

Dell Fabric Manager Deployment Guide 1.0.0



Notes, Cautions, and Warnings



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



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



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

Information in this publication is subject to change without notice.

© 2012 Dell Inc. All rights reserved.

Reproduction of these materials in any manner whatsoever without the written permission of Dell Inc. is strictly forbidden.

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

Other trademarks and trade names may be used in this publication to refer to either the entities claiming the marks and names or their products. Dell Inc. disclaims any proprietary interest in trademarks and trade names other than its own.

2012 - 06

Rev. A0X

Contents

Notes, Cautions, and Warnings.....	2
1 Introduction.....	7
Conventional Core Versus Distributed Core.....	7
Conventional Core.....	7
Distributed Core.....	8
Key Advantages.....	9
Designing a Distributed Core.....	9
Terminology.....	10
Gathering Useful Information.....	11
Key Considerations for Designing a Distributed Core	11
Selecting a Distributed Core Design Template.....	13
Type 1: Large Core Design.....	13
Type 2: Medium Core Design.....	14
Type 3: Small Core Design.....	16
2 Getting Started.....	17
Designing and Deploying a Distributed Core.....	17
Flowchart for Designing and Deploying a Distributed Core.....	18
How to Design and Deploy a Distributed Core.....	18
3 Using the Core Design Wizard.....	19
Core Design – Step 1: Welcome Page.....	19
Core Design – Step 2: Core Name and Type.....	20
Core Design – Step 3: Port Count.....	21
Core Design – Step 4: Interlink Configuration.....	22
Core Design – Step 5: Uplink Configuration.....	23
Core Design – Step 6: Downlink Configuration.....	23
Core Design – Step 7: Output.....	23
Core Design – Step 8: Summary.....	25
4 Using the Pre-deployment Wizard.....	27
Pre-Deployment – Step 1: Introduction	27
Prerequisites.....	27
Flowchart for preparing the distributed core for deployment.....	28
Pre-Deployment Screens.....	28
Pre-deployment – Step 2: Assign Switch Identities.....	29

Pre-Deployment – Step 3: Management IP	29
Pre-Deployment – Step 4: Software Images	30
Pre-Deployment – Step 5: DHCP Integration.....	30
Pre-Deployment – Step 6: Output.....	31
Pre-Deployment – Step 7: Summary.....	31
5 Deploying and Validating the Core.....	33
Viewing Deployment and Validation Status.....	35
6 Understanding Core Phases.....	37
7 Operations Allowed During Each Core State.....	39
8 Troubleshooting.....	41
Switch Deployment Status Errors.....	41
Validating Connectivity to the ToR.....	44
Validation Errors.....	44
9 Expanding the Core	47
10 Modifying and Viewing the Distributed Core.....	49
Dashboard.....	49
Cores	50
Editing the Core.....	50
Deleting the Core.....	51
Viewing and Exporting Wiring Diagram.....	51
Viewing the DHCP Configuration File.....	51
11 Alerts.....	53
Active Alerts.....	53
Alerts and Event History.....	54
12 Monitor.....	55
Reports.....	55
Creating a New Report.....	55
Running a Report.....	56
Editing a Report.....	56
Duplicating Reports.....	56
Deleting a Report.....	57
Global Statistics.....	57
Data Collection.....	57
13 Administration.....	59

Settings.....	59
TFTP Settings.....	59
Syslog IP Addresses.....	59
SNMP Configuration.....	60
CLI Credentials	60
Data Retention.....	61
Client Settings.....	61
Managing User Accounts.....	61
Adding a User.....	62
Deleting a User.....	63
Editing a User.....	63
Changing Your Password.....	64
Unlocking a User.....	64
Managing User Sessions.....	64

Introduction

Dell Fabric Manager (DFM) is a graphical user interface (GUI) based network automation and orchestration tool that allows you design, build, deploy, and optimize a distributed core for your current and future workload requirements. This tool helps you simplify network operations, automate tasks, and improve efficiency in the data center and campus environments. DFM supports Dell Z9000 and S4810 switches.

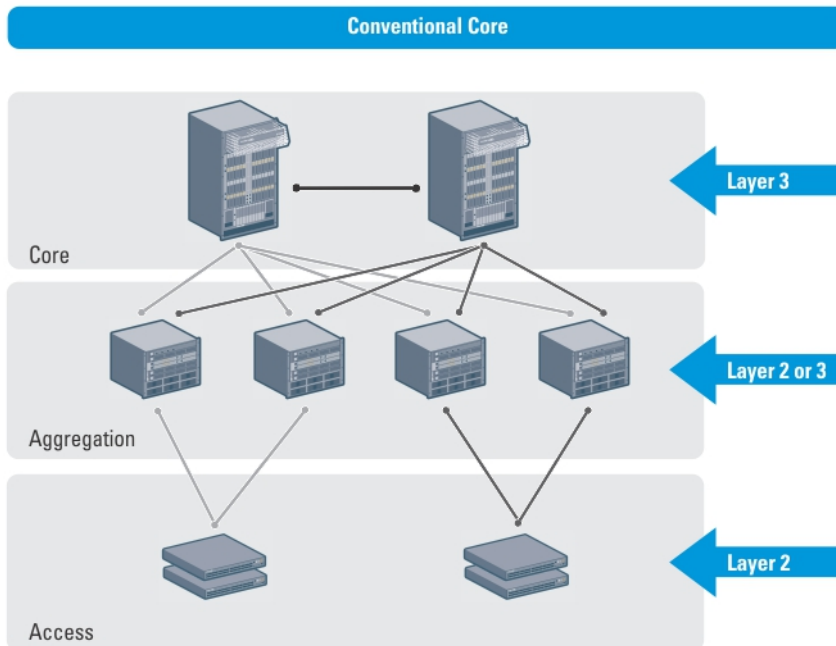
Conventional Core Versus Distributed Core

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:

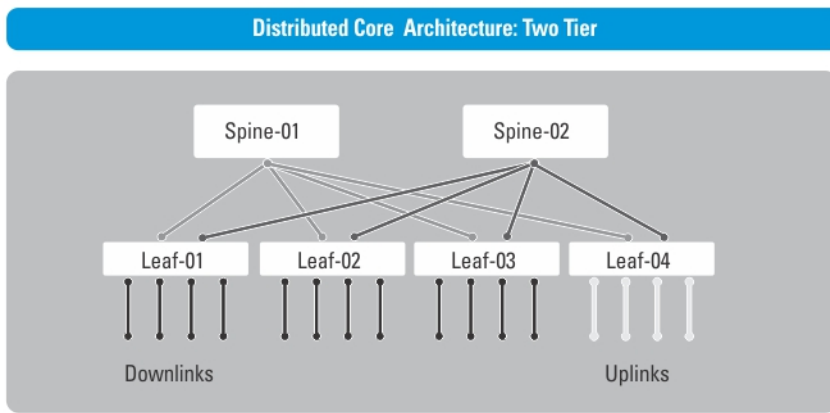
- **Core**—The core layer routes the traffic to and from the internet and the extranet. Redundancy and resiliency is the main factor for high availability of core routers, which requires chassis-based core routers.
- **Aggregation layer**—The aggregation layer connects with top of rack switches (ToR) 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 allowing all the servers in the rack to be cabled into the switch. A ToR typically has a small 1 to 2 rack unit (RU) form factor.




Distributed Core

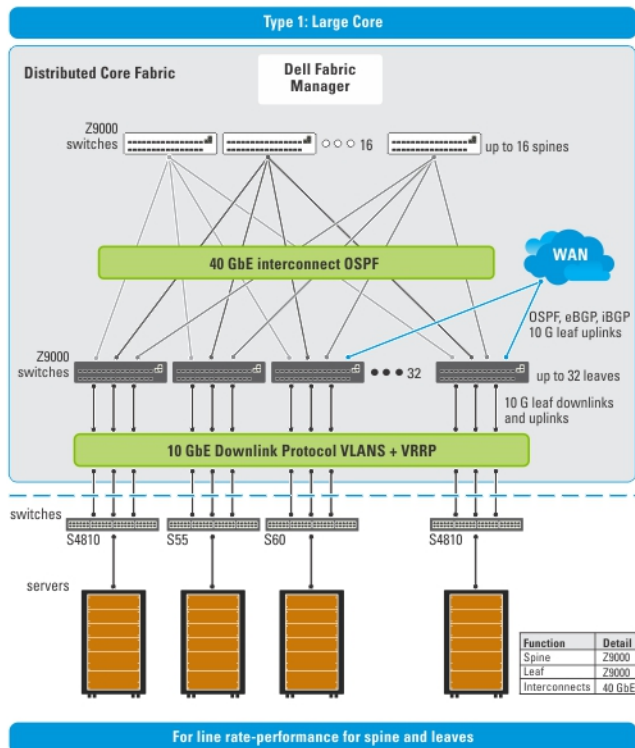
A distributed core is a two-tier architecture composed of multiple switches interconnected to provide a scalable, high-performance network that replaces the traditional and aggregation layers in a conventional core. Switches are arranged as spines and leaves; the spines interlink (connect) the leaves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

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



 **NOTE:** There are no uplinks on the spines.

The following illustration shows a large distributed core deployment.



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

Designing a Distributed Core

The core design wizard templates define the basic configuration for a distributed core. Use the core design wizard at the **Home > Getting Started** screen to design a two-tier distributed core (spine and leaf architecture) based on the workload requirements for your current and future needs.

This section contains the following topics:

- [Terminology](#)
- [Gather Useful Information](#)
- [Key Core Design Considerations](#)
- [Select a Core Design Template](#)
- [Type 1: Large Core Design](#)
- [Type 2: Medium Core Design](#)
- [Type 3: Small Core Design](#)

Terminology

The following terms are unique to the design and deployment of a distributed core:

- Leaf—A switch that connects switch, servers, storage devices, or top-of-rack (TOR) elements.
- Spine—A switch that connects to leaf switches. The spines provides 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 that connects to the WAN, which typically connects to an internet server provider (ISP).
- Downlinks—An edge port link that connects the leaves to the data access layer. For example, servers or ToR elements.



NOTE: You must specify an even number of uplinks. The minimum number of uplinks is **2**. One uplink is for redundancy.

- Interconnect links—Links that connect the spines to the leaves. The interconnect link bandwidth is fixed: 40 GbE or 10 GbE.
- Interlink over-subscription ratio—Varies the maximum number of available interconnect links. This ratio determines the number of interconnect links (the number of communication links between the spine and leaf devices). The ratio that you specify 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 interlink over-subscription ratio:


- The total number of ports for the uplinks and downlinks increase.
- The number of interconnect links from the leaves to the spines decrease.
- The maximum number of available ports increases.

Use the 1:1 interlink over-subscription rate for the non-blocking, line rate between the leaves and spines. Use this option when you require a lot of bandwidth and not a lot of ports.

Gathering Useful Information

Before you begin, gather the following useful information:

- Comma separated values (.csv) file that contains all the chassis MAC addresses for the switches. If you do not have this file, write down the chassis MAC addresses.
- Location of the switches, including the rack and row number.
- Trivial File Transfer Protocol (TFTP) address from your system administrator.
- Software image for each type of switch: Z9000, S4810, or both. Each type of switch must use the same version of the software image. Place the software images on the TFTP site so that the switches can install the appropriate FTOS software image and configuration file. To specify a TFTP site, go to the **Administration > Settings** screen. For information about which software packages to use, see the release notes.
- Dynamic Host Configuration Protocol (DHCP) server address to be used for the distributed core from your DHCP system administrator. If a DHCP server is not available, set one up. After you power cycle the switches, the switches communicate with the DHCP server to obtain an management IP address based on the chassis 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 site during bare metal provisioning (BMP).

 **NOTE:** As a best practice, configure the DHCP server on the same server where the DFM is installed. This assists in an easier copy and paste of the **dhcpd.cfg** files, which are generated by the DFM.

- Pool of IP addresses for the management port for each switch in the distributed core.
- If you are using eBGP uplinks, gather the following information for each uplink:
 - Local IP
 - Remote neighbor IP
 - AS number
 - Remote AS number
- If you are using iBGP uplinks, gather the following information for each uplink:
 - Local IP address
 - Remote neighbor IP
 - AS number
- If you are using OSPF uplinks, gather the following information for each uplink:
 - Local IP address
 - Remote neighbor IP
 - Area ID

Key Considerations for Designing a Distributed Core

This section describes the key considerations for designing a distributed core.

Use the following flowchart to help you design a distributed core.

