Brocade® Fabric OS® Web Tools User Guide, 9.2.x

User Guide
April 28, 2023

Table of Contents

Introduction

Brocade® Web Tools is a graphical user interface (GUI) embedded in the Fabric OS® firmware that enables administrators to monitor and manage single or small fabrics, switches, and ports.

Web Tools is launched directly from a Web browser or from the SANnav™ Management Portal. This document contains the system requirements and features of Web Tools.

Supported Hardware and Software

The following hardware platforms are supported by Brocade Fabric OS v9.2.x.

Brocade Gen 7 (64G) Fixed-Port Switches

- Brocade G720 Switch
- Brocade G730 Switch
- Brocade 7850 Extension Switch

Brocade Gen 7 (64G) Directors

- Brocade X7-4 Director
- Brocade X7-8 Director

Brocade Gen 6 (32G) Fixed-Port Switches

- Brocade G610 Switch
- Brocade G620 Switch
- Brocade G630 Switch
- Brocade 7810 Extension Switch
- Brocade G648 Blade Server SAN I/O Module
- Brocade MXG610 Blade Server SAN I/O Module

Brocade Gen 6 (32G) Directors

- Brocade X6-4 Director
- Brocade X6-8 Director

Contacting Technical Support for Your Brocade® Product

If you purchased Brocade® product support from a Broadcom® OEM or solution provider, contact your OEM or solution provider for all your product support needs.

- OEM and solution providers are trained and certified by Broadcom to support Brocade products.
- Broadcom provides backline support for issues that cannot be resolved by the OEM or solution provider.
- Brocade Supplemental Support augments your existing OEM support contract, providing direct access to Brocade expertise. For more information on this option, contact Broadcom or your OEM.
- For questions regarding service levels and response times, contact your OEM or solution provider.

If you purchased Brocade product support directly from Broadcom, use one of the following methods to contact the Technical Assistance Center 24x7. For product support information and the latest information on contacting the Technical Assistance Center, go to www.broadcom.com/support/fibre-channel-networking/contact-brocade-support.

Online	Telephone
For nonurgent issues, the preferred method is to log on to the Support portal at support.broadcom.com. (You must initially register to gain access to the Support portal.) Once registered, log on and then select **Brocade Products**. You can now navigate to the following sites: • **Case Management** • **Software Downloads** • **Licensing** • **SAN Reports** • **Brocade Support Link** • **Training & Education**	For Severity 1 (critical) issues, call Brocade Fibre Channel Networking Global Support at one of the phone numbers listed at www.broadcom.com/support/fibre-channel-networking/contact-brocade-support.

Document Feedback

Quality is our first concern. We have made every effort to ensure the accuracy and completeness of this document. However, if you find an error or an omission or if you think that a topic needs further development, we want to hear from you. Send your feedback to documentation.pdl@broadcom.com. Provide the publication title; topic heading; publication number and page number (for PDF documents); URL (for HTML documents); and as much detail as possible.

Getting Started with Web Tools

Brocade Web Tools is an embedded graphical user interface (GUI) that enables administrators to monitor and manage single or small fabrics, switches, and ports. Before launching Web Tools, verify that your workstation uses a supported operating system and Web browser.

Web Tools does not require a license. It is installed on the switch when you install Fabric OS.

Supported Operating Systems

Web Tools supports the following operating systems:

- Red Hat Enterprise Linux
- Windows 10 Pro
- Windows 2019

Supported Web Browsers

The following browsers can be used to access Web Tools:

- Firefox version 95 and later
- Chrome version 96 and later
- MS Edge version 97 and later

> **NOTE**
> Web Tools shows the U.S. English language irrespective of the language setting of the browser or operating system.

Launching Web Tools

Web Tools is launched directly from a web browser or from SANnav Management Portal. You can launch Web Tools on any workstation with a compatible OS and web browser installed.

If the switch is configured with logical fabrics, you can log in to any of the logical fabrics for which you have permission.

1. Launch Web Tools directly from a browser or from SANnav Management Portal.

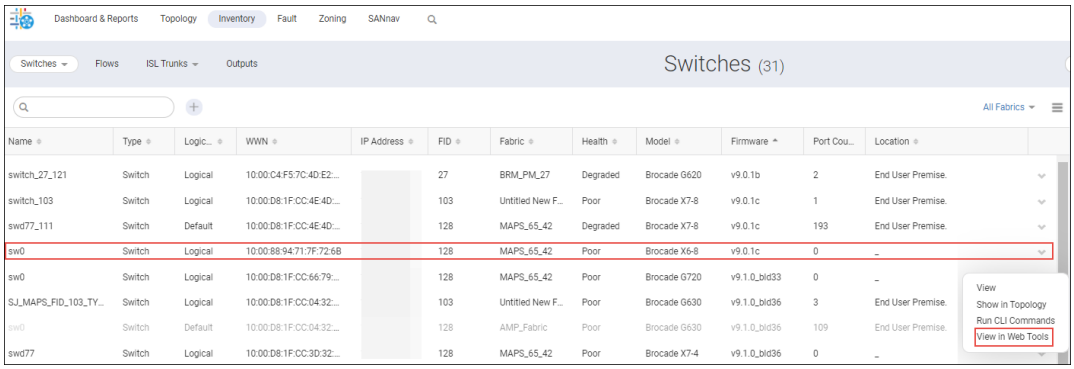
   > **NOTE**
   > To ensure that the latest version of Web Tools is loaded in the browser, close the previous version of Web Tools (browser) and clear the browser cache before launching the new version of Web Tools.

   - To launch directly from a web browser, open your browser, enter HTTP or HTTPS followed by the IP address of the switch.

     For example: `http://10.77.77.77` Or `https://10.77.77.77`
   - To launch from SANnav Management Portal, locate the switch on the SANnav **Inventory** page, click the down arrow to the right of the switch, and select **View in Web Tools** from the action menu.

     > **NOTE**
     > You can also launch Web Tools from SANnav Management Portal (**Health Summary** dashboard). For detailed information, refer to the *Brocade SANnav Management Portal User Guide*.

   Figure 1: Launching Web Tools from SANnav Management Portal



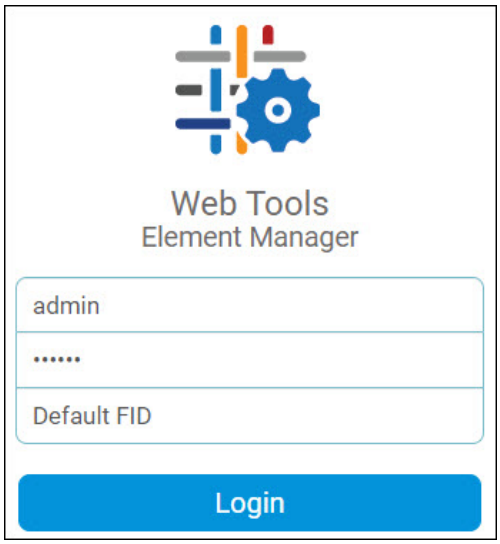
NOTE
Note the firmware version of the switch. The corresponding version of Web Tools launches, which might not be a version that is supported by this guide.

2. Enter the user name, password, and logical switch name or fabric ID (FID).

   For the behavior of launching Web Tools (SSO or non-SSO) from SANnav, refer to the *Brocade SANnav Management Portal User Guide*.

   If you are logging in to a Virtual Fabrics-enabled platform and you do not specify a logical switch, you are logged in to the default FID of the switch.

   If you launch from SANnav Management Portal, you might not be required to log in, depending on the SANnav single sign-on configuration.



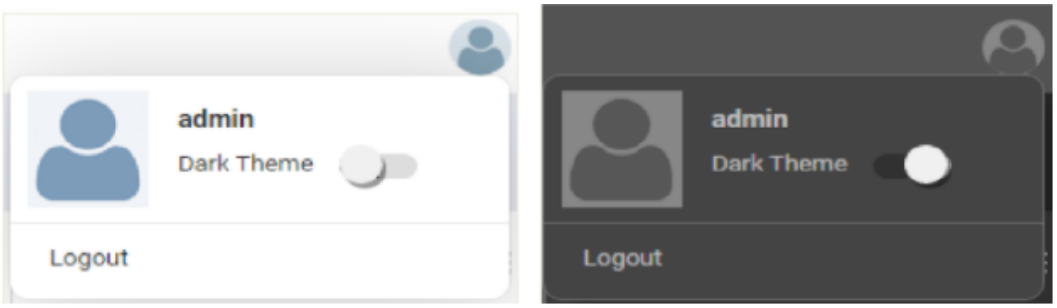
3. Click **Login**.

Support for Dark Mode Theme

From Fabric v9.2.0, support for the dark mode theme is provided. This feature reduces the light that is emitted by device screens while maintaining the minimum color contrast ratios required for readability.

You can click the toggle button to select the dark mode theme as per your preference.

Figure 2: Dark Mode Toggle option



Once the option is selected, the dark mode theme changes the style of all scrollbars, chart backgrounds, legends & labels, investigation view, dropdown, pop over, filters, tables related to all the activities and text colors, and so on. The applied theme is reflected immediately; there is no needs to start a new session.

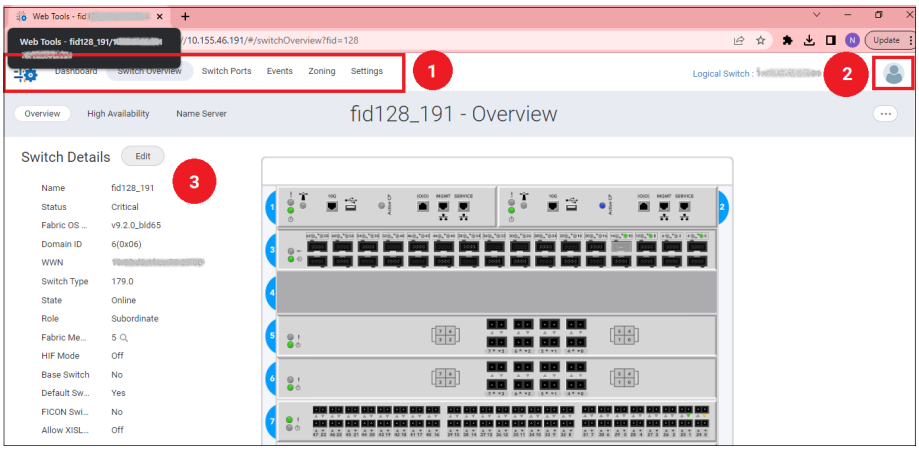
NOTE
The exported files, such as PDF or HTML files, will remain in a classic view format.

Overview of the Web Tools User Interface

Once familiar with the basic components of Web Tools, you can quickly start monitoring and managing your switch.

The following screenshot shows the basic layout of the Web Tools user interface.

Figure 3: Web Tools User Interface

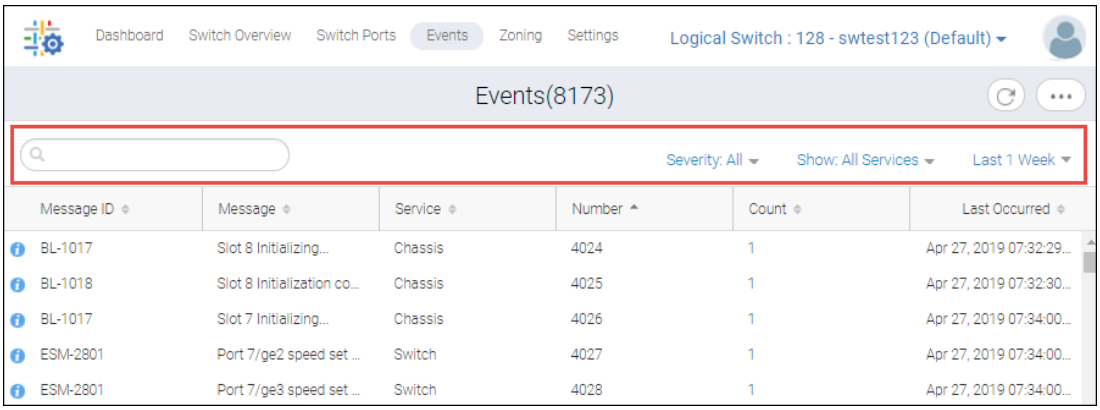


1. Navigation bar. Contains links to feature pages.
2. Profile menu. Displays the link for logging out.
3. Subnavigation bar. Provides the page title and includes buttons and menus to take action within the page.

NOTE
From Fabric OS v9.2.0, the browser's title bar displays the switch name and switch IP address.

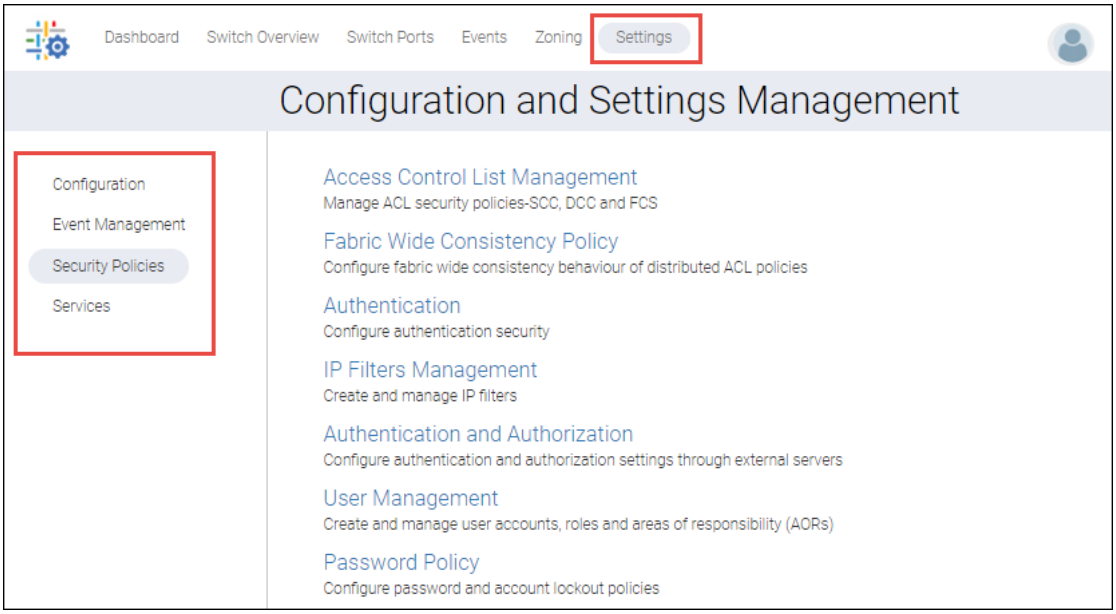
In addition, some pages include a filter bar for searching and filtering the displayed content.

Figure 4: Filter Bar



The **Settings** page contains navigation options on the left side of the page. Clicking each item on the left navigation bar displays additional options. For example, to configure user accounts, click **Settings** > **Security Policies** > **User Management**.

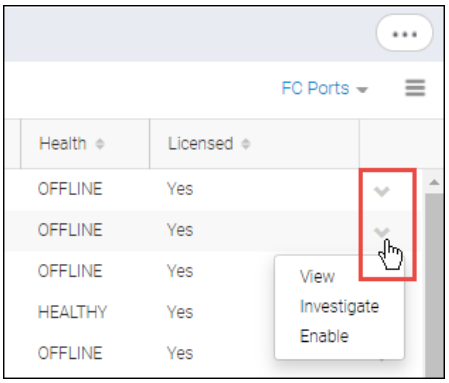
Figure 5: Settings Page



Tables

Some tables have an action menu that you can access by clicking the down arrow in the rightmost column. Click this arrow to display additional actions that you can perform on the associated object.

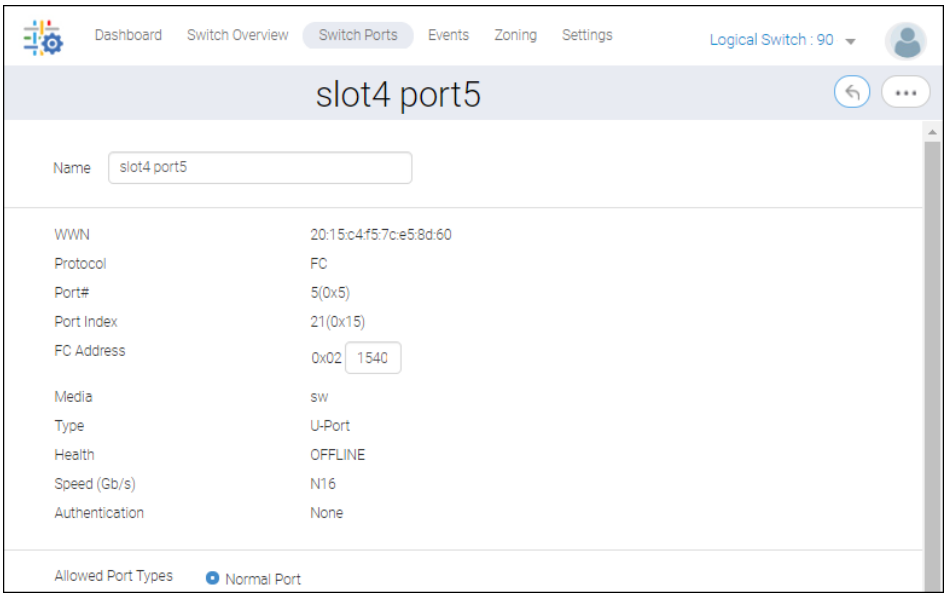
Figure 6: Using the Down Arrow to Display Additional Actions



Detail Pages

Clicking **View** in the action menu opens a detail page for that object. You can also open the detail page by clicking the name of the object in the table. The detail page displays additional information about the object and may contain additional actions that you can perform.

Figure 7: Detail Page for a Switch Port



Configuring a New Switch

To configure a new switch, perform the following steps:

1. Assign an IP address.
2. Launch Web Tools directly from a Web browser or from SANnav Management Portal. For detailed information, see Launching Web Tools.
3. Enter the user name, password, and logical switch name or fabric ID (FID) to log in to the switch.
4. Install the required license.
   For detailed information, see Adding a License.

Licensing Overview

The **License** tab allows you to view the licenses installed on the switch with the feature name, serial number, supported count, and expiry date details. It allows you to set and manage the licenses.

Licenses that are required for accessing specific Fabric OS features are known as feature licenses. The following table lists the platforms and the supported license types:

Platforms	License Types
Gen 7	Certificate
Gen 6+ or Gen 7 upgraded	Certificate/Key
Gen 6	Key

NOTE
The serial number field is applicable only for Gen 6+ and Gen 7 platforms.

Web Tools supports the following license types:

- Universal time-based licensing
  Web Tools supports universal time-based licensing. Each universal key is for a single feature, and the key can be used on any product that supports the feature for a defined trial period. At the end of the trial period, the feature is disabled. You can extend the universal key license. For time-based licenses, **Expiry Date** displays in the **License Management** table.
  The following features are supported for universal time-based licensing:
  - Extended Fabric
  - Fabric Vision
  - FICON Management Server (CUP)
  - Trunking
- Capacity-based licensing
  This license type is for a feature that has a scale or count parameter such as the count of additional ports or towers allowed. The capacity-based license that is installed is overwritten by any new license for the same feature that is subsequently installed. For capacity-based licenses, **Supported Count** displays in the **License Management** table and shows the number of supported ports.
  The following features are supported for capacity-based licensing:
  - Ports on demand
  - Double density ports on demand
  - Q flex license
  - Integrated Routing (IR) ports on demand license

For detailed information on licensing, refer to the *Brocade Fabric OS Software Licensing User Guide*.

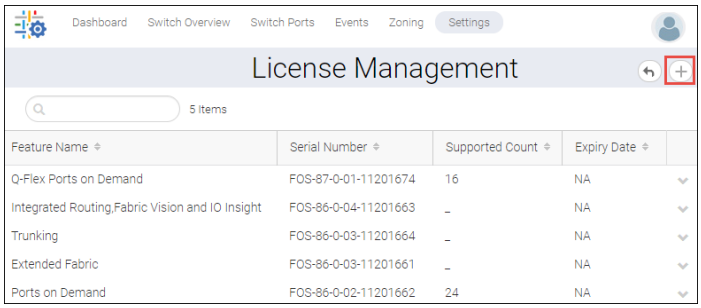
Adding a License

This section explains the process of adding a license in the **License Management** window.

You can add a license in the **License Management** window either by importing it from a file or by entering the license key. Refer to the *Brocade Fabric OS Software Licensing User Guide* for the type of license that a platform accepts.

To add a license, perform the following steps:

1. Click **Settings** from the navigation bar, and then select **License** from the **Services** tab. The **License Management** window is displayed.

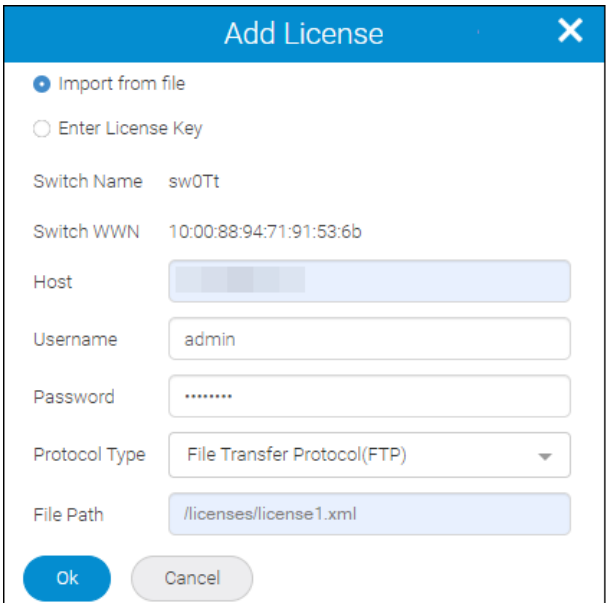


2. Click the plus sign (+) icon on the top-right corner of the **License Management** window. The **Add License** window is displayed.
3. Select any one of the options (**Import from file** / **Enter License Key**) to add a license.
   a) **Import from file**

      To import a license certificate from a file, perform the following steps:

      1. Select the **Import from file** option.
      2. Enter the host IP address, login credentials (SCP, SFTP, or FTP login credentials) and protocol type (SCP, SFTP, or FTP).
      3. Enter the file path. In a Linux-based system, provide the full path of the SCP or SFTP root directory. For example, `/home/user1` is the root directory for SCP running on a Linux host logged in with `user1`; if the license is present in `/home/user1/licenses/license1.xml`, then enter the file path as `/home/user1/licenses/license1.xml`. In a Windows-based system, enter the file path after the FTP root directory. For example, if a Windows FTP root folder is `c:/users/user1/ftproot/` and the license is present in `c:/users/user1/ftproot/licenses/license1.xml`, then enter the file path as `/licenses/license1.xml`.

      Figure 8: Add License



b) **Enter License Key**

To enter a license key, perform the following steps:

1. Select the **Enter License Key** option.
2. Enter the license key in the **Enter License Key** field.

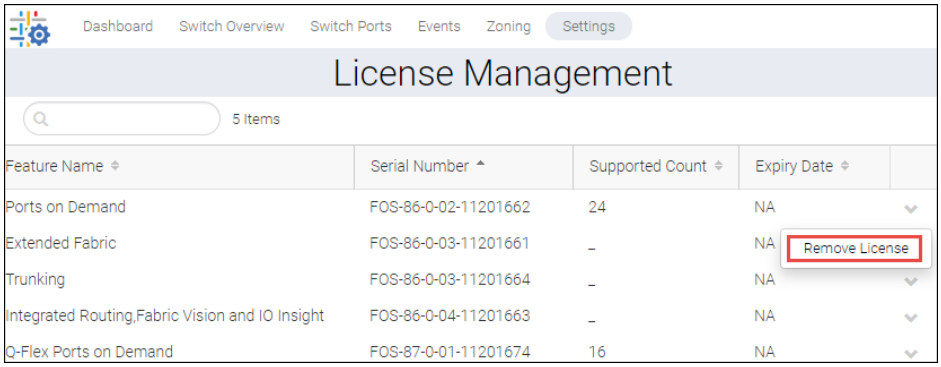
4. Click **OK**.

The license is added and displayed under the **License Management** window.

Removing a License

To remove a license, perform the following steps:

1. Click **Settings** from the navigation bar, and then select the **License Management** from the **Services** tab. The **License Management** window is displayed.
2. Click the ( ) icon next to the license that you want to remove, and then click **Remove License**. The **Delete License** window is displayed.



3. Click **OK**. The license is removed from the **License Management** window.

Security

This section describes various configuration policies such as the access control list policy, fabric wide consistency policy, and authentication policy. This section also includes IP filter management, remote authentication and authorization, and user and password management.

Access Control List Policy Configuration

Access control lists (ACLs) are filters that allow you to control which routing packets are permitted or denied. The reason to configure ACLs is to provide security for your network.

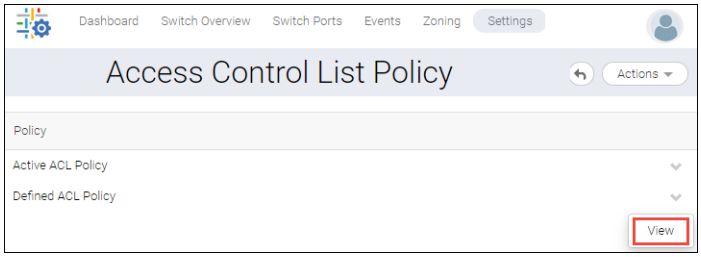
Each supported ACL policy is identified by a specific name, and only one policy of each type can exist, except for DCC policies. Policy names are case-sensitive and must be entered in all uppercase.

The following are the supported ACL policies in Fibre Channel networking.

- Fabric configuration server (FCS) policy – This policy decides which switch can change the configuration of the fabric.
- Device connection control (DCC) policy – This policy decides which Fibre Channel device ports can connect to the respective Fibre Channel switch ports.
- Switch connection control (SCC) policy – This policy decides the connection between switches.

Creating and Activating an SCC, a DCC, or an FCS Policy

1. Select **Settings** > **Security Policies**, and then select **Access Control List Policy**. The **Access Control List Policy** window is displayed.
2. Click the ( ) icon next to the **Defined ACL Policy**, and then select **View**. The **Defined ACL Policy** window is displayed.



3. You can create SCC, DCC, and FCS policies in the **Defined ACL Policy** window. To create these policies, perform the following steps:
   a) In **Switch Connection Control Policy**, select **Create SCC policy having all switches in fabric** to include all the switches in the fabric, or click **Add** to select a particular switch in a fabric. You can add the switches either by selecting them from the available list or by manually entering them.
   b) In the **Device Connection Control Policy**, select **Create unique policy for each port** to include all ports, or click **Add** to select a particular port. Enter a name for the device connection control policy. You can add the WWN ports either by selecting them from the available list or by manually entering them.

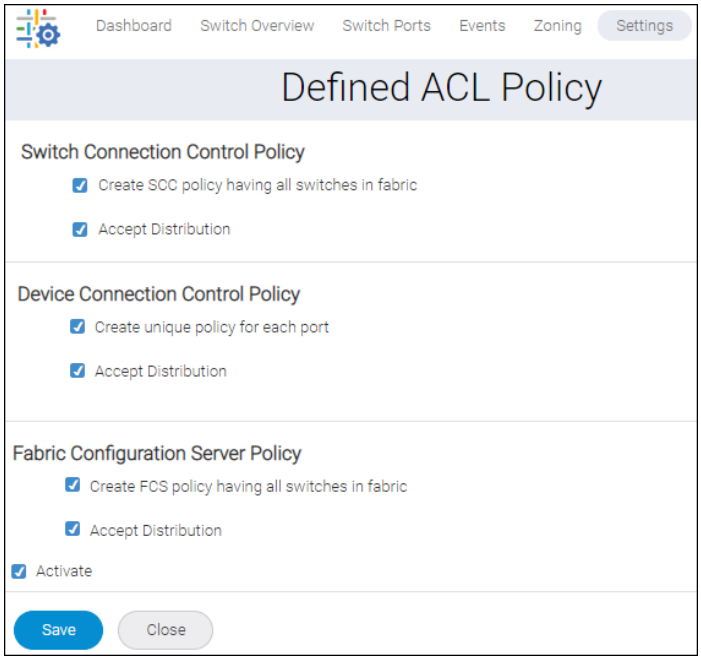
NOTE

- You must prefix the name of the device connection control policy with DCC_Policy_.
- The device connection control name must be unique.
- For the DCC policy, the **Domain, Port Index** type is supported only for local ports on the switch that is managed by Web Tools.

c) In **Fabric Configuration Server Policy**, select **Create FCS policy having all switches in fabric** to include all switches in the fabric, or click **Add** to select a particular switch in fabric. You can add the switches either by selecting them from the available list or by manually entering them.

NOTE
If a policy is already created or exists in the switch database, you cannot automatically create an SCC, a DCC, or an FCC policy.

4. Select **Accept Distribution** to distribute the SCC, DCC, or FCS policies to the FOS switches. You can distribute a policy to a fabric after a policy is created or modified.



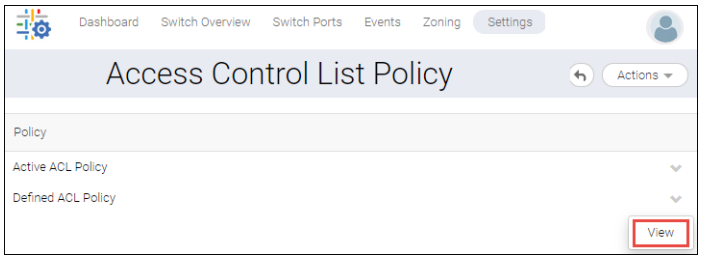
NOTE

- All the policies can be distributed from a primary FCS only when the FCS policy is enabled.
- You must select **Accept Distribution** to distribute a policy from the **Active ACL Policy** window.

5. Select **Activate** to activate all the policies. You can view the active policies under the **Active ACL Policy** window.
6. Click **Save**.

Configuring an SCC, a DCC, or an FCS Policy

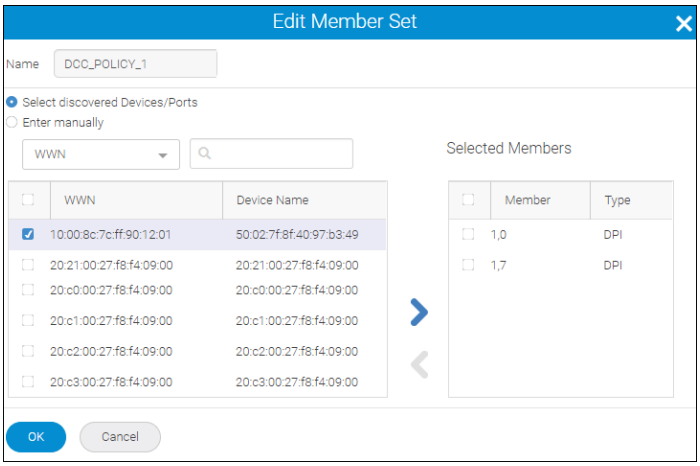
1. Click **Settings** in the navigation bar, and then select **Security Policies** > **Access Control List Policy**. The **Access Control List Policy** window is displayed.
2. Click the ( ) icon next to the **Defined ACL Policy**, and then select **View**. The **Defined ACL Policy** window is displayed.



3. Perform the following steps to configure an ACL policy.

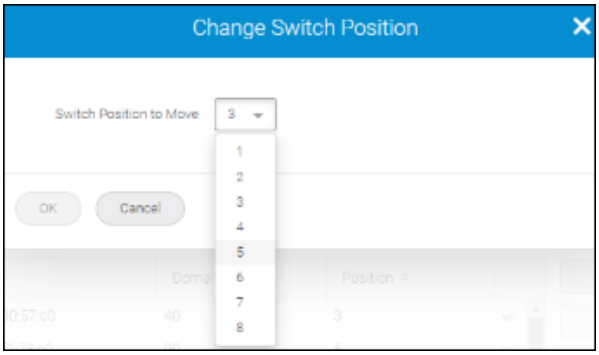
   NOTE
   You cannot configure an SCC policy.

   a) To configure a DCC policy, click the ( ) icon next to a DCC policy, and then select **Configure**. The **Edit Member Set** window is displayed. Make the changes based on your requirements.



   NOTE
   You cannot rename a DCC policy.

   b) To configure an FCS policy, click the ( ) icon next to an FCS policy, and then select **Configure**. The **Change Switch Position** window is displayed. You can change the position of a switch in a fabric by selecting the position from the **Switch Position to Move** drop-down.



   NOTE

   - The total number of switch positions is based on the number of configured switches in the FCS policy.
   - You can move the position of a primary switch in the FCS policy.

You can remove the switches, member set, and fabric from an SCC, a DCC, and an FCS policy respectively by selecting the **Remove** option.

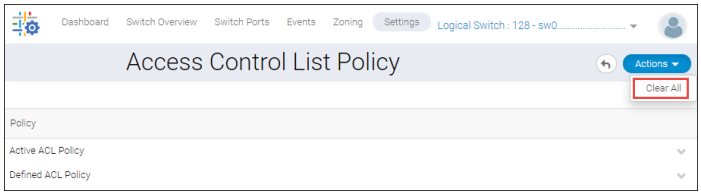
4. Click **OK**.

Deleting an SCC, a DCC, and an FCS Policy

NOTE
You cannot delete the FCS policy from non-primary or non-FCS switches.

To delete ACL policies, perform the following steps:

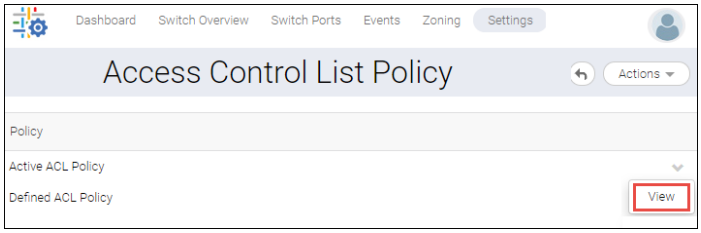
1. Click **Settings** in the navigation bar, and then select **Security Policies** > **Access Control List Policy**. The **Access Control List Policy** window is displayed.
2. Select **Clear All** from the **Actions** menu. This option deletes all the ACL policies.



Distributing an SCC, a DCC, or an FCS Policy

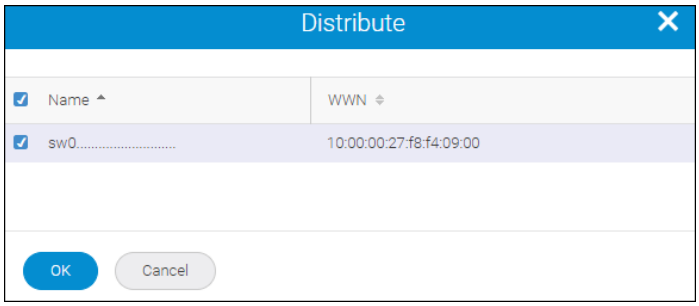
You can distribute an SCC, a DCC, or an FCS policy from the **Active ACL Policy** window. You must select the **Accept Distribution** option in the **Defined ACL Policy** window to distribute the SCC, DCC, or FCS policies to the Fabric OS switches.

1. Click **Settings** in the navigation bar, and then select **Security Policies** > **Access Control List Policy**. The **Access Control List Policy** window is displayed.
2. Click the ( ) icon next to the **Active ACL Policy**, and then select **View**. The **Active ACL Policy** window is displayed.



NOTE
The SCC and DCC policies can be distributed only for a primary switch.

3. Select **Distribute** from the SCC, DCC, or FCS policy.
4. Select the switches to which you want to distribute the ACL policy.



5. Click **OK**.

Fabric Wide Consistency Policy Configuration

The Fabric Wide Consistency Policy (FWCP) configures the fabric-wide consistency behavior for the activated access control list (ACL) policies. The FWCP ensures that all switches in the fabric enforce the same policies. You can set either the `Strict` or `Tolerant` FWCP policy for each SCC, DCC, and FCS policy. If a fabric-wide consistency policy is not set, the policies are managed on a per-switch basis.

To set the FWCP for an SCC, a DCC, or an FCS policy, perform the following steps:

1. Click **Settings** in the navigation bar, and then select **Security Policies** > **Fabric Wide Consistency Policy**. The **Fabric Wide Consistency Policy** window is displayed.
2. Select **Absent**, **Strict**, or **Tolerant** consistency behavior for each policy and click **Save**.

NOTE
You must select strict consistency behavior for FICON.

Authentication Policy Configuration

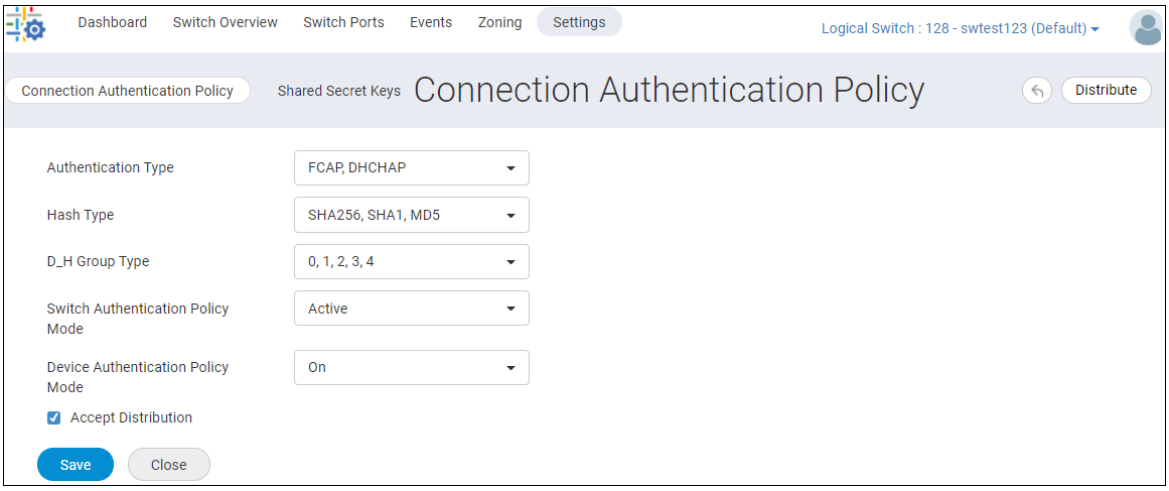
You can configure an authentication protocol policy for E_Ports and F_Ports and can distribute the policy to other switches in the fabric. You may set shared keys for configured authentication policies.

The following table describes the switch authentication policy parameters that are configured for different ports.

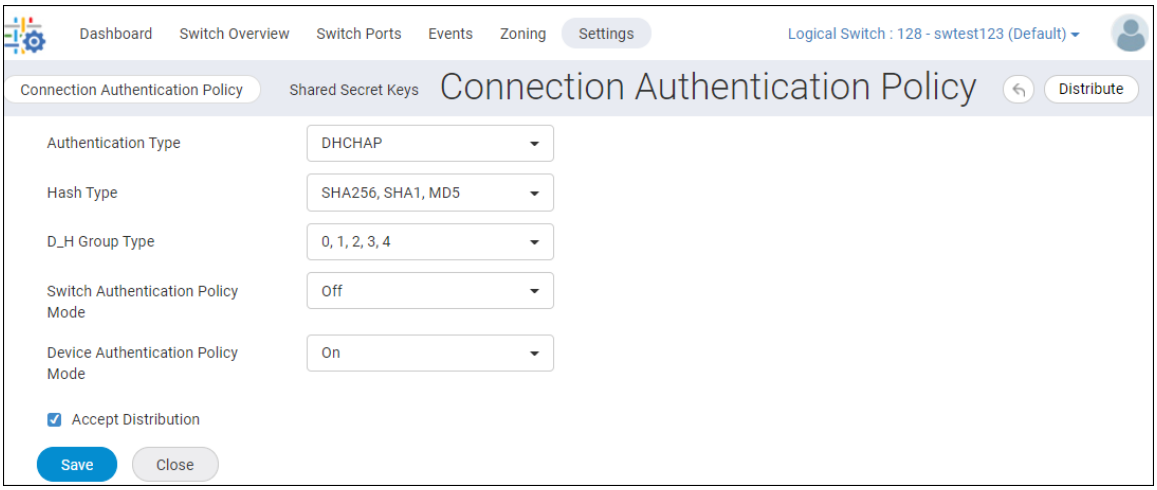
Policy Mode	Description
Authentication Type	The following authentication types are allowed: • FCAP, DHCHAP • DHCHAP • FCAP
Hash Type	The hash functions, such as `SHA1` , `SHA256` , or `MD5` , are used for authentication.
D_H Group Type	The following D_H group types are allowed: • 0,1,2,3,4 • 0 (DH Null option) • 1 (1024-bit key) • 2 (1280-bit key) • 3 (1563-bit key) • 4 (2048-bit key)
Switch Authentication Policy Mode	The following switch authentication policy modes are allowed: • Passive – The switch does not initiate authentication but participates if the connecting switch initiates an authentication. • Active – The switch is more tolerant and can be connected to a switch with any type of policy. During switch initialization, authentication is initiated on all E_Ports, but the port is not disabled if the connecting switch does not support the authentication or the authentication policy is turned off. • On – A strict authentication is enforced on all E_Ports. The authentication handshaking is performed before the switches exchange the fabric parameters (EFP) for E_Port. Regardless of the policy, E_Port is disabled if the DHCHAP or FCAP protocol fails to authenticate each other. • Off – The switch does not support the authentication. Any authentication negotiation is rejected.
Device Authentication Policy Mode	The following device authentication policy modes are allowed: • Passive – The device does not initiate authentication but participates if the connecting device initiates an authentication. • On – A strict authentication is enforced on all devices. • Off – The device does not support authentication. Any authentication negotiation is rejected.

Configuring and Distributing an Authentication Policy for E_ Ports and F_Ports

1. Click **Settings** in the navigation bar, and then select **Security Policies** > **Connection Authentication Policy**. The **Connection Authentication Policy** window is displayed.
2. To configure an authentication policy for E_Ports, perform the following steps:
   a) Select **Authentication Type** as FCAP or DHCHAP.
   b) Select values for the **Hash Type** and **D_H Group Type** parameters.
   c) Select **Switch Authentication Policy Mode** as **Passive** or **Active** or **On** or **Off**.
   d) Select **Device Authentication Policy Mode** either as **Off** or as **Passive**.

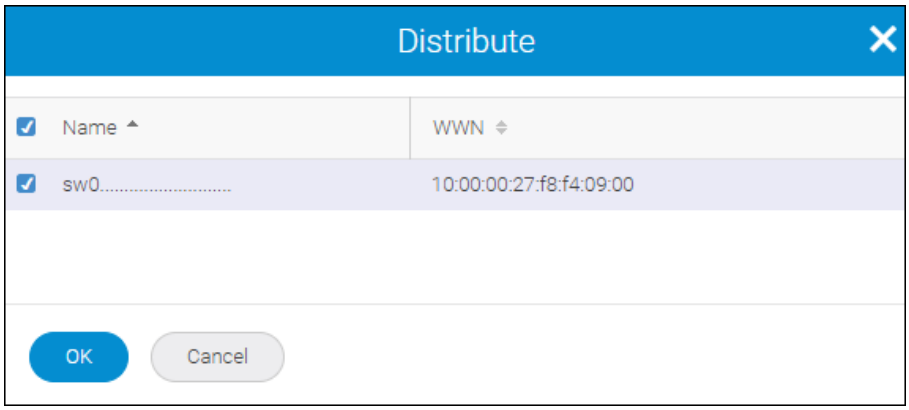


3. To configure an authentication policy for F_Ports, perform the following steps:
   a) Select **Authentication Type** as DHCHAP.
   b) Select values for the **Hash Type** and **D_H Group Type** parameters.
   c) Select **Switch Authentication Policy Mode** either as **Passive** or as **Off**.
   d) Select **Device Authentication Policy Mode** as **Passive** or **On** or **Off**.



4. Select **Accept Distribution** to distribute the policy to the Fabric OS switches.
5. Click **Save**.
6. Select **Distribute** to distribute the authentication policy to the selected switches. The **Distribute** window is displayed.

   Authentication policies are distributed only if all selected switches accept the distribution. Only the policy mode is distributed to the selected switches. The switch that initiates the distribution must accept the distribution.



7. Select the switch, and then click **OK**.

Setting a Shared Secret Key Pair

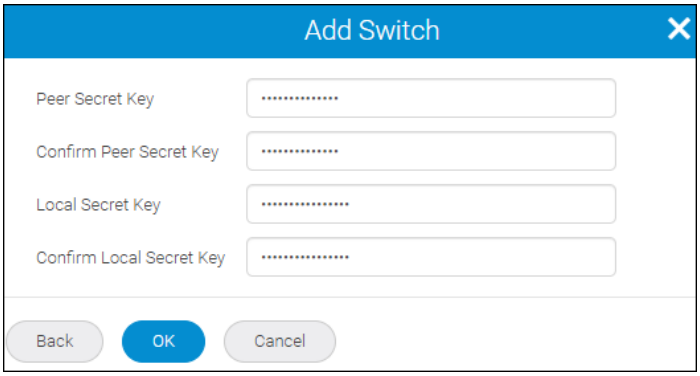
A shared secret key is data that is known to only the entities that are involved in communication so that any party's possession of that data can be provided as proof of identity for authentication. DHCHAP requires a shared secret key pair between two entities to authenticate with each other. A key pair consists of a local secret and peer secret keys. The local secret key identifies the local switch, and the peer secret key identifies the entity to which the local switch may authenticate.

NOTE

Web Tools does not support adding DHCHAP secret key for a switch that is not present in the regular fabric such as an edge fabric. In this scenario, you must use the `secAuthSecret –set` CLI command.

To set a shared secret key pair, perform the following steps:

1. Click **Settings** in the navigation bar, and then select **Security Policies** > **Authentication**. The **Authentication Policy** window is displayed.
2. Select the **Shared Secret Keys** tab.
3. Click **Add**. The **Add Switch** window is displayed. The **Add Switch** window displays the switches that are available in the fabric.
4. Select the switch, and then click **Next**.
5. In the **Add Switch** window, perform the following steps:
   a) Enter a value for **Peer Secret key** and **Confirm Peer Secret Key** fields.
   b) Enter a value for **Local Secret key** and **Confirm Local Secret Key** fields.
   c) Click **OK**.

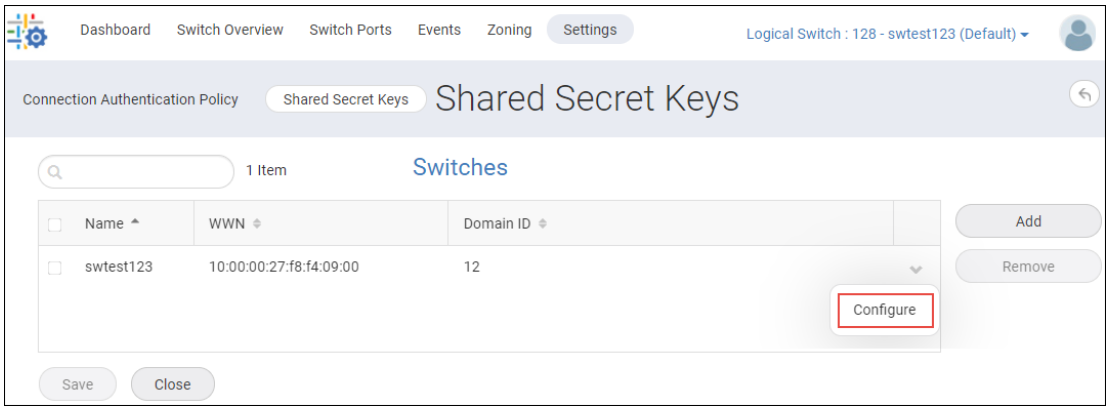


Modifying a Shared Secret Key Pair

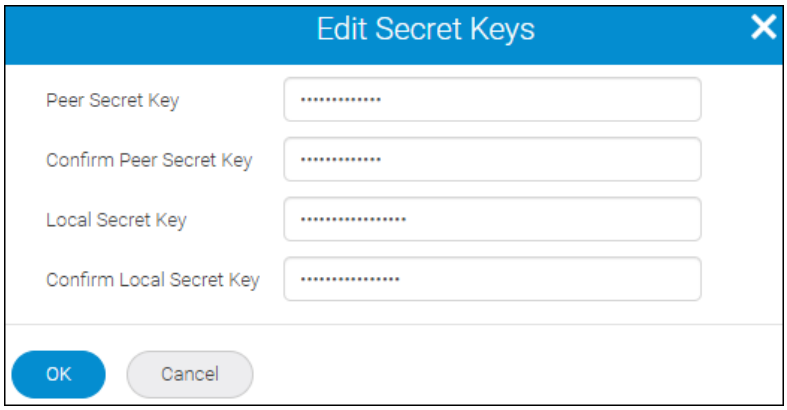
You can modify the secret key pairs in the switch.

To modify a shared secret key pair, perform the following steps:

1. Click **Settings** in the navigation bar, and then select **Security Policies** > **Connection Authentication Policy**. The **Connection Authentication Policy** window is displayed.
2. Click the **Shared Secret Keys** tab.



3. Click the ( ) icon next to a switch, and then select **Configure**.
   The **Edit Secret Keys** window is displayed.
4. Make the appropriate changes and click **OK**.



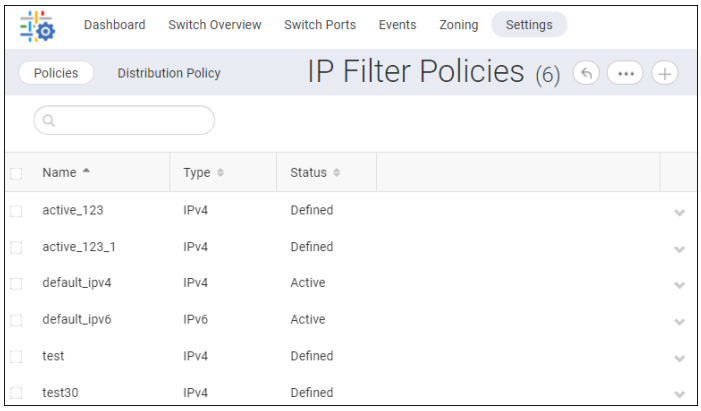
IP Filter Management

The IP filter policy sets up a packet filtering firewall to provide access control on the management IP interface. It allows you to manage and configure the IP filters. The IPv4 and IPv6 policies are either in the defined configuration or in the active configuration.

Configuring IP Filters

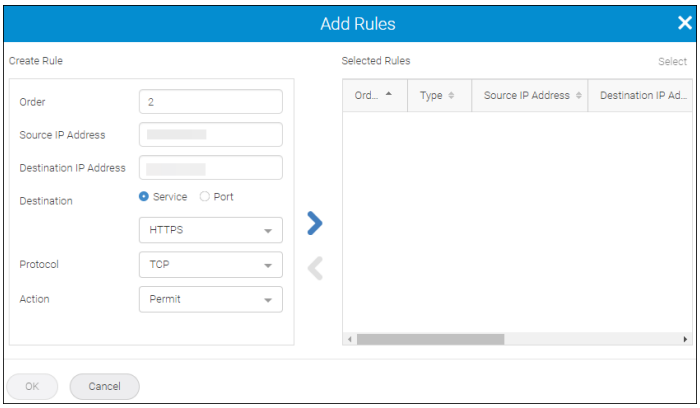
To configure IP filters, perform the following steps:

1. Click **Settings** in the navigation bar, and then select **Security Policies** > **IP Filters Management**.



   The **IP Filter Policies** window is displayed.

2. In the **Policies** tab, click the (**+**) icon on the top-right corner of the window. The **Create New Policy** window is displayed.
3. In the **Create New Policy** window, perform the following steps:
   a) Enter the policy **Name** and select a policy **Type** (IPv4 or IPv6).
   b) Click **Add** to add the rules to create an IP filter. The **Add Rules** window is displayed.
   c) Enter the rule **Order**, **Source IP Address**, and **Destination IP Address**. Select the rule **Destination**, **Protocol**, and **Action**. Select **Destination** either as **Service** or as **Port**.



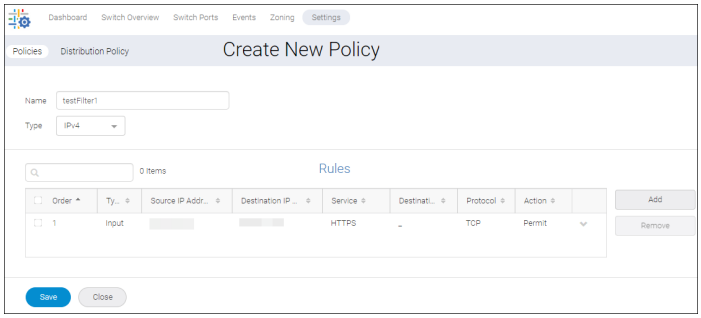
NOTE

- The order must be unique and in an incremental order.
- Only the source IP address is required for the input rule type.
- The rules are processed in a top-down sequence when the policy is activated.

d) Click the (›) icon to move the rules to the **Selected Rules** area.

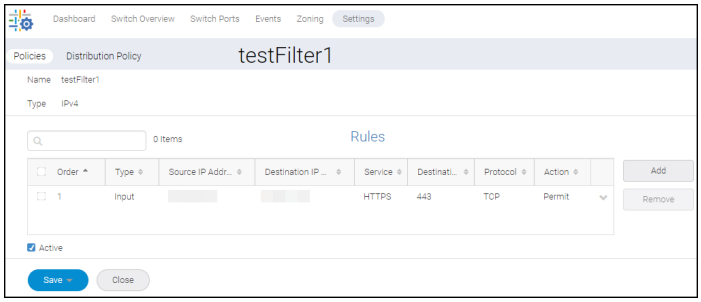
e) Click **OK**. The new rules are added under the **Rules** table.

4. Click **Save** to create an IP filter policy.



The IP filter policy is saved under the **IP Filters Policies** window with the **Defined** status.

5. Select the IP filter policy that you want to activate, and then select the **Active** checkbox.



To delete a rule, click the (⌄) icon next to a rule, and then select the **Remove** option.

NOTE

- The following actions are supported while adding or deleting IP filter policy rules:
  - You can add one or more rules in a single operation.
  - You can delete only one rule at a time.
- You cannot add and delete rules at the same time. If a combination of add and delete operations are required, you must perform the following:

– Group all the add operations together.
– Delete each operation individually.

