** You can modify how the screen displays by clicking a column name to sort displayed items by that column. You can also [refresh](#) the information on the screen.

### Adding Virtual iSCSI Identities

You can add as few as one and as many as 1,024 [virtual iSCSI identities](#) at one time. The maximum number of virtual iSCSI identities that Active System Manager can manage is 250,000.

1. Click **Networking** → **Virtual Identities** → **iSCSI** in the left pane.
2. Click **Add**.
3. Enter the **Number of iSCSI Identities** to add (any whole number between 1 – 1,024).
4. Select the **Pool Name** to associate with the identities. The default pool is *Global*.
5. Optionally, select **Customize Identity** to specify the naming format for the identities.
  - a) Enter the **IQN Prefix** that Active System Manager will add to the beginning of the IQN. Examples of possible prefixes include product types, serial numbers, host identifiers, and/or software keys.
 

 **NOTE:** The IQN Prefix can include up to 213 characters. Valid characters include uppercase and lowercase letters, numbers, and these special characters: – \_ , : .

 **NOTE:** If the prefix includes the characters *EUI.<Valid Hex chars>* or *eui.<Valid Hex chars>*, then Active System Manager will configure the identity into the EUI format of a 16 character hex string that includes the sequence number (based on the Starting Number). For example, if the prefix is *eui.1234567890B* and the Starting Number is 1, then the identities will start at *eui.1234567890B00001*.
  - b) Enter the **Starting Number** at which Active System Manager will begin consecutively creating the identities. The maximum valid starting number is 200000000.
6. Click **Save**.

## Virtual FCoE Identities

Virtual FCoE identities are unique device identifiers that facilitate communication in a storage area network with Fibre Channel over Ethernet (SAN FCoE) topology. Each FCoE identity comprises a World Wide Port Name (WWPN) and World Wide Node Name (WWNN) that are generated based on a Virtual FCoE Initialization Protocol (FIP) MAC Address. Adding FCoE identities enables Active System Manager to automatically assign a WWPN and WWNN to each FCoE virtual NIC during deployment.

The **Virtual FCoE Identities** screen displays information about existing addresses including:

- Virtual WWPN – Unique identifier assigned to a port; uses the format 20:01 <FIP MAC address>
- [Pool](#) to which the identity is assigned
- State
  - *Assigned* if associated with a device
  - *Unassigned* if not associated with a device
  - *Reserved* if pending assignment
- Deployment Name
- Deployment Template
- Server IP Address
- Virtual FIP MAC Address – MAC address on which the WWPN and WWNN are based
- Virtual WWNN – Unique identifier assigned to a node; uses the format 20:00 <FIP MAC address>

From this screen, you can [add](#) new FCoE identities.

For example, a virtual FCoE identity with World Wide Port Name (WWPN): 20:01:00:0E:AA:E0:00:01, virtual FIP MAC address: 00:0E:AA:E0:00:01, and virtual World Wide Node Name (WWNN): 20:00:00:0E:AA:E0:00:01.

Additionally, you can click an identity to see its details, including:

- Summary information
- Network configurations



**NOTE:** You can modify how the screen displays by clicking a column name to sort displayed items by that column. You can also [refresh](#) the information on the screen.

### Adding Virtual FCoE Identities

You can add as few as one and as many as 1,024 virtual FCoE identities at one time. The maximum number of virtual FCoE identities that Active System Manager can manage is 250,000.

1. Click **Networking** → **Virtual Identities** → **FCoE** in the left pane.
2. Click **Add**.
3. Enter the **Number of FCoE Identities** to add (any whole number between 1 – 1,024).
4. Select the **Pool Name** to associate with the identities. The default pool is *Global*.
5. Click **Save**.

# Jobs


The **Jobs** screen displays information about jobs (for example, discovery and inventory) that are currently running or have already run in Active System Manager, including:

- Name
- Progress
  - Pending (percentage complete is calculated by the number of tasks completed, not the estimated completion time)
  - Failed
  - Successful
  - Completed with errors (job is complete but failed on one or more devices)
- Start Time
- End Time
- Started By
- Description

From this screen, you can:

- [Export](#) a .csv file with job details
- [Purge](#) the job queue

Additionally, you can click a job to see its details.

 **NOTE:** You can modify how the screen displays by clicking a column name to sort displayed items by that column. You can also [refresh](#) the information on the screen.

## Exporting All Job Details

You can export a .csv file that contains details of jobs that have run since the last time the job queue was purged.

1. Click **Jobs** in the left pane.
2. Click **Export All**.
3. Open or save the file.

## Purging the Job Queue

Purging the job queue deletes job entries from the screen. You can choose to delete job details that are older than a specified date and/or assigned a particular status.

1. Click **Jobs** in the left pane.
2. Click **Purge Job Entries**.
3. Optionally, enter an **Older Than** date in the format MM/DD/YYYY. All job details created before this date will be deleted.



**NOTE:** If you do not enter a date, job details from *all* dates will be purged from the queue.

4. Optionally, select one or more **Status** types. Only jobs with the selected statuses will be deleted.
5. Click **Apply**.

## Retry a Job on a Device or Deployment in Error State

You can retry the last failed job on a device or deployment.

1. Click the error icon or link from one of the following areas:
  - Details areas on the **Getting Started** screen
  - **State** column on the **Deployments** screen
  - **State** column on the **Devices** → **Servers**, **Devices** → **Chassis**, or **Devices** → **I/O Modules** screens
2. Click **Retry** to retry the last failed job.



**NOTE:** If the device or deployment is in a state that does not support a retry, or if the failed job is not the last failed job on the device, then you must manually recreate the failed operation and run a new job.

## Force an Action on a Device or Deployment in Error State

Forcing an operation causes Active System Manager to forcefully remove all identity data from a device, even in cases where it is unable to communicate with the device.



**CAUTION:** Forcing an action can have serious repercussions and should only be attempted if a server has gone offline. For example, if you force the deletion of a deployment from an offline server, then all the identity data on the server (assigned by Active System Manager) remains on the server. Active System Manager reclaims the identity data from its database, but is unable to clear those attributes on the server. The same identity data could be assigned to a second server during another deployment. If the first server comes back online, then there are two servers with same identity data. Any devices that have been forcefully removed will need to be reset manually.

If one of the following actions puts a device or deployment in an *Error* state because of communication failure, you can force the action:

- Detach a deployment
  - Migrate a deployment
  - Delete a deployment
  - Remove a chassis
1. If trying one of the above actions puts the device or deployment in a *Error* state, click the error icon or link from one of the following areas:
    - **State** column on the **Deployments** screen
    - **State** column on the **Devices** → **Chassis** screen
  2. Click **Force** to force the action.

# Settings

From the **Settings** screens, you can:

- Manage Active System Manager [users](#)
- Configure [environment](#) settings such as the default monitoring configuration applied to new Management Templates and NTP settings for the Active System Manager virtual appliance
- Create the [credentials](#) that Active System Manager will use to access chassis, servers, and I/O modules
- Access system [logs](#)
- Perform [appliance management](#) tasks related to firmware updates, proxy server settings, SSL certificates, and license management for the Active System Manager virtual appliance
- Configure automatically scheduled and manual [backup and restore](#) jobs
- Set [polling intervals](#) to update device status

## Users

The **Settings** → **Users** screen displays information about Active System Manager user accounts, including

- User Name
- [Role](#)
- Last Name
- First Name
- State (*Enabled* or *Disabled*)

From this screen, you can:

- [Edit](#) or [delete](#) an existing user
- [Create](#) a new user
- [Enable or disable](#) a user account


Additionally, you can click a user account to see its details, including:

- Email
- Phone number



**NOTE:** You can modify how the screen displays by clicking a column name to sort displayed items by that column. You can also [refresh](#) the information on the screen.

## Creating a User

1. Click **Settings** → **Users** in the left pane.
2. Click **Create**.
3. Enter a unique **User Name** to identify the user account.
4. Enter a **Password** that the user will enter to access Active System Manager. Confirm the password.  
 **NOTE:** Passwords must be between 8-32 characters long, and include at least one number, one capital letter, one lowercase letter, and one special character.
5. Enter the user's **First Name** and **Last Name**.
6. Select a [Role](#).
7. Enter the **Email** address and **Phone** number for contacting the user.
8. Select **Enable User** to create the account with an *Enabled* status, or deselect this option to create the account with a *Disabled* status.
9. Click **Save**.

## Deleting a User

1. Click **Settings** → **Users** in the left pane.
2. Select one or more user accounts to delete.
3. Click **Delete**.
4. Click **Yes** to delete the account(s).

## Editing a User

1. Click **Settings** → **Users** in the left pane.
2. Select one user account to edit.
3. Click **Edit**.
4. Modify the user account information.
5. Click **Save**.

## Enabling or Disabling a User

1. Click **Settings** → **Users** in the left pane.
2. Select one or more user accounts to enable/disable.
3. In the **Other Tasks** drop-down menu, select **Enable** or **Disable**.
4. Click **Yes** to enable/disable the account(s).

## About Roles

Every Active System Manager user account is assigned an Operator or Admin role with the following permissions:

- Operator
  - **Deployments** – All operations are permitted
  - **Devices** → **Servers** – [Run inventory](#), [power on](#), [power off](#), [remote console](#), hide/show unsupported servers
  - **Devices** → **Chassis** – [Run inventory](#), open the Chassis Management Controller (CMC) console (click the chassis IP address)



- **Devices** → **I/O Modules** – [Run inventory](#)
- **Management and Deployment Templates** – View templates
- **Logs** – [Export all](#)
- **Jobs** – [Export all](#)
- **Settings** → **Appliance Management** – [Generate troubleshooting bundle](#)
- **Admin** – Full access to all features

## Environment

The **Settings** → **Environment** screen displays environmental settings, including:

- Default monitoring configuration that is applied to new Management Templates
- Time zone and NTP configuration for the Active System Manager virtual appliance

From this screen, you can:

- Edit default [monitoring settings](#)
- Edit [NTP settings](#)

### Editing Default Environment Monitoring Settings

Configuring environment monitoring settings enables sending Chassis Management Controller (CMC) hardware alerts to recipients and syslog information for I/O modules to a destination server.

On the **Settings** → **Environment** screen, you can edit the default environment monitoring settings that automatically apply to new Management Templates. It is important to note that you can always override these default settings for a specific Management Template by entering different information in the [Create/Edit Management Template](#) wizards.

Editing default settings does not apply changes to existing templates and does not affect the Active System Manager virtual appliance. Additionally, trap settings and email alerts apply only to chassis, and the syslog destination applies only to I/O modules.

1. Click **Settings** → **Environment** in the left pane.
2. Click > next to **Monitoring**, and then click **Edit**.
3. On the **Monitoring** screen, do one of more of the following:
  - [Configure](#) default monitoring settings, including adding trap settings, destination emails, and a syslog destination.
  - Edit an existing alert destination — Click **Edit** next to the alert destination to change, and enter a new [configuration](#).
  - Edit an existing destination email — Click **Edit** next to the destination email to change, and enter a new [configuration](#).
  - Remove an existing alert destination — Click **Remove** next to the alert destination you wish to delete.
  - Remove an existing destination email — Click **Remove** next to the destination email you wish to delete.
4. Click **Save**.