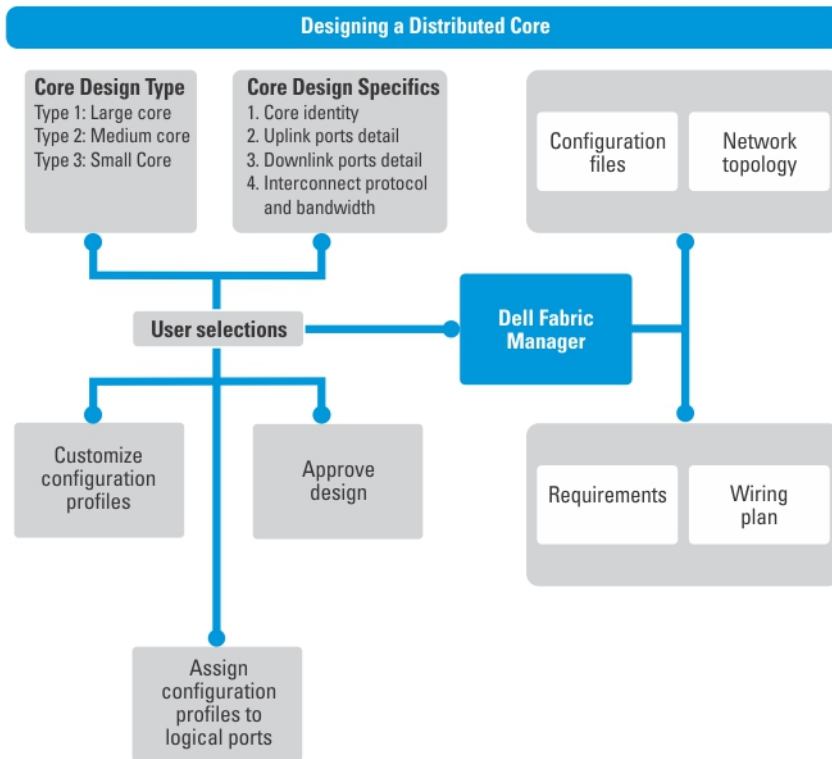


Figure 1. Flowchart for Designing a Distributed Core

When designing the distributed core, consider the following:

- You can deploy up to four distributed cores. However, the distributed cores do not communicate with each other.
- DFM manages Dell Z9000 and S4810 switches.

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

The number and type of spines and leaves (switches) in a distributed core are based on the following:

- Core type
 - Type 1: Large Core
 - Type 2: Medium Core
 - Type 3: Small Core
- Number of current uplinks and downlinks for the leaves.
- Number of planned edge ports (future uplinks and downlinks) for the leaves.
- Whether non-blocking (line rate) performance is required.
- Whether the leaves need to act as a ToR or are connecting to a server. If so, select the Type 2: Medium Core or Type 3: Small Core template.
- Interconnect link bandwidth (the links between the spines and leaves).
- Downlinks, which are always 10 GbE.

- The uplinks or interlinks must be in area 0 for OSPF.
- Interlink over-subscription ratio.



NOTE: The Interconnect bandwidth link is fixed and based on the core type:

- For a Type 1: Large Core and Type 2: Medium Core the interconnect bandwidth is 40 GbE.
- For a Type 3: Small Core the interconnect bandwidth is 10 GbE.



CAUTION: If you do not specify any additional links in the core design for future expansion in the Port Count screen:

- Any future expansion requires rewiring the hardware.
- IP addresses are not reserved.
- You might have to bring down current switches to expand the core. For information on how to expand a core, see [Using the Expand the Core Wizard](#).

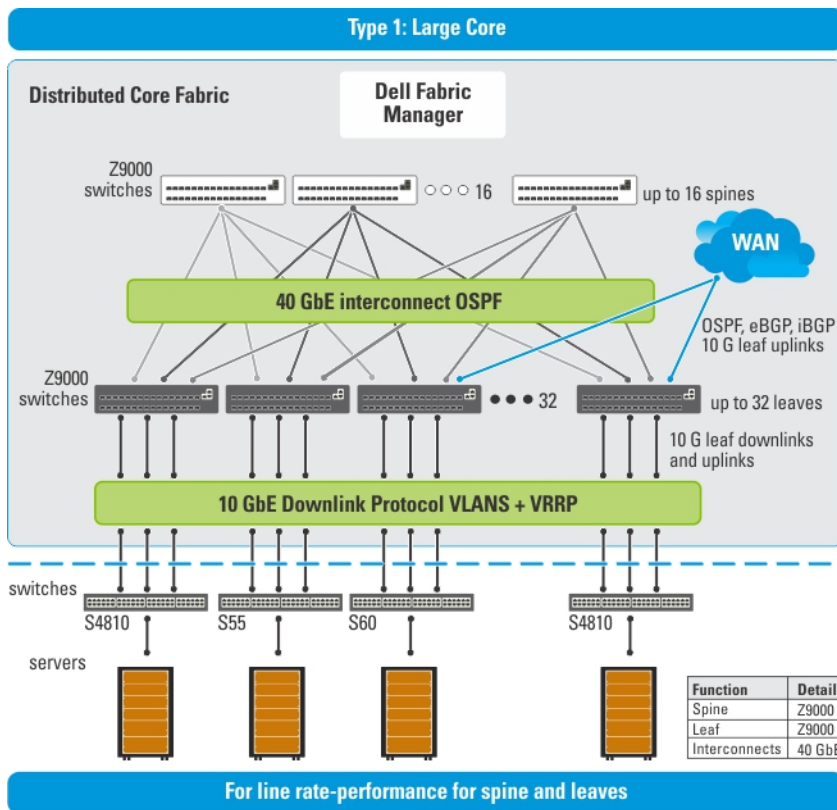
Selecting a Distributed Core Design Template

Use the following table as a guide to select the appropriate distributed core design template.

Core Design Template	Type 1-Large Core	Type 2- Medium Core	Type 3 -Small Core
Spine device	Z9000	Z9000	S4810
Leaf device	Z9000	S4810	S4810
Interlink over-subscription rate	1:1 (default) 2:1 3:1 5:1	3:1 (default) 5:1	3:1 (default) 5:1
Max # of spine devices	16	4	4
Max # of leaf devices	32	32	16
Interconnect link bandwidth	1 x 40 GbE link	1 x 40 GbE link	1 x 10 GbE link
Max # of ports (10g) based on interlink over-subscription rate.	1:1 – 2048 2:1 – 2720 3:1 – 3072 5:1 – 3392	3:1 – 1536 5:1 – 1696	3:1 – 768 5:1 – 848

Type 1: Large Core Design

With a Type 1: Large Core design, the Z9000 spines connect to the Z9000 leaves at a fixed 40 GbE line rate. The maximum number of leaves is based on the maximum number of ports on the spine, with the Z9000, 32 ports, as shown in the following figure.



For line rate-performance for spine and leaves

NOTE: The Dell Fabric Manager does not configure or manage anything beyond the distributed core.

Use the Type 1: Large Core design when:

- The line rate-performance with an oversubscription ratio of 1:1 between the spines and leaves is required.
- The current and future planned uplinks and downlinks on the leaves for the distributed core is less than or equal to 2048 ports.
- The leaves do not act as a ToR.

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

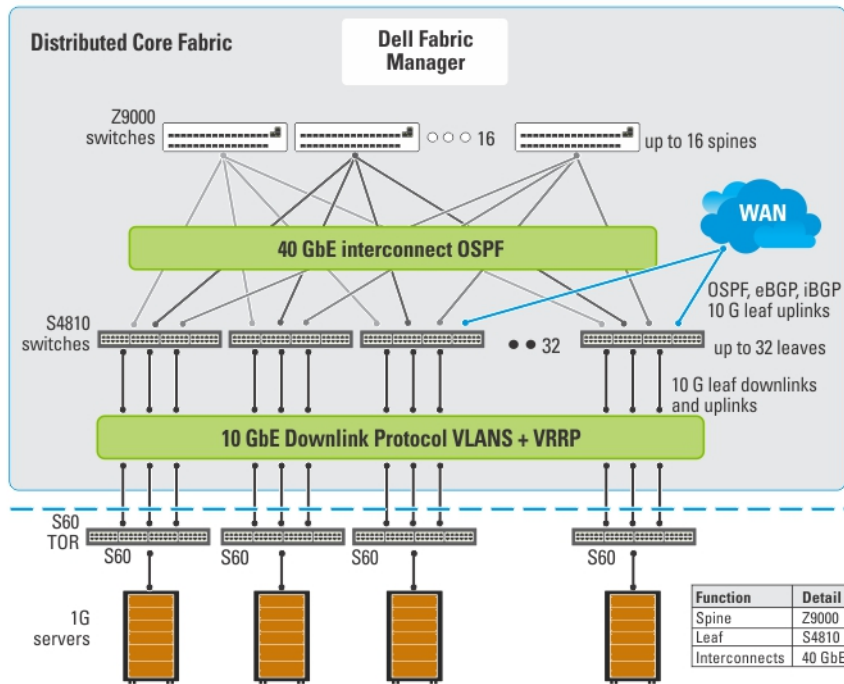
Each Z9000 leaf for the Type 1: Large Core design has the following:

- 640 Gigabit of interlink maximum capacity to the Spine (16 x 40Gig)
- 64 10 Gig Ethernet ports for server connectivity and WAN connectivity

Type 2: Medium Core Design

With a Type 2: Medium Core design, the Z9000 spines connect to the S4810 leaves at a fixed 40 GbE line rate. The maximum number of leaves is based on the maximum number of ports on the spine, with the Z9000, 32 ports. The maximum number of spines is 4 and the maximum number of leaves is 32, as shown in the following figure. This illustration shows a networking system architecture in a data center which is composed of a distributed core containing a set of ToRs to which servers, storage devices, and network appliances such as load balancers or network security appliances are connected. Application services, network services, and network security services can be running either on physical machines or virtual machines.

Type 2: Medium Core



NOTE: The Dell Fabric Manager does not configure or manage anything beyond the distributed core.

Use the Type 2: Medium Core design when:

- An interconnect link bandwidth between the spines and leaves at a 40 GbE line rate is required.
- The current and future planned uplinks and downlinks on the leaves for your core is less than or equal to 1536 ports.
- The leaves act as a switch or ToR-leaf switch. Within the ToR, the protocol can be either "VLAN" or "VLAN and LAG".

NOTE: To enable the leaves to act as a ToR, check the **Enable the Leaves to Act as a ToR** box at the **Cores > Core Deployment > Design > Create a New Core > Downlink Configuration** screen.

Each Z9000 spine for the Type 2: Medium Core design has the following:

- 640 Gigabit of interlink maximum capacity to the spine (16 x 40Gig)
- 64 10 Gig Ethernet ports for server connectivity and WAN connectivity

Each S4810 leaf for the Type 2: Medium Core design has the following:

- 160 Gigabit of interlink maximum capacity to the spine (4x 40Gig)
- 48 10 Gig Ethernet ports for servers per node and WAN connectivity

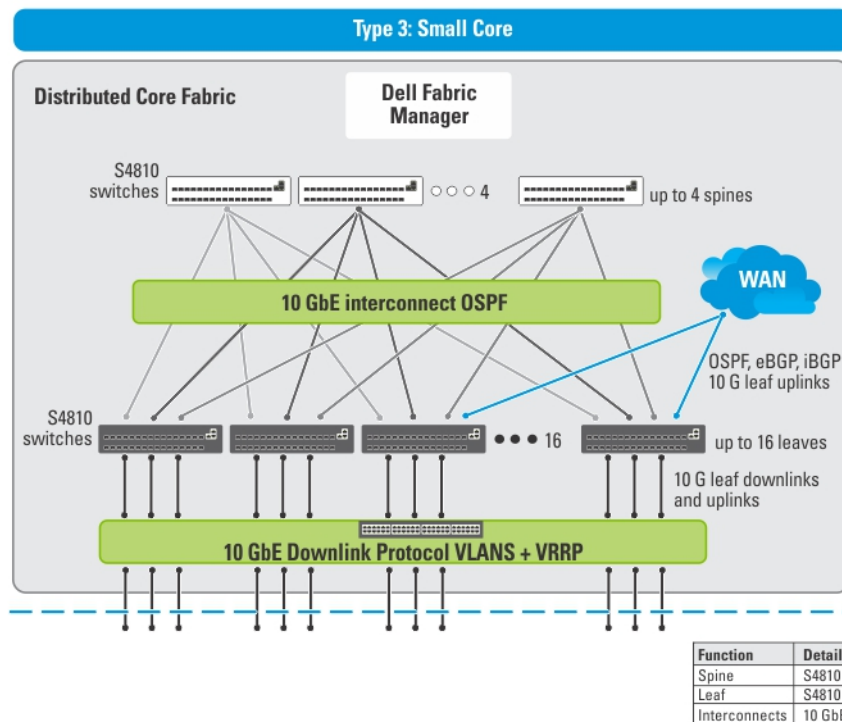
Type 3: Small Core Design

Use the Type 3: Small Core design when:

- An interconnect link bandwidth between the spines and leaves of 10 GbE is required.
- The current and future planned uplinks and downlinks on the leaves for your core is less than or equal to 960 ports.
- The leaves act as a switch or ToR-leaf switch. Within the ToR, the downlink protocol can be either "VLAN" or "VLAN and LAG".

