

# Active Fabric Manager (AFM) User Guide 2.7



**Copyright © 2015 Dell Inc. All rights reserved.** This product is protected by U.S. and international copyright and intellectual property laws. Dell™ and the Dell logo are trademarks of Dell Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

2015 - 10

Rev. A01

# Contents

|   |           |
|---|-----------|
| <b>1 Introduction.....</b>  | <b>8</b>  |
| <b>2 Getting Started.....</b>   | <b>9</b>  |
| Designing and Deploying a Fabric.....   | 9         |
| <b>3 Supported Fabric Types.....</b>  | <b>11</b> |
| Key Considerations for Designing a Layer 3 with Resiliency (Routed VLT) Fabric..... | 12        |
| Gathering Useful Information for a Layer 3 with Resiliency (Routed VLT) Fabric..... | 13        |
| Conventional Core Versus Distributed Core.....                                      | 13        |
| Conventional Core.....  | 14        |
| Distributed Core.....   | 14        |
| Key Advantages.....   | 15        |
| Distributed Core Terminology .....  | 15        |
| Gathering Useful Information for a Distributed Core.....                            | 16        |
| Selecting a Layer 3 Distributed Core Fabric Design.....                             | 17        |
| VLT.....  | 22        |
| Multidomain VLT.....  | 23        |
| VLT Terminology.....  | 23        |
| VLT Fabric Terminology.....   | 23        |
| VLT Components.....   | 24        |
| Typical VLT Topology.....   | 24        |
| Key Considerations for Designing a Layer 2 VLT Fabric.....                          | 24        |
| Gathering Useful Information for a Layer 2 VLT Fabric.....                          | 25        |
| Selecting a Layer 2 and Layer 3 with Resiliency (Routed VLT) Fabric Design.....     | 26        |
| <b>4 Designing a Fabric.....</b>  | <b>45</b> |
| Network Deployment Summary .....  | 46        |
| Fabric Configuration Phases and States.....   | 46        |
| Switch Configuration Phases and States.....   | 47        |
| Operations Allowed in Each Fabric State.....  | 48        |
| Deployment Topology Use Cases.....  | 50        |
| Use Case 1: One-Tier Layer 2 Fabric.....  | 50        |
| Use Case 2: One-Tier Layer 3 with Resiliency (Routed VLT).....                      | 50        |
| Use Case 3: Two-Tier Layer 2 .....  | 50        |
| Use Case 4: Two-Tier Layer 3 Distributed Core.....                                  | 51        |
| Use Case 5: Two-Tier Layer 3 Resiliency (Routed VLT).....                           | 51        |
| Use Case 6: Three-Tier Layer 2.....   | 52        |
| Use Case 7: Three-Tier Layer 3 Resiliency (Routed VLT).....                         | 52        |

|  |           |
|--|-----------|
| Using the Fabric Design Wizard.....                                | 53        |
| Fabric Design — Fabric Name and Type.....                          | 54        |
| Standard Fabric.....   | 56        |
| Advanced Fabric Design.....  | 64        |
| Fabric Design — Viewing and Exporting Output.....                  | 84        |
| Output Types.....  | 85        |
| Fabric Design — Summary.....                                       | 88        |
| Using Existing Fabric Designs.....                                 | 89        |
| Importing an Existing Fabric Design.....                           | 89        |
| Editing and Expanding an Existing Fabric Design .....              | 89        |
| Deleting the Fabric.....   | 90        |
| Viewing the Wiring Plan.....                                       | 90        |
| <b>5 IOA Fabric Designer Wizard.....</b>                           | <b>91</b> |
| <b>6 Configuring and Deploying the Fabric.....</b>                 | <b>96</b> |
| Pre-Deployment Configuration.....                                  | 96        |
| IOA Fabric Pre-Deployment.....                                     | 97        |
| Layer 2 VLT/ Advanced Fabric Pre-Deployment.....                   | 97        |
| Layer 3 Distributed Core Fabric Pre-Deployment.....                | 97        |
| Layer 3 with Resiliency (Routed VLT) Pre-Deployment.....           | 98        |
| Device MAC Association.....  | 98        |
| IOA Pre-Deployment Wizard.....                                     | 104       |
| VLT/Distributed Core Pre-Deployment Wizard.....                    | 114       |
| Prerequisites.....   | 114       |
| Pre-Deployment Screens.....  | 114       |
| Protocol Configuration — Layer 2 VLT Fabric Designs.....           | 115       |
| Protocol Configuration — Layer 3 Distributed Core Fabric.....      | 123       |
| Protocol Configuration — Layer 3 with Resiliency (Routed VLT)..... | 126       |
| Pre-Deployment — Change Port Status.....                           | 137       |
| Pre-Deployment — Assign Switch Identities.....                     | 139       |
| Pre-Deployment — Management IP.....                                | 139       |
| Pre-Deployment — License Update.....                               | 140       |
| Pre-Deployment — SNMP and CLI Credentials.....                     | 140       |
| Pre-Deployment — Software Images .....                             | 141       |
| Pre-Deployment — DHCP Integration.....                             | 142       |
| Pre-Deployment — Summary.....                                      | 142       |
| Viewing the DHCP Configuration File.....                           | 143       |
| Deploying and Validating the Fabric.....                           | 143       |
| Deploying the Fabric.....  | 143       |
| Advanced Configuration.....  | 146       |
| Validation.....  | 148       |

|  |            |
|--|------------|
| Viewing Deployment and Validation Status.....              | 151        |
| Custom CLI Configuration.....                              | 151        |
| Managing Templates.....                                    | 151        |
| Associating Templates.....                                 | 152        |
| Adding a Switch-Specific Custom Configuration .....        | 154        |
| Viewing Custom Configuration History.....                  | 154        |
| <b>7 Discovering and Deploying an Existing Fabric.....</b> | <b>156</b> |
| Step 1: Discover an Existing Fabric.....                   | 157        |
| Step 2: View Discovery Status of an Existing Fabric.....   | 160        |
| Step 3: Deploy Discovered Fabric.....                      | 161        |
| <b>8 Viewing the Fabric.....</b>                           | <b>162</b> |
| Inventory Management.....                                  | 162        |
| Dashboard.....   | 163        |
| Network Topology.....                                      | 165        |
| Network Topology Tabular View.....                         | 165        |
| Network Topology Graphical View.....                       | 165        |
| Fabric Summary .....                                       | 167        |
| Displaying the Fabric in a Tabular View.....               | 167        |
| Displaying the Fabric in a Graphical View.....             | 167        |
| Switch Summary.....  | 168        |
| <b>9 Troubleshooting.....</b>                              | <b>169</b> |
| Ping, Traceroute, Telnet, and SSH.....                     | 169        |
| Validation Alarms.....                                     | 169        |
| Deployment and Validation Errors.....                      | 171        |
| Pre-deployment Errors.....                                 | 171        |
| Deployment Errors.....                                     | 172        |
| Validation Errors.....                                     | 174        |
| Switch Deployment Status Errors.....                       | 178        |
| Deployment Task Errors.....                                | 182        |
| TFTP/FTP Errors.....                                       | 184        |
| Validating Connectivity to the ToR.....                    | 184        |
| <b>10 Alerts and Events.....</b>                           | <b>185</b> |
| Current Active Alerts.....                                 | 185        |
| Historical Alerts and Event History.....                   | 187        |
| <b>11 Performance Management.....</b>                      | <b>189</b> |
| Network Performance Management.....                        | 189        |
| Fabric Performance Management.....                         | 190        |


|  |            |
|--|------------|
| Switch Performance Management.....                       | 190        |
| Port Performance Management.....                         | 191        |
| Detailed Port Performance Management.....                | 192        |
| Data Collection.....                                     | 193        |
| Threshold Settings.....                                  | 193        |
| Reports.....   | 195        |
| Creating New Reports.....                                | 195        |
| Editing Reports.....                                     | 197        |
| Running Reports.....                                     | 197        |
| Duplicating Reports.....                                 | 197        |
| Deleting Reports.....                                    | 197        |
| <b>12 Maintenance.....</b>                               | <b>198</b> |
| Using the AFM Virtual Appliance.....                     | 198        |
| Configuring the System.....                              | 199        |
| Configuring DNS Settings.....                            | 201        |
| Changing the AFM Superuser Password.....                 | 202        |
| Updating the AFM Server.....                             | 202        |
| Setting the AFM Software to the Next Restart.....        | 203        |
| Restarting AFM.....                                      | 203        |
| Rebooting the AFM Server (VM).....                       | 203        |
| Transferring Files.....                                  | 203        |
| Editing AFM Files.....                                   | 204        |
| Editing the config.properties AFM System File.....       | 205        |
| Uploading Switch Software Images.....                    | 206        |
| Backing up the AFM Database.....                         | 208        |
| Restoring the Database.....                              | 208        |
| Logging Out of the AFM Virtual Appliance.....            | 209        |
| Backing Up a Switch.....                                 | 210        |
| Restoring a Switch Configuration.....                    | 210        |
| Deleting a Backup Configuration.....                     | 210        |
| Editing a Description.....                               | 210        |
| Viewing and Editing the Switch Backup Configuration..... | 211        |
| Updating the Switch Software.....                        | 211        |
| Replacing an IOA Blade Switch.....                       | 212        |
| Replacing a Switch.....                                  | 212        |
| Step 1: Decommission a Switch.....                       | 212        |
| Step 2: Replacing a Switch.....                          | 213        |
| Step 3: Deploy Replacement Switch.....                   | 214        |
| Updating AFM.....  | 214        |
| <b>13 Jobs.....</b>                                      | <b>215</b> |

|  |            |
|--|------------|
| Displaying Job Results.....                    | 215        |
| Scheduling Jobs.....                           | 215        |
| Switch Backup.....                             | 216        |
| Switch Software Image Updates.....             | 216        |
| Switch Software Image Activation.....          | 217        |
| Scheduling Switch Software Updates.....        | 217        |
| Activating Standby Partition Software.....     | 218        |
| Scheduling a Back Up Switch Configuration..... | 219        |
| <b>14 Administration.....</b>                  | <b>220</b> |
| Administrative Settings.....                   | 220        |
| Active Link Settings.....                      | 220        |
| CLI Credentials.....                           | 222        |
| Client Settings.....                           | 222        |
| Data Retention Settings.....                   | 223        |
| DHCP Server Settings.....                      | 223        |
| NTP Server Settings.....                       | 223        |
| SMTP Email.....                                | 223        |
| SNMP Configuration.....                        | 224        |
| Syslog Server IP Addresses.....                | 224        |
| System Information.....                        | 224        |
| TFTP/FTP Settings.....                         | 224        |
| Managing User Accounts.....                    | 225        |
| Adding a User.....                             | 226        |
| Editing a User.....                            | 227        |
| Deleting a User.....                           | 227        |
| Unlocking a User.....                          | 228        |
| Changing Your Password.....                    | 228        |
| Managing User Sessions.....                    | 228        |
| Audit Log.....                                 | 229        |
| Updating the Server.....                       | 230        |
| <b>15 Technical Support.....</b>               | <b>231</b> |
| Accessing Dell License Portal .....            | 231        |
| Contacting Dell Technical Support.....         | 231        |

# Introduction


Active Fabric Manager (AFM) is a network automation and orchestration tool with a graphical user interface (GUI) that allows you to design, build, deploy, and optimize a Layer 3 distributed core, Layer 3 with Resiliency (Routed VLT), and Layer 2 VLT fabric for your current and future capacity requirements. This tool helps you simplify network operations, automate tasks, and improve efficiency in the data center.

Use AFM to monitor performance at the network, fabric, switch, and port level or display additional performance statistics through AFM using a Dell OpenManage Network Manager (OMNM) server. It automates common network management operations and provides advanced network element discovery, remote configuration management, and system health monitoring to proactively alert network administrators to potential network problems. OMNM provides SOAP-based web services to provide integration with non-Dell products. AFM supports Dell Networking S4048-ON, S3048-ON, S4810, S4820T, S55, S60, S5000, S6000, IOA blade, MXL blade, N20XX series, N30XX series, N40XX series, Z9500, and Z9000 (standard mode only) switches.

 **NOTE:** Before you begin, review the [Getting Started](#) page. To learn how to install AFM, including instructions on completing the Initial Setup, refer to the *Active Fabric Manager Deployment Guide*.



# Getting Started

 **NOTE:** To view this document in AFM, select the **User Guide** option from the **Help** drop-down menu in the upper right.

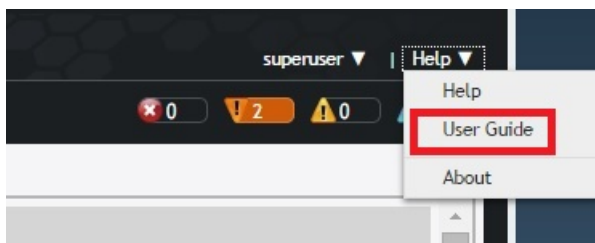


Figure 1. Help Menu — User Guide

## Designing and Deploying a Fabric

This section provides an overview of the steps required to design and deploy a fabric, including the information you need before you begin.

After completing the installation, configure AFM using the **Getting Started** configuration wizard on the **Home > Getting Started** screen. AFM automatically launches this wizard after you complete the installation process. The **Getting Started** configuration wizard provides launch points for designing, pre-deploying, and deploying the fabric. With this wizard, you can also [edit and expand an existing fabric design](#) , [import an existing design](#), and [discover an existing fabric](#).

To design and deploy a Layer 2 VLT, Layer 3 distributed core fabric, or Layer 3 with Resiliency (Routed VLT)

1. Gather useful information.

Related links.

- [Gather Useful Information for Layer 2 VLT Fabric](#)
- [Gathering Useful Information for a Layer 3 Distributed Core Fabric.](#)
- [Gathering Useful Information for a Layer 3 with Resiliency \(Routed VLT\) Fabric](#)

2. Design the fabric.

Related links for designing a Layer 2 VLT fabric:

- [Overview of VLT](#)
- [Key Considerations for Designing a VLT Fabric](#)
- [Selecting a Layer 2 VLT and Layer 3 with Resiliency \(Routed VLT\) Fabric Design](#)


Related links for designing a Layer 3 distributed core fabric:


- [Overview of a Distributed Core](#)
- [Terminology](#)

- [Selecting a Distributed Core Design](#)

Related links for designing a Layer 3 with Resiliency (Routed VLT):

- [Key Considerations for Designing Layer 3 with Resiliency \(Routed VLT\)](#)
  - [Selecting a Layer 2 VLT and Layer 3 with Resiliency \(Routed VLT\) Fabric Design](#)
3. Build the physical network.
  4. Configure the following settings:
    - [TFTP/FTP](#)
    - [SNMP](#)
    - [CLI Credentials](#)
  5. [Prepare the Fabric for Deployment](#)
  6. [Deploy and Validate the Fabric](#)
  7. Validate the deployed fabric against the fabric design.
  8. Monitor the fabric health and performance. Refer to [Performance Management](#).

 **NOTE:** To provision the fabric, enter the Dell Networking operating system user's CLI credentials and enable the configuration credential for all the switches in the fabric. For information, refer to [CLI Credentials](#).

 **CAUTION:** Reset any pre-deployed switches to factory settings. Switches must be in Bare Metal Provision (BMP) mode.

## Supported Fabric Types

The fabric design wizard defines the basic configuration for a Layer 2 VLT, Layer 3 distributed core, and Layer 3 with Resiliency (Routed VLT) fabric.

- Use the Layer 3 distributed core fabric for large fabric deployments. For information about distributed core fabrics, refer to [Conventional Core Versus Distributed Core](#) and [Selecting a Layer 3 Distributed Core Fabric Design](#).
- Use the Layer 2 VLT fabric for workload migration over virtualized environments. For information about Layer 2 fabrics, refer to [VLT](#) and [Selecting a Layer 2 VLT and Layer 3 with Resiliency \(Routed VLT\) Fabric Design](#).
- Use the Layer 3 with Resiliency (Routed VLT) fabric to extend equal cost multipathing capabilities. For information about supported tiers, refer to [Selecting a Layer 2 VLT and Layer 3 with Resiliency \(Routed VLT\) Fabric Design](#).
- Use the IOA fabric design wizard to design a Layer 2 fabric with an I/O Aggregator (IOA) blade switch in a M1000e chassis. For more information about the IOA Fabric Design Wizard, refer to [IOA Fabric Design Wizard](#).

For more information on supported topologies, refer to [Deployment Topology Use Cases](#). For information about tiers, refer to [Standard Fabric Design – Deployment Topology](#).

To design a fabric based on current or prospective capacity requirements, use the fabric design wizard at the **Network > Configure Fabric > Design New Fabric** screen. When you start AFM, the **Getting Started** configuration wizard in the **Welcome to Active Fabric Manager** screen starts automatically.

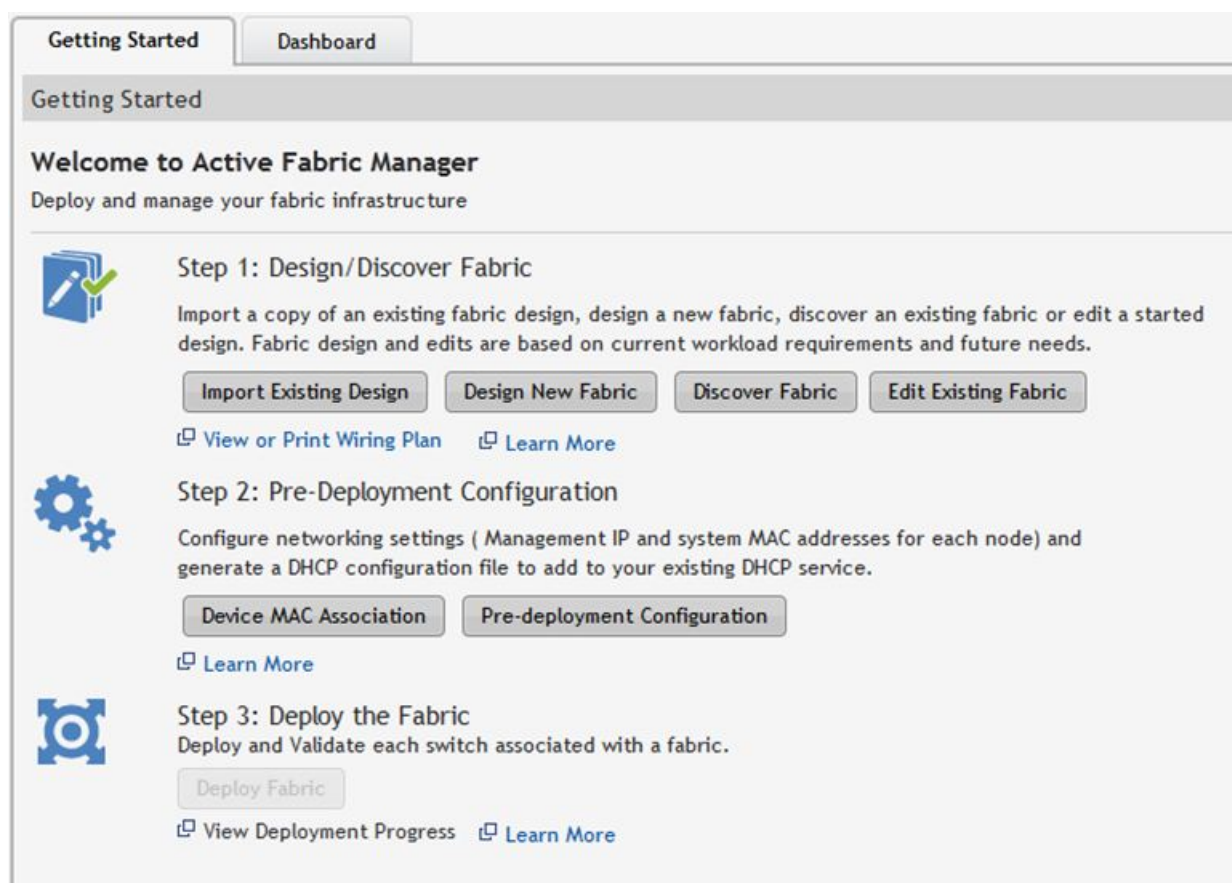


Figure 2. Getting Started Tab

## Key Considerations for Designing a Layer 3 with Resiliency (Routed VLT) Fabric

To extend equal cost multipathing capabilities, use the Layer 3 with Resiliency (Routed VLT) fabric. When designing a Layer 3 with Resiliency (Routed VLT) fabric, consider the following:

- You can deploy up to 10 fabric designs. However, the fabric designs do not communicate with each other.
- AFM manages Dell Networking S4810, S4820T, S6000, Z9000, and Z9500 switches.


**NOTE:** If you are using a deployed switch, reset the factory settings. The switch must be in BMP mode.

For more information on BMP, refer to [DHCP Integration](#) and the *Configuration Guide* for the Dell Networking S4810, S4820T, S6000, Z9000, and Z9500 switches.

The number and type of switches in a Layer 3 with Resiliency (Routed VLT) fabric are based on the following:

- The number of current uplinks (at least two) and downlinks for the access switches.

- The number of planned edge ports (future uplinks and downlinks) for the access switches.
- Whether the access switches need to act as a ToR or access.
- Fabric interlink bandwidth (the links between the aggregation and access switches).
- Downlinks (1 GB, 10 GB, or 40 GB).
- The fabric interlink bandwidth (10 GB or 40 GB) is fixed and based on the fabric type.

 **NOTE:** If you do not specify additional links for future expansion in the fabric design in the **Bandwidth and Port Count** screen, you can only expand the downlinks on the existing fabric.

For information on how to expand a fabric, refer to [Editing and Expanding an Existing Fabric Design](#). For information about tiers, refer to [Standard Fabric Design – Deployment Topology](#) and [Deployment Topology Use Cases](#).

## Gathering Useful Information for a Layer 3 with Resiliency (Routed VLT) Fabric

Gather the following useful information for a Layer 3 with Resiliency (Routed VLT) fabric before you begin:

- Obtain the CSV file with the system MAC addresses, Service Tag, and serial numbers for each Dell-provided switch, or manually enter this information.
- Obtain the location of the switches, including the rack and row number, from the network administrator or network operator.
- Obtain the remote Trivial File Transfer Protocol (TFTP) / File Transfer Protocol (FTP) address from the network administrator or network operator. To specify a TFTP/FTP site, go to the **Administration > Settings > TFTP/FTP** screen. For information about which software packages to use, refer to the Release Notes.
- Download the software image for each type of switch in the fabric. Each type of switch within the fabric must use the same version of the software. Place the software images on the TFTP/FTP site so that the switches can install the appropriate Dell Networking OS software image and configuration file.
- Obtain the Dynamic Host Configuration Protocol (DHCP) server address for the fabric from your DHCP network administrator or network operator. If a remote DHCP server is not available, AFM also provides local DHCP. The DHCP server must be in the same subnet as the switches.

After you power cycle the switches, the switches communicate with the DHCP server to obtain a management IP Address based on the system MAC Address. The DHCP server contains information about where to load the correct software image configuration file for each type of switch from the TFTP/FTP site during BMP. For information about BMP, refer to [DHCP Integration](#).

- Obtain the pool of IP addresses for the management port for each switch in the fabric.
- Obtain an even number of IP addresses for the uplink configuration from the ISP service. The uplink port number range is based on the selected bandwidth (10 GB or 40 GB).
  - For 10 GB uplink bandwidth, AFM supports 2–32 uplinks.
  - For 40 GB uplink bandwidth, AFM supports 2–8 uplinks.
- Obtain IP addresses or VLAN IDs for the downlink configuration of the server or ToR connection.
- Gather protocol configuration for uplinks and downlinks.

## Conventional Core Versus Distributed Core

This section describes the differences between a conventional core and a distributed core.

## Conventional Core

A conventional core is a three-tier network that is typically chassis-based and is composed of the following:

- **Core** — The core layer routes traffic to and from the Internet and the extranet. High availability, which provides redundancy and resiliency, requires chassis-based core routers.
- **Aggregation layer** — The aggregation layer connects with top of rack (ToR) switches and aggregates the traffic into fewer high-density interfaces such as 10GbE or 40GbE. This layer aggregates the traffic to the core layer.
- **Access layer (ToR)** — The access layer typically contains ToRs. A ToR is a small form-factor switch that sits on top of the rack and allows all the servers in the rack to be cabled into the switch. A ToR has a small 1–2 rack unit (RU) form factor.

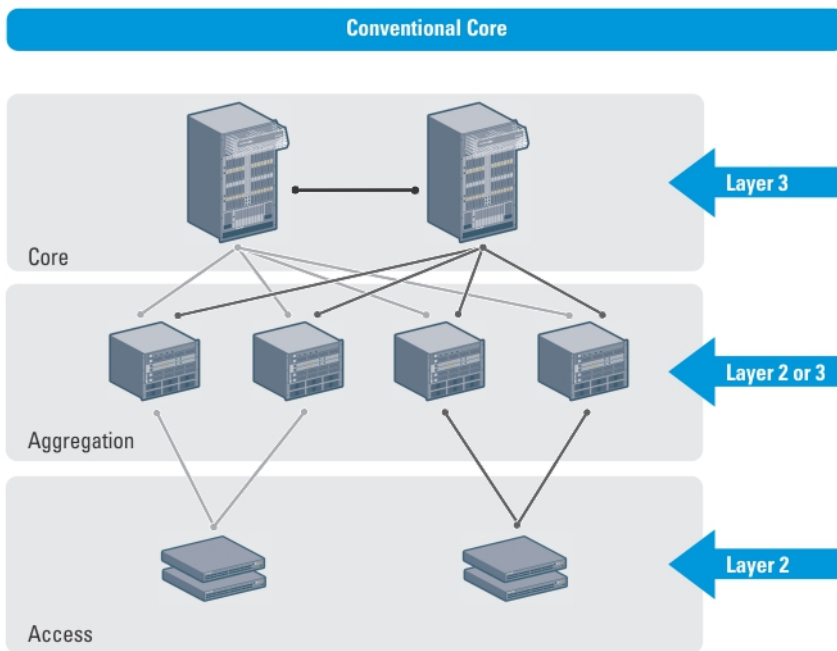
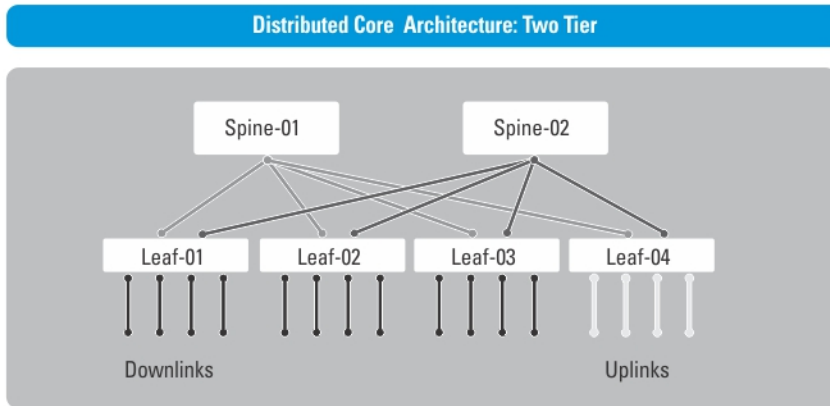


Figure 3. Conventional Core


## Distributed Core

A distributed core is a two-tier architecture composed of multiple interconnected switches, providing a scalable, high-performance network that replaces the traditional core and aggregation layers in a conventional core. Switches are arranged as spines and leaves. The spines in the fabric connect the leaves using a routing protocol. The leaves' edge ports connect to the switches, ToR switches, servers, other devices, and the WAN. The spines move traffic bidirectionally between the leaves to provide redundancy and load balancing. Collectively, the spine and leaf architecture forms the distributed core fabric.

This two-tier network design allows traffic to move more efficiently in the core and at a higher bandwidth with lower latencies than most traditional three-tier networks. Since there is no single point of failure that can disrupt the entire fabric, the distributed core architecture is more resilient and there is less impact on the network if a link or node failure occurs. AFM views the distributed core as one logical switch.



**Figure 4. Distributed Core Architecture: Two-Tier**

 **NOTE:** There are no uplinks on the spines. All the leaves have downlinks. Configure the uplink in the first two leaves.

## Key Advantages

The key advantages of a distributed core architecture are:

- Simplified fabric
- Higher bandwidth
- Highly resilient
- Higher availability
- Low power consumption
- Less cooling
- Lower latency
- Lower cost
- Less rack space
- Easier to scale

## Distributed Core Terminology

The following terms are unique to the design and deployment of a Layer 3 distributed core fabric.

- **Leaf** — A switch that connects switches, servers, storage devices, or top-of-rack (TOR) elements. The role of the leaf switches is to provide access to the fabric. The leaf switch connects to all of spines above it in the fabric.
- **Spine** — A switch that connects to the leaves switches. The role of the spine is to provide an interconnect to all the leaves switches. All the ports on the spine switches are used to connect the leaves, various racks together. The spines provide load balancing and redundancy in the distributed core. There are no uplinks on the spines.
- **Edge ports** — The uplinks and downlinks on the leaves.
- **Uplinks** — An edge port link on the first two leaves in the distributed core fabric that connects to the edge WAN, which typically connects to an internet server provider (ISP). The uplink can also connect to a router gateway or an external switch.
- **Downlinks** — An edge port link that connects the leaves to the data access layer; for example, servers or ToR elements.

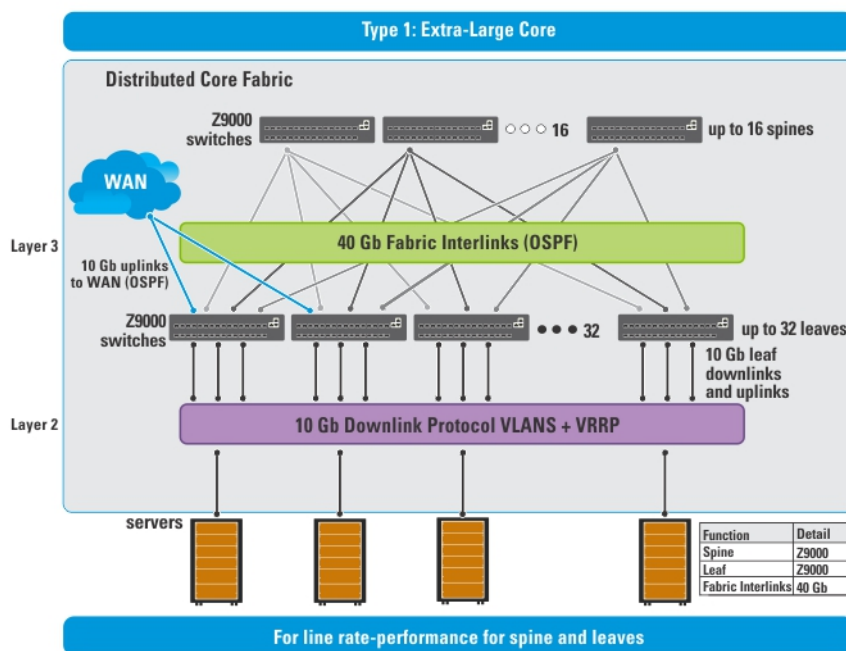
**NOTE:** Specify an even number of uplinks. The minimum number of uplinks is two. One uplink is for redundancy.

- **Fabric Interlinks** – Links that connect the spines to the leaves. The fabric interlink bandwidth is fixed: 10 GB or 40 GB.
- **Fabric over-subscription ratio** – Varies the maximum number of available interconnect links. This ratio determines the number of fabric interlinks (the number of communication links between the spine and leaf devices). The specified ratio depends on the bandwidth, throughput, and edge port requirements. The interlink over-oversubscription ratio does not come off the edge port downlinks.

As you increase the fabric over-subscription ratio:

- The total number of ports for the downlinks increases.
- The number of interconnect links from the leaves to the spines decreases.
- The maximum number of available ports increases.

For non-blocking (line rate) between the leaves and spines, select the 1:1 fabric over-subscription ratio. This ratio is useful when you require a large amount of bandwidth but not many ports. The following image illustrates a distributed core fabric.



**NOTE:** The AFM does not configure or manage anything beyond the distributed core fabric.

**Figure 5. Extra-Large Core**

**NOTE:** In a single distributed fabric, all the leaves can act as a non-ToR or as a ToR, not both at the same time.

## Gathering Useful Information for a Distributed Core

Gather the following useful information for a Layer 3 distributed core fabric before you begin:

- The comma-separated values (CSV) file that contains the system media access control (MAC) addresses, Service Tag, and serial numbers for each switch provided from Dell manufacturing or manually enter this information
- The location of the switches, including the rack and row number from your network administrator or network operator



- The Remote Trivial File Transfer Protocol (TFTP) or File Transfer Protocol (FTP) address from your network administrator or network operator. To specify a TFTP/FTP site, go to **Administration > Settings > TFTP/FTP** screen. For information about which software packages to use, refer to the Release Notes.
- The software image for each type of switch in the fabric. Each type of switch must use the same version of the software image within the fabric. Place the software images on the TFTP or FTP site so that the switches can install the appropriate FTOS software image and configuration file.
- The Dynamic Host Configuration Protocol (DHCP) server address for the fabric from your DHCP network administrator or network operator. If a remote DHCP server is not available, AFM also provides a local DHCP server. The DHCP server must be in the same subnet where the switches are located. After you power cycle the switches, the switches communicate with the DHCP server to obtain a management IP address based on the system MAC address. The DHCP server contains information about where to load the correct software image configuration file for each type of switch from the TFTP/FTP site during BMP. For information about BMP, see [DHCP Integration](#).
- The pool of IP addresses for the management port for each switch in the fabric
- The IP addresses (must be an even number) for the uplink configuration from the ISP service. The uplink port number range is based on whether a 10 GB or 40 GB bandwidth is selected
  - For a 10 GB bandwidth, AFM supports 2–32 uplinks.
  - For a 40 GB bandwidth, AFM supports 2–8 uplinks.
- The IP addresses for the downlink configuration for connecting to the server or ToR.
- The IP addresses for the fabric link configuration for the spine and leaf switches.
- The protocol configuration for uplinks, downlinks and fabric link configuration

## Selecting a Layer 3 Distributed Core Fabric Design

For large fabric deployments, use the Layer 3 distributed core fabric. AFM supports the following distributed core fabric designs:

- [Type 1: Extra Large Core Fabric](#)
- [Type 2: Large Distributed Core Fabric](#)
- [Type 3: Medium Distributed Core Fabric](#)
- [Type 4: Small Distributed Core Fabric](#)

To select the appropriate Layer 3 distributed core fabric design, use the following table as a guide. For more information about a Layer 3 distributed core, see:

- [Overview of a Distributed Core](#)
- Key Core Design Considerations


For a Layer 3 distributed core topology, select the **Layer 3** option in the Design Wizard on the **Deployment Topology** screen. For information about distributed core fabric, refer to [Conventional Core Versus Distributed Core](#).

**DL BW** — Downlink Bandwidth

**UL BW** — Uplink Bandwidth

**FLBSL** — Fabric Link bandwidth between the spine and leaf

**MND** — Maximum number of downlinks

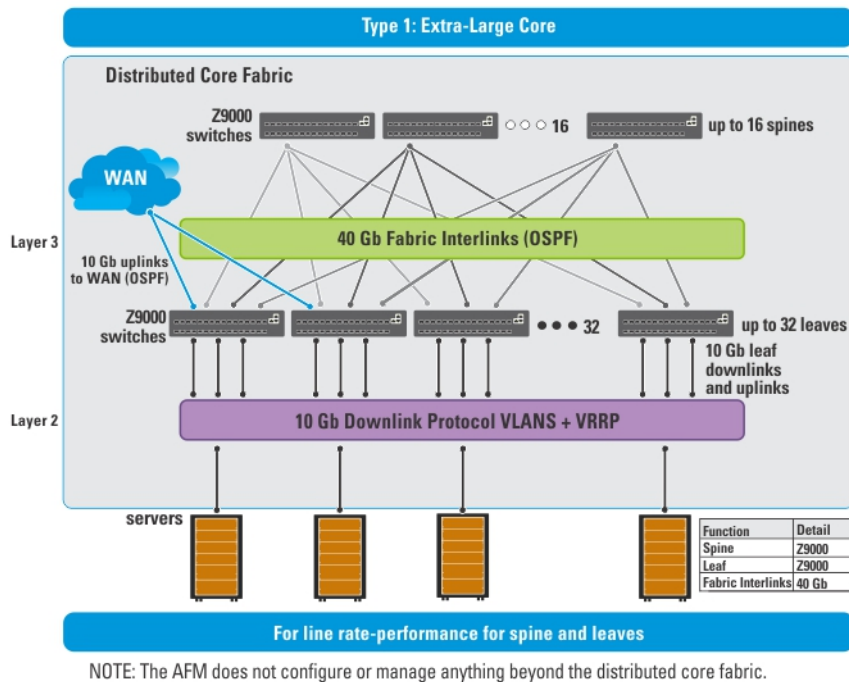
 **NOTE:** The maximum number of downlinks is based on two uplinks.

**Table 1. 2 Tier Layer 3 Distributed Core Topologies**

| Type                     | OS Ratio | DL BW | MND  | Maximum # of Spines | Maximum # of Leafs | UL BW | FLBSL | Possible Topologies (Spine and Leaf) |
|--------------------------|----------|-------|------|---------------------|--------------------|-------|-------|--------------------------------------|
| Type 1- Extra Large Core | 1:1      | 10G   | 2046 | 16                  | 32                 | 10G   | 40G   | Z9000/Z9000 or S6000/S6000           |
| Type 2- Large Core       | 1:1      | 10G   | 2046 | 32                  | 64                 | 10G   | 10G   | S4810/S4810                          |
| Type 3- Medium Core      | 3:1      | 10G   | 766  | 4                   | 32                 | 10G   | 10G   | S4810/S4810                          |
| Type 3- Medium Core      | 4:1      | 10G   | 1662 | 3                   | 32                 | 10G   | 40G   | Z9000/S4810 or S6000/S4810           |
| Type 4- Small Core       | 5:1      | 10G   | 894  | 2                   | 8                  | 10G   | 10G   | S4810/S4810                          |
| Type 4- Small Core       | 3:1      | 10G   | 1534 | 4                   | 16                 | 10G   | 40G   | Z9000/S4810 or S6000/S4810           |

**Type 1: Extra Large Distributed Core Fabric**

With a Type 1: Extra Large Distributed Core fabric design, the Z9000 or S6000 spines connect to the Z9000 or S6000 leaves at a fixed 40 GB line rate. The maximum number of leaves is based on the maximum number of ports on the spine (for example, 32 ports for the Z9000, as shown in the following figure).



**Figure 6. Type 1: Extra Large Distributed Core Fabric Design**

Use the Type 1: Extra Large Distributed Core fabric design when:

- The line rate-performance with a fabric oversubscription ratio of 1:1 between the spines and leaves.
- The current and planned uplinks and downlinks on the leaves for the distributed core is less than or equal to 2048 ports.

For redundancy, each leaf in a large core design can connect 2–16 spines. The Type 1: Extra Large Distributed Core Design uses a 1:1 spine-to-leaf ratio. As a result, the maximum number of spines for this design is 16 and the maximum number of leaves is 32.

Each Z9000 or S6000 leaf for the Type 1: Extra Large Distributed Core design has the following:

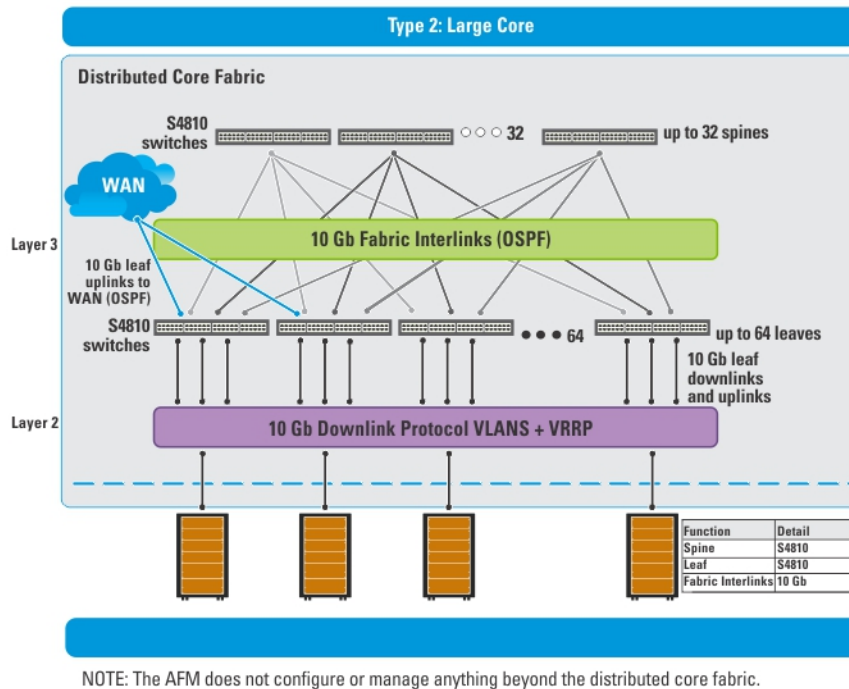
- 640 Gigabits of fabric interlink (fabric links) maximum capacity to the Spine (16 x 40 GB)
- 48 ports for server connectivity and WAN connectivity (10 GB)

### Type 2: Large Distributed Core Fabric

Use the Type 2: Large Distributed Core fabric design when:

- You require a 10 GB fabric interlink (fabric links) bandwidth between the spines and leaves.
- The current and planned uplinks and downlinks on the leaves for the fabric is less than or equal to 2048 ports.
- The leaves act as a switch or ToR-leaf switch. Within the ToR, the downlink protocol can be either **VLAN** or **VLAN and LAG**.

With a Type 2: Large Distributed Core fabric design, the S4810 spines connect to the S4810 leaves at a fixed rate of 10 GB. The maximum number of spines is 32 and the maximum number of leaves is 64, as shown in the following figure.



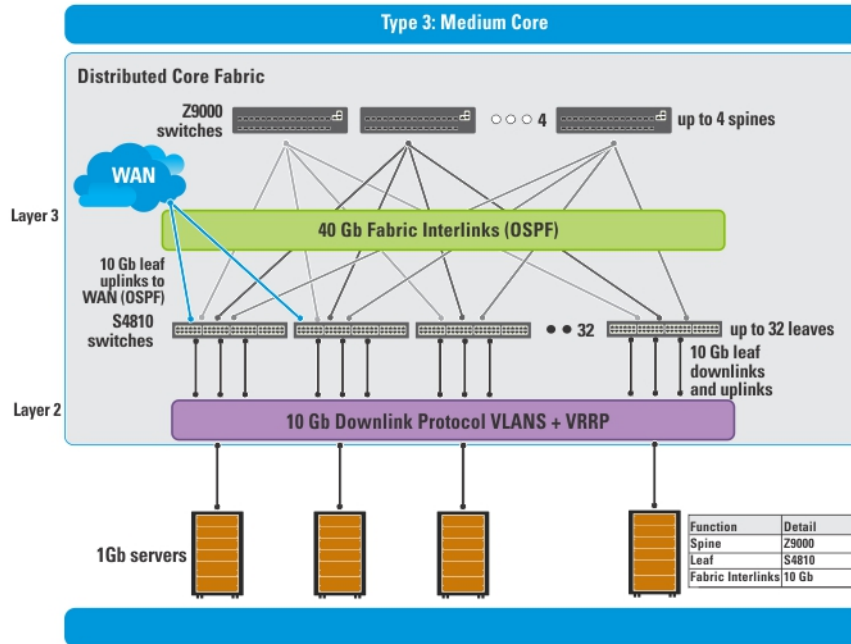
**Figure 7. Type 2: Large Distributed Core Fabric Design**

Each S4810 leaf for the Type 2: Large Distributed Core fabric design has the following:

- 40 GB of fabric interlink (fabric links) maximum capacity to the spine (4x 10 GB)
- 32 ports are used for fabric links (10 GB) and 32 ports are used for the downlinks (10 GB)

### Type 3: Medium Distributed Core Fabric

With a Type 3: Medium Distributed Core design, the Z9000 spines (S6000 spines) connect to the S4810 leaves at a fixed 40 GB line rate as shown in the following figure. The maximum number of leaves is based on the maximum number of ports on the spine (for example, 32 ports for the Z9000). The maximum number of spines is 16 and the maximum number of leaves is 32, as shown in the following illustration. This illustration shows a networking system architecture in a data center as a distributed core fabric containing a set of ToRs that connect to servers, storage devices, and network appliances (such as load balancers or network security appliances). You can run application services, network services, and network security services either on physical machines or virtual machines.



NOTE: The AFM does not configure or manage anything beyond the distributed core fabric.

**Figure 8. Type 3: Medium Distributed Core Fabric Design**

Use the Type 3: Medium Distributed Core design if:

- You require a 40 GB fabric interlink (fabric links) bandwidth between the spines and leaves.
- The current and planned uplinks and downlinks on the leaves for your distributed core fabric are less than or equal to 1536 ports.
- The leaves act as a switch or ToR-leaf switch. Within the ToR, the protocol can be either **VLAN** or **VLAN and LAG**.

Each Z9000 spine (S6000 spine) for the Type 3: Medium Distributed Core design has the following:

- 640 Gigabit of interlink (fabric links) maximum capacity to the spine (16 x 40 GB)
- 640 Ethernet ports for WAN connectivity (10 Gig)

Each S4810 leaf for the Type 3: Medium Distributed Core design has the following:

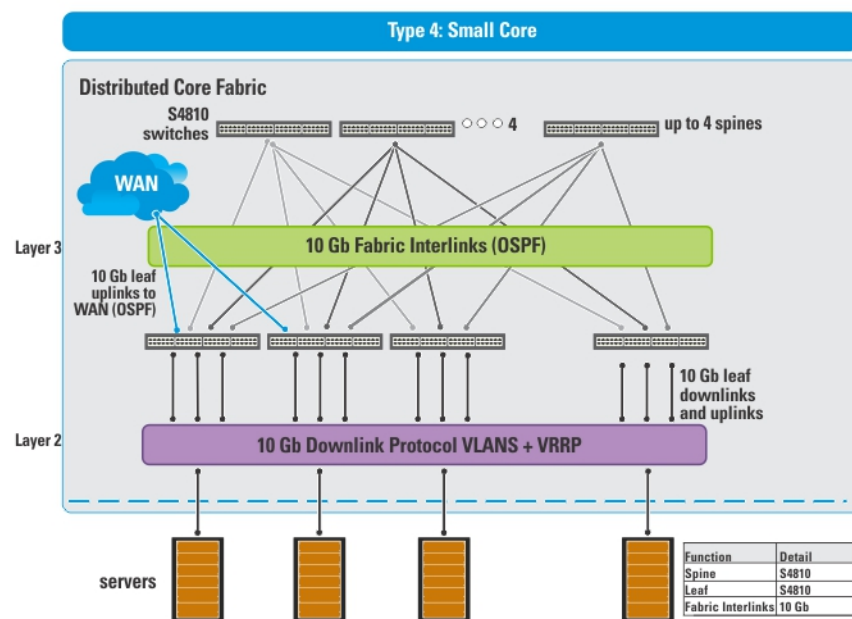
- 160 GB of interlink (fabric links) maximum capacity to the spine (4x 40 GB)
- 48 Ethernet ports for WAN connectivity (10 GB)

#### **Type 4: Small Distributed Core Fabric**

Use the Type 4: Small Distributed Core design when:

- You require a fabric interlink (fabric links) bandwidth between the spines and leaves of 10 GB.
- The current and planned uplinks and downlinks on the leaves for your core are less than or equal to 960 ports.
- The maximum port count for a Type 4: Small Distributed Core fabric with an OS ratio of 3:1 is 768. For an OS ratio of 5:1, the maximum port count is 896.
- The leaves act as a switch or ToR-leaf switch. Within the ToR, the downlink protocol can be either **VLAN** or **VLAN and LAG**.

With a Type 4: Small Distributed Core fabric design, the S4810 spines connect to the S4810 leaves at a fixed 10 GB. The maximum number of spines is 4 and the maximum number of leaves is 16, as shown in the following figure.



**Figure 9. Type 4: Small Distributed Core Fabric Design**

Each S4810 leaf for the Type 4: Small Distributed Core design has the following:

- 16 ports of fabric interlink (fabric links) port capacity to the spine (10 GB)
- 48 Ethernet downlinks (10 GB)
- 60 Ethernet ports for servers per node and WAN connectivity (10 GB)

## VLT


Virtual link trunking (VLT):

- Allows a single device to use a LAG across two upstream devices
- Eliminates ports blocked due to Spanning Tree Protocol (STP)
- Provides a loop-free topology
- Uses all available uplink bandwidth
- Provides fast convergence if either the link or a device fails
- Optimized forwarding with Virtual Router Redundancy Protocol (VRRP)
- Provides link-level resiliency
- Assures high availability


VLT allows physical links between two chassis to appear as a single virtual link to the network core or other switches such as Edge, Access or Top of Rack (ToR). VLT provides Layer 2 multipathing, creates redundancy through increased bandwidth, and enables multiple parallel paths between nodes and load-balancing traffic where alternative paths exist. VLT reduces the role of STP:

- by allowing LAG terminations on two separate distribution or core switches

- by supporting a loop-free topology, similar to how STP prevents any initial loops that may occur prior to VLT being established

 **NOTE:** After VLT is established, RSTP may be used to prevent loops from forming with new links that are incorrectly connected and outside the VLT domain.

For information about VLT, refer to the *Dell Networking Configuration Guide* for the S4048–ON, S3048–ON, S4810, S6000, or the Z9000, or refer to [Selecting a Layer 2 and Layer 3 with Resiliency \(Routed VLT\) Fabric Design](#).

 **NOTE:**  
Dell Networking recommends that you do not enable stacking and VLT simultaneously.

If both are enabled at the same time, unexpected behavior occurs.

## Multidomain VLT

A multidomain VLT (mVLT) configuration connects two different VLT domains in a standard Link Aggregation Control protocol (LACP) LAG to form a loop-free Layer 2 topology in the aggregation layer. This configuration supports up to four units, increasing the number of available ports and enabling dual redundancy for VLT. For more information about mVLT deployments, refer to [Selecting a Layer 2 VLT and Layer 3 with Resiliency \(Routed VLT\) Fabric Design](#).

## VLT Terminology

- **Virtual link trunk (VLT)** — The combined port channel between an attached device and the VLT peer switches.
- **VLT backup link** — The backup link that monitors the health of VLT peer switches. The backup link sends configurable periodic messages (also known as keep-alive messages) between VLT peer switches.
- **VLT interconnect (VLTi)** — The link used to synchronize states between the VLT peer switches. Both ends of the link must use 10 GB or 40 GB interfaces.
- **VLT domain** — Includes both VLT peer devices, the VLT interconnect, and all port channels connected to the attached VLT devices. It is also associated with the configuration mode used to assign VLT global parameters.
- **VLT peer device** — One of a pair of devices that are connected with to the port channel specified as the VLTi.

## VLT Fabric Terminology

The following terms are unique to the design and deployment of a Layer 2 VLT fabric.

- **Core** — A switch that connects to aggregation switches. The role of the core is to provide an interconnect to all the aggregation switches. All ports on the core switch connect to the aggregation switches and racks.
- **Access** — A switch that connects switch, servers, storage devices, or top-of-rack (TOR) elements. The role of the access switch is to provide connectivity to the fabric. The access switch connects to all of aggregation switches above it in the fabric.
- **Aggregation** — A switch that connects to access switches. The role of the aggregation layer is to provide an interconnect to all the access switches. All the ports on the aggregation switches are used to connect the access, various racks together. The aggregation switch provides redundancy.
- **Edge ports** — The uplinks on the aggregation and downlinks on the access.
- **Uplinks** — An edge port link on the first two aggregation switches in the VLT fabric that connects to outside the fabric.

- **Downlinks** — An edge port link that connects the access switches to the access layer. For example, servers or ToR elements.
- **Fabric Interlinks (Fabric Links)** — The fabric interlink bandwidth is fixed: 10 GB or 40 GB.
  - For a one-tier fabric, fabric interlinks connect a pair of aggregation switches.
  - For a two-tier fabric, fabric interlinks connect the aggregation switches to the access switches.
  - For a three-tier fabric, fabric interlinks connect the core, aggregation, and access switches together.

## VLT Components

VLT peer switches have independent management planes. A VLT interconnect (VLTi) between the VLT chassis maintains synchronization of Layer 2 and Layer 3 control planes across the two VLT peer switches. The VLTi uses either 10 GB or 40 GB ports on the switch.

A separate backup link maintains heartbeat messages across an out-of-band (OOB) management network. The backup link ensures that node failure conditions are correctly detected and are not incorrectly identified as VLTi failures by the software. VLT ensures that local traffic on a chassis does not traverse the VLTi and takes the shortest path to the destination using direct links.

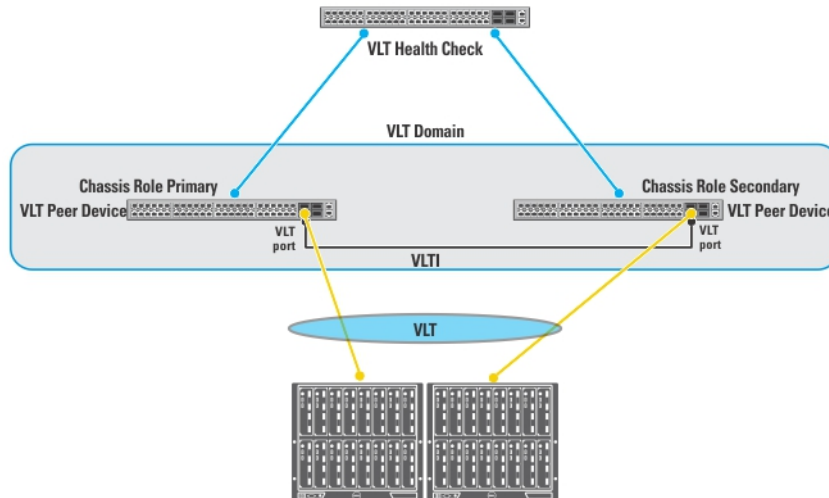


Figure 10. VLT Components

## Typical VLT Topology


The VLT domain uses VLTi links between VLT peers and VLT port-channels to connect to a single access switch, a switch stack, a server supporting LACP on its NIC, or another VLT domain. The backup-link connects through the OOB management network. Some hosts can connect through the non-VLT ports.

## Key Considerations for Designing a Layer 2 VLT Fabric

Use the Layer 2 VLT fabric for workload migration over virtualized environments. When designing the Layer 2 VLT fabric, consider the following:

- You can deploy up to 10 fabrics. However, the fabrics do not communicate with each other.
- For a VLT fabric, AFM manages Dell Networking S4810 and S55 switches.




 **CAUTION:** If you are already using a deployed switch, reset the factory settings. The switch must be in BMP mode.

For more information on BMP, refer to [DHCP Integration](#) and the *Configuration Guide* for the Dell Networking OS.

The number and type of switches in a VLT fabric are based on the following:

- The number of current uplinks (at least two) and downlinks for the access switches.
- The number of planned edge ports (future uplinks and downlinks) for the access switches.
- Whether the access switch needs to act as a switch or ToR.
- Fabric interlink bandwidth (the links between the aggregation and access switches).
- The number of available 1 GB, 10 GB, or 40 GB downlinks.
- The fabric interlink bandwidth (10 GB or 40 GB) is static and based on the fabric type.

 **NOTE:** If you do not specify additional ports in the fabric design for future expansion in the **Bandwidth and Port Count** screen, you can only expand the downlinks on the existing fabric.

For information on how to expand a fabric, see [Editing and Expanding an Existing Fabric Design](#).

## Gathering Useful Information for a Layer 2 VLT Fabric

Gather useful information for a Layer 2 VLT fabric before you begin:

- The CSV file Dell provides that contains the system MAC addresses, Service Tag and serial numbers for each switch or manually enter this information.
- The location of the switches, including the rack and row number, from your network administrator or network operator.
- The remote Trivial File Transfer Protocol (TFTP) / File Transfer Protocol (FTP) address from your network administrator or network operator. To specify a TFTP/FTP site, go to **Administration > Settings > TFTP/FTP** screen. For information about which software packages to use, refer to the Release Notes.
- The software image for each type of switch in the fabric. Each switch type within the fabric must use the same version of the software. Place the software images on the TFTP/FTP site so that the switches can install the appropriate Dell Networking OS software image and configuration file.
- The Dynamic Host Configuration Protocol (DHCP) server address to use for the fabric from your DHCP network administrator or network operator. If a remote DHCP server is not available, AFM also provides local DHCP. The DHCP server must be in the same subnet as the switches. After you power cycle the switches, the switches communicate with the DHCP server to obtain a management IP Address based on the system MAC Address. The DHCP server contains information about where to load the correct software image configuration file for each type of switch from the TFTP/FTP site during BMP. For information about BMP, refer to [DHCP Integration](#).
- The pool of IP addresses for the management port for each switch in the fabric.
- The IP addresses (must be an even number) for the uplink configuration from the ISP service. The uplink port number range is based whether a 10 GB or 40 GB bandwidth is selected.
  - For a 10 GB bandwidth, AFM supports 2–32 uplinks.
  - For a 40 GB bandwidth, AFM supports 2–8 uplinks.
- The IP addresses or VLAN ID for the downlink configuration to connect to the server or ToR.
- The protocol configuration for uplinks and downlinks.

## Selecting a Layer 2 and Layer 3 with Resiliency (Routed VLT) Fabric Design

For workload migration in virtualized environments, use a Layer 2 VLT fabric design. To extend equal cost multipath capabilities, use the Layer 3 with Resiliency (Routed VLT) fabric .

AFM supports the following Layer 2 VLT and Layer with 3 with Resiliency (Routed VLT) fabric designs:

- One and Two Tier ToR 10 Gb for Layer 2 LAN/SAN for iSCSI Topologies
- One and Two Tier ToR 10 Gb for Layer 2 LAN/SAN for Fibre Channel Topologies
- One Tier for 10 Gb and 40 Gb ToR for Layer 2 and Layer 3 Resiliency (Routed VLT)
- Two Tier and Three Tier Topologies for 1 Gb ToR VLT Deployment for Layer 2 and Layer 3 with Resiliency (Routed VLT)
- 10 Gb or 40 Gb ToR (mVLT)
- Two and Three Tier 10 Gb ToR (mVLT) Deployment Topologies for Layer 2 or Layer 3 with Resiliency
- Three Tier Topologies for a 10 Gb or 40 Gb ToR (mVLT) Deployment Layer 2 or Layer 3 with Resiliency (Routed VLT)
- Two and Three Tier MXL Blade Topologies for Layer 2 and Layer 3 with Resiliency (Routed VLT)
- 10 Gb Blade Switch (MXL) VLT Deployment

For more information about VLT, refer to the following sections:

- [Overview of VLT](#)
- [Getting Started](#)

### One and Two Tier ToR 10 Gb for Layer 2 LAN/SAN for iSCSI Topologies

**Table 2. One Tier ToR Layer LAN/SAN for iSCSI Topologies**

| DL BW | UL BW | UL Port Range | iSCSI Port Range | DL Port Range | AVC     | Possible Topologies |        |
|-------|-------|---------------|------------------|---------------|---------|---------------------|--------|
|       |       |               |                  |               |         | Aggregation         | Access |
| 10G   | 10G   | 2 - 32        | 2 - 8            | 1 - 108       | 2 * 40G | S4810               | NA     |
| 10G   | 40G   | 2 - 4         | 2 - 8            | 1 - 102       | 2 * 40G | S4810               | NA     |

**DL** = Downlink

**DL BW** = Down Link Bandwidth

**UL BW** = Uplink Bandwidth

**UL** = Uplink

**AVC** = Aggregation VLTi Capacity

**Table 3. Two Tier ToR Layer 2 LAN/SAN for iSCSI Topologies**

| Uplink Port Range | iSCSI Port Range | Downlink Port Range | Aggregation VLTi Capacity | Access VLTi Capacity | FL BW AA | Possible Topologies |        |
|-------------------|------------------|---------------------|---------------------------|----------------------|----------|---------------------|--------|
|                   |                  |                     |                           |                      |          | Aggregation         | Access |
| 2 - 32            | 2 - 8            | 71 - 3410           | 2 * 40G                   | NA                   | 20G      | S4810               | S4810  |
| 2 - 4             | 2 - 8            | 101 - 3224          | 2 * 40G                   | NA                   | 20G      | S4810               | S4810  |
| 2 - 32            | 2 - 8            | 71 - 2916           | 2 * 40G                   | 2 * 40G              | 20G      | S4810               | S4810  |
| 2 - 4             | 2 - 8            | 101 - 2808          | 2 * 40G                   | 2 * 40G              | 20G      | S4810               | S4810  |
| 2 - 32            | 2 - 8            | 71 - 2970           | 2 * 40G                   | 2 * 40G              | 20G      | S4810               | S4810  |
| 2 - 4             | 2 - 8            | 101 - 2808          | 2 * 40G                   | 2 * 40G              | 20G      | S4810               | S4810  |

**FL BW AA** = Fabric Link Bandwidth between Aggregation & Access

**Table 4. Two Tier MXL for Layer 2 LAN/SAN for iSCSI Topologies**

| Uplink Port Range | Uplink Bandwidth | Deployment Type               | iSCSI Port Range | MXL Blade Pairs Range | FL BW AA | Possible Topologies |        |
|-------------------|------------------|-------------------------------|------------------|-----------------------|----------|---------------------|--------|
|                   |                  |                               |                  |                       |          | Aggregation         | Access |
| 2 - 32            | 10G              | Basic                         | 2 - 8            | 2 - 27                | 20G      | S4810               | MXL    |
| 2 - 4             | 40G              | Basic                         | 2 - 8            | 2 - 26                | 20G      | S4810               | MXL    |
| 2 - 32            | 10G              | Stacking                      | 2 - 8            | 2 - 27                | 40G      | S4810               | MXL    |
| 2 - 4             | 40G              | Stacking                      | 2 - 8            | 2 - 26                | 40G      | S4810               | MXL    |
| 2 - 32            | 10G              | MXL - intraChassis resiliency | 2 - 8            | 2 - 27                | 20G      | S4810               | MXL    |
| 2 - 4             | 40G              | MXL - intraChassis resiliency | 2 - 8            | 2 - 26                | 20G      | S4810               | MXL    |

**FL BW AA** = Fabric Link Bandwidth between Aggregation & Access

## One and Two Tier ToR 10 Gb for Layer 2 LAN/SAN for Fibre Channel Topologies

Table 5. One Tier LAN/SAN Layer 2 for Fibre Channel – 10 Gb Downlinks

| Downlink Bandwidth | Uplink Bandwidth | Downlink Port Range | Aggregation VLTi Capacity | Possible Aggregation Topologies |
|--------------------|------------------|---------------------|---------------------------|---------------------------------|
| 10 Gb              | 10 Gb            | 1 - 86              | 2 * 40G                   | S5000                           |
| 10 Gb              | 40 Gb            | 1 - 80              | 2 * 40G                   | S5000                           |

Table 6. Two Tier LAN/SAN Layer 2 for Fibre Channel – 10 Gb Downlinks

| DL BW | UL BW | Deployment Type | Downlink Port Range | AVC     | Access VLTi Capacity | FL BW AA | Possible Aggregation Topologies |        |
|-------|-------|-----------------|---------------------|---------|----------------------|----------|---------------------------------|--------|
|       |       |                 |                     |         |                      |          | Aggregation                     | Access |
| 10 Gb | 10G   | Basic           | 87 - 2268           | 2 * 40G | NA                   | 20G      | S4810                           | S5000  |
| 10 Gb | 40G   | Basic           | 81 - 2184           | 2 * 40G | NA                   | 20G      | S4810                           | S5000  |
| 10 Gb | 10G   | Resiliency      | 87 - 2750           | 2 * 40G | 2 * 40G              | 20G      | S4810                           | S5000  |
| 10 Gb | 40G   | Resiliency      | 81 - 2600           | 2 * 40G | 2 * 40G              | 20G      | S4810                           | S5000  |

**DL BW** = Downlink Bandwidth

**UL BW** = Uplink Bandwidth

**FL BW AA** = Fabric Link Bandwidth between Aggregation & Access

## One Tier for 10 Gb and 40 Gb ToR for Layer 2 and Layer 3 Resiliency (Routed VLT)

Table 7. One Tier for 10 Gb and 40 Gb ToR for Layer 2 and Layer 3 Resiliency (Routed VLT)

| DL BW | UL BW | Downlink Port Range | Aggregation VLTi Capacity | Possible Aggregation Topologies |
|-------|-------|---------------------|---------------------------|---------------------------------|
| 10 Gb | 10 Gb | 1 - 110             | 2 * 40 Gb                 | S4810 or S4820T                 |
| 10 Gb | 40 Gb | 1 - 104             | 2 * 40 Gb                 | S4810 or S4820T                 |
| 40 Gb | 10 Gb | 1 - 59              | 2 * 40 Gb                 | Z9000 or S6000                  |
| 40 Gb | 40 Gb | 1 - 58              | 2 * 40 Gb                 | Z9000 or S6000                  |

**DL** = Downlink

**DL BW** = Downlink Bandwidth

**UL BW** = Uplink Bandwidth

## Two Tier and Three Tier Topologies for 1 Gb ToR VLT Deployment for Layer 2 and Layer 3 with Resiliency (Routed VLT)

In a 1 Gb ToR VLT Deployment fabric design, the S4810 aggregation switches connect to access switches at 10 Gb. The maximum number of VLT aggregation is two switches and the maximum number of VLT access switches is based on the number of uplinks and downlinks in the fabric. With this topology, the downlinks connect to access S55 or S60 switches using a 1 Gb bandwidth.

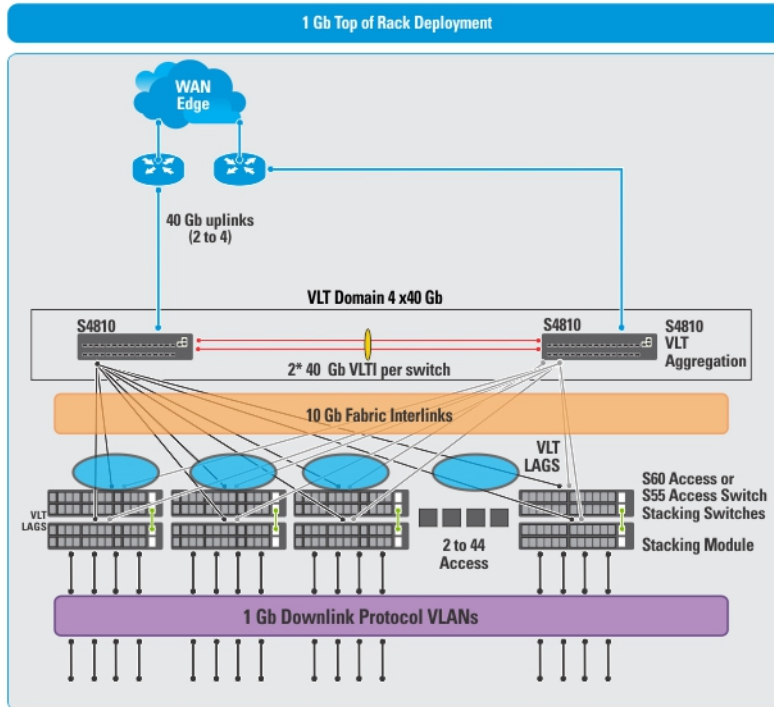


Figure 11. 1 Gb ToR VLT Deployment

**Important:** All the VLT aggregation switches must be same model type for aggregation; for example, S4810. On the VLT access, you must configure the same model type.

**AVG** = Aggregation VLTi Capacity

**DL** = Downlink

**DL BW** = Down Link Bandwidth

**FL BW AA** = Fabric Link Bandwidth between Aggregation & Access

**UL BW** = Uplink Bandwidth

**BW** = Bandwidth

Use the following table as guideline to select the appropriate two tier Layer 2 VLT or Layer 3 with Resiliency (Routed VLT) fabric design for a 1 Gb ToR VLT deployment.



**NOTE:** With a Layer 2 VLT fabric, the uplinks come from the first two switches on the aggregation side. For information about tiers, see [Standard Fabric Design – Deployment Topology](#).

**Table 8. Two Tier (1 Gb Downlinks)**

| DL BW | ULBW  | Type     | DL Port Range | AVG       | Access VLTi Capacity | FL BW A & A | Possible Topologies |                     |
|-------|-------|----------|---------------|-----------|----------------------|-------------|---------------------|---------------------|
|       |       |          |               |           |                      |             | Aggregation         | Access              |
| 1 Gb  | 10 Gb | Stacking | 1 - 2640      | 2 * 40 Gb | NA                   | 40 Gb       | S4810               | S60<br>(12G or 24G) |
| 1 Gb  | 10 Gb | Stacking | 1 - 2640      | 2 * 40 Gb | NA                   | 40 Gb       | S4810               | S55 (12G )          |
| 1 Gb  | 40 Gb | Stacking | 1 - 2496      | 2 * 40 Gb | NA                   | 40 Gb       | S4810               | S60<br>(12G or 24G) |
| 1 Gb  | 40 Gb | Stacking | 1 - 2496      | 2 * 40 Gb | NA                   | 40 Gb       | S4810               | S55<br>(12G )       |
| 1 Gb  | 10 Gb | Basic    | 1 - 2640      | 2 * 40 Gb | NA                   | 20 Gb       | S4810               | S60                 |
| 1 Gb  | 10 Gb | Basic    | 1 - 2640      | 2 * 40 Gb | NA                   | 20 Gb       | S4810               | S55                 |
| 1 Gb  | 40 Gb | Basic    | 1 - 2496      | 2 * 40 Gb | NA                   | 20 Gb       | S4810               | S60                 |
| 1 Gb  | 40 Gb | Basic    | 1 - 2496      | 2 * 40 Gb | NA                   | 20 Gb       | S4810               | S55                 |

Use the following table as guideline to select the appropriate three tier Layer 2 VLT or Layer 3 with Additional Resiliency (Routed VLT) fabric design for a 1 Gb ToR VLT deployment.