## Editing Default NTP Settings

Changes on this screen affect the time zone and NTP server(s) that are applied to the Active System Manager virtual appliance. All time data is stored in UTC format, and is used to display log and event time stamps.

1. Click **Settings** → **Environment** in the left pane.
2. Click > next to **NTP**, and then click **Edit**.
3. Select a **Time Zone**.
4. Optionally, select **Enable NTP Server** and enter the IP address or hostname of a **Preferred NTP Server** and **Secondary NTP Server (optional)** for time synchronization.
5. Click **Submit**. The virtual appliance will restart and become unavailable for a few minutes, and all active users will be logged out.

## Credentials


A root-level credential (user name and password) is required for Active System Manager to access and manage chassis, servers, and I/O modules. To configure credentials on a device, you must first [create](#) the credential, and then assign it to the [Management Template](#) that will apply to the device.

 **NOTE:** The default root-level credential for Dell hardware is a user name of *root* and a password of *calvin*. It is strongly recommended to change the password; however, the user name for root-level credentials in Active System Manager must remain *root*.

After adding a credential, the following information displays on the **Settings** → **Credentials** screen:


- Name – User-defined name that identifies the credential
- Type – Type of device that uses the credential (chassis, server, I/O module, or storage)
- Devices – Total number of devices to which the credential is assigned

From this screen, you can:

- [Edit](#) an existing credential
-  **NOTE:** Editing a credential that is applied to a Management Template that currently configures a chassis can cause device communication to fail. To restore communication, return the credential to its original settings, wait 5 to 10 minutes, and rerun any failed jobs.
- [Create](#) a new credential required to access one or more devices
- [Delete](#) an existing credential


Additionally, you can click a credential to see its details, including:


- Summary information
- Devices to which the credential is assigned
- Templates to which the credential is assigned

 **NOTE:** You can modify how the screen displays by clicking a column name to sort displayed items by that column. You can also [refresh](#) the information on the screen.

## Creating a New Credential

1. Do one of the following:
  - Click **Settings** → **Credentials** in the left pane, and then click **Create**. Select the **Credential Type** (*Server, Chassis, I/O Module, or Storage*).
  - On the **Device Access** → **Credentials** page of the Create/Edit Management Template wizards, click **New** next to the device type.
2. Enter a unique **Credential Name** used to identify the credential.
3. Enter the **User Name**.
 

 **NOTE:** *Root* is the only valid user name for root-level credentials on chassis (CMC), servers (iDRAC), and I/O modules. You can add local [CMC](#) and [iDRAC](#) users with user names other than *Root*.
4. Enter and verify a **Password**.
 


 **NOTE:** For valid user name and password formats, see the iDRAC, CMC, I/O module, or storage third-party documentation.
5. Optionally, for a **Server** or **Chassis** credential, select **Enable Certificate Check** to verify that the SSL certificate for the associated device is valid.
6. For an **I/O Module** credential:
  - a) Select the connection **Protocol** used to remotely access the device (*Telnet* or *SSH*).
  - b) Enter the **SNMP v2 Community String** required to access the device.
7. Click **Save**.

## Editing a Credential

Editing a credential that is applied to a Management Template that currently configures a chassis can cause device communication to fail. To restore communication, return the credential to its original settings, wait 5 to 10 minutes, and rerun any failed jobs.

1. Click **Settings** → **Credentials** in the left pane.
2. Select a credential to edit.
3. Click **Edit**.
4. Modify the credential information.
5. Click **Save**.

## Deleting a Credential

 **NOTE:** You cannot delete a credential that is currently assigned to a Management Template.

1. Click **Settings** → **Credentials** in the left pane.
2. Select the credential to delete.
3. Click **Delete** from the **Other Tasks** drop-down list.
4. Click **Yes** to delete the credential.

## Logs

Active System Manager provides an activity log of user- and system-generated actions to use for troubleshooting activities. By default, log entries display in the order they occurred. To sort entries by a specific category, click the arrow next to a column name.

Information provided in the logs includes:

- **Severity**
  - Critical – Fatal error communicating with a managed device; corrective action immediately required.
  - Warning – Device is in a state that requires corrective action, but does not impact overall system health. For example, a discovered device is not supported.
  - Information – General information about system health or activity.
- **Category**
  - Security – Authentication failures, operations on users or credentials
  - Appliance Configuration – Initial Setup, appliance settings, upgrading, backup/restore
  - Template Configuration – Operations on templates
  - Network Configuration – Operations on networks, MAC addresses, IQNs, WWNs
  - Infrastructure or Hardware Configuration – Discovery, inventory, configuration, firmware updates
  - Infrastructure or Hardware Monitoring – Device health
  - Deployment – Deployment and migration operations
  - Licensing – License updates or expirations
  - Miscellaneous – All other issues
- **Description** – Brief summary of activity
- **Date and Time** – When activity occurred
- **User** – User name from which activity originated

From this screen, you can:

- View log entries
- [Export all](#) log entries to a .csv file
- [Purge](#) all log entries



**NOTE:** You can modify how the screen displays by clicking a column name to sort displayed items by that column. You can also [refresh](#) the information on the screen.

## Exporting All Log Entries




You can export all current log entries to a comma-delimited (.csv) file for troubleshooting.

1. Click **Settings** → **Logs** in the left pane.
2. Click **Export All**.
3. Open or save the file.

## Purging Log Entries

You can delete log entries based on date and/or severity.

1. Click **Settings** → **Logs** in the left pane.
2. Click **Purge**.
3. To delete entries by date, click **Older Than** and select a day.

-  **CAUTION:** If you do not select a date, then ALL entries with the selected severity level(s) will be deleted.
4. To delete entries by severity level, select **Information**, **Warning**, and/or **Critical**.
-  **CAUTION:** If you do not select a severity level, then ALL entries older than the selected date will be deleted.
5. Click **Apply**.
-  **NOTE:** You must select either a date or at least one severity level.


## Appliance Management

From the **Settings** → **Appliance Management** screen, you can:

- [Update](#) Active System Manager software on the virtual appliance
- [Edit](#) the location where the Active System Manager upgrade file is stored
- [Generate](#) a troubleshooting bundle
- [Edit](#) proxy server settings
- [Generate](#) a certificate signing request (CSR) and [upload](#) the resulting SSL certificate
- [Upload](#) a Active System Manager license


### Updating the Virtual Appliance

Updating the virtual appliance upgrades Active System Manager software to the most recent version, including any operating system security patches that are required. The update file loads from the location specified in the [Update Repository Path](#).

 **NOTE:** During an update, the virtual appliance restarts and becomes unavailable for a few minutes, and all active users are logged out. Additionally, all pending jobs are interrupted, which will cause some jobs to enter an *Error* state. For this reason, it is recommended to wait for all pending jobs to complete before starting the update process.

1. Click **Settings** → **Appliance Management** in the left pane.
2. Click **Update Virtual Appliance**.
3. Read the warning, and then click **Yes**.

The update immediately begins.

 **NOTE:** After the update completes, make sure to clear the history (or temporary Internet files) in your Web browser. Failing to do so may prevent changes from displaying in the Active System Manager user interface.

### Editing the Update Repository Path

The **Update Repository Path** indicates the location where package for [updating the virtual appliance](#) is stored.

 **CAUTION:** By default, the path points to the primary Active System Manager update repository. It is not recommended to update the repository path, unless directed to do so by Dell Support.

1. Click **Settings** → **Appliance Management** in the left pane.
2. Click **Edit** next to **Update Repository Path**.
3. Enter the path to the repository where the upgrade file is stored.
4. Click **Save**.

## Generating a Troubleshooting Bundle

A troubleshooting bundle is a .zip file that contains appliance logging information for the Active System Manager virtual appliance. You can send the bundle to Dell Support, if needed.

1. Click **Settings** → **Appliance Management** in the left pane.
2. Click **Generate Troubleshooting Bundle**.
3. Open or save the file.

## Proxy Settings

If your network uses a proxy server for external communication, then you must enter critical information to enable communication with the Active System Manager virtual appliance.

1. Click **Settings** → **Appliance Management** in the left pane.
2. Click **Edit** next to **Proxy Settings**.
3. Select **Use HTTP Proxy Settings**.
4. Enter a **Server Address** (IP address or host name) for the proxy server.
5. Enter a valid **Port** number between 1 – 65535. Ports commonly used for a proxy server are 80 and 8080.
6. If the proxy server requires credentials to log in, select **Use proxy credentials** and then enter the required **User Name** and **Password**. Verify the password.
7. Click **Test Proxy Connection** to validate the settings entered on this page.
8. Click **Save**.

## SSL Certificates

It is recommended to upload an SSL certificate to Active System Manager. Doing so provides a number of benefits, including:

- Encrypting data that Active System Manager sends over the web to help ensure secure transmission
- Providing authentication to make sure data is routed to its intended endpoint
- Preventing users from receiving browser security errors

To upload an SSL certificate:

1. [Generate](#) a certificate signing request (CSR).
2. [Download](#) the CSR.
3. Submit the CSR to a certificate authority (CA). The CA will provide a valid SSL certificate.
4. [Upload](#) the SSL certificate to Active System Manager.

## Generating a Certificate Signing Request

A certificate signing request (CSR) includes server information (such as domain name, locale, and so on) that certificate authorities require in order to provide a valid SSL certificate.

After generating the CSR, you will [download](#) the encrypted text, and then submit it to a certificate authority. In return, the certificate authority will provide a valid SSL certificate for you to [upload](#).

1. Click **Settings** → **Appliance Management** in the left pane.
2. Click the > next to **SSL Certificates**.
3. Click **Generate Certificate Signing Request**, and then enter the required information:
  - a) Enter a **Distinguished Name** (Fully-Qualified Domain Name) in the format *www.domain.com*.
  - b) Enter the **Business Name** under which the certificate will be recorded.
  - c) Enter the **Department Name** of the organizational unit (for example, IT, HR, or Sales) for which the certificate will be generated.
  - d) Enter the **Locality** (town or city) in which the organization is located.
  - e) Enter the **State (Province/Region)** in which the organization is located (do not abbreviate).
  - f) Select the **Country** in which the organization is located.
  - g) Enter a valid **Email** address.
  - h) Click **Generate**.
  - i) Click **Yes** to confirm.
4. Click **Download Certificate Signing Request**, and then copy the text that displays. Submit this text to a certificate authority to receive a valid SSL certificate.

### Downloading the Certificate Signing Request

After [generating](#) the CSR, you must download the resulting text and submit it to a certificate authority. The certificate authority will provide an SSL certificate for you to upload to Active System Manager.

1. Click **Settings** → **Appliance Management** in the left pane.
2. Click the > next to **SSL Certificates**.
3. Click **Download Certificate Signing Request**.
4. Copy the displayed text, and submit it to a certificate authority to receive a valid SSL certificate.

After the certificate authority provides the SSL certificate, [upload](#) it to Active System Manager.

### Uploading the SSL Certificate

Before you upload the SSL certificate, you must first [generate](#) and [download](#) a certificate signing request (CSR). Then, submit the CSR to a certificate authority to receive a valid SSL certificate, and save the certificate to a local network share.

