Dell Blade I/O Manager
Version 1.0

2015 - 07

Rev. A00

Contents

1

About Dell Blade I/O Manager

You can use Dell Blade I/O Manager to manage the configuration and monitoring of the following I/O Aggregator devices:

- MIOA for M1000e chassis
- FN IOA for FX2 chassis

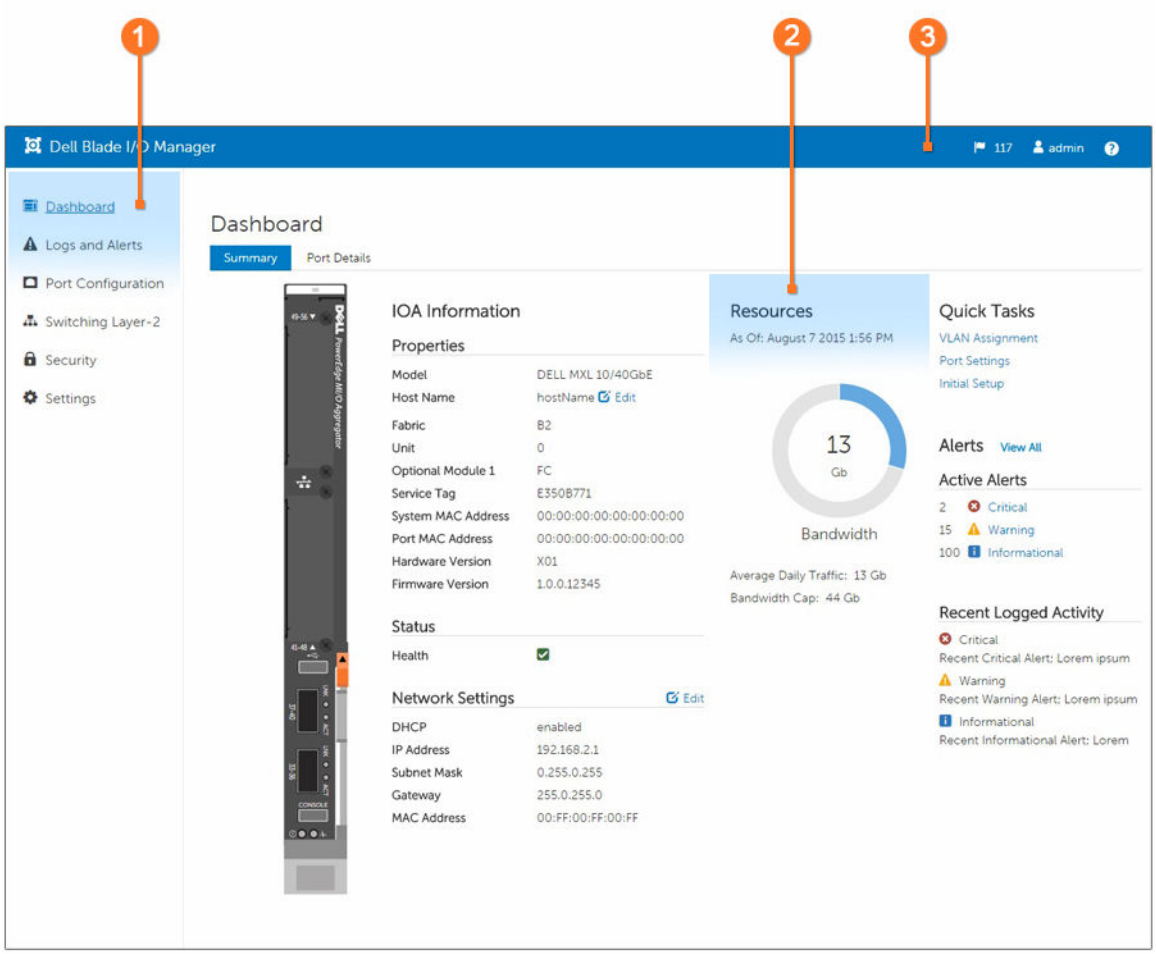

Figure 1. Dell Blade I/O Manager User Interface

1. Navigation Menu
2. Page

3. Toolbar

The Dell Blade I/O Manager user interface consists of the following elements:

- **Toolbar** — From this area, you can log out from Dell Blade I/O Manager, view the number of alerts, reboot the I/O Aggregator device, and open online help.
- **Navigation menu** — From this area, you can navigate to the pages in Dell Blade I/O Manager: **Dashboard**, **Logs and Alerts**, **Port Configuration**, **Switching Layer-2**, **Security**, and **Settings**.
- **Pages** — The main area where information appears and you can configure settings.

Logging In

You can log in to Dell Blade I/O Manager from Chassis Management Controller (CMC).
You can view Dell Blade I/O Manager in one of the following web browsers:

- Apple Safari
- Google Chrome
- Microsoft Internet Explorer 9 or later

NOTE: If you upgrade Dell Blade I/O Manager, clear the browser memory cache before opening the new version in the browser.

1. Open CMC for the managed I/O Aggregator device.
2. In the navigation menu, under I/O Module Overview, select the slot containing the I/O Aggregator device.
3. On the page that appears, click **Launch I/O Module GUI**.
   Dell I/O Blade Manager appears.
4. Make the appropriate entries in the **User name** and **Password** fields.
5. Click **Log in**.

Logging Out

You can log out of the Dell Blade I/O Manager from the toolbar.

1. From the toolbar, click your user name.
2. From the drop-down menu, select **Logout**.

Initial Setup Wizard

The Initial Setup Wizard guides you through initial I/O Aggregator device configuration so that you can get the device running quickly.
The Initial Setup Wizard appears upon your first login. You can also open it from the Quick Tasks section of the **Dashboard** page.

Before you begin, gather the following information from your device:

- IOA Mode
- IP address and subnet mask

- (optional) Root user password and enable password
- (optional) SNMP credentials

The wizard has the following steps:

- Mode Settings
- Combo Port Settings
- Network Settings
- Credentials
- SNMP Settings
- Uplink Failure Detection
- Network Time Protocol
- Summary

To begin configuration using the wizard, click **Next** to configure Mode Settings.

Configuring Mode Settings

On the Mode Settings of the Initial Setup Wizard, you select an I/O Aggregator device operational mode.

1. If not already done, from the Welcome screen, click **Next**.

   The Mode Settings screen appears.
2. Select one of the following modes:
   - **Standalone Mode (default)** — Default mode of the I/O Aggregator device. In this mode, all ports are configured as members of all VLANs. All VLANs are up and can send or receive Layer 2 traffic.
   - **Stack Mode** — Multiple switches operate as single unit. A single switch in the stack (Master switch) manages all units in the stack and uses a single IP address that you can use to manage every port in the stack.
   - **VLT Mode** — Virtual Link Trunking. VLT enables physical links between two chassis to appear as a single virtual link to the network core or other switches such as Edge, Access or ToR. VLT reduces the role of Spanning Tree protocols by allowing LAG terminations on two separate distribution or core switches, and by supporting a loop free topology. VLT institutes Layer 2 multipathing, creating redundancy through increased bandwidth, enabling multiple parallel paths between nodes and load-balancing traffic where alternative paths exist.
   - **Programmable MUX Mode** — Programmable multiplex mode. This mode provides flexibility of operation with added configurability. This mode creates multiple LAGs, configuring VLANs on uplinks and the server side, and configuring data center bridging (DCB) parameters. Programmable MUX mode supports both stacking and VLT operations.
   - **Full-switch Mode** — All commands and configurations supported on MXL available in this mode. This mode offers Layer 2/Layer 3 switching functionalities on the Dell FX2 chassis.

     NOTE: This mode is only available for FN IOA for FX2 chassis devices.

   (Standalone, Stack, and VLT Modes for MIOA for M1000e chassis devices only). You can also select **Enable Quadport** to configure solitary QSFP+ 40 G ports into four 10 G ports.
3. (Stack Mode only) In the Stacking Unit area, from the **Unit** drop-down menu, select a unit from 0–5.

   NOTE: This number is the factory-assigned unit number, not a priority number.
4. Click **Next**. The next wizard screen depends on the device and device mode:
   - For FN2210S SKU FN IOA for FX2 chassis devices in all modes except programmable multiplex, proceed to the Combo Port screen.

- For MIOA for M1000e chassis devices, FN410S SKU and FN410T SKU FN IOA for FX2 chassis devices in programmable multiplex mode, or FN MXL devices screen proceed to the Network Settings screen.

Configuring Combo Port Settings (Initial Setup Wizard)

On the Combo Port Settings screen of the Initial Setup Wizard, you can configure ports 9 and 10 in FN2210S SKU FN IOA for FX2 chassis devices to work either as Ethernet ports or Fibre Channel ports. Ethernet ports handle common traffic. Fibre Channel ports connect to a Storage Area Network (SAN).

NOTE: This screen does not apply for MIOA for M1000e chassis devices, FN410S SKU and FN410T SKU FN IOA for FX2 chassis devices in Programmable Multiplex mode, or FN MXL devices.

1. If not already done, from the Mode Settings screen, click **Next**.
   The Combo Port Settings screen appears.
2. Make one of the following selections:
   - **Ethernet**
   - **Fibre Channel**
3. Click **Next** and proceed to the Network Settings screen.

Configuring Network Settings

On the Mode Settings screen of the Initial Setup Wizard, you configure the IP address of the Management Interface in the I/O Aggregator module.
Make sure that the configured IP address is in the same subnet as the management device.

1. If not already done, from the Mode Settings screen, click **Next**.
   The Network Settings screen appears.
2. In the **IP Address Source** field, select **Static IP** or **Dynamic IP**.
   The **IP Version**, **IP Address**, **Subnet Mask**, and **Gateway** settings appear by default.
3. Click **Next** and proceed to the Credentials screen.

Configuring Credentials

On the Credentials screen of the Initial Setup Wizard, you configure the user name and password to log on to the switch interface.

1. If not already done, from the Network Settings screen, click **Next**.
   The Credentials screen appears.
2. In the **User Name** field, enter a user name. The minimum user name length is one alphanumeric character and the maximum user name length is 63 alphanumeric characters.
3. In the **Password** and **Re-enter Password** fields, enter the password. The minimum password length is one alphanumeric character and the maximum password length is 32 alphanumeric characters.
4. In the **Enable Password** and **Re-enter Password** fields, enter the password to enter the Enable mode on the switch. The minimum password length is one alphanumeric character and the maximum password length is 32 alphanumeric characters.
5. Click **Next** and proceed to the SNMP Settings screen.

Configuring SNMP Settings

On the SNMP Settings screen of the Initial Setup Wizard, you can configure Simple Network Management Protocol (SNMP) for network management and monitoring.

