Active Fabric Manager for Microsoft Cloud Platform System

User Guide for AFM-CPS 2.2(0.0)

Notes, cautions, and warnings

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

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

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

2017 - 04

Rev. A03

Contents

1

Introduction

Active Fabric Manager (AFM) for Microsoft Cloud Platform Systems (CPS) 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.

You can use AFM to simplify network operations, automate tasks, and improve data center efficiency.

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.

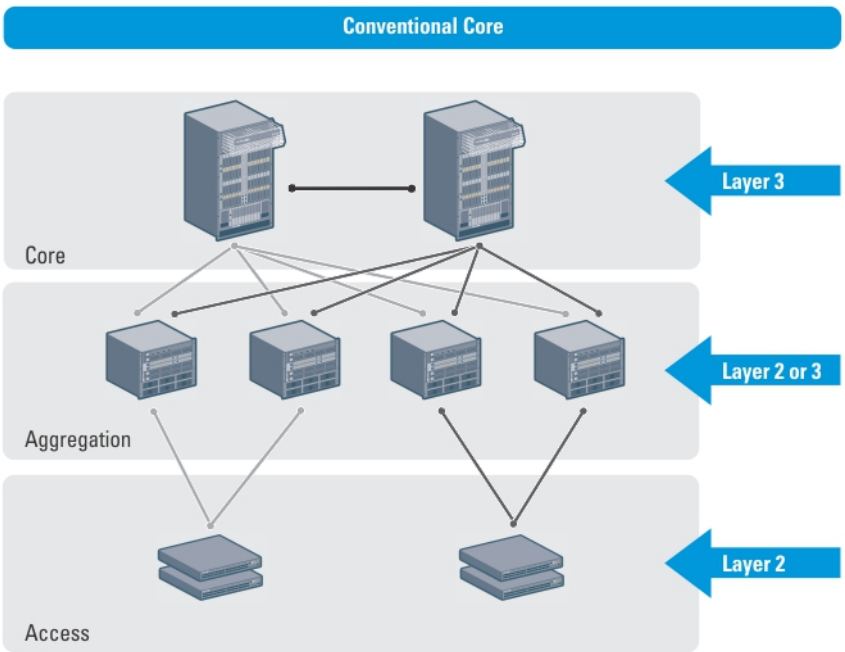


Figure 1. Conventional Core

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 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 distribute 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.

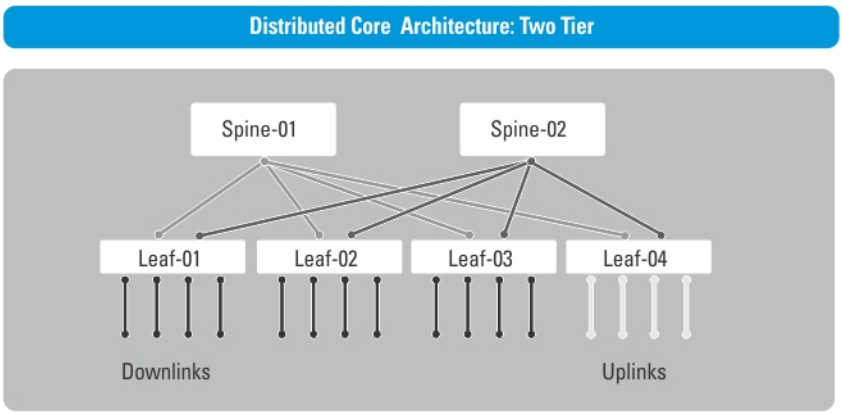


Figure 2. Distributed Core Architecture: Two-Tier

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 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.

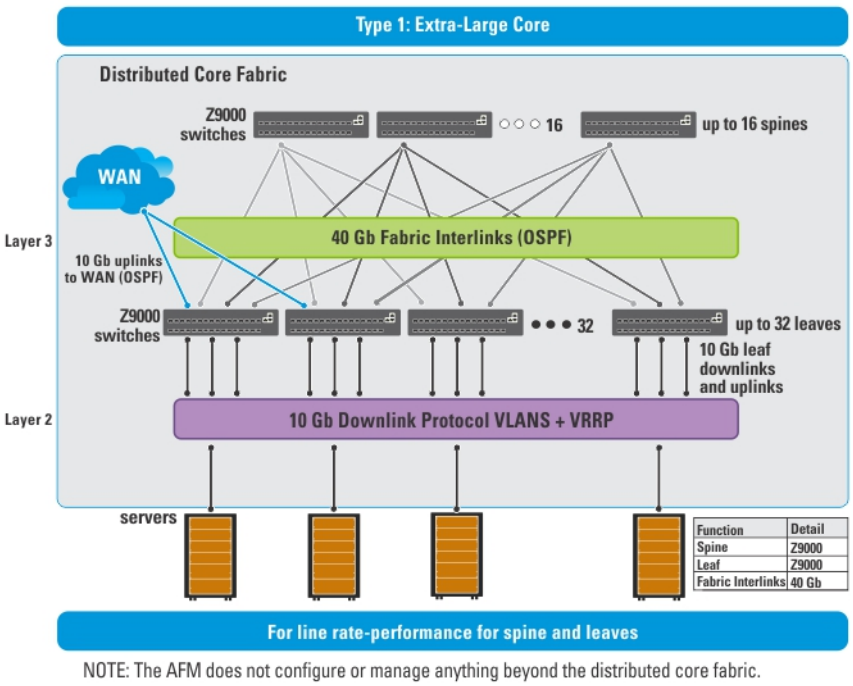
  NOTE: Specify an even number of uplinks. The minimum number of uplinks is two. One uplink is for redundancy.

- **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 3. 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.

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 initial loops that may occur before establishing VLT.

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.

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 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.

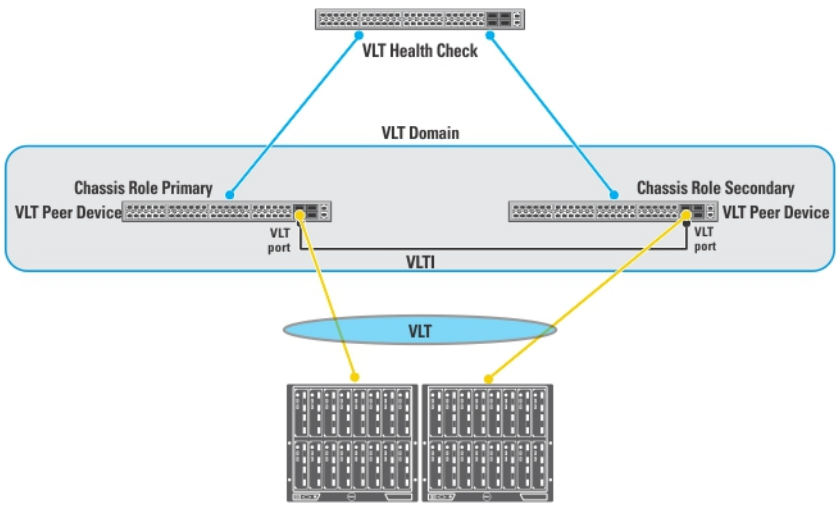


Figure 4. VLT Components

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.

2

Getting Started

The Active Fabric Manager (AFM) user interface provides easy-to-use wizards that allow you to design a new fabric or to edit an existing fabric based on current workload requirements and future needs.

NOTE: To view this documentation in AFM, from the Help drop-down menu, select User Guide.

To display the **Getting Started** tab, start AFM.

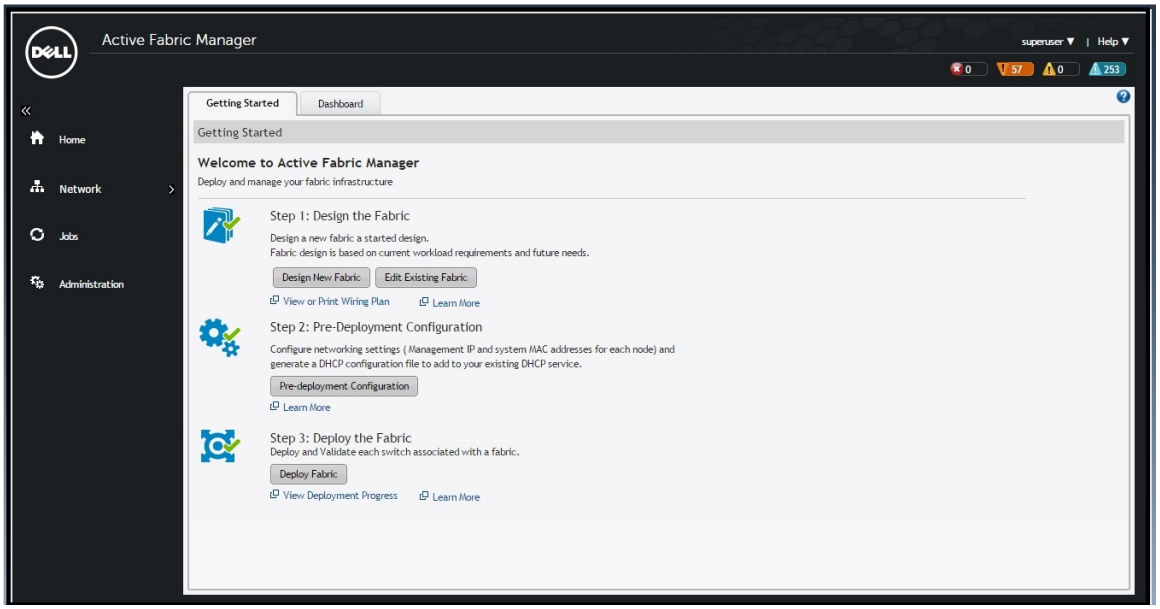


Figure 5. Getting Started

For information on installing AFM, including instructions on completing the initial setup, see the *Active Fabric Manager for Microsoft Cloud Platform System Installation Guide*.

Fabric Design Overview

To design and deploy a one, two, three, or four-rack distributed core design:

1. Gather required information.
2. Design the fabric.
   Related links:
   - Conventional Core Versus Distributed Core Overview
   - Distributed Core Design Considerations
3. Build the physical network.
4. Configure the following settings:
   - TFTP/FTP/SCP Settings
   - SNMP Configuration
   - CLI Credentials
5. Prepare the Fabric for Deployment

6. Deploy the Fabric
7. Validate the deployed fabric against the fabric design.
8. Monitor the fabric health and performance. See Performance Management.

To provision the fabric, enter the Dell networking operating system CLI user's credentials and enable the configuration credential for all the switches in the fabric. For information about this topic, see CLI Credentials.

Distributed Core Design Considerations

When designing the distributed core fabric, consider the following:

- AFM-CPS 2.2(0.0) manages Dell Network S4048-ON, S3048-ON, S4810, and S55 switches.
- AFM-CPS 1.0 manages Dell Networking S4810 and S55 switches.

Important: If you are using a switch that has already been deployed, reset its factory settings. The switch must be in Bare Metal Provision (BMP) mode. For information on BMP, see the *Dell Networking Configuration Guide*.

Templates in AFM-CPS

AFM-CPS requires a template and a template value file to deploy. The template file is based on the deployment configuration file from Microsoft.

The value for `${ variablename }` is unique for each deployment. A default template file is included with AFM. Provide the template value file using the Microsoft IP Address Generator tool. Use the `<SubnetName>` value for the gateway and the `<AddressName>` value for the IP address.

The template value file contains the value for each variable in the following format: *variablename=variablevalue*. Create a unique template value file for each deployment using the Microsoft IP Address Generator.

CPS Templates

AFM-CPS uses one template file for configuration:

- The template value file is prepopulated with the variable values after running the IP Address Generator tool against this file. Edit these values before deploying AFM.
- The template file associates the variables and edited information from the template file with the commands AFM uses to deploy the switches. Associate this file with the correct switch on the Pre-Deployment Wizard — Switch Specific Configuration screen.

Editing Template Value Files

1. Open the template value file (`Template_Value_NumberofRacks_tokenized.txt`) provided with CPS.
2. Look for the section of the file titled `MANUAL EDIT START`.
3. Copy the rack numbers from the file.

```
# These are the Rack Number for the Racks.
SU1_RackNumber=1
SU2_RackNumber=2
#SU3_RackNumber=44
#SU4_RackNumber=45
LB_RackNumber=0
```

NOTE: The # indicates a variable value that you can change. Do not change variable values for lines that do not begin with a #.

4. Note the AFM logging address.

```
# LOGGING is IP V4 address, which will act as syslog server for the switches.
LOGGING=@@("SWMGMT-SU01","AFMVM",4,"{0}")@@
```

5. Note the host names of the border switches for the aggregation devices.

```
# These are host name of the border connecting to Agg Ports. This is used for
description of Ports/PortChannel.
uplinkHostName_0_0=Ealplaswd01-labdist-e0
uplinkHostName_0_1=Ealplaswd02-labdist-e0
uplinkHostName_0_2=Ealplaswd01-labdist-e1
uplinkHostName_0_3=Ealplaswd02-labdist-e1
```

6. Configure the port channel values.

<codeblock cid="1bsB5O"># All four uplink Port Channel number should always be configured, irrespective it is used or NOT.

Following are the default values, which can be changed if needed.

uplinkPortChannel_0_0=86

uplinkPortChannel_0_1=87

uplinkPortChannel_0_2=88

uplinkPortChannel_0_3=89</codeblock>

7. Configure the NTP values.

NOTE: The default time zone is the universal time coordinated (UTC) time zone. Coordinated universal time (UTC) is the time standard based on the International Atomic Time standard, commonly known as Greenwich Mean time. When determining system time, include the differentiator between UTC and your local time zone. For example, San Jose, CA is the Pacific time zone with a UTC offset of -8.

- To change the time, change the `CLOCK_TIMEZONE` value to offset the time (for example, `-5` to move the time back by five hours or `2` to move the time forward two hours). The range is 1–23.
- To convert to daylight saving time, change the `CLOCK_SUMMER_TIMEZONE` to the three-letter name for your local time zone (for example, `EST` to change to Eastern Standard Time). To display the local time zone information, use the `show clock` command.

```
CLOCK_TIMEZONE=EST -5
CLOCK_SUMMER_TIMEZONE=EDT
CLOCK_DAYLIGHT_SAVING=2 Sun Mar 02:00 1 Sun Nov 02:00
```

NOTE: Do not edit after `END MANUAL EDIT` or unexpected behavior might occur.

3

Designing a Fabric

To design a Layer 3 two-tier distributed core fabric, use the **Fabric Design** wizard.
The design consists of a wiring plan and network topology information. Refer also to Network Deployment Summary.

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

- Create a fabric
- Edit and expand an existing fabric
- Delete the fabric
- View the wiring diagram
- Display the status of the fabric design (if the design, predeployment, 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 —
   Choose a fabric design type:
   a. Number of Racks — Select the number of racks
   b. Hardware platform — Select the type of switches (CPS 2014 or CPS 2016)
2. Fabric Design — Output

NOTE: After designing the fabric, prepare it for deployment. For more information, see Pre-Deployment — Introduction.

Network Deployment Summary

You can 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, see the following table for phases, states, and descriptions.

Table 1. Fabric Configuration Phases and States

Phase	State	State Description
Design	Complete	All required input to complete the design is available.
Pre-deployment Configuration	Required	Required Pre-deployment Configuration information for the switches is necessary.

Phase	State	State Description
		The Pre-deployment Configuration state for all switches is Required.
	Error	Pre-deployment Error exists when a configuration file transfer fails 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. 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.
	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. 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. During this state, AFM 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.

Phase	State	State Description
	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. 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 2. Switch Level States

Phase	State	State Description
Design	Complete	Fabric design is complete for the switch.
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. **NOTE: 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. Deployment can be initiated/re-initiated only if Pre-deployment Configuration is complete.
	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.

Phase	State	State Description
		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.

Designing a Fabric

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

AFM-CPS 2.2(0.0) Fabric Designs

- **One rack** — Contains one S3048-ON switch and five S4048-ON switches (two for aggregation, two tenants configured as a VLT pair, and two data center switches)
- **Two racks** — Contains two S3048-ON switches and (10) S4048-ON switches (two for aggregation, four tenants configured as a VLT pair, and four data center switches)
- **Three racks** — Contains three S3048-ON switches and (15) S4048-ON switches (three for aggregation, six tenants configured as a VLT pair, and six data center switches)
- **Four racks** — Contains four S3048-ON switches and (20) S4048-ON switches (four for aggregation, eight tenants configured as a VLT pair, and eight data center switches)

The aggregation, tenant, and data center switches are connected using a distributed core mesh. The management port of each S4048-ON switch in the same rack connects to the S3048-ON switch from ports 37–41. Each rack has its own subnet and default gateway. AFM-CPS 2.2(0.0) also supports the fabric designs listed for AFM-CPS 1.0. In addition, AFM-CPS 2.2(0.0) supports a one-rack fabric with S4810 and S55 devices.

AFM-CPS 1.0 Fabric Designs

- **Two racks** — Contains two S55 switches and (10) S4810 switches (two for aggregation, four tenants configured as a VLT pair, and four data center switches)
- **Three racks** — Contains three S55 switches and (15) S4810 switches (three for aggregation, six tenants configured as a VLT pair, and six data center switches)
- **Four racks** — Contains four S55 switches and (20) S4810 switches (four for aggregation, eight tenants configured as a VLT pair, and eight data center switches)

The aggregation, tenant, and data center switches are connected using a distributed core mesh. The management port of each S4810 switch in the same rack connects to the S55 switch from port 37 to 41. Each rack has its own subnet and default gateway.

In the **Fabric Design** wizard you can create, edit, delete, and view the fabric.

To access the **Fabric Design** wizard, select one of the following methods:

- From the menu, click **Home** and then on the **Getting Started** tab, click **Design New Fabric**.
- From the menu, click **Network** and then on the **Design Fabric** tab, click **New Fabric**.

The **Fabric Design** wizard has the following screens:

- **Fabric Name and Rack** — Displays the fabric name, number of racks, hardware platforms, supported device types, and description.
- **Output** — Displays future switches and links and the fabric in the following formats:
  - Graphical wiring plan

- Tabular wiring plan
- Graphical network topology
- Tabular network topology

Fabric Design — Fabric Name and Rack

To generate a physical wiring diagram for the fabric during the design phase, enter your data center capacity requirements. The wiring diagram is typically given to the network operator who uses it to build the physical network.

1. From the menu, click **Network**.
2. On the **Design Fabric** tab, click **New Fabric**.

   The **Fabric Design** wizard appears.

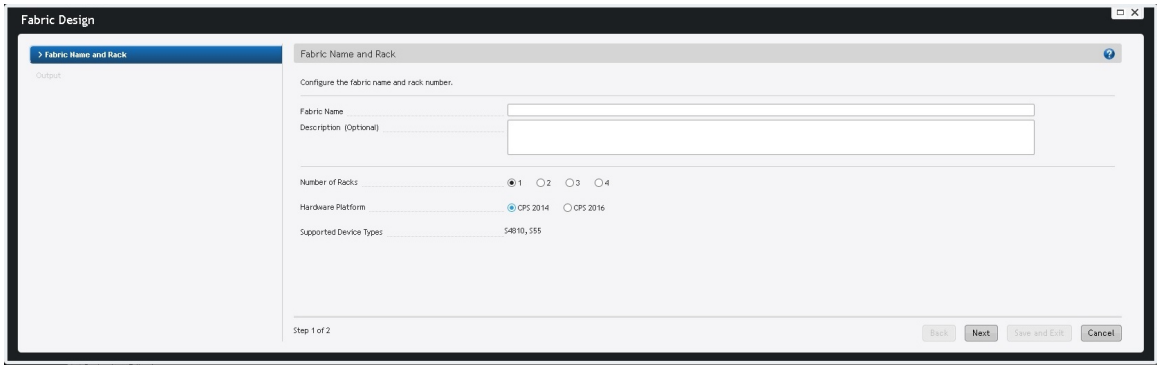


Figure 6. Fabric Name and Rack

3. In the **Fabric Name** field, enter the name of the fabric.

   The fabric name must be a unique name. The range is from one to 17 characters. AFM supports the following character types:

   - alphanumeric
   - underscore (_)

   When you specify the name of the fabric, AFM automatically names the switches in the fabric using the following convention: `{FabricName}-SU{RackNumber}AG-1` (where `{FabricName}` is the name of the fabric and `{RackNumber}` is the number of the rack.