NOTE

- You can activate only one IP filter policy per IPv4 and IPv6.
- There can be a maximum of six policies in the defined configuration and one policy per IPv4 and IPv6 type in the active configuration apart from the default policies.
- The policy to be activated replaces the existing active policy of the same type.

6. Click **Save** from the **Save** drop-down. The active IP filter policy is displayed under the **IP Filters Policies** window with the **Active** status. You can enforce the IP filters only after activating them.

NOTE
By using the **Save As** option from the **Save** drop-down, you can do the following:

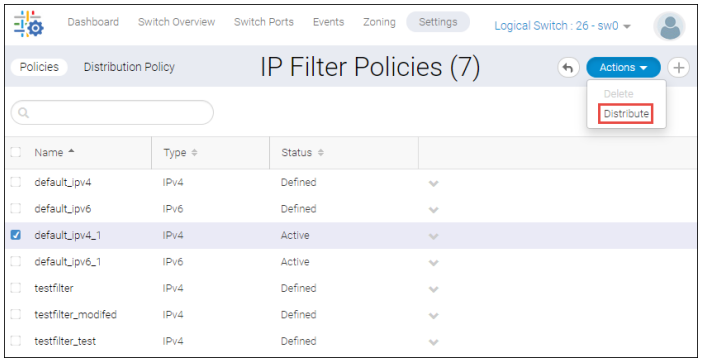
- Create an IP filter policy from the already existing policies.
- Clone a policy by renaming it.

Distributing an IP Filter Policy

IP filters are rules that are defined to either discard or permit packets through a switch or a fabric. IP filtering matches a filter rule to data traffic based on any combination of IP source or destination. IP filtering can control traffic being routed to a switch or fabric.

To distribute an IP filter policy, perform the following steps:

1. Click **Settings** in the navigation bar, and then select **Security Policies** > **IP Filters Management**. The **IP Filter Policies** window is displayed.
2. Select the IP filter policies that you want to distribute. You can distribute only active IP filter policies.



3. Select **Distribute** from the **Actions** menu. The **Distribute** window is displayed.
4. Select the switch to which you want to distribute the policy, and then click **OK**. The IP filter policy is distributed to the switch.

Deleting an IP Filter Policy

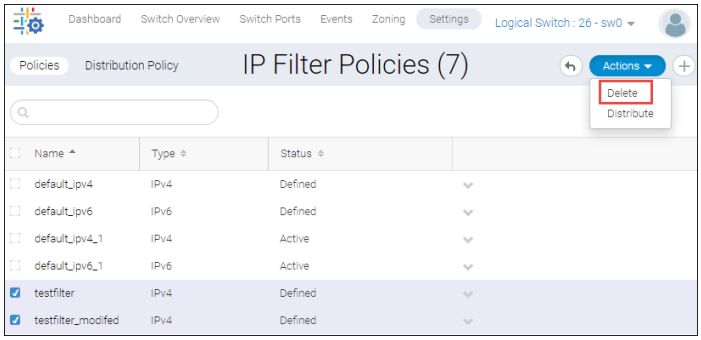
You can delete an IP filter policy that you created. You cannot delete a default IP filter policy. Deleting an IP filter policy removes it from the temporary buffer.

To delete an IP filter policy, perform the following steps:

1. Click **Settings** in the navigation bar, and then select **Security Policies** > **IP Filters Management**. The **IP Filter Policies** window is displayed.
2. Select the IP filter policies that you want to delete.

   NOTE
   You cannot delete an active IP filter policy.

3. Select **Delete** from the **Actions** menu.



   The **Delete** window is displayed.

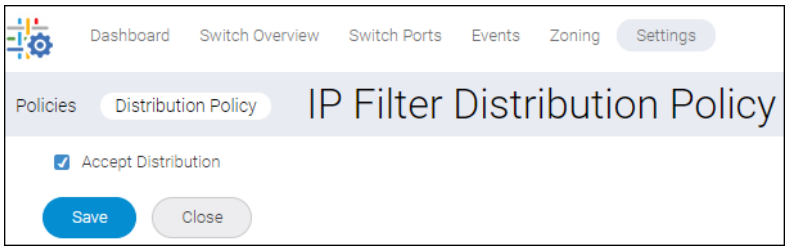
4. Click **OK**. The IP filter policies are deleted.

Enabling an IP Filter Distribution Policy

The IP filter distribution policy is used to set the policy to accept or reject distributions of an IP filter policy.

To enable the distribution of an IP filter policy, perform the following steps:

1. Click **Settings** in the navigation bar, and then select **Security Policies** > **IP Filters Management**. The **IP Filter Policies** window is displayed.
2. Click the **Distribution Policy** tab. The **IP Filter Distribution Policy** window is displayed.



3. Select the **Accept Distribution** checkbox, and then click **Save**.

Remote Authentication and Authorization

You can configure Web Tools to use an external server for authentication of user names and passwords. Web Tools supports the following types of external servers for authentication and authorization:

- RADIUS
- LDAP
- TACACS+

Remote Authentication Configuration Using a RADIUS Server

Fabric OS supports the RADIUS authentication, authorization, and accounting (AAA) service. When configured for RADIUS, the switch becomes a network access server (NAS) that acts as a RADIUS client. The switch sends all AAA service requests to the authentication server. The authentication server receives the request, validates it, and sends its response back to the switch. In this configuration, authentication records are stored in the RADIUS authentication server. Login and logout account name, assigned role, and time accounting records are also stored on the RADIUS authentication server.

You must set up the RADIUS authentication server through SSH to protect the shared secret.

The following are the three choices in the drop-down when RADIUS is selected as the primary service:

- **Switch Database when RADIUS authentication failed** – When selected, the switch user login database is used for authentication whenever RADIUS authentication fails.
- **Switch Database when RADIUS Timeout** – The switch user login database is checked only if the physical connection to the RADIUS authentication server fails.
- **None** – The switch user login database is never used for authentication. Only a RADIUS authentication server can be used for authentication.

If the switch database is selected as primary, there is no secondary option. The RADIUS authentication server cannot be configured as a backup for the switch user login database.

When the RADIUS login fails, even though the RADIUS authentication server is available, the additional service allows you the option to use the switch database as a backup authentication service. Alternatively, you can have no secondary AAA service, which means that only the primary service is used for authentication.

Configuring and Enabling Remote Authentication Using a RADIUS Server

The configuration of remote authentication using RADIUS is chassis-based, so it applies to all logical switches (domains) on the switch, and it is replicated on a standby CP if one is present. The configuration is saved in a configuration upload, and it can be applied to other switches in a configuration download. You should configure at least two RADIUS servers so that if one fails, the other server assumes the service. At least one RADIUS server must be configured before you enable the RADIUS server.

You can configure five RADIUS servers. You must be logged in as admin, switchadmin, or securityadmin to configure a RADIUS server.

To configure and enable remote authentication using RADIUS, perform the following steps:

1. Click **Settings** from the navigation bar, and then select **Security Policies** > **Authentication and Authorization**.
2. Select **RADIUS Server** as the **Primary Authentication**.
3. Select **Switch Database when RADIUS authentication failed**, **Switch Database when RADIUS Timeout**, or **None** from the **Secondary Authentication** list.

   The **RADIUS Server** list is displayed.
4. Click **Add**.

   The **Add Server** window is displayed. You can configure up to five RADIUS servers. If all five RADIUS servers are already configured, the **Add** button is disabled.
5. In the **Add Server** window, perform the following:
   a) Enter the **Host** name.

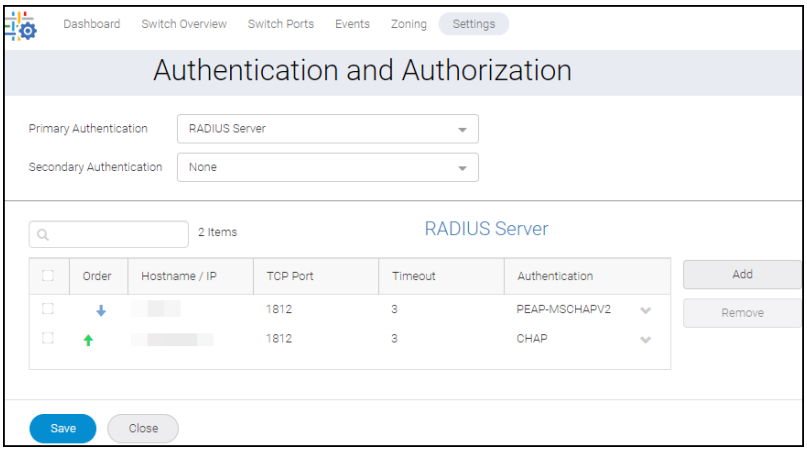
      The host name must be a valid IP address (in either IPv4 or IPv6 format) or an FQDN string. Each RADIUS server must have a unique IP address or DNS name.

b) Enter the **Port** number, the **Timeout(s)** in seconds, and **Secret String**.

By default, the port number is 1812, timeout is 3 seconds, and secret string is sharedsecret.

c) Select **CHAP**, **PAP,** or **PEAP-MSCHAPV2** as the authentication protocol.

By default, the value is **CHAP**.



You can rearrange the RADIUS servers by clicking the up arrow or down arrow in the **Order** column.

d) Click **OK** to return to the **RADIUS Server** window.

6. Click **Save** to enable the RADIUS server.

NOTE

- To modify an already configured RADIUS server, click the down arrow next to a server, and then select **Configure**.
- To disable RADIUS, select **Switch Database** from the **Primary Authentication** list.

Removing a RADIUS Server

To remove a RADIUS server, perform the following steps:

1. Click **Settings** from the navigation bar, and then select **Security Policies** > **Authentication and Authorization**.
2. Select **RADIUS Server** as the **Primary Authentication**. The **RADIUS Server** list is displayed.
3. Click the ( ) icon next to a RADIUS server from the **RADIUS Server** list.
4. Click **Delete**.

   If there is no RADIUS server that is configured, the **Delete** button is disabled.

   A confirmation dialog is displayed asking whether you want to remove the RADIUS server.
5. Click **OK** to delete the RADIUS server.

Remote Authentication Configuration Using a TACACS+ Server

Fabric OS can authenticate users with a remote server using the Terminal Access Controller Access-Control System Plus (TACACS+) protocol. This protocol is used in AAA server environments consisting of a centralized authentication server and multiple network access servers (NASs) or clients. When configured to use TACACS+, a Brocade switch acts as a NAS.

The following are the three choices in the drop-down when TACACS is selected as the primary service:

- **Switch Database when TACACS authentication failed** – When selected, the switch user login database is used for authentication whenever TACACS authentication fails.
- **Switch Database when TACACS Timeout** – The switch user login database is checked only if the physical connection to the TACACS authentication server fails.
- **None** – The switch user login database is never used for authentication. Only a TACACS authentication server can be used for authentication.

The following authentication protocols are supported by the TACACS+ server for the user authentication:

- Password Authentication Protocol (PAP)
- Challenge Handshake Authentication Protocol (CHAP)

Configuring and Enabling Remote Authentication Using a TACACS+ Server

At least one TACACS+ server must be configured before you can enable TACACS+.

NOTE
The TACACS+ password expiration message is not displayed during the login from Web Tools.

To configure and enable TACACS+, perform the following steps:

1. Click **Settings** from the navigation bar, and then select **Security Policies** > **Authentication and Authorization**.
2. Select **TACACS+ Server** as the **Primary Authentication**.
3. Select **Switch Database when TACACS authentication failed**, **Switch Database when TACACS Timeout**, or **None** from the **Secondary Authentication** list.

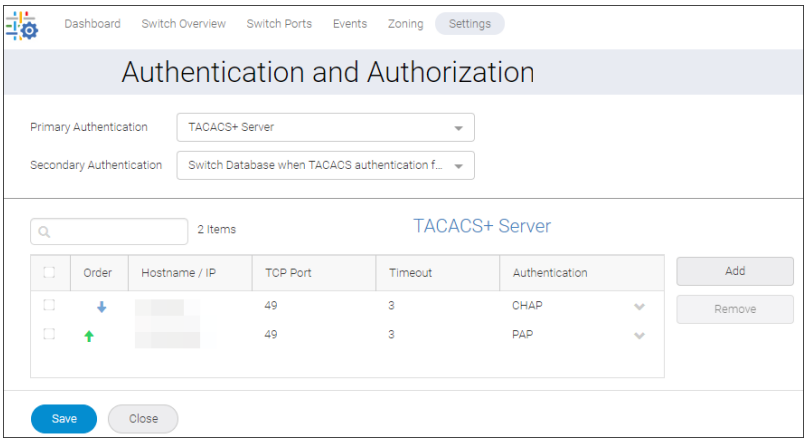
   The **TACACS+ Server** list is displayed.
4. Click **Add**.

   The **Add Server** window is displayed. You can configure up to five TACACS+ servers. If all five TACACS+ servers are already configured, the **Add** button is disabled.
5. In the **Add Server** window, perform the following:
   a) Enter the **Host** name.

      The host name can be a valid IP address (in either IPv4 or IPv6 format) or an FQDN string. Each TACACS+ server must have a unique IP address or DNS name.
   b) Enter the **Port** number, **Timeout(s)** in seconds, and **Secret String**.

      By default, the port number is 49, the timeout is 3 seconds, and the secret string is sharedsecret.
   c) Select either **CHAP** or **PAP** as the authentication protocol.

      By default, the value is **CHAP**.



You can rearrange the order of the TACACS+ servers by clicking the up or down arrow in the **Order** column.

d) Click **OK** to return to the **TACACS+ Server** window.

6. Click **Save** to enable the TACACS+ server.

NOTE

- To modify an already configured TACACS+ server, click the down-arrow next to a server, and then select **Configure**.
- To disable TACACS+, select **Switch Database** from the **Primary Authentication** list.

Removing a TACACS+ Server

To remove a TACACS+ server, perform the following steps:

1. Click **Settings** from the navigation bar, and then select **Security Policies** > **Authentication and Authorization**.
2. Select **TACACS+ Server** as the **Primary Authentication**.
3. Click the ( ) icon next to a TACACS+ server from the **TACACS+ Server** list.
4. Click **Delete**.

   If there is no TACACS+ server that is configured, the **Delete** button is disabled.

   A confirmation dialog is displayed asking whether you want to remove the TACACS+ server.
5. Click **OK** to delete the TACACS+ server.

Remote Authentication Configuration Using an LDAP Server

LDAP provides user authentication and authorization using the Microsoft Active Directory service or using OpenLDAP. This section describes the configuration of authentication and authorization using the Active Directory service.

The following are the three choices in the drop-down when LDAP is selected as the primary service:

- **Switch Database when LDAP authentication failed** – When selected, the switch user login database is used for authentication whenever LDAP authentication fails.
- **Switch Database when LDAP Timeout** – The switch user login database is checked only if the physical connection to the LDAP authentication server fails.
- **None** – The switch user login database is never used for authentication. Only an LDAP authentication server can be used for authentication.

If the switch database is selected as primary, there is no secondary option. The LDAP authentication server cannot be configured as a backup for the switch user login database.

Configuring and Enabling Remote Authentication Using an LDAP Server

To add a new LDAP server, you must provide the server IP address, port number, timeout value, and base domain, and you must choose LDAP as the authentication protocol. The server IP address may be in either IPv4 or IPv6 format or FQDN format. By default, the LDAP connections are unencrypted. To encrypt LDAP connections, FOS uses the **STARTTLS** or **LDAPS** parameters. The **STARTTLS** parameter unencrypts an LDAP connection by upgrading the unencrypted connection by wrapping it with TLS during or after the connection. The **LDAPS** (LDAP over TLS or SSL) parameter encrypts the entire connection from start to finish. A secure connection is established before communicating with the LDAP server.

NOTE

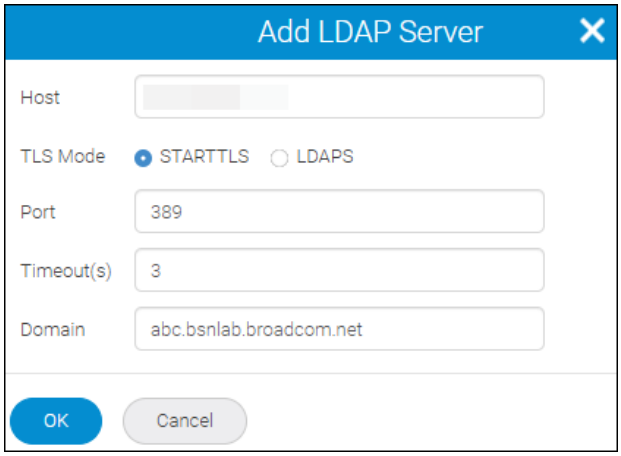
- STARTTLS and LDAPS connections are supported from Fabric OS v9.0.1 onward.
- STARTTLS and LDAPS connections are supported on all port configurations.
- By default, the designated STARTTLS port is 389 and the LDAPS port is 636.

To configure and enable the LDAP server, perform the following steps:

1. Click **Settings** from the navigation bar, and then select **Security Policies** > **Authentication and Authorization**.
2. Select **LDAP Server** as the **Primary Authentication**.
3. Select **Switch Database when LDAP authentication failed**, **Switch Database when LDAP Timeout**, or **None** from the **Secondary Authentication** list.

   The **LDAP Server** list is displayed.
4. Click **Add**.

   The **Add LDAP Server** window is displayed.
5. In the **Add LDAP Server** window, perform the following steps:



   a) Enter the **Host** name.

      The host name can be a valid IP address (in either IPv4 or IPv6 format) or an FQDN string. Each LDAP server must have a unique IP address or DNS name.

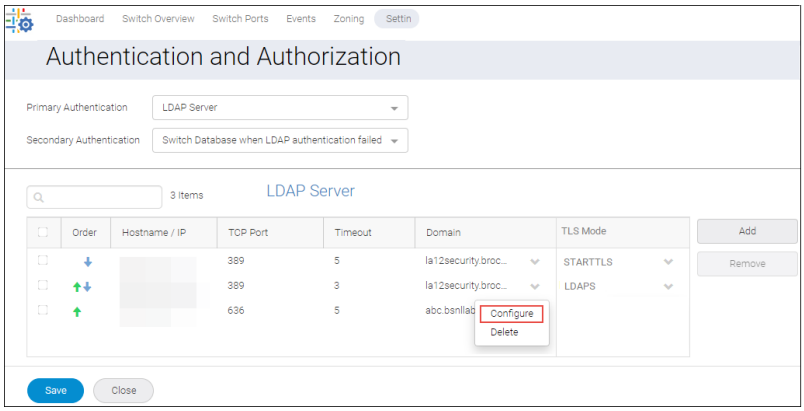
   b) Select the **TLS Mode**. By default, the TLS mode is selected as **STARTTLS** and the port is 389. If you select the TLS mode as **LDAPS**, the port is populated with 636.

   c) Enter the **Timeout(s)** in seconds and the **Domain**.

      By default, the timeout is 3 seconds.

d) Click **OK** to return to the **LDAP Server** list.

6. Click **Save** to enable the LDAP server.



NOTE

- You can rearrange the LDAP servers by clicking the up arrow or down arrow in the Order column.
- To modify an already configured LDAP server, click the down arrow next to a server, and then select **Configure**.
- To disable LDAP, select **Switch Database** from the **Primary Authentication** list.
- From Fabric OS v9.2.0, you can view the selected **TLS Mode** option in the LDAP server screen.

Removing an LDAP Server

To remove an LDAP server, perform the following steps:

1. Click **Settings** from the navigation bar, and then select **Security Policies** > **Authentication and Authorization**.
2. Select **LDAP Server** as the **Primary Authentication**.
3. Click the (⌄) icon next to an LDAP server from the **LDAP Server** list.
4. Click **Delete**.

   If there is no LDAP server that is configured, the **Delete** button is disabled.

   A confirmation dialog is displayed asking whether you want to remove the LDAP server.
5. Click **OK** to delete the LDAP server.

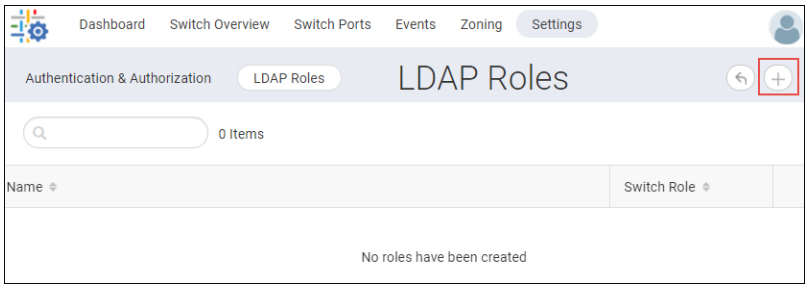
Mapping LDAP Roles to Switch Roles

Web Tools supports mapping LDAP roles for VF-enabled switches to the switch role, chassis access role, and Home LFID. You can map LDAP roles for non-VF-enabled switches only to the switch role.

To map an LDAP role, perform the following steps:

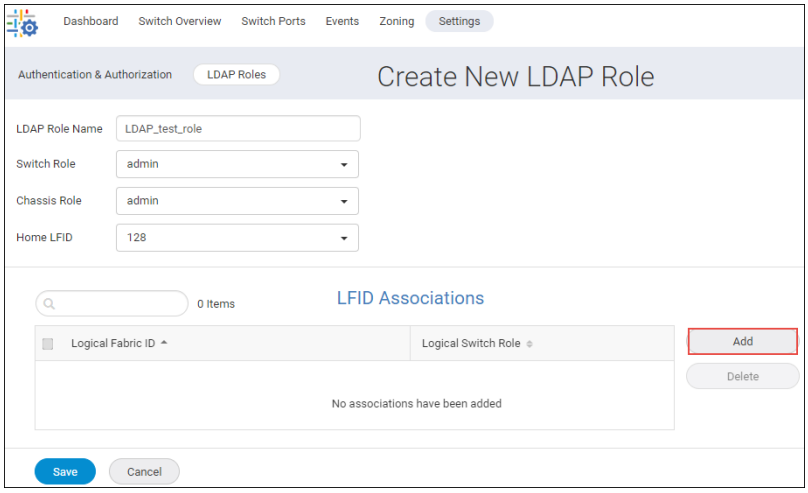
1. Click **Settings** from the navigation bar, and then select **Security Policies** > **Authentication and Authorization** > **LDAP Roles**.

   The **LDAP Roles** window displays.
2. Click the (**+**) icon from the top-right corner.



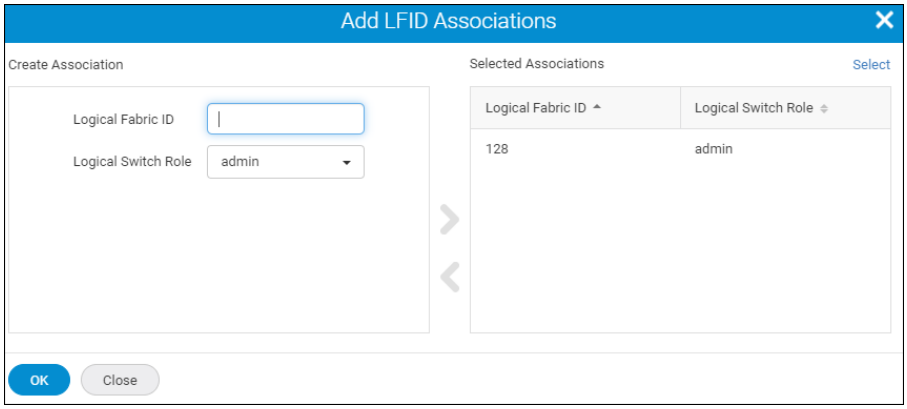
The **Create New LDAP Role** window displays.

3. Enter the LDAP role name and select the switch role, chassis role, and home LFID values from the respective drop-downs. For a non-VF switch, enter the LDAP role name and select the switch role from the drop-down. For switches running Fabric OS (FOS) 9.1.0 or higher, LDAP role names may contain underscore (_).



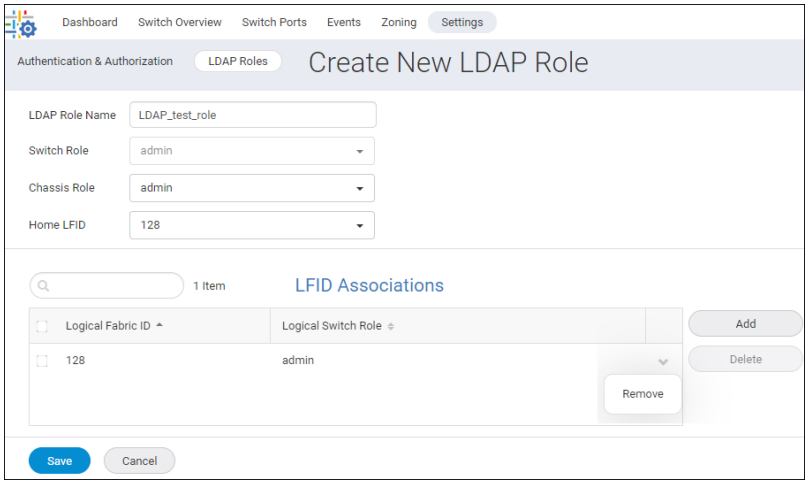
NOTE
The **Chassis Role** and **Home LFID** parameters are optional.

4. Select **Add** from the **LFID Associations** table to associate the logical fabric ID to a logical switch role.
   The **Add LFID Associations** window displays.
5. Enter the logical fabric ID and then associate it with a logical switch role.
6. Move the logical fabric ID to the **Selected Associations** table, and then click **OK**.



NOTE
Once you associate the LFID switch role, you cannot select the switch role from the drop-down.

The logical fabric ID with the associated logical switch role is placed in the **LFID Associations** table.

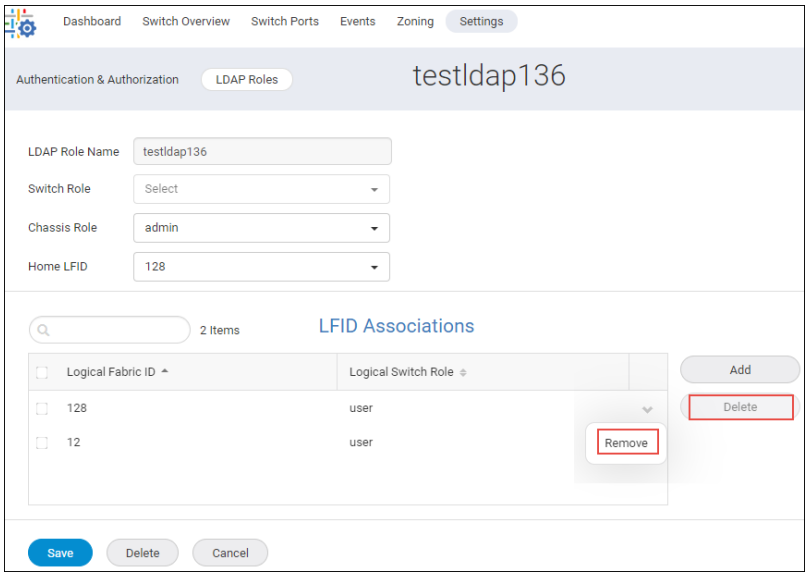


7. Click **Save**.
   The LDAP role is configured and listed in the **LDAP Roles** window.

Modifying an Existing LDAP Role

Web Tools supports modifying an existing LDAP role. To modify an existing LDAP role, perform the following steps:

1. Click **Settings** from the navigation bar, and then select **Security Policies** > **Authentication and Authorization** > **LDAP Roles**.
   The **LDAP Roles** window displays.
2. Select **View** next to an LDAP role that you want to modify.
   The selected LDAP role appears.
3. Make the required changes. You can update the chassis role and home LFID options. Also, you can remove LFID associations from an LDAP role and can add LFID associations to an LDAP role.



NOTE

- Web Tools does not support modifying LDAP role name. Web Tools supports modifying the switch role if the **LFID Associations** table is empty.
- Web Tools supports removing single or multiple LFID associations from an LDAP role. To remove a single LFID association, select **Remove** from an LFID that you want to remove. To remove multiple LFID associations, select the LFIDs and then select the **Delete** option next to the **LFID Associations** table.
- To add an LFID association, see Mapping LDAP Roles to Switch Roles.

4. Click **Save**.

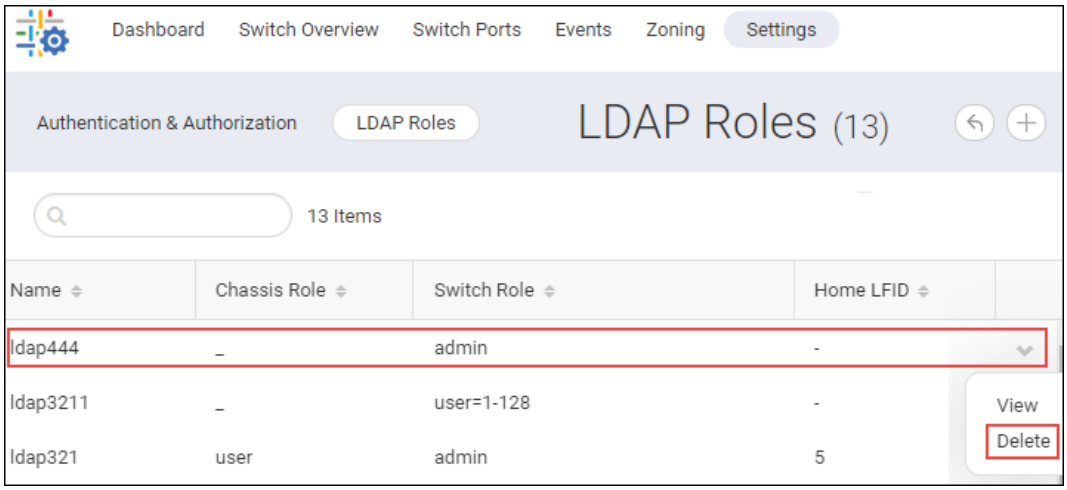
Removing an LDAP Role

To delete an LDAP role, perform the following steps:

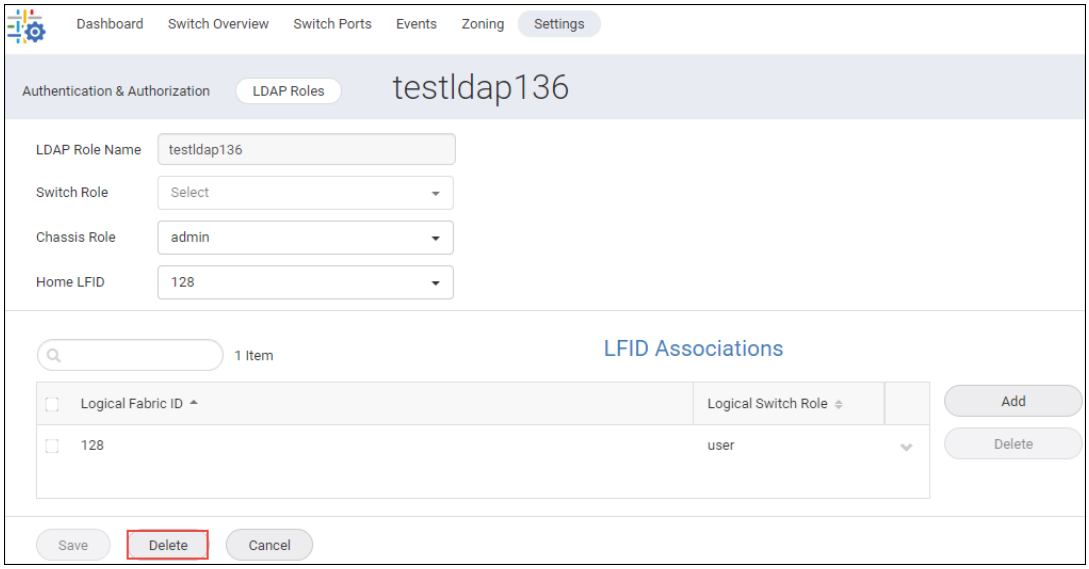
1. Click **Settings** from the navigation bar, and then select **Security Policies** > **Authentication and Authorization** > **LDAP Roles**.

   The **LDAP Roles** window displays. You can remove an LDAP role either from the **LDAP Roles** window or by drilling down to the LDAP role that you want to remove.

2. From the **LDAP Roles** window, select **Delete** for the LDAP role that you want to remove. A warning message displays. Click **Ok** to remove the LDAP role.



3. From the **LDAP Roles** window, drill down to the LDAP role that you want to remove. The selected LDAP role is displayed. Click **Delete**.



User and Role Management

Access to Web Tools is controlled by the authentication and authorization of users. Authentication is the process of validating user names and passwords. Authorization is the process of validating the roles and areas of responsibility (AORs) for each user. You can configure Web Tools to perform authentication and authorization locally or by using an external server (such as LDAP, RADIUS, or TACACS+).

User Management

In addition to the default accounts (admin, maintenance and user), Fabric OS supports up to 256 user-defined accounts in each logical switch (domain). These accounts expand your ability to track account access and audit administrative activities.

When Virtual Fabrics capability is enabled, each user-defined account is associated with the following:

- Virtual fabric ID – Specifies the accessible virtual fabric for a user account.
- Home virtual fabric – Specifies the default virtual fabric for a user account.
- Role – Determines the functional access level within the virtual fabric.

NOTE
The admin user IDs cannot be used to log in from Web Tools.

The access right for any user session is determined by the user's role. You can create and manage accounts depending on your role. The roles and permissions are listed in the following table.

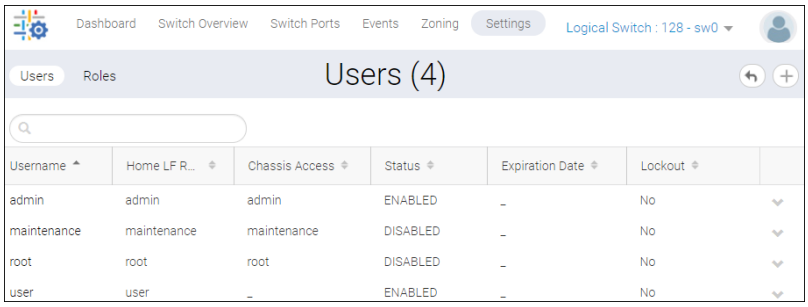
Role	Permissions
admin	Create and manage all predefined accounts and user-defined accounts.
operator	Change your own password but cannot create, modify, or view predefined or user-defined accounts.
securityadmin	Create and manage all security roles.
switchadmin	Change your own password but cannot create, modify, or view predefined or user-defined accounts.
zoneadmin	Change your own password but cannot create, modify, or view predefined or user-defined accounts.
fabricadmin	Change your own password but cannot create, modify, or view predefined or user-defined accounts.
basicswitchadmin	Change your own password but cannot create, modify, or view predefined or user-defined accounts.
user	Change your own password but cannot create, modify, or view predefined or user-defined accounts.

Creating User-Defined Accounts

An admin can create a new user with any of the default or user-defined roles.

To create user-defined accounts, perform the following steps:

1. Select **Settings** in the navigation bar, and then select **Security Policies** > **User Management**. The **Users** window is displayed. You can view a list of default and user-defined accounts in the **Users** window.



2. Click the (**+**) icon on the top-right corner of the window. The **Create New User** window is displayed.
3. In the **Create New User** window, perform the following steps:
   a) Enter the **Username**.

      The username must begin with an alphabetic character. The name can be up to 40 characters long. It is case-sensitive and contains alphabetic and numeric characters, the period (.), and the underscore (_). It must be different from all other account names on the logical switch.

b) Enter the **Password** for the account. Retype the password in the **Confirm Password** field.

The password must be from 8 to 40 characters. The password can include alphanumeric characters, the period (.), and the underscore (_) and is case-sensitive.

Passwords must also meet any additional password rules that are set earlier. (See the procedure Setting Rules for Passwords for more information.)

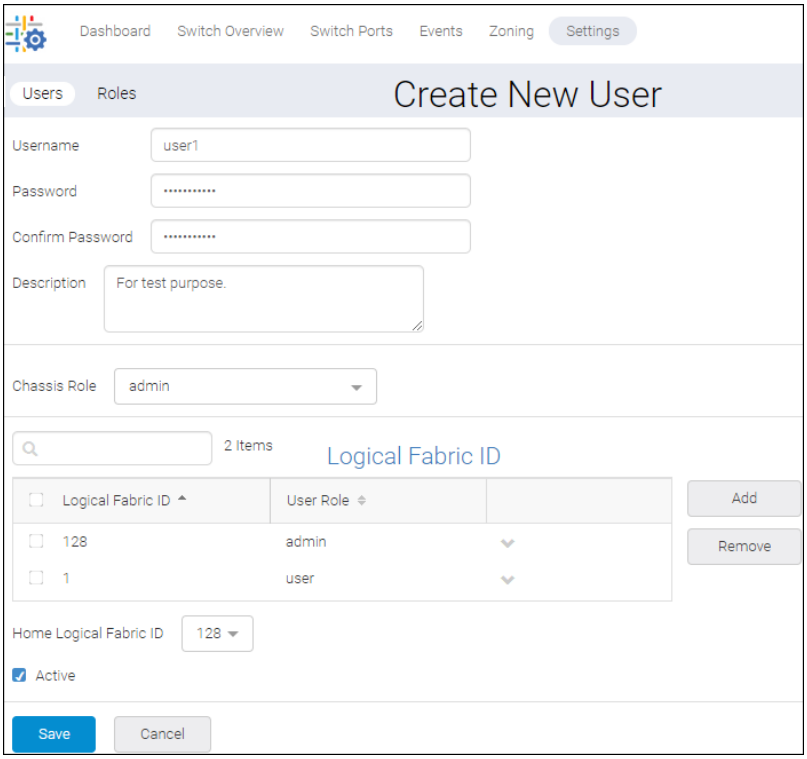
c) Enter the description of the new user in the **Description** field. This field is optional.

d) Select the role of the user from the **Chassis Role** drop-down. The **Chassis Role** drop-down displays the default roles (admin, user, switchadmin, operator, zoneadmin, fabricadmin, securityadmin, and basicswitchadmin) and the user-defined roles.

e) The **Logical Fabric ID** table displays the logical fabric IDs with assigned user roles. Click **Add** to enter the role that you want to assign to each FID present in the switch.

- For virtual fabrics, all logical fabric IDs (1–128) are displayed even if they are not created.
- In switches with multiple logical fabrics, users are created with a role for each logical fabric.

f) Select **Home Logical Fabric ID** from the drop-down. The default home logical fabric ID is 128.



4. Select **Active** to enable the user.
5. Click **Save**.

Modifying User Accounts

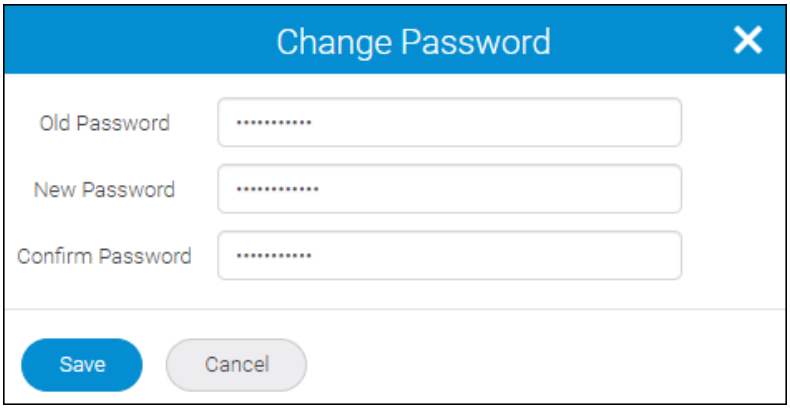
An admin can configure user accounts to do the following:

- Change the password for any user.
- Modify the role of user-defined accounts.
- Add or remove the logical fabric IDs for user-defined accounts.
- Activate or deactivate the user-defined and maintenance accounts.

1. Click **Settings** in the navigation bar, and then select **Security Policies** > **User Management**. The **Users** window is displayed.
2. Click the ( ) icon next to a user account, and then select **Configure** from the available options. The user account is displayed.
3. To change the password for a user account, perform the following steps:

   NOTE
   An admin can enforce the password expiry for an account.

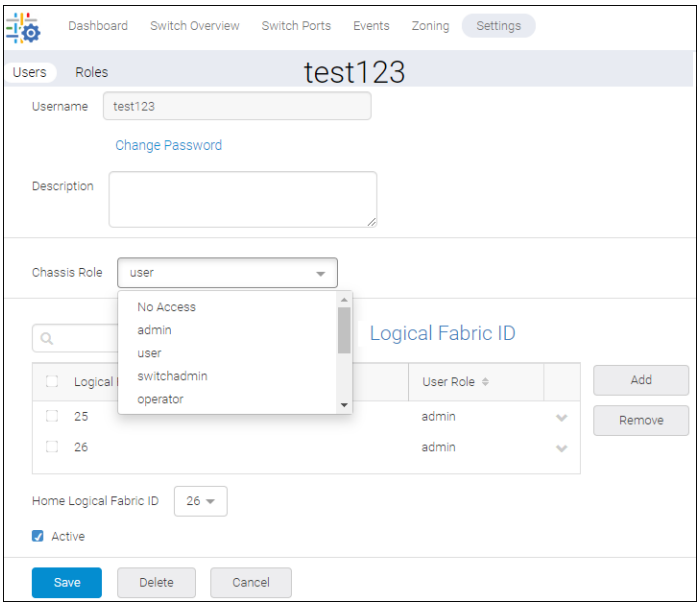
   a) Select the **Change Password** option under the **Username** field. The **Change Password** window is displayed.



   b) Enter the old password and the new password, and confirm the new password.
   c) Click **Save**.
   For more information on setting a password rule, see Setting Rules for Passwords.
4. To modify the role and add or remove the logical fabric IDs of a user-defined account, perform the following steps:

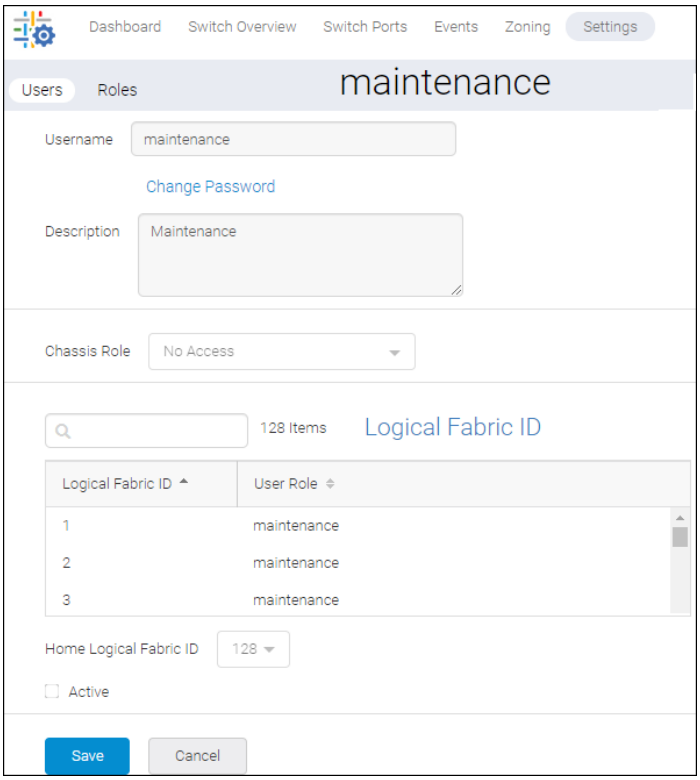
   NOTE
   An admin cannot modify the role and logical fabric ID of a default account.

   a) Select the role from the **Chassis Role** drop-down.



b) Add or remove the logical fabric ID from the **Logical Fabric ID** table.
c) Modify the **Home Logical Fabric ID** based on your requirements.
d) Click **Save**.

5. To activate or deactivate the user-defined and maintenance accounts, perform the following steps:
   a) Enable or disable the **Active** checkbox.

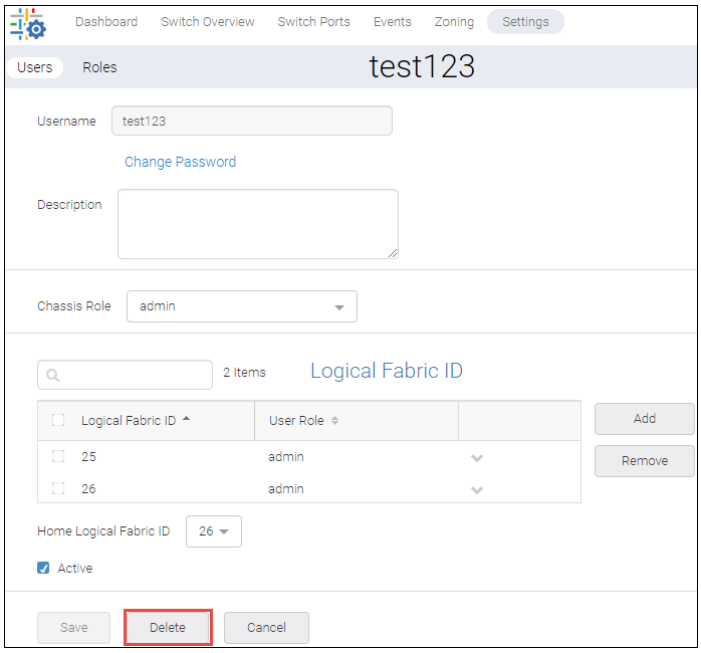


b) Click **Save**.

Deleting User-Defined Accounts

To delete a user account, perform the following steps:

1. Select **Settings** in the navigation bar, and then select **Security Policies** > **User Management**. The **Users** window displays the list of default and user-defined accounts.
2. Select the user-defined account that you want to remove. An admin cannot delete default accounts.



3. Click **Delete**, and then click **OK**.

User-Defined Roles

User-defined roles provide the ability to dynamically create roles on the switch. The default roles are defined based on individual permissions for different features or by restricting access to various features. The default roles cannot be edited for assigning different privileges to a particular user. However, user-defined roles provide the ability to create new roles and define permissions for the role-based access control (RBAC) class.

Guidelines and Restrictions

The following points must be noted before creating and configuring user-defined roles:

- To edit the Port Admin and FCR configuration, you must assign the SwitchPortManagement and SwitchPortConfiguration privileges to the user-defined role.
- To set the fabric ID, you must assign the FabricRouting and SwitchConfiguration privileges to the user-defined role.
- To view reports, you must assign the SwitchManagement, SwitchConfiguration, and FRUManagement privileges to the user-defined role.

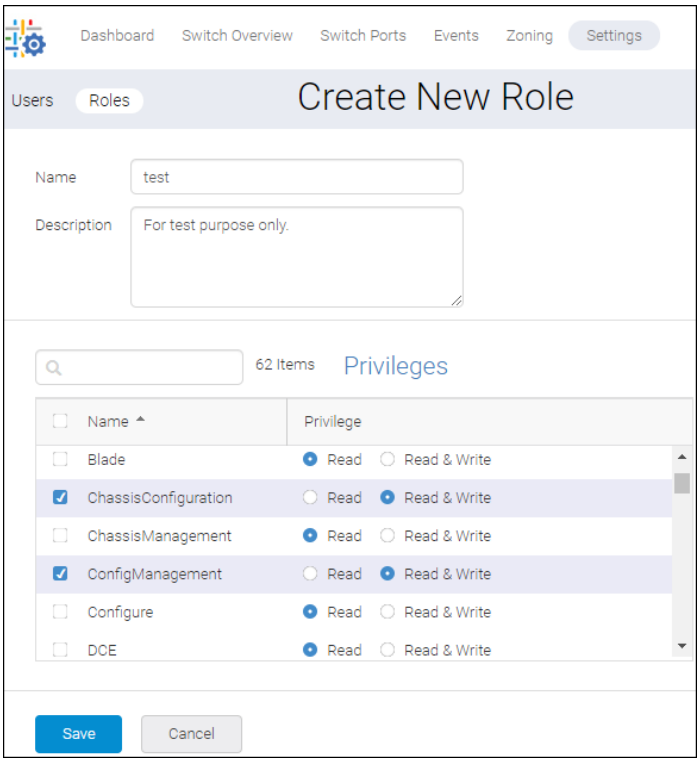
For some functionality and operations that need chassis-level access, the user-defined role privileges must be assigned at both the chassis level and the logical fabric level to have the corresponding tab enabled.

- To access **CPU Utilization** and **Memory Utilization** under the **Dashboard** tab, you must assign the read/write MAPS permission and the CHASSIS_CONTEXT context type to a user-defined account.
- To access the **Settings** > **Configuration** tab, you must assign the ConfigManagement, SwitchConfiguration, or Configure privileges to the user-defined role, which is applied at the logical fabric level. Any of these three privileges is sufficient.
- To access the **Security Policies** tab, you must assign the Authentication, FabricDistribution, Security, IPSec, AG, or IPfilter privileges to the user-defined role, which is applied at the logical fabric level. Any of these six privileges is sufficient.
- To access the **Switch Ports** tab, you must assign the SwitchConfiguration, SwitchManagement, FRUManagement, AG, or Configure privileges to the user-defined role, which is applied at the logical fabric level. Any of these five privileges is sufficient.

Creating a User-Defined Role

To add a user-defined role, perform the following steps:

1. Click **Settings** in the navigation bar, and then select **Security Policies** > **User Management**.
2. Click the **Roles** tab. The **Roles** window is displayed.
3. Click the (**+**) icon on the top-right corner of the window. The **Create New Role** window is displayed.
4. In the **Create New Role** window, perform the following steps:
   a) Enter the **Name**. The role name must contain 4 to 16 alphabetic characters.
   b) Enter the description of the new role in the **Description** field. This field is optional.
   c) In the **Privileges** section, select the privileges that you want to assign to the new role. Each privilege is selected with either the **Read** mode or the **Read & Write** mode.

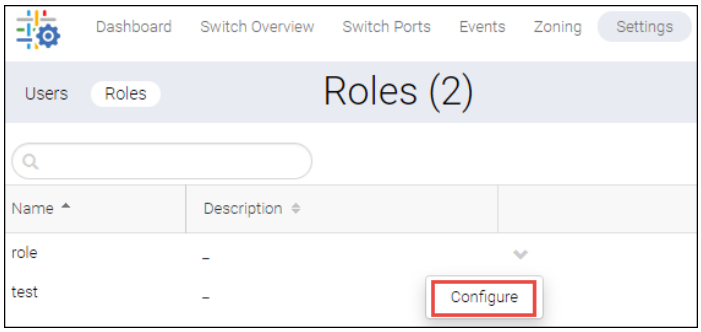


   d) Click **Save**.

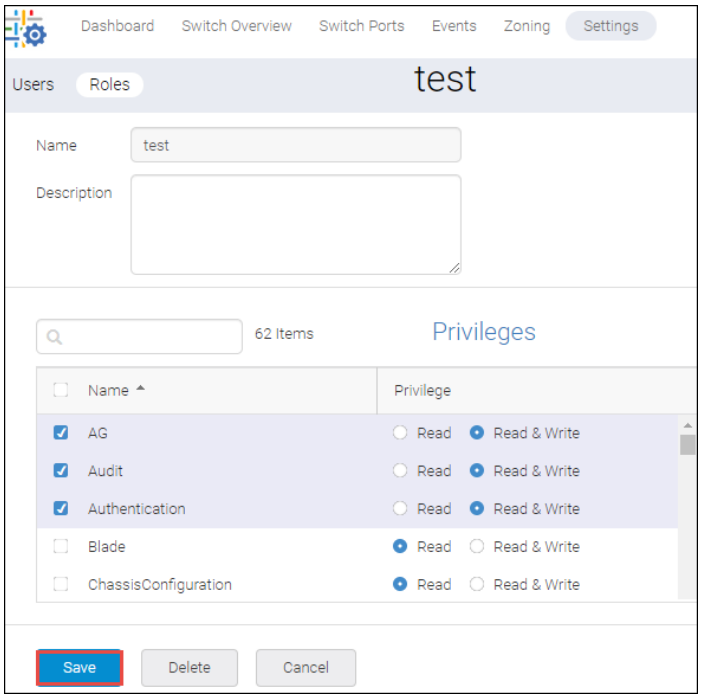
Editing a User-Defined Role

To edit a user-defined role, perform the following steps:

1. Click **Settings** in the navigation bar, and then select **Security Policies** > **User Management**.
2. Click the **Roles** tab. The **Roles** window displays the list of configured roles.
3. Click the (⌄) icon next to a role, and click **Configure**. The window displays the role name as the title.



4. In the **Privileges** section, edit the privileges for the role. You can add new privileges or remove existing privileges, or you can switch between the **Read** and **Read & Write** option.



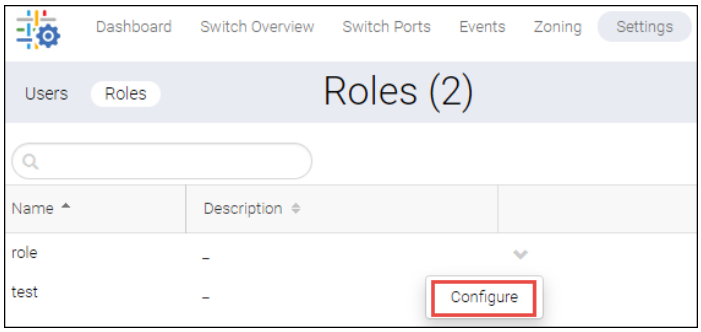
NOTE
You can edit the privileges section only in the role window.

5. Click **Save**.

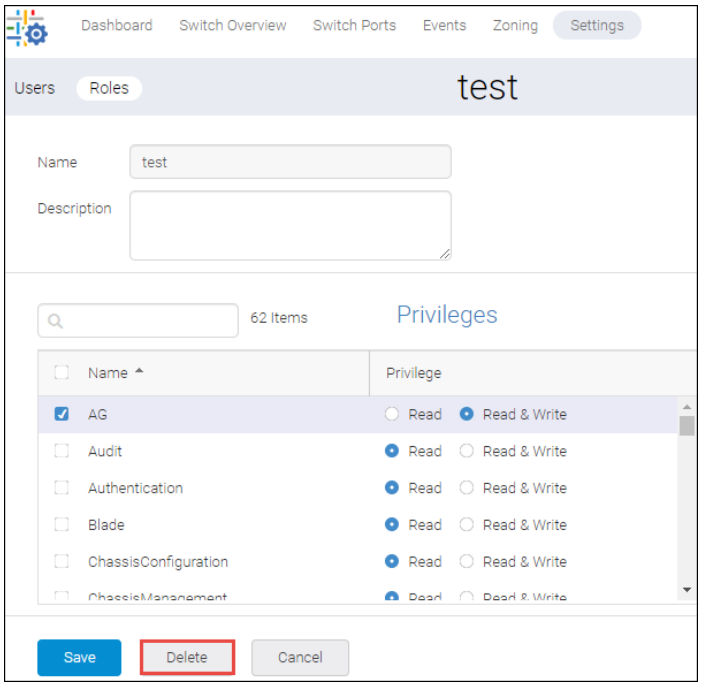
Deleting a User-Defined Role

To delete a user-defined role, perform the following steps:

1. Click **Settings** in the navigation bar, and then select **Security Policies** > **User Management**.
2. Click the **Roles** tab. The **Roles** window displays the list of configured roles.
3. Click the (⌄) icon next to a role, and click **Configure**. The window displays the role name as the title.