**AVG** = Aggregation VLTi Capacity

**AVC** = Access VLTi Capacity

**CVG** = Core VLTi Capacity

**DL** = Downlink

**DL BW** = Downlink Bandwidth

**FL BW C A** = Fabric Link Bandwidth between Core & Aggregation

**FL BW AA** = Fabric Link Bandwidth between Aggregation & Access

**FL BW** = Fabric Link Bandwidth

UL BW = Uplink Bandwidth

BW = Bandwidth

**Table 9. Three Tier ToR (1 Gb Downlinks) for Layer 2 and Layer 3 with Resiliency (Routed VLT)**

| DL BW | UL BW | Type     | DL Port Range | CVG       | AVG       | AVC | FL BW CA | FL BW AA | Possible Topologies |             |                  |
|-------|-------|----------|---------------|-----------|-----------|-----|----------|----------|---------------------|-------------|------------------|
|       |       |          |               |           |           |     |          |          | Core                | Aggregation | Access           |
| 1 Gb  | 10 Gb | Stacking | 2641 - 32256  | 2 * 40 Gb | 2 * 40 Gb | NA  | 80G      | 40 Gb    | Z9000 or S6000      | S4810       | S55 (12G)        |
| 1 Gb  | 10 Gb | Stacking | 2641 - 32256  | 2 * 40 Gb | 2 * 40 Gb | NA  | 80G      | 40 Gb    | Z9000 or S6000      | S4810       | S60 (12G or 24G) |
| 1 Gb  | 40 Gb | Stacking | 2497 - 32256  | 2 * 40 Gb | 2 * 40 Gb | NA  | 80G      | 40 Gb    | Z9000 or S6000      | S4810       | S55 (12G)        |
| 1 Gb  | 40 Gb | Stacking | 2497 - 32256  | 2 * 40 Gb | 2 * 40 Gb | NA  | 80G      | 40 Gb    | Z9000 or S6000      | S4810       | S60 (12G or 24G) |
| 1 Gb  | 10 Gb | Basic    | 2641 - 32256  | 2 * 40 Gb | 2 * 40 Gb | NA  | 80G      | 20 Gb    | Z9000 or S6000      | S4810       | S60              |
| 1 Gb  | 10 Gb | Basic    | 2641 - 32256  | 2 * 40 Gb | 2 * 40 Gb | NA  | 80G      | 20 Gb    | Z9000 or S6000      | S4810       | S55              |
| 1 Gb  | 40 Gb | Basic    | 2497 - 32256  | 2 * 40 Gb | 2 * 40 Gb | NA  | 80G      | 20 Gb    | Z9000 or S6000      | S4810       | S60              |
| 1 Gb  | 40 Gb | Basic    | 2497 - 32256  | 2 * 40 Gb | 2 * 40 Gb | NA  | 80G      | 20 Gb    | Z9000 or S6000      | S4810       | S55              |

## 10 Gb or 40 Gb ToR (mVLT)

Use the 10 Gb or 40 Gb ToR Deployment (mVLT) fabric when you require 10 Gb or 40 Gb downlinks for a ToR. For information about mVLT, refer to [Multi-domain VLT](#). Refer to the MXL Topologies for MXL Blade Deployment.

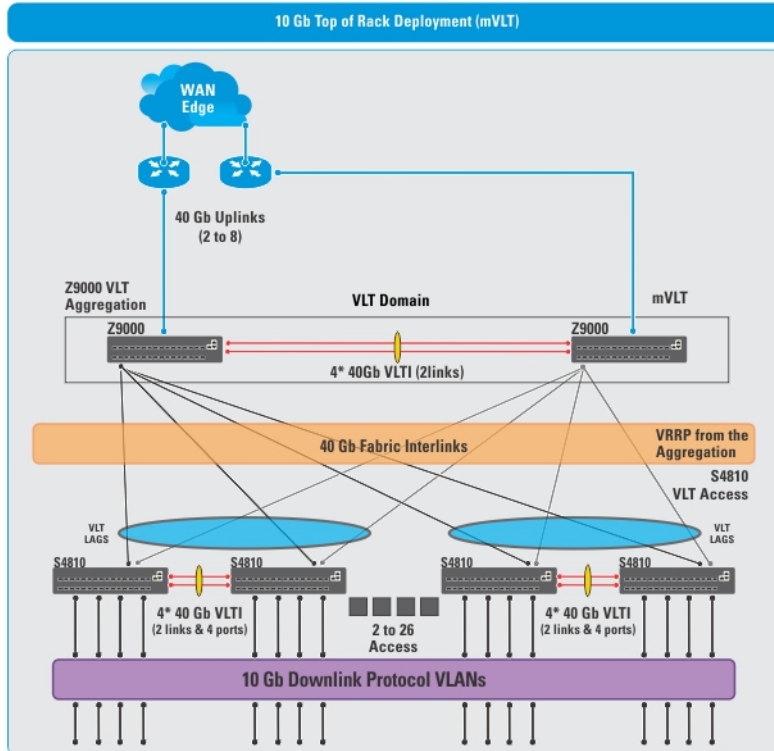


Figure 12. 10 Gb or 40 Gb ToR VLT Deployment (mVLT)

### 👉 Important:

All the VLT aggregation switches must be same model for aggregation (for example, all Z9000 switches). On the VLT access, you can configure the same model or mixed the following models : S4810 and S4820T.

## Two and Three Tier 10 Gb ToR (mVLT) Deployment Topologies for Layer 2 or Layer 3 with Resiliency

**AVC** = Aggregation VLTi Capacity

**DL** = Downlink

**DL BW** = Down Link Bandwidth

**FL BWB A & A** = Fabric Link Bandwidth between Aggregation & Access

**UL BW** = Uplink Bandwidth



Use the following tables as guideline to select the appropriate two tier Layer 2 VLT or Layer 3 with Resiliency (Routed VLT) fabric design.

 **NOTE:** With a Layer 2 VLT fabric, the uplinks come from the first two switches on the aggregation side. For information about tiers, see [Standard Fabric Design – Deployment Topology](#).

**Table 10. 2 Tier ToR (mVLT) – 10 G Downlinks**

| DL BW | UL BW | Type                  | DL Port Range | AVC       | Access VLTi Capacity | FL BWB A & A | Possible Topologies |                |                 |
|-------|-------|-----------------------|---------------|-----------|----------------------|--------------|---------------------|----------------|-----------------|
|       |       |                       |               |           |                      |              | Core                | Aggregation    | Access          |
| 10 Gb | 10 Gb | Mixed node Stacking   | 111 - 2970    | 2 * 40 Gb | NA                   | 40 Gb        | NA                  | S4810          | S4810 or S4820T |
| 10 Gb | 10 Gb | Mixed node Stacking   | 111 - 1392    | 2 * 40 Gb | NA                   | 160 Gb       | NA                  | Z9000 or S6000 | S4810 or S4820T |
| 10 Gb | 10 Gb | Stacking              | 111 - 2970    | 2 * 40 Gb | NA                   | 40 Gb        | NA                  | S4810          | S4810           |
| 10 Gb | 10 Gb | Stacking              | 111 - 1392    | 2 * 40 Gb | NA                   | 160 Gb       | NA                  | Z9000 or S6000 | S4810           |
| 10 Gb | 10 Gb | Basic                 | 111 - 3410    | 2 * 40 Gb | NA                   | 20 Gb        | NA                  | S4810          | S4810           |
| 10 Gb | 10 Gb | Basic                 | 111 - 1624    | 2 * 40 Gb | NA                   | 80 Gb        | NA                  | Z9000 or S6000 | S4810           |
| 10 Gb | 10 Gb | Mixed node Basic      | 111 - 3410    | 2 * 40 Gb | NA                   | 20 Gb        | NA                  | S4810          | S4810 or S4820T |
| 10 Gb | 10 Gb | Mixed node Basic      | 111 - 1624    | 2 * 40 Gb | NA                   | 80 Gb        | NA                  | Z9000 or S6000 | S4810 or S4820T |
| 10 Gb | 10 Gb | Resiliency            | 111 - 2916    | 2 * 40 Gb | 2 * 40 Gb            | 20 Gb        | NA                  | S4810          | S4810           |
| 10 Gb | 10 Gb | Resiliency            | 111 - 1344    | 2 * 40 Gb | 2 * 40 Gb            | 80 Gb        | NA                  | Z9000 or S6000 | S4810           |
| 10 Gb | 10 Gb | Mixed node Resiliency | 111 - 2916    | 2 * 40 Gb | 2 * 40 Gb            | 20 Gb        | NA                  | S4810          | S4810 or S4820T |
| 10 Gb | 10 Gb | Mixed node Resiliency | 111 - 1344    | 2 * 40 Gb | 2 * 40 Gb            | 80 Gb        | NA                  | Z9000 or S6000 | S4810 or S4820T |

| DL BW | UL BW | Type                  | DL Port Range | AVC       | Access VLTi Capacity | FL BWB A & A | Possible Topologies |                |                 |
|-------|-------|-----------------------|---------------|-----------|----------------------|--------------|---------------------|----------------|-----------------|
|       |       |                       |               |           |                      |              | Core                | Aggregation    | Access          |
| 10 Gb | 40 Gb | Mixed node Stacking   | 105 - 2808    | 2 * 40 Gb | NA                   | 40 Gb        | NA                  | S4810          | S4810 or S4820T |
| 10 Gb | 40 Gb | Mixed node Stacking   | 105 - 1392    | 2 * 40 Gb | NA                   | 160 Gb       | NA                  | Z9000 or S6000 | S4810 or S4820T |
| 10 Gb | 40 Gb | Stacking              | 105 - 2808    | 2 * 40 Gb | NA                   | 40 Gb        | NA                  | S4810          | S4810           |
| 10 Gb | 40 Gb | Stacking              | 105 - 1392    | 2 * 40 Gb | NA                   | 160 Gb       | NA                  | Z9000 or S6000 | S4810           |
| 10 Gb | 40 Gb | Basic                 | 105 - 3224    | 2 * 40 Gb | NA                   | 20 Gb        | NA                  | S4810          | S4810           |
| 10 Gb | 40 Gb | Basic                 | 105 - 1624    | 2 * 40 Gb | NA                   | 80G          | NA                  | Z9000 or S6000 | S4810           |
| 10 Gb | 40 Gb | Mixed node Basic      | 105 - 3224    | 2 * 40 Gb | NA                   | 20 Gb        | NA                  | S4810          | S4810 or S4820T |
| 10 Gb | 40 Gb | Mixed node Basic      | 105 - 1624    | 2 * 40 Gb | NA                   | 80G          | NA                  | Z9000 or S6000 | S4810 or S4820T |
| 10 Gb | 40 Gb | Resiliency            | 105 - 2808    | 2 * 40 Gb | 2 * 40 Gb            | 20 Gb        | NA                  | S4810          | S4810           |
| 10 Gb | 40 Gb | Resiliency            | 105 - 1344    | 2 * 40 Gb | 2 * 40 Gb            | 80G          | NA                  | Z9000 or S6000 | S4810           |
| 10 Gb | 40 Gb | Mixed node Resiliency | 105 - 2808    | 2 * 40 Gb | 2 * 40 Gb            | 20 Gb        | NA                  | S4810          | S4810 or S4820T |
| 10 Gb | 40 Gb | Mixed node Resiliency | 105 - 1344    | 2 * 40 Gb | 2 * 40 Gb            | 80G          | NA                  | Z9000 or S6000 | S4810 or S4820T |

**AVC** = Aggregation VLTi Capacity

**BW** = Bandwidth

**DL** = Downlink

**DL BW** = Downlink Bandwidth

**FL BW AA** = Fabric Link Bandwidth between Aggregation & Access

**UL BW** = Uplink Bandwidth

Use the following tables as guideline to select the appropriate two tier Layer 2 VLT or Layer 3 with Resiliency (Routed VLT) fabric design for a 40 Gb ToR (mVLT deployment).

 **NOTE:** With a Layer 2 VLT fabric, the uplinks come from the switches on the aggregation side. For information about tiers, refer to [Standard Fabric Design – Deployment Topology](#).

**Table 11. Two Tier ToR (mVLT) – 40 G Downlinks for Layer 2 or Layer 3 with Resiliency (Routed VLT)**

| DL BW | UL BW | Type       | DL Port Range | AVC       | Access VLTi Capacity | FL BW AA | Possible Topologies |        |
|-------|-------|------------|---------------|-----------|----------------------|----------|---------------------|--------|
|       |       |            |               |           |                      |          | Aggregation         | Access |
| 40 Gb | 10 Gb | Basic      | 60 - 870      | 2 * 40 Gb | NA                   | 80 Gb    | Z9000               | Z9000  |
| 40 Gb | 10 Gb | Basic      | 60 - 870      | 2 * 40 Gb | NA                   | 80 Gb    | S6000               | S6000  |
| 40 Gb | 10 Gb | Resiliency | 60 - 784      | 2 *40 Gb  | 2 * 40 Gb            | 80 Gb    | Z9000               | Z9000  |
| 40 Gb | 10 Gb | Resiliency | 60 - 784      | 2 * 40 Gb | 2 * 40 Gb            | 80 Gb    | S6000               | S6000  |
| 40 Gb | 40 Gb | Basic      | 59 - 870      | 2 * 40 Gb | NA                   | 80 Gb    | Z9000               | Z9000  |
| 40 Gb | 40 Gb | Basic      | 59 - 870      | 2 * 40 Gb | NA                   | 80 Gb    | S6000               | S6000  |
| 40 Gb | 40 Gb | Resiliency | 59 - 784      | 2 *40 Gb  | 2 * 40 Gb            | 80 Gb    | Z9000               | Z9000  |
| 40 Gb | 40 Gb | Resiliency | 59 - 784      | 2 *40 Gb  | 2 * 40 Gb            | 80 Gb    | S6000               | S6000  |

**Three Tier Topologies for a 10 Gb or 40 Gb ToR (mVLT) Deployment Layer 2 or Layer 3 with Resiliency (Routed VLT)**

Use the following tables as guideline to select the appropriate three tier Layer 2 VLT or Layer 3 with Resiliency (Routed VLT) fabric design for a 40 Gb Tor (mVLT) Deployment.

 **NOTE:** With a Layer 2 VLT fabric, the uplinks come from the switches on the aggregation side. For information about tiers, refer to [Standard Fabric Design – Deployment Topology](#).

**AVC** = Aggregation VLTi Capacity

**CVC** = Core VLTi Capacity

**BW** = Bandwidth

**DL** = Downlink

**DL BW** = Downlink Bandwidth

**FL BW CA** = Fabric Link Bandwidth between Core & Aggregation

**FL BW AA** = Fabric Link Bandwidth between Aggregation & Access

**UL BW** = Uplink Bandwidth

**Table 12. 3 Tier ToR (mVLT) – 10 Gb Downlinks**

| DL BW | UL BW | Type       | DL Port Range | CVC       | AVC       | AVC       | FL BW CA | FL BW AA | Possible Topologies |                |        |
|-------|-------|------------|---------------|-----------|-----------|-----------|----------|----------|---------------------|----------------|--------|
|       |       |            |               |           |           |           |          |          | Core                | Aggregation    | Access |
| 10 Gb | 10 Gb | Stacking   | 2971 - 36288  | 2 * 40 Gb | 2 * 40 Gb | NA        | 80 Gb    | 40 Gb    | Z9000 or S6000      | S4810          | S4810  |
| 10 Gb | 10 Gb | Stacking   | 2971 - 36288  | 2 * 40 Gb | 2 * 40 Gb | NA        | 80 Gb    | 40 Gb    | Z9000 or S6000      | S4810          | S4820  |
| 10 Gb | 10 Gb | Stacking   | 2971 - 18816  | 2 * 40 Gb | 2 * 40 Gb | NA        | 80 Gb    | 160 Gb   | Z9000 or S6000      | Z9000 or S6000 | S4810  |
| 10 Gb | 10 Gb | Stacking   | 2971 - 18816  | 2 * 40 Gb | 2 * 40 Gb | NA        | 80 Gb    | 160 Gb   | Z9000 or S6000      | Z9000 or S6000 | S4820  |
| 10 Gb | 10 Gb | Basic      | 3411 - 41664  | 2 * 40 Gb | 2 * 40 Gb | NA        | 80 Gb    | 20 Gb    | Z9000 or S6000      | S4810          | S4810  |
| 10 Gb | 10 Gb | Basic      | 3411 - 41664  | 2 * 40 Gb | 2 * 40 Gb | NA        | 80 Gb    | 20 Gb    | Z9000 or S6000      | S4810          | S4820  |
| 10 Gb | 10 Gb | Basic      | 1625 - 21952  | 2 * 40 Gb | 2 * 40 Gb | NA        | 80 Gb    | 80 Gb    | Z9000 or S6000      | Z9000 or S6000 | S4810  |
| 10 Gb | 10 Gb | Basic      | 1625 - 21952  | 2 * 40 Gb | 2 * 40 Gb | NA        | 80 Gb    | 80 Gb    | Z9000 or S6000      | Z9000 or S6000 | S4820  |
| 10 Gb | 10 Gb | Resiliency | 2917 - 36288  | 2 * 40 Gb | 2 * 40 Gb | 2 * 40 Gb | 80 Gb    | 20 Gb    | Z9000 or S6000      | S4810          | S4810  |
| 10 Gb | 10 Gb | Resiliency | 2917 - 36288  | 2 * 40 Gb | 2 * 40 Gb | 2 * 40 Gb | 80 Gb    | 20 Gb    | Z9000 or S6000      | S4810          | S4820  |
| 10 Gb | 10 Gb | Resiliency | 1355 - 18816  | 2 * 40 Gb | 2 * 40 Gb | 2 * 40 Gb | 80 Gb    | 80 Gb    | Z9000 or S6000      | Z9000 or S6000 | S4810  |

| DL BW | UL BW | Type       | DL Port Range | CVC       | AVC       | AVC       | FL BW CA | FL BW AA | Possible Topologies |                |        |
|-------|-------|------------|---------------|-----------|-----------|-----------|----------|----------|---------------------|----------------|--------|
|       |       |            |               |           |           |           |          |          | Core                | Aggregation    | Access |
| 10 Gb | 10 Gb | Resiliency | 1355 - 18816  | 2 * 40 Gb | 2 * 40 Gb | 2 * 40 Gb | 80 Gb    | 80 Gb    | Z9000 or S6000      | Z9000 or S6000 | S4820  |
| 10 Gb | 40 Gb | Stacking   | 2809 - 36288  | 2 * 40 Gb | 2 * 40 Gb | NA        | 80 Gb    | 40 Gb    | Z9000 or S6000      | S4810          | S4810  |
| 10 Gb | 40 Gb | Stacking   | 2809 - 36288  | 2 * 40 Gb | 2 * 40 Gb | NA        | 80 Gb    | 40 Gb    | Z9000 or S6000      | S4810          | S4820  |
| 10 Gb | 40 Gb | Stacking   | 1393 - 18816  | 2 * 40 Gb | 2 * 40 Gb | NA        | 80 Gb    | 160 Gb   | Z9000 or S6000      | Z9000 or S6000 | S4810  |
| 10 Gb | 40 Gb | Stacking   | 1393 - 18816  | 2 * 40 Gb | 2 * 40 Gb | NA        | 80 Gb    | 160 Gb   | Z9000 or S6000      | Z9000 or S6000 | S4820  |
| 10 Gb | 40 Gb | Basic      | 3225 - 41664  | 2 * 40 Gb | 2 * 40 Gb | NA        | 80 Gb    | 20 Gb    | Z9000 or S6000      | S4810          | S4810  |
| 10 Gb | 40 Gb | Basic      | 3225 - 41664  | 2 * 40 Gb | 2 * 40 Gb | NA        | 80 Gb    | 20 Gb    | Z9000 or S6000      | S4810          | S4820  |
| 10 Gb | 40 Gb | Basic      | 1225 - 21952  | 2 * 40 Gb | 2 * 40 Gb | NA        | 80 Gb    | 80 Gb    | Z9000 or S6000      | Z9000 or S6000 | S4810  |
| 10 Gb | 40 Gb | Basic      | 1225 - 21952  | 2 * 40 Gb | 2 * 40 Gb | NA        | 80 Gb    | 80 Gb    | Z9000 or S6000      | Z9000 or S6000 | S4820  |
| 10 Gb | 40 Gb | Resiliency | 2809 - 36288  | 2 * 40 Gb | 2 * 40 Gb | 2 * 40 Gb | 80 Gb    | 20 Gb    | Z9000 or S6000      | S4810          | S4810  |
| 10 Gb | 40 Gb | Resiliency | 2809 - 36288  | 2 * 40 Gb | 2 * 40 Gb | 2 * 40 Gb | 80 Gb    | 20 Gb    | Z9000 or S6000      | S4810          | S4820  |
| 10 Gb | 40 Gb | Resiliency | 1345 - 18816  | 2 * 40 Gb | 2 * 40 Gb | 2 * 40 Gb | 80 Gb    | 80 Gb    | Z9000 or S6000      | Z9000 or S6000 | S4810  |

| DL BW | UL BW | Type       | DL Port Range | CVC       | AVC       | AVC       | FL BW CA | FL BW AA | Possible Topologies |                |        |
|-------|-------|------------|---------------|-----------|-----------|-----------|----------|----------|---------------------|----------------|--------|
|       |       |            |               |           |           |           |          |          | Core                | Aggregation    | Access |
| 10 Gb | 40 Gb | Resiliency | 1345 - 18816  | 2 * 40 Gb | 2 * 40 Gb | 2 * 40 Gb | 80 Gb    | 80 Gb    | Z9000 or S6000      | Z9000 or S6000 | S4820  |

**AVC** = Aggregation VLTi Capacity

**CVC** = Core VLTi Capacity

**BW** = Bandwidth

**DL** = Downlink

**DL BW** = Downlink Bandwidth

**FL BWB C & A** = Fabric Link Bandwidth between Core and Aggregation Switches

**FL BWB A & A** = Fabric Link Bandwidth between Aggregation and Access Switches

**UL BW** = Uplink Bandwidth

**Table 13. Three Tier ToR (mVLT) – 40 Gb Downlinks**

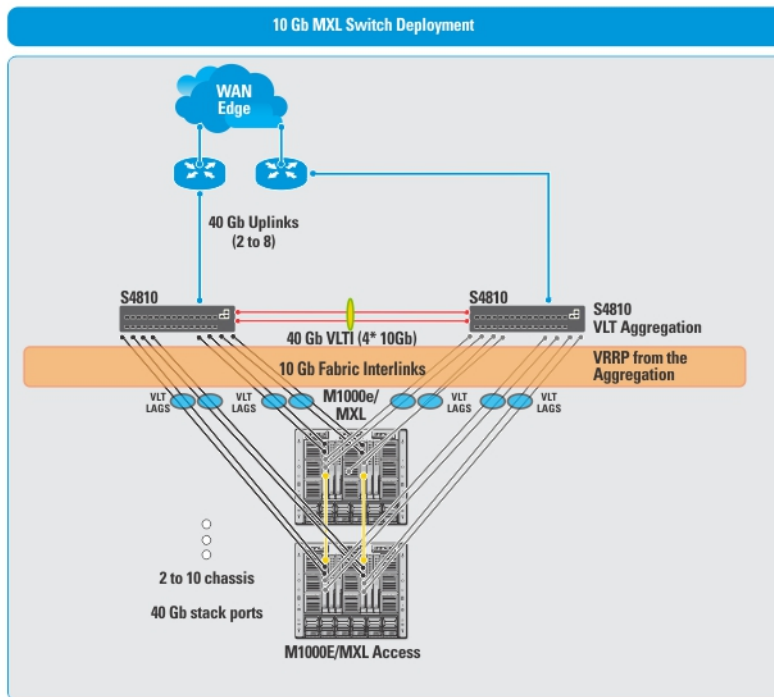
| DL BW | UL BW | Type       | DL Port Range | CVC       | AVC       | Access VLTi Capacity | FL BWB C & A | FL BWB A & A | Possible Topologies |             |        |
|-------|-------|------------|---------------|-----------|-----------|----------------------|--------------|--------------|---------------------|-------------|--------|
|       |       |            |               |           |           |                      |              |              | Core                | Aggregation | Access |
| 40 Gb | 10 Gb | Basic      | 871 - 11760   | 2 * 40 Gb | 2 * 40 Gb | NA                   | 80 Gb        | 80 Gb        | Z9000               | Z9000       | Z9000  |
| 40 Gb | 10 Gb | Basic      | 871 - 11760   | 2 * 40 Gb | 2 * 40 Gb | NA                   | 80 Gb        | 80 Gb        | S6000               | S6000       | S6000  |
| 40 Gb | 10 Gb | Resiliency | 785 - 10976   | 2 * 40 Gb | 2 * 40 Gb | 2 * 40 Gb            | 80 Gb        | 80 Gb        | Z9000               | Z9000       | Z9000  |
| 40 Gb | 10 Gb | Resiliency | 785 - 10976   | 2 * 40 Gb | 2 * 40 Gb | 2 * 40 Gb            | 80 Gb        | 80 Gb        | S6000               | S6000       | S6000  |
| 40 Gb | 40 Gb | Basic      | 871 - 11760   | 2 * 40 Gb | 2 * 40 Gb | NA                   | 80 Gb        | 80 Gb        | Z9000               | Z9000       | Z9000  |
| 40 Gb | 40 Gb | Basic      | 871 - 11760   | 2 * 40 Gb | 2 * 40 Gb | NA                   | 80 Gb        | 80 Gb        | S6000               | S6000       | S6000  |

## Two and Three Tier MXL Blade Topologies for Layer 2 and Layer 3 with Resiliency (Routed VLT)

You can create a fabric using MXL blades by selecting the **MXL blade** option and **10 Gb** downlinks. For information about MXL fabric deployments, refer MXL Topologies for MXL Blade Deployment..

**NOTE:** All the VLT aggregation switches must be same model (for example, all S4810 switches). On the VLT access, all the switches must be MXL blades. Refer to the previous tables in this section for more information.

### 10 Gb Blade Switch (MXL) VLT Deployment



**BW** = Bandwidth

**DL** = Downlink

**FL BWB A & A** = Fabric Link Bandwidth between Aggregation and Access

**UL BW** = Uplink Bandwidth

**VLTi A BW** = VLTi Aggregation Bandwidth

**Table 14. MXL Blade Two Tier Topologies for 10 GB MXL Blade Switch For Layer 2 and Layer 3 with Resiliency (Routed VLT)**

| MXL Blade Pairs Range | UL BW | Type     | Fabric Type  | FL BWBA & A | VLTi A BW       | VLTi Access BW | MXL Inter-chassis BW | Possible Topologies |        |
|-----------------------|-------|----------|--|-------------|-----------------|----------------|----------------------|---------------------|--------|
|                       |       |          |  |             |                 |                |                      | Aggregation         | Access |
| 2 - 27                | 10 Gb | Basic    | Layer 2/<br>Layer 3<br>with<br>Resiliency<br>(Routed<br>VLT) | 20 Gb       | 2 *<br>40<br>Gb | NA             | NA                   | S4810 or<br>S4820T  | MXL    |
| 2 - 14                | 10 Gb | Basic    | Layer 2/<br>Layer 3<br>with<br>Resiliency<br>(Routed<br>VLT) | 80 Gb       | 2 *<br>40<br>Gb | NA             | NA                   | Z9000 or<br>S6000   | MXL    |
| 2 - 14                | 40 Gb | Basic    | Layer 2/<br>Layer 3<br>with<br>Resiliency<br>(Routed<br>VLT) | 80 Gb       | 2 *<br>40<br>Gb | NA             | NA                   | Z9000 or<br>S6000   | MXL    |
| 2 - 26                | 40 Gb | Basic    | Layer 2/<br>Layer 3<br>with<br>Resiliency<br>(Routed<br>VLT) | 20 Gb       | 2 *<br>40<br>Gb | NA             | NA                   | S4810 or<br>S4820T  | MXL    |
| 2 - 27                | 10 Gb | Stacking | Layer 2/<br>Layer 3<br>with<br>Resiliency<br>(Routed<br>VLT) | 40 Gb       | 2 *<br>40<br>Gb | NA             | NA                   | S4810 or<br>S4820T  | MXL    |
| 2 - 14                | 10 Gb | Stacking | Layer 2/<br>Layer 3<br>with<br>Resiliency<br>(Routed<br>VLT) | 160G        | 2 *<br>40<br>Gb | NA             | NA                   | Z9000 or<br>S6000   | MXL    |
| 2 - 14                | 40 Gb | Stacking | Layer 2/<br>Layer 3<br>with<br>Resiliency<br>(Routed<br>VLT) | 160G        | 2 *<br>40<br>Gb | NA             | NA                   | Z9000/S6000         | MXL    |



| MXL Blade Pairs Range                          | UL BW | Type                                     | Fabric Type  | FL BWBA & A | VLTi A BW       | VLTi Access BW | MXL Inter-chassis BW | Possible Topologies |        |
|--|-------|--|--|-------------|-----------------|----------------|----------------------|---------------------|--------|
|  |       |  |  |             |                 |                |                      | Aggregation         | Access |
| 2 - 26   | 40 Gb | Stacking                                 | Layer 2/<br>Layer 3<br>with<br>Resiliency<br>(Routed<br>VLT) | 40 Gb       | 2 *<br>40<br>Gb | NA             | NA                   | S4810 or<br>S4820T  | MXL    |
| 2 - 27   | 10 Gb | MXL -<br>intra-<br>Chassis<br>resiliency | Layer 2/<br>Layer 3<br>with<br>Resiliency<br>(Routed<br>VLT) | 20 Gb       | 2 *<br>40<br>Gb | 2 * 40<br>Gb   | NA                   | S4810 or<br>S4820T  | MXL    |
| 2 - 14   | 10 Gb | MXL -<br>intra-<br>Chassis<br>resiliency | Layer 2/<br>Layer 3<br>with<br>Resiliency<br>(Routed<br>VLT) | 80 Gb       | 2 *<br>40<br>Gb | 2 * 40<br>Gb   | NA                   | Z9000/S6000         | MXL    |
| 2 - 14   | 40 Gb | MXL -<br>intra-<br>Chassis<br>resiliency | Layer 2/<br>Layer 3<br>with<br>Resiliency<br>(Routed<br>VLT) | 80 Gb       | 2 *<br>40<br>Gb | 2 * 40<br>Gb   | NA                   | Z9000/S6000         | MXL    |
| 2 - 26   | 40 Gb | MXL -<br>intra-<br>Chassis<br>resiliency | Layer 2/<br>Layer 3<br>with<br>Resiliency<br>(Routed<br>VLT) | 20 Gb       | 2 *<br>40<br>Gb | 2 * 40<br>Gb   | NA                   | S4810 or<br>S4820T  | MXL    |
| 2 - 30<br>(for all<br>even<br>numbers<br>only) | 10 Gb | MXL -<br>inter-<br>Chassis<br>resiliency | Layer 3<br>with<br>Resiliency<br>(Routed<br>VLT)             | 20 Gb       | 2 *<br>40<br>Gb | 2 * 40<br>Gb   | 40<br>Gb             | S4810 or<br>S4820T  | MXL    |
| 2 - 14<br>(for all<br>even<br>numbers<br>only) | 10 Gb | MXL -<br>inter-<br>Chassis<br>resiliency | Layer 3<br>with<br>Resiliency<br>(Routed<br>VLT)             | 80 Gb       | 2 *<br>40<br>Gb | 2 * 40<br>Gb   | 40<br>Gb             | Z9000 or<br>S6000   | MXL    |
| 2 - 30<br>(for all<br>even)                    | 40 Gb | MXL -<br>inter-<br>Chassis               | Layer 3<br>with<br>Resiliency                                | 20 Gb       | 2 *<br>40<br>Gb | 2 * 40<br>Gb   | 40<br>Gb             | S4810 or<br>S4820T  | MXL    |

| MXL Blade Pairs Range | UL BW | Type       | Fabric Type  | FL BWBA & A | VLTi A BW | VLTi Access BW | MXL Inter-chassis BW | Possible Topologies |        |
|-----------------------|-------|------------|--------------|-------------|-----------|----------------|----------------------|---------------------|--------|
|                       |       |            |              |             |           |                |                      | Aggregation         | Access |
| numbers only)         |       | Resiliency | (Routed VLT) |             |           |                |                      |                     |        |

**BW** = Bandwidth

**DL** = Downlink

**FL BWBA & A** = Fabric Link Bandwidth between Aggregation and Access

**FL BWB C & A** = Fabric Link Bandwidth between Core and Access

**UL BW** = Uplink Bandwidth

**VCBW** = VLTi Core Bandwidth

**Table 15. Three Tier Deployment Topologies for MXL Blade Switch for Layer 2 and Layer 3 with Resiliency (Routed VLT)**

| MXL Blade Pairs Range | UL BW | Type  | Fabric Type                                     | FL BWB C & A | FL BWB A & A | VCBW      | VLTi Aggregation BW | Possible Topologies |                 |        |
|-----------------------|-------|-------|---|--------------|--------------|-----------|---------------------|---------------------|-----------------|--------|
|                       |       |       |   |              |              |           |                     | Core                | Aggregation     | Access |
| 28 - 336              | 10 Gb | Basic | Layer 2 or Layer 3 with Resiliency (Routed VLT) | 80G          | 20 Gb        | 2 * 40 Gb | 2 * 40 Gb           | Z9000 or S6000      | S4810 or S4820T | MXL    |
| 28 - 336              | 40 Gb | Basic | Layer 2 or Layer 3 with Resiliency (Routed VLT) | 80G          | 20 Gb        | 2 * 40 Gb | 2 * 40 Gb           | Z9000 or S6000      | S4810 or S4820T | MXL    |
| 15 - 196              | 10 Gb | Basic | Layer 2 or Layer 3 with Resiliency (Routed VLT) | 80G          | 80G          | 2 * 40 Gb | 2 * 40 Gb           | Z9000               | Z9000           | MXL    |
| 15 - 196              | 10 Gb | Basic | Layer 2 or Layer 3 with Resiliency (Routed VLT) | 80G          | 80G          | 2 * 40 Gb | 2 * 40 Gb           | S6000               | S6000           | MXL    |

| MXL Blade Pairs Range | UL BW | Type     | Fabric Type                                     | FL BWB C & A | FL BWB A & A | VCBW      | VLTi Aggregation BW | Possible Topologies |                 |        |
|-----------------------|-------|----------|---|--------------|--------------|-----------|---------------------|---------------------|-----------------|--------|
|                       |       |          |   |              |              |           |                     | Core                | Aggregation     | Access |
| 15 - 196              | 40 Gb | Basic    | Layer 2 or Layer 3 with Resiliency (Routed VLT) | 80G          | 80G          | 2 * 40 Gb | 2 * 40 Gb           | Z9000               | Z9000           | MXL    |
| 15 - 196              | 40 Gb | Basic    | Layer 2/ Layer 3 with Resiliency (Routed VLT)   | 80G          | 80G          | 2 * 40 Gb | 2 * 40 Gb           | S6000               | S6000           | MXL    |
| 28 - 336              | 10 Gb | Stacking | Layer 2 or Layer 3 with Resiliency (Routed VLT) | 80G          | 40 Gb        | 2 * 40 Gb | 2 * 40 Gb           | Z9000 or S6000      | S4810 or S4820T | MXL    |
| 28 - 336              | 40 Gb | Stacking | Layer 2/ Layer 3 with Resiliency (Routed VLT)   | 80G          | 40 Gb        | 2 * 40 Gb | 2 * 40 Gb           | Z9000 or S6000      | S4810 or S4820T | MXL    |
| 15 - 196              | 10 Gb | Stacking | Layer 2 or Layer 3 with Resiliency (Routed VLT) | 80G          | 160G         | 2 * 40 Gb | 2 * 40 Gb           | Z9000               | Z9000           | MXL    |
| 15 - 196              | 10 Gb | Stacking | Layer 2/ Layer 3 with Resiliency (Routed VLT)   | 80G          | 160G         | 2 * 40 Gb | 2 * 40 Gb           | S6000               | S6000           | MXL    |
| 15 - 196              | 40 Gb | Stacking | Layer 2/ Layer 3 with Resiliency (Routed VLT)   | 80G          | 160G         | 2 * 40 Gb | 2 * 40 Gb           | Z9000               | Z9000           | MXL    |
| 15 - 196              | 40 Gb | Stacking | Layer 2/ Layer 3 with                           | 80G          | 160G         | 2 * 40 Gb | 2 * 40 Gb           | S6000               | S6000           | MXL    |

| MXL Blade Pairs Range | UL BW | Type                           | Fabric Type                                     | FL BWB C & A | FL BWB A & A | VCBW      | VLTi Aggregation BW | Possible Topologies |                 |        |
|-----------------------|-------|--------------------------------|---|--------------|--------------|-----------|---------------------|---------------------|-----------------|--------|
|                       |       |                                |   |              |              |           |                     | Core                | Aggregation     | Access |
|                       |       |                                | Resiliency (Routed VLT)                         |              |              |           |                     |                     |                 |        |
| 28 - 336              | 10 Gb | MXL - intra-Chassis resiliency | Layer 2 or Layer 3 with Resiliency (Routed VLT) | 80G          | 20 Gb        | 2 * 40 Gb | 2 * 40 Gb           | Z9000 or S6000      | S4810 or S4820T | MXL    |
| 27 - 336              | 40 Gb | MXL - intra-Chassis resiliency | Layer 2 or Layer 3 with Resiliency (Routed VLT) | 80G          | 20 Gb        | 2 * 40 Gb | 2 * 40 Gb           | Z9000 or S6000      | S4810 or S4820T | MXL    |
| 15 - 196              | 10 Gb | MXL - intra-Chassis resiliency | Layer 2 or Layer 3 with Resiliency (Routed VLT) | 80G          | 80G          | 2 * 40 Gb | 2 * 40 Gb           | Z9000               | Z9000           | MXL    |
| 15 - 196              | 10 Gb | MXL - intra-Chassis resiliency | Layer 2 or Layer 3 with Resiliency (Routed VLT) | 80G          | 80G          | 2 * 40 Gb | 2 * 40 Gb           | S6000               | S6000           | MXL    |
| 15 - 196              | 40 Gb | MXL - intra-Chassis resiliency | Layer 2 or Layer 3 with Resiliency (Routed VLT) | 80G          | 80G          | 2 * 40 Gb | 2 * 40 Gb           | Z9000               | Z9000           | MXL    |
| 15 - 196              | 40 Gb | MXL - intra-Chassis resiliency | Layer 2 or Layer 3 with Resiliency (Routed VLT) | 80G          | 80G          | 2 * 40 Gb | 2 * 40 Gb           | S6000               | S6000           | MXL    |

# Designing a Fabric

To design a Layer 3 two-tier distributed core fabric or Layer 2 VLT fabric based on your current or future needs, use the **Fabric Design Wizard**. The design consists of a wiring plan, network topology information, summary of the inventory requirement, and a design specification. Refer also to [Network Deployment Summary](#).

 **NOTE:** If you are designing a fabric using an IOA blade switch, refer to [IOA Fabric Design Wizard](#).

You can use the **Fabric Design Wizard** to perform the following tasks:

- [Create a fabric](#)
- [Edit and Expand an Existing Fabric](#)
- [Delete the Fabric](#)
- [Import an Existing Fabric Design](#)
- [View the Wiring Diagram](#)
- Display the status of the fabric design (if the design, pre-deployment, deployment, and validation phases have been successfully completed)
- Display detailed information about the fabric

Before you begin, review the [Getting Started](#) section.

To design a fabric, complete the following tasks using the **Fabric Design Wizard**.

1. [Fabric Design — Fabric Name and Type](#)

Choose a fabric design type:

a. Standard Fabric Design:


1. [Standard Fabric Design — Bandwidth and Port Count](#)
2. [Standard Fabric Design — Deployment Topology](#)
3. [Standard Fabric Design — Fabric Customization](#)

b. Advanced Fabric Design:

1. [Advanced Fabric Design — Aggregation Configuration \(One- or Two-Tier Topologies\)](#) or [Advanced Fabric Design — Aggregation Configuration \(Three-Tier Topologies\)](#)
2. [Advanced Fabric Design — Access Configuration](#)
3. [Advanced Fabric Design — Port Configuration](#)

2. [Fabric Design — Output](#)

3. [Fabric Design — Summary](#)

 **NOTE:** After designing the fabric, prepare it for deployment. For more information, refer to [Pre-deployment Wizard](#).



# Network Deployment Summary



Use AFM to design a fabric, change the pre-deployment configuration, deploy the fabric, and validate the fabric designed by comparing it to a discovered fabric. AFM provides up-to-date status during each phase of the fabric from design to validate. AFM displays any pending steps required to ensure that the fabric is fully functional for each fabric design.

## Fabric Configuration Phases and States

The following table describes the four fabric phases displayed on the **Deploy** tab of the **Deploy and Validation** dialog box. To correct the fabric design and pre-deployment configuration before or after deploying the fabric, refer to the following table for phases, states, and descriptions.

**Table 16. Fabric Configuration Phases and States**




| Phase                        | State            | State Description   |
|------------------------------|------------------|---|
| Design                       | Incomplete       | Required information to complete the design is necessary.   |
|                              | Complete         | All required input to complete the design is available.   |
| Pre-deployment Configuration | Required         | Required Pre-deployment Configuration information for the switches is necessary.<br> <b>NOTE:</b> The Pre-deployment Configuration state for all switches is Required.   |
|                              | Error            | Deployment errors exist for one or more switches.   |
|                              | Partial Complete | Pre-deployment is successful for one or more switches but not for all switches; provides information about the count of switches successfully deployed versus the count of total switches in the fabric design.<br> <b>NOTE:</b> In this state, the information provided is sufficient to proceed with deployment of the subset of switches. |
|                              | Complete         | Pre-deployment Configuration information is complete for all switches.  |
| Deployment                   | Required         | Deployment state for all switches is required.  |
|                              | In-progress      | Deployment is in progress on one or more switches; displays a progress bar and provides information about the count of switches successfully deployed versus the count of total switches per design (based on the current port count — future port count is not included).  |
|                              | Error            | Deployment errors exist for one or more switches.   |
|                              | Partial Complete | Deployment is successful for one or more switches but not for all switches per design; provides information about number of switches successfully deployed versus the number of total switches in the design.   |


| Phase      | State            | State Description   |
|------------|------------------|---|
|            |                  |  <b>NOTE:</b> Deployment on any of the switches is not In-progress while in this state.  |
|            | Complete         | Deployment is successful for the switch.  |
| Validation | Required         | Validation state for all switches is required.  |
|            | In-progress      | Validation is in progress for one or more switches; displays a progress bar and provides information about count of switches successfully validated vs. count of total switches per design (based on current port count — future port count is not included).   |
|            | Error            | Validation errors exist for one or more switches.   |
|            | Partial Complete | Validation is successful for one or more switches but not all switches per design; provides information about the count of switches successfully validated versus the count of total switches per design.<br><br> <b>NOTE:</b> Validation of any of the switches is not in progress during this state. |
|            | Complete         | Validation is successful for all switches.  |

## Switch Configuration Phases and States

This section describes the phases and possible states for a switch.

**Table 17. Switch Level States**

| Phase                        | State    | State Description   |
|------------------------------|----------|---|
| Design                       | Complete | Fabric design is complete for the switch.<br><br> <b>NOTE:</b> At the switch level, Partial Complete designs are not tracked. Partial Complete designs are only tracked at the fabric level.   |
|                              |          |   |
| Pre-deployment Configuration | Required | Required Pre-deployment Configuration information is necessary.   |
|                              | Error    | An error occurred during file transfer (transfer of minimum configuration file) to FTP/TFTP server or an error occurred during automatic DHCP integration for local DHCP server.<br><br> <b>NOTE:</b> For a remote DHCP server, AFM does not report errors for the DHCP integration step as it is not an automated step from AFM. If a DHCP error occurs, manually integrate DHCP. |
|                              | Complete | Pre-deployment Configuration information is complete for the switch.  |
| Deployment                   | Required | Deployment has not been initiated for the switch or the Deployment state was reset due to a Design/Pre-deployment Configuration change.<br><br> <b>NOTE:</b> Deployment can be initiated/re-initiated only if Pre-deployment Configuration is Complete.  |
|                              |          |   |

| Phase      | State       | State Description  |
|------------|-------------|--|
|            | In-progress | Deployment is in progress; provides the percentage of completion.  |
|            | Error       | Deployment errors exist.   |
|            | Complete    | Deployment is successful for the switch.   |
| Validation | Required    | Validation has not been initiated for the switch or the validation state was reset due to a Design/Pre-deployment Configuration/Deployment change.<br> <b>NOTE:</b> Validation can be initiated only if Deployment is Complete. |
|            | In-progress | Deployment is in progress; provides the percentage of completion.  |
|            | Error       | One or more validation errors exist.   |
|            | Complete    | Validation is successful for the switch.   |

## Operations Allowed in Each Fabric State

To determine which operations are allowed during the design, pre-deployment configuration, deployment, and validation states, use the following table. Switch groups can be added or deleted at any time. If none of the switches in the fabric are pre-deployed or deployed, all fabric properties can be edited.

**Table 18. Operations Allowed in Each Fabric State**

| Design State | Pre-Deploy Configuration State   | Deployment State | Validation State | Operation Allowed  |
|--------------|--|------------------|------------------|--|
| Incomplete   | Not Started  | Not Started      | Not Started      | <ul style="list-style-type: none"> <li>Edit Fabric (All fabric attributes)</li> <li>Switch model, type, and name</li> <li>Delete Fabric</li> </ul>   |
| Complete     | Not Started  | Not Started      | Not Started      | <ul style="list-style-type: none"> <li>View Wiring Plan</li> <li>Edit Fabric (All fabric attributes)</li> <li>Switch model, type, and name</li> <li>Pre-deployment Configuration</li> <li>Delete Fabric</li> </ul> |
| Complete     | Incomplete. The system MAC and IP address are not configured for the switches. | Not Started      | Not Started      | <ul style="list-style-type: none"> <li>View Wiring Plan</li> <li>Edit Fabric (All fabric attributes except fabric name)</li> <li>Switch model, type, and name</li> <li>Pre-deployment Configuration</li> </ul>     |



| Design State | Pre-Deploy Configuration State  | Deployment State   | Validation State                                       | Operation Allowed  |
|--------------|---|--|--|--|
|              |   |  |  | <ul style="list-style-type: none"> <li>Delete Fabric</li> </ul>  |
| Complete     | Partial Complete / Complete–Partial complete indicates that at least 1 switch has its system MAC and IP address configured. | Not Started  | Not Started  | <ul style="list-style-type: none"> <li>View Wiring Plan</li> <li>Edit Fabric Description</li> <li>Aggregation &amp; Access Config Speed (Advanced fabric)</li> <li>Number of switches per stack (stack mode)</li> <li>Pre-deployment Configuration</li> <li>View DHCP Configuration</li> <li>Deploy and Validate Fabric</li> <li>View Deployment and Validation Status</li> <li>Delete Fabric</li> </ul> |
| Complete     | Partial Complete / Complete   | In-progress  | Not Started / In-progress / Stopped / Error / Complete | <ul style="list-style-type: none"> <li>Edit Fabric Description</li> <li>Aggregation &amp; Access Config Speed (Advanced fabric)</li> <li>Number of switches per stack (stack mode)</li> <li>View Wiring Plan</li> <li>View DHCP Configuration</li> <li>View Deployment and Validation Status</li> <li>Delete Fabric</li> </ul>   |
| Complete     | Partial Complete / Complete   | Incomplete / Partial Complete / Complete<br><br>Incomplete indicates that AFM is deploying the switches.<br><br>Complete indicates all the | Not Started / In-progress / Stopped / Error / Complete | <ul style="list-style-type: none"> <li>View Wiring Plan</li> <li>Edit Fabric Description</li> <li>Aggregation &amp; Access Config Speed (Advanced fabric)</li> <li>Number of switches per stack (stack mode)</li> <li>Pre-deployment Configuration</li> <li>View DHCP Configuration</li> </ul>   |

| Design State | Pre-Deploy Configuration State | Deployment State                                 | Validation State | Operation Allowed  |
|--------------|--------------------------------|--|------------------|--|
|              |                                | switches in the distributed fabric are deployed. |                  | <ul style="list-style-type: none"> <li>Deploy and Validate Fabric – Validation is only allowed when deployment is partial or fully complete</li> <li>View Deployment and Validation Status</li> <li>Delete Fabric</li> </ul> |

## Deployment Topology Use Cases

To select a deployment topology, refer to the following use cases as a guide.

### Use Case 1: One-Tier Layer 2 Fabric

If you select a one-tier Layer 2 fabric:

- The uplinks between the two aggregation switches and external switch support the Layer 3 protocol (OSPF, iBGP or eBGP).
- The downlinks from the two aggregation switches support the Layer 2 protocol (VLAN or VLAN/VRRP). The default setting on the pre-deployment screen is VLAN configuration, which allows you to configure downlink connections to servers. To support redundancy between the aggregation switches and ToR switches, select **VLAN and VRRP Configuration**.

### Use Case 2: One-Tier Layer 3 with Resiliency (Routed VLT)

If you select a one-tier Layer 3 with Resiliency (Routed VLT) fabric:

- The uplinks between the two aggregation switches and external switch (WAN) support the Layer 3 protocol (OSPF, iBGP or eBGP).
- The downlinks from the two aggregation switches support the Layer 2 protocol (VLAN/VRRP or VLAN IP). During the design phase on the **Deployment Topology** screen of the **Fabric Design** wizard, select the fabric type and deployment type (topology). Based on the selected deployment type options, different downlink options are configured in the access tier.

### Use Case 3: Two-Tier Layer 2

If you select a two-tier Layer 2 VLT fabric:

- The fabric links between aggregation and access switches support the Layer 2 protocol.
- The uplinks between the aggregation switches and external switch (WAN) support the Layer 3 protocol (OSPF, iBGP or eBGP).
- The downlinks from the access switches support the Layer 2 protocol (VLAN or VLAN/VRRP). The default setting on the pre-deployment screen is VLAN configuration, which allows you to configure downlink connections to servers. To support redundancy between the access switch and ToR switches, select the **VLAN and VRRP Configuration** option.

## Use Case 4: Two-Tier Layer 3 Distributed Core

If you select a two-tier Layer 3 distributed core fabric:

- The fabric links between the spine and leaf switches support the Layer 3 OSPF routing protocol.
- The uplinks between spine switch and external switch (WAN) support the Layer 3 protocol (OSPF, iBGP or eBGP).
- The downlinks from the access switches support the Layer 2 protocol (**VLAN** or **VLAN and LAG**).
  - If the **VLAN** option is selected, the downlinks connecting to server are configured to use the VLAN protocol.
  - If the **VLAN and LAG** option is selected, the downlinks between the leaves and ToR are configured to use VLAN, VRRP, and LAG for redundancy.

## Use Case 5: Two-Tier Layer 3 Resiliency (Routed VLT)

If you select a two-tier Layer 3 with Resiliency (Routed VLT) fabric:

- The fabric links between the aggregation and access switches support the Layer 3 protocol with OSPF in the VLAN interfaces.
- The uplinks between the aggregation switch and external switch (WAN) support the Layer 3 protocol (OSPF, iBGP or eBGP).
- The downlinks from the access switches support the Layer 2 protocol (VLAN/VRRP or VLAN IP). During the design phase on the **Deployment Topology** screen of the **Fabric Design** wizard, select the fabric type and deployment type (topology). Based on the deployment type option selected, different options are available to configure the downlink at the access tier.

The following section lists the available topology types:

1. **Layer 3 with Resiliency (Routed VLT) with stacking option** — If you select the **Stacking** option, configure the VLAN with the primary and secondary IP addresses for each access switch.
2. **Layer 3 with Resiliency (Routed VLT) with VLT option** — If you select the **VLT** option, enter the VLAN ID, Primary IP address and Secondary address. If you select the **Enable Layer 3 Protocol in Access Switches** option, configure the VLAN ID and the IP Range. When you complete the pre-deployment configuration, the **Advanced VLAN IP Configuration** option is available at the **Configure and Deploy** tab.

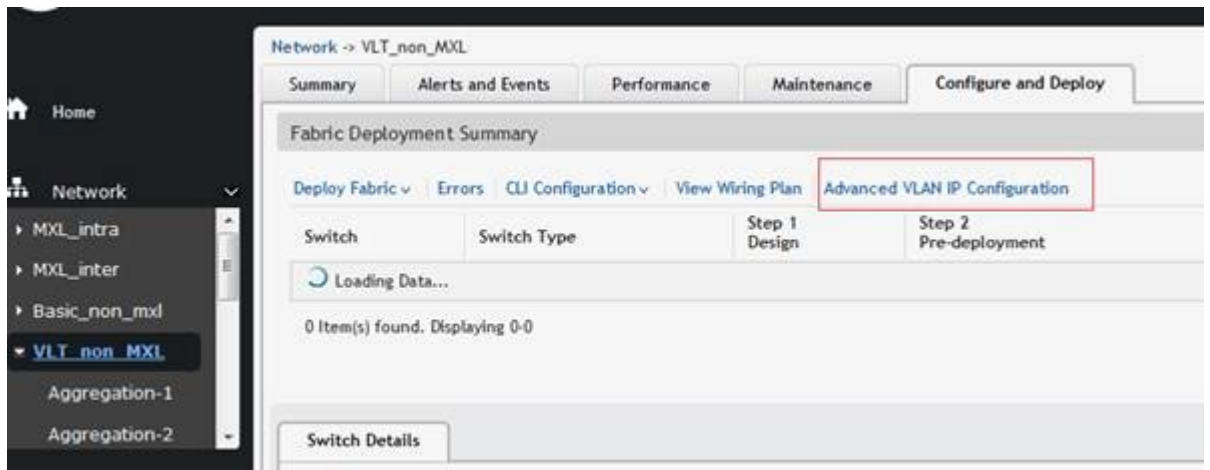


Figure 13. Layer 3 with Resiliency (Routed VLT) with VLT option + Advanced VLAN IP Configuration

3. **Layer 3 with Resiliency (Routed VLT) — Basic option** – If you select the **Basic** option, configure the VLAN with the primary and secondary IP addresses for each access switch.
4. **Layer 3 with Resiliency (Routed VLT) with MXL Blade with InterChassis option** – For this topology, select the Deployment Type with an MXL Blade switch with Resiliency (VLT) and Interchassis (across chassis) resiliency. Enter the VLAN ID and the IP range. When you complete the pre-deployment configuration, the **Advanced VLAN IP Configuration** option is available on the **Configure and Deploy Summary** screen.
5. **Layer 3 with Resiliency (Routed VLT) — Blade MXL with IntraChassis option:** With this topology, select the deployment with an MXL Blade switch with Resiliency (VLT) and the **Intrachassis (within the same chassis) resiliency** option. Enter the VLAN ID, primary, and secondary IP addresses.

## Use Case 6: Three-Tier Layer 2

If you select a three-tier Layer 2 fabric:

- The fabric links between the core and aggregation switches support the Layer 3 protocol.
- The fabric links between the aggregation and access switches support the Layer 2 protocol.
- The uplinks between the aggregation switches and external switch (WAN) support the Layer 3 protocol (OSPF, iBGP or eBGP).
- The downlinks from the access switches support the Layer 2 protocol (VLAN or VLAN/VRRP). The default setting on the pre-deployment screen is VLAN configuration, which allows you to configure downlink connections to servers. To support redundancy between the access switch and ToR switches, select the **VLAN and VRRP Configuration** option.

## Use Case 7: Three-Tier Layer 3 Resiliency (Routed VLT)

If you select a three-tier Layer 3 with Resiliency (Routed VLT) fabric:

- The fabric links between the core and aggregation switches support Layer 3 protocol with OSPF in the VLAN interfaces.
- The fabric links between the aggregation and access switches support the Layer 2 protocol.
- The uplinks between the aggregation switch and external switch (WAN) support the Layer 3 protocol (OSPF, iBGP or eBGP).
- The downlinks from the access switches support the Layer 2 protocol (VLAN/VRRP or VLAN IP). During the design phase on the **Deployment Topology** screen of the **Fabric Design** wizard, select the fabric type and deployment type (topology). Based on the selected deployment type options, different downlinks options are configured at the access tier.

The following section lists the available topology types:

1. **Layer 3 with Resiliency (Routed VLT) with stacking option** — If you select the **Stacking** option, configure the VLAN with the primary and secondary IP addresses for each access switch.
2. **Layer 3 with Resiliency (Routed VLT) with VLT option** — If you select the **VLT** option, enter the VLAN ID, Primary IP address and Secondary address. If you select the **Enable Layer 3 Protocol in Access Switches** option, configure the VLAN ID and the IP Range. When you complete the pre-deployment configuration, the **Advanced VLAN IP Configuration** option is available in the **Configure and Deploy** tab.

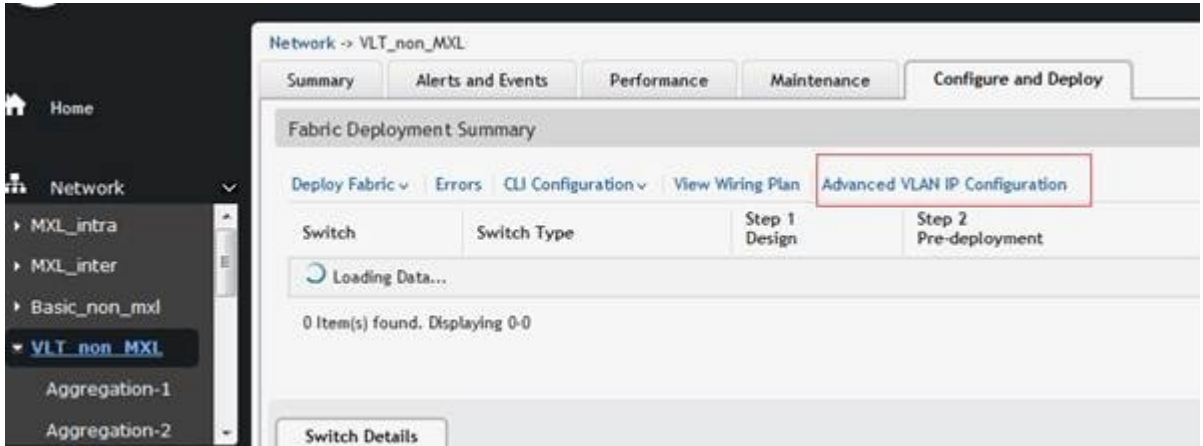



Figure 14. Three-Tier Layer 3 with Resiliency (Routed VLT) with VLT Option + Advanced VLAN IP Configuration

3. **Layer 3 with Resiliency (Routed VLT) — Basic option** — If you select the **Basic** option, configure the VLAN with the primary and secondary IP addresses for each access switch.
4. **Layer 3 with Resiliency (Routed VLT) — Blade MXL with IntraChassis option**: For this topology, select the deployment type with an MXL Blade switch with Resiliency (VLT) and the **Intrachassis (within the same chassis) resiliency** option. Enter the VLAN ID, primary, and secondary IP addresses.

## Using the Fabric Design Wizard

To design the following types of customized fabrics based on your workload requirements for your current and future needs, use the **Fabric Design Wizard**:

 **NOTE:** If you are designing a Layer 2 fabric using an IOA blade, refer to [Using the IOA Pre-deployment Wizard](#).

- **Layer 2** — Use the Layer 2 VLT fabric for workload migration over virtualized environments. Refer to [VLT](#) and [Selecting a Layer 2 and Layer 3 with Resiliency \(Routed VLT\)](#) fabric.
- **Layer 3 distributed core** — Use the Layer 3 distributed core for large fabric deployments. Refer to [Conventional Core Versus Distributed Core](#)
- **Layer 3 with Resiliency (Routed VLT)** — Use the Layer 3 fabric to extend equal cost multipathing capabilities. Refer to [Selecting a Layer 2 and Layer 3 with Resiliency \(Routed VLT\)](#).

This wizard allows you to create, edit, delete, and view the fabric.

To design a fabric, use the following settings:

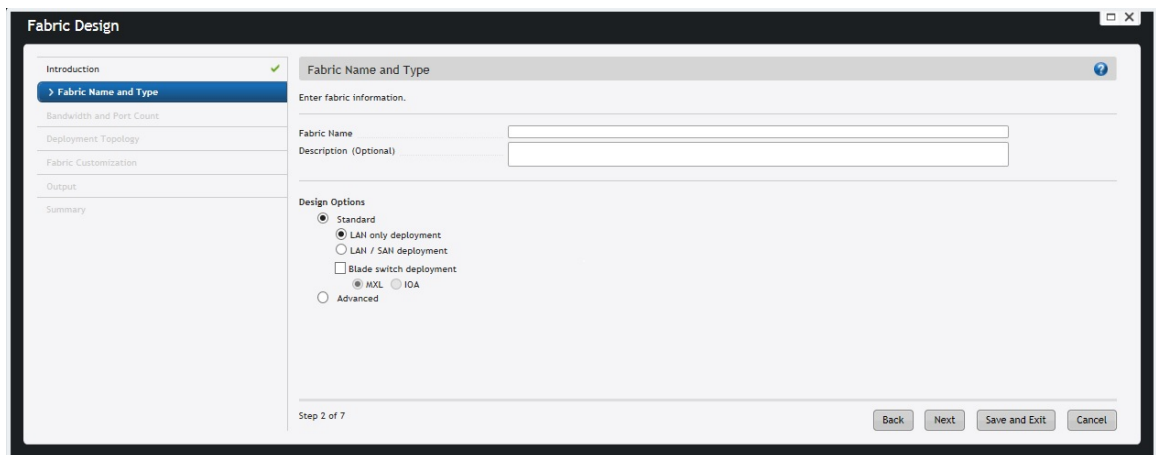
1. **Fabric Name and Type** — Select the fabric name, type, and description. Enable LAN, LAN/SAN, and blade switch deployments, if needed.

- a. To design a Standard Fabric:
  1. **Bandwidth and Port Count** — Configure the number of edge port uplinks to the WAN connection and downlinks required (for example, to servers or ToRs) for deployment as well as for future expansion.
  2. **Deployment Topology** — Select a Layer 2 or Layer 3 solution from a list of all applicable deployment topologies based on the fabric requirements entered on the **Bandwidth and Port Count** and **Fabric Name and Type** screens. To configure VLTi links and fabric links, use the **Advanced options**. For more information, refer to [Deployment Topology Use Cases](#).
  3. **Fabric Customization** — Select the switch names, models, and switch roles (aggregation or access) and modify the fabric link bandwidth for two-tier and three-tier fabrics.
- b. To design an Advanced Fabric:
  1. **Core Configuration** (Three-tier topologies only) — Configure the core switch names and models. Allocate the remaining bandwidth to the appropriate link types.
  2. **Aggregation Configuration** — Configure the aggregation switch names and models. Allocate the remaining bandwidth to the appropriate link types.
  3. **Access Configuration** — Configure access switch names and models. Configure switch model-specific settings. Allocate the remaining bandwidth to the appropriate link types.
  4. **Port Configuration** — Configure the proposed port numbers for links.
2. **Output** — View future switches and links and the fabric in the following formats:
  - graphical wiring plan
  - tabular wiring plan
  - graphical network topology
  - tabular network topology
3. **Summary** — View a summary of the fabric design or export the design.

## Fabric Design — Fabric Name and Type

To simplify and automate the design process, AFM provides the **Fabric Design Wizard** to design a Layer 2, Layer 3, or Layer 3 with Resiliency (Routed VLT) fabric based on current and future data center capacity requirements. Refer to [Designing the Fabric](#) and [Using the Fabric Design Wizard](#).

To generate a physical wiring plan for the fabric during the design phase, enter the data center capacity requirements. The wiring plan is typically given to the network operator, who uses it to build the physical network. For information about designing a fabric, refer to [Selecting Distributed Core](#) and [Selecting a Layer 2 and Layer 3 with Resiliency \(Routed VLT\)](#).



**Figure 15. Fabric Design Wizard — Fabric Name and Type**

1. From the menu, click **Network** and then the **Design Fabric** tab.
2. Click **New Fabric**.  
The **Introduction** screen of the **Fabric Design** wizard appears.
3. Review the introduction and click **Next**.  
The **Fabric Name** screen appears.
4. Enter the name of the fabric in the **Fabric Name** field.  
The fabric name must be unique. The range is 1–17 characters. AFM supports the following character types:
  - alphanumeric
  - underscore ( \_ )
  - +
5. (Optional) In the **Description** field, enter the description of the fabric.  
There is no character restriction. The range is 1–128 characters.
6. Navigate to the **Design Options** area.  
Select one of the following options:
  - **Standard** — View suggested topologies based on available switch types. For more information, refer to the following section.
    - **LAN only deployment**
      - \* **Blade Switch Deployment** — Create a fabric using blade switches (MXL or IOA). This option is for a Layer 2 fabric or Layer 3 with Resiliency (Routed VLT) fabric LAN deployment. Select a blade switch type:
        - **MXL**: To use an MXL blade switch, select the **MXL** radio button.
        - **IOA**: To use an IOA blade switch, select the **IOA** radio button. Use this option for a Layer 2 fabric.
    - **LAN/SAN deployment**
      - \* **NPIV Proxy Gateway (NPG)** — Supports fibre channel (FC) interfaces. Uses the S5000 as a N\_Port ID Virtualization (NPIV) Proxy Gateway. This option provides a gateway between

the fibre channel switch and server. Configure up to eight VLANs with a VLAN ID range of 2–4094 on the fiber channel and associate these VLANs with any FC port.

- \* **iSCSI** — Supports iSCSI interfaces.
- **Advanced** — Select to create one of the following topologies:
  - One-tier
  - Two-tier.
  - Three-tier.

For more information, refer to [Advanced Fabric Design](#).

7. Click **Next** and review the uplink and downlink bandwidth settings on the **Bandwidth and Port Count** screen.

## Standard Fabric

To design a standard Layer 2, Layer 3, or Layer 3 with Routed VLT fabric, use the following screens. Specify the available amount and type of bandwidth, then select a topology from the provided options.

1. [Standard Fabric Design — Bandwidth and Port Count](#)
2. [Standard Fabric Design — Deployment Topology](#)
3. [Standard Fabric Design — Fabric Customization](#)

### Standard Fabric Design — Bandwidth and Port Count

The **Bandwidth and Port Count** screen displays the default values for the fabric uplinks and downlinks. Uplinks connect from the fabric up to the next upstream tier of devices toward the core of the network. The minimum number of uplinks is two: one uplink is the active link and one uplink is for redundancy. Downlinks connect from the fabric to the next tier down of devices or servers towards the edge of the network. These values (1 GB, 10 GB, or 40 GB) are based on the selected options in the **Fabric Name and Type** screen. The values for the uplink ports, downlink ports, and bandwidth that you enter determine the AFM fabric topology.



**Fabric Design: North\_Core**

Introduction ✓

Fabric Name and Type ✓

> **Bandwidth and Port Count**

Deployment Topology

Fabric Customization

Output

Summary

**Bandwidth and Port Count** ?

Enter Bandwidth and Port Specifications.

**Bandwidth Specification**

Uplink Bandwidth (in Gb) 10

Downlink Bandwidth (in Gb) 10

Number of edge ports required by the fabric:

|                | Current | Future | Total |
|----------------|---------|--------|-------|
| Uplink Ports   | 2       | 0      | 2     |
| Downlink Ports | 2       | 0      | 2     |

Step 3 of 7

Back Next Save and Exit Cancel

**Figure 16. Standard Fabric Design — Bandwidth and Port Count**

1. In the **Bandwidth Specification** section:
  - a. Select the uplink bandwidth (10 GB or 40 GB) from the **Uplink Bandwidth** drop-down menu.
  - b. Select the downlink bandwidth (1 GB, 10 GB, or 40 GB) from the **Downlink Bandwidth** drop-down menu.
    - If you select the **1 Gb Downlink Bandwidth** option, AFM supports deployment topologies using S55 and S60 switches on the access side.
    - If you select the **10 Gb Downlink Bandwidth** option, AFM supports deployment topologies using S4810 and S4820T switches on the access side.
    - If you select the **40 Gb Downlink Bandwidth** option, AFM supports deployment topologies using Z9000 and S6000 switches on the access side.
2. In the **Number of edge ports required by the fabric** section, enter the number of required uplink ports (connections to the WAN) for initial deployment in the **Uplink Ports Current** column.
  - The minimum number of uplinks is two and the number of uplinks must be even. One uplink is for redundancy.
  - For fabric using 10 GB bandwidth, AFM supports 2–32 uplinks.
  - For fabric using 40 GB Bandwidth, AFM supports 2–8 uplinks.
  - For a Layer 2 VLT fabric or a Layer 3 with Resiliency (Routed VLT) fabric, an edge port link (uplink) connects to the aggregation or core switches that connect outside the fabric. For a three-tier fabric, edge links connect to the core switches. For a two-tier fabric, edge links connect to aggregation switches.
  - For Layer 3 distributed core, an edge port link (uplink) connects to the first two leaves that connect to the edge WAN, which typically connects to an internet service provider (ISP).
3. In the **Downlink Ports Current** column, enter the required number of downlink ports for initial deployment. The default is two downlink ports and the number of ports must be even.
4. In the **Uplink Ports Future** column, enter the required number of uplink ports (connections to the WAN) for future expansion of the fabric. If the future ports are not reserved, you cannot expand the fabric in the future.

- In the **Downlink Ports Future** column, enter an even number of downlink ports (connections to the servers, switches, or ToR) required for future expansion of the fabric.

**NOTE:** If you select the **Blade switch (MXL) deployment** option in the **Fabric Name and Type** screen, the **Bandwidth and Port Count** screen displays a **Blade Switch Pairs** option instead of a **Downlink Ports** option in the **Number of edge ports required by the fabric** area.

- If you are connecting to Fibre Channel ports, navigate to the NPG Ports column and then enter the required number of current and future ports for this interface in the **Current** and **Future** columns. The minimum number of Fibre Channel ports is two.

The maximum number of Fibre Channel ports (current and future) is the number of S5000 access switches multiplied by 12.

- If you are connecting to iSCSI ports, navigate to the iSCSI ports column and then enter the required number of current and future ports for this interface in the **Current** and **Future** columns. The minimum number of iSCSI ports is two.

The maximum number of iSCSI ports (current and future) is eight.

- Review the values and then click **Next** to go to the **Deployment Topology** screen.

## Standard Fabric Design — Deployment Topology

AFM displays applicable deployment topologies based on the data center workload requirements specified in the **Fabric Name and Type** and **Bandwidth and Port Count** screens. By default, AFM selects one of the topologies. To display additional deployment topology options, click the deployment topology filter icon on the top right of the screen. The output from these screens and the **Deployment Topology** and **Fabric Customization** screens create the network topology and the detailed wiring plan. For more information, refer to [Deployment Topology Use Cases](#). Based on your design requirements, create a one, two, or three-tier topology. To filter the deployment topologies, select the **Layer 2**, **Layer 3**, or **Layer 3 with Resiliency (Routed VLT)** options. You can also filter by device type, cable type, or other information by selecting the filter icon in the upper right of the screen.

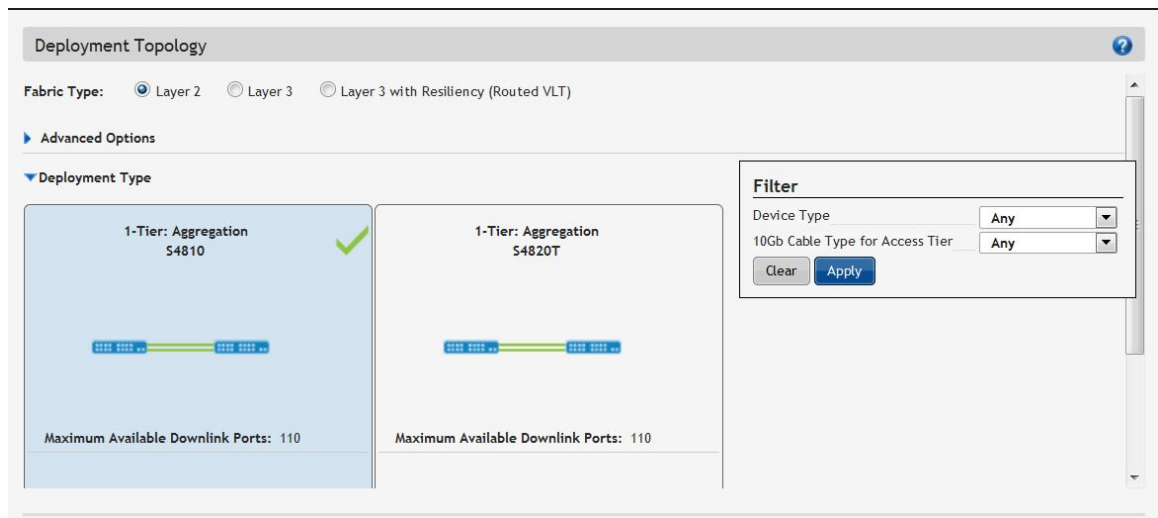


Figure 17. Standard Fabric Design — Deployment Topology

**Table 19. Deployment Topology (Filter) Options**

| Deployment Options   | Description  |
|--|--|
| Oversubscription Ratio (Layer 3 distributed core deployment topology only) | For a Layer 3 deployment, the following oversubscription ratios are available: <ul style="list-style-type: none"> <li>• 1:1</li> <li>• 3:1</li> <li>• 4:1</li> <li>• 5:1</li> </ul>              |
| Resiliency in Access Devices   | Configures Virtual Router Redundancy Protocol (VRRP) on the downlink.  |
| 10 GB Cable Type for Access Tier   | This option is applicable only for topologies where S4810 and S4820T can be swapped. <ul style="list-style-type: none"> <li>• <b>SFP+</b></li> <li>• <b>RJ-45</b></li> </ul>                     |
| Stacked/Non-Stacked  | Selects stacking for the applicable topologies. If you select stacking, you can enable VLTi.   |
| High Stream Buffering  | <ul style="list-style-type: none"> <li>• <b>high stream buffering</b> – For an access layer using S60 switches</li> <li>• <b>low latency</b> – For an access layer using S55 switches</li> </ul> |
| Resiliency In MXL (Routed VLT)   | <ul style="list-style-type: none"> <li>• <b>Intra-chassis</b> – Within the chassis (mVLT)</li> <li>• <b>Inter-chassis resiliency</b> – Across 2 chassis (VLT)</li> </ul>                         |

- **One-Tier Topology** – Contains two switches and a downlink and uplink configuration. There are no fabric links.