   - Aggregation switches are `SU1AG-1` and `SU2AG-1`.
   - Tenant switches are named `SU1DC-1`, `SU1DC-2`, `SU1TE-1`, and `SU1TE-2` (where `DC` represents a data center switch and `TE` represents a tenant switch.)
4. (Optional) In the **Description** field, enter the description of the fabric.

   There is no character restriction. The range is from one to 128 characters.
5. In the **Number of Racks** field, select the number of racks to include in the fabric (one, two, three, or four).
6. In the **Hardware Platform** field, select the platform: **CPS 2014** or **CPS 2016**.

   NOTE: CPS 2015 is now named CPS 2016.
7. To confirm your selection and design the fabric, click **Save and Exit** or to review the designed fabric in the **Output** screen, click **Next**.

Expanding a Deployed Fabric

You can use the AFM-CPS 2.2(0.0) web client to expand an existing fabric from one to four racks.

NOTE: AFM-CPS 2.2(0.0) only supports expanding a deployed fabric for CPS 2016 racks.

1. From the menu, click **Home** (if necessary).
2. From the **Getting Started** tab, click **Edit Existing Fabric**.

The **Select a Fabric** dialog box appears.

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

   The **Fabric Design** wizard appears, displaying the fabric name as read-only.

4. In the **Description** field, add or edit the fabric description.
5. In the **Number of Racks** field, select a new number of racks.

   You cannot change the **Hardware Platform** setting for existing racks. The **Output** screen shows the network topology and wiring plan of the racks. You can view the topology and wiring diagrams using the **Graphical** and **Tabular** views.

6. To complete the design and update the wiring plan, click **Next** and then click **Finish**.

Deleting the Fabric

You can delete a fabric that is no longer needed.

1. From the menu, click **Network**.
2. Click the **Design Fabric** tab (if necessary).
3. Select the fabric that you want to delete.
4. Click **Delete Fabric**.
5. In the confirmation dialog box, click **Yes**.

Viewing the Wiring Plan

In the **Output** screen of the **Fabric Design** wizard, you can view the graphical wiring, tabular wiring, and network topology wiring plans for your fabric design.

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 the physical wiring plan that you can print or export as a PDF or Microsoft Visio file. The wiring plans display the cabling maps (the connections between the switches) and the switches and links for current and future expansion. Review the wiring plan and then export it to a file.

Typically, after the fabric design is approved, the wiring plan is given to the data center operator to build the physical network according to the fabric design. The fabric design is displayed in the following formats:

- **Graphical Network Topology** — Displays information about how the switches are physically connected using a topology map. By default, the links in the fabric do not automatically display. To display the links in the fabric, click a switch:
  - When you select an aggregation switch, the links to the access switches display.
  - When you select the access switches, the links to aggregation switches display.
  - When you select the core switches, the links to all the switches in the fabric (aggregation and access) display.

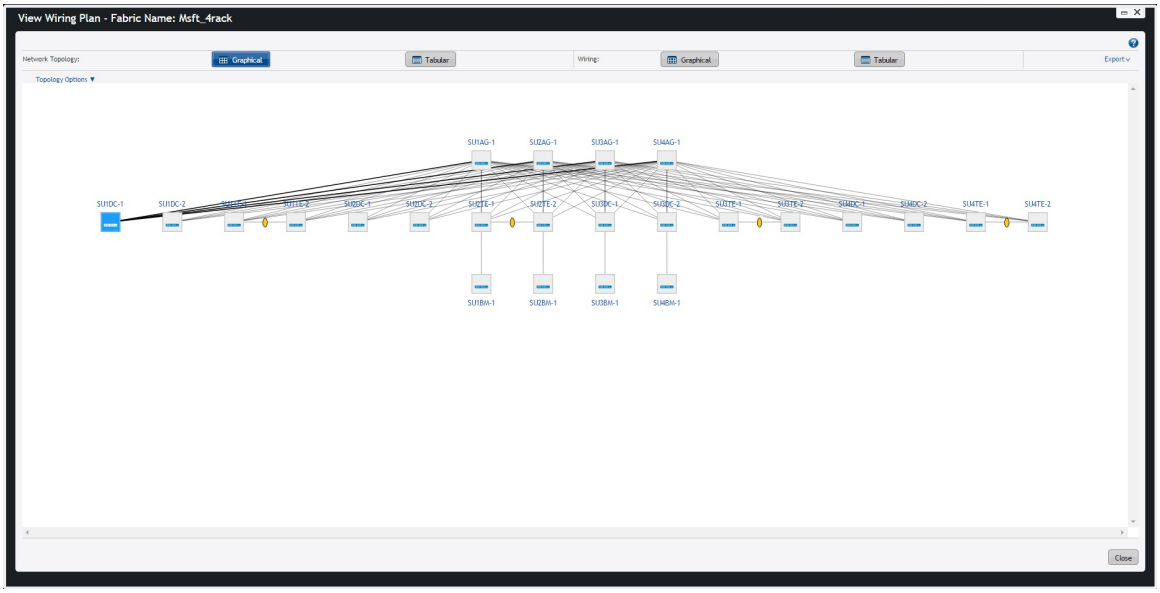


Figure 7. Network Topology Wiring Plan

- **Graphical Wiring Plan** — Displays information about how the switches are connected graphically.

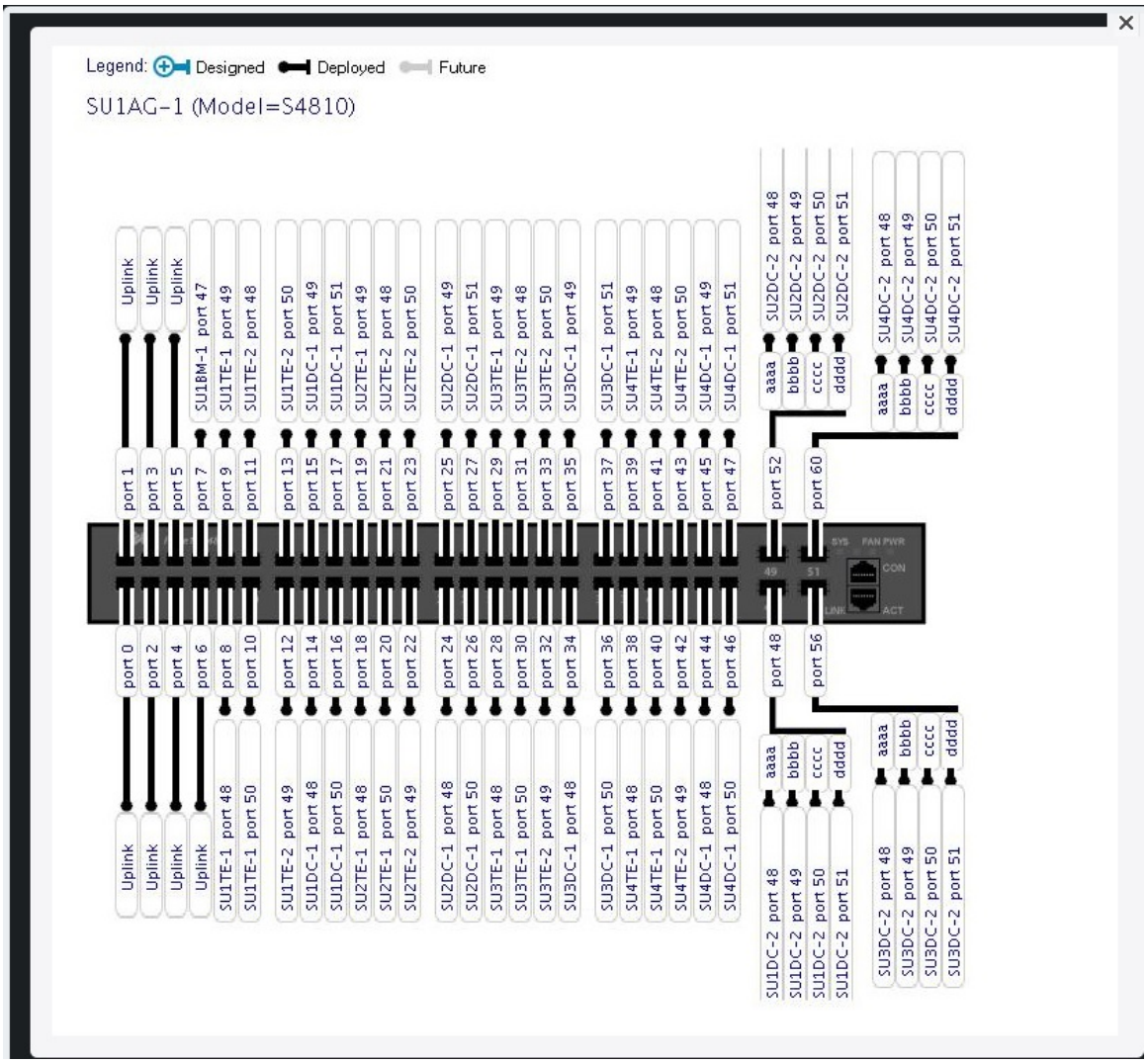


Figure 8. Graphical Wiring Plan

- **Tabular Wiring Plan** — Uses a tabular format to display information about how the switches are connected in the fabric design. The tabular wiring plan contains a list of switches with their names and ports that connect to the ports on the other switches in the fabric.

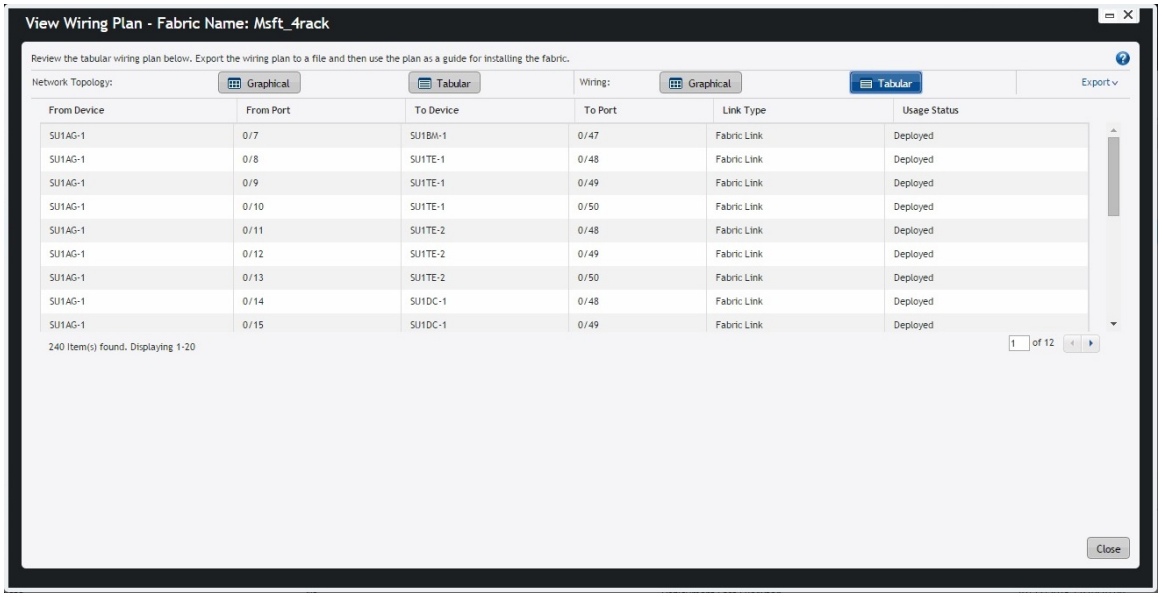


Figure 9. Tabular Wiring Plan

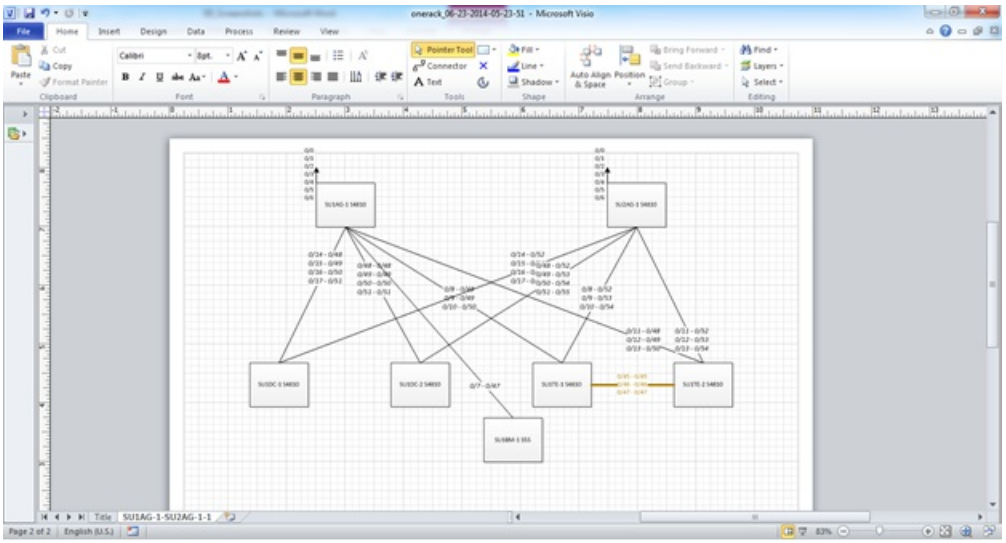


Figure 10. Visio Diagram of Wiring Plan

NOTE: If the wiring plan is customized, then the wiring validation procedure will be skipped for that particular wiring segment.

The following list describes the field names and functions.

- **From Device (Switch)**: Displays the name of the device from the side.
- **From Port**: Displays the port number on the switch from the side.
- **To Device (Switch)**: Displays the name of the device to the side.
- **To Port**: Displays the port number on the device to the side.
- **Usage Status**:
  - Current — Represents the links based on your current needs.
  - Future — Represents links based on the fabric's future needs.

– Displays usage status — current and future expansion.

1. Navigate to the **Network > Design Fabric > New Fabric > Output** screen.
2. Click the type of wiring plan that you want to export: **Wiring** (Graphical or Wiring), or **Network Topology** (Graphical or Tabular format).
3. Click the **Export** link.

   The **Generate Wiring Plan** window appears.
4. Specify the following export options.
   a. **PDF** — Table, Data, Graphical Wiring Plan, or Both.
   b. **Visio** — Network Topology.
5. Click the **Generate** button.

4

Configuring and Deploying the Fabric

This tab displays switch configuration settings including autogenerated and custom configurations. The following options are available:

- **Deploy Fabric** — Prepares the fabric for deployment and deploys the fabric.
  - Pre-Deployment Configuration
  - Deploying and Validating the Fabric
  - Viewing the DHCP Configuration File
- **Errors** — Displays errors in the fabric.
  - Deployment and Validation Errors
  - Troubleshooting
- **CLI Configuration** — Uses CLI commands for template and custom configuration.
  - Associating Templates
  - Custom CLI Configuration
  - Viewing Custom Configuration History
- **View Wiring Plan** — Displays the wiring plan in tabular, network topology, and graphical formats. You can export wiring plans.

Fabric Deployment Summary

To view switch configuration details, on the menu click **Network** > *Fabric Name*.

Then click the **Configure and Deploy** tab. On this tab, you can view the Fabric Deployment Summary screen. You can quickly identify the status of the switch configuration depending on the switch configuration phase and state shown in the following table.

Table 3. Switch Configuration Phases and States

Phase	State	State Description
Design	Complete	Indicates that the design is complete for the switch.
Pre-deployment	Required	Indicates that not all required Pre-deployment Configuration information was provided.
	Error	Indicates that an error occurred during file transfer (transfer of a minimum configuration file) to the FTP/TFTP server or an error occurred during automatic DHCP integration for the local DHCP server.

Phase	State	State Description
		NOTE: For a remote DHCP server, no errors are reported for the DHCP integration step because it is not automated step. Manually integrate the DHCP configuration.
	Complete	Indicates that Pre-deployment Configuration information is complete for the switch.
Deployment	Required	Indicates that deployment was never initiated for the switch or the Deployment state was reset due to a Design/Pre-deployment Configuration change. **NOTE: Deployment can be initiated or reinitiated only if Pre-deployment Configuration is in a Complete state.**
	In-progress	Indicates that deployment is in progress and provides the percentage of completion.
	Error	Indicates that deployment errors exist.
	Complete	Indicates that deployment for the switch was successful.
Validation	Required	Indicates that validation was not initiated for the switch or the Validation state was reset due to a Design/Pre-deployment Configuration/Deployment change. **NOTE: Validation can be initiated only if deployment is in a Complete state.**
	In-progress	Indicates that deployment is in progress and provides the percentage of completion.
	Error	Indicates that one or more validation errors exist.
	Complete	Indicates that validation was 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 4. Operations Allowed in Each Fabric State

Design State	Pre-deployment Configuration State	Deployment State	Validation State	Operation Allowed
Complete	Not Started	Not Started	Not Started	• View Wiring Plan • Edit Fabric (All fabric attributes) • Pre-deployment Configuration • Delete Fabric
Complete	Incomplete. The system MAC and IP address are not configured for the switches.	Not Started	Not Started	• View Wiring Plan • Edit Fabric (All fabric attributes except fabric name) • Pre-deployment Configuration • Delete Fabric
Complete	Partial Complete / Complete–Partial complete indicates that at least 1 switch has its system MAC and IP address configured.	Not Started	Not Started	• View Wiring Plan • Edit Fabric (All fabric attributes except fabric name) • Pre-deployment Configuration • View DHCP Configuration • Deploy and Validate Fabric • View Deployment and Validation Status • Delete Fabric
Complete	Partial Complete / Complete	In-progress	Not Started / In-progress / Error / Complete	• Edit Fabric Description • View Wiring Plan • View DHCP Configuration • View Deployment and Validation Status • Delete Fabric
Complete	Partial Complete / Complete	Incomplete / Partial Complete / Complete Incomplete indicates that AFM is deploying the switches. Complete indicates all the switches in the distributed fabric are deployed.	Not Started / In-progress / Error / Complete	• View Wiring Plan • Edit Fabric Description • Pre-deployment Configuration • View DHCP Configuration • Deploy and Validate Fabric — Validation is only allowed when deployment is partial or fully complete • View Deployment and Validation Status

Design State	Pre-deployment Configuration State	Deployment State	Validation State	Operation Allowed
				• Delete Fabric

Pre-Deployment Configuration

To prepare the fabric for deployment, complete the following tasks using the **Predeployment Configuration** wizard.

1. Pre-Deployment — Introduction
2. Pre-Deployment — BGP Password Authentication
3. Pre-Deployment — Assign Switch Identities
4. Pre-Deployment — Management IP
5. Pre-Deployment — Switch Specific Configuration
6. Pre-Deployment - Authentication Settings
7. Pre-Deployment — SNMP and CLI Credentials
8. Pre-Deployment — Software Images
9. Pre-Deployment — DHCP Integration
10. Pre-Deployment — Summary

Gathering Useful Information

To prepare for pre-deployment configuration, gather the following information:

- Obtain the CSV file that contains the system MAC addresses, Service Tag, and serial numbers for each switch provided from Dell manufacturing, or manually enter this information.
- Obtain the location of the switches, including the rack and row number, from your network administrator or network operator.
- Obtain the remote Trivial File Transfer Protocol (TFTP) / File Transfer Protocol (FTP) / Secure Copy Protocol(SCP) address from your network administrator or network operator. To specify a TFTP/FTP/SCP site, go to the **Administration** > **Settings** > **TFTP/FTP/SCP** screen. For information about which software packages to use, see the Release Notes.
- Download 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/FTP/SCP 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 a local DHCP. 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/SCP site during BMP. For information about BMP, see Pre-Deployment — DHCP Integration.
- For the **Predeployment Configuration** wizard:
  - Provide a switch configuration template
  - Provide a name/value file for the template variables
  - Assign system MAC, management IP addresses, and network routes and gateways for the switches deployment
  - Specify software images based on the switch types in the fabric
  - Generate a DHCP configuration file
  - Configure a DHCP server

Pre-Deployment — Introduction

To prepare a fabric for deployment, use the **Predeployment Configuration** wizard. After you initiate the pre-deployment configuration, you can only update the fabric description.
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.