4. Click **Delete**. A warning message appears to confirm the deletion.



5. Click **OK** to delete the role.

Maintaining Passwords

When you log in after the password is expired, Web Tools allows you to provide a new password.

A password is locked if you exceed the maximum number of failed login attempts. To unlock a password, see Unlocking a Password for more information.

Setting Rules for Passwords

To set rules for passwords, perform the following steps:

1. Click **Settings** in the navigation bar, and then select **Security Policies** > **Password Policy**. The **Password Policy** window is displayed.
2. Fill out the **Password Policy** window for the password rules that you want to enforce.

   The table below describes the password rule parameters:

Password Rule Parameter	Description
Minimum Length	Minimum password length (8–40 characters).
Uppercase Letters	Minimum number of uppercase characters required.
Lowercase Letters	Minimum number of lowercase characters required.
Numbers	Minimum number of digits required.
Special Characters	Minimum number of punctuation characters required.
Maximum Repeat	The maximum number of repeated characters in the password.
Maximum Sequence	The maximum sequence of characters in the password.
Password Age	Minimum number of days (0–999) before you can change the password again.
Warning Period	Number of days to warn a user before a password is expired (0–999).
Password History	Number of password changes before you can reuse a password.
Lockout After	Number of failed login attempts (0–999) before the password is locked from further change attempts and the amount of time for which the password is locked (0–99999 minutes).
Lockout Duration	Number of failed login attempts (0–999) before the password is locked from further change attempts and the amount of time for which the password is locked (0–99999 minutes).
Min Difference	Number of characters that must differ between the current password and the new password.

3. Select **Reserve Password** to prevent reusing a recently used password.
4. Select **Lockout Admin** to enable lockout configurations for an admin.
   - The account lockout policy disables a user account when the user exceeds a configurable number of failed login attempts.
   - If you do not enable the **Lockout Admin** option, an admin is never locked out of the system.
5. Click **Save** to save your changes.

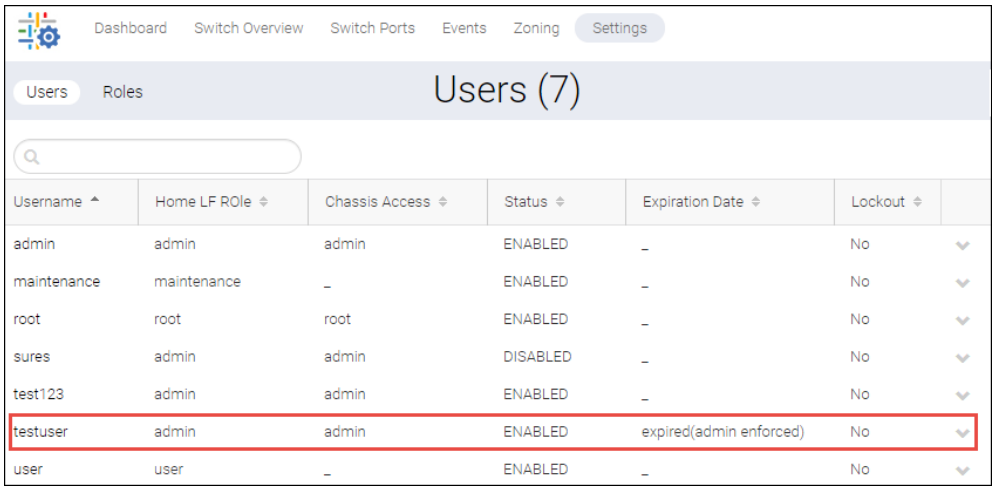
Setting a Password as Expired

The password expiration policy forces expiration of a password after a specified period of time.

To set a password as expired, perform the following steps:

1. Click **Settings** in the navigation bar, and then select **Security Policies** > **User Management**. The **Users** window is displayed with a list of the default and user-defined accounts.
2. Click the ( ) icon next to a user account, and then select **Expire Password** from the available options. The button is disabled for the expired password.

   The **expired(admin enforced)** status is displayed in the **Expiration Date** column. In the next login, the expire dialog is displayed to change the password.



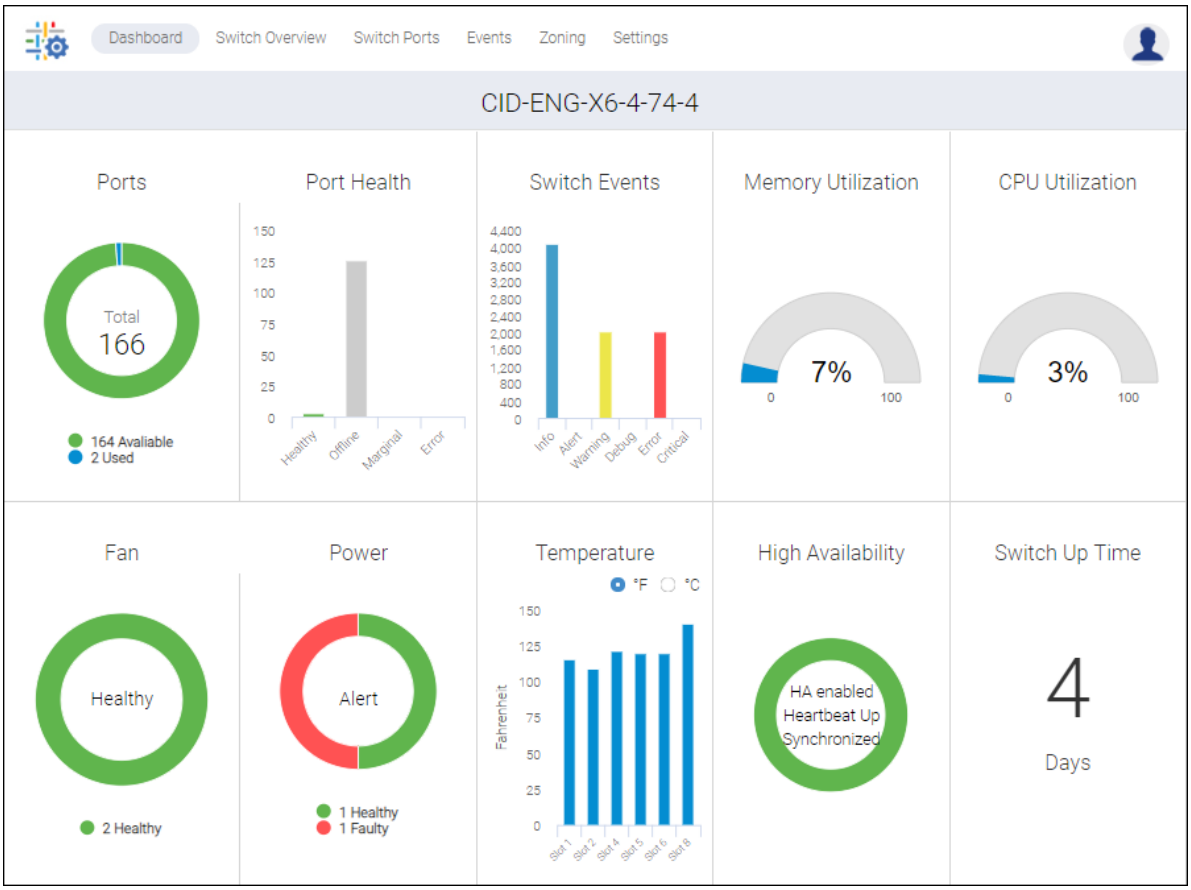
Unlocking a Password

To unlock a password, perform the following steps:

1. Click **Settings** in the navigation bar, and then select **Security Policies** > **User Management**. The **Users** window is displayed with a list of the default and user-defined accounts.
2. Click the ( ) icon next to a user account, and then select **Unlock Password** from the available options.
   If the button is disabled, the password is already unlocked or not locked out.

Monitoring the Web Tools Dashboard

The Web Tools dashboard provides a quick glance of switch ports, health, and utilization. From the dashboard, you can quickly see the overall health and status of the switch.



The dashboard consists of 10 widgets that provide information about switch and port status. Some of the widgets show information for a logical switch, and some show information for a physical switch.

Widget Name	Switch	Description
Ports	Logical	Number of ports that are available and in use for the logical switch.
Port Health	Logical	Health status of the ports in the logical switch.
Switch Events	Logical	Number of events, organized by severity, for the logical switch.
Memory Utilization	Physical	Percentage of memory that is currently being utilized on the switch.
CPU Utilization	Physical	Percentage of the CPU that is currently being utilized on the switch.
Fan	Physical	Overall status of the fans in the chassis.
Power	Physical	Overall status of the power supplies in the chassis.
Temperature	Physical	Temperature of the chassis on a per-slot (director) or per-sensor (switch) basis.
High Availability	Physical	(For directors only) Status of high availability (HA) features on the director.
Switch Up Time	Physical	Length of time for which the switch has been in operation since the last reboot.

Monitoring Ports

The Web Tools **Ports** widget displays the number of ports that are available and in the use for the logical switch. The **Port Health** widget displays the health status of the ports for the logical switch.

Note that the **Port Health** widget is displayed only if the Fabric Vision® license is installed on the switch.

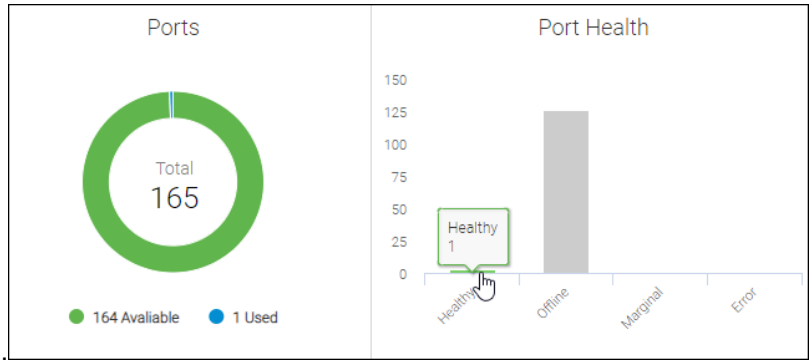
1. Click **Dashboard** in the navigation bar.
2. View the **Ports** widget to see the number of ports available and the number of ports in use for the logical switch.

   If the port status is "Online", ports are indicated as "Used."
3. View the **Port Health** widget to see the overall health status for the ports in the logical switch.

   The widget displays the data in a bar graph, with one bar for each of the following health states:

   - Healthy
   - Offline
   - Marginal
   - Error

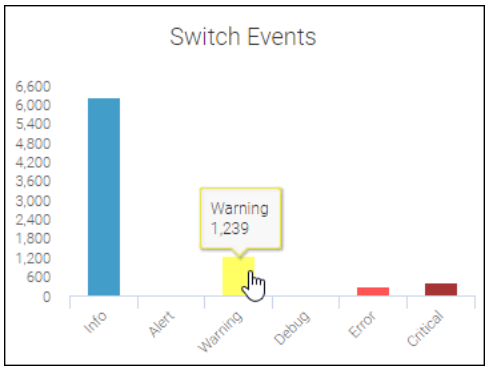
   Hover over a bar in the graph to display the number of ports with that health status.



Monitoring Events

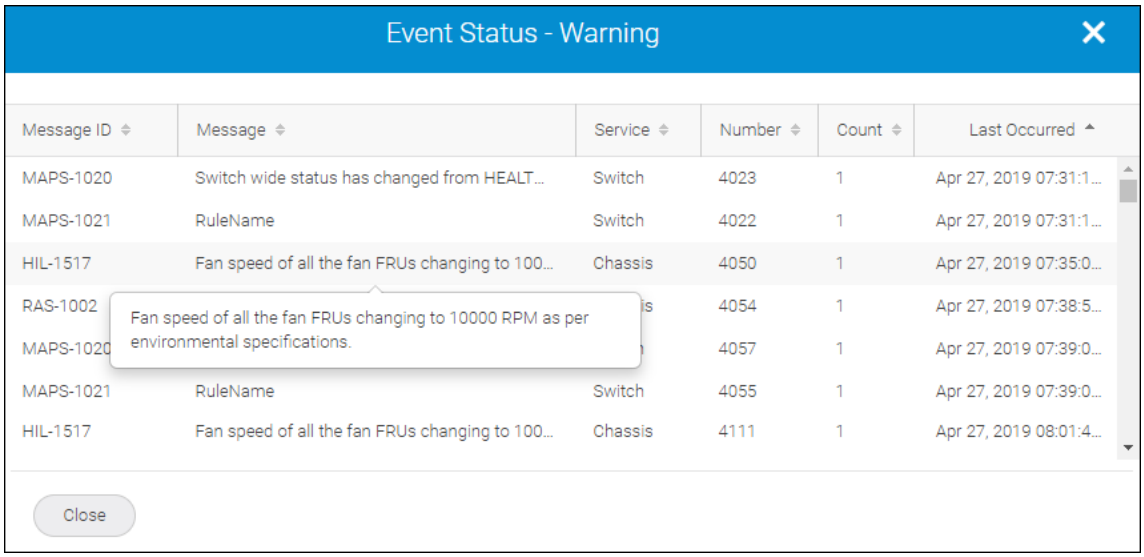
The Web Tools **Switch Events** widget displays all events for the logical switch. Events are characterized by severity level.

1. Click **Dashboard** in the navigation bar.
2. View the **Switch Events** widget, which shows the number of events in a bar graph, organized by severity.
3. Hover over a bar in the graph to display the number of events with that severity.



4. Click a bar in the graph to display the list of events with that severity.

   You can adjust the **Event Status** column widths to display longer messages. Hover over messages that are too long for the table column in order to display a tool tip with the complete message.

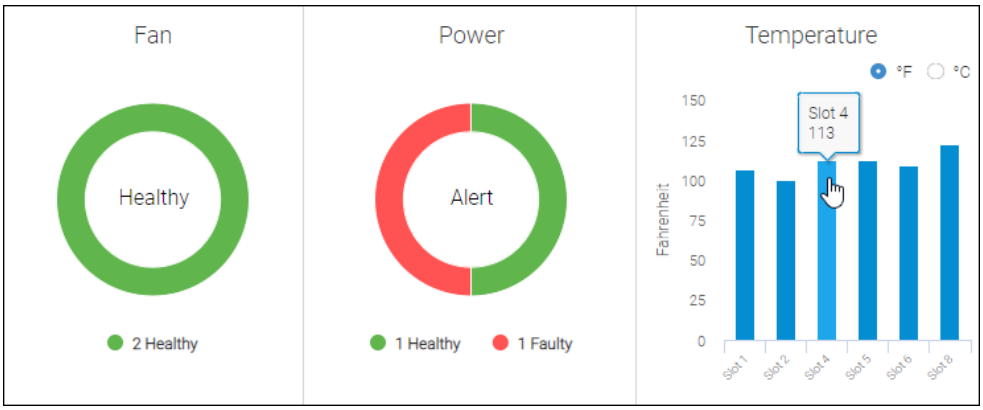


   Refer to the *Brocade Fabric OS Message Reference Manual* for the probable cause and recommended action for each message.

The **Events** page displays the events in a table that you can filter and sort. See Fault Management: Displaying and Filtering Events for additional information about monitoring events from the **Events** page.

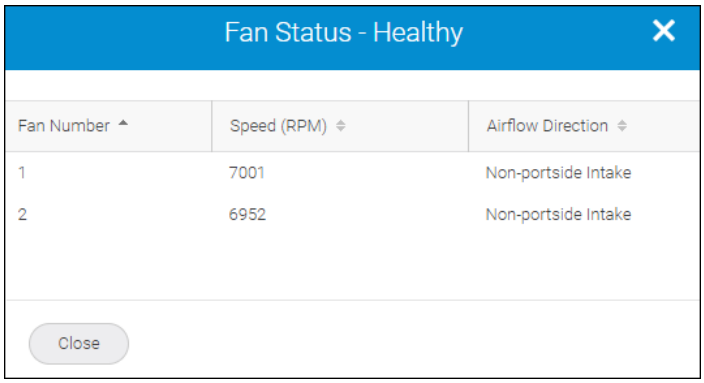
Monitoring Switch Health

The Web Tools dashboard provides several widgets with which you can monitor the physical health of the switch.



1. Click **Dashboard** in the navigation bar.
2. View the **Fan** widget to see the number of healthy, faulty, and absent fans in the chassis.

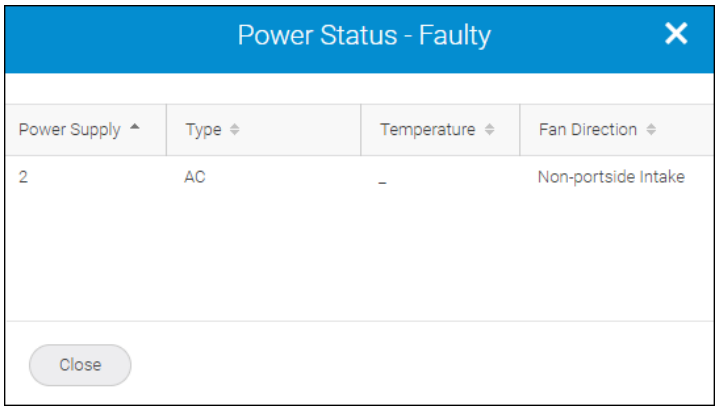
   Click the widget to display detailed information about the fans.



In this table, the **Fan Number** column indicates either the fan number or the fan FRU number, depending on the switch model. A fan FRU can contain one or more fans.

3. View the **Power** widget to see the number of healthy, faulty, and absent power supplies in the chassis.

   Click the widget to display additional information about the power supplies. For example, clicking the red section of the widget displays information about the faulty power supplies.

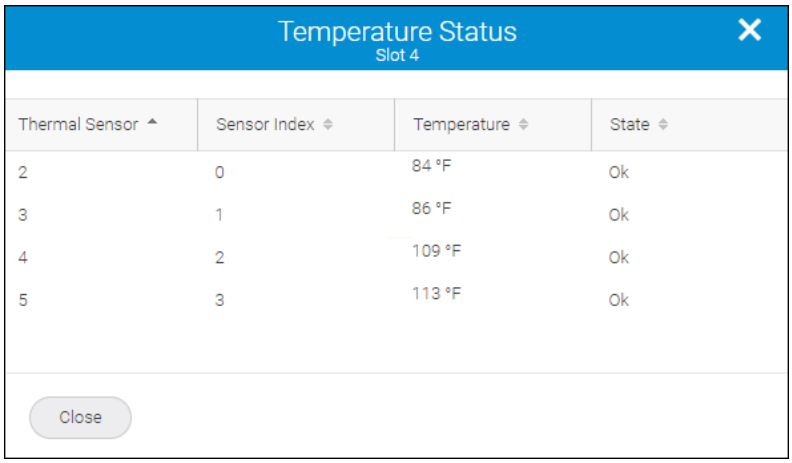


4. View the **Temperature** widget to display the overall temperature of the chassis, in Fahrenheit or Celsius.

   - For directors, the temperature is calculated on a per-slot basis, with each slot indicated in a separate bar in the graph. The temperature displayed is the highest of all the thermal sensors in that slot.
   - For switches, each bar in the graph represents a single thermal sensor.

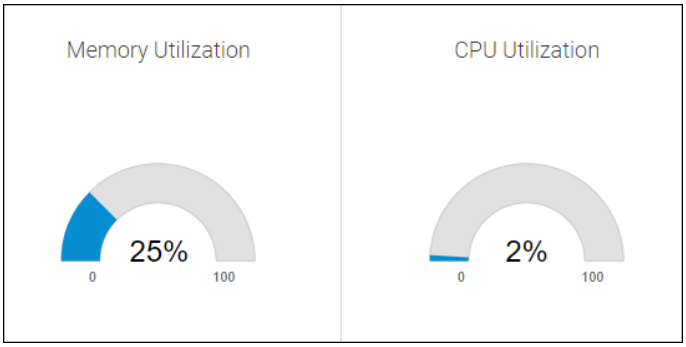
   Hover over a bar in the graph to display the exact temperature.

   Click a bar in the graph to display detailed information about the temperature status.

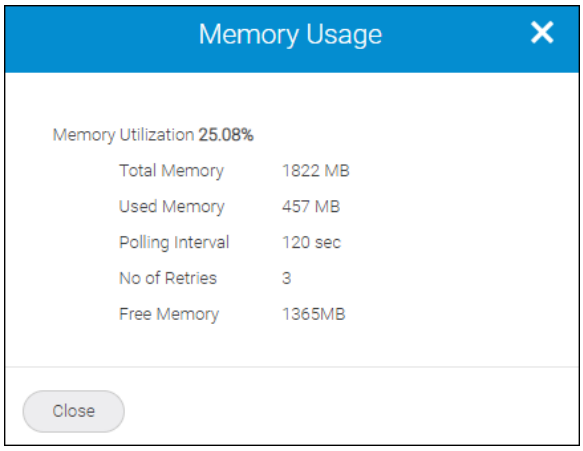


Monitoring Switch Utilization

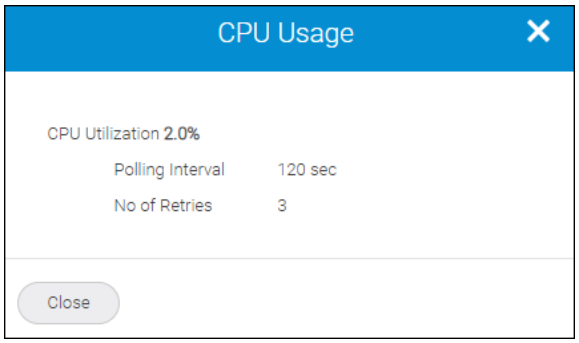
The Web Tools dashboard provides two widgets for monitoring memory and CPU utilization on the physical switch.



1. Click **Dashboard** in the navigation bar.
2. View the **Memory Utilization** widget to see the percentage of memory that is currently utilized on the switch.
   Click the blue section of the chart to display additional memory usage details.



3. View the **CPU Utilization** widget to see the CPU usage as a percentage of available CPU resources on the switch.
   Click the blue section of the chart to display additional CPU usage details.



Generating a Switch Report

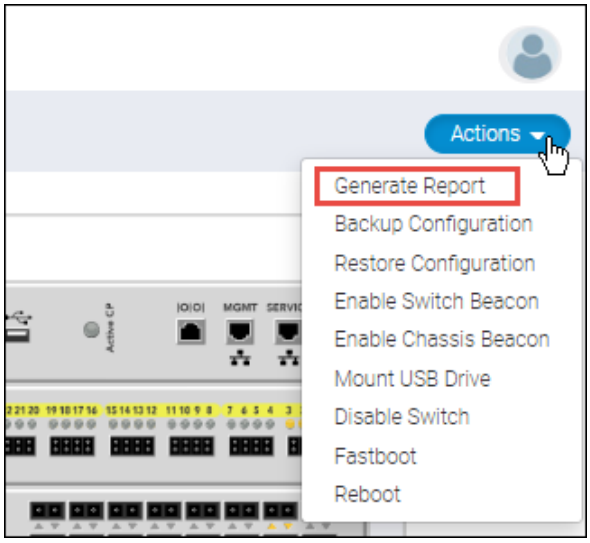
From the Web Tools **Switch Overview** page, you can generate a report of all switch-related information.

The report consists of the following sections:

- List of Switches
- Current Switch Information
- List of Inter-Switch Links
- List of Ports
- Name Server
- Zoning Information
- SFP Serial ID Information

To generate the switch report, perform the following steps:

1. Select **Switch Overview** from the navigation bar.
2. From the **Actions** menu in the upper-right corner of the page, select **Generate Report**.



3. When finished viewing the report, scroll to the bottom and click **Close**.

Switch Management

Using Web Tools, you can configure several features on your switches.

- Switch configuration
- Zone configuration
- Firmware upgrade
- IPv4 and IPv6 configuration

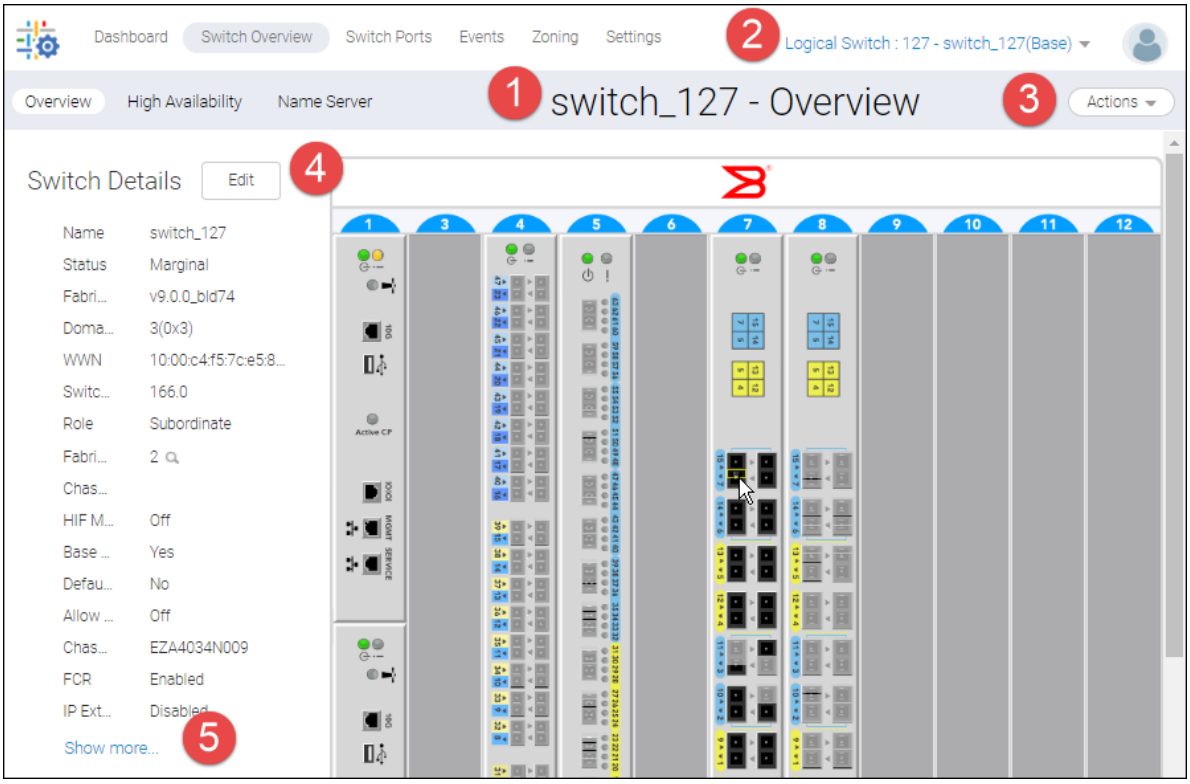
Switch Overview

The**Switch Overview** tab allows you to edit the switch information, perform various switch actions, and initiate CP failover.

The **Switch Overview** tab displays an image of the switch and allows you to perform the following tasks:

- Display detailed switch, network, and fabric information.
- Edit the switch name, IP network parameters, and switch settings, such as Access Gateway mode and FCR.
- Perform switch actions, such as reboot, fast boot, and switch disable/enable.
- Display information on all Name Server entries in the fabric.
- Initiate a CP failover (for products that support high availability).
- Change the logical switch context.

Figure 9: Switch Overview Tab



1. Switch name
2. Logical switch context
3. Switch actions menu

4. Click to edit switch details
5. Click to display more or fewer switch details

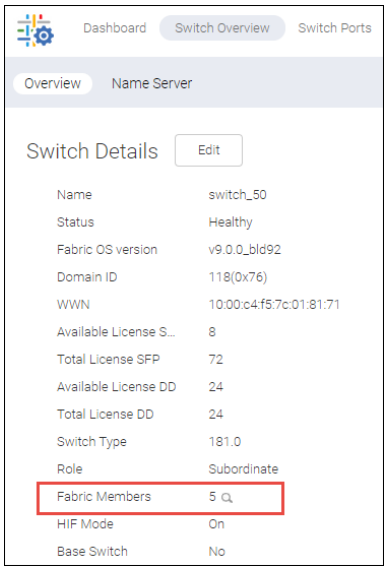
Note that the logical switch context is not displayed if you launched Web Tools from SANnav Management Portal.

Hover the mouse over different elements in the switch image to display a tool tip with details about that element. Note that blade model numbers are displayed in the image for Gen 7 blades. For Gen 6 blades, you can see the model numbers in the tool tip by hovering over the blades.

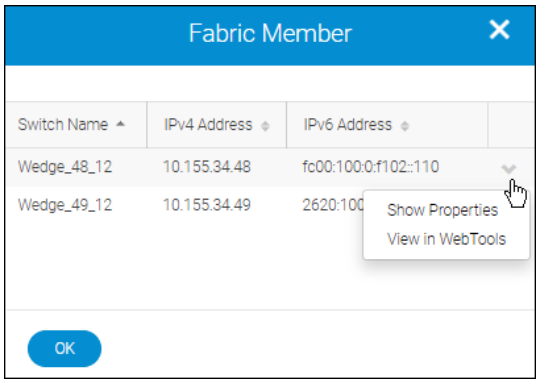
Displaying Fabric Properties

From the **Switch Overview** page, you can display additional details about the other members of the fabric.

1. Select the **Switch Overview** tab in the navigation bar.
2. Click the magnifying glass icon next to the **Fabric Members** detail to display all of the fabric members.



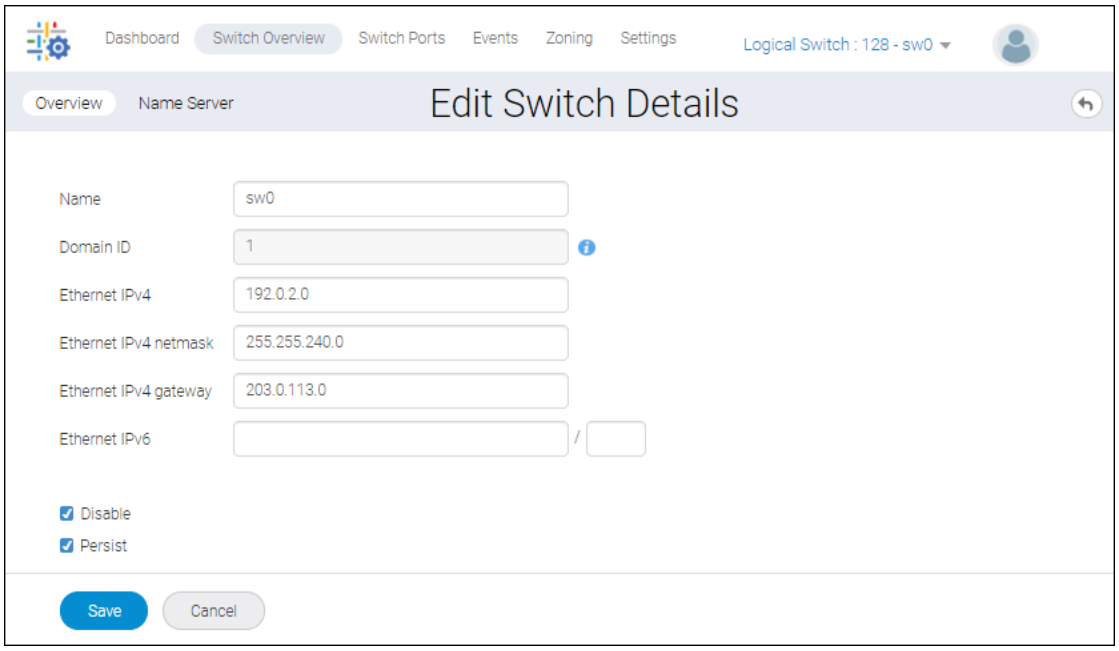
3. Click **Show Properties** in the action menu to view additional properties for each switch.



Editing the Switch Name and Network Configuration

You can edit the switch name and network configuration and persistently disable the switch from the **Switch Overview** page.

1. Select **Switch Overview** from the navigation bar.
2. Click **Edit** next to the **Switch Details** heading to display the **Edit Switch Details** dialog.



3. Update the fields that you want to change.

   NOTE
   Domain ID cannot be edited. To edit a **Domain ID**, you must disable the switch.

4. Select the **Disable** checkbox to disable the switch.

   If the **Disable** checkbox is already selected, clearing the checkbox enables the switch.

5. Select the **Persist** checkbox to persistently disable the switch.

   "Persistent disable" means that the switch is set to a disabled state without being disabled. When the switch reboots, it is disabled and must be enabled.

6. Click **Save** to save the changes to the switch.

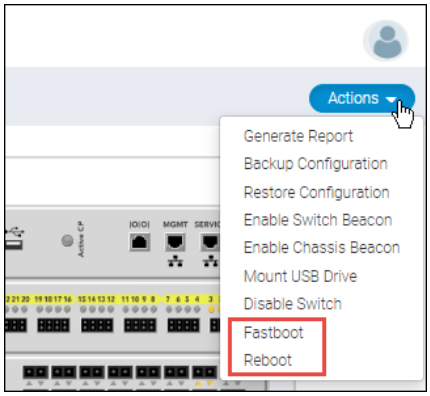
Initiating a Reboot or Fast Boot of the Switch

A reboot or fast boot restarts the switch immediately. A fast boot reduces boot time significantly by bypassing the power-on self-test (POST); although traffic will be interrupted, frames are not dropped.

Ensure that there are no traffic or management processes occurring on the switch before you perform these actions. Be sure to save any configuration changes before the restart because any changes not saved will be lost.

To perform a switch reboot or fast boot, perform the following steps:

1. Select **Switch Overview** from the navigation bar.
2. From the **Actions** menu in the upper-right corner of the page, select **Fastboot** or **Reboot**.



3. Select **OK** in the confirmation dialog.

Enabling and Disabling a Switch

By default, the switch is enabled after power is applied and diagnostics and switch initialization routines have finished. You can disable and re-enable the switch as necessary.

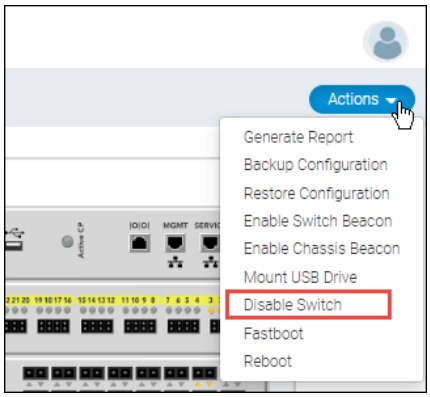
When you enable or disable a switch, the affected ports depend on whether Virtual Fabrics is enabled. The following table describes which ports are affected for each type of enable or disable operation.

Operation	Virtual Fabrics Enabled	Virtual Fabrics Not Enabled
Enable switch	Enables all ports on the logical switch	Enables all ports on the physical chassis
Enable chassis	Enables all ports on the physical chassis	Not allowed
Disable switch	Disables all ports on the logical switch	Disables all ports on the physical chassis
Disable chassis	Disables all ports on the physical chassis	Not allowed

To enable or disable a switch, perform the following steps:

1. Select **Switch Overview** from the navigation bar.
2. From the **Actions** menu in the upper-right corner of the page, select **Enable Switch** or **Disable Switch**.

   If the switch is enabled, the **Disable Switch** option displays on the **Actions** menu. If the switch is disabled, **Enable Switch** is displayed.



3. Select **OK** in the confirmation dialog.

Configuring Switch and Chassis Beacons

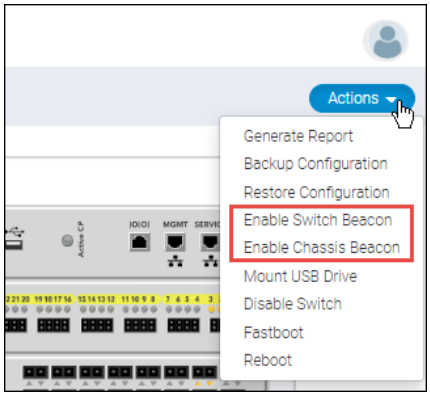
Enable switch or chassis beaconing to locate a failing unit. When beaconing is enabled, the port LEDs flash green at various rates across the chassis. The beaconing continues until you turn it off.

Switch beaconing enables or disables beaconing on all ports in the current logical switch. Chassis beaconing enables or disables beaconing on all ports in the chassis.

In addition to switch and chassis beaconing, port and port peer beaconing are also supported. See Advanced Port Configuration for more information about configuring beaconing at the port level.

Only one beaconing mode can be active at a time. For example, if you want to enable switch beaconing, you must first disable chassis or port beaconing.

1. Select **Switch Overview** from the navigation bar.
2. From the **Actions** menu in the upper-right corner of the page, select one of the beacon options.
   - **Enable** (or **Disable**) **Switch Beacon**
   - **Enable** (or **Disable**) **Chassis Beacon**



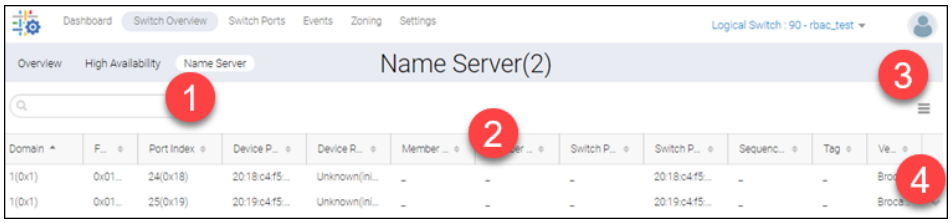
3. Click **OK** in the confirmation dialog.

Displaying Name Server Information

Display a table of name server entries in the Simple Name Server Database. The table includes all Name Server entries for the fabric, not just those related to the local domain. Each row in the table represents a different device.

1. Click the **Name Server** tab on the **Switch Overview** page.

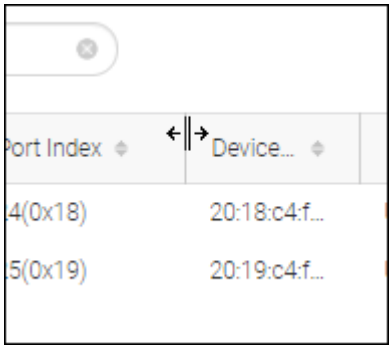
   You can click the arrows in the column headings to sort in ascending and descending order.



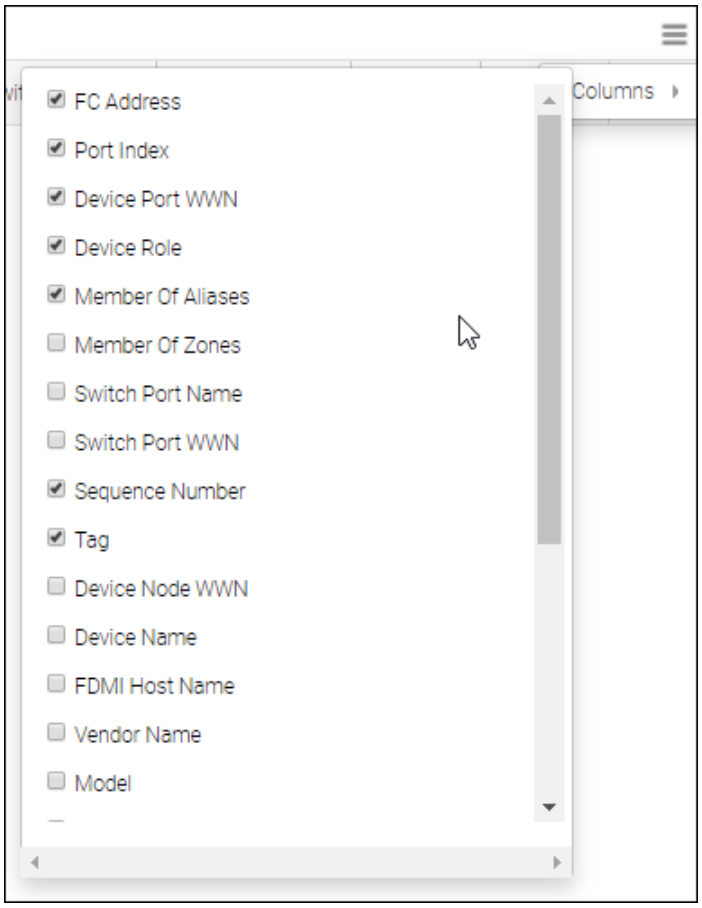
   1. Search box.
   2. Table of name server entries.
   3. Hamburger icon to manage table columns (see list below).
   4. Action menu to view the accessible devices associated with this name server.

2. Customize the display of columns and data using the following methods:

   - To sort the entries by the specific column, click the column header. Click the head again to reverse the sort.
   - To resize a column, drag a column divider.



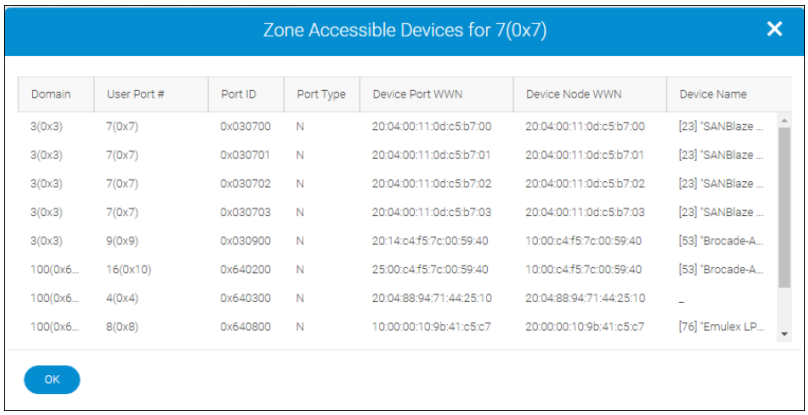
   - To display a checklist of possible columns for the table, click the hamburger icon ≡ in the top-right corner and select **Columns**.



Add or remove columns by selecting or deselecting a checkbox in the checklist.

3. Display specific device rows by entering known device information in the search box at the upper left of the table. For example, to display a device with a port WWN of 10:00:00:10:9b:1c:2a:e0, enter that WWN in the search box. Similarly, to display all devices with the initiator role, enter "initiator" in the search box.
4. View the zone-accessible devices by selecting **Accessible Devices** from the action menu.

The **Zone Accessible Devices** window is displayed.

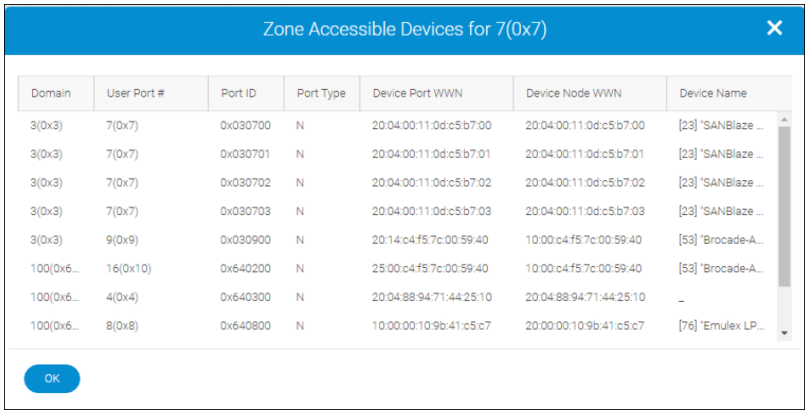


Displaying Zone Members for a Device

Use the following steps to display information on zone members for a specific device listed in the **Name Server** tab.

1. Click the **Name Server** tab on the **Switch Overview** page.
2. Click the actions menu icon (⌄) at the end of the device row.
3. Select **Accessible Devices**.

The **Zone Accessible Devices** window is displayed. Here you will find information about all accessible zone members for the device, such as the domain, user port number, port ID, port type, device port WWN, device name, and WWN company ID.



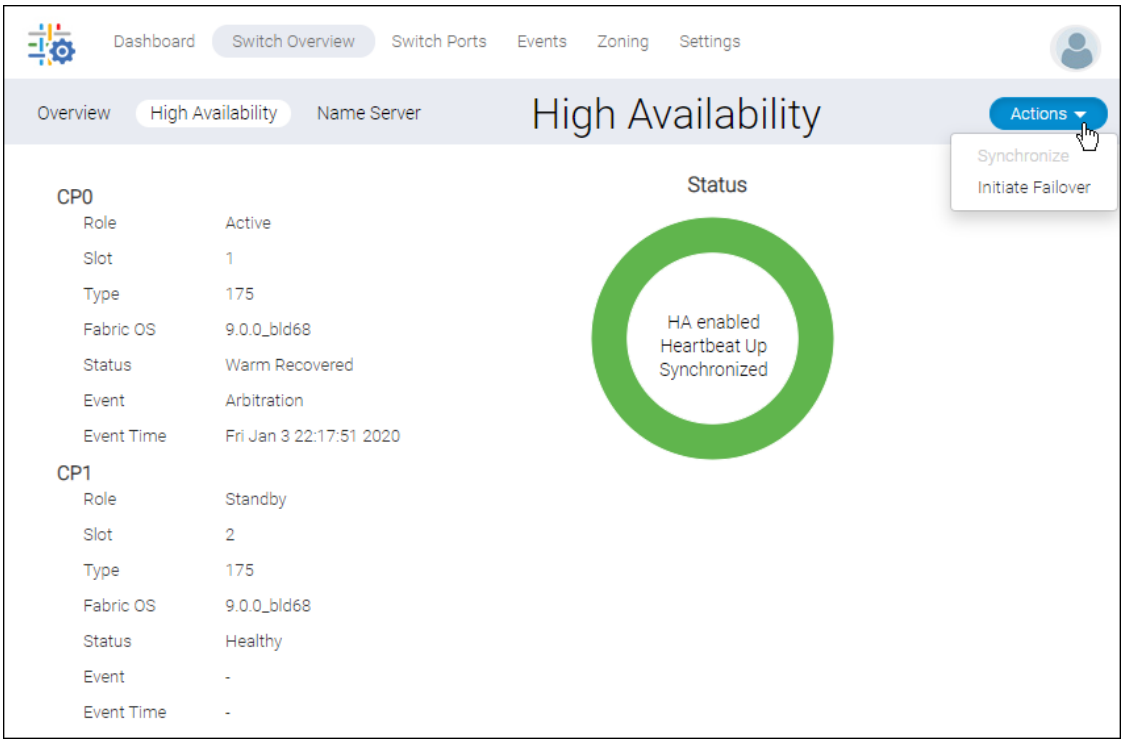
Using Switch High Availability Features

High availability (HA) features provide maximum reliability and nondisruptive replacement of key hardware and software modules. High availability is available only on modular chassis director products.

Select the **High Availability** tab on the **Switch Overview** page to display information about the status of the HA feature on each control processor (CP) in the switch and to perform the following tasks:

- Synchronize all services between both CPs. A nondisruptive CP failover is possible only when all services are synchronized.
- Initiate a CP failover.

Figure 10: High Availability Tab



Information about CP0 and CP1 displays on the left side of the page, including whether the CP has a standby or active status, the chassis slot where the CP is installed, and the Fabric OS firmware installed on the CP.

The background color of the **HA Status** icon indicates the overall status of high availability on the switch.

- Green – Healthy. The HA status is HA enabled, the heartbeat is up, and the HA state is synchronized.
- Yellow – Disruptive mode. The HA status is HA enabled, the heartbeat is up, and the HA state is not synchronized.
- Red – HA is unavailable, and the HA status is not enabled.

Click the **Actions** menu in the upper-right corner of the page to synchronize all services between both CPs and initiate a CP failover.

Synchronizing Services between Control Processors

Before you can initiate a nondisruptive CP failover, all services must be synchronized between both CPs.

1. Click **Switch Overview** in the navigation bar, and then select the **High Availability** tab.
2. Verify that services need to be synchronized by checking the color of the HA **Status** icon.
   If the color is green, services are already synchronized between the CPs.
3. If the HA status is not synchronized, click the **Actions** button in the top-right corner and select **Synchronize**.
4. Click **OK** in the confirmation dialog and wait for the CPs to synchronize the services.
   When the HA **Status** button is green, indicating that the HA status is enabled, the heartbeat is up, and the HA state is synchronized, you can initiate a failover.

Initiating a CP Failover

A CP failover forces the standby CP to become the active CP.

Initiate a CP failover through the action menu on the **Switch Overview** page, **High Availability** tab.

1. Click **Switch Overview** in the navigation bar, and then click the **High Availability** tab.
2. Verify that the HA **Status** icon is green, indicating that the HA status is HA enabled and the heartbeat is up.
3. Click the action button in the top-right corner, and select **Initiate Failover**.
4. Click **OK** in the confirmation message.
   A nondisruptive failover might take about 30 seconds to complete. During the failover, your Web Tools session expires and the login page is displayed. You must log in to Web Tools again to determine the HA status.

Zoning Overview

This chapter describes zoning and provides the procedures to manage zones. An administrator can partition the network into logical groups of devices through zoning. This partition allows the devices to interconnect and prevent access from other devices outside the group, thereby providing increased network security and stability.

Zoning also relieves the network from registered state change notification (RSCN) storms created due to multiple device interactions. The information in the **Zone Configurations** window is collected from the selected switch. Using the **Zoning** tab in the Web Tools Element Manager navigation bar, you can perform the following tasks:

- Create zone aliases
- Create zones
- Create standard zones
- Create peer zones
- Create LSAN zones
- Create LSAN peer zones
- Create zone configurations
- Configure the fabric-lock timeout

For details, refer to the *Brocade Fabric OS Administration Guide*.

Zone Database Size

The zone database size for fabric is:

- 4 MB per fabric and logical switch
- 16 MB per chassis (combined size of all zone databases across all logical switches)

The 4-MB configuration size is allowed only if all switches in the fabric are running Fabric OS v9.0.0 or later. The 16-MB zone database limit is chassis wide, and hence on virtual-fabric enabled systems, the sum of the zone database size of all partitions cannot exceed 16 MB. You can create and save a defined configuration up to 4 MB in the fabric and the compressed configuration size must not exceed 2 MB during config save or enable operation. You can configure a larger number of zone configurations, zones, and zone aliases in the fabric; in multiple logical switches existing in the virtual fabric configuration on the same chassis.

Naming Conventions

Zone objects, such as the zone configuration name, zone name, and alias name, can have the following characters, if all switches in the fabric and both CPs in a chassis system are running Fabric OS 8.1.0 or later.

- Start with a number or a letter.
- Contain a hyphen (-) other than the first character.
- Contain an underscore (_) other than the first character.
- Contain a dollar sign ($) other than the first character.
- Contain a caret (^) other than the first character.

You can use these characters in the zone object names while creating them and subsequently on add, remove, delete, show, enable, copy, rename, and expunge commands related to zone objects.

Standard Zones

Standard zoning enables you to partition a storage area network (SAN) into logical groups of devices that can access each other. For example, you can partition a SAN into two zones, winzone and unixzone, so that the Windows servers and storage do not interact with the UNIX servers and storage. Zones can be configured dynamically. They can vary in size, depending on the number of fabric-connected devices, and devices can belong to more than one zone. Because zone members can access only other members of the same zone, a device not included in a zone is not available to members of that zone.

Peer Zones

Peer zoning introduces the concept of principal zone members and nonprincipal peer members that are defined within a single zone. A peer zone can be created with one or more devices designated as a principal device for that zone. Peer zoning allows the principal zone members to communicate with nonprincipal peer members. Within a zone, principal and peer members can communicate with one another. However, peer members cannot communicate with other peer members, and principal members cannot communicate with other principal members. If multiple principal members are present within the same peer zone, they will not be visible to one another, nor will they be able to communicate with one another. Peer zoning supports LSAN and QoS peer zoning. In Fabric OS v8.1.0 and later, you can add aliases to a peer zone. However, you cannot move a mixed-type alias to a peer zone. The alias members must be of the same type as the existing peer zone members. For example, if a peer zone is of type Domain, Port Index, the alias must also be of the Domain, Port Index type. If the switches in the fabric are not compatible with the configuration, an error message is displayed.

LSAN Zones

An LSAN zone enables device connectivity between fabrics that are connected in Fibre Channel Routing (FCR) without forcing you to merge fabrics. Extension switches provide multiple mechanisms to manage inter-fabric device connectivity. Zones that contain hosts and targets that are shared between the two fabrics must be explicitly coordinated. To share devices between any two fabrics, you must create an LSAN zone in both the fabrics. The name of an LSAN zone must begin with the prefix LSAN_. The prefix is not case-sensitive.

LSAN Peer Zones

An LSAN peer zone combines the properties of both LSAN zoning and peer zoning. You can select any edge fabrics or backbone fabric to create an LSAN peer zone. The name of an LSAN peer zone must begin with the prefix LSAN_. The prefix is not case-sensitive.

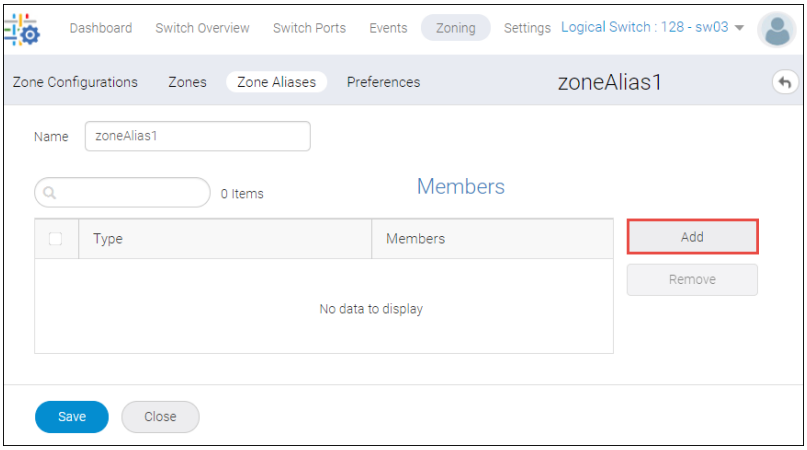
Creating and Editing Zone Aliases

A zone alias is a logical group of the domain, port index numbers, or WWNs. Zone aliases facilitate zone configuration by using the alias instead of selecting individual WWNs or domain, port index numbers.