1. Click **Settings** → **Appliance Management** in the left pane.
2. Click the > next to **SSL Certificates**.
3. Click **Upload Certificate**.
4. Click **Browse**, and select the SSL certificate.  
Active System Manager supports X.509 certificates with RSA 2048 bit key encryption. The certificate must be in PEM format.
5. Click **Yes** to upload the certificate.  
When the certificate uploads, web services will restart, the virtual appliance will become unavailable for a few minutes, and all active users will be logged out.

## License Management

Active System Manager licensing is based on the total number of managed servers. There are two valid license types:

- Standard – Full-access license with no expiration date
- Trial – Limited license that expires after a specified number of days

For both license types, you will receive an email from customer service with instructions on how to download the license file to a local network share.

The first time you use Active System Manager, you must upload the license file through the Initial Setup wizard. However, you can upload subsequent licenses on the **Appliance Management** screen.

1. Click **Settings** → **Appliance Management** in the left pane.
2. Click **Edit** next to **License Management**.
3. Click **Browse**, select a valid license file, and then click **Open**.  
The license file uploads, and its details display, including *License Type*, *Number of Servers*, and *Expiration*.
4. Click **Save** to immediately activate the license.

## Backup and Restore

Performing a backup saves all [user-created data](#) to a remote share from which it can be restored.



**NOTE:** It is recommended to perform frequent backups to guard against data loss and/or corruption. Additionally, it is recommended to take a snapshot of the Active System Manager virtual appliance every time you perform a restore (see VMware documentation for more information).

The **Settings** → **Backup and Restore** screen displays information about the last backup operation performed on the Active System Manager virtual appliance. Information in the **Settings and Details** section applies to both [manual](#) and [automatically scheduled](#) backups, including:

- Last backup date
- Last backup status
- Backup directory path to an NFS or CIFS share, including an optional user name required to access the share, if needed

Additionally, the **Backup and Restore** screen displays information about automatically scheduled backups, including:

- Status of automatically scheduled backups (*Enabled* or *Disabled*)
- Days of the week and time (24-hour format) that backups occur
- Date and time of the next scheduled backup
- Local time zone of the Active System Manager virtual appliance

From this screen, you can:

- [Backup now](#) (manually start an immediate backup)
- [Restore now](#)
- [Edit](#) general backup settings
- [Edit](#) automatically scheduled backup settings

## Backup Details

The data saved in a Active System Manager backup file includes details about:

- Activity logs
- Credentials
- Deployments




- Device inventory and status
- Events
- Identity Pools
- Initial setup
- IP addresses
- Jobs
- Licensing
- Networks
- Templates
- Users and roles

## Editing Backup Settings And Details

1. Click **Settings** → **Backup and Restore** in the left pane.
2. Under **Settings and Details**, click **Edit**.
3. Optionally, enter a **Backup Directory Path** to indicate the network share location where the backup file will be saved. Use one of the following formats:
  - NFS – **host/share/**
  - CIFS – **\\host\share\**

You can also enter a **Backup Directory User Name** and **Backup Directory Password**, if required to access the network share.

4. Enter an **Encryption Password** that will be required to open the backup file. Verify the encryption password.
 

 **NOTE:** The password *can* include any alphanumeric characters and these special characters: !@#\$%\*
5. Click **Save**.


## Editing Automatically Scheduled Backups

On this screen, you can specify the days and times to run automatically scheduled backups. To change the location where backup files are saved or the password required to access a backup file, see [Editing Backup Settings And Details](#).

1. Click **Settings** → **Backup and Restore** in the left pane.
2. Under **Automatically Scheduled Backups**, click **Edit**.
3. To schedule automatic backups, select **Enabled**. To discontinue automatically scheduled backups, select **Disabled**.
4. Select **Days for Backup** to specify day(s) on which backups will occur.
5. Select the **Time to Start Backup**.  
The date and time of the **Next Backup** displays.
6. Click **Save**.

## Backup Now


In addition to [automatically scheduled backups](#), you can manually run an immediate backup.

1. Click **Settings** → **Backup and Restore** in the left pane.
  2. Click **Backup Now**.
  3. Choose one of these options:
    - To use the [general settings](#) that are applied to all backup files, select **Use Backup Directory Path and Encryption Password from Settings and Details**.
    - To use custom settings:
      1. Enter a **Backup Directory Path** where the backup file will be saved. Use one of these formats:
        - NFS – **host/share/**
        - CIFS – **\\host\share\**
      2. Optionally, enter a **Backup Directory User Name** and **Backup Directory Password**, if they are required to access the location you entered in the previous step.
      3. Enter an **Encryption Password** that will be applied to the backup file, and verify the encryption password. Make sure to note this password somewhere; it will be required to access the backup file during the restore process.
-  **NOTE:** The password *can* include any alphanumeric characters and these special characters: !@#\$/%\*
4. Click **Submit**.

## Restore Now

Restoring the Active System Manager virtual appliance returns user-created data to a previous configuration that is saved in a backup file.

 **CAUTION:** Restoring a previous configuration restarts the Active System Manager virtual appliance and deletes data created after the backup file to which you are restoring.

 **NOTE:** It is recommended to perform frequent backups to guard against data loss and/or corruption. Additionally, it is recommended to take a snapshot of the Active System Manager virtual appliance every time you perform a restore (see VMware documentation for more information).

1. Click **Settings** → **Backup and Restore** in the left pane.
2. Click **Restore Now**.
3. Enter a **File Path** that specifies the backup file to be restored. Use one of these formats:
  - NFS – **host/share/filename.gz**
  - CIFS – **\\host\share\filename.gz**
4. If needed, enter the **Backup Directory User Name** and **Backup Directory Password** required to log into the location where the backup file is stored.
5. Enter the **Encryption Password** required to access the backup file. This is the password that was entered when the backup file was [created](#).
6. Click **Apply**.

The restore process begins.

# Polling Intervals

The **Settings** → **Polling Intervals** screen displays the days and times set for chassis inventory polling and status polling (across all devices and templates), including:

- Status of polling intervals (*Enabled* or *Disabled*)
- Day(s) of the week and time(s) inventory jobs are scheduled to run
- How often device status is checked

From this screen, you can:

- [Schedule](#) how often Active System Manager runs inventory jobs on all discovered chassis
- [Set](#) status polling intervals

## Editing Automatically Scheduled Chassis Inventory Jobs

1. Click **Settings** → **Polling Intervals** in the left pane.
2. Under **Chassis Inventory Polling**, click **Edit**.
3. On the **Chassis Inventory Polling** screen, select **Enable scheduled chassis inventory polling**.
4. Select **Daily** and a time (UTC) to run inventory jobs every day, or select **Weekly** and a day and time (UTC) to run inventory jobs once a week.
5. Click **Submit**.

## Setting Status Polling Interval

Use the **Status Polling** screen to set how often Active System Manager analyzes devices to determine their status.

1. Click **Settings** → **Polling Intervals** in the left pane.
2. Under **Status Polling**, click **Edit**.
3. On the **Status Polling** screen, select how often Active System Manager will check device status ( *1 hour, 6 hours, 12 hours, or 24 hours*).
4. Click **Submit**.



## Use Cases

The use cases in this chapter describe how to configure chassis, servers, and Active System Manager templates to support the following deployment types:

- [ESXi using FCoE datastores and networking on converged fabric with initial iDRAC boot](#)
- [ESXi using FCoE datastores and networking on converged fabric with initial PXE boot](#)
- [ESXi using FCoE datastores and networking on separate fabric with FCoE boot](#)
- [ESXi using FCoE datastores and networking on converged fabric with initial iDRAC boot](#)
- [Red Hat Enterprise Linux using iSCSI datastores and networking on converged fabric](#)
- [Windows Server 2008 R2 using FCoE datastores and networking on converged fabric](#)



**NOTE:** Use cases offer an example of one possible way to configure Active System Manager for a specific deployment type. The hardware environment and values suggested for configuring devices and templates are recommendations based on best practices—not necessarily requirements. Make sure to use values that are appropriate for your specific environment.

### ESXi Using FCoE Datastores and Networking on Converged Fabric with Initial iDRAC Boot

The purpose of this use case is to boot an ESXi deployment from the local RAID disks in servers, and enable the servers to utilize both FCoE storage and networking on a converged FCoE and LAN network. This example uses the following hardware environment:

- I/O modules – Two supported I/O modules installed to A1 and A2 fabrics of the chassis for redundant converged FCoE and LAN network
- Top-of-rack switch – Two Nexus 5000 series for converged FCoE and LAN network
- Blade Servers – Four Dell PowerEdge 12th generation blade servers with an NDC on each server to enable redundancy and multipathing in the ESXi cluster (you can add additional servers after creating the cluster)
- Converged Network Adapters (CNAs) – On each server, supported Network Daughter Card (NDC) or supported Mezzanine card for FCoE and LAN connectivity
- Networks (VLANs) – One FCoE VSAN VLAN, one FCoE FIP-discovery VLAN, one VM VLAN, one vMotion VLAN, and one hypervisor management VLAN.
- Storage Type – Dell Compellent Series 40 ESX datastore on a single volume
- Operating System/Hypervisor – ESXi 5.1




**NOTE:** Use cases offer an example of one possible way to configure Active System Manager for a specific deployment type. The hardware environment and values suggested for configuring devices and templates are recommendations based on best practices—not necessarily requirements. Make sure to use values that are appropriate for your specific environment.

### Prerequisites

Configure the networks that servers and chassis will use, and prepare the images to use for hypervisor installation from iDRAC virtual media.

1. [Add networks](#) to Active System Manager. These networks should be consistent with the VLANs available on the top-of-rack (ToR) switch.
  - a) Add two SAN (FCoE) networks—one will act as the FCoE FIP Discovery VLAN (VLAN ID must be set to 1), the second VLAN is the FCoE VSAN VLAN and is specific to your FCoE environment. These VLANs must be consistent with the FCoE networks used on the FCoE (ToR) switch and FCoE network.

 **NOTE:** Active System Manager cannot currently support a default VLAN ID other than VLAN 1 on the I/O module. For this reason, the Native VLAN in your FCoE deployment must be set to VLAN 1. Your FCoE environment must also be configured to use VLAN 1 for FIP Discovery.
  - b) Add one Public LAN with the VLAN ID set to any number between 1 - 4000 and 4021 - 4094. The VLAN should be consistent with other VLANs available on the ToR switch.
  - c) Add one Private LAN with the VLAN ID set to any number between 1 - 4000 and 4021 - 4094. This network will be used for vMotion traffic.
  - d) Add one Hypervisor Management network with the VLAN ID set to any number between 1 - 4000 and 4021 - 4094. The VLAN should be consistent with other VLANs available on the ToR switch.
  - e) If using static IP addressing, add one Management Network to support servers and I/O modules.
2. Create an NFS or CIFS share that the Active System Manager virtual appliance can access. Place the ESXi ISO image on the share.
3. Do one of the following:
  - (Recommended) If using static IP addresses, add an [IP address range](#) to the Management Network. Make sure to add a range that is large enough to support the total number of IP addresses you will need in the future.
  - If using DHCP, configure a DHCP server to assign IP addresses to servers and I/O modules.