1. If not already done, from the Credentials screen, click **Next**.

   The SNMP Settings screen appears.
2. In the **SNMP Mode** field, select **Enabled** to configure SNMP.
3. In the **SNMP Community String** field, enter the string that grants access to the statistics of the switch.
4. Click **Next**. The next wizard screen depends on the device mode:
   - For Programmable Multiplex mode and FN MXL devices, proceed to the Summary screen.
   - For all other device modes, proceed to the Uplink Failure Detection screen.

Configuring Uplink Failure Detection

On the Uplink Failure Detection screen of the Initial Setup Wizard, you can configure Uplink Failure Detection (UFD). UFD provides detection of the loss of upstream connectivity. If there is a link failure, the I/O Aggregator device disables downlink interfaces.

NOTE: This screen does not apply for devices in Programmable Multiplex mode or FN MXL devices.

1. If not already done, from the SNMP Settings screen, click **Next**.

   The Uplink Failure Detection (UFD) screen appears.
2. To configure uplink failure detection, select **Enabled** or select **Disabled** to disable it.
3. If you select **Enabled**, configure a timer setting that prevents unwanted flapping of downstream ports when the uplink port channel goes down and comes up. The configured value in seconds is how long the device waits for the upstream port channel (LAG 128) to come back up before it disables the server ports. Select one of the following:
   - **Default Defer Timer (10 sec)**

     NOTE: If you select this setting, if the uplink goes down, the device disables the downlink within 10 seconds.
   - **Custom Defer Timer** (enter a setting in seconds from 0 to 100)
4. Click **Next** and proceed to the Network Time Protocol screen.

Configuring Network Time Protocol

On the Network Time Protocol screen of the Initial Setup Wizard, you can configure an NTP time-serving host to synchronize with the switch. With NTP, the switch can act only as a client to an NTP clock host.

NOTE: This screen does not apply for devices in Programmable Multiplex mode or FN MXL devices.

1. If not already done, from the Uplink Failure Detection screen, click **Next**.

   The NTP screen appears.
2. From the **Time Zone** drop-down menu, select the time zone
3. Select **Enable NTP Server**.
4. In the **Preferred NTP Server IP Address or URL** field, enter the host name or IP address of the primary NTP server.
5. In the **Secondary NTP Server IP Address or URL (optional)** field, enter the host name or IP address of a secondary or backup NTP server.

NOTE: Dell Blade I/O Manager only supports IPv4 management address notation.

6. Click **Next** and proceed to the Summary screen.

Viewing the Summary

The Summary screen is the final step of the Initial Setup Wizard.
This screen summarizes your configuration settings for the IOA device. From this screen, you can save the configuration settings to the start-up configuration file.

1. If not already done, from the Network Time Protocol screen, click **Next**.
2. Review these settings.
3. To edit settings, click the **Back** button to navigate to the appropriate screen.
4. If the settings are correct, click **Apply**.
   The I/O Aggregator device reboots to apply the settings.

2

Dashboard

You can quickly view a summary of all key details of your I/O Aggregator device on the **Dashboard** page.

The **Dashboard** page can consist of the following tabs:

- Summary
- Port Details
- Stack Summary
- Stack Port Summary
- VLT Summary

NOTE: The appearance of the Dashboard can vary depending on the type of managed I/O Aggregator device.

Summary

The **Summary** tab of the **Dashboard** page displays properties, network settings, bandwidth usage, shortcut links to common tasks, and alerts for the I/O Aggregator device.

This tab has the following sections:

- IOA Information
- Resources
- Quick Tasks
- Alerts

Device Image

The device image is a graphic representation of the I/O Aggregator device that Dell Blade I/O Manager manages.

You can hover your mouse over the ports in the graphic to display the following information about external ports:

- **Port** — Port number or port range for QSFP+ 40 G ports configured for quad-port.

  NOTE: External port numbers do not begin with 1; which is reserved for internal ports.
- **Link Status** — State of the link: **Up** or **Down**.
- **Speed** — Port speed.
- **Administrative State** — If enabled, the port can link to another port.
- **VLANs** — VLAN to which the port is assigned.
- **LAG** — Link Aggregation Group to which the port is assigned.

NOTE: QSFP+ 40 G ports configured for quad-port into four 10 G ports display information for all four ports.

IOA Information

The IOA Information section of the **Dashboard** page displays information about the managed I/O Aggregator device in three subsections:

- **Properties**
- **Status**
- **Settings**

The **Properties** subsection lists the following information about the managed I/O Aggregator device:

- **Model** — The I/O Aggregator device type: MIOA (for Dell I/O Aggregator M1000e chassis) or FN IOA (for Dell PowerEdge IOM FX2 chassis).
- **Active IOA Mode** — Current mode of the IOA device:
  - **Standalone Mode (default)** — Single device. This mode is the default setting.
  - **Stack Mode** — Multiple switches operate as single unit. A single switch in the stack (Master switch) manages all units in the stack and uses a single IP address that you can use to manage every port in the stack.
  - **VLT Mode** — Virtual Link Trunking. VLT enables physical links between two chassis to appear as a single virtual link to the network core or other switches such as Edge, Access, or ToR. VLT reduces the role of Spanning Tree protocols by allowing LAG terminations on two separate distribution or core switches, and by supporting a loop free topology. VLT institutes Layer 2 multipathing, creating redundancy through increased bandwidth, enabling multiple parallel paths between nodes and load-balancing traffic where alternative paths exist.
  - **Programmable MUX Mode** — Programmable Multiplex mode. This mode provides flexibility of operation with added configurability. This mode creates multiple LAGs, configuring VLANs on uplinks and the server side, and configuring data center bridging (DCB) parameters. Programmable MUX mode supports both stacking and VLT operations. You can make any configuration or provisioning of the device through the CLI.
  - **Full Switch** — Applicable only for FN IOA for FX2 chassis. Supports layer 2 and layer 3 routing. You can make any configuration or provisioning of the device through the CLI.
- **IOA Mode After Reboot** — The IOA mode for the device after a reboot.
- **Host Name**
- **Fabric** — The slot in the chassis: A1, A2, B1, B2, C1, or C2.

  NOTE: Slots B1, B2, C1, and C2 apply only to MIOA.
- **Unit** — The device value assigned at factory: 0 to 5.

  NOTE: If you stack I/O Aggregator devices, two units cannot both have the unit value of 0. The system reassigns one device with a unit value of 0 to 1.
- **Optional Module 1** — m1000e chassis only. Module 1 contains ports 49–56.
- **Optional Module 2** — m1000e chassis only. Module 2 contains ports 41–48.
- **Service Tag** — The identifier used when contacting Dell Customer Support.
- **System MAC Address** — The MAC address of the entire I/O Aggregator device.
- **Port MAC Address** — The MAC address for the I/O Aggregator interfaces.
- **Hardware Version** — The I/O Aggregator device version.
- **Firmware Version** — The I/O Aggregator firmware version.

The **Status** subsection displays the device health.

The **Network Settings** subsection displays out-of-band management settings about the managed I/O Aggregator device:

- **DHCP Enabled** — **Enabled** or **Disabled**
- **IP Address**
- **Subnet Mask**
- **Gateway**
- **MAC Address**

Editing the Active IOA Mode

From the **Dashboard** page you can edit the operational mode of the I/O Aggregator device.

1. From the navigation menu, select **Dashboard**.
   The **Dashboard** page appears.
2. In the IOA Information Properties section, select **Edit** in the **Active IOA Mode** field.
   The **Mode Settings** dialog box appears.
3. In the IOA Operational Mode section, select the new mode:
   - **Standalone Mode (default)** — Default mode of the I/O Aggregator device. In this mode, all ports are configured as members of all VLANs. All VLANs are up and can send or receive Layer 2 traffic.
   - **Stack Mode** — Multiple switches operate as single unit. A single switch in the stack (Master switch) manages all units in the stack and uses a single IP address that you can use to manage every port in the stack.
   - **VLT Mode** — Virtual Link Trunking. VLT enables physical links between two chassis to appear as a single virtual link to the network core or other switches such as Edge, Access or ToR. VLT reduces the role of Spanning Tree protocols by allowing LAG terminations on two separate distribution or core switches, and by supporting a loop free topology. VLT institutes Layer 2 multipathing, creating redundancy through increased bandwidth, enabling multiple parallel paths between nodes and load-balancing traffic where alternative paths exist.
   - **Programmable MUX Mode** — Programmable Multiplex mode. This mode provides flexibility of operation with added configurability. This mode creates multiple LAGs, configuring VLANs on uplinks and the server side, and configuring data center bridging (DCB) parameters. Programmable MUX mode supports both stacking and VLT operations. You can make any configuration or provisioning of the device through the CLI.
   - **Full Switch** — All commands and configurations supported on MXL available in this mode. This mode offers Layer 2/Layer 3 switching functionalities on the Dell FX2 chassis.

     NOTE: This mode is only available for FN IOA for FX2 chassis devices.
4. (Standalone, Stack, and VLT Modes for MIOA for M1000e chassis devices only) In the Quadport Mode section, select **Enable Quadport** to configure solitary QSFP+ 40 G ports into four 10 G ports.
5. (Stack mode only) In the Stacking Unit area, from the **Unit** drop-down menu, select a unit from 0–5.
6. Click **Apply**.
7. Reboot the I/O Aggregator device.

   NOTE: After you reboot the I/O Aggregator device, the selected active IOA mode might not remain the one previously selected.

Editing the Host Name

In the **Summary** tab of the **Dashboard** page, you can edit the host name of the I/O Aggregator device.

1. From the navigation menu, click **Dashboard**.
2. In the Properties section of the **Summary** tab, click **Edit** next to the **Host Name** field.

The **Host Name** dialog box appears.

3. In the **Host Name** field, enter a new host name for the device. The new host name must have a minimum of one character and a maximum of 32.
4. Click **Apply**.

Editing Network Settings

You can configure the IP address of the management interface in the IOA module from the **Summary** tab on the **Dashboard** page.
Make sure that the configured IP address is in the same subnet as the management device.

1. From the navigation menu, click **Dashboard**.
2. In the Network Settings section of the **Summary** tab, click **Edit**.

   The **Network Settings** dialog box appears.
3. In the **IP Address Source** field select what type of IP address the management interface has: **Static IP** or **Dynamic IP**.

   IP Version and **VLAN ID** settings appear by default.
4. (Static IP only) In the **IP Address** field, enter the IP address of the management interface. Dell Blade I/O Manager only supports IPv4 addresses.
5. (Static IP only) In the **Subnet Mask** field, enter the subnet mask of the management interface.
6. (Static IP only) In the **Gateway** field, enter the gateway IP address for the management interface.
7. Click **Apply**.
8. Reboot the I/O Aggregator device.