NOTE: To enable the leaves to act as a ToR, check the **Enable the Leaves to Act as a ToR** box at the **Cores > Core Deployment > Design > Create a New Core > Downlink Configuration** screen

With a Type 3: Small Core design, the S4810 spines connect to the S4810 leaves at a fixed 10 GbE. The maximum number of spines is 4 and the maximum number of leaves is 16, as show in the following figure.



NOTE: The Dell Fabric Manager does not configure or manage anything beyond the distributed core.

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

- 40 Gigabit of interlink maximum capacity to the spine (4x 10Gig)
- 60 10 Gig Ethernet ports for servers per node and WAN connectivity

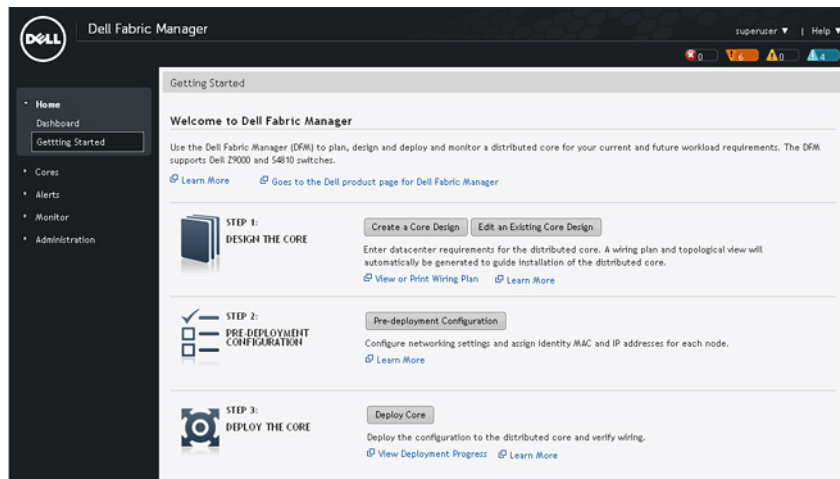
Getting Started

Designing and Deploying a Distributed Core

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

After you do the basic installation of the Dell Fabric Manager (DFM), you must configure it. This is done using the **Configuration Wizard** when the application first starts, as shown below. You can also start the configuration wizard at the **Home > Getting Started** screen or the **Cores > Core Deployment > Design > New Core** screen.

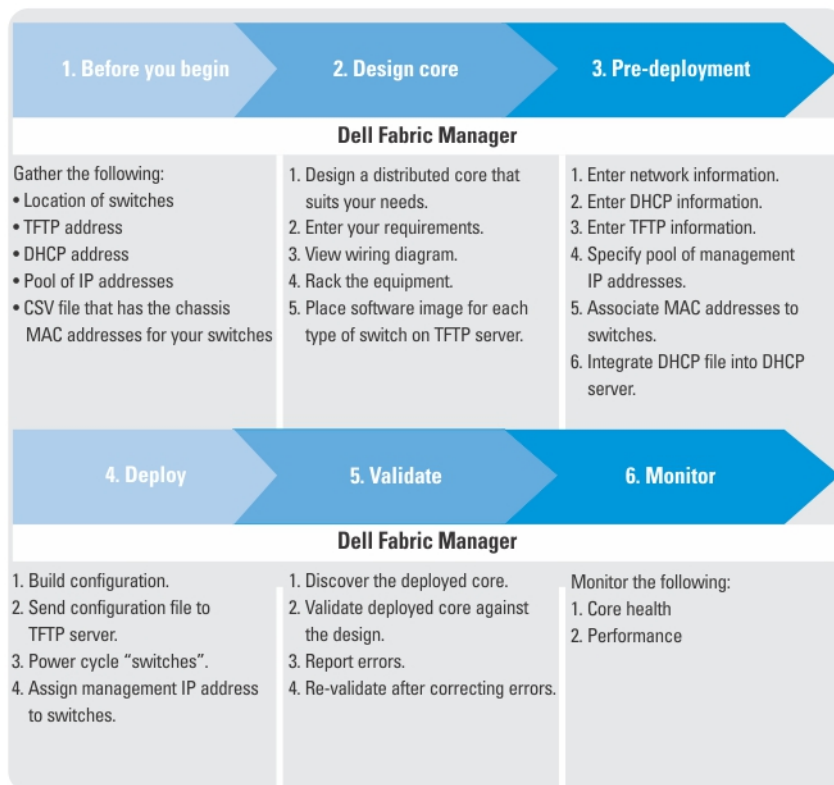
Review the steps in the wizard and the online help before you begin.



The user interfaces are similar in both areas.

The following flowchart shows how to design and deployment a new distributed core.


Flowchart for Designing and Deploying a Distributed Core




How to Design and Deploy a Distributed Core

To design and deploy a distributed core:

1. [Gather Useful Information.](#)
2. [Design a Distributed Core](#)
3. Build the physical network.
4. Configure the [TFTP](#), [SNMP](#), and [CLI Credentials](#) settings.
5. [Prepare the Core for Deployment.](#)
6. [Deploy and Validate the Core.](#)
7. Validate the deployed core against the core design .
8. Monitor the core health and performance. For more information, see the [Cores > Cores](#) and [Home > Dashboard](#) online help.

 **NOTE:** To provision the distributed core, you must also enter the FTOS CLI user's credential and enable configuration credential for all the switches in the distributed core. For information about this topic, see [CLI Credentials](#).

 **CAUTION:** If you are using a switch that has already been deployed, you must reset its factory settings to use it in the distributed core. The switch must be in BMP mode.


Using the Core Design Wizard

Use the **Core Design Wizard** at the **Home > Getting Started** screen or the **Cores > Core Deployment > Design > New Core** screen to design a two-tier distributed core (spine and leaf architecture) based on your workload requirements for your current and future needs. The design consists of a wiring plan, network topology information, summary of the inventory requirement, and a design specification.

Before you begin, review the [Getting Started](#) and [Designing a Distributed Core](#) sections. For information about a distributed core, see [Conventional Core Vs Distributed Core](#).

To design a distributed core, complete the following tasks using the **Core Design Wizard**.

1. [Core Design – Step 1: Welcome Page](#)
2. [Core Design – Step 2: Core Name, Type, OS Ratio, and Description](#)
3. [Core Design – Step 3: Port Count](#)
4. [Core Design – Step 4: Interlink Configuration](#)
5. [Core Design – Step 5: Uplink Configuration](#)
6. [Core Design – Step 6: Downlink Configuration](#)
7. [Core Design – Step 7: Output](#)
8. [Core Design – Step 8: Summary](#)

 **NOTE:** When you are finished designing the distributed core, prepare the core for deployment at the **Core Deployment > Pre-Deployment** screen. For more information, see [Preparing the Core for Deployment](#).

Core Design – Step 1: Welcome Page

Use the Core Design Wizard at the **Home > Getting Started** or **Cores > Design > New Core** screen to design a two-tier distributed core (spine and leaf architecture) based on your workload requirements for your current and future needs.

Use the following screens to design a distributed core:

1. Core Name and Type – The core name, type, interlink-oversubscription ratio, and description.
2. Port Count – The number of edge port uplinks and downlinks required for the initial deployment as well as for future expansion.
3. Interlink Configuration – The interconnect links (the links that connect the leaves and spines) using the OSPF routing protocol.
4. Uplink – The uplink connects to the WAN connection.
5. Downlink – The downlink connects to the servers, ToR, or switches.
6. Output view – Displays wiring, tabular, and topology diagrams.
7. Summary – Displays a summary of your distributed core design.

This profile is then applied to the distributed core design.

Core Design – Step 2: Core Name and Type

Use the **Core Design Wizard** at the **Home > Getting Started** screen to design a two-tier distributed core (spine and leaf architecture) based on the workload requirements for your current and future needs. To simplify and automate the design process, the Core Design provides three templates to build the following types of distributed cores:

- Type 1: Large Core
- Type 2: Medium Core
- Type 3: Small Core

The core designer wizard templates define the basic configuration for a distributed cores shown in the **Core Name and Type** screen, including:

- core name
- core type
- core description
- interlink over-subscription ratio

After you enter the basic core design information, the Core Design Wizard displays a list of requirements to build in the **Requirements based on the selected core type and oversubscription** section at the bottom right of the screen.

During the design phase, you enter information to generate a physical wiring diagram for the distributed core. The wiring diagram is typically given to the network operator who uses it to build the physical network. For information about designing a core, see [Designing a Distributed Core](#).

The screenshot shows the 'Core Design Wizard' interface. The 'Core Name and Type' step is active. The 'Core Name' field contains 'Test'. The 'Core Type' is set to 'Type 1 - Large Core'. The 'Interlink Over-subscription' is set to '1:1'. The 'Naming Example' section shows a list of devices: 'Test', 'Test-Spine-1', 'Test-Leaf-1', and '...'. The 'Requirement based on selected core type and oversubscription' section shows a table of requirements: Spine Device: 29000, Leaf Device: 29000, Max Spine devices: 16, Max Leaf devices: 32, Interconnect: 40Gb, Max Ports(10G): 2048. The progress indicator shows 'Step 2 of 8'.

To configure the core name and type:

1. Enter the name of the distributed core in the **Core Name** field.

The core name must be a unique name. It can have 1 to 21 characters. Valid characters are as follows:

- alphanumeric

- underscore (_)
- @
- +

When you specify the name of the distributed core, Dell Fabric Manager automatically names the nodes (spines and leaves) in the distributed core with the core name as the prefix. For example, if the name of the core is **EastCore**, the node names assigned are **EastCore-Spine-1** and **EastCore-Leaf1**.

2. (Optional) Enter the description of the distributed core.

There is no character restriction. The length of the description can be between 1 and 128 characters.

3. Select the core type from the **Core Type** pull-down menu.

For guidelines about selecting the core type, see [Designing a Distributed Core](#).

4. Select the interlink over-subscription rate that is appropriate for your deployment from the **interlink over-subscription ratio** pull-down menu.

The interlink over-subscription rate varies the maximum number of available interconnect links. The ratio you specify depends on the bandwidth, throughput, and available edge port requirements. The interlink over-subscription does **not** come off the edge port downlinks. As you increase the interlink over-subscription ratio:

- The total number of ports for the uplinks and downlinks increase.
- The total number interconnect links from the leaves to the spines decrease.
- The maximum number of available ports increases.

Use the 1:1 interlink over-subscription rate for the non-blocking, line rate between the leaves and spines. Use this option when you require a lot of bandwidth and not a lot of ports.

After entering the basic core design information, the Core Design Wizard displays a list of requirements to build the core in the **Requirements based on core type and oversubscription** section at the bottom right of the screen.

5. Click **Next** to go to the **Port Count** screen.

Core Design – Step 3: Port Count

Use the **Port Count** screen to enter the number of edge port uplinks and downlinks required for the initial deployment and future expansion.

This screen displays the following information:

- **Available Ports**—Displays the maximum available ports based on the selected core type and interlink over-subscription rate in the **Core Name and Type** screen. This is a read only field.
- **Total Planned Ports**—Displays the total number of ports for all the current and future uplinks and downlinks on the leaves.
- **Remaining Available Ports**—Displays the difference of available ports and total planned ports. This is a read-only field.
- **Uplinks**—Each uplink connects to a WAN, which typically connects to a ISP. The minimum number of current and future uplinks is 2 (one uplink is for redundancy) and the maximum is 32.
- **Downlinks**—The sum of downlink ports (current + future) should be minimum of 2 but not exceed the maximum available ports (available ports – (current + future uplink ports)).

When designing the distributed core, it is important to determine the future needs of the distributed core so that you can later expand it as the data center grows. After you finalized the core design, you **cannot** change it. As a result, make sure you enter the future requirements for the edge (leaf switch) ports in the **Number of additional edge ports for future expansion** area during the core design phase.

 **CAUTION:**

If you do not specify any additional links in the core design for future expansion:

- Any future expansion requires rewiring the hardware.
- IP addresses are not reserved.
- You might have to bring down currently deployed switches to expand the core.


For information on how to expand the core, see [Expanding the Core](#).

To specify the number of edge port uplinks and downlinks for initial deployment and for future expansion:

1. In the **Enter the number of edge ports required by the core (to be assigned to leaf switches area)**:
 - a) Enter an even number of uplink ports (connections to the WAN) required by the distributed core for initial deployment.
 - b) Enter an even number of downlink ports (connections to the servers, switches, or ToR) required by the distributed core for initial deployment.
2. In the **Number of additional edge ports for future expansion**
 - a) Enter an even number of uplink ports (connections to the WAN) required by the distributed core for future deployment.
 - b) Enter an even number of downlink ports (connections to the servers, switches, or ToR) required by the distributed core for future deployment.
3. Click **Next** to go the **Interlink Configuration** screen.