Creating a Zone Alias

To create zone aliases, perform the following steps:

1. Click **Zoning** in the navigation bar, and then select the **Zone Aliases** tab. The **Zone Aliases** window is displayed.
2. Click the (**+**) icon on the top-right corner of the window.
3. Enter the zone alias name in the **Name** field. As a best practice, use a unique alias name for a member.
4. Add members to the zone alias.
    1. Click the **Add** button.



    2. Select either **Select discovered Devices/Ports** to choose the members from a list or **Enter manually** to type them in yourself.
    3. Select the type of the zone member (WWN or Domain, Port Index) from the drop-down.
    4. Select the discovered members or type the name of the offline members, and then click (›) to move them to the **Selected Members** list.

5. Click **OK** to add the members to the zone alias.
6. Click **Save** to save the zone alias.

Editing an Existing Zone Alias

To edit an existing zone alias, perform the following steps:

1. Click **Zoning** in the navigation bar, and then select the **Zone Aliases** tab. The **Zone Aliases** window is displayed.
2. Select the ( ) icon next to the zone alias that you want to edit, and then click **View**.
3. Select **Save As** from the **Save** drop-down and perform the required changes. You can re-name the alias or modify the existing zone alias with the same name.

   You can remove the selected members by selecting **Remove** button.
4. Click **Save**.

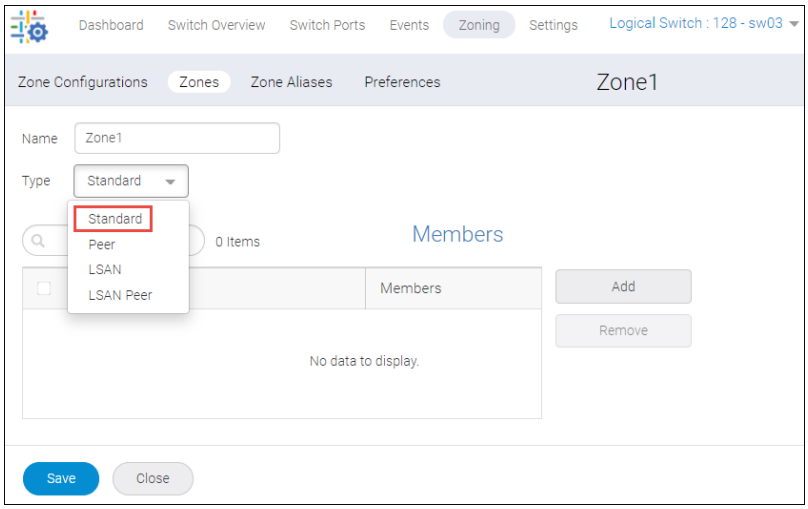
Creating and Editing Zones

You can create new zones for a fabric. If you want to create a different type of zone, you can select from any of the zone types. You can create any of the four types of zones such as standard zones, peer zones, LSAN Zones, and LSAN peer zones.

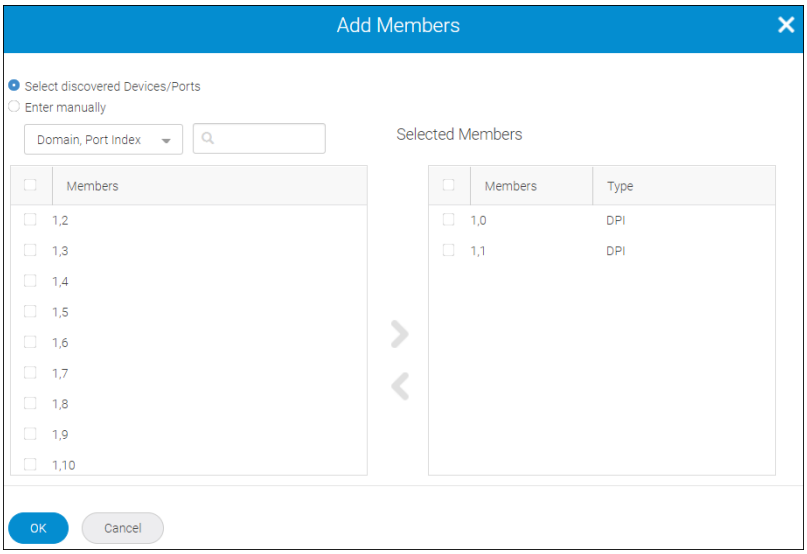
Creating Zones

To create a zone, perform the following steps:

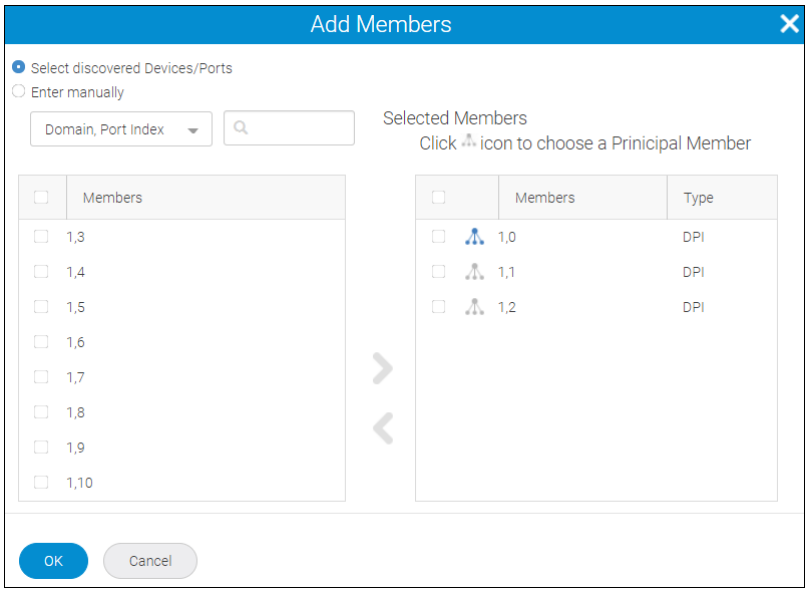
1. Click **Zoning** in the navigation bar, and then select the **Zones** tab.
2. Click the (**+**) icon on the top-right corner of the window.
3. Enter the name of the zone, and then select zone type from the **Type** drop-down.



4. Add members to the zone:
   a) Click the **Add** button. The **Add Members** window is displayed.
   b) Select the type of the zone member (WWN; Domain, Port Index; or Alias) from the drop-down.
   c) Select either **Select discovered Devices/Ports** to choose the members from a list or **Enter manually** to type them in yourself, and then click ( ) to move them to the **Selected Members** list.



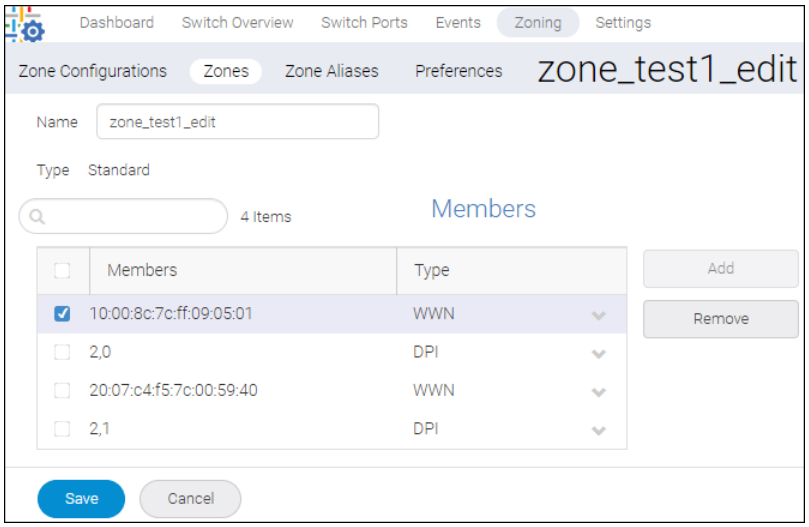
- For a peer zone and an LSAN peer zone, click the ( ) icon to add a selected member as a principal member in the zone. At least one principal member must be present in a peer zone or in an LSAN peer zone.
- The nonselected members are present as peer members of the principal members in the zone.
- When configuring an LSAN zone, Web Tools does not support members of the same name as the same member already present in the other edge fabric. Newly created peer zones are automatically activated in the fabrics based on the devices selected. For example, if a host that has ports in fabrics A and B is chosen and target ports from fabrics A and B are selected, LSAN peer zones are created and activated in both fabrics A and B.



Editing an Existing Zone

To edit an existing zone, perform the following steps:

1. Click **Zoning** in the navigation bar, and then select the **Zones** tab.
2. Select the ( ) icon next to the zone that you want to edit, and then click **View**.
3. Select **Save As** from the **Save** drop-down and perform the required changes. You can re-name the zone or modify the existing zone with the same name.



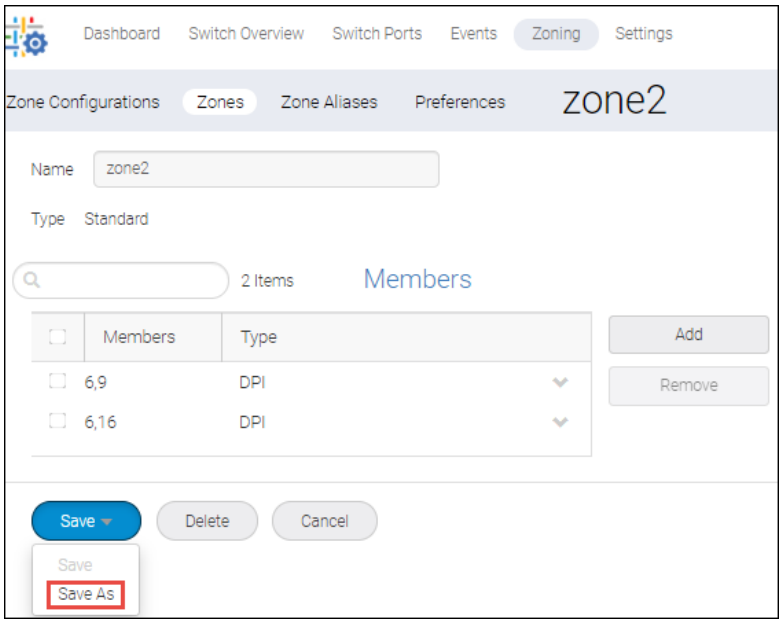
You can remove the selected members by selecting the **Remove** button.

4. Click **Save**.

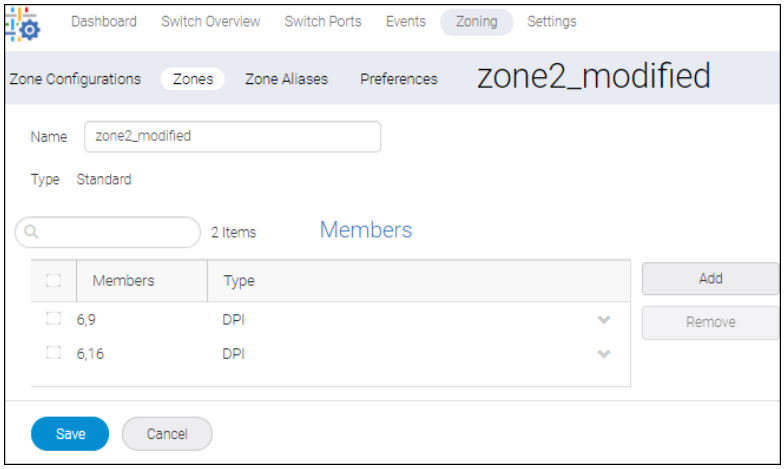
Cloning an Existing Zone

To clone an existing zone, perform the following steps:

1. Click **Zoning** in the navigation bar, and then select the **Zones** tab.
2. Select the ( ) icon next to the zone that you want to clone, and then click **View**.
3. Click **Save As** from the **Save** drop-down to clone the zone with a different name.



4. Enter a name, and then click **Save**.



5. Click **OK**.

   The cloned zone is saved under the **Zones** window.

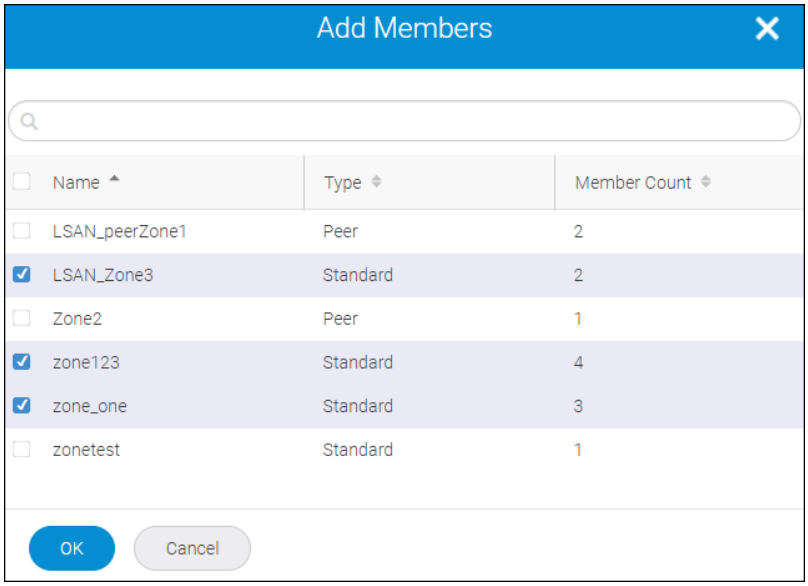
Configuring Zones

A zone configuration is a group of one or more zones. A zone can be included in more than one zone configuration. When a zone configuration is activated, all zones that are members of that configuration are in effect.

Creating and Activating a Zone Configuration

To create and activate a zone configuration, perform the following steps:

1. Click **Zoning** in the navigation bar. By default, the **Zone Configurations** window is displayed.
2. Click the (**+**) icon on the top-right corner of the **Zone Configurations** window.
3. Enter a name for the zone configuration.
4. Click **Add** to add one or more zones to the zone configuration. The **Add Members** window is displayed.
5. Select the existing zones to add to the zone configuration.
6. Click **OK** to add the zones to the zone configurations.



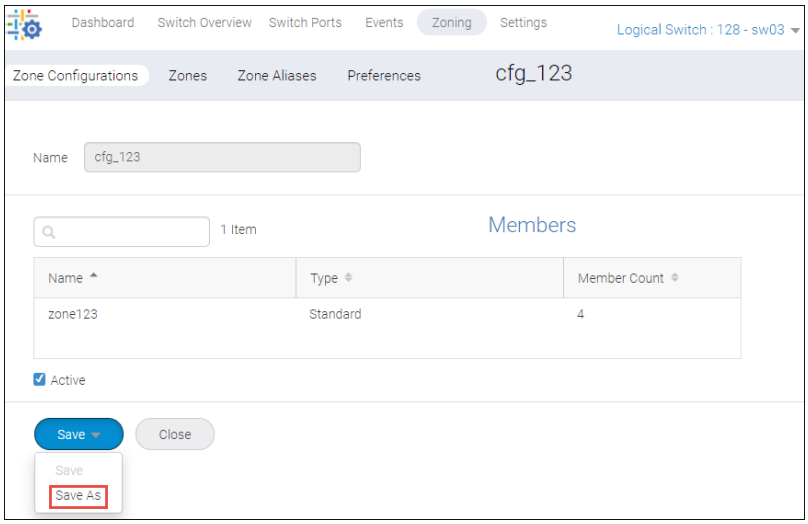
7. Click **Active** to activate the zone configuration, and then click **Save**.

NOTE
You can have only one active zone configuration in a fabric.

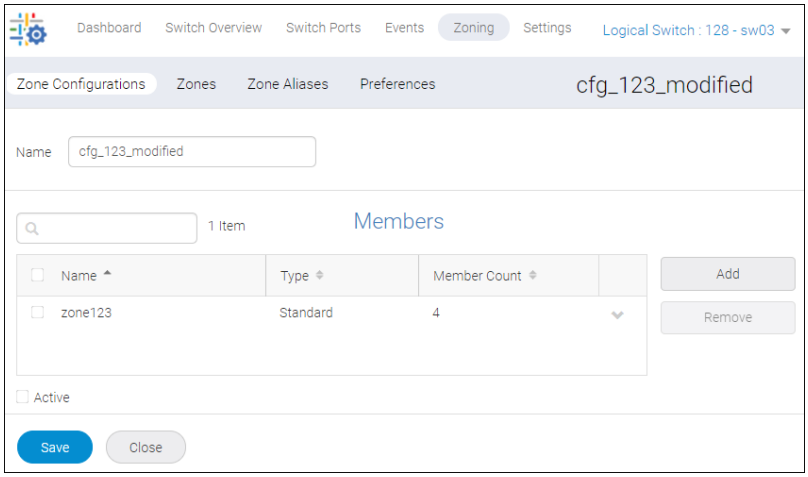
Cloning an Existing Zone Configuration

To clone a zone configuration, perform the following steps:

1. Click **Zoning** in the navigation bar. By default, the **Zone Configurations** window is displayed.
2. To clone a zone configuration, select an existing zone configuration. The selected zone configuration is displayed. You can clone both **Active** and **InActive** zone configurations.
3. Click **Save As** from the **Save** drop-down to clone the configuration with a different name.



4. Enter a name, and then click **Save**.



5. Click **OK**.

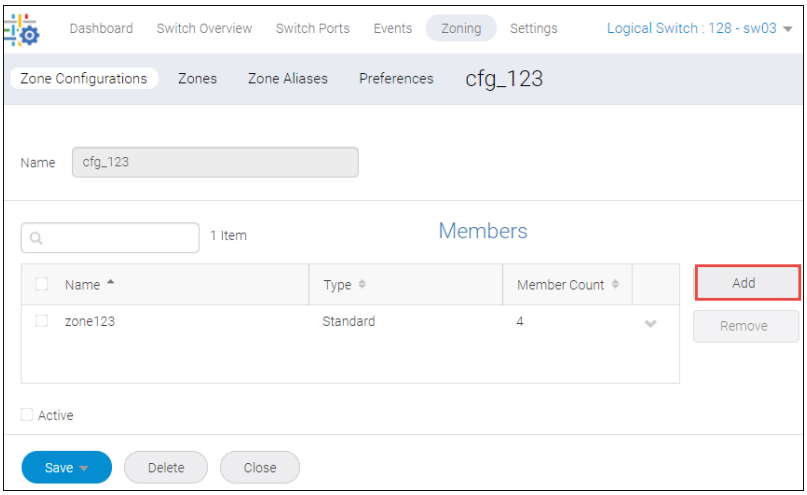
   The cloned zone configuration is saved under the **Zone Configurations** window.

Modifying an Existing Zone Configuration

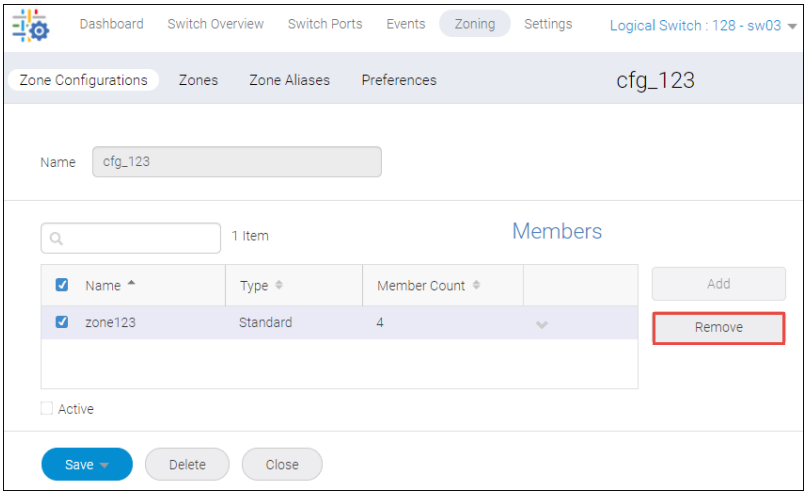
> **NOTE**
> You cannot modify an active zone configuration directly. To modify an active zone configuration, you must clone the zone configuration with a different name.

To modify an existing zone configuration, perform the following steps:

1. Click **Zoning** in the navigation bar. By default, the **Zone Configurations** window is displayed.
2. Select the desired zone configuration with the **InActive** status. The selected zone configuration is displayed. Modify (add, remove, or both) as required.
   1. To add a zone, click the **Add** button, select the desired zone in the **Add Members** window, and then click **OK**.



2. To remove a zone, select the zone that you want to remove, and then click **Remove**. The zone is removed from the **Members** list.



Removing a zone from the zone configuration deletes all the references of that zone from that zone configuration.

3. Click the **Save** button, and then click either **Save** or **Save As** if you want to save the configuration with a different name.
4. Click **OK** in the confirmation dialog to save the changes.

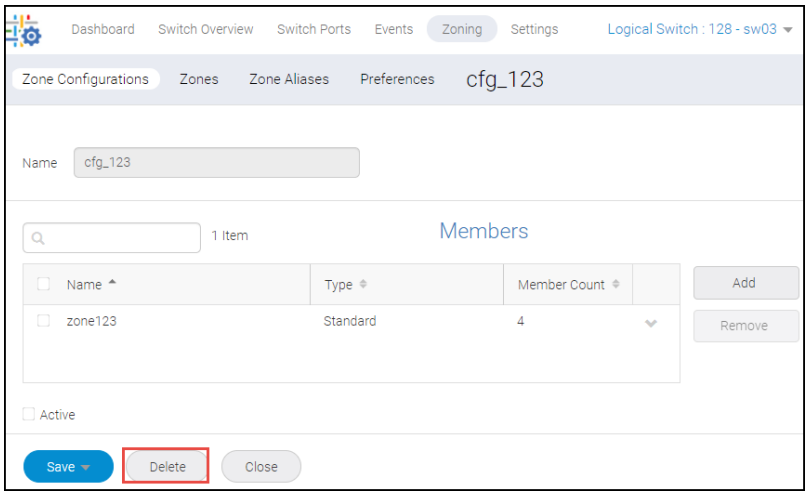
Deleting a Zone Configuration

NOTE

- The last zone member of the active zone configuration cannot be deleted. Any attempt to delete the last zone results in an error message indicating that the zone was not found.
- You cannot delete an active zone configuration from the fabric.

To delete a zone configuration, perform the following steps:

1. Click the zone configuration that you want to delete.
   The selected zone configuration is displayed.
2. Click **Delete** button. The **Delete** button appears only for the inactive zone configurations.



The **Delete Zone Configuration** message is displayed.

3. Click **OK**.

   The selected zone configuration is deleted from the **Zone Configurations** window.

Setting Zone Preferences

You can configure the zoning policy and the zone fabric-lock failsafe timer using the **Preferences** tab. You can also clear zones from the **Preferences** tab.

Configuring a Zoning Policy

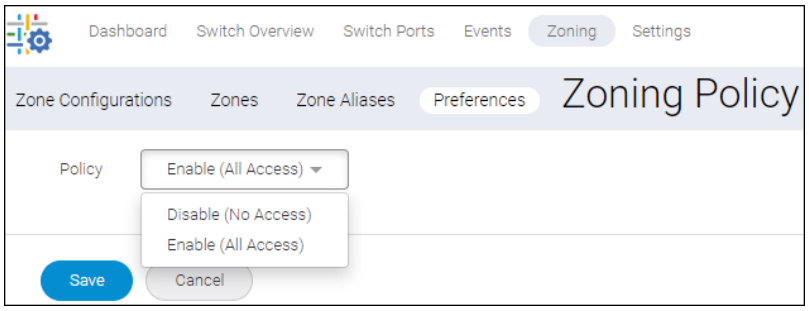
The zoning policy controls device access when there is no effective zone configuration. The zoning policy has two options:

- **Enable (All Access)** – All devices within the fabric can communicate with all other devices.
- **Disable (No Access)** – Devices in the fabric cannot access any other device in the fabric.

The zoning policy applies to the entire fabric, regardless of the switch model. The default setting is **Enable (All Access)**. When you disable the zoning configuration in a large fabric with thousands of devices, the name server indicates to all hosts that they can communicate with each other. Each host can receive an enormous list of PIDs and ultimately cause other hosts to run out of memory or crash. To ensure that all devices in a fabric do not see each other during a configuration disable operation, set the zoning policy to **Disable (No Access)**.

To configure a zoning policy, perform the following steps:

1. Click **Zoning** in the navigation bar, and then select **Preferences**. The **Preferences** window is displayed.
2. Click **Edit** next to the **Zoning Policy** option. The **Zoning Policy** window is displayed.
3. Select either **Disable (No Access)** or **Enable (All Access)** from the **Policy** drop-down.
4. Click **Save**.

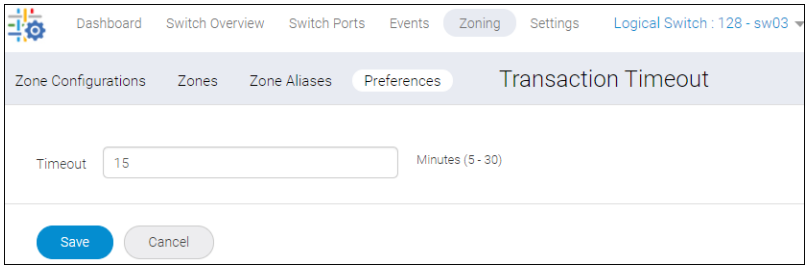


Configuring the Zone Fabric-Lock Failsafe Timer

Fabric OS provides fabric-level detection support that warns you if a transaction is open on a remote switch. However, it does not prevent you from committing changes if the current transaction exists across the fabric. The Zone Fabric Locking feature is extended to all switches in the fabric. This feature is enabled by default. If a zone edit or commit command is occurring in a fabric, you cannot perform a zone edit or commit on the same or another switch for a default timeout period of 5 minutes. A lock request is sent at the beginning of a zone edit operation. The Fabric Lock Failsafe Timer is configurable and it is a fabric-wide setting. When a zone fabric lock is active, a failsafe timer is started on all remote switches. When the failsafe timer expires, the open zone transaction is not aborted. If the same user attempts to resume the transaction by performing another edit or commit operation after the zone fabric lock has expired, the transaction is allowed and the fabric lock is restarted. If a different user attempts to start a new transaction after the first user's transaction timer has expired, the transaction is allowed and the first user's transaction is aborted before the second user's transaction starts.

To configure the zone fabric-lock failsafe timer, perform the following steps:

1. Click **Zoning** in the navigation bar, and then select **Preferences**. The **Preferences** window is displayed.
2. Click **Edit** next to the **Transaction Timeout** option. The **Transaction Timeout** window is displayed.
3. Provide a timeout value in the **Timeout** field. By default, the timeout value is set to 5 minutes.

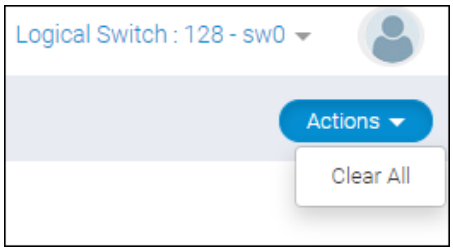


4. Click **Save**.

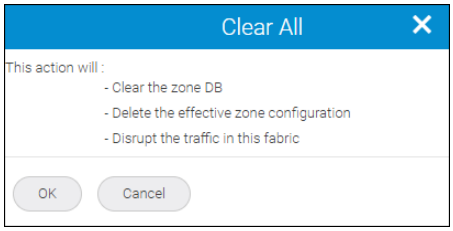
Clearing the Zone Database

The **Clear All** option disables the zoning on the fabric and deletes the entire zone database. It clears all aliases, zones, and configurations in the defined configuration. The **Clear All** option sets the policy to default zoning policy.

1. Click **Zoning** in the navigation bar, and then select **Preferences**. The **Preferences** window is displayed.
2. From the top-right corner of the window, select **Clear All** from the **Actions** menu. The **Clear All** window is displayed.



3. Click **OK**.



Performing a Firmware Upgrade

Upgrading the Fabric OS firmware involves a firmware download and swapping the partitions to upgrade.

During a firmware download, the switch restarts, and the browser temporarily loses connection with the switch. When the connection is restored, the new software version is installed and activated on the switch. You must close all Web Tools windows and log in again to avoid a firmware version mismatch. Note that for chassis-based switches, you might get pop-up messages that imply that the loss of connection is temporary and will soon be resolved. You must still close all windows and log in again.

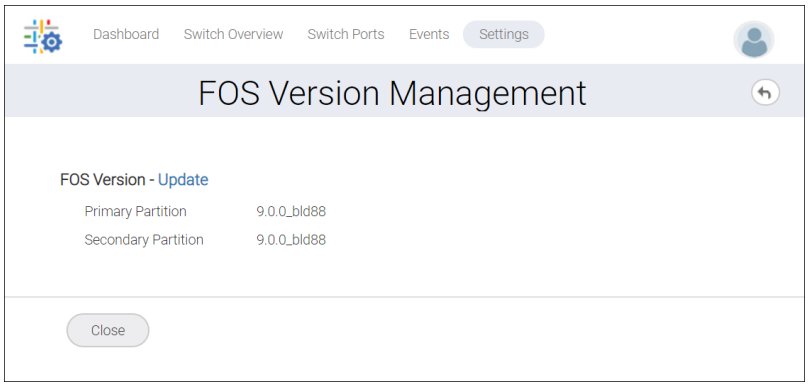
NOTE

If you are upgrading the firmware using Web Tools versions Fabric OS v8.2.1c and earlier or versions Fabric OS v8.2.2 to Fabric OS v9.0.0 and later, use the Fabric OS command line interface (CLI) or SANnav. Ensure that the end-user license agreement is accepted during the firmware download. You can also use Web Tools to upgrade firmware from Fabric OS v9.0.0 and later.

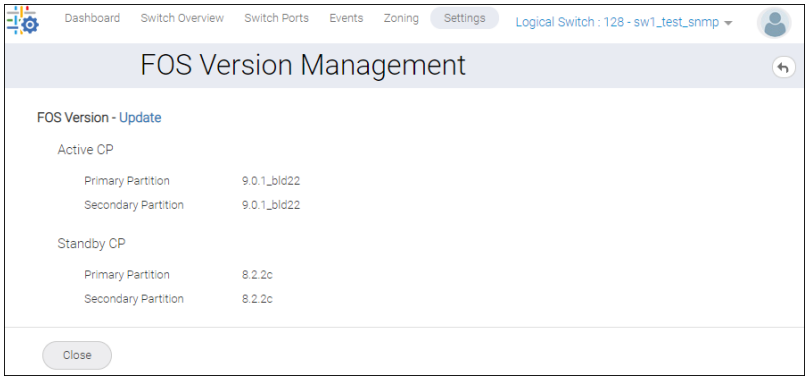
When you request a firmware download, the system first checks the size of the file being downloaded. If the compact flash does not have enough space, Web Tools displays a message and the download does not occur. In such cases, contact your switch support supplier.

To upgrade to a new firmware version, perform the following steps:

1. Click **Settings** in the navigation bar, and then select **FOS Version Management**. The **FOS Version Management** window is displayed.



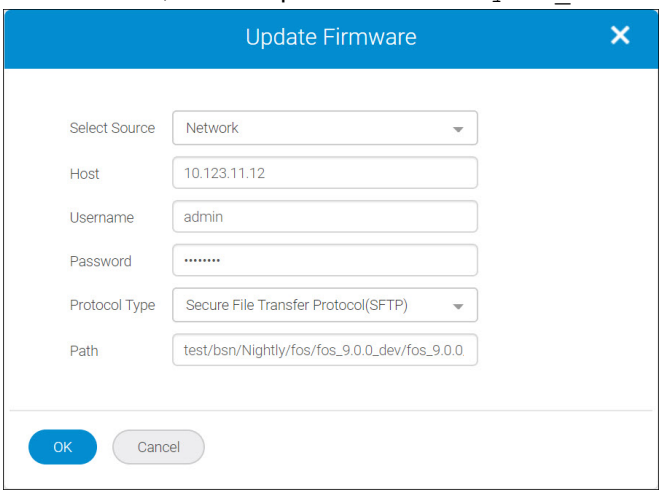
For a chassis, you can view the firmware version of the primary and secondary partition of both the active and standby CPs.



2. Click the **Update** link. The **Update Firmware** dialog is displayed.
3. Perform any one of the following:
   a) Download the firmware from the network source.

      If you are downloading the firmware from the network source, perform the following steps:

      1. Select **Network** from the **Select Source** drop-down.
      2. Enter the host name or IP address, user name, password, and a fully qualified path to the firmware folder. You can enter the IP address in either IPv4 or IPv6 format.
      3. Select the type of protocol in the **Protocol Type** field : **Secure Copy Protocol (SCP)**, **Secure File Transfer Protocol (SFTP)**, or **File Transfer Protocol (FTP)**.
      4. Enter the path name in the **Path** field in the following structure: `//<directory>/<fos_version_directory>` . In this syntax, `<directory>` is the path up to the entry point of `<fos_version_directory>` , and `<fos_version_directory>` is where the unzipped version of Fabric OS is located, for example: `//directory/FW_directory/v9.2.0` .

   b) Download the firmware from the USB.

      If you are downloading the firmware from the USB, perform the following steps:

      1. Click **USB** from the **Select Source** drop-down.
      2. Specify only the fully qualified directory path as the firmware file path.

4. Click **OK** to proceed with the firmware download.
5. Read the terms and conditions of the end-user license agreement, and then click **Agree**. The firmware download begins with a warning message that specifies the time it will take to complete. If you try to initiate the download when a download is in progress, a warning message is displayed. A reboot is required to activate the newly downloaded firmware. This reboot is done automatically. Web Tools invalidates all windows because the upfront login is always enabled and cannot be disabled.
6. Close all Web Tools applications and log in again.

   When Web Tools reports that the firmware download has completed successfully, this indicates that a basic confidence check, package retrieval, package unloading, and verification are successful. The firmware is downloaded to the secondary partition and then the partitions are swapped, so the secondary partition becomes the primary partition.

IP Address Management

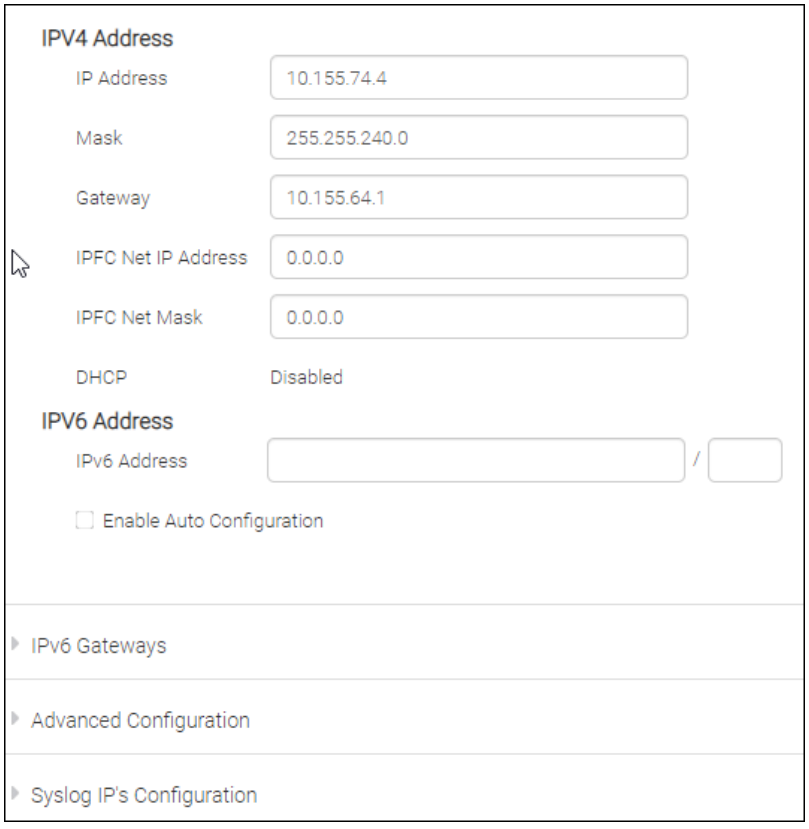
The IP Address Management feature allows you to manage the IPv4 and IPv6 configuration for the switch that you launched through Web Tools. IP Address Management comprises Advanced, Auto IP Configurations, and Syslog IP Configurations.

Before proceeding, collect all the information that you need to configure the Ethernet IP interface: the subnet mask, gateway IP address, IPFC, and subnet mask for your system.

> **NOTE**
> When you configure or change any of these items, you typically lose the network connection to the switch. To remedy this situation, close all current windows and restart Web Tools with the new IP address.

To configure IP address management, perform the following steps:

1. Select the **Configuration** > **IP Address Management** on the **Settings** page.



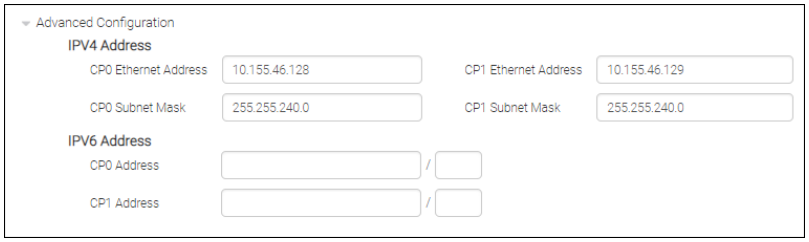
The IPFC address is specific for each logical switch and is set to FC0 for switches that do not support Virtual Fabrics.

2. Enter values for **IP Address**, **Mask**, **Gateway**, **IPFC Net IP Address**, **IPFC Net Mask**, and **DHCP** under **IPV4 Address**. For this example, values have been entered.
3. Specify an IPv6 address. For this example, the field is left blank.
4. Check **Enable Auto Configuration** to enable automatic configuration of the IPv6 addresses. This displays a list of autoconfigured IPv6 addresses.

Eight autoconfigured addresses are created per switch, and up to 24 addresses are created for a DCX® chassis or X6 chassis (eight per chassis and eight per each installed CP).

5. To display a list of current IPv6 gateways, scroll down the **IP Address Management** page and click the down arrow for **IPv6 Gateways**.

6. To view or configure the IPV4 and IPv6 address of both CP0 and CP1 that are available on the chassis-based system, click the down arrow for **Advanced Configuration**.



For an IPv4 address, you can configure a subnet mask along with the Ethernet IP address.

7. Click the down arrow for **Syslog IP's Configuration**. This allows you to add new syslog trap recipients.

You can also delete an existing recipient and its managing server IP by checking the appropriate box and clicking **Remove**.

8. If you want to add a new IP address, click the **Add** button.

You can click the **Add** button to add a new IP Address for a maximum of six recipients.

Enter an IP address and click **OK**. The new IP is displayed in the **IP Addresses** table.

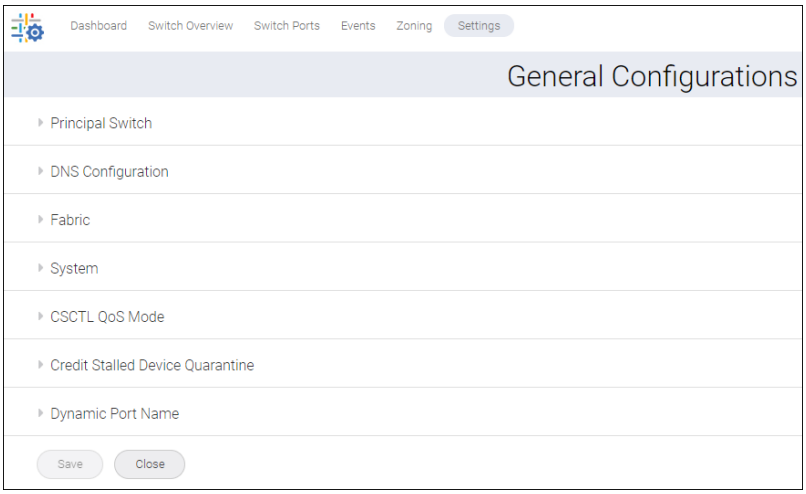
If you want to delete an address, check the appropriate box and click **Remove**.

9. Click **Save** at the bottom of the **IP Address Management** window to preserve all the configuration changes.

General Configuration

General configuration enables you to set the basic switch-based configurations.

Figure 11: General Configurations Window



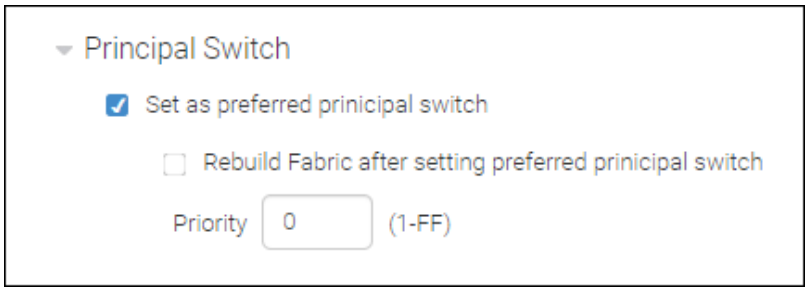
Setting the Principal Switch

In a fabric with one or more switches interconnected by an inter-switch link (ISL) or inter-chassis links (ICLs), a principal switch is automatically elected. This switch maintains time (the clock) for the entire fabric and manages domain ID assignments within the fabric.

The Principal Switch feature allows you to set the preference for a switch to become the next principal switch in the fabric.

To set the preference, perform the following steps:

1. Select **Settings** > **Configuration** > **General Configuration**, and then click **Principal Switch**.



NOTE
The principal switch can be configured only when the switch is disabled.

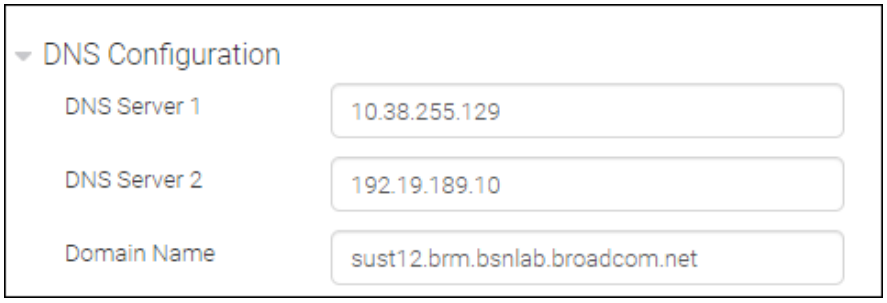
2. Select **Set as preferred principal switch** to establish the switch as the principal switch in the next fabric rebuild.
3. Assign a priority for the switch in the text box.
4. Select **Rebuild Fabric after setting preferred principal switch** to apply the changes with the principal switch and trigger a rebuild forcefully.
5. Click **Save** to preserve those changes for the switch in which it is configured.

Configuring the Domain Name Server

The DNS Configuration feature allows you to view and configure the DNS (Domain Name Server) IP address and Domain Name information for the switch in which you are logged in through Web Tools.

To configure the DNS IP address and domain name, perform the following steps:

1. Select **Settings** > **Configuration** > **General Configuration**, and then click **DNS Configuration**.
   Initially, the fields for DNS Server 1 and 2 are blank. After you click each field, it is populated with default values.



2. Enter the DNS server IP address with the specified format.
3. Enter a value for the **Domain Name**.
4. Disable the switch. This applies the configuration to the switch.
5. Click **Save** to apply the updates to the switch.

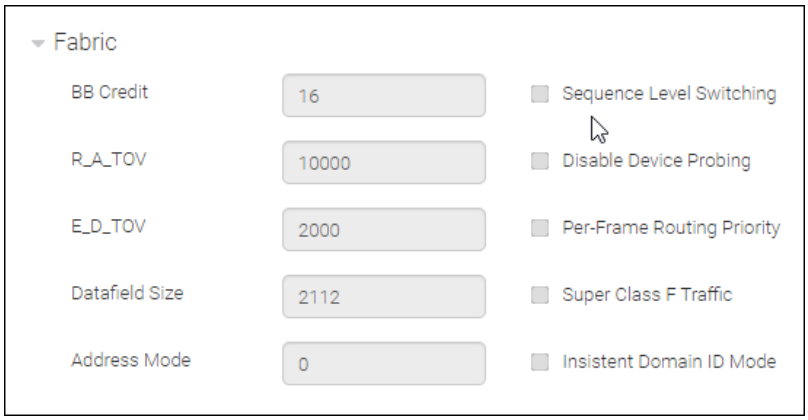
Configuring Packet Data Transmission Data for a Fabric

The Fabric feature allows you to configure the values for packet data transmission on the switch.

> **NOTE**
> Before applying these configuration settings, you must first disable the switch. Otherwise, Web Tools will not allow you to change these fields.

To configure the transmission data, perform the following steps:

1. Select **Settings** > **Configuration** > **General Configuration**, and then click **Fabric**.



2. Specify the **BB Credit**.

   This is the number of buffers (that is, BB credits) available to attached devices for frame receipt.

   Values can range from 1 through 27. The default is 16.

3. Specify **R_A_TOV**.

   This variable, the resource allocation timeout value, works with E_D_TOV to determine switch actions when an error condition exists.

   The default is 10000 milliseconds. Values can range from (2*E_D_TOV) through 120000 and must be multiples of 1000.

4. Specify **E_D_TOV**.

   This timer, the error detect timeout value, is used to flag a potential error condition when an expected response is not received within a given time.

   The default is 10000 milliseconds. Values can range from 1000 through (R_A_TOV/2) and must be multiples of 1000.

5. Specify **Datafield Size**.

   This value specifies the largest possible data field size (in bytes).

   Values can range from 256 through 2112.

6. Specify **Address Mode**.

   This represents the currently configured addressing mode in the switch.

7. Select **Sequence-Level Switching** to enable frames of a particular group to be transmitted together.

   If this option is not selected, frames are transmitted interleaved among multiple sequences.

   Typically, sequence-level switching is disabled for better performance. However, some host adapters have issues when receiving interleaved frames among multiple sequences.

8. Select **Disable Device Probing** to ensure that devices not registered with the Name Server are not present in the Name Server database.

   NOTE
   You can configure this mode only if the switch N_Port discovery process (that is, PLOGI, PRLI, and INQUIRY) causes an attached device to fail.

9. Select **Per-Frame Routing Priority** to enable you to configure per-frame routing priority.

   When this option is enabled, the virtual channel ID and the frame header together form the final virtual channel ID.

10. Select **Suppress Class F Traffic** to disable translate addressing and allow private devices to communicate with public devices.

    NOTE
    This configuration is applicable only if VC-encoded address mode is also set.

11. Select **Insistent Domain ID Mode** to make the current domain ID insistent across reboots, power cycles, and failovers.

    NOTE
    This mode is required fabric-wide to transmit FICON data.

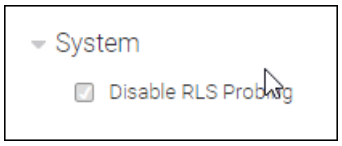
Configuring the System Read Link Status

The System feature enables you to disable or enable read link status (RLS) probing for F_Ports and FL_Ports.

If device probing is enabled, an embedded port performs a PLOGI and attempts a PRLI into the device to retrieve information to enter into the Name Server (NS). Successful probing reveals the probing status of the device along with the error stats.

To configure RLS probing, perform the following steps:

1. Select **Settings** > **Configuration** > **General Configuration**, and then click **System**.



2. Select **Disable RLS Probing** to disable probing.
3. Click **Save** to apply this configuration to the switch.

Setting CSCTL QoS Mode

The CSCTL QoS Mode feature enables you to configure switch-level Class-Specific Control (CSCTL) Quality of Service (QoS).

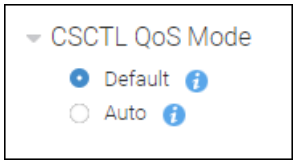
After the CSCTL mode is enabled on an F_Port or FL_Port, the CSCTL value in the frame header of all the incoming frames on that port is used to index into the ASIC's CSCTL database table to compute the VC number. This number defines the frame's flow priority throughout its life in the fabric until it exits the fabric through another F_Port to FL_Port.

The QoS links (inter-switch links [ISLs]) preserve this classification during the frame's transit across all the hops in the fabric.

To manage the traffic priority between specified host-target pairs, you might configure QoS zones to assign pairs high, medium, or low QoS-level priority for that level, and then identify those pairs as members of the appropriate zone. When both CSCTL mode and QoS zones are enabled, QoS zones lose priority to CSCTL mode.

To configure CSCTL Quality of Service mode, perform the following steps:

1. Select **Settings** > **Configuration** > **General Configuration**, and then click **CSCTL QoS Mode**.



2. Click the **Default** radio button to clear the previously configured CS_CTL to VC_mapping and set one-to-one mapping between the CS_CTL value and the VC number.
3. Click the **Auto** radio button to allow for both one-to-one mapping and mapping to more than one virtual channel.
4. Before applying the changes for this configuration, consider the following:
   - If the product type is a director, turn on the blade power off and then power.
   - If product type is a switch, reboot the product.
5. Click **Save** to apply these configurations to the switch.

   Once the change is applied and before the change is configured, a switch reboot warning message is displayed.

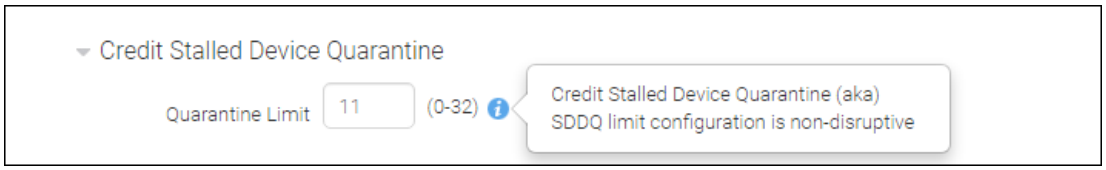
Establishing Credit Stalled Device Quarantine

The Credit Stalled Device Quarantine (CSDQ) feature enables you to reduce unnecessary side effects, such as backpressure caused by a slow draining device. The CSDQ-supported switches quarantine such devices by restricting or moving them. Because this impacts switch CPU performance, quarantine is limited to 32 devices and is configurable.

NOTE
CSDQ is a chassis-level configuration, and so this number is for the entire chassis (including all switches in the VF environment).

To set CSDQ, perform the following steps:

1. Select **Settings** > **Configuration** > **General Configuration**, and then click **Credit Stalled Device Quarantine**.



2. Set the **Credit Stalled Device Quarantine** limit.
3. Click **Save** to apply this configuration to the switch.

Configuring a Dynamic Port Name

The Dynamic Port Name feature allows you to display any available field as part of the port name.

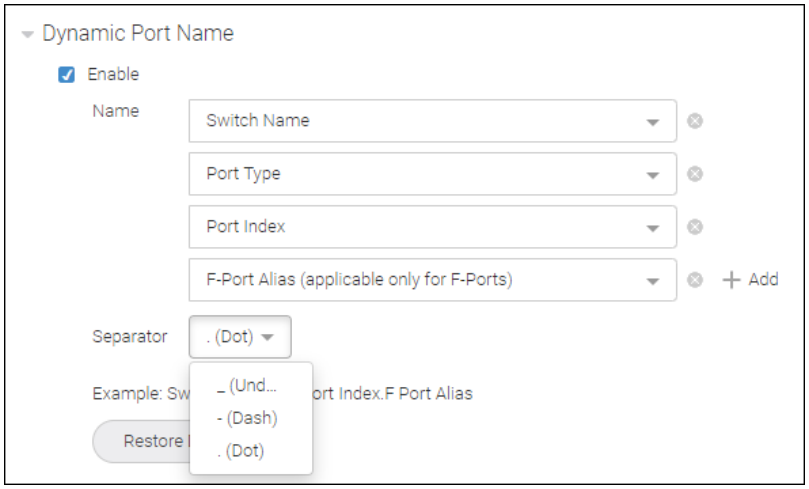
By default, the supported list includes Switch Name, Port Type, Port Index, and Slot Number. You must select at least one field in this list to set the dynamic port name format.

The supported separators are the dot (.), dash (-), and underscore (_; default).

NOTE
You can configure the Dynamic Port Name feature even if the switch is enabled.

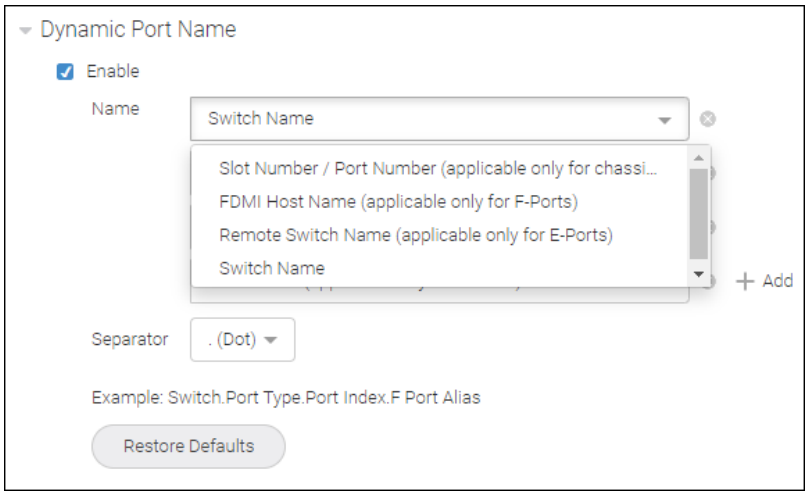
To configure the Dynamic Port Name, perform the following steps:

1. Select **Settings** > **Configuration** > **General Configuration**, and then click **Dynamic Port Name**.
2. Check **Enable**.

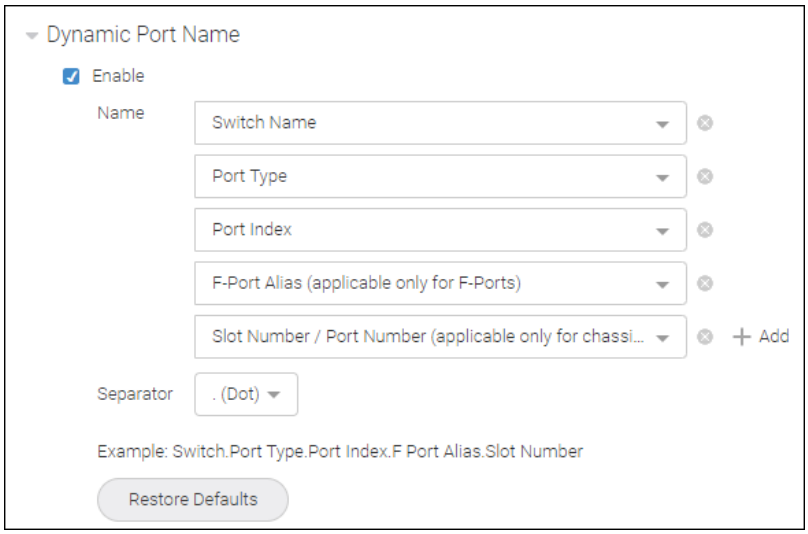


By default, the name string Switch_Port Type_Port Index_Slot Number is generated.