NOTE: The Dell Blade I/O Manager user interface might be unreachable after changing network settings. To refresh Dell Blade I/O Manager, close your web browser and start a new browsing session.

Resources

The Resources section of the **Dashboard** page displays bandwidth information for the uplink ports of the I/O Aggregator device.

This section displays:

- **Bandwidth graph** — Circle graph displaying the average daily bandwidth usage on the device.
- **Average Daily Traffic** — Average bandwidth of traffic traversing the uplink ports in the last 24 hours.
- **Bandwidth Cap** — Total bandwidth capacity of all uplink ports on the device.

Quick Tasks

The Quick Tasks section of the **Dashboard** page lists links to commonly used tasks in the Dell Blade I/O Manager:

- VLAN Assignment

  NOTE: This link is not available for I/O Aggregator devices in programmable multiplex mode or FN MXL devices.
- Port Assignments
- Initial Setup

Alerts

The Alerts section of the **Dashboard** page displays alerts from the I/O Aggregator device. Dell Blade I/O Manager polls the device every 60 seconds for new alerts.

This section has two subsections:

- **Active Alerts** — Lists total alerts by category: Critical, Warning, Informational
- **Recently Logged Activity** — Lists the three most recent alerts.

You can click **View All** to go to the **Logs and Alerts** page for more details on alerts.

Port Details

The **Port Details** tab of the **Dashboard** page displays the following details about each port on the I/O Aggregator device:

- **Port** — Port number.
- **Link Status** — Status of the link: **Up** or **Down**.
- **Link Speed** — Link speed of the port when it is up in M or G.
- **Administrative State** — Displays **Enabled** or **Disabled**. The port can only link up if connected to another enabled port.
- **VLANs** — Displays the VLAN number to which the port belongs.
- **LAG** — Link Aggregation Group number to which the port is configured to be part.

  NOTE: To view the actual LAG status of a port, go to the Link Aggregation (LAG) section of the **Switching Layer-2** page.

To filter the list by internal or external ports only, make the appropriate selection from the **Filter By** menu.

Stack Summary

For I/O Aggregator devices in stack mode, the **Stack Summary** tab displays details about all devices in the stack and their interface details.

This tab has two sections: Stack Information and Stacked Ports.

The Stack Information section displays the following information:

- **Unit** — The stack unit number: 0 to 5.
- **Unit Type** — The stack unit type: **Master**, **Standby**, or **Member**.
- **Status** — The state of the stack unit.
- **Required Type** — The type of I/O Aggregator device.
- **Firmware Version** — Version of Operating System on stack unit.
- **Number of IOA Ports** — You can click **View Details** to jump to the Stack Port Summary tab.

The Stacked Ports section displays the following information:

- **Topology** — Topology of connected stack ports: ring, daisy chain, or standalone.
- **Interface** — Port ID of connected stack port on this unit.
- **Connection** — Port ID of other unit's stack port to which this one connects.

- **Link Speed** — Link speed of this stack port: 10 or 40 Gb/s.
- **Administrative State** — **Enabled** or **Disabled**. If enabled, the port can link to another port
- **Link Status** — Operational status of the stack port: **Up** or **Down**.

Stack Port Summary

For I/O Aggregator devices in stack mode, the **Stack Port Summary** tab displays details about the ports and their status present in each stack unit.

This tab displays the following information:

- **Port** — Stacking port. There can be a maximum of 32 internal ports and 24 external ports displayed.
- **Link Status** — Status of port: **Up** or **Down**.
- **Link Speed** — Link speed of this stack port.
- **Administrative State** — Displays **Enabled** or **Disabled**. If enabled, the port can link to another port.
- **VLANs** — VLANs to which the port is a member.
- **LAG** — Link Aggregation Group number to which the port is configured to be part.

  NOTE: To view the actual LAG status of a port, go to the Link Aggregation (LAG) section of the **Switching Layer-2** page.

From the **Filter By** drop-down menus you can filter these details in the following ways:

- (First menu) **Stack unit** number and role
- (Second menu) **All** ports
- (Second menu) **Internal Ports** only
- (Second menu) **External Ports** only

VLT Summary

For I/O Aggregator devices in VLT mode, the **VLT Summary** tab displays details about the VLT role of that unit. This tab displays the following information:

- General information about VLT domains currently configured on the switch.
- Detailed information about the VLT-domain configuration, including local and peer port-channel IDs, local VLT switch status, and number of active VLANs on each port channel.
- VLT peer status, role of the local VLT switch, VLT system MAC address and system priority, and the MAC address and priority of the locally attached VLT device.
- Current configuration of all VLT domains or a specified group on the switch.
- Statistics of VLT operation.

3

Logs and Alerts

Dell Blade I/O Manager polls the I/O Aggregator device in 60–second intervals for new log entries and alerts. The **Logs and Alerts** page displays all log entries and alerts from the I/O Aggregator device.

This page lists log entries and alerts in table format with the following columns:

- **Severity**: **Informational**, **Warning**, or **Critical**.
- **Date and Time**: Date and time stamp of when the device recorded the log entry or alert.
- **Description**: Description of the log entry.

You can perform the following actions on this page:

- Click **Refresh**, if you want to display log entries and alerts from the device before the next polling period.
- From the **Filter By** menu, you can filter the log entries and alerts by severity type.

Editing Alert Settings

Alerts in Dell Blade I/O Manager reside in RAM. You can configure the number of alerts listed in Dell Blade I/O Manager.
After the configured limit is reached, a new alert replaces the oldest alert displayed on the **Logs and Alerts** page.

1. From the navigation menu, click **Logs and Alerts**.
2. Click **Settings**.

   The **Settings** dialog box appears.
3. In the **Maximum Logs** field, enter a number from 20 to 1000 of the maximum logs you want the Dell Blade I/O Manager to display at one time.
4. Click **Apply**.

4

Port Configuration

The **Port Configuration** page is where you can configure various port settings on an I/O Aggregator device.

This page consists of the following sections:

- Port Settings
- Uplink Ports
- Uplink Failure Detection
- Combo Port (FN2210S SKU FN IOA for FX2 devices only)

Port Settings

The Port Settings section of the **Port Configuration** page displays in circular graph format the number of configured external and internal ports of the I/O Aggregator device.

NOTE: You can only edit these settings for M1000e and FN IOA devices in standalone or VLT mode.

In the circular graphs, blue represents configured ports.

From this section you can:

- View port configurations
- Configure port settings

Viewing Current Port Configurations

From the Port Settings section of the **Port Configuration** page, you can view all current port configuration settings on the I/O Aggregator device.
M1000e devices have a maximum of 32 internal ports and 24 external ports. FX2 devices have a maximum of eight internal ports and four external ports.

NOTE: You can only edit these settings for M1000e and FN IOA devices in standalone or VLT mode.

1. From the navigation menu, click **Port Configuration**.
   The **Port Configuration** page appears.
2. In the Port Settings section, click **View Port Configurations**.
   The **Current Port Configurations** dialog box appears, listing the following information for each configured port:
   - **Interface** — Displays the interface type with chassis slot and port number.
   - **Description** — Displays the user-configured description of the port.
   - **Port Type** — Displays the port type: **Internal**, **Copper**, **Fibre**, **QSFP**, or **SFP+**.
   - **Link Status** — Displays whether the port link is **Up** or **Down**.

- **Auto Negotiation** — Displays whether auto-negotiation is **Enabled** or **Disabled** on the interface. Autonegotiation allows two devices at either end of a 10 Mbps, 100 Mbps, or 1000 Mbps link to advertise and negotiate the link operational mode — such as the speed of the link and the duplex configuration of half or full duplex — to the highest common denominator.
- **Speed** — Displays the speed of the port.
- **MTU** — Displays the Maximum Transmission Unit (MTU) (frame size) for an Ethernet interface. This setting is the limit for the largest packet that can be passed through the interface.
- **Remote Fault Signaling** — (If applicable) Displays whether the remote fault signaling feature is **Enabled** or **Disabled**. This feature brings the interface up or down when a Remote Fault Indication (RFI) error is detected.
- **Auto LAG** — (If applicable) Displays whether the Auto LAG feature is **Enabled** or **Disabled**. This feature has the device automatically assign internal ports to Link Aggregation Groups.
- **Keep Alive** — Displays whether the keep alive feature is **Enabled**, **Disabled**, or blank (not applicable). This feature periodically transmits keepalive packets to keep an interface alive when not transmitting data.

You can also filter this list from the **Filter By** menu and select **All Ports**, **Internal Ports**, or **External Ports**.

3. To close the **Current Port Configurations** dialog box, click **Close**.

Enter an example that illustrates the current task (optional).
Enter the tasks the user should do after finishing this task (optional).

Configuring Port Settings

From the Port Settings section of the **Port Configuration** page, you can configure port settings on the I/O Aggregator device.

NOTE: You can only configure these settings for M1000e and FN IOA devices in standalone or VLT mode.

Tip: You can click **View Port Configurations** to view all currently configured port settings.

1. From the navigation menu, click **Port Configuration**.
   The **Port Configuration** page appears.
2. From the **Interface** drop-down menu, you can select one of the following filters:
   - **All Ports**
   - **Internal Ports**
   - **External Ports**
   - **Custom Range**
   - **Individual port number**
3. If you select **Custom Range** in step 2, in the **Port Range** field, enter the ports in the range. Separate individual ports with a comma. You can use a dash to denote a range. For example: 1,2,6–8.
   The **Interface(s) Selected** field displays the selected interface types with chassis slot and port number
4. In the **Interface Description** field, enter a description of the interface. The maximum description length is 240 alphanumeric characters.
5. In the **Administrative State** field, select **Enabled** or **Disabled**. If enabled, the port can link to another port.
6. In the **Auto Negotiation** field, select **Enabled** or **Disabled**. Autonegotiation allows two devices at either end of a 10 Mbps, 100 Mbps, or 1000 Mbps link to advertise and negotiate the link operational mode — such as the speed of the link and the duplex configuration of half or full duplex — to the highest common denominator. If you select **Enabled**, skip to step 8.

NOTE: Autonegotiation is not available for QSFP+ ports.

7. From the **Speed** drop-down menu, select the port speed.

   NOTE: This setting is not available if you enabled autonegotiation.

   The **MTU (bytes)** field displays the Maximum Transmission Unit setting for the Ethernet interface in bytes from 594 to 12000. This setting is the limit for the largest packet that can be passed through the interface.

   NOTE: This setting is not available for fibre channel ports.