Core Design – Step 4: Interlink Configuration

Use the **Interlink Configuration** screen to configure the interconnect links (the links that connect the leaves and spines) using the OSPF routing protocol. The port bandwidth (a read-only field) is automatically determined by the selected core type and interlink-oversubscription rate.

 **NOTE:** The uplinks or interlinks must be in area 0 for OSPF.

To configure the interlink:


1. In **Protocol Settings**, click **Configure Protocol Settings**.
The **Interlink Protocol Settings** screen is displayed.
2. Specify the OSPF area ID.
The area ID can be a value between 0 and 65535.

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

3. Enter the starting IP address and prefix for the interconnect links in the **Starting IP address/Prefix** field.
Enter a valid IP address and prefix from 8 to 29.
4. Click on the **Preview range of IP addresses** link to view this information.
5. Enter the loopback address and prefix in the **Loopback IP Address/Prefix** fields.
Enter a valid IP address and prefix from 8 to 29.
6. Click on the **Preview range of IP addresses** link to view this information.
7. Click **Next** to go to the **Uplink Configuration** screen.

Core Design – Step 5: Uplink Configuration

The **Uplink Configuration** page displays the port bandwidth (a read-only field) and the number of specified ports entered on the **Core Name and Type** and **Port Count** screens. Use the **Uplink Configuration** screen to configure the uplink protocol for the edge port uplinks to the WAN.

 **NOTE:** The uplinks or interlinks must be in area 0 for OSPF.

To configure the uplink protocol for the edge port uplinks to the WAN:

1. From the **Protocol Settings** pull-down menu, select a routing protocol (OSPF, IBGP, or eBGP) for the edge port uplinks. The number of uplinks are specified in the **Port Count** screen.
The **Configure Uplink Protocol** is displayed.
The range of IP addresses belong to the **/30** subnet.
 - a) For OSPF, for each specified uplink, enter the local IP address, remote neighbor IP address, and area ID. A valid area ID area is 0 to 65535.
 - b) For iBGP, for each specified uplink, enter the AS number, local IP address, and remote neighbor IP address. For the AS number, enter a value from 1 to 4294967295.
 - c) For eBGP, for each specified uplink, enter the local AS number, local IP, remote neighbor IP address, and remote AS number. For the AS number, enter a value from 1 to 4294967295.
2. Click **Next** to go the **Downlinks Configuration** screen.

Core Design – Step 6: Downlink Configuration

Downlinks are edge port links which connect to servers, switches, or ToRs. When you enable the ToR configuration, the leaves function as a ToR. When you disable the ToR configuration, the leaves function as a switch.

To configure the edge port downlinks.

1. In the **Starting VLAN ID** field, enter a starting VLAN ID.
Range: 2 and 4094.
2. Enter the number of ports to be grouped for the VLAN and VRRP configuration.
Range: 1 to 16.
3. If you have a Type 2: Medium Core or Type 3: Small Core design and you want to enable the leaves to act as a ToR, check the **Enable Leaves as Top-of-Rack Switch** box and then select the **VLAN** or **VLAN and LAG** protocol setting.
4. If the leaves are acting as a leaf switch (the switches are directly connected to the server) , select the **VLAN and VRRP and LAG** protocol setting.
5. In the **Start IP Address Range/Prefix** field, enter the starting IP address and prefix.
Enter a valid IP address and a prefix from 8 to 23.
6. Click on the **Preview Range of IP Addresses that will be used** link to view this information.
7. Click **Next** to go the **Output** screen.

Core Design – Step 7: Output

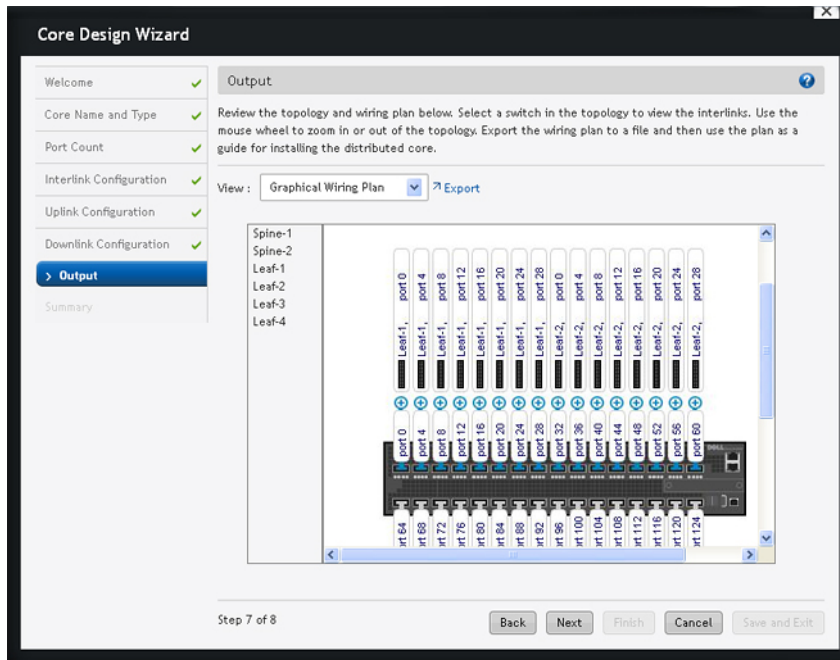
Use the **Output** screen to view the graphical wiring, tabular wiring, and network topology wiring plans for your core design. Use the wiring plan as a guide for installing your equipment into the distributed core. Based on the configuration, the DFM calculates the number of leaf and spine switches required for the design and displays the physical wiring plan which you can export and print in PDF. The wiring plans display the cabling maps (the connections between the spines and leaves).

After the distributed core design is approved, the wiring plan is then typically given to your data center operator who uses this information to build the physical network according to the distributed core design.

Review the wiring plans and then export them to a file.

The distributed core design configuration is displayed in the following formats from the **View** pull-down menu.

- **Graphical Wiring Plan**–Displays information about how the spines and leaves (switches) are connected graphically as shown below.




- **Network Topology**–Displays information about how the spines and leaves are connected physically using a topology map. Select a switch in the topology to view the interconnect links. Use the mouse wheel to zoom in or out of the network topology.
- **Tabular Wiring Plan**–Displays information about how the spines and leaves are connected in the distributed core design in a tabular format, shown below. The tabular wiring plan contains a list of switches along with their names and ports which connect to the ports on the other switches.

Field Name	Description
From Port	Displays the port number on the spine – from the side.
From Spine	Displays the name of the spine - from the side.
To Leaf	Displays the name of the leaf – to the side.
To Port	Displays the port number on the leaf – to the side.
Usage Status	Displays usage status: <ul style="list-style-type: none"> • Current – Represents the links based on your current needs • Future – Represents links based on your future needs • Expanded – Represents links based on your expansion needs (applicable only for the Expand Core Option)

To review and export the wiring plan:

1. Navigate to the **Cores > Core Deployment > Design > New Core > Output** screen.
2. Click the **Export** button.

The **Export Wiring Plan** window displays.

 **NOTE:** Exporting the network topology is not supported.

3. Specify the following export options.
 - a) In **What to export**, select one of the following options: **Save wiring table only (CSV)**, **Save graphical wiring plan only**, or **Save Both (CSV + graphical wiring plan)**.
 - b) In the **Include in graphical wiring plan**, select the following options that apply: **Interlinks**, **Uplinks**, **Downlinks**.
 - c) In the **Format for graphical wiring plan**, select **PDF**.

Core Design – Step 8: Summary

The **Summary** screen displays a summary of your distributed core design. Carefully review the design before you commit the changes.

To commit the changes, click **Finish**.

Next Steps

After you have designed the distributed core, complete the following to prepare the distributed core for deployment:

1. Check with system administrator for the TFTP IP address. Use this address to stage the switch software images. When you prepare the software images:
 - a) Make sure the software version is the same for each type of switch across the core.
 - b) Download the software image for each type of Dell switch Z9000 or S4810.
 - c) Stage the software images on the TFTP site.
2. Obtain a pool of management IP addresses from the lab or system administrator that will be used for switches in the distributed core.
3. Download the comma separate values (.csv) file that contains the switches chassis MAC address, if available. If not available, consult with Dell customer support.
4. Use the wiring plan to rack and cable the hardware according to the distributed core design wiring plan.
5. Document the location of the switches, including the rack and row.
6. Document the chassis MAC address and name of the switches in the distributed core so that you can map the address to the appropriate switch.
7. Return to DFM and select the **Pre-deployment** from the **Cores > Core Deployment > Deploy** pull-down menu.

Using the Pre-deployment Wizard

To prepare the distributed core for deployment, complete the following tasks using the **Pre-deployment Wizard**.

1. [Pre-deployment – Step 1: Introduction](#)
2. [Pre-deployment – Step 2: Assign Switch Identities](#)
3. [Pre-deployment – Step 3: Management IP](#)
4. [Pre-deployment – Step 4: Software Images](#)
5. [Pre-deployment – Step 5: DHCP Integration](#)
6. [Pre-deployment – Step 6: Output](#)
7. [Pre-deployment – Step 7: Summary](#)

Related Links:

- [Getting Started](#)
- [Gathering Useful Information](#)


Pre-Deployment – Step 1: Introduction

Use the **Pre-deployment Configuration Wizard** at the **Cores > Core Deployment > Pre-deployment** screen to prepare the distributed core for deployment:

Prerequisites

Before you begin:

- Rack the equipment in the distributed core.

 **NOTE:** Before racking the switches, make sure that you have the csv. file that contains the chassis MAC addresses for each switch in the distributed core. If you do not have this file, record the MAC addresses before you rack the switches.

- Power off the switches in the distributed core.

Gather the useful information listed in the **Introduction** screen, then click **Next**.

Use the following pre-deployment flowchart to prepare the distributed core for deployment.

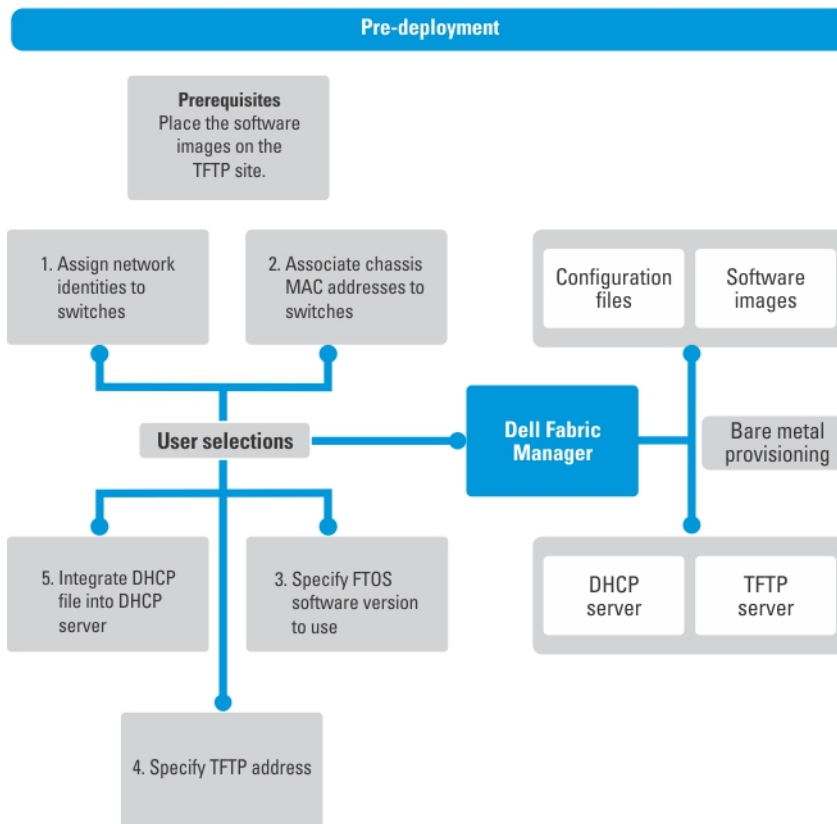



Figure 2. Pre-Deployment Flowchart


Flowchart for preparing the distributed core for deployment

 **NOTE:** The pre-deployment flowchart does not list all the prerequisites. For more information, see [Prerequisites](#).

Pre-Deployment Screens

Use the following **Pre-deployment** screens to prepare the distributed core for deployment. These screens automate the deployment process.