**Figure 18. VLT One-Tier Topology: Aggregation Layer**

For more information about one-tier topologies, refer to [Designing a Layer 2 VLT and Layer 3 with Resiliency \(Routed VLT\) Fabric](#).

- **Two-Tier Topology** – Contains two layers of switches. Has fabric interlinks, uplinks, and downlinks. Uses Distributed Core (spine and leaf) or VLT (aggregation and access). For more information about two-tier topologies, refer to [Designing a Layer 2 VLT and Layer 3 with Resiliency \(Routed VLT\) Fabric](#) and [Selecting a Layer 3 Distributed Core Fabric Design](#).

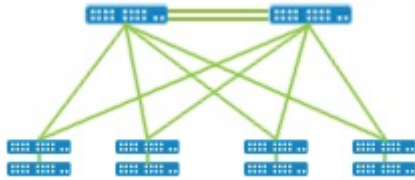


Figure 19. Two-Tier VLT Topology: Aggregation and Access Layer

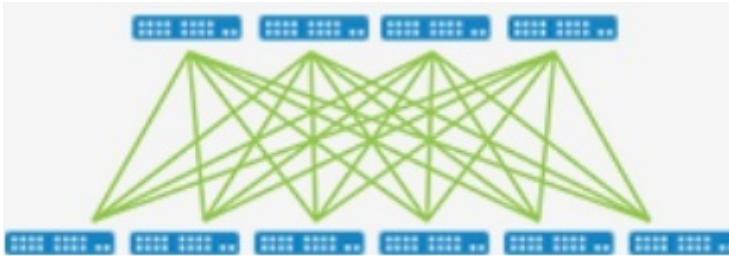


Figure 20. Two-Tier Distributed Core Topology: Spine and Leaf

- **Three-Tier Topology** — Layer 3 with Resiliency (Routed VLT). Has three layers of switches, fabric interlinks, uplinks and downlinks. For more information about three-tier topologies, refer to [Designing a Layer 2 VLT and Layer 3 with Resiliency \(Routed VLT\) Fabric](#).

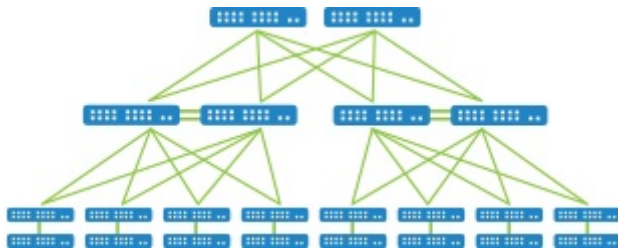


Figure 21. Three-Tier VLT Topology Core: Aggregation — Access Layer

The following illustration and table describe the deployment types for a fabric.

 **NOTE:** For more information about topologies, refer to the [Designing a Layer 2 VLT and Layer 3 with Resiliency \(Routed VLT\) Fabric](#) and [Selecting a Layer 3 Distributed Core Fabric Design](#).

### Selecting a Fabric Deployment Type


1. From the menu, click **Network** and then the **Design Fabric** tab.
2. Click **New Fabric**.
3. Navigate to the **Deployment Topology** screen.
4. In the Fabric Type area, select one of the following fabric types:
  - **Layer 2** — Use the Layer 2 VLT fabric for workload migration over virtualized environments. For more information, refer to VLT and Selecting a Layer 2 VLT and Layer 3 with Resiliency (Routed VLT) Fabric Design.
  - **Layer 3** — Use the Layer 3 distributed core for large fabric deployments. For more information, refer to Conventional Core Versus Distributed Core.
  - **Layer 3 with Resiliency (Routed VLT)** — Use the Layer 3 fabric to extend equal cost multipathing capabilities. For more information, refer to Selecting a Layer 2 VLT and Layer 3 with Resiliency (Routed VLT) Fabric Design.

If you select LAN/SAN deployment with iSCSI or Fibre Channel storage facing ports using the Fabric Designer wizard, AFM automatically selects a Layer 2 fabric and the Layer 2, Layer 3, and Layer 3 options in the Deployment Topology screen are not displayed.

5. Select the appropriate deployment topology that uses the core switches and aggregation switch types in the fabric.
6. (Optional) Click **Advanced Options** to configure VLTi links and fabric links.
  - a. Configure the VLTi and fabric link options:
    - Interchassis Link options:
      - Core — Specify the number of links and bandwidth.
      - Aggregation — Specify the number of links and bandwidth
      - Access — Specify the number of links and bandwidth.
    - Fabric Link options:
      - Core and Aggregation — Specify the bandwidth.
      - Aggregation and Access — Specify the bandwidth.
  - b. Click **Refresh Deployment Type** to apply the advanced options and view the new deployment topologies.
7. To display deployment topology options, click the deployment topology filter icon on the top right of the screen . Only applicable filter options are displayed.
8. Configure the filter options for the deployment topology and click **Apply**.
9. Click **Next** to go to the **Fabric Customization** screen.

### **Configuring Advanced Options**

For a Layer 2 or Layer 3 with Resiliency (Routed VLT) fabric, customize the bandwidth between the aggregation and access switches. If you configure the fabric link bandwidth between the aggregation and access switches from the **Enabled Link Bandwidth Customization** option on the **Deployment Topology** screen, the two redundant links share the selected bandwidth equally. For example, if you select a fabric link bandwidth of 80 GB between the aggregation and access switches, you can configure 40 GB for each redundant link on the **Fabric Customization** screen.

 **NOTE:** If you select LAN/SAN deployment with iSCSI or Fibre Channel storage facing ports using the Fabric Designer wizard, AFM automatically selects a Layer 2 fabric and the Layer 2, Layer 3, and Layer 3 options in the **Deployment Topology** screen do not appear.

1. In the **Deployment Topology** section, select one of the following options:
  - **Layer 2**
  - **Layer 3 with Resiliency (Routed VLT)**
2. Click the blue arrow by **Advanced Options**.  
The **Advanced Options** appear.

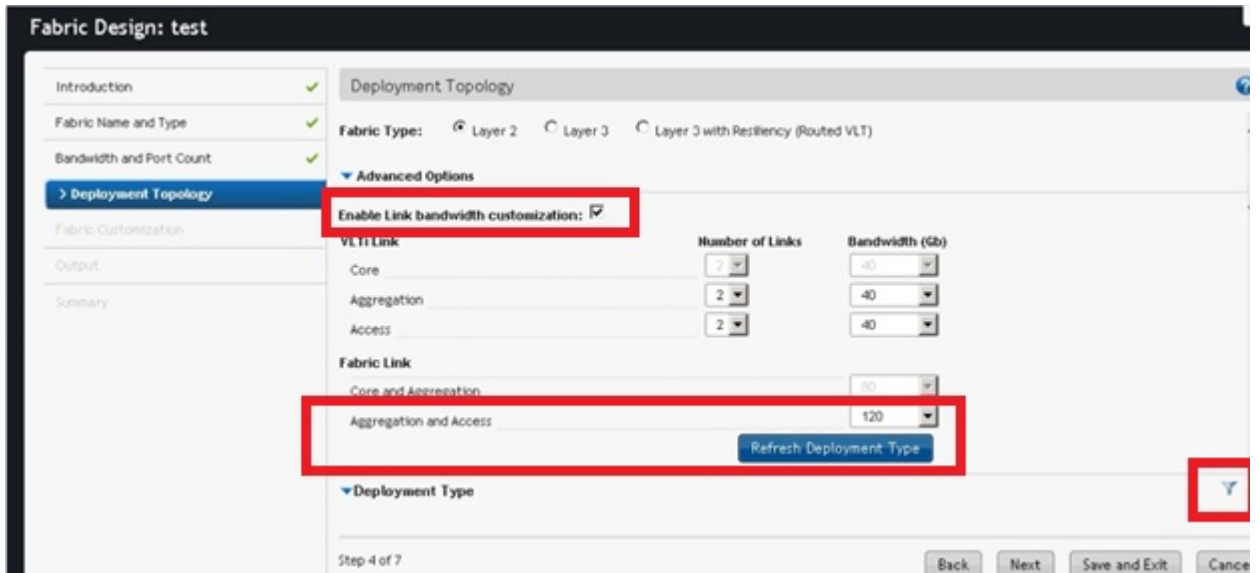


Figure 22. Enabled Link Bandwidth Customization Option

3. Check the **Enable Link Bandwidth Customization** check box.
4. Select the number of links and the fabric bandwidth value from the appropriate drop-down menu. Only the applicable options for a select topology are configurable. For example, for a two-tier topology, select the **120 Gb** bandwidth option to customize the bandwidth from 20 to 120 GB in increments of 20 GB on the **Fabric Customization** screen.
5. In the **Deployment Type** section, select the appropriate deployment type.
6. (Optional) To display deployment topology filtering options, click the deployment topology filtering icon on the top right of the screen. Only applicable options are displayed. Configure the filter options for the deployment topology and click **Apply**.
7. Select a topology and click **Next**.
8. (Optional) From the **Fabric Link Bandwidth** drop-down menu, select the fabric link bandwidth for each switch that you want to customize.

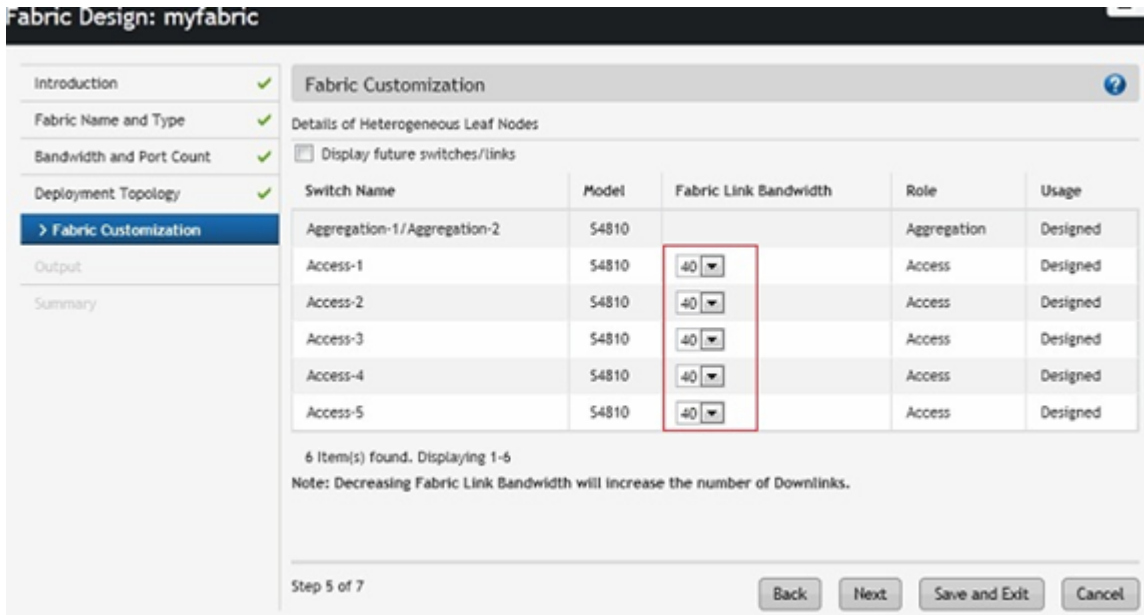


Figure 23. Customizing Fabric Link Bandwidth between Switches

9. Click **Next** to go to the **Output** screen.

### Standard Fabric Design — Fabric Customization

To modify the fabric link bandwidth between the aggregation and access switches for two-tier and three-tier fabrics, use the **Fabric Customization** screen, which displays the switch names, models, and switch roles (spine, leaf, aggregation or access). For a Layer 2 or Layer 2 with Resiliency (Routed VLT) deployment topology, select S4810 or S4820T switches (mixed node) on the access side.

To customize the fabric, configure the **Advance Configuration** option for **Fabric Link between Aggregation and Access** to the maximum bandwidth for each access switch. For example, configure the maximum bandwidth as 120 GB at the **Deployment Topology** screen of the **Fabric Design** wizard. If you do not configure this option, the **Fabric Customization** screen is read-only. For information about the **Advanced Options**, refer to [Advanced Fabric Design](#). For information about tiers, refer to [Standard Fabric Design — Deployment Topology](#) and [Deployment Topology Use Cases](#).

1. From the menu, click **Network** and then the **Design Fabric** tab.
2. Click **New Fabric**.
3. Navigate to the **Fabric Customization** screen.
4. From the **Fabric Link Bandwidth** drop-down menu, select the fabric link maximum bandwidth for each access switch.

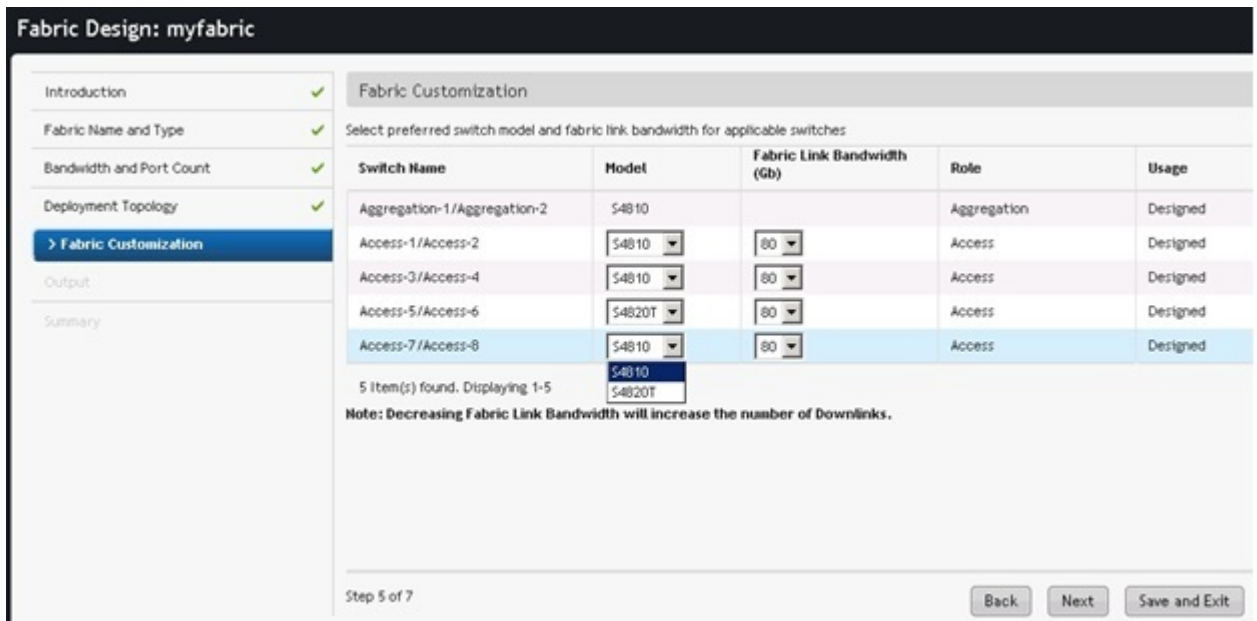


Figure 24. Standard Fabric Design — Fabric Customization

5. Click **Next** to go the **Output** screen.

## Advanced Fabric Design

To design custom fabrics for Layer 2 fabric or mixed node topologies with one-, two-, or three-tiers, refer to the following topics:

- [Advanced Fabric Design — Advanced Core Config](#)
- [Advanced Fabric Design — Advanced Aggregation Config \(One- or Two-Tier Topologies\)](#)
- [Advanced Fabric Design — Advanced Aggregation Config \(Three-Tier Topologies\)](#)
- [Advanced Fabric Design — Advanced Access Config](#)
- [Advanced Fabric Design — Port Configuration](#)

### Advanced Fabric Design — Advanced Core Config

On the **Advanced Core Config** screen of the **Fabric Design** wizard, you can configure the switch settings for the core.

This screen displays the default values for the fabric uplinks and inter chassis (VLT or MLAG) links. Uplinks connect the fabric from the next upstream tier of devices to the aggregation layer of the network. The minimum number of uplinks is two: one uplink is the active link and one uplink is for redundancy.



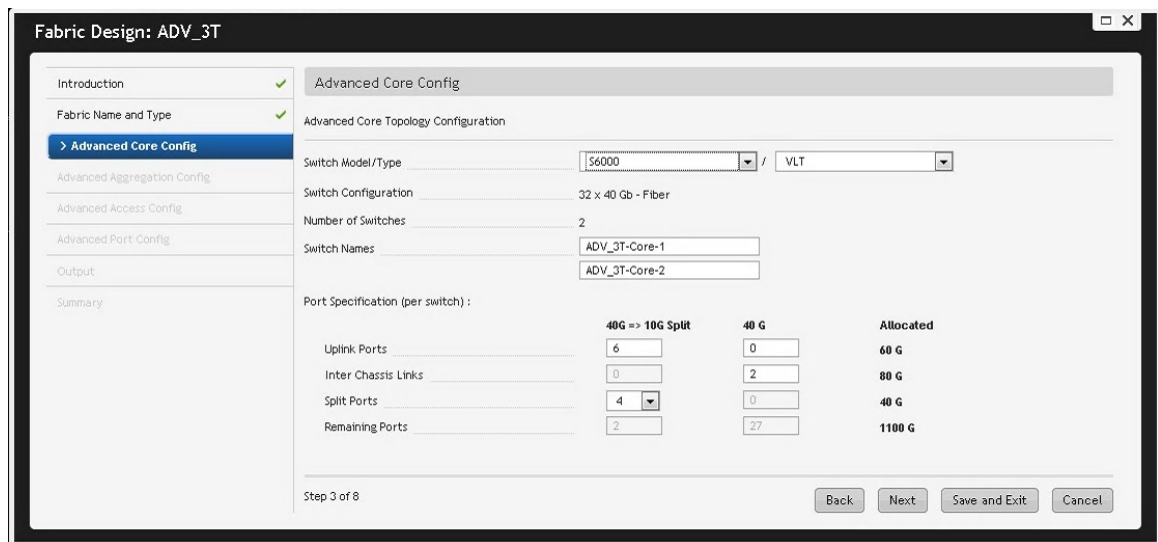


Figure 25. Advanced Core Config Screen

1. Select a switch model from the **Switch Model** drop-down menu:
  - Z9500
  - S6000
  - S4820T
  - S4810
  - S4048-ON
  - N4064F
  - N4064
  - N4032F
  - N4032
  - N3048P
  - N3048
  - N3024P
  - N3024F
  - N3024
2. For one-tier topologies, from the **Type** menu, this setting is automatically **VLT** or **MLAG**.

Table 20. Multi-Tier Topology Core Switches

| Aggregation Switch | Deployment Type |      |
|--------------------|-----------------|------|
|                    | VLT             | MLAG |
| N3000 series       |                 | NE   |
| N4000 series       |                 | NE   |
| S4048-ON           | NE              |      |
| S4810              | NE              |      |
| S4820              | NE              |      |


| Aggregation Switch | Deployment Type |      |
|--------------------|-----------------|------|
|                    | VLT             | MLAG |
| S6000              | NE              |      |
| Z9500              | NE              |      |

“NE” denotes non-endpoint switches that can extend with another tier.

The **Number of switches** field displays the number switches in the inter chassis pair.

- (N3000 and N4000 series switch models only) Select an optional module type from the **Optional Module** drop-down menu. Options vary based on the core switch type. Refer to the following table for supported options.

**Table 21. Core Config Optional Module Options**

| Switch Type and Mode | Optional Module | Supported Options  |
|----------------------|-----------------|--|
| N3000 series         | 1/1/1           | 2 x 10 G – Fiber<br>2 x 10 G – Copper  |
| N4000 series         | 1/1/1           | 4 x 10 G – Fiber<br>4 x 10 G – Copper<br>2 x 40 G – Fiber  |
| None                 |                 |  <b>NOTE:</b> Select this option if you do not have any optional modules in this slot. |

- (Z9500 series switch model only) In the **License Type** field, select the number of ports licensed: **36** (default); **84**; or **132**.

 **NOTE:**

- AFM does not validate whether the specified number of licensed ports is correct for the switch. An incorrect setting causes the fabric deployment to fail.
  - This setting applies for both members in VLT mode.
  - You can edit this value without restriction before beginning pre-deployment steps for the switch. After pre-deployment begins, you can only edit the number of ports licensed upwards (for example, 36–84).
- The default switch names are *FabricName-Core-1* and *FabricName-Core-2*. To customize the switch names, enter a name in each of the **Switch Names** fields.
  - In the **Port Specification (per switch)** section, configure the number of ports for uplinks, downlinks, inter chassis links, or split ports, in the appropriate entry fields.

**NOTE:**

- The type of ports you can configure for this setting depend upon the number of topology tiers you select and the switch model type.
- Configure at least one inter chassis link and one uplink for **VLT** or **MLG** type topologies.
- You cannot edit the **Remaining Ports** field.
- All values must be even.
- The maximum configurable bandwidth is 160 GB for **VLT** or **MLG** type topologies.
- The **Inter Chassis** link range is 2–16 for Dell OS switches and 2–8 for N series switches.
- In the **Split Ports** field, you can enable available 40G ports to act as 10G ports for any device port. You can select the number of 10G ports split from the 40G port from the drop-down menu.

The **Allocated** column displays the total amount of configured link bandwidth (in GB).

7. The **10 G Uplink Physical Type** setting appears if the selected switch has 10G ports of both physical types. In this setting, you can customize the 10G physical type as either **Copper** or **Fiber**



**NOTE:** You cannot change the physical type for an uplink after the fabric is pre-deployed.

8. Review the values and click **Next** to go to the **Advanced Aggregation Config** screen.

### Advanced Fabric Design — Advanced Aggregation Config (One- or Two-Tier Topologies)

The **Advanced Aggregation Config** screen of the **Fabric Design** wizard displays the default values for the fabric uplinks and inter chassis (VLT or MLAG) links. Uplinks connect the fabric from the next upstream tier of devices to the core of the network. The minimum number of uplinks is two: one uplink is the active link and one uplink is for redundancy.

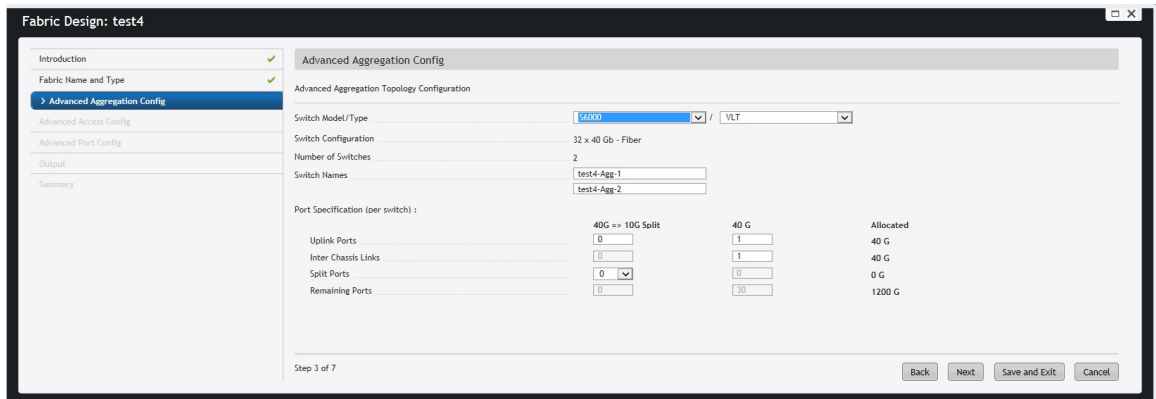


Figure 26. Advanced Aggregation Config Screen

1. Select a switch model from the **Switch Model** drop-down menu:
  - **Z9500**
  - **S55** (one-tier topology only)
  - **S60** (one-tier topology only)
  - **S6000**
  - **S4820T**
  - **S4810**
  - **S4048-ON**
  - **S3048-ON** (one-tier topology only)
  - **N4064F**

- **N4064**
- **N4032F**
- **N4032**
- **N3048P**
- **N3048**
- **N3024P**
- **N3024F**
- **N3024**
- **N2048P** (one-tier topology only)
- **N2048** (one-tier topology only)
- **N2024P** (one-tier topology only)
- **N2024** (one-tier topology only)
- **MXL** (one-tier topology only)

The **Number of switches** field displays the number switches in the inter chassis pair.

**Table 22. One-Tier Topology Aggregation Switches**

| Aggregation Switch | Deployment Type |      |       |            |
|--------------------|-----------------|------|-------|------------|
|                    | VLT             | MLAG | Stack | Standalone |
| S55                |                 |      | E     | E          |
| S60                |                 |      | E     | E          |
| S3048-ON           | E               |      | E     | E          |
| S4048-ON           | E               |      | E     | E          |
| S4810              | E               |      | E     | E          |
| S4820              | E               |      | E     | E          |
| S6000              | E               |      | E     | E          |
| MXL                | E               |      | E     | E          |
| N2000 series       |                 | E    | E     | E          |
| N3000 series       |                 | E    | E     | E          |
| N4000 series       |                 | E    | E     | E          |
| Z9500              | E               |      |       | E          |

"E" denotes endpoint switches that cannot extend to another tier.

**Table 23. Two-Tier Topology Aggregation Switches**


| Aggregation Switch | Deployment Type |      |       |            |
|--------------------|-----------------|------|-------|------------|
|                    | VLT             | MLAG | Stack | Standalone |
| N3000 series       |                 | NE   |       |            |
| N4000 series       |                 | NE   |       |            |
| S4048-ON           | NE              |      |       |            |

| Aggregation Switch | Deployment Type |      |       |            |
|--------------------|-----------------|------|-------|------------|
|                    | VLT             | MLAG | Stack | Standalone |
| S4810              | NE              |      |       |            |
| S4820              | NE              |      |       |            |
| S6000              | NE              |      |       |            |
| Z9500              | NE              |      |       |            |

"NE" denotes non-endpoint switches that can extend with another tier.

- (N3000 and N4000 series switch models only) Select an optional module type from the **Optional Module** drop-down menu. Options vary based on the switch type. Refer to the following table for supported options.

**Table 24. Aggregation Config Optional Module Options**

| Switch Type and Mode         | Optional Module                | Supported Options  |
|------------------------------|--------------------------------|--|
| N3000 series                 | 1/1/1                          | 2 x 10 G – Fiber<br>2 x 10 G – Copper  |
| N4000 series                 | 1/1/1                          | 4 x 10 G – Fiber<br>4 x 10 G – Copper<br>2 x 40 G – Fiber  |
| S55 (one-tier topology only) | 0/50<br>0/48                   | 2 x 10 G – Fiber<br>2 x 12 G – Fiber (Stack mode only)<br>2 x 10 G – Fiber   |
| S60 (one-tier topology only) | 0/48<br>0/50 (Stack mode only) | 2 x 10 G – Fiber<br>2 x 12 G – Fiber<br>1 x 24 G – Fiber   |
| MXL (one-tier topology only) | 0/41<br>0/49                   | 2 x 40 G – Fiber<br>4 x 10 G – Fiber<br>4 x 10 G – Copper  |
| None                         |                                |  <b>NOTE:</b> Select this option if you do not have any optional modules in this slot. |

- (Z9500 switch model only) In the **License Type** field, select the number of ports licensed: **36** (default); **84**; or **132**.

 **NOTE:**

- AFM does not validate whether the specified number of licensed ports is correct for the switch. An incorrect setting causes the fabric deployment to fail.
  - This setting applies for both members in VLT mode.
  - You can edit this value without restriction before beginning pre-deployment steps for the switch. After pre-deployment begins, you can only edit the number of ports licensed upwards (for example, 36–84).
4. The default switch names are *FabricName-Agg-1* and *FabricName-Agg-2*. To customize the switch names, enter a name in each of the **Switch Names** fields.
  5. In the **Port Specification (per switch)** section, configure the number of ports for uplinks and inter chassis links in the appropriate entry fields. If available for a particular switch configuration, you can also select the number of split ports.

**Table 25. Support for 40 GB to 10 GB Split**

| Core Switch | Aggregation Switch |       |       |       |          |          |
|-------------|--------------------|-------|-------|-------|----------|----------|
|             | Z9500              | S6000 | S4820 | S4810 | S4048-ON | S3048-ON |
| Z9500       |                    |       |       | S     | S        | S        |
| S6000       |                    |       |       | S     | S        | S        |
| S4820       |                    |       |       |       |          | S        |
| S4810       |                    |       |       | S     | S        | S        |
| S4048-ON    |                    |       | S     | S     | S        | S        |
| N4000       |                    |       |       |       |          | S        |

"S" denotes support for 40 GB to 10 GB split.

**Table 26. Support for 40 GB to 10 GB Split (Continued)**

| Core Switch | S60   | S55 | MXL | N4000 | N3000 | N2000 |
|-------------|-------|-----|-----|-------|-------|-------|
|             | Z9500 | S   | S   | S     | S     | S     |
| S6000       | S     | S   | S   | S     | S     | S     |
| S4820       | S     | S   | S   |       | S     | S     |
| S4810       | S     | S   | S   | S     | S     | S     |
| S4048-ON    | S     | S   | S   | S     | S     | S     |
| N4000       | S     | S   | S   | S     | S     | S     |

"S" denotes support for 40 GB to 10 GB split.

 **NOTE:**

- Configure at least two inter chassis links and two uplinks.
- All values must be even.
- You cannot edit the **Remaining Ports** field.
- The maximum configurable bandwidth is 320 GB.
- Inter chassis links do not support **40G ⇒10G Split**.

- The **40G ⇌ 10G Split** uplink bandwidth range is 2–32. This setting is not applicable to N3048, N3048P, N3024P, N3024F, or N3024 switch models.
- The **40G** uplink bandwidth range is 2–8. This setting is not applicable to N3048, N3048P, N3024P, N3024F, or N3024 switch models.
- The **10G** uplink bandwidth range is 2–32. This setting not applicable to Z9500 or S6000 switch models.
- The **Inter Chassis** link range is 2–16.

The **Allocated** column displays the total amount of configured uplink bandwidth (in GB).

6. The **10 G Uplink Physical Type** setting appears if the selected switch has 10G ports of both physical types. In this setting, you can customize the 10G physical type as either **Copper** or **Fiber**

 **NOTE:** You cannot change the physical type for an uplink after the fabric is pre-deployed.

7. Review the values and click **Next** to go to the **Advanced Access Config** screen.

### Advanced Fabric Design — Advanced Aggregation Config (Three-Tier Topologies)

On the **Advanced Access Config** screen of the **Fabric Design** wizard, you can:

- [Add aggregation switches](#)
- [Edit aggregation switch information](#)
- [Remove aggregation switches](#)

The selected core switch model and the available, used, and total bandwidth values appear at the top of the screen.

#### Adding Aggregation Switches

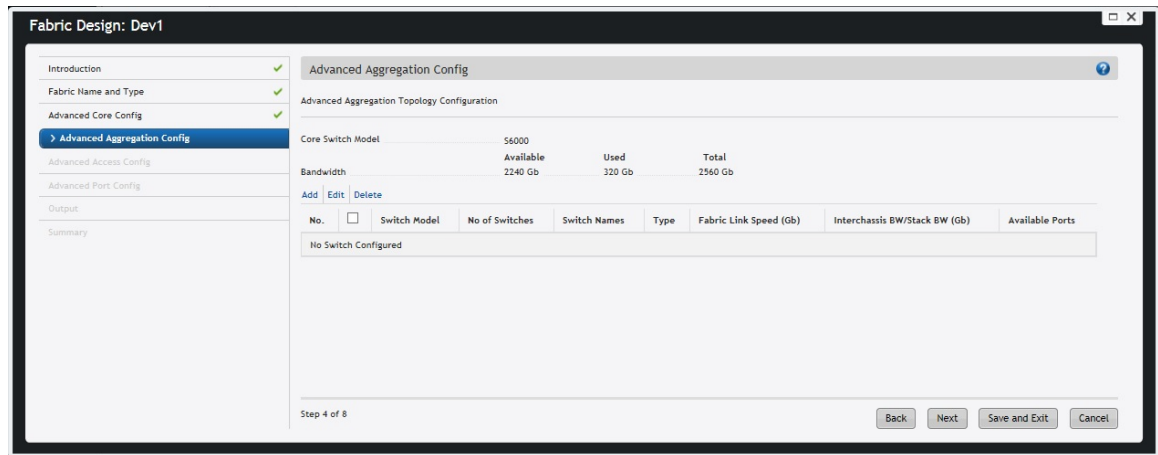


Figure 27. Advanced Aggregation Config Screen (Three-Tier Topologies)

1. In the upper left of the **Advanced Aggregation Config** screen, click **Add**. The **Add Switch Unit** dialog box appears.

### Add Switch Unit ✕

Fill the Aggregation switch configuration to be associated with fabric.

---

Core Switch ..... 3tier-Core-1,3tier-Core-2

Core Switch Model ..... S6000

| Bandwidth | Available | Used   | Total   |
|-----------|-----------|--------|---------|
|           | 1840 Gb   | 720 Gb | 2560 Gb |

Supports downlink

Switch Model/Type ..... S4810 / VLT

Switch Configuration ..... 48 x 10 Gb - Fiber, 4 x 40 Gb - Fiber

Number of VLT pairs ..... 1

Prefix Switch Name ..... 3tier-Agg

Use 40Gb => 10Gb Split for Fabric Link in Core

Port Specification (per switch) :

|                     | 10 G | 40G => 10G<br>Split | 40 G | Total |
|---------------------|------|---------------------|------|-------|
| Fabric Links        | 0    | 0                   | 0    | 0 G   |
| Inter Chassis Links | 0    | 0                   | 0    | 0 G   |
| Split Ports         | 0    | 8                   | 0    | 80 G  |
| Remaining Ports     | 48   | 0                   | 2    | 560 G |


**Figure 28. Add Switch Unit Dialog Box**

**NOTE:** The information and options in the **Add Switch Unit** dialog box vary based on the selected aggregation switch model.

2. Select **Supports downlink** if the switch connect servers or other switches which are not part of the fabric. When a switch is configured this way, that part of the fabric cannot extend any further.
3. Select a switch model from the **Switch Model** drop-down menu.
  - **S6000**
  - **S55** (only available if you select **Supports downlink**)
  - **S60** (only available if you select **Supports downlink**)
  - **S4820T**
  - **S4810**
  - **S4048-ON**
  - **S3048-ON** (only available if you select **Supports downlink**)
  - **N4064F**
  - **N4064**




- N4032F
- N4032
- N3048P
- N3048
- N3024P
- N3024F
- N3024
- MXL (only available if you select **Supports downlink**)
- Z9500

 **NOTE:** The switch model options vary depending on the core switch model.

4. From the **Type** menu, select one of the following settings:

- **Stack**
- **Standalone**
- **VLT** or **MLAG** (depending on the switch model selected).

 **NOTE:** **Stack** and **Standalone** settings are only available if you selected **Supports downlink** in step 1.

The **Number of switches** field displays the number switches in the inter chassis pair.

**Table 27. Three-Tier Topology Aggregation Switches**


| Aggregation Switch | Deployment Type |      |       |            |
|--------------------|-----------------|------|-------|------------|
|                    | VLT             | MLAG | Stack | Standalone |
| N3000 series       |                 | NE   |       |            |
| N4000 series       |                 | NE   |       |            |
| S4048-ON           | NE              |      |       |            |
| S4810              | NE              |      |       |            |
| S4820              | NE              |      |       |            |
| S6000              | NE              |      |       |            |
| Z9500              | NE              |      |       |            |

"NE" denotes non-endpoint switches that can extend with another tier.

5. (N3000 and N4000 series switch models only) Select an optional module type from the **Optional Module** drop-down menu. Options vary based on the core switch type. Refer to the following table for supported options.

**Table 28. Aggregation Config Optional Module Options**

| Switch Type and Mode   | Optional Module | Supported Options                  |
|--|-----------------|------------------------------------|
| S55 (available only if you select <b>Supports downlink</b> ) | 0/50            | 2 x 10 G — Fiber                   |
|  | 0/48            | 2 x 12 G — Fiber (Stack mode only) |

| Switch Type and Mode   | Optional Module        | Supported Options  |
|--|------------------------|--|
|  |                        | 2 x 10 G – Fiber   |
| S60 (available only if you select <b>Supports downlink</b> ) | 0/48                   | 2 x 10 G – Fiber   |
|  | 0/50 (Stack mode only) | 2 x 12 G – Fiber<br>1 x 24 G – Fiber   |
| MXL (available only if you select <b>Supports downlink</b> ) | 0/41<br>0/49           | 2 x 40 G – Fiber<br>4 x 10 G – Fiber<br>4 x 10 G – Copper  |
| N3000 series   | 1/1/1                  | 2 x 10 G – Fiber<br>2 x 10 G – Copper  |
| N4000 series   | 1/1/1                  | 4 x 10 G – Fiber<br>4 x 10 G – Copper<br>2 x 40 G – Fiber  |
| None   |                        |  <b>NOTE:</b> Select this option if you do not have any optional modules in this slot. |

6. (Z9500 switch model only) In the **License Type** field, select the number of ports licensed: **36** (default); **84**; or **132**.

 **NOTE:**


- AFM does not validate whether the specified number of licensed ports is correct for the switch. An incorrect setting causes the fabric deployment to fail.
- This setting applies for both members in VLT mode.
- You can edit this value without restriction before beginning pre-deployment steps for the switch. After pre-deployment begins, you can only edit the number of ports licensed upwards (for example, 36–84).

7. Select a deployment mode from the **Type** drop-down menu:

- **Standalone**
- **Stack**
- **VLT or MLAG** (N series only)

 **NOTE:** You can only select **Standalone** or **Stack** if you select **Supports downlink** in step 5.


8. (Z9500 switch model only) In the **License Type** field, select the number of ports licensed: **36** (default); **84**; or **132**.
9. (MXL, S55, or S60) Select an optional module type from the first and second **Optional Module** drop-down menus:

 **NOTE:** The first optional module menu name and options vary based on the access switch type and mode (standalone or stack). Refer to the following table for supported options.

**Table 29. Aggregation Config Optional Module Options**

| Switch Type and Mode | Optional Module | Supported Options   |
|----------------------|-----------------|---|
| S55 (standalone)     | 0/48            | 2 x 10 G – Fiber  |
|                      | 0/50            | 2 x 10 G – Fiber  |
| S55 (stack)          | 0/48            | 2 x 10 G – Fiber  |
|                      | 0/50            | 2 x 12 G – Fiber  |
| S60 (standalone)     | 0/48            | 2 x 10 G – Fiber  |
| S60 (stack)          | 0/48            | 2 x 10 G – Fiber  |
|                      | 0/50            | 2 x 12 G – Fiber<br>1 x 24 G – Fiber                      |
| MXL                  | 0/41            | 2 x 40 G – Fiber<br>4 x 10 G – Fiber<br>4 x 10 G – Copper |
|                      |                 | 0/48  |

None

 **NOTE:** Select this option if you do not have any optional modules in this slot.

**10.** (VLT or MLAG mode only) Enter a value in the **Number of VLT pairs** or **Number of MLAG** pairs field.

 **NOTE:** Both switches in the VLT or MLAG pair must be the same model type.


**11.** (Stack mode only) Enter a value in the **Number of Stacks** field.

 **NOTE:** All switches in the stack must be the same model type.

The **Number of Switches Per Stack** menu is automatically set to **2**.

**12.** (Standalone mode only) Enter a value in the **Number of Switches** field.

**13.** The default switch name is *FabricName-Agg*. To specify a custom name, enter one in the **Prefix Switch Name** field.

 **NOTE:** Only the name of the first switch in a stack can be changed. The other switch is appended (*standby*).

The name must be unique. The range is 1–18 characters. AFM supports the following character types:

- alphanumeric
- underscore ( \_ )
- -

**14.** To use 40 GB split port from the core layer, select **Use 40 Gb => 10 Gb for Fabric Link in Core**.

**Table 30. Support for 40 GB to 10 GB Split**

| Core Switch | Aggregation Switch |       |       |       |          |          |
|-------------|--------------------|-------|-------|-------|----------|----------|
|             | Z9500              | S6000 | S4820 | S4810 | S4048-ON | S3048-ON |
| Z9500       |                    |       |       | S     | S        | S        |
| S6000       |                    |       |       | S     | S        | S        |
| S4820       |                    |       |       |       |          | S        |
| S4810       |                    |       |       | S     | S        | S        |
| S4048-ON    |                    |       |       | S     | S        | S        |
| N4000       |                    |       |       |       |          | S        |

"S" denotes support for 40 GB to 10 GB split.

**Table 31. Support for 40 GB to 10 GB Split (Continued)**

| Core Switch | S60   | S55 | MXL | N4000 | N3000 | N2000 |
|-------------|-------|-----|-----|-------|-------|-------|
|             | Z9500 | S   | S   | S     | S     | S     |
| S6000       | S     | S   | S   | S     | S     | S     |
| S4820       | S     | S   | S   |       | S     | S     |
| S4810       | S     | S   | S   | S     | S     | S     |
| S4048-ON    | S     | S   | S   | S     | S     | S     |
| N4000       | S     | S   | S   | S     | S     | S     |

"S" denotes support for 40 GB to 10 GB split.

- 15.** To allocate ports, enter or select a value in the appropriate field in the **Port Specification (per switch)** or **Port Specification (per stack)** section.


- **Fabric Link**
- **Stack Ports** (Stack mode only)
  - ✎ **NOTE:** Configure at least two fabric links.
- **Inter Chassis Link** (VLTi or MLAG)
- **Split Ports** (If switch model configuration allows)

The **Split Ports** field enables available 40G ports to act as 10G ports for any device type. You can select the number of 10G ports split from a 40G port from the drop-down menu. The **Remaining Ports** field displays the number of available ports; you cannot edit this field. The **Total** column displays the amount of bandwidth in GB allocated to each link type.

- 16.** To save the current switch information, click **OK**.  
To close the window without saving information, click **Cancel**.
- 17.** To go to the **Advanced Access Config** screen, click **Next**.

## Editing Aggregation Switch Information

1. Select a configured switch.
2. In the upper left of the **Advanced Aggregation Config** screen, click **Edit**.  
The **Edit Switch Unit** dialog box appears.

 **NOTE:** Depending on pre-deployment/deployment status, some options cannot be changed. Refer to [Operations Allowed](#).

3. To save changes, click **OK**.

## Removing Aggregation Switches

1. Select a configured switch.
2. In the upper left of the **Advanced Aggregation Config** screen, click **Delete**.
3. To confirm the switch deletion, click **Yes**.

## Advanced Fabric Design — Advanced Access Config

On the **Advanced Access Config** screen of the **Fabric Design** wizard, you can add:

- [Add access switches](#)
- [Editing access switch information](#)
- [Remove access switches](#)

The selected aggregation switch model and the available, used, and total bandwidth values appear at the top of the screen.

## Adding Access Switches

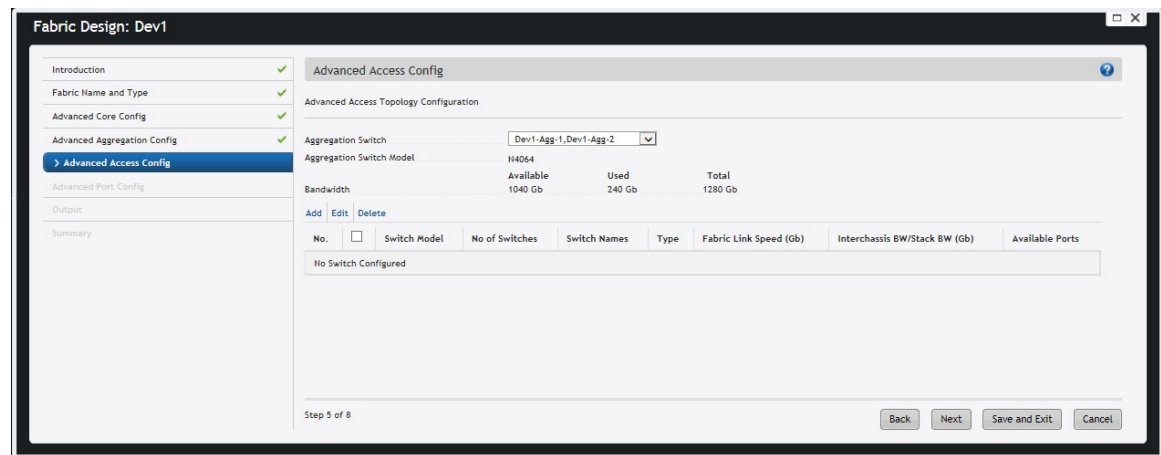


Figure 29. Advanced Access Config Screen

1. (Three-tier topologies only). From the **Aggregation Switch** menu, select the aggregation switches for which you want to configure access switches.
2. In the upper left of the **Advanced Access Config** screen, click **Add**.  
The **Add Switch Unit** dialog box appears.

X

### Add Switch Unit

Fill the Access switch configuration to be associated with fabric.

---

Aggregation Switch ..... FabricC-Agg-1,FabricC-Agg-2  
 Aggregation Switch Model ..... S6000

| Bandwidth | Available | Used   | Total   |
|-----------|-----------|--------|---------|
|           | 2080 Gb   | 480 Gb | 2560 Gb |

---

Switch Model/Type ..... S4810 / Standalone

Switch Configuration ..... 48 x 10 Gb - Fiber, 4 x 40 Gb - Fiber

Number of Switches ..... 1


Prefix Switch Name ..... FabricC-Acc

Use 40Gb => 10Gb Split for Fabric Link in Aggregation

Port Specification (per switch) :

|                 | 10 G | 40G => 10G<br>Split | 40 G | Total |
|-----------------|------|---------------------|------|-------|
| Fabric Links    | 0    | 0                   | 0    | 0 G   |
| Downlink Ports  | 0    | 0                   | 0    | 0 G   |
| Split Ports     | 0    | 4                   | 0    | 40 G  |
| Remaining Ports | 48   | 0                   | 3    | 600 G |

Figure 30. Add Switch Unit Dialog Box

 **NOTE:** The information and options in the **Add Switch Unit** dialog box vary based on the selected aggregation switch model.

3. Select a switch model from the **Switch Model** drop-down menu.
  - **S6000**
  - **S55**
  - **S60**
  - **S4820T**
  - **S4810**
  - **S4048-ON**
  - **S3048-ON**
  - **Z9500**
  - **N4064F**
  - **N4064**
  - **N4032F**
  - **N4032**

- N3048P
- N3048
- N3024P
- N3024F
- N3024
- N2048P
- N2048
- N2024P
- N2024
- MXL

**Table 32. Aggregation Layer-Access Layer Switch Combinations**

| Aggregation Switch (Non-Endpoint) | Access Switch |       |       |       |          |          |     |     |     |       |       |       |   |
|-----------------------------------|---------------|-------|-------|-------|----------|----------|-----|-----|-----|-------|-------|-------|---|
|                                   | Z9500         | S6000 | S4820 | S4810 | S4048-ON | S3048-ON | S60 | S55 | MXL | N4000 | N3000 | N2000 |   |
| Z9500                             | E             | E     | E     | E     | E        | E        | E   | E   | E   | E     | E     | E     | E |
| S6000                             |               | E     | E     | E     | E        | E        | E   | E   | E   | E     | E     | E     | E |
| S4820                             |               |       | E     |       |          |          | E   | E   | E   |       | E     | E     |   |
| S4810                             |               |       | E     | E     | E        | E        | E   | E   | E   | E     | E     | E     | E |
| S4048-ON                          |               |       | E     | E     | E        | E        | E   | E   | E   | E     | E     | E     | E |
| N4000                             |               |       |       |       | E        | E        | E   | E   | E   | E     | E     | E     | E |
| N3000                             |               |       |       |       | E        | E        |     |     |     |       | E     | E     |   |

"E" denotes endpoint switches that cannot be extended to another tier.

**Table 33. Access Switches**

| Access Switch | Deployment Type |      |       |            |
|---------------|-----------------|------|-------|------------|
|               | VLT             | MLAG | Stack | Standalone |
| MXL           | E               |      | E     | E          |
| N2000 series  |                 | E    | E     | E          |
| N3000 series  |                 | E    | E     | E          |

|               |     | Deployment Type |       |            |
|---------------|-----|-----------------|-------|------------|
| Access Switch | VLT | MLAG            | Stack | Standalone |
| N4000 series  |     | E               | E     | E          |
| S55           |     |                 | E     | E          |
| S60           |     |                 | E     | E          |
| S3048-ON      | E   |                 | E     | E          |
| S4048-ON      | E   |                 | E     | E          |
| S4810         | E   |                 | E     | E          |
| S4820         | E   |                 | E     | E          |
| S6000         | E   |                 | E     | E          |
| Z9500         | E   |                 |       | E          |

“E” denotes endpoint switches that cannot be extended to another tier.

- Select a deployment mode from the **Type** drop-down menu:

- **Standalone**
- **Stack**
- **VLT or MLAG** (N series only)

 **NOTE:**


- Z9500 does not support stack mode.
- S55, S60 do not support VLT.
- N2024, N2024P, N2048, N2048P do not support MLAG.

- (Z9500-series switch model only) In the **License Type** field, select the number of ports licensed: **36** (default); **84**; or **132**.


 **NOTE:**

- AFM does not validate whether the specified number of licensed ports is correct for the switch. An incorrect setting causes the fabric deployment to fail.
- This setting applies for both members in VLT mode.
- You can edit this value without restriction before beginning pre-deployment steps for the switch. After pre-deployment begins, you can only edit the number of ports licensed upwards (for example, 36–84).

- (VLT or MLAG mode only) Enter a value in the **Number of VLT pairs** or **Number of MLAG** pairs field.

 **NOTE:** Both switches in the VLT or MLAG pair must be the same model type.

- (MXL, S55, S60, or N Series) Select an optional module type from the first and second **Optional Module** drop-down menus:

 **NOTE:** The first optional module menu name and options vary based on the access switch type and mode (standalone or stack). Refer to the following table for supported options.



**Table 34. Access Config Optional Module Options**

| Switch Type and Mode         | Optional Module        | Supported Options                                      |
|------------------------------|------------------------|--|
| S55                          | 0/50                   | 2 x 10 G – Fiber                                       |
|                              | 0/48                   | 2 x 12 G – Fiber (Stack mode only)<br>2 x 10 G – Fiber |
| S60                          | 0/48                   | 2 x 10 G – Fiber                                       |
|                              | 0/50 (Stack mode only) | 2 x 12 G – Fiber<br>1 x 24 G – Fiber                   |
| MXL (one-tier topology only) | 0/41                   | 2 x 40 G – Fiber                                       |
|                              | 0/49                   | 4 x 10 G – Fiber<br>4 x 10 G – Copper                  |
| N3000 series                 | 1/1/1                  | 2 x 10 G – Fiber<br>2 x 10 G – Copper                  |
| N4000 series                 | 1/1/1                  | 4 x 10 G – Fiber<br>4 x 10 G – Copper                  |
|                              |                        | 2 x 40 G – Fiber                                       |

None



**NOTE:** Select this option if you do not have any optional modules in this slot.

8. (Stack mode only) Enter a value in the **Number of Stacks** field.



**NOTE:** All switches in the stack must be the same model type.

The **Number of Switches Per Stack** menu is automatically set to **2**.

9. (Standalone mode only) Enter a value in the **Number of Switches** field.

10. The default switch name is *FabricName-Access*. To specify a custom name, enter one in the **Prefix Switch Name** field.



**NOTE:** Only the name of the first switch in a stack can be changed. The other switch is appended (*standby*).

The name must be unique. The range is 1–18 characters. AFM supports the following character types:

- alphanumeric
- underscore ( \_ )
- -

11. To use 40 GB split port from the aggregation layer, select **Use 40 Gb => 10 Gb for Fabric Link in Aggregation**.

**Table 35. Support for 40 GB to 10 GB Split**

| Core Switch | Aggregation Switch |       |       |       |          |          |
|-------------|--------------------|-------|-------|-------|----------|----------|
|             | Z9500              | S6000 | S4820 | S4810 | S4048-ON | S3048-ON |
| Z9500       |                    |       |       | S     | S        | S        |
| S6000       |                    |       |       | S     | S        | S        |
| S4820       |                    |       |       |       |          | S        |
| S4810       |                    |       |       | S     | S        | S        |
| S4048-ON    |                    |       | S     | S     | S        | S        |
| N4000       |                    |       |       |       |          | S        |


"S" denotes support for 40 GB to 10 GB split.

**Table 36. Support for 40 GB to 10 GB Split**

| Core Switch | S60   | S55 | MXL | N4000 | N3000 | N2000 |
|-------------|-------|-----|-----|-------|-------|-------|
|             | Z9500 | S   | S   | S     | S     | S     |
| S6000       | S     | S   | S   | S     | S     | S     |
| S4820       | S     | S   | S   |       | S     | S     |
| S4810       | S     | S   | S   | S     | S     | S     |
| S4048-ON    | S     | S   | S   | S     | S     | S     |
| N4000       | S     | S   | S   | S     | S     | S     |

"S" denotes support for 40 GB to 10 GB split.

- To allocate ports, enter or select a value in the appropriate field in the **Port Specification (per switch)** or **Port Specification (per stack)** section.

- Fabric Link**
- Stack Ports** (Stack mode only)
  -  **NOTE:** Configure at least two fabric links.
- Inter Chassis Link** (VLTi or MLAG)
- Split Ports** (If switch model configuration allows)


The **Split Ports** field enables available 40G ports to act as 10G ports for any device type. You can select the number of 10G ports split from a 40G port from the drop-down menu. The **Remaining Ports** field displays the number of available ports; you cannot configure this field. The **Total** column displays the amount of bandwidth in GB allocated to each link type.

- To save the current switch information, click **OK**.  
To close the window without saving information, click **Cancel**.
- To go to the **Advanced Port Config** screen, click **Next**.

### **Editing Access Switch Information**

- In the **Add Switch Unit** dialog box, select a configured switch.
- In the upper left of the **Advanced Access Config** screen, click **Edit**.

The **Edit Switch Unit** dialog box appears.

 **NOTE:** Depending on pre-deployment/deployment status, some options cannot be changed. Refer to [Operations Allowed](#).


3. To save changes, click **OK**.

### Removing Access Switches

1. In the **Add Switch Unit** dialog box, select a configured switch.
2. In the upper left of the **Advanced Access Config** screen, click **Delete**.
3. To confirm the switch deletion, click **Yes**.

### Advanced Fabric Design — Port Configuration

On the **Advanced Port Config** screen of the **Fabric Design** wizard, you can configure the proposed port numbers for uplinks, stack ports, inter chassis (VLTi and MLAG) links, and fabric links. To export the data, click **Export**.

 **NOTE:** Configure only one source port number for each switch.

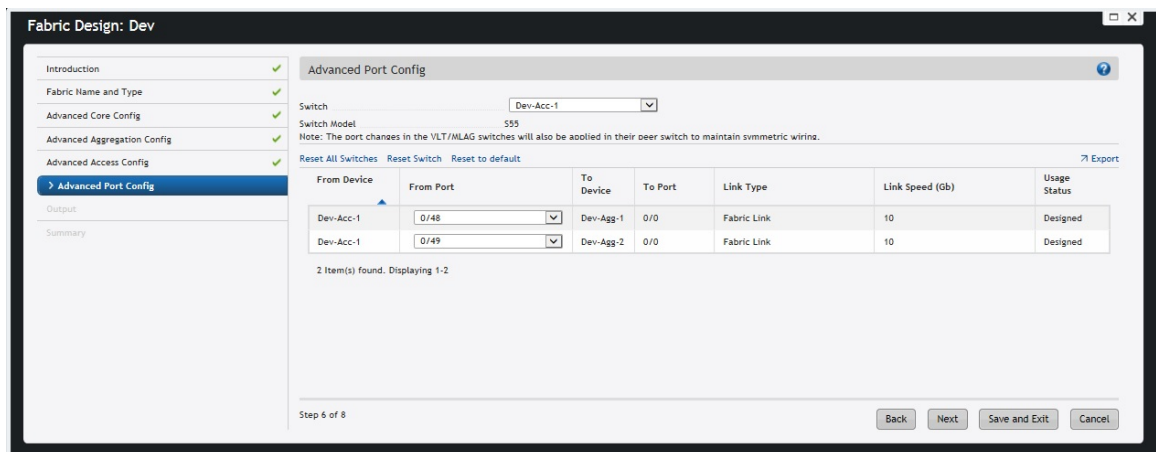


Figure 31. Advanced Port Config

1. From the **Switch** drop-down menu, select a switch.
2. For each device, from the **From Port** drop-down menu, select a port.

 **NOTE:**

- To reset a switch to previous port configurations, select it and then click **Reset Switch**.
  - To reset all switches to previous port configurations, click **Reset All Switches**.
  - To reset a switch to default settings, select it and click **Reset to default**.
  - For switches that are not pre-deployed, the drop-down menus display both used and available ports. For pre-deployed switches, only available ports appear.
  - If you change aggregation or access information, AFM resets port configurations.
  - If you change port information for either of the VLT or MLAG switches, AFM updates the port configuration in the other switch in the pair to maintain symmetry.
3. To validate the port configurations, click **Next**. If AFM finds errors, correct them to continue to the **Output** screen.

## Fabric Design — Viewing and Exporting Output

To view the graphical wiring, tabular wiring, and network topology wiring plans for your fabric design, use the **Output** screen. Use the wiring plan as a guide for installing your equipment into the fabric. Based on the configuration, AFM calculates the number of switches required for the design and displays a physical wiring plan in PDF or Microsoft Visio® 2010 format that you can export and print. The wiring plans display the switches and links for current and future expansion and the cabling maps (the connections between the switches). Review the wiring plan and then export it to a file.

After the fabric design is approved, provide the wiring plan to the data center operator to build the physical network according to the fabric design.

1. From the menu, click **Network** and then the **Design Fabric** tab.
2. Click **New Fabric**.
3. Navigate to the **Output** screen.
4. Click the type of wiring plan that you want to export: **Wiring** (Graphical or Tabular), or **Network Topology** (Graphical or Tabular format).
5. To view additional pages, use the arrow buttons or enter the page number in the page number entry field to the left of the arrow buttons.
6. Click **Export**.  
The **Generate Wiring Plan** dialog box appears.
7. Specify the following export options.
  - **PDF** — Table, Data, Graphical Wiring Plan, or Both.
  - **Visio** — Network Topology.
8. Click **Generate**.  
The output appears in the selected format.

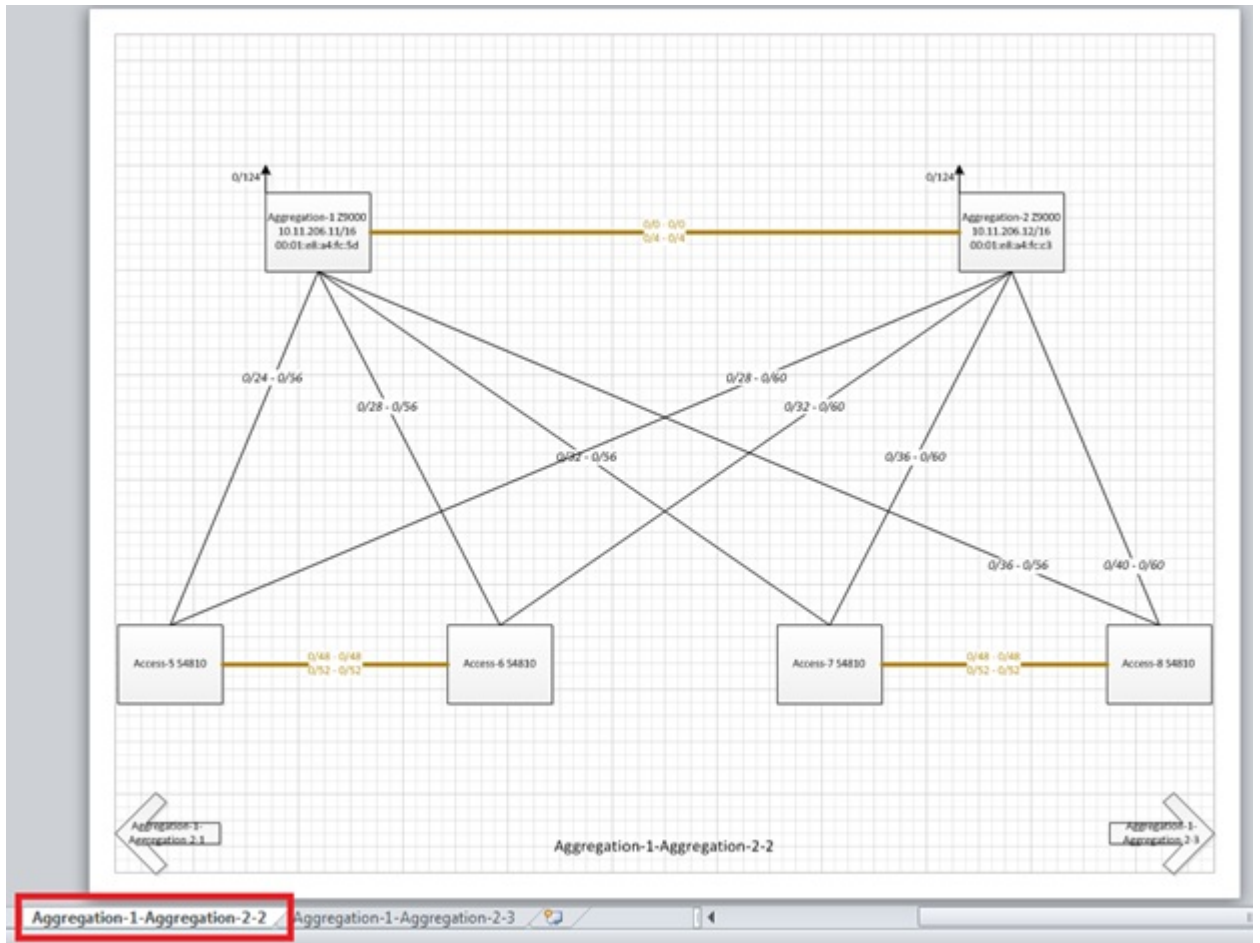


Figure 32. Example: Visio Output

## Output Types

### Network Topology

- **Graphical Network Topology** — View information about how the switches are connected physically using a topology map. By default, no links are displayed in the fabric. To display the links in the fabric, click a switch.
  - If you select a switch, all the fabric interlinks appear.
  - If you select a spine switch, the links to the leaf switches appear.
  - If you select an aggregation switch, the links to the access switches appear.
  - If you select a leaf switch, the links to the spine switches appear.
  - If you select the access switches, the links to aggregation switches appear.
  - If you select the core switches, the links to all the switches in the fabric (aggregation and access) appear.

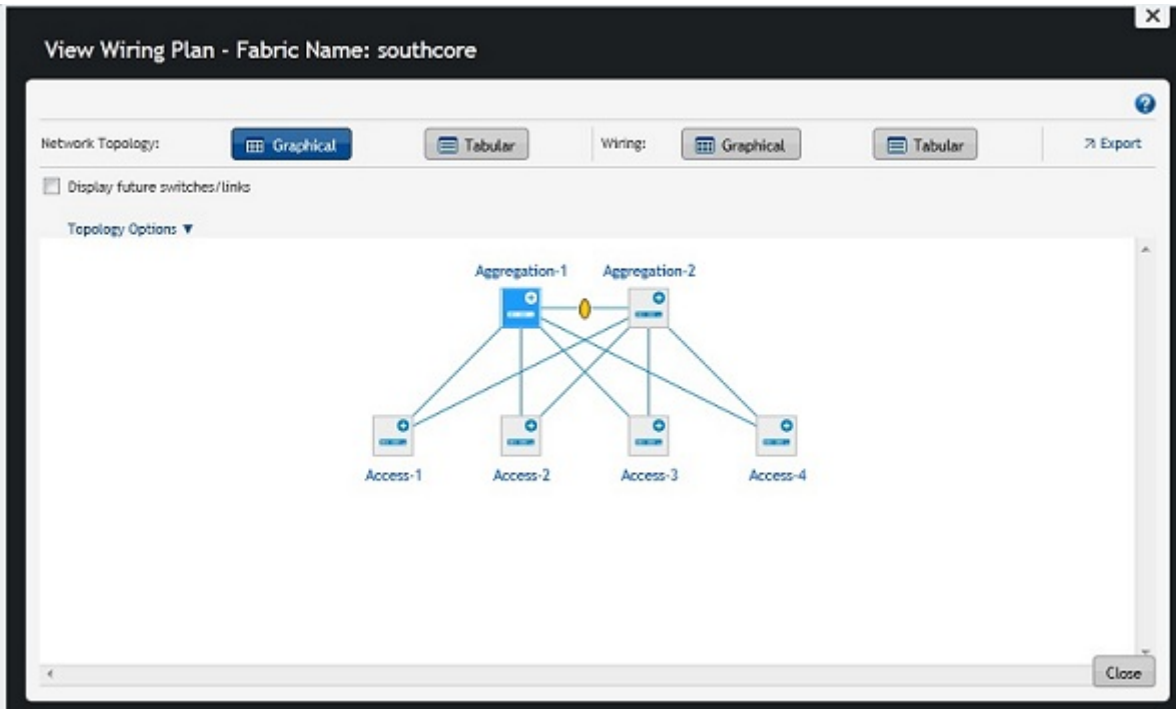


Figure 33. Graphical Network Topology

- **Tabular Network Topology** – View information about the network topology in a tabular format, including switch names, model types, role (core, aggregation, or access), and usage status (designed or deployed).

Output

Network Topology: Graphical **Tabular** Wiring: Graphical Tabular Export

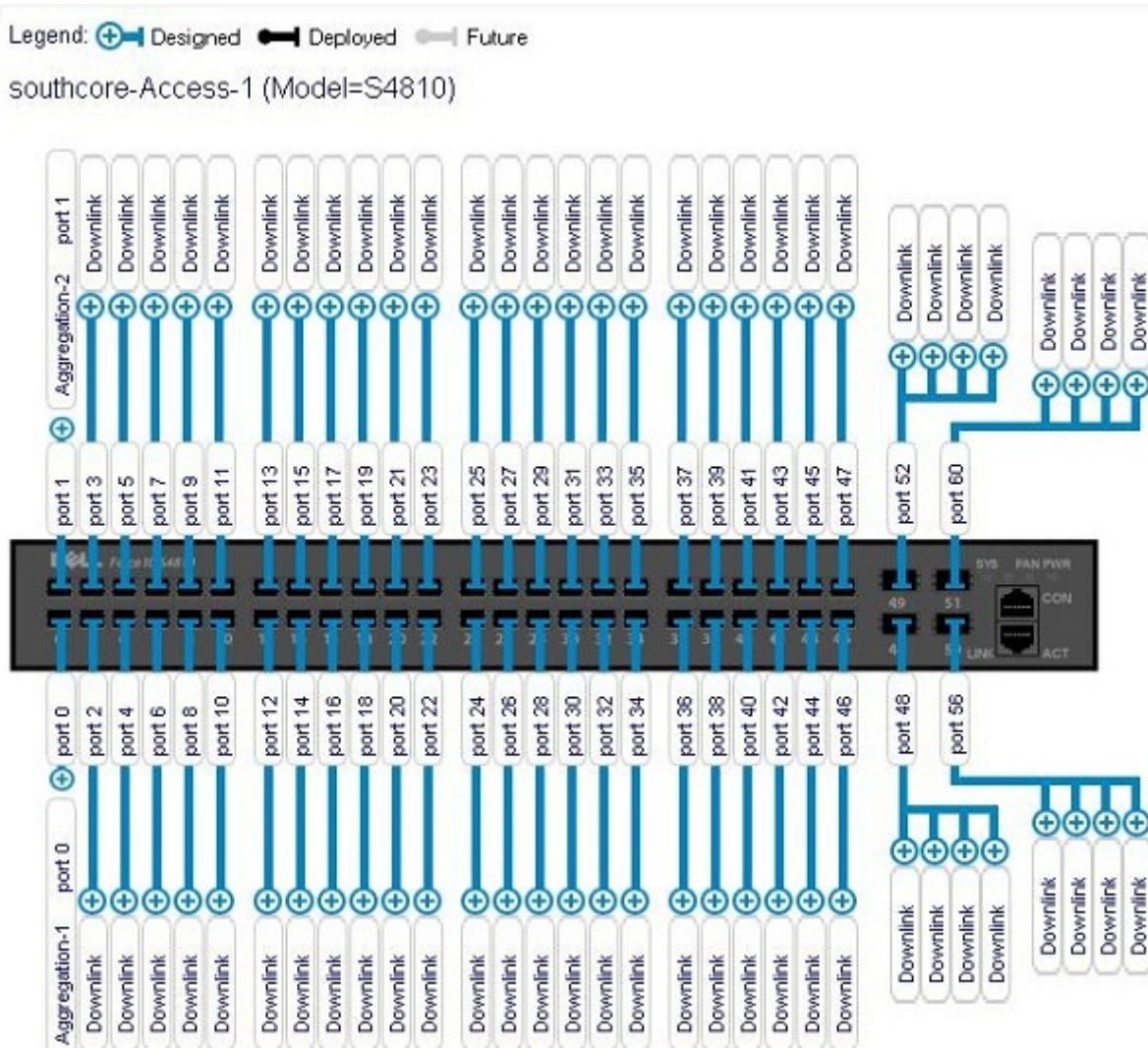
| Switch Name    | Model        | Role        | Usage    |
|----------------|--------------|-------------|----------|
| Advanced-Acc-1 | MXL-10/40GbE | Access      | Designed |
| Advanced-Agg-1 | S6000        | Aggregation | Designed |
| Advanced-Agg-2 | S6000        | Aggregation | Designed |

3 Item(s) found. Displaying 1-3

Figure 34. Tabular Network Topology

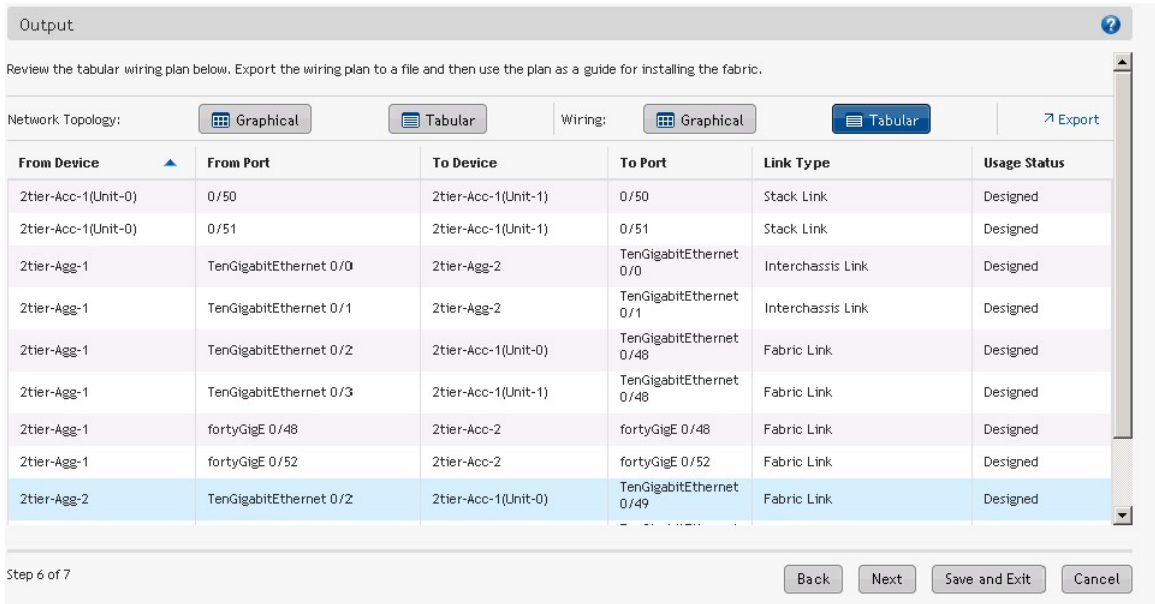
### Wiring

- **Graphical Wiring Plan** – View a diagram of each switch, including uplinks, downlinks, and port numbers, in the fabric. This diagram includes information for designed switches that have not been deployed, deployed switches, and planned capacity.