To provide the fabric the minimum configuration to the switches, use the following **Predeployment Configuration** wizard screens. These screens automate the deployment process.

- **BGP Password Authentication** — Allows you to enable BGP neighbor password authentication.
- **Assign Switch Identities** — Assigns 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.
- **Management IP** — Specifies a management IP address to each switch.
- **Switch Specific Configuration** — Uploads a template containing the switch information variables.

  The template encoding type should be ANSI.
- **Authentication Settings** — Allows you to enable TACACS Authentication and configure it.
- **SNMP and CLI Credentials** — Configures SNMP and CLI credentials at the fabric level. Configure SNMP so that the AFM can perform SNMP queries on the switches in the fabric.
- **Software Images** — Specifies the TFTP, FTP or SCP address (local or remote server) and the path of the Dell Networking OS software image download to each type of switch. To stage the software, use this address.
- **DHCP Integration** — Creates a `dhcp.conf` file that loads the correct software image and then a configuration file for each type of switch. 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.
- **Summary** — Displays the fabric name, location of the software image, and DHCP configuration file.

1. On the menu, click **Network** and then the *Fabric Name*.
2. Click the **Configure and Deploy** tab.
3. From the **Deploy Fabric** menu, select **Pre-deployment Configuration**.

   The **Predeployment Configuration** wizard appears.
4. Review the introduction, verify that you have the required information, and click **Next**.

   The **BGP Password Authentication** screen appears.

Pre-Deployment — BGP Password Authentication

To setup BGP password authentication on the switches in the fabric, use the **BGP Password Authentication** screen of the **Predeployment Configuration** wizard.

1. On the menu, click **Network** and then the *Fabric Name*.
2. Click the **Configure and Deploy** tab.
3. From the **Deploy Fabric** menu, select **Pre-deployment Configuration**.

   The **Predeployment Configuration** wizard appears.
4. Navigate to the **BGP Password Authentication** screen.

5. Click the check box next to **Enable BGP Authentication** to enable the feature.
6. Enter a password in the **BGP Password** field.
7. Re-enter the password in the **BGP Confirm Password** field.
8. Click **Save and Exit** to exit the predeployment configuration wizard or **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 of the **Predeployment Configuration** wizard.

The following is a sample `.csv` file.

Table 5. 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. On the menu, click **Network** and then the *Fabric Name*.
3. Click the **Configure and Deploy** tab.
4. From the **Deploy Fabric** menu, select **Pre-deployment Configuration**.

   The **Predeployment Configuration** wizard appears.
5. Navigate to the **Assign Switch Identities** screen.
6. Click **Choose File** and specify the path of the `.csv` file.

   NOTE: If you do not have this file, manually enter this information in the System MAC Address fields.
7. Click **Upload**.
8. Click the **Choose MAC** icon in each row and associate the switch name with the MAC address, serial number (optional), 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.
9. Associate the system MAC address, serial number, and Service Tag with each switch.
10. Click **Next** to go to the **Management IP** screen.

Predeployment — Management IP

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

1. From the menu, click **Network** and then the *Fabric Name*.
2. Click the **Configure and Deploy** tab.
3. From the **Deploy Fabric** menu, select **Pre-deployment Configuration**.

   The **Predeployment Configuration** wizard appears.
4. Navigate to the **Management IP** screen.
5. In the **Start Management IP Address/Prefix** fields, enter the starting management IP address and prefix.
6. In the **Network** field, enter the route and prefix of the management interface.

   You can click **Auto-fill Selected Switches** to assign the network.
7. In the **Gateway** field, enter the address of the default gateway for the management interface.

You can click **Auto-fill Selected Switches** to assign the gateway.

8. To assign a management IP address, select the switches.
9. Click **Auto-fill Selected Switches**.

   The system automatically assigns a management IP address and gateway (if not already specified), and the network to all the selected switches in the fabric.
10. Click **Next** to go to the **Switch Specific Configuration** screen.

Pre-Deployment — Switch-Specific Configuration

You can specify switch-specific configuration on the **Switch Specific Configuration** screen of the **Predeployment Configuration** wizard.

NOTE: Before you begin, verify that you have the template and template value file. For more information, see Templates in AFM-CPS and CPS Templates.

1. On the menu, click **Network** and then the *Fabric Name*.
2. Click the **Configure and Deploy** tab.
3. From the **Deploy Fabric** menu, select **Pre-deployment Configuration**.

   The **Predeployment Configuration** wizard appears.
4. Navigate to the **Switch Specific Configuration** screen.

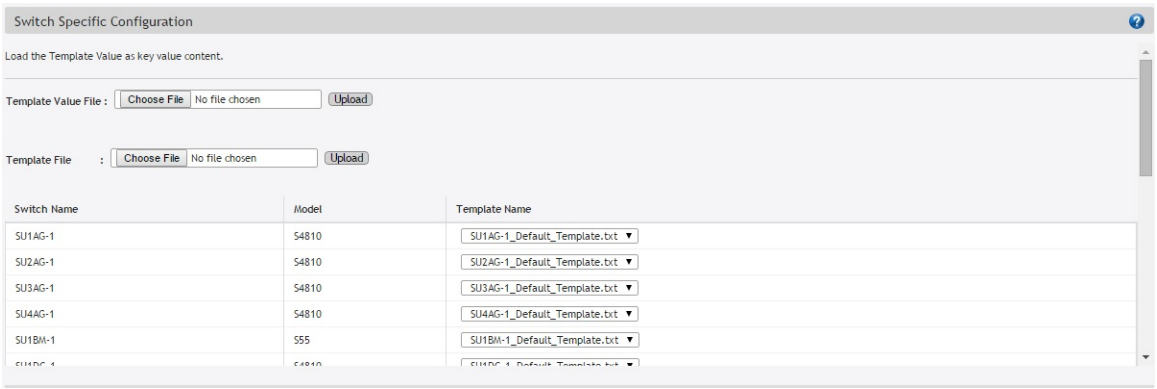


Figure 11. Predeployment — Switch Specific Configuration

5. In the **Template Value File** field, click **Browse** and select the template value file.

   NOTE: By default, the template is assigned to the switch. If you are using an existing template, you do not need to perform any additional steps.
6. Click **Upload**.
7. In the **Template File** field, click **Browse** and select the template file.
8. Click **Upload**.
9. Assign a template for each switch by selecting one from the **Template Name** menu.

   NOTE: The menu shows only the switch-specific template and any uploaded custom template.
10. After you assign a template for each switch, click **Next**.

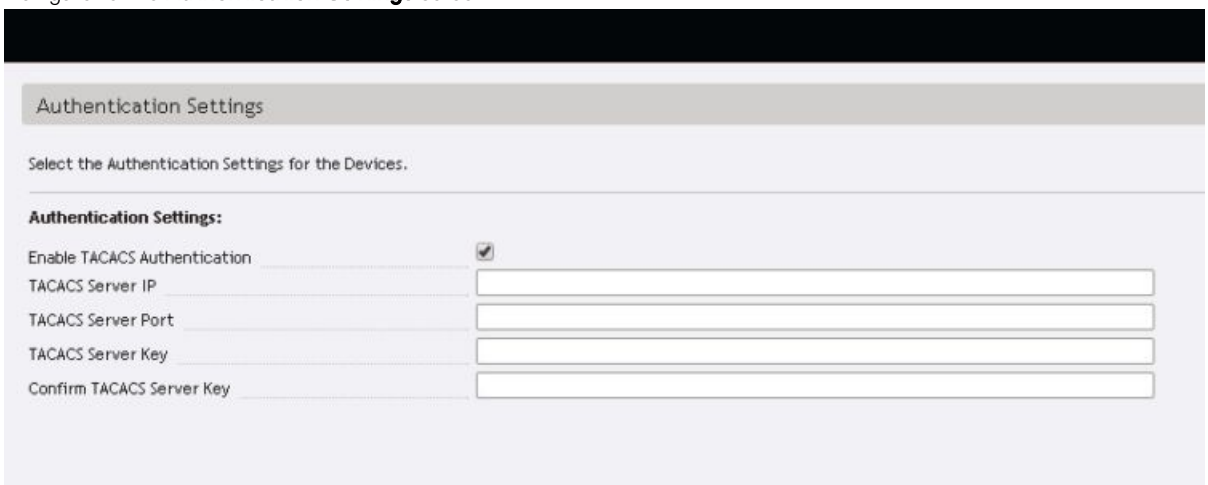
    NOTE: AFM validates the template and template values when you click Next. If the configuration file values do not match, a warning displays the missing variable names for each switch.

    After the template and template values are validated, the **Authentication Settings** screen appears.

Pre-Deployment — Authentication Settings

To setup TACACS Authentication on the switches in the fabric, use the **Authentication Settings** screen of the **Predeployment Configuration** wizard.

1. On the menu, click **Network** and then the *Fabric Name*.
2. Click the **Configure and Deploy** tab.
3. From the **Deploy Fabric** menu, select **Pre-deployment Configuration**.
   The **Predeployment Configuration** wizard appears.
4. Navigate to the **Authentication Settings** screen.



5. Click the check box next to **Enable TACACS Authentication** to enable the feature. Note, if TACACS is used for authentication, you will need a TACACS server to be configured. Click here for the instructions to setup a TACACS server.
6. Enter the **TACACS Server IP**, **TACACS Server Port**, and **TACACS Server Key** in the respective fields.
   The TACACS default server port is 49.
7. Re-enter the **TACACS Server Key** in the **Confirm TACACS Server Key** field.
8. Click **Save and Exit** to exit the predeployment configuration wizard or **Next** to go to the **SNMP and CLI Credentials** screen.

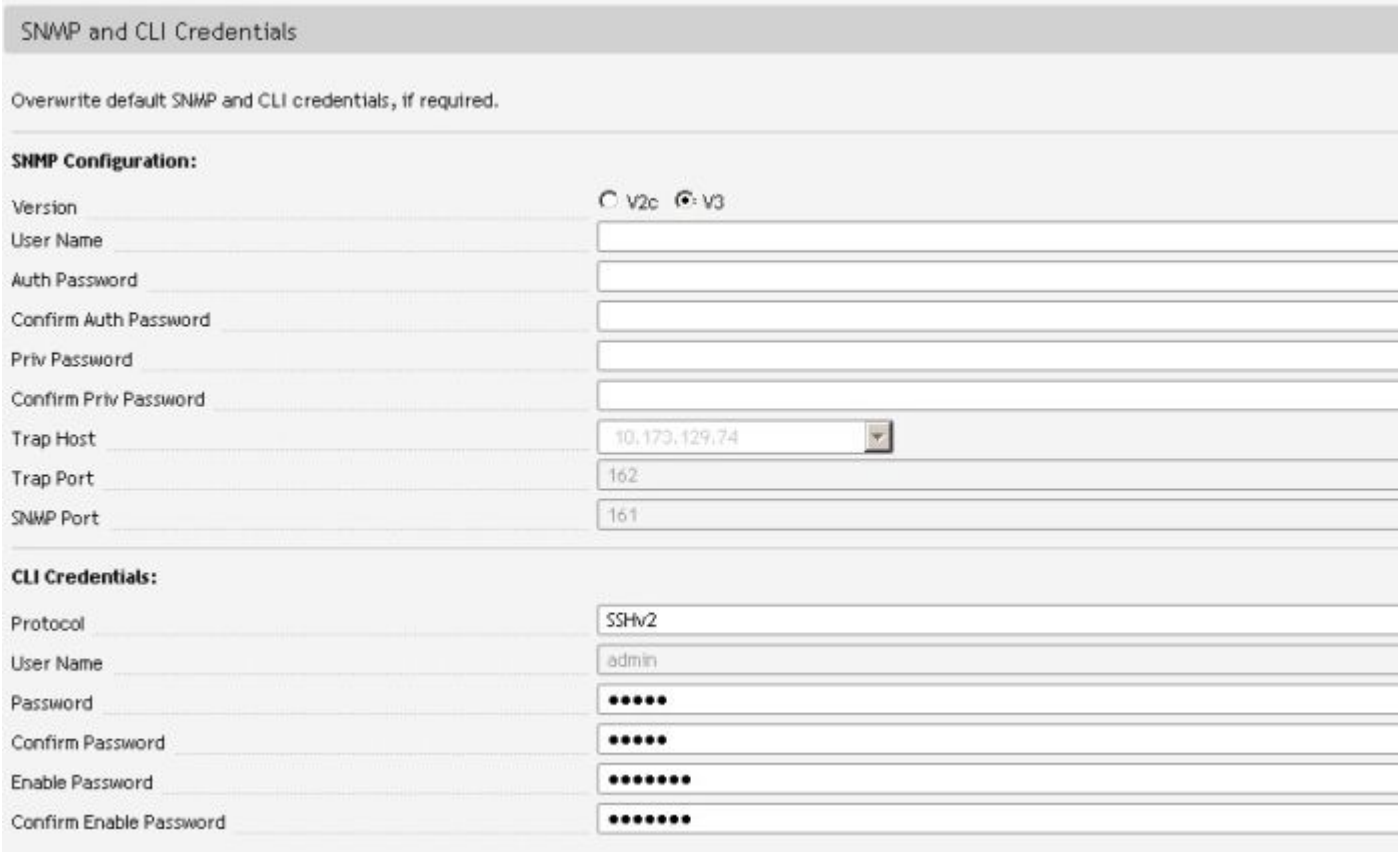
Pre-Deployment — SNMP and CLI Credentials

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 of the **Predeployment Configuration** wizard.
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.

To setup **SNMP V2c** or **V3** settings follow the respective flow:

1. On the menu, click **Network** and then the *Fabric Name*.
2. Click the **Configure and Deploy** tab.
3. From the **Deploy Fabric** menu, select **Pre-deployment Configuration**.
   The **Predeployment Configuration** wizard appears.
4. Navigate to the **SNMP and CLI Credentials** screen.

5. In the Version field, select **V2c** or **V3**.



If you select **V2c** follow the steps below. For **V3** follow this flow.

6. In the **Read Community String** field, enter the read community string (for example, `public`).
7. In the **Write Community String** field, enter the write community string (for example, `private`).

   The **Trap Host**, **Trap Port**, and **SNMP** fields are set by default and not configurable. The default trap port is 162 and the default SNMP port is 161.
8. **Protocol** — The protocol chosen in the Administration settings would be shown.
9. In the **User Name** — Enter the user name.
10. In the **Password** — Enter the password.
11. In the **Confirm Password** — confirm the password. The privilege level is a read-only field and the default is 15.
12. In the **Enable Password** — enter a password for the privilege level.
13. In the **Confirm Enable Password** — confirm the enabled password for the privilege level.
14. Click **Next** to go to the **Software Images** screen.

Pre-Deployment — Software Images

To specify which software images to stage for each type of switch in the fabric from a TFTP, FTP or SCP site, use the **Software Images** screen of the **Predeployment Configuration Wizard**.
The software image must be the same for each type of platform. Place the software images for the switches on the TFTP, FTP or SCP 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, FTP or SCP site, navigate to the **Administration > Settings** tab > **TFTP/FTP/SCP Settings**.

NOTE:

- Before you begin, make sure that you have loaded on to the TFTP, FTP or SCP site, the software image for each type of switch.
- To download the latest FTOS switch software version, see the “Upload Switch Software" section in the *AFM-CPS Installation Guide*.
- SCP support is available only from FTOS 9.10(0.1)P13 or later.
- The S55 switch does not support SCP.

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

Pre-Deployment — DHCP Integration

The **DHCP Integration** screen of the **Predeployment Configuration** wizard uses the information configured at the **Assign Switch Identities**, **Management IP**, and **Software Images** screens to create a DHCP configuration file named `dhcpd.conf`, 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, FTP or SCP 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, FTP or SCP 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, see 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. On the menu, click **Network** and then the *Fabric Name*.
2. Click the **Configure and Deploy** tab.
3. From the **Deploy Fabric** menu, select **Pre-deployment Configuration**.
   The **Predeployment Configuration** wizard appears.
4. Navigate to the **DHCP Integration** screen.
5. Click **Save File** and specify the location for the generated DHCP configuration file or you can copy and paste the configuration into the text field.
6. Install the DHCP file onto the DHCP server before deploying the fabric.
7. Click **Next** to go to the **Summary** screen.

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** and then the *Fabric Name*.
2. Click the **Configure and Deploy** tab.
3. From the **Deploy Fabric** drop-down menu, select **View DHCP Configuration**.
   The **DHCP Integration** dialog box appears.
4. Click **Save to** to save the DHCP configuration file to your local disk.

Pre-Deployment — Summary

To review the pre-deployment configuration, use the **Summary** screen of the **Predeployment Configuration** wizard, 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, FTP or SCP server

1. On the menu, click **Network** and then the *Fabric Name*.
2. Click the **Configure and Deploy** tab.
3. From the **Deploy Fabric** menu, select **Pre-deployment Configuration**.
   The **Predeployment Configuration** wizard appears.
4. Navigate to the **Summary** screen.
5. Review the pre-deployment configuration.
6. To commit your changes, click **Finish**.

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 Pre-Deployment — DHCP Integration and the *Open Automation Guide*.

3. On the menu, click **Network** and then the *Fabric Name*.
4. To deploy and validate the fabric, click the **Configure and Deploy** tab and from the **Deploy Fabric** menu, select **Deploy and Validate**.

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.

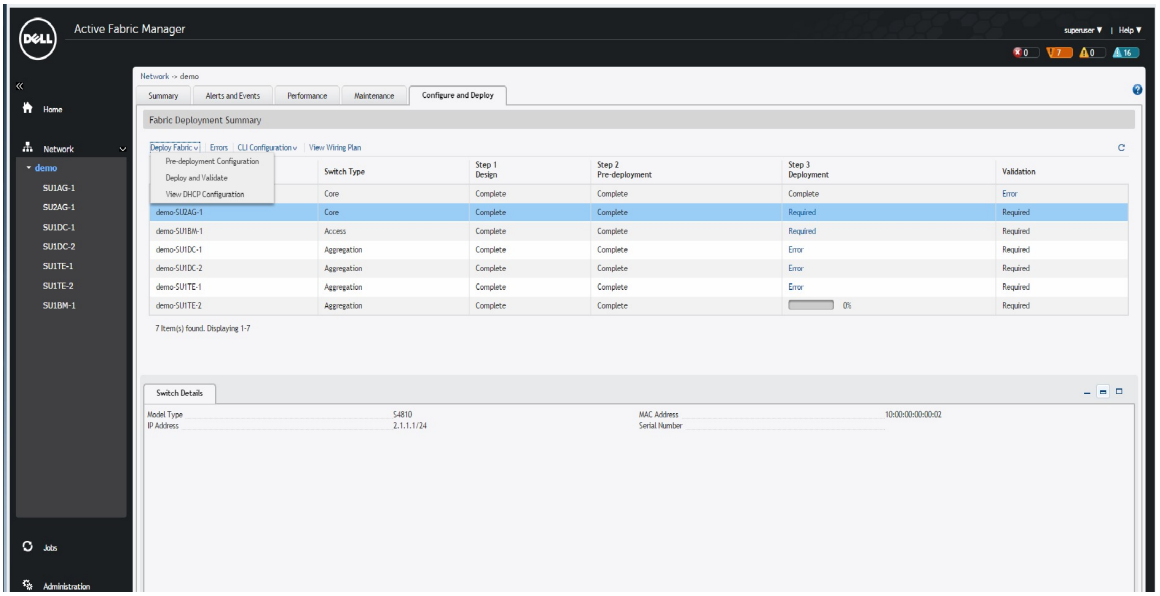


Figure 12. Configure and Deploy — Deploy and Validate

NOTE: During initial deployment, the BMP-process wait time to install the software onto the switches is approximately 10 minutes.

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 6. 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/SCP connectivity and FTP credentials
5	Error	Device cleanup task failed	1. Verify the switch connectivity from AFM using Telnet or SSH. 2. Redeploy the switch. See the following procedure.