3. If you do not accept the default string, you have two options:
   - You can select an available field from the drop-down for any of the existing name fields.

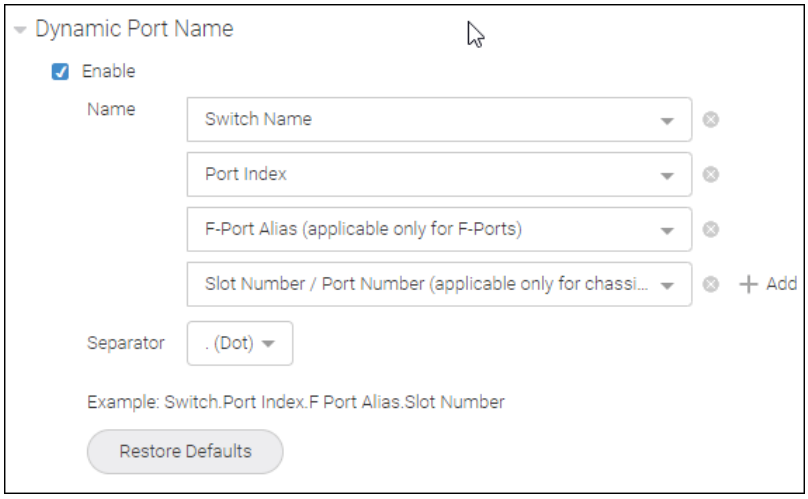


   The name in the field changes and the new field replaces the old one in the name string.
   - Alternatively, you can add **+ Add** or delete **x** from the string as needed.
     Through the **+ Add** option, you can expand the list of available fields to include the F-Port alias, remote switch name, and FDMI host name, and this field is appended to your name string. These fields are visible when you click the down arrow for any of the current fields.



Typically, there is a common field to separate each field of the dynamic port name. So if you were to use the default fields, you could generate the field name string Switch_Port Type_Port Index_Slot Number (for example, sw0_port1_01_10).

If you delete a name field, it is dropped from the name string and made available in each of the drop-downs during the next **+ Add** action. So, if you dropped **Port Type**, it would disappear from the name string.



4. Click **Save** to apply this new port name to the switch.

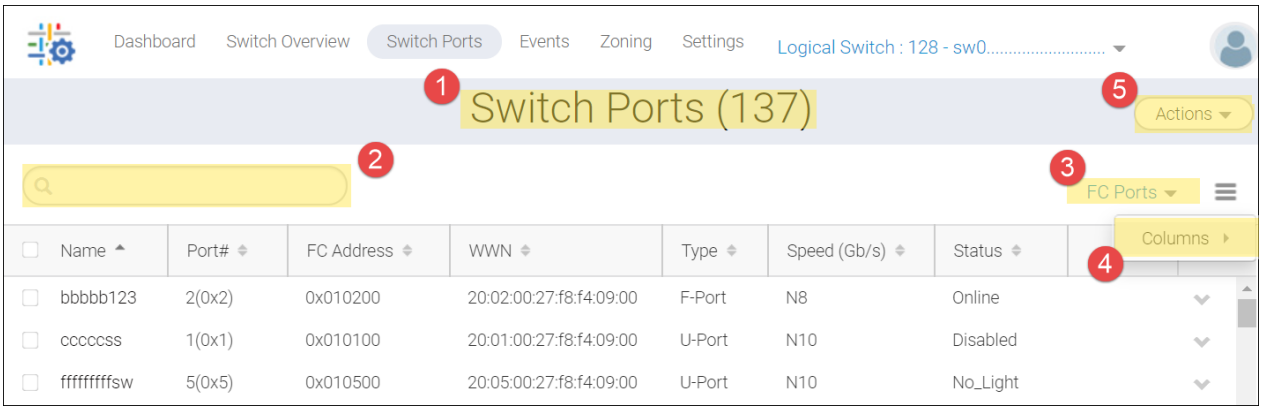
Port Management - Switch Port Overview

This section describes managing port configurations and performing advanced configurations for multiple ports.

You can perform the following functionalities with the **Switch Ports** window.

- Manage the port configurations with the real-time information on the switch ports
- View basic port information and statistics
- View error statistics of the ports and statistical information of the frames
- Perform advanced configurations for multiple ports
- Perform the bulk actions, such as renaming, enabling or disabling the ports, and editing port action settings

To view the **Switch Ports** window, click the **Switch Ports** tab from the Web Tools GUI.



1. Switch Name (with port count)
2. Search Bar
3. Port Type Selection
4. Columns
5. Actions

The **Switch Ports** window lists a table of ports with detailed information in a tabular format depending on the type of port and columns selected in the switch. The **Switch Ports** window is refreshed automatically for every 60 seconds and is refreshed immediately when you make any changes to the port through the Web Tools interface.

To manage ports, you must be logged in with the role of switchadmin, admin, basicswitchadmin, operator, or fabricadmin. If you are logged in with a user, securityadmin, or zoneadmin role, you can only view the port information.

The **Switch Ports** window allows you to perform the following tasks:

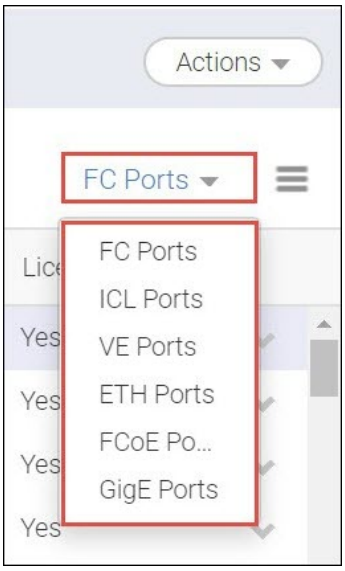
- Filtering Port Type
- Renaming Ports
- Enabling or Disabling Ports
- Viewing Error Statistics
- Reserving Port Licenses
- Releasing Port Licenses
- Customizing Columns
- Performing Advanced Port Configurations

Filtering by Port Type

The **Switch Ports** window displays the following category of ports:

- **FC** – Displays all FC ports on the switch including the physical FC ports and logical ports.
- **ICL** – Displays the inter-chassis link (ICL) switch ports for end devices in the fabric.
- **VE** – Displays the Virtual E (VE) ports that are used for an extension tunnel.
- **ETH (CEE)** – Displays the Converged Enhanced Ethernet (CEE) ports.
- **FCoE** – Displays the Fibre Channel over Ethernet (FCoE) ports.
- **GigE** – Displays all Gigabit Ethernet (GigE) ports.

To select the desired port category, click the **Switch Ports** tab and select the drop-down on the right side of the **Switch Ports** window.



The available columns in the table may vary depends on the category of the port selected. You can customize the columns as required. For more information on customizing columns, see Customizing Columns. The following columns are available for the **FC** port category:

- Name
- Port#
- FC Address
- WWN
- Type
- Speed (Gb/s)
- Slot
- Status
- Health
- Licensed
- Remote Port
- Remote Node
- Port ID
- Port Index
- Additional Port Info
- Controllable
- FEC
- FEC via TTS
- NPIV

The following columns are available for the **ICL** port category:

- Name
- Port#
- Slot
- Type
- Speed (Gb/s)
- Licensed
- Status
- Health
- Additional Port Info
- Port Id
- Port Index
- FEC
- FEC via TTS
- Remote Port
- Remote Node

The following columns are available for the **VE** port category:

- Port ID
- Name
- Port#
- Slot
- Type
- Speed (Gb/s)
- Status
- Health
- Controllable
- Additional Port Info
- Remote Port
- Remote Node

The following columns are available for the **ETH** port category:

- Name
- MAC Address
- Status
- Operational Status
- Speed (Gb/s)
- Port Channel Name
- FCoE Provisioned
- LLDP Status
- LLDP Profile
- DCBX Version

The following columns are available for the **FCoE** port category:

- Name
- Type
- WWN
- Status
- State

The following columns are available for the **GigE** port category:

- Slot
- Port#
- MAC Address
- Media Type

  NOTE
  This is supported only on the 7810 platform.
- Speed (Gb/s)
- Status
- State
- Mode
- Type

Renaming Ports

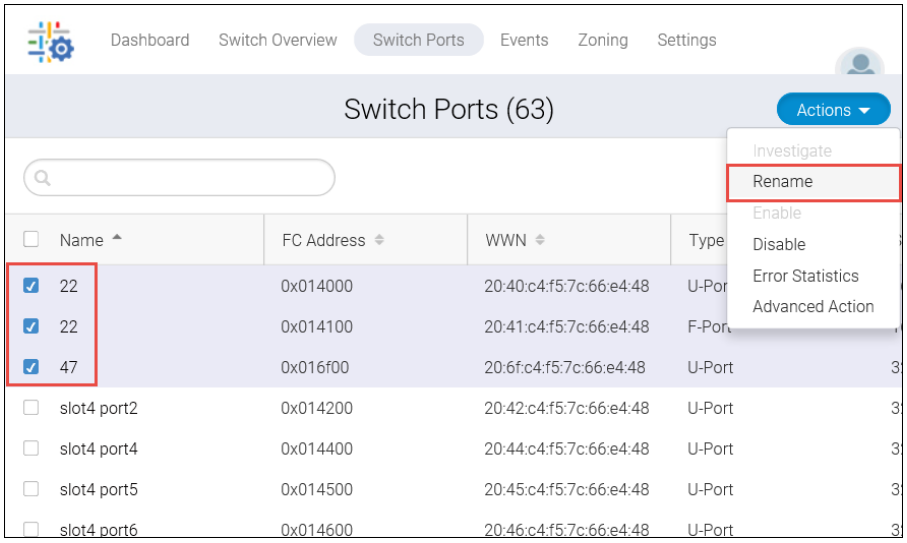
You can rename an individual port or multiple ports at once to facilitate port management, port grouping, and identification. This feature is optional. Using the **Actions** menu in the **Switch Ports** window, you can assign unique port names to rename the automatically assigned numeric port names.

NOTE
You can rename the ports pertaining to all port categories except the GigE port category.

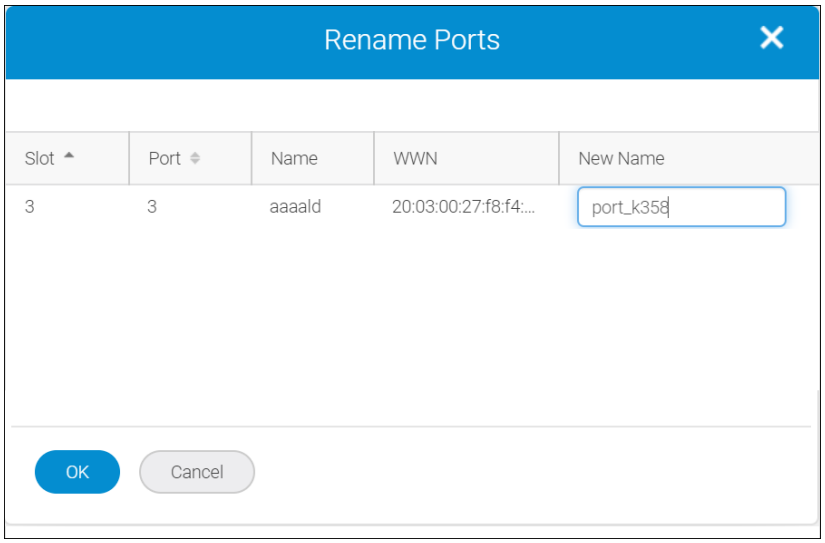
NOTE
You can assign the alphanumeric port names up to 128 characters. The duplicate port names are not allowed. The special characters such as the comma (,), semicolon (;), and (@) symbol are not allowed in the port names.

To rename the switch ports, perform the following steps:

1. Click **Switch Ports** from the navigation bar, and select one or more ports that you want to rename from the **Switch Ports** window.
2. Click the **Actions** menu on the top-right corner, and then select **Rename** from the drop-down.
   The **Rename Ports** window appears.



3. From the **Rename Ports** window, enter the naming values in the **New Name** field.



4. Click **OK** to apply this new port name to the switch.

Enabling or Disabling Ports

This feature allows the ports to remain enabled or disabled across power cycles, switch reboots, and switch enables.

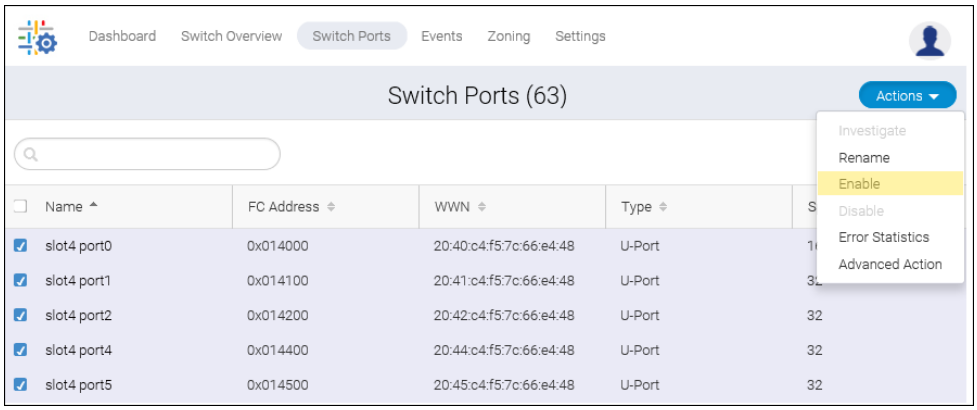
NOTE
You cannot enable the unlicensed ports. Ensure that the appropriate license is installed before enabling a port.

To enable a switch port, perform the following steps:

1. Click **Switch Ports** from the navigation bar, and select one or more ports that you want to enable from the **Switch Ports** window.
2. Click the **Actions** menu on the top-right corner, and then select **Enable** from the drop-down.
   A prompt appears to enable the selected ports.

NOTE

- If you select multiple ports that are in both the enabled and disabled states, both the **Enable** or **Disable** options are available. The selected action is applied to all selected ports.
- If the **Enable** or **Disable** options are not available, this means that the port is already in the enabled or disabled state.



3. Click **OK** to enable the selected ports to the switch.
4. Follow the same steps above and select the **Disable** option in the **Actions** button to disable the selected ports. When you disable a port that is online, a message that warns about the possible traffic disruption. Click **OK** to proceed.

NOTE
If you disable a switch port that was connected to a device, that device cannot be accessed from the fabric.

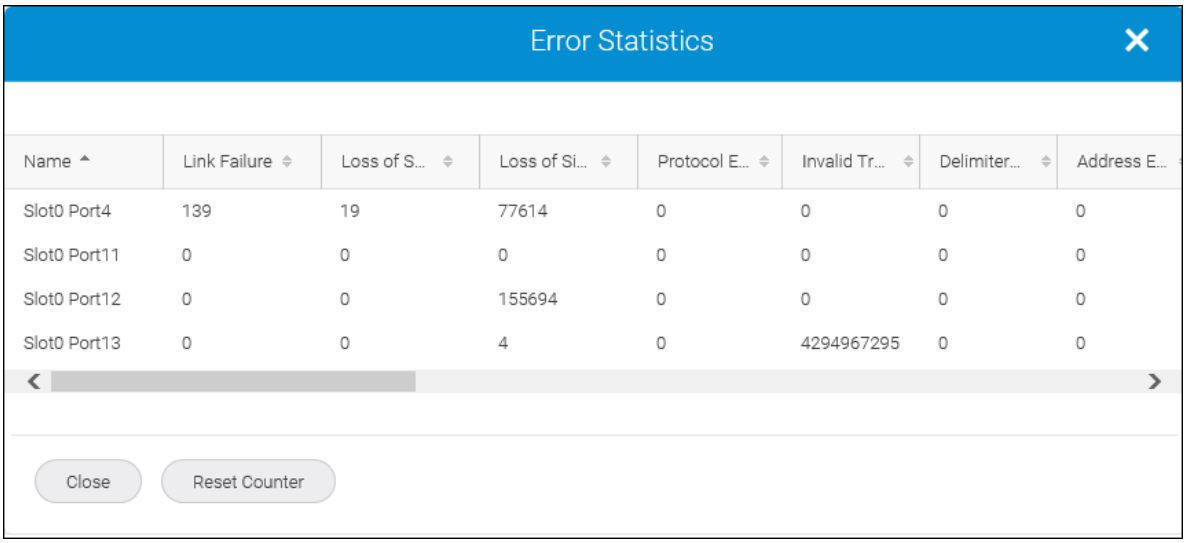
Viewing Error Statistics

The Error Statistics feature presents the detailed error statistics information of each port or multiple selected ports. The **Error Statistics** window shows the errors related to the health of the physical link between the switch and the host HBA, CRC errors, frames, inbound, and outbound links.

The **Error Statistics** window displays the following columns in the tabular format:

- Name
- Link Failure
- Loss of Sync
- Loss of Signal
- Protocol Error
- Invalid Transmitted Word
- Delimiter Error
- Address Error
- Inbound Link Reset
- Outbound Link Reset
- Inbound Offline Sequence
- Outbound Offline Sequence
- Frames Transmitted
- CRC Error
- Frames Received
- Long Frames
- Bad End-of-Frames
- Encd Errs Outside Frames
- C3 Frames Discarded
- Frames Rejected
- Frames Busied
- Tx Discarded Frames
- Rx Discarded Frames
- FEC Uncorrected

The **Error Statistics** window displays the error information in tabular format.



To view the error statistics for the selected ports, perform the following steps:

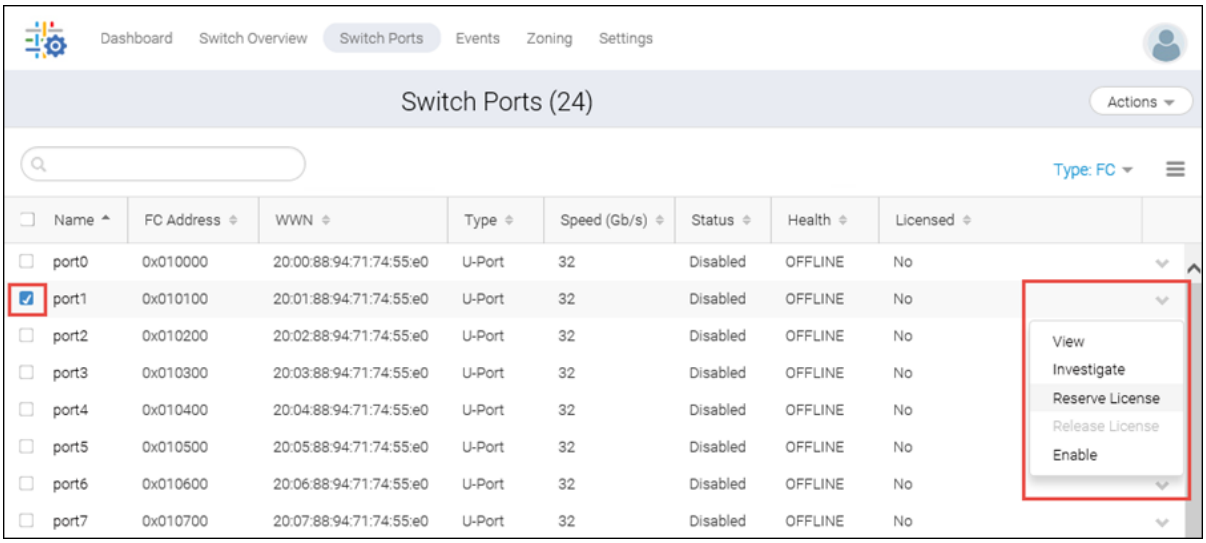
1. Click **Switch Ports** from the navigation bar, select one or more ports for which you want to view the error statistics from the **Switch Ports** window.
2. Click the **Actions** menu on the top-right corner, and then select **Error Statistics** from the drop-down.
   The **Error Statistics** window appears.
3. To reset the statistics information, click the **Reset Counter** button. The error data starts from 0.

Reserving Port Licenses

The Dynamic Ports on Demand (DPOD) feature automatically assigns the Ports on Demand (POD) licenses from the pool of available licenses based on the server blade or switch installation.

For the blade server SAN I/O modules, Dynamic POD detects and assigns ports to a POD license only if the server blade is installed with an HBA. A server blade that does not have a functioning HBA is treated as an inactive link during the initial POD port assignment. Dynamic POD assigns ports to the POD license when they come online. Typically, assignments are sequential, starting with the lowest port number. However, variations in the equipment attached to the ports can cause the ports to come online at different times. This means that the port assignment order is not guaranteed.

The license assigned to the ports is determined by the total number of ports and the licenses available on the license pool. You can reserve the license to single or multiple ports with the allocated license keys with the admin access.



To reserve the licenses for ports, perform the following steps:

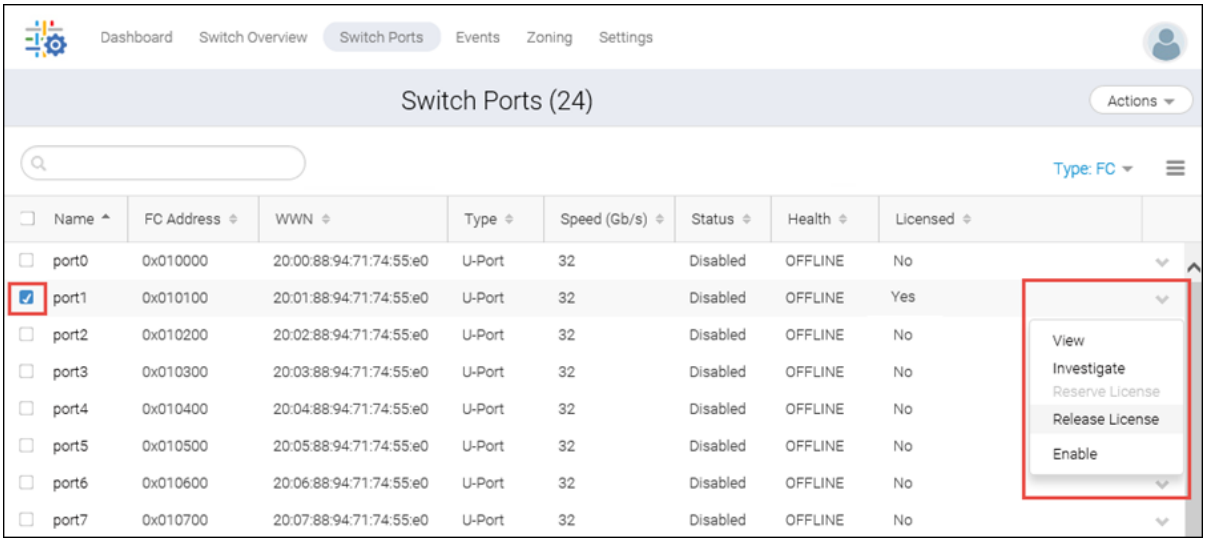
1. Click **Switch Ports** from the navigation bar, and select one or more logical ports to which the licenses to be reserved.
2. Click the **Actions** menu on the top-right corner, and then select **Reserve License** from the drop-down. The ports reserved with a license can be identified by the state of the **Licensed** column in the **Switch Ports** window and it is displayed as **Yes**. The **Licensed** column displays the state as **No** for the ports on which the licenses are not reserved.

NOTE
The port must be in the disabled state before reserving the license.

Releasing Port Licenses

You can release a license on a single port or multiple ports that are activated with the DPOD feature. You must be logged in as Admin to release licenses. Releasing a port removes it from the POD set.

Before releasing a license, you must disable the port and release the license. After a port is assigned to the POD set, the port is licensed until it is manually removed from the POD port set. When a port is released from its POD port set (base, single, or double), a vacancy is created in that port set.



To release the licenses from ports, perform the following steps:

1. Click **Switch Ports** from the navigation bar, and select one or more logical ports to which the licenses are released. You can identify the ports with reserved licenses by the **Licensed** column that is displayed as **Yes**.
2. Click the **Actions** menu on the top-right corner, and then select **Release License** from the drop-down. The ports with licenses released to POD can be identified by the state of the **Licensed** column in the **Switch Ports** window that is displayed as **No**.

Customizing Columns

Web Tools displays a default list of columns depends on the selected port with the real-time information. You can customize the columns that you want to display in the **Switch Ports** window.

To customize the displayed columns, perform the following steps:

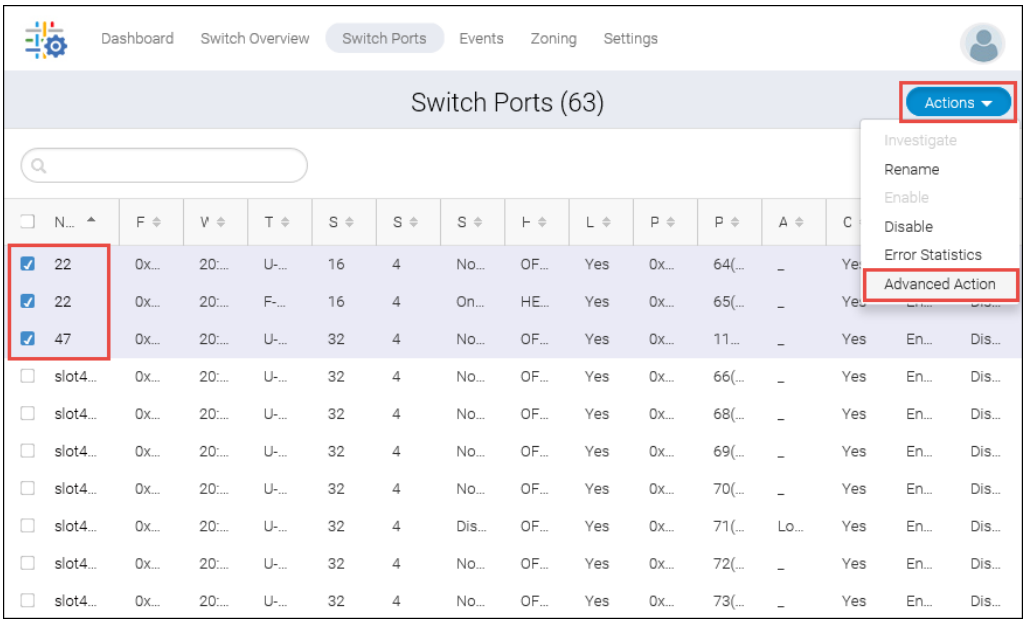
1. Click **Switch Ports** in the navigation bar, and then select the hamburger (≡) icon on the right-side corner. The **Columns** button appears.
2. Click the **Columns** button and check the names of the columns that you want to display in the view.

3. Based on the names of the columns that you selected, the selected set of columns for the selected FC ports are displayed in the **Switch Ports** window.

NOTE
The available columns may vary based on the category of the port selected.

Advanced Port Configuration

The **Actions** drop-down contains options for all tasks that you can perform on the selected ports. If you select multiple ports, options are available for only those tasks that you can perform on all of the selected ports. Options are unavailable if they are not applicable to the selected ports.



The **Advanced Action** option under the **Actions** menu is available only for the FC and VE ports category. The different advanced port configuration options are displayed for the selected port category. You can use the **Advanced Action** features to perform the following advanced configuration tasks for multiple ports.

- Configuring Encryption
- Configuring Compression
- Configuring FEC
- Configuring FEC via TTS
- Configuring NPIV Ports
- Configuring NPIV Max Login
- Configuring CSCTL Mode
- Configuring Port Beacons
- Configuring Port Peer Beacons
- Configuring Trunking
- Configuring Port Binding
- Configuring Target Driven Zoning Mode
- Configuring BB Credit

Configuring Encryption

The Encryption feature allows frames to be encrypted at the egress point of an ISL between two Brocade switches and then to be decrypted or decompressed at the ingress point of the ISL. Frames are in the decrypted state when delivered to an end device. The encryption is port-based encryption, and you can enable the in-flight encryption feature for both E_Ports and EX_Ports on a per-port basis. By default, this feature is initially disabled for all ports on a switch.

NOTE
For directors, the total bandwidth supported per blade for encryption is 64G. For a fixed-port switch, the total bandwidth for encryption is 64G.

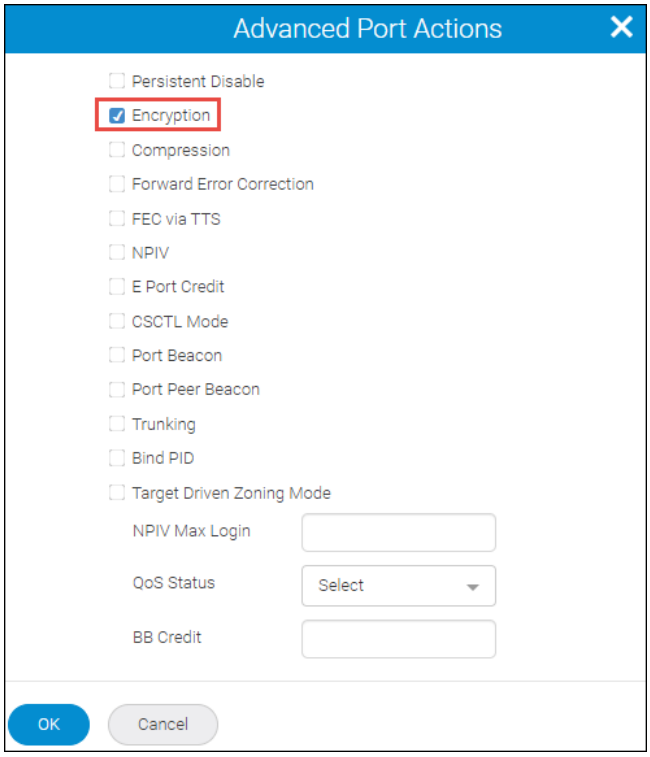
NOTE
The Encryption feature is not supported in the Access Gateway mode.

To enable or disable encryption on a port, the following requirements must be met.

- The Authentication policy must be activated.
- DH Group must be set to 0, 1, 2, 3, 4, or all.

To enable encryption, perform the following steps:

1. Click **Switch Ports** in the navigation bar, and then select **FC Ports** type from the drop-down.
2. From the list of ports, select a port on which encryption is to be configured.
3. Select **Actions** > **Advanced Action**. The **Advanced Port Actions** window appears.



4. Select the **Encryption** option, and then click **OK**. By default, the **Encryption** option is disabled.

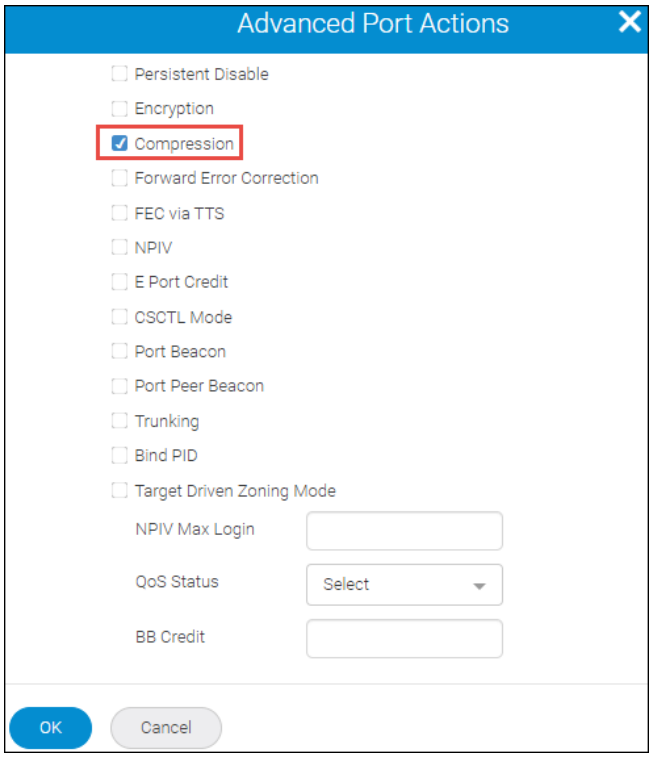
Configuring Compression

The Compression feature provides better bandwidth use on the ISLs, especially over long distance. The in-flight compression feature allows frames to be compressed at the egress point of an ISL between two Brocade switches, and then to be decompressed at the ingress point of the ISL. Frames are never left in an encrypted or compressed state when delivered to an end device. These features use port-based compression. You can enable the in-flight compression features for both E_Ports and EX_Ports on a per-port basis. By default, this feature is initially disabled for all ports on a switch.

NOTE
No license is required to configure and enable in-flight compression. Both ends of the ISL must terminate in 16G-capable or 32G-capable FC ports. Encryption and compression can be enabled at the same time, or you can enable either encryption or compression selectively.

To enable compression, perform the following steps:

1. Click **Switch Ports** in the navigation bar, and then select **FC Ports** type from the drop-down.
2. From the list of ports, select a port on which compression is to be configured.
3. Select **Actions** > **Advanced Action**. The **Advanced Port Actions** window appears.



4. Select the **Compression** option, and then click **OK**. By default, the **Compression** option is disabled.

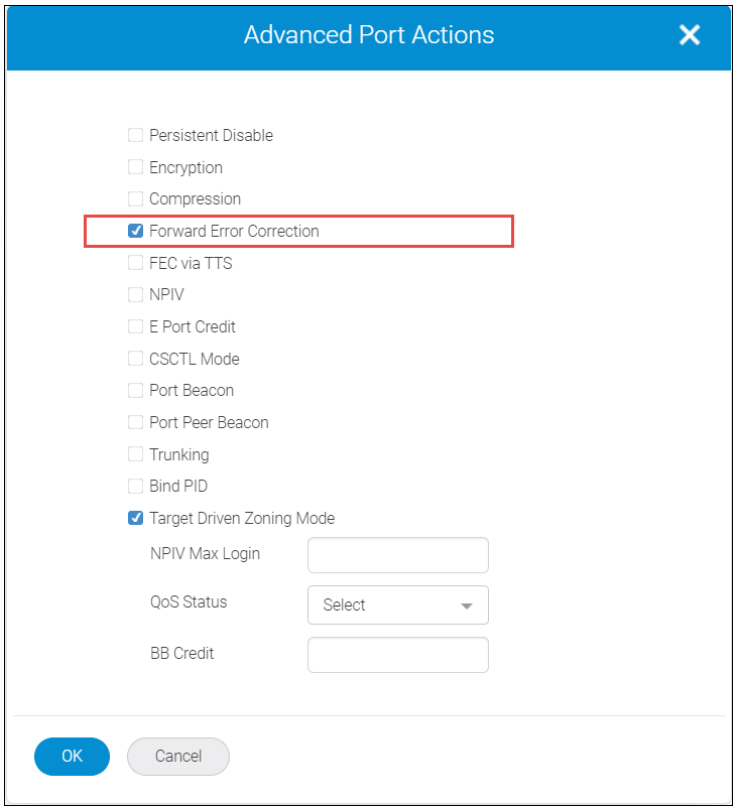
Configuring FEC

Forward error correction (FEC) provides a data transmission error control method by including redundant data (error-correcting code) to ensure the error-free transmission on a specified port or a range of ports. FEC allows the recovery of error bits in a 10, 16, 32, or 64G data stream. This feature is enabled by default on all ISLs and ICLs of 64G FC platforms on Gen 7 platforms. FEC is supported in the Access Gateway mode.

> **NOTE**
> Enabling FEC is disruptive to traffic. FEC can be enabled or disabled only at 16G or at 10G on E_Ports with octet mode 2 or 3 on Gen 6 and Gen 7 devices. The FEC is always enabled at 64G by default on Gen 7 devices.

To configure the FEC, perform the following steps:

1. Click **Switch Ports** in the navigation bar, and then select **FC Ports** or **ICL Ports** type from the drop-down.
2. From the list of ports, select a port or multiple ports to which the FEC to be configured.
3. Select **Actions** > **Advanced Action**. The **Advanced Port Actions** window appears.
4. Select the **Forward Error Correction** checkbox.



5. Click **OK**.

   By default, FEC is enabled. To disable the FEC, unselect the **Forward Error Correction** checkbox if it is already selected. Generally, any of the following FEC statuses are displayed on the port details page.

   - **Enabled (Active)** – FEC is enabled on a port, and the configuration is Active.
   - **Enabled (Inactive)** – FEC is enabled on a port, and the configuration is Inactive.
   - **Disabled** – FEC is not enabled on a port.
   - **NA** – FEC is not supported.

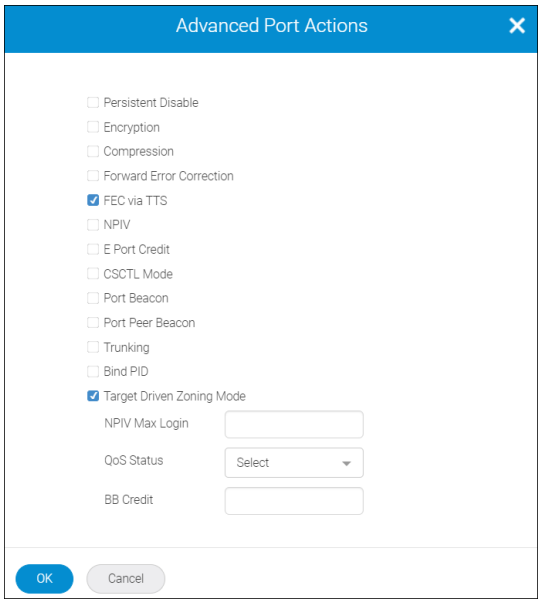
Configuring FEC via TTS

Forward Error Correction (FEC) provides a mechanism to reduce the data transmission error by including redundant data (error-correcting code) to ensure an error-free transmission on a specified port or port range. If the FEC via Transmitter Training Signal (TTS) mode is enabled, the port negotiates FEC through TTS. The 16G TTS is not compatible with the more commonly used 16G 64B/66B. Thus, the FEC via TTS mode should be enabled only if a similarly TTS-capable and enabled device is connected to the port.

> **NOTE**
> FEC via TTS must be disabled on all E_Ports. E_Port connectivity is not supported when FEC via TTS is enabled on the switch port.

To configure FEC via TTS, perform the following steps:

1. Click **Switch Ports** in the navigation bar, and then select **FC Ports** type from the drop-down.
2. From the list of ports, select a port on which the FEC via TTS is to be configured.
3. Select **Actions** > **Advanced Action**. The **Advanced Port Actions** window appears.
4. Select the **FEC via TTS** option, and then click **OK**. By default, **FEC via TTS** is disabled.



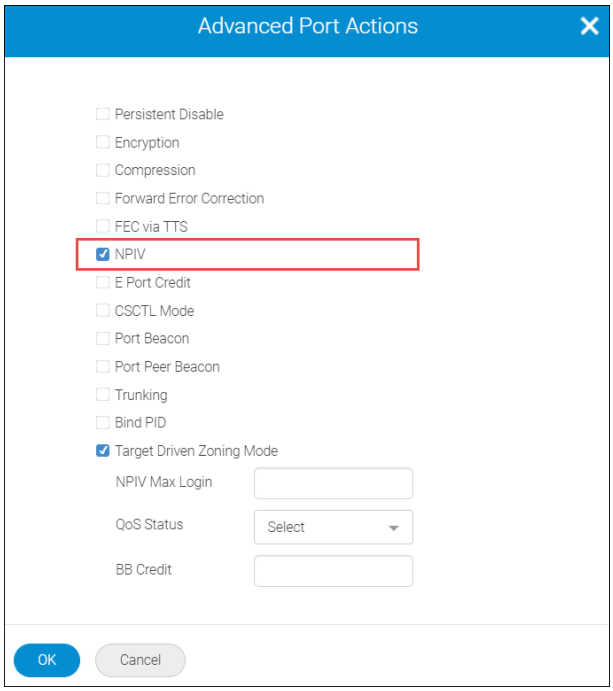
Configuring NPIV Ports

N_Port ID Virtualization (NPIV) enables a single FC port to appear as multiple, distinct ports, providing separate port identification within the fabric for each operating system image behind the port (as if each operating system image had its unique physical port). NPIV assigns a different virtual port ID to each FC device. NPIV is designed to enable you to allocate virtual addresses without affecting your existing hardware implementation. The virtual port has the same properties as a N_Port, and it is capable of registering with all the services of the fabric. For detailed information about understanding and configuring NPIV ports, refer to the *Brocade Fabric OS Administration Guide*.

NOTE
The NPIV feature cannot be disabled when the Access Gateway mode is enabled.

To enable an NPIV port, perform the following steps:

1. Click **Switch Ports** in the navigation bar, and then select **FC Ports** type from the drop-down.
2. From the list of ports, select one or more logical ports to be configured.
3. Click **Actions** > **Advanced Port Actions**. The **Advanced Port Actions** window is displayed.
4. Select the **NPIV** checkbox, and then click **OK**.



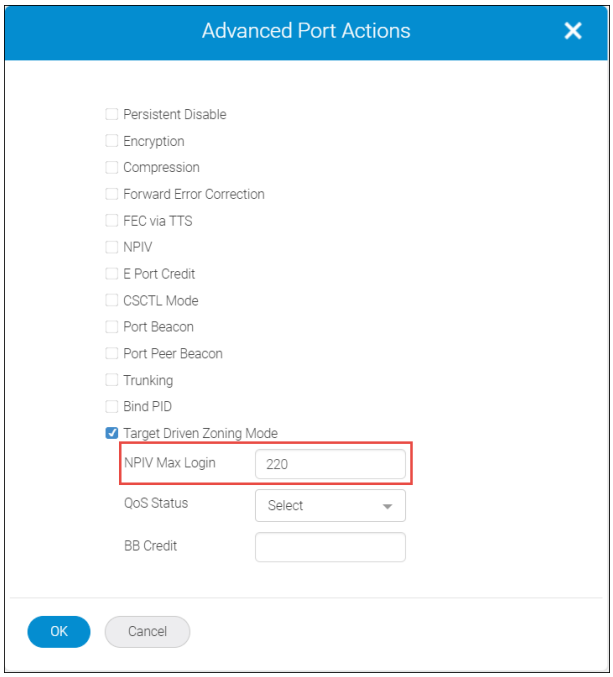
Configuring NPIV Max Login

The NPIV Max Login enables the maximum number of permitted logins per NPIV port. Each NPIV port can support up to 255 logins. The range of valid values is from 1 through 255 logins per port. The default value is 126 logins.

The NPIV feature supports virtual switches, but not on physical switches. Each port can have a different NPIV login limit value in each logical switch. The **NPIV Max Login** column displays the value assigned to each port.

To configure the maximum number of logins to be allowed for the selected NPIV ports, perform the following steps:

1. Click **Switch Ports** in the navigation bar, and then select **FC Ports** type from the drop-down.
2. From the list of ports, select one or more logical ports to be configured.
3. Click **Actions** > **Advanced Port Actions**.
   The **Advanced Port Actions** window is displayed.
4. Enter the maximum number of logins in the **NPIV Max Login** field and, then click **OK**.



Configuring CSCTL Mode

Class-Specific Control (CSCTL) enables the same SID/DID pair exchange frames with different priorities, unlike the QoS zone-based FC flow prioritization method.

To prioritize a frame flow between two end nodes, Fabric OS supports up to 32 virtual channels (VCs) per port. This categorizes the frames that enter a fabric based on the preset behavior that is defined with these VCs, and it conserves the frame's behavior until it is transmitted out of the fabric. However, of the 32 VCs for each external port, only 16 are used.

With the CSCTL method of prioritization, there is no need to have explicit traffic segregation, such as QOS_H, QOS_M, and QOS_L. The classification is based entirely upon the CSCTL database that is programmed into the ASIC. As the name suggests, CSCTL bits in each frame are used to define the VC number on the transmit port. To achieve this kind of classification, Fabric OS provides a CSCTL database table on each chip, which is capable of storing 256 entries. Each entry in the database table is populated with a VC number that, if this feature is enabled, is retrieved by indexing the CSCTL value into the table for each frame that enters the fabric. Irrespective of the type of frame classification method used, the flow priority of a frame is primarily determined by the VC number that is used to transmit the frames across the ISL ports. In both methods of classification, the VC number for a frame is determined at the ingress Fabric port (F_Port) or Fabric Loop port (FL_Port) when the frame enters the fabric for the first time. To maintain the same flow priority for a frame across all ISL hops in a fabric, the same VC number is used while transmitting the frame at the egress E_Port until it leaves the fabric through an F_Port or FL_Port.

The main difference between the QoS zone method of classification and the CSCTL VC-based method of classification is how the VC number is computed when the frame enters the fabric through an F_Port or FL_Port port and, of course, the manner of setting up these two frame classification methods.

Once CSCTL mode is enabled on an F_Port or FL_Port in a switch, the CSCTL value in the frame header of all incoming frames on that F_Port or FL_Port is used to index into the ASIC's CSCTL database table to compute the VC number. The VC number defines the frame's flow priority throughout its life in the fabric until it exits the fabric through another F_Port or FL_Port. The QoS links (ISLs) preserve this classification during the frame's traversal across all hops in the fabric.

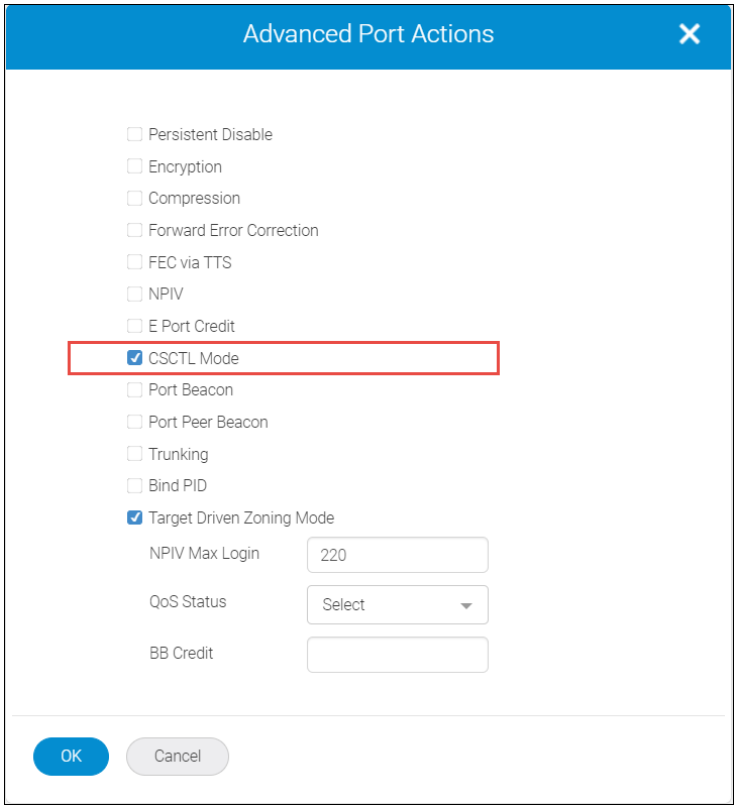
NOTE
When CSCTL mode and QoS zones are enabled, QoS zones lose the priority to CSCTL mode.

NOTE
When the QoS zone is configured as the default, CSCTL mode is disabled.

Enabling or Disabling CSCTL Mode

To enable CSCTL mode, perform the following steps:

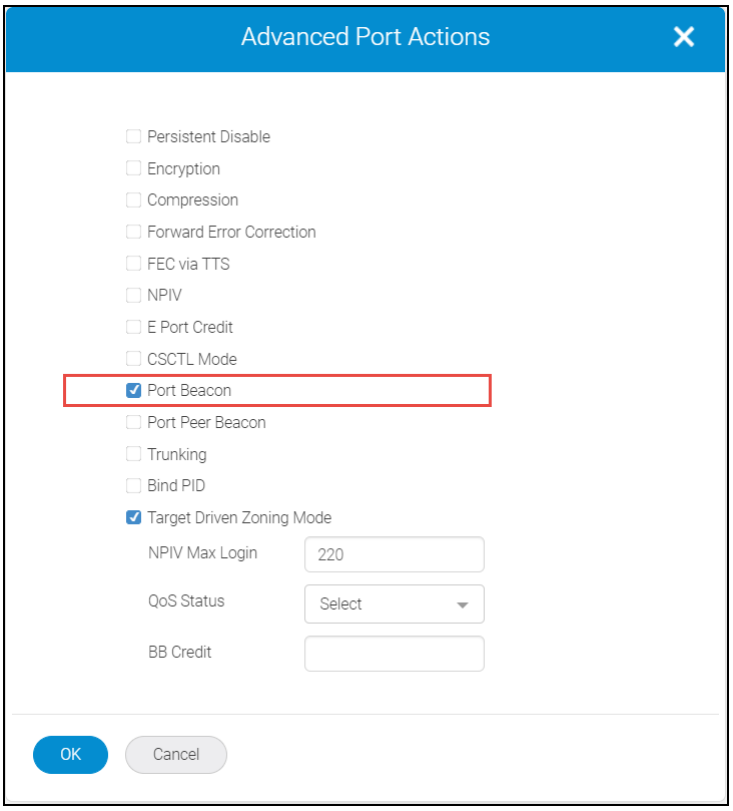
1. Click **Switch Ports** in the navigation bar, and then select **FC Ports** type from the drop-down.
2. From the list of ports, select a port or multiple ports for which CSCTL mode is to be enabled.
3. Select **Actions** > **Advanced Action**.
   The **Advanced Port Actions** window appears.



4. Select the **CSCTL Mode** checkbox.
5. Click **OK**. To disable CSCTL mode, unselect the **CSCTL Mode** checkbox if it is already selected.

Configuring Port Beacons

Individual FC ports can be set to beacon using the **Ports Listing** window from the **Switch Ports** tab. The **Switch Overview** tab displays the port beaconing status by flashing the port amber and green for 2.5 seconds each, in an alternating pattern.



To configure beaconing for an FC port, perform the following steps:

1. Click **Switch Ports** in the navigation bar, and then select **FC Ports** type from the drop-down.
2. From the list of ports, select a port or multiple ports on which the beaconing is to be enabled.
3. Select **Actions** > **Advanced Action**.
   The **Advanced Port Actions** window appears.
4. Select **Port Beacon** checkbox, and then click **OK**.

   NOTE
   You may select all ports on the switch, but if you select a port that is not valid for beaconing, the **Port Beacon** option is disabled.

   While enabling port beacon, an error message appears under the following conditions:

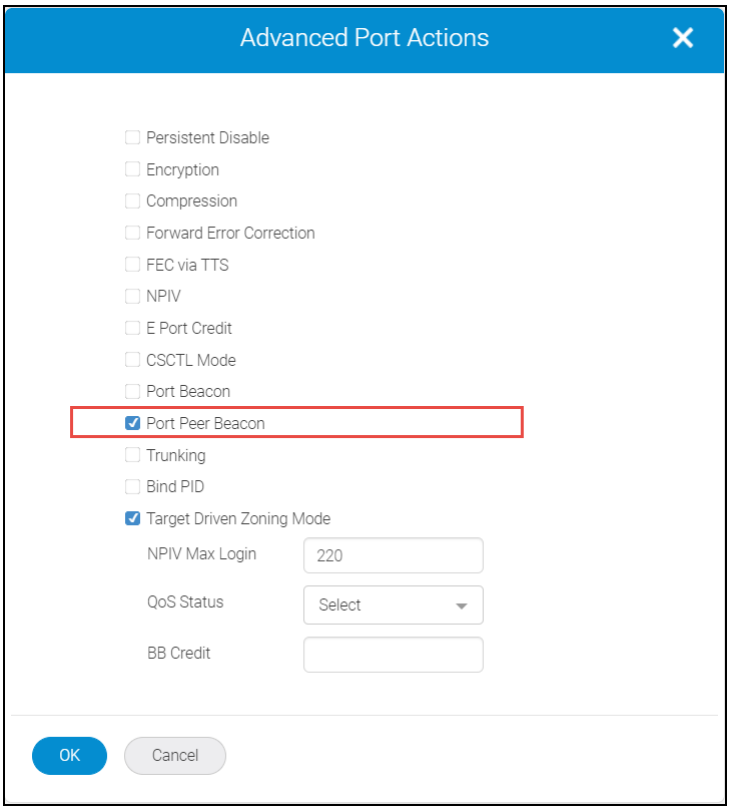
   - If switch beacon or chassis beacon is enabled on the switch.
   - If the Port Peer Beacon feature is enabled on the port.

Configuring Port Peer Beaconing

You can use the **Port Peer Beacon** option to turn on or off the port peer beaconing to physically identify the interconnections between FC ports. Using this configuration, the administrator can turn on the beaconing on both ends of the link and physically search the other switches or devices for the beacon pattern to find the peer port. The beaconing pattern is alternating green and amber LEDs every 1.2 seconds.

In the case of the trunk ports, the entire trunk group is beaconed. The Port Peer Beacon configuration is supported for one port or trunk only. Newly added trunk ports are automatically included in to beacon. Similarly, disabling the port peer beacon on a trunk port disables beaconing on the entire trunk group.

NOTE
The Port Peer Beacon configuration is supported in the native switch mode and in the Access Gateway mode.



The port peer beacon configuration is not supported in the following cases:

- On ICL, VE, and GigE ports.
- If a port is faulty or disabled.
- If diagnostic tests are running on the port.

NOTE
Port peer beaconing is disabled when a port is disconnected, toggled, or disabled.

To configure port peer beaconing for an FC port, perform the following steps.

1. Click **Switch Ports** in the navigation bar, and then select **FC Ports** type from the drop-down.
2. From the list of ports, select a port or multiple ports on which the beaconing is to be enabled.
3. Select **Actions** > **Advanced Action**. The **Advanced Port Actions** window appears.
4. Select the **Port Peer Beacon** checkbox, and then click **OK**.

NOTE
You may select all ports on the switch, but if you select a port that is not valid for peer beaconing, an error message is displayed.

NOTE
You can configure the Port Peer Beacon configuration only for a single AE_Port.

While enabling port peer beacon, an error message is displayed if the switch beacon or chassis beacon is enabled on the switch.