## Configuring the Management Template

[Create a Management Template](#) with the following settings.

- **Device Access** → **IP Addressing** – Choose static (recommended) or DHCP addressing option.
- **Device Access** → **Credentials** – Create credentials for servers and I/O modules.
- **Networking** – It is not recommended to change the settings on this screen. Use the default settings, unless you have a very specific reason to do otherwise.

All other settings are optional. Configure them to meet the needs of your specific environment.

## Configuring the Chassis




After [discovering](#) the chassis, [configure](#) it with the following settings. Configuring the network fabrics prepares the I/O modules to carry converged FCoE and LAN network traffic.

- **Connectivity** → **Fabric A** – Select *Converged* for the **Fabric Purpose**, and deselect **Customize networks for this fabric**.
- **Connectivity** → **Fabric B** – Do not select a fabric purpose.
- **Connectivity** → **Fabric C** – Do not select a fabric purpose.
- **Templates** – Select the Management Template configured for this use case.

All other settings are optional. Configure them to meet the needs of your specific environment.

## Configuring the Deployment Template

[Create](#) a Deployment Template with the following BIOS, RAID, network, and I/O module settings that will prepare the server and the chassis for ESXi installation.

- **BIOS** – Select **Integrated RAID Controller**, **Processor Virtualization Technology**, and **Execute Disable**.
- **RAID** – For PowerEdge M420 and M620 servers, select *RAID 0* or *RAID 1*. For PowerEdge M820 servers, select *RAID 5*.
- **Networks** – Select [Enable Bandwidth Oversubscription](#) to enable setting a higher maximum bandwidth for each of the virtual NICs on a server, so that the total exceeds 100% of the network bandwidth available to the NIC port to which the virtual NIC is assigned. Use a physical partition for the virtual NIC mapping order. Additionally, create four new virtual NIC configurations that will each correspond to a partition on the network adapter:
  - Virtual NIC 1 to carry FCoE VLAN traffic and use the native VLAN for untagged FCoE discovery traffic
    1. Select a **Connection Type** of *SAN (FCOE)*.
    2. For the **Native VLAN**, select the native FCoE VLAN created as a prerequisite in this use case to use for FCoE discovery.
    3. Enter *10 GB* for the **Maximum Bandwidth** and *5 GB* for the **Minimum Bandwidth**.
    4. Select **Redundancy** to configure an identical partition on the second network adapter.
    5. Select a **Virtual Identity Pool**.  
 **NOTE:** You can [create a custom pool](#), if desired. Otherwise, select the default *Global* pool.
    6. For the network to associate with this virtual NIC configuration, select the custom FCoE network created as a prerequisite in this use case.
  - Virtual NIC 2 for vMotion private LAN
    1. Select a **Connection Type** of *LAN*.
    2. Do not select a **Native VLAN**.
    3. Enter *10 GB* for the **Maximum Bandwidth** and *2 GB* for the **Minimum Bandwidth**.
    4. Select **Redundancy** to configure an identical partition on the second network adapter.
    5. Select a **Virtual Identity Pool**.  
 **NOTE:** You can [create a custom pool](#), if desired. Otherwise, select the default *Global* pool.
    6. For the network to associate with this virtual NIC configuration, select the Private LAN created as a prerequisite in this use case.
  - Virtual NIC 3 for hypervisor management
    1. Select a **Connection Type** of *LAN*.
    2. Do not select a **Native VLAN**.
    3. Enter *10 GB* for the **Maximum Bandwidth** and *2 GB* for the **Minimum Bandwidth**.
    4. Select **Redundancy** to configure an identical partition on the second network adapter.
    5. Select a **Virtual Identity Pool**.  
 **NOTE:** You can [create a custom pool](#), if desired. Otherwise, select the default *Global* pool.
    6. For the network to associate with this virtual NIC configuration, select the Hypervisor Management network created as a prerequisite in this use case.
  - Virtual NIC 4 for Public LAN
    1. Select a **Connection Type** of *LAN*.
    2. Do not select a **Native VLAN**.

3. Enter *10 GB* for the **Maximum Bandwidth** and *2 GB* for the **Minimum Bandwidth**.
4. Select **Redundancy** to configure an identical partition on the second network adapter.
5. Select a **Virtual Identity Pool**.



**NOTE:** You can [create a custom pool](#), if desired. Otherwise, select the default *Global* pool.

6. For the network to associate with this virtual NIC configuration, select the Public LAN created as a prerequisite in this use case.

- **Boot Information** – Select *iDRAC image boot (one time)* to boot the server from the ESXi ISO staged on the NFS or CIFS share. Then, specify your **Share Type**, **Path**, and, if required, **Credentials**.

All other settings are optional. Review the boot sequence to make sure it is correct. Configure the other settings to meet the needs of your specific environment.

## Deploying Servers

On the **Templates** → **Deployment Templates** screen, select the Deployment Template created for this use case, and then click **Deploy**. [Complete the Deploy wizard](#) two times with the following settings:

- Deployment 1 – For **Server Selection**, select **Manual Server Selection**, and then select the four servers to which ESXi will be deployed.
- Deployment 2 – Do one of the following to deploy additional servers for expanded workload capacity:
  - Deploy Now: On the **Server Selection** page, select **Manual Server Selection**, and then select the two servers to deploy.
  - Deploy Later: On the **Server Selection** page, select **Deferred Deployment**, and enter *2* for the **Number of deployments to create**. Later, you can [attach](#) these deployments to servers for expanded workload capacity.

The servers are now ready to deploy ESXi 5.

## ESXi Using FCoE Datastores and Networking on Converged Fabric with Initial PXE Boot

The purpose of this use case is to boot an ESXi deployment from the local RAID disks in servers, and enable the servers to utilize both FCoE storage and networking on a converged FCoE and LAN network. This example uses the following hardware environment:

- I/O modules – Two supported I/O modules for redundant converged FCoE and LAN network
- Top-of-rack switch – Two Nexus 5000 series for converged FCoE and LAN network
- Blade Servers – Four Dell PowerEdge 12th generation blade servers with two NDCs on each server to enable redundancy and multipathing in the ESXi cluster (you can add additional servers after creating the cluster)
- Converged Network Adapters (CNAs) – On each server, Network Daughter Cards (NDCs) for FCoE and LAN connectivity
- Networks (VLANs) – One FCoE VLAN, one FCoE discovery VLAN, one public VLAN, one PXE traffic VLAN, one vMotion VLAN, and one hypervisor management VLAN
- Storage Type – Dell Compellent Series 40 ESX datastore on a single volume
- Operating System/Hypervisor – ESXi 5.0 or 5.1





**NOTE:** Use cases offer an example of one possible way to configure Active System Manager for a specific deployment type. The hardware environment and values suggested for configuring devices and templates are recommendations based on best practices—not necessarily requirements. Make sure to use values that are appropriate for your specific environment.



## Prerequisites

Configure the networks that servers and chassis will use, and prepare the images to use for hypervisor installation from PXE virtual media.

1. [Add networks](#) to Active System Manager. These networks should be consistent with the VLANs available on the top-of-rack (ToR) switch.
  - a) Add two SAN (FCoE) networks—one will act as the FCoE FIP Discovery VLAN (VLAN ID must be set to 1), the second VLAN is the FCoE VSAN VLAN and is specific to your FCoE environment. These VLANs must be consistent with the FCoE networks used on the FCoE (ToR) switch and FCoE network.  
 **NOTE:** Active System Manager cannot currently support a default VLAN ID other than VLAN 1 on the I/O module. For this reason, the Native VLAN in your FCoE deployment must be set to VLAN 1. Your FCoE environment must also be configured to use VLAN 1 for FIP Discovery.
  - b) Add two Public LANs—one for Public traffic with the VLAN ID set to any number between 1 - 4000 and 4021 - 4094 and one for PXE network traffic with the VLAN ID set to any number between 1 - 4000 and 4021 - 4094. The VLAN should be consistent with other VLANs available on the ToR switch.
  - c) Add one Private LAN with the VLAN ID set to any number between 1 - 4000 and 4021 - 4094. This network will be used for vMotion traffic.
  - d) Add one Hypervisor Management network with the VLAN ID set to any number between 1 - 4000 and 4021 - 4094. The VLAN should be consistent with other VLANs available on the ToR switch.
  - e) If using static IP addressing, add one Management Network to support servers and I/O modules.
2. Have a running PXE service with desired operating system/hypervisor image running on VLAN 1.  
 **NOTE:** PXE requires an untagged VLAN and FCoE requires VLAN 1 to be untagged. Only a single untagged VLAN is supported, so both the PEX service and the FIP-discovery must function on VLAN 1.
3. Do one of the following:
  - (Recommended) If using static IP addresses, add an [IP address range](#) to the Management Network. Make sure to add a range that is large enough to support the total number of IP addresses you will need in the future.
  - If using DHCP, configure a DHCP server to assign IP addresses to servers and I/O modules.

## Configuring the Management Template

[Create a Management Template](#) with the following settings.

- **Device Access** → **IP Addressing** – Choose static (recommended) or DHCP addressing option.
- **Device Access** → **Credentials** – Create credentials for servers and I/O modules.
- **Networking** – It is not recommended to change the settings on this screen. Use the default settings, unless you have a very specific reason to do otherwise.

All other settings are optional. Configure them to meet the needs of your specific environment.

## Configuring the Chassis

After [discovering](#) the chassis, [configure](#) it with the following settings. Configuring the network fabrics prepares the I/O modules to carry converged FCoE and LAN network traffic.

- **Connectivity** → **Fabric A** – Select *Converged* for the **Fabric Purpose**, and deselect **Customize networks for this fabric**.
- **Connectivity** → **Fabric B** – Do not select a fabric purpose.


- **Connectivity** → **Fabric C** – Do not select a fabric purpose.
- **Templates** – Select the Management Template configured for this use case.


All other settings are optional. Configure them to meet the needs of your specific environment.


## Configuring the Deployment Template

[Create](#) a Deployment Template with the following BIOS, RAID, network, and I/O module settings that will prepare the server and the chassis for ESXi installation.


- **BIOS** – Select **Integrated RAID Controller**, **Processor Virtualization Technology**, and **Execute Disable**.
- **RAID** – For PowerEdge M420 and M620 servers, select *RAID 0* or *RAID 1*. For PowerEdge M820 servers, select *RAID 5*.
- **Networks** – Select [Enable Bandwidth Oversubscription](#) to enable setting a higher maximum bandwidth for each of the virtual NICs on a server, so that the total exceeds 100% of the network bandwidth available to the NIC port to which the virtual NIC is assigned. Use a physical partition for the virtual NIC mapping order. Additionally, create new virtual NIC configurations that will each correspond to a partition on the network adapter:
  - Virtual NIC 1 to carry FCoE VLAN traffic and use the native VLAN for untagged FCoE discovery traffic
    1. Select a **Connection Type** of *SAN (FCOE)*.
    2. For the **Native VLAN**, select the native FCoE FIP-discovery VLAN (which must be set to VLAN 1) created as a prerequisite in this use case to use for FCoE FIP-discovery.
    3. Enter *10 GB* for the **Maximum Bandwidth** and *5 GB* for the **Minimum Bandwidth**.
    4. Select **Redundancy** to configure an identical partition on the second network adapter.
    5. Select a **Virtual Identity Pool**.
 