8. In the **Remote Fault Signaling** field, select **Enabled** or **Disabled**.
9. In the **Keep Alive** field, select **Enabled** or **Disabled**.
10. Click **Apply**.

Uplink Ports

The Uplink Ports section of the **Port Configuration** page is where you can enable or disable quadport mode. This mode has I/O Aggregator ports a 1x40GE port operate as 4x10GE ports.

NOTE: You can only view these settings for M1000e devices in standalone or VLT mode.

This section displays whether quad-port mode is enabled or disabled. It also displays a graphic representation of the ports on the device.

Configuring Uplink Ports

You can configure quad-port mode on certain I/O Aggregator devices so that a 1x40GE port operates as 4x10GE ports.

NOTE: You can only configure these settings for M1000e devices in standalone or VLT mode.

1. From the navigation menu, click **Port Configuration**.
   The **Port Configuration** page appears.
2. In the Uplink Ports section, click **Edit**.
   The **Uplink Ports** dialog box appears.
3. To enable the feature, select **Quadport Mode**, to disable it, clear this setting.
4. Click **Apply**.
   Changing uplink port settings requires a reboot of the device. The **Confirm** dialog box appears.
5. Click **Confirm**.

Uplink Failure Detection

Uplink Failure Detection (UFD) provides detection of the loss of upstream connectivity. If there is a link failure, the I/O Aggregator device disables downlink interfaces. The Uplink Failure Detection (UFD) section of the **Port Configuration** page displays whether this feature is enabled for the I/O Aggregator device.

If UFD is enabled, the page also displays the **Defer Timer** setting in seconds. This setting prevents unwanted flapping of downstream ports when the uplink port channel goes down and comes up. The configured value in seconds is how long the device waits for the upstream port channel (LAG 128) to come back up before it disables the server ports.

NOTE: You can only edit these settings for M1000e and FN IOA devices in standalone or VLT mode.

Configuring Uplink Failure Detection (Port Configuration Page)

Uplink Failure Detection (UFD) provides detection of the loss of upstream connectivity. If there is a link failure, the I/O Aggregator device disables downlink interfaces.

NOTE: You can only configure these settings for M1000e and FN IOA devices in standalone or VLT mode.

You can configure this feature the Initial Setup Wizard. But if you need to change its configuration afterwards, you can enable or disable UFD from the **Port Configuration** page.

1. From the navigation menu, click **Port Configuration**.
2. In the Uplink Failure Detection (UFD) section, click **Edit**.

   The **Uplink Failure Detection** dialog box appears.
3. To configure uplink failure detection, select **Enabled** or select **Disabled** to disable it.
4. If you select **Enabled**, configure a timer setting that prevents unwanted flapping of downstream ports when the uplink port channel goes down and comes up. The configured value in seconds is how long the device waits for the upstream port channel (LAG 128) to come back up before it disables the server ports. Select one of the following:
   - **Default Defer Timer (10 sec)**

     NOTE: If you select this setting, if the uplink goes down, the device disables the downlink within 10 seconds.
   - **Custom Defer Timer** (enter a setting in seconds from 0 to 100)
5. Click **Apply**.

Combo Port

Ports 9 and 10 in FN2210S SKU FN IOA for FX2 chassis devices can work either as Ethernet ports or Fibre Channel ports. Ethernet ports handle common traffic. Fibre Channel ports connect to a Storage Area Network (SAN).

NOTE: You can only edit these settings for FN IOA devices in standalone or VLT mode.

Configuring Combo Port Settings (Port Configuration Page)

For FN IOA for FX2 chassis devices (except when in Programmable Multiplex or Full Switch mode), you can configure ports 9 and 10 to work as Ethernet ports or Fibre Channel ports.

NOTE: You can only configure these settings for FN IOA devices in standalone or VLT mode.

You can configure this feature the Initial Setup Wizard. But if you need to change its configuration afterwards, you can do so from the **Port Configuration** page.

1. From the navigation menu, click **Port Configuration**.
2. In the Combo Port section, click **Edit**.

   The **Combo Port Settings** dialog box appears.
3. In the **Port Type** field, make one of the following selections:
   - **Ethernet**
   - **Fibre Channel**
4. Click **Apply**.

Changing the Combo Port setting requires a reboot of the I/O Aggregator device. A confirmation dialog box appears.

5. On the toolbar, click the user name and name select **Reboot IOA** from the drop-down menu.

5

Switching Layer-2

The **Switching Layer-2** page of Dell I/O Blade Manager is where you can configure the following layer 2 networking settings for an I/O Aggregator device:

- VLAN Assignment
- Link Aggregation (LAG)
- IGMP
- Port Mirroring
- Fibre Channel
- iSCSI
- DCB

VLAN Assignment

In the VLAN Assignment section of the Switching Layer-2 page, you can configure Virtual LANs (VLANs) for the I/O Aggregator device.

You can configure VLANs to separate users into individual network segments for security and other reasons. You can associate selected ports on a switch with selected VLAN and treat these ports as a separate switch.

This section displays a graphic representation of the ports on the device. You can click a port to display the interface name to which tagged or untagged VLANs to which it is assigned.

From this section to you can:

- View VLAN Port Assignments
- Assign Ports to a VLAN

Viewing Current VLAN Assignments

From the VLAN Assignment section of the **Switching Layer-2** page, you can view VLAN assignments for the I/O Aggregator device.

1. From the navigation menu, click **Switching Layer-2**.
   The **Switching Layer-2** page appears.
2. In the VLAN Assignment section, click **View VLAN Assignments**.
   The **VLAN Port Assignment** dialog box appears displaying the following information for each assignment:
   - **Interface** — Interface type with chassis slot and port number.

- **Mode** — VLAN assignment mode for I/O Aggregator device: **Auto** (port automatically added as untagged to the default VLAN and tagged to the remainder of the VLANs) or **Admin** (manually configured as to tagged or untagged to VLANs).
- **Tagged** — Numbers of tagged VLANs to which the port belongs
- **Untagged** — Numbers of untagged VLANs to which the port belongs
- **Port Channel** — Number of the Link Aggregation Group (LAG) to which the port belongs.

3. You can filter this list by making a selection from the **Filter By** menu: **Internal Ports** or **Uplink LAG Po 128**.
4. To close the **VLAN Port Assignment** dialog box, click **Close**.

Assigning Ports to a VLAN

From the VLAN Assignment section of the Switching Layer-2 page, you can view VLAN port assignments for the I/O Aggregator device.

1. From the navigation menu, click **Switching Layer-2**.

   The **Switching Layer-2** page appears.
2. In the VLAN Assignment section, click **Edit**.

   The **VLAN Port Assignment** dialog box appears.

   NOTE: You can click **View Current VLAN Port Assignments** to view existing VLAN port assignments.
3. In the **Server Slots** area, select the ports you want to configure.
4. In the **Edit VLANs** area, select one of the following tasks:
   - **Add VLANs** — Select to add ports to VLANs you specify in steps 5 or 6.
   - **Remove VLANs** — Select to remove ports from VLANs you specify in steps 5 or 6.
   - **Load Defaults (Auto VLAN)** — Select to load default switch VLAN assignments.
   - **Overwrite VLAN Assignments** — Select to have existing VLAN configurations are removed and overwritten with a new set of configurations to selected ports.
5. In the **Tagged VLANs** box, enter the tagged VLAN numbers or range of VLAN numbers to which the selected ports belong. You can enter a range of VLAN numbers from 1–4094. You can also enter individual VLAN numbers and a range, for example: 5, 8, 10–20.
6. In the **Untagged VLANs** box, enter the untagged VLAN number to which the selected ports belong.
7. Click **Apply**.

   A progress dialog box might appear. The **Status** dialog box then appears displaying the results of the port assignments. You can click **Configure Another Port** to return to the **VLAN Port Assignment** dialog box and configure more VLAN port assignments or click **Close** to return to the **Switching Layer-2** page.

Link Aggregation (LAG)

You can view and configure details for Link Aggregation Groups (LAGs) on the Link Aggregation (LAG) section of the **Switching Layer-2** page.

In standalone, and VLT modes, all uplink ports (except port 9 in VLT mode of FN IOA and except ports 33 and 37 in VLT mode of MIOA) are configured in a single LAG (LAG 128). For FN IOA, there can be multiple uplink LAGs in Programmable Multiplex mode and Full-switch mode.

This section displays the following two subsections:

- **External Ports** — The status of each LAG: **Up** or **Down**. Also displays bar graphs for the status of each individual uplink port in the LAG.

NOTE: The status of the LAG and its individual ports might not be the same.

- **Internal Ports** — Lists whether the Auto LAG feature is **Enabled** or **Disabled**. Also displays a circular graph displaying how many downlink ports are assigned as part of Auto LAG.

From this section you can:

- View LAG Memberships
- Configure Internal Ports for LAGs

Viewing LAG Memberships

You can view members currently assigned to Link Aggregation Groups (LAGs) from the Link Aggregation (LAG) section of the **Switching Layer-2** page.

1. From the navigation menu, click **Switching Layer-2**.
   The **Switching Layer-2** page appears.
2. In the Link Aggregation (LAG) section, click **View LAG Memberships**.
   The **LAG Membership** dialog box appears, displaying the following information about each LAG member:
   - **Connection** — Connection type
   - **LAG** — LAG name
   - **Minimum Links** — Minimum links in the LAG
   - **Members** — Interface labels of the LAG members
   - **LAG Port Channel Status** — Status of the port channel: Up or Down
3. You can filter this list by selecting one of the following from the **Filter By** drop-down menu:
   - **All**
   - **Uplink**
   - **Downlink**
   - **Interconnect (ICL/VLTi)** (VLT mode only)
4. Click **Apply**.

Configuring Internal Ports for LAGs

From the Link Aggregation (LAG) section of the Switching Layer-2 page, you can view VLAN port assignments for the I/O Aggregator device.

1. From the navigation menu, click **Switching Layer-2**.
2. In the Link Aggregation (LAG) Internal Ports section, click **Edit**.
   The **Link Aggregation Group (LAG)** dialog box appears.
3. In the **Auto LAG** field, select **Enabled** to enable the Auto LAG feature or **Disabled** to disable it.
   If you select **Enabled**, all ports on the I/O Aggregator device are selected by default. Perform the following steps.
4. In the graphic representing the ports on the I/O Aggregator device, you can clear any ports you do not want the Auto LAG to assign.
   Ports eligible for assignment by Auto LAG appear in the **Selected Internal Ports** field.
5. Click **Apply**.

The **Status** dialog box appears displaying the results of the port assignments. You can click **Configure Another Port** to return to the **Link Aggregation Group (LAG)** dialog box and configure more internal port assignments for LAGs or click **Close** to return to the **Switching Layer-2** page.