Configuring Trunking

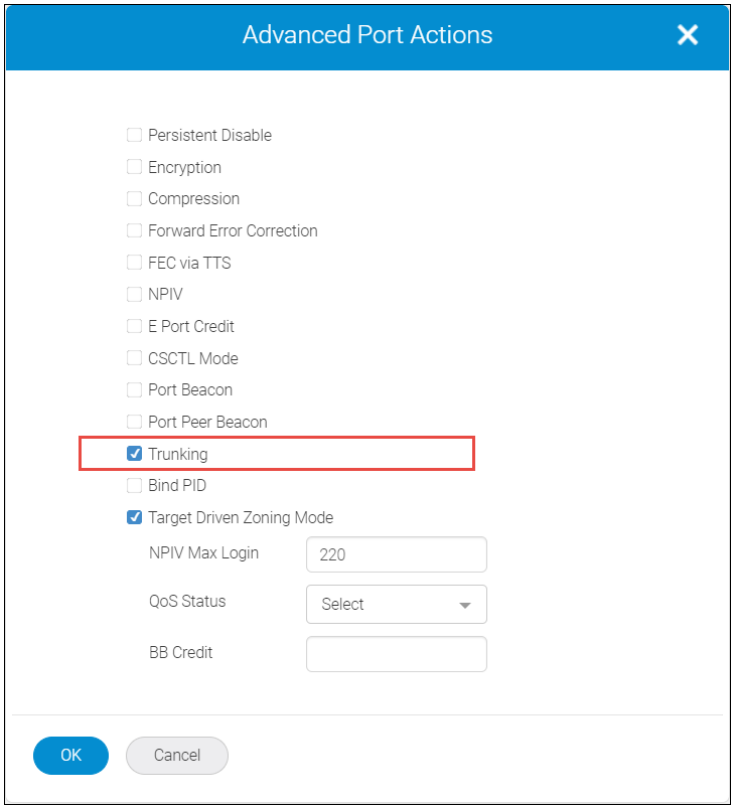
The trunking configuration optimizes network performance by forming trunking groups that can distribute traffic between switches across a shared bandwidth. Trunking is configured on an inter-switch link (ISL) between two Fabric OS switches and applies only to E_Ports. Trunking is enabled by default for a port, which enables an ISL connected from the same port group to form a trunk.

The ISL trunking license is required on each switch that participates in the trunk. After activating the ISL trunking license, trunking is enabled automatically by default across all eligible ports. You must re-initialize the ports that are used for ISL trunking to ensure that these ports recognize that the trunking is enabled.

NOTE
Trunking is not supported on the ICL, VE, and GigE port types.

To manually enable the trunking configuration on a port, perform the following steps:

1. Click **Switch Ports** in the navigation bar, and then select port type from the drop-down.
2. From the list of ports, select a port or multiple ports on which the trunking is to be enabled.
3. Select **Actions** > **Advanced Action**.
   The **Advanced Port Actions** window appears.
4. Select the **Trunking** checkbox.



5. Click **OK**.
   To disable the trunking configuration, unselect the **Trunking** checkbox if it is already selected.

Configuring Port Binding

The **Port Binding** option allows you to prevent unauthorized devices from joining a fabric and to restrict host or storage devices that connect to particular switch ports. The **Port Binding** option allows you to configure a PID persistently using a device WWN. When the device logs in to the switch, the PID is bound to the device WWN. If the device is moved to another port in the same switch, or a new blade is hot-plugged, the device receives the same PID (area) at its next login. Once WWN-based PID assignment is enabled, you must manually enter the WWN-based PID assignments through the CLI for any existing devices. For more information on WWN-based PID assignments, refer to the *Brocade Fabric OS Administration Guide*.

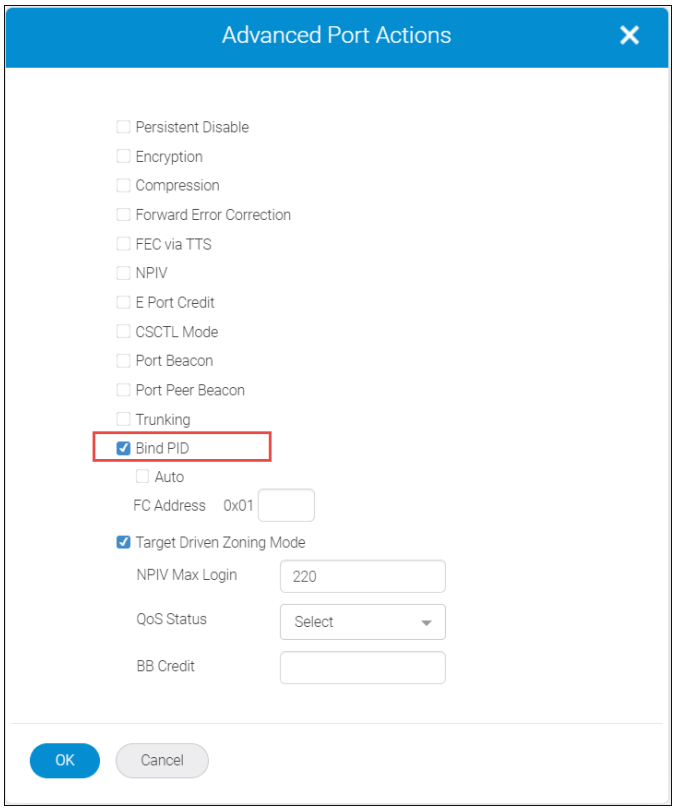
PID assignments are supported for a maximum of 4096 devices; this includes both point-to-point and NPIV devices. The number of point-to-point devices that are supported depends on the areas available. For example, 448 areas are available on Directors and 256 areas are available on switches. When the number of entries in the WWN-based PID database reaches 4096 areas that are used up, the oldest unused entry is purged from the database to free up the reserved area for the new FLOGI.

NOTE
The total number of ports in the default switch must be 256 or less.

NOTE
When the WWN-based PID assignment feature is enabled, and a new blade is plugged into the director, the ports for which the area is not available are disabled.

To bind a port or multiple ports, perform the following steps:

1. Click **Switch Ports** in the navigation bar, and then select **FC Ports** type from the drop-down.
2. From the list of ports, select a port or multiple ports on which the port binding is to be enabled.
3. Select **Actions** > **Advanced Action**.
   The **Advanced Port Actions** window appears.
4. Select the **Bind PID** checkbox. The **FC Address** field with the option to enter the middle byte to be set appears.



5. Enter the middle byte and for the selected ports, the middle bytes are assigned sequentially.
6. Click **OK**.

NOTE
A warning message is displayed if the port is already bound.

NOTE
To unbind a port or ports that are already bound, unselect the **Bind PID** checkbox if it is already selected.

Configuring Target Driven Zoning Mode

A target-driven peer zone is a peer zone that is configured in a fabric through a target. Target-driven zoning is a variant of peer zoning wherein a device, usually a target, can manage peer zones by itself. Where a regular peer zone is defined by a user-specified configuration, the target device must be the principal device of the peer zone. This device is usually a storage device, but not always. To permit a target-driven peer zone, target-driven zoning must be enabled on the F_Port that connects the principal device to the fabric.

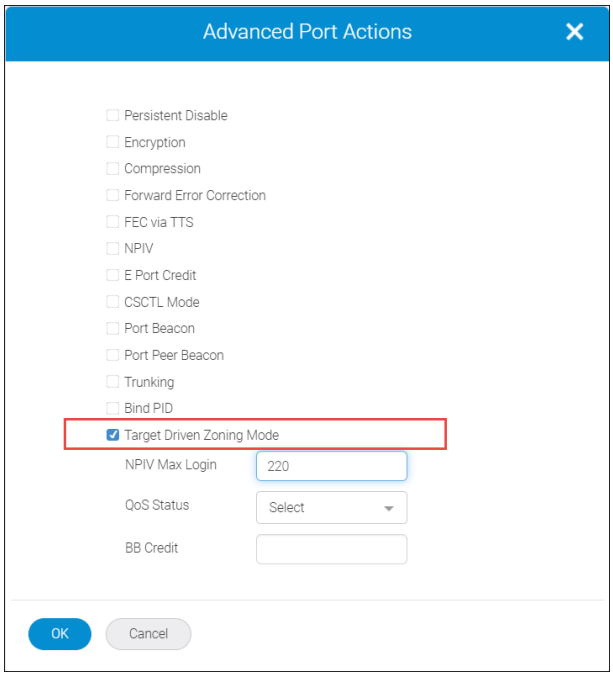
The Target Driven Zoning mode can be used only in read-only mode. You can read, delete, activate, or deactivate only the members present in the target-driven peer zone. The principal and non-principal members should be only the WWN type. You can view the target-driven peer zones in the **Zone Administration** window. You can configure Target Driven Zoning mode on multiple devices that are connected to the target-driven peer-zone-enabled ports.

NOTE
Target-driven zones are allowed to have aliases as members. Aliases that are members of target-driven zones are not allowed to be edited from Web Tools.

You can enable Target Driven Zoning mode for target-driven peer-zone-enabled ports.

To enable Target Driven Zoning mode on a port, perform the following steps:

1. Click **Switch Ports** in the navigation bar, and then select the **FC Ports** type from the drop-down.
2. From the list of ports, select a port or multiple ports on which Target Driven Zoning mode is to be enabled.
3. Select **Actions** > **Advanced Action**.
   The **Advanced Port Actions** window is displayed.
4. Select the **Target Driven Zoning Mode** checkbox.



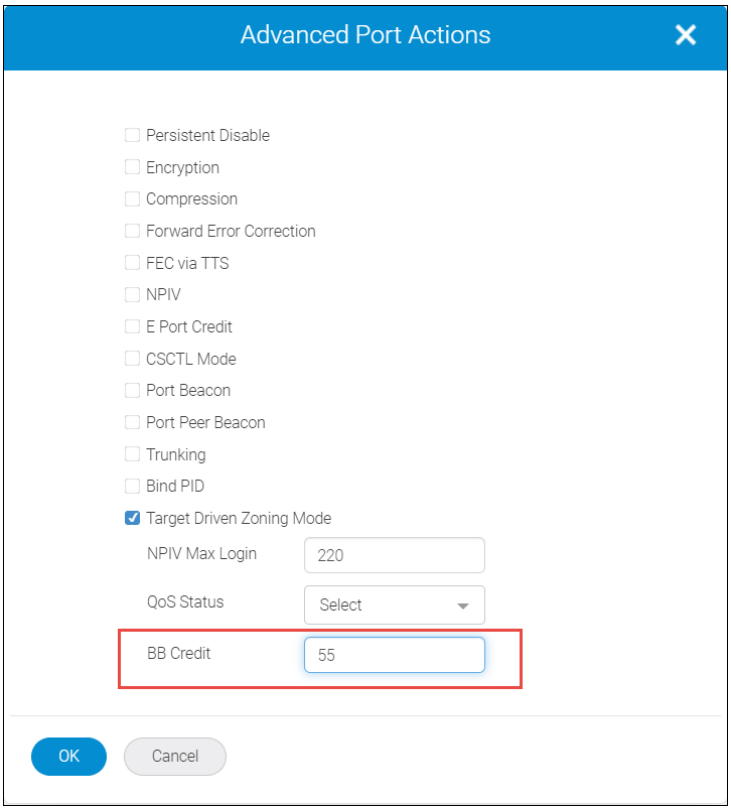
5. Click **OK**.

Configuring BB Credit

The buffer-to-buffer credit (BB credit) is the number of buffers available to the attached devices for frame receipt. The default BB credit is 8. The range of valid values is from 5 through 160.

To prevent the dropping of frames in the fabric, a device can never send frames without the receiving device being able to receive them, so an end-to-end flow control is used on the switch. Flow control in Fibre Channel uses BB credits, which are distributed by the switch. When all BB credits are utilized, a device waits for a VC_RDY or an R_RDY primitive from the destination switch before resuming I/O. The primitive is dependent on whether you have R_RDYs enabled on your switch. When a device logs in to a fabric, it typically requests from two to 16 buffer credits from the switch, depending on the device type, driver version, and configuration. This determines the maximum number of frames that the port can transmit before receiving an acknowledgment from the receiving device.

NOTE
BB credit is not applicable for VE and ICL ports.



To configure the BB credits value on a F_Port, perform the following steps:

1. Click **Switch Ports** in the navigation bar, and then select the **FC Ports** type from the drop-down.
2. From the list of ports, select a port or multiple ports on which the BB credit value is to be entered.
3. Select **Actions** > **Advanced Action**. The **Advanced Port Actions** window is displayed.
4. Enter the BB credit value for the selected ports in the **BB Credit** text box.
5. Click **OK**. If you do not enter the credit value, the default value is selected.

Viewing Port Details

You can view the configuration details of selected ports from the **Switch Ports** window. The **Switch Ports** window allows you to view the configuration properties of the selected port. You can view the details that are related to the port, speed, and port configuration properties depending on the type of the selected port. Also, you can edit the port configuration properties, such as Port Beacon, Encryption, FEC, NPIV, CSCTL, QOS, SFP, Statistics, Investigate, and enabling and disabling ports.

The following table describes the port configuration properties that are displayed in the **Switch Ports** window for the selected port type.

Field Name	Description
Name	Displays the name that is assigned to the port. You can rename the port, using this field. For more information on renaming a port, see Renaming Ports.
WWN	Displays the World Wide Name of the port which is a 64-bit unique identifier.

Field Name	Description
Protocol	Displays the type of protocol that is used on the port.
Port #	Displays the location of the port in a physical-location format.
Port Index	Displays whether a port was swapped with other ports. For ports that were swapped, the attribute name displays as *Port Index Value* (Swapped). For example, 5(0x5) (Swapped).
FC Address	Displays the address of the FC port.
Media	Displays information about the type of media that are installed or connected to the port.
Type	Displays the actual or current port type. If the port is offline, this value is the allowed types (or U_Port, if no type constraint is specified). If the port is online, this value is the configured port type.
Health	Displays the health status of the ports in the logical switch.
Speed (Gb/s)	Displays the actual speed at which the port is connected. The speed is set with the options 4, 8, 16, or 32G, or with auto-negotiate, which sets the highest possible port speed.
Configured Speed	Displays the value as AUTO for the auto negotiated speed or the fixed speed if configured.
Authentication	Displays the authentication type and associated parameters if configured.
Allowed Port Types	Displays the allowed or configurable port types for the specific port. The allowed port types indicate any constraints on what types the port can be configured when it comes online.
Speed Combinations	Displays the options to set the port octet speed combination.
Speed	Displays the speed at which the port is configured. You can configure a 4G, 8G, 16G, or 32G port speed or set the port to auto-negotiate the highest possible port speed. The Auto Max options are displayed only when you set the port speed as auto-negotiation, and these options allow you to set the speed limit that the port can auto-negotiate. The following Auto Max speed levels are supported: • Auto Max 4G • Auto Max 8G • Auto Max 16G • Auto Max 32G
Long Distance	Displays the long-distance settings and identifies which settings require a Brocade Extended Fabrics license. To set the long-distance mode, the default is L0 (Normal); as per distance, LE≤10 kms, L0.5≤25 kms, L1≤50 kms, L2≤100 kms, LD=auto, LS=Static will display.
Desired Distance (km)	Displays the recommended buffer value changes according to the current port configuration. When the number of buffers that are needed is configured for a port, the recommended buffer value is set to N/A for the same port. This field cannot be configured when the **Buffers Needed** value is specified.
Frame Size	Displays the size of the frame. When you edit the *Frame Size* value, the desired distance value can also be changed for LD and LS modes (configured in *Long Distance*) and in reverse. *Frame Size* cannot be configured when the *Buffers Needed* value is specified.

Field Name	Description
Buffers Needed	Displays the number of buffers needed. The Desired Distance value is set to *Not Applicable* when the Buffer Needed is configured for the selected port.
Recommended Buffer	Displays the number of recommended buffers. The recommended buffer value is non-editable. When you change *Frame Size* and *Desired Distance (km)*, the recommended buffer value changes according to the current port configuration. When the number of buffers that are needed is configured for a port, the recommended buffer value is set to *Not Applicable* for the same port.
Remaining Buffer	Displays the number of remaining buffers. The remaining buffer value is non-editable.
VC Link Init	Displays the fill words used on long-distance links. When set to IDLE (0) mode, the link uses IDLE fill words. When set to ARB (1) mode, the link uses the default ARB fill words.
Persistent Disable	Enables or disables a port so that it remains enabled or disabled across switch restarts.
Encryption	Enables or disables in-flight encryption for both E_Ports and EX_Ports on a per-port basis. By default, these features are disabled for all ports on a switch.
Compression	Enables or disables the in-flight compression, which allows better bandwidth utilization over long distance.
Forward Error Correction	Enables or disables forward error correction (FEC) on all ISLs and ICLs of 32G FC platforms.
FEC via TTS	Enables or disables FEC through Transmitter Training Signal (TTS). All devices that support FEC-via-TTS have it enabled by default; however, not all devices that support 16G support FEC-via-TTS. FEC-via-TTS is negotiated during speed negotiation when a link comes up. Any HBA or device connection that supports 16G but not FEC-via-TTS auto-negotiates to 8G. Therefore, FEC-via-TTS must be enabled only on switch ports that are intended for connections to HBAs and devices that support FEC-via-TTS. A Brocade-to-Brocade ISL connection does not use TTS to enable FEC; consequently, FEC-via-TTS must be disabled on all E_Ports.
NPIV	Enables or disables NPIV for a port.
E Port Credit	Enables or disables the E_Port credit. The allowed range is 5 to 160.
CSCTL Mode	Enables the same SID/DID pair exchange frames with different priorities, unlike the QoS zone-based FC flow prioritization method.
Port Beacon	Displays the individual FC ports that can be set to beacon using the **Port Beacon** option. While enabling port beaconing, an error message is displayed, if the Port Beacon feature is enabled on the port.
Port Peer Beacon	The Port Peer Beacon feature allows you to physically identify the interconnections between FC ports. You can configure the Port Peer Beacon feature for a single port or for multiple ports. The Port Peer Beacon feature is supported on E_Ports, EX_Ports, F_Ports, N_Ports, AE_Ports, and trunk ports. When you enable the port peer beacon configuration on any port that is part of a trunk group, it enables port peer beaconing on all trunk ports in the same trunk. The Port Peer Beacon feature is supported in native switch mode and in Access Gateway mode.
Trunking	Enables or disables the trunking.

Field Name	Description
Target Driven Zoning Mode	Enables or disables Target Driven Zoning mode for target-driven peer-zone-enabled ports.
NPIV Max Login	Configures the maximum number of permitted logins per NPIV port. Each NPIV port can support up to 255 logins. The range of valid values is from 1 through 255 logins per port. The default value is 126 logins.
QoS Status	Displays the QoS status of the FC port. Since CSCTL mode is already enabled, even if QoS zone flows are enabled, CSCTL mode has the highest priority.
BB Credit	Displays the buffer-to-buffer credit, that is the number of buffers available to attached devices for frame receipt.
SFP	Displays information about the small form-factor pluggable (SFP) optical transceivers that plug into the SFP port of a network switch and connect to Fibre Channel and Gigabit Ethernet (GigE) optical fiber cables at the other end. The SFP option is applicable only for the physical ports such as FC, ETH, and GigE. The SFP section displays the following SFP port-related information: • Vendor Name • Vendor OUI • Vendor PN • Vendor Rev • Serial No • Data Code • Media Form Factor • Connector • FC Speed (Gb/s) • Distance • Voltage • Current • Wave Length • Encoding • Max Case Temperature • Temperature • TX Power • RX Power • Power On Time

Field Name	Description
SFP DD	The SFP DD section displays the following port-related information: • Vendor Name • Vendor OUI • Vendor PN • Vendor Rev • Serial No • Data Code • Media Form Factor • Connector • FC Speed (Gb/s) • Distance • Unit Number • Channel Index • Device Technology • Voltage • Current • Wave Length • Encoding • Max Case Temperature • Temperature • TX Power • RX Power • Power On Time
QSFP	Displays information about the quad small form-factor pluggable (QSFP) optical transceivers. The QSFP port is applicable only for the FC and ICL Ports. The QSFP section displays the following port-related information: • Vendor Name • Vendor OUI • Vendor PN • Vendor Rev • Serial No • Data Code • Media Form Factor • Connector • FC Speed (Gb/s) • Distance • Unit Number • Channel Index • Device Technology • Voltage • Current • Wave Length • Encoding • Max Case Temperature • Temperature • TX Power • RX Power • Power On Time

Field Name	Description
Extension Tunnels	Displays the FCIP tunnels and FCIP circuit details.
IP Route	Displays the IP route information that is applicable to the FCIP platforms. This option is applicable only to GigE ports.
IP Interfaces	Displays the status of the IP interface and the configuration of all interfaces or a specific interface that is applicable for the FCIP-supported switch. This option is applicable only to GigE ports.
Disable Port	Disables the port on selection.

Configuring Allowed Port Types

The **Allowed Port Type** option displays the allowed port types for the physical ports. The **Allowed Port Type** option appears on the port details page. The allowed port types indicate any constraints on what types the port can be configured with when it comes online. For normal (that is, non-EX_Port) ports, the following port types are allowed:

- **L_Port** – The port can be used to connect a loop device.
- **F_Port** – The port can be used to connect a non-loop device.
- **E_Port** – The port can be used to connect to another switch.
- **U_Port** – For a physical FC port, the port can be an E_Port, F_Port, or L_Port. For a logical FC port, the port can be a VE_Port.

When the **Allowed Port Type** option prompts you to select allowed port types, if all of these boxes are selected, there are no constraints on the port type. The port negotiates to its preferred type when the switch comes up, depending on what type of device or switch it is connected.

Clearing a checkbox guarantees that the port does not attempt to function as a port of the unchecked type. At least one type must remain selected. An FC port cannot be configured as an E_Port or L_Port.

NOTE
To configure a port as an EX_Port, the switch must be capable of supporting FCR features. The EX_Port option is disabled in the **Allowed Port Type** option if the switch does not meet this requirement.

Configuring Speed Combinations

You can change the octet combination of a director or switch. The octet speed must be set consistently across all members of the port octet. The following port octet speed combinations are available on the port details page.

Port Octet in Combination	Available Port Speeds within the Octet
1	Auto or Fixed 32G|16G|8G|4G
2	Auto or Fixed 10G|8G|4G

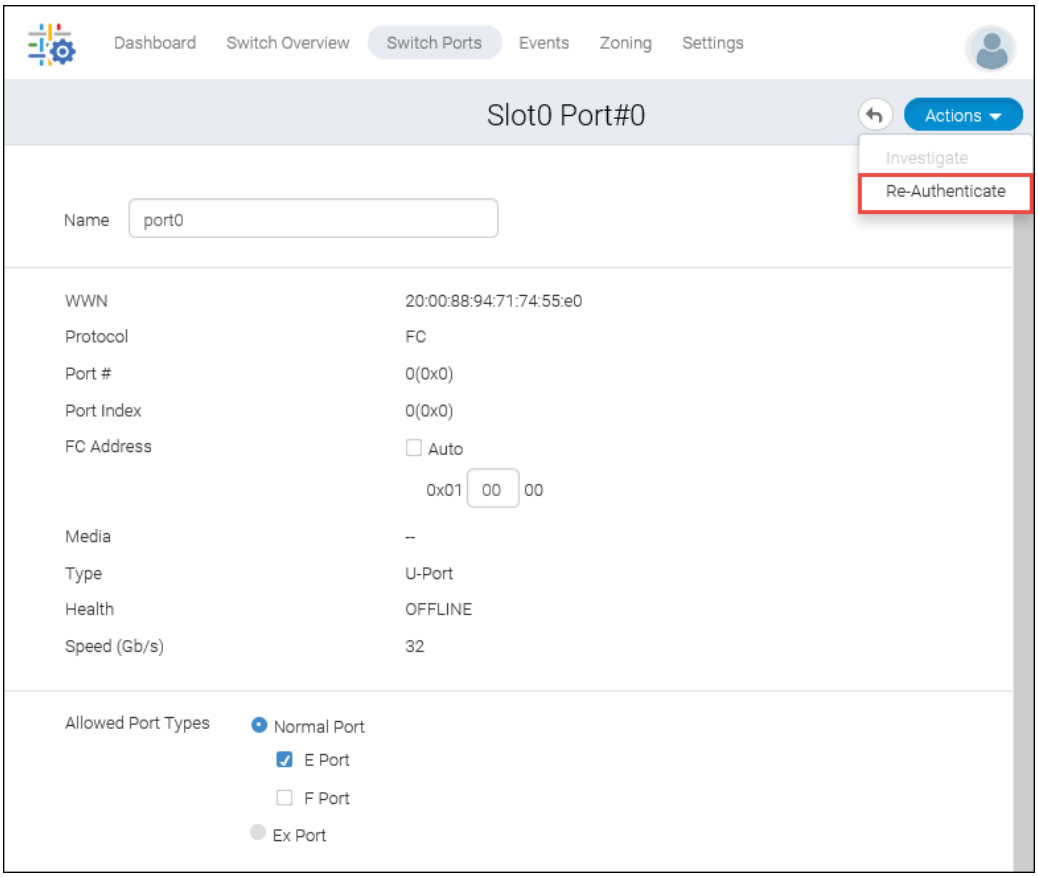
The default speed mode is 1, which means that any port in the eight-port group octet can operate either at 32, 16, 8, or 4G, utilizing 32G SFP+ optics, or at 16, 8, 4, or 2G, utilizing 16G SFP+ optics. Speed combination mode 2 enables any port in the octet to operate at a 10G line rate, but it also specifically requires 10G SFP+ optics. These are also available in SWL and LWL models.

Re-Authenticating Ports

You can re-authenticate the switches connected by F_Port or E_Port if the DH-CHAP group, hash type, or shared secret between a pair of switches is set with the switch level security policy. The re-authentication can be initiated by the user who has configured the policy parameters and only if the switch was previously authenticated. You can establish a secure

connection by authenticating the remote and peer secret keys. If the authentication fails because shared keys do not match, the port is disabled.

For more information on configuring authentication protocols, see Authentication Policy Configuration.



NOTE
The re-authentication does not work on loop, NPIV, and FICON devices or on ports configured for in-flight encryption.

Enabling or Disabling Application Header Support

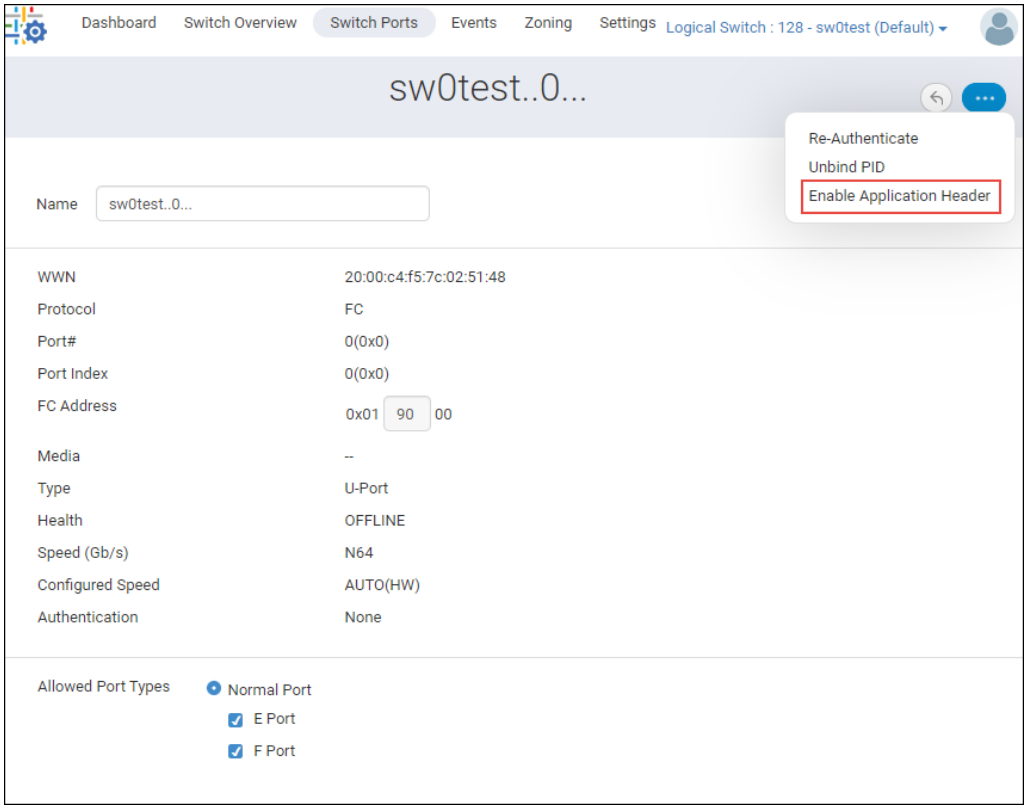
Web Tools supports spoofing application header support on a target or storage port so that end-to-end VM metrics can be captured even on targets, which do not support the application header. You can enable or disable application header support.

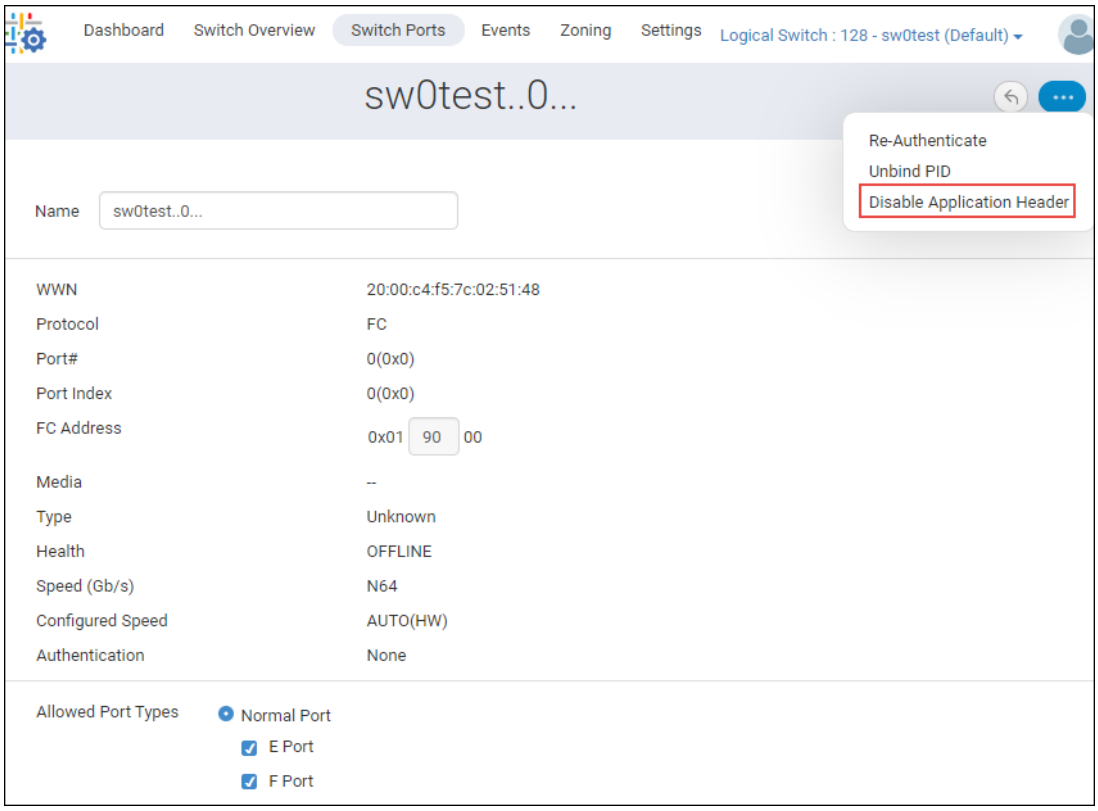
NOTE

- You can enable or disable the application header support only for Gen 7 platforms.
- For a VF-enabled switch, you can configure application header support for four ports per logical switch. For a non-VF chassis, a maximum of 64 ports can be configured with this configuration. Whereas, for a non-VF switch, a maximum of 16 ports can be configured with this configuration.
- Firmware Downgrade to pre Fabric OS (FOS) 9.1.0 version is not supported if application header support is enabled on any port of the chassis or switch.
- You cannot configure application header support on Access Gateway and FICON modes.

To enable or disable application header support, perform the following steps:

1. Click **Switch Ports** in the navigation bar, and then select the **FC Ports** type from the drop-down.
2. Drill down to the port for which you want to enable or disable application header support.
   The port details window appears.
3. To enable application header support, select **Enable Application Header** option from the more icon on the top-right corner of the window. To disable application header support, select **Disable Application Header** option.





Configuring Investigation Mode

The Investigation mode feature provides monitoring capabilities and presents real-time data in detailed performance graphs. The performance graph allows you to investigate the information about basic performance measures such as port throughput, port utilization, and port error rate over a given timeframe using the performance graphs.

The following list describes the measures of the selected ports that are plotted in the performance graphs:

1. **Rx % Utilization** – Displays the percentage of the selected port bandwidth that is used for receiving traffic at the time the sampling is done.
2. **Tx % Utilization** – Displays the percentage of the selected port bandwidth that is used for transmitting traffic at the time the sampling is done.
3. **Rx Bytes (Mb/Sec)** – Displays the traffic information including the number of bytes and frames that are received for the selected interval.
4. **Tx Bytes (Mb/Sec)** – Displays the traffic information including the number of bytes and frames that are transmitted for the selected interval.
5. **CRC Errors** – Displays the count of cyclic redundancy check (CRC) errors for a given port for the configured polling period.

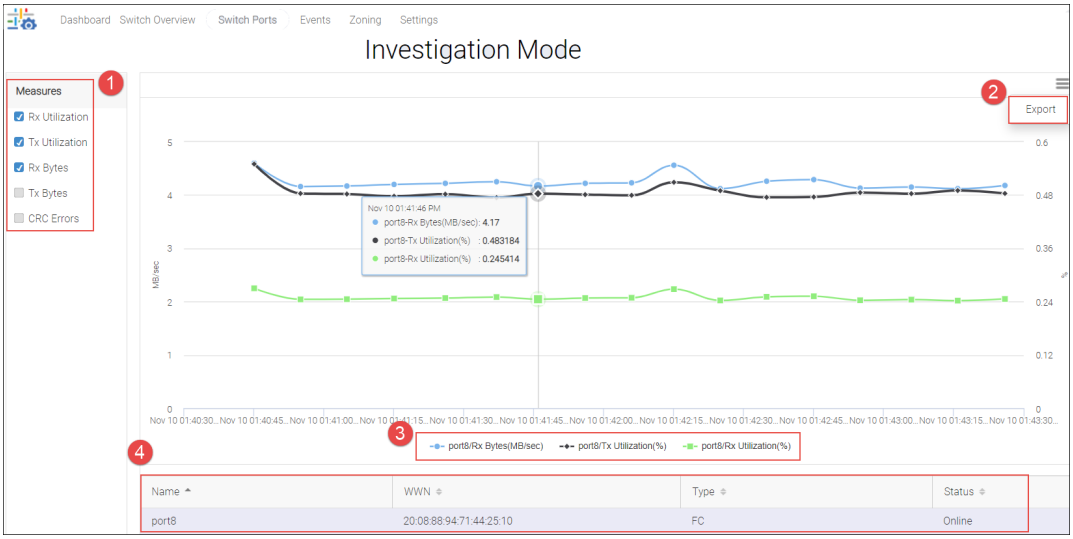
Pause on a data point to view data about the selected measure. Data includes name, type, utilization, traffic, and the maximum or average for the selected measures, and the data collection date and time.

NOTE
The port % utilization is not displayed for VE ports.

The X-axis displays the date and time. The bottom right displays the port performance in a table format.

- **Name**: The port name.
- **WWN**: The world wide name of the port.
- **Type**: The port type.
- **Status**: The status of the port (such as No_Light).

All performance graphs for the selected measures are displayed in a single combined graph in the **Investigation Mode** window. The graph in the **Investigation Mode** window is updated every 30 seconds. When you first view the graph or if you modify the graph (such as to add additional ports), you might have to wait up to 30 seconds before the new values are displayed. You can export the performance graphs by using the **hamburger** (≡) icon at the right corner of the **Investigation Mode** window as an HTML file to the desired location.



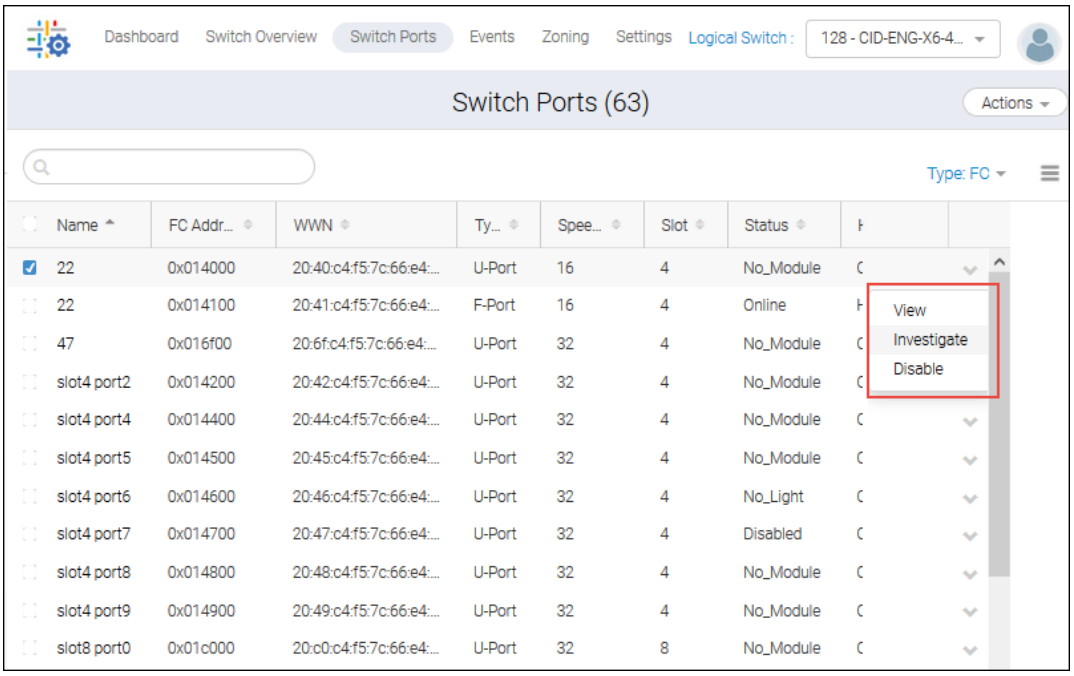
1. Measures
2. Export menu
3. Selected measures
4. Port information

You can access the **Investigation Mode** window with the performance graph for the following ports:

- FC
- ICL
- GigE
- ETH

NOTE
The users with the zone admin or security admin privileges cannot access the **Investigate** options.

To view a real-time performance graph in the **Investigation Mode** window for a port, perform the following steps:



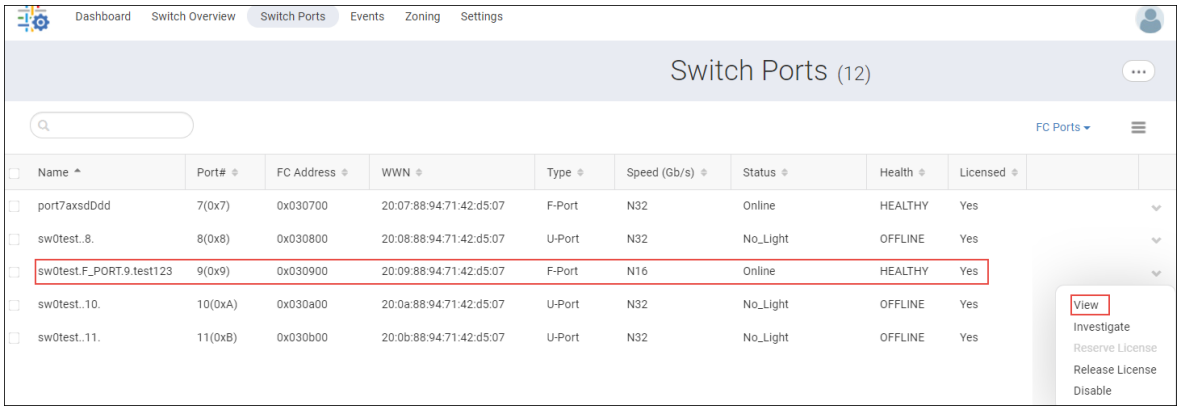
1. Click **Switch Ports** in the navigation bar, and then select port type from the drop-down on which the investigation is to be done.
2. Click the ( ) icon on the right side of the selected port.
3. Select the **Investigate** option from the drop-down.
   The **Investigation Mode** window appears.
4. Select the parameters from the **Measures** section on the left. The graph appears on the right side based on the selected parameters. The time intervals are on the X axis and plotted against the selected parameters on the Y axis in the performance graph.

Viewing FC Port Statistics

The FC statistics section provides various statistics such as in bytes (MB), out bytes (MB), word received, word transmitted, in frames, and out frames.

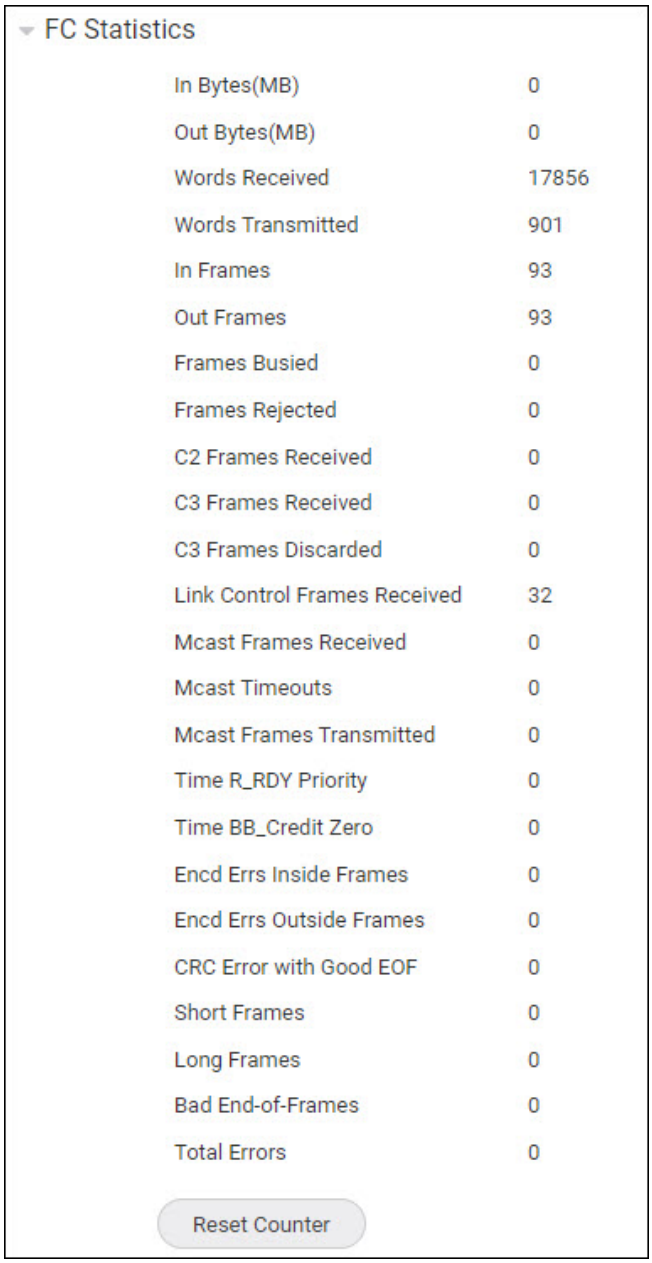
To view FC port statistics, perform the following steps:

1. Click **Switch Ports** from the navigation bar, and then select **FC Ports** from the drop-down.
2. Click the ( ) icon for a selected port, and then select **View** from the available options.



The port details window appears.

3. Expand the **FC Statistics** option to view the port statistics.



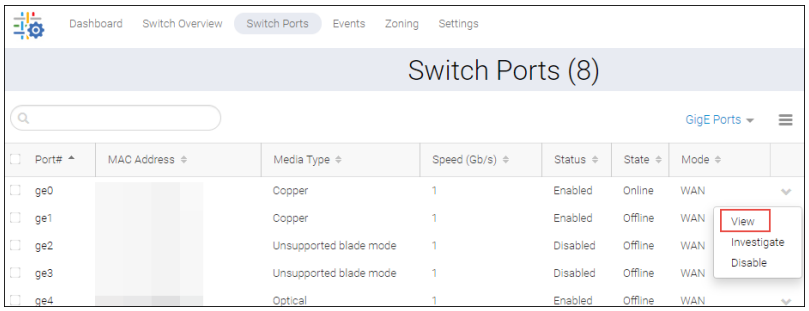
The port statistics data are not refreshed automatically. To reset the statistics to zero, you must click the **Reset Counter** option.

Viewing GigE Port Statistics

The GigE port statistics section provides various statistical information such as In Bytes, Out Bytes, In Frames, and Out Frames.

To view GigE port statistics, perform the following steps:

1. Click **Switch Ports** from the navigation bar, and then select **GigE Ports** from the drop-down.
2. Click the ( ) icon, and then select **View** from the available options. The port details window appears.



3. Select **Statistics** to view the port statistics.

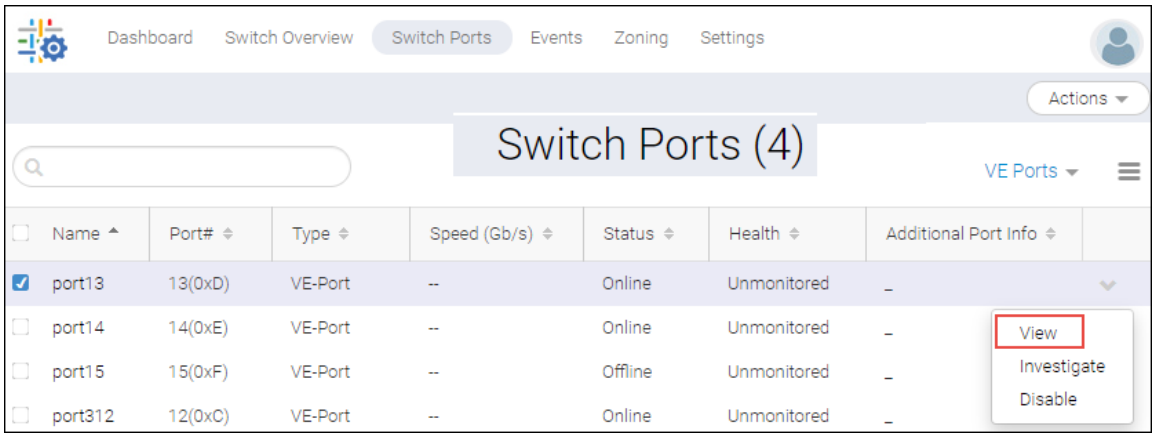
The port statistics data is not refreshed automatically. To reset the statistics to zero, you must select the **Reset Counter** option from the port details window.

Viewing VE Port and Tunnel Statistics

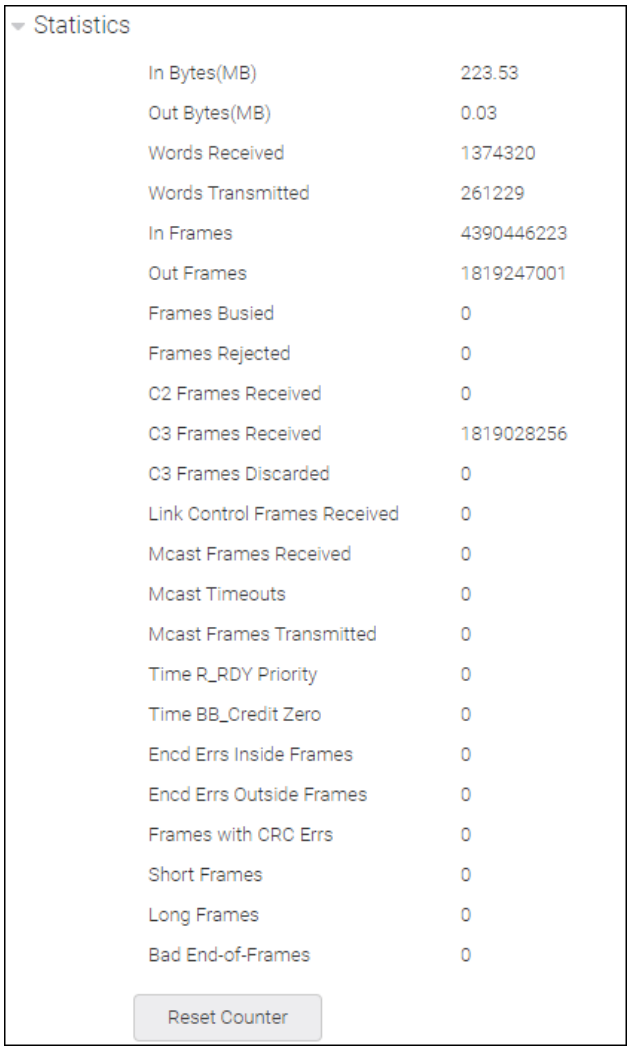
The VE port statistics section provides statistical information such as in bytes, out bytes, in frames, out frames, words received, and words transmitted. The tunnel statistics section provides information such as FCIP aggregate, FCIP QoS, and FCIP TCP statistics of the selected VE port.

To view VE port and tunnel statistics, perform the following steps:

1. Click **Switch Ports** from the navigation bar, and then select **VE Ports** from the drop-down.
2. Click the (⌄) icon, and then select **View** from the available options. The port details window appears.

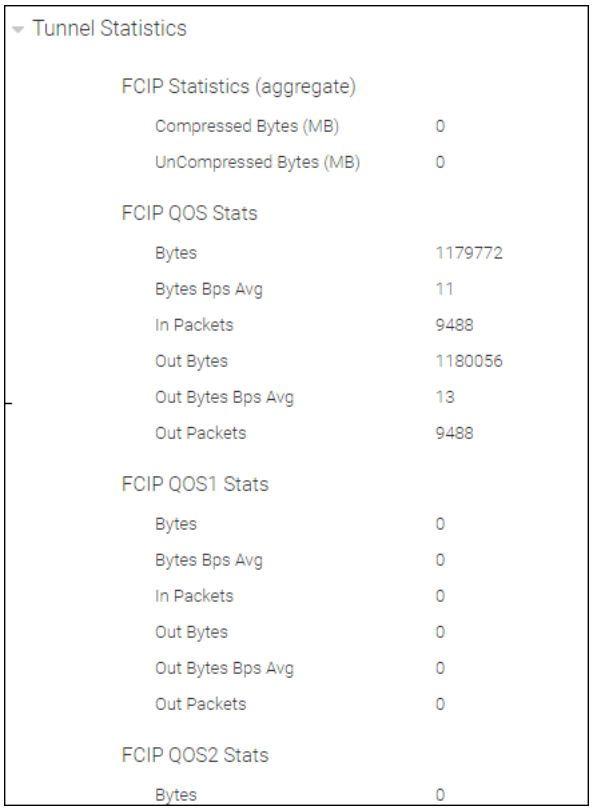


3. Select **Statistics** to view the port statistics.



The port statistics data is not refreshed automatically. To reset the statistics to zero, you must select the **Reset Counter** option from the port details window.

4. Select **Tunnel Statistics** to view the tunnel statistics.



The **Tunnel Statistics** table displays the following information:

- FCIP Statistics (aggregate)
  - Compressed Bytes (MB)
  - UnCompressed Bytes (MB)
- FCIP QOS Stats
  - Bytes
  - Bytes Bps Avg
  - In Packets
  - Out Bytes
  - Out Bytes Bps Avg
  - Out Packets
- FCIP TCP Stats

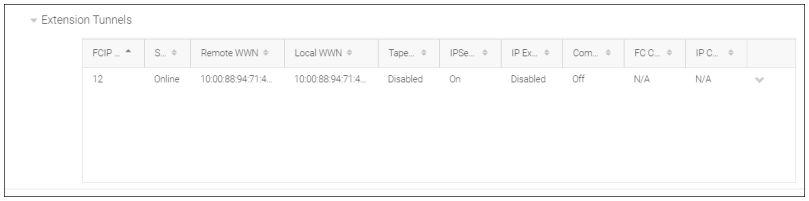
- Circuits Number
- TCP Priority
- Out Packets
- Out Bytes
- In Packets
- In Bytes
- Sender Smothed Round Trip
- Sender Variance
- Sender Congestion Window
- Sender Operation Mode
- Sender Queued Packages
- Sender Queued Packages Seq Min
- Sender Queued Packages Seq Max
- Sender Queued Packages Seq NXT
- Sender In Fight Packets
- Sender Variance High
- Sender UnAcknowledged Seq No
- Sender Retransmit Timeout(ms)
- Sender ReTransmit
- Sender Duplicate ACKs
- Sender Max ReTransmits
- Sender Fast Retransmits
- Receiver Advertised Window Max
- Receiver Negotiated Window Scale
- Receiver Queued Packets
- Receiver Queued Packets Next Seq No
- Receiver Queued Out of Order Packets
- Keep Alive Since Last Act(sec)
- Keep Alive Idle Connection Probe Interval(sec)
- FCIP TCP Runtime Control Stats

Viewing FCIP Tunnels and Circuits

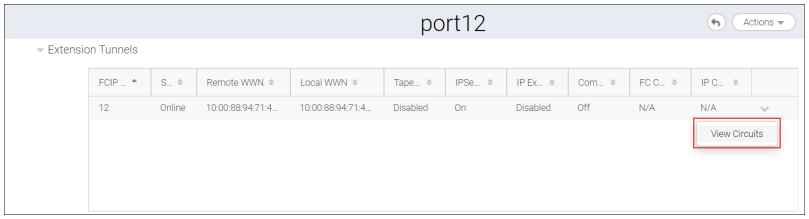
An FCIP tunnel is a transport entity that allows communication between two geographically distributed entities. An FCIP tunnel acts like a Fibre Channel inter-switch link (ISL) over an IP network. An FCIP tunnel consists of two endpoints that are characterized by their IP addresses. Each FCIP tunnel between two FCIP entities may contain one or more TCP endpoints in the IP-based network. An FCIP tunnel is used by applications such as remote backup and disaster recovery. An FCIP tunnel emulates FC ports on the extension switch or blade at each end of the tunnel. When FCIP tunnels are configured, and the TCP connections are established for a complete FCIP circuit, a logical ISL is activated between the switches. An FCIP tunnel is assigned to a VE port on the switch or blade at each end of the tunnel.

To view the FCIP tunnels and FCIP circuit details on a VE port, perform the following steps:

1. Click **Switch Ports** in the navigation bar, and then select **VE Ports** from the drop-down.
2. Select a port, and then click the **View** option that is available on the extreme right. A window is displayed with the selected port details.
3. Select **Extension Tunnels**. The FCIP tunnel information is displayed in the FCIP Tunnel table.