 **NOTE:** You can [create a custom pool](#), if desired. Otherwise, select the default *Global* pool.
    6. For the network to associate with this virtual NIC configuration, select the custom FCoE network created as a prerequisite in this use case.
  - Virtual NIC 2 for Public LAN and PXE
    1. Select a **Connection Type** of *LAN*.
    2. For the **Native VLAN**, select the native PXE VLAN created as a prerequisite in this use case to use for PXE discovery.
    3. Enter *10 GB* for the **Maximum Bandwidth** and *2 GB* for the **Minimum Bandwidth**.
    4. Select **Redundancy** to configure an identical partition on the second network adapter.
    5. Select a **Virtual Identity Pool**.
 

 **NOTE:** You can [create a custom pool](#), if desired. Otherwise, select the default *Global* pool.
    6. For the network to associate with this virtual NIC configuration, select the Public LAN created as a prerequisite in this use case.
  - Virtual NIC 3 for vMotion private LAN
    1. Select a **Connection Type** of *LAN*.
    2. Do not select a **Native VLAN**.
    3. Enter *10 GB* for the **Maximum Bandwidth** and *2 GB* for the **Minimum Bandwidth**.
    4. Select **Redundancy** to configure an identical partition on the second network adapter.
    5. Select a **Virtual Identity Pool**.
 

 **NOTE:** You can [create a custom pool](#), if desired. Otherwise, select the default *Global* pool.
    6. For the network to associate with this virtual NIC configuration, select the Private LAN created as a prerequisite in this use case.

- Virtual NIC 4 for hypervisor management
  1. Select a **Connection Type** of *LAN*.
  2. Do not select a **Native VLAN**.
  3. Enter *10 GB* for the **Maximum Bandwidth** and *1 GB* for the **Minimum Bandwidth**.
  4. Select **Redundancy** to configure an identical partition on the second network adapter.
  5. Select a **Virtual Identity Pool**.
 

 **NOTE:** You can [create a custom pool](#), if desired. Otherwise, select the default *Global* pool.
  6. For the network to associate with this virtual NIC configuration, select the Hypervisor Management network created as a prerequisite in this use case.
- **Boot Information** – Select *PXE (one time)* to boot the server from your PXE service (PXE service and FIP-discovery must be on VLAN 1).

All other settings are optional. Review the boot sequence to make sure it is correct. Configure the other settings to meet the needs of your specific environment.

## Deploying Servers

On the **Templates** → **Deployment Templates** screen, select the Deployment Template created for this use case, and then click **Deploy**. [Complete the Deploy wizard](#) two times with the following settings:

- Deployment 1 – For **Server Selection**, select **Manual Server Selection**, and then select the four servers to which ESXi will be deployed.
- Deployment 2 – Do one of the following to deploy additional servers for expanded workload capacity:
  - Deploy Now: On the **Server Selection** page, select **Manual Server Selection**, and then select the two servers to deploy.
  - Deploy Later: On the **Server Selection** page, select **Deferred Deployment**, and enter *2* for the **Number of deployments to create**. Later, you can [attach](#) these deployments to servers for expanded workload capacity.

The servers are now ready to deploy ESXi 5.

## ESXi Using iSCSI Datastores and Networking on Separate Fabric with Initial iSCSI Boot

The purpose of this use case is to boot an ESXi server directly from an iSCSI volume from a dedicated iSCSI network fabric, using a second fabric for regular LAN traffic required for the ESXi server (for example, virtual machine management network traffic). This example uses the following hardware environment:

- I/O modules – Four supported I/O modules—two on fabric A and two on fabric B to support redundancy and multipathing for failover
- Top-of-rack switch – Minimum of two Dell Force10 S4810 switches—one for SAN (iSCSI) and one for LAN
- Blade Servers – Four Dell PowerEdge 12th generation blade servers with NDCs on each server to enable redundancy and multipathing in the ESXi cluster (you can add additional servers after creating the cluster)
- Converged Network Adapters (CNAs) – On each server, Network Daughter Cards (NDCs) for iSCSI and LAN connectivity, and two mezzanine cards for expansibility
- Networks (VLANs) – One iSCSI VLAN, one public VLAN, one vMotion VLAN, and one hypervisor management VLAN
- Storage Type – Dell EqualLogic PS6110 ESX datastore on a single volume
- Operating System/Hypervisor – ESXi 5.0 or 5.1



**NOTE:** Use cases offer an example of one possible way to configure Active System Manager for a specific deployment type. The hardware environment and values suggested for configuring devices and templates are recommendations based on best practices—not necessarily requirements. Make sure to use values that are appropriate for your specific environment.

## Prerequisites

Configure the networks that servers and chassis will use, and create storage volumes for booting from iSCSI.

1. [Add networks](#) to Active System Manager. These networks should be consistent with the VLANs available on the top-of-rack (ToR) switch.
  - a) Add one custom SAN (iSCSI) network (set the VLAN ID to any number between 1 - 4000 and 4021 - 4094). This VLAN must be consistent with the iSCSI VLAN configured on the ToR switch for storage access.
  - b) Add one Public LAN with the VLAN ID set to any number between 1 - 4000 and 4021 - 4094. This VLAN must be consistent with the iSCSI VLAN configured on the ToR switch for networking.
  - c) Add one Private LAN with the VLAN ID set to any number between 1 - 4000 and 4021 - 4094. This network will be used for vMotion traffic.
  - d) Add one Hypervisor Management network with the VLAN ID set to any number between 1 - 4000 and 4021 - 4094. This VLAN must be consistent with the iSCSI VLAN configured on the ToR switch for hypervisor management.
  - e) If using static IP addressing, add one Management Network to support servers and I/O modules.
2. On the storage device, create a storage volume for each server that will boot from iSCSI. Make sure these volumes are accessible by the network on which the servers are located. Also, install a server-compatible ESXi image on each volume.
3. Do one of the following:
  - (Recommended) If using static IP addresses, add an [IP address range](#) to the Management Network. Make sure to add a range that is large enough to support the total number of IP addresses you will need in the future.
  - If using DHCP, configure a DHCP server to assign IP addresses to servers and I/O modules.

## Configuring the Management Template

[Create a Management Template](#) with the following settings.

- **Device Access** → **IP Addressing** – Choose static (recommended) or DHCP addressing option.
- **Device Access** → **Credentials** – Create credentials for servers and I/O modules.
- **Networking** – It is not recommended to change the settings on this screen. Use the default settings, unless you have a very specific reason to do otherwise.

All other settings are optional. Configure them to meet the needs of your specific environment.

## Configuring The Chassis

After [discovering](#) the chassis, [configure](#) it with the following settings. Configuring the network fabrics prepares the I/O modules to carry diverged iSCSI and LAN network traffic.

- **Connectivity** → **Fabric A** – Select *SAN (iSCSI)* for the **Fabric Purpose**, and deselect **Customize networks for this fabric**.
- **Connectivity** → **Fabric B** – Select *All LAN* for the **Fabric Purpose**, and deselect **Customize networks for this fabric**.
- **Connectivity** → **Fabric C** – Do not select a fabric purpose.


- **Templates** – Select the Management Template configured for this use case.


All other settings are optional. Configure them to meet the needs of your specific environment.


## Configuring the Deployment Template

[Create](#) a Deployment Template with the following BIOS, RAID, network, and I/O module settings that will prepare the server and the chassis for ESXi installation.


- **BIOS** – Select **Processor Virtualization Technology** and **Execute Disable**.
- **RAID** – Deselect **Include RAID configuration in this template** (no RAID will be created or enabled for boot), since they will boot directly to iSCSI storage.
- **Networks** – Select [Enable Bandwidth Oversubscription](#) to enable setting a higher maximum bandwidth for each of the virtual NICs on a server, so that the total exceeds 100% of the network bandwidth available to the NIC port to which the virtual NIC is assigned. Use a physical partition for the virtual NIC mapping order. Additionally, create new virtual NIC configurations that will each correspond to a partition on the network adapter:
  - Virtual NIC 1 for iSCSI boot
    1. Select a **Connection Type** of *SAN (iSCSI)*.
    2. For the **Native VLAN**, select the iSCSI network created as a prerequisite in this use case.
    3. Enter *10 GB* for the **Maximum Bandwidth** and *1 GB* for the **Minimum Bandwidth**.
    4. Select **Redundancy** to configure an identical partition on the second network adapter.
    5. Select a **Virtual Identity Pool**.
 

 **NOTE:** You can [create a custom pool](#), if desired. Otherwise, select the default *Global* pool.
    6. For the network to associate with this virtual NIC configuration, select the iSCSI network created as a prerequisite in this use case.
  - Virtual NIC 2 for iSCSI data
    1. Select a **Connection Type** of *SAN (iSCSI)*.
    2. Do not select a **Native VLAN**.
    3. Enter *10 GB* for the **Maximum Bandwidth** and *9 GB* for the **Minimum Bandwidth**.
    4. Select **Redundancy**.
    5. Select a **Virtual Identity Pool**.
 

 **NOTE:** You can [create a custom pool](#), if desired. Otherwise, select the default *Global* pool.
    6. For the network to associate with this virtual NIC configuration, select the iSCSI network created as a prerequisite in this use case.
  - Virtual NIC 3 for public LAN
    1. Select a **Connection Type** of *LAN*.
    2. Do not select a **Native VLAN**.
    3. Enter *10 GB* for the **Maximum Bandwidth** and *6 GB* for the **Minimum Bandwidth**.
    4. Select **Redundancy**.
    5. Select a **Virtual Identity Pool**.
 

 **NOTE:** You can [create a custom pool](#), if desired. Otherwise, select the default *Global* pool.
    6. For the network to associate with this virtual NIC configuration, select the public LAN created as a prerequisite in this use case.
  - Virtual NIC 4 for vMotion traffic
    1. Select a **Connection Type** of *LAN*.


2. Do not select a **Native VLAN**.
3. Enter *10 GB* for the **Maximum Bandwidth** and *3 GB* for the **Minimum Bandwidth**.
4. Select **Redundancy**.
5. Select a **Virtual Identity Pool**.

 **NOTE:** You can [create a custom pool](#), if desired. Otherwise, select the default *Global* pool.

6. For the network to associate with this virtual NIC configuration, select the private LAN created as a prerequisite in this use case.

– Virtual NIC 5 for hypervisor management

1. Select a **Connection Type** of *LAN*.
2. Do not select a **Native VLAN**.
3. Enter *10 GB* for the **Maximum Bandwidth** and *1 GB* for the **Minimum Bandwidth**.
4. Select **Redundancy**.
5. Select a **Virtual Identity Pool**.

 **NOTE:** You can [create a custom pool](#), if desired. Otherwise, select the default *Global* pool.

6. For the network to associate with this virtual NIC configuration, select the iSCSI network you created as virtual NIC 1.

• **Boot Information** – Make the following selections, and add a storage connection:


- a. Select *SAN (iSCSI)*.
- b. For **Virtual Boot NIC**, select Virtual NIC 1 that you created for this use case.
- c. For **Initiator IP Address**, select *Static* or *DHCP*.
- d. [Add connection information](#) for the EqualLogic storage device. Enter 3260 for the **Port Number**, and do not enable authentication.