IGMP

In the IGMP section of the **Switching Layer-2** page, you can configure Internet Group Management Protocol (IGMP).

Multicast is based on identifying many hosts by a single destination IP address. Hosts that the same IP address represents are a multicast group. IGMP is a Layer 3 multicast protocol that hosts use to join or leave a multicast group. Multicast routing protocols (such as protocol-independent multicast [PIM]) use the information in IGMP messages to discover which groups are active and to populate the multicast routing table.

This page displays whether the following settings are enabled or disabled:

- **IGMP Snooping Status** — IGMP snooping enables switches to use information in IGMP packets to generate a forwarding table that associate ports with multicast groups, so that the received multicast frames are forwarded only to interested receivers.
- **IGMP Flood Restrict** — When enabled, unregistered multicast data traffic is forwarded to only multicast router ports on all VLANs. If there is no multicast router port in a VLAN, unregistered multicast data traffic is dropped.

In this section you can configure IGMP settings.

Configuring IGMP Settings

In the IGMP section of the **Switching Layer-2** page, you can configure IGMP flood restrict.

1. From the navigation menu, click **Switching Layer-2**.
   The **Switching Layer-2** page appears.
2. In the IGMP section, click **Edit**.
   The **IGMP** dialog box appears.
3. Select **Enabled** or **Disabled** for the following feature:
   - **IGMP Flood Restrict** — When enabled, unregistered multicast data traffic is forwarded to only multicast router ports on all VLANs. If there is no multicast router port in a VLAN, unregistered multicast data traffic is dropped.
4. Click **Apply**.

Port Mirroring

You can view and configure port mirroring settings in the Port Mirroring section of the **Switching Layer-2** page.

In most situations, switches only forward frames to relevant ports. To monitor traffic, either for information gathering, such as statistical analysis, or for troubleshooting higher-layer protocol operation, the port mirroring feature forwards frames to a monitoring port. This feature c to specify that a desired destination (target) port receives a copy of all traffic passing through designated source ports. The frames arriving at the destination port are copies of the frames passing through the source port at ingress, prior to any switch action.

This section displays source and destination ports configured for port mirroring and transmission direction. From this section, you can configure port mirroring settings.

Configuring Port Mirroring Settings

You can configure port mirroring settings in the Port Mirroring section of the **Switching Layer-2** page. Port mirroring forwards frames to a monitoring port.

1. From the navigation menu, click **Switching Layer-2**.
   The **Switching Layer-2** page appears.
2. In the Port Mirroring section, click **View Details**.
   The **Port Mirroring** dialog box appears.
3. To create a port mirroring session to monitor, click **Add**.
4. In the **Select Source (Internal Ports)** section, select the ports on the I/O Aggregator device whose traffic you want to copy. You can select a maximum of four.
5. From the **Select Destination (External Port)**, select the monitoring port.
6. In the **Direction** area, select the type of traffic you want copied:
   - **Rx** — Receiving
   - **Tx** — Transmitting
   - **Rx** and **Tx** — Both receiving and transmitting
7. Click **Apply**.

To edit the monitoring ports in a session, select the check box of the session and click **Edit**. You can only edit the source ports. To delete a session, select the check box of the session and click **Delete**.

Fibre Channel

The Fibre Channel section of the **Switching Layer-2** page displays options for Fibre Channel mode for I/O Aggregator devices

This page displays settings depending on the selected Fibre Channel mode.

Table 1. Fibre Channel Modes

Mode	Description
FIP Snooping Bridge (FCoE)	FIP Snooping Bridge when enabled monitors FCoE Initiation Protocol (FIP) logins, solicitations, and advertisements. In this monitoring or snooping process, the switch gathers information about ENode and FCF addresses. With this information, the switch places filters that only allow access to ENode devices that successfully log in. The FCoE VLAN can then deny all other traffic except this loss-less FCoE storage traffic
NPIV Proxy Gateway	In Fibre Channel networks, FC switches are trusted devices that act as a Fibre Channel Forwarder (FCF). Other devices must log in to these switches before they can communicate with the rest of the fabric. FC connections usually are point-to-point allowing the FC switches complete control over the traffic that connected devices insert into the

Mode	Description
	fabric. An NPIV Proxy Gateway (NPG) allows numerous point-to-point connects over a single device (in this case, the I/O Aggregator device). This feature allows each converged network adapter (CNA) in each server to present itself as a trusted connection to the storage fabric.
Fabric-Services (FPORT)	The F_Port connects from the FC switch to the N_Port of an end device. The F_Port on an FC switch provides access to Fabric Services such as Fabric Name Server and Fabric Login Server.

NOTE: Your I/O Aggregator device must have a Fibre Channel module (Flex FC IOM or FN2210S) installed to view and configure Fabric-Services (FPORT) and NPIV Proxy Gateway.

For FIP Snooping Bridge (FCoE):

- **Fibre Channel Mode** — Displays FIP Snooping Bridge (FCoE).
- **FCoE VLAN List** — Displays IDs of FCoE VLANs that pass storage traffic.
- **FCoE Forwarders** — Displays number of FCoE Forwarders that act as an Ethernet and FC switch combined.
- **End Nodes** — Displays the list of ENodes (FCoE initiators) that request a session.
- **FIP Snooping Sessions** — Displays number of FIP snooping sessions.

For NPIV Proxy Gateway (NPG):

- **Fibre Channel Mode** — Displays NPIV Proxy Gateway (NPG).
- **FC Switch WWN** — Displays the 64–bit World Wide Name that uniquely identifies each component in the Fibre Channel switch network.

For Fabric-Services (FPORT):

- **Fibre Channel Mode** — Displays Fabric Services (FPORT).
- **FC Switch WWN** — Displays the 64–bit World Wide Name that uniquely identifies each component in the Fibre Channel switch network.
- **Domain ID**
- **Zoning** — Displays whether zoning is enabled and configured.
- **Active Zoneset** — Displays the active zone set. A zone set consists of multiple zones.
- **Number of Zones** — Displays number of zones present in the active zoneset. Zones create functional areas within a SAN and prevent unauthorized access
- **Default Zone** — Displays the default zone.

From this section you can:

- Edit the Fibre Channel mode
- View Fibre Channel details
- Configure zoning

Editing Fibre Channel Settings

From the Fibre Channel section of the **Switching Layer-2** page, you can select the Fibre Channel (FC) mode.

1. From the navigation menu, select **Switching Layer-2**.
   The **Switching Layer-2** page appears.
2. In the Fibre Channel section, in the **Fibre Channel Mode** field, click **Edit**.
   The **Fibre Channel** dialog box appears.
3. For the **Fibre Channel Mode** setting, select one of the following:
   - **FIP Snooping Bridge (FSB)** — Uses FCoE to inspect frames and applies policies based on frame information.

     NOTE: FSB is disabled for Flex IOM on M1000e and FN2210S SKU for FX2.
   - **NPIV Proxy Gateway (NPG)** — Acts as an FC forwarder and does not support name service or zoning.
   - **Fabric-Services (FPORT)** — Supports name service and zoning. In the **Domain ID** field, enter a number.
   - **Disabled** — Select to disable Fibre Channel mode.
4. Click **Apply**.

Viewing Fibre Channel Details

From the Fibre Channel section of the **Switching Layer-2** page, you can view additional Fibre Channel settings. These settings can depend on the selected Fibre Channel mode.

1. From the navigation menu, select **Switching Layer-2**.
   The **Switching Layer-2** page appears.
2. In the Fibre Channel section, click **View Details**.
   A dialog box appears. The information that appears depends on the selected Fibre Channel mode.
   For FIP Snooping Bridge (FCoe) mode, this dialog box displays:

   - **MAC Address** and **Interface** of the End Node.
   - **MAC Address**, **Interface**, and **VLAN** of the FCF
   - **FCoE Address**, **FC ID**, **Port WWPN**, and **Port WWNN** of Session Info.

   For **NPIV Proxy Gateway**, this dialog box displays:

   - **FCoE Sessions** tab
     - **MAC Address** and **Interface** of the End Node.
     - **MAC Address**, **Interface**, and **VLAN** of the FCF
     - **FCoE Address**, **FC ID**, **Port WWPN**, and **Port WWNN** of Session Info.
   - **FCoE Map**
     - **FCoE Map**
     - **Fabric ID**
     - **VLAN ID**

- **FC-Map**
- **FCF Priority**
- **Members**

Fabric Services (FPORT):

- **Name Server** — This tab displays Fibre Channel hosts or connections.
  - **FC-ID**
  - **Interface**
  - **End Node WWPN**
  - **End Node WWNN**

  You can click the + button to view additional details for each host or connection:

  - **Class of Service (CoS)**
  - **Symbolic Port Name**
  - **Port Type**
  - **Registered with Name Server**
  - **Registered for SCN**
- **FCoE Map** — This tab displays FCoE traffic mapped to the respective VLAN.
- **Zoning** — This tab is where you can view and configure zoning. Refer to Configuring Zoning for more information.

Configuring Zoning

From the Fibre Channel section of the **Switching Layer-2** page, you can configure zoning settings for Fibre Channel Fabric Services (FPORT) mode.

Zoning helps improve Storage Area Network (SAN) security by restricting information access to the member devices in a defined zone. Any two devices that are not members of one common zone are not permitted to communicate with one another. Zoning can be used to create functional areas within the SAN and prevent unauthorized access. For example, some organizations use zones to ensure that finance systems on the SAN cannot access the data that engineering or test systems own. Zoning also makes SANs easier to manage. A common use of zoning is to segregate servers and enterprise storage that use different operating systems to avoid undesirable results that the accidental transfer of information from one to another can cause.

1. From the navigation menu, select **Switching Layer-2**.

   The **Switching Layer-2** page appears.
2. In the Fibre Channel section, make sure that **Fabric Services (FPORT)** is selected. If not, refer to Editing the Fibre Channel Mode.
3. Under the Zoning settings, click **View Details**.

   The **Fibre Channel** dialog box appears.
4. Make sure that the **Zoning** tab is selected.
5. You can configure multiple zones but only one can be active at a time. To select the active zone, click **Settings**.

   The **Settings** dialog box appears.
6. From the **Select Active Zone** drop-down menu, make a selection.
7. In the **Default Mode** section, select **All Access** or **No Access**.

8. Click **Save**.
9. A zone set consists of multiple zones. You can use zone sets to switch between zone configurations without having to recreate the entire zone configuration. To configure zone sets, click **Edit**.