Number	Status	Status Details	Recommended Action
6	Error	Complete config upload failed	1. Verify TFTP/FTP/SCP or Telnet/SSH connectivity and verify credentials. 2. Redeploy the switch. See the following procedure.
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	1. Verify Telnet or SSH connectivity from AFM. 2. Redeploy the switch. See the following procedure.
10	InProgress	Verifying that the switch is eligible for the deploy process	None
11	InProgress	Protocol transfer in progress...	None
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	Back up 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, FTP or SCP server.
2. Verify that you have configured the correct TFTP, FTP or SCP address on the **Administration > Settings** tab. If you change the TFTP server now, the address is not correct unless you re-configure the predeployment.
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 start-up 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, see Pre-Deployment — DHCP Integration. For information about how to view the DHCP configuration file for a fabric, see 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, see Validation. See also Troubleshooting. For information about the progress and status of selected switches and operations allowed during a fabric state, see Operations Allowed During Each Fabric State and Network Deployment Summary.

Advanced Configuration

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

- View the Auto-Generated Configuration
- Associate the Templates to Fabric Switches
- 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** 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 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 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.

- **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.

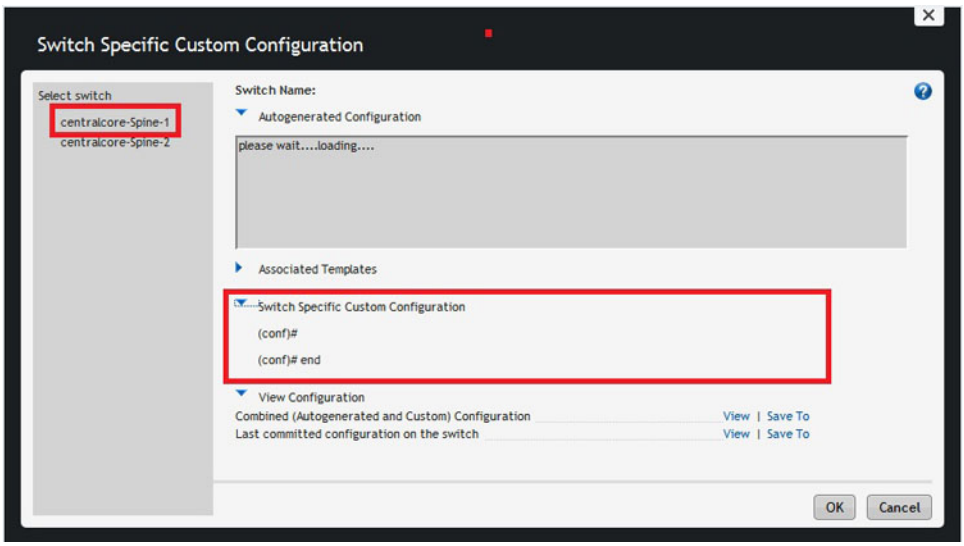


Figure 13. Switch-Specific Custom Configuration

View the autogenerated 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 autogenerated 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 edit the combined configuration, click **Save To** to save the combined autogenerated 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.

NOTE: If the wiring is customized, then the wiring validation procedure will be skipped for that particular wiring segment.

After fixing errors found during validation, verify that all issues were resolved according to the planned fabric by validating the fabric again.

Table 7. 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: 1. From the menu, click **Network >** *Fabric Name* and then click the **Configure and Deploy** tab. 2. Click **Errors**. 3. To view error details, click the **Discovered Errors** tab. 4. Fix any errors.
4	Error	Switch is not reachable	To verify switch connectivity from AFM: 1. From the menu, click **Network >** *Fabric Name* and then click the **Configure and Deploy** tab. 2. Click **Errors**. 3. To view error details, click the **Discovered Errors** tab. 4. Fix any errors.
5	Error	Switch is not Discovered	To verify switch connectivity from AFM: 1. From the menu, click **Network >** *Fabric Name* and then click the **Configure and Deploy** tab. 2. Click **Errors**. 3. To view error details, click the **Discovered Errors** tab. 4. Fix any errors.
6	Error	Configuration mismatch errors exist	To check for switch configuration mismatch errors:

Number	Status	Status Details	Response Action
			1. From the menu, click **Network** > *Fabric Name* and then click the **Configure and Deploy** tab. 2. Click **Errors**. 3. To view error details, click the **Config Mismatch Errors** tab. 4. Fix any errors.
7	Error	Custom Configuration errors exist	To check for switch custom configuration errors: 1. From the menu, click **Network >** *Fabric Name* and then click the **Configure and Deploy** tab. 2. Click **Errors**. 3. To view error details, click the **Custom Config Errors** tab. 4. Fix any errors.
8	Error	Wiring Errors Exist	To verify the Errors in the **Wiring Error** tab: 1. From the menu, click **Network >** *Fabric Name* and then click the **Configure and Deploy** tab. 2. Click **Errors**. 3. To view error details, click the **Wiring Errors** tab. 4. Fix any errors.
9	Error	Interlink Ping Errors	To check for interlink ping errors: 1. From the menu, click **Network >** *Fabric Name* and then click the **Configure and Deploy** tab. 2. Click **Errors**. 3. To view error details, click the **Interlink Ping Errors** tab. 4. Fix any errors.
10	Error	Loopback Ping Errors	To check for interlink ping errors: 1. From the menu, click **Network >** *Fabric Name* and then click the **Configure and Deploy** tab. 2. Click **Errors**.

Number	Status	Status Details	Response Action
			3. To view error details, click the **Loopback Ping Errors** tab. 4. Fix any errors.
11	InProgress	Node validation in progress...	None
12	InProgress	Configuration Validation in progress...	None
13	InProgress	Wiring Validation in progress...	None

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 errors found during validation, verify that all issues were fixed according to the planned fabric by validating the fabric again.
9. Click **Close**.

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:

- Associating Templates
- Viewing Custom Configuration History
- Adding a Switch-Specific Custom Configuration

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 manually create associations. 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.

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.

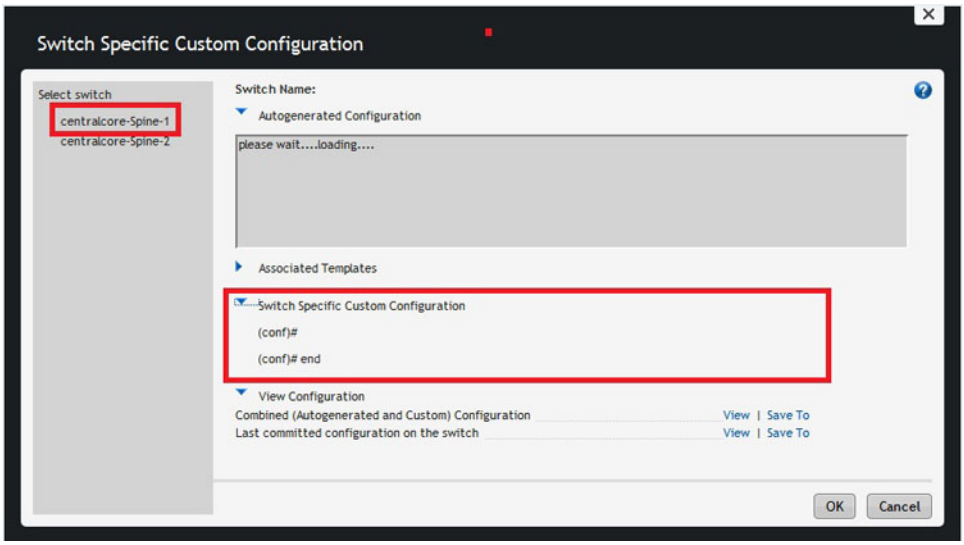


Figure 14. Switch-Specific Custom Configuration

View the autogenerated 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 autogenerated 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 edit the combined configuration, click **Save To** to save the combined autogenerated 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.

5

Viewing the Fabric

You can view detailed information about the fabric using tabular or graphical formats.
See the following topics:

- Dashboard
- Fabric Summary
- Switch Summary

Related Links: Fabric Performance Management

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.

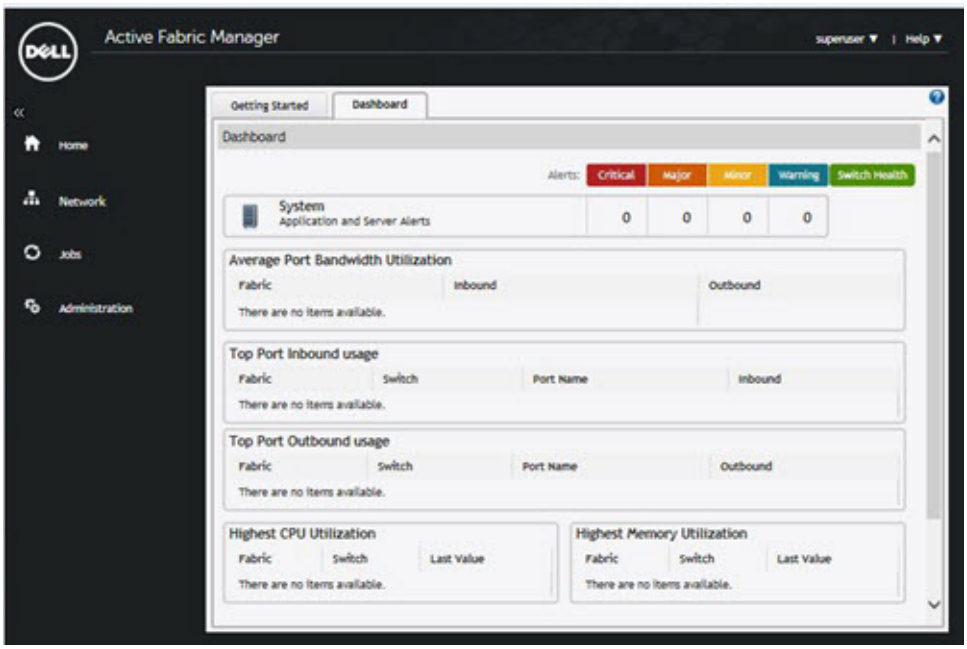


Figure 15. Active Fabric Manager Dashboard

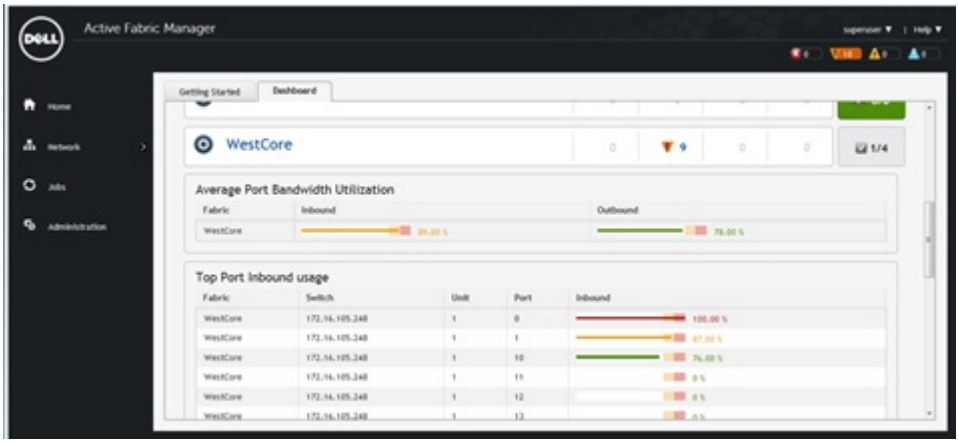


Figure 16. Dashboard with Color Codes

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 Inbound Usage** — View the ten most frequently used inbound ports for all fabrics by:
  - Fabric
  - Switch
  - Port number
  - Inbound (%): number with color code bar

Table 8. Inbound Link Utilization Color Codes

Color	Range	Description
Green (Good)	x < 80%	Represents normal inbound link utilization.
Yellow (Minor)	x > = 80% and x < 90%	Represents low link utilization.
Red (Critical)	x > = 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.

- **Top Port Outbound Usage** — View the ten most frequently used ports for all fabrics by:
  - Fabric
  - Switch
  - Port number
  - Outbound (%): number with color code bar

Table 9. Outbound Link Utilization Color Codes

Color	Range	Description
Green (Good)	x < 80%	Represents normal outbound link utilization.
Yellow (Minor)	x > = 80% and x < 90%	Represents low link utilization.
Red (Critical)	x > = 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 (percent): number with color code bar

Table 10. CPU Utilization Color Codes

Color	Range	Description
Green (Good)	x < 70%	Represents normal CPU utilization.
Yellow (Minor)	x > = 70% and x < 80%	Represents low CPU utilization.
Red (Critical)	x > = 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 (percent): number with color code

Table 11. 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.

Fabric Summary

You can view information about a network fabric and its constituent switches in tabular or graphical format on the **Summary** tab of the **Network** > *Fabric Name* screen.

This information refreshes every 60 seconds. You can click the **Refresh** button for an immediate data refresh.

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** menu, click **Manage/Un-manage Switch**.
- To view additional performance statistics about a fabric:
  a. Select the switch row.
  b. From the **Action** 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. To zoom in, click the **+** button; to zoom out, click the **-** button.

The following option is available from the **Action** menu:

- **View Switch Topology** — View the switch summary view. See Switch Summary for more information.
- **Manage/Un-manage Switch** — `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.

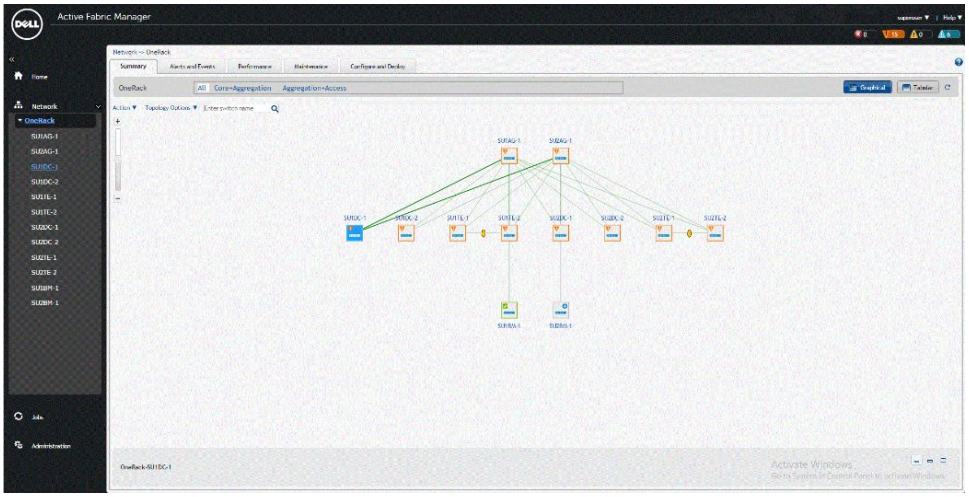


Figure 17. Fabric Summary — Graphical View

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** or **Hide Links** — View or hide 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.

You can expand the bottom pane of either view to view switch links, hardware, VLT domains, VLANs, or port channels in tabular format.

Switch Summary

To view switch summary information from a graphical view, from the menu, click **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. This information refreshes every 60 seconds. You can click the **Refresh** button for an immediate data refresh.

You can perform the following tasks in the **Summary** tab:

- To display information about the state of the port in the Graphical view, click the port.
- To display port legends, click the **Port Legends** arrow.

You can view additional information in the **Summary** and **Performance** tabs.

6

Troubleshooting

This section contains the following topics:

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** 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 12. Validation Alarms

Alarm	Recommended Action
Validation failed because the switch cannot be discovered.	Log on to the switch console to isolate the fault.

Alarm	Recommended Action
	NOTE: Make sure that the switch has been power cycled and check the physical connection.
Validation failed because the switch has a mismatch MAC address. Validation failed because the switch has a name mismatch. Validation failed because the switch has a model mismatch.	1. To verify that you have correctly mapped the system MAC address to the associated switches: a. On the menu, click **Network >** *Fabric Name* and then the **Configure and Deploy** tab. b. From the **Deploy Fabric** menu, select **Pre-deployment Configuration**. c. Navigate to the **Assign Switch Identities** screen and check the system MAC address mapping for the associated switches. 2. To verify changes, validate the switch: a. On the menu, click **Network >** *Fabric Name* and then the **Configure and Deploy** tab. b. From the **Deploy Fabric** drop-down menu, select **Deploy and Validate**. c. Click the **Validation** tab. d. Select the switch and click **Validate Selected**.
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.	1. Review the wiring plan. 2. Wire according to the wiring plan to fix the wiring mismatch. 3. Make sure that the ports on the switches are mapped accurately.
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.	1. On the menu, click **Network >** *Fabric Name* and then the **Configure and Deploy** tab. 2. Click **Errors**. 3. Select the **Config Mismatch Errors** tab. 4. Review the configuration mismatch and correct the configuration errors.

Deployment and Validation Errors

Pre-deployment Errors

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

Table 13. Pre-deployment Errors

Error Details	Recommended Action
Failed to transfer minimum configuration file using TFTP/FTP/SCP.	Verify the TFTP, FTP or SCP connectivity from AFM. For FTP, verify the credentials and restart the **DHCP Integration** step using the **Predeployment Configuration** wizard.

Error Details	Recommended Action
	1. On the menu, click **Network >** *Fabric Name* and then the **Configure and Deploy** tab. 2. From the **Deploy Fabric** menu, select **Pre-deployment Configuration**. 3. Navigate to the **DHCP Integration** screen and re-configure the settings.
Overwrite DHCP contents to local DHCP server failed.	Verify the following: • the permissions of the directory • disk space availability on the AFM server • the local DHCP server configuration Restart the **DHCP Integration** step using the **Predeployment Configuration** wizard. 1. On the menu, click **Network >** *Fabric Name* and then the **Configure and Deploy** tab. 2. From the **Deploy Fabric** menu, select **Pre-deployment Configuration**. 3. Navigate to the **DHCP Integration** screen and re-configure the settings.

Deployment Errors

To troubleshoot deployment errors, use the following table.

Table 14. Deployment Errors

Error Details	Recommended Action
Protocol transfer failed	1. Verify TFTP, FTP or SCP connectivity from AFM. For FTP, verify the credentials. 2. Restart switch deployment from the **Configure and Deploy** tab by selecting the switch from the list. a. On the menu, click **Network >** *Fabric Name* and then the **Configure and Deploy** tab. b. From the **Deploy Fabric** menu, select **Deploy and Validate**. c. Click the **Deploy** tab. d. Select the switches and click **Deploy Selected**. e. In the confirmation dialog box, click **Yes**.
Device cleanup task failed	1. Verify Telnet or SSH connectivity from AFM. 2. Restart switch deployment from the **Configure and Deploy** tab by selecting the switch from the list. a. On the menu, click **Network** > *Fabric Name* and then the **Configure and Deploy** tab. b. From the **Deploy Fabric** menu, select **Deploy and Validate**. c. Click the **Deploy** tab. d. Select the switches and lick **Deploy Selected**. e. In the confirmation dialog box, click **Yes**.
Complete configuration upload failed	1. Verify TFTP/FTP/SCP or Telnet/SSH connectivity from AFM.

Error Details	Recommended Action
	2. Restart the deployment of the switch from the **Network > Fabric Name > Configure and Deploy** tab by selecting the switch from the list. a. On the menu, click **Network** > *Fabric Name* and then the **Configure and Deploy** tab. b. From the **Deploy Fabric** menu, select **Deploy and Validate**. c. Click the **Deploy** tab. d. Select the switches and click **Deploy Selected**. e. In the confirmation dialog box, click **Yes**.
Smart script transfer failed	1. Verify connectivity to the switch from AFM. 2. Restart switch deployment from the **Network >** *Fabric Name* > **Configure and Deploy** tab by selecting the switch from the list. a. On the menu, click **Network** > *Fabric Name* and then the **Configure and Deploy** tab. b. From the **Deploy Fabric** menu, select **Deploy and Validate**. c. Click the **Deploy** tab. d. Select the switches and click **Deploy Selected**. e. In the confirmation dialog box, click **Yes**.
Custom configuration upload failed	1. Verify the switch login credentials and commands. 2. Restart switch deployment from the **Network** > *Fabric Name* **> Configure and Deploy** tab by selecting the switch from the list. a. On the menu, click **Network** > *Fabric Name* and then the **Configure and Deploy** tab. b. From the **Deploy Fabric** menu, select **Deploy and Validate**. c. Click the **Deploy** tab. d. Select the switches and click **Deploy Selected**. e. In the confirmation dialog box, click **Yes**.
Backup config failed	1. Verify the Telnet SSH connectivity. 2. Restart switch deployment from the **Network** > *Fabric Name* > **Configure and Deploy** tab by selecting the switch from the list. a. On the menu, click **Network >** *Fabric Name* and then the **Configure and Deploy** tab. b. From the **Deploy Fabric** menu, select **Deploy and Validate**. c. Click the **Deploy** tab. d. Select the switches and click **Deploy Selected**. e. In the confirmation dialog box, click **Yes**.