All other settings are optional. Review the boot sequence to make sure it is correct. Configure the other settings to meet the needs of your specific environment.


## Deploying Servers

On the **Templates** → **Deployment Templates** screen, select the Deployment Template created for this use case, and then click **Deploy**. [Complete the Deploy wizard](#) two times with the following settings:

- Deployment 1 – For **Server Selection**, select **Manual Server Selection**, and then select the four servers to which ESXi will be deployed. For each server, enter a **Target Identity** and **Boot LUN** (enter 0) for four of the preconfigured ESXi images created as a prerequisite in this use case.
- Deployment 2 – To add additional servers for expanded workload capacity, repeat the steps for Deployment 1, except with two servers instead of four.

 **NOTE:** It may be necessary to configure the storage device to permit access from the appropriate source identity (initiator IQN or IP) for each target LUN.

The servers are now ready to boot to the iSCSI volumes that are preconfigured with ESXi.

 **NOTE:** You must preconfigure an operating system image on each of the iSCSI volumes to which you are booting. Active System Manager does not support using an iDRAC boot image to boot any operating system installation media (for example, ESX, Windows, or RHEL) and install the operating system to the target iSCSI volumes.

# ESXi Using FCoE Datastores and Networking on Separate Fabric with FCoE Boot

The purpose of this use case is to FCoE boot to ESXi using a non-converged network fabric. This example uses the following hardware environment:

- I/O modules – Four Force10 I/O modules—two on fabric A and two on fabric B to support redundancy and multipathing for failover
- Top-of-rack switch – Two Nexus 5000 series and two Dell Force10 S4810 for LAN
- Blade Servers – Four Dell PowerEdge 12th generation blade servers with NDCs on each server to enable redundancy and multipathing in the ESXi cluster (you can add additional servers after creating the cluster)
- Converged Network Adapters (CNAs) – On each server, Network Daughter Cards (NDCs) for FCoE and LAN connectivity, and two mezzanine cards for expansibility
- Networks (VLANs) – One FCoE VLAN, one FCoE discovery VLAN, one public VLAN, one vMotion VLAN, and one hypervisor management VLAN
- Storage Type – Dell Compellent Series 40 ESX volume for datastore and a volume for boot mapped to separate LUNs
- Operating System/Hypervisor – ESXi 5.0 or 5.1

## Prerequisites

Configure the networks that servers and chassis will use, and create storage volumes for booting from FCoE.

1. [Add networks](#) to Active System Manager:
  - a) Add two SAN (FCoE) networks—one to act as the FCoE discovery VLAN or native FCoE VLAN (set the VLAN ID to 1) and one for the FCoE network (set the VLAN ID to any number between 1 - 4000 and 4021 - 4094). The VLAN should be consistent with other VLANs available on the ToR switch.
  - b) Add one private LAN with the VLAN ID set to any number between 1 - 4000 and 4021 - 4094. The VLAN should be consistent with other VLANs available on the ToR switch.
  - c) Add another private LAN with the VLAN ID set to any number between 1 - 4000 and 4021 - 4094. This network will be used for vMotion traffic.
  - d) Add one Hypervisor Management network with the VLAN ID set to any number between 1 - 4000 and 4021 - 4094.
  - e) If using static IP addressing, add one Management Network to support servers and I/O modules.
2. On the storage device, create a storage volume for each server that will boot from FCoE. Make sure these volumes are accessible by the network on which the servers are located. Also, install a server-compatible ESXi image on each volume.
3. Do one of the following:
  - (Recommended) If using static IP addresses, add an [IP address range](#) to the Management Network. Make sure to add a range that is large enough to support the total number of IP addresses you will need in the future.
  - If using DHCP, configure a DHCP server to assign IP addresses to servers and I/O modules.

## Configuring the Management Template

[Create a Management Template](#) with the following settings.

- **Device Access** → **IP Addressing** – Choose static (recommended) or DHCP addressing option.
- **Device Access** → **Credentials** – Create credentials for servers and I/O modules.

- **Networking** – It is not recommended to change the settings on this screen. Use the default settings, unless you have a very specific reason to do otherwise.

All other settings are optional. Configure them to meet the needs of your specific environment.

## Configuring the Chassis

After [discovering](#) the chassis, [configure](#) it with the following settings. Configuring the network fabrics prepares the I/O modules to carry converged FCoE and LAN network traffic.

- **Connectivity** → **Fabric A** – Select *SAN (FCoE)* for the **Fabric Purpose**, and deselect **Customize networks for this fabric**.
- **Connectivity** → **Fabric B** – Select *Private LAN* for the **Fabric Purpose**, and deselect **Customize networks for this fabric**.
- **Connectivity** → **Fabric C** – Do not select a fabric purpose.
- **Templates** – Select the Management Template configured for this use case.

All other settings are optional. Configure them to meet the needs of your specific environment.

## Configuring the Deployment Template

[Create](#) a Deployment Template with the following BIOS, RAID, network, and I/O module settings that will prepare the server and the chassis for ESXi installation.

- **BIOS** – Select **Processor Virtualization Technology** and **Execute Disable**.
- **RAID** – Deselect **Include RAID configuration in this template**, since they will boot directly to FCoE storage.
- **Networks** – Select [Enable Bandwidth Oversubscription](#) to enable setting a higher maximum bandwidth for each of the virtual NICs on a server, so that the total exceeds 100% of the network bandwidth available to the NIC port to which the virtual NIC is assigned. Use a physical partition for the virtual NIC mapping order. Additionally, create new virtual NIC configurations that will each correspond to a partition on the network adapter:

### – Virtual NIC 1 for FCoE boot

1. Select a **Connection Type** of *SAN (FCoE)*.
2. For the **Native VLAN**, select the native FCoE FIP-discovery VLAN (must be set to VLAN 1) created as a prerequisite in this use case to use for FCoE FIP-discovery.
3. Enter *10 GB* for the **Maximum Bandwidth** and *1 GB* for the **Minimum Bandwidth**.
4. Select **Redundancy** to configure an identical partition on the second network adapter.
5. Select a **Virtual Identity Pool**.



**NOTE:** You can [create a custom pool](#), if desired. Otherwise, select the default *Global* pool.

6. For the network to associate with this virtual NIC configuration, select the SAN (FCoE) network created as a prerequisite in this use case.

### – Virtual NIC 2 for FCoE data


1. Select a **Connection Type** of *SAN (FCoE)*.
2. Do not select a **Native VLAN**.
3. Enter *10 GB* for the **Maximum Bandwidth** and *9 GB* for the **Minimum Bandwidth**.
4. Select **Redundancy** to configure an identical partition on the second network adapter.
5. Select a **Virtual Identity Pool**.





**NOTE:** You can [create a custom pool](#), if desired. Otherwise, select the default *Global* pool.



6. For the network to associate with this virtual NIC configuration, select the SAN (FCoE) network created as a prerequisite in this use case.
- Virtual NIC 3 for virtual machine traffic
    1. Select a **Connection Type** of *LAN*.
    2. Do not select a **Native VLAN**.
    3. Enter *10 GB* for the **Maximum Bandwidth** and *6 GB* for the **Minimum Bandwidth**.
    4. Select **Redundancy** to configure an identical partition on the second network adapter.
    5. Select a **Virtual Identity Pool**.
 

 **NOTE:** You can [create a custom pool](#), if desired. Otherwise, select the default *Global* pool.
    6. For the network to associate with this virtual NIC configuration, select the private LAN created as a prerequisite in this use case.
  - Virtual NIC 4 for vMotion private LAN
    1. Select a **Connection Type** of *LAN*.
    2. Do not select a **Native VLAN**.
    3. Enter *10 GB* for the **Maximum Bandwidth** and *3 GB* for the **Minimum Bandwidth**.
    4. Select **Redundancy** to configure an identical partition on the second network adapter.
    5. Select a **Virtual Identity Pool**.
 

 **NOTE:** You can [create a custom pool](#), if desired. Otherwise, select the default *Global* pool.
    6. For the network to associate with this virtual NIC configuration, select the private LAN created as a prerequisite in this use case.
  - Virtual NIC 5 for hypervisor management
    1. Select a **Connection Type** of *LAN*.
    2. Do not select a **Native VLAN**.
    3. Enter *10 GB* for the **Maximum Bandwidth** and *1 GB* for the **Minimum Bandwidth**.
    4. Select **Redundancy** to configure an identical partition on the second network adapter.
    5. Select a **Virtual Identity Pool**.
 

 **NOTE:** You can [create a custom pool](#), if desired. Otherwise, select the default *Global* pool.
    6. For the network to associate with this virtual NIC configuration, select the Hypervisor Management network created as a prerequisite in this use case.
- **Boot Information** – Select *SAN (FCoE)* and select virtual NIC 1 as the virtual boot NIC.

All other settings are optional. Review the boot sequence to make sure it is correct. Configure the other settings to meet the needs of your specific environment.

## Deploying Servers

On the **Templates** → **Deployment Templates** screen, select the Deployment Template created for this use case, and then click **Deploy**. [Complete the Deploy wizard](#) two times with the following settings:

- Deployment 1 – For **Server Selection**, select **Manual Server Selection**, and then select the four servers to which ESXi will be deployed. For each server, enter a **Target Identity** and **Boot LUN** (enter 0) for four of the preconfigured ESXi images created as a prerequisite in this use case.
- Deployment 2 – To add additional servers for expanded workload capacity, repeat the steps for Deployment 1, except with two servers instead of four.



**NOTE:** It may be necessary to configure the storage device to permit access from the appropriate source identity (initiator IQN or IP) for each target LUN.

The servers are now ready to boot from the pre-configured volumes according to the prerequisites of this use case

## Red Hat Enterprise Linux Using iSCSI Datastores and Networking on Converged Fabric

The purpose of this use case is to boot a Red Hat Enterprise Linux (RHEL) deployment from the local RAID disks in servers, and enable the servers to utilize both iSCSI storage and networking on a converged iSCSI and LAN network. This example uses the following hardware environment:

- I/O modules – Two supported I/O modules for redundant converged iSCSI and LAN network
- Top-of-rack switch – Two Nexus 5000 series for converged iSCSI and LAN network
- Blade Servers – Two Dell PowerEdge 12th generation blade servers NDCs on each server to enable redundancy and multipathing in the cluster (you can add additional servers after creating the cluster)
- Converged Network Adapters (CNAs) – On each server, Network Daughter Cards (NDCs) for iSCSI and LAN connectivity
- Networks (VLANs) – One iSCSI VLAN, one iSCSI discovery VLAN, one public VLAN, one vMotion VLAN, and one hypervisor management VLAN
- Storage Type – Dell EqualLogic PS 6110 series
- Operating System/Hypervisor – Red Hat Enterprise Linux 6



**NOTE:** Use cases offer an example of one possible way to configure Active System Manager for a specific deployment type. The hardware environment and values suggested for configuring devices and templates are recommendations based on best practices—not necessarily requirements. Make sure to use values that are appropriate for your specific environment.