**Figure 35. Graphical Wiring Plan**

- **Tabular Wiring Plan** — Displays information about how the switches are connected in the fabric in a tabular format, as the following figure illustrates. The tabular wiring plan contains a list of switches, their names, link types, and the ports that connect to ports of other switches in the fabric.



**Figure 36. Tabular Wiring Plan**

**Table 37. Tabular Wiring Plan Field Descriptions**

| Field Name           | Description  |
|----------------------|--|
| From Device (Switch) | Displays the name of the device from the side.                                   |
| From Port            | Displays the port number and speed on the switch from the side.                  |
| To Device (Switch)   | Displays the name of the device to the side.                                     |
| To Port              | Displays the port number and speed on the device to the side.                    |
| Link Type            | Displays the type of link (Inter chassis, Fabric, or Stack link)                 |
| Usage Status         | <ul style="list-style-type: none"> <li>– Designed</li> <li>– Deployed</li> </ul> |

## Fabric Design – Summary

The **Summary** screen displays a summary of your fabric design.

1. Click one of the following export options:
  - **Export Wiring Plan**
  - **Export Summary**
  - **Export Design**
2. If you select Export Wiring Plan, select a display format:
  - **PDF (Table Data, Graphical Wiring Plan, Both)**
  - **Visio**

If you select Export Summary, the file saves to your local disk in PDF format. If you select Export Design, the file saves to your local disk in XML format.



3. Click **Generate**.
4. Review the design carefully before committing the changes.
5. Click **Finish** to commit your changes.

### Next Steps

To prepare the fabric for deployment:

1. Check with your system administrator for the TFTP or FTP IP address. To stage the switch software images, use this address. When you prepare the software images:
  - Make sure that the software version is the same for each switch type in the fabric.
  - Download the software image for each type of Dell Networking switch.
  - Stage the software images on the TFTP or FTP site.
2. Obtain a pool of management IP addresses for the switches in the fabric from the lab or system administrator.
3. Prepare the DHCP server so that the switches can be assigned a management IP address.
4. Download the **.csv** file that has the switches' system MAC addresses provided by Dell Networking, if available. If this file is not available, record the system MAC addresses of the switches in the fabric so that you can associate the address to the appropriate switch before you rack the switches.
5. Print the wiring plan and use it to rack and cable the hardware.
6. Document the location of the switches, including the rack and row.
7. Select the fabric for pre-deployment. Refer to [Pre-Deployment Configuration](#).

## Using Existing Fabric Designs

From the **Getting Started** tab, you can:

- Import an existing design
- Edit an existing design
- Delete a fabric

### Importing an Existing Fabric Design

1. From the menu, click **Home** and make sure that the **Getting Started** tab is selected.
2. Click **Import Existing Design**.  
The **Import Existing Design** dialog box appears.
3. In the **Switch XML file** area, click **Browse** and locate the fabric XML design file that you have exported from the AFM design wizard.
4. Click **Upload**.

### Editing and Expanding an Existing Fabric Design

You can edit or expand an existing fabric from the **Getting Started** screen. After you initiate the pre-deployment configuration, you can only update the fabric description and port count for expanding uplinks and downlinks.

1. From the menu, click **Home** and make sure that the **Getting Started** tab is selected.
2. Click **Edit Existing Fabric**.  
The **Select a Fabric** dialog box appears.

3. Select a fabric to edit and then click **OK**.  
The **Fabric Design** wizard appears.
4. Edit the fabric.

## Deleting the Fabric

1. From the menu, click to **Network**.
2. Click the **Design Fabric** tab.
3. Select the fabric to delete.
4. Click **Delete Fabric**.
5. In the confirmation dialog box, click **Yes**.

## Viewing the Wiring Plan

1. From the menu, click **Network** and then click the **Design Fabric** tab.
2. Select the fabric and then click **View Wiring Plan**.
3. To display future switches and links, click **Display future switches/links**.
4. Click one of the following options:
  - **Tabular Wiring Plan**
  - **Graphical Wiring Plan**
  - **Network Topology Plan**
  - **Network Topology Tabular Plan**
5. To view additional pages, use the arrow buttons or enter the page number in the page number entry field to the left of the arrow buttons.
6. To export the wiring plan, click **Export** .

# IOA Fabric Designer Wizard

To design a Layer 2 fabric that has an I/O Aggregator (IOA) blade switch in a M1000e chassis, use the IOA fabric design wizard. AFM supports IOA in standalone mode only.

1. To verify that the IOA blade switch is in standalone mode (default mode), use the following CLI command:

```
show system stack-unit iom-mode
```

For more information about this command, refer to the *Dell PowerEdge Command Line Reference Guide for the M I/O Aggregator*.

2. From the menu, click **Network** and then the **Design Fabric** tab.

Figure 37. IOA Fabric Design

**NOTE:** If you are designing a fabric without an IOA blade switch, refer to [Using the Fabric Design Wizard](#).

3. Click **New Fabric**.

The **Introduction** screen appears.

**NOTE:** Click **Save & Exit** to save the current information and exit the wizard or click **Cancel** to exit the wizard without saving the current information.

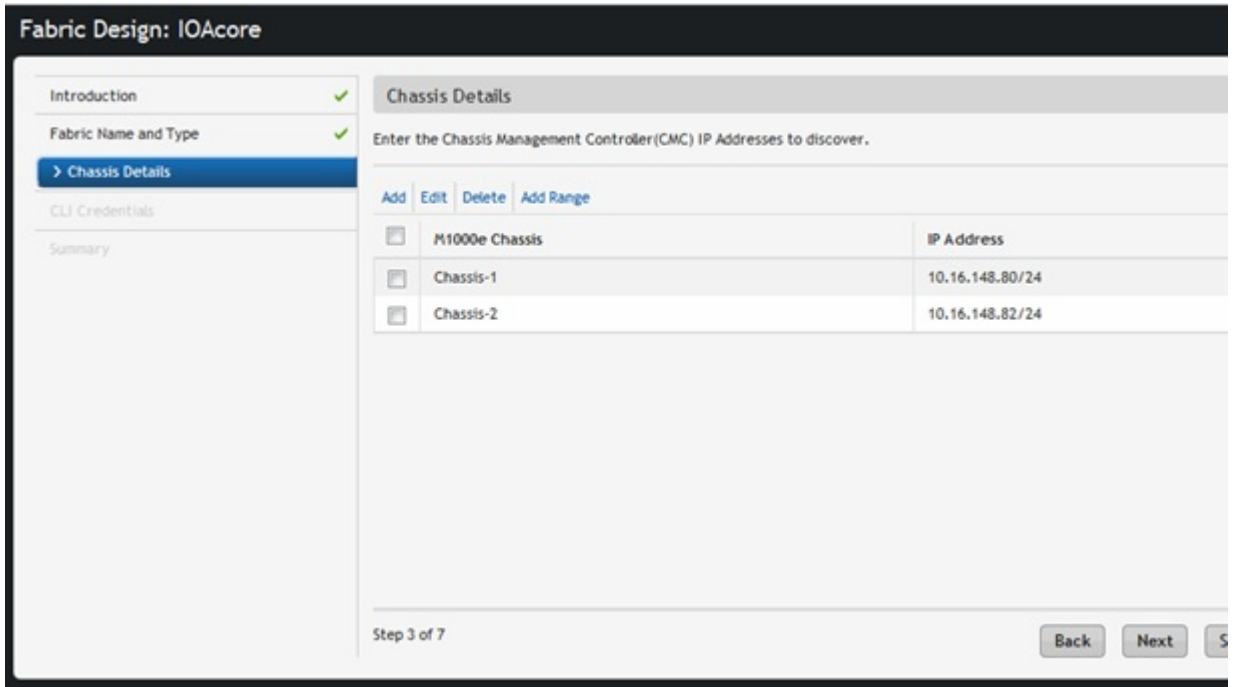
4. Review the introduction and click **Next**.

The **Fabric Name** screen appears.

5. On the **Fabric Name and Type** screen, select the **Blade Switch Deployment** check box, then select the **IOA** radio button.

6. Click **Next**.  
The **IOA Fabric Design wizard** appears.
7. Click **Next**.  
The **Chassis Details** screen appears.

**Figure 38. IOA Fabric Design Wizard – Chassis Details Screen**



8. Enter the Chassis Management Controller (CMC) IP addresses to include in the fabric.
  - **Add** — Enter the chassis IP address in the first field and the prefix in the field after the slash and click **OK**. To close the window without adding the IP address, click **Cancel**.
  - **Edit** — Edit information for a specific chassis by selecting the checkbox for that chassis then clicking **Edit**. After changing the IP address, click **OK**. To close without saving changes, click **Close**.
    - ✎ **NOTE:** You cannot edit information for multiple chassis simultaneously.
  - **Delete:** — Check the check box for the chassis that you want to delete, then click **Delete**. To confirm the deletion, click **Yes**. To cancel the deletion, click **No**.
  - **Add Range** — Enter the chassis ID in the **Number of M1000e Chassis** field. Enter the first IP address in the range in the **Start IP Address/Prefix** field. Enter the prefix in the field after the slash. To add the range, click **OK**. To close without adding the IP range, click **Cancel**.
9. Click **Next**.  
The **CLI Credentials** screen appears.

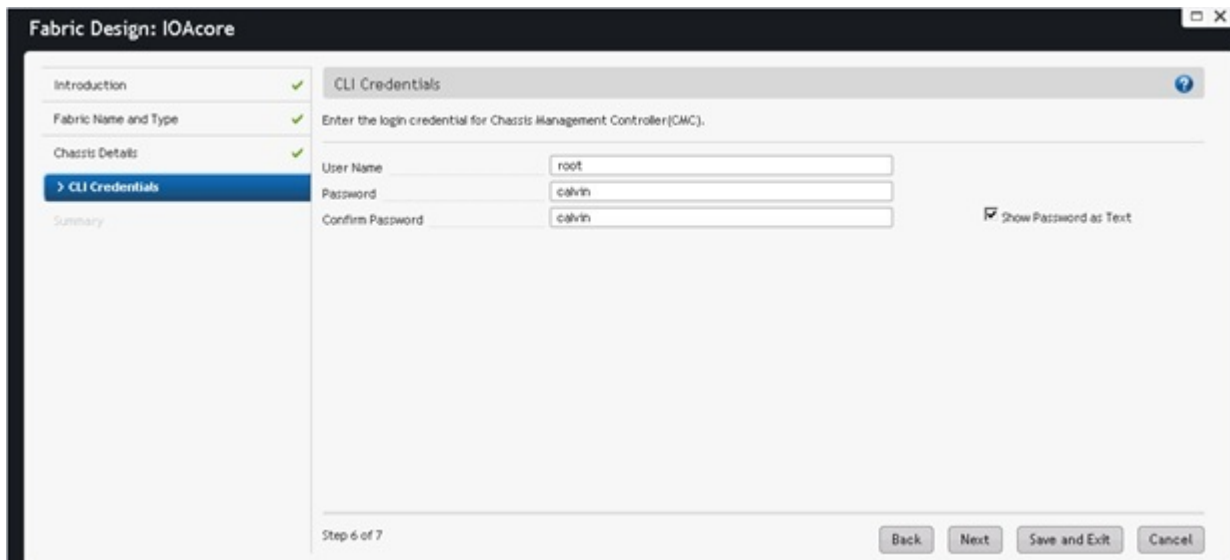


Figure 39. IOA Fabric Design Wizard – CLI Credentials Screen


10. Enter the user credentials for the CMC.

This information is used to log in to all CMCs in the fabric. By default, the **CLI Credentials** screen uses the following CLI credentials:

- username – root
- password – calvin

If you have changed the CLI credentials, update these fields with the new information.

- a. Enter the user name in the **User Name** field.
- b. Enter the password in the **Password** and **Confirm Password** fields.

 **NOTE:** To unmask the CLI credentials, check the **Show Password as Text** checkbox.

11. Click **Next**.

The **Summary** screen appears. The design summary screen shows the added chassis number and IP addresses, and CLI credentials.

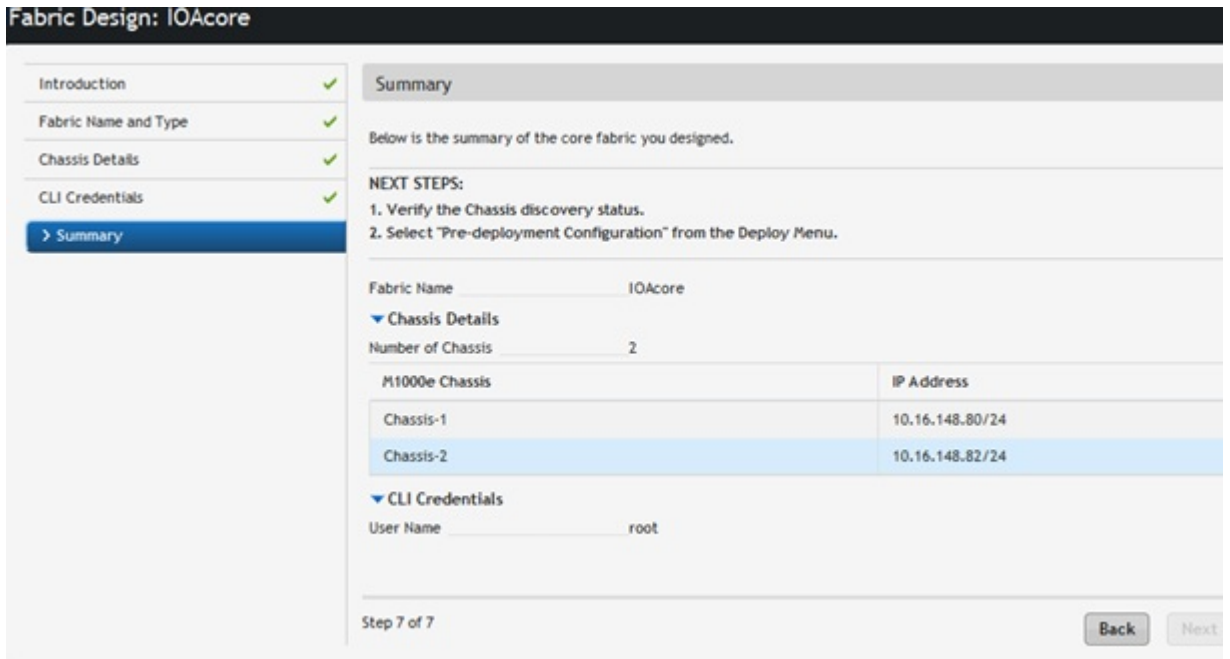


Figure 40. IOA Design Summary Screen

12. Review the fabric design information on the **Summary** screen. To confirm the information, click **Finish**.

The **Discovery Confirmation** screen appears.

13. Click **Yes** to start the fabric discovery process. The **Discovery Status** screen displays detailed information about the installed IOA blade switches in the M1000e chassis. For information about the Discover Status screen, refer to [View Discovery Status of an Existing Fabric](#).

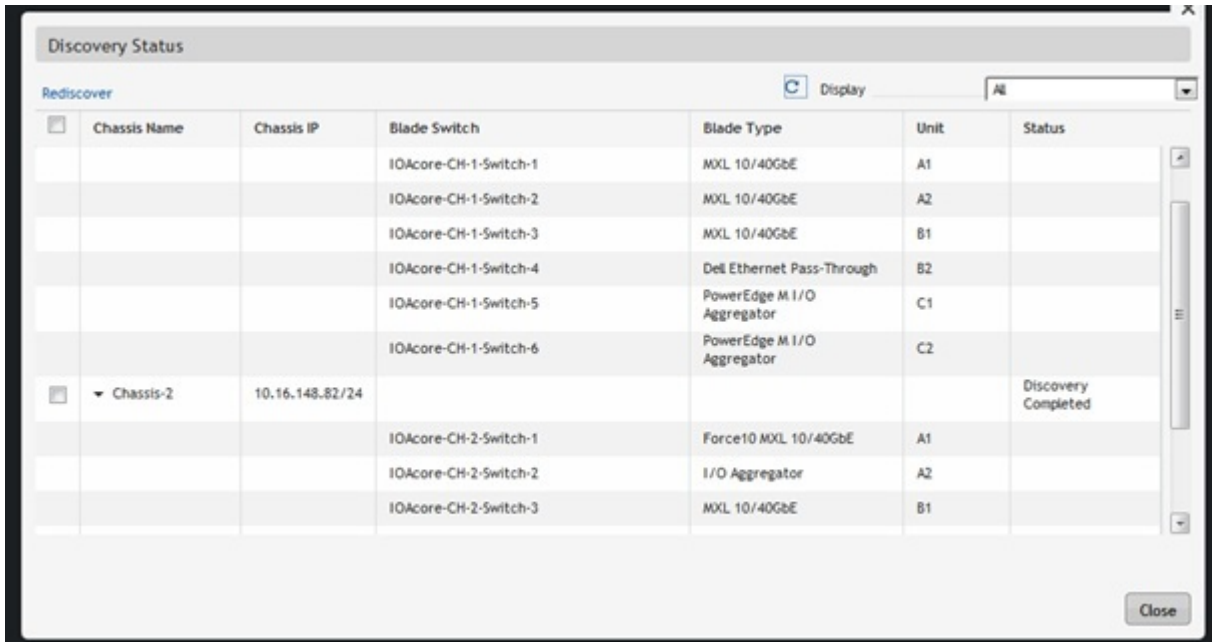


Figure 41. IOA Discovery Status Screen

14. After the IOA fabric is successfully discovered, complete the pre-deployment configuration. For information about IOA pre-deployment configuration, refer to [IOA Pre-deployment Wizard](#).

# Configuring and Deploying the Fabric

This tab displays settings for the configuration of the switches in the fabric, as well as auto-generated and custom configurations. This screen contains the following options:

- **Deploy Fabric** — Prepares the fabric for deployment and deploys the fabric.
  - [Pre-deployment Configuration](#)  
For information about using the pre-deployment wizard for an IOA fabric, see [IOA Pre-deployment Wizard](#)
  - [Deploying and Validate](#)
  - [View DHCP Configuration](#)
- **Errors** — Displays errors in the fabric.

Related Links:

- [Deployment and Validation Errors](#)
- [Troubleshooting](#)
- **CLI Configuration** — Uses CLI commands for template and custom configuration.
  - [Manage Templates](#)
  - [Associate Templates](#)
  - [Custom Configuration](#)
  - [Viewing Custom Configuration History](#)
- **View Wiring Plan** — Displays the wiring plan in tabular, network topology, and graphical formats, which can be exported.

Related Links:

- [Pre-deployment Configuration](#)
- [Using the Pre-deployment Configuration Wizard](#). For information about using the pre-deployment wizard for an IOA fabric, refer to [IOA Pre-deployment Wizard](#).

## Pre-Deployment Configuration

In the **Step 2: Pre-deployment Configuration** section of the **Getting Started** tab:

- To automatically discover MAC addresses and the locations of the devices in the fabric, click **Device MAC Association**, select a fabric, and click **OK**. For more information, refer to [Device MAC Association](#).
- To use the wizard to complete the pre-deployment process, click **Pre-deployment Configuration**, select a fabric, and click **OK**. For more information, refer to the following subsections.




## IOA Fabric Pre-Deployment

To prepare the IOA fabric for deployment, complete the following tasks using the **Pre-deployment Configuration** wizard.

1. [Pre-Deployment IOA – Management IP](#)
2. [Pre-Deployment IOA – VLAN Configuration](#)
3. [Pre-Deployment IOA – SNMP and CLI Credentials](#)
4. [Pre-Deployment \(IOA\) – Software Images](#)
5. [Pre-Deployment IOA – Summary](#)

## Layer 2 VLT/ Advanced Fabric Pre-Deployment

To prepare the Layer 2 VLT or Advanced fabric designs for deployment, complete the following tasks using the **Pre-deployment Configuration** wizard.

 **NOTE:** The pre-deployment processes for a Layer 2 VLT standard fabric and for an advanced fabric are similar. The exceptions are the **Storage Facing Ports** screen applies only to standard fabric pre-deployment and the **Change Port Status** screen applies only to advanced fabric pre-deployment.

1. Protocol Configuration for a Layer 2 VLT fabric:
  - a. [L2 VLT Pre-Deployment – Uplink Configuration](#)
  - b. [L2 VLT Pre-Deployment – VLAN Configuration](#)
  - c. [Pre-deployment L2 VLT – Port Channel Configuration](#)
  - d. [L2 VLT Pre-Deployment – Storage Facing Port](#)
  - e. [L2 VLT Pre-Deployment – VLAN Mapping](#)
2. [Pre-Deployment – Change Port Status \(Advanced Fabric only\)](#)
3. [Pre-Deployment – Assign Switch Identities](#)
4. [Pre-Deployment – Management IP](#)
5. [Pre-Deployment – License Update \(Advanced Fabric Z9500 switches only\)](#)
6. [Pre-Deployment – SNMP and CLI Credentials](#)
7. [Pre-Deployment – Software Images](#)
8. [Pre-Deployment – DHCP Integration](#)
9. [Pre-Deployment – Summary](#)

## Layer 3 Distributed Core Fabric Pre-Deployment

To prepare the Layer 3 Distributed Core fabric for deployment, complete the following tasks using the **Pre-deployment Configuration** wizard.

1. Protocol Configuration for Layer 3 fabric:
  - [Pre-Deployment L3 DC – Fabric Link Configuration](#)
  - [Pre-Deployment L3 DC – Uplink Configuration](#)
  - [Pre-Deployment L3 DC – Downlink Configuration](#)
2. [Pre-Deployment – Assign Switch Identities](#)
3. [Pre-Deployment – Management IP](#)


4. [Pre-Deployment – SNMP and CLI Credentials](#)
5. [Pre-Deployment – Software Images](#)
6. [Pre-Deployment – DHCP Integration](#)
7. [Pre-Deployment – Summary](#)

## Layer 3 with Resiliency (Routed VLT) Pre-Deployment

To prepare the Layer 3 with Resiliency (Routed VLT) fabric for deployment, complete the following tasks using the **Pre-deployment Configuration** wizard.


1. Protocol Configuration for Layer 3 fabric:
  - [Pre-Deployment L3 Routed VLT – Fabric Link Configuration](#)
  - [Pre-Deployment L3 Routed VLT – Uplink Configuration](#)
  - [Pre-Deployment L3 Routed VLT – VLAN Configuration](#)
  - [Pre-Deployment L3 Routed VLT – Port Channel Configuration](#)
  - [Pre-Deployment L3 Routed VLT – VLAN Mapping](#)
2. [Pre-Deployment – Assign Switch Identities](#)
3. [Pre-Deployment – Management IP](#)
4. [Pre-Deployment – SNMP and CLI Credentials](#)
5. [Pre-Deployment – Software Images](#)
6. [Pre-Deployment – DHCP Integration](#)
7. [Pre-Deployment – Summary](#)

## Device MAC Association

 **NOTE:** Device MAC association does not support S55 or S60.

To automatically discover MAC addresses for devices, use the **Device MAC Association** screen. In the Pre-deployment wizard, you must manually enter the MAC address of each device. After using Device MAC Association, AFM lists the applicable MAC addresses for each device in the fabric for your selection.

In previous versions of AFM, the MAC address for each device in the fabric had to manually load in the **Pre-Deployment** wizard. If a **.csv** file was used, each MAC address had to be manually matched with the correct device. **Device MAC Association** automatically discovers MAC addresses for devices in the fabric. If you use Device MAC Association, you do not need to upload a **.csv** file or enter the MAC addresses manually.

 **NOTE:**

- Use Device MAC Association on only one fabric at a time. If you select a fabric for Device MAC Association and then try to select a different fabric while Device MAC Association is in progress, the following message appears:

MAC discovery already enabled for the fabric "*FabricName*". Do you want to disable it and enable MAC discovery for the current fabric?

To disable Device MAC Association for the first fabric and enable it on the current fabric, click **Yes**. To leave Device MAC Association enabled on the first fabric and cancel it for the current fabric, click **No**.

- Device MAC Association is only available for fabrics that have not been pre-deployed or deployed. After you pre-deploy or deploy a fabric that uses Device MAC Association, AFM disables Device MAC Association for that fabric to help prevent IP address conflicts.

Before using Device MAC Association:

- Complete the fabric design
- Download the wiring diagram
- Complete the wiring according to the wiring diagram

### Using Device MAC Association

1. On the **Getting Started** tab, in the **Step 2: Pre-deployment Configuration** section, click **Device MAC Association**.

The **Select a Fabric** window appears.

 **NOTE:**

You can also access Device MAC Association by going to the **Network > FabricName > Configure and Deploy** tab. From the drop-down **Deploy Fabric** menu, select **Device MAC Association**.

2. Select a fabric and click **OK**.

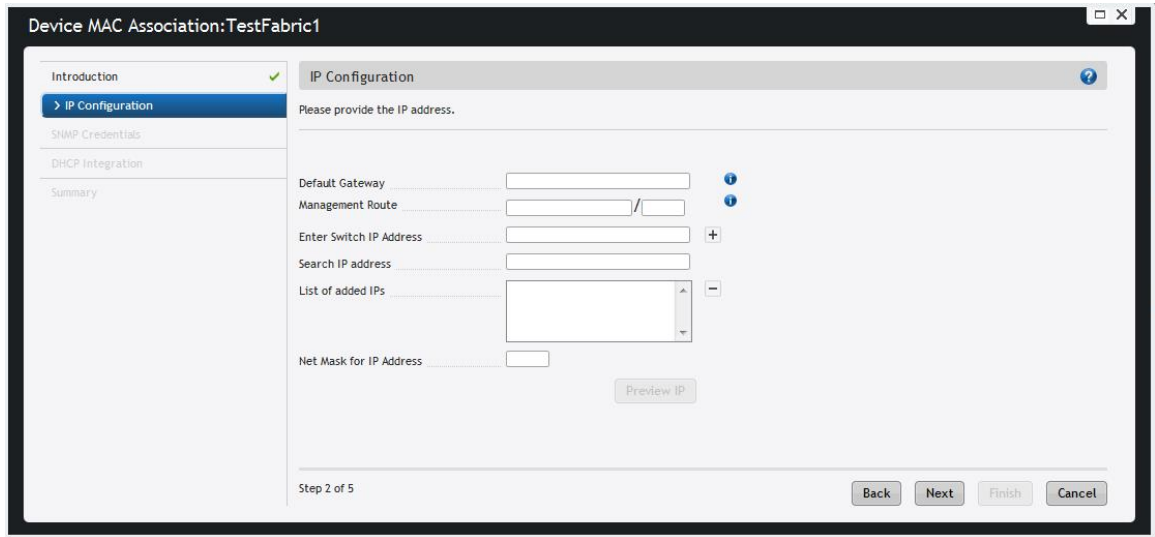
The **Introduction** screen appears.



**NOTE:** You can also access Device MAC Association by going to the **Network > FabricName > Configure and Deploy** tab. From the drop-down **Deploy Fabric** menu, select **Device MAC Association**.


3. Read the introduction and click **Next**.

The **IP Configuration** screen appears.



**Figure 42. Device MAC Association — IP Configuration**

4. Enter the default gateway in the **Default Gateway** field.
5. Enter the management route in the **Management Route** field. Enter the netmask in the / field.
6. Enter the switch's IP address in the **Enter Switch IP Address** field and click the + button. Repeat for any additional switches.

 **NOTE:** You can add an individual IP address or IP address with a subnet or a range (for example: 10.16.133.1-150).

- To search for a previously entered IP address, enter a portion of or the entire IP address in the **Search IP address list:** field. The software displays all IP addresses that match the search term in the **List of added IPs** field. If you do not enter a search term, all known IP addresses appear.
- To remove an IP address from the displayed list, select the IP address and click the — button.
- To view a list of all IP addresses selected for device MAC association, click **Preview IP**. The **Preview IP** dialog box displays only the devices participating in the discovery. To view additional pages, use the arrow buttons or enter the page number in the page number entry field to the left of the arrow buttons.



Figure 43. Preview IP Address Window

7. Add at least one IP address to the **List of added IPs:** field.
8. Enter the netmask in the **Net Mask for IP Address** field (for example: 24). The netmask range is 8–30.
9. To go to the SNMP Credentials screen, click **Next**.

### **SNMP Credentials**

 **NOTE:** AFM populates the CLI and SNMP credentials from the Administration settings.

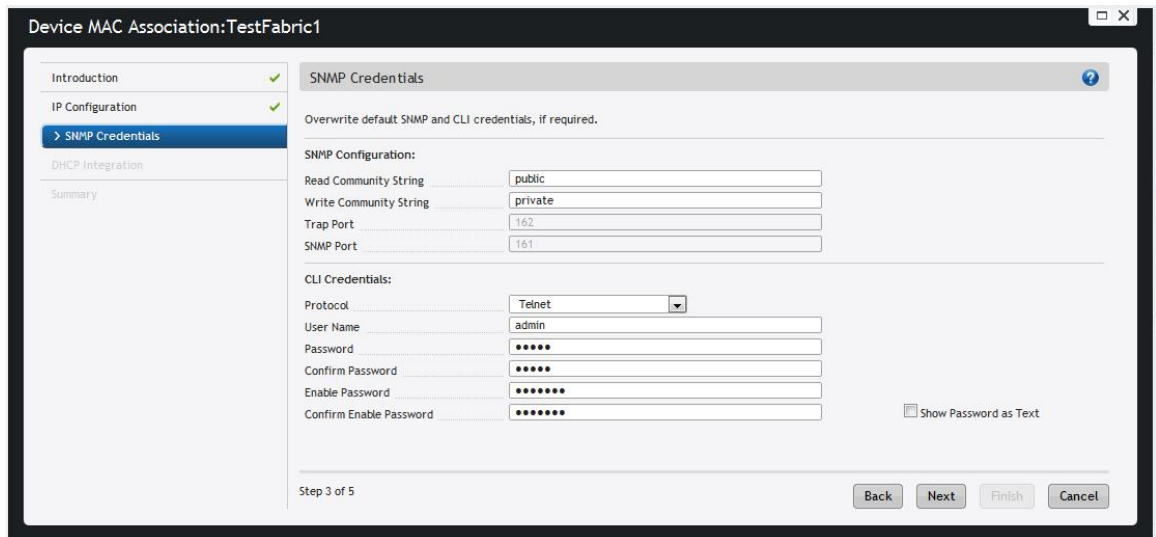




Figure 44. Device MAC Association — SNMP Credentials

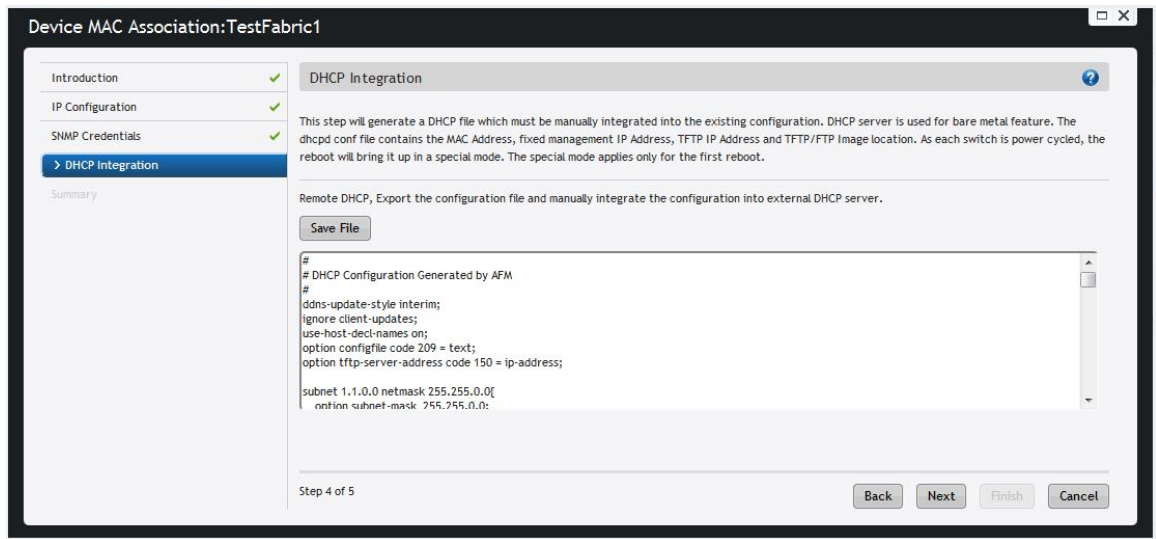
1. In the **Read Community String** field, enter the read community string (for example, `public`).
2. In the **Write Community String** field, enter the write community string (for example, `private`).  
The trap port and SNMP port numbers display as read-only fields.
3. From the **Protocol** drop-down menu, select one of the following protocols:
  - **Telnet**
  - **SSHv2**

 **NOTE:** AFM automatically enters the default credentials for the user name, password, and enable password. To unmask the passwords, check the **Show Password as Text** checkbox.

4. Click **Next**.  
The **DHCP Integration** screen appears.

### DHCP Integration

 **NOTE:** If you are using a local DHCP server, you do not need to make changes on this screen. If you are using a remote DHCP server, download the DHCP config file from the AFM server, upload it to the remote DHCP server, and restart the remote server. For more information, refer to [Pre-Deployment — DHCP Integration](#) and [DHCP Server Settings](#).



**Figure 45. Device MAC Association – DHCP Integration**

1. Click **Save File** and specify the location for the generated DHCP configuration file or copy and paste the configuration into the DHCP server.
2. Verify the TFTP or FTP file transfer for the DHCP configuration file is successful and verify the CLI and SNMP information on the **Summary** screen, then click **Finish**.

After completing the **Device MAC Association** wizard:

1. Enable BMP on all devices.
2. Go to the **Network > FabricName > Configure and Deploy** tab. From the drop-down **Deploy Fabric** menu, select **Device MAC Association Status** and verify that the Device MAC Association completes successfully.

### **Viewing Device MAC Association Status**

The Device MAC Association Status screen displays detailed information for the IP address list that the Device MAC Association wizard generates, including the following:

- IP address
- Associated Name
- Vendor
- Model
- MAC Address
- Serial Number
- Status Description
- Reason

| IP Address    | Associated Name   | Vendor       | Model  | Mac Address       | Serial Number | Status   | Status Description                       | Reason                                  |
|---------------|-------------------|--------------|--------|-------------------|---------------|----------|--|---|
| 10.16.133.147 | mix12-mix12-Agg-1 | Dell Force10 | S4810  | 00:01:e8:8b:52:f7 | HADL126120021 | Failed   | Mac Discovery=Mac Discovery: Failed]...  | Wiring errors exist                     |
| 10.16.133.148 | mix12-mix12-Agg-2 | Dell Force10 | S4810  | 00:01:e8:8b:50:84 | HADL125U20262 | Failed   | Mac Discovery=Mac Discovery: Failed]...  | Wiring errors exist                     |
| 10.16.133.149 |                   | Dell Force10 | S4820T | 90:b1:1c:f4:2d:ab | 5WDL134M20065 | Failed   | Mac Discovery=Mac Discovery: Failed]...  | Unable to associate MAC based on wiring |
| 10.16.133.150 |                   | Dell Force10 | S4820T | 90:b1:1c:f4:2e:26 | 5WDL134M20106 | Failed   | Mac Discovery=Mac Discovery: Failed]...  | Unable to associate MAC based on wiring |
| 10.16.133.151 | mix12-mix12-Acc-3 | Dell Force10 | S4810  | 00:01:e8:8b:64:34 | HADL128620092 | Complete | Mac Discovery=Mac Discovery: Success]... |   |
| 10.16.133.152 | mix12-mix12-Acc-4 | Dell Force10 | S4810  | 00:01:e8:8b:53:12 | HADL126120030 | Complete | Mac Discovery=Mac Discovery: Success]... |   |

**Figure 46. Device MAC Association Status Screen**

If the wiring is correct, AFM automatically populates the **Associated Name** column. If the wiring is not correct, this column is blank. If wiring errors exist, AFM displays the cause in the **Reason** column.

## IOA Pre-Deployment Wizard

To provide the IOA fabric the minimum configuration, use the following IOA **Pre-deployment** screens. These screens automate the IOA deployment process. See also [Using the Pre-deployment Configuration Wizard](#).

- **CMC Management IP** — Displays all the IOA blades available in the discovered CMC. If the discovered CMC is configured with an IP address, AFM populates with an IP address that you can edit.
- **Blade Discovery** — Discovers all switch blades, such as IOA and MXL, in the CMC chassis.
- **SNMP and CLI Credentials** — Configures SNMP and CLI credentials at the fabric level. Configure SNMP so that AFM can perform SNMP queries on the switches in the fabric. It is prepopulated with default IOA credentials - **root/calvin**.
- **Deploy selected switches** — Deploys the selected IOA switches
- **Identify Deployment Failures** — Identifies IOA switches that failed to deploy due to mode setting. You must put all listed IOA switches in standalone mode and redeploy them.
- **Summary** — Displays the fabric name and location of the software image.

The pre-deployment configuration for IOA consists of the following tasks:

- [Pre-Deployment IOA — Step 1: Management IP](#)
- [Pre-Deployment IOA — Step 2: VLAN Configuration](#)
- [Pre-Deployment IOA — Step 3: SNMP and CLI Credentials](#)
- [Pre-Deployment IOA — Step 4: Software Images](#)
- [Pre-Deployment IOA — Step 5: Summary](#)


For information about IOA pre-deployment error messages, see [IOA Pre-deployment Error Messages](#).

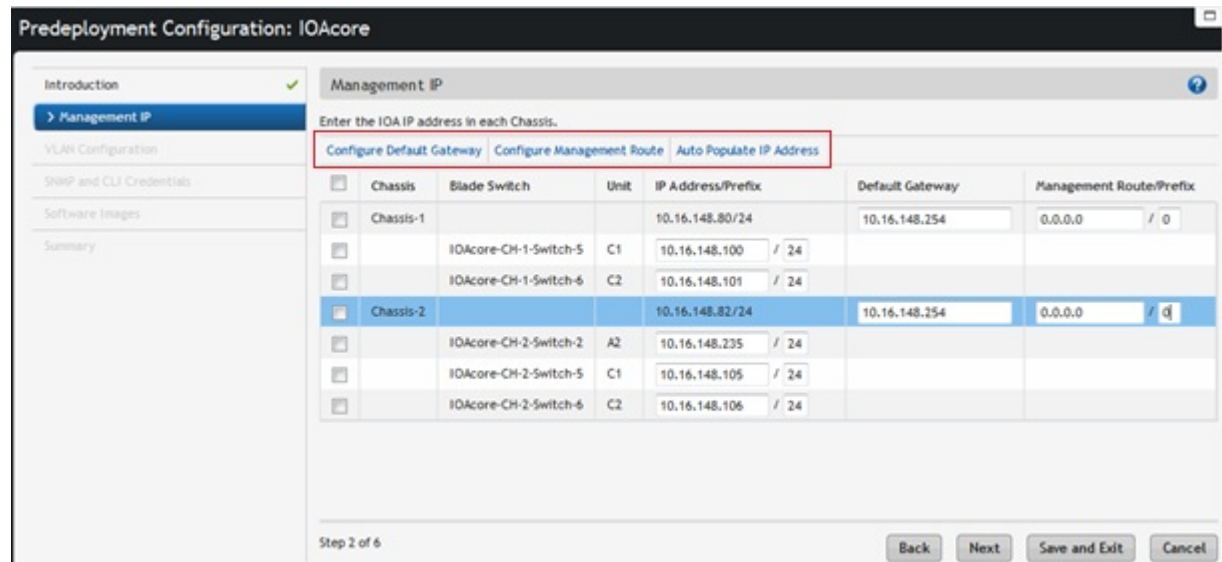
### Pre-Deployment (IOA) — Management IP

Before you begin:



1. Review the [IOA Pre-deployment Wizard](#) information.
2. Insert the IOA blade switch into the M1000e chassis.
3. Make sure that the IOA blade switch is in standalone mode (default mode) using the following FTOS CLI command: `show system stack-unit <unit-number> iom-mode`  
For more information about this command, refer to the *Dell PowerEdge Command Line Reference Guide for the M I/O Aggregator*.
4. Obtain the Chassis Management Controller (CMC) M1000e chassis IP address. Use this address to discover all the IOA switch blades in the CMC chassis.

 **NOTE:** For a description of each IOA Pre-deployment screen, refer to [IOA Pre-deployment Wizard](#)



**Figure 47. IOA Pre-deployment Management IP Address Screen**

1. From the menu, click **Network** > *Fabric Name* and then click the **Configure and Deploy** tab.
2. From the **Deploy Fabric** drop-down menu, select **Pre-deployment Configuration**.  
The pre-deployment **Introduction** screen appears.
3. On the **Introduction** screen, review the useful information that you need to gather before you begin.
4. Click **Auto Populate IP Address** and enter the starting IP address and prefix in the **Start IP Address/Prefix** field.
5. Click the **Configure Default Gateway** link and then enter the address of the default gateway for the management interface.
6. Click the **Configure Management Route** link and enter the IP address used by the management route. Enter the gateway prefix in the field after the slash.
7. Click **Next** to go to the **VLAN Configuration** screen.

### Pre-deployment (IOA) – VLAN Configuration

1. From the menu, click **Network** > *Fabric Name* and then click the **Configure and Deploy** tab.

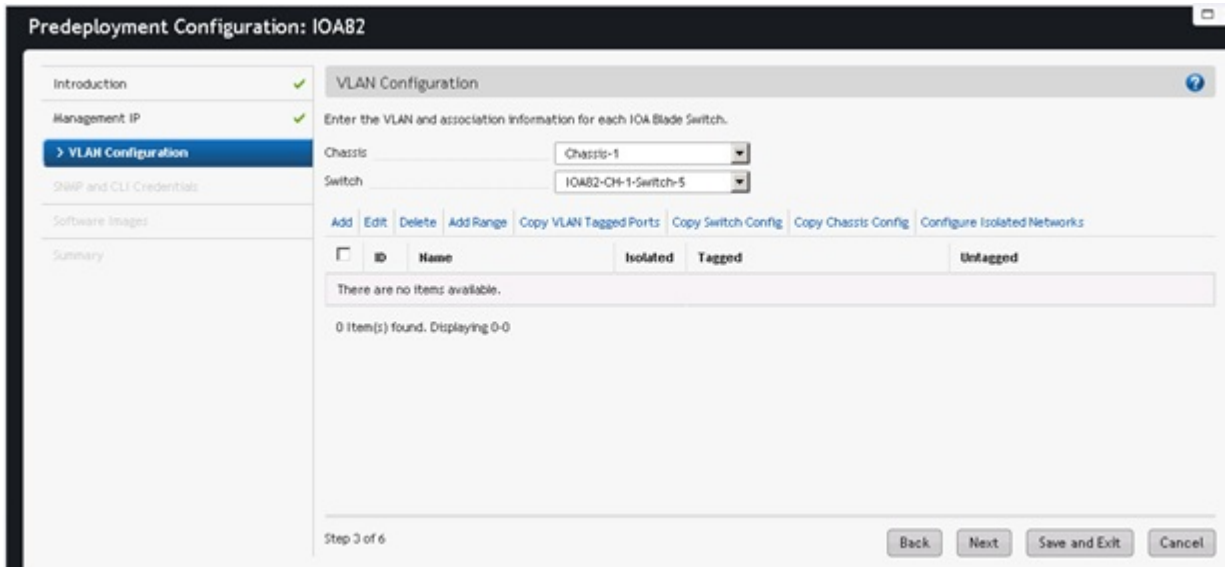


Figure 48. IOA Pre-deployment VLAN Configuration

2. From the **Deploy Fabric** drop-down menu, select **Pre-deployment Configuration**. The pre-deployment **Introduction** screen displays.
3. Navigate to the **VLAN Configuration** screen.
4. From the **Chassis** drop-down menu, select a chassis name that you want to configure.
5. From the **Switch** drop-down menu, select the name of the switch that you want to configure.

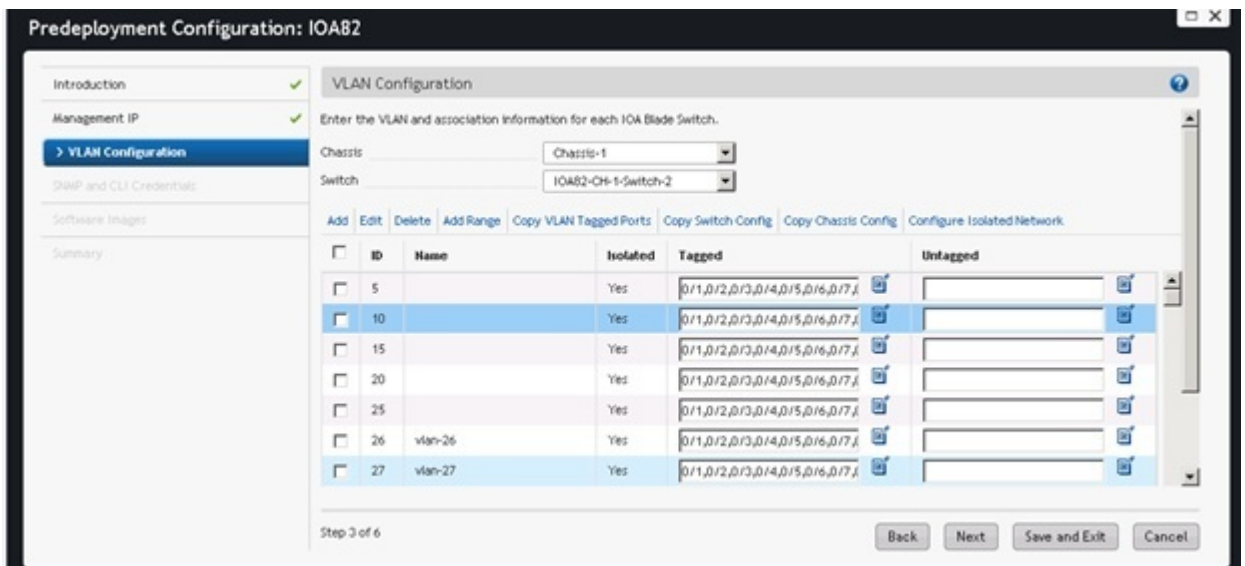
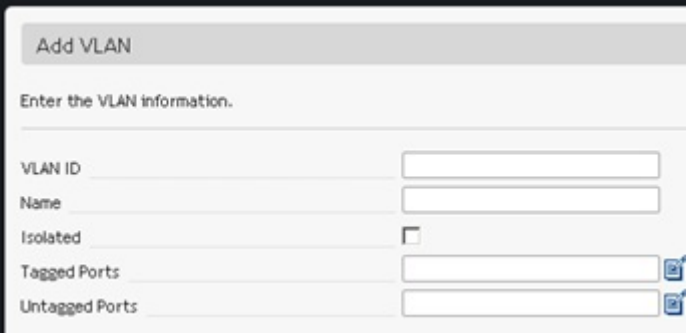

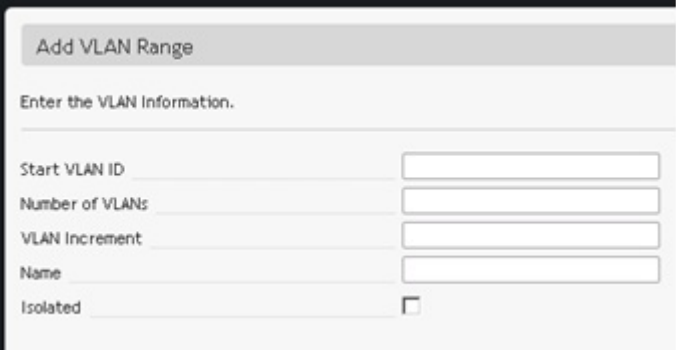
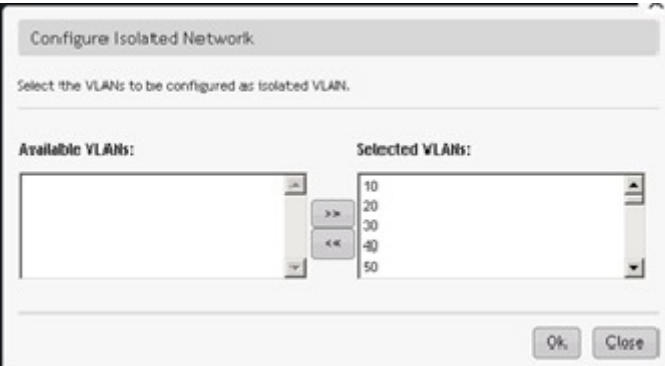

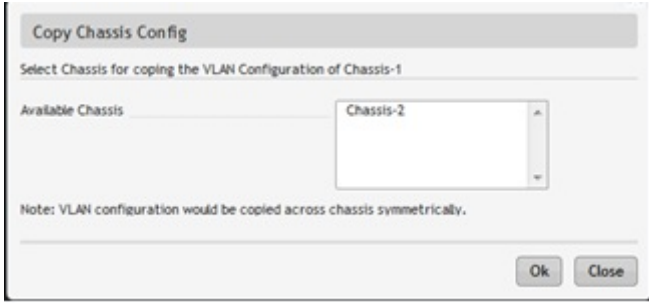
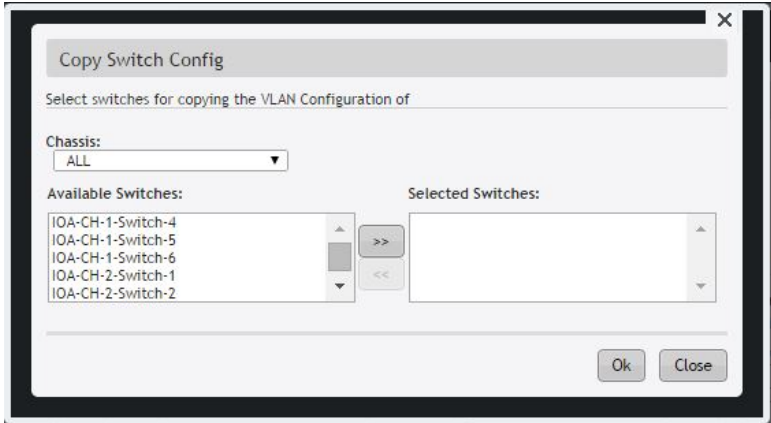


Figure 49. IOA Pre-deployment VLAN Configuration with Populated Data

The following Pre-deployment IOA VLAN configuration options are available:

Table 38. IOA VLAN Pre-deployment Options

| VLAN Option                              | Description  |
|--|--|
| <p><b>Add VLAN</b></p>                   | <p>Create a VLAN. The range is 2–4094.</p>  <p> <b>NOTE:</b> VLAN ID 1003 is reserved.</p>                                  |
| <p><b>Add VLAN Range</b></p>             | <p>Create a VLAN range.</p>   |
| <p><b>Configure Isolated Network</b></p> | <p>Enable the isolated network security feature on a VLAN or a range of VLANs. Only standalone mode is supported. For more information about this option, refer to <a href="#">Isolated Networks</a>.</p>  |

| VLAN Option                       | Description  |
|-----------------------------------|--|
| <b>Copy Chassis Configuration</b> | <p>Copy the chassis configuration from the current chassis to another chassis in the fabric.</p> <p> <b>NOTE:</b> The VLAN configuration is copied symmetrically to the new chassis. For example, the port assigned as Port 1 on the source chassis is also assigned as Port 1 on the destination chassis.</p>  |
| <b>Copy Switch Config</b>         | <p>Copy the IOA VLAN configuration to any IOAs inserted in the same or different M1000e chassis. Copy the VLAN configuration from and to multiple chassis or switches.</p>    |
| <b>Copy VLAN Tagged Ports</b>     | Copy the VLAN tagged port configuration from a selected port to other ports within a switch.   |
| <b>Edit</b>                       | Edit the VLAN configuration.   |
| <b>Delete</b>                     | Remove the VLAN configuration.   |

6. Click **Next** to go to the **SNMP and CLI Credentials** screen.

### Isolated Networks

The isolated networks security feature can be enabled on a VLAN or a range of VLANs. Only standalone mode is supported, as there is only a single LAG uplink.

When you enable this feature:

- Server-to-server communication is disabled on VLANs where the isolated networks feature is enabled.
- Servers on those VLANs can only communicate through the uplink LAG (core).

- The uplink core (ToR) applies all the required security measures and other services before switching or routing traffic.
- The VLAN is configured only on the server-side interface specified as the isolated network. All traffic arriving on this interface from the server is sent to the associated uplink.
- Multiple servers belonging to the same VLAN cannot communicate with each other over IOA because all traffic is sent to the single uplink LAG and is not switched locally.
- For security, unknown unicast and multicast traffic received at the IOA uplink LAG is blocked towards the server-side interfaces over VLANs that have the isolated network feature enabled.

The following illustration shows multiple servers (server M620A and server M620B) belonging to the same VLAN (VLAN 5). For security, the servers cannot communicate with each other over IOA because all the traffic is sent to the single uplink LAG (ToR) and is not switched locally. There is no switching between the server ports.

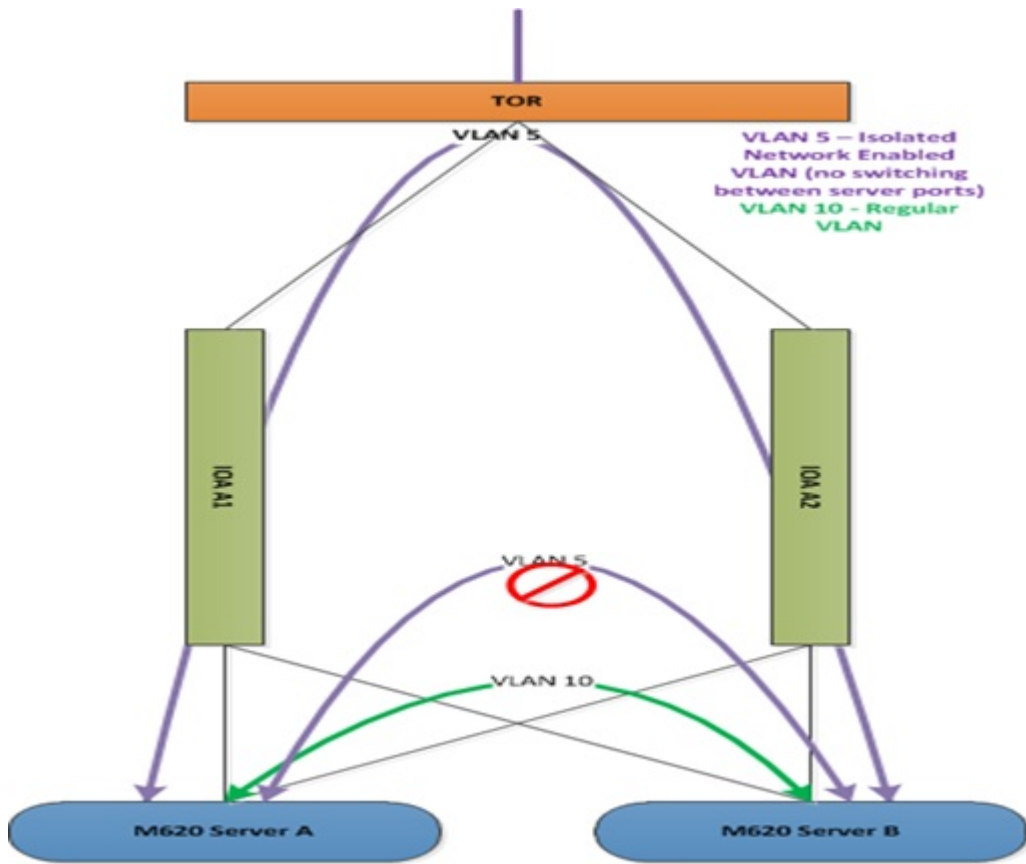


Figure 50. Isolated Networks Enabled on VLAN 5

### Pre-deployment (IOA) — SNMP and CLI Credentials

Configure SNMP so that the AFM can perform SNMP queries on the switches in the fabric. Configure SNMP and CLI credentials at the fabric level.

1. From the menu, click **Network** > *Fabric Name* and then click the **Configure and Deploy** tab.
2. From the **Deploy Fabric** drop-down menu, select **Pre-deployment Configuration**.
3. Navigate to the **SNMP and CLI Credentials** screen.

**Predeployment Configuration: IOAcore**

Introduction ✓  
Management IP ✓  
VLAN Configuration ✓  
**> SNMP and CLI Credentials**  
Software Images  
Summary

**SNMP and CLI Credentials**

Overwrite default SNMP and CLI credentials, if required.

**SNMP Configuration:**

Read Community String: public  
Write Community String: private  
Trap Host: 10.16.140.43  
Trap Port: 162  
SNMP Port: 161

**CLI Credentials:**

Protocol: SSHv2  
User Name: root  
Password: \*\*\*\*\*  
Confirm Password: \*\*\*\*\*  
Enable Password: \*\*\*\*\*  
Confirm Enable Password: \*\*\*\*\*

Show Password as Text

Step 4 of 6

Back Next Save and Exit Cancel

**Figure 51. IOA SNMP and CLI Credentials Screen**

4. In the **Read Community String** field, enter the read community string (for example, `public`).
5. In the **Write Community String** field, enter the write community string (for example, `private`).
6. From the **Protocol** drop-down menu, select one of the following protocols:
  - **Telnet**
  - **SSHv2**




**NOTE:** AFM automatically enters the default IOA credentials (username `root`, password `calvin`).

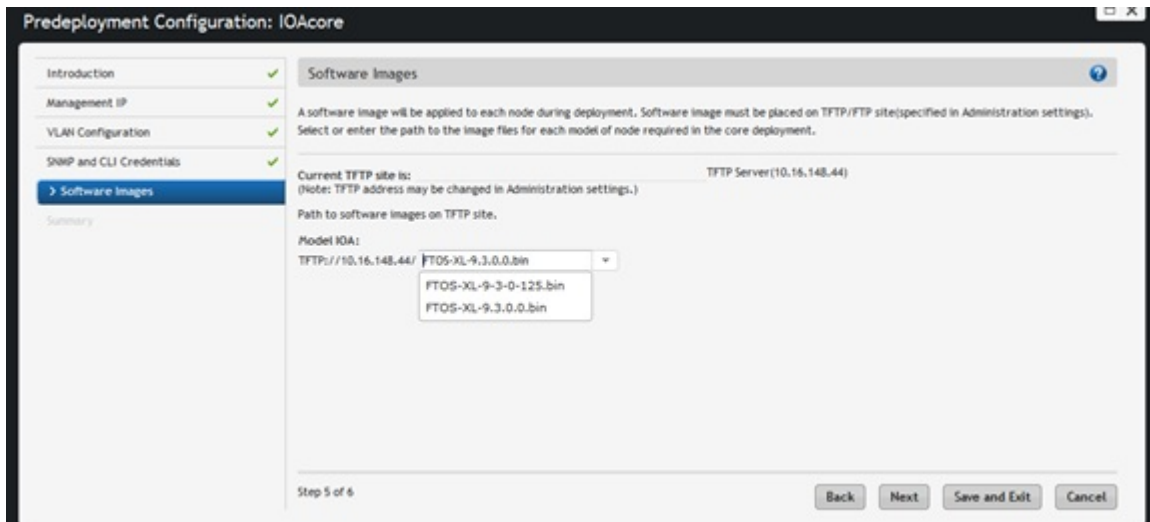
7. In the **User Name** field, enter the user name.
8. In the **Password** field, enter the password.
9. In the **Confirm Password** field, confirm the password.
10. In the **Enable Password** field, enter the enable password.
11. In the **Confirm Enable Password** field, confirm the enable password
12. Click **Next** to go to the **Summary** screen.

### **Pre-Deployment (IOA) – Software Images**

To specify the software images for each type of switch in the fabric, use the Software Images screen. The software image must be the same for each type of platform. Place the software image for the switches on the TFTP or FTP site so that the switches can install the appropriate Dell Networking operating system software image and configuration file from this site. To change the address of the TFTP or FTP site, navigate to the **Administration > Settings > TFTP/FTP** screen.

 **NOTE:** To download the latest Dell Networking operating system software version for the switch, refer to *Upload Switch Software* in the *AFM Installation Guide*.

1. From the menu, click **Network** > *Fabric Name* and then click the **Configure and Deploy** tab.
2. From the **Deploy Fabric** drop-down menu, select the **Pre-deployment Configuration** option.
3. Navigate to the **Software Images** screen.



**Figure 52. IOA Pre-deployment Software Images Screen**

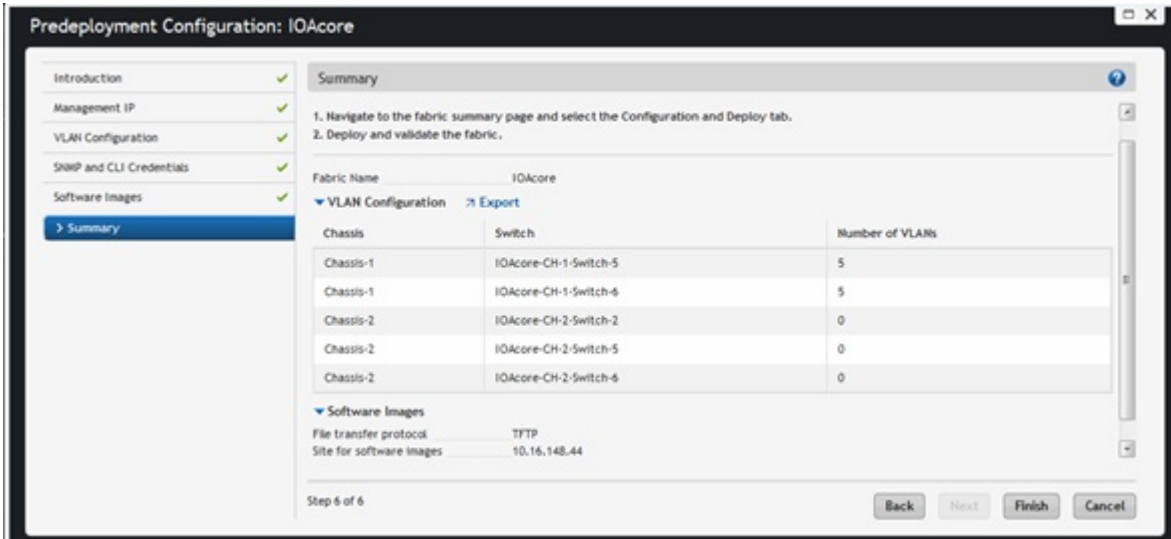
4. Select the TFTP or FTP site option that contains the software image.
5. Enter the path of the software image on the TFTP or FTP site.
6. Click **Next** to go to the **Summary** screen.

### **Pre-Deployment (IOA) – Summary**

To review the IOA pre-deployment configuration, use the **Summary** screen. This screen displays the specified IP and protocol settings for the fabric, uplink, and downlink configuration. It also displays the software image information for each type of switch and the configuration file transfer status to the remote or local TFTP or FTP server.

1. From the menu, click **Network** > *Fabric Name* and then click the **Configure and Deploy** tab.
2. From the **Deploy Fabric** drop-down menu, select the **Pre-deployment Configuration** option.
3. Navigate to the **Summary** screen.
4. Review the IOA pre-deployment summary information. To export configure VLAN information, click **Export**.

**Figure 53. IOA Pre-deployment Summary Information**



5. Click **Finish**.

### Next Steps

1. Deploy the IOA switches from the **Network > Fabric > Configuration and Deploy > Deploy and Validate > Deploy** screen.

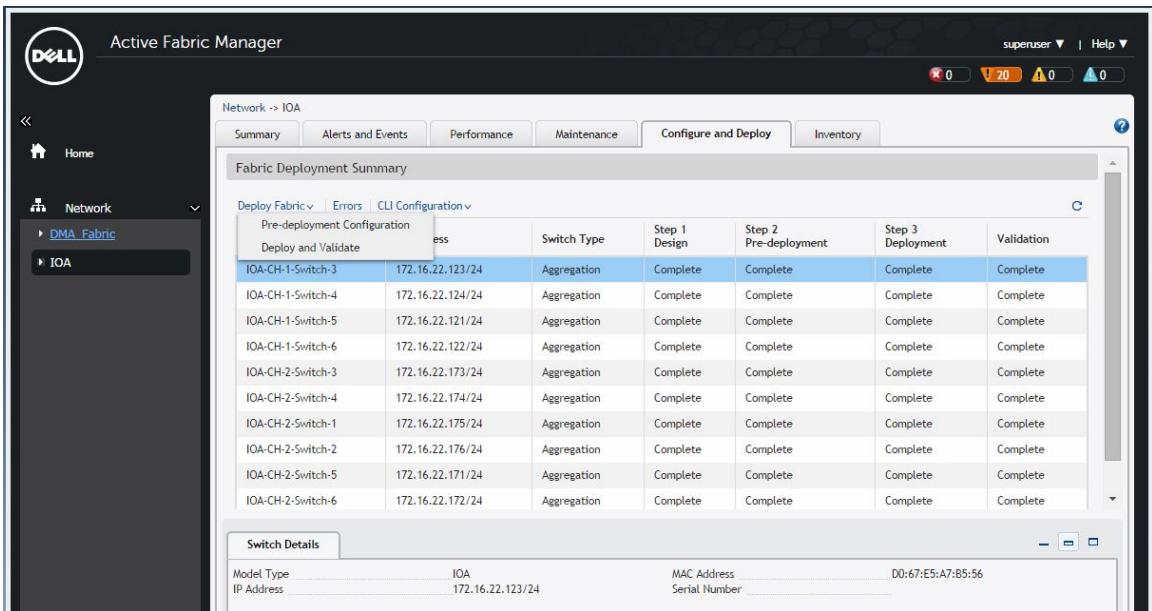


Figure 54. IOA Deploy and Validate



**NOTE:**

Before deployment, make sure that the IOA switches are in standalone mode using the following CLI command:

```
show system stack-unit <unit-number> iom-mode
```

For more information about this command, refer to the *Dell PowerEdge Command Line Reference Guide for the M I/O Aggregator*.

2. During deployment, check for IOA deployment failures such as **Not being in Standalone Mode** in the **Response Actions** column. To correct this issue, set the IOA to standalone mode and then redeploy it. For information about IOA pre-deployment error messages, see [IOA Pre-deployment Error Messages](#).

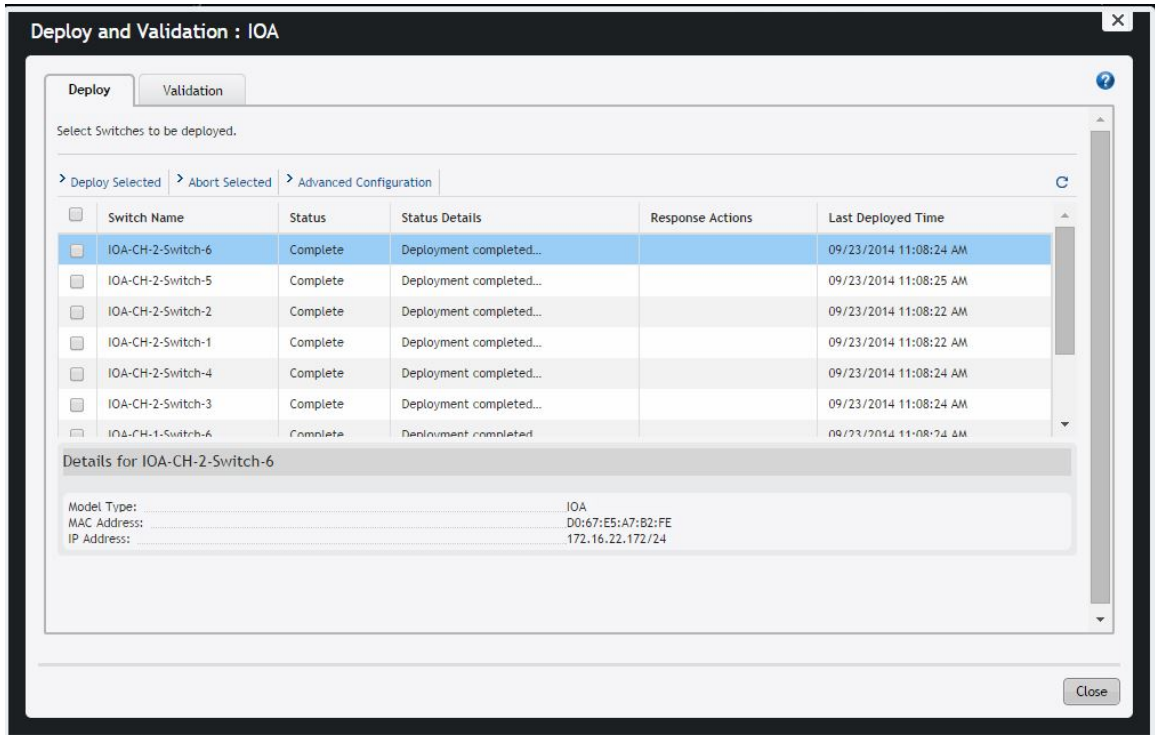


Figure 55. Deploy and Validation Tabs

### IOA Pre-Deployment Error Messages

To troubleshoot the IOA pre-deployment, use the following table.