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:

NOTE: If the wiring is customized, then the wiring validation procedure will be skipped for that particular wiring segment.

- Configuration
- Custom Configuration
- Custom Configuration Deployment
- Discovered Switch Errors
- Predeployment
- Undiscovered Switch Errors
- Wiring
- Interlink ping Errors
- Loopback ping Errors
- Deployment Response

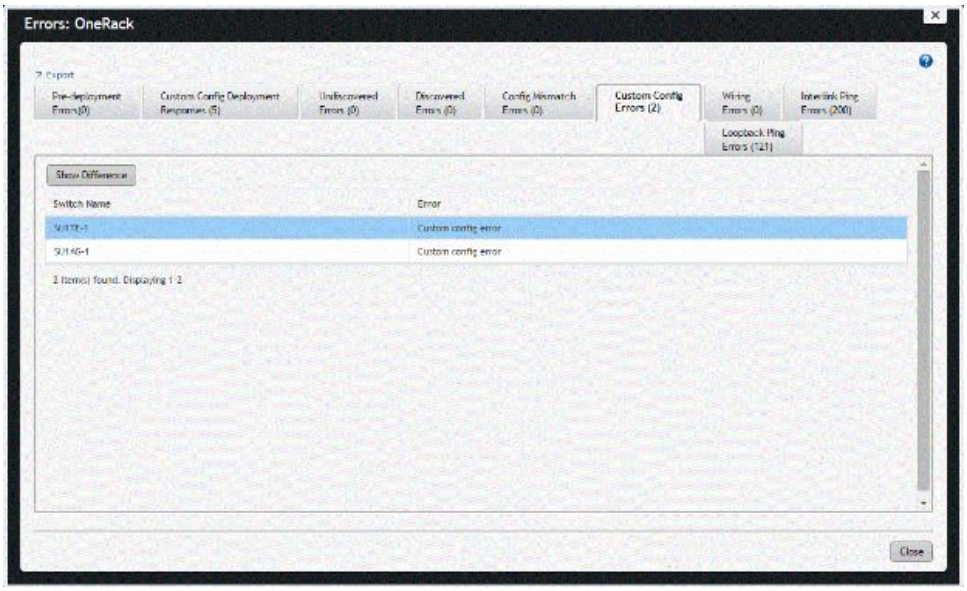


Figure 18. Validation Errors

Table 15. Configuration Errors

Error Details	Recommended Action
Configuration Mismatch	1. On the menu, click **Network >** *Fabric Name* and then the **Configure and Deploy** tab. 2. Click **Errors**. 3. Click the **Config Errors Mismatch** tab. 4. Click **View Mismatch**. 5. Review the configuration mismatch and correct the configuration errors. 6. Restart switch validation from the **Configure and Deploy** tab by selecting the switch from the list and from the **Deploy Fabric** menu, click **Deploy and Validate**. In the **Deploy and Validation** dialog box, click the **Validation** tab, select the switch and click **Validate Selected**.

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 16. Wiring Errors

Error Details	Recommended Action
Wiring Mismatch	1. Review the wiring plan. 2. Wire the switch according to the wiring plan to fix the wiring mismatch. 3. Validate the switch. a. On the menu, click **Network >** *Fabric Name* and then the **Configure and Deploy** tab. b. From the **Deploy Fabric** menu, select **Deploy and Validate**. c. Click the **Validation** tab. d. Select the switches and click **Validate Selected**.
Missing Link	1. Review the wiring plan. 2. Wire the switch according to the wiring plan to fix the missing link. 3. Validate the switch. a. On the menu, click **Network >** *Fabric Name* and then the **Configure and Deploy** tab. b. From the **Deploy Fabric** menu, select **Deploy and Validate**. c. Click the **Validation** tab. d. Select the switches and click **Validate Selected**.
Partial Link	1. Verify that the switch is wired according to the wiring plan. 2. Verify the connectivity on AFM from both switches in the link. 3. Validate the switch. a. On the menu, click **Network >** *Fabric Name* and then the **Configure and Deploy** tab. b. From the **Deploy Fabric** menu, select **Deploy and Validate**. c. Click the **Validation** tab. d. Select the switches and click **Validate Selected**.

Table 17. Undiscovered Switch Error

Error Details	Recommended Action
Undiscovered Switch Error	1. Verify that the IP address for the switch is valid. 2. If necessary, correct the pre-deployment configuration. 3. From the AFM server, verify connectivity to the switch. 4. Verify that the switch is running the minimum required software. 5. Validate the switch. a. On the menu, click **Network >** *Fabric Name* and then the **Configure and Deploy** tab. b. From the **Deploy Fabric** menu, select **Deploy and Validate**.

Error Details	Recommended Action
	c. Click the **Validation** tab. d. Select the switches and click **Validate Selected**.

Table 18. Discovered Switch Error

Error Details	Recommended Action
Disconnected	1. Verify connectivity from the AFM server to the switch. 2. Verify that the switch is running the minimum required software. 3. Validate the switch. a. On the menu, click **Network >** *Fabric Name* and then the **Configure and Deploy** tab. b. From the **Deploy Fabric** menu, select **Deploy and Validate**. c. Click the **Validation** tab. d. Select the switches and click **Validate Selected**.
Switch Name Mismatch	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. 2. Validate the switch. a. On the menu, click **Network >** *Fabric Name* and then the **Configure and Deploy** tab. b. From the **Deploy Fabric** menu, select **Deploy and Validate**. c. Click the **Validation** tab. d. Select the switches and click **Validate Selected**.
Switch Model Mismatch	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. 2. Validate the switch. a. On the menu, click **Network >** *Fabric Name* and then the **Configure and Deploy** tab. b. From the **Deploy Fabric** menu, select **Deploy and Validate**. c. Click the **Validation** tab. d. Select the switches and click **Validate Selected**.
System MAC Address Mismatch	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. 2. Validate the switch. a. On the menu, click **Network >** *Fabric Name* and then the **Configure and Deploy** tab. b. From the **Deploy Fabric** menu, select **Deploy and Validate**. c. Click the **Validation** tab. d. Select the switches and click **Validate Selected**.

Switch Deployment Status Errors

Table 19. Switch Deployment Status Errors

Switch Deployment Status	Description	Requires Action	Recommended Actions
NOT STARTED	Not Started	No	1. Start the switch deployment on the **Network >** *Fabric Name* **> Configure and Deploy** tab by selecting the switch from the list. 2. From the **Deploy Fabric** menu, select **Deploy and Validate**. 3. On the **Deploy** tab, select the switch and click **Deploy Selected**. **NOTE: Verify that the switch is in BMP mode.**
CONFIG GENERATION IN PROGRESS	Configuration File Generation In-progress	No	Information only
CONFIG GENERATION FAILED	Configuration File Generation Failed	Yes	1. Check the write permission for the AFM installation directory on the AFM server. 2. Verify that there is enough disk space on the AFM server. 3. Restart switch deployment from the **Network >** *Fabric Name* **> Configure and Deploy** tab by selecting the switch from the list. **NOTE: Verify that the switch is in BMP mode.** 4. From the **Deploy Fabric** menu, select **Deploy and Validate**. 5. On the **Deploy** tab, select the switch and click **Deploy Selected**.
CONFIG GENERATION SUCCESS	Configuration File Generation Completed Successfully	No	Information only
CONFIG FILE TRANSFER IN PROGRESS	Configuration File Transfer In-progress	No	Information only
CONFIG FILE TRANSFER FAILED	Configuration File Transfer Failed	Yes	1. Verify the connectivity to the TFTP server from the AFM server. 2. Restart switch deployment from the **Network >** *Fabric Name* **> Configure and Deploy** tab by selecting the switch from the list.

Switch Deployment Status	Description	Requires Action	Recommended Actions
			NOTE: Verify that the switch is in BMP mode. 3. From the **Deploy Fabric** menu, select **Deploy and Validate**. 4. On the **Deploy** tab, select the switch and click **Deploy Selected**.
CONFIG FILE TRANSFER SUCCESS	Configuration File Transferred Successfully	No	Information only
REQUEST TO DISCOVER NODE	Request To Discover Switch	Yes	1. Power on the switch. 2. Restart switch deployment from the **Network >** *Fabric Name* **> Configure and Deploy** tab by selecting the switch from the list. **NOTE: Verify that the switch is in BMP mode.** 3. From the **Deploy Fabric** menu, select **Deploy and Validate**. 4. On the **Deploy** tab, select the switch and click **Deploy Selected**.
MIN CONFIG UPLOAD INPROGRESS	Minimum Configuration Upload In-Progress	No	Information only
MIN CONFIG UPLOAD ERROR	Minimum Configuration Upload Error	Yes	1. Verify the connectivity to the TFTP/FTP/SCP server from the switch. 2. Resolve any errors the **Validation Status** column. 3. Verify that the system MAC address in the **dhcpd.conf** file matches the **csv.** file with the MAC addresses of the switches. 4. Verify that the **min.cfg** file is in the correct directory on the TFTP/FTP/SCP server. 5. Redeploy the switch from the **Network >** *Fabric Name* **> Configure and Deploy** tab by selecting the switch from the list. **NOTE: Verify that the switch is in BMP mode.** 6. From the **Deploy Fabric** menu, select **Deploy and Validate**.

Switch Deployment Status	Description	Requires Action	Recommended Actions
			7. On the **Deploy** tab, select the switch and click **Deploy Selected**.
MIN CONFIG UPLOAD COMPLETED	Minimum Configuration Upload Successful	No	Information only
INIT SOFT RELOAD	Initiated Soft Reload on Switch	No	Information only
INIT SOFT RELOAD ERROR	Error During Soft Reload on Switch	Yes	1. Check the switch syslogs for a reload command failure. 2. Resolve any errors. 3. Restart switch deployment from the **Network >** *Fabric Name* **> Configure and Deploy** tab by selecting the switch from the list. 4. From the **Deploy Fabric** menu, select **Deploy and Validate**. 5. On the **Deploy** tab, select the switch and click **Deploy Selected**. **NOTE: Verify that the switch is in BMP mode.**
PROTOCOL CONFIG UPLOAD INPROGRESS	Protocol Configuration Upload In-Progress	No	Information only
PROTOCOL CONFIG UPLOAD ERROR	Protocol Configuration Upload Error	Yes	1. Verify the connectivity to the TFTP server from switch. 2. Resolve any errors in the **Validation Status** column. 3. Verify that the DHCP server is running. 4. Verify that the CFG file is on the TFTP/FTP server and the switch can reach it using the **ping** command. 5. Redeploy the switch. **NOTE: Verify that the switch is not in BMP mode.** 6. Navigate to the **Network >** *Fabric Name* **> Configure and Deploy** tab by selecting the switch from the list. 7. From the **Deploy Fabric** menu, select **Deploy and Validate**. 8. On the **Deploy** tab, select the switch and click **Deploy Selected**.

Switch Deployment Status	Description	Requires Action	Recommended Actions
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	1. Verify the connectivity between AFM and the switch. 2. Resolve any errors in the **Validation Status** column. 3. Restart the deployment. **NOTE: Verify that the switch is not in BMP mode.** 4. Navigate to the **Network** > *Fabric Name* > **Configure and Deploy** tab by selecting the switch from the list. 5. From the **Deploy Fabric** menu, select **Deploy and Validate**. 6. On the **Deploy** tab, select the switch and click **Deploy Selected**.
UPLINK RECONFIGURED REDEPLOY REQUIRED	Uplink reconfigured, Redeployment of Switch is required	Yes	Restart switch deployment. **NOTE: Verify that the switch is not in BMP mode.** 1. Navigate to the **Network** > *Fabric Name* > **Configure and Deploy** tab by selecting the switch from the list. 2. From the **Deploy Fabric** menu, select **Deploy and Validate**. 3. On the **Deploy** tab, select the switch and click **Deploy Selected**.
REDEPLOYMENT REQUIRED	Redeployment of the switch is required	Yes	Restart switch deployment. **NOTE: Verify that the switch is not in BMP mode.** 1. Navigate to **Network** > *Fabric Name* > **Configure and Deploy** tab by selecting the switch from the list.

Switch Deployment Status	Description	Requires Action	Recommended Actions
			2. From the **Deploy Fabric** menu, select **Deploy and Validate**. 3. On the **Deploy** tab, select the switch and click **Deploy Selected**.

TFTP/FTP/SCP Errors

Table 20. Deployment Status Configuration Errors

Deployment Status	Error Category	Error Details	Recommended Action
TFTP/FTP/SCP Failed	Configuration Deployment Error	Error occurred during TFTP/FTP/SCP	1. Check the TFTP/FTP/SCP connectivity on the network. 2. Make sure that you have specified the correct TFTP/FTP/SCP address in the **Settings** tab of the **Administration** screen.

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.

7

Alerts and Events

This section contains the following topics:

- Current — Active Alerts
- Historical — Alerts and Events

Current Active Alerts

You can view current active network, fabric, and switch alerts. Alert information refreshes every 60 seconds. You can click the **Refresh** button for an immediate data refresh.
You can display alert information in the following ways:

- To filter active network alerts, from the menu, click **Network** and then click the **Alerts and Events** tab.

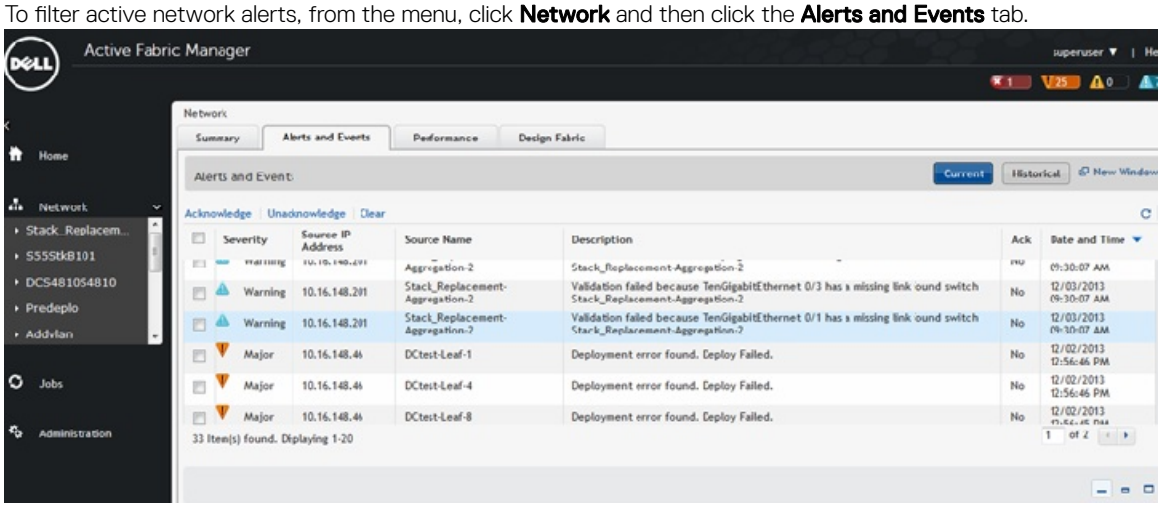


Figure 19. Network Alerts

- 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 fabric alerts, from the menu, click **Network >** *Fabric Name* and then click the **Alerts and Events** tab.

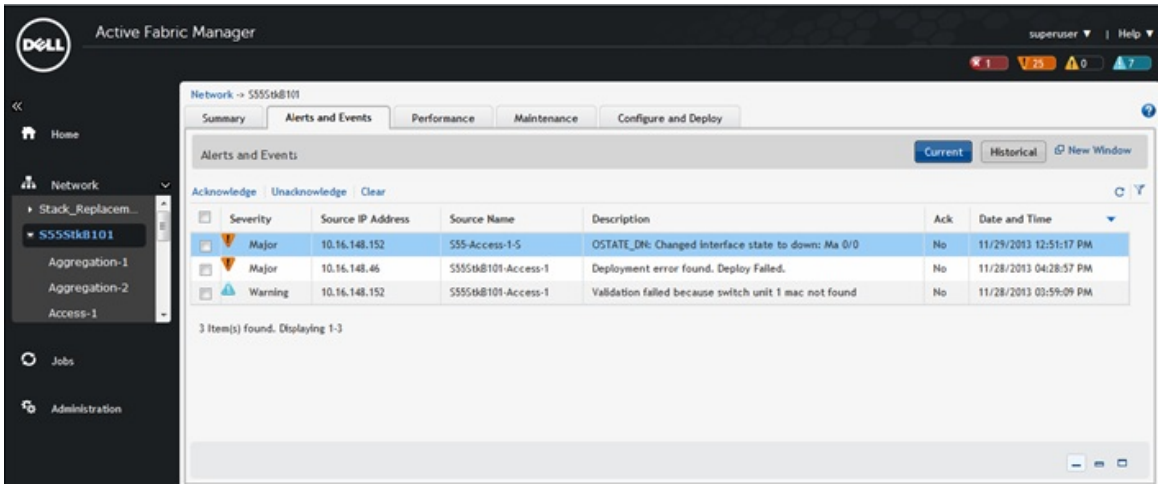


Figure 20. Fabric Alerts

- To filter active switch alerts, click **Network >** *Fabric Name* **>** *Switch Name* and then click the **Alerts and Events** tab.

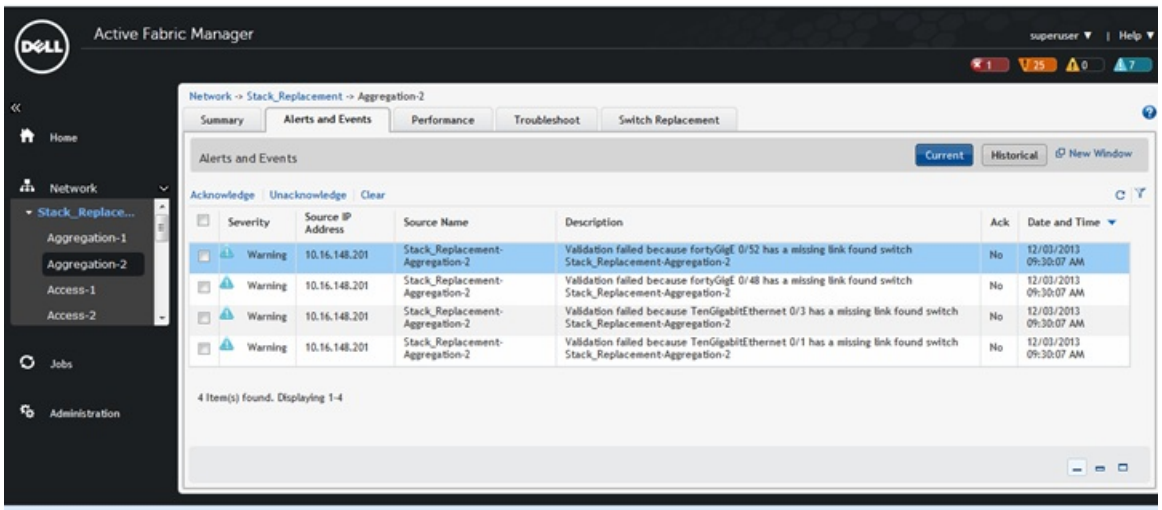


Figure 21. Switch Alerts

- 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**.

You can also filter alerts.

1. Make sure **Current** is selected.
2. Click the filtering icon on the right of the screen.
   The **Filter** dialog box appears.
3. To filter results, use the filter options: **Date From** and **Date To**.
4. In the **Severity** drop-down menu, select one of the following filtering criteria:
   - **All**
   - **Critical**
   - **Major**
   - **Minor**
   - **Warning**
   - **Cleared**
   - **Unknown**
   - **Info**

- **Indeterminate**

5. In the **Source IP Address** field, enter the source IP address.
6. In the **Source Name** field, enter the source name.
7. In the **Description** field, enter a description.
8. In the **Ack** (acknowledgement) drop-down menu, select one of the following options:
   - **All**
   - **Yes**
   - **No**
9. Click **Apply**.