### Prerequisites

Configure the networks that servers and chassis will use, and prepare the images to use for hypervisor installation from iDRAC virtual media.

1. [Add networks](#) to Active System Manager:
  - a) Add one custom SAN (iSCSI) network with the VLAN ID set to any number between 1 - 4000 and 4021 - 4094 (static or DHCP).
  - b) Add one public LAN with the VLAN ID set to any number between 1 - 4000 and 4021 - 4094.
  - c) If using static IP addressing, add one Management Network to support servers and I/O modules.
2. Create an NFS or CIFS share that the Active System Manager virtual appliance can access. Place the RHEL 6 ISO image on the share.
3. Do one of the following:
  - (Recommended) If using static IP addresses, add an [IP address range](#) to the Management Network. Make sure to add a range that is large enough to support the total number of IP addresses you will need in the future.
  - If using DHCP, configure a DHCP server to assign IP addresses to servers and I/O modules.

## Configuring the Management Template

[Create](#) a Management Template with the following settings:

- **Device Access** → **IP Addressing** – Choose static (recommended) or DHCP addressing option.
- **Device Access** → **Credentials** – Create credentials for servers and I/O modules.
- **Networking** – It is not recommended to change the settings on this screen. Use the default settings, unless you have a very specific reason to do otherwise.

All other settings are optional. Configure them to meet the needs of your specific environment.

## Configuring the Chassis

After [discovering](#) the chassis, [configure](#) it with the following settings. Configuring the network fabrics prepares the I/O modules to carry converged iSCSI and LAN network traffic.

- **Connectivity** → **Fabric A** – Select *Converged* for the **Fabric Purpose**, and deselect **Customize networks for this fabric**.
- **Connectivity** → **Fabric B** – Do not select a fabric purpose.
- **Connectivity** → **Fabric C** – Do not select a fabric purpose.
- **Templates** – Select the Management Template configured for this use case.

All other settings are optional. Configure them to meet the needs of your specific environment.

## Configuring the Deployment Template

[Create](#) a Deployment Template with the following BIOS, RAID, network, and I/O module settings that will prepare the server and the chassis for Red Hat Enterprise Linux (RHEL) 6 installation.

- **BIOS** – Select **Integrated RAID Controller**, **Processor Virtualization Technology**, and **Execute Disable**.
- **RAID** – For PowerEdge M420 and M620 servers, select *RAID 0* or *RAID 1*. For PowerEdge M820 servers, select *RAID 5*.
- **Networks** – Select [Enable Bandwidth Oversubscription](#) to enable setting a higher maximum bandwidth for each of the virtual NICs on a server, so that the total exceeds 100% of the network bandwidth available to the NIC port to which the virtual NIC is assigned. Use a physical partition for the virtual NIC mapping order. Additionally, create new virtual NIC configurations that will each correspond to a partition on the network adapter:
  - Virtual NIC 1 to carry iSCSI VLAN traffic and use the native VLAN for untagged iSCSI discovery traffic
    1. Select a **Connection Type** of *SAN (iSCSI)*.
    2. For the **Native VLAN**, select the native iSCSI VLAN created as a prerequisite in this use case to use for iSCSI discovery.
    3. Enter *10 GB* for the **Maximum Bandwidth** and *7 GB* for the **Minimum Bandwidth**.
    4. Select **Redundancy** to configure an identical partition on the second network adapter.
    5. Select a **Virtual Identity Pool**.**NOTE:** You can [create a custom pool](#), if desired. Otherwise, select the default *Global/pool*.
    6. For the network to associate with this virtual NIC configuration, select the custom iSCSI network created as a prerequisite in this use case.
  - Virtual NIC 2 for Private LAN

1. Select a **Connection Type** of *LAN*.
2. Do not select a **Native VLAN**.
3. Enter *10 GB* for the **Maximum Bandwidth** and *1 GB* for the **Minimum Bandwidth**.
4. Select **Redundancy** to configure an identical partition on the second network adapter.
5. Select a **Virtual Identity Pool**.



**NOTE:** You can [create a custom pool](#), if desired. Otherwise, select the default *Global* pool.

6. For the network to associate with this virtual NIC configuration, select the Public LAN created as a prerequisite in this use case.

– Virtual NIC 3 for Public LAN

1. Select a **Connection Type** of *LAN*.
2. Do not select a **Native VLAN**.
3. Enter *10 GB* for the **Maximum Bandwidth** and *2 GB* for the **Minimum Bandwidth**.
4. Select **Redundancy** to configure an identical partition on the second network adapter.
5. Select a **Virtual Identity Pool**.



**NOTE:** You can [create a custom pool](#), if desired. Otherwise, select the default *Global* pool.

6. For the network to associate with this virtual NIC configuration, select the Public LAN created as a prerequisite in this use case.

- **Boot Information** – Select *iDRAC image boot (one time)* to boot the server from the RHEL 6 ISO staged on the NFS or CIFS share. Then, specify your **Share Type**, **Path**, and **Credentials** (if required).

All other settings are optional. Review the boot sequence to make sure it is correct. Configure the other settings to meet the needs of your specific environment.

## Deploying Servers

On the **Templates** → **Deployment Templates** screen, select the Deployment Template created for this use case, and then click **Deploy**. [Complete the Deploy wizard](#) with the following settings:

- **Server Selection** – Select **Manual Server Selection**, and then select the two servers to which Red Hat Enterprise Linux 6 will be deployed.
- **Deployment Settings** – No entries required

The servers are now ready to deploy Red Hat Enterprise Linux 6.

## Windows Server 2008 R2 Using FCoE Datastores and Networking on Converged Fabric

The purpose of this use case is to boot a Windows Server 2008 R2 deployment from the local RAID disks in servers, and enable the servers to utilize both FCoE storage and networking on a converged FCoE and LAN network. This example uses the following hardware environment:

- I/O modules – Two supported I/O modules for redundant converged FCoE and LAN network
- Top-of-rack switch – Two Nexus 5000 series for converged FCoE and LAN network
- Blade Servers – Two Dell PowerEdge 12th generation blade servers to use as an ESXi cluster (you can add additional servers after creating the cluster)
- Converged Network Adapters (CNAs) – On each server, Network Daughter Cards (NDCs) for FCoE and LAN connectivity

- Networks (VLANs) – One FCoE VLAN, one FCoE discovery VLAN, one public VLAN, one vMotion VLAN, and one hypervisor management VLAN
- Storage Type – Dell Compellent Series 40 Windows Server 2008 R2 datastore on a single volume
- Operating System/Hypervisor – Windows Server 2008 R2 SP2



**NOTE:** Use cases offer an example of one possible way to configure Active System Manager for a specific deployment type. The hardware environment and values suggested for configuring devices and templates are recommendations based on best practices—not necessarily requirements. Make sure to use values that are appropriate for your specific environment.

## Prerequisites

Configure the networks that servers and chassis will use, and prepare the images to use for hypervisor installation from iDRAC virtual media.

1. [Add networks](#) to Active System Manager. These networks should be consistent with the VLANs available on the top-of-rack (ToR) switch.
  - a) Add two SAN (FCoE) networks—one will act as the FCoE discovery VLAN or native FCoE VLAN (set the VLAN ID to 1) and one will be the FCoE network (set the VLAN ID to any number between 1 - 4000 and 4021 - 4094). These VLANs must be consistent with the FCoE networks used on the FCoE (ToR) switch and FCoE network.
  - b) Add one Public LAN with the VLAN ID set to any number between 1 - 4000 and 4021 - 4094. The VLAN should be consistent with other VLANs available on the ToR switch.
  - c) Add one Private LAN with the VLAN ID set to any number between 1 - 4000 and 4021 - 4094.
  - d) If using static IP addressing, add one Management Network to support servers and I/O modules.
2. Create an NFS or CIFS share that the Active System Manager virtual appliance can access. Place the Windows Server 2008 ISO image on the share.
3. Do one of the following:
  - (Recommended) If using static IP addresses, add an [IP address range](#) to the Management Network. Make sure to add a range that is large enough to support the total number of IP addresses you will need in the future.
  - If using DHCP, configure a DHCP server to assign IP addresses to servers and I/O modules.

## Configuring the Management Template

[Create a Management Template](#) with the following settings:

- **Device Access** → **IP Addressing** – Choose static (recommended) or DHCP addressing option.
- **Device Access** → **Credentials** – Create credentials for servers and I/O modules.
- **Networking** – It is not recommended to change the settings on this screen. Use the default settings, unless you have a very specific reason to do otherwise.

All other settings are optional. Configure them to meet the needs of your specific environment.

## Configure the Chassis

After [discovering](#) the chassis, [configure](#) it with the following settings. Configuring the network fabrics prepares the I/O modules to carry converged FCoE and LAN network traffic.

- **Connectivity** → **Fabric A** – Select *Converged* for the **Fabric Purpose**, and deselect **Customize networks for this fabric**.
- **Connectivity** → **Fabric B** – Do not select a fabric purpose.


- **Connectivity** → **Fabric C** – Do not select a fabric purpose.
- **Templates** – Select the Management Template configured for this use case.

All other settings are optional. Configure them to meet the needs of your specific environment.


## Configuring the Deployment Template

[Create](#) a Deployment Template with the following BIOS, RAID, network, and I/O module settings that will prepare the server and the chassis for Windows Server 2008 R2 installation.


- **BIOS** – Select **Integrated RAID Controller**, **Processor Virtualization Technology**, and **Execute Disable**.
- **RAID** – For PowerEdge M420 and M620 servers, select *RAID 0* or *RAID 1*. For PowerEdge M820 servers, select *RAID 5*.
- **Networks** – Select [Enable Bandwidth Oversubscription](#) to enable setting a higher maximum bandwidth for each of the virtual NICs on a server, so that the total exceeds 100% of the network bandwidth available to the NIC port to which the virtual NIC is assigned. Use a physical partition for the virtual NIC mapping order. Additionally, create new virtual NIC configurations that will each correspond to a partition on the network adapter:
  - Virtual NIC 1 to carry FCoE VLAN traffic and use the native VLAN for untagged FCoE discovery traffic
    1. Select a **Connection Type** of *SAN (FCOE)*.
    2. For the **Native VLAN**, select the native FCoE FIP-discovery VLAN ( must be set to VLAN 1) created as a prerequisite in this use case to use for FCoE FIP-discovery.
    3. Enter *10 GB* for the **Maximum Bandwidth** and *7 GB* for the **Minimum Bandwidth**.
    4. Select **Redundancy**.
    5. Select a **Virtual Identity Pool**.

 **NOTE:** You can [create a custom pool](#), if desired. Otherwise, select the default *Global* pool.

    6. For the network to associate with this virtual NIC configuration, select the custom FCoE network created as a prerequisite in this use case.
  - Virtual NIC 2 for Private LAN
    1. Select a **Connection Type** of *LAN*.
    2. Do not select a **Native VLAN**.
    3. Enter *10 GB* for the **Maximum Bandwidth** and *1 GB* for the **Minimum Bandwidth**.
    4. Select **Redundancy**.
    5. Select a **Virtual Identity Pool**.

 **NOTE:** You can [create a custom pool](#), if desired. Otherwise, select the default *Global* pool.

    6. For the network to associate with this virtual NIC configuration, select the Public LAN created as a prerequisite in this use case.
  - Virtual NIC 3 for Public LAN
    1. Select a **Connection Type** of *LAN*.
    2. Do not select a **Native VLAN**.
    3. Enter *10 GB* for the **Maximum Bandwidth** and *2 GB* for the **Minimum Bandwidth**.
    4. Select **Redundancy**.
    5. Select a **Virtual Identity Pool**.

 **NOTE:** You can [create a custom pool](#), if desired. Otherwise, select the default *Global* pool.

    6. For the network to associate with this virtual NIC configuration, select the Public LAN created as a prerequisite in this use case.

- **Boot Information** – Select *iDRAC image boot (one time)* to boot the server from the Windows Server 2008 R2 ISO staged on the NFS or CIFS share.

All other settings are optional. Review the boot sequence to make sure it is correct. Configure the other settings to meet the needs of your specific environment.

## Deploying Servers

On the **Templates** → **Deployment Templates** screen, select the Deployment Template created for this use case, and then click **Deploy**. [Complete the Deploy wizard](#) with the following settings:

- **Server Selection** – Select **Manual Server Selection**, and then select the two servers to which Windows Server 2008 R2 SP2 will be deployed.
- **Deployment Settings** – No entries required

The servers are now ready to deploy Windows Server 2008 R2 SP2.





# Troubleshooting

This chapter includes details for resolving common issues encountered in Active System Manager.

For additional support information, go to <http://support.dell.com/support/topics/topic.aspx/global/shared/support/prosupport/en/prosupport-software-contacts?c=us&l=en&s=biz>.

## Browser Errors

If users receive browser-based security warnings when logging into Active System Manager, then an administrator should [generate](#) and [upload](#) a valid SSL certificate to the virtual appliance. In addition to preventing security warnings, this encrypts data sent over the web to help ensure secure transmission, and provides authentication to make sure data is routed to its intended endpoint.

## Cannot Enable Or Disable DCB on Broadcom 57810 NIC

You cannot enable or disable Data Center Bridging (DCB) on a Broadcom 57810 NIC device from within Active System Manager. Instead, the device has an explicit setting for DCB, and when this setting is enabled, the device is considered to be in *willing* mode. To prevent certain DCB issues within the environment, only configure DCB from within the Broadcom 57810 device. The default factory setting for DCB is enabled.

## I/O Module Is Down On Active Deployment

Sometimes, a server deployment will succeed, even though the I/O module state indicates that a server-facing port is down. When this happens, the server will not have end-to-end connectivity to networks and/or storage.

The likely cause of this issue is that an administrator manually shut down the server-facing ports on the I/O module. To resolve the issue, check the port status, and execute the `no shutdown` command to change the port status to *UP*.

1. Log into the I/O module.
2. Enter these commands to change the port status:
 

```
IOM#en
IOM#configure
IOM(conf)#interface tengigabitethernet 0/1    (for server in slot 1)
IOM(conf-if-te-0/1)#no shutdown
IOM(conf-if-te-0/1)#end
```
3. Enter this command to verify the port status:
 

```
IOM#show interfaces status
```

## Deployment in an Error State

Sometimes, deployments will enter an *Error* state when they are in the process of being applied to a server, migrated, or deleted. A possible cause is that the virtual appliance rebooted while the deployment or deletion job was still in process. Specifically for migrations, a possible cause is that one of the servers is not ready for migration—for example, one of the servers is logged into a utility like Lifecycle Controller.

If the error occurred during deployment, then the server will be marked as *In Use*, even though the deployment is marked as *Error*. To resolve this issue, [delete](#) the deployment to return the server to a *Ready* state, and then [deploy](#) the server, again.

If the error occurred during migration, then the server and the deployment will both be marked as *Error*. To resolve this issue, [delete](#) the deployment to return the server to a *Ready* state, and then [deploy](#) the server, again.

If the deployment entered an *Error* state while it was being deleted, try to run the [delete](#) job again.

## Errors with QLogic Cards

Active System Manager, version 1.0 does not support QLogic cards. See [Hardware Requirements](#) for a list of all supported devices.

## Failed to Configure Server with Deployment Template

Sometimes, attempting to apply a Deployment Template to a server will result in the following error message:

```
Failed to configure server with Deployment Template. The job either took too long to finish, or the connection to the target server was lost. See the User Guide for troubleshooting information.
```

To resolve this issue, make sure you can issue a ping command from the Active System Manager subnet to the iDRAC IP address of the server experiencing the problem. Also, make sure the server's iDRAC console (or physical server console, if it can be accessed) is not stuck at an F1/F2 user confirmation prompt.

## Failed to Connect to I/O Module Services

Occasionally, Active System Manager will fail to connect to I/O module services. To resolve this issue, log into the Active System Manager virtual appliance console, and execute the following command to verify whether I/O module services are currently running. This command will also reset I/O module services, if needed.

```
/opt/dell/cim/bin/cimstatus.sh
```



**NOTE:** For details on how to log into the Active System Manager virtual appliance console, see the *Active System Manager Version 1.0.1 Quick Installation Guide*.

## Failed to Create Virtual Disk

This error can occur when a virtual disk already exists. To correct, delete the virtual disk using the iDRAC remote console.

1. Select **Power** → **Power Cycle System (cold boot)**.
2. After the system reboots, press <CTRL>+<R> when prompted.
3. On BIOS screen, select **Delete virtual disk**.
4. In the PERC H301 Mini BIOS Configuration Utility, press <F2>.
5. Select **Delete VD**.
6. Click **Yes** on the confirmation screen to delete the virtual disk.

## FlexAddress Not Available on a Server

Active System Manager does not support FlexAddress. For this reason, before a server is deployed, FlexAddress addressing is disabled. Active System Manager uses internally generated addresses for assignment to the system.

## I/O Module Unit Number Not Zero

All active I/O modules should have a unit number of zero (0). If the unit number is not zero, then there are two likely causes:

- Active System Manager failed to configure the I/O module when applying the Management Template.
- Active System Manager failed to configure ports when applying the Deployment Template to the server.

To resolve this issue, clear the NVRAM and startup configuration for the I/O module:

1. Log into the I/O module.
2. Delete all saved configurations by executing these commands:  

```
FTOS# delete startup-config
Proceed to delete startup-config [confirm yes/no]: yes
```
3. Reload the startup configuration by executing these commands:  

```
FTOS# reload
Proceed with reload [confirm yes/no]: yes
```
4. Stop at the second countdown for the boot prompt (the first countdown is for x-loader), and execute these commands to erase the NVRAM:  

```
BOOT_USER # enable admin
Password : <I/O module password>
BOOT_ADMIN # nvram erase
Are you sure (y/n)? : yes
Erasing NVRAM sectors....done
BOOT_ADMIN #
BOOT_ADMIN # exit
BOOT_USER #
```
5. Reboot the I/O module.

## Migrating Deployments

When migrating a deployment from one server to another, Active System Manager migrates the target identity, boot LUN, source identity, initiator IP address, and virtual MAC address. Active System Manager does not migrate any installed operating systems during this process.

## Operating System Security Patches for the Virtual Appliance

The Active System Manager virtual appliance runs on CentOS. At this time, it is not recommended to apply general security patches to the operating system, because they may cause system instability. If you have an urgent need to apply a specific security patch, contact Dell Support.

## Scheduled Inventory Jobs Failing

When a server or I/O module is physically removed from a chassis, Active System Manager updates the device status to *Offline* during the next inventory job. If you do not remove the device from Active System Manager, then scheduled and manual inventory jobs will fail for the device. To resolve this issue, remove the [server](#) or [I/O module](#) from Active System Manager.

## Server Not Found in Deploy Wizard

If a server does not display as expected on the **Server Selection** screen of the [Deploy wizard](#), then it is possible that Active System Manager is not aware of a physical change to the server's hardware components. Run an inventory job on the [server](#) to bring Active System Manager up to date.

## UEFI Mode Not Working As Expected

UEFI mode is not available in Active System Manager for FCoE and iSCSI networks. Additionally, UEFI mode may not work as expected for other network types, depending on the details associated with the configuration.

To resolve issues with UEFI not working as expected, change the **Boot Mode** on the **Boot Sequence** page of the Deployment Template to BIOS.

## Deploy Wizard Does Not Display Desired Chassis

If a chassis does not display as expected in the Deploy wizard, it is likely because the fabrics associated with the chassis are configured with [customized networks](#). When a new network is [added](#) from within a Deployment Template, chassis with customized network fabrics do not automatically display.

To resolve this issue, go to the **Devices** → **Chassis** screen, select the chassis, and then click **Configure**. In the Configure Chassis wizard, on the **Connectivity** page for the desired fabric, do one of the following:

- Select **Customize networks for this fabric** and [add the desired network](#).
- Deselect **Customize networks for this fabric**.

## Unresponsive User Interface in Internet Explorer 9

A sluggish or unresponsive Active System Manager user interface on Windows Server 2008 with Internet Explorer 9 is due to encrypted communication between the virtual appliance and managed servers. To resolve this issue, go to **Tools** → **Internet Options** in Internet Explorer. On the **Advanced** tab under **Security**, deselect the option **Do not save encrypted pages to disk**.

## Updated Virtual Appliance Does Not Display Changes

After [updating the virtual appliance](#), all users must clear the history (or temporary Internet files) in their Web browsers. Failing to do so may prevent changes from displaying in the Active System Manager user interface.

## Web Interface Time Out Causes Source Identity Information Conflict

In general, the Active System Manager web interface times out after 30 minutes.

When deploying multiple servers using the Deploy wizard, if the deployment will boot from iSCSI or FCoE, you must enter the **Target Identity** (iSCSI Qualified Name or WWPN) and **Boot LUN** on the **Deployment Settings** page. Then, you must enter that same information on the storage array before the Active System Manager web interface times out. Otherwise, you must restart the Deploy wizard, which will cause Active System Manager to generate new source identity information.

# COPYRIGHT AND PERMISSION NOTICE

Copyright © 1991–2012 Unicode, Inc. All rights reserved. Distributed under the Terms of Use in <http://www.unicode.org/copyright.html>.

Permission is hereby granted, free of charge, to any person obtaining a copy of the Unicode data files and any associated documentation (the "Data Files") or Unicode software and any associated documentation (the "Software") to deal in the Data Files or Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, and/or sell copies of the Data Files or Software, and to permit persons to whom the Data Files or Software are furnished to do so, provided that (a) the above copyright notice(s) and this permission notice appear with all copies of the Data Files or Software, (b) both the above copyright notice(s) and this permission notice appear in associated documentation, and (c) there is clear notice in each modified Data File or in the Software as well as in the documentation associated with the Data File(s) or Software that the data or software has been modified.

THE DATA FILES AND SOFTWARE ARE PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR HOLDERS INCLUDED IN THIS NOTICE BE LIABLE FOR ANY CLAIM, OR ANY SPECIAL INDIRECT OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THE DATA FILES OR SOFTWARE.

Except as contained in this notice, the name of a copyright holder shall not be used in advertising or otherwise to promote the sale, use or other dealings in these Data Files or Software without prior written authorization of the copyright holder.