- Assign Switch Identities – Assigns chassis MAC address to each switch. You can optionally assign serial numbers and service tags to each switch.
- Management IP – Assigns management IP address to each switch.
- Software Images – Specifies the TFTP address and the path of the FTOS software image to load for each type of switch. Use this address to stage the software.
- DHCP Integration – Creates a **dhcp.cfg** 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:** You must install the DHCP configuration file on the DHCP server before you deploy the distributed core.

- Output – Displays the uplink and downlink configuration on the leaves. Verify that this information is correct before deploying the switches.

- Summary – Displays the core name, location of the software image, and DHCP configuration file.

Pre-deployment – Step 2: Assign Switch Identities

Use the **Assign Switch Identities** page to associate the chassis MAC addresses to the switches in the distributed core. Entering the serial numbers and service tags are recommend but not required. Load the CSV file that contains the chassis MAC addresses, serial numbers, and service tags for the switches in the distributed core. To get a sample CSV file, go to the **webapps/dfm/conf** directory.



NOTE: Before you begin, obtain the CSV file that contains the chassis MAC addresses, service tag, and serials numbers for each switch provided from Dell manufacturing or manually enter this information.

To assign switch identities:

1. Locate the CSV file that contains the chassis MAC addresses, serial numbers, and service tags for the switches in the distributed core. If you do not have this file, manually enter this information.
2. Navigate to the **Cores > Core Deployment > Deploy > Pre-deployment Configuration > Assign Switch Identities** screen.
3. In the **Default Gateway** field, enter the IP address of the default gateway and then the prefix-length.
4. In the route management, enter a static route that points to the management interface or a forwarding router.
forwarding-router-address—Enter an IPv4 or IPv6 address of a forwarding router and then the prefix-length for the IP address of the management interface.
management ethernet—Enter a static route that points to the management interface.
5. Click the **Browse** button and specify the path of the CSV file.
6. Click the **Upload** button.
7. Click the **Action** icon in each row to associate the switch name with the MAC address, serial number, and service tags.
8. Map the chassis MAC address, serial number, and service tag to each switch.
9. Click **Next** to go to the **Assign Management IP Addresses** screen.

Pre-Deployment – Step 3: Management IP

Use the **Management IP** screen to assign a management IP address to each switch in the distributed core.




NOTE: Before you begin, gather the pool of address for the management port for all the switches in the distributed core.

To assign a management IP address to the switches:

1. Navigate to the **Cores > Core Deployment > Deploy > Pre-deployment Configuration > Management IP** screen.
2. In the **Default Gateway** field, enter the address of the default gateway for the management interface.
3. In the **Management Route** field, enter the route and prefix of the management interface.
4. In the **Start Management IP Address/Prefix** fields, enter the starting management IP address and prefix.
5. Select the switches that you want to assign a management IP address.
6. Click the **Autofill Selected IP Addresses** button.
The system automatically assigns a management IP address to all the selected switches in the distributed core.
7. Click **Next** to go to the **Software Images** screen.

Pre-Deployment – Step 4: Software Images

Use the **Software Images** screen to specify which software images to stage for each type of switch for the distributed core from a TFTP site. The software image must be the same for each type of platform. Place the software image(s) for the switches on the TFTP site so that the switches can install the appropriate FTOS software image and configuration file. To change the address of the TFTP site, navigate to the **Administration > Settings** screen.

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

To specify which software images to load onto each switch in the distributed core from the TFTP site:

1. Navigate to the **Cores > Core Deployment > Deploy > Pre-deployment Configuration > Software Images** screen
2. Select the TFTP site containing the software image.
3. Enter the path of the software image(s) on the TFTP site.
4. Click **Next** to go to the **DHCP** Integration screen.

Pre-Deployment – Step 5: DHCP Integration

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

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

Install the DHCP file to an existing server or enable a DHCP server with this file. After you power cycle the switches, the switches use bare metal provisioning (BMP).

BMP provides the following features:

- Automatic network switch configuration and 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 Force10 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 a you install a switch, the switch searches the network for a DHCP server. The DHCP server provides the switch with an management IP address and the location of a TFTP file server. The file server maintains a configuration file and an approved version of FTOS for the Dell Z9000 and S4810 switches. The switch automatically configures itself by loading and installing an embedded FTOS image with the startup configuration file.

For more information about BMP, refer to the *Open Automation Guide* at <https://www.force10networks.com/CSPortal20/KnowledgeBase/Documentation.aspx> . Select the Open Automation heading.

To integrate the newly created DHCP file into the DHCP server:

1. Navigate to the **Cores > Core Deployment > Deploy > Pre-deployment Configuration > Software Images** screen.
2. Click **Save to ...** and then specify the location to save the generated DHCP configuration file. You can also copy and paste the configuration into the DHCP server.
3. Install the DHCP file onto the DHCP server before you deploy the core.

 **NOTE:** You must install the DHCP configuration file onto your DHCP server before you deploy the distributed core.


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

Pre-Deployment – Step 6: Output

Use the **Pre-deployment Output** screen to review the edge port uplinks and downlinks.

To modify an edge port uplink or downlink IP address or VLAN ID:

1. Navigate to the **Cores > Core Deployment > Pre-Deployment Configuration > Output** screen.
2. From the **View** pull-down menu, select the **Uplink Output** or **Downlink Output** option.
3. Click **Export** to export this information.
4. Click **Next** to go to the **Summary** screen.

 **NOTE:** Only hardware inventory for the interlinks (the connections between the spines and leaves) are displayed in the pre-deployment summary screen.

Pre-Deployment – Step 7: Summary

Use the **Summary** screen to review the pre-deployment configuration.

To view the pre-deployment configuration:

1. Navigate to the **Cores > Core Deployment > Deploy > Pre-deployment Configuration > Summary** screen.
2. Carefully review the pre-deployment configuration before you commit it.
3. Click **Finished** to commit the changes.

Next Steps:

1. Verify that the DHCP configuration file that you created for your distributed core has been integrated into the DHCP server so that the switches can be assigned a management IP address.
2. Navigate to the **Cores > Core Deployment > Deploy > Core Deployment** screen.
3. Deploy and validate the core.

Deploying and Validating the Core

Use the **Core Deployment** screen to deploy the distributed core. Make sure that the designed core matches the deployed core. DFM prompts you to fix any errors when you deploy the distributed core. To view the DHCP file for the selected core, navigate to the **Core Deployment > Deploy > View DHCP Configuration** screen.

Use the core validation to verify that the discovered distributed core matches the planned distributed core and correct any errors. If errors found during validation are fixed, you must validate the core to verify that all the issues were fixed according to the planned core using the **Start Validation** option.

To view a configuration file, select the switch you want to look at, and click the **View Configuration File** button.

To deploy a distributed core:

1. Verify that the software images for the switches have been installed on to the TFTP server.
2. Verify that you have configured the correct TFTP address at the **Administration > Settings > TFTP Settings** screen.
3. Verify that the DHCP configuration file generated by the DFM for the switches in the distributed core has been integrated into the DHCP server. This file enables the switch to connect to the DHCP server and download the correct configuration and boot.
4. Restart the DHCP server that contains the generated DHCP file that you created in the DHCP integration screen. For information about DHCP integration, see [Pre-Deployment Wizard – Step 4: DHCP Integration](#)
5. Navigate to the **Cores > Core Deployment** screen.
6. Select **Deploy** from the **Core** menu.
7. Select the core that you want to deploy.
8. On the **Deploy Status** tab, select the spines and leaves that you want to deploy.

Deploy and Validate Core: CoreTyp2

Core Deployment

To deploy the distributed core, select one or more switches and then click the Deploy Selected Nodes button. View errors on the Validation Errors tab. This screen may be closed and brought up again by selecting Deployment Progress from the Cores menu.

The DHCP Configuration must be manually installed on the DHCP server before continuing past this point. Deploying the core with an incorrect DHCP configuration may cause unpredictable results.

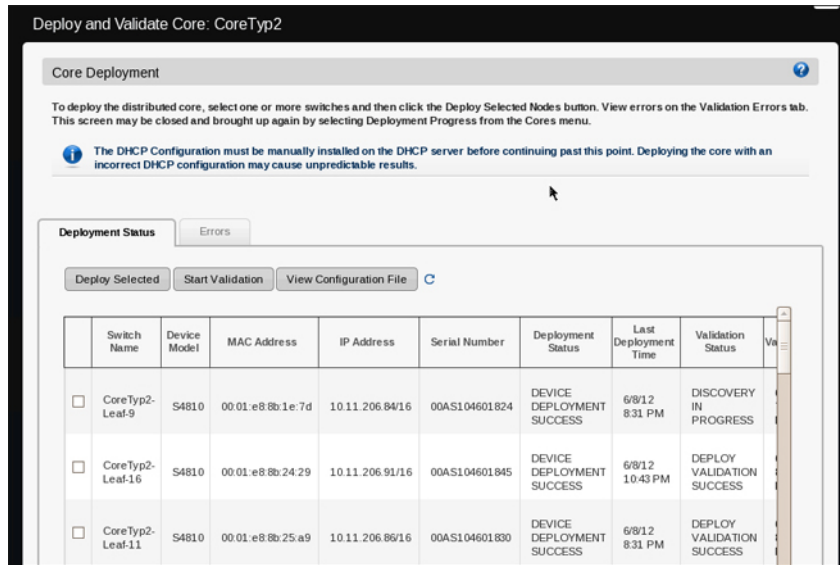
Deployment Status Errors

Deploy Selected Start Validation View Configuration File

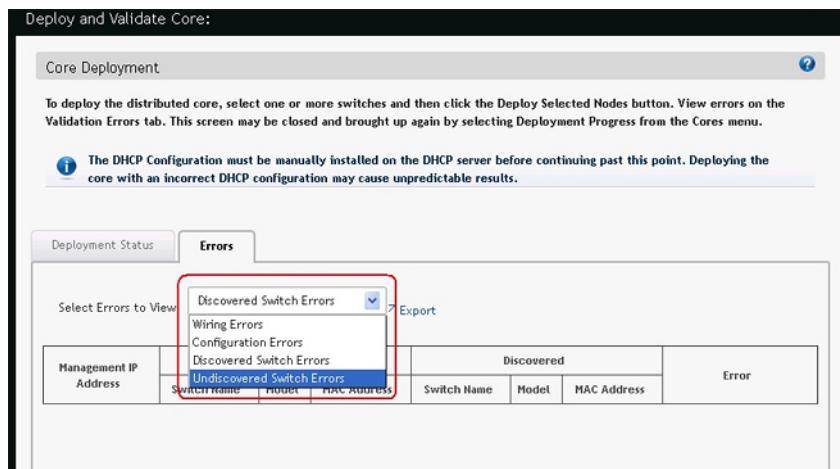
	Switch Name	Device Model	MAC Address	IP Address	Serial Number	Deployment Status	Last Deployment Time	Validation Status	View
<input type="checkbox"/>	CoreTyp2-Leaf-9	S4810	00 01 e8 8b 1e 7d	10.11.206.84/16	00AS104601824	DEVICE DEPLOYMENT SUCCESS	6/8/12 8:31 PM	DISCOVERY IN PROGRESS	
<input type="checkbox"/>	CoreTyp2-Leaf-16	S4810	00 01 e8 8b 24 29	10.11.206.91/16	00AS104601845	DEVICE DEPLOYMENT SUCCESS	6/8/12 10:43 PM	DEPLOY VALIDATION SUCCESS	
<input type="checkbox"/>	CoreTyp2-Leaf-11	S4810	00 01 e8 8b 25 a9	10.11.206.86/16	00AS104601830	DEVICE DEPLOYMENT SUCCESS	6/8/12 8:31 PM	DEPLOY VALIDATION SUCCESS	

9. Click **Deploy Selected Nodes** and wait for the distributed core to deploy.
10. **Power up** the selected nodes.
11. Check the progress and status of the deployment in the **Progress** and **Status** columns.

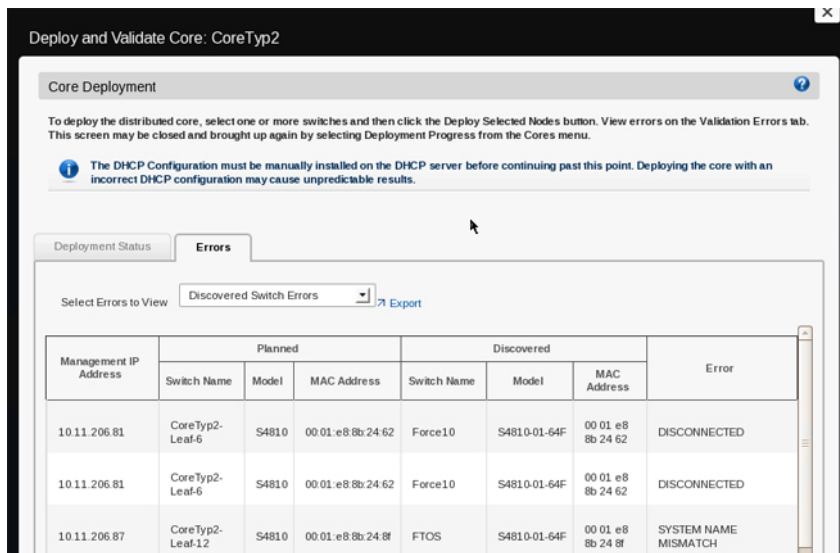
For information about the progress and status of selected nodes and operations allowed during a core state, see [Operations Allowed During Each Core State](#) and [Understanding Core Phases](#).