Historical Alerts and Event History

On the **Alerts and Events** tab, you can view historical events at the network, fabric, or switch level.

This information refreshes every 60 seconds. You can click the **Refresh** button for an immediate data refresh. You can access this tab by clicking **Network** on the menu. You can filter the level displayed on this tab in the following ways:

- 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.

Whichever level you select, make sure to click **Historical**. You can also filter historical alerts.

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**.

8

Performance Management

This section contains the following topics:

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, see Dashboard.

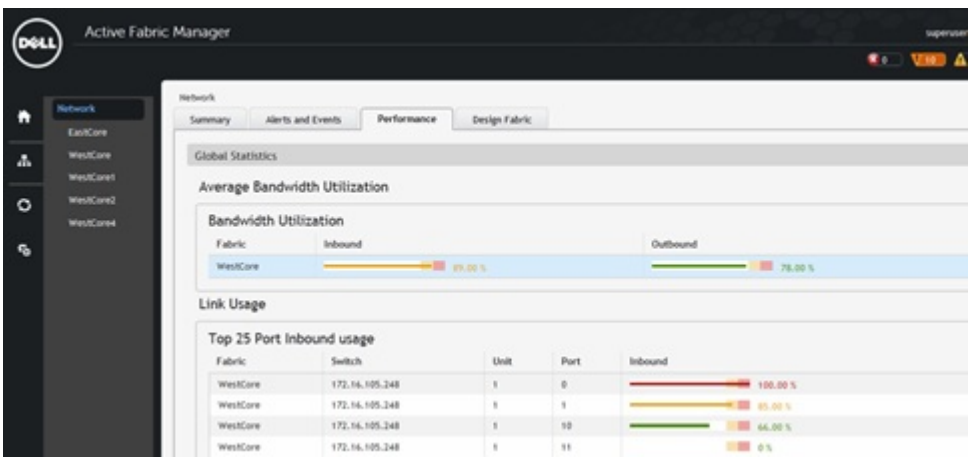


Figure 22. Global Statistics Screen of the Performance Tab

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

You access the **Performance** tab by clicking **Network >** *Fabric Name* on the menu.

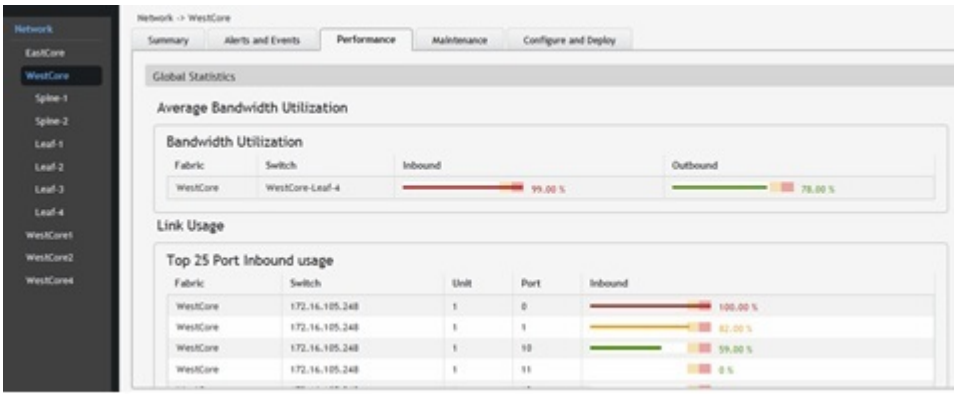


Figure 23. Fabric Statistics Screen — Performance Tab

Port Performance Management

1. From the menu, click **Network >** *Fabric Name* **>** *Switch Name* and then make sure that the **Summary** tab is selected.

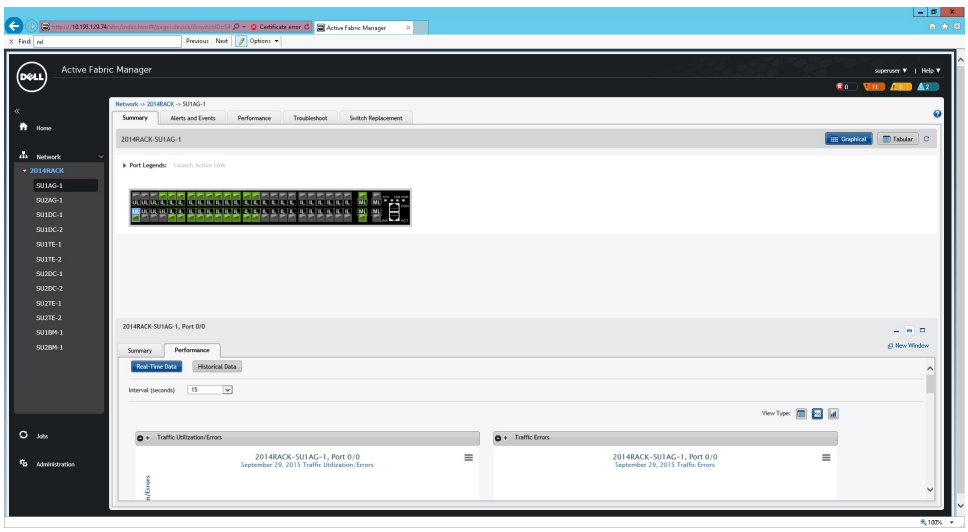


Figure 24. Port Performance Summary

2. Select a port and then click the **Performance** tab.
3. Select a data type:
   - **Real-Time Data**
   - **Historical**

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

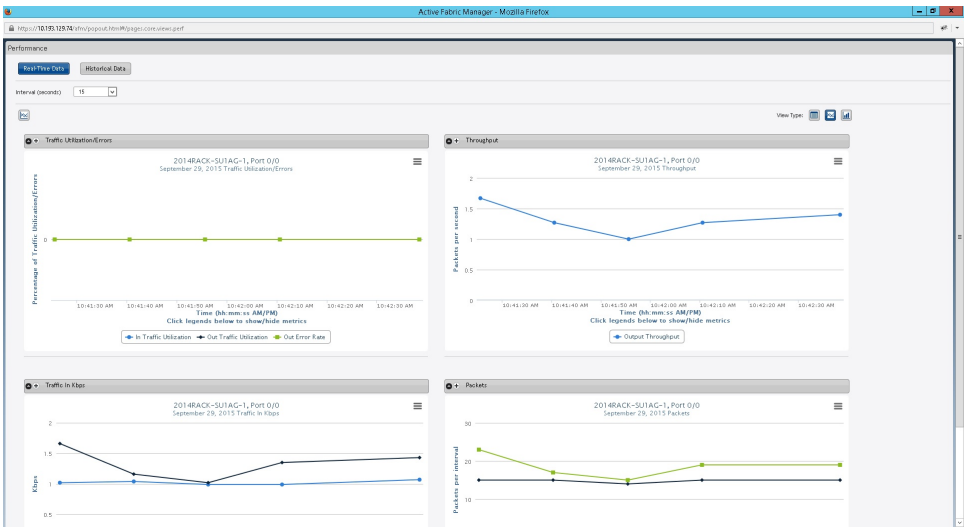


Figure 25. Detailed Port Performance

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** (default)
     - 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

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 appears 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 you can access by clicking Jobs from the menu.

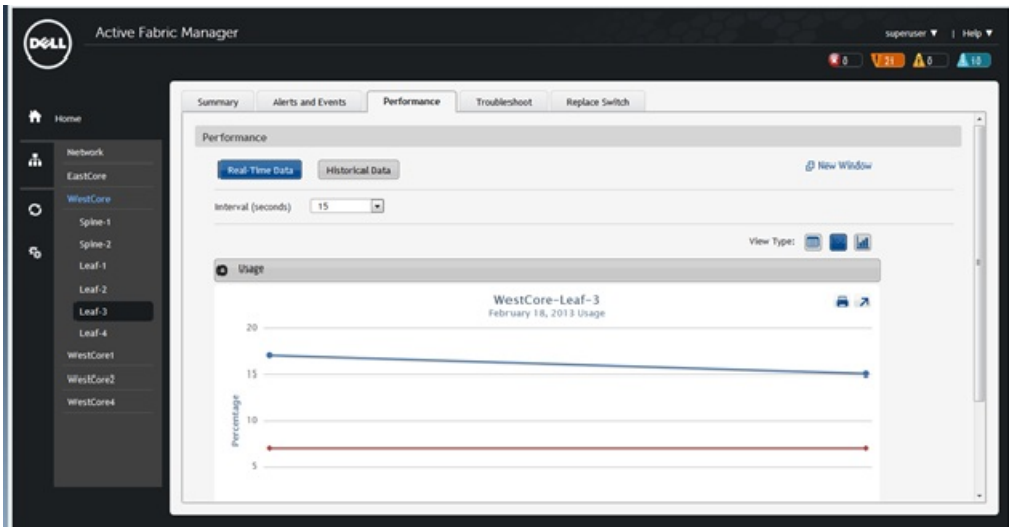


Figure 26. Switch Performance Tab

Data Collection

By default, AFM automatically enables data collection after deployment.
This information refreshes every 60 seconds. You can click the **Refresh** button for an immediate data refresh. 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**. 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 displays an alarm from the switch on the **Alerts and Events** tab.

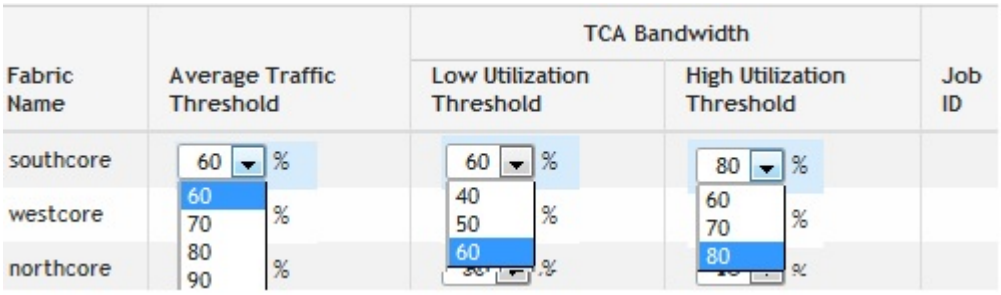


Figure 27. TCA Bandwidth

- **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.

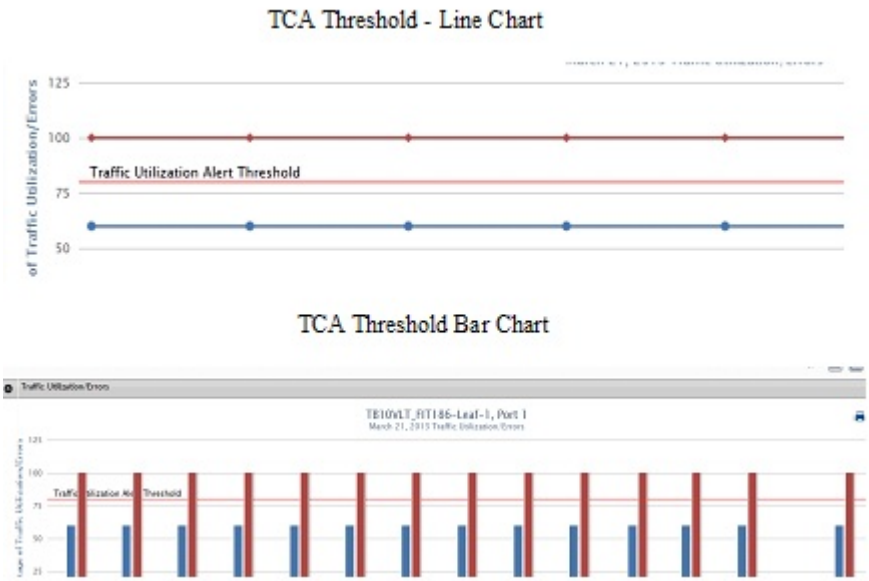


Figure 28. Traffic Utilization Alert Threshold

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

- Duplicating Reports

NOTE: To run a report, schedule data collection. See Data Collection.

Creating New Reports

You can create reports in the **Jobs** screen.

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**.
   The **Type and Output** screen appears.
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**.
   The **Monitors** screen appears.
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**.
    The **Switches** screen appears.
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**.
    The **Time Span** screen appears.
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**.

The list of reports on this tab refreshes every 60 seconds. You can click the **Refresh** button for an immediate data refresh.

Editing Reports

1. From the menu, click **Jobs** and then click the **Reports** tab.
2. Select the report and click **Edit**.
   The **Add/Modify Report** window appears.
3. Edit the report.
4. To navigate to different parts of the report, click **Next**.
5. In the **Summary** area, review the changes.
6. Click **Finish**.

Running Reports

Before running a report, schedule data collection. For information on scheduling data collection, see Data Collection.

1. From the menu, click **Jobs** and then click the **Reports** tab.
2. Select the report and click **Run**.

Duplicating Reports

You can create reports based on existing 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**.

9

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 System
- Install Keystore
- 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
- Back Database
- Restore 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.

Figure 29. AFM Virtual Appliance Options Screen

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 (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**.

Backing Up a Switch

On the **Backup 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.

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 start 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. (Optionally) In the **Description** field, enter a description for the schedule software update.
6. Click **Next**.

   The **Select Switches** screen appears.
7. On the **Select Switches** screen, in the **Available** area, select the fabric and then the switches (core, aggregation, and access) to update.
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, FTP or SCP site for the software updates, click **Edit TFTP, FTP or SCP settings**.
11. Enter the path and image name of the software file on the TFTP, FTP or SCP site for each type of switch.
12. Enter the path and image name of the software file on the TFTP, FTP or SCP 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**.

Enabling Standby Partition Software

To enable 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 All Racks, 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**.

Replacing a Switch

1. Decommission a Switch.
2. Replacing a Switch.
3. Deploy Replacement Switch.

NOTE: Replace the decommissioned switch with same switch type.

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, see 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**.

Replacing a Switch

Before you replace a switch, gather the following useful information:

- System MAC address, Service Tag and serial number for the replacement switch
- Location of the switch, including the rack and row number
- Remote Trivial File Transfer Protocol (TFTP) / File Transfer Protocol (FTP) / Secure Copy Protocol (SCP) address
- Last deployed Dell Networking operating system software image for the replacement switch uploaded to the TFTP/FTP/SCP 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.
- If the wiring is customized, then the wiring validation procedure will be skipped for that particular wiring segment.

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/SCP 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. In the **MAC Assignment** screen, enter the new serial number for the replacement switch in the **New Serial Number** field.
7. Enter the new Service Tag for the replacement switch in the **New Service Tag** field.
8. Enter the new system MAC address for the replacement switch in the **New MAC Address** field.
9. Click **Next**.

   The **DHCP** screen appears.
10. Save the replacement switch DHCP configuration file.
11. Review the **Summary** screen and click **Finish**.
12. 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.
13. Click **Deploy Switch**.

Deploy Replacement Switch

1. From the menu, click **Network >** *Fabric Name* **>** *Switch Name*.
2. Click the **Switch Replacement** tab.
3. Click **Deploy Switch**.

NOTE: For information about how to replace a switch, see 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 .deb packing file location** area, select one of the following options:

   - **Local Drive (DVD, USB)**
   - **Remote Server**

     If the location is a remote server, enter the URL location of the .deb 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 .deb package using the following formats:

NOTE: The .deb filename must start with AFM (for example, AFM2.5.0.79.noarch.deb).

- https://*ipaddress/path_to_deb.file*
- ftp://*ipaddress/path_to_deb.file*
- sftp://*ipaddress/path_to_deb.file*

3. (Optional) Enter the user name.
4. (Optional) Enter the password.

3. From the **Select the software method** area, select one of the following options:
   - **AFM Upload/Download** — Copy the update to the standby partition on the server but do not apply it or restart. To update, manually start the update from the AFM server update page.
   - **Apply Installation and Restart Server** — Copy the update to the standby partition on the server. Apply the update and restart automatically after the update completes.
4. Click **Update**.

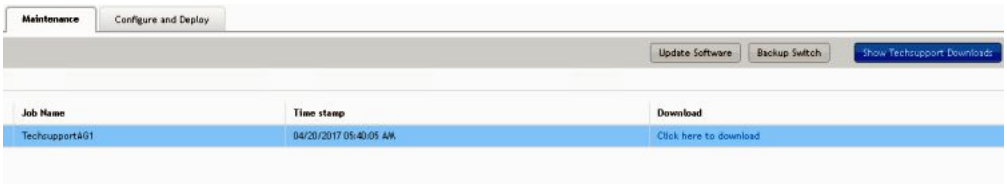
Enabling the AFM Standby Partition

1. From the menu, click **Administration** and then click the **Server Update** tab.
2. Click **Activate Available Partition**.

.

Show TechSupport Downloads

When a user clicks the **Show Techsupport Downloads** button, AFM lists the available switch techsupport files. On clicking the respective job, a download link will appear, which allows the user to download the compressed format of Switch TechSupport outputs.



10

Jobs

This section contains the following topics:

Displaying Job Results

You can view job status in the **Jobs** screen.

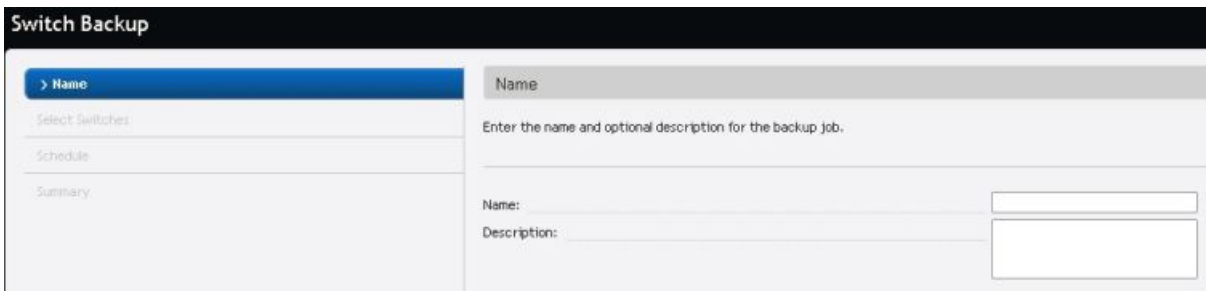
This status refreshes every 60 seconds. You can click the **Refresh** button for an immediate data refresh.

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**.

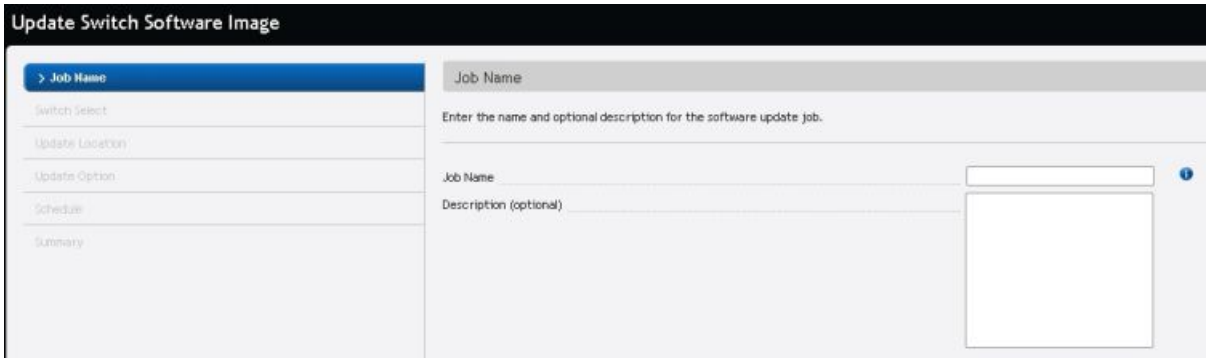
Scheduling Jobs

In AFM, you can schedule the following jobs on the **Scheduled Jobs** tab of the **Jobs** screen:

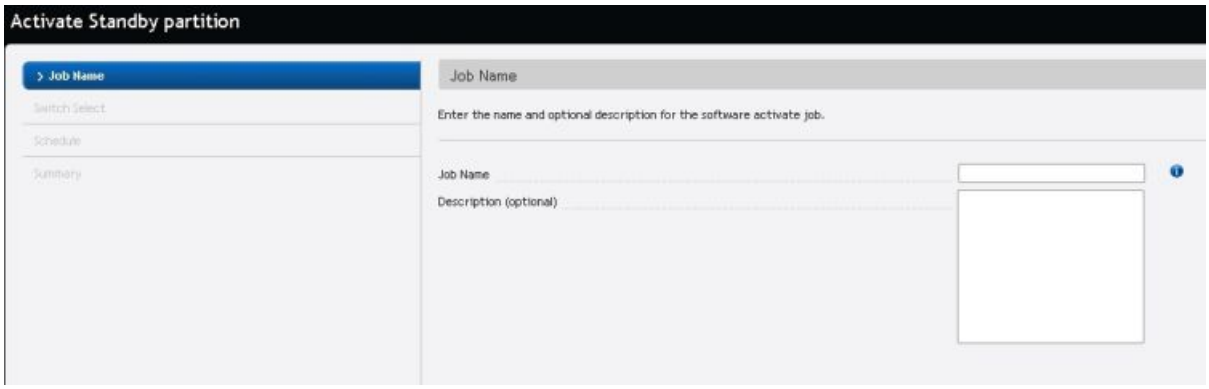
- **Add** — Schedule a new job. There are presently four kinds of jobs that can be scheduled.
  - **Switch Backup** —
    You can schedule a backup of the configuration or startup configuration files on a switch.