Table 39. IOA Pre-Deployment Error Messages

| Error  | Recommended Action  |
|--|---|
| Discovered MAC is different from planned MAC     | Make sure that the MAC provided for this device is correct. |
| Discovered model is different from planned model | Make sure the model provided for this device is correct.    |
| IOA is not in standalone mode                    | Make sure that the IOA is in standalone mode.               |


| Error   | Recommended Action   |
|---|--|
| IOA Software Upgrade task: Failed   | <ol style="list-style-type: none"> <li>1. Power cycle the IOA.</li> <li>2. Make sure that the image is present on the TFTP or FTP site.</li> <li>3. Verify Telnet/SSH connectivity from AFM server and re-deploy.</li> </ol> |
| Ping verification: Failed   | From the AFM server, verify connectivity to the IOA device.  |
| Telnet/SSH session verification: Failed   | Make sure Telnet/SSH session available from the AFM server has the correct credentials.  |
| Racadm Set IP error — Stacked switches do not support the specified switch operation. | Change the switch mode to standalone mode and then complete pre-deployment.  |
| Unable to get the MAC Address through Racadm  | Verify that the chassis/device is reachable and then rediscover it.  |
| Unable to set the Management IP in IOA device   | Verify that the chassis/device is reachable or a valid management IP/subnet mask/gateway IP is specified.  |
| Unable to upgrade required software version   | Make sure that the IOA is using the required software release.   |

## VLT/Distributed Core Pre-Deployment Wizard

 **NOTE:** If you are designing a fabric using an IOA blade switch, refer to [IOA Pre-deployment Wizard](#).

### Prerequisites

Before you begin:

1. Rack the equipment in the fabric.
  -  **NOTE:** Before racking the switches, make sure that you have the `.csv` file that contains the system MAC addresses for each switch in the fabric. If you do not have this file, record the system addresses before you rack the switches.
2. Power off the switches in the fabric.
3. Gather the useful information listed in [Gathering Useful Information for a Layer 3 Distributed Core Fabric](#), [Gathering Useful Information for a Layer 2 VLT Fabric](#), or [Gathering Useful Information for a Layer 3 with Resiliency \(Routed VLT\) Fabric](#).

### Pre-Deployment Screens

To provide the minimum configuration to the switches for the fabric, use the following **Pre-deployment** screens. These screens automate the deployment process.

- **Assign Switch Identities** — Assign a system media access control (MAC) address to each switch in the fabric. You can optionally assign serial numbers and Service Tags to each switch.
- **Change Port Status** — (Advanced fabric only) Enable, disable, or manually select downlinks for Advanced fabric designs.

- **DHCP Integration** — Create a `dhcp.cfg` file that loads the correct software image and the configuration file for each switch type. The DHCP server also uses this file to assign a management IP address to each switch.
  - ✍ **NOTE:** Install the DHCP configuration file on the DHCP server before you deploy the fabric.
- **Downlink Configuration** — For a Layer 3 Distributed Core or Layer 3 with Resiliency (Routed VLT) fabric. Configure an EdgePort that connects to the access layer, such as servers or a ToR.
- **Fabric link Configuration** — For a Layer 3 or Layer 3 with Resiliency (Routed VLT) fabric. For a Layer 3 fabric, configure options for the communication between the spine and leaf. For a Layer 3 with Resiliency (Routed VLT) fabric, configure the links that connect the core, access, and aggregation switches in the fabric.
- **License Update** — For Advanced fabric designs with Z9500-series switches, specify license files.
- **Management IP** — Specify a management IP address to each switch.
- **Output** — View the uplink and downlink configuration on the leaf or access switches. Verify that this information is correct before deployment.
- **Port Channel Configuration** — Add, edit, delete, and automatically populate the port channel configuration or copy a switch port channel configuration to another port.
- **SNMP and CLI Credentials** — Configure SNMP and CLI credentials at the fabric level. Configure SNMP so that AFM can perform SNMP queries on the switches in the fabric.
- **Software Images** — Specify the TFTP or FTP address (local or remote server) and the path of the Dell Networking operating system software image to download to each type of switch. To stage the software, use this address.
- **Storage Facing Ports** — (LAN/SAN with iSCSI or fibre channel only) Establish storage connectivity to iSCSI or fibre channel port.
- **Summary** — View the fabric name, location of the software image, and DHCP configuration file.
- **Uplink Configuration** — Specify an even number of uplinks. The minimum number of uplinks is two. One uplink is reserved for redundancy.
  - For a Layer 3 distributed core fabric, configure an EdgePort link on the first two leaves that connect to the edge WAN, which typically connects to an internet service provider (ISP).
  - For a Layer 2 VLT fabric or Layer 3 with Resiliency (Routed VLT) fabric, configure an EdgePort link (uplinks) on the first two aggregation devices that connect outside the fabric.
- **VLAN Configuration** — Specify a VLT VLAN to apply to the Layer 2 VLT or Layer 3 with Resiliency (Routed VLT) fabric. Include at least one VLAN configuration.
- **VLAN Mapping** — For a Layer 2 VLT fabric or Layer 3 fabric with Resiliency (Routed VLT). Associate each of the ports of an access switch to one or more VLANs. You can associate one or more tagged VLANs. Untagged VLANs support only one association.

## Protocol Configuration — Layer 2 VLT Fabric Designs

Complete the following pre-deployment protocol configuration tasks for Layer 2 fabric designs.

1. Review the pre-deployment workflow for a Layer 2 fabric at [Using the Pre-Deployment Configuration Wizard](#).
2. [Pre-Deployment — Uplink Configuration](#)
3. [Pre-Deployment — VLAN Configuration](#)
4. [Pre-Deployment — Port Channel Configuration](#)
5. [Pre-Deployment — Storage Facing Ports \(For LAN/SAN deployments only\)](#)
6. [Pre-Deployment — VLAN Mapping](#)

## L2 VLT Pre-Deployment – Uplink Configuration

The **Uplink Configuration** screen displays the port bandwidth and the number of specified ports as read-only fields on the **Fabric Name and Type** and **Port Specification** screens. To configure the uplink protocol for the EdgePort uplinks to the WAN, use the **Uplink Configuration** screen.

**NOTE:** If you enable OSPF, the uplinks or interlinks must be in area 0.

Predeployment Configuration: 2tier

Uplink Configuration

Configure protocol settings below

Specified number of uplink ports: 12

Type of Uplink Ports:  L2  L3

Protocol Settings:  Static Route  OSPF  IBGP  eBGP

Area ID:

Loopback IP Address/Prefix:  /

| Switch Name | Port No                 | Local IP/Prefix                             | Remote IP/Prefix                            | Area ID              |
|-------------|-------------------------|---|---|----------------------|
| 2tier-Agg-1 | TenGigabitEthernet 0/4  | <input type="text"/> / <input type="text"/> | <input type="text"/> / <input type="text"/> | <input type="text"/> |
| 2tier-Agg-1 | TenGigabitEthernet 0/5  | <input type="text"/> / <input type="text"/> | <input type="text"/> / <input type="text"/> | <input type="text"/> |
| 2tier-Agg-1 | TenGigabitEthernet 0/56 | <input type="text"/> / <input type="text"/> | <input type="text"/> / <input type="text"/> | <input type="text"/> |
| 2tier-Agg-1 | TenGigabitEthernet 0/57 | <input type="text"/> / <input type="text"/> | <input type="text"/> / <input type="text"/> | <input type="text"/> |
| 2tier-Agg-1 | TenGigabitEthernet 0/58 | <input type="text"/> / <input type="text"/> | <input type="text"/> / <input type="text"/> | <input type="text"/> |
| 2tier-Agg-1 | TenGigabitEthernet 0/59 | <input type="text"/> / <input type="text"/> | <input type="text"/> / <input type="text"/> | <input type="text"/> |

Step 2 of 12

Back Next Save and Exit Cancel

Figure 56. Uplink Configuration Screen

Predeployment Configuration: 2tNS

Uplink Configuration

Configure protocol settings below

Specified number of uplink ports: 4

Type of Uplink Ports:  L2  L3

Protocol Settings:  Static Route  OSPF  IBGP  eBGP

Area ID:

Loopback IP Address/Prefix:  /

| Switch Name | Port No | Local IP/Prefix                             | Remote IP/Prefix                            | Area ID              | Vlan ID              |
|-------------|---------|---|---|----------------------|----------------------|
| 2tNS-Agg-1  | Te1/0/4 | <input type="text"/> / <input type="text"/> | <input type="text"/> / <input type="text"/> | <input type="text"/> | <input type="text"/> |
| 2tNS-Agg-1  | Te1/0/5 | <input type="text"/> / <input type="text"/> | <input type="text"/> / <input type="text"/> | <input type="text"/> | <input type="text"/> |
| 2tNS-Agg-2  | Te1/0/4 | <input type="text"/> / <input type="text"/> | <input type="text"/> / <input type="text"/> | <input type="text"/> | <input type="text"/> |
| 2tNS-Agg-2  | Te1/0/5 | <input type="text"/> / <input type="text"/> | <input type="text"/> / <input type="text"/> | <input type="text"/> | <input type="text"/> |


Step 2 of 12

Back Next Save and Exit Cancel

Figure 57. Uplink Configuration Screen (N Series Switches)

1. From the menu, click **Network** > *Fabric Name* and then click the **Configure and Deploy** tab.
2. From the **Deploy Fabric** drop-down menu, select **Pre-deployment Configuration**.
3. Navigate to the **Uplink Configuration** screen.
4. In the **Type of Uplink Ports** area, select one of the following options:
  - **L2** — Configure Layer 2 uplinks for a Layer 2 fabric.

- **L3** — Configure uplinks for a Layer 2 VLT or Layer 3 Distributed Core fabric. If you select the L3 option, the **Uplink Configuration** screen displays additional options to configure the Layer 3 protocol settings.
5. **Static Route** — If you select this option, click **Add** in the **Route Configuration** area to display **Add Static Route** dialog box. Configure up to 10 static routes for each aggregation device. If you select the **Default Route** check box, AFM automatically populates the destination network field to 0.0.0.0/0. For static routes, enter the destination network and the next hop.
  6. (For Layer 3 uplinks only) For the **Protocol Settings**, select a routing protocol (OSPF, IBGP, or eBGP) or static route for the EdgePort uplinks. AFM automatically populates the range of IP addresses in the /30 subnet.
    - If you enable OSPF, enter the local IP address, remote neighbor IP address, and area ID for each specified uplink. For all switches except N series, the area ID range is 0–65535; for N series switches it is 0–4294967295.
    - If you enable iBGP, enter the local IP address, remote neighbor IP address, and local AS number for each specified uplink. For all switches except N series, the AS number range is 1–4294967295. For N series switches, the AS number should be between 1 and 65534 but excluding the range of 56320 to 64511.
    - If you enable eBGP, enter the local IP address, remote neighbor IP address, local AS number, and remote AS number for each specified uplink. The AS number range is 1–4294967295. For N series switches, the AS number should be between 1 and 65534 but excluding the range of 56320 to 64511.
  7. In the **Loopback IP Address Range/Prefix** area, enter the loopback IP address and prefix.
  8. (N series switches only) In the **Vlan ID** field, enter the VLAN ID. The VLAN ID range is 2–4094; for Z9500 series switches the VLAN ID range is 2–4093.
 

 **NOTE:** The VLAN ID 4093 is reserved for N20XX series switch management purposes.
  9. To go to the **VLAN Configuration** screen, click **Next**.

## L2 VLT Pre-Deployment — VLAN Configuration

Specify at least one VLAN for the Layer 2 fabric manually or automatically using this screen.

1. From the menu, click **Network** > *Fabric Name* and then the **Configure and Deploy** tab.
2. From the **Deploy Fabric** drop-down menu, select the **Pre-deployment Configuration** option.
3. Navigate to the **VLAN Configuration** screen.

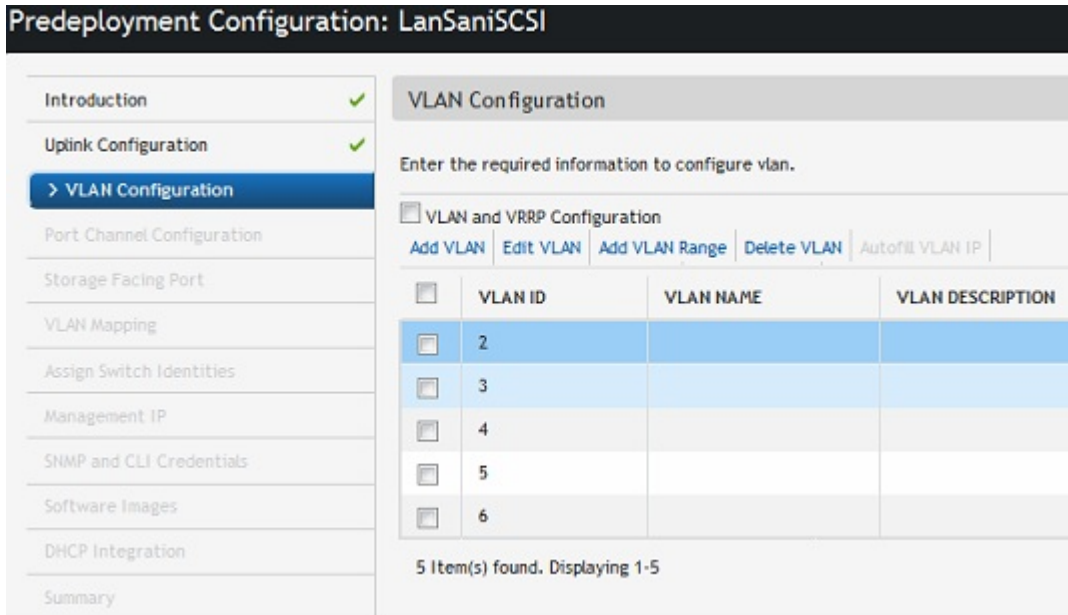


Figure 58. VLAN Configuration without VLAN and VRRP Configuration



4. To configure the VLAN ID, primary IP address, secondary IP address, and virtual address, select **VLAN and VRRP Configuration**.
5. Click the **Add VLAN** link.  
The **Add VLAN** dialog box appears.
  -  **NOTE:** If you add a VLAN and do not enable the **VLAN and VRRP Configuration** option, you can only enter the VLAN ID name and description.
6. In the mandatory **VLAN ID** field, enter the VLAN ID. The range is 2–511. There is no default value.
7. In the **Primary IP address** field, enter the primary IP address. AFM automatically enters the default prefix (24), but there is no default IP address. The range is 8–29.
8. In the **Secondary IP** address field, enter the secondary IP address. AFM automatically enters the default prefix (24), but there is no default secondary IP address. The range is 8–29.
9. In the **Virtual IP** address field, enter the virtual IP address. AFM automatically enters the default prefix (24), but there is no default virtual IP address. The range is 8–29.
10. Click **Next** to view the **Port Channel Configuration** screen.

Table 40. VLAN Configuration Options

| VLAN Option    | Description  |
|----------------|--|
| Add VLAN       | Enter the VLAN ID.   |
| Edit VLAN      | Change the VLAN ID or VLAN ID, primary IP address, secondary IP address.   |
| Add VLAN Range | Automates VLAN creation and automatically populates IP addresses. Enter the following mandatory VLAN settings: <ul style="list-style-type: none"> <li>• <b>Starting VLAN ID</b> — Specify the starting VLAN ID. The range is 2–511.</li> <li>• <b>Number of VLANs</b> — Specify the number of VLANs.</li> <li>• <b>VLAN Increment</b> — Specify the increment of the VLAN. If you do not specify an increment, the default VLAN increment is one.</li> <li>• <b>VLAN Name Prefix</b> — Specify the name prefix of the VLAN.</li> </ul> |

| VLAN Option   | Description   |
|---|---|
|   | <ul style="list-style-type: none"> <li>• <b>VLAN Description</b> – Specify a description of the VLAN range.</li> <li>• <b>Start Subnet IP Address/Prefix</b> – Specify the IP range to automatically populate VLAN IP addresses. Valid IP addresses include primary, secondary peer VLAN, and VRRP IP.</li> </ul> <p> <b>NOTE:</b> Select the <b>VLAN and VRRP Configuration</b> check box in the <b>VLAN Configuration</b> screen. to view this option.</p> |
| Delete VLAN   | Remove the selected VLAN row.   |
| Autofill VLAN IP (For VLAN and VRRP Configuration only) | Enter the starting subnet IP address/prefix for the range of selected VLAN. AFM automatically populates the IP addresses.   |
| VLAN and VRRP Configuration                             | Configure an IP address using VRRP. If you select <b>VLAN and VRRP Configuration</b> , the following fields appear: <ul style="list-style-type: none"> <li>• Primary IP</li> <li>• Secondary IP</li> <li>• Virtual IP</li> </ul>  |

## L2 VLT Pre-Deployment – Port Channel Configuration

You can add, edit, delete, and automatically populate the port channel information, on the **Port Channel Configuration** screen. Once you add a port channel configuration, you can copy it for use in another fabric. You can also configure uplink LAGs on this screen.

1. From the menu, click **Network** > *Fabric Name* and then the **Configure and Deploy** tab.
2. From the **Deploy Fabric** drop-down menu, select **Pre-deployment Configuration**.
3. Navigate to the **Port Channel Configuration** screen.

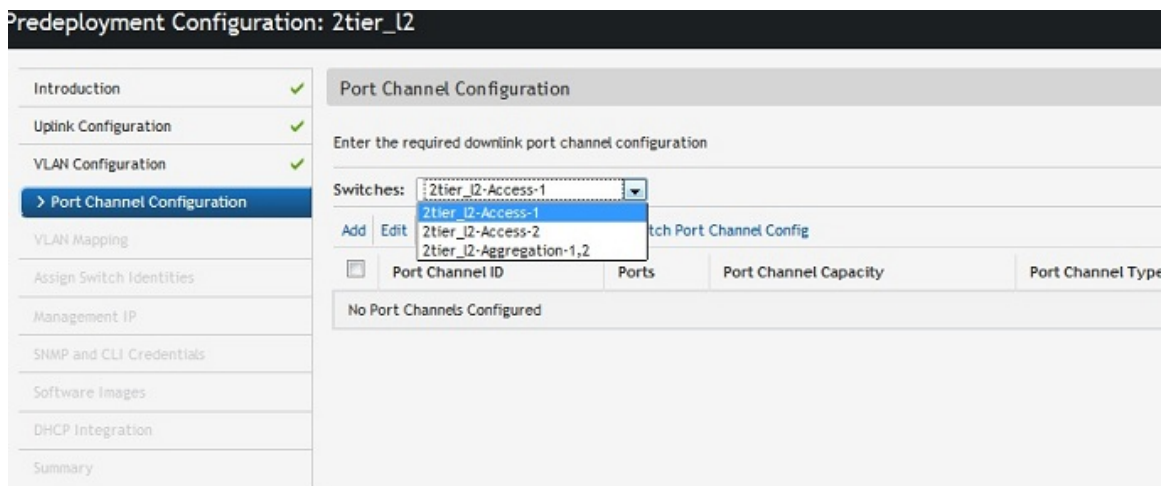


Figure 59. Port Channel Configuration Screen

4. From the **Switch** drop-down menu, select the switch for the port channel configuration.
5. Click **Add** to add a port channel manually or click **Auto Populate** to automatically populate the port channels. For more port channel configuration options, refer to the following table.

**Table 41. Layer 2 Port Channel Configuration Options**

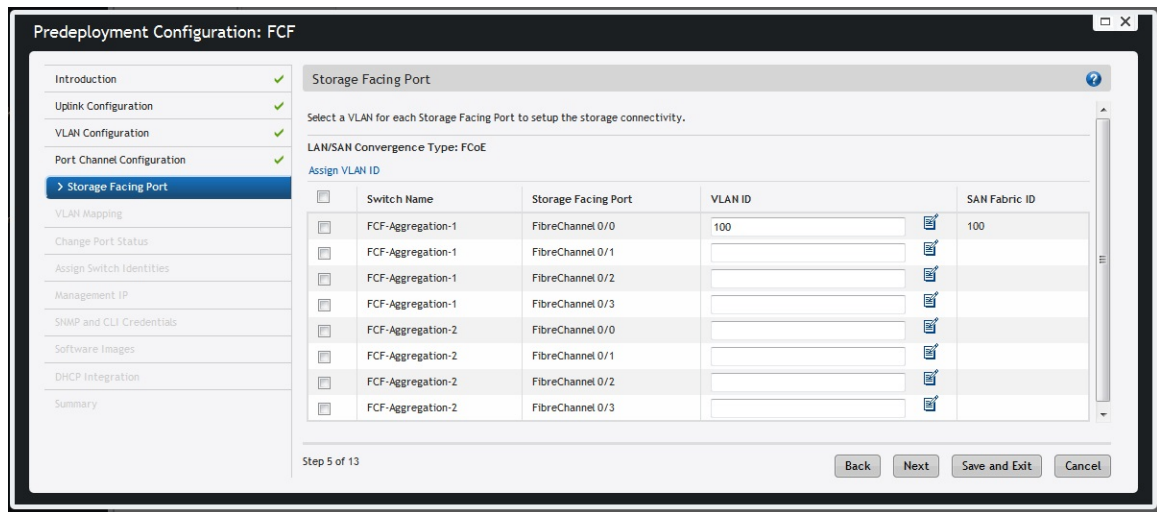
| Command                                       | Description  |
|---|--|
| <b>Add</b>                                    | Enter port channel information and enable LACP.  |
| <b>Edit</b>                                   | Enter the port channel configuration.  |
| <b>Delete</b>                                 | Delete the selected port channel configuration.  |
| <b>Auto Populate</b>                          | Enter the following port channel information to automatically assign port channels to switches in the fabric and enable LACP. <ul style="list-style-type: none"> <li>• <b>Number of Ports per Port Channel</b></li> <li>• <b>Start Port Channel ID</b></li> <li>• <b>Port Channel Increment</b></li> <li>• <b>Number of Port Channel</b></li> <li>• <b>Enable LACP</b> (optional)</li> </ul> |
| <b>Copy Switch Port Channel Configuration</b> | Copy switch port channel configuration from another switch. Create a port channel configuration and copy the configuration to another switch.  |

6. Click **Next** to go to the **VLAN Mapping** screen.

### L2 VLT Pre-Deployment — Storage Facing Port

To establish storage connectivity to iSCSI or fibre channel port, use the **Storage Facing Port** screen. The **Storage Facing Port** pre-deployment screen is available only for LAN/SAN deployments using iSCSI or fibre channel ports.

1. From the menu, click **Network > Fabric Name** and then the **Configure and Deploy** tab.
2. From the **Deploy Fabric** drop-down menu, select **Pre-deployment Configuration**.
3. Navigate to the **Storage Facing Port** screen.

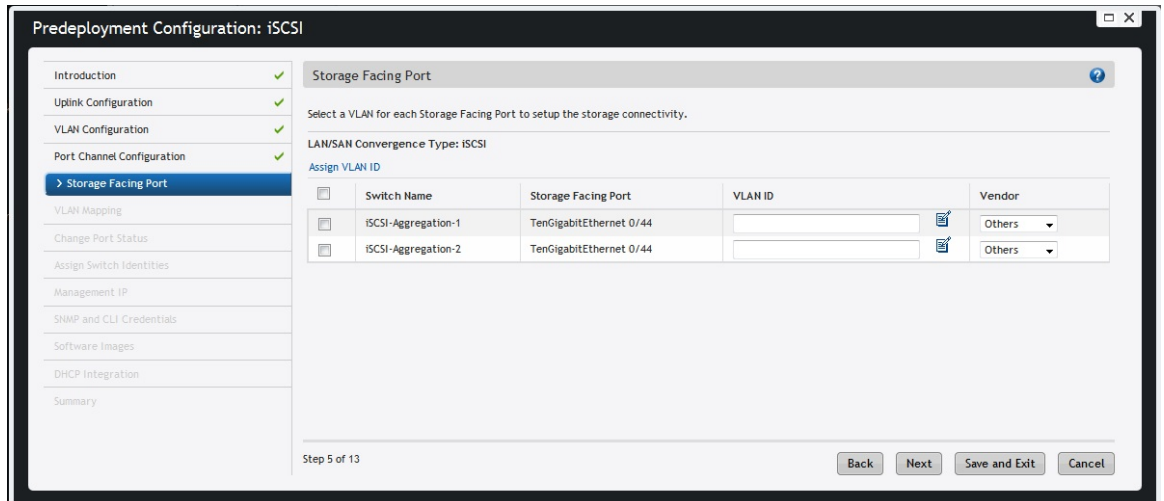


**Figure 60. Storage Facing Port Screen**


4. Navigate to the **VLAN ID** column.
5. Click the VLAN ID icon to the right of the VLAN ID field, select a VLAN ID, and associate it with the storage-facing port.



- a. If you connect to fibre channel storage-facing ports, AFM automatically populates the SAN Fabric ID when you select the VLAN ID.
- b. If you connect to iSCSI storage-facing ports, select a VLAN ID and associate it with a vendor. Navigate to the **Vendor** drop-down menu and select one of the following options:
  - Compellent
  - EqualLogic
  - Other



**Figure 61. Selecting a Vendor**

 **NOTE:** Associate only one vendor for each VLAN. If you associate a VLAN to multiple storage-facing ports, AFM automatically sets the vendor as the same across for all associated entries.

6. Click **Next** to go to the **VLAN Mapping** screen.

## L2 VLT/L3 Routed VLT Pre-Deployment — VLAN Mapping

To add VLANs and associate ports on the different switches for a Layer 2 fabric, use the **Downlink Port Configuration** screen. After you add a VLAN and associate it, you can copy switch VLAN or port VLAN configurations. You can associate one or more tagged VLANs with a port. You can only associate one VLAN per port.

1. From the menu, click **Network** > *Fabric Name* and then the **Configure and Deploy** tab.
2. From the **Deploy Fabric** drop-down menu, select **Pre-deployment Configuration**.
3. Navigate to the **VLAN Mapping** screen.

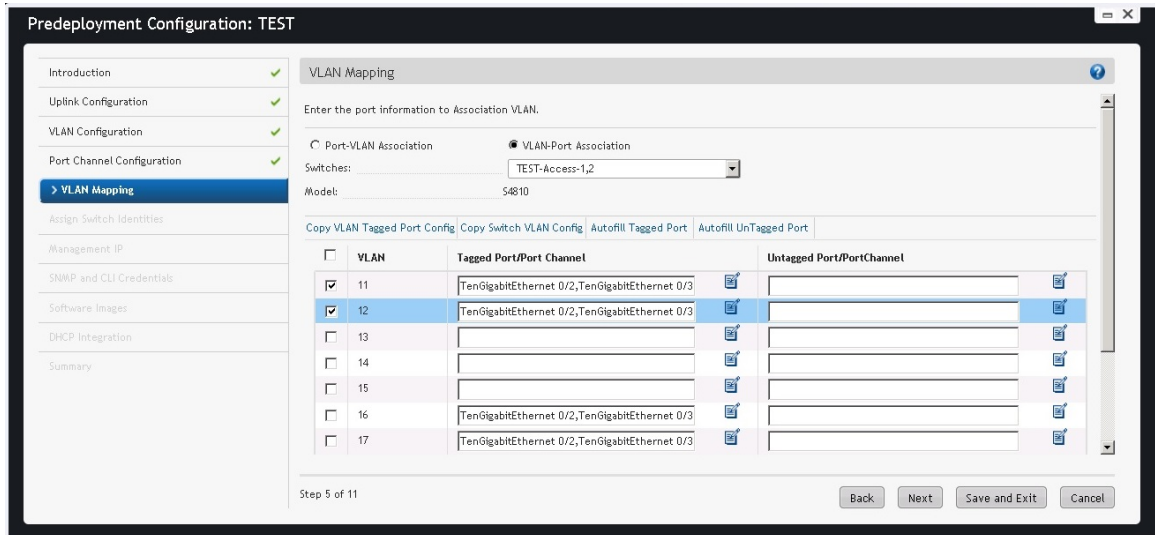



Figure 62. Pre-deployment Configuration – VLAN Mapping

Table 42. VLAN Mapping Field Descriptions

| Field Name       | Description  |
|------------------|--|
| Configured VLANs | View a list of VLANs specified in the VLT VLAN Configuration screen.   |
| Port Name        | View the port name (read-only).  |
| Tagged VLANs     | <p>Enter one or more VLANs to associate with the port. The VLANs must be in the Configured VLANs list and the Untagged VLAN field must be empty. There is no default value.</p> <ol style="list-style-type: none"> <li>Click the icon next to the field entry and select a VLAN from the list.</li> <li>Select one or more VLANs to associate with the port.</li> </ol> <p> <b>NOTE:</b> VLANs previously associated with storage-facing ports are included in the selection list.</p> |
| Untagged VLANs   | <p>Select a VLAN to associate with the port. The Tagged VLAN field must be empty. There is no default value.</p> <p> <b>NOTE:</b> VLANs previously associated with storage-facing ports are included in the selection list.</p>  |

Table 43. Layer 2 VLAN Mapping Options

| Option                  | Description  |
|-------------------------|--|
| Auto-fill Tagged Port   | For selected VLANs, apply sequential tagging to the available ports and the number of ports specified on a VLAN. |
| Auto-fill Untagged Port | For selected VLANs, apply untagged ports. Based on available ports, associate only one port per VLAN.            |

| Option                       | Description   |
|------------------------------|---|
|                              |  <b>NOTE: The number of Port/VLAN Ports</b> option is disabled on the <b>Autofill Tagged/Untagged Port</b> screen. |
| Copy Switch VLAN Config      | Copy the VLAN association from the current switch to other switches in the fabric.  |
| Copy VLAN Port Config        | Copy the VLAN association from a selected port to other ports in a switch.  |
| Port-VLAN Association        | Map the physical port to the VLAN ID. For example, map one port to multiple VLANs.  |
| VLAN-Port Association        | Map the VLAN ID to physical port interfaces. For example, map one VLAN to multiple ports.   |
| Copy VLAN Tagged Port Config | Copy the VLAN tagged port configuration from a selected port to other ports in a switch.  |

- From the **Switches** drop-down menu, select an access or aggregation switch. The selected switch for the VLAN mapping displays in the read-only **Model** field.
- In the **Tagged VLANs** field, click the icon to the right and enter one or more VLANs to associate with the port.
- Click **Next** to go to the **Assign Network Identities** screen.

Enter an example that illustrates the current task (optional).

Enter the tasks the user should do after finishing this task (optional).

## Protocol Configuration — Layer 3 Distributed Core Fabric

To configure the pre-deployment protocol configuration for a Layer 3 distributed core fabric, complete the following tasks:


- Review the pre-deployment workflow for a Layer 3 distributed core fabric at [Using the Pre-deployment Configuration Wizard](#)
- Pre-deployment — fabric link configuration
- Pre-deployment — uplink configuration
- Pre-deployment — downlink configuration

### L3 DC/Routed VLT Pre-Deployment — Fabric Link Configuration

Before you begin, review [Using the Pre-deployment Configuration Wizard](#) and [Pre-deployment Wizard: Introduction](#). To configure links connecting the leaves and spines for a Layer 3 distributed core fabric or links connecting the core, access, and aggregation switches for a Layer 3 with Resiliency (Routed VLT) fabric using the OSPF routing protocol, use the **Fabric link Configuration** screen. The selected fabric type and fabric oversubscription ratio determines the value that AFM automatically assigns to the **Port Bandwidth** read-only field. To automate the pre-deployment process, AFM automatically:

- populates the starting IP address range and prefix
- populate the loop IP address and prefix based on the fabric design
- sets the area ID for OSPF to 0


Review these settings before deployment. You can modify the IP address range and loopback address. The range for the starting prefix for both types of addresses is 8–29 and the range for the loopback prefix is 8–26.

 **NOTE:** The area ID for the interconnect link must not be the same as the area ID for the uplink.

1. From the menu, click **Network** > *Fabric Name* and then the **Configure and Deploy** tab.
2. From the **Deploy Fabric** drop-down menu, select **Pre-Deployment Configuration**.  
The **Introduction** screen appears.
3. Review the **Introduction** screen and gather the useful information for deployment.
4. Click **Next**.  
The **Fabric Link Configuration** screen appears.
5. In the **Start IP Address Range/Prefix** area, enter the starting IP address and prefix.  
The prefix range is 8–29.
6. In the **Loopback IP Address Range/Prefix** area, enter the loopback address range and prefix.  
The prefix range is 8–26.
7. In the **Area ID** field, use the default setting (zero) or enter the area ID.  
The area ID range is 0–65535. The uplinks or interlinks must be in area 0 for OSPF.

### L3 DC/Routed VLT Pre-Deployment — Uplink Configuration

The **Uplink Configuration** screen for a Layer 3 and Layer 3 with Resiliency (Routed VLT) fabric displays the port bandwidth and the number of specified ports as read-only fields on the **Bandwidth and Port Count** screen. To configure the uplink protocol for the EdgePort uplinks to the WAN, use the **Uplink Configuration** screen. For more information about uplinks for a Layer 3 distributed core fabric, refer to [Distributed Core Terminology](#).

 **NOTE:** When OSPF is selected for both uplinks and interlinks, one of uplinks or interlinks must be in area 0.

1. From the menu, click **Network** > *Fabric Name* and then the **Configure and Deploy** tab.
2. From the **Deploy Fabric** drop-down menu, select **Pre-deployment Configuration**.
3. Navigate to the **Uplink Configuration** screen.
4. In the **Type of Uplink Ports** area, select one of the following options:
  - **L2** — Configures Layer 2 uplinks for a Layer 2 fabric. This option is disabled by default on a Layer 3 Distributed Core fabric.
  - **L3** — Configures uplinks for a Layer 2 VLT or Layer 3 Distributed Core fabric. If you select the L3 option, the **Uplink Configuration** screen displays additional options to configure the Layer 3 protocol settings.
5. In the **Protocol Settings** area, select **Static Routes** or routing protocol (**OSPF**, **IBGP**, or **eBGP**) for the EdgePort uplinks.
6. If you select **Static Routes**, AFM displays the **Static Route Configuration** section. Do the following steps:

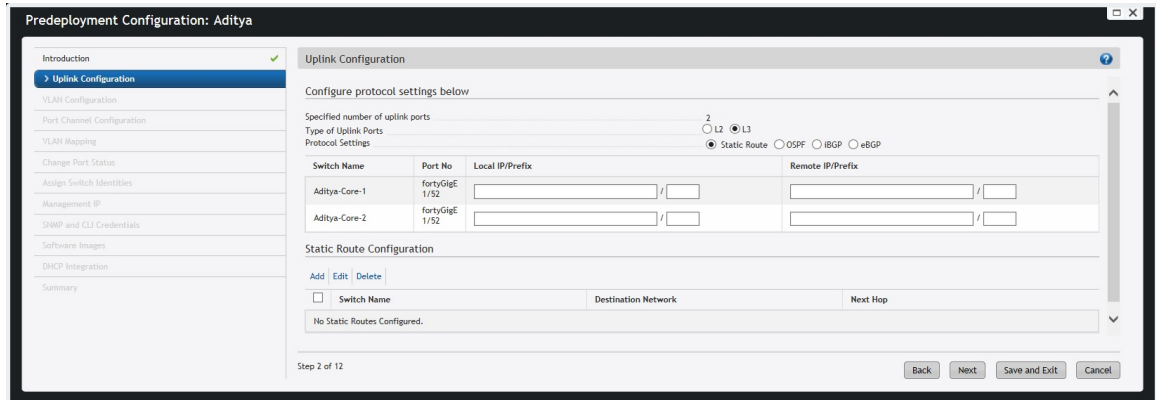


Figure 63. Static Route Configuration Screen

- a. Click **Add** to configure a static route. The **Add Static Route** dialog box appears.

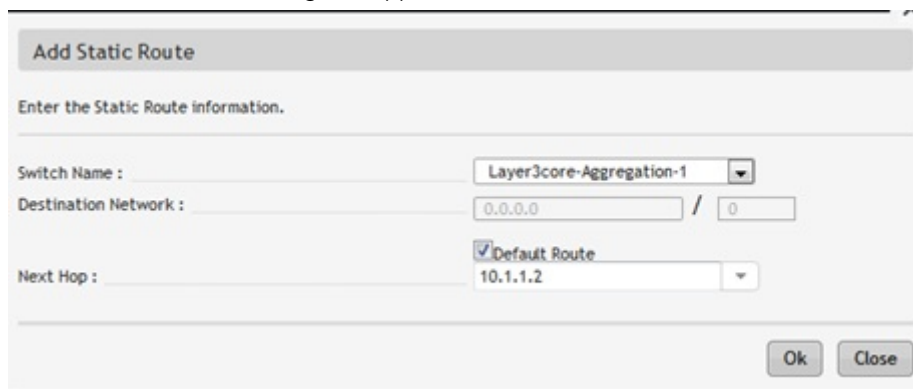



Figure 64. Add Static Route Dialog Box

- b. For static routes, enter the destination network and the next hop. If you select **Default Route**, AFM automatically populates the destination network field as 0.0.0.0/0.
  - c. Click **OK**.
  - d. Repeat steps a-c to add an additional static route. You can configure up to 10 static routes for each aggregation switch.
 

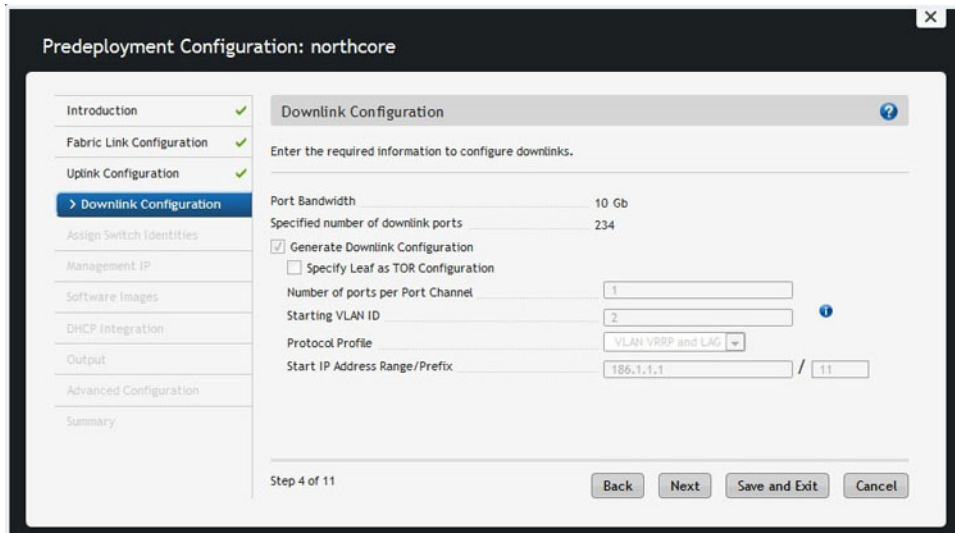
You can edit a configured static route by selecting it and clicking **Edit**; you can delete a configured static route by selecting it and clicking **Delete**.
7. If you select a routing protocol, do the following:
    - Enter settings for **Area ID** or **Local AS Number** and **Loopback IP Address Range/Prefix**.
    - If you select **OSPF**, enter the local IP address, remote neighbor IP address, and area ID for each specified uplink. The area ID area range is 0–65535.
    - If you select **iBGP**, enter the local IP address, remote neighbor IP address, local AS number for each specified uplink. The AS number range is 1–4294967295.
    - If you select **eBGP**, enter the local IP, remote neighbor IP address, local AS number, and remote AS number for each specified uplink. The AS number range is 1–4294967295.
    - If your topology has an N series switch in the top-tier, then for each switch, enter the **Local IP/Prefix**; **Remote IP/Prefix**; **Area ID**; and **Vlan ID** settings.

 **NOTE:** AFM automatically populates the range of IP addresses in the /30 subnet.

8. Click **Next** to go the **Downlink Configuration** screen.

### L3 DC Pre-Deployment — Downlink Configuration

Downlinks are EdgePort links that connect to servers, switches, or ToRs. If you enable the ToR configuration, the leaf switch functions as a ToR. If you disable the ToR configuration, the leaf functions as a switch. The read-only port bandwidth for the downlinks is 1 GB, 10 GB, or 40 GB. For more information about downlinks, refer to [Distributed Core Terminology](#).



**Figure 65. Downlink Configuration for Layer 3 Distributed Core Fabric**

1. From the menu, click **Network** > *Fabric Name* and then the **Configure and Deploy** tab.
2. From the **Deploy Fabric** drop-down menu, select **Pre-deployment Configuration**.
3. Navigate to the **Downlink Configuration** screen.
4. To specify a leaf as a ToR, select **Specify Leaf as ToR**.
5. Manually configure the downlinks or automatically generate the downlink configuration by checking the **Generate Downlink Configuration** option.
6. In the **Start IP Address Range/Prefix** field, enter the starting IP address and prefix. The range is 8–23.
7. In the **Number of ports per port channel** field, enter the number of ports assigned to a port channel for a particular VLAN ID. The range is 1–16.
8. In the **Starting VLAN ID** field, enter a starting VLAN ID. The range is 2–4094.
9. If the leaves are acting as a leaf switch and the switches are directly connected to the server, select the **Downlink VLAN and VRRP and LAG** protocol setting from the **Protocol Profile** drop-down menu. The default setting is **Downlink VLAN**.
10. Click **Next** to go the **Assign Switch Identities** screen.

### Protocol Configuration — Layer 3 with Resiliency (Routed VLT)

To configure the pre-deployment protocol configuration for a Layer 3 with Resiliency (Routed VLT), complete the following tasks:

1. Review the pre-deployment workflow at [Using the Pre-Deployment Configuration Wizard](#).
2. [Pre-Deployment — Step 1a: Fabric Link Configuration](#)
3. [Pre-Deployment — Step 1b: Uplink Configuration](#)


4. [Pre-Deployment – Step 1c: VLAN Configuration](#)
5. [Pre-Deployment – Step 1d: Port Channel Configuration](#)
6. [Pre-Deployment – Step 1e: VLAN Mapping](#)

### L3 DC/Routed VLT Pre-Deployment – Fabric Link Configuration

Before you begin, review [Using the Pre-deployment Configuration Wizard](#) and [Pre-deployment Wizard: Introduction](#). To configure links connecting the leaves and spines for a Layer 3 distributed core fabric or links connecting the core, access, and aggregation switches for a Layer 3 with Resiliency (Routed VLT) fabric using the OSPF routing protocol, use the **Fabric link Configuration** screen. The selected fabric type and fabric oversubscription ratio determines the value that AFM automatically assigns to the **Port Bandwidth** read-only field. To automate the pre-deployment process, AFM automatically:

- populates the starting IP address range and prefix
- populate the loop IP address and prefix based on the fabric design
- sets the area ID for OSPF to 0


Review these settings before deployment. You can modify the IP address range and loopback address. The range for the starting prefix for both types of addresses is 8–29 and the range for the loopback prefix is 8–26.

 **NOTE:** The area ID for the interconnect link must not be the same as the area ID for the uplink.

1. From the menu, click **Network** > *Fabric Name* and then the **Configure and Deploy** tab.
2. From the **Deploy Fabric** drop-down menu, select **Pre-Deployment Configuration**.  
The **Introduction** screen appears.
3. Review the **Introduction** screen and gather the useful information for deployment.
4. Click **Next**.  
The **Fabric Link Configuration** screen appears.
5. In the **Start IP Address Range/Prefix** area, enter the starting IP address and prefix.  
The prefix range is 8–29.
6. In the **Loopback IP Address Range/Prefix** area, enter the loopback address range and prefix.  
The prefix range is 8–26.
7. In the **Area ID** field, use the default setting (zero) or enter the area ID.  
The area ID range is 0–65535. The uplinks or interlinks must be in area 0 for OSPF.

### L3 DC/Routed VLT Pre-Deployment – Uplink Configuration

The **Uplink Configuration** screen for a Layer 3 and Layer 3 with Resiliency (Routed VLT) fabric displays the port bandwidth and the number of specified ports as read-only fields on the **Bandwidth and Port Count** screen. To configure the uplink protocol for the EdgePort uplinks to the WAN, use the **Uplink Configuration** screen. For more information about uplinks for a Layer 3 distributed core fabric, refer to [Distributed Core Terminology](#).

 **NOTE:** When OSPF is selected for both uplinks and interlinks, one of uplinks or interlinks must be in area 0.

1. From the menu, click **Network** > *Fabric Name* and then the **Configure and Deploy** tab.
2. From the **Deploy Fabric** drop-down menu, select **Pre-deployment Configuration**.
3. Navigate to the **Uplink Configuration** screen.
4. In the **Type of Uplink Ports** area, select one of the following options:

- **L2** – Configures Layer 2 uplinks for a Layer 2 fabric. This option is disabled by default on a Layer 3 Distributed Core fabric.
  - **L3** – Configures uplinks for a Layer 2 VLT or Layer 3 Distributed Core fabric. If you select the L3 option, the **Uplink Configuration** screen displays additional options to configure the Layer 3 protocol settings.
5. In the **Protocol Settings** area, select **Static Routes** or routing protocol (**OSPF**, **IBGP**, or **eBGP**) for the EdgePort uplinks.
  6. If you select **Static Routes**, AFM displays the **Static Route Configuration** section. Do the following steps:

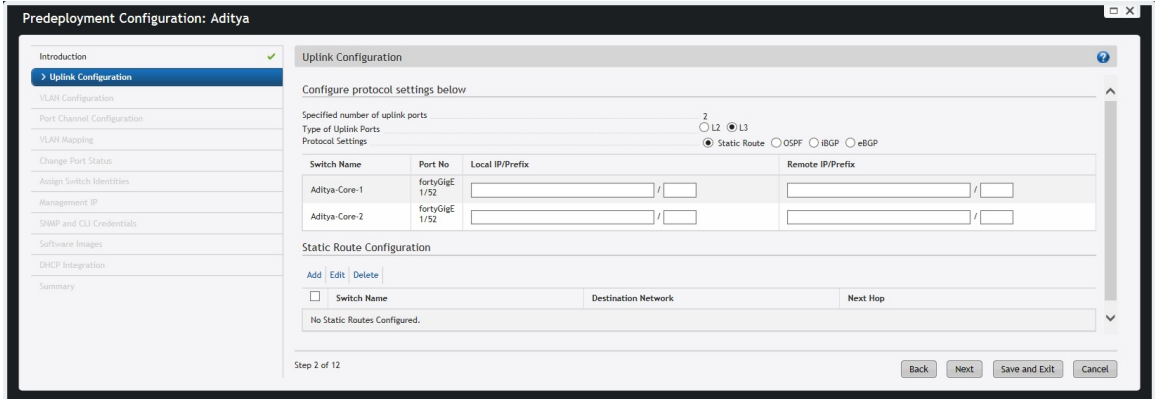


Figure 66. Static Route Configuration Screen

- a. Click **Add** to configure a static route. The **Add Static Route** dialog box appears.

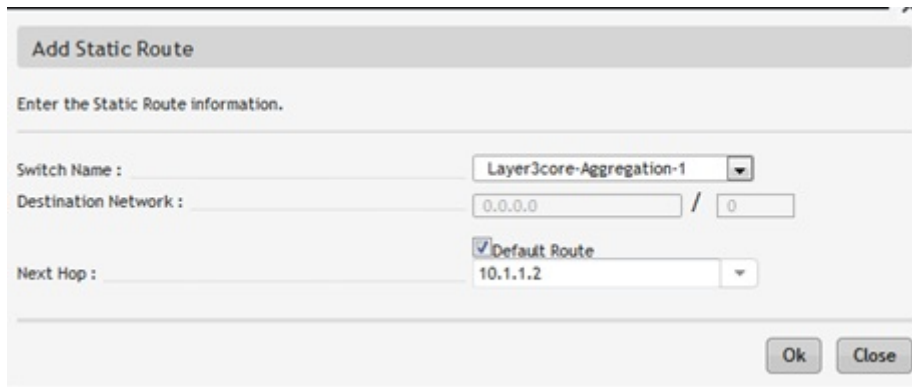



Figure 67. Add Static Route Dialog Box

- b. For static routes, enter the destination network and the next hop. If you select **Default Route**, AFM automatically populates the destination network field as 0.0.0.0/0.
  - c. Click **OK**.
  - d. Repeat steps a-c to add an additional static route. You can configure up to 10 static routes for each aggregation switch. You can edit a configured static route by selecting it and clicking **Edit**; you can delete a configured static route by selecting it and clicking **Delete**.
7. If you select a routing protocol, do the following:
    - Enter settings for **Area ID** or **Local AS Number** and **Loopback IP Address Range/Prefix**.



- If you select **OSPF**, enter the local IP address, remote neighbor IP address, and area ID for each specified uplink. The area ID area range is 0–65535.
- If you select **iBGP**, enter the local IP address, remote neighbor IP address, local AS number for each specified uplink. The AS number range is 1–4294967295.
- If you select **eBGP**, enter the local IP, remote neighbor IP address, local AS number, and remote AS number for each specified uplink. The AS number range is 1–4294967295.
- If your topology has an N series switch in the top-tier, then for each switch, enter the **Local IP/Prefix; Remote IP/Prefix; Area ID; and Vlan ID** settings.

 **NOTE:** AFM automatically populates the range of IP addresses in the /30 subnet.

8. Click **Next** to go the **Downlink Configuration** screen.


### L3 Routed VLT Pre-Deployment – VLT VLAN Configuration

To configure the VLT VLAN configuration for a Layer 3 with Resiliency (Routed VLT) fabric, use the **VLT VLAN Configuration for Layer 3 with Resiliency (Routed VLT)** screen.

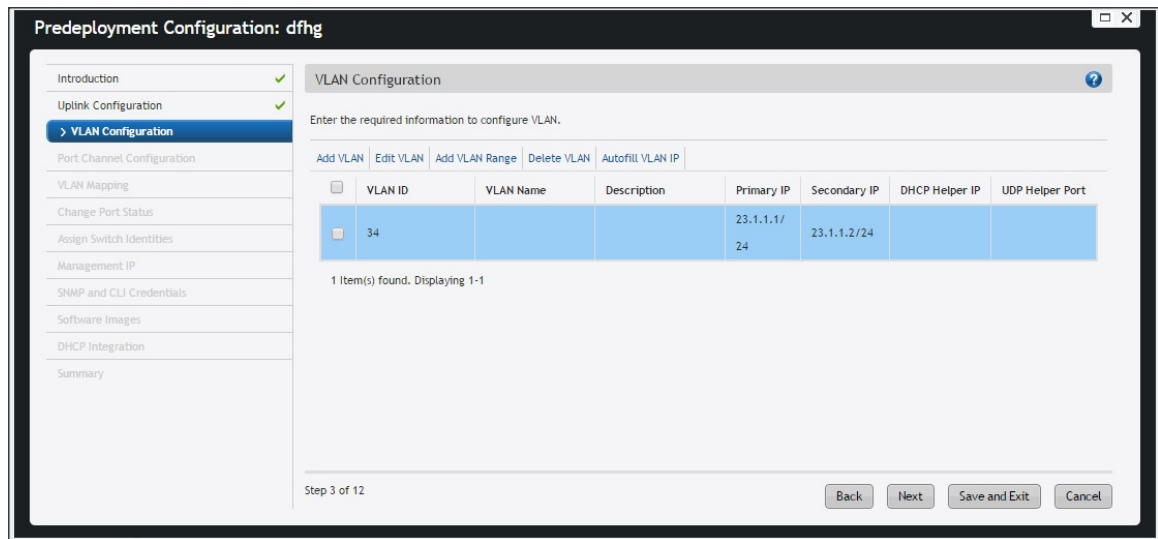
1. From the menu, click **Network > Fabric Name** and then click the **Configure and Deploy** tab.
2. From the **Deploy Fabric** drop-down menu, select **Pre-deployment Configuration**.
3. Navigate to the **VLT VLAN Configuration** screen.
4. Check the **Enable Layer 3 Protocol in Access Switches** option.
5. Click the **Add VLAN** link.  
The **Add VLAN Window** appears.
6. To assign the IP addresses to the switches for the Layer 3 with Resiliency (Routed VLT) fabric, click **Add VLAN Range** and specify the VLAN range.
7. Click **Next** to view the **Port Channel Configuration** screen.

**Table 44. VLT VLAN Configuration Options for Layer 3 with Resiliency (Routed VLT) Fabric**

| VLAN Option    | Description   |
|----------------|---|
| Add VLAN       | <p>Create a VLAN row. You can also configure the IP helper feature for data center routers to forward configured UDP broadcast packets to a specific IP address. This feature also configures which UDP ports are forwarded.</p> <p>Enter the following information:</p> <ul style="list-style-type: none"> <li>• <b>VLAN ID</b></li> <li>• <b>VLAN Name</b></li> <li>• <b>VLAN Description</b></li> <li>• <b>Primary IP</b></li> <li>• <b>Secondary IP</b></li> <li>• <b>DHCP Helper IP</b> – The IPv4 unicast or broadcast address to which relayed UDP broadcast packets are sent. Click + to specify additional addresses or click – to remove an address.</li> <li>• <b>UDP Helper Port</b> – The destination UDP port number from 0 to 65535. Click + to specify additional addresses or click – to remove an address.</li> </ul> |
| Add VLAN Range | <p>Automate VLAN creation and automatically populate IP addresses. You can also configure the IP helper feature for data center routers to forward configured UDP broadcast packets to a specific IP address. This feature also configures which UDP ports are forwarded.</p>   |

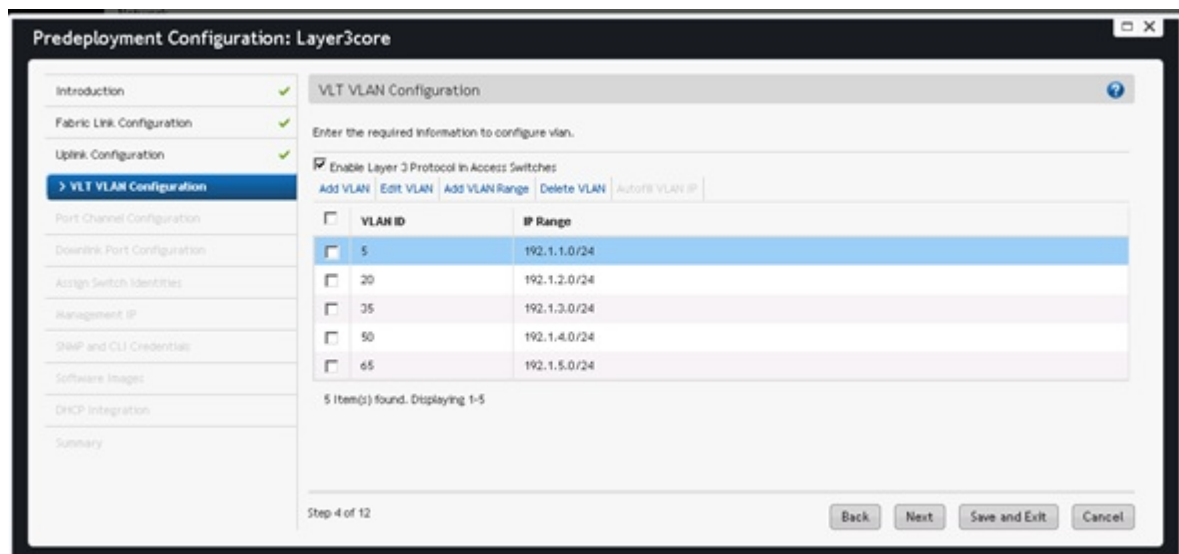
| VLAN Option  | Description   |
|--|---|
|  | <p>Enter the following VLAN information:</p> <ul style="list-style-type: none"> <li>• <b>Starting VLAN ID</b> – Enter the starting VLAN ID. The range is 2–511.</li> <li>• <b>Number of VLANs</b> – Enter the number of VLANs.</li> <li>• <b>VLAN Increment</b> – Enter the increment of the VLANs. If you do not specify an increment, the default value is 1.</li> <li>• <b>Start Subnet IP Address/Prefix</b> – Enter an IP range to automatically populate the VLAN IP addresses. The IP addresses include primary, secondary peer VLAN, and VRRP IP.</li> </ul> <p> <b>NOTE:</b> To view this option, check the <b>VLAN and VRRP Configuration</b> check box.</p> <ul style="list-style-type: none"> <li>• <b>DHCP Helper IP</b> – The IPv4 unicast or broadcast address to which relayed UDP broadcast packets are sent. Click + to specify additional addresses or click – to remove an address.</li> <li>• <b>UDP Helper Port</b> – The destination UDP port number from 0 to 65535. Click + to specify additional addresses or click – to remove an address.</li> </ul> |
| VLAN and VRRP Configuration (for a Layer 3 fabric for Resiliency (Routed VLT))                                   | <p>Configure an IP address with VRRP. If the <b>VLAN and VRRP Configuration</b> option is selected, the following fields appear:</p> <ul style="list-style-type: none"> <li>• Primary IP</li> <li>• Secondary IP</li> <li>• Virtual IP</li> </ul>   |
| Autofill VLAN IP (For Enable Layer 3 Protocol in Access Switches option only)                                    | <p>Enter the starting subnet IP address/prefix for the range of selected VLANs. The IP addresses are automatically populated.</p>   |
| Autofill VLAN IP (For enable Layer 3 protocol in Aggregation switches option only in a three-tier Core topology) | <p>Enter the starting subnet IP address/prefix for the range of selected VLANs. The IP addresses are automatically populated.</p>   |
| Delete VLAN  | <p>Remove the selected VLAN row.</p>  |
| Edit VLAN  | <p>Edit the VLAN ID, primary IP address, and secondary IP address. For campus devices, you can configure the IP helper feature by specifying the IPv4 unicast or broadcast address to which relayed UDP broadcast packets are sent in the <b>DHCP Helper IP</b> field. Click + to specify additional addresses or click – to remove an address.</p>   |
| VLAN ID  | <p>Enter the VLAN ID. The range is 2–511. There is no default VLAN ID.</p>  |
| Primary IP   | <p>Enter the primary IP address. AFM automatically enters the prefix. The prefix range is 8–29 and the default prefix is 24. There is no default primary IP address.</p>  |
| Secondary IP   | <p>Enter the secondary IP address. AFM automatically enters the prefix. The prefix range is 8–29 and the default prefix is 24. There is no default secondary IP address.</p>  |

The following screen shot displays the VLAN Configuration screen without selecting the **Enable Layer 3 protocol in Access Switches** option. By default, the VLAN screen requires the primary and secondary IP address for the core devices.



**Figure 68. VLAN Configuration Without Using the Enable Layer 3 Protocol in Access Switches Option**

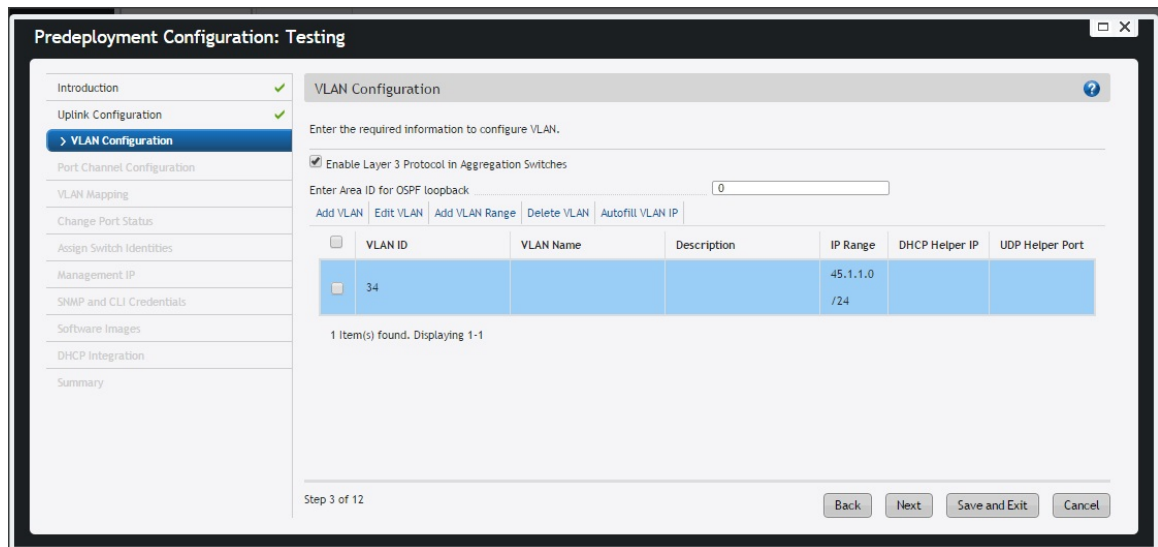
The following figure displays a VLT VLAN Configuration screen using the **Enable Layer 3 protocol in Access Switches** option. To support both access and aggregation devices in a Layer 3 with Resiliency (Routed VLT) topology, select the **Enable Layer 3 protocol in Access Switches** option. If you use this option, provide the network IP address range using the **Add VLAN Range** link. AFM assigns IP addresses to all the access and aggregation switches.



**Figure 69. Adding VLANs and Enabling the Layer Protocol in Access Switches Option**

To support both Core and Aggregation devices in a Layer 3 topology, select **Enable Layer 3 Protocol in Aggregation Switches**. if you use this option, provide the network IP address range using the **Add VLAN**

**Range** command. AFM assigns IP addresses to all the Core and Aggregation switches. The following figure displays the results after selecting the **Enable Layer 3 Protocol in Aggregation Switches** option and adding VLANs for a Layer 3 fabric.



**Figure 70. Layer 3 Support for Aggregation Layer**

### **Advanced VLAN IP Configuration**

After completing pre-deployment, modify the VLT VLAN configuration for Layer 3 with Resiliency (Routed VLT) topology using the **Advanced VLAN IP Configuration** option at the **Network > Fabric > Switch > Configure and Deploy** tab.

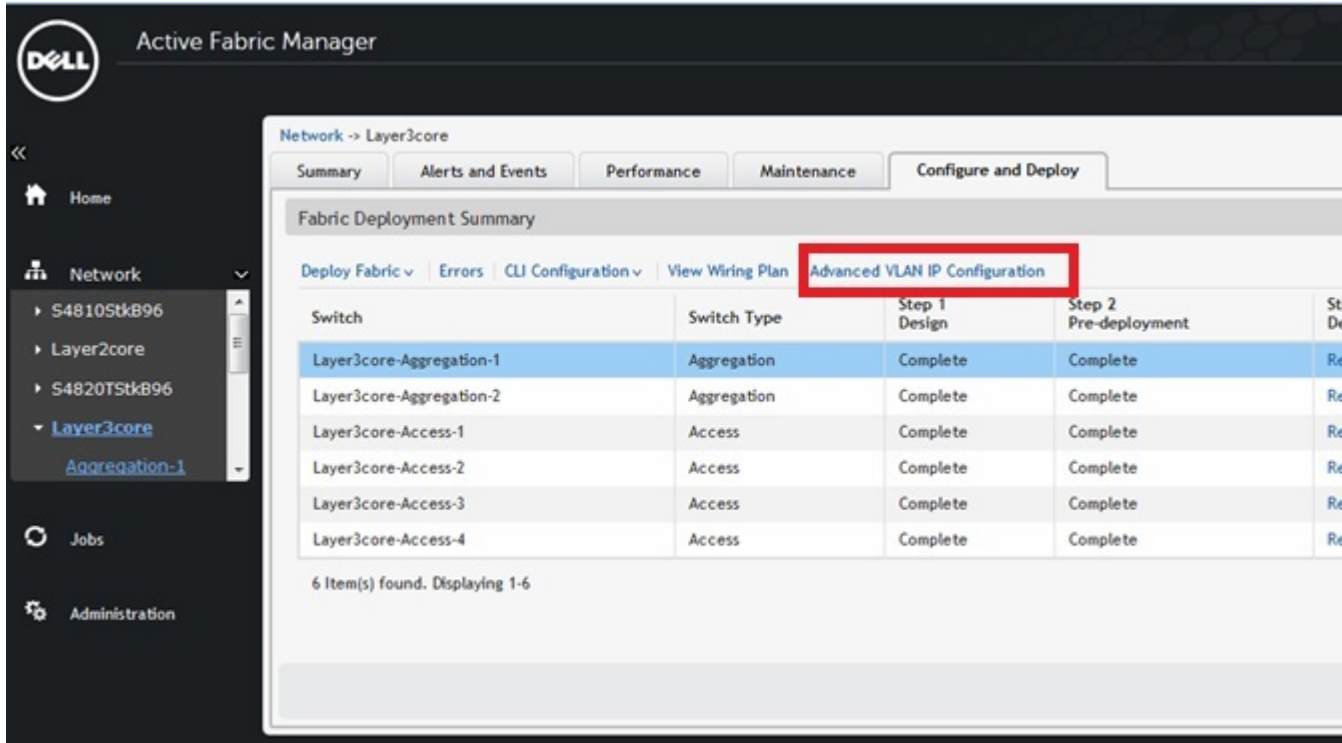


Figure 71. Advanced VLAN IP Configuration Option

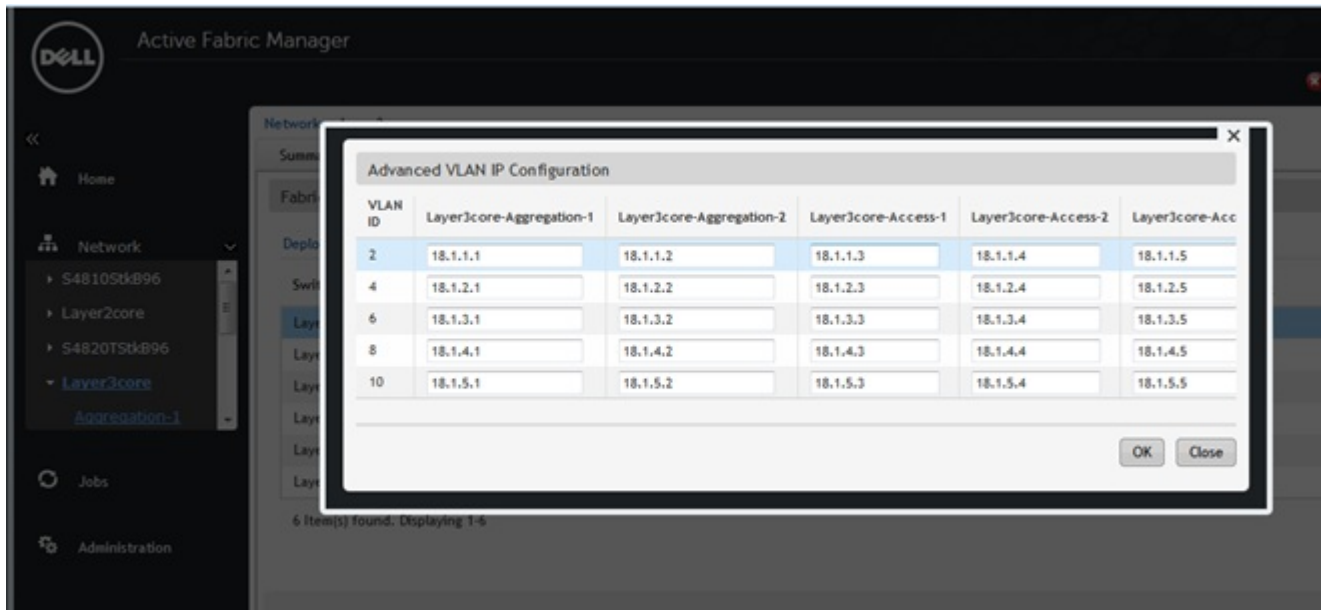


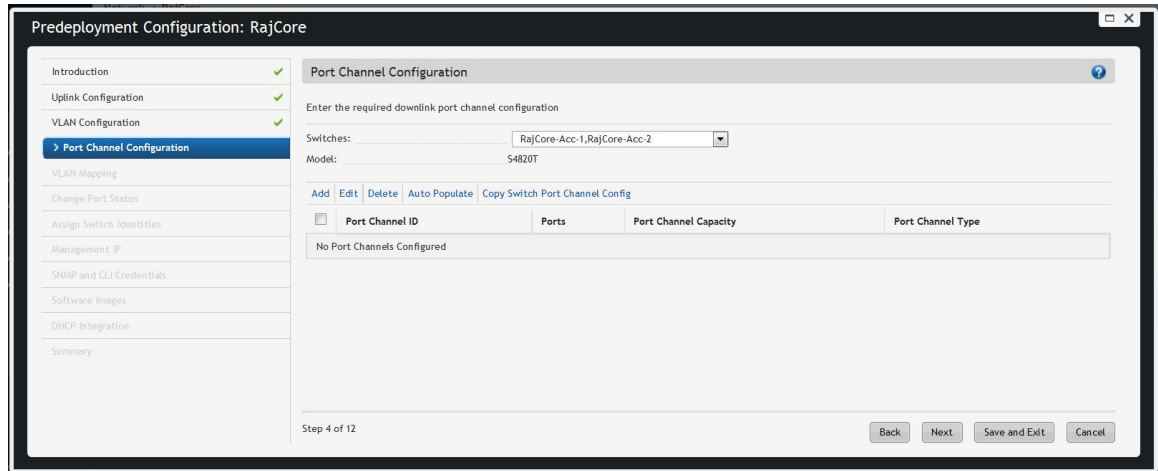
Figure 72. Advanced VLAN IP Configuration Window

### L3 Routed VLT Pre-deployment — Port Channel Configuration

To add, edit, delete, and automatically populate the port channel configuration for Layer 3 with Resiliency (Routed VLT) fabric, use the **Port Channel Configuration** screen. After you add a port channel configuration, you can copy it to use on another switch in the fabric.

**Table 45. Port Channel Configuration Options**

| Field Name                             | Description   |
|--|---|
| Add                                    | Enter the port channel information and enable LACP.   |
| Auto Populate                          | Enter port channel information to automatically assign port channels to switches in the fabric and enable LACP. <ul style="list-style-type: none"> <li>Number of Ports per Port Channel</li> <li>Start Port Channel ID</li> <li>Number of Port Channel</li> <li>Port Channel Increment</li> <li>Enable LACP (optional)</li> </ul> |
| Copy Switch Port Channel Configuration | Copy the switch port channel configuration from another switch. Create a port channel configuration and then copy the configuration to another switch.  |
| Delete                                 | Delete a selected port channel configuration.   |
| Edit                                   | Enter the port channel configuration.   |



**Figure 73. Pre-deployment — Port Channel Configuration**



1. From the menu, click **Network** > *Fabric Name* and then click the **Configure and Deploy** tab.
2. From the **Deploy Fabric** drop-down menu, select **Pre-deployment Configuration**.
3. Navigate to the **Port Channel Configuration** screen.
4. From the **Switches** drop-down menu, select a switch for the port channel configuration. The selected switch for the port channel configuration displays in the read-only **Model** field.
5. Click **Add** to manually add a port channel or click **Auto Populate** to automatically populate the port channels. For more port channel configuration options, refer to the Port Channel Options table.
6. Click **Next** to go to the **Downlink Port Configuration** screen.

## L2 VLT/L3 Routed VLT Pre-Deployment – VLAN Mapping


To add VLANs and associate ports on the different access switches to which VLAN for a Layer 3 with Resiliency (Routed VLT) fabric, use the **VLAN Mapping** screen. After adding the VLANs and associating them with ports, you can copy switch VLAN or port VLAN configurations. Associate one or more tagged VLANs with a port. For untagged VLANs, only one association is supported.

To map the physical port to the VLAN ID (for example, map one port to multiple VLANs), select **Port-VLAN Association**.