4. Select an FCIP tunnel and click **View Circuits** from the **View** option at the extreme right of the table.

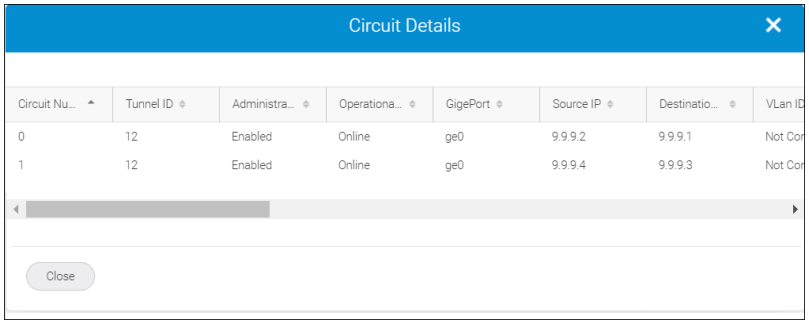


5. The **Circuit Details** dialog appears with the FCIP tunnels and circuit information for the selected FCIP tunnel.

   The FCIP Tunnel table displays the following information:

   - FCIP Port
   - Status
   - Remote WWN
   - Local WWN
   - Tape Pipelining
   - IPSec Policy
   - IP Extension
   - Compression
   - FC Compression
   - IP Compression

   When you select an FCIP tunnel from the FCIP Tunnel table, the following FCIP circuit-specific information is displayed:



- Circuit Number
- Tunnel ID
- Administrator Status
- Operational Status
- GigePort
- Source IP
- Destination IP
- VLan ID
- MTU Size
- HA GigePort
- HA Source IP
- HA Destination IP
- HA VLan ID
- HA MTU Size
- L2CoS (FC: h/m/l)
- L2CoS (IP: h/m/l)
- DSCP (FC: h/m/l)
- DSCP: (IP: h/m/l)
- Keep Alive Timeout (ms)
- Maximum Communication Rate (Mbps)
- Minimum Communication Rate (Mbps)
- Max Retransmits
- Min Retransmit Rate(ms)
- Metric Selective Ack

Viewing a Tunnel Graph

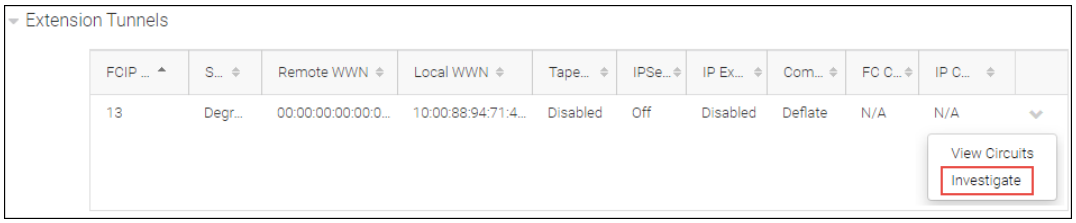
The tunnel graph helps to monitor real-time performance data for the selected tunnel. The polling interval for the tunnel graph is 10 seconds.

The following measures are considered to view a tunnel graph:

- Throughput (MB/sec)
  Indicates the throughput for each tunnel in a switch.
- Effective Throughput (MB/sec)
  Indicates the effective throughput for each tunnel in a switch.
- Compression Ratio (count)
  Indicates the compression ratio for each selected tunnel in a switch.

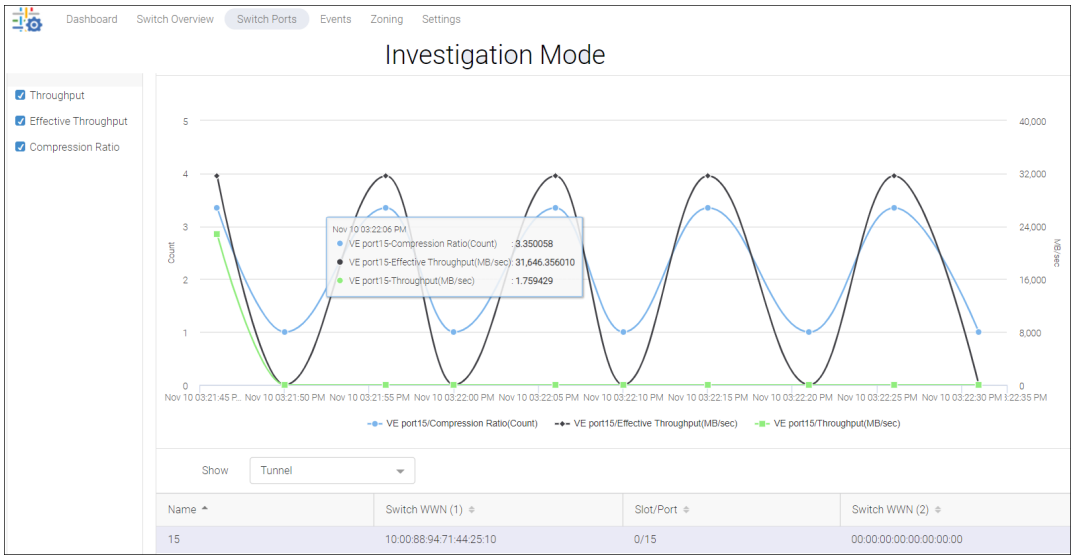
To view a tunnel graph, perform the following steps:

1. Click **Switch Ports** from the navigation bar, and then select **VE Ports** from the drop-down.
2. Click the (⌄) icon, and then select **View** from the available options. The port details window is displayed.
3. Select **Extension Tunnels**. The FCIP tunnel information is displayed in the FCIP Tunnel table.
4. Select an FCIP tunnel, and click **Investigate** from the available options.



The **Investigation Mode** window is displayed. By default, the investigation mode for the selected tunnel appears.

5. Select the measures for which you want to view the graph. You can view the tunnel graph by selecting required tunnel measures from the **Measures** list.



Viewing a TCP Graph

The TCP graph helps to monitor real-time performance data for the circuits of the selected tunnel. The polling interval for the circuit graph is 10 seconds.

The following measures are considered to view a circuit graph:

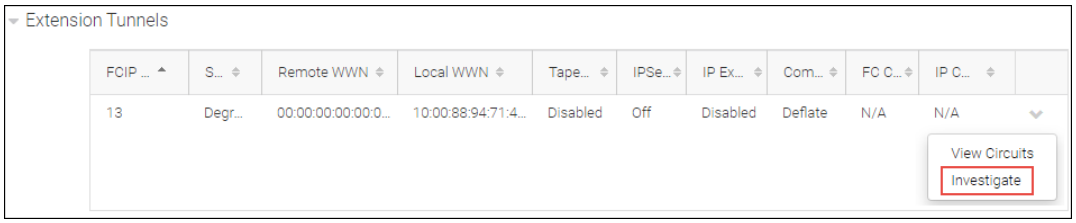
- Sender RTT
  Indicates sender round-trip time for each circuit in a tunnel.
- Sender RTTVariance
  Indicates sender round-trip time variance for each circuit in a tunnel.
- DupAck
  Indicates duplicate acknowledgment for each circuit in a tunnel.
- OOS
  Indicates out-of-order segments for each circuit in a tunnel.
- Slow Starts
  Indicates slow starts for each circuit in a tunnel.
- Fast Retransmit
  Indicates fast retransmits for each circuit in a tunnel.
- TCP Tx
  Indicates TCP Tx for each circuit in a tunnel.
- TCP Rx
  Indicates TCP Rx for each circuit in a tunnel.

NOTE

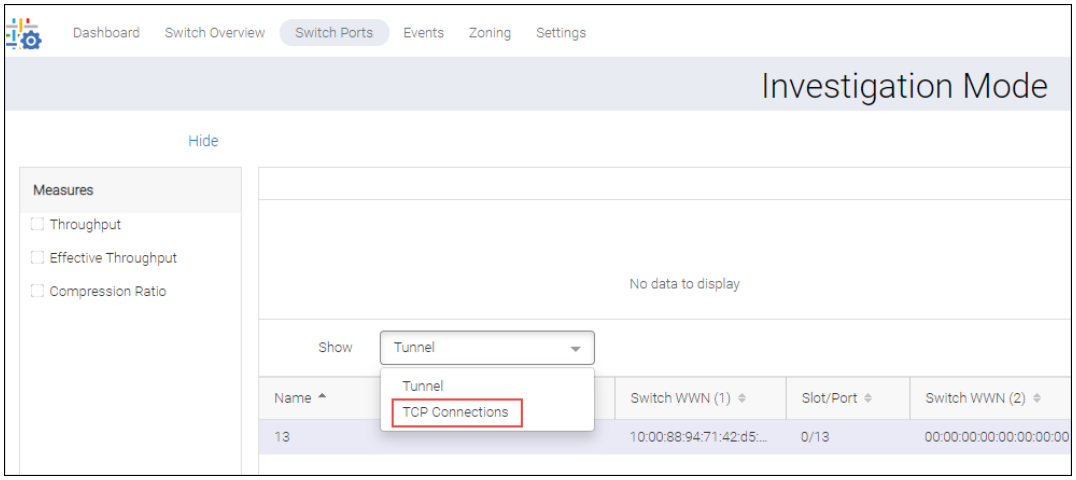
- For a single TCP connection, you can view the graph for a maximum of three selected measures. The remaining measures are in a disabled state. To view the graph for disabled measures, you must clear the already selected measure, and then select the three desired measures.
- For a single measure, you can view the graph for a maximum of four selected TCP connections.
- If you select more than one TCP connection, only one measure can be selected and the remaining measures are in a disabled state.

To view the TCP graph, perform the following steps:

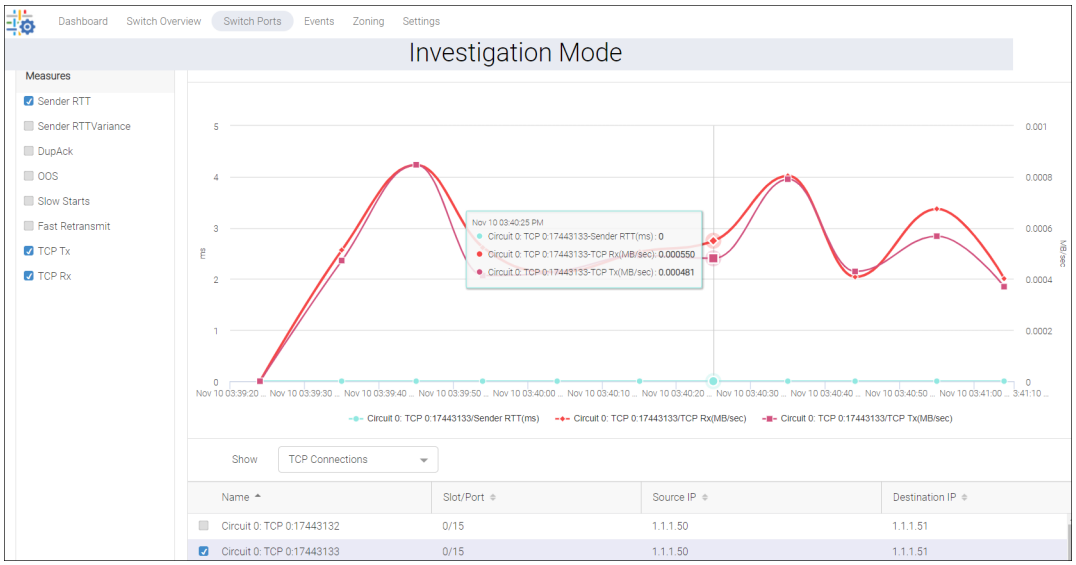
1. Click **Switch Ports** from the navigation bar, and then select **VE Ports** from the drop-down.
2. Click the ( ) icon, and then select **View** from the available options. The port details window appears.
3. Select **Extension Tunnels**. The FCIP tunnel information is displayed in the FCIP Tunnel Table.
4. Select an FCIP tunnel and click **Investigate** from the available options. The **Investigation Mode** window is displayed.

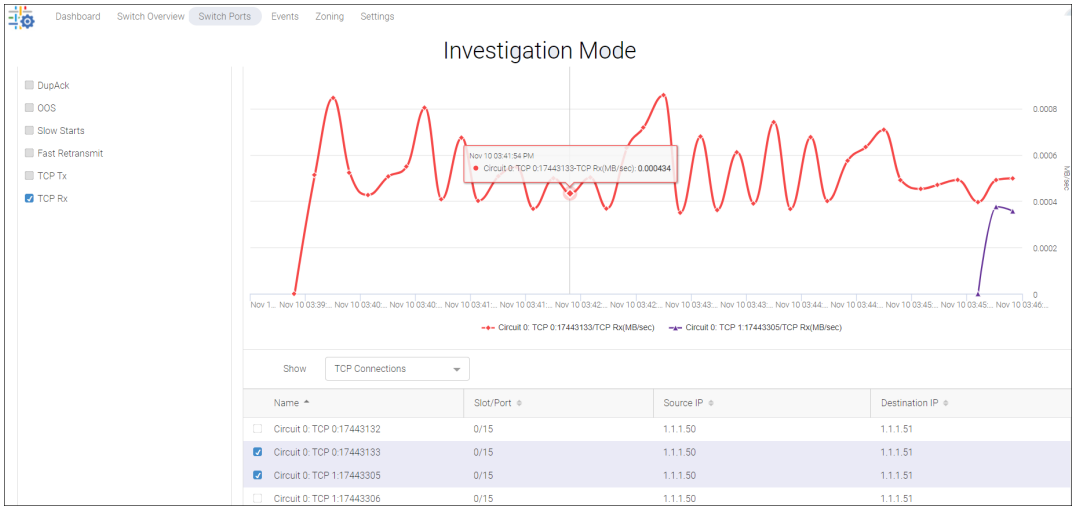


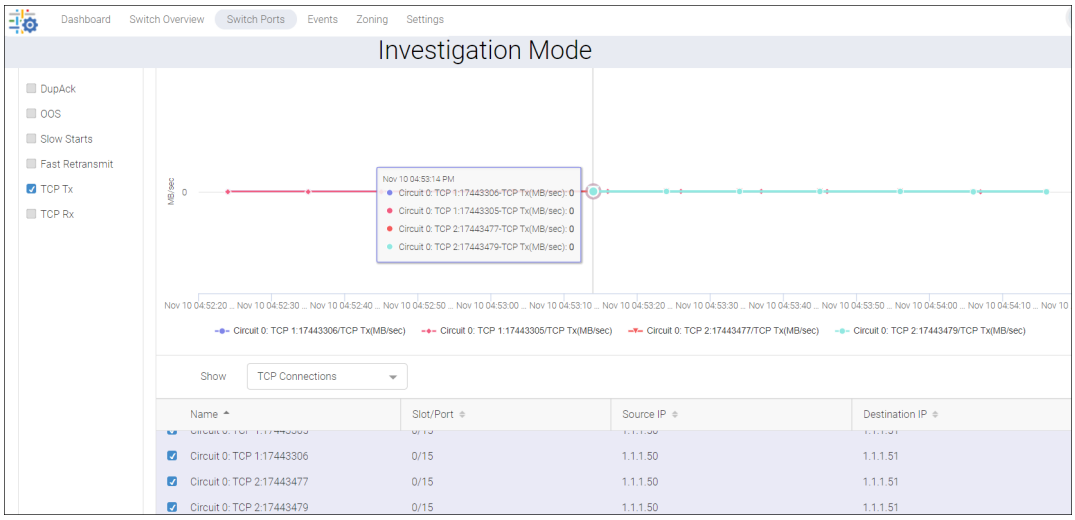
5. Select **TCP Connections** from the **Show** drop-down. The **Measures** list for the TCP connections appears.



6. Select a single TCP connection or a maximum of four TCP connections, and then select the required measures. You can view the TCP graph based on the selected TCP connections and measures.


Dashboard
Switch Overview
Switch Ports
Events
Zoning
Settings
Investigation Mode
Measures
Sender RTT
Sender RTTVariance
DupAck
OOS
Slow Starts
Fast Retransmit
TCP Tx
TCP Rx
Nov 10 03:40:25 PM
Circuit 0: TCP 0:17443133-Sender RTT(ms): 0
Circuit 0: TCP 0:17443133-TCP Rx(MB/sec): 0.000550
Circuit 0: TCP 0:17443133-TCP Tx(MB/sec): 0.000481
Circuit 0: TCP 0:17443133/Sender RTT(ms)
Circuit 0: TCP 0:17443133/TCP Rx(MB/sec)
Circuit 0: TCP 0:17443133/TCP Tx(MB/sec)
Show
TCP Connections
Name
Slot/Port
Source IP
Destination IP
Circuit 0: TCP 0:17443132 0/15 1.1.1.50 1.1.1.51
Circuit 0: TCP 0:17443133 0/15 1.1.1.50 1.1.1.51


Dashboard
Switch Overview
Switch Ports
Events
Zoning
Settings
Investigation Mode
DupAck
OOS
Slow Starts
Fast Retransmit
TCP Tx
TCP Rx
Nov 10 03:41:54 PM
Circuit 0: TCP 0:17443133-TCP Rx(MB/sec): 0.000434
Circuit 0: TCP 0:17443133/TCP Rx(MB/sec)
Circuit 0: TCP 1:17443305/TCP Rx(MB/sec)
Show
TCP Connections
Name
Slot/Port
Source IP
Destination IP
Circuit 0: TCP 0:17443132 0/15 1.1.1.50 1.1.1.51
Circuit 0: TCP 0:17443133 0/15 1.1.1.50 1.1.1.51
Circuit 0: TCP 1:17443305 0/15 1.1.1.50 1.1.1.51
Circuit 0: TCP 1:17443306 0/15 1.1.1.50 1.1.1.51



Trunking

Trunking optimizes network performance by allowing a group of links to merge into a single logical link, called a *trunk group*, that can distribute traffic between switches across a shared bandwidth. Trunking also improves system reliability by maintaining in-order delivery of data and avoiding I/O retries if one link within the trunk group fails.

Trunking can be between two switches, between a switch and an Access Gateway module, or between a switch and a Brocade adapter. The types of trunking are as follows:

- ISL trunking, or E_Port trunking, is configured on an inter-switch link (ISL) between two Fabric OS switches and is applicable only to E_Ports.
- EX_Port trunking is configured on an inter-fabric link (IFL) between an FC router (EX_Port) and an edge fabric (E_Port). The trunk ports are EX_Ports connected to E_Ports.
- F_Port trunking is configured on a link between a switch and either an Access Gateway module or a Brocade adapter. The trunk ports are F_Ports (on the switch) connected to N_Ports (on the Access Gateway or adapter).

The Trunking license is required for any type of trunking, and it must be installed on each switch that participates in trunking.

Creating Trunk Groups

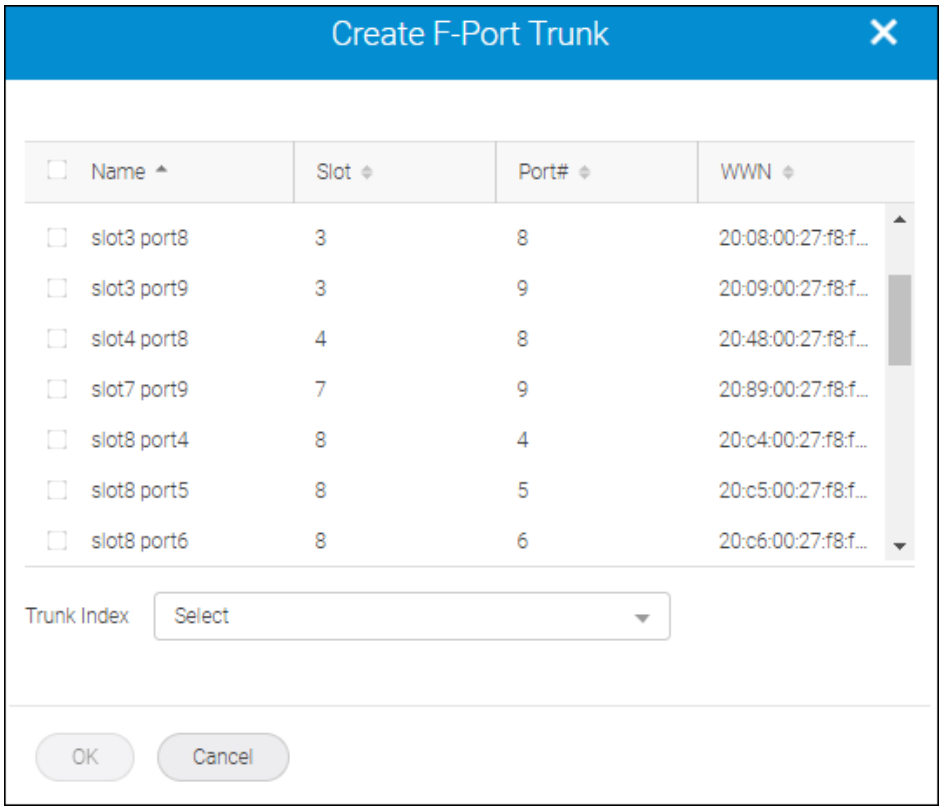
You can create ISL trunks using E_Ports and EX_Ports, and you can create trunks between a switch and an Access Gateway from F_Ports on the switch.

1. Click **Settings** in the navigation bar, and then select **Configuration** > **Trunking**.

   The **Trunks** page displays the list of trunks that have been created on the switch, including offline F_Port trunks.

2. Click the (**+**) icon in the upper right corner, and select the type of trunk you want to create.
3. Select the ports that you want to include in the trunk group.

   For trunk groups to form, all ports in a trunk group must belong to the same port group. A port group is a group of eight ports, based on the user port number, such as 0–7, 8–15, 16–23, and up to the number of ports on the switch. When you select the first port, all other ports that are not in the same port group as the selected port are grayed out. You can select only ports that belong to the same port group.



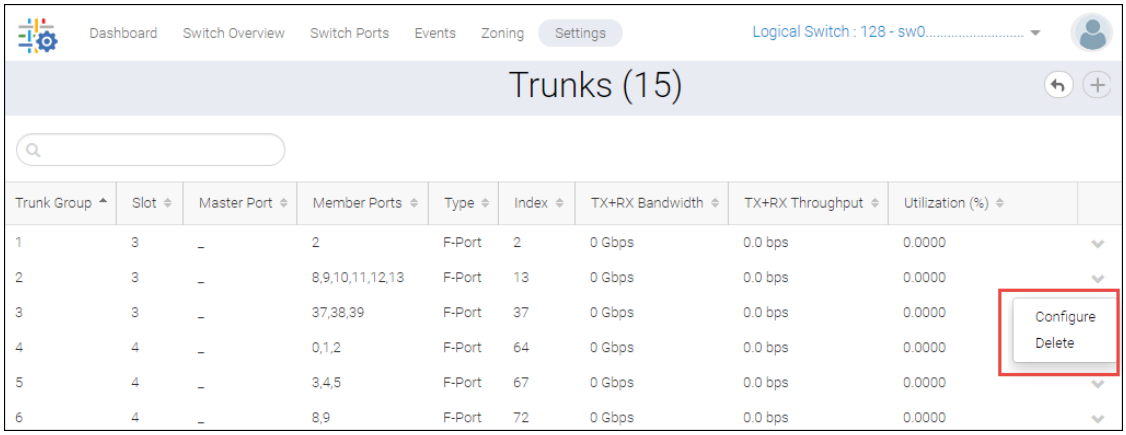
4. For F_Port trunks, select a trunk index from the drop-down at the bottom of the dialog.
5. Click **OK**.
   The trunk group is added to the list.

Modifying Trunk Groups

1. Click **Settings** in the navigation bar, and then select **Configuration** > **Trunking**.
2. Locate the trunk group that you want to modify, and select **Configure** from the action menu in the rightmost column.
3. Select the ports that you want to include in the trunk group, and click **OK**.

Deleting Trunk Groups

1. Click **Settings** in the navigation bar, and then select **Configuration** > **Trunking**.
2. Locate the trunk group that you want to delete, and select **Delete** from the action menu in the rightmost column.



3. Click **OK** in the confirmation message.

Fault Management: Displaying and Filtering Events

The**Events** option allows the user to collect all the fabric and switch-wide events for the selected logical switch and display the information in a bar. It enables you to analyze and troubleshoot the number of events with respect to event severity.

Event information includes sortable fields for the following:

- Message number
- Message
- Service
- Event occurrence count
- Event last occurred

You can filter the chassis and switch events by severity, service, and time, and you can apply either one type of filter at one time or multiple types of filters simultaneously. The impact is cumulative.

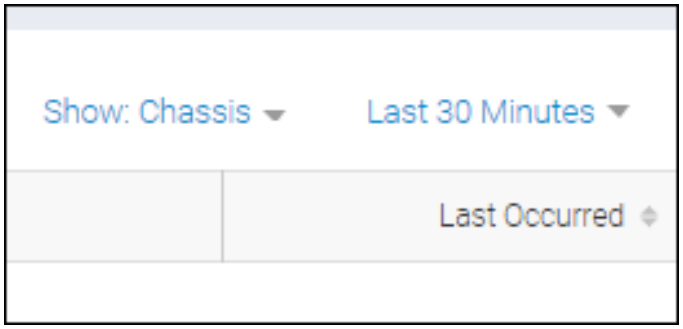
The following table lists the event message severity levels displayed on the **Switch Events** tab and explains what qualifies event messages to be at certain levels.

Level	Description
Critical (Red)	Critical-level messages indicate that the software has detected serious problems that will eventually cause a partial or complete failure of a subsystem if they are not corrected immediately. For example, a power supply failure or a rise in temperature must receive immediate attention.
Alert (Green)	This event does not compromise data or prevent the use of the system; however, the event warrants your attention.
Error (Pink)	Error-level messages represent an error condition that does not impact overall system functionality significantly. For example, error-level messages might indicate timeouts on certain operations, failures of certain operations after retries, invalid parameters, or failure to perform a requested operation.
Warning (Yellow)	Warning-level messages highlight a current operating condition that should be checked or it might lead to a failure in the future. For example, a power supply failure in a redundant system relays a warning that the system is no longer operating in redundant mode. The failed power supply must be replaced or fixed.
Information (Blue)	Information-level messages report the current nonerror status of the system components, such as the online and offline status of a fabric port.
Debug (Pale green)	Debug messages deliver status messages relating to debugging systems.

To display and filter events, perform the following steps:

1. Click **Events** in the navigation bar.

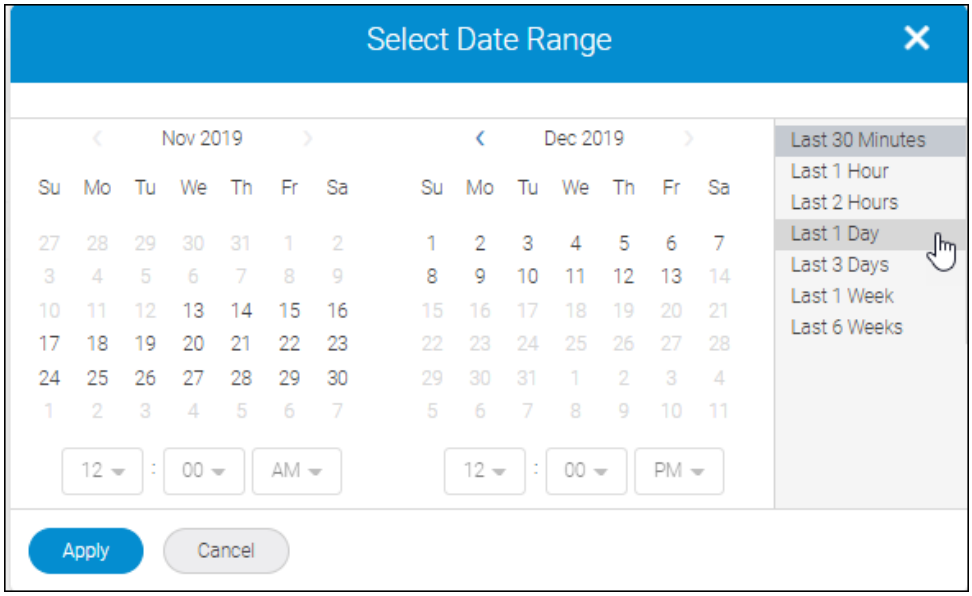
   In the upper right, you see **Last 30 Minutes**. This is the default time interval for the display.



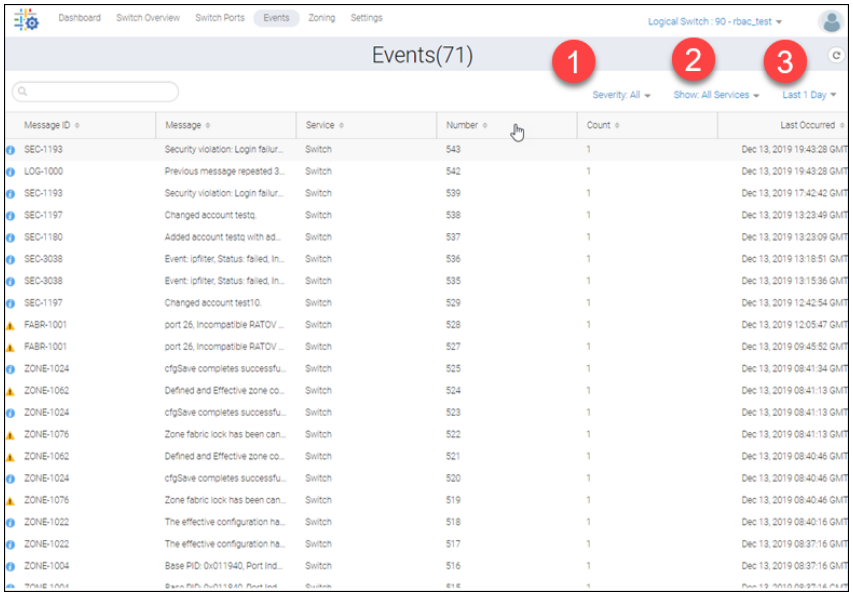
2. Click **Last 30 Minutes**. This displays the **Select Date Range** window.

   Here you can customize the date and time range or select a predefined time interval.

3. For this example, **Last 1 Day** is selected from the predefined time intervals.



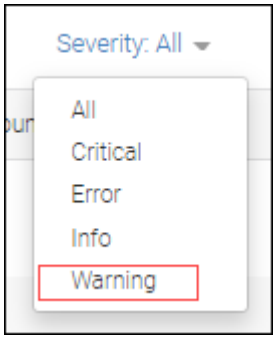
When you click **Last 1 Day**, the table refreshes to display the following.



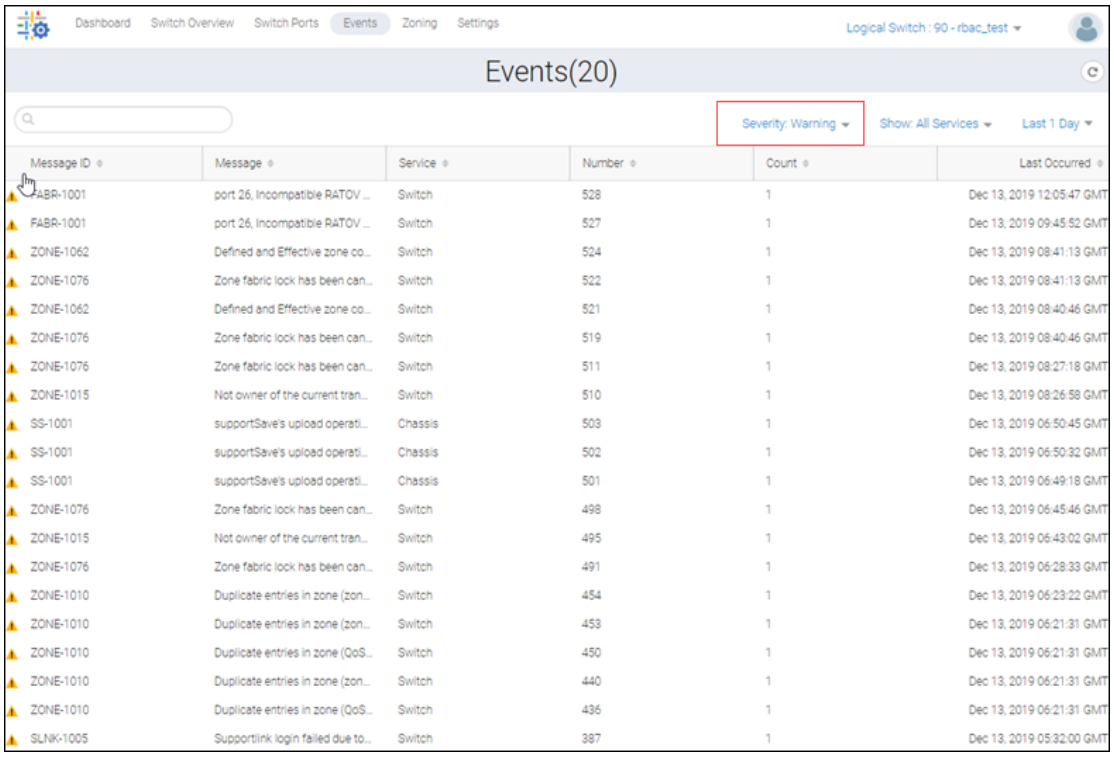
1. Severity Filter
2. Services Filter
3. Date Filter

All the switch events are displayed in this table and the total number of events is shown at the top of the table.

4. By default, all switch events are displayed. Select from the **Severity** menu to filter the specific kind of events with regard to severity. In this example, the selection **Warning** displays only events flagged "Warning."

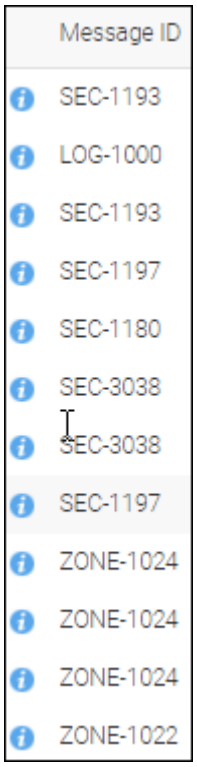


When the filter is enabled, the page refreshes to display the filtered information.



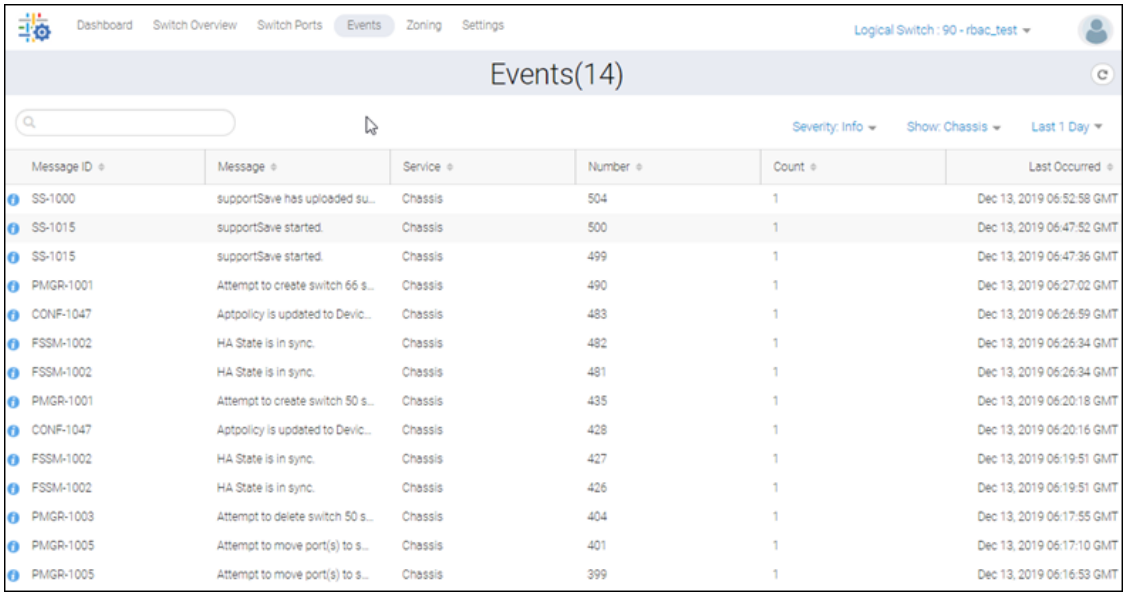
5. To display background details on a particular message, select **Info** from the **Severity** menu.

After the page refreshes, you see blue **i** buttons to the left of each event row.



6. By default, the system displays information for both the chassis and the switch. By selecting from the **Show** menu, you can limit the display to chassis or switches.

   In the following example, **Chassis** is selected. After page refreshes, the chassis related events are displayed.



SNMP Configurations

Simple Network Management Protocol (SNMP) is a set of protocols for managing complex networks. SNMP protocols are application layer protocols. Using SNMP, devices within a network send messages, called protocol data units (PDUs), to different parts of a network. Network management using SNMP requires three components:

- SNMP Manager
- SNMP Agent
- Management Information Base (MIB)

This section describes how to manage the configuration of the SNMP agent in the switch. The configuration includes SNMPv1 configuration, SNMPv3 configuration, and access control list (ACL). Access is read-only if you do not have admin or security admin authority. For detailed information on SNMP, refer to the *Brocade Fabric OS Administration Guide*.

SNMPv3 Configuration

Web Tools supports the following SNMPv3 roles:

- snmpadmin
- snmpuser

The snmpadmin provides read-write access, and the snmpuser role provides read-only access.

The following are the default SNMPv3 users:

- User 1: snmpadmin1
- User 2: snmpadmin2
- User 3: snmpadmin3
- User 4: snmpuser1
- User 5: snmpuser2
- User 6: snmpuser3

NOTE
You can configure a maximum of 12 SNMPv3 users.

The new authKey and privKey are generated when a new password is entered for user entry. You have to update the new passwords on the client (such as a MIB browser). The authKey and privKey can also be updated using the delta key mechanism that is provided by the SNMPv3 protocol.

NOTE

- The length of the protocol password must be in the range of 8 to 32 characters.
- The trap recipient value must be associated with one of the six users of SNMPv3 and the trap severity level. The default value for the SNMPv3 trap recipient of each user is 0.0.0.0.
- The SNMPv3 configuration screen allows you to add the trap recipient server IPs along with the fields, such as the port number and trap level with the user IDs for adding the SNMP users, which are preexisting with the switch in UI, such as snmpadmin1, snmpadmin2, snmpuser1, snmpuser2.

The following table shows the authentication and privacy protocols that are supported to configure SNMPv3 users.

Protocols	Options
Auth. protocol	• MD5 • SHA • noAuth • SHA-512
Priv. protocols	• DES • noPriv • AES128 • AES256

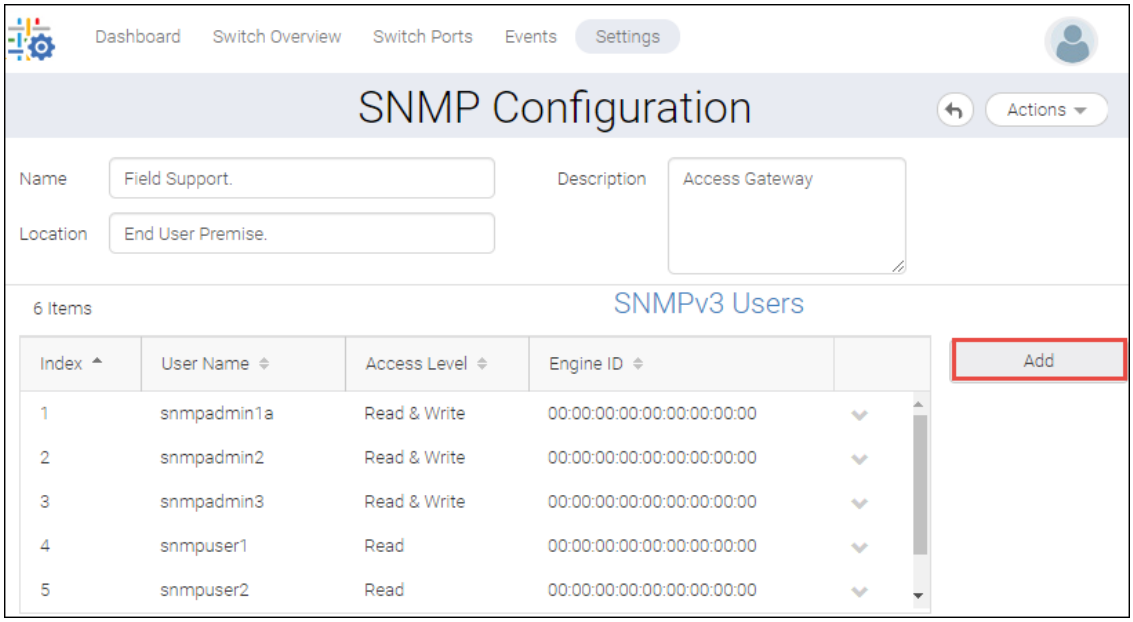
NOTE
From Fabric OS v9.2.0, it is strongly recommended to use SHA512. The Auth. Protocol MD5 and SHA are deprecated and will not be supported in a future release.

NOTE
From Fabric OS v9.2.0, it is strongly recommended to use AES128 or AES256. The privacy protocol DE5 is deprecated and will not be supported in a future release.

Configuring an SNMPv3 User

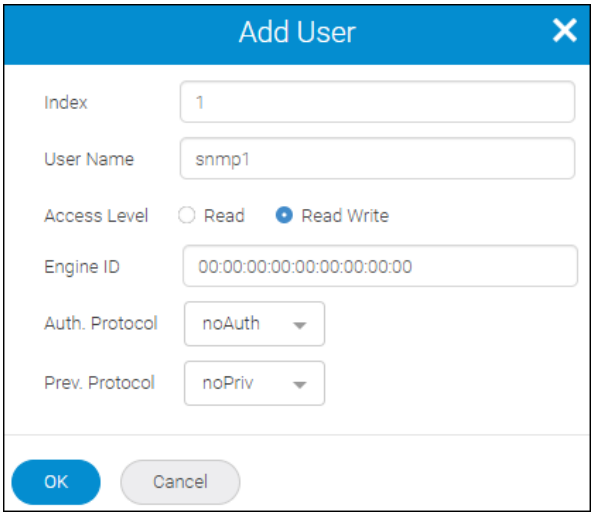
To create an SNMPv3 user, perform the following steps:

1. Click **Settings** from the navigation bar, and then select the **Event Management** > **SNMP Configuration** tab.
   The **SNMP Configuration** window is displayed.



2. Click **Add** from the **SNMPv3 Users** table. The **Add User** window is displayed.
   a) Enter the index and user name. The index and user name must be unique.
   b) Select the access level either as **Read** or as **Read Write** and provide an **Engine ID**.
   c) Select the required protocol from the **Auth. Protocol** and **Priv. Protocol** drop-down, and then provide the password in the **Auth Password** and **Priv Password** fields, respectively. Select the **Encrypt Password Enable**

option from the **Actions** menu to encrypt the password. To disable the encryption, select **Encrypt Password Disable** from the **Actions** menu.



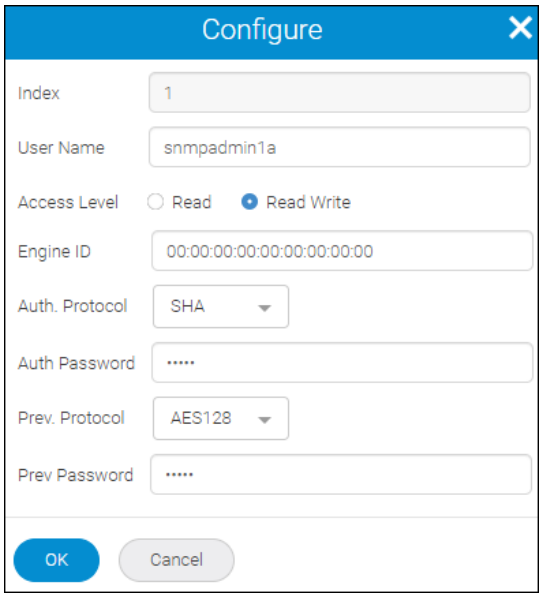
The **Engine ID** field does not appear if you do not select **Informs Enable** from the **Actions** menu.

3. Click **OK**. The SNMPv3 user is added to the **SNMPv3 Users** table.

Modifying an SNMPv3 User Configuration

To modify an existing SNMPv3 user, perform the following steps:

1. Click **Settings** from the navigation bar, and then select the **Event Management** > **SNMP Configuration** tab.
   The **SNMP Configuration** window is displayed.
2. Click the ( ) icon next to the SNMPv3 user that you want to modify, and then select **Configure** from the available options.
   The **Configure** window is displayed.



3. You can modify the parameters based on your requirements.
   You cannot modify the index ID of an SNMPv3 user.

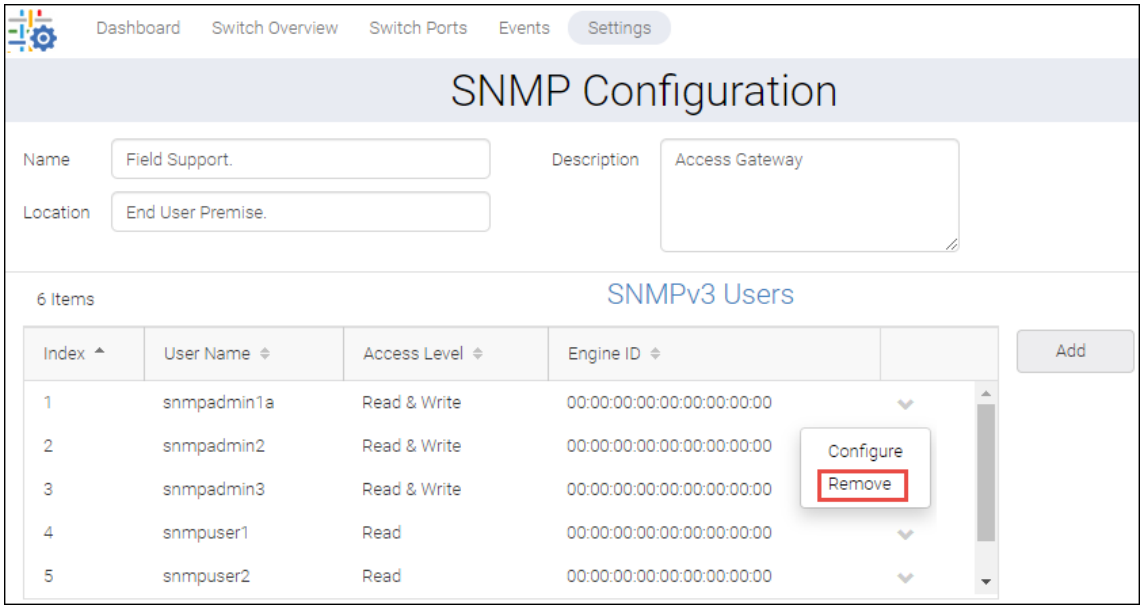
4. Click **OK**.

Removing an SNMPv3 User

NOTE
You cannot remove an SNMPv3 user if the trap recipient is configured for this account.

To remove an existing SNMPv3 user, perform the following steps:

1. Click **Settings** from the navigation bar, and then select the **Event Management** > **SNMP Configuration** tab.
   The **SNMP Configuration** window is displayed.
2. Click the ( ) icon next to the SNMPv3 user that you want to remove, and then select **Remove** from the available options.
3. Select **Remove** from the available options. The SNMPv3 user is removed from the **SNMPv3 Users** table.



Configuring SNMPv3 Trap Recipients

SNMPv3 has a tabular column of informs or trap recipients. The column is empty by default if there are no existing recipients. You can add a maximum of six SNMPv3 trap recipients to the **SNMPv3 Informs/Trap Recipients** table. The **SNMPv3 Informs/Trap Recipients** table contains the status of informs and the host IP address.

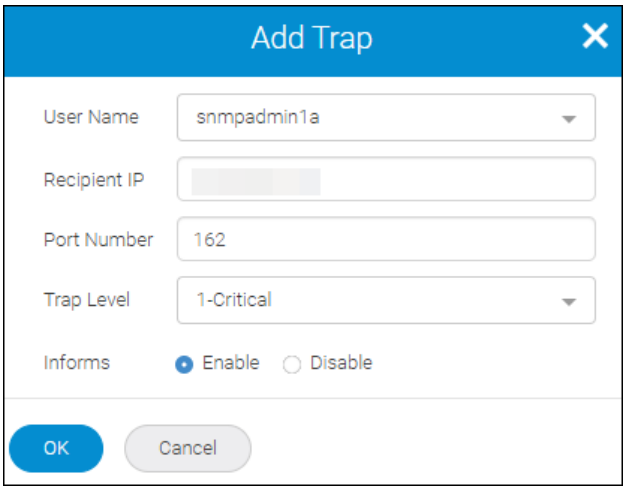
There are six trap levels:

- 0 – None
- 1 – Critical
- 2 – Error
- 3 – Warning
- 4 – Informational
- 5 – Debug

NOTE
You can configure the maximum of six trap recipients, or each user can be assigned to a maximum of six traps.

To configure an SNMPv3 trap recipient, perform the following steps:

1. Click **Settings** from the navigation bar, and then select the **Event Management** > **SNMP Configuration** tab.
   The **SNMP Configuration** window is displayed.
2. Click **Add** from the **SNMPv3 Informs/Trap Recipients** table. The **Add Trap** window is displayed.
   a) Select the user from the **User Name** drop-down.
   b) Enter the recipient IP address and the port number.
   c) Select the trap level from the **Trap Level** drop-down.
   d) Enable or disable the informs.

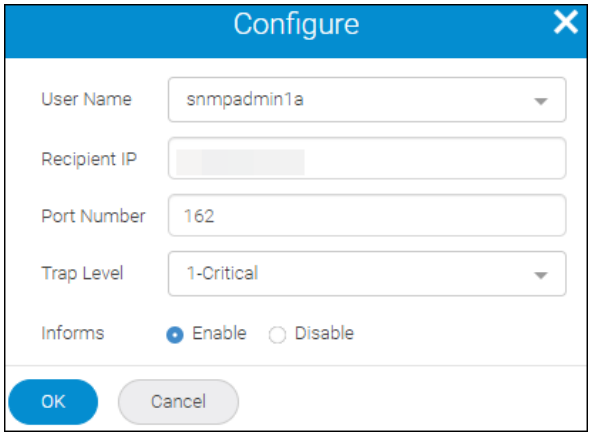


   You must select **Informs Enable** from the **Actions** menu to enable or disable informs in the **Add Trap** window.
3. Click **OK**. The trap is added to the **SNMPv3 Informs/Trap Recipients** table.

Modifying SNMPv3 Trap Recipients

To modify SNMPv3 recipients, perform the following steps:

1. Click **Settings** from the navigation bar, and then select the **Event Management** > **SNMP Configuration** tab.
   The **SNMP Configuration** window is displayed.
2. Click the ( ) icon next to the SNMPv3 trap that you want to modify, and then select **Configure** from the available options.
   The **Configure** window is displayed.

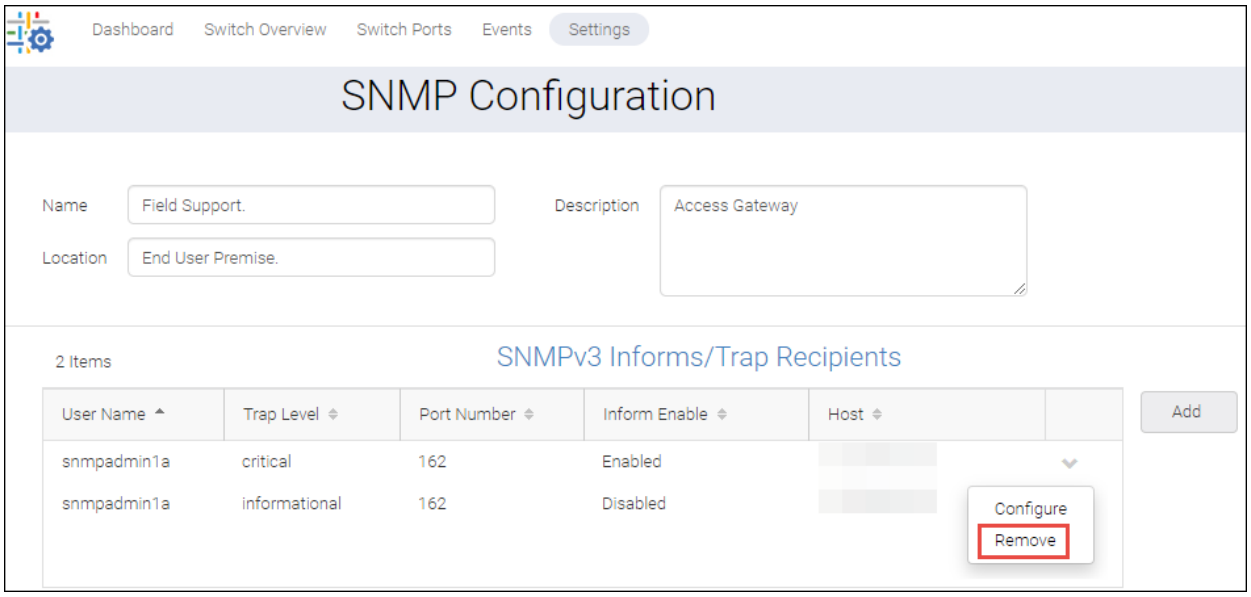


3. Modify the already configured parameters based on your requirements.
4. Click **OK**.

Removing an SNMPv3 Trap

To remove an existing SNMPv3 trap, perform the following steps:

1. Click **Settings** from the navigation bar, and then select the **Event Management** > **SNMP Configuration** tab.
   The **SNMP Configuration** window is displayed.
2. Click the ( ) icon next to the SNMPv3 trap that you want to remove.
3. Select **Remove** from the available options. The SNMPv3 trap is removed from the **SNMPv3 Informs/Trap Recipients** table.