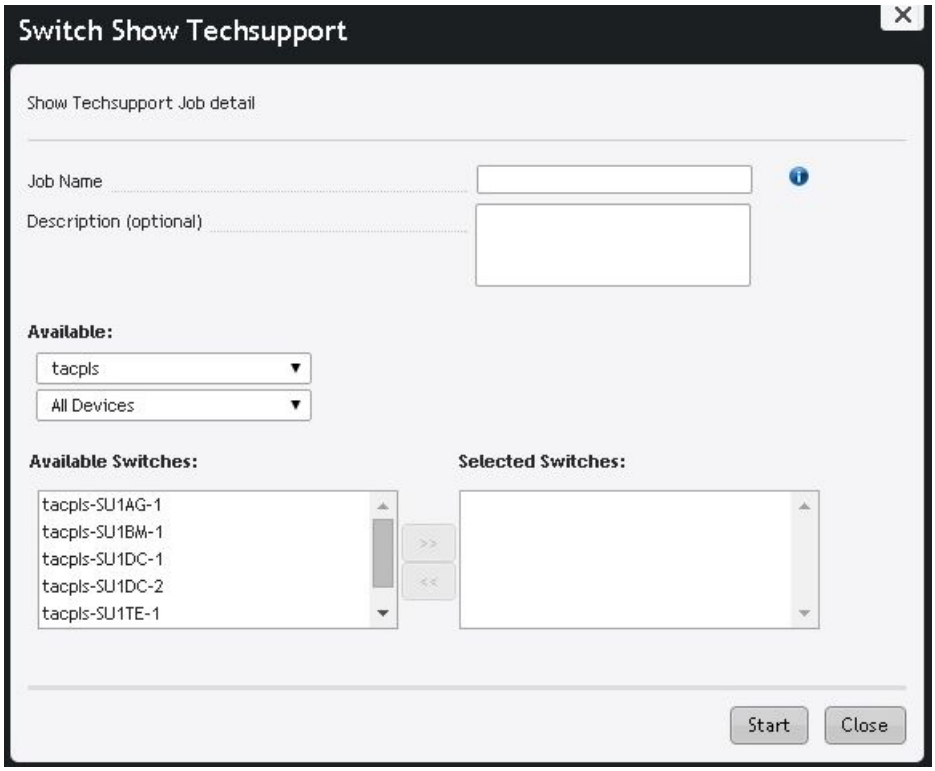
- **Switch Software Image Update** —
  You can schedule an update of the software image on a switch.



- **Switch Software Image Activation** —
  You can enable the software available in the standby partition of the switch as a scheduled job for later or to run immediately.



- **Switch Show TechSupport** —
  You can run the Show Techsupport command immediately and store the output of that command in a file which is available from the **Maintenance** tab.



- **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 the schedule.
- **Disable** — Disable the job or the schedule without deleting the job.

Job information refreshes every 60 seconds. You can click the **Refresh** button for an immediate data refresh.

11

Administration

This section contains the following topics:

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.

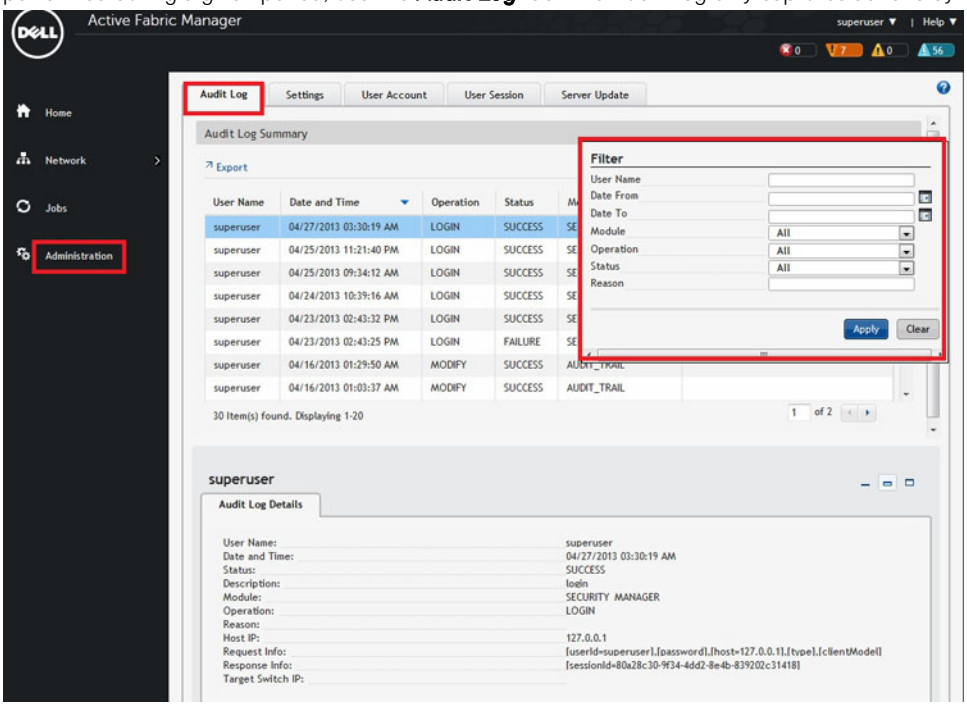


Figure 30. Audit Log Tab

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**.

Administrative Settings

You can configure administrative settings on the **Settings** tab of the **Administration** screen.

CLI Credentials

NOTE:

- AFM allows you to configure the Authentication Settings before designing and deploying the fabric. You cannot edit Authentication Settings after the fabric has been deployed.
- 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 after the fabric has been deployed.

To provision the fabric, enter the Dell Networking OS 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.

You can configure the CLI credentials and enable the configuration credential for all the switches in the fabric in the **Administration** screen.

1. From the menu, click **Administration** and then the **Settings** tab.
2. In the **CLI Credentials** area, click **Edit**.

   The **Client Settings** dialog box appears.
3. In the **Protocol** menu, select one of the following options: **Telnet** or **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.

   NOTE: The privilege level is a read-only field and is set at 15.
7. In the **Enable Password** field, enter a password for the privilege level.
8. In the **Confirm Enable Password** field, confirm the enabled password for the privilege level.
9. Click **OK**.

Client Settings

You can configure the maximum number of browser windows for each user's session and the polling interval from AFM to the switches in the fabric in the **Administration** screen.

1. From the menu, click **Administration** and then the **Settings** tab.
2. In the **Client Settings** area, click **Edit**.

   The **Client Settings** dialog box appears.
3. In the **GUI Polling Interval (in Seconds)** menu, select one of the following options. The default value is 60 seconds.
   - 15 seconds
   - 30 seconds
   - 60 seconds (default)
   - 120 seconds
4. In the **New Window per Client Session** menu, select the maximum number of browser windows for each user's session. The range is from **3** to **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 the **Settings** tab.
2. In the **Data Retention** area, click **Edit**.
3. In the **Performance History** area, enter the number of days you want to retain your performance history. The range is from 1 to 180 days.
4. In the **Daily Purge Execution Time** menu, specify the time to begin purging the performance history data.
5. Click **OK**.

DHCP Server Settings

You can configure DHCP settings in the **Administration** screen.

1. From the menu, click **Administration** and then the **Settings** tab.
2. In the **DHCP Server Settings** area, click **Edit**.

   The **DHCP Server Settings** dialog box appears.
3. 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 the 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.
4. Click **OK**.

NTP Server Settings

You can configure NTP server settings in the **Administration** screen.

NOTE: To ensure that time settings are correct, enter the NTP server information from the token file. Configure AFM to synchronize with AFM server and configure the switches to point to AFM.

1. From the menu, click **Administration** and then the **Settings** tab.
2. In the **NTP Server Settings** area, click **Edit**.
   The **NTP Server Settings** dialog box appears.
3. In the **Primary IP Address** field, enter the NTP server primary IP address.
4. In the **Secondary IP Address** field, enter the NTP server secondary IP address.

   NOTE: The IP Status and Secondary IP Status fields display the status of the servers.
5. Click **OK**.

SMTP Email

You can configure SMTP email notifications in the **Administration** screen.

1. From the menu, click **Administration** and then the **Settings** tab.
2. In the **Secure SMTP Email Settings** area, click **Edit**.
   The **Secure SMTP Email Settings** dialog box appears.
3. In the **Outgoing Mail Server** field, enter the IP address 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 **Password** field, enter the password.
7. In the **From Email Address** field, enter the email address of the user account configured in the SMTP server.
8. In the **To Email Address(es)** field, enter the email addresses of recipients. Separate multiple addresses with a semicolon (;).
9. In the **Minimum severity level to Email Notification** menu, select one of the following settings:
   - **Critical**
   - **Major**
   - **Minor**
   - **Warning**
10. Click **OK**.

SNMP Support

AFM-CPS supports SNMPv3 and retains support for SNMPv2.

You can configure the SNMPv2 or SNMPv3 credentials for designed and deployed fabrics. By default, AFM-CPS uses MD5 authentication and DES-56 encryption for SNMPv3 configuration. You can enable SNMPv3 in AFM-CPS in the following ways:

- A fresh installation with the AFM-CPS .VHDx image file.
- A .deb file upgrade. See the *Active Fabric Manager for Microsoft Cloud Platform System User Guide* for more details.

You can configure SNMPv2 or SNMPv3 credentials for a fabric in the following ways:

- AFM Setup Wizard
- Administrative Settings
- Predeployment Configuration Wizard

Configuring the SNMP Version in the AFM Setup Wizard

You can configure the SNMP version — SNMPv2 or SNMPv3 — in the **AFM Setup** wizard.

1. In the SNMP and CLI screen of the **AFM Setup** wizard, you can select the version as **V2c** or **V3**.

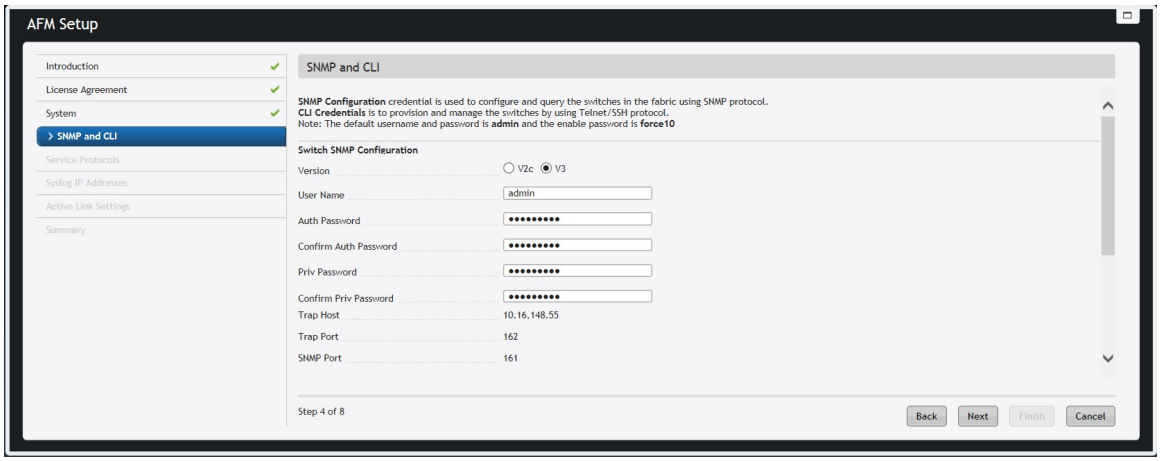


Figure 31. AFM Setup Wizard

2. In the **User Name** field, enter the user name.
3. In the **Auth Password** field, enter the auth password.
4. In the **Confirm Auth Password** field, confirm the auth password.
5. In the **Priv Password** field, enter the priv password.
6. In the **Confirm Priv Password** field, confirm the priv password.
7. Click **Next**.

Configuring SNMP Credentials Globally

You can configure SNMPv2 or SNMPv3 credentials globally in which AFM-CPS applies the settings to all fabrics designed in AFM-CPS.

NOTE: You cannot edit SNMP credentials after a fabric has been deployed.

1. From the menu, click **Administration** and then the **Settings** tab
2. In the SNMP configuration area, click **Edit**.
   The **SNMP Configuration** dialog box appears.

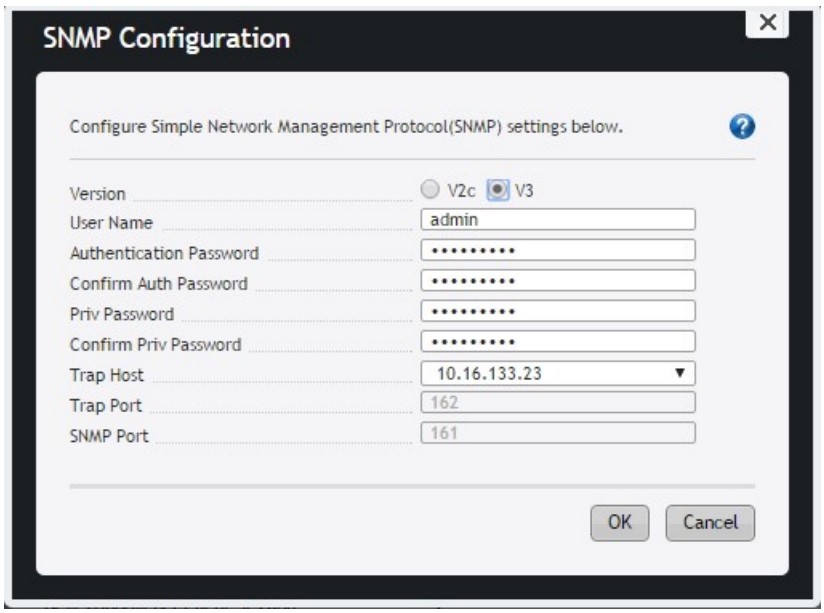


Figure 32. SNMP Configuration Dialog Box

3. In the **Version** field select one of the following options: **V2c** or **V3**.

4. In the **User Name** field, enter the user name.
5. In the **Authentication Password** field, enter the auth password.
6. In the **Confirm Auth Password** field, confirm the auth password.
7. In the **Priv Password** field, enter the priv password.
8. In the **Confirm Priv Password** field, confirm the priv password.
   - In **Trap Host** field, the default setting is the server IP.
   - In **SNMP Port** field, the default setting 161.
9. Click **OK**.

Configuring SNMP in the Predeployment Configuration Wizard

You can configure SNMPv2 or SNMPv3 credentials for each fabric during pre-deployment configuration.
You can edit these settings even after the fabric is deployed.

1. From the **SNMP and CLI Credentials** screen in the **Predeployment Configuration** wizard, in the **Version** field, select **V2c** or **V3**.

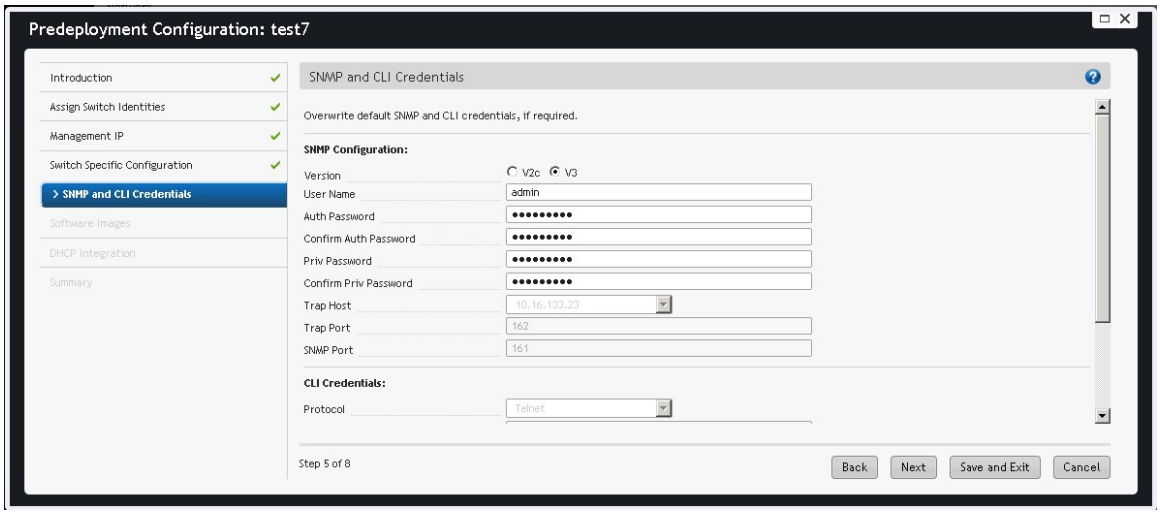


Figure 33. Predeployment Configuration Wizard

2. In the **User Name** field, enter the user name.
3. In the **Auth Password** field, enter the auth password.
4. In the **Confirm Auth Password** field, confirm the auth password.
5. In the **Priv Password** field, enter the priv password.
6. In the **Confirm Priv Password** field, confirm the priv password.
   - In the **Trap Host** field, by default is set as server IP.
   - In the **Trap Port** field, the default is set to 162.
   - In the **SNMP Port** field, the default is set to 161.
7. Click **Next**.

Converting from SNMPv2 to SNMPv3

You can convert from SNMPv2 to SNMPv3.

1. From the menu, select **Network** and then select the fabric.
2. Click the **Configure and Deploy** tab.
3. Click **Deploy Fabric**, and select **Pre-deployment Configuration**.
   The **Predeployment Configuration** wizard appears.
4. Navigate through the wizard to the **SNMP and CLI Credentials** screen.

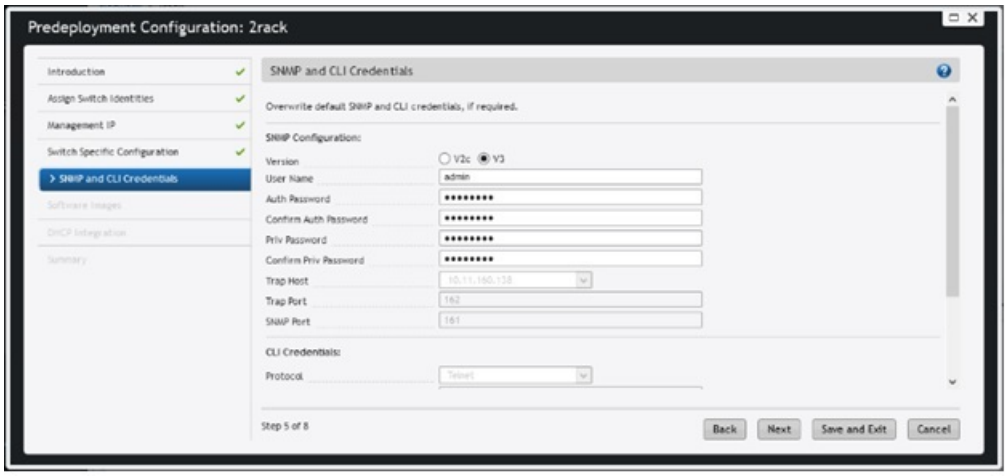


Figure 34. SNMP and CLI Credentials Screen

5. In the **Version** field, select **V3**.
6. Make entries for the **User Name**, **Auth Password**, **Confirm Auth Password**, **Priv Password**, and **Confirm Priv Password** fields.
7. Click **Next**.
8. Navigate through the remainder of the wizard and click **Finish**.
9. Return to the **Configure and Deploy** tab.
10. Click **Deploy Fabric** and select **Deploy and Validate**.
11. In the **Deploy and Validation** screen, select the switches to deploy and click **Deploy Selected**.
    The **Configuration deployment option** dialog box appears.
12. Select **Overwrite entire configuration on the switch** and click **OK**.
    AFM-CPS applies the SNMPv3 configuration to the switches and the reloads them. You must select **Overwrite** instead of **Apply** when changing between SNMPv2 and SNMPv3 to work around issue #161062. This issue can result in an error when applying the SNMP configuration to the switch that causes the AFM-CPS validation to fail with the error “Switch not discovered.”
13. Deploy remaining switches using the previous steps.