12. Click on the **Errors** tab to view the following type of errors from the **Select Errors to View** pull-down menu.



- a) Discovered Switch Errors—If you have discovered switch errors, log on to switch console to isolate the fault.



- b) Undiscovered Switch Errors—If you have undiscovered switch errors, log on to switch console to isolate the fault. Make sure that the switch has been power cycled on and check the physical connection.
 - c) Configuration Errors—Click the **View Mismatch** button to view the configuration errors. Review the configuration mismatch and correct it.
 - d) Wiring Errors—Click the **View Mismatch** button to view the wiring errors. Review the wiring mismatch and correct it.
13. Click on the **Export** button to export the errors.
 14. Fix any errors.
 15. When the deployment status for a switch is successful on the DFM, log on to the switch and verify that the switch has the correct software version, system name, management IP address, VLANs, and MAC address.

Viewing Deployment and Validation Status


To view the deployment and validation status of the distributed core.

1. Navigate to the **Cores > Core Deployment** screen.
2. Select the distributed core that you want to view.
3. From the **Deploy** pull-down menu, select **Viewing Deployment and Validation Status**.
The **Deployment Status** screen is displayed.

Understanding Core Phases

DFM allows you to create a distributed core design, make changes to the pre-deployment configuration, deploy the core, and validate the core designed with the discovered core. DFM provides up-to-date status during each phase of the core from design to validate. The DFM displays any pending steps required that you need to complete to ensure the distributed core is fully functional for each core design.

The following table describes the four core phases displayed on the **Cores > Core Deployment** screen. Use this information to correct the distributed core design and pre-deployment configuration before and after you deploy the distributed core.

Phase	State
Design	<ul style="list-style-type: none"> • Incomplete—Indicates that only partial information was provided to the core design. This state is applicable only during initial design. After a design is completed, it will never revert back to this state. • Complete—Indicates that all required information was entered to complete the core design.
Pre-deployment Configuration	<ul style="list-style-type: none"> • Not Started—Indicates that pre-deployment configuration was never initiated. • Incomplete—Indicates that only part of the pre-deployment configuration was entered and the information provided is not sufficient to proceed with the deployment. • Partial Complete—Indicates that only part of the pre-deployment configuration was entered and the information provided is sufficient to proceed with deployment. • Complete—Indicates that all pre-deployment configurations were entered and the information provided is sufficient to proceed with the deployment.
Deployment	<ul style="list-style-type: none"> • Not Started—Indicates that deployment was never initiated. • In-progress—Indicates that deployment is in-progress. • Incomplete—Indicates that deployment did not succeed on any switches. Validation is not performed automatically. • Partial Complete—Indicates that the deployment succeeded for one or more nodes. Validation is not performed automatically. • Complete—Indicates that all the switches the distributed core were deployed.
Validation	<ul style="list-style-type: none"> • Not Started—Indicates that core validation was never initiated.
	 NOTE: Validation can be initiated if the deployment configuration is in the partial complete or complete state.
	<ul style="list-style-type: none"> • In-progress—Indicates that core validation is in-progress. The deployment configuration is in a partial complete or complete state. • Error—Indicates that one or more validation errors exist. • Complete—Indicates that no validation error exists.

Operations Allowed During Each Core State

Use the following table to determine which operations are allowed during the design, pre-deployment configuration, deployment, and validation states.

Table 1. Operations Allowed the Each Core State

Design State	Pre-Deploy Configuration State	Deployment State	Validation State	Operation Allowed
Incomplete	Not Started	Not Started	Not Started	<ul style="list-style-type: none"> Edit Core Delete Core
Complete	Not Started	Not Started	Not Started	<ul style="list-style-type: none"> View Wiring Plan Edit Core (All core attributes) Pre-deployment Configuration Delete Core
Complete	Incomplete. The chassis MAC and IP address are not configured for any of the switches.	Not Started	Not Started	<ul style="list-style-type: none"> View Wiring Plan Edit Core (All core attributes except core name) Pre-deployment Configuration Delete Core
Complete	Partial Complete / Complete–Partial complete indicates that at least 1 switch has its chassis MAC and IP address configured.	Not Started	Not Started	<ul style="list-style-type: none"> View Wiring Plan Edit Core (All core attributes except core name) Pre-deployment Configuration View DHCP Configuration Deploy and Validate Core View Deployment and Validation Status Delete Core
Complete	Partial Complete / Complete	In-progress	Not Started / In-progress /	<ul style="list-style-type: none"> View Wiring Plan

			Stopped / Error / Complete	<ul style="list-style-type: none"> • View DHCP Configuration • View Deployment and Validation Status • Delete Core
Complete	Partial Complete / Complete	<p>Incomplete / Partial Complete / Complete</p> <p>Incomplete indicates that the DFM is in the middle of deploying the switches.</p> <p>Complete indicates all the switches in the distributed core are deployed.</p>	Not Started / In-progress / Stopped / Error / Complete	<ul style="list-style-type: none"> • View Wiring Plan • Edit Core—Allow editing of all core attributes except core name, core type interlink over-subscription, port count, and expand core. • Expand Core—Port Count and uplink Configuration (allow additions in Configure Protocol Setting) • Pre-deployment Configuration • View DHCP Configuration • Deploy and Validate Core – Validation is only allowed when deployment is partial or fully complete • View Deployment and Validation Status • Delete Core

Troubleshooting

Use this section to troubleshooting a deployed distributed core.



This section contains the following topics:




- [Validation Errors](#)
- [Validating Connectivity to the ToR](#)
- [Switch Deployment Status Errors](#)

Switch Deployment Status Errors


Use the following table to troubleshoot switch deployment status errors.

Table 2. Switch Deployment Status Errors

Switch Deployment Status	Description	Requires Action	Recommended Actions
NOT STARTED	Not Started	No	Start the deployment of the switch from the Core Development > Deploy > Deploy and Validate Core screen by selecting the switch from the list and then click on the Deploy Selected button.  NOTE: 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	<ol style="list-style-type: none"> 1. Check the write permission for the DFM installation directory in the DFM server machine. 2. Verify that the disk space is not full in the DFM server. 3. Restart the deployment of the switch from the Core Development > Deploy > Deploy and Validate Core screen by selecting the switch from the list and then click on the Deploy Selected button.  NOTE: The switch is in BMP mode.
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	<ol style="list-style-type: none"> 1. Verify the connectivity to the TFTP server from the DFM server. 2. Restart the deployment of the switch from the Core Development > Deploy > Deploy and Validate Core screen by selecting the switch from the list and then click on the Deploy Selected button. <p> NOTE: The switch is in BMP mode.</p>
CONFIG FILE TRANSFER SUCCESS	Configuration File Transferred Successfully	No	Information only.
REQUEST TO DISCOVER NODE	Request To Discover Switch	Yes	<ol style="list-style-type: none"> 1. Power on the switch. 2. Restart the deployment of the switch from the Core Development > Deploy > Deploy and Validate Core screen by selecting the switch from the list and then click on the Deploy Selected button. <p> NOTE: The switch is in BMP mode.</p>
MIN CONFIG UPLOAD INPROGRESS	Minimum Configuration Upload In-Progress	No	Information only.
MIN CONFIG UPLOAD ERROR	Minimum Configuration Upload Error	Yes	<ol style="list-style-type: none"> 1. Verify the connectivity to the TFTP server from the switch. 2. Check the Validation Status column for errors and fix them. 3. Verify that the MAC address in the dhcpd.conf file matches the csv. file that contains the MAC addresses of the switches. 4. Verify that the min.cfg file is in the correct directory on the TFTP server. 5. Redeploy the switch from the Core Development > Deploy > Deploy and Validate Core screen by selecting the switch from the list and then click on the Deploy Selected button. <p> NOTE: The switch is in BMP mode.</p>
MIN CONFIG UPLOAD COMPLETED	Minimum Configuration Upload Successful	No	Information only.
INIT SOFT RELOAD	Initiated Soft Re-load on Switch	No	Information only.
INIT SOFT RELOAD ERROR	Error During Soft Re-load on Switch	Yes	<ol style="list-style-type: none"> 1. Check the switch syslogs for a reload command failure.


2. Make any necessary fixes.
3. Restart the deployment of the switch from the **Core Development > Deploy > Deploy and Validate Core** screen by selecting the switch from the list and then click on the **Deploy Selected** button.

 **NOTE:** The switch is in BMP mode.

PROTOCOL CONFIG UPLOAD INPROGRESS	Protocol Configuration Upload In-Progress	No
PROTOCOL CONFIG UPLOAD ERROR	Protocol Configuration Upload Error	Yes

Information only.

1. Verify the connectivity to the TFTP server from switch.
2. Check the **Validation Status** column for errors and fix them.
3. Verify that the DHCP server is running.
4. Verify that the CFG file correctly has been placed on the TFTP server and that you can ping it from the switch.
5. Redeploy the switch from the **Core Development > Deploy > Deploy and Validate Core** screen by selecting the switch from the list and then click the **Deploy Selected** button.

 **NOTE:** The switch is not in BMP mode.

PROTOCOL CONFIG UPLOAD COMPLETED	Protocol Configuration Upload Successful	No
DEVICE DEPLOYMENT SUCCESS	Switch Deployment Successful	No
UPLINK CONFIG GENERATED	Uplink Configuration Generated	No
UPLINK CONFIG UPLOAD IN PROGRESS	Uplink Configuration Upload In-Progress	No
UPLINK CONFIG UPLOAD ERROR	Uplink Configuration Upload Error	Yes

Information only.

Information only.

Information only.


Information only.

1. Verify the connectivity between the DFM server and switch.
2. Check the **Validation Status** column for errors and fix them
3. Restart the deployment of the switch from the **Core Development > Deploy > Deploy and Validate Core** screen by selecting the switch from the list and then click on the **Deploy Selected** button.


UPLINK RECONFIGURED
REDEPLOY REQUIRED

Uplink re-configured, Re-
deployment of Switch is
required

Yes

 **NOTE:** The switch is not in BMP mode.

Restart the deployment of the switch from the **Core Development > Deploy > Deploy and Validate Core** screen by selecting the switch from the list and then click on the **Deploy Selected** button.


 **NOTE:** The switch is not in BMP mode.

Restart the deployment of the switch from **Core Development > Deploy > Deploy and Validate Core** screen by selecting the switch from the list and then click on the **Deploy Selected** button.

REDEPLOYMENT REQUIRED

Re-deployment of the switch
is required

Yes

 **NOTE:** The switch is not in BMP mode.

Validating Connectivity to the ToR

To validate the leaves downlink connections to the ToR:

1. Ping the ToRs from the leaves.
2. Confirm the VLAN configured on the leaf is same on the port.

Validation Errors

Use the following tables to troubleshoot the following validation errors when you deploy a distributed core.

To view validation errors, navigate to the **Core Development > Deploy > Deployment and Validate Core** screen and click on the **Errors** tab as shown below to view the following type of errors from the **Select Errors to View** pull-down menu

- Wiring Errors
- Configuration Errors
- Discovered Switch Errors
- Undiscovered Switch Errors

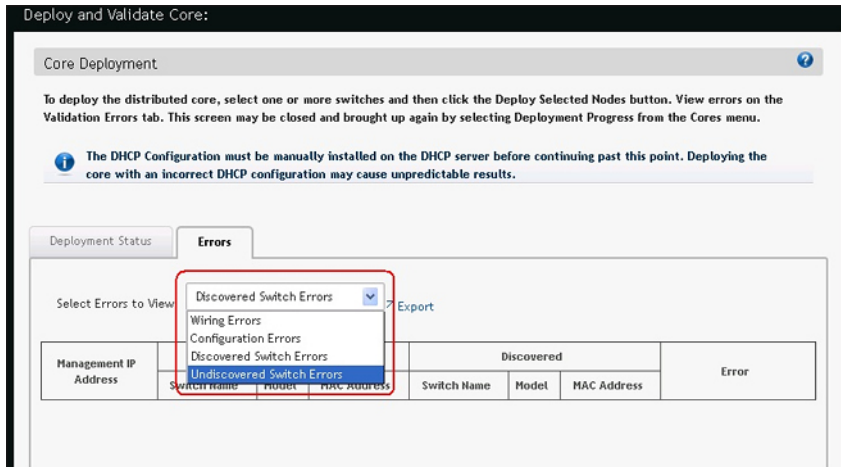


Table 3. Configuration Errors

Configuration Error

Recommended Action

Configuration Mismatch

1. On the **Deployment and Validation Status** screen, select the switch that you want to view.
2. Click the **View Mismatch** button.
3. Review the configuration mismatch and correct the configuration errors.
4. Restart validation of the switch from the **Deploy and Validate Core** screen by selecting the switch from the list and clicking the **Start Validation** button.