   The **Edit Zoning** dialog box appears.
10. Configure aliases, An alias is a logical name that can denote one or more zone members. Perform the following steps:
    a. In the Alias section, click **Add Alias**.

       The **Add Alias** dialog box appears.
    b. Make an entry in the **Name** field.
    c. Click **Save**.

       A confirmation dialog box appears.
    d. Click **Close**.
    e. Configure members of the alias: To view all potential members, click the **+** button. Add a member to the Alias Members section from the Available Members section by using the **>** button. You can also click **Add Manually** to open the **Add Member** dialog box and specify a WWPN or FC-ID member to add to the zone. You can remove a member from the alias by selecting it and using the **<** button. You can permanently delete a device from the list by selecting it from the drop-down list and clicking **Delete**.
    f. Click **Apply**.

       A confirmation dialog box appears.
    g. Click **Close**.
    h. Repeat steps a-g to add additional aliases.
11. Configure zones. Zones contain a minimum of two devices that are not members of one common zone that are permitted to communicate with each other. Use zones to create functional areas within the SAN and prevent unauthorized access. You can also use zones to segregate serves that use different operation systems. Click **Zone** to expand that section and perform the following steps:
    a. Click **Add Zone**.

       The **Add Zone** dialog box appears.
    b. Make an entry in the **Name** field.
    c. Click **Save**.

       A confirmation dialog box appears.
    d. Click **Close**.
    e. Configure members of the zone. Click the **+** button to expand to view all members. Add a member to the Zone Members section from the Available Members section by using the **>** button. Conversely, you can remove a member from the zone by selecting it and using the **<** button. You can permanently delete a zone from the list by selecting it and clicking **Delete**.
    f. Click **Apply**.

       A confirmation dialog box appears.
    g. Click **Close**.
    h. Repeat steps a-g to add additional zones.
12. Zone sets consist of multiple zones. You can configure them so you can switch between zone configurations without having to recreate an entire configuration. Click **Zoneset** to expand that section and perform the following steps:
    a. Click **Add Zoneset**.

       The **Add Zoneset** dialog box appears.
    b. Make an entry in the **Name** field.
    c. Click **Save**.

       A confirmation dialog box appears.
    d. Click **Close**.

e. Configure members of the zone set. Click the **+** button to expand to view all members. Add a member to the Zoneset Members section from the Available Members section by using the **>** button. Conversely, you can remove a member from the zone set by selecting it and using the **<** button. You can permanently delete a zoneset from the list by selecting it from the drop-down menu and clicking **Delete**.

f. Click **Apply**.

   A confirmation dialog box appears.

g. Click **Close**.

h. Repeat steps a-g to add additional zone set.

13. To close the **Edit Zoning** dialog box, click **Close**.

iSCSI

In the iSCSI section of the **Switching Layer-2** page, you can review Internet Small Computer System Interface (iSCSI) storage sessions.

iSCSI optimization enables quality-of-service (QoS) treatment for iSCSI storage traffic on an I/O Aggregator device.

This section displays the following details for iSCSI:

- **iSCSI Status** — Displays whether iSCSI sessions are active on the I/O Aggregator device: **Enabled** or **Disabled**.
- **iSCSI Class of Service (CoS)** — Displays the QoS policy applied to iSCSI flows.
- **Session Aging Time (min)** — Displays the time-out value in minutes for iSCSI sessions.
- **Number of iSCSI Monitoring TCP Ports** — Displays the number of enabled iSCSI ports.
- **iSCSI Connections** — Displays the number of active iSCSI connections.
- **Maximum Number of Connections** — Displays the maximum number (256) of potential iSCSI connections.
- **TCP Port** — Displays the TCP initiator port (860 or 3260) used to contact the iSCSI service.

From this section you can view additional iSCSI storage session details.

Viewing iSCSI Sessions

In the iSCSI section of the **Switching Layer-2** page, you can view each iSCSI session between target (storage) and initiators (host)

1. From the navigation menu, click **Switching Layer-2**.

   The **Switching Layer-2** page appears.

2. In the iSCSI section, click **View Details**.

   The **iSCSI Sessions** dialog box appears.

3. From the **Filter By** menu, select **Target** or **Initiator**.

   All iSCSI sessions for the selected category appear, displaying the session number, target, and ISID. You can click the + symbol next to the session to view the following additional information:

   - **Target**
   - **Initiator**
   - **Up Time**
   - **Time for Aging** — The time out value in minutes for this session.
   - **ISID**

For each connection:

- **Connection ID**
- **Initiator IP Address**
- **Initiator TCP Port**
- **Target IP Address**
- **Target TCP Port**

4. To close the **iSCSI Sessions** dialog box, click **Cancel**.

DCB

You can view Data Center Bridging (DCB) settings from the DCB section of the **Switching Layer-2** page.

DCB refers to a set of IEEE Ethernet enhancements that provide data centers with a single, robust, converged network to support multiple traffic types, including local area network (LAN), server, and storage traffic.

This section lists the following:

- **Status** — Displays whether DCB is **Enabled** or **Disabled** on the I/O Aggregator device.
- **DCBx Configuration Source** — Port role when DCBx is enabled: **Auto-Upstream**, **Auto-Downstream**, **Configuration Source**, or **Manual**.

You can also view more Data Center Bridging settings.

Viewing Data Center Bridging Settings

You can view additional Data Center Bridging (DCB) settings from the DCB section of the **Switching Layer-2** page.

1. From the navigation menu, click **Switching Layer-2**.
   The **Switching Layer-2** page appears.
2. In the DCB section, click **View Details**.
   The **DCB** dialog box appears. You can choose to view details by protocol by selecting **PFC**, **DCBx**, or **ETS** from the **Filter By** menu.
   For Priority-based Flow Control (PFC), the following information appears:

   - **Interface** — Interface type with chassis slot and port number.
   - **Operational Status** — Displays the status of DCB on an individual port: **Up** or **Down**.
   - **Application Priority FCoE** — Displays the order in which bandwidth (according to displayed priority) is allocated for FCoE.
   - **Application Priority iSCSI** — Displays the order in which bandwidth (according to displayed priority) is allocated for iSCSI.

   For DCBx, the following information appears:

   - **Interface** — Displays the interface type with chassis slot and port number.
   - **Operational Status** — Displays the operational status (**enabled, Port Up** or **disabled, Port Shutdown**) used to elect a configuration source and internally propagate a DCB configuration. The DCBx operational status is the combination of PFC and ETS operational status.
   - **Operating Version** — Displays the DCBx version configured on the port: **CEE**, **CIN**, or **IEEE**.

- **Port Role** — Displays the DCBx port role: **Auto upstream**, **Auto downstream**, **Configuration Source**, or **Manual**.

For Enhanced Transmission Selection (ETS), the following information appears:

- **Interface** — Displays the interface type with chassis slot and port number.
- **Operational Status** — Displays the status of DCB on an individual port: **Up** or **Down**.
- **Priority Group** — Displays the number of the priority group that specifies the range of 802.1p priority traffic to which a QoS output policy with ETS settings is applied on an egress interface.
- **Priority** — Displays the priority levels assigned to that interface.
- **Bandwidth** — Displays the allocated bandwidth percentage for that interface.
- **Scheduling Algorithms** — Displays the selected scheduling algorithm: **Strict** (highest bandwidth used for that interface is set in the strict priority feature) or ETS (bandwidth is configured as part of ETS).

3. To close the **DCB** dialog box, click **Close**.

6

Security

You can view and configure settings for access, authentication, authorization, security, and users on the **Security** page.

This page consists of the following sections:

- TACACS+
- RADIUS
- AAA

  NOTE: You can only view and configure TACACS+, RADIUS, or AAA settings for M1000e and FN IOA devices in standalone or VLT mode.
- Passwords and Credentials

TACACS+

Dell Networking OS supports TACACS+ as an alternate method for login authentication for I/O Aggregator devices. On the **Security** page, you can configure up to 10 Terminal Access Controller Access-Control System Plus (TACACS+) servers.

NOTE: You can only view and configure TACACS+ settings for M1000e and FN IOA devices in standalone or VLT mode.

This page displays the number of servers configured. On this page, you can perform the following tasks:

- View TACACS+ settings
- Add TACACS+ settings
- Remove TACACS+ settings

Viewing TACACS+ Settings

On the **Security** page, you can view TACACS+ server settings. You can configure a maximum of 10 TACACS+ servers.

1. From the navigation menu, select **Security**.
2. In the TACACS+ section, click **View Details**.

   The **TACACS Settings** dialog box appears.

This dialog box displays the following information about each TACACS+ server:

- **Number** — System assigned from 0 to 10.
- **Source** — IP address or host name of the server.
- **Key String** — Key string used for encryption and decryption.
- **TCP-Port** — TCP port used to connect to the TACACS+ server.

- **Timeout for reply (sec)** — Seconds that I/O Aggregator device waits for a reply from the TACACS+ server before it times out the connection.

Adding TACACS+ Settings

On the **Security** page, you can add new TACACS+ server settings. You can configure a maximum of 10 TACACS+ servers.

NOTE: You can only configure TACACS+ settings for M1000e and FN IOA devices in standalone or VLT mode.

1. From the navigation menu, select **Security**.
2. In the TACACS+ section, click **Edit**.

   The **TACACS Settings** dialog box appears.
3. Click **Add**.

   The **Add TACACS+** dialog box appears.
4. In the **Source** field, select whether you want to enter an **IP Address** or **Host Name** for the TACACS+ server.
5. In the **Source IP Address or Host Name** field, enter the IP address or host name (depending on the selection you made in step 1) for the TACACS+ server.

   NOTE: IP addresses must be in IPv4 notation. You cannot enter a host name if the I/O Aggregator device is in stack or VLT mode.
6. In the **Key String** field, enter the authentication key string exchanged between the TACACS+ server and the I/O Aggregator device. The maximum length of the key string is 42 characters.
7. In the **TCP-Port** field, enter the TCP port used to connect to the TACACS+ server. The default value is 49.
8. In the **Timeout for Reply (sec)** field, enter the number of seconds the I/O Aggregator device waits for a reply from the TACACS+ server before timing out the connection. The default value is 10.
9. Click **Apply**.

   The settings for the server appear in the **TACACS settings** dialog box.

Removing TACACS+ Settings

On the **Security** page, you can remove TACACS+ server settings.

1. From the navigation menu, select **Security**.
2. In the TACACS+ section, click **Edit**.

   The **TACACS settings** dialog box appears.
3. Select the check box of the server settings and click **Remove**.

NOTE: Removing a TACACS+ server settings causes the remaining settings to move up one number. For example, if you delete settings number 3, the previous settings number 4 becomes the new number 3.