Changing the SNMP Password

You can change the SNMPv2 or SNMPv3 password.

1. Navigate to the **SNMP and CLI Credentials** screen of the **Predeployment Configuration** wizard.

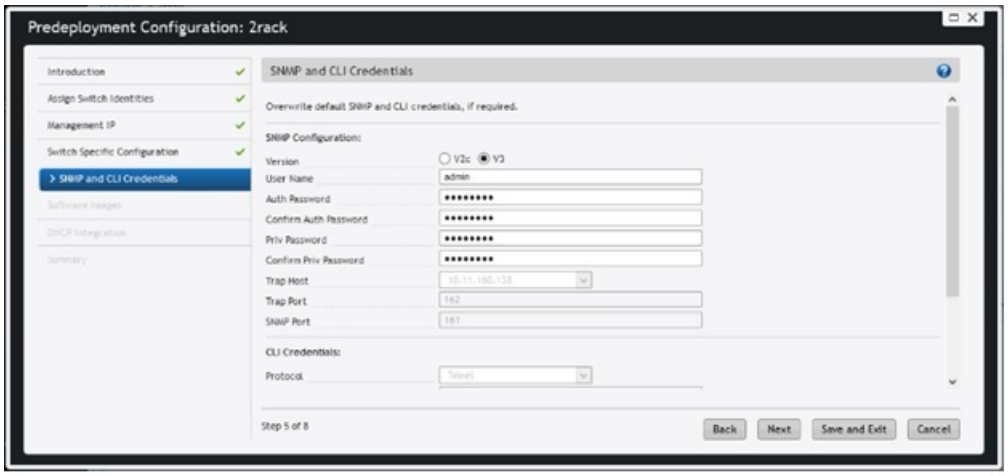


Figure 35. SNMP and CLI Credentials Screen

2. Navigate to the **SNMP Configuration** area.
3. In the **Version** field, make sure the correct SNMP version is selected: **V2c** or **V3**.
4. Edit any of the following fields as necessary: **User Name**, **Auth Password**, or **Priv Password**.
5. Navigate through the remainder of the wizard and click **Finish**.
6. Navigate to the **Deploy and Validation** dialog box.
7. Select the switches that you want to deploy and then click **Deploy Selected**.

   The **Configuration deployment option** dialog box appears.

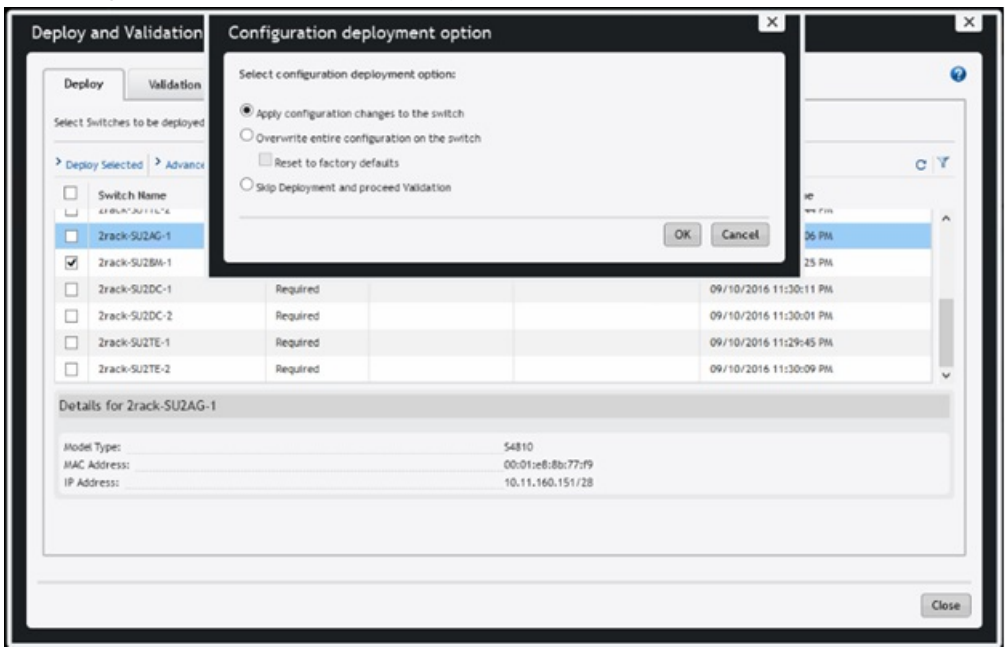


Figure 36. Configuration deployment option Dialog Box

8. Select **Apply configuration changes to the switch.**
9. Deploy remaining switches using the previous steps.

Changing CLI Credentials

You can change the CLI credentials.

1. Navigate to the **SNMP and CLI Credentials** screen of the **Predeployment Configuration** wizard.

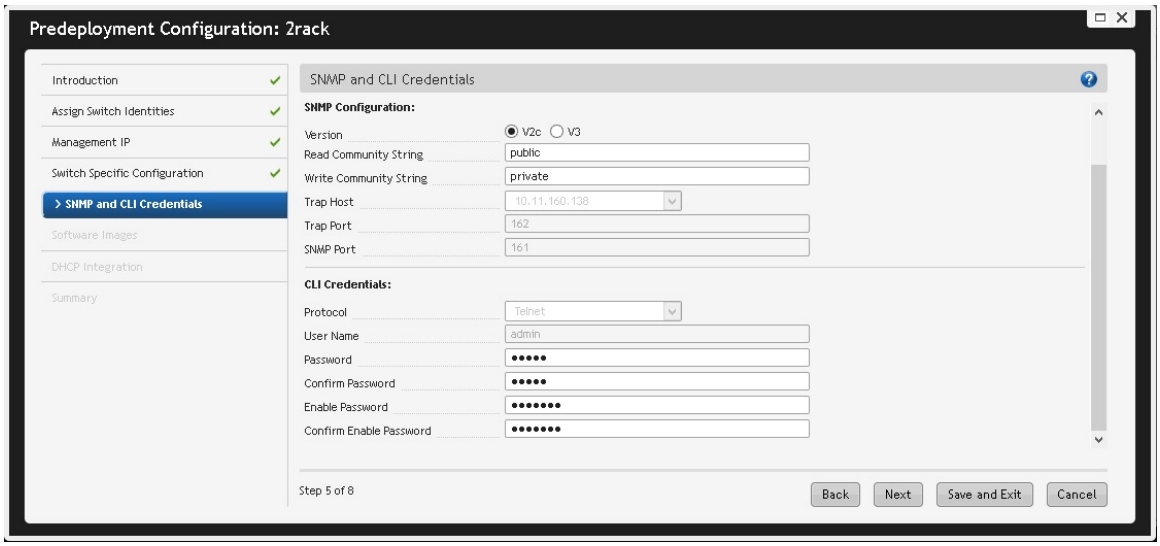


Figure 37. SNMP and CLI Credentials Screen

2. Navigate to the **CLI Credentials** area.
3. Edit any of the following fields as necessary: **Password** and **Confirm Password** or **Enable Password** and **Confirm Enable Password**.
4. Navigate through the remainder of the wizard and click **Finish**.
5. Navigate to the **Deploy and Validation** dialog box.
6. Select the switches that you want to deploy and then click **Deploy Selected**.

   The **Configuration deployment option** dialog box appears.

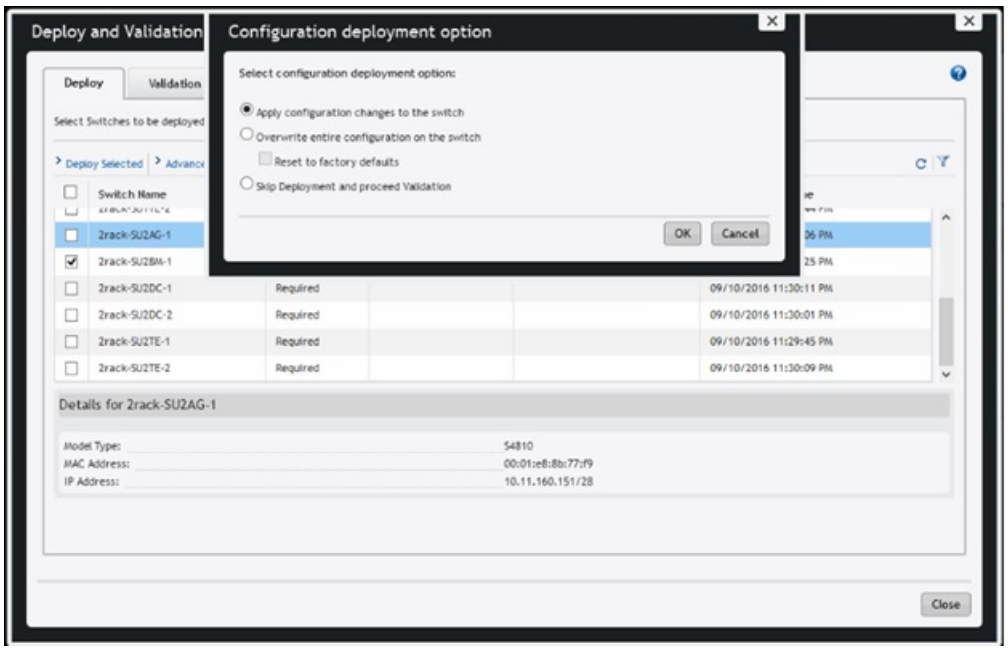


Figure 38. Configuration deployment option Dialog Box

7. Select **Apply configuration changes to the switch.**
8. Deploy remaining switches using the previous steps.

Syslog IP Addresses

You can configure syslog settings in the **Administration** screen.

1. From the menu, click **Administration** and then the **Settings** tab.
2. In the **Syslog IP Address(es)** area, click **Edit**.

   A dialog box appears.
3. In the **Syslog IP Addresses** area, enter the IP addresses of the syslog servers. You can configure up to eight syslog server IP addresses to log events on the switches in the fabric. By default, the first syslog IP address entry is the AFM system IP address.
4. Click **OK**.

System Information

You can configure the IP address that manages AFM in the **Administration** screen.

1. From the menu, click **Administration** and then the **Settings** tab.
2. In the **System Information** area, click **Edit**.

   The **System Information** dialog box appears.
3. In the **System IP Address** menu, select the IP address that manages AFM.

   NOTE: If there are multiple Network Interface Card (NIC) adapter cards on the AFM, select the IP address that manages AFM.
4. Click **OK**.

TFTP/FTP/SCP Settings

You can configure administrative settings, in the **Administration** screen.

1. From the menu, click **Administration** and then the **Settings** tab.
2. In the **TFTP/FTP/SCP Settings** area, click **Edit**.

   The **TFTP/FTP/SCP Settings** dialog box appears.
3. Select one of the following options:
   - **Local** — Provision AFM as a TFTP/FTP/SCP server.

     NOTE: When you use the Local option, the TFTP/FTP/SCP server must be in the same subnet.
     - If you select the local TFTP server option, the TFTP server uses the AFM management IP address.
     - 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 SCP server option, the SCP server uses the AFM management IP address. Enter the AFM user name, and password.
   - **Remote** — Use an external TFTP/FTP/SCP server.
     - If you select the FTP protocol and remote options, enter the FTP server IPv4 address, user name, and password.
     - If you select the TFTP protocol and remote options, enter the TFTP IPv4 address.
     - If you select the SCP protocol and remote options, enter the SCP server IPv4 address, user name, and password.
4. From the **File Transfer Protocol** drop-down menu, select one of the following options:
   - **TFTP** (default)
   - **FTP**
   - **SCP**
5. Click **OK**.

SCP Settings

AFM-CPS supports configuration for secure copy (SCP) from the **Administration** screen.

NOTE: S55 switches do not support SCP with BMP.

1. From the menu, click **Administration**, and select the **Settings** tab.
2. In the **TFTP/FTP/SCP Settings** area, click **Edit**.
   The **TFTP/FTP/SCP Settings** dialog box appears.

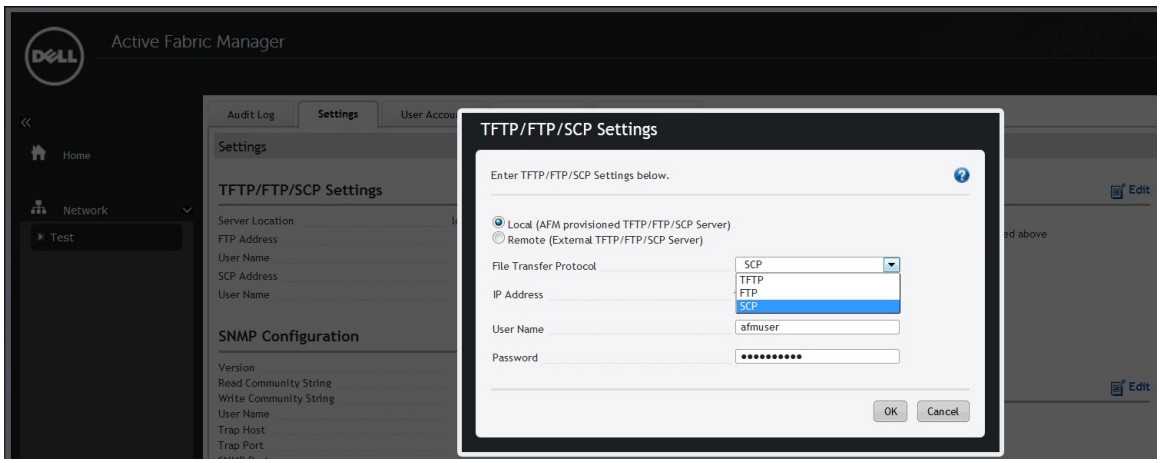


Figure 39. TFTP/FTP/SCP Settings Dialog Box

.

3. Enter the user name and password to enable SCP for file transfer on the AFM-CPS server.

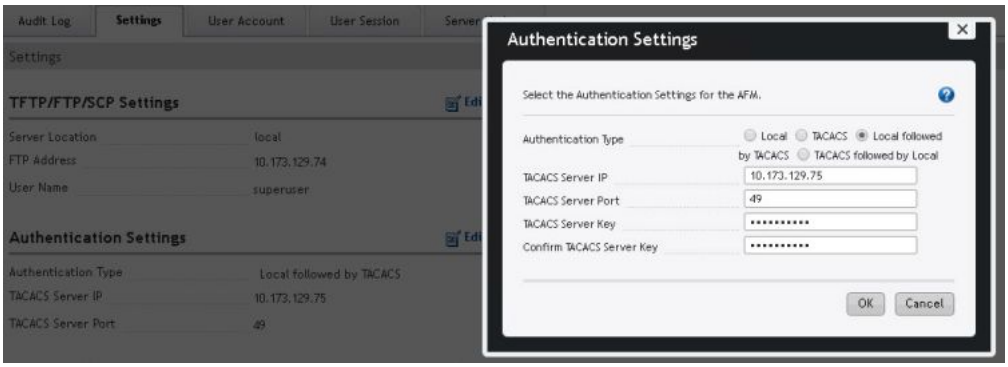
   NOTE: For local SCP for the AFM-CPS server, the default user name is `afm` and the default password is `Superuser1`.

4. Navigate to the **Summary** screen and confirm that the selected File Transfer Protocol setting is SCP.
   After you configure SCP, the following occurs in AFM-CPS:
   - In the **Predeployment Configuration** wizard, the **Introduction**, **Software Images**, **DHCP Integration**, and the **Summary** screens now refer to SCP.
   - For the job of updating switch software image, SCP site settings is displayed.

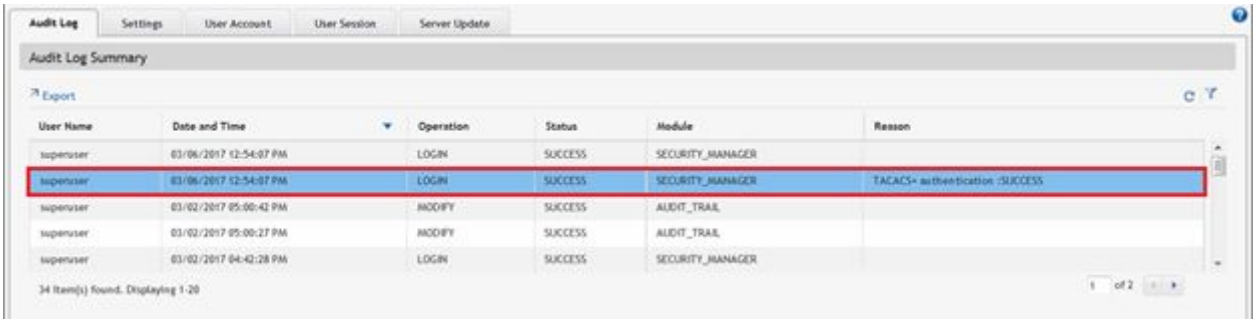
     NOTE: For S3048-ON, S4048-ON, and S4810 switches, to use SCP for file transfer, the OS version must be 9.10(0.1)P13 or later.

Configure TACACS in AFM server

1. From **Administration** —> **Settings** —> **Authentication Settings**, choose **Local followed by TACACS** and provide tacacs server ip address, port (49) and server key.



2. From **Administration** —> **Audit Log**, make sure tacacs is working for AFM logins. Once verified, change the option from **Local followed by TACACS** to **TACACS**.



Managing User Accounts

NOTE: User Management is not supported if the AFM server has TACACS authentication enabled.

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

To view and manage user accounts, use the **Administration > User Accounts** screen.

- View configuration and performance monitoring information.
- Change password for own account.

User

NOTE: The AFM root user name is `superuser` and the password is `Superuser1`.

- **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, see 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
   - Lowercase 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, see 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**.

Deleting a User

To add or delete users, log in as a `Superuser`. For more information about user accounts, see 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**.

Editing a User

To edit a user, log in as a `Superuser`. For more information about user accounts, see 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**.

Unlocking a User

To unlock a user, log in as a **Superuser**. For information about user accounts, see 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**.

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, see 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 check mark 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**.

Changing Your Password

To change your password, use the **Change User Account Password** screen. This screen does not allow you to change another user's password. If a user's password needs to be reset, the Superuser must reset it using the **Edit User** option.

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
   - Lowercase 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, see Managing User Accounts.

Basic TACACS Server Configuration for AFM

This section covers how to setup a TACACS server in case you want to use TACACS for authentication.

TACACS+ Server Setup in Debian

Please follow the steps below to install and setup tacacs+ server on a fresh debian server:

1. Execute the following command as root user to install tacacs+ server: `apt-get install tacacs+`.
2. If you want to use linux users for authentication then uncomment the following line in `/etc/tacacs+/tac_plus.conf`: `default authentication = file /etc/passwd`.
3. Re-start tacacs+ server using the command: `service tacacs_plus restart`.

Please set up a required linux user account on the tacacs server using the below commands:

1. `useradd <username>`.
2. `passwd <username>` (while prompted for password, enter a password).

Following default users should be set on the tacacs server with any password:

1. Username : **root**

2. Username : **afm**
3. Username : **superuser**

The default switch access should also be created on the tacacs server with the following credentials:

- Username : **admin**
- Password : **admin**