Table 4. Wiring Errors

Wiring Error

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 from the **Deploy and Validate Core** screen by selecting the switch from the list and clicking on the **Start Validation** button.

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 from the **Core Deployment > Deploy > Deploy and Validate Core** screen by selecting the switch from the list and then clicking the **Start Validation** button.

Partial Link

1. Verify that the switch is wired according to the wiring plan.
2. Verify the connectivity on the DFM from both of switches of the link.
3. Validate the switch from the **Core Deployment > Deploy > Deploy and Validate Core** screen by selecting the switch from the list and then clicking the **Start Validation** button.

Table 5. Undiscovered Switch Error

Undiscovered Switch Error

Recommended Action:


1. Verify that the switch has a valid IP address.
2. If required, correct the pre-deployment configuration.
3. From the DFM server, verify that the connectivity to the switch exists.
4. Verify that the switch is running the minimum required software.
5. Validate the switch from the **Core Deployment > Deploy > Deploy and Validate Core** screen by selecting the switch from the list and then clicking the **Start Validation** button.

Table 6. Discovered Switch Error

Discovered Switch Error	Recommended Action
Disconnected	<ol style="list-style-type: none"> 1. Verify that the connectivity to the switch exists from the DFM server. 2. Verify that the switch is running the minimum required software. 3. Validate the switch from the Core Deployment > Deploy > Deploy and Validate Core screen by selecting the switch from the list and then clicking the Start Validation button.
Switch Name Mismatch	<ol style="list-style-type: none"> 1. Verify that the IP address to switch name mapping is correct in the pre-deployment configuration. 2. If the pre-deployment configuration is updated, you might need to redeploy the switch. 3. Validate the switch from the Core Deployment > Deploy > Deploy and Validate Core screen by selecting the switch from the list and then clicking the Start Validation button.
Model Mismatch	<ol style="list-style-type: none"> 1. Verify that the IP address to switch name mapping is correct in the pre-deployment configuration. 2. If the pre-deployment configuration is updated, you might need to redeploy the switch. 3. Validate the switch from the Core Deployment > Deploy > Deploy and Validate Core screen by selecting the switch from the list and then clicking the Start Validation button.
MAC Address Mismatch	<ol style="list-style-type: none"> 1. Verify that the IP address to switch name mapping is correct in the pre-deployment configuration. 2. If the pre-deployment configuration is updated, you might need to redeploy the switch. 3. Validate the switch from the Core Deployment > Deploy > Deploy and Validate Core screen by selecting the switch from the list and then clicking the Start Validation button.


Expanding the Core

Use the **Expand Core Design** screens to expand a deployed core. If you have configured the distributed core for future expansion and deployed it, you can later expand it. For information on configuring future expansion, see the [Core Design – Step 3: Port Count](#).

 **NOTE:** When you use the Expand the Core wizard, the **Core Name and Type** and **Downlink Configuration** screens are read-only. The DFM automatically configures the downlinks entered in the **Port Count** screen.

To expand the distributed core:

1. Navigate to the **Cores > Core Deployment** screen.
2. Click the distributed core that you want to expand.
3. Click on the **Design** pull-down menu and select the **Expand Selected Design** option.
The **Expand Core Design** screen displays.
4. In the **Port Count** screen, enter the additional edge uplink and downlink ports for expansion.
5. In the **Uplink Configuration** screen, click **Configure Protocol Settings Link**, and then add only the entries corresponding to the newly added uplinks.

 **NOTE:** When you expand the core, you cannot edit or delete prior entries or change the protocol.

6. In the **Output** screen, review the wiring plan and export it. For more information, see the online help page associated with this screen.
7. In the **Summary** screen, save the settings and follow the next steps. For more information, see the online help page associated with this screen.
8. Prepare the core for deployment at the **Cores > Core Deployment > Deploy > Pre-deployment** screen. For more information, see [Preparing the Core for Deployment](#).
9. Deploy the core at the **Cores > Core Deployment > Deploy > Deploy** screen. For more information, see [Deploying and Validating the Core](#).

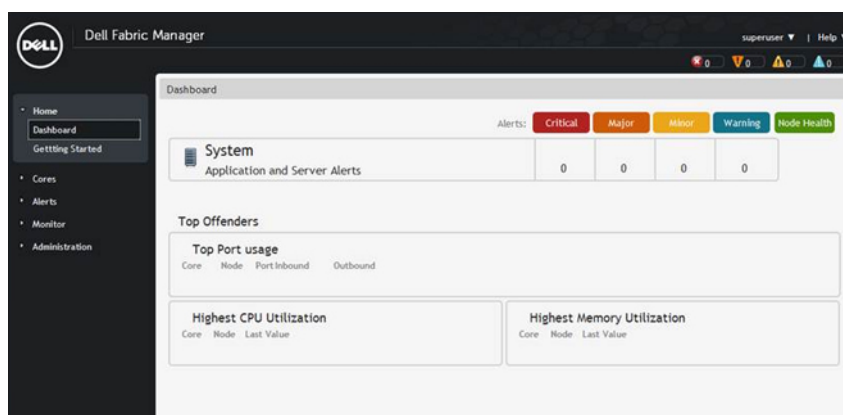
Modifying and Viewing the Distributed Core

This section contains the following topics:

- [Dashboard](#)
- [Cores](#)
- [Editing the Core](#)
- [Deleting the Core](#)
- [Viewing and Exporting Wiring Diagram](#)
- [Viewing the Core DHCP Configuration File](#)

Dashboard

Use the **Home > Dashboard** screen as shown below to view the distributed core and system health.



This screen provides the following information about key performance:

- **System/Network Health**—Provides a tabular listing of system and distributed cores being managed by the system and lists the corresponding alert count by severity. The **Node Health** column displays the number of nodes that are alert free and the total nodes that are part of the distributed core.
- **Top 5 Highest Memory Utilization**—Displays the top 5 switches whose memory utilization is the most across all the distributed cores.
- **Top Link Usage**—Displays the top 10 link ports whose link use is the most across all the distributed cores.
- **Highest CPU Utilization**—Displays the top 5 switches whose CPU utilization is the most across all the distributed cores.

Related links:

- [Alerts](#)
- [Monitor](#)

Cores

Use the **Cores > Cores** screen to display information about a deployed distributed core at the network, core, spine, leaf, and port level. The view is split into the tree view, tabular view, and tabbed view.



NOTE: You must deploy a distributed core to view information about the core.

- **Tree view**—The tree view on the left pane allows you to easily navigate across the cores and nodes. The tree hierarchy consists of the Network, Core, and Node (spine or leaf).
Tabular view—The tabular view format provides a tabular listing of the cores managed by the system. The core and node names are unique within their hierarchy. You can expand or collapse the cores. By default, the cores are not expanded. To view the core in a tabular, click the **Tabular** icon in the top right of the screen
- **Tabbed view**—Information in the tabbed view is displayed only when at least a single distributed core is selected.
- To view the core graphical format, click the **Graphical** icon in the top right of the screen.
- To view statistics at the port level, select **Port Details**. For information about a specific port, place your cursor on a specific port. Use the legend at the top right of the screen to determine the status of the ports.
- To change a node (spine or leaf) to **managed** or **un-managed**, select the appropriate option from the **Actions** pull-down menu.

All the relevant statistics for the spine or leaf at the switch level are displayed in the bottom window in the following tabs:

- **Summary**—Displays summary information about the switch.
- **Active Alerts**—Displays active alerts.
- **Event History**—Displays event history.
- **Links**—Displays the status of the links (up or down) on the ports.
- **Performance**—Displays statistics as a table or chart. You can specify a time interval. With the chart, you can also specify the following metrics: **cpuUsage** and **memUsage**.
- **Hardware Components**—Displays the status of the fan tray and power supplies.

Related links:

- [Alerts](#)
- [Monitor](#)
- [Dashboard](#)

Editing the Core

Use **Edit Core** option to modify an existing core design. Prior to deploying a core, you can modify all the parameters of the core design except the core name. After the deployment of the core has started you cannot edit the core.

To edit an existing core:

1. Navigate to the **Cores > Core Deployment** screen.
2. Select the core that you want to edit.
3. From the **Design** pull-down menu, select the **Edit Core** option.

Deleting the Core

When you delete a distributed core, Dell Fabric Manager manages the switches in the distributed core and removes the core related information from the system.

To delete the a distributed core:

1. Navigate to the **Cores > Cores Deployment** screen.
2. Select the core that you want to delete.
3. Click the **Delete** button.

Viewing and Exporting Wiring Diagram

To view and export the wiring diagram:

1. Navigate to the **Cores > Core Deployment** screen.
2. Select the core that you want to view.
3. From the **Design** pull-down menu, select **View/Export Wiring Plan**.

Viewing the DHCP Configuration File

To view the DHCP configuration file created for the distributed core:

1. Navigate to the **Cores > Core Deployment** screen.
2. Select the distributed core associated with the DHCP configuration that you want to view.
3. From the **Deploy** pull-down menu, select **View DHCP Configuration**.

The DHCP configuration for the selected distributed core is displayed.

For more information on DHCP, see the [Pre-Deployment – Step 5: DHCP Integration](#).

Alerts

This section contains the following topics:

- [Active Alerts](#)
- [Alerts and Event History](#)

Active Alerts

Use the **Alerts > Active Alerts** screen to display the active alerts in the distributed core and DFM. The top navigation pane also displays a summary of alerts for each severity across all cores. The system also displays the name of the user logged in, along with the options to **Logout** and access **Help**. Clicking an alert from this pane opens the **Alerts > Active Alerts** screen.

- 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 acknowledge an active alert, select the active alert and then click the **Acknowledge** button.
- To unacknowledge an active alert, select the active alert and then click the **Unacknowledge** button.

To filter active alerts:

1. Navigate to the **Alerts > Active Alerts** screen.
2. Click the filtering icon.
The filtering options display.
3. In the **Severity** pull-down menu, select one of the following filtering criteria:
 - a) **All**
 - b) **Critical**
 - c) **Major**
 - d) **Minor**
 - e) **Warning**
 - f) **Unknown**
 - g) **Info**
 - h) **Indeterminate**
4. In the **Source IP** field, enter the source IP address.
5. In the **Source Name** field, enter the source name.
6. In the **Probable Cause** field, enter a probable cause.
7. In the **Ack** (acknowledgement) pull-down menu, select one of the following:
 - a) **All**
 - b) **Yes**
 - c) **No**

Alerts and Event History

Use this screen to view alerts and event history.

- To refresh the screen, click the reload grid icon.
- To export alerts and event history, click the **Export** button.

To filter alerts and event history in the distributed core and DFM:

1. Navigate to the **Alerts > Alerts and Events** screen.
2. Click the filtering icon.
The filtering options display.
3. In the **Severity** pull-down menu, select one of the following filtering criteria:
 - a) **All**
 - b) **Critical**
 - c) **Major**
 - d) **Minor**
 - e) **Warning**
 - f) **Unknown**
 - g) **Info**
 - h) **Indeterminate**
4. In the **Source IP** field, enter the source IP address.
5. In the **Source Name** field, enter the source name.
6. In the **Description** field, enter the description.
7. In the **Ack** (acknowledgement) pull-down menu, select one of the following:
 - a) **All**
 - b) **Yes**
 - c) **No**

Monitor


This section contains the following:

- [Reports](#)
- [Global Statistics](#)
- [Data Collection](#)

Reports

This section contains the following topics:

- [Creating a new report](#)
- [Running a Report](#)
- [Editing a report](#)
- [Duplicating reports](#)
- [Deleting a report](#)

 **NOTE:** To run a report, you must schedule the data collection to start the task.

Creating a New Report

To create a new report:

1. Navigate to the **Monitor > Reports** screen.
2. Click the **New Report** button.
The **Add/Modify Reports** screen displays.
3. In the **Report Name** field, enter the name of the report.
4. (Optional) In the **Description** field, enter a description of the report, then click **Next**.
5. In the **Type and Output** field:
 - a) Select a report type: **Switch** or **Port**.
 - b) Select a report output format: **Tabular** or **Chart**.
6. Click **Next**.
7. In the **Date/Time Range** pull-down menu, select a date or time range using one of the following options. If you select the custom range, specify a start and end date.
 - a) **30 days**
 - b) **7 days**
 - c) **24 hours**
 - d) **Custom Range**
8. Click **Next**.
9. In the **Monitors** field, select which monitors to use for the report: **CpuUtilization** (CPU utilization), **MemUtilization** (memory utilization), and then click the **>>** button.