RADIUS

Dell Networking OS supports RADIUS as an alternate method for login authentication for I/O Aggregator devices. On the **Security** page, you can configure up to 10 RADIUS servers.

NOTE: You can only view and configure RADIUS settings for M1000e and FN IOA devices in standalone or VLT mode.

This page displays the number of servers configured and the current dead time setting. On this page, you can perform the following tasks:

- View RADIUS settings
- Add RADIUS settings
- Configure Global RADIUS settings
- Remove RADIUS settings

Viewing RADIUS Settings

On the **Security** page, you can view RADIUS server settings. You can configure a maximum of 10 RADIUS servers.

1. From the navigation menu, select **Security**.
2. In the RADIUS section, click **View Details**.
   The **RADIUS Settings** dialog box appears.

This dialog box displays the following information about each RADIUS server:

- **Number** — System assigned from 0 to 10.
- **Source** — IP address or host name of the server.
- **Key String** — Key string used for encryption and decryption.
- **Auth-Port** — Authorization port number used to connect to the external RADIUS server. The port number is set to 1812 by default.
- **Timeout for reply (sec)** — Seconds that I/O Aggregator device waits for a reply from the RADIUS server before it times out the connection. The maximum number of seconds you can enter is 1000. The default setting is 5 seconds.
- **Number of Retransmits** — Number of times the I/O Aggregator device attempts to connect to RADIUS server. The maximum number you can enter is 100. The default value is 3.

Adding RADIUS Settings

On the **Security** page, you can add new RADIUS server settings. You can configure a maximum of 10 RADIUS servers.

NOTE: You can only configure RADIUS settings for M1000e and FN IOA devices in standalone or VLT mode.

1. From the navigation menu, select **Security**.
2. In the RADIUS section, click **Edit**.
   The **RADIUS Settings** dialog box appears.
3. Click **Add**.
   The **Add RADIUS** dialog box appears.
4. In the **Source** field, select whether you want to enter an **IP Address** or **Host Name** for the RADIUS server.
5. In the **Source IP Address or Host Name** field, enter the IP address or host name (depending on the selection you made in step 1) for the RADIUS server.

   NOTE: IP addresses must be in IPv4 notation. You cannot enter a host name if the I/O Aggregator device is in stack or VLT mode.
6. In the **Key String** field, enter the authentication key string exchanged between the RADIUS server and the I/O Aggregator device. The maximum length of the key string is 42 characters.

7. In the **Auth-port** field, enter the Auth port used to connect to the RADIUS server.
8. In the **Timeout for Reply (sec)** field, enter the number of seconds the I/O Aggregator device waits for a reply from the RADIUS server before timing out the connection. The maximum number of seconds you can enter is 1000.
9. In the **Number of Retransmits** field, enter the number of times the I/O Aggregator device attempts to connect to RADIUS server. The maximum number you can enter is 100.
10. Click **Apply**.

    The settings for the server appear in the **RADIUS settings** dialog box.

Configuring Global RADIUS Settings

On the **Security** page, you can configure the dead time setting that applies to all configured RADIUS servers. Dead time is the time interval during which the I/O Aggregator device skips authentication requests to nonresponsive RADIUS servers.

NOTE: You can only configure RADIUS settings for M1000e and FN IOA devices in standalone or VLT mode.

1. From the navigation menu, select **Security**.
2. In the RADIUS section, click **Edit**.

   The **Radius settings** dialog box appears.
3. Click **Settings**.

   The **RADIUS Global Settings** dialog box appears.
4. In the **Dead Time (sec)** field, enter a number in seconds. The maximum number of seconds you can enter is 2147483647.
5. Click **Apply**.

Removing RADIUS Settings

On the **Security** page, you can remove RADIUS server settings.

1. From the navigation menu, select **Security**.
2. In the RADIUS section, click **Edit**.

   The **RADIUS settings** dialog box appears.
3. Select the check box of the server settings and click **Remove**.

NOTE: Removing a RADIUS server setting causes the remaining settings to move up one number. For example, if you delete settings number 3, the previous settings number 4 becomes the new number 3.

AAA

The AAA section of the **Security** page is where you can manage identity, grant access, or track users of an I/O Aggregator device.

NOTE: You can only view and configure AAA settings for M1000e and FN IOA devices in standalone or VLT mode.

From this section, you can configure the following three categories of settings:

- Authentication
- Authorization

- Accounting

Configuring Authentication

You can configure authentication settings in the **Security** page.
These settings control management access to the I/O Aggregator device.

NOTE: You can only view and configure these settings for M1000e and FN IOA devices in standalone or VLT mode.

1. From the navigation menu, click **Security**.
2. In the AAA section, click **Edit**.

   The **AAA settings** dialog box appears.
3. Make sure that the **Authentication** tab is selected and click **Edit**.

   The **Edit Authentication Profile** dialog box appears.
4. In the Authentication Login Profile section, configure the AAA Authentication methods for user access to EXEC mode. Select from the following authentication methods you want to enable in the **Optional Methods** box and use the **>** button to move them into the **Selected Methods** box:
   - **Line** — Use the password the `password` command defines in LINE mode.
   - **Enable** — Use the password the `enable` password command defines in CONFIGURATION mode.
   - **TACACS+** — Use configured TACACS+ servers.
   - **None** — No authentication.
   - **Local** — Use the local device authorization server.
   - **RADIUS** — Use configured RADIUS servers.

   NOTE: You can click **Clear Methods** to clear all selections from the **Selected Methods** box.
5. In the Authentication Enable Profile section, configure the AAA Authentication methods for user access to EXEC privilege mode (the "Enable" access). Select from the following authentication methods you want to enable in the **Optional Methods** box and use the **>** button to move them into the **Selected Methods** box:
   - **Line** — Use the password the `password` command defines in LINE mode.
   - **Enable** — Use the password the `enable` password command defines in CONFIGURATION mode.
   - **TACACS+** — Use configured TACACS+ servers.
   - **None** — No authentication.
   - **Local** — Use the local device authorization server.
   - **RADIUS** — Use configured RADIUS servers.

   NOTE: You can click **Clear Methods** to clear all selections from the **Selected Methods** box.
6. Click **Apply**.

   Your selections appear on the **Authentication** tab.
7. To close the **AAA settings** dialog box, click **Close**.

Configuring Authorization

You can configure AAA authorization settings in the **Security** page.
You can configure parameters that restrict (or permit) user access to the EXEC and CONFIGURATION level commands.

NOTE: You can only configure these settings for M1000e and FN IOA devices in standalone or VLT mode.

1. From the navigation menu, click **Security**.
2. In the AAA section, click **Edit**.

   The **AAA settings** dialog box appears.
3. Make sure that the **Authorization** tab is selected and click **Edit**.

   The **Edit Authorization Profile** dialog box appears.
4. In the Configuration Commands section, select whether a user has access to CONFIGURATION level commands: **Enabled** or **Disabled**.
5. In the Commands section, select the authorization methods for CONFIGURATION level commands that you want to enable in the **Available Methods** box and use the **>** button to move them into the **Selected Methods** box. Select from the following options:
   - **Line** — Use terminal line.
   - **Enable** — Use password protection on I/O Aggregator device.
   - **TACACS+** — Use the TACACS+ protocol to perform user authorization.
   - **None** — No authorization.
   - **Local** — Use the local device authorization server to perform user authorization.
   - **RADIUS** — Use the RADIUS protocol to perform user authorization.

   NOTE: You can click **Clear Methods** to clear all selections from the **Selected Methods** box.
6. In the Exec-Auth section, select the authorization methods for EXECUTIVE level commands that you want to enable in the **Available Methods** box and use the **>** button to move them into the **Selected Methods** box. Select from the following options:
   - **Line** — Use terminal line.
   - **Enable** — Use password protection on I/O Aggregator device.
   - **TACACS+** — Use the TACACS+ protocol to perform user authorization.
   - **None** — No authorization.
   - **Local** — Use the local device authorization server to perform user authorization.
   - **RADIUS** — Use the RADIUS protocol to perform user authorization.

   NOTE: You can click **Clear Methods** to clear all selections from the **Selected Methods** box.
7. Click **Apply**.

   Your selections appear on the **Authorization** tab.
8. To close the **AAA settings** dialog box, click **Close**.

Configuring Accounting

You can configure AAA accounting settings in the **Security** page.
AAA accounting enables tracking of services that users access and the amount of network resources that those services consume. When you configure AAA accounting, the I/O Aggregator device reports user activity to the TACACS+ security server in the form of accounting records. Each accounting record consists of accounting AV pairs and resides on the access control server.

NOTE: You can only view and configure these settings for M1000e and FN IOA devices in standalone or VLT mode.

1. From the navigation menu, click **Security**.
2. In the AAA section, click **Edit**.

The **AAA settings** dialog box appears.

3. Make sure that the **Accounting** tab is selected and click **Edit**.

   The **Edit Accounting** dialog box appears.

4. In the Exec section, you can configure whether accounting information is sent when a user logs on to the I/O Aggregator device in EXEC mode. Make one of the following selections:
   - **Start-Stop** — Sends a "start accounting" notice at the beginning of the requested event and a "stop accounting" notice at the end of the event.
   - **Stop-Only** — Instructs the TACACS+ server to send a "stop record accounting" notice at the end of the requested user process.
   - **Wait-Start** — Ensures that the TACACS + server acknowledges the start notice before granting the user's process request.
   - **None (default)**

   The selected method appears in this section.

5. In the Command Accounting section, you can configure whether accounting information is sent when a user logs in at the specified method and method level. Makes one of the following selections:
   - **Start-Stop** — Sends a "start accounting" notice at the beginning of the requested event and a "stop accounting" notice at the end of the event.
   - **Stop-Only** — Instructs the TACACS+ server to send a "stop record accounting" notice at the end of the requested user process.
   - **Wait-Start** — Ensures that the TACACS + server acknowledges the start notice before granting the user's process request.
   - **None (default)**

   The selected method and level appear in this section. The default method level is 15.

6. In the System Accounting section, you can configure whether to send accounting information of any other AAA configuration. Make one of the following selections:
   - **Start-Stop** — Sends a "start accounting" notice at the beginning of the requested event and a "stop accounting" notice at the end of the event.
   - **Stop-Only** — Instructs the TACACS+ server to send a "stop record accounting" notice at the end of the requested user process.
   - **Wait-Start** — Ensures that the TACACS + server acknowledges the start notice before granting the user's process request.
   - **None (default)**

   The selected method appears in this section.

7. Dell Networking OS issues accounting records for all users on the system, including users whose user name string, due to protocol translation, is NULL. To prevent the accounting records from being generated for sessions that do not have user names associated to them, in the Suppressing Null User Name section, select **Enabled**. To continue to have the device generate these records, select **Disabled**.