**Table 46. Port-VLAN Mapping Field Descriptions**

| Field Name     | Description  |
|----------------|--|
| Port Name      | View the port name (read-only).  |
| Hybrid         | Displays whether hybrid port mode is enabled or not. Hybrid port mode enables interfaces to accept untagged packets (added to the default VLAN) and tagged ones.   |
| Tagged VLANs   | <p>Enter one or more VLANs to associate with the port. The VLANs must be in the Configured VLANs list and the Untagged VLAN field must be empty. There is no default value.</p> <ol style="list-style-type: none"> <li>1. Click on the icon next to the field entry and select a VLAN from the list.</li> <li>2. Select one or more VLANs to associate with the port.</li> </ol> <p> <b>NOTE:</b> VLANs previously associated with storage-facing ports are included in the selection list.</p> |
| Untagged VLANs | <p>Select a VLAN to associate with the port. The Tagged VLAN field must be empty. There is no default value.</p> <p> <b>NOTE:</b> VLANs previously associated with storage-facing ports are included in the selection list.</p>   |

**Table 47. Port-VLAN Mapping Options**



| Option   | Description   |
|--|---|
| Enable Hybrid Port<br><br>Disable Hybrid Port Mode | <p>Enable or disable hybrid port mode for selected ports on downlink switches. For data center switches, the same VLAN cannot be tagged and untagged for a hybrid port.</p> <p> <b>NOTE:</b> These options are not available for N-series devices as N-series device ports are hybrid by default. For one-tier advanced fabric designs, these options are available only for uplinks. For data center switches, the same VLAN cannot be tagged and untagged for a hybrid port.</p> |
| Copy Switch VLAN Config                            | Copy the VLAN association from the current switch to other switches in the fabric.  |
| Copy Port VLAN Config                              | Copy the VLAN association from a selected port to other ports in a switch.  |

To map the VLAN ID to physical port interfaces (for example, map one VLAN to multiple ports), select **VLAN-Port Association**.

**Table 48. VLAN-Port Mapping Field Descriptions**

| Field Name                 | Description  |
|----------------------------|--|
| VLAN                       | View the port name (read-only).  |
| Tagged Port/Port Channel   | Enter one or more tagged ports to associate with the VLAN.<br><ol style="list-style-type: none"> <li>1. Click on the icon next to the field entry.</li> <li>2. Select one or more ports to associate with the VLAN.</li> </ol>   |
| Untagged Port/Port Channel | Enter one or more untagged ports to associate with the VLAN.<br><ol style="list-style-type: none"> <li>1. Click on the icon next to the field entry.</li> <li>2. Select one or more ports to associate with the VLAN.</li> </ol> |

**Table 49. Layer 2 VLAN Mapping Options**

| Option                       | Description  |
|------------------------------|--|
| Copy VLAN Tagged Port Config | Copy the VLAN tagged port configuration from a selected port to other ports in a switch.   |
| Copy Switch VLAN Config      | Copy the VLAN association from the current switch to other switches in the fabric.   |
| Auto-fill Tagged Port        | For selected VLANs, apply sequential tagging to the available ports and the number of ports specified on a VLAN.   |
| Auto-fill Untagged Port      | For selected VLANs, apply untagged ports. Based on available ports, associate only one port per VLAN.<br> <b>NOTE: The number of Port/VLAN Ports</b> option is disabled on the <b>AutofillTagged/Untagged Port</b> screen.                              |
| Select Hybrid Ports          | Select ports/port channels to be hybrid.<br> <b>NOTE:</b><br>This option is not available for N-series devices as N-series device ports are hybrid by default. For data center switches, the same VLAN cannot be tagged and untagged for a hybrid port. |

1. From the menu, click **Network** > *Fabric Name* and then the **Configure and Deploy** tab.
2. From the **Deploy Fabric** drop-down menu, select **Pre-deployment Configuration**.
3. Navigate to the **VLAN Mapping** screen.



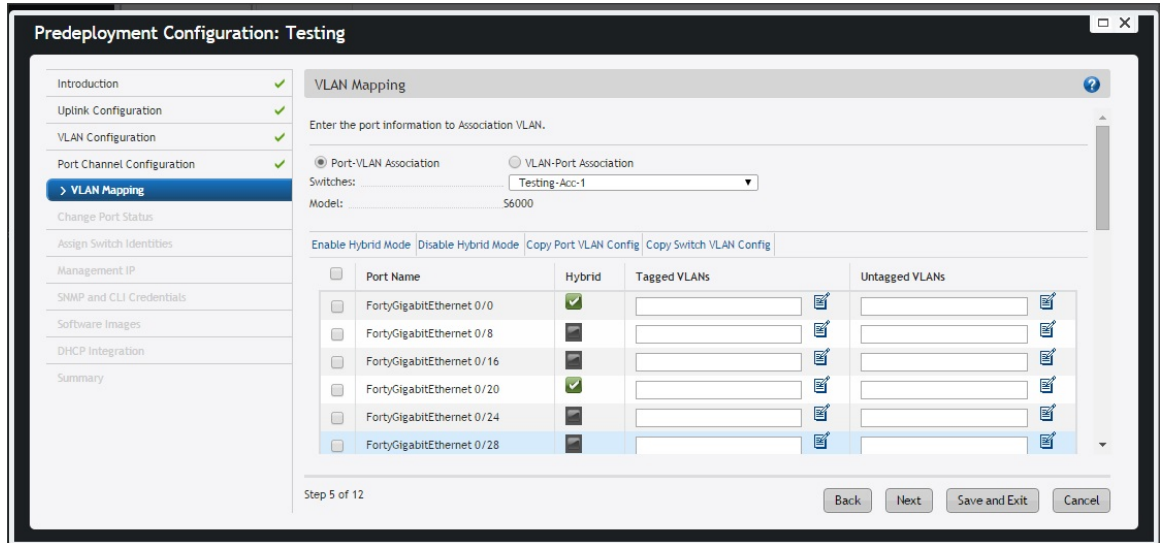



Figure 74. Pre-deployment Configuration — VLAN Mapping

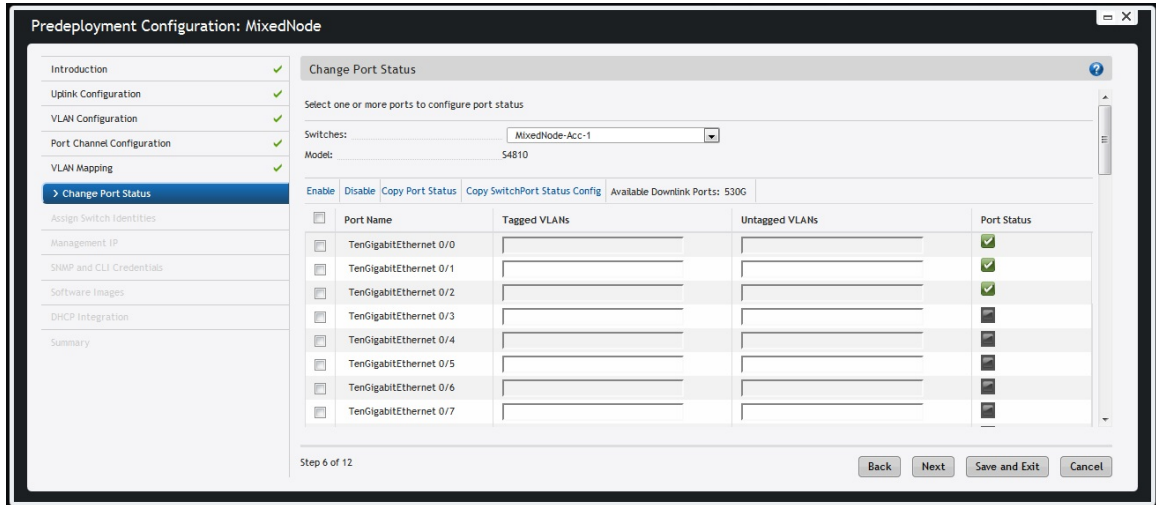
4. From the **Switches** drop-down menu, select an access or aggregation switch. The selected switch for the VLAN mapping displays in the read-only **Model** field.
5. In the **Tagged VLANs** field, click the icon to the right and enter one or more VLANs to associate with the port.
6. To enable hybrid port mode, select one or more ports and click **Enable Hybrid Mode**. To disable hybrid port mode, select the ports and click **Disable Hybrid Mode**.
  -  **NOTE:** You cannot enable Hybrid Mode for uplink ports.
7. Click **Next** to go to the **Change Port Status** screen.

## Pre-Deployment — Change Port Status

 **NOTE:** The **Change Port Status** pre-deployment screen applies to advanced fabric only.

To enable or disable a downlink, use the **Change Port Status** screen. If you use an **Advanced** configuration, AFM does not automatically assign any available ports as downlinks. Manually assign the downlink ports by selecting them and clicking **Enable**. To disable a downlink port, select and click **Disable**. VLAN ports and port channels automatically display as enabled downlinks. The remaining amount of bandwidth (in Gb) displays in the **Available Downlink Ports** field. Enabled ports display a green checkmark in the **Port Status** column. Disabled ports display a black box in the **Port Status** column.

1. From the menu, click **Network** > *Fabric Name* and then the **Configure and Deploy** tab.
2. From the **Deploy Fabric** drop-down menu, select **Pre-deployment Configuration**.
3. Navigate to the **Change Port Status** screen.




**Figure 75. Change Port Status Screen**

4. From the **Switches** drop-down menu, select an access switch to enable the downlinks on that switch.

The selected access switch for the port status appears in the read-only **Model** field. By default, AFM enables the configured port channels and VLANs on the access switch as downlink ports and displays the status details for these ports.


5. Select one or more ports and click **Enable**.

- To disable one or more ports, select the port or ports and click **Disable**.

 **NOTE:** You cannot disable port channels or VLANs.

- To copy a port status to another port on the switch, select the port or ports and click **Copy Port Status**. Select a port from the **Available Ports** list and click **Ok**.

- To copy a port status configuration to a switch, select the port or ports and click **Copy Switch Port Status Configuration**. Select a switch from the **Available Switches** list and click **Ok**.

 **NOTE:** You can only copy port status configurations to switches that are the same model and access switch type.

6. (N2024P, N2048P, N3024P, and N3048P switch models only). For switches that support Power over Ethernet (PoE), PoE ports are automatically enabled.

- To disable one or more PoE ports, select the port or ports and click **Disable PoE**.
- To enable one or more PoE ports, select the port or ports and click **Enable PoE**.

The following table lists all possible PoE-port configurations and behavior.

**Table 50. PoE Port Configurations**


| Port Status | PoE Status | Result            |
|-------------|------------|-------------------|
| Enabled     | Enabled    | PoE downlink port |
| Enabled     | Disabled   | Downlink port     |
| Disable     | Enable     | PoE downlink port |
| Disable     | Disable    | Default/free port |

 **NOTE:** When configured ports are part of a VLAN, the fabric design only configures VLAN access.

7. Click **Next** to go to the **Assign Switch Identities** screen.

## Pre-Deployment — Assign Switch Identities


To assign the system MAC addresses to the switches in the fabric, use the **Assign Switch Identities** screen.

 **NOTE:** If you use the **Device MAC Association** feature, the MAC addresses, IP addresses, and Service Tags of the switches are automatically entered and no additional configuration is required but you can change any of the pre-populated information. If you change the IP address, manually reload the switch in BMP mode. For more information, refer to [Device MAC Association](#). If you perform this step manually and do not associate the switches with the correct system MAC address, the wiring plan is inaccurate.

The following is a sample **.csv** file.

**Table 51. Sample CSV Format**

| serial_number | purchase_order | mfg_part_number   | mac_address       | server_tag |
|---------------|----------------|-------------------|-------------------|------------|
| HADL134J20193 | 163            | 759-0096-02 REV.F | 00:01:E8:8B:15:77 | 9RGZTS2    |

 **NOTE:** Before you begin, obtain the **.csv** file with the system MAC addresses, Service Tag, and serial numbers for each Dell switch or enter this information manually.

1. Locate the **.csv** file that contains the system MAC addresses, serial numbers, and Service Tags for the switches in the fabric. Contact your Dell Networking sales representative for this file.
2. From the menu, click **Network** > *Fabric Name* and then click the **Configure and Deploy** tab.
3. From the **Deploy Fabric** drop-down menu, select **Pre-deployment Configuration**.
4. Navigate to the **Assign Switch Identities** screen.
5. Click **Browse** and specify the path of the **.csv** file. If you do not have this file, enter this information in the **System MAC Address** fields manually.
6. Click **Upload**.
7. Click the **Choose MAC** icon in each row and associate the switch name with the MAC address, (optional) serial number, and (optional) Service Tags using the **.csv** file or enter this information manually.

 **NOTE:**

- If you are using a **.csv** file, the **Select MAC Address Selection** screen appears.
  - If you type part of a MAC address, AFM displays any matching configured MAC addresses. If you select a MAC address, AFM automatically enters any associated IP addresses or Service Tags.
8. Associate the system MAC address, serial number, and Service Tag with each switch.
  9. Click **Next** to go to the **Management IP** screen.

## Pre-Deployment — Management IP

To assign a management IP address to each switch in the fabric, use the **Management IP** screen.

**NOTE:** Before you begin, gather the management IP addresses for all the switches in the Layer 2 or Layer 3 fabric for the management port. All management switch IP addresses must be on the same subnet.

1. From the menu, click **Network** > *Fabric Name* and then click the **Configure and Deploy** tab.
2. From the **Deploy Fabric** drop-down menu, select **Pre-deployment Configuration**.
3. Navigate to the **Management IP** screen.
4. In the **Default Gateway** field, enter the address of the default gateway for the management interface.
5. In the **Management Route** field, enter the route and prefix of the management interface.
6. In the **Start Management IP Address/Prefix** fields, enter the starting management IP address and prefix.
7. To assign a management IP address, select the switches.
8. Click **Auto-fill Selected Rows**.  
The system automatically assigns a management IP address to all the selected switches in the fabric.
9. Click **Next**.

## Pre-Deployment — License Update

On the **License Update** screen of the **Pre-Deployment Configuration** wizard, you can upload the license for Z9500–series switches.

1. From the menu, click **Network** > *Fabric Name* and then click the **Configure and Deploy** tab.
2. From the **Deploy Fabric** drop-down menu, select **Pre-deployment Configuration**.
3. Navigate to the **License Update** screen.

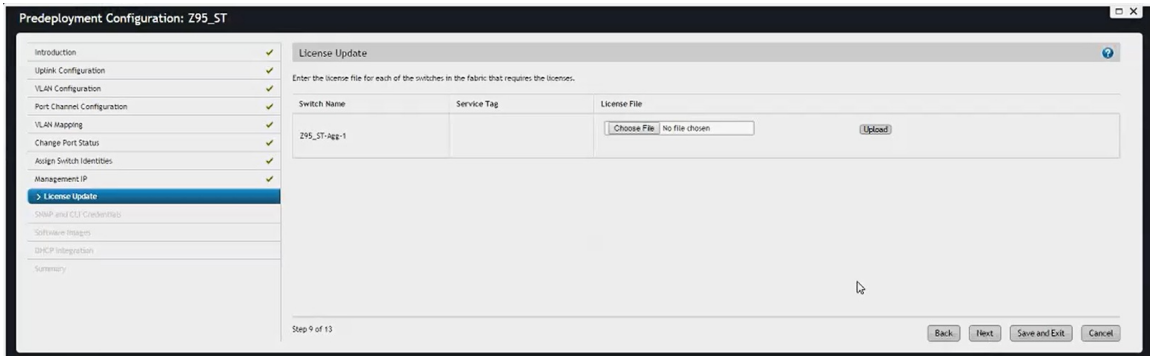



Figure 76. License Update Screen

4. Upload the license file for each Z9500–series switch in your fabric. For each switch:
  - a. Click **Choose File** and navigate to the license file on your local disk.
  - b. Click **Upload**.
5. Click **Next** to continue to the **SNMP and CLI Credentials** screen.

## Pre-Deployment — SNMP and CLI Credentials

To configure SNMP and CLI credentials at the fabric level. Configure SNMP so that the AFM can perform SNMP queries on the switches in the fabric, use the **SNMP and CLI Credentials** screen. The values you enter in the SNMP configuration are also used for configuring the switches during the build phase and for monitoring during the run phase. The write community string is populated from the AFM global setting, which is configured during installation. To provision the fabric, enter the Dell Networking operating


system CLI user's credentials and enable the configuration credentials for all the switches in the fabric. This option allows you to remotely make configuration changes to the switches in the fabric.


1. From the menu, click **Network** > *Fabric Name* and then click the **Configure and Deploy** tab.
2. From the **Deploy Fabric** drop-down menu, select **Pre-deployment Configuration**.
3. Navigate to the **SNMP and CLI Credentials** screen.
4. Navigate to the **SNMP Configuration** area.
5. In the **Read Community String** field, enter the read community string (for example, `public`).
6. In the **Write Community String** field, enter the write community string (for example, `private`).
7. Navigate to the **CLI Credentials** area.
8. In the **Protocol** drop-down menu, select one of the following options:
  - **Telnet**
  - **SSHv2**
9. In the **User Name** field, enter the user name.
10. In the **Password** field, enter the password.
  -  **NOTE:** You can click **Show Password as Text** to display the characters of your password entries rather than security symbols.
11. In the **Confirm Password** field, confirm the password. The privilege level is a read-only field and the default is 15.
12. In the **Enable Password** field, enter a password for the privilege level.
13. In the **Confirm Enable Password** field, confirm the enabled password for the privilege level.
14. Click **Next**.

## Pre-Deployment — Software Images

To specify which software images to stage for each type of switch in the fabric from a TFTP or FTP site, use the **Software Images** screen. The software image must be the same for each type of platform. Place the software images for the switches on the TFTP or FTP site so that the switches can install the appropriate FTOS software image and configuration file from this site.

To change the address of the TFTP or FTP site, navigate to the **Administration** > **Settings** tab > **TFTP/FTP Settings**

 **NOTE:** Before you begin, make sure that you have loaded on to the TFTP or FTP site the software image for each type of switch.

 **NOTE:** To download the latest FTOS switch software version, see the "Upload Switch Software" section in the *AFM Installation Guide*.

**To specify which software images to load onto each switch in the fabric from the TFTP or FTP site:**

1. From the menu, click **Network** > *Fabric Name* and then click the **Configure and Deploy** tab.
2. From the **Deploy Fabric** drop-down menu, select **Pre-deployment Configuration**.
3. Navigate to the **Software Images** screen.
4. Select the **TFTP** or **FTP** site option that contains the software image.
5. Select the path of the software images to the TFTP or FTP site.
6. Click **Next** to go to the **DHCP Integration** screen.

## Pre-Deployment — DHCP Integration

The **DHCP Integration** screen uses the information configured at the **Assign Switch Identities**, **Management IP**, and **Software Images** screens to create a DHCP configuration file named `dhcpd.cfg`, which contains the following information:

- System MAC addresses and fixed management IP addresses for each switch in the fabric
- Location of the software images and configurations for the switches on the TFTP or FTP server

To automatically integrate the file into the AFM local DHCP server, use the default setting **Local (AFM provisioned to be a DHCP server)**. AFM automatically generates a switch configuration file and transfers it to the local DHCP server.

To manually integrate the DHCP configuration into the external DHCP server, select **Remote (External DHCP server)**.


After you power cycle the switches, the switches use BMP. BMP provides the following features:

- Automatic network switch configuration
- Automated configuration updates
- Enforced standard configurations
- Reduced installation time
- Simplified operating system upgrades

Automated BMP reduces operational expenses, accelerates switch installation, simplifies upgrades, and increases network availability by automatically configuring Dell Networking switches. BMP eliminates the need for a network administrator to manually configure a switch, resulting in faster installation, elimination of configuration errors, and enforcing standard configurations.

With BMP, after you install a switch, the switch searches the network for a DHCP server. The DHCP server provides the switch with a management IP address and the location of a TFTP or FTP file server. The file server maintains a configuration file and an approved version of FTOS for the Dell Networking switches. The switch automatically configures itself by loading and installing an embedded Dell Networking OS image with the startup configuration file.

For more information about BMP, refer to the *Open Automation Guide*.

 **NOTE:** When you enter the system MAC address into the **Assign Switch Identities** screen, AFM generates a port MAC address from the pre-deployment configuration, not a chassis MAC address.


1. From the menu, click **Network** > *Fabric Name* and then click the **Configure and Deploy** tab.
2. From the **Deploy Fabric** drop-down menu, select **Pre-deployment Configuration**.
3. Navigate to the **DHCP Integration** screen.
4. Click **Save** and specify the location for the generated DHCP configuration file. You can also copy and paste the configuration into the DHCP server.
5. Install the DHCP file onto the DHCP server before deploying the fabric.
6. Click **Next** to go to the **Summary** screen.

## Pre-Deployment — Summary


To review the pre-deployment configuration, use the **Summary** screen, which displays the following information:

- Specified IP and protocol settings for the fabric, uplink, and downlink configuration
  - Software image information for each type of switch
  - Configuration file transfer status to the remote or local TFTP or FTP server
1. From the menu, click **Network** > *Fabric Name* and then click the **Configure and Deploy** tab.
  2. From the **Deploy Fabric** drop-down menu, select **Pre-deployment Configuration**.
  3. Navigate to the **Summary** screen.
  4. Carefully review the pre-deployment configuration.
  5. To commit your changes, click **Save and Exit**.

#### Next Steps:

1. Verify that the DHCP configuration file for the fabric is integrated into the DHCP server so that the switches are assigned a management IP address before you deploy the fabric.
2. Power on the switches in the fabric when you have completed the pre-deployment process. After you power cycle the switches, the switches use bare metal provisioning (BMP).
  -  **NOTE:** If you are using a switch that has already been deployed, reset the switch to factory defaults to use it in the fabric. The switch must be in BMP mode. For more information about BMP, see [DHCP Integration](#) and refer to the *Open Automation Guide*.
3. From the menu, click **Network** > *Fabric Name* and then click the **Configure and Deploy** tab.
4. To deploy and validate the fabric, from the **Deploy Fabric** drop-down menu, select **Deploy and Validate**.

## Viewing the DHCP Configuration File

 **NOTE:** If you are using Internet Explorer and the Windows 7 OS, change your indexing options by performing the following steps:

1. Navigate to the **Control Panel** > **Indexing Options** screen.
  2. Click **Advanced** and then click the **File Types** tab.
  3. In the **Add new extension to list** field, enter `conf` as the extension file type and then click **Add**.
  4. Click **OK**.
1. From the menu, click **Network** > *>Fabric Name >* and then click the **Configure and Deploy** tab.
  2. From the **Deploy Fabric** drop-down menu, select **View DHCP Configuration**.  
The **DHCP Integration** dialog box appears.
  3. Click **Save To** to save the DHCP configuration file to your local disk.

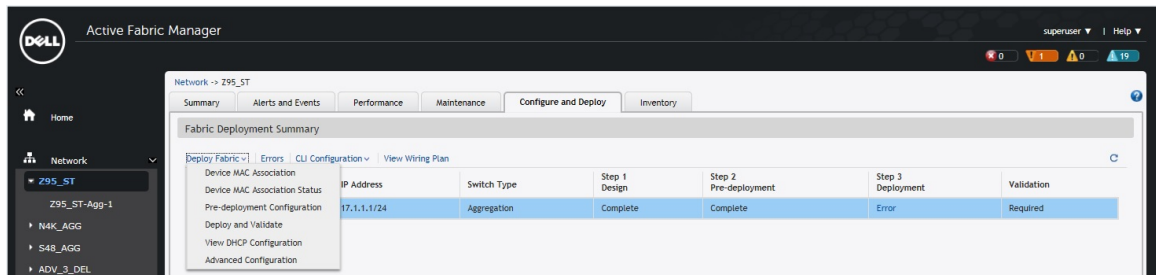
For more information about DHCP, refer to [DHCP Integration](#).

## Deploying and Validating the Fabric

This section discusses how to deploy and validate the fabric.

### Deploying the Fabric

To deploy the fabric, use the following procedure. AFM prompts you to fix any errors when you deploy the fabric.



**Figure 77. Configure and Deploy — Deploy and Validate**

**NOTE:** During initial deployment, the BMP process wait time to install the software onto the switches in the fabric depends on whether stacking is enabled. Approximate wait times are:

- 10 minutes for a non-stacked fabric
- 20 minutes for stacked fabric

To view a custom configuration file, navigate to the **Network > Fabric Name > Configure and Deploy** tab. From the **CLI Configuration** drop-down menu, select the **Custom Configuration** option.

To troubleshoot deployment issues, use the following table.

**Table 52. Deployment Status**

| Number | Status     | Status Details   | Recommended Action  |
|--------|------------|--|---|
| 1      | Required   | Deployment Required  | None  |
| 2      | Complete   | Deployment successfully completed                            | None  |
| 3      | Error      | Protocol transfer failed                                     | Verify TFTP/FTP connectivity and FTP credentials  |
| 5      | Error      | Device cleanup task failed                                   | <ol style="list-style-type: none"> <li>1. Verify the switch connectivity from AFM using Telnet or SSH.</li> <li>2. Re-deploy the switch. Refer to the following procedure.</li> </ol>       |
| 6      | Error      | Complete config upload failed                                | <ol style="list-style-type: none"> <li>1. Verify TFTP/FTP or Telnet/SSH connectivity and verify credentials.</li> <li>2. Re-deploy the switch. Refer to the following procedure.</li> </ol> |
| 7      | Error      | Smart script transfer failed                                 | None  |
| 8      | Error      | Custom config upload failed                                  | Verify the login and configuration commands on the switch   |
| 9      | Error      | Backup config failed   | <ol style="list-style-type: none"> <li>1. Verify Telnet or SSH connectivity from AFM.</li> <li>2. Re-deploy the switch. Refer to the following procedure.</li> </ol>                        |
| 10     | InProgress | Verifying that the switch is eligible for the deploy process | None  |
| 11     | InProgress | Protocol transfer in progress...                             | None  |



| Number | Status     | Status Details                                  | Recommended Action |
|--------|------------|---|--------------------|
| 12     | InProgress | Device cleanup task done, reload in progress... | None               |
| 13     | InProgress | Complete config upload in progress...           | None               |
| 14     | InProgress | Smart script transfer in progress...            | None               |
| 15     | InProgress | Custom config upload in progress...             | None               |
| 16     | InProgress | Backup config in progress...                    | None               |
| 17     | InProgress | Merged config upload in progress...             | None               |

1. Verify that the software images for the switches are installed on the TFTP or FTP server.
2. Verify that you have configured the correct TFTP or FTP address on the **Administration > Settings** tab. If you change the TFTP server now, the address is not correct unless you reconfigure the pre-deployment.
3. If you use a remote DHCP server, verify that the DHCP configuration file that AFM generates for the switches in the fabric is integrated into the DHCP server. This file enables the switch to connect to the DHCP server and download the correct configuration and boot files.
4. Restart the DHCP server that contains the generated DHCP file that you created on the **DHCP Integration** screen. For information about DHCP integration, refer to [DHCP Integration](#). For information about how to view the DHCP configuration file for a fabric, refer to [Viewing the DHCP Configuration File](#).
5. From the menu, click **Network > Fabric Name** and then the **Configure and Deploy** tab.
6. From the **Deploy Fabric** drop-down menu, select **Deploy and Validate**.  
The **Deploy and Validate** dialog box appears.
7. On the **Deploy** tab, select the switches to deploy.
8. Power up the selected IP-ready switches.
9. Click **Deploy Selected** and in the confirmation dialog box, click **Yes**.  
The **Configuration deployment option** dialog box appears.
10. Select a configuration deployment option:
  - **Apply configuration changes to the switch** — Apply new configuration changes from AFM to the switch.
  - **Overwrite entire configuration on the switch** — Overwrite the entire current configuration on the switch instead of applying only the changes to the current switch configuration.
    - If the **Reset to factory defaults** option is selected, AFM resets the switch to the factory default mode (BMP mode). AFM deploys the new configuration on the switch by overwriting the current configuration.
    - If the **Reset to factory defaults** option is not selected, AFM deploys the new configuration on the switch by overwriting the current configuration.
  - **Skip Deployment and proceed to Validation** — Skip the deployment process and validate the switch.
11. Check the progress and status of the deployment in the **Status**, **Status Details**, **Response Actions**, and **Last Deployed Time** columns.  
For information about how to view validation errors, refer to [Validation](#). See also [Troubleshooting](#). For information about the progress and status of selected switches and operations allowed during a fabric state, refer to [Operations Allowed During Each Fabric State](#) and [Understanding Fabric Phases](#).

## Aborting Deployment

1. From the menu, click **Network** > *Fabric Name* and then the **Configure and Deploy** tab.
2. From the **Deploy Fabric** drop-down menu, select **Deploy and Validate**.  
The **Deploy and Validation** dialog box appears.
3. On the **Deploy** tab, select the switches.
4. Click **Abort Selected**.
5. In the confirmation dialog box, click **Yes**.

## Advanced Configuration

To perform the following tasks, use the **Advanced Configuration** screen:

- [View the Auto-Generated Configuration](#)
- [Associate the Templates to Fabric Switches](#)
  - ✎ **NOTE:** Create a template for the fabric before associating it to the fabric. For more information, refer to the Adding Templates section in [Managing Templates](#).
- [Add the Switch Specific Custom Configuration](#)
- [Preview the Combined Configuration](#)

### View the Auto-Generated Configuration

1. From the menu, click **Network** > *Fabric Name* and then click the **Configure and Deploy** tab.
2. From the **Deploy Fabric** drop-down menu, select **Advanced Configuration**.  
The **Advanced Configuration** dialog box appears.
3. Click **Auto-Generated Configuration**.
4. Click **View Auto-Generated Configuration** link and wait for the configuration to appear.

### Associating Templates

Associate one or more existing configuration templates to the entire fabric, all spines, all leaves, all aggregation switches, all core switches, all access switches, or a set of switches. If you associate a template with an entire fabric or all spines, all leaves, all core switches, all aggregation switches, or all core switches, the template is automatically applied to all new switches so you do not need to create new associations manually.

✎ **NOTE:** Each template can have only one association per fabric. AFM does not support template ordering for command sequencing. If you want to order templates for command sequencing, Dell Networking recommends manually combining the templates into a single template.

1. Navigate to the **Network** > *Fabric Name* > **Configure and Deploy** screen.
2. From the **Deploy Fabric** drop-down, select **Deploy and Validate**.
3. On the **Deploy** tab, click **Advanced Configuration**.
4. Click **Associate Templates to Fabric Switches**.  
The **Associate Templates** screen appears.
5. Click **Add Association**.
6. In the **Template Name** drop-down menu, select a template.
7. (Optionally) In the **Comments** field, enter any comments for the template.
8. In the **Select Association** area, select one of the following options:

- **All** — Associate the template to all the switches in the fabric.
- **Aggregation** — Associate the template to all aggregation switches.
- **Access** — Associate the template to all access switches.
- **Core** — Associate the template to all core switches.
- **Spines** — Associate the template to all spine switches.
- **Leafs** — Associate the template to all leaf switches.
- **Custom** — Associate the template with specific switches. In the **Available Switches**, select the switches to associate with the template.

9. Click **Apply**.

### Adding a Switch-Specific Custom Configuration

Before editing the existing configuration, back up the existing running configuration in the flash with a unique name that includes the date and time.

1. From the menu, click **Network > Fabric Name** and then the **Configure and Deploy** tab.
2. From the **Deploy Fabric** drop-down menu, select **Advanced Configuration**.  
The **Advanced Configuration** dialog box appears.
3. On the **Deploy** tab, select **Advanced Configuration**.  
The **Advanced Configuration** dialog box appears.
4. Click **Add Switch Specific Custom Configuration**.  
The **Switch Specific Custom Configuration** dialog box appears.

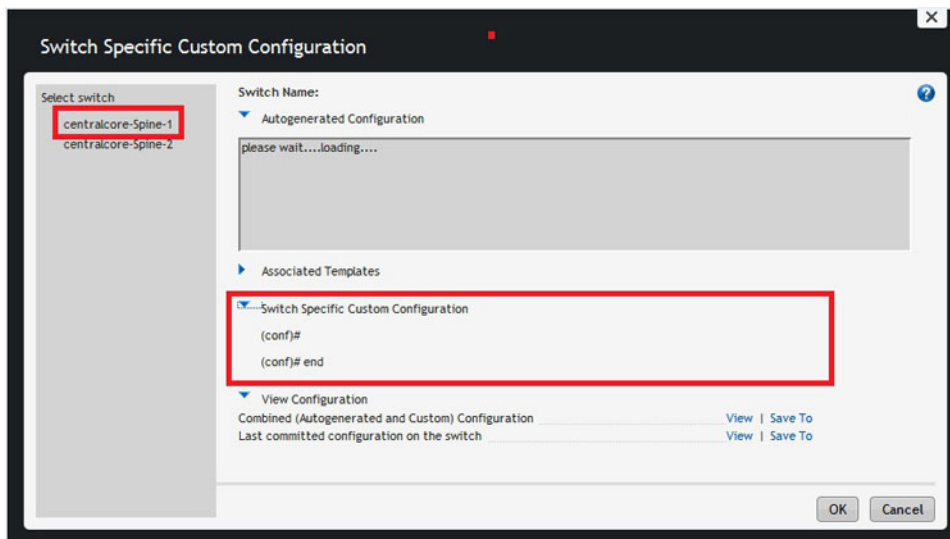


Figure 78. Switch Specific Custom Configuration

View the auto-generated configuration and switch-specific custom configuration applied to the deployed switches in the fabric on the **Switch Specific Custom Configuration** screen.

5. Enter the switch specific-custom configuration using CLI commands in the **Switch Specific Custom Configuration** area.
6. To view the auto-generated configuration, global custom configuration, and switch specific configuration or save it, click **View** or **Save To** next to **Combined (Auto-generated and Custom) Configuration**.

The **View Combined Configuration** dialog box appears. Click **Close** to close this dialog box.

7. To view the last applied configuration or save it, click **View** or **Save To** next to the **Last committed configuration on the switch** area.
8. Review the combined configuration and make any necessary changes.
9. If you make changes, click **Save To** to save the combined auto-generated and custom configuration.
10. Click **OK** to close the **Switch Specific Custom Configuration** dialog box.

### Preview Combined Configuration

To preview the combined configuration:

1. From the menu, click **Network** > *Fabric Name* and then click the **Configure and Deploy** tab.
2. From the **Deploy Fabric** drop-down menu, select **Advanced Configuration**.  
The **Advanced Configuration** dialog box appears.
3. Click **Preview Combined Configuration**.  
The **Combined Configuration** screen appears.

### Validation

You can verify that the discovered fabric matches the planned fabric and correct any errors. AFM reports mismatches as errors and generates the corresponding alarms. After fixing any errors found during validation, verify that all issues were resolved according to the planned fabric by re-validating the fabric.

1. From the menu, click **Network** > *Fabric Name* and then click the **Configure and Deploy** tab.
2. In the **Switch** column, select the switches for validation.
3. From the **Deploy Fabric** drop-down menu, click **Deploy and Validate**.  
The **Deploy and Validation** dialog box appears.
4. Click the **Validation** tab.
5. Select the switches for validation.
6. Review the progress in the **Status**, **Status Details**, **Response Actions**, and **Last Validated Time** columns.
7. Correct any errors.
8. If you fix any errors found during validation, verify that all issues were fixed according to the planned fabric by re-validating the fabric.
9. Click **Close**.

**Table 53. Validation Status**

| Number | Status   | Status Details                      | Response Action  |
|--------|----------|-------------------------------------|--|
| 1      | Required | Validation Required                 | None   |
| 2      | Complete | Validation completed                | None   |
| 3      | Error    | HOSTNAME/MAC Address/MODEL Mismatch | To check for switch mismatch errors:<br><br><ol style="list-style-type: none"> <li>1. From the menu, click <b>Network</b> &gt; <i>Fabric Name</i> and then click the <b>Configure and Deploy</b> tab.</li> <li>2. Click <b>Errors</b>.</li> <li>3. To view error details, click the <b>Discovered Errors</b> tab.</li> </ol> |

| Number | Status | Status Details  | Response Action   |
|--------|--------|---|---|
|        |        |   | 4. Fix any errors.  |
| 4      | Error  | HOSTNAME/MAC Address/MODEL Mismatch and STANDBY UNIT down | To check for switch mismatch errors:<br><ol style="list-style-type: none"> <li>From the menu, click <b>Network</b> &gt; <i>Fabric Name</i> and then click the <b>Configure and Deploy</b> tab.</li> <li>Click <b>Errors</b>.</li> <li>To view error details, click the <b>Discovered Errors</b> tab.</li> <li>Fix any errors.</li> </ol>    |
| 5      | Error  | STANDBY UNIT down   | To check for switch mismatch errors:<br><ol style="list-style-type: none"> <li>From the menu, click <b>Network</b> &gt; <i>Fabric Name</i> and then click the <b>Configure and Deploy</b> tab.</li> <li>Click <b>Errors</b>.</li> <li>To view error details, click the <b>Discovered Errors</b> tab.</li> <li>Fix any errors.</li> </ol>    |
| 6      | Error  | Switch is not reachable                                   | To verify switch connectivity from AFM:<br><ol style="list-style-type: none"> <li>From the menu, click <b>Network</b> &gt; <i>Fabric Name</i> and then click the <b>Configure and Deploy</b> tab.</li> <li>Click <b>Errors</b>.</li> <li>To view error details, click the <b>Discovered Errors</b> tab.</li> <li>Fix any errors.</li> </ol> |
| 7      | Error  | Switch is not Discovered                                  | To verify switch connectivity from AFM:<br><ol style="list-style-type: none"> <li>From the menu, click <b>Network</b> &gt; <i>Fabric Name</i> and then click the <b>Configure and Deploy</b> tab.</li> <li>Click <b>Errors</b>.</li> <li>To view error details, click the <b>Discovered Errors</b> tab.</li> <li>Fix any errors.</li> </ol> |
| 8      | Error  | Configuration mismatch errors exist                       | To check for switch configuration mismatch errors:<br><ol style="list-style-type: none"> <li>From the menu, click <b>Network</b> &gt; <i>Fabric Name</i> and then click the <b>Configure and Deploy</b> tab.</li> <li>Click <b>Errors</b>.</li> </ol>   |

| Number | Status     | Status Details   | Response Action   |
|--------|------------|--|---|
|        |            |  | <ol style="list-style-type: none"> <li>To view error details, click the <b>Config Mismatch Errors</b> tab.</li> <li>Fix any errors.</li> </ol>  |
| 9      | Error      | Custom Configuration errors exist  | <p>To check for switch custom configuration errors:</p> <ol style="list-style-type: none"> <li>From the menu, click <b>Network &gt; Fabric Name</b> and then click the <b>Configure and Deploy</b> tab.</li> <li>Click <b>Errors</b>.</li> <li>To view error details, click the <b>Custom Config Errors</b> tab.</li> <li>Fix any errors.</li> </ol>  |
| 10     | Error      | Wiring Errors Exist  | <p>To verify the Errors in the <b>Wiring Error</b> tab:</p> <ol style="list-style-type: none"> <li>From the menu, click <b>Network &gt; Fabric Name</b> and then click the <b>Configure and Deploy</b> tab.</li> <li>Click <b>Errors</b>.</li> <li>To view error details, click the <b>Wiring Errors</b> tab.</li> <li>To sort the errors by tier (aggregation, access or all), use the <b>Tier</b> drop-down menu. To sort the errors by type (missing link, wiring mismatch, or all), use the <b>Show</b> drop-down menu.</li> <li>Fix any errors.</li> </ol> |
| 11     | Error      | Validation failed because switch license mismatch (Z9500-series switches only) | <p>A Z9500-series switch has fewer licensed ports than the switch in the fabric design. To view details from AFM:</p> <ol style="list-style-type: none"> <li>From the menu, click <b>Network &gt; Fabric Name</b> and then click the <b>Configure and Deploy</b> tab.</li> <li>Click <b>Errors</b>.</li> <li>To view error details, click the <b>Discovered Errors</b> tab.</li> <li>Fix any errors.</li> </ol>   |
| 12     | InProgress | Node validation in progress...   | None  |
| 13     | InProgress | Configuration Validation in progress...  | None  |
| 14     | InProgress | Wiring Validation in progress...   | None  |

## Viewing Deployment and Validation Status

1. From the menu, click **Network** > *Fabric Name* and then click the **Configure and Deploy** tab.
2. Select the fabric.
3. From the **Deploy Fabric** drop-down menu, select **Deploy and Validate**.  
The **Deploy and Validation** dialog box appears, displaying all configured switches and their status.

## Custom CLI Configuration

This section contains the following topics.

- [Managing Templates](#)
- [Associating Templates](#)
- [Viewing Custom Configuration History](#)
- [Switch Specific Custom Configuration](#)

### Managing Templates

For information on how to associate a template to a switch or fabric, refer to [Associating Templates](#).

### Adding Templates

To apply a custom configuration to the following switch types, create a CLI configuration template:

- Specific switches in a fabric
  - All aggregation switches in the fabric
  - All access switches in the fabric
  - All core switches
  - All switches in the fabric
  - All leaf switches in the fabric
  - All spines in the fabric
1. From the menu, click **Network** > *Fabric Name* and then click the **Configure and Deploy** tab.
  2. From the **CLI Configuration** drop-down menu, select **Manage Templates**.  
The **Templates** dialog box appears.
  3. Click **Add**.  
The **Add Template** dialog box appears.
  4. In the **Template Name** field, specify a unique name for the template.
  5. (Optional) In the **Description** field, enter a description for the template.
  6. In the **Configuration Commands** area, enter the CLI configuration commands that you want to include in the template.
  7. Click **OK**.

### Editing Templates

1. From the menu, click **Network** > *Fabric Name* and then click the **Configure and Deploy** tab.
2. From the **CLI Configuration** drop-down menu, select **Manage Templates**.  
The **Templates** dialog box appears.

3. Select the template.
4. Click **Edit**.  
The **Edit Template** dialog box appears.
5. In the **Template Name** field, enter a name for the template.
6. (Optional) In the **Description** field, enter a description for the template.
7. In the **Configuration Commands** area, edit the CLI commands.
8. Click **OK**.

## Deleting Templates

- Before you delete a template, make sure that the template is not in use. You can only delete templates that are not being used. If you attempt to delete a template that is being used, AFM displays an error message with the associated fabric for the template.
  - You cannot delete a template if it is associated with one or more switches.
  - You can only delete one template at a time.
  - To delete a template, you must have superuser or administrator privileges.
1. From the menu, click **Network** > *Fabric Name* and then click the **Configure and Deploy** tab.
  2. From the **CLI Configuration** drop-down menu, select **Manage Templates**.  
The **Templates** dialog box appears.
  3. Select the template and then click **Delete**.
  4. Click **Yes**.


## Copying Templates

You can copy an existing template, modify it, and then apply it to fabric or switch. If you copy a template, AFM does not copy any associations to the switches. For information about how to associate templates, refer to [Associating Templates](#).

1. From the menu, click **Network** > *Fabric Name* and then click the **Configure and Deploy** tab.
2. From the **CLI Configuration** drop-down menu, select **Manage Templates**.  
The **Templates** dialog box appears.
3. Select a template to copy.
4. Click **Copy Template**.  
The **Copy Template** dialog box appears.
5. In the **Template Name** field, enter a unique name for the new template.
6. Click **OK**.

## Associating Templates

Associate one or more existing configuration templates to the entire fabric, all spines, all leaves, all aggregation devices, all access devices, all core switches, or a set of switches. If you associate a template with an entire fabric, all spines, all leaves, all aggregation devices, all access devices, or core switches, the template is automatically applied to the newly added switches so you don't have to create new associations manually. You can also edit and delete templates.

 **NOTE:** Each template can have only one association per fabric. AFM does not support template ordering for command sequencing. If you want sequence commands, Dell Networking recommends manually combining the templates into a single template.



## Associating Templates

1. From the menu, click **Network** > *Fabric Name* and then click the **Configure and Deploy** tab.
2. From the **CLI Configuration** drop-down menu, select the **Associate Templates** option.  
The **Associate Templates** dialog box appears.
3. Click **Add Association**.  
The **Associate Template** dialog box appears.
4. In the **Template Name** drop-down menu, select the template.
5. (Optional) In the **Comments** field, enter any comments about this association.
6. In the **Select association** area, select one of the following options:
  - **All** — Associate the template with all switches in the fabric
  - **Aggregation** — Associate the template with all aggregation switches
  - **Access** — Associate the template with all access switches
  - **Core** — Associates the template with all core switches
  - **Custom** — Associate the template with specific switches. Specify the switches in the **Available Switches** area.
  - **Leafs** — Associate the template with all leaf switches
  - **Spines** — Associate the template with all spine switches
7. Click **Apply**.

## Editing Template Associations

1. From the menu, click **Network** > *Fabric Name* and then click the **Configure and Deploy** tab.
2. From the **CLI Configuration** drop-down menu, select **Associate Templates**.  
The **Associate Templates** dialog box appears.
3. Select the template.
4. Click **Edit Association**.  
The **Edit Association** dialog box appears.
5. Edit the association.
6. Click **OK**.

## Deleting Template Associations

1. From the menu, click **Network** > *Fabric Name* and then click the **Configure and Deploy** tab.
2. From the **CLI Configuration** drop-down menu, select **Associate Templates**.  
The **Associate Templates** dialog box appears.
3. Select the template.
4. Click **Delete Association**.
5. In the confirmation dialog box, click **Yes**.

## Adding a Switch-Specific Custom Configuration

Before editing the existing configuration, back up the existing running configuration in the flash with a unique name that includes the date and time.

1. From the menu, click **Network** > *Fabric Name* and then the **Configure and Deploy** tab.
2. From the **Deploy Fabric** drop-down menu, select **Advanced Configuration**.  
The **Advanced Configuration** dialog box appears.
3. On the **Deploy** tab, select **Advanced Configuration**.  
The **Advanced Configuration** dialog box appears.
4. Click **Add Switch Specific Custom Configuration**.  
The **Switch Specific Custom Configuration** dialog box appears.

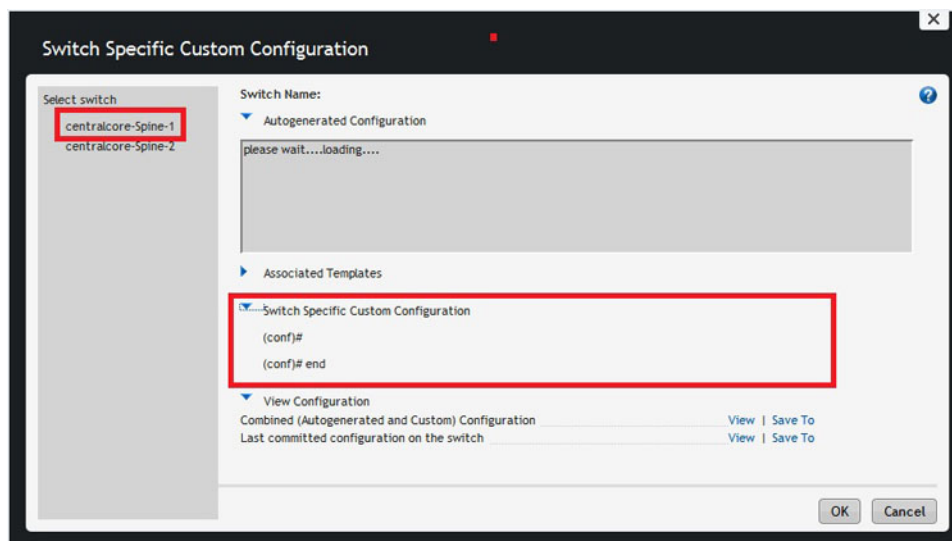


Figure 79. Switch Specific Custom Configuration

View the auto-generated configuration and switch-specific custom configuration applied to the deployed switches in the fabric on the **Switch Specific Custom Configuration** screen.

5. Enter the switch specific-custom configuration using CLI commands in the **Switch Specific Custom Configuration** area.
6. To view the auto-generated configuration, global custom configuration, and switch specific configuration or save it, click **View** or **Save To** next to **Combined (Auto-generated and Custom) Configuration**.  
The **View Combined Configuration** dialog box appears. Click **Close** to close this dialog box.
7. To view the last applied configuration or save it, click **View** or **Save To** next to the **Last committed configuration on the switch** area.
8. Review the combined configuration and make any necessary changes.
9. If you make changes, click **Save To** to save the combined auto-generated and custom configuration.
10. Click **OK** to close the **Switch Specific Custom Configuration** dialog box.

## Viewing Custom Configuration History

To view a complete history of all custom configuration applied to each of the switches, use the **Custom Configuration History** screen.

- **Custom Configuration History** – View a chronological list of custom configurations applied to the switch. To view details for a configuration, select a row in the table.
  - **Applied Custom Configuration Commands** – View all template-based custom configuration commands and switch-specific custom configuration commands applied during deployment or redeployment, including command execution errors.
1. Navigate to the **Network** > *Fabric Name* > **Configure and Deploy** screen.
  2. From the **CLI Configuration** drop-down menu, select **View Custom Configuration History**.  
The **Custom Configuration History** appears.

# Discovering and Deploying an Existing Fabric

To discover an existing fabric or an IOA blade switch in a M1000e chassis, use the **Discover Fabric** option. After you deploy the discovered fabric, the fabric sends alarms and events to AFM. For information about IOA, refer to [Designing an IOA Fabric](#).



**Figure 80. Discovering and Deploying an Existing Fabric**

1. Initiate discovery of an existing fabric. Refer to [Step 1: Discover an Existing Fabric](#).
2. Check the status of the discovered fabric. Refer to [Step 2: View Discovery Status of an Existing Fabric](#).
3. Deploy the successfully discovered fabric. Refer to [Step 3: Deploy Discovered Fabric](#).
4. Perform maintenance, such as monitoring and software updates. Refer to [Maintenance](#) and [Performance Management](#).

## Step 1: Discover an Existing Fabric

For more information about discovering and deploying an existing fabric, refer to [Discovering and Deploying an Existing Fabric](#).



1. From the menu, click **Network** and then the **Design Fabric** tab.  
The **Network Deployment Summary** screen appears.
2. Click **Discover Fabric**.  
The **Introduction** screen for the **Discover Fabric** wizard appears.
3. Read the introduction and click **Next**.  
The **Fabric Name and Type** screen appears.
4. Enter the fabric name in the **Fabric Name** field.  
 **NOTE:** The fabric name must be unique.
5. (Optional) Enter a description for the fabric in the **Description** field.
6. Click **Next**.  
The **Discovery Information** screen appears.
7. Enter the switch's IP address in the **Enter the Switch IP Address** field. To add the IP address, click the **+** button.  
 **NOTE:** You can add an individual IP address or IP address with a subnet or a range. AFM does not support netmasks less than 24.
  - IP range example: 10.16.133.1-150
  - Network with mask example: 10.16.132.0/24
  - To search for a previously entered IP address, enter a portion of or the entire IP address in the **Search IP address list:** field. The software displays all IP addresses that match the search term in the **List of added IPs** field. If you do not enter a search term, all known IP addresses display.
  - To remove an IP address from the displayed list, select the IP address and click the **—** button.
  - To exclude an IP address, enter it in the **Enter Exclusion IP Address** field.
  - To view a list of all IP addresses selected for discovery, click **Preview IP**. The **Preview IP** screen displays only the devices participating in the discovery. To view additional pages, use the arrow buttons or enter the page number in the page number entry field to the left of the arrow buttons.



Figure 81. Preview IP Address Window

8. Add at least one IP address to the **List of added IPs:** field and click **Next**.  
The **Credentials** screen appears.
9. In the **SNMP** section, click **Add**.  
The **SNMP Credential** window appears.

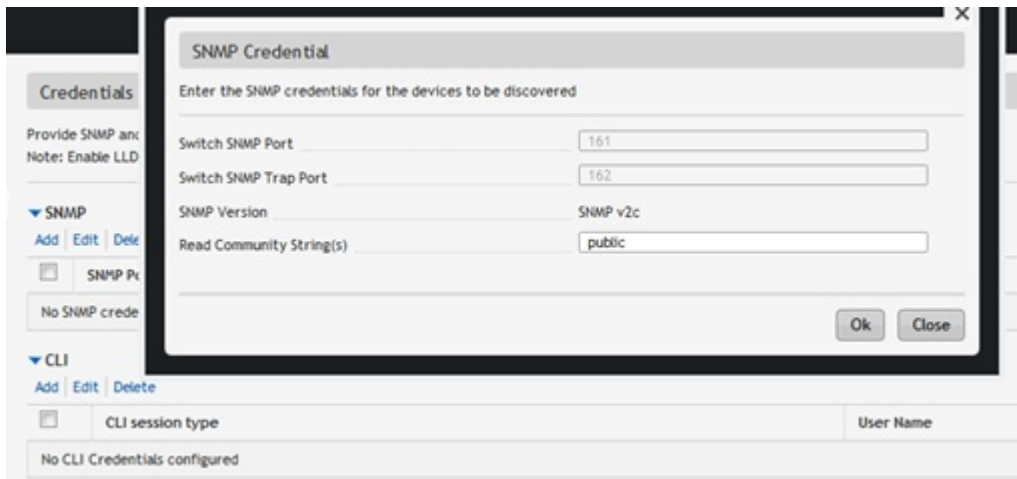



Figure 82. Discover Fabric SNMP Credential Screen

10. Enter the SNMP credential information and click **OK** to confirm the information or click **Close** to close the window. By default, the SNMP port number is 161 and the trap port number is 162. The maximum number of SNMP credentials is five.

- Enter the read community string in the **Read Community String(s)** field. You can only enter one read community string.

 **NOTE:** The SNMP credential information requires the read community string.

 **NOTE:**

- To delete SNMP credentials, check the checkbox for the credentials you want to delete and click **Delete** in the SNMP section. There is no confirmation message before the credentials are deleted.
- To edit SNMP credentials, check the checkbox for the credentials you want to edit and click **Edit** in the SNMP section. Click **OK** to save changes or click **Close** to close the window.

11. Click **Add** in the **CLI Credentials** section.

The **CLI Credential** window appears.

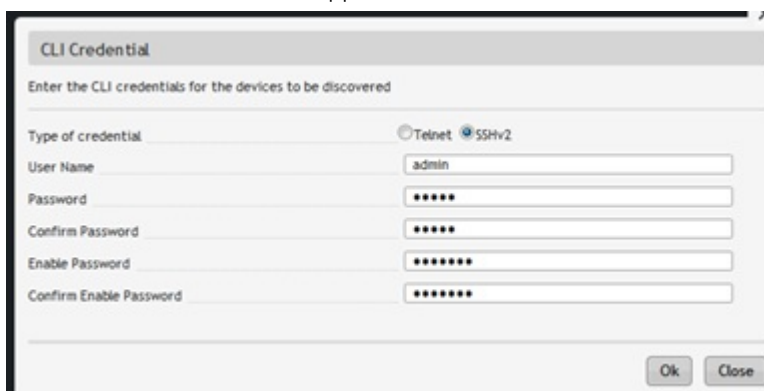



Figure 83. Discover Fabric CLI Credential Screen

 **NOTE:** Configure up to five CLI credentials for a single fabric. AFM supports combinations of credential types (SSHv2 and Telnet).

12. Enter the CLI credential information.

- a. Select the appropriate credential type (Telnet or SSHv2).
- b. Enter the user name in the **User Name** field and enter the password in the **Password** and **Confirm Password** fields.
- c. If you configured an enable password, enter it in the **Enable Password** and **Confirm Enable Password** fields.
- d. Click **OK** to confirm the information or click **Close** to close the window.

 **NOTE:**

- To delete CLI credentials, check the checkbox for the credentials you want to delete and click **Delete** in the CLI section. There is no confirmation message before the credentials are deleted.
- To edit CLI credentials, check the checkbox for the credentials you want to edit and click **Edit** in the CLI section. Click **OK** to save changes or click **Close** to close the window.

**13. Click Next.**

The **Summary** screen appears.

**14. In the Summary screen, review the summary information and click Finish.** AFM starts the fabric discovery process and displays the **Network Deployment Summary** screen.

To check the discovery status of an existing fabric, click **Discover Status**. For information about the **Discover Status** screen, refer to [Step 2: View Discovery Status of an Existing Fabric](#).

## Step 2: View Discovery Status of an Existing Fabric

Use the **Discovery Status** screen to:

- Display the current fabric discovery status and details for switches and chassis used in the existing fabric or an IOA in a M1000e chassis.
- Verify that AFM has discovered all the switches in an existing fabric or IOA fabric.
- Rediscover an existing chassis or switch for troubleshooting.
- Remove a switch from the discovered fabric.


For more information about fabric discovery, refer to [Discovering and Deploying an Existing Fabric](#).

The following discover options are available:

- **Rediscover Fabric** — Rediscover an existing fabric.
- **Rediscover Switches** — Rediscover an existing chassis or switch for troubleshooting. If a device is not discovered, check the **Reason** column for the recommended action. To rediscover an existing chassis or switch, select the check box for the device and then click **Rediscover Switches**. To select all devices, selecting the top-left check box.
- **Remove Switches** — Remove a switch from the discovered fabric by excluding the switch's IP from the fabric.

The following information displays:

- IP address
- Switch name
- Vendor
- Model

 **NOTE:** Only Dell IOA and MXL blades are identified. All other blade types are listed as Unknown.

- Software version



- SNMP status
- CLI login status
- Discovery status
- Reason (Completed, In Progress, Failed, or Not Yet Started) — If a device is not discovered, check the **Reason** Column for the recommended action.

For information about how to discover a fabric, see [Discovering an Existing Fabric](#).

View the tabular wiring plan for a discovered fabric on the **Network > Design > View Wiring Plan** screen.

1. From the menu, click **Network** and then the **Design Fabric** tab.
2. Click **Discovery Status**.

 **NOTE:**

To remove a chassis, navigate to the **Edit Fabric** screen and delete the IP address of the chassis.

3. To check the discovery status of an existing fabric, click **Discover Status**. Check for failed devices and look for error messages in the **Reason** column for the cause, such as an authentication failure.

After you close the Discovery Status screen, deploy the discovered fabric. For information about deploying an existing fabric, refer to [Step 3: Deploy Discovered Fabric](#).

## Step 3: Deploy Discovered Fabric

After you deploy the discovered fabric, the fabric sends alarms and events to AFM. The design, pre-deployment, and validation fields on the **Network > Fabric Name > Configure and Deploy** screen do not apply to fabric discovery. For more information, refer to [Discovering and Deploying an Existing Fabric](#)

1. Close the **Discovery Status** screen.
2. From the menu, click **Network** and then click the **Design Fabric** tab.
3. Select the fabric and click **Edit Fabric**.
4. Navigate to the **Step 3 Deployment** column.
5. To deploy the discovered fabric, click the **Required** link for the discovered fabric.  
The **Deploy and Validation** screen appears.
6. On the **Deploy** tab, select the switches in the fabric you want to deploy.
7. Click **Deploy Selected**.  
The **Configuration deployment option** screen appears.
8. Select **Apply configuration changes to the switch** or **Skip Deployment and proceed to Validation** and click **OK**.

## Viewing the Fabric

This section contains the following topics:

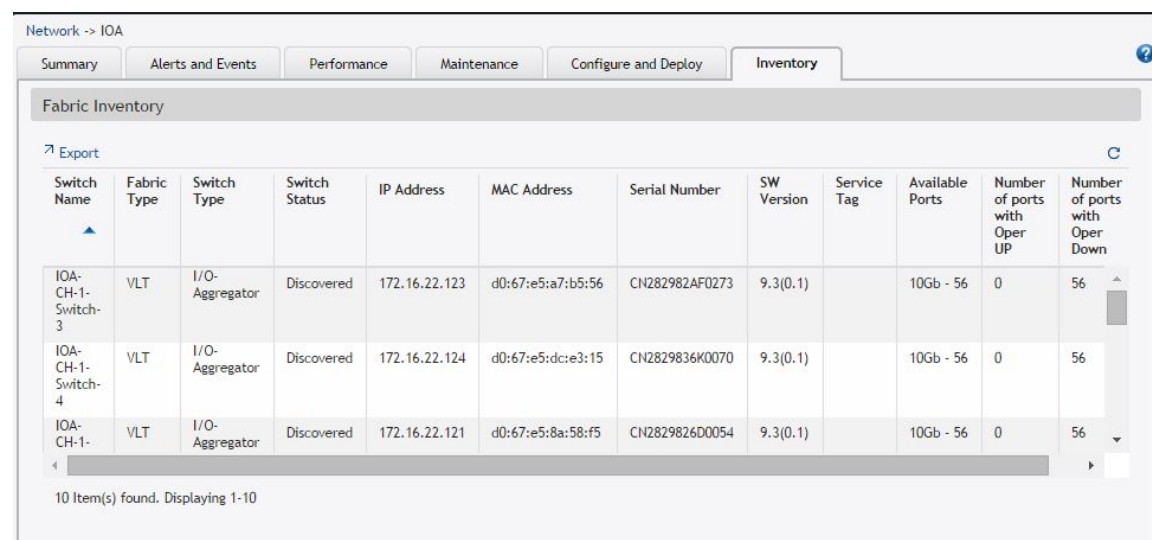
- [Inventory Management](#)
- [Dashboard](#)
- [View Network Summary](#)
- [View Fabric Summary](#)
- [Switch Summary](#)

Related Links: [Fabric Performance Management](#).

## Inventory Management

The **Inventory** tab displays all discovered switches in the fabric. From this screen, you can:

- View simplified or detailed inventory information
- Refresh the inventory
- Export the current inventory as a comma-separated value (CSV) file



The screenshot shows the 'Inventory' tab in a network management interface. The interface includes a navigation bar with tabs for Summary, Alerts and Events, Performance, Maintenance, Configure and Deploy, and Inventory. Below the navigation bar is a 'Fabric Inventory' section with an 'Export' button. The main content is a table with the following columns: Switch Name, Fabric Type, Switch Type, Switch Status, IP Address, MAC Address, Serial Number, SW Version, Service Tag, Available Ports, Number of ports with Oper UP, and Number of ports with Oper Down. The table displays three rows of data for switches IOA-CH-1-Switch-3, IOA-CH-1-Switch-4, and IOA-CH-1-Switch-5. At the bottom of the table, it indicates '10 Item(s) found. Displaying 1-10'.

| Switch Name       | Fabric Type | Switch Type    | Switch Status | IP Address    | MAC Address       | Serial Number  | SW Version | Service Tag | Available Ports | Number of ports with Oper UP | Number of ports with Oper Down |
|-------------------|-------------|----------------|---------------|---------------|-------------------|----------------|------------|-------------|-----------------|------------------------------|--------------------------------|
| IOA-CH-1-Switch-3 | VLT         | I/O-Aggregator | Discovered    | 172.16.22.123 | d0:67:e5:a7:b5:56 | CN282982AF0273 | 9.3(0.1)   |             | 10Gb - 56       | 0                            | 56                             |
| IOA-CH-1-Switch-4 | VLT         | I/O-Aggregator | Discovered    | 172.16.22.124 | d0:67:e5:dc:e3:15 | CN2829836K0070 | 9.3(0.1)   |             | 10Gb - 56       | 0                            | 56                             |
| IOA-CH-1-Switch-5 | VLT         | I/O-Aggregator | Discovered    | 172.16.22.121 | d0:67:e5:8a:58:f5 | CN2829826D0054 | 9.3(0.1)   |             | 10Gb - 56       | 0                            | 56                             |

**Figure 84. Inventory Tab**

1. For the Network level: From the menu, click **Network** and then click the **Inventory** tab. For the Fabric level: From the menu, click **Network** > *Fabric Name* and then click the **Inventory** tab. Details for the switches in the selected fabric appear in tabular format.
2. To export the data, click **Export**.

AFM exports the fabric data as a spreadsheet.

## Dashboard

You can view the fabric and system health on the **Dashboard** tab. You can access this tab by selecting **Home** from the menu and then clicking the **Dashboard** tab.

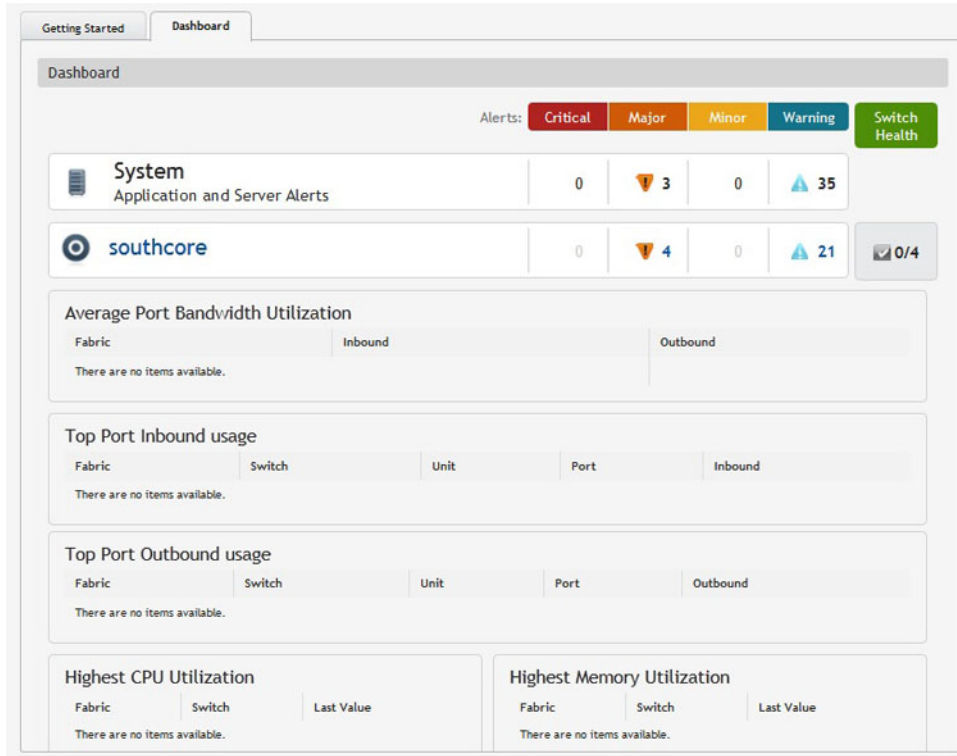


Figure 85. Dashboard

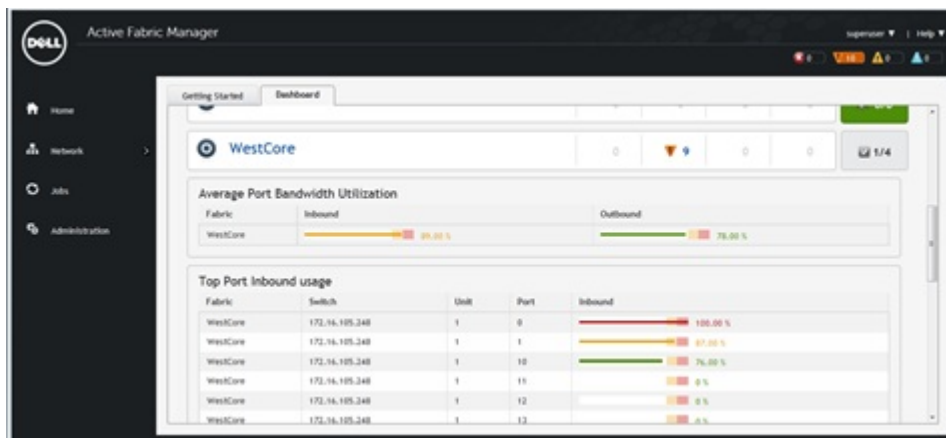


Figure 86. Dashboard with Color Codes

The Dashboard provides the following performance information:

- **System** – View a tabular listing of system health and fabrics and the corresponding alert count in order of severity. The **Switch Health** column displays the number of switches that have no alerts and the number of switches in the fabric.
- **Average Port Bandwidth Utilization** – View the average port bandwidth utilization for all fabrics.
- **Top Port Usage** – View the ten most frequently used ports for all fabrics by:
  - Fabric
  - Switch
  - Port number
  - Inbound (%): number with color code bar
  - Outbound (%): number with color code bar

**Table 54. Inbound and Outbound Link Utilization Color Codes**

| Color          | Range                        | Description   |
|----------------|------------------------------|---|
| Green (Good)   | $x < 80\%$                   | Represents normal inbound or outbound link utilization. |
| Yellow (Minor) | $x \geq 80\%$ and $x < 90\%$ | Represents low link utilization.                        |
| Red (Critical) | $x \geq 90\%$                | Represents high link utilization.                       |

 **NOTE:** If the color code is yellow or red, AFM displays an alarm on the **Network > Fabric Name > Switch Name > Alerts and Events** tab > **Current** view.

- **Highest CPU Utilization** – View the five CPUs with the highest utilization (by five-minute intervals) for all fabrics by:
  - Fabric
  - Switch
  - Last Values (%): number with color code bar

**Table 55. CPU Utilization Color Codes**


| Color          | Range                        | Description                        |
|----------------|------------------------------|------------------------------------|
| Green (Good)   | $x < 70\%$                   | Represents normal CPU utilization. |
| Yellow (Minor) | $x \geq 70\%$ and $x < 80\%$ | Represents low CPU utilization.    |
| Red (Critical) | $x \geq 80\%$                | Represents high CPU utilization.   |

 **NOTE:** If the color code is yellow or red, AFM displays an alarm on the **Network > Fabric Name > Switch Name > Alerts and Events** tab > **Current** view.

- **Highest Memory Utilization** – View the highest five instances of memory utilization for all fabrics by:
  - Fabric
  - Switch
  - Last value (%): number with color code

**Table 56. Memory Utilization Color Codes**

| Color          | Range                   | Description                           |
|----------------|-------------------------|---------------------------------------|
| Green (Good)   | $x < 82\%$              | Represents normal memory utilization. |
| Yellow (Minor) | $> = 82\%$ and $< 92\%$ | Represents low memory utilization.    |
| Red (Critical) | $> = 92\%$              | Represents high memory utilization.   |

 **NOTE:** If the color code is yellow or red, AFM displays an alarm on the **Network > Fabric Name > Switch Name > Alerts and Events > Current** screen.

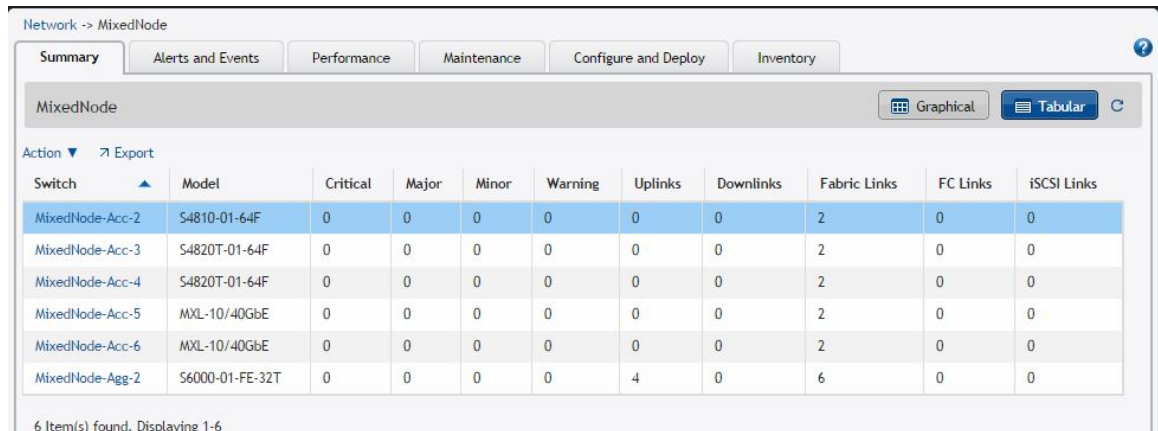
For more information, refer to [Alerts and Events](#).

## Network Topology

To display all the fabrics in the network topology in a graphical or tabular view, use the **Network > Summary** tab. The network topology view contains a collection of fabric icons with a color-coded status and fabric names. There are no links between fabrics.

### Network Topology Tabular View

Navigate to the **Network > Summary** tab and then click the **Tabular**.