SNMPv1 Configuration

SNMPv1 supports six communities, respective trap recipients, and trap recipient severity. The first three communities are for Read Write access, and the last three are for Read access. The default value for the trap recipient of each community is 0.0.0.0. The length of the community string must be in the range of 2 to 20 characters.
The following are the default values for the community strings:

- Community 1: Secret C0de
- Community 2: OrigEquipMfr
- Community 3: private
- Community 4: public
- Community 5: common
- Community 6: FibreChannel

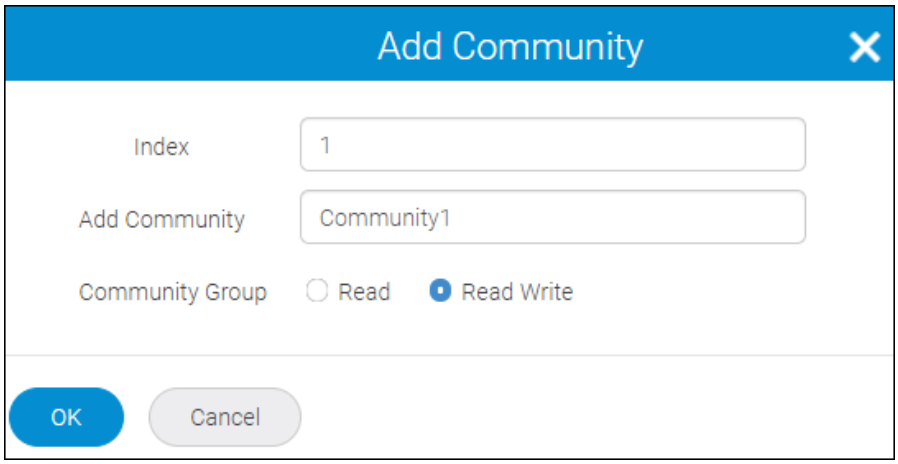
When secure mode is enabled, community strings can be changed only on the primary FCS switch and the changes are propagated across the fabric.

NOTE
You can configure a maximum of six SNMPv1 users.

Configuring an SNMPv1 Community

To add an SNMPv1 community, perform the following steps:

1. Click **Settings** from the navigation bar, and then select the **Event Management** > **SNMP Configuration** tab.
   The **SNMP Configuration** window is displayed.
2. Click **Add** from the **SNMPv1 Community** table.
   The **Add Community** window is displayed.
3. Enter the index and the name of the community. Assign the community group as either **Read** or **Read Write**.

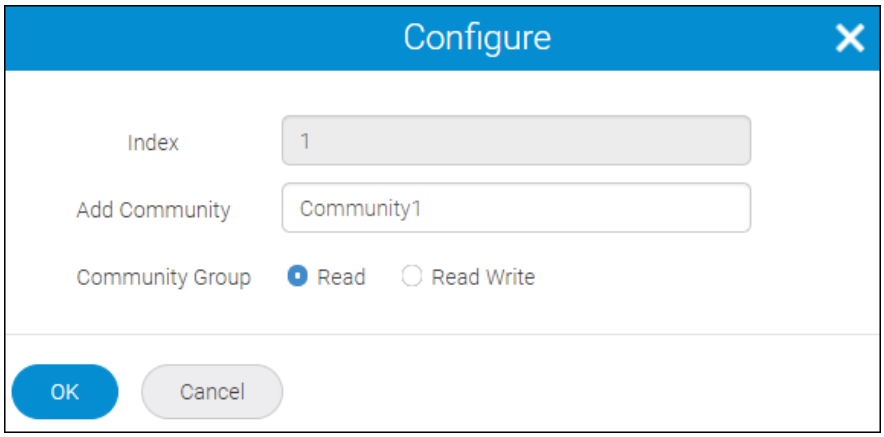


4. Click **OK**. The community is added to the **SNMPv1 Community** table.

Modifying an SNMPv1 Community

To modify an SNMPv1 community, perform the following steps:

1. Click **Settings** from the navigation bar, and then select the **Event Management** > **SNMP Configuration** tab.
   The **SNMP Configuration** window is displayed.
2. Click the ( ) icon next to the SNMPv1 community that you want to modify, and then select **Configure** from the available options.



3. You can modify the already configured parameters based on your requirements except for the index value.
4. Click **OK**.

Removing an SNMPv1 Community

NOTE
You cannot remove an SNMPv1 community if the trap recipient is configured for this account.

To remove an SNMPv1 community, perform the following steps:

1. Click **Settings** from the navigation bar, and then select the **Event Management** > **SNMP Configuration** tab.
   The **SNMP Configuration** window is displayed.
2. Click the ( ) icon next to the SNMPv1 community that you want to remove.

3. Select **Remove** from the available options. The SNMPv1 community is removed from the **SNMPv1 Community** table.

Configuring an SNMPv1 Trap Recipient

SNMPv1 has a tabular column of informs or trap recipients. The column is empty by default if there are no existing recipients. You can add a maximum of six SNMPv1 trap recipients to the **SNMPv1 Informs/Trap Recipients** table. For an SNMP management station to receive a trap generated by the agent, the administrator must configure a trap recipient to correspond to the IP address of the management station. In addition, the trap recipient must be able to pass the access control list (ACL) check.

When an event occurs and if its severity level is at or below the set value, the SNMP traps and Event Trap traps (swEventTrap, connUnitEventTrap, and swFabricWatchTrap) are sent to the configured trap recipients. By default, the trap severity level is set to zero.

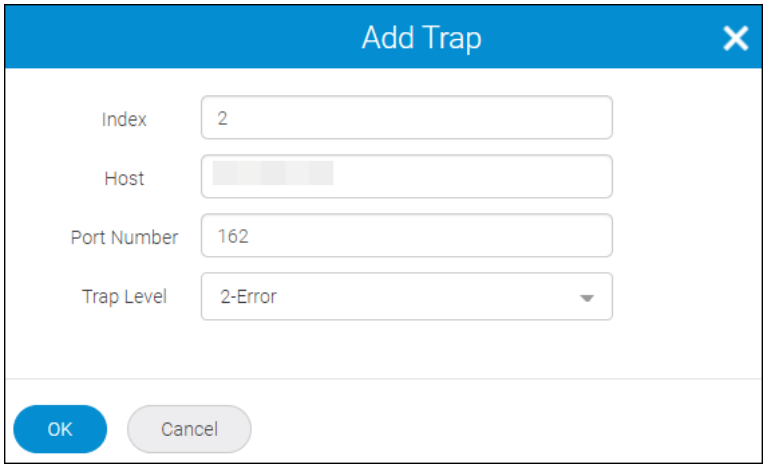
There are six trap levels:

- 0 – None
- 1 – Critical
- 2 – Error
- 3 – Warning
- 4 – Informational
- 5 – Debug

NOTE
You can configure a maximum of six trap recipients, or each user can be assigned to a maximum of six traps.

To configure an SNMPv1 trap recipient, perform the following steps:

1. Click **Settings** from the navigation bar, and then select the **Event Management** > **SNMP Configuration** tab.
   The **SNMP Configuration** window is displayed.
2. Click **Add** from the **SNMPv1 Informs/Trap Recipients** table. The **Add Trap** window is displayed.
   a) Enter the index, host IP address, and port number.
   b) Select the trap level from the **Trap Level** drop-down.

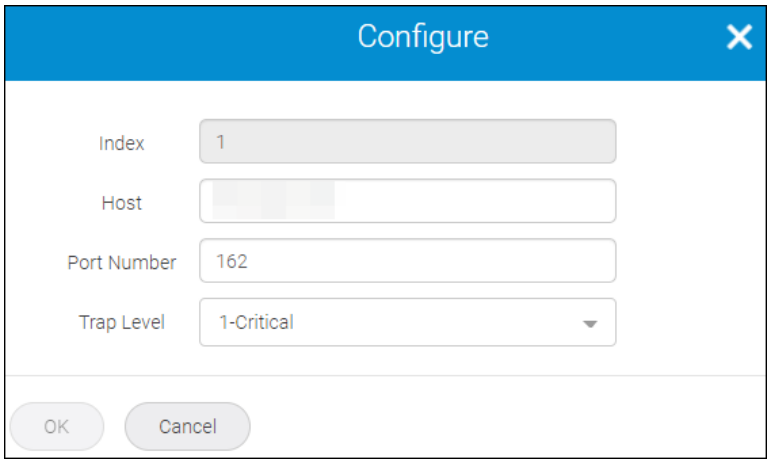


3. Click **OK**. The trap is added to the **SNMPv1 Informs/Trap Recipients** table.

Modifying an SNMPv1 Trap Recipient

To modify an SNMPv1 trap recipient, perform the following steps:

1. Click **Settings** from the navigation bar, and then select the **Event Management** > **SNMP Configuration** tab.
   The **SNMP Configuration** window is displayed.
2. Click the ( ) icon next to the SNMPv1 trap that you want to modify, and then select **Configure** from the available options.
   The **Configure** window is displayed.

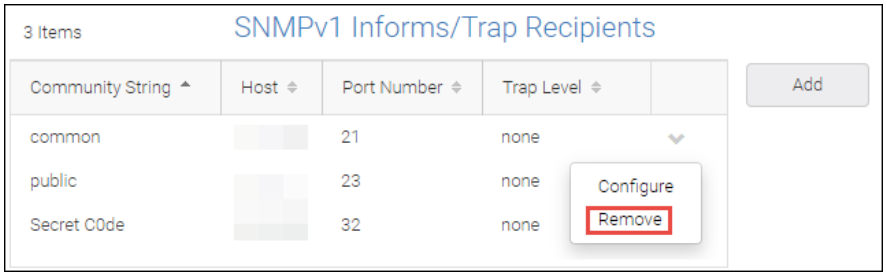


3. Modify the already configured parameters based on your requirements (you cannot modify the index value).
4. Click **OK**.

Removing an SNMPv1 Trap Recipient

To remove an SNMPv1 trap recipient, perform the following steps:

1. Click **Settings** from the navigation bar, and then select the **Event Management** > **SNMP Configuration** tab.
   The **SNMP Configuration** window is displayed.
2. Click the ( ) icon next to the SNMPv1 trap that you want to remove.



3. Select **Remove** from the available options. The SNMPv1 trap is removed from the **SNMPv1 Informs/Trap Recipients** table.

Configuring an SNMP Agent

To configure an SNMP agent, perform the following steps:

1. Click **Settings** from the navigation bar, and then select the **Event Management** > **SNMP Configuration** tab.
   The **SNMP Configuration** window is displayed.

2. Configure an SNMPv3 user. For detailed information, see the section SNMPv3 Configuration.
3. Configure an SNMPv3 trap recipient. For detailed information, see the section SNMPv3 Configuration.
4. Configure an SNMP v1 community. For detailed information, see the section SNMPv1 Configuration.
5. Configure an SNMPv1 trap recipient. For detailed information, see the section SNMPv1 Configuration.
6. Click **Save**.

Access Control List Configurations

An access control list (ACL) allows you to restrict the access permissions between the devices within the fabric. The following are the three types of ACLs:

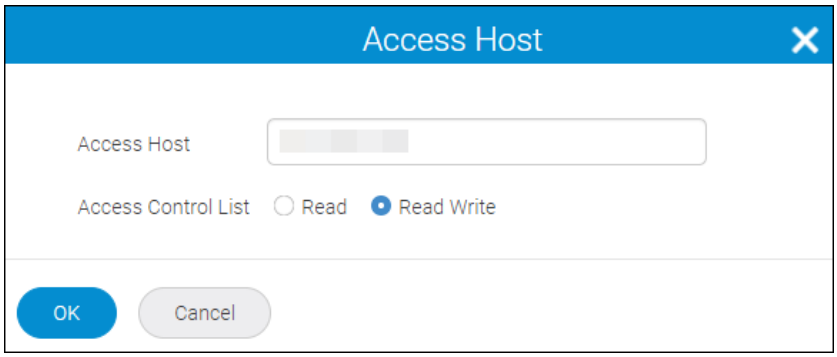
- Switch Connection Control (SCC)
- Fabric Configuration Server (FCS)
- Device Connection Control (DCC)

There are six ACLs to restrict SNMP get or set or trap operations to hosts under a host-subnet-area. The host-subnet-area is defined by comparing nonzero IP octets. For example, an ACL of 192.168.64.0 enables access by any hosts that start with the specified octets. The ACL check is turned off when all six entries contain 0.0.0.0. The default values of all six entries are 0.0.0.0. The ACL can be provided with the Access Host and ACL details for the users with read-only and read-write permission.

Adding an Access Host

To add an access host, perform the following steps:

1. Click **Settings** from the navigation bar, and then select the **Event Management** > **SNMP Configuration** tab.
   The **SNMP Configuration** window is displayed.
2. Click **Add** from the **Access Control List** table. The **Access Host** window is displayed.
3. Enter the access host IP, and then select ACL either as **Read** or as **Read Write**.



4. Click **OK**.
   The ACL is added to the **Access Control List** table.

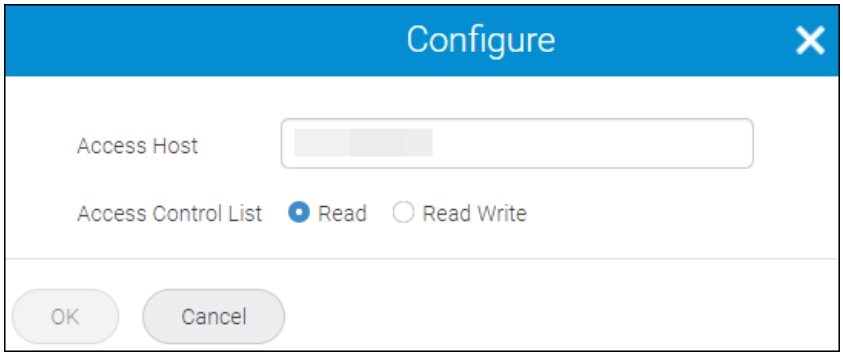
Modifying an Access Host

To modify an access host, perform the following steps:

1. Click **Settings** from the navigation bar, and then select the **Event Management** > **SNMP Configuration** tab.
   The **SNMP Configuration** window is displayed.

2. Click the ( ) icon next to the access host that you want to modify, and then select **Configure** from the available options.

   The **Configure** window is displayed.



3. Edit the already configured parameters based on your requirements.
4. Click **OK**.

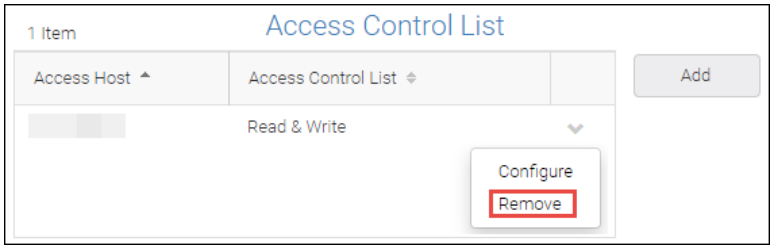
Removing an Access Host

To remove an access host, perform the following steps:

1. Click **Settings** from the navigation bar, and then select the **Event Management** > **SNMP Configuration** tab.

   The **SNMP Configuration** window is displayed.

2. Click the ( ) icon next to the access host that you want to remove.



3. Select **Remove** from the available options. The access host is removed from the **Access Control List** table.

Traffic Management - Routing Policies

Web Tools allows you to perform routing operations and Dynamic Load Sharing (DLS) configurations.

The supported routing policies follow:

- Exchange-based (the default)
- Port-based
- Device-based

Exchange-based

Exchange-based routing (EBR) always uses *dynamic path selection*, in which the software defines a path based on current traffic conditions. When EBR is selected, dynamic load sharing (DLS) is automatically selected, as exchange depends on DLS. It cannot be disabled.

Port-based

Port-based routing (PBR) is a per-switch policy, where a path (default or user-configured) is based solely on the ingress port and destination. All ports with FICON devices attached must have PBR enabled.

When PBR is active, you can enable DLS to optimize routing by sharing traffic among multiple equivalent paths between switches. Load-sharing is recomputed either when a switch boots up or whenever an E_Port or EX_Port goes online or offline. Enabling this feature allows a path to be discovered automatically by the FSPF-path-selection protocol.

Device-based

Device-based routing (DBR) uses the address of the source (SID) and destination (DID) devices to determine the path inside the switch. So, traffic between different SID and DID uses different paths to better utilize the path in the switch.

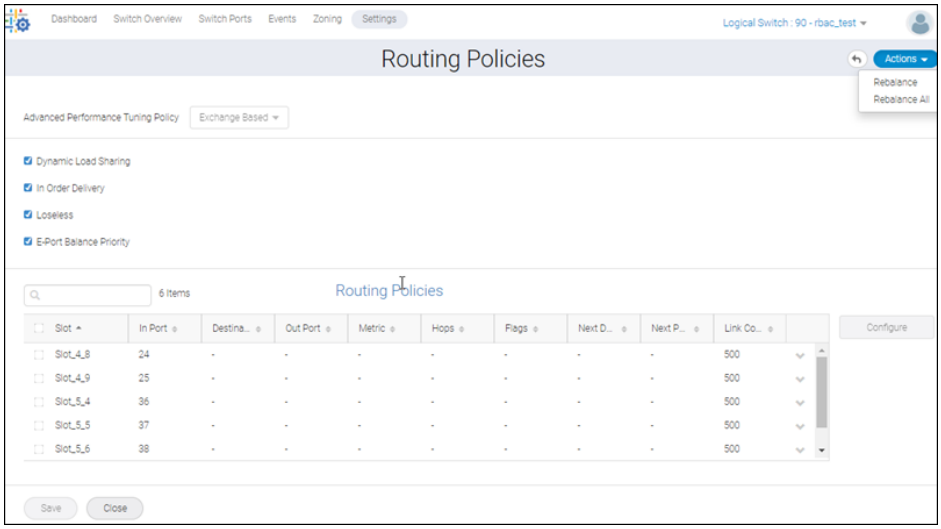
DBR is read-only; if DBR is set, the DBR radio button appears auto-selected and is unavailable in Web Tools.

NOTE
To perform any operation and to reflect configuration changes, your switch must be in a disabled state.

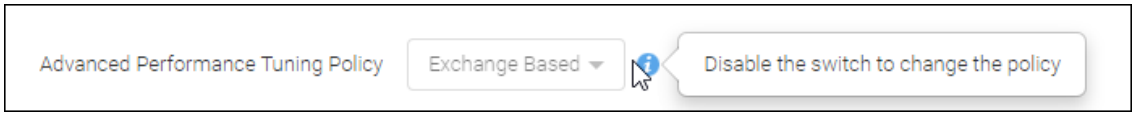
Displaying and Configuring Routing Policies

To display and configure routing policies, perform the following steps:

1. Select the **Configuration > Routing Policies** on the **Settings** page.



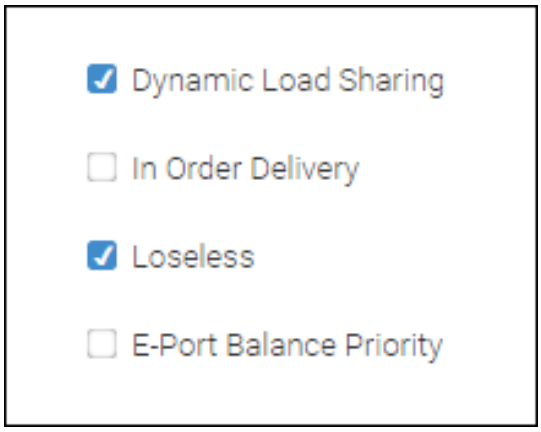
2. The **Advanced Performance Tuning Policy** menu allows you to select a routing method, which establishes collision domains to reduce network traffic.



   By default, exchange-based routing is in effect. To change the policy, select it from the routing list.

   This setting here dictates what is displayed in the table at the bottom of the **Routing Policies** page.

3. Check **Dynamic Load Sharing** (DLS) to optimize the selected routing policy by balancing the load across the available output ports within a domain. DLS recomputes load sharing whenever a switch boots up or an E_Port or FX_Port goes online or offline. This avoids input/output (I/O) failures while rebalancing port paths.



4. Check **E-Port Balance Priority** to balance the E_Port load across all E_Ports with the same domain during a topology change.

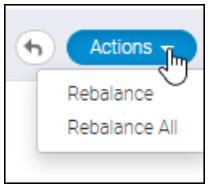
   Because E-Port Balance Priority (EBR) depends on DLS for dynamic routing path selection, DLS is always active (when EBR is selected) and cannot be disabled.

5. The order in which frames are delivered is determined by the prevailing routing policy within the switch. To enable In Order Delivery (IOD) frame delivery and thereby ensure that frames are either delivered or dropped, select **In Order Delivery**.

   In a stable fabric, frames are always delivered in order, even when the traffic between switches is shared among multiple paths. However, when topology changes occur in the fabric (for example, if a link goes down), traffic is rerouted around the failure, and some frames could be delivered out of order.

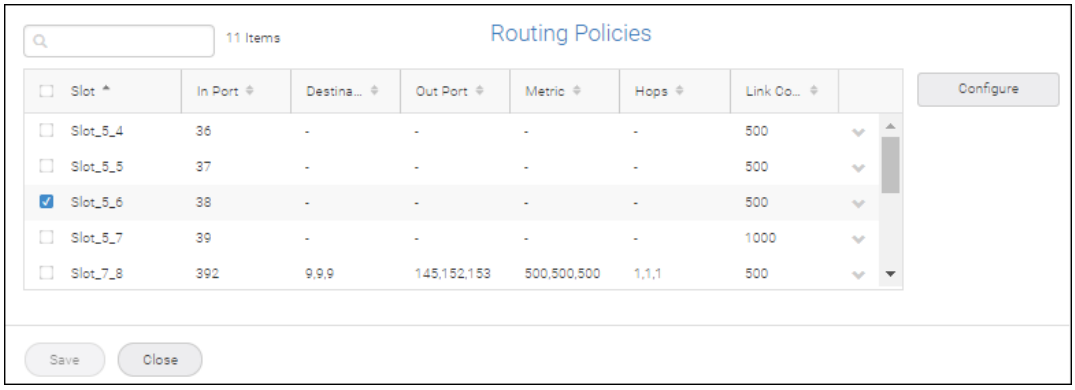
   NOTE
   Enabling in order delivery can delay the establishment of a new path when a topology change occurs, and therefore it should be used with care.

6. To rebalance the E_Port load on a particular logical switch or on all logical switches, without waiting for a topology change to occur, you can select **Rebalance** or **Rebalance All** from the **Actions** menu on the top far right of the **Routing Policies** page. Rebalancing is also necessary when you remove an F_Port or the last E_Port from a neighbor domain.

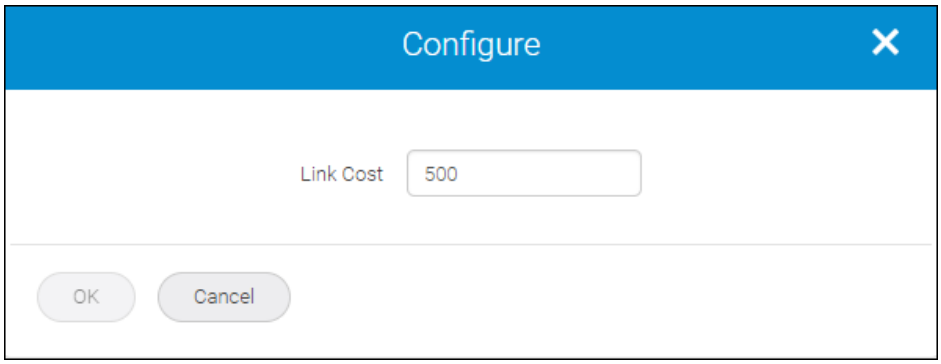


7. At the bottom of the **Routing Policies** page, you see a table of routing policies. From this list, you can configure the cost of an inter-switch link (ISL).

   The cost of a link is a dimensionless positive number. The Fabric Shortest Path First (FSPF) protocol compares the cost of various paths between the source and destination switch by adding the costs of all ISLs along each path. It then defines the path with the least cost. If multiple paths exist with the same minimum cost, FSPF employs load-sharing over these paths.



8. To configure the cost of an ISL, select a box at the far left, and then click the **Configure** button on the upper right.



9. Provide a link cost value.
10. Click **OK** to save the value to the switch.

Using Access Gateway Mode

Access Gateway is a software feature that allows multiple host bus adapters (HBAs) to access the fabric using fewer physical ports. You can set a switch to Access Gateway mode to transform it into a device management tool that is compatible with different types of fabrics, including Brocade Enterprise OS (EOS) and Cisco-based fabrics.

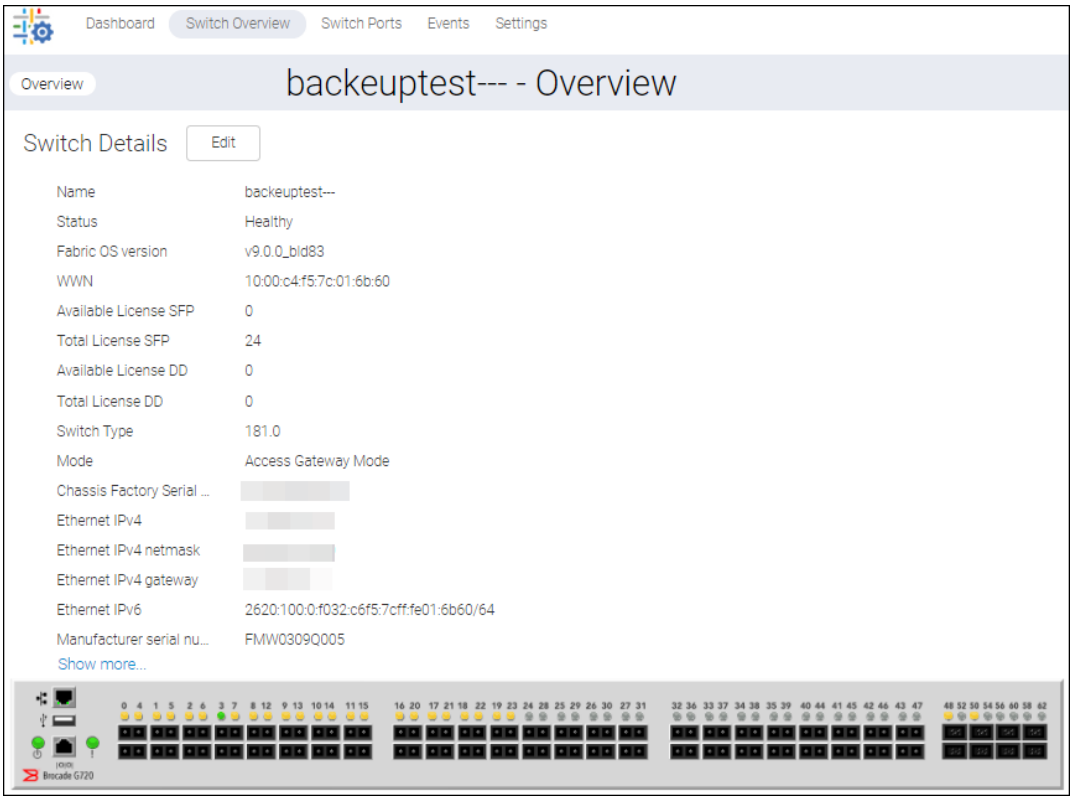
When a switch is in Access Gateway mode, it is logically transparent to the host and the fabric. Brocade Access Gateway mode allows hosts to access the fabric without increasing the number of switches, and it simplifies configuration and management in a large fabric by reducing the number of domain IDs and ports.

For detailed descriptions of the Access Gateway, refer to the *Brocade Fabric OS Access Gateway User Guide*.

NOTE
When Access Gateway mode is enabled on switches that are managed through Web Tools, only a limited subset of menus and options related to device management are available. A switch in Access Gateway mode is considered a device management tool and not a fabric switch; therefore fabric-related options are disabled, fabric management menus are unavailable, and fabric-related service requests are forwarded to the fabric switches.

Viewing the Switch Explorer for Access Gateway Mode

The Switch Explorer for Access Gateway mode is displayed as shown in the following figure.



The **Switch Overview** tab allows you to perform the following tasks:

- Display detailed switch, network, and fabric information.
- Edit the switch name, IP network parameters, and switch settings, such as Access Gateway mode and FCR.
- Perform switch actions, such as reboot, fast boot, and switch disable/enable.

Enabling or Disabling Access Gateway Mode

The Access Gateway feature on a FOS switch enables interoperability with Cisco fabrics. The Access Gateway mode of the switch presents standard F_Ports to the hosts, but it connects to the enterprise fabric as an N_Port (rather than as an E_Port in the case of a regular switch). Before enabling AG mode, you must perform the following actions:

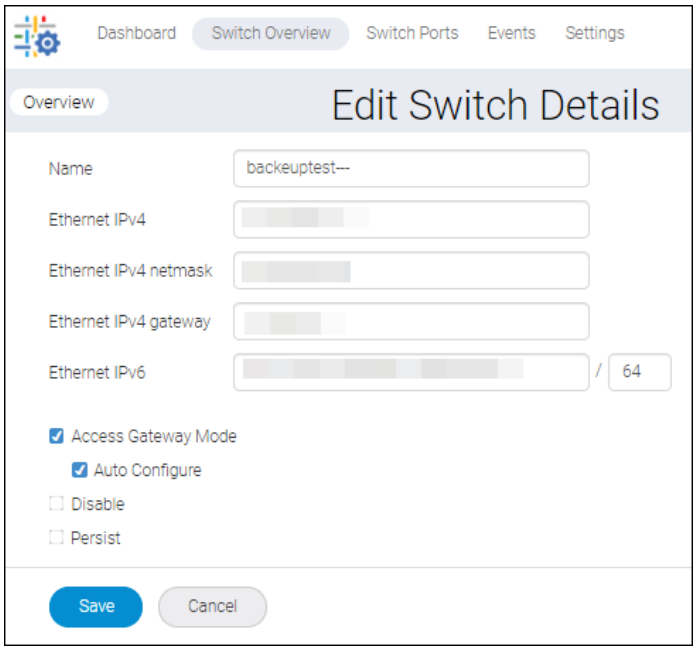
- Disable VF, and remove all logical switches present in the fabric.
- Back up the switch configuration using the **Actions > Backup Configuration** menu on the **Switch Overview** window before enabling AG mode. This avoids the deletion of fabric information such as the zone and security database.
- Disable the management server using the `MsplmgmtDeactivate` command. You cannot enable AG mode if the management server is enabled.

NOTE

- AG mode is not supported on the chassis platform.
- If any error is encountered while enabling AG mode, the switch is disabled and remains in the disabled state until you manually enable it. Access Gateway mode is unavailable when VF is enabled.

To enable Access Gateway mode, perform the following steps:

1. Select **Switch Overview** from the navigation bar.
2. Click the **Edit** option next to the **Switch Details** heading. The **Edit Switch Details** window appears.
3. Select the **Access Gateway Mode** option to enable AG mode. When you select the **Auto Configure** option, it automatically configures the port type assignments, and mappings are configured automatically based on device and switch connections and internal load balancing and grouping.



Clear the **Access Gateway Mode** checkbox to disable AG mode.

NOTE
Access Gateway mode enables the switch as an Access Gateway switch, which presents standard F_Ports to the hosts, but connects to the enterprise fabric as an N_Port (rather than as an E_Port in the case of a regular switch).

4. Click **Save** to save the details.

Port Configuration and Mappings

NOTE
The port mapping configuration is applicable only in Access Gateway mode. You can manage N_Port groups, F-N, and WWN-N mapping configurations.

You can configure a port types (N_Port, F_Port) on each individual port on an Access Gateway enabled switch. You can set the default for port types, groups, and F_Port-to-N_Port mappings. When the policy is Automatic, the port type assignments and mappings are configured automatically based on device and switch connections and internal load-balancing and grouping; user controls are disabled.

When you configure ports, perform the following steps:

1. Configure N_Ports, if necessary.
2. Configure N_Port groups.
3. Configure F_Port-to-N_Port mappings. You can set up primary and secondary mappings. The secondary mapping is the N_Port to which an F_Port is mapped when the primary N_Port mapping goes offline.
4. Configure WWN-N_Port mappings.

Configuring a Port

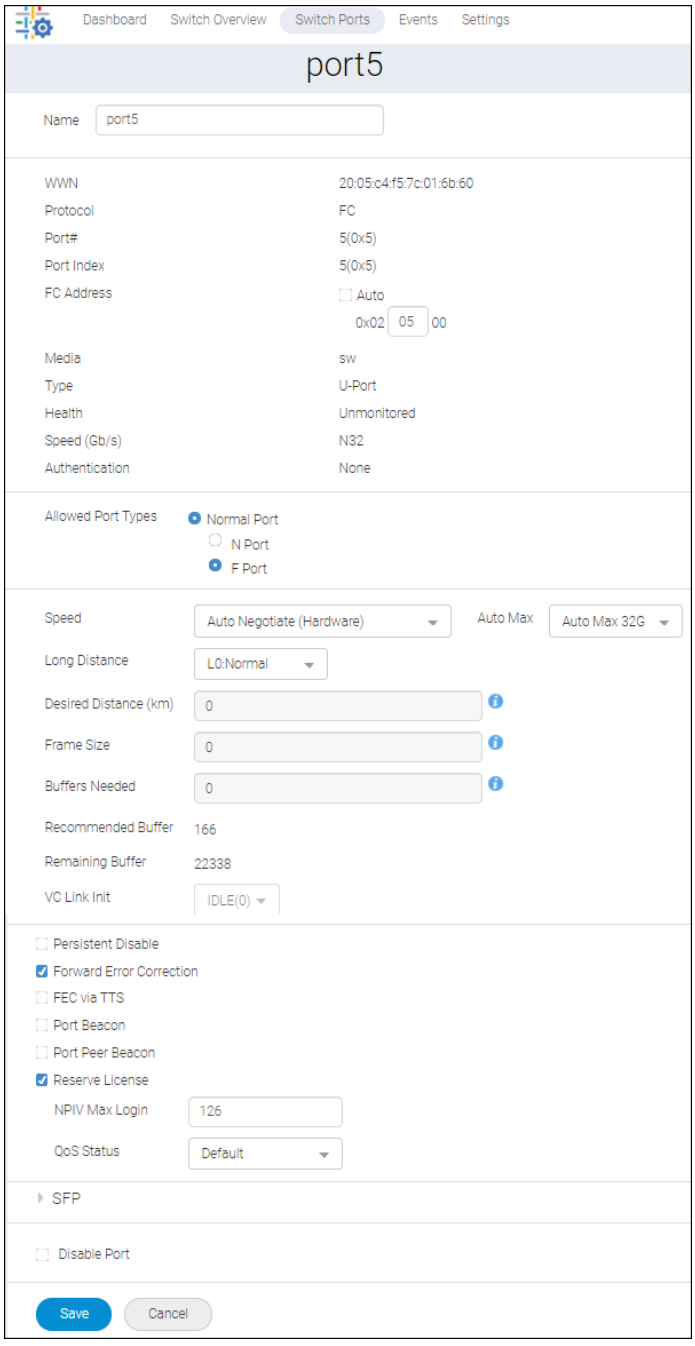
You can edit the port to configure port types and the port speed for physical ports.

NOTE

- Long distance is not displayed from the **Edit** window.
- The Auto Max speed levels are displayed only when you set the port speed to Auto Negotiate; these options allow you to set the speed limit that the port can auto-negotiate.

1. Click **Switch Ports** from the navigation bar. The **Switch Ports** window is displayed.
2. Select the **FC Ports** type.
3. Click any port from the list of ports to display the port details window.
   The window displays the slot number and port number as the title of the window.

4. Select the **Allowed Port Types** and port **Speed**.



5. Click **Save** to save the changes.

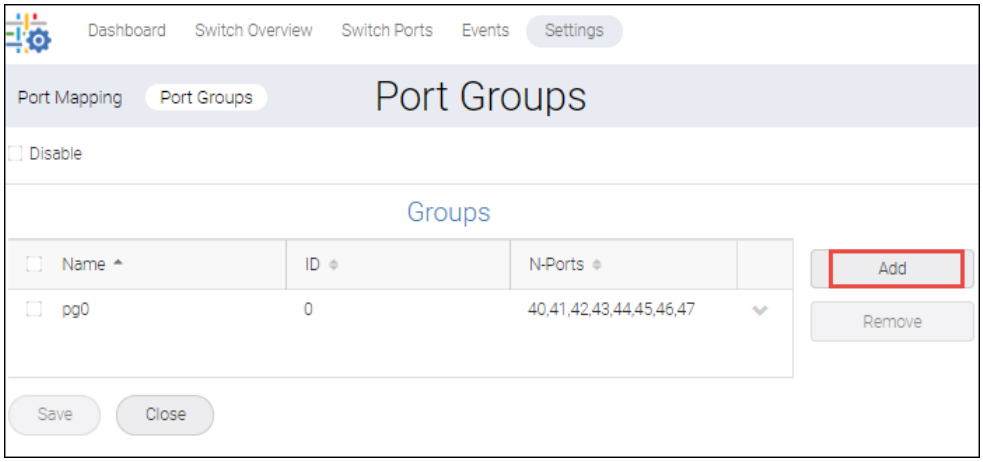
Creating Port Groups

You can group a number of N_Ports (and their mapped F_Ports) together to connect to multiple independent fabrics or to create performance-optimized ports. To group a number of ports, you must create a new port group and must assign desired N_Ports to it. The N_Port grouping option is enabled by default, and all N_Ports are members of the default port group 0 (pg0). Access Gateway prevents failover of F_Ports across N_Port groups.

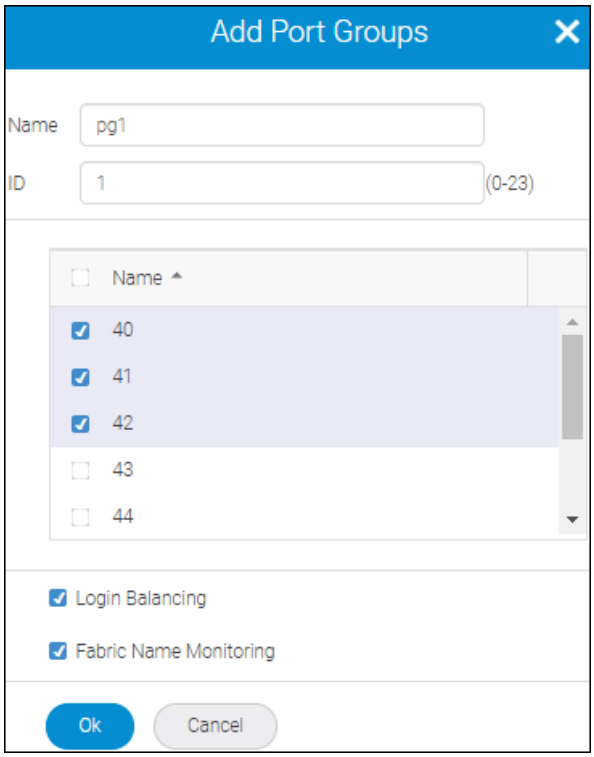
NOTE
If you want to distribute F_Ports among groups, you can leave all ports in the default port group 0, or you can disable the N_Port grouping by selecting the **Disable** option.

To create port groups, perform the following steps:

1. Click **Settings** from the navigation bar, and then select **Access Gateway** from the **Configuration** tab.
2. Select the **Port Groups** tab. The **Port Groups** window is displayed. It displays the default port group policy (pg0).
3. Click **Add** from the **Groups** table. The **Add Port Groups** window is displayed.



4. Enter a name and an ID, and select the ports to configure.
5. Select the **Login Balancing** checkbox to enable the login balance for the port group.
6. Select the **Fabric Name Monitoring** checkbox to manually configure the managed fabric name to be monitored.

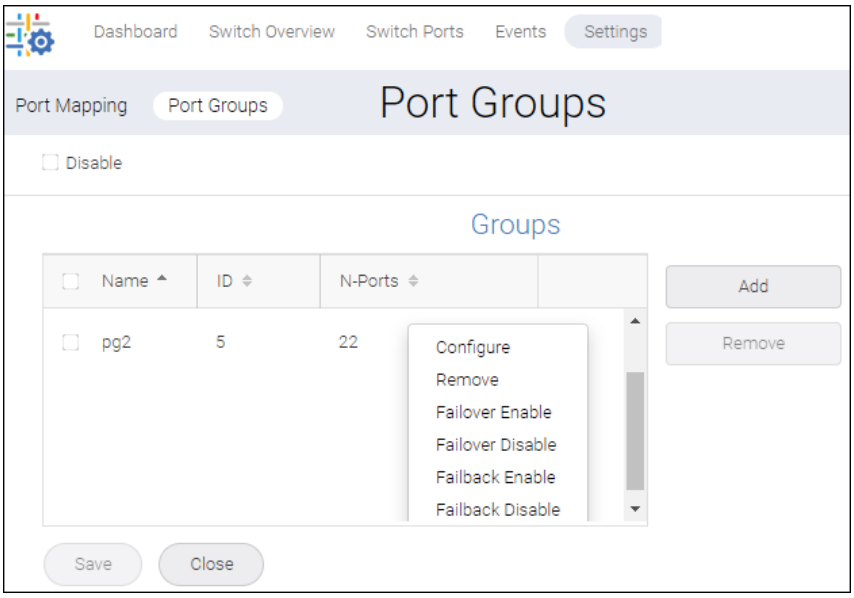


7. Click **OK**.

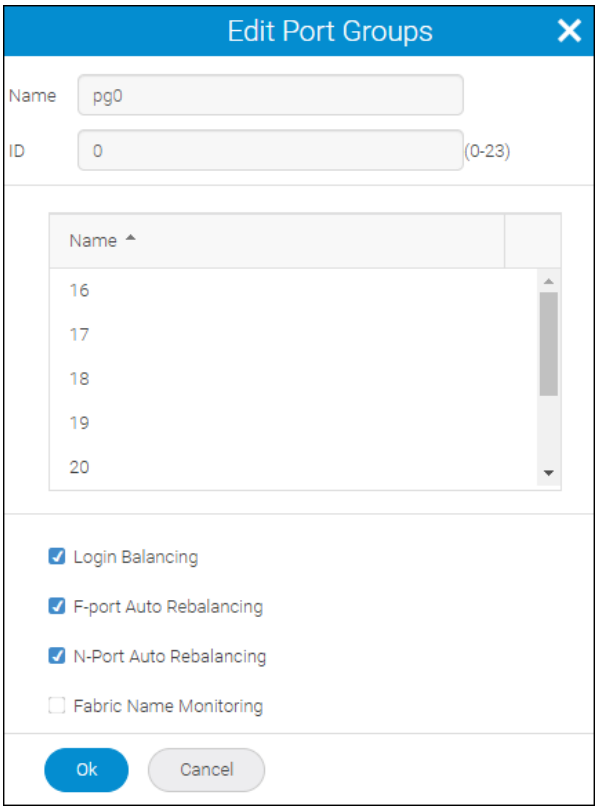
Editing Port Groups

You can edit the default port group as well as custom port groups. To edit port groups, perform the following steps:

1. Click **Settings** from the navigation bar, and then select **Access Gateway** from the **Configuration** tab.
2. Select the **Port Groups** tab. The **Port Groups** window is displayed.
   a. Click the (⌄) icon next to a port group, and perform the following steps:



- For a default group, you can configure only **Login Balancing** and **Fabric Name Monitoring** options.
- The **F-Port Auto Rebalancing** and **N-Port Auto Rebalancing** options are available only in edit port groups. Upon selecting the **Login Balancing** checkbox, the **F-Port Auto Rebalancing** and **N-Port Auto Rebalancing** options are available.
  - You cannot modify the ID for any port groups (default and customized).

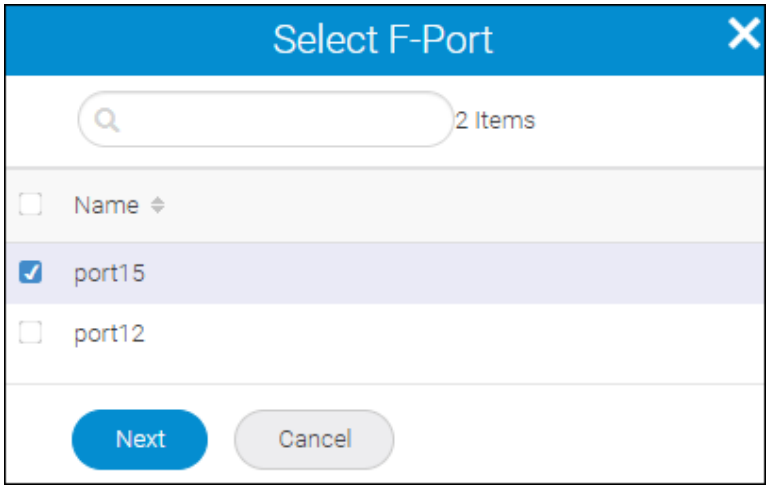


You cannot remove a default port group. The **Remove** option is disabled for the default port group.

Defining Custom Primary and Secondary F-N Port Mappings

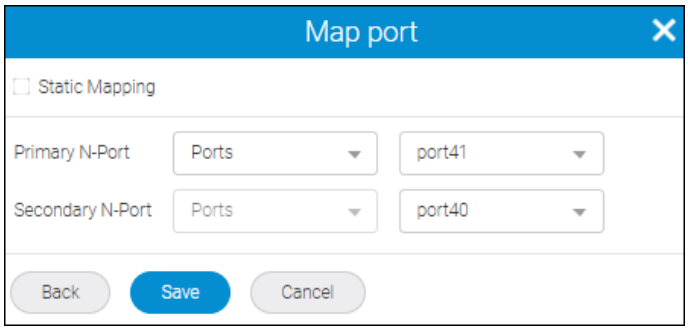
To manually change primary and secondary F-N port mappings, perform the following steps:

1. Click **Settings** in the navigation bar, and then select **Access Gateway** from the **Configuration** tab.
2. Click the (⌄) icon from the right corner of the window, and then select **F-Ports** from the available options.
3. Click the (**+**) icon on the top-right corner of the window. The **Select F-Port** window is displayed.
4. Select the F_Port, and then click **Next**.



The **Map port** window is displayed.

5. Assign a primary and secondary N_Ports, and then click **Save**. The secondary port assignment is optional.



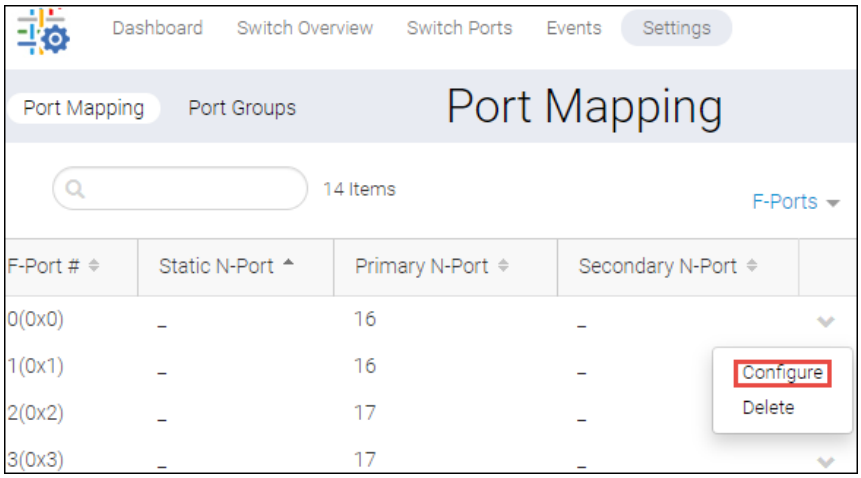
- You can assign a primary N_Port to the available ports or groups based on the requirements.
- The secondary mappings must be a different port in the same group than the primary mapping. If a secondary port is not defined, the failover moves to any online ports within the same port group.

NOTE
From Fabric OS v9.2.0, you can select the secondary N-Port value as None from the dropdown.

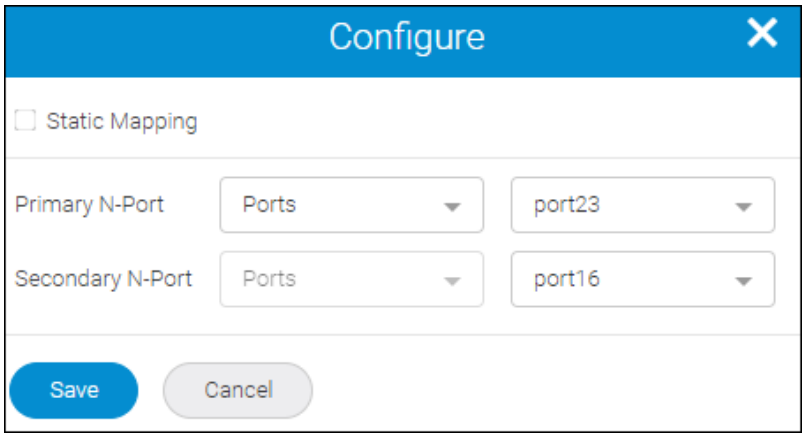
Configuring and Removing Custom Primary and Secondary F-N Port Mappings

To configure a port mapping configuration, perform the following steps:

1. Click **Settings** in the navigation bar, and then select **Access Gateway** from the **Configuration** tab.
2. Click the (⌄) icon next to an F-N port mapping, and then select **Configure**. The **Configure** window is displayed.



3. Edit the existing mapping based on the requirements, and then click **Save**.



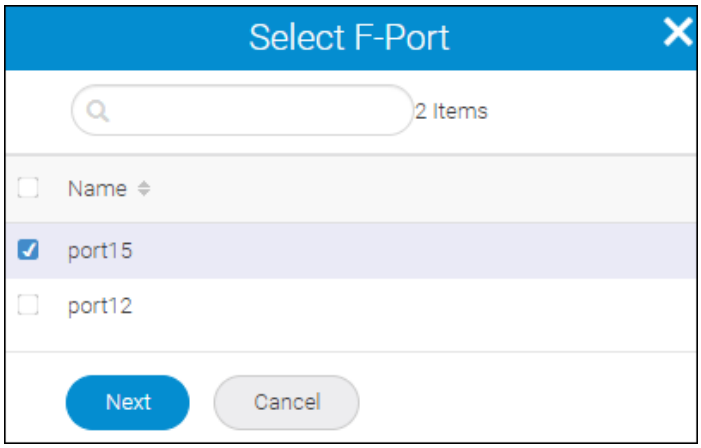
To delete an F-N mapping, click the (⌄) icon next to an F-N port mapping, and then select **Delete**.

Defining Custom Static F-N Port Mappings

NOTE
Static mappings and custom WWN-N port mappings are mutually exclusive.

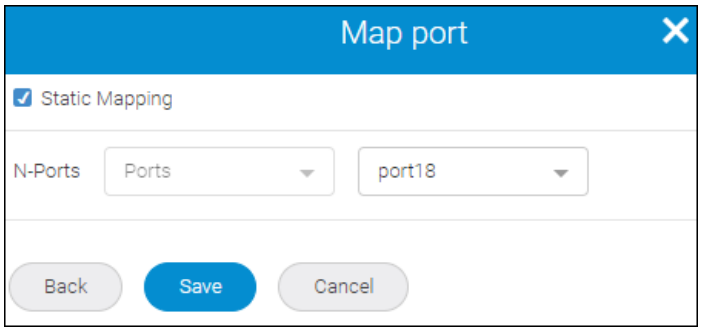
To manually change static F-N port mappings, perform the following steps:

1. Click **Settings** in the navigation bar, and then select **Access Gateway** from the **Configuration** tab.
2. Click the (⌄) icon from the right corner of the window, and then select **F-Ports** from the available options.
3. Click the (**+**) icon on the top-right corner of the window. The **Select F-Port** window is displayed.
4. Select the F_Port, and then click **Next**.



The **Map port** window is displayed.

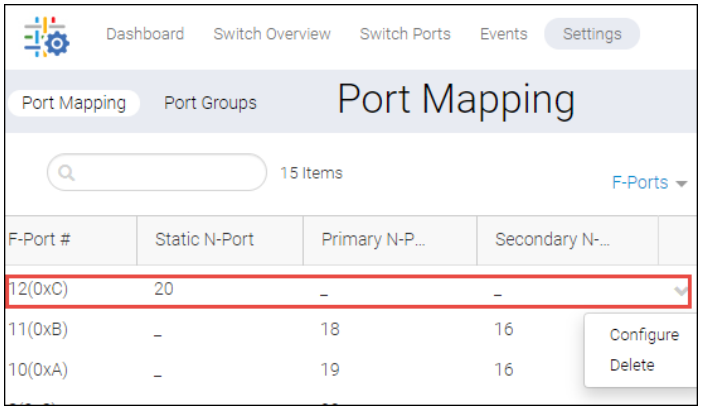
5. Assign the N_Port, and then click **Save**.



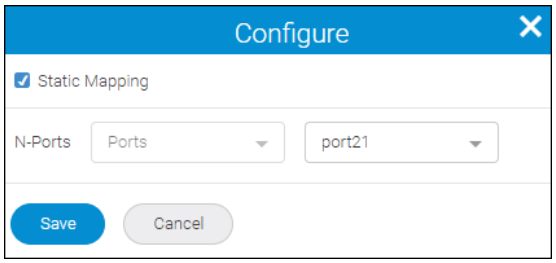
Configuring and Removing Custom Static F-N Port Mappings

To configure a port mapping configuration, perform the following steps:

1. Click **Settings** in the navigation bar, and then select **Access Gateway** from the **Configuration** tab.
2. Click the ( ) icon next to a static F-N port mapping, and then select **Configure**. The **Configure** window is displayed.



3. Edit the existing mapping based on the requirements, and then click **Save**.



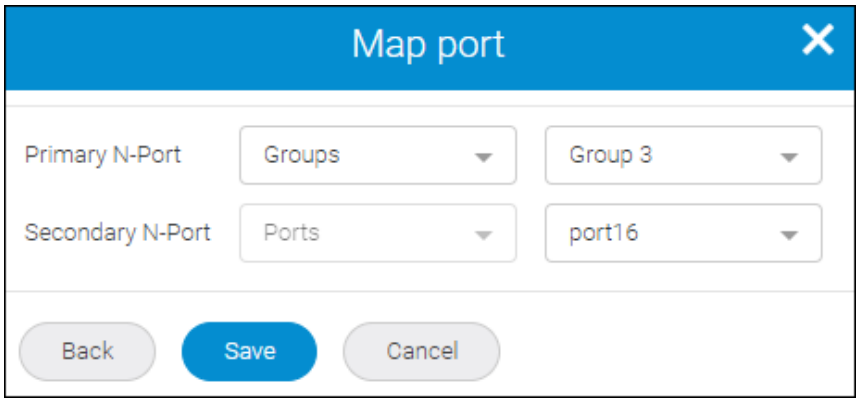
To delete a static F-N mapping, click the (⌄) icon next to the mapping, and then select **Delete**.

Defining Custom Primary and Secondary WWN-N Port Mappings

NOTE
Static mappings and custom WWN-N port mappings are mutually exclusive.

To manually change WWN-N port mappings, perform the following steps:

1. Click **Settings** in the navigation bar, and