10. In the **Query** field, to determine what to nodes should be included in the report for a core:
 - a) Select the core to query from the first pull-down menu.
 - b) Select the type of switches (spine and leaves) from the 2nd pull-down menu.
11. In the **Available Nodes/Ports** area, select the nodes that you want to include in the report, and then click the **>>** button.
12. In **Summary** screen, review the report settings.
13. If you want to run the report now, check the **Run Report Now** option.
14. Click the **Finish** button.

Running a Report

Before you can run a report, you must schedule the data collection to start the task. For information on scheduling data collection, see [Data Collection](#).

To run a report:

1. Navigate to the **Monitor > Reports** screen.
2. Select the report that you want to run.
3. Click the **Run** button.

Editing a Report

To edit a report:

1. Navigate to the **Monitor > Reports** screen.
2. Select the report that you want to edit.
3. Click the **Edit** button.
The **Add/Modify Report** screen displays.
4. Edit the report. Click the **Next** button to navigate to different parts of the report.
5. In the **Summary** area, review your changes.
6. Click **Finish**.

Duplicating Reports

To duplicate a report

1. Navigate to the **Monitor > Reports** screen.
2. Select a report that you want to duplicate.
3. Click the **Duplicate** button.
The **Duplicate** screen displays.
4. In the **Report Name** field, enter the name of the report.
5. (Optional) In the **Description** field, optionally enter a description.
6. Modify the report as needed.
7. Click the **Next** button to navigate to different parts of the report that you want to duplicate.
8. Click **Finish**.

Deleting a Report

To delete a report:

1. Navigate to the **Monitor > Reports** screen.
2. Select the report that you want to delete.
3. Click the **Delete** button.
The **Delete Confirmation** window displays.
4. Click **Yes**.

Global Statistics

The **Global Statistics** screen displays the following statistics at the core level:

- Top 25 ports used.
- Top 10 highest CPU utilization.
- Top 10 highest memory utilization.

To view global statistics:

1. Navigate to the **Monitor > Global Statistics** screen.
2. In upper right of the screen, select the core that you want to view from the **Select a Core** pull-down menu.

Data Collection

To configure the data collection schedule:

1. Navigate to the **Monitor > Data Collection** screen.
2. Click the **Schedule Data Collection** button.
The **Data Collection Schedule** window displays.
3. (Optional) In the **Description** field, enter a description of the data collection schedule.
4. In **Select Cores**, click on the cores that you want to include in the data collection schedule.
5. Click **Next**.
6. In the **Date/Time Range** pull-down menu, select one of the following ranges:
 - a) **15 Minutes**
 - b) **30 Minutes**
 - c) **45 minutes**
 - d) **1 Hour**
7. Click **Next**.
8. In **Summary**, confirm your data collection schedule settings.
9. Click **Finish**.

Administration

Use the **Administration** screens to configure the following:

- [Administrative Settings](#)
- [User Accounts](#)
- [User Sessions](#)


Settings

This section contains the following topics:

- [TFTP Settings](#)
- [Syslog IP Addresses](#)
- [SNMP Configuration](#)
- [CLI Credentials](#)
- [Data Retention](#)
- [Client Settings](#)

TFTP Settings

Use the TFTP settings to specify to where to load the software images onto each switch in the distributed core from the TFTP site. Place the software images on the TFTP site so that the switches can install the appropriate FTOS software and configuration file. For more information on using the TFTP settings, see [Pre-Deployment Wizard – Step 3: Software Images DHCP Integration](#).

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

To configure TFTP settings:

1. Navigate to the **Administration > Settings** screen.
2. In the **TFTP** area, click the **Edit** button.
The **TFTP Settings** screen displays.
3. In the **TFTP Address** field, enter the TFTP address.
4. Click **OK**.

Syslog IP Addresses

You can specify up to 8 syslog server IP addresses to store your syslog messages.

Enter the syslog server IP ipv4 address that will collect the syslog messages from the switches in the distributed core:

1. Navigate to the **Administration > Settings** screen.
2. In the **Syslog IP Addresses** area, click **Edit**.
The **Syslog IP Address** screen displays.
3. In the **Sylog IP Addresses** fields, enter the IP address of the syslog server.
4. Click **OK**.

SNMP Configuration

Configure SNMP so that the DFM can perform SNMP queries on the switches in the distributed core. 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.

To configure SNMP:

1. Navigate to the **Administration > Settings** screen.
2. In the **SNMP Configuration** area, click **Edit**.
The **Configuration SNMP** window display:
3. In the **Read Community String** field, enter the read community string. For example, "public".
4. In the **Write Community String** field, enter the write community string. For example, "private".
5. In the **Port** field, enter the SNMP port number of the switches. The port number is typically 161.
6. In the **Trap Host** field, specify the IP address of the DFM Dell Fabric Manager
7. Click **OK**.

CLI Credentials

To provision the distributed core, enter the FTOS CLI user's credential and enable the configuration credential for all the switches in the distributed core. This option allows you to remotely make configuration changes to the switches in the distributed core.

To configure the CLI credentials and enable the configuration credential for all the switches in the distributed core:

1. Navigate to the **Administration > Settings** screen.
2. In the **CLI Credentials** area, click the **Edit** button.
The **CLI Credentials** screen displays.
3. In the **Protocol** pull-down menu, select one of the following options:
 - a) **Telnet**
 - b) **SSHv2**
 - c) **Telnet & SSHv2**
4. In the **User Name** field, enter the user name.
5. In the **Password** field, enter the password.
6. In the **Confirm Password** field, confirm the password.
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**.

Data Retention

To configure the amount of time to retain performance history:

1. Navigate to the **Administration > Settings** screen.
2. In the **Data Retention** area, click the **Edit** button.
3. In the **Performance History** area, enter the number of days you want to retain your performance history. The range is between 1 and 180 days.
4. In the **Daily Purge Execution Time** pull-down menu, specify the time to begin purging the performance history data.
5. Click **OK**.

Client Settings

To configure the maximum number of browser windows for each user's session and the polling interval from the DFM to the switches in the distributed core:

1. Navigate to the **Administration > Settings** screen
2. In the **Client Settings** area, click **Edit**.
The **Client Settings** window displays.
3. In the **GUI Polling Interval (in Seconds)** pull-down menu, select one of the following options. The default value is **60** seconds.
 - a) **15 Secs**
 - b) **30 Secs**
 - c) **60 Secs**
 - d) **120 Secs**
4. In the **Pop-out Client Session** pull-down menu, select the maximum number of browser windows (3 to 7) for each user's session. The default value is **3**.
5. Click **OK**.

Managing User Accounts

Use the **Administration > User Accounts** screen to view and manage user accounts.

- **User Accounts Summary View** – Displays a summary view of user accounts when the user's role is **Superuser**. When the role is a **user** or **administrator**, only the current logged in user's account information displays.
- **Add User** – Adds new user accounts. You can have up to 50 user accounts but only one **Superuser**.
- **Edit User** – Edits user accounts.
- **Change Password** – Allows a user to change his or her password.
- **Delete User** – Deletes one or more user accounts. The system default user, **Superuser**, cannot be deleted.
- **Unlock** – Unlocks a user who was locked out because he or she exceeded the maximum login attempts. To unlock a user, select the user and click the **Unlock** option.
- **Default User** – During the installation process, Dell Fabric Manager prompts you to create a **Superuser**.
- **Reset Default User (Superuser) Password** – Contact technical support if you need to reset the **Superuser** password.

- Password Rules – The DFM enforces special password rules for enhanced security. The password must be a minimum of 6 characters and contain one capital letter and one number. The password is masked when you enter it.
- Unsuccessful Login Limit – Specifies the unsuccessful login limit for a user’s account. When the unsuccessful login limit is exceeded, the lockout duration is applied.
- Lockout Duration – Specifies the amount of time a user is locked out when he or she exceeds the unsuccessful login limit.
- Sessions Allowed – Specifies the number of sessions a user is allowed.
- Session Timeout – Specifies the session timeout values.

The system comes with three predefined roles with the following permissions:

Superuser

- Views a summary of user accounts.
- Adds, deletes, and edits users.
- Locks and unlocks users.
- Resets passwords.
- Performs configuration changes.
- Sets session timeout values.
- Terminates DFM users’ sessions at the **Administration > User Session** screen.

Administrator

- Performs configuration changes.
- Views performance monitoring.
- Changes his or her own password.

User

- Views configuration and performance monitoring information.
- Changes his or her own password.

Adding a User

You must be a **Superuser** to add a user account. For more information on user accounts, see [Managing User Accounts](#).

To add a user:

1. Navigate to the **Administration > User Accounts** screen.
2. Click **Add User**.
The **Add User** screen displays.
3. In the **User Name** field, enter the user’s name.
Enter a unique name that is alphanumeric.
Length: 1 to 25 characters.
4. In the **Password** field, enter the user’s password.
The password must contain one capital letter and one number. The length must 6 to 25 characters.
5. In the **Confirm Password** field, enter the user’s password.

6. In the **First Name** field, enter the user's first name.
The first name can contain any characters.
Length: 1 to 50 characters.
7. (Optional) In the **Last Name** field, enter the user's last name.
The last name can contain any characters.
Length: 1 to 50 characters.
8. From the **Role** pull-down menu, select one of the following roles: **Admin** or **User**.
For information about roles, see [Managing User Accounts](#).
9. In the **Sessions Allowed** pull-down menu, specify the number sessions allowed for the user.
You can specify between 1 to 5 sessions. The default value is 5.
10. In the **Session Timeout** pull-down menu, specify one of the following timeout values. The default value is 15 minutes.
 - a) 15 minutes
 - b) 30 minutes
 - c) 45 minutes
 - d) 60 minutes
11. In the **Unsuccessful Login Limit** pull-down menu, select value from 3 to 10. The default value is 5.
12. In the **Lockout Duration** pull-down menu, select one of the following options. The default value is 30 minutes.
 - a) 15 minutes
 - b) 30 minutes
 - c) 45 minutes
 - d) 60 minutes
 - e) Permanent
13. Click **OK**.

Deleting a User

You must be a **Superuser** to add or delete users. For more information on user accounts, see [Managing User Accounts](#).

To delete a user:

1. Navigate to the **Administration > User Accounts** screen.
2. Select the user that you want to delete.
3. Click the **Delete** button.
4. Click **Yes**.

Editing a User

You must be a **Superuser** to edit a user. For more information on user accounts, see [Managing User Accounts](#).

To edit a user:

1. Navigate to the **Administration > Settings > User Accounts** screen and modify the following fields as needed.
2. Click on the user that you want to edit.
3. Click **Edit**.
The **Edit User** screen displays.
4. In the **Password** field, enter the user's password.

5. In the **Confirm Password** field, enter the user's password.
6. In the **First Name** field, enter the user's first name.
7. In the **Last Name**, enter the user's last name.
8. In the **Sessions Allowed** pull-down menu, specify the number sessions allowed for the user.
9. In the **Session Timeout** pull-down menu, specify one of the following timeout values:
 - a) **15 minutes**
 - b) **30 minutes**
 - c) **45 minutes**
 - d) **60 minutes**
10. Click **OK**.

Changing Your Password

To change your password:

1. Go to the upper right of the screen next to your login name.
A pull-down menu displays.
2. Select **Change Password**.
The **Change Current Account Password** screen displays.
3. In the **Current Password** field, enter your current password.
4. In the **New Password** field, enter your new password.
The password can be 6 to 25 characters long and must contain at least one number.
5. In the **Confirm Password** field, confirm your new password.
6. Click **OK**.
For more information on user accounts, see [Managing User Accounts](#).

Unlocking a User

You must be a **Superuser** to unlock a user. For information about user accounts, see [Managing User Accounts](#).

To unlock a user:

1. Navigate to the **Administration > Users Accounts** screen.
2. Select the user you want to unlock.
3. Click the **Unlock** button.
4. Click **OK**.

Managing User Sessions

Use the **User Sessions** screen to display active DFM users and terminate users' sessions. Only the **Superuser** can terminate a DFM user's session. For more information on user accounts, see [Managing User Accounts](#).

This screen displays the following information:

- **Username**
- **Session Login Time**
- **Client IP Address**

- **Current Session**

To terminate DFM users' sessions:

1. Navigate to the **Administration > User Sessions** screen.
2. Select the users that you want to log off.
3. Click the **Force Logoff** button.
4. Click **OK**.