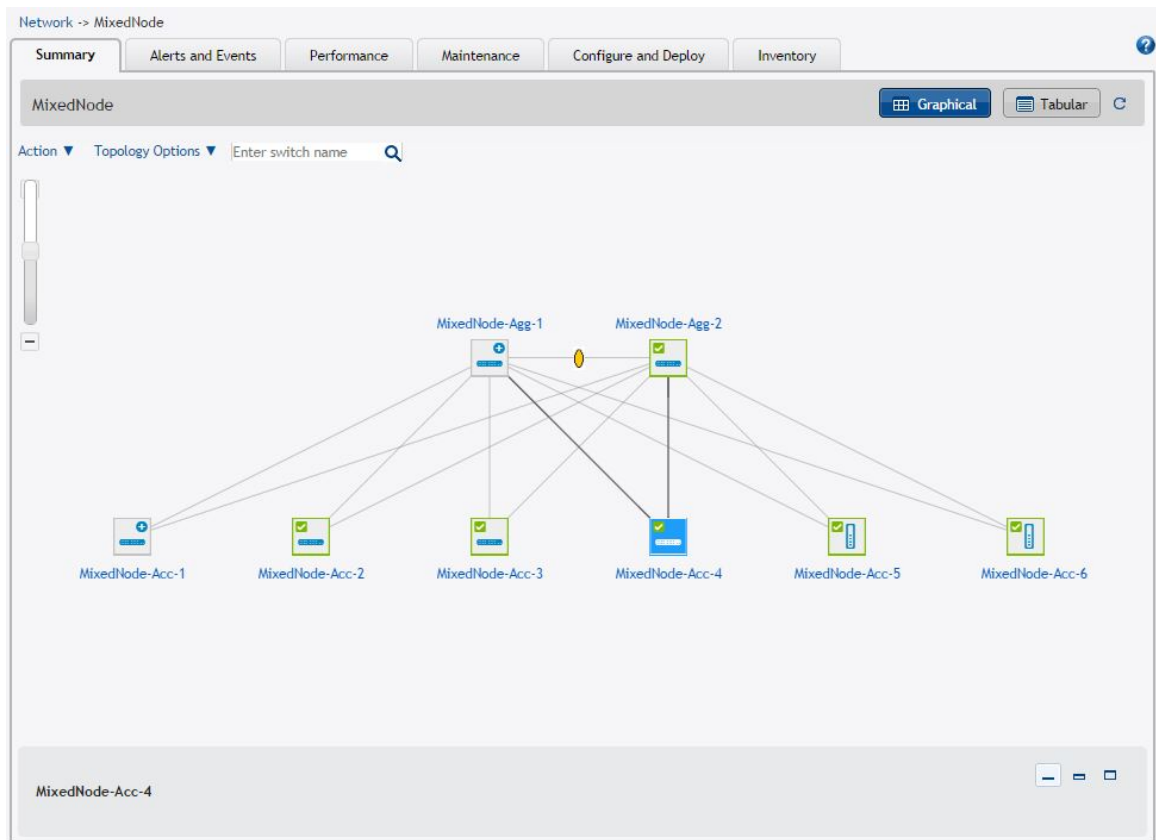
| Switch          | Model           | Critical | Major | Minor | Warning | Uplinks | Downlinks | Fabric Links | FC Links | iSCSI Links |
|-----------------|-----------------|----------|-------|-------|---------|---------|-----------|--------------|----------|-------------|
| MixedNode-Acc-2 | S4810-01-64F    | 0        | 0     | 0     | 0       | 0       | 0         | 2            | 0        | 0           |
| MixedNode-Acc-3 | S4820T-01-64F   | 0        | 0     | 0     | 0       | 0       | 0         | 2            | 0        | 0           |
| MixedNode-Acc-4 | S4820T-01-64F   | 0        | 0     | 0     | 0       | 0       | 0         | 2            | 0        | 0           |
| MixedNode-Acc-5 | MXL-10/40GbE    | 0        | 0     | 0     | 0       | 0       | 0         | 2            | 0        | 0           |
| MixedNode-Acc-6 | MXL-10/40GbE    | 0        | 0     | 0     | 0       | 0       | 0         | 2            | 0        | 0           |
| MixedNode-Agg-2 | S6000-01-FE-32T | 0        | 0     | 0     | 0       | 4       | 0         | 6            | 0        | 0           |

**Figure 87. Network Topology Tabular View**

### Network Topology Graphical View

Navigate to the **Network > Summary** tab and then click **Graphical**.

The network topology contains fabric icons. Each fabric icon has the following functions:



**Figure 88. Network Topology Graphical View**

- **Status:** — View the status of the fabric using the following colors:
  - Red: Critical alerts
  - Orange: Major alerts
  - Yellow: Minor alerts
  - Blue: Warning alerts
  - Green: Information alerts or no alerts
  - Gray: AFM has not deployed or managed these fabrics
- **Selection** — To view the fabric data in the **Summary** tab, click a fabric icon.
- **Popup menu** — To display a menu of available actions and the fabric name, right-click a fabric.
- **Enter fabric name** — To locate a fabric, enter the name and then click the search icon.

The following options are available from the **Action** pull-down menu:

- **View Fabric Topology** — Displays topology for a selected fabric.
- **Load Background Map** — Load a geographical background map for the network.
- **Delete Background Map** — Delete a geographical background map for the network.

The following options are available from the **Topology Options** pull-down menu:

- **Show Tooltips** — View information about a fabric, such fabric name, status, active alerts, and the number of switches in the fabric, as a tooltip when you place your mouse over a fabric icon.

- **Enable Move** — To move each fabric icon to a new location in the map, enable this option.
- **Revert to Last Saved** — Revert fabric locations to the last saved version.
- **Save Move** — Save changes to fabric locations.

## Fabric Summary

The **Network** > *Fabric Name* > **Summary** tab displays information about a network fabric and its constituent switches in tabular or graphical format.

### Displaying the Fabric in a Tabular View

To view the switches in the fabric and check alarms, click **Tabular**.

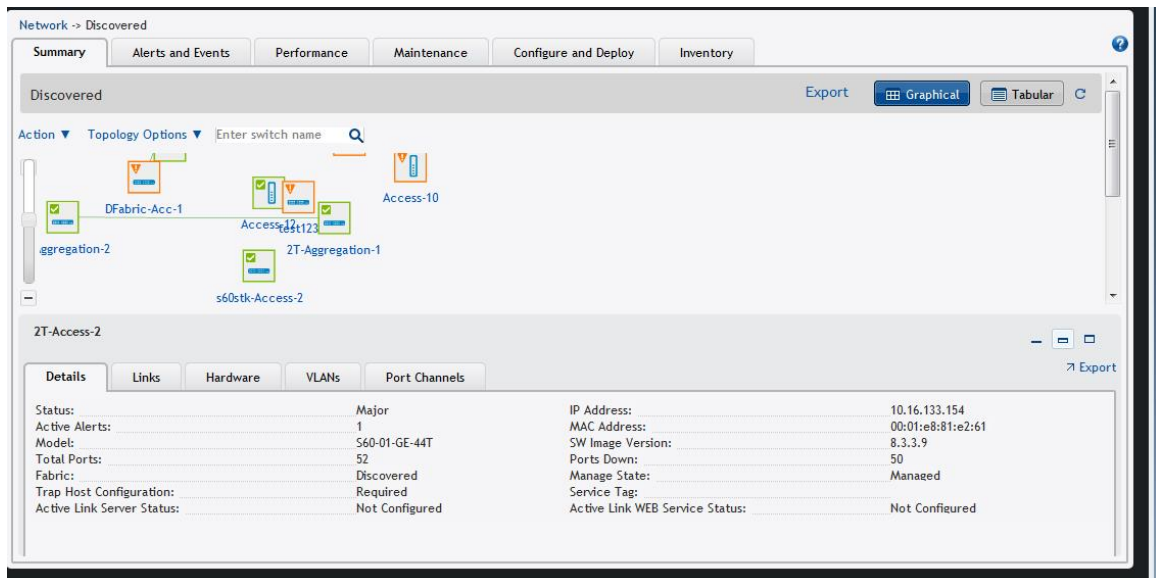
- To export results, click **Export**.
- To manage or remove a switch, from the **Action** pull-down menu, click **Manage/Unmanage Switch**.
- To view additional performance statistics about a fabric:
  - a. Select the switch row.
  - b. From the **Action** drop-down menu, click **Launch Active Link**.

For information about how to configure the Active Link, navigate to the **Administration** > **Settings** tab > **Active Link Settings** area.

### Displaying the Fabric in a Graphical View

To view the fabric topology, click **Graphical**. The fabric type and name appear at the top of the screen. View the leaf switches associated with a spine by clicking the spine or view aggregation switches associated with the access switches by clicking an aggregation switch. The following options are available from the **Action** menu:

- **Manage/Unmanage** — *Unmanaged* switches are switches that appear in the fabric but AFM does not manage them. To monitor and manage a switch, place it in a managed state.
- **Launch Active Link** — View additional performance statistics about a fabric in a graphical view by navigating to the following screens:
  - Right-click the switch icon and select **Active Link**.
  - Select the **Launch Active Link** option from the **Action** drop-down menu.



**Figure 89. Fabric Summary Screen — Graphical View**

For information about how to configure the Active Link, navigate to the [Active Link Settings screen](#).

The following options are available from the **Topology Options** menu:

- **Show Tooltips** — View information about a switch such as associated fabric, switch name, model name, IP address, alarm status, and managed state when you place the cursor over the switch.
- **Show All Links** — View all the links between the spines and the leaves, aggregation and access, or aggregation, access, and core.

The following search option is available:

- **Enter switch name** — To locate a switch in the fabric, enter the switch name and click the search icon. The switch name is case-sensitive.

## Switch Summary

To view the following switch summary information from a graphical view, from the menu, navigate to **Network** > *Fabric Name* > *Switch Name* and then the **Summary** tab. Make sure that the **Graphical** button is selected in the upper right of the screen. You can also view this information in a tabular view by selecting the **Tabular** button.

- To display information about the state of the port, click the port.
- To display port legends, click the **Port Legends** arrow.
- To display additional statistics about a switch through the AFM using an OMNM server, click the **Launch Active Link** from the graphical or tabular view. For information about how to configure a element management service, navigate to the [Active Link Settings screen](#) screen.
- Status
- Active Alerts
- Speed
- Manage State



# Troubleshooting

This section contains the following topics:

- [Ping, Traceroute, Telnet, and SSH](#)
- [Validation Alarms](#)
- [Deployment and Validation Errors](#)
- [TFTP/FTP Error](#)
- [Switch Deployment Status](#)
- [Validating Connectivity to the ToR](#)

## Ping, Traceroute, Telnet, and SSH

To troubleshoot a switch in the fabric, use ping, traceroute, SSH, or Telnet.

 **NOTE:** SSH or Telnet functionality depends on the switch protocol configuration.

1. From the menu, select **Network** > *Fabric Name* > *Switch Name* and then click the **Troubleshoot** tab.
2. To display the traceroute results, click the **Ping, Traceroute, Telnet,** or **SSH** or tab as appropriate.
3. Based on your selection, perform the following steps:

For ping:

- To display the ping results, click **Ping**

For traceroute:

- Click **TraceRoute**

For Telnet:

- In the **Telnet Command** field, enter the Telnet command.
- To display the Telnet results, click **Send Command**.


For SSH:

- In the **SSH Command** field, enter the SSH command.
- To display the SSH results, click **Send Command**

## Validation Alarms

To troubleshoot alarms triggered during deployment, use the following table:

**Table 57. Validation Alarms**

| Alarm  | Recommended Action  |
|--|---|
| Validation failed because the switch cannot be discovered.       | Log on to the switch console to isolate the fault.<br> <b>NOTE:</b> Make sure that the switch has been power cycled and check the physical connection.   |
| Validation failed because the switch has a mismatch MAC address. | <ol style="list-style-type: none"> <li>1. To verify that you have correctly mapped the system MAC address to the associated switches:                             <ol style="list-style-type: none"> <li>a. Navigate to the <b>Network</b>&gt; <i>Fabric Name</i> &gt; <b>Configure and Deploy</b> tab.</li> <li>b. From the <b>Deploy Fabric</b> drop-down menu, select <b>Pre-deployment Configuration</b>.</li> <li>c. Navigate to the <b>Assign Switch Identities</b> screen and check the system MAC address mapping for the associated switches.</li> </ol> </li> <li>2. To verify changes, validate the switch:                             <ol style="list-style-type: none"> <li>a. Navigate to the <b>Network</b>&gt; <i>Fabric Name</i> &gt; <b>Configure and Deploy</b> tab.</li> <li>b. From the <b>Deploy Fabric</b> drop-down menu, select <b>Deploy and Validate</b>.</li> <li>c. Click the <b>Validation</b> tab and select the switch.</li> <li>d. Click <b>Validate Selected</b>.</li> </ol> </li> </ol> |
| Validation failed because the switch has a name mismatch.        | <ol style="list-style-type: none"> <li>1. To verify that you have correctly mapped the system MAC address to the associated switches:                             <ol style="list-style-type: none"> <li>a. Navigate to the <b>Network</b>&gt; <i>Fabric Name</i> &gt; <b>Configure and Deploy</b> tab.</li> <li>b. From the <b>Deploy Fabric</b> drop-down menu, select <b>Pre-deployment Configuration</b>.</li> <li>c. Navigate to the <b>Assign Switch Identities</b> screen and check the system MAC address mapping for the associated switches.</li> </ol> </li> <li>2. To verify changes, validate the switch:                             <ol style="list-style-type: none"> <li>a. Navigate to the <b>Network</b>&gt; <i>Fabric Name</i> &gt; <b>Configure and Deploy</b> tab.</li> <li>b. From the <b>Deploy Fabric</b> drop-down menu, select <b>Deploy and Validate</b>.</li> <li>c. Click the <b>Validation</b> tab and select the switch.</li> <li>d. Click <b>Validate Selected</b>.</li> </ol> </li> </ol> |
| Validation failed because the switch has a model mismatch.       | <ol style="list-style-type: none"> <li>1. Verify that you have correctly mapped the system MAC address to the associated switches:</li> </ol>   |

| Alarm   | Recommended Action  |
|---|---|
|   | <ol style="list-style-type: none"> <li>a. Navigate to the <b>Network</b> &gt; <i>Fabric Name</i> &gt; <b>Configure and Deploy</b> tab.</li> <li>b. From the <b>Deploy Fabric</b> drop-down menu, select the Pre-deployment Configuration option</li> <li>c. Navigate to the <b>Assign Switch Identities</b> screen and check the system MAC address mapping for the associated switches.</li> </ol> <ol style="list-style-type: none"> <li>2. To verify changes, validate the switch: <ol style="list-style-type: none"> <li>a. Navigate to the <b>Network</b> &gt; <i>Fabric Name</i> &gt; <b>Configure and Deploy</b> tab.</li> <li>b. From the <b>Deploy Fabric</b> drop-down menu, select <b>Deploy and Validate</b>.</li> <li>c. Click the <b>Validation</b> tab and select the switch.</li> <li>d. Click <b>Validate Selected</b>.</li> </ol> </li> </ol> |
| Validation failed because the switch is in a disconnected state.          | The switch is not reachable. Verify the connectivity of the switch.   |
| Validation failed because Te 0/1 has a wiring mismatch.                   | <ol style="list-style-type: none"> <li>1. Review the wiring plan.</li> <li>2. Wire according to the wiring plan to fix the wiring mismatch.</li> <li>3. Make sure that the ports on the switches are mapped accurately.</li> </ol>  |
| Validation failed because Te 0/1 has a missing link.                      | No connectivity is detected to the switch. Check the cables.  |
| Validation failed because only a partial link can be verified for Te 0/1. | Check the connectivity of the link and the connectivity of the switch.  |
| Validation failed because the switch has a configuration mismatch.        | <ol style="list-style-type: none"> <li>1. Navigate to the <b>Network</b> &gt; <i>Fabric Name</i> &gt; <b>Configure and Deploy</b> tab.</li> <li>2. Click <b>Errors</b>.</li> <li>3. Select the <b>Config Mismatch Errors</b> tab.</li> <li>4. Review the configuration mismatch and correct the configuration errors.</li> </ol>  |

## Deployment and Validation Errors

### Pre-deployment Errors

To troubleshoot pre-deployment errors, use the following table. For information about IOA pre-deployment errors, refer to [IOA Pre-deployment Errors](#).

**Table 58. Pre-deployment Errors**

| Error Details   | Recommended Action   |
|---|--|
| Failed to transfer minimum configuration file via TFTP/FTP. | <p>Verify the TFTP or FTP connectivity from AFM. For FTP, verify the credentials and restart the <b>DHCP Integration</b> step using the <b>Pre-deployment Configuration</b> wizard.</p> <ol style="list-style-type: none"> <li>1. Navigate to the <b>Network &gt; Fabric Name &gt; Configure and Deploy</b> tab.</li> <li>2. From the <b>Deploy Fabric</b> drop-down menu, select <b>Pre-deployment Configuration</b>.</li> <li>3. Redo the <b>DHCP Integration</b> step.</li> </ol>   |
| Overwrite DHCP contents to local DHCP server failed.        | <p>Verify the following:</p> <ul style="list-style-type: none"> <li>• the permissions of the directory</li> <li>• disk space availability on the AFM server</li> <li>• the local DHCP server configuration</li> </ul> <p>Restart the <b>DHCP Integration</b> step using the <b>Pre-deployment Configuration</b> wizard.</p> <ol style="list-style-type: none"> <li>1. Navigate to the <b>Network &gt; Fabric Name &gt; Configure and Deploy</b> tab.</li> <li>2. From the <b>Deploy Fabric</b> drop-down menu, select <b>Pre-deployment Configuration</b>.</li> <li>3. Redo the <b>DHCP Integration</b> step.</li> </ol> |

## Deployment Errors

To troubleshoot deployment errors, use the following table.

**Table 59. Deployment Errors**

| Error Details              | Recommended Action  |
|----------------------------|---|
| Protocol transfer failed   | <ol style="list-style-type: none"> <li>1. Verify TFTP or FTP connectivity from AFM. For FTP, verify the credentials.</li> <li>2. Restart switch deployment from the <b>Network &gt; Fabric Name &gt; Configure and Deploy</b> tab by selecting the switch from the list.               <ol style="list-style-type: none"> <li>a. Navigate to the <b>Network &gt; Fabric Name &gt; Configure and Deploy</b> tab.</li> <li>b. From the <b>Deploy Fabric</b> drop-down menu, select <b>Deploy and Validate</b>.</li> <li>c. Click the <b>Deploy</b> tab and then select the switches.</li> <li>d. Click <b>Deploy Selected</b>.</li> <li>e. In the confirmation dialog box, click <b>Yes</b>.</li> </ol> </li> </ol> |
| Device cleanup task failed | <ol style="list-style-type: none"> <li>1. Verify Telnet or SSH connectivity from AFM.</li> <li>2. Restart switch deployment from the <b>Network &gt; Fabric Name &gt; Configure and Deploy</b> tab by selecting the switch from the list.               <ol style="list-style-type: none"> <li>a. Navigate to the <b>Network &gt; Fabric Name &gt; Configure and Deploy</b> tab.</li> </ol> </li> </ol>   |

| Error Details                        | Recommended Action   |
|--------------------------------------|--|
|                                      | <ul style="list-style-type: none"> <li>b. From the <b>Deploy Fabric</b> drop-down menu, select <b>Deploy and Validate</b>.</li> <li>c. Click the <b>Deploy</b> tab and then select the switches.</li> <li>d. Click <b>Deploy Selected</b>.</li> <li>e. In the confirmation dialog box, click <b>Yes</b>.</li> </ul>  |
| Complete configuration upload failed | <ul style="list-style-type: none"> <li>1. Verify TFTP/FTP or Telnet/SSH connectivity from AFM.</li> <li>2. Restart the deployment of the switch from the <b>Network &gt; Fabric Name &gt; Configure and Deploy</b> tab by selecting the switch from the list. <ul style="list-style-type: none"> <li>a. Navigate to the <b>Network &gt; Fabric Name &gt; Configure and Deploy</b> tab.</li> <li>b. From the <b>Deploy Fabric</b> drop-down menu, select <b>Deploy and Validate</b>.</li> <li>c. Click the <b>Deploy</b> tab and then select the switches.</li> <li>d. Click <b>Deploy Selected</b>.</li> <li>e. In the confirmation dialog box, click <b>Yes</b>.</li> </ul> </li> </ul> |
| Smart script transfer failed         | <ul style="list-style-type: none"> <li>1. Verify connectivity to the switch from AFM.</li> <li>2. Restart switch deployment from the <b>Network &gt; Fabric Name &gt; Configure and Deploy</b> tab by selecting the switch from the list. <ul style="list-style-type: none"> <li>a. Navigate to the <b>Network &gt; Fabric Name &gt; Configure and Deploy</b> tab.</li> <li>b. From the <b>Deploy Fabric</b> drop-down menu, select <b>Deploy and Validate</b>.</li> <li>c. Click the <b>Deploy</b> tab and then select the switches.</li> <li>d. Click <b>Deploy Selected</b>.</li> <li>e. In the confirmation dialog box, click <b>Yes</b>.</li> </ul> </li> </ul>                     |
| Custom configuration upload failed   | <ul style="list-style-type: none"> <li>1. Verify the switch login credentials and commands.</li> <li>2. Restart switch deployment from the <b>Network &gt; Fabric Name &gt; Configure and Deploy</b> tab by selecting the switch from the list. <ul style="list-style-type: none"> <li>a. Navigate to the <b>Network &gt; Fabric Name &gt; Configure and Deploy</b> tab.</li> <li>b. From the <b>Deploy Fabric</b> drop-down menu, select <b>Deploy and Validate</b>.</li> <li>c. Click the <b>Deploy</b> tab and then select the switches.</li> <li>d. Click <b>Deploy Selected</b>.</li> <li>e. In the confirmation dialog box, click <b>Yes</b>.</li> </ul> </li> </ul>               |
| Backup config failed                 | <ul style="list-style-type: none"> <li>1. Verify the Telnet SSH connectivity.</li> <li>2. Restart switch deployment from the <b>Network &gt; Fabric Name &gt; Configure and Deploy</b> tab by selecting the switch from the list. <ul style="list-style-type: none"> <li>a. Navigate to the <b>Network &gt; Fabric Name &gt; Configure and Deploy</b> tab.</li> <li>b. From the <b>Deploy Fabric</b> drop-down menu, select <b>Deploy and Validate</b>.</li> </ul> </li> </ul>   |

| Error Details | Recommended Action   |
|---------------|--|
|               | <ul style="list-style-type: none"> <li>c. Click the <b>Deploy</b> tab and then select the switches.</li> <li>d. Click <b>Deploy Selected</b>.</li> <li>e. In the confirmation dialog box, click <b>Yes</b>.</li> </ul> |

## Validation Errors

To troubleshoot the following validation errors when you deploy a fabric, use the following tables. The validation process reports any inconsistencies between the design and the discovered fabric. AFM reports mismatches as errors and generates the corresponding alarms.

To view validation errors, navigate to the **Network** > *Fabric Name* > **Configure and Deploy** tab and click **Errors**. The validation process reports the following error types:

- Configuration
- Custom Configuration
- Custom Configuration Deployment
- Discovered Switch Errors
- Pre-deployment
- Undiscovered Switch Errors
- Wiring

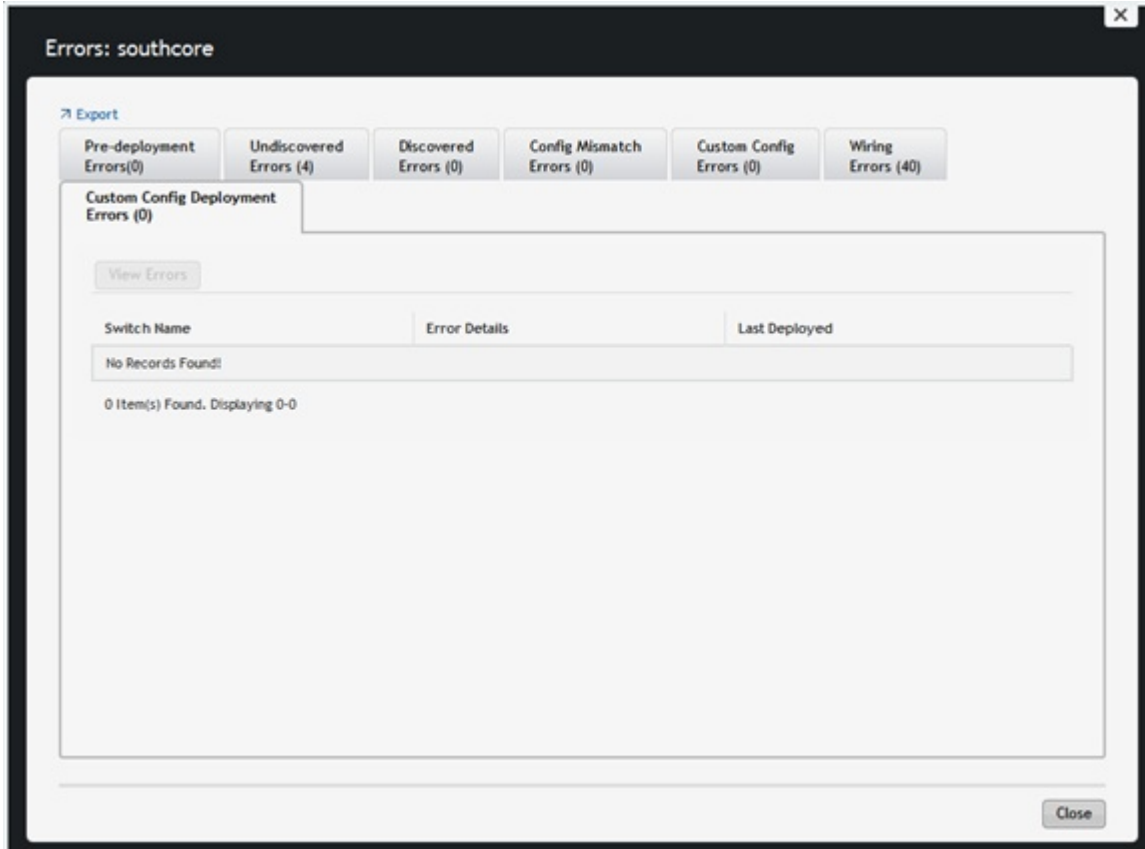


Figure 90. Validation Errors Screen

Table 60. Configuration Errors

| Error Details          | Recommended Action   |
|------------------------|--|
| Configuration Mismatch | <ol style="list-style-type: none"> <li>1. On the <b>Configure and Deploy</b> tab, select the switch.</li> <li>2. Click <b>Errors</b>.</li> <li>3. Click the <b>Config Errors Mismatch</b> tab.</li> <li>4. Click <b>View Mismatch</b>.</li> <li>5. Review the configuration mismatch and correct the configuration errors.</li> <li>6. Restart switch validation from the <b>Configure and Deploy</b> tab by selecting the switch from the list and from the <b>Deploy</b> drop-down menu, click <b>Deploy and Validate</b>. In the <b>Deploy and Validation</b> dialog box, click the <b>Validation</b> tab, select the switch and click <b>Validate Selected</b>.</li> </ol> |


 **NOTE:** To filter the wiring errors by type, click the drop-down **Tier** menu and select a switch type (Aggregation, Access, or all). Only the selected error types display.

Table 61. Wiring Errors

| Error Details   | Recommended Action  |
|-----------------|---|
| Wiring Mismatch | <ol style="list-style-type: none"> <li>1. Review the wiring plan.</li> <li>2. Wire the switch according to the wiring plan to fix the wiring mismatch.</li> </ol> |

| Error Details | Recommended Action   |
|---------------|--|
|               | <ol style="list-style-type: none"> <li>3. Validate the switch. <ol style="list-style-type: none"> <li>a. Navigate to the <b>Network</b> &gt; <i>Fabric Name</i> &gt; <b>Configure and Deploy</b> tab.</li> <li>b. From the <b>Deploy Fabric</b> drop-down menu, select <b>Deploy and Validate</b>.</li> <li>c. Click the <b>Validation</b> tab and then select the switches.</li> <li>d. Click <b>Validate Selected</b>.</li> </ol> </li> </ol>  |
| Missing Link  | <ol style="list-style-type: none"> <li>1. Review the wiring plan.</li> <li>2. Wire the switch according to the wiring plan to fix the missing link.</li> <li>3. Validate the switch. <ol style="list-style-type: none"> <li>a. Navigate to the <b>Network</b> &gt; <i>Fabric Name</i> &gt; <b>Configure and Deploy</b> tab.</li> <li>b. From the <b>Deploy Fabric</b> drop-down menu, select <b>Deploy and Validate</b>.</li> <li>c. Click the <b>Validation</b> tab and then select the switches.</li> <li>d. Click <b>Validate Selected</b>.</li> </ol> </li> </ol>                                |
| Partial Link  | <ol style="list-style-type: none"> <li>1. Verify that the switch is wired according to the wiring plan.</li> <li>2. Verify the connectivity on AFM from both switches in the link.</li> <li>3. Validate the switch. <ol style="list-style-type: none"> <li>a. Navigate to the <b>Network</b> &gt; <i>Fabric Name</i> &gt; <b>Configure and Deploy</b> tab.</li> <li>b. From the <b>Deploy Fabric</b> drop-down menu, select <b>Deploy and Validate</b>.</li> <li>c. Click the <b>Validation</b> tab and then select the switches.</li> <li>d. Click <b>Validate Selected</b>.</li> </ol> </li> </ol> |

**Table 62. Undiscovered Switch Error**

| Error Details             | Recommended Action  |
|---------------------------|---|
| Undiscovered Switch Error | <ol style="list-style-type: none"> <li>1. Verify that the IP address for the switch is valid.</li> <li>2. If necessary, correct the pre-deployment configuration.</li> <li>3. From the AFM server, verify connectivity to the switch.</li> <li>4. Verify that the switch is running the minimum required software.</li> <li>5. Validate the switch. <ol style="list-style-type: none"> <li>a. Navigate to the <b>Network</b> &gt; <i>Fabric Name</i> &gt; <b>Configure and Deploy</b> tab.</li> <li>b. From the <b>Deploy Fabric</b> drop-down menu, select <b>Deploy and Validate</b>.</li> <li>c. Click the <b>Validation</b> tab and select the switches.</li> <li>d. Click <b>Validate Selected</b>.</li> </ol> </li> </ol> |





**Table 63. Discovered Switch Error**



| Error Details               | Recommended Action   |
|-----------------------------|--|
| Disconnected                | <ol style="list-style-type: none"> <li>1. Verify connectivity from the AFM server to the switch.</li> <li>2. Verify that the switch is running the minimum required software.</li> <li>3. Validate the switch.               <ol style="list-style-type: none"> <li>a. Navigate to the <b>Network</b> &gt; <i>Fabric Name</i> &gt; <b>Configure and Deploy</b> tab.</li> <li>b. From the <b>Deploy Fabric</b> drop-down menu, select <b>Deploy and Validate</b>.</li> <li>c. Click the <b>Validation</b> tab and select the switches.</li> <li>d. Click <b>Validate Selected</b>.</li> </ol> </li> </ol>                                       |
| Switch Name Mismatch        | <ol style="list-style-type: none"> <li>1. Verify that the IP address to switch name mapping is correct in the pre-deployment configuration. If the pre-deployment configuration is updated, redeploy the switch.</li> <li>2. Validate the switch.               <ol style="list-style-type: none"> <li>a. Navigate to the <b>Network</b> &gt; <i>Fabric Name</i> &gt; <b>Configure and Deploy</b> tab.</li> <li>b. From the <b>Deploy Fabric</b> drop-down menu, select <b>Deploy and Validate</b>.</li> <li>c. Click the <b>Validation</b> tab and select the switches.</li> <li>d. Click <b>Validate Selected</b>.</li> </ol> </li> </ol>    |
| Switch Model Mismatch       | <ol style="list-style-type: none"> <li>1. Verify that the IP address to switch name mapping is correct in the pre-deployment configuration. If the pre-deployment configuration is updated, redeploy the switch.</li> <li>2. Validate the switch.               <ol style="list-style-type: none"> <li>a. Navigate to the <b>Network</b> &gt; <i>Fabric Name</i> &gt; <b>Configure and Deploy</b>.</li> <li>b. From the <b>Deploy Fabric</b> drop-down menu, select <b>Deploy and Validate</b>.</li> <li>c. Click the <b>Validation</b> tab and select the switches.</li> <li>d. Click <b>Validate Selected</b>.</li> </ol> </li> </ol>        |
| System MAC Address Mismatch | <ol style="list-style-type: none"> <li>1. Verify that the IP address to switch name mapping is correct in the pre-deployment configuration. If the pre-deployment configuration is updated, redeploy the switch.</li> <li>2. Validate the switch.               <ol style="list-style-type: none"> <li>a. Navigate to the <b>Network</b> &gt; <i>Fabric Name</i> &gt; <b>Configure and Deploy</b> screen.</li> <li>b. From the <b>Deploy Fabric</b> drop-down menu, select <b>Deploy and Validate</b>.</li> <li>c. Click the <b>Validation</b> tab and select the switches.</li> <li>d. Click <b>Validate Selected</b>.</li> </ol> </li> </ol> |
| License Mismatch            | <ol style="list-style-type: none"> <li>1. Verify that the designed and provided license ports count are same.</li> <li>2. Verify that you have a valid license file.</li> </ol>  |




| Error Details | Recommended Action  |
|---------------|---|
|               | 3. Verify that the license installation task is successful during deployment. |



## Switch Deployment Status Errors


Table 64. Switch Deployment Status Errors

| Switch Deployment Status         | Description  | Requires Action | Recommended Actions  |
|----------------------------------|--|-----------------|--|
| NOT STARTED                      | Not Started  | No              | <ol style="list-style-type: none"> <li>1. Start the switch deployment on the <b>Network &gt; Fabric Name &gt; Configure and Deploy</b> tab by selecting the switch from the list.</li> <li>2. From the <b>Deploy Fabric</b> drop-down menu, select <b>Deploy and Validate</b>.</li> <li>3. On the <b>Deploy</b> tab, select the switch and click <b>Deploy Selected</b>.</li> </ol> <p> <b>NOTE:</b> Verify that the switch is in BMP mode.</p>   |
| CONFIG GENERATION IN PROGRESS    | Configuration File Generation In-progress            | No              | Information only   |
| CONFIG GENERATION FAILED         | Configuration File Generation Failed                 | Yes             | <ol style="list-style-type: none"> <li>1. Check the write permission for the AFM installation directory on the AFM server.</li> <li>2. Verify that there is enough disk space on the AFM server.</li> <li>3. Restart switch deployment from the <b>Network &gt; Fabric Name &gt; Configure and Deploy</b> tab by selecting the switch from the list.</li> </ol> <p> <b>NOTE:</b> Verify that the switch is in BMP mode.</p> <ol style="list-style-type: none"> <li>4. From the <b>Deploy Fabric</b> drop-down menu, select <b>Deploy and Validate</b>.</li> <li>5. On the <b>Deploy</b> tab, select the switch and click <b>Deploy Selected</b>.</li> </ol> |
| CONFIG GENERATION SUCCESS        | Configuration File Generation Completed Successfully | No              | Information only   |
| CONFIG FILE TRANSFER IN PROGRESS | Configuration File Transfer In-progress              | No              | Information only   |

| Switch Deployment Status     | Description                                 | Requires Action | Recommended Actions   |
|------------------------------|---|-----------------|---|
| CONFIG FILE TRANSFER FAILED  | Configuration File Transfer Failed          | Yes             | <ol style="list-style-type: none"> <li>1. Verify the connectivity to the TFTP server from the AFM server.</li> <li>2. Restart switch deployment from the <b>Network &gt; Fabric Name &gt; Configure and Deploy</b> tab by selecting the switch from the list.<br/> <b>NOTE:</b> Verify that the switch is in BMP mode.</li> <li>3. From the <b>Deploy Fabric</b> drop-down menu, select <b>Deploy and Validate</b>.</li> <li>4. On the <b>Deploy</b> tab, select the switch and click <b>Deploy Selected</b>.</li> </ol> |
| CONFIG FILE TRANSFER SUCCESS | Configuration File Transferred Successfully | No              | Information only  |
| REQUEST TO DISCOVER NODE     | Request To Discover Switch                  | Yes             | <ol style="list-style-type: none"> <li>1. Power on the switch.</li> <li>2. Restart switch deployment from the <b>Network &gt; Fabric Name &gt; Configure and Deploy</b> tab by selecting the switch from the list.<br/> <b>NOTE:</b> Verify that the switch is in BMP mode.</li> <li>3. From the <b>Deploy Fabric</b> drop-down menu, select <b>Deploy and Validate</b>.</li> <li>4. On the <b>Deploy</b> tab, select the switch and click <b>Deploy Selected</b>.</li> </ol>  |
| MIN CONFIG UPLOAD INPROGRESS | Minimum Configuration Upload In-Progress    | No              | Information only  |
| MIN CONFIG UPLOAD ERROR      | Minimum Configuration Upload Error          | Yes             | <ol style="list-style-type: none"> <li>1. Verify the connectivity to the TFTP/FTP server from the switch.</li> <li>2. Resolve any errors the <b>Validation Status</b> column.</li> <li>3. Verify that the system MAC address in the <b>dhcpd.conf</b> file matches the <b>csv</b>. file with the MAC addresses of the switches.</li> <li>4. Verify that the <b>min.cfg</b> file is in the correct directory on the TFTP/FTP server.</li> <li>5. Redeploy the switch from the <b>Network &gt; Fabric Name &gt;</b></li> </ol>  |

| Switch Deployment Status          | Description                               | Requires Action | Recommended Actions   |
|-----------------------------------|---|-----------------|---|
|                                   |   |                 | <p><b>Configure and Deploy</b> tab by selecting the switch from the list.</p> <p> <b>NOTE:</b> Verify that the switch is in BMP mode.</p> <ol style="list-style-type: none"> <li>From the <b>Deploy Fabric</b> drop-down menu, select <b>Deploy and Validate</b>.</li> <li>On the <b>Deploy</b> tab, select the switch and click <b>Deploy Selected</b>.</li> </ol>  |
| MIN CONFIG UPLOAD COMPLETED       | Minimum Configuration Upload Successful   | No              | Information only  |
| INIT SOFT RELOAD                  | Initiated Soft Re-load on Switch          | No              | Information only  |
| INIT SOFT RELOAD ERROR            | Error During Soft Re-load on Switch       | Yes             | <ol style="list-style-type: none"> <li>Check the switch syslogs for a reload command failure.</li> <li>Resolve any errors.</li> <li>Restart switch deployment from the <b>Network &gt; Fabric Name &gt; Configure and Deploy</b> tab by selecting the switch from the list.</li> <li>From the <b>Deploy Fabric</b> drop-down menu, select <b>Deploy and Validate</b>.</li> <li>On the <b>Deploy</b> tab, select the switch and click <b>Deploy Selected</b>.</li> </ol> <p> <b>NOTE:</b> Verify that the switch is in BMP mode.</p>                                      |
| PROTOCOL CONFIG UPLOAD INPROGRESS | Protocol Configuration Upload In-Progress | No              | Information only  |
| PROTOCOL CONFIG UPLOAD ERROR      | Protocol Configuration Upload Error       | Yes             | <ol style="list-style-type: none"> <li>Verify the connectivity to the TFTP server from switch.</li> <li>Resolve any errors in the <b>Validation Status</b> column.</li> <li>Verify that the DHCP server is running.</li> <li>Verify that the CFG file is on the TFTP/FTP server and the switch can reach it using the <b>ping</b> command.</li> <li>Redeploy the switch.</li> </ol> <p> <b>NOTE:</b> Verify that the switch is not in BMP mode.</p> <ol style="list-style-type: none"> <li>Navigate to the <b>Network &gt; Fabric Name &gt; Configure and</b></li> </ol> |

| Switch Deployment Status              | Description   | Requires Action | Recommended Actions   |
|---------------------------------------|---|-----------------|---|
|                                       |   |                 | <p><b>Deploy</b> tab by selecting the switch from the list.</p> <ol style="list-style-type: none"> <li>From the <b>Deploy Fabric</b> drop-down menu, select <b>Deploy and Validate</b>.</li> <li>On the <b>Deploy</b> tab, select the switch and click <b>Deploy Selected</b>.</li> </ol>   |
| PROTOCOL CONFIG UPLOAD COMPLETED      | Protocol Configuration Upload Successful                  | No              | Information only  |
| DEVICE DEPLOYMENT SUCCESS             | Switch Deployment Successful                              | No              | Information only  |
| UPLINK CONFIG GENERATED               | Uplink Configuration Generated                            | No              | Information only  |
| UPLINK CONFIG UPLOAD IN PROGRESS      | Uplink Configuration Upload In-Progress                   | No              | Information only  |
| UPLINK CONFIG UPLOAD ERROR            | Uplink Configuration Upload Error                         | Yes             | <ol style="list-style-type: none"> <li>Verify the connectivity between AFM and the switch.</li> <li>Resolve any errors in the <b>Validation Status</b> column.</li> <li>Restart the deployment.</li> </ol> <p> <b>NOTE:</b> Verify that the switch is not in BMP mode.</p> <ol style="list-style-type: none"> <li>Navigate to the <b>Network &gt; Fabric Name &gt; Configure and Deploy</b> tab by selecting the switch from the list.</li> <li>From the <b>Deploy Fabric</b> drop-down menu, select <b>Deploy and Validate</b>.</li> <li>On the <b>Deploy</b> tab, select the switch and click <b>Deploy Selected</b>.</li> </ol> |
| UPLINK RECONFIGURED REDEPLOY REQUIRED | Uplink re-configured, Re-deployment of Switch is required | Yes             | <p>Restart switch deployment.</p> <p> <b>NOTE:</b> Verify that the switch is not in BMP mode.</p> <ol style="list-style-type: none"> <li>Navigate to the <b>Network &gt; Fabric Name &gt; Configure and Deploy</b> tab by selecting the switch from the list.</li> <li>From the <b>Deploy Fabric</b> drop-down menu, select <b>Deploy and Validate</b>.</li> <li>On the <b>Deploy</b> tab, select the switch and click <b>Deploy Selected</b>.</li> </ol>  |

| Switch Deployment Status | Description                             | Requires Action | Recommended Actions   |
|--------------------------|---|-----------------|---|
| REDEPLOYMENT REQUIRED    | Re-deployment of the switch is required | Yes             | <p>Restart switch deployment.</p> <p> <b>NOTE:</b> Verify that the switch is not in BMP mode.</p> <ol style="list-style-type: none"> <li>1. Navigate to <b>Network &gt; Fabric Name &gt; Configure and Deploy</b> tab by selecting the switch from the list.</li> <li>2. From the <b>Deploy Fabric</b> drop-down menu, select <b>Deploy and Validate</b>.</li> <li>3. On the <b>Deploy</b> tab, select the switch and click <b>Deploy Selected</b>.</li> </ol> |

## Deployment Task Errors

Table 65. Deployment Task Errors

| AFM Deployment Task                                 | Error Status                             | Recommended Action   |
|---|--|--|
| Verify switch eligibility                           | Eligibility check for deployment: Failed | Verify that the VLT switch deployment has a management IP for all peers.   |
| License installation task for Z9500 series switches | License upgrade: Failed                  | Verify that valid license file appears in pre-deployment for selected device.  |
| Ping verification                                   | Ping verification: Failed                | Verify that the DHCP offer was received on the device console. Power cycle if needed.  |
| Telnet/SSH connectivity verification                | Telnet/SSH session verification: Failed  | Verify Telnet/SSH connection and that the DHCP offer was received on the device console. Power cycle if needed.  |
| Reset to factory defaults                           | Reset to factory defaults task: Failed   | Verify Telnet/SSH connectivity and redeploy.   |
| Minimal configuration upload to switch              | Minimal config upload: Failed            | Verify Telnet/SSH connectivity and redeploy.   |
|   | Minimal config upload on Unit-1: Failed  | Verify Telnet/SSH connectivity and redeploy.   |
| Reload of switch                                    | Reboot of switch: Failed                 | Verify Telnet/SSH connectivity and redeploy.   |
| Boot image error                                    | Boot image was not loaded from flash     | <ol style="list-style-type: none"> <li>1. To change the boot image path to flash, enter CONFIG mode and use the following CLI command through console session: <code>no boot system stack-unit 0 primary tftp://10.16.148.24/FTOS-SE-9.5.0.0P3.bin</code></li> </ol> |

| AFM Deployment Task                 | Error Status   | Recommended Action   |
|-------------------------------------|--|--|
|                                     |  | 2. Enable BMP on the switch. <ul style="list-style-type: none"> <li>For S55 or S60, use the <code>reload-type jump-start config-download enable</code> command.</li> <li>For all other switch types, enter CONFIG mode and use the <code>reload-type bmp config-scr-download enable</code> command.</li> </ul> |
| Stack unit cleanup                  | Stack unit renumbering task: Failed  | Verify Telnet/SSH/SNMP connectivity.   |
| Upgrade standby                     | Upgrade standby: Failed  | The standby MAC was not found or reported a card problem. Verify that the standby switch is active.  |
| Full configuration file transfer    | Full config file transfer to TFTP/FTP server: Failed                                 | Verify the TFTP/FTP connectivity and FTP credentials.  |
| TFTP/FTP connectivity               | TFTP/FTP connection issue between switch and TFTP server                             | Verify TFTP/FTP connectivity from the switch to the TFTP server.   |
| Full configuration upload to switch | Full config upload: Failed   | Verify TFTP/FTP and Telnet/SSH connectivity and redeploy. Verify that optional modules are installed according to the fabric design. Verify that AFM is using the supported software version.  |
| Smart script transfer failed        | Smart script transfer: Failed  | Verify Telnet/SSH connectivity and redeploy.   |
| Wiring validation                   | Unable to validate Wiring  | Verify SNMP connectivity.  |
|                                     | Wiring Errors Exist  | To resolve the errors, review error details on the Errors screen.  |
| Merge configuration changes         | Apply configuration changes: Failed  | Verify Telnet/SSH connectivity and redeploy.   |
| Custom configuration upload         | Custom configuration upload: Failed  | Verify Telnet/SSH connectivity and redeploy.   |
| Backup running configuration        | Backup config: Failed  | Verify Telnet/SSH connectivity and redeploy.   |
| Deployment                          | Software image selected in pre-deploy wizard is not available in AFM image location. | Upload the software image as a superuser using the AFM Virtual Appliance: <ol style="list-style-type: none"> <li>Log in to the AFM server as a superuser.</li> <li>Select <b>Upload Switch Software Image</b>.</li> <li>Enter the number for the switch model.</li> </ol>                                      |

| AFM Deployment Task | Error Status | Recommended Action  |
|---------------------|--------------|---|
|                     |              | <ol style="list-style-type: none"> <li>4. Enter your user name and password for the FTP connection.</li> <li>5. Enter the URL location for the switch software image.</li> <li>6. Press Enter.</li> </ol> <p>For more information, refer to <i>Uploading Switch Software Images</i> in the <i>AFM Deployment Guide</i>.</p> |

## TFTP/FTP Errors

Table 66. Deployment Status Configuration Errors

| Deployment Status | Error Category                 | Error Details                  | Recommended Action  |
|-------------------|--------------------------------|--------------------------------|---|
| TFTP/FTP Failed   | Configuration Deployment Error | Error occurred during TFTP/FTP | <ol style="list-style-type: none"> <li>1. Check the TFTP/FTP connectivity on the network.</li> <li>2. Make sure that you have specified the correct TFTP/FTP address in the <b>Settings</b> tab of the <b>Administration</b> pane.</li> </ol> |

## Validating Connectivity to the ToR

1. Ping the ToRs from the leaf or access switches.
2. Confirm the VLAN configured on the leaf or access switch is the same on the port.



# Alerts and Events

This section contains the following topics:

- [Current – Active Alerts](#)
- [Historical – Alerts and Events](#)

## Current Active Alerts

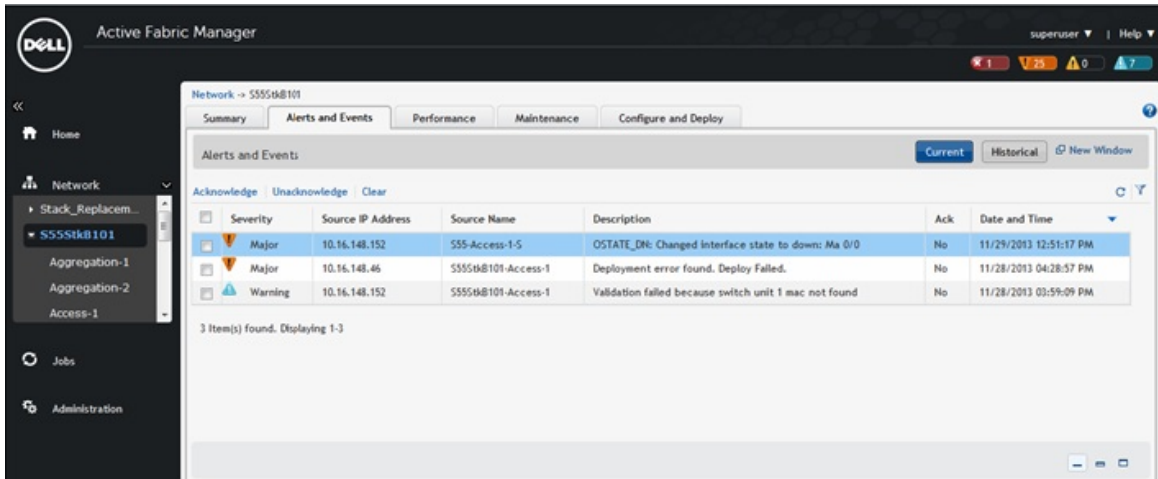
You can view active network, fabric, and switch alerts on the Current view of **Alerts and Events** tab. You can perform the following tasks on this tab:

- To display more information about the active alert, select the active alert. The system displays more information about the alert at the bottom of the screen.
- To filter active network alerts, from the menu, click **Network** and then click the **Alerts and Events** tab.

| Severity | Source IP Address | Source Name                     | Description  | Ack | Date and Time          |
|----------|-------------------|---------------------------------|--|-----|------------------------|
| Warning  | 10.16.148.291     | Aggregation-2                   | Stack_Replacement-Aggregation-2  | No  | 09:30:07 AM            |
| Warning  | 10.16.148.291     | Stack_Replacement-Aggregation-2 | Validation failed because TenGigabitEthernet 0/3 has a missing link round switch Stack_Replacement-Aggregation-2 | No  | 12/03/2013 09:30:07 AM |
| Warning  | 10.16.148.291     | Stack_Replacement-Aggregation-2 | Validation failed because TenGigabitEthernet 0/1 has a missing link round switch Stack_Replacement-Aggregation-2 | No  | 12/03/2013 09:30:07 AM |
| Major    | 10.16.148.44      | DCtest-Leaf-1                   | Deployment error found. Deploy Failed.   | No  | 12/02/2013 12:56:46 PM |
| Major    | 10.16.148.44      | DCtest-Leaf-4                   | Deployment error found. Deploy Failed.   | No  | 12/02/2013 12:56:46 PM |
| Major    | 10.16.148.44      | DCtest-Leaf-8                   | Deployment error found. Deploy Failed.   | No  | 12/02/2013 12:56:46 PM |

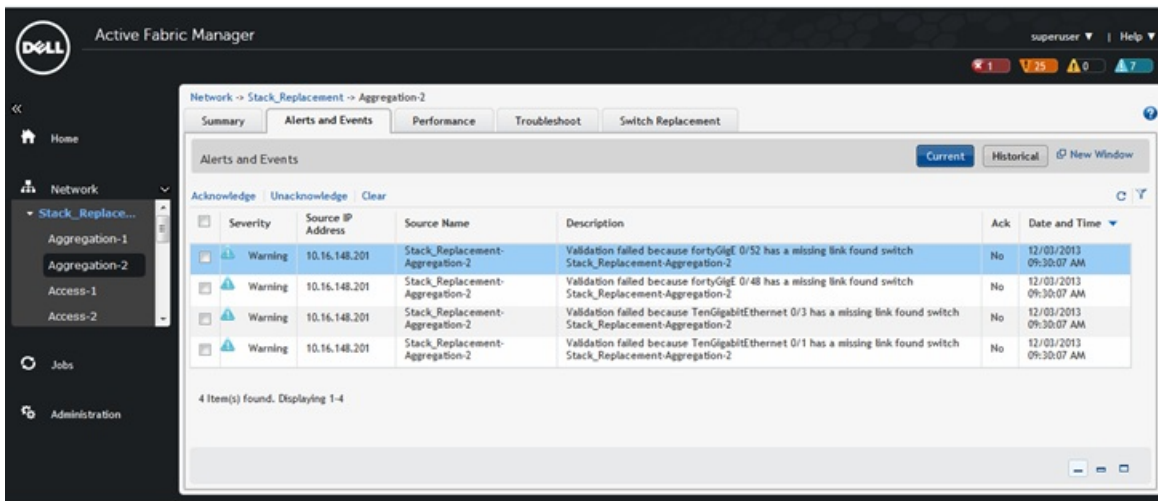
**Figure 91. Network Alerts**

- To filter active fabric alerts, from the menu, click **Network** > *Fabric Name* and then click the **Alerts and Events** tab.



**Figure 92. Fabric Alerts**

- To filter active switch alerts, click **Network** > *Fabric Name* > *Switch Name* and then click the **Alerts and Events** tab.



**Figure 93. Switch Alerts**

- To acknowledge an active alert, select the active alert and then click **Acknowledge**.
  - To dismiss an acknowledged alert, select the alert and then click **Unacknowledge**.
  - To dismiss an active alert, select the alert and then click **Clear**.
1. Click **Current**.
  2. Click the filtering icon on the right of the screen. To filter results, use the filter options: **from date** and **to date**.  
The filtering options appear.
  3. In the **Severity** drop-down menu, select one of the following filtering criteria:
    - All
    - Critical
    - Major
    - Minor
    - Warning

- **Cleared**
  - **Unknown**
  - **Info**
  - **Indeterminate**
4. In the **Source IP Address** field, enter the source IP address.
  5. In the **Source Name** field, enter the source name.
  6. In the **Description** field, enter a description.
  7. In the **Ack** (acknowledgement) drop-down menu, select one of the following options:
    - **All**
    - **Yes**
    - **No**
  8. Click **Apply**.

## Historical Alerts and Event History

On the **Alerts and Events** tab, you view historical events at the network, fabric, or switch level. You can access this tab by clicking **Network** on the menu.

- To filter active alerts at the network level, from the menu, click **Network** to view the **Alerts and Events** tab.
  - To filter active alerts at the fabric level, from the menu, click **Network** > *Fabric Name* to view the > **Alerts and Events** tab.
  - To filter active alerts at the switch level, from the menu, click **Network** > *Fabric Name* > *Switch Name* to view the **Alerts and Events** tab.
1. On the **Alerts and Events** tab, click **Historical**.
  2. Click the filtering icon.  
The filtering options appear.
  3. In the **Severity** drop-down menu, select one of the following filtering criteria:
    - **All**
    - **Critical**
    - **Major**
    - **Minor**
    - **Warning**
    - **Cleared**
    - **Unknown**
    - **Info**
    - **Indeterminate**
  4. In the **Source IP Address** field, enter the source IP address.
  5. In the **Source Name** field, enter the source name.
  6. In the **Description** field, enter a description.
  7. In the **Ack** (acknowledgement) drop-down menu, select one of the following options:
    - **All**
    - **Yes**
    - **No**
  8. In the **Date From** and **Date To** fields, enter a start and end date to filter alerts. You can also click the calendar icons to select dates.

9. Click **Apply**.

# Performance Management

This section contains the following topics:

- [Network Performance Management](#)
- [Fabric Performance Management](#)
- [Switch Performance Management](#)
- [Port Performance Management](#)
- [Detailed Port Performance Management](#)
- [TCA Threshold Setting](#)
- [Data Collection](#)
- [Reports](#)

## Network Performance Management

On the **Performance** tab, you can monitor the following network historical data for all the fabrics:

- Bandwidth utilization
- Top 25 port inbound usage
- Top 25 port outbound usage
- Top 10 highest CPU utilization
- Top 10 highest memory utilization

You access the **Performance** tab by clicking **Network** on the menu.

For information about the color codes for the historical data, refer to [Dashboard](#).

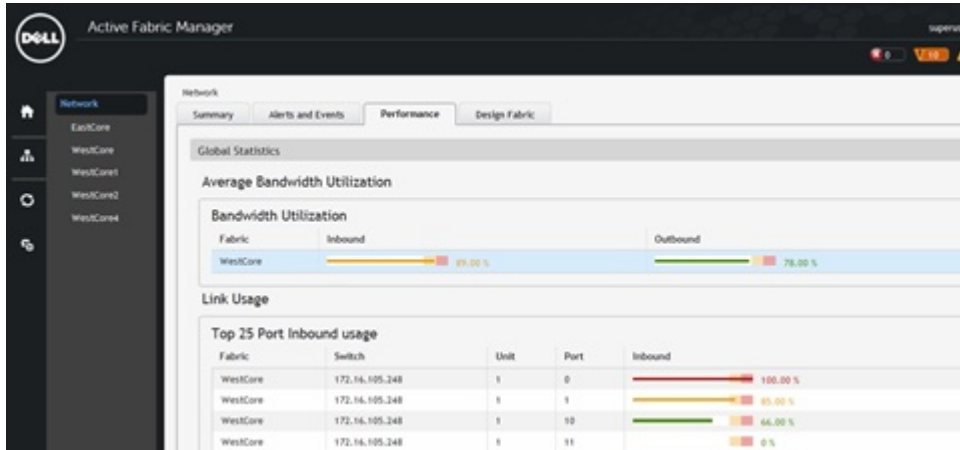


Figure 94. Global Statistics Screen of the Performance Tab

## Fabric Performance Management

On the **Performance** tab, you can monitor the following information for all the switches in the fabric:

- Bandwidth utilization
- Top 25 port inbound usage
- Top 25 port outbound usage
- Top 10 highest CPU utilization
- Top 10 high memory utilization

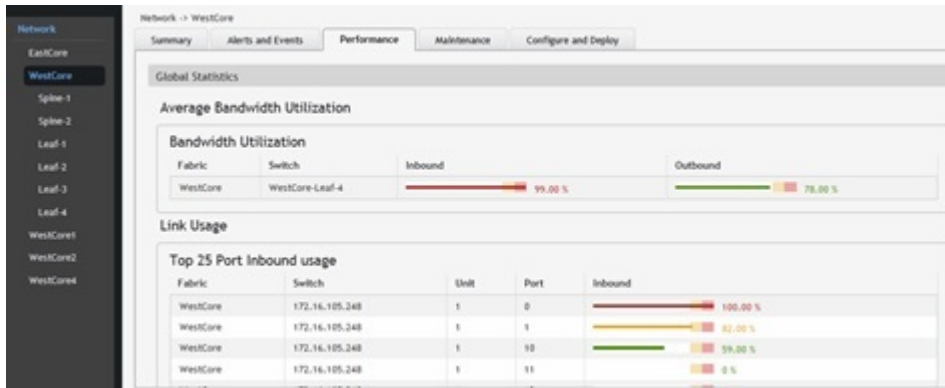


Figure 95. Fabric Statistics Screen – Performance Tab

You access the **Performance** tab by clicking **Network** > *Fabric Name* on the menu.

## Switch Performance Management

You can view historical and real-time data switch level performance on the **Performance** tab. To access this tab, from the menu, click **Network** > *Fabric Name* > *Switch Name*. By default, the historical view displays in tabular format. Monitor performance in graphical (chart, line, or bar) format in the **View Type** area or move to the real-time data monitoring from this screen.



**NOTE:** To view performance, enable data collection on the **Data Collections** tab, which is accessed by clicking **Jobs** from the menu.

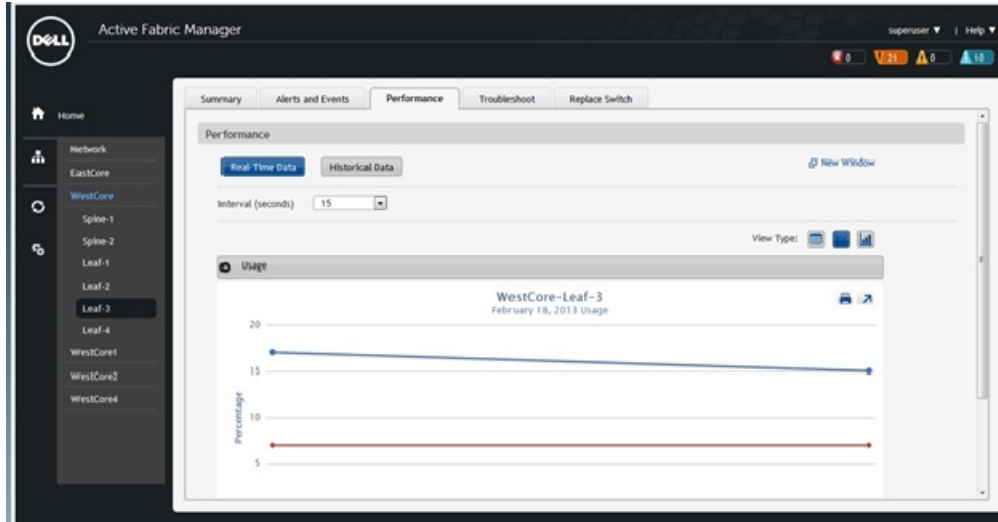


Figure 96. Switch Performance Tab

## Port Performance Management

1. From the menu, click **Network** > *Fabric Name* > *Switch Name* and then make sure that the **Summary** tab is selected.

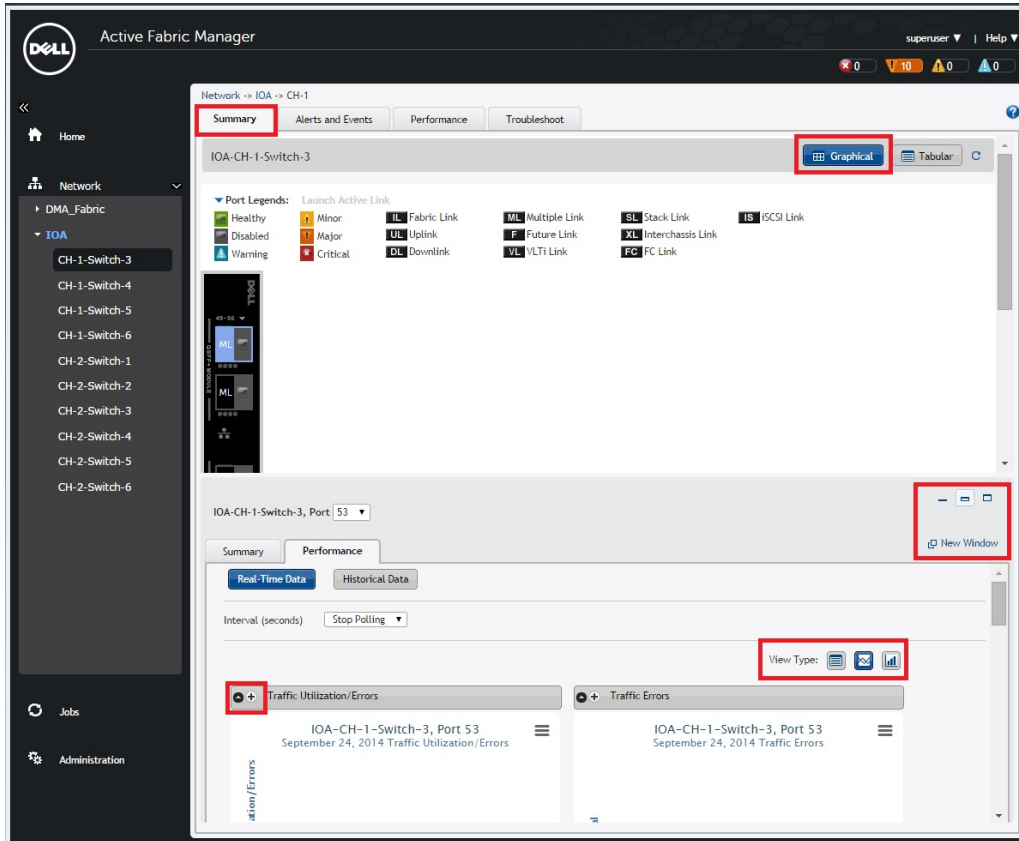


Figure 97. Summary and Performance Tabs with Port Performance Details

2. Select a port and then click the **Performance** tab.
3. Select a date type:
  - **Real-Time Data**
  - **Historical**
4. To display port performance, select one of the following **View Type** options:
  - **Bar**
  - **Graphical**
  - **Tabular**
5. Review the performance information.

## Detailed Port Performance Management

View the following information in a graphical (chart) or tabular format on the **Detailed Port Level Performance** screen:

- Traffic utilization
- Traffic errors
- Throughput
- Traffic in kbps
- Packets



For Power over Ethernet (PoE) ports, the following metrics are available:

- Power in Milliwatts
  - Voltage in volts
  - Current in MilliAmps
  - Temperature in celsius
1. From the menu, click **Network** > *Fabric Name* > *Switch Name* and then make sure that the **Summary** tab is selected.
  2. Click the **Performance** tab at the bottom of the screen.
  3. In the upper right of the screen, select the format for the data:
    - **Graphical**
    - **Tabular**
  4. Select a data option:
    - **Real-Time Data**
      - If you select real-time data, select the interval real-time data collection (in seconds) from the **Interval (seconds)** drop-down menu:
        - \* **15**
        - \* **30**
        - \* **45**
        - \* **60**
    - **Historical Data**
      - If you select historical data, select one of the following options from the **Date Range** drop-down menu:
        - \* **Last 12 hours**
        - \* **Last 24 hours**
        - \* **Last 7 days**
        - \* **Last 30 days**
        - \* **Custom Date Range** — Enter start and end dates

## Data Collection

By default, AFM automatically enables data collection after deployment. To disable data collection for a fabric:

1. From the **Jobs** menu, click the **Data Collections** tab.
2. Click **Schedule Data Collection**.  
The **Edit Data Collection** window appears.
3. To disable data collection for a specific fabric, clear the check box for the fabric.  
The **Polling Rate** is 15 minutes.
4. Click **OK**.

## Threshold Settings

You can configure the monitoring link bundle and Threshold Crossing Alert (TCA) between the spine switches and the leaf switches. You can access these settings by clicking **Jobs** on the menu and then

clicking the **Data Collections** tab. Next, click **Edit Threshold Settings**. The **Average Traffic Threshold** option monitors the Layer 3 fabric link bundle. The **TCA Bandwidth** option monitors low bandwidth and high bandwidth for Layer 2 and Layer 3 fabrics.

If the average traffic or both utilization thresholds are exceeded, AFM receives an alarm from the switch on the **Alerts and Events** tab.

| Fabric Name | Average Traffic Threshold | TCA Bandwidth             |                            | Job ID |
|-------------|---------------------------|---------------------------|----------------------------|--------|
|             |                           | Low Utilization Threshold | High Utilization Threshold |        |
| southcore   | 60 %                      | 60 %                      | 80 %                       |        |
| westcore    | 70 %                      | 50 %                      | 70 %                       |        |
| northcore   | 80 %                      | 60 %                      | 80 %                       |        |

**Figure 98. TCA Bandwidth**

- **Average Traffic Threshold** – Configure the threshold for a Layer 3 fabric. The range is 60–90 percent. The monitoring value applies only to the fabric link between the spine and leaf switches.
- **Low Utilization Threshold** – Configure the value for TCA. The range is 40–60 percent. If AFM exceeds this value, the graphical performance monitoring displays a solid red line labeled **Traffic Utilization Alert Threshold**. AFM clears the alarm and removes the red line when traffic is within the specified values.
- **High Utilization Threshold** – Sets the highest value for TCA. The range is 60–80 percent. If AFM exceeds this value, the graphical performance monitoring displays a solid red line labeled **Traffic Utilization Alert Threshold**. AFM clears the alarm and removes the red line when traffic is within the specified values.
- **Job ID** – AFM creates a job ID when you create the schedule.

Using real-time performance management at the port level, AFM displays a solid red line appears on the threshold label **Traffic Utilization Alert Threshold** when traffic exceeds the TCA.

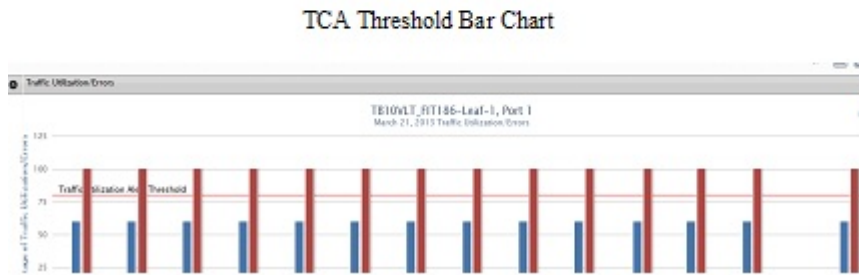
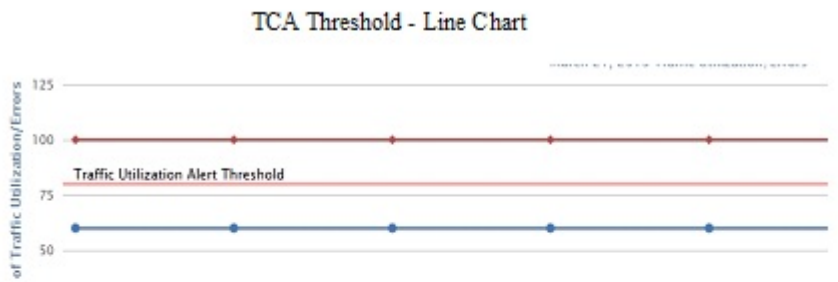



Figure 99. Traffic Utilization Alert Threshold

For information about how to view port performance, refer to [Detailed Port Performance Management](#). Select the **Real-Time Data** option.

## Reports

This section contains the following topics:

- [Creating New Reports](#)
- [Editing Reports](#)
- [Running Reports](#)
- [Deleting Reports](#)
- [Duplicating Reports](#)

 **NOTE:** To run a report, schedule data collection. Refer to [Data Collection](#).

### Creating New Reports

1. From the menu, click **Jobs** and then click the **Reports** tab.
2. Click **New Report**.  
The **Add/Modify Report** window appears.
3. In the **Report Name** field, enter a name for the report.
4. (Optional) In the **Description** field, enter a description for the report.
5. Click **Next**.
6. In the **Report Type** area, select a report type:
  - **Switch**
  - **Port**

7. In the **Output Format** area, select a report output format:
  - **Tabular**
  - **Chart**
8. Click **Next**.
9. In the **Monitors** field, select the monitors to use for the report and click the **>>** button. The monitors that you can select depend on whether you selected **Switch** or **Port**.