8. Click **Apply**.

   Your selections appear on the **Accounting** tab.

9. To close the **AAA settings** dialog box, click **Close**.

Passwords and Credentials

You can view or configure users who access the I/O Aggregator device in the Passwords and Credentials section of the **Security** page.

This page lists the active users who are currently logged on to the device and all users in the local user database.

On this page, you can perform the following tasks:

- View users
- Add users
- Edit users
- Delete users

Viewing Users

You can view users who have access to the I/O Aggregator device from the Passwords and Credentials section of the **Security** page.
Dell Blade I/O Manager can have a maximum of 64 users.

1. From the navigation menu, click **Security**.
2. In the Passwords and Credentials section, click **Edit**.
   The **Password Settings** dialog box appears.

This dialog box lists the following information about each user:

- **Number** — Displays the system-assigned number. This number is not static but can change depending on users who are deleted. For example, user 3 becomes user 2 if the original user 2 is deleted.
- **User ID** — Displays the user ID.
- **User Name** — Displays the user name. User names do not need to be unique.
- **Access Level** — Displays 0 for read-only or 15 for read-write.
- **Login Status** — Displays whether the user is logged in or logged out.
- **Protocol** — Displays what protocols the user logged in to the I/O Aggregator device. Multiple protocols listed indicate the user access the device through multiple methods.
- **Location** — Displays the IP address of the host accessing the device.

Adding Users

You can add users who have access to the I/O Aggregator device in the Passwords and Credentials section of the **Security** page.
You can add a maximum of 64 users.

1. From the navigation menu, click **Security**.
2. In the Passwords and Credentials section, click **Edit**.
   The **Password Settings** dialog box appears.
3. Click **Add**.
   The **Add User to Local Database** dialog box appears.
4. In the **User Name** field, enter the user name. The user name can be 1 to 63 characters in length.

5. In the **Privilege Level** field, select the user's access privileges to the device: **0 (read-only)** or **15 (read-write)**.
6. Enter the user's password in the **User Password** and **Confirm Password** fields. The password can be from 1 to 32 characters in length.
7. Click **Add**.

Editing Users

You can edit details for users who have access to the I/O Aggregator device in the Passwords and Credentials section of the **Security** page.

NOTE: After you add a user, you cannot edit their user name.

1. From the navigation menu, click **Security**.
2. In the Passwords and Credentials section, click **Edit**.

   The **Password Settings** dialog box appears.
3. Select a user and click **Edit**.

   The **Edit User** dialog box appears.
4. In the **Privilege Level** field, select the user's access privileges to the device: **0 (read-only)** or **15 (read-write)**.
5. Edit the user's password in the **User Password** and **Confirm Password** fields. The password can be from 1 to 32 characters in length.
6. Click **Apply**.

Deleting Users

You can delete who have access to the I/O Aggregator device in the Passwords and Credentials section of the **Security** page.

NOTE: If you delete a user who is logged in to Dell Blade I/O Manager, their current session continues. Upon logout, the deleted user can no longer access the I/O Aggregator device.

1. From the navigation menu, click **Security**.
2. In the Passwords and Credentials section, click **Edit**.

   The **Password Settings** dialog box appears.
3. Select a user and click **Delete**.

NOTE: Deleting a user causes the remaining users to move up one number. For example, if you delete user number 3, the previous user number 4 becomes the new number 3.

7

Device Settings

In Dell Blade I/O Manager, you can view or configure the following settings for I/O Aggregator devices:

- Global configuration
- IOA firmware (view only)
- Network Time Protocol
- Restore IOA

Global Configuration

The Global Configuration section of the **Settings** page displays the following settings for the I/O Aggregator device:

- **IOA Mode**:
  - **Standalone Mode (default)** — Default mode of the I/O Aggregator device. In this mode, all ports are configured as members of all VLANs. All VLANs are up and can send or receive Layer 2 traffic.
  - **Stack Mode** — Multiple switches operate as single unit. A single switch in the stack (Master switch) manages all units in the stack and uses a single IP address that you can use to manage every port in the stack.
  - **VLT Mode** — Virtual Link Trunking. VLT enables physical links between two chassis to appear as a single virtual link to the network core or other switches such as Edge, Access, or ToR. VLT reduces the role of Spanning Tree protocols by allowing LAG terminations on two separate distribution or core switches, and by supporting a loop free topology. VLT institutes Layer 2 multipathing, creating redundancy through increased bandwidth, enabling multiple parallel paths between nodes and load-balancing traffic where alternative paths exist.
  - **Programmable MUX Mode** — Programmable Multiplex mode. This mode provides flexibility of operation with added configurability. This mode creates multiple LAGs, configuring VLANs on uplinks and the server side, and configuring data center bridging (DCB) parameters. Programmable MUX mode supports both stacking and VLT operations. You can make any configuration or provisioning of the device through the CLI.
  - **Full Switch** — All commands and configurations supported on MXL available in this mode. This mode offers Layer 2/Layer 3 switching functionalities on the Dell FX2 chassis.

    NOTE: This mode is only available for FN IOA for FX2 chassis devices.
- **Broadcast Storm Control** — **Enabled** or **Disabled**. Broadcast storm control causes the device to limit or stop forwarding all broadcast traffic if they consume bandwidth beyond a configured threshold.
- **IGMP Flood Restrict** — **Enabled** or **Disabled**. When enabled, unregistered multicast data traffic is forwarded to only multicast router ports on all VLANs. If there is no multicast router port in a VLAN, unregistered multicast data traffic is dropped.
- **Auto LAG** — **Enabled** or **Disabled**. Determines if the device automatically assigns internal ports to Link Aggregation Groups.
- **Default VLAN** — Default VLAN to which the device assigns ports.

Editing Global Settings

You can edit settings that apply to the I/O Aggregator device that the Dell Blade I/O Manager manages.

1. In the navigation menu, click **Settings**.
2. In the Global Configuration section, click **Edit**.

   The **Global Settings** dialog box appears.
3. To enable broadcast storm control, in the **Broadcast Storm Control** area, select **Enabled**; to disable this feature, select **Disabled**.

   NOTE: You can only configure this setting for M1000e and FN IOA devices in standalone or VLT mode. For other devices and device modes, this setting is read-only.
4. To enable IGMP flood restrict, in the **IGMP Flood Restrict** area, select **Enabled**; to disable this feature, select **Disabled**.

   NOTE: You can only configure this setting for M1000e and FN IOA devices is standalone or VLT mode. For other devices and device modes, this setting is read-only.
5. To enable Auto LAG, in the **Auto LAG** area, select **Enabled**; to disable this feature, select **Disabled**.

   NOTE: You can only configure this setting for M1000e and FN IOA devices is standalone or VLT mode. For other devices and device modes, this setting is read-only.
6. In the **Default VLAN** field, enter the VLAN number to which the device automatically assigns internal ports.

   NOTE: You can only configure this setting for M1000e and FN IOA devices is standalone or VLT mode. For other devices and device modes, this setting is read-only.
7. Click **Apply**.

IOA Firmware

The IOA Firmware section of the **Settings** page displays the following information about the firmware on the I/O Aggregator device:

NOTE: You cannot upload or download firmware from the I/O Aggregator device using Dell Blade I/O Manager. Use a CLI terminal for these tasks.

- Current system version — The version of the Operating System on the I/O Aggregator device.
- Current boot flash — The version of the boot flash the device currently uses to load Dell Networking OS.
- Current boot selector — The version of the boot selector that chooses the boot flash.
- Current CPLD — The version of the Complex Programmable Logic Device that the device uses.

Network Time Protocol

In the Network Time Protocol (NTP) section of the **Settings** page, you can view the time zone and NTP servers applied to the I/O Aggregator device.

NOTE: You can only view these settings for M1000e and FN IOA devices in standalone or VLT mode.

This page lists the following information:

- **Time zone** — Displays the Coordinated Universal Time (UTC) offset and geographic area

- **NTP server** — Displays **enabled** or **disabled**
- **Preferred NTP server IP address or URL** — Displays the primary NTP server IP address or URL.
- **Secondary NTP server IP address or URL** — Displays the secondary or backup NTP server IP address or URL.

You can edit these settings.

Editing Network Time Protocol Settings

In the Network Time Protocol (NTP) section of the **Settings** page, you can edit the time zone and NTP servers applied to the I/O Aggregator device.

NOTE: You can only configure these settings for M1000e and FN IOA devices in standalone or VLT mode.

1. From the navigation menu, click **Settings**.
2. In the Network Time Protocol (NTP) section, click **Edit**.

   The **Host Name** dialog box appears.
3. From the **Time Zone** menu, select a time zone.
4. To configure NTP servers, select **Enable NTP Server**.
5. In the **Preferred NTP Server IP Address or URL** field, enter the IP address or URL for the primary NTP server you want to apply to the device.
6. (Optional) In the **Secondary NTP Server IP Address or URL** field, enter the IP address or URL for a secondary or backup NTP server you want to apply to the device.
7. Click **Apply**.

Restore IOA

In the Restore IOA section of the **Settings** page, you can:

- Restoring an I/O aggregator device to factory defaults
- Deleting the I/O aggregator startup configuration

Restoring an I/O Aggregator Device to Factory Defaults

From the Restore IOA section of the **Settings** page, you can restore an I/O Aggregator device to its factory default settings.

WARNING: Restoring a device to factory default settings erases all configurations, including mode settings, logs, and credentials. The device IP address/subnet mask is set to a DHCP value. The device username is set to `root` and its password to `calvin`.

1. From the navigation menu, click **Settings**.
2. In the Restore IOA section, click **Edit**.

   The **Restore IOA** dialog box appears.
3. From the **Configuration Option** drop-down menu, select **Restore Factory Defaults**.
4. Click **Apply**.

   The **Confirm** dialog box appears.
5. Click **Confirm**.

   The **Restore IOA** dialog box appears, displaying the progress of the factory default restoration.

Deleting the I/O Aggregator Startup Configuration

From the Restore IOA section of the **Settings** page, you can delete the startup configuration of an I/O Aggregator device.

WARNING: Performing this task erases all configurations, including mode settings and logs. The device IP address/subnet mask and user name/password are not affected.

1. From the navigation menu, click **Settings**.
2. In the Restore IOA section, click **Edit**.
   The **Restore IOA** dialog box appears.
3. From the **Configuration Option** drop-down menu, select **Delete Startup Configuration**.
4. Click **Apply**.
   The **Confirm** dialog box appears.
5. Click **Confirm**.
   The **Restore IOA** dialog box appears, displaying the progress of the deletion.