Switches:

  - **CpuUtilization** (CPU utilization)
  - **MemUtilization** (memory utilization)

Ports:

  - **InTrafficErrors**
  - **InTrafficUnicastPkts**
  - **InTrafficMulticastPkts**
  - **InTrafficBroadcastPkts**
  - **InTrafficUtilization**
  - **OutTrafficErrors**
  - **OutTrafficUnicastPkts**
  - **OutTrafficMulticastPkts**
  - **OutTrafficBroadcastPkts**
  - **OutTrafficUtilization**
  - **OutputThroughput**
  - **OutErrorRate**
  - **InTrafficInKbps**
  - **InputThroughput**
  - **InErrorRate**
  - **OutTrafficInKbps**
  - **PowerOutput**
  - **CurrentOutput**
  - **VoltageOutput**
  - **Temperature**
10. Click **Next**.
11. In the **Available** area, select the core to query from the first drop-down menu.
12. Select the switch type from the second drop-down menu.
13. In the **Available Switches/Ports** area, select the nodes for the report and click the **>>** button.
14. Click **Next**.
15. In the **Date/Time Range** drop-down menu, select a date or time range using one of the following options.
  - **30 days**
  - **7 days**
  - **12 hours**
  - **24 hours**
  - **Custom Range**



**NOTE:** If you select a custom range, specify a start and end date.

16. Click **Next**.
17. On the **Summary** screen, review the report settings.
18. To run the report now, check the **Run Report Now** check box.
19. Click **Finish**.

## Editing Reports

1. From the menu, click **Jobs** and then click the **Reports** tab.
2. Select the report.
3. Click **Edit**.  
The **Add/Modify Report** window appears.
4. Edit the report.
5. To navigate to different parts of the report, click **Next**.
6. In the **Summary** area, review the changes.
7. Click **Finish**.

## Running Reports

Before running a report, schedule the data collection. For information on scheduling data collection, refer to [Data Collection](#).

1. From the menu, click **Jobs** and then click the **Reports** tab.
2. Select the report.
3. Click **Run**.

## Duplicating Reports

1. From the menu, click **Jobs** and then click the **Reports** tab.
2. Select a report.
3. Click **Duplicate**.  
The **Add/Modify Report** window appears.
4. In the **Report Name** field, enter a name for the report.
5. (Optional) In the **Description** field, enter a description.
6. Modify the report as needed.
7. To navigate to different parts of the report, click **Next**.
8. Click **Finish**.

## Deleting Reports

1. From the menu, click **Jobs** and then click the **Reports** tab.
2. Select the report.
3. Click **Delete**.  
A confirmation dialog box appears.
4. Click **Yes**.

# Maintenance

This section discusses maintenance tasks for Active Fabric Manager.

## Using the AFM Virtual Appliance

After you have deployed and configured AFM VM, use the AFM Virtual Appliance to perform the following tasks:

- Configure the system
- Change the AFM superuser password
- Update the AFM server
- Set AFM software to the next reboot
- Restart AFM Application
- Reboot the AFM server
- Shutdown AFM Server Transfer File
- Edit files
- Upload switch software images
- Back up the AFM database
- Restore the AFM database
- Log out

To access the AFM virtual appliance, go to the AFM VM, click the **Console** button, and login as `superuser`. The first time you log in from the console or SSH using `superuser`, if there is an IP assigned to the VM, AFM prompts you to change the password for `superuser`. This password is used for both the web URL login and console login. If no IP is assigned to the VM (which means that the DHCP is not enabled), AFM prompts you to configure the network. After you configure the network, the VM reboots.

The AFM virtual appliance options are shown in the following screen shot.

```
Active Fabric Manager (AFM) VIRTUAL APPLIANCE

AFM Portal:
  https://192.168.44.129/index.html

Use the <UP> and <DOWN> arrow keys to select an option:

  Configure System
  Change AFM superuser Password
  Update AFM Server
  Set AFM Software to Next Reboot
  Restart AFM Application
  Reboot AFM Server
  Shutdown AFM Server
  Transfer File
  Edit File
  Upload Switch Software Image
  Backup Database
  Restore Database
  Log out
  Press <Enter> to continue.
```

Figure 100. AFM Virtual Appliance Options Screen

## Configuring the System

To configure the AFM server settings, use the **Configure System** option.

- **Device configuration** (Network Configuration) — Use this option to configure a static IP as the AFM Ethernet controller or change another device's eth0 attribute.
  - **DNS configuration** — Use this option to configure the AFM DNS settings.
1. Select **Configure System** and press **Enter**.  
The following network configuration warning message appears: \*WARNING\* System will have to restart to properly update all the service if network configuration is changed. Do you wish to continue?
  2. Enter Y to continue.  
The **Select Action** screen appears.

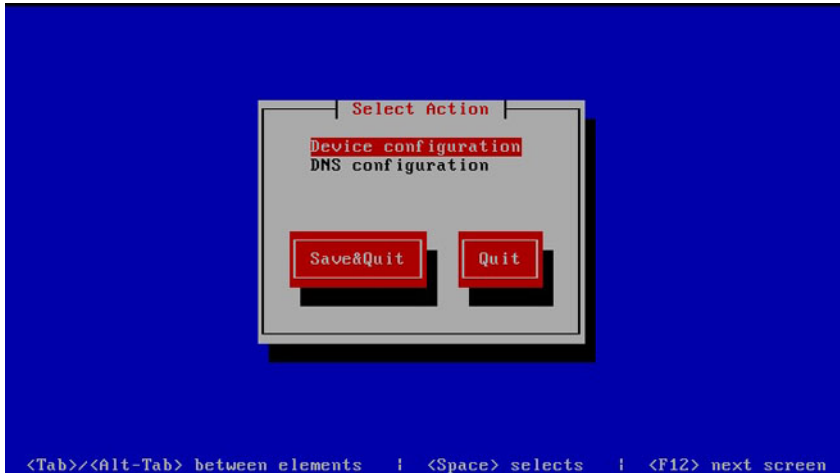


Figure 101. Select Action Screen

3. Select **Device configuration**. To navigate between elements, use the **Tab** and down arrow keys. The **Network Configuration** screen appears.

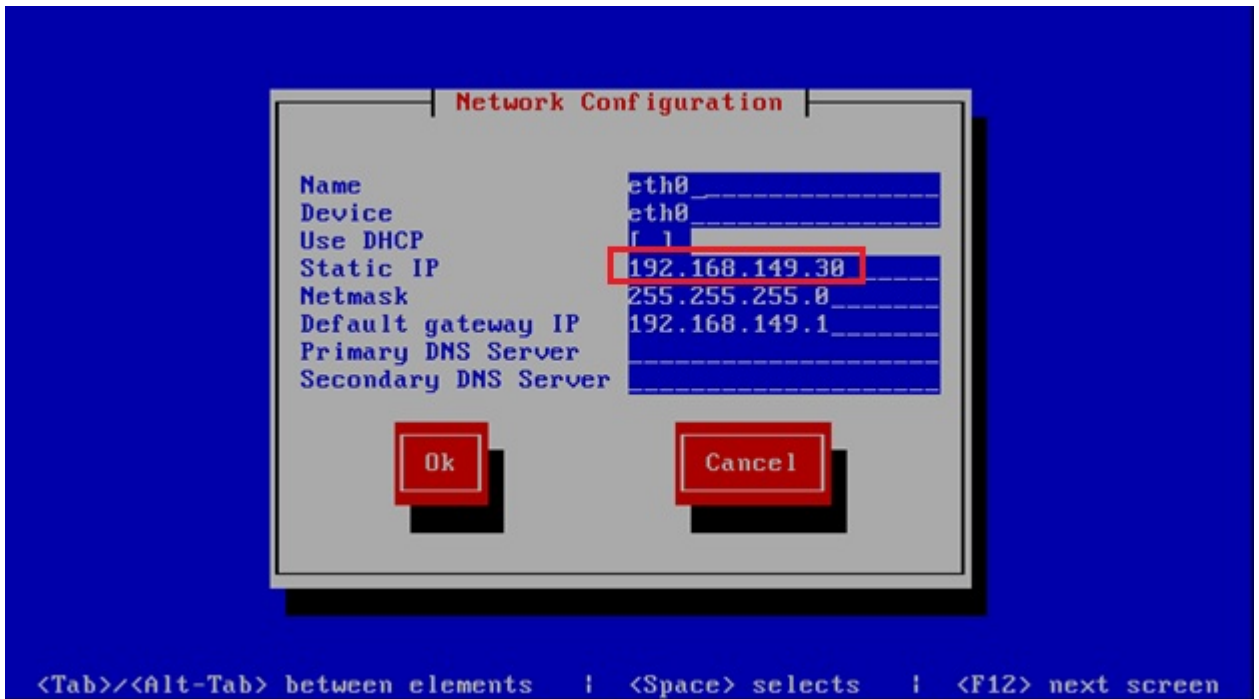


Figure 102. Network Configuration Settings Screen

4. View or modify the following settings as needed:
  - **Name** – Displays the name of AFM Server.
    - ✎ **NOTE:** Do not change the default device name (eth0).
  - **Device** – Displays the NIC Card.
    - ✎ **NOTE:** Do not change the default device name (eth0).



- **Use DHCP** – Allow DHCP to assign an IP address to the VM.
  - **Static IP** – Specify the static IP Address of the AFM server.
    - ✎ **NOTE:** To verify connectivity, ping the IP address assigned to the AFM. If the destination host is unreachable, assign the same IP address.
  - **Netmask** – Specify the subnet mask of the static IP address for the AFM Server.
  - **Default gateway IP** – Specify the gateway IP Address of the AFM server.
  - **Primary DNS Server** – Specify the primary DNS server address. To enable the DNS server on AFM Server, use this option.
  - **Secondary DNS Server** – Specify the secondary DNS server address.
5. Select **OK** to save your changes.
  6. Select **Quit** to exit this screen.

## Configuring DNS Settings

1. Select the **Configure System** option.
2. Select the **DNS configuration** option.  
To navigate between elements, use the **Tab** and down arrow.
3. Modify the following settings as needed:

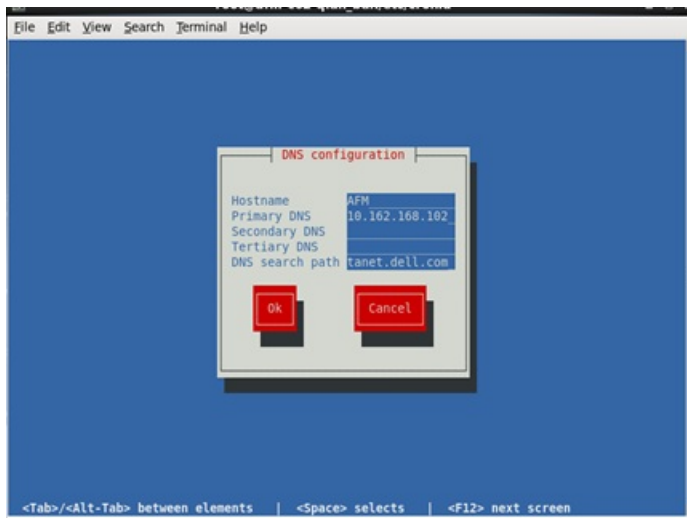


Figure 103. DNS Configuration Screen

- **Hostname** – Configure the host name for the AFM server.
  - **Primary DNS** – Configure the primary DNS.
  - **Secondary DNS** – (Optional) Configure the secondary DNS.
  - **Tertiary DNS** – (Optional) Configure the tertiary DNS.
  - **DNS search path** – Configure the DNS search path.
4. To save your changes, select the **OK**.
  5. To exit this screen, select **Quit**.

## Changing the AFM Superuser Password

1. Select **Change AFM Superuser Password** option.
2. Press **Enter**.  
The **CHANGE AFM SUPERUSER PASSWORD** screen appears.

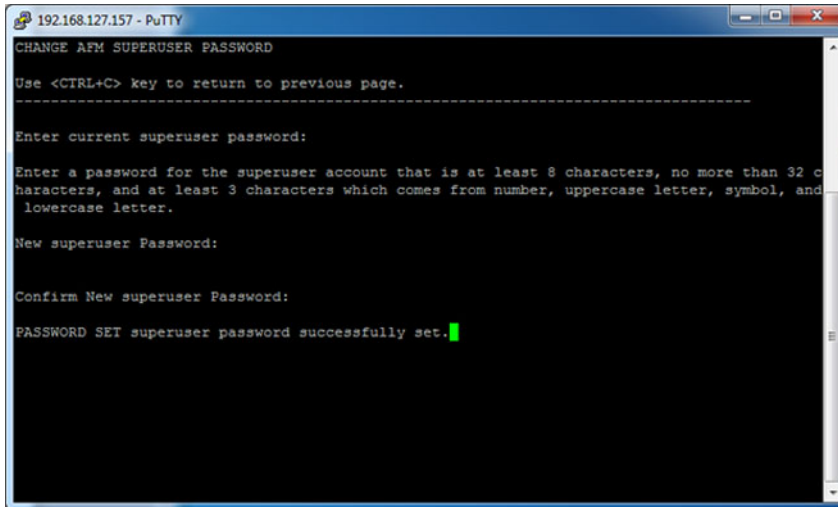



Figure 104. Change AFM Superuser Password

3. In the **Enter current superuser password** field, enter the superuser password (for example, **Superuser1**).  
 **NOTE:** The password must have 8–32 characters and include at least three of the following character types:
  - lowercase alphabetic character
  - uppercase alphabetic character
  - numeric character (0-9)
  - special character
4. Press **Enter**.
5. In the **Confirm New Superuser Password** field, enter the new superuser password again to confirm the superuser password.
6. Press **Enter** to return to the main menu.

## Updating the AFM Server

1. Select **Update AFM Server** and press **Enter**.  
The **UPDATE AFM Server** screen displays the current software version and any available version updates. The following message appears: The download file will overwrite the available software. Do you want to download RPM file from the Remote Server?
2. Choose one of the following:
  - To download the latest AFM software package in RPM format from a remote URL to the available partition, enter **Y**.
  - To download the AFM software package as an RPM formatted file from the local workstation (where the AFM console is launched) to the AFM server, enter **N**.

3. If the location is a remote server, enter the URL location of the RPM file on the remote server using the following formats and click **Enter**:
  - **https**://*ipaddress/path\_to\_rpm.file*
  - **ftp**://*ipaddress/path\_to\_rpm.file*
  - **sftp**://*ipaddress/path\_to\_rpm.file*
4. If the location is local, enter the absolute path of the RPM file and then click **Enter**.
5. If necessary, enter your user name and password.
6. Press **Enter** to return to the main menu.

 **NOTE:**

To use the new RPM on the active partition, set the AFM software to the next reboot and then restart AFM.

## Setting the AFM Software to the Next Restart

There are two versions of the AFM software package: one in the current partition and the other in the available partition.

1. Select **Set AFM Software to Next Restart** and press **Enter**.
2. Enter *y* and then press **Enter** to apply the available update on the next reboot.
3. Press **Enter** to return to the main menu.

## Restarting AFM


1. Select **Restart AFM Application** and press **Enter**.

The **Restart AFM Application** displays the following query: The next software version is AFM#-#-#-# from current software. Are you sure you want to restart AFM application? (where # is the software version).
2. To restart the application, enter *y*.
3. Press **Enter** to return to the main menu.

## Rebooting the AFM Server (VM)

1. Select **Reboot AFM Server** and press **Enter**.
2. To reboot the AFM server VM, enter *y*.
3. Select **Shutdown AFM Server** and press **Enter**.
4. To shut down the AFM server VM, enter *y*.

## Transferring Files

 **NOTE:** FTP or TFTP is configured during the initial AFM server configuration.

1. Select **Transfer File**.

```
Transfer File
Use <CTRL+C> key to return to previous page.
-----
---

Available File types for transfer:

1. Syslog
2. AFM Database Backup
3. AFM Configuration and Database Backup
4. AFM Performance Database Backup

Enter File Type for Transfer(1 or 2 or 3 or 4): _
```

Figure 105. Transfer Files

2. Press **Enter**.
3. Enter the file type to transfer:
  - **1. Syslog**
  - **2. AFM Database Backup**
  - **3. AFM Configuration and Database Backup**
  - **4. AFM Performance Database Backup**
4. Press **Enter**.
5. To upload all the files to the FTP or TFTP server, click **y**.
6. Press **Enter**.
7. Press **Enter** to return to the main menu.

## Editing AFM Files

You can edit the following types of files using the **Edit File** option:

- **1. logback.xml** — The **logback.xml** file contains the database logging file and enables or disables debugging. By default, the logging level is set to **INFO**. The logging levels are as follows: **ALL**, **DEBUG**, **ERROR**, **INFO**, **OFF**, **TRACE**, or **WARN**.

The typical use case is change the logging level from **INFO** to **DEBUG**,

```
<logger name="com.dell.indigo" level="INFO" /> change to <logger
name="com.dell.indigo" level=" DEBUG" />
<logger name="com.dell.dfm" level=" INFO " /> changed to <logger
name="com.dell.dfm" level="DEBUG" />
<logger name="com.dell.wnm" level=" INFO " /> changed to <logger
name="com.dell.wnm" level="DEBUG" />
```

- **2. config.properties** — The **config.properties** file contains the system level configuration for the database backup.

1. Select **Edit File**.
2. Enter the edit file option **1** to select the **1.logback.xml** option.

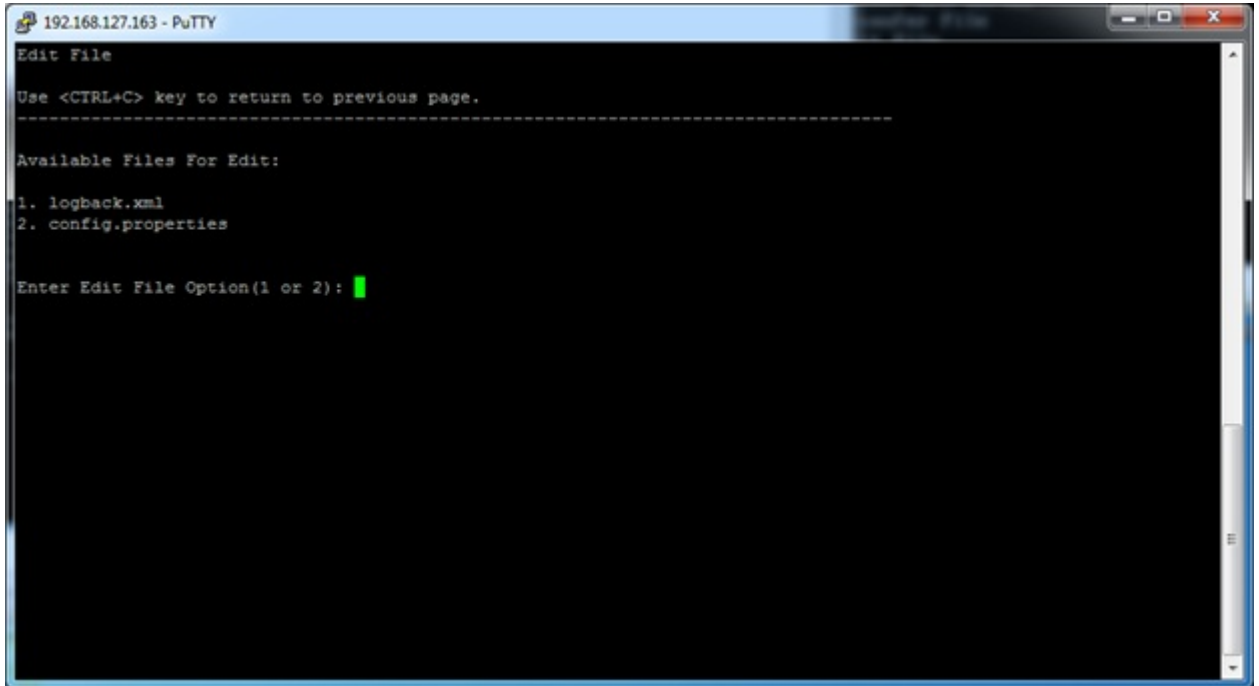


Figure 106. Edit AFM File System

3. Press **Enter**.
4. Search for `com.dell.dfm` and `com.dell.wnm`. Change the logging level from `level=INFO` to `level=DEBUG`.

For example:

```
<logger name="com.dell.dfm" level="DEBUG">
    <appender-ref ref="DCM-MESSAGE" />
    <!-- appender-ref ref="DCM-ERROR" />
    <appender-ref ref="DCM-TRACE" /-->
</logger>
<logger name="com.dell.wnm" level="DEBUG">
    <appender-ref ref="WNM-MESSAGE" />
    <!-- appender-ref ref="WNM-ERROR" />
    <appender-ref ref="WNM-TRACE" /-->
</logger>
```

5. Save the file using the **vi** editor commands such as **:w** (save file) and quit **:q**: (quit editing).
6. Press **Enter** to return to the main menu.

## Editing the config.properties AFM System File

1. Select **Edit File**.
2. Enter the edit file option **2** and then select the **2. config.properties** option.

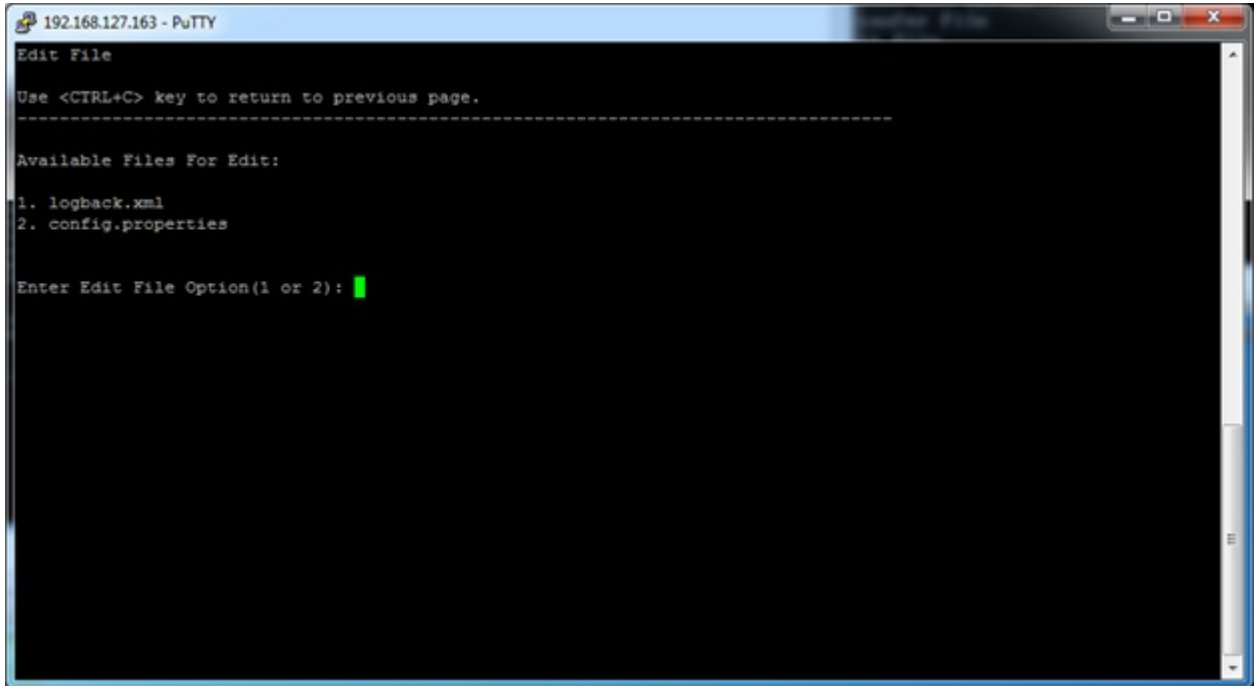


Figure 107. Edit AFM File System

3. Press **Enter**.
4. To change the time, search for **2am** or **1am**. You can change **2am** to **3am** for backup Postgres DB or change it from **1am** to **4am** for the HBase.

For example:

```
# The folder to store backed up database files. If the folder does not
exist, the backup program will try to create it
wnm.database.backup.folder=/data/backup/postgres
# The backup job will be started every day at 2am.
wnm.database.backup.schedule=0 0 2am * * ?
# ***** Database parameter : END *****
# ***** HBASE parameter : Start *****
# The folder to store backed up database files. If the folder does not
exist, the backup program will try to create it
wnm.database.hbase.backup.folder=/data/backup/hbase
#The backup job will be started every day at 1am.
wnm.database.hbase.backup.schedule=0 0 1am * * ?
```

Save the file using the **vi** editor commands such as **:w** (save file) and quit **:q**: (quit editing).

5. Press the **Enter** button to return to the main menu.

## Uploading Switch Software Images

To upload a new switch software image to the AFM local FTP/TFTP server from a remote URL, use the **Upload Switch Software Image** option.

1. Select the **Upload Switch Software Image** option and press the **Enter** button.  
The **Upload Switch Software Image** screen appears.

```
UPLOAD Switch Software Image

Use <CTRL+C> key to return to previous page.
-----
---

Choose a switch model:

1. MXL Blade
2. S4810
3. S4820T
4. S55
5. S60
6. Z9000
7. S6000
8. S5000
9. IOA

Enter switch model option (1, 2, 3, 4, 5, 6, 7, 8 or 9): █
```

Figure 108. AFM Virtual Appliance Upload Switch Software Image Screen

2. Enter a switch model option. The range is 1–9.
  - 1. MXL Blade
  - 2. S4810
  - 3. S4820T
  - 4. S55
  - 5. S60
  - 6. Z9000
  - 7. S6000
  - 8. S5000
  - 9. IOA

For FTP, enter your user name and password. This option transfers the Dell Networking OS image file into the `/data/FTOS/<SwitchModel>` directory and copies the files to the TFTP/FTP location.

3. To upload the switch software image using the formats listed in the **Upload Switch Software Image** screen, enter the URL location.
4. To return to the main menu, press **Enter**.

## Backing up the AFM Database


### NOTE:

- The backup file does not include AFM historical performance data.
- The AFM server IP must be the same as the location of the database backup file.


#### 1. Select **Backup Database**.

The **Backup Configuration and Database** screen appears.

#### 2. Select a backup option:

 **NOTE:** If AFM uses the local DHCP server and/or a local FTP server, select **AFM Configuration and Database** to back up the database instead of **AFM Database**.

- **1. AFM Database** — Back up the AFM database files only. The switch configuration and `dhcpd.conf` files are not included.
- **2. AFM Configuration and Database** — Back up the AFM configuration and database files.

 **NOTE:** The backup file extensions are type-specific. You cannot restore the AFM database files using the **2. AFM Performance Database** or **3. AFM Configuration and Database** options. Use the **1. AFM Database** option. Similarly, you cannot restore configuration files using the **1. AFM Database** option.

#### 3. Wait while AFM backs up the files.

The backup location is displayed at the bottom of the screen.

```
pg_dump: dumping contents of table wnm_seededipaddr
pg_dump: dumping contents of table wnm_slot
pg_dump: dumping contents of table wnm_stackport
pg_dump: dumping contents of table wnm_swmodule
pg_dump: dumping contents of table wnm_unit
pg_dump: dumping contents of table wnm_vlan
pg_dump: dumping contents of table wnm_vltdomain
pg_dump: dumping contents of table wnm_vltmember
pg_dump: dumping contents of table wnm_vltpeerlag
pg_dump: dumping contents of table wnm_vrrpoperation

Database backup created: /data/backup/postgres/afm-db-backup-2014_06_04-04_32_27.custom

Backup completed. Press <Enter> to return main menu.
```

Figure 109. Backup Location on AFM Virtual Appliance Screen

## Restoring the Database

### NOTE:

- AFM historical performance data is not included in the database file.
- The AFM server IP must be the same as the location of the database backup file.
- Restoring backup files overwrites all existing data.

#### 1. Select **Restore Database**.

The **RESTORE DATABASE** screen appears.



```
RESTORE CONFIGURATION AND DATABASE
Use <CTRL+C> key to return to previous page.
-----
Choose option for restore:

1. AFM Database
2. AFM Performance Database
3. AFM Configuration and Database

Enter restore option (1, 2 or 3): 1
Choose option to restore file from:

1. Default backup file location
2. User specified location


Enter database option (1 or 2): 1

AFM DATABASE FILES
Use <CTRL+C> key to return to previous page.
-----
1. afm-db-backup-2014_06_04-02_00_00_106.custom Wed Jun  4 02:00:00 2014      308.43 KB
2. afm-db-backup-2014_06_03-14_21_53.custom   Tue Jun  3 14:29:52 2014      305.43 KB

Choose AFM database file option: 1
```

Figure 110. Restore Configuration and Database Screen

2. Select a restoration option:

 **NOTE:** The backup file extensions are type-specific. You cannot restore the AFM database files using the **2. AFM Performance Database** or **3. AFM Configuration and Database** options. Use the **1. AFM Database** option. Similarly, you cannot restore configuration files using the **1. AFM Database** option.

- **1. AFM Database** — Restore the AFM database files only.
  - **2. AFM Performance Database** — Restore the AFM historical performance files only.
  - **3. AFM Configuration and Database** — Restore the AFM configuration and database files.
3. Specify the location of the backup file:
    - **1. Default backup file location** — Displays a list of database files available in the default backup file location.
    - **2. User specified location** — Select a specific location for the database file.
  4. Select the backup file:
    - If you selected **1. Default backup file location** in the previous step, enter the number of the backup file to restore.
    - If you selected **2. User specified location** in the previous step, type the complete file path of the backup file location.
  5. To restore the database and restart AFM, enter **Y**.

## Logging Out of the AFM Virtual Appliance

1. Select the **Log out** option.
2. Press the **Enter** button.


## Backing Up a Switch

On the **Back Up Switch** view of the **Maintenance** tab, you can schedule the number of days to keep switch backup files, view the fabric, switch name, software version that the switch is running, the startup configuration, running configuration, backup time, and description of the backup configuration.

This screen has the following options:

- [Backup Switch](#) — Schedule a backup for a switch's running configuration and startup configuration files now or later.
- [Edit Description](#) — Edit the description of the backup. This option is only available for existing backups.
- [Restore](#) — Restore the startup configuration (default) or running configuration from a backup.
- [Delete](#) — Delete a backup configuration.

## Restoring a Switch Configuration

 **NOTE:** AFM only supports startup configuration restoration for an IOA blade switch.

1. From the menu, click **Network** > *Fabric Name* and then click the **Maintenance** tab.
2. To display the switch backup options, click **Backup Switch**.
3. Select a backup switch configuration for restoration.
4. Click **Restore**.
5. Select one of the following restoration options:
  - **Restore Startup Config (default)**
  - **Restore Running Config**
6. Click **OK**.

## Deleting a Backup Configuration

1. From the menu, click **Network** > *Fabric Name* and then click the **Maintenance** tab.
2. To display the switch backup options, click **Backup Switch**.
3. Select a backup switch configuration for deletion.
4. Click **Delete**.
5. Click **Yes**.

## Editing a Description

1. From the menu, click **Network** > *Fabric Name* and then click the **Maintenance** tab.
2. To display the switch backup options, click **Backup Switch**.
3. Select a backup switch configuration.
4. Click **Edit Description**.
5. Edit the description.
6. Click **OK**.

# Viewing and Editing the Switch Backup Configuration

You can use AFM to edit the running or startup configuration on deployed devices. The edited configuration is available after you restore the switch backup configuration.

1. From the menu, click **Network** > *Fabric Name* and then click the **Maintenance** tab.
2. Click **Backup Switch** in the upper right of the screen and then click **View/Edit**.

The **View and Edit Switch Backup Screen Configuration** screen appears.

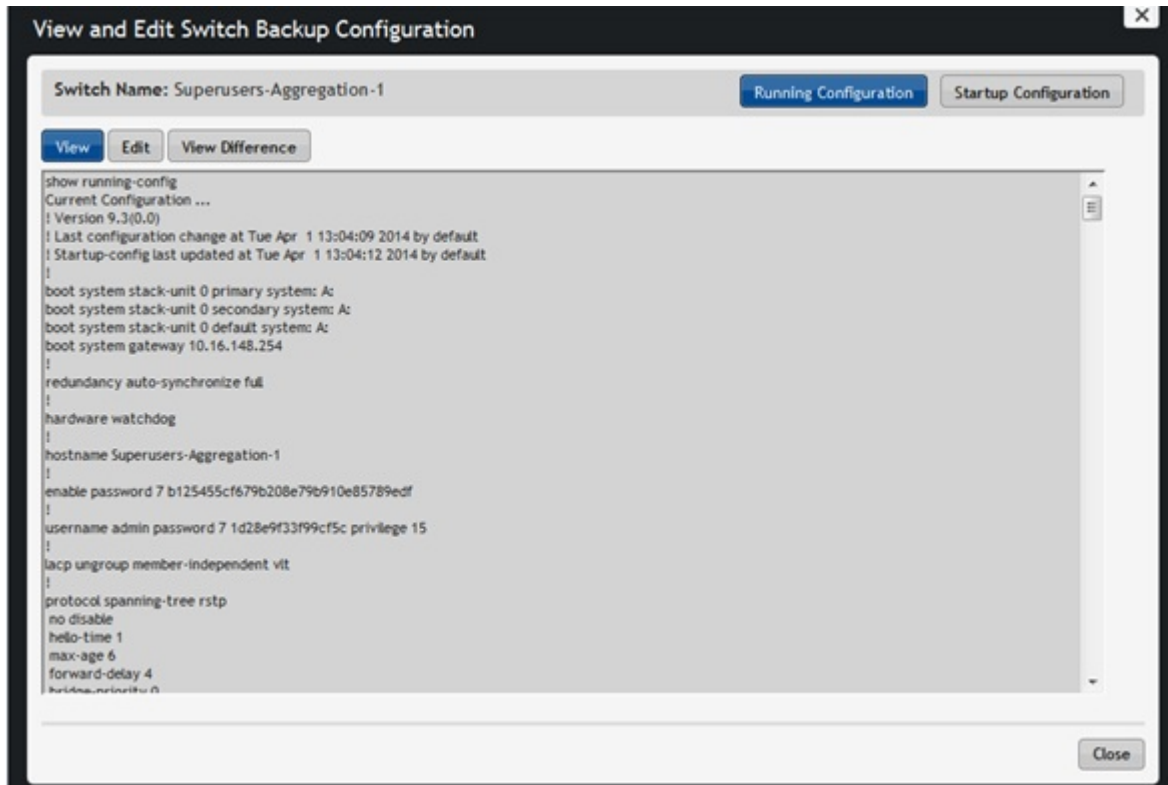


Figure 111. View and Edit Switch Backup Screen Configuration Screen

3. Select one of the following options:
  - **Edit** — Edit the running or startup configuration on the deployed devices.
  - **View Difference** — View difference between the backed up configuration (either running or startup) and an edited configuration. Use this option to verify all modifications to the current backed up configuration before you save it.
  - **View** — View the running or startup configuration on deployed devices.
4. To exit from this screen, click **Close**.



## Updating the Switch Software

You can view a summary of software for each switch in the fabric on the **Maintenance** tab. This tab has the following options:

- [Scheduling Switch Software Updates](#) — Create a new scheduled software image upgrade and software image activation job.
- [Activating Standby Partition Software](#) — Activate the software in the standby partition of the device as a scheduled job later or immediately.

## Replacing an IOA Blade Switch

This section describes how to replace an IOA blade switch. For information about how to replace other switch types, refer to [Replacing a Switch](#).

1. Remove the decommissioned IOA blade switch from the M1000e chassis.
2. Replace the decommissioned IOA blade switch with the replacement IOA blade switch in the same slot of the M1000e chassis.
3. Use the **Network > Design Fabric > Discovery Status** tab to rediscover the chassis.
  -  **NOTE:** During the rediscovery process, AFM restores the previously configured IP address to the replacement IOA blade switch.
4. To deploy the successfully discovered replacement IOA blade switch, select **Overwrite entire configuration on the switch** and click **OK**.
  -  **NOTE:** For IOA replacement, the **Overwrite entire configuration on the switch** option is selected by default and the **Apply configuration changes to the switch** option is not available.

## Replacing a Switch

 **NOTE:** To replace an IOA blade switch, refer to [Replacing an IOA Blade Switch](#).


1. [Decommission a Switch](#).
2. [Replacing a Switch](#).
3. [Deploy Replacement Switch](#).

 **NOTE:** Replace the decommissioned switch with same switch type.

### Step 1: Decommission a Switch

When you decommission (replace) a switch, consider the following requirements:

- The switch must be powered off manually.
- The switch is automatically placed in `unmanaged` state and AFM stops managing the switch.
- The new switch must use the factory default setting.
- To use the old switch, reset it to the factory default setting.
- AFM generates information for Return Material Authorization (RMA) for submittal to iSupport.

 **NOTE:** Replace the switch with the same switch type. For information about how to replace a switch, refer to [Replacing a Switch](#).

1. From the menu, click **Network > Fabric Name > Switch Name**.
2. Click the **Switch Replacement** tab.  
The **Switch Replacement Summary** screen appears.
3. Click **Decommission Switch**.  
The **Decommission Switch** screen appears.
4. Review and follow the instructions on the **Decommission** screen.


5. To save the text file that contains information for submitting a Return Material Authorization (RMA), click **Save**. Send this information to your Dell Networking software support representative for switch replacement.
6. Once a replacement switch is available, click **Replace Switch**.

## Step 2: Replacing a Switch

 **NOTE:** To replace an IOA blade switch, refer to [Replacing an IOA Blade Switch](#).

Before you replace a switch, gather the following useful information:

- System MAC address, Service Tag and serial number for the replacement switch
- (MXL, N series ) IP address of the replacement MXL switch
- Location of the switch, including the rack and row number
- Remote Trivial File Transfer Protocol (TFTP) / File Transfer Protocol (FTP) address
- Last deployed Dell Networking operating system software image for the replacement switch uploaded to the TFTP/FTP site so the switch can install the appropriate software image and configuration file
- Updated Dynamic Host Configuration Protocol (DHCP) server configuration file.

 **NOTE:**


- If you use a remote DHCP server, manually update the DHCP configuration file based on the configuration AFM provides.
- If you use a local DHCP server, AFM updates the DHCP server automatically.

After you power cycle the switches, the switches communicate with the DHCP server to obtain a management IP Address based on the system MAC Address. The DHCP server contains information about the location of the TFTP/FTP site for the software image configuration file for each switch type used during bare metal provisioning (BMP).

1. From the menu, click **Network** > *Fabric Name* > *Switch Name* screen.
2. Click the **Switch Replacement** tab and click **Replace Switch**.
3. Review the introduction and the instructions on the **Switch Cabling** screen.
4. Confirm that the replacement switch is racked, cabled, and powered on.
5. Click **Next**.  
The **MAC Assignment** screen appears.
6. (MXL and N series only) Enter the new IP address of the replacement MXL switch in the **New IP Address** field.
7. In the **MAC Assignment** screen, enter the new serial number for the replacement switch in the **New Serial Number** field.
8. Enter the new Service Tag for the replacement switch in the **New Service Tag** field.
9. Enter the new system MAC address for the replacement switch in the **New MAC Address** field.
10. Click **Next**.  
The **DHCP** screen appears.
11. Save the replacement switch DHCP configuration file.
12. Review the **Summary** screen and click **Finish**.
13. Before deploying the switch:
  - a. If you use a remote DHCP server, integrate the new DHCP file with the system MAC address of the replacement switch and then restart the DHCP service.
  - b. Rack the hardware according to the wiring plan.
14. Click **Deploy Switch**.

### Step 3: Deploy Replacement Switch


1. From the menu, click **Network** > *Fabric Name* > *Switch Name*.
2. Click the **Switch Replacement** tab.
3. Click **Deploy Switch**.


 **NOTE:** If you change the switch outside of AFM (for example, using Telnet), refer to [Restoring a Switch Configuration](#) to restore the switch configuration. For information about how to replace a switch, refer to [Replacing a Switch](#).


## Updating AFM

You can view and manage AFM server updates on the **Server Update** tab.

1. From the menu, click **Administration** and then click the **Server Update** tab.
2. In the **Select RPM packing file location** area, select one of the following options:
  - **Local Drive (DVD, USB)**
  - **Remote Server**

 **NOTE:** If the location is a remote server, enter the URL location of the RPM file on the remote server.

1. From the **Protocol Type** drop-down menu, select the protocol type:
  - **https**
  - **ftp**
  - **sftp**
2. Specify the path of the RPM package using the following formats:
  -  **NOTE:** The RPM filename must start with AFM and must end with **.noarch.rpm** (for example, **AFM2.5.0.79.noarch.rpm**).
  - **https://ipaddress/path\_to\_rpm.file**
  - **ftp://ipaddress/path\_to\_rpm.file**
  - **sftp://ipaddress/path\_to\_rpm.file**
3. Click **Update**.

 **NOTE:** To activate the new AFM software and set it to the new version, from the AFM console, select **Set AFM Software to Next Reboot**. Then, restart or reboot the AFM server.

The new software is uploaded to the standby partition.

# Jobs

This section contains the following topics:

- [Displaying Job Results](#)
- [Scheduling Jobs](#)

## Displaying Job Results

To view job status, use the **Job Results** tab.

1. From the menu, click **Jobs** and then make sure that the **Job Results** tab is selected
2. In the upper right of the screen, click the filter icon to filter the job results.
3. In the **Job Name** field, enter the job name.
4. From the **Status** drop-down menu, select a filter option:
  - **All**
  - **Success**
  - **Failure**
  - **In Progress**
5. In the **Start Date From** area, click the select date and time icon to specify the beginning date of the range of the starting date of the job.
6. In the **Start Date To** area, click the select date and time icon to specify the ending date of the range of the starting date of the job.
7. In the **End Date From** area, click the select date and time icon the beginning date of the range of the ending date of the job.
8. In the **End Date To** area, click the select date and time icon to specify the ending date of the range of the ending date of the job.
9. Click **Apply**.

## Scheduling Jobs

In AFM, you can schedule the following jobs:

- Backups of running configuration or startup configuration files on a switch. Refer to [Switch Backup](#) — Back up a switch running configuration and startup configuration file.
- Upgrading the software image on a switch. Refer to [Switch Software Image Updates](#) — Create a job to upgrade the switch software image.
- Activate software available in the standby partition of a switch. Refer to [Switch Software Image Activation](#) — Activate the software available in the standby partition of the switch as a scheduled job for later or to run immediately.
- **Add** — Schedule a new job.

- **Edit** — Edit or modify an existing job schedule.
  - ✎ **NOTE:** You can only change the scheduled time. You cannot change the job name, image location, or switch.
- **Run Now** — Start a job immediately. Select a job and click **Run**.
- **Delete** — Delete a job. Select a job and then click **Delete**.
- **Enable** — Enable the job or activate the schedule.
- **Disable** — Disable the job or the schedule without deleting the job.

## Switch Backup

To back up a running configuration and startup configuration files from a switch, use the **Switch Backup** screen.

1. From the menu, click **Jobs** and then click the **Scheduled Jobs** tab.
2. From the **Add** drop-down menu, select **Switch Backup**.  
The **Switch Backup** screen appears.
3. In the **Name** field, enter the name of the job.
4. (Optional) In the **Description** field, enter a description for the job.
5. Click **Next**.  
The **Select Switches** screen appears.
6. In the **Available** area, select the fabric and then switches to back up:
  - **Two-tier distributed core filtering options** — All, Spine, and Leaves
  - **Two-tier VLT options** — All, Aggregation and Access
  - **Three-tier filtering options** — All, Core, Aggregation and Access
7. To move the switches to the **Selected Switches** area, click the **>>** button and click **Next**.
8. On the **Schedule** screen, select one of the following options:
  - **Run Now** — Back up the switch software immediately.
  - **Schedule job to start on** — Specify a date and time for the switch software backup.
 The **Summary** screen appears.
9. Review the settings on the **Summary** screen and click **Finish**.

## Switch Software Image Updates

As part of ongoing data center operations, periodically update the software and configurations in the fabric. Update one or more switches by specifying the location for the software updates and then schedule the updates immediately or for a later date and time.

1. From the menu, click **Jobs** and then click the **Scheduled Jobs** tab.
2. From the **Add** drop-down menu, select **Switch Software Image Update**.  
The **Update Switch Software Image** window appears.
3. In the **Job Name** field, enter the name of the switch software job.
4. (Optional) In the **Description** field, enter a description of the job.
5. Click **Next**.  
The **Switch Select** screen appears..
6. In the **Available** area, select the fabric and the switch types to update:
  - **Two-tier VLT options** — All, Aggregation and Access
  - **Three-tier filtering options** — All, Core, Aggregation and Access



7. In the **Update Location** area, if necessary, click **Edit TFTP or FTP settings**.
8. In the **Path and Image file name to the software updates on selected TFTP or FTP site** field, specify the path and image file for the switch software update.
9. Click **Next**.
10. In the **Update Option** area, select one of the following options and click **Next**:
  - **Manual** — Stage the update to the secondary partition but do not apply it.
  - **Automatic** — Apply the software update and reboot.

The **Schedule** screen appears.

11. On the **Schedule** screen, select one of the following options:
  - **Run Now** — Update the switch software immediately.
  - **Schedule job to start on** — Specify a date and time for the switch software update.

The **Summary** screen appears.

12. Review the settings on the **Summary** screen and click **Finish**.

## Switch Software Image Activation

To activate the software available in the standby partition of the switch as a scheduled job to happen at later time or to run immediately, use the **Switch Software Image Activation** option.

1. From the menu, click **Jobs** and then click the **Scheduled Jobs** tab.
2. From the **Add** drop-down menu, select **Switch Software Activation**.

The **Activate Standby partition** window appears.
3. In the **Job Name** field, enter a name for the job.
4. (Optional) In the **Description** field, enter a description for the job.
5. Click **Next**.

The **Switch Select** screen appears.
6. In the **Available Switches** area, select the fabric and then the switch types to update:
  - **Two-tier distributed core filtering options** — All, Spine, and Leaves
  - **Two-tier VLT options** — All, Aggregation and Access
  - **Three-tier filtering options** — All, Core, Aggregation and Access
7. To move the selected switches into the **Selected** area, click the **>>** button and click **Next**.

The **Schedule** screen appears.
8. Select one of the following options and click **Next**:
  - **Run Now** — Active the standby partition immediately.
  - **Schedule job to start on** — Schedule the job by specifying a date and time.

The **Summary** screen appears.

9. Review the settings and then click **Finish**.

## Scheduling Switch Software Updates

The **Update Software** screen displays a software summary for each switch in the fabric. To create a new scheduled job for backup, software image upgrade, and software image activation, use the **Schedule Switch Software Image Update** option. As part of ongoing data center operations, periodically update the software and configurations in the fabric. Update one or more switches. Specify the location for the

software updates and then schedule the update to load immediately or schedule it for a later date and time.

1. From the menu, click **Network** > *Fabric Name* and then click the **Maintenance** tab.
2. Click **Update Software**.
3. Click **Schedule Switch Software Image Update**.
4. On the **Job Name** screen, in the **Job Name** field, enter a unique name for the software job.
5. (Optional) In the **Description** field, enter a description for the schedule software update.
6. Click **Next**. The **Select Switches** screen displays.
7. On the **Select Switches** screen, in the **Available** area, select the fabric and then the switches to update:
  - **Two-tier distributed core filtering options** — All, Spine, and Leaves
  - **Two-tier VLT options** — All, Aggregation and Access
  - **Three-tier filtering options** — All, Core, Aggregation and Access
8. To move the selected switches to the **Selected Switches** area, click the >> button.
9. Click **Next**.  
The **Update Location** screen appears.
10. On the **Update Location** screen, to select the TFTP or FTP site for the software updates, click **Edit TFTP or FTP settings**.
11. Enter the path and image name of the software file on the TFTP or FTP site for each type of switch.
12. Enter the path and image name of the software file on the TFTP or FTP site for each type of switch.  
The **Update Option** screen appears.
13. On the **Update Option** screen, select one of the following options:
  - **Manual** — Stage the update to the secondary partition but do not apply it.
  - **Automatic** — Apply software update and reboot.
14. Click **Next**.  
The **Schedule** screen appears.
15. On the **Schedule** screen, select one of the following options and click **Next**:
  - **Run Now** — Run the switch software update immediately.
  - **Schedule job to start on** — Schedule the job for later. Specify the start date and time for the software update job.
16. On the **Summary** screen, review the software update software settings and click **Finish**.

## Activating Standby Partition Software

To activate the software available in the standby partition of the switch as a scheduled job to occur later or to run immediately, use the **Schedule Activate Standby Partition** option.

1. From the menu, click **Network** > *Fabric Name* and then click the **Maintenance** tab.
2. Click **Update Software**.
3. Click **Schedule Activate Standby Partition**.
4. In the **Job Name** field, enter a name for the job.
5. (Optional) In the **Description** field, enter a description for the job.
6. Click **Next**.
7. From the drop-down menu, select one of the following options:
  - **Two-tier distributed core filtering options** — All, Spine, and Leaves
  - **Two-tier VLT options** — All, Aggregation and Access

- **Three-tier filtering options** — All, Core, Aggregation and Access
8. Select the switches for standby partition activation and then click the >> button to move them to the **Selected** area.
  9. Click **Next**.
  10. From the **Schedule** screen, select one of the following options and click **Next**:
    - **Run Now** — Schedule the job to run immediately.
    - **Schedule job to start on** — Schedule the job to run later.
  11. Review the **Summary** settings and click **Finish**.

## Scheduling a Back Up Switch Configuration

1. From the menu, click **Network** > *Fabric Name* and then click the **Maintenance** tab.
2. Click the **Backup Switch** button.  
The switch backup options appear.
3. Click **Schedule Switch Backup**.  
The **Switch Backup** window appears.
4. In the **Name** field, enter the name of the software job name.
5. (Optional) In the **Description** field, enter a description.
6. Click **Next**.  
The **Select Switches** screen appears.
7. From the **Available** drop-down menu, select the type of switches to update.
8. In the **Available Switches** area, select the types of switches to update:
  - **Two-tier distributed core filtering options** — All, Spine, and Leaves
  - **Two-tier VLT options** — All, Aggregation and Access
  - **Three-tier filtering options** — All, Core, Aggregation and Access
9. To move the selected switches to the **Selected Switches** area, click the >> button and then click **Next**.  
The **Schedule** screen appears.
10. In the **Start** area, select one of the following options:
  - **Run Now** — Run the job now.
  - **Schedule job to start** — Specify when to schedule the job.
11. In the **Summary** screen, review your settings, and then click **Finish**. For more information about backing up switches, refer to [Viewing and Editing the Switch Backup Configuration](#).


# Administration

This section contains the following topics:

- [Administrative Settings](#)
- [Managing User Accounts](#)
- [Managing User Sessions](#)
- [Audit Log](#)
- [Updating the Server](#)

## Administrative Settings


To configure administrative settings, use the **Administration > Settings** screen:

 **NOTE:** AFM allows you to configure the SNMP configuration and CLI credentials before designing and deploying the fabric. You cannot edit SNMP and CLI credentials settings during the run phase.

### Active Link Settings

To display additional performance statistics in AFM using a Dell OpenManage Network Manager (OMNM) server, use the **Active Link Settings** option. OMNM monitors and manages Dell network devices. It automates common network management operations and provides advanced network element discovery, remote configuration management, and system health monitoring to proactively alert network administrators to potential network problems. OMNM provides SOAP-based web services to allow third-party integration.

AFM provides view-only integration with the Dell OMNM web application. When you enable **Active Link**, it displays another browser to view AFM performance statistics. For information about how to install and configure OMNM, refer to <http://www.dell.com/support/Manuals/us/en/555/Product/dell-openmanage-network-manager>. Refer to the release notes or the *AFM Installation Guide* for supported versions of OMNM.

 **NOTE:** Install the Dell OMNM software on a different server than AFM. To activate the performance statics, log in to Dell OMNM web service directly using `write` permissions.



**NOTE:** By default, the web service is turned off in the OMNM server.

To enable web service, follow these steps:

1. On the OMNM server, go to the server installation directory.
2. Navigate to the **installed.properties** file at **C:\ProgramFiles\Dell\OpenManage\Network Manager\awareapps\installprops\lib**.
3. Disable the Application Server and Synergy Network Management server.
4. Disable the Application Server and Synergy Network Management server.

```
com.dorado.core.ws.disable=false
com.dorado.core.ws.legacy.soap.enabled=true
aware.webservices.authrequired=false
```

5. Enable the **Resource Monitoring** option for performance monitoring.
6. Start the Application server and Synergy Network Management server.

Before configuring Active Link, gather the following OMNM server information:

- OMNM server IP address
- communication protocol (HTTP or HTTPS)
- user name and password

AFM provides the Active Link server and Active Link web service status in the following areas:

- **Administration** > **Settings** > **Active Link Settings** area
- **Network** > **Alerts and Events** tab **Description** column
- **Network** > *Switch* > **Summary** tab

AFM disables the **Active Link** feature if:

- AFM cannot connect to Active Link server
- AFM cannot connect to Active Link web service
- AFM does not manage the selected switch
- The Active Link server is not configured

The topology view and link status refresh every 60 seconds by default. Change the refresh rate interval on the **Administration** > **Settings** > **Client Settings** dialog box > **GUI Polling** setting.

- The AFM UI provides the Active Link server status and Active Link web service status on the following screens:
  - **Administration** > **Settings** tab > **Active Link Settings** area
  - **Network** > *Switch* > **Summary** tab


The Active link is available at the following screens.

- Navigate to the **Network** > *Fabric* > **Summary** tab > **Graphical** view. From the **Action** menu, select **Launch Active Link**.
- Navigate to the **Network** > *Fabric* > **Summary** tab > **Graphical** view. Right-click the switch icon and select **Launch Active Link**.
- Navigate to the **Network** > *Fabric* > **Summary** tab > **Tabular** view. From the **Action** menu, select the switch row and then select **Launch Active Link**. The Active Link displays the selected switch view and performance charts.
- Navigate to the **Network** > *Switch* > **Summary** tab > **Graphical** view and click **Launch Active Link**. The Active Link displays the selected switch view and performance charts.

- Navigate to the **Network >Switch > Summary** tab > **Tabular** view and click **Launch Active Link**. The Active Link displays the selected switch view and performance charts.
1. From the menu, click **Administration** and then click the **Settings** tab.
  2. Navigate to the **Active Link Settings** area and click **Edit**.
  3. In the **Active Link Type** area, select the **Integrate to Dell OpenManage Network Manager (OMNM)** check box to display additional performance statistics.
  4. In the **Active Link System IP Address** field, enter the Active Link server IP address for the element management system. In the **Communication Protocol** area, select one of the following options:
    - **Use HTTP protocol to connect through AFM Server**
    - **Use HTTPS protocol to connect through AFM Server**
  5. In the **User Name**, enter the Active Link user name.
  6. In the **Password** field, enter the Active Link user password.
  7. Click **OK**.

## CLI Credentials

To provision the fabric, enter the CLI user's credential and enable the configuration credentials for all the switches in the fabric. This option allows you to remotely make configuration changes to the switches in the fabric.

 **NOTE:** If you change the password on a switch in a currently deployed fabric, the switch reboots and redeploys. Re-deploy the fabric using the pre-deployment wizard and update the password on the **CLI Credentials** screen.

**To configure the CLI credentials and enable the configuration credentials for all the switches in the fabric:**

1. From the menu, click **Administration** and then click the **Settings** tab.
2. In the **CLI Credentials** area, click the **Edit** button.
3. In the **Protocol** drop-down menu, select one of the following options:
  - **Telnet**
  - **SSHv2**
4. In the **User Name** field, enter the user name.
5. In the **Password** field, enter the password.
6. In the **Confirm Password** field, confirm the password.
7. In the **Enable Password** field, enter a password for the privilege level. The privilege level is 15 and is a read-only field.
8. In the **Confirm Enable Password** field, confirm the enable password for the privilege level.
9. Click **OK**.

## Client Settings

**To configure the polling interval and the maximum number of browser windows for each user's session:**

1. From the menu, click **Administration** and then click the **Settings** tab.
2. In the **Client Settings** area, click **Edit**.
3. From the **GUI Polling Interval (in Seconds)** drop-down menu, select one of the following options. The default value is 60 seconds.
  - **15 Seconds**

- **30 Seconds**
  - **60 Seconds**
  - **120 Seconds**
4. From the **New Window per Client Session** drop-down menu, select the maximum number of browser windows for each user's session. The range is 3–7 and the default value is 3.
  5. Click **OK**.

## Data Retention Settings

To configure the amount of time to retain performance history:

1. From the menu, click **Administration** and then click the **Settings** tab.
2. In the **Data Retention** area, click **Edit**.
3. In the **Performance History** area, enter the number of days to retain the performance history. The range is 1–180.
4. From the **Daily Purge Execution Time** drop-down menu, specify when to purge the performance history data.
5. Click **OK**.

## DHCP Server Settings

To select a local or remote DHCP server:

1. From the menu, click **Administration** and then click the **Settings** tab.
2. Navigate to the **DHCP Server Settings** area and select one of the following settings:
  - **Local** — Provision AFM as a DHCP server. If you select this option, AFM automatically integrates the generated **dhcp.config** file into the DHCP server on AFM during pre-deployment.
  - **Remote** — Use an external DHCP server. If you select this option, manually install the **dhcp.config** file generated during pre-deployment on the DHCP server before deploying the fabric.
3. Click **OK**.

## NTP Server Settings

To configure NTP server settings:

1. From the menu, click **Administration** and then click the **Settings** tab.
2. In the **NTP Server Settings** area, click **Edit**.
3. Enter the NTP server primary IP address.



**NOTE:** The **IP Status** and **Secondary IP Status** fields display the current status of the servers.

4. Enter the NTP server secondary IP address.
5. Click **OK**.

## SMTP Email

To configure SMTP email:

1. From the menu, click **Administration** and then click the **Settings** tab.
2. In the **Secure SMTP Email Settings** area, click **Edit**.
3. In the **Outgoing Mail Server** field, enter the IP address or complete host name of the email server.
4. In the **Server Port** field, enter the port number of the email server.

5. In the **User Name** field, enter the user name.
6. In the **To Email Address(es)** field, enter the mail addresses separated by a semicolon (;).
7. In the **To Email Address(es)** field, enter the mail addresses separated by a semicolon (;):
  - **Critical**
  - **Major**
  - **Minor**
  - **Warning**
8. Click **OK**.

## SNMP Configuration

Configure SNMP so that AFM can perform SNMP queries on the switches in the fabric. AFM uses the SNMP configuration values for configuring and monitoring the switches.

1. From the menu, click **Administration** and then click the **Settings** tab.
2. In the **SNMP Configuration** area, click **Edit**.
3. In the **Read Community String** field, enter the read community string (for example, `public`).
4. In the **Write Community String** field, enter the write community string (for example, `private`).
5. In the **Trap Port** field, enter the SNMP port number of the switches. The port number is typically 161.
6. In the **Trap Host** field, specify the IP address for AFM so that the traps are sent to AFM.
7. Click **OK**.


## Syslog Server IP Addresses

To configure the syslog server for event logging:

1. From the menu, click **Administration** and then click the **Settings** tab.
2. In the **Syslog IP Address(es)** area, click **Edit**.
3. In the **System IP Addresses** area, configure up to eight syslog server IP addresses for logging events on the switches in the fabric. By default, the first syslog IP address entry is the AFM system IP address.

## System Information

1. From the menu, click **Administration** and then click the **Settings** tab.
2. In the **System Information** area, click **Edit**.
3. From the **System IP Address** drop-down menu, select the AFM management IP address.

 **NOTE:** If you configured multiple Network Interface Card (NIC) adapter cards on AFM, select the AFM management IP address.

## TFTP/FTP Settings

1. From the menu, click **Administration** and then click the **Settings** tab.
2. For FTOS switches, select either **TFTP** or **FTP** to configure settings for that type of server. For PowerConnect switches, you can only configure TFTP server settings.
3. For PowerConnect switches, in the **PowerConnect TFTP Configuration** area, select one of the following options:
  - **Local** — Provision AFM as a TFTP server. The TFTP server uses the AFM management IP address.



- **Remote** — Use an external TFTP server. Enter the TFTP IPv4 address.
4. For FTOS switches, in the **TFTP/FTP Settings** area, select one of the following options:
- **Local** — Provision AFM as a TFTP or FTP server.
    - ✎ **NOTE:** If you use the **Local** option, the TFTP or FTP server must be in the same subnet as AFM.
      - If you select the local FTP server option, the FTP server uses the AFM management IP address. Enter the AFM user name and password.
      - If you select the local TFTP server option, the TFTP server uses the AFM management IP address.
  - **Remote** — Use an external TFTP or FTP server.
    - If you select the FTP protocol and remote option, enter the FTP server IPv4 address, user name and password.
    - If you select the TFTP protocol and remote option, enter the TFTP IPv4 address.

## Managing User Accounts

AFM users are categorized as one of three predefined roles with the following permissions:

### Superuser

- View a summary of user accounts
- Add, delete, and edit users
- Lock and unlock users
- Reset passwords for all accounts
- Perform configuration changes
- Set session timeout values
- Terminate AFM users' sessions on the **Administration > User Session** screen

### Administrator

- Perform configuration changes
- View performance monitoring
- Change password for own account

### User

- View configuration and performance monitoring information.
- Change password for own account.

✎ **NOTE:** The AFM root user name is `superuser` and the password is `Superuser1`.

To view and manage user accounts, use the **Administration > User Accounts** screen.

- **User Accounts Summary View** — Display a summary view of all user accounts when the current user's role is `Superuser`. When the role is `user` or `administrator`, only the current user's account information displays.
- **Add User** — Add new user accounts. Configure up to 50 user accounts but AFM supports only one `superuser` account.
- **Edit User** — Edit settings for user accounts.
- **Delete** — Delete one or more user accounts. The system default user account, `Superuser`, cannot be deleted.

- **Unlock** — Unlock account for a user who was locked out because he or she exceeded the maximum number of login attempts. To unlock a user account, select the user and click **Unlock**.
- **Default User** — During the installation process, AFM prompts you to create a `Superuser` account.
- **Reset Default User** (`Superuser`) Password — Contact technical support if you need to reset the `Superuser` password.
- **Password Rules** — Enforces special password rules for enhanced security. The password must contain at least six characters, one capital letter, and one number. AFM masks the password when you enter it.

## Adding a User

To add a user account, log in as a `Superuser`. For more information about user accounts, refer to [Managing User Accounts](#).

1. From the menu, click **Administration** and then click the **User Account** tab.
2. Click **Add User**.  
The **Add User** dialog box appears.
3. In the **User Name** field, enter a unique alphanumeric name for the user. The range is 1–25 characters.
4. In the **Password** field, enter the user's password.  
The password length must be from 8 – 32 characters and include three characters from the following categories:
  - At least one upper-case letter
  - Lower-case letters
  - At least one numeric digit
  - At least one special character
5. In the **Confirm Password** field, enter the user's password.
6. In the **First Name** field, enter the user's first name. The range is 1–50 characters. There are no character restrictions.
7. (Optional) In the **Last Name** field, enter the user's last name. The range is 1–50 characters. There are no character restrictions.
8. From the **Role** drop-down menu, select one of the following roles:
  - **Admin**
  - **User**

For information about roles, refer to [Managing User Accounts](#).

9. In the **Sessions Allowed** drop-down menu, specify the number of sessions allowed for the user. The range is 1–5 and the default is 5.
10. In the **Session Timeout** drop-down menu, specify a session timeout value. If a user is inactive for this amount of time, AFM automatically logs out of the account. Select one of the following options:
  - **15 minutes**
  - **30 minutes**
  - **45 minutes**
  - **60 minutes**

The default value is 15 minutes.

11. In the **Unsuccessful Login Limit** drop-down menu, specify the number of permissible unsuccessful login attempts for a user's account. When the unsuccessful login limit is exceeded, AFM applies the **Lockout Duration** setting. The range is 3–10 and the default is 5.

12. In the **Lockout Duration** drop-down menu, select one of the following options.

- **15 minutes**
- **30 minutes**
- **45 minutes**
- **60 minutes**
- **Permanent**

The default value is 30 minutes.

13. Click **OK**.

## Editing a User

To edit a user, log in as a `Superuser`. For more information about user accounts, refer to [Managing User Accounts](#).

1. From the menu, click **Administration** and then click the **User Accounts** tab.
2. Select the user.
3. Click **Edit**.

The **Edit User** dialog box appears.

4. In the **First Name** field, enter the user's first name.
5. In the **Last Name**, enter the user's last name.
6. In the **Password** field, enter the user's password.
7. In the **Confirm Password** field, enter the user's password.
8. From the **Sessions Allowed** drop-down menu, specify the number of sessions allowed for the user.
9. From the **Session Timeout** drop-down menu, specify the session timeout. If a user is inactive for this amount of time, AFM automatically logs out of the account. Select one of the following options:
  - **15 minutes**
  - **30 minutes**
  - **45 minutes**
  - **60 minutes**
10. From the **Unsuccessful Login Limit** drop-down menu, select the number of allowed unsuccessful login attempts. When the unsuccessful login limit is exceeded, AFM applies the **Lockout Duration** setting. The range is 3–10.
11. From the **Lockout Duration** drop-down menu, select one the following options:
  - **15 minutes**
  - **30 minutes**
  - **45 minutes**
  - **60 minutes**
  - **Permanent**
12. Click **OK**.

## Deleting a User

To add or delete users, log in as a `Superuser`. For more information about user accounts, refer to [Managing User Accounts](#).

 **NOTE:** You cannot delete the Superuser account.

1. From the menu, click **Administration** and then click the **User Account** tab.
2. Select the user.
3. Click **Delete**.
4. In the confirmation dialog box, click **Yes**.

## Unlocking a User

To unlock a user, log in as a **Superuser**. For information about user accounts, refer to [Managing User Accounts](#).

1. From the menu, click **Administration** and then click the **Users Account** tab.
2. Select the user.
3. Click **Unlock**.
4. Click **OK**.

## Changing Your Password

1. Go to the upper right of the screen next to your login name.  
A drop-down menu appears.
2. Select **Change Password**.  
The **Change Password** screen appears.
3. In the **Current Password** field, enter the current password.
4. In the **New Password** field, enter the new password.  
The password length must be from 8–32 characters and include three characters from the following categories:
  - At least one upper-case letter
  - Lower-case letters
  - At least one numeric digit
  - At least one special character
5. In the **Confirm Password** field, re-enter the new password.
6. Click **OK**.  
For more information about user accounts, refer to [Managing User Accounts](#).

## Managing User Sessions

To display active AFM users and terminate users' sessions, use the **User Session** tab. Only the **Superuser** can terminate an AFM user's session. For more information about user accounts, refer to [Managing User Accounts](#).

This tab displays the following information:

- **User Name** — View a list of user names for users who are currently logged in.
- **Session Login Time** — View the date and time of the user's last login.
- **Client IP Address** — View the IP address of the user.
- **Current Session** — Displays a checkmark if the user is logged in.

To terminate users' sessions:

1. From the menu, click **Administration** and then click the **User Session** tab.
2. Select the users that you want to log off.
3. Click **Force Logoff**.
4. Click **OK**.

## Audit Log

To log a chronological sequence of audit records with information on who has accessed the switch and what operations the user has performed during a given period, use the **Audit Log** tab. The Audit Log only captures actions by AFM users.

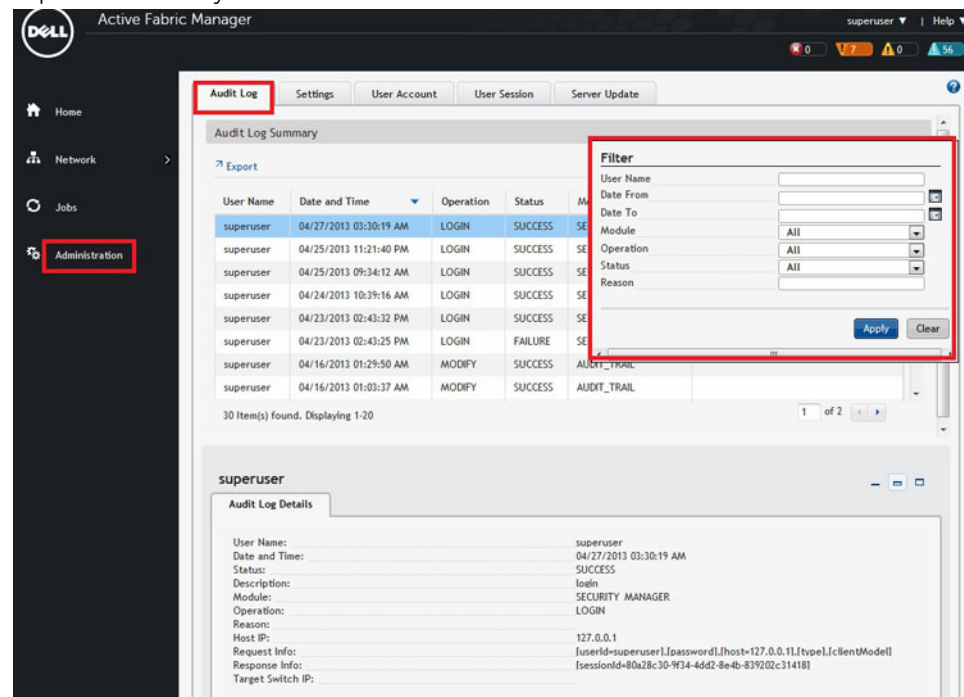


Figure 112. Audit Log Tab

1. From the menu, click **Administration**, and make sure that the **Audit Log** tab is selected.
2. To display the audit trail options, click the filter icon on the upper right of the screen.
3. Enter your filter criteria for the **User Name** field (for example, `superuser`).
4. From the **Date From** drop-down menu, select the beginning date and time of the operation.
5. From the **Date To** drop-down menu, select the end date and time of the operation.
6. From the **Module** drop-down menu, select one of the following AFM modules:
  - All
  - Security Activation
  - Security Manager
  - Audit Trail
  - UI Manager
7. From the **Operation** drop-down menu, select an operation:
  - All


- Query
  - Create
  - Modify
  - Cancel
  - Move
  - SNC Config
  - Monitor
  - Login
  - Logout
8. From the **Status** drop-down menu, select an audit trail progress status:
    - All
    - Queued
    - In Progress
    - Success
    - Failure
    - Timeout
    - Response Delivered
    - Invalid Request
  9. (Optional) In the **Reason** field, enter a reason.
  10. Click **Apply**.
    - To export the results, click **Export**.


## Updating the Server

You can begin the process of updating the Active Fabric Manager software version from the AFM graphical user interface.

The latest AFM software package is in RPM format.

1. From the menu, click **Administration**, and click the **Server Update** tab.
2. Click **Update Server**.  
The **Update Server** dialog box appears.
3. From the **Select RPM packaging file location** section, choose one of the following:
  - **Local Drive (DVD, USB)** – Specify this setting if the RPM packaging file is on a local workstation from where the AFM console is launched. To navigate to the RPM packaging file location on a local disk or drive, click **Browse**.
  - **Remote Server** – Specify the following settings to load the RPM packaging file if it is on a remote server:
    - **Protocol Type**
    - **Path**
    - **User Name (optional)**
    - **Password (optional)**

 **NOTE:** If you download an updated RPM from the remote server, it overwrites the current software version.

 **NOTE:** To complete the update process, refer to “Applying AFM Updates on Restart” and “Restarting AFM” in the *AFM Installation Guide 2.7*.

# Technical Support

Dell Networking Technical Support provides a range of documents and tools to assist you with effectively using Dell Networking equipment and mitigating the impact of network outages.

## Accessing Dell License Portal

When you receive the Order Fulfillment email, follow these instructions to download the software.

1. Go to <http://www.dell.com/support/licensing>.
2. Enter your order number and click **Available Software List**.
3. Select the latest released version.
4. Accept the End User License Agreement (EULA).
5. Choose to download the file directly or use the NetSession client.
6. Click the **Download Now** button.

## Contacting Dell Technical Support

- Downloading Software — Download the latest released version of the software at <http://www.dell.com/support/licensing>
- Technical Documentation — [www.dell.com/support](http://www.dell.com/support)
- Contact Information — [DellNetworking-Support@dell.com](mailto:DellNetworking-Support@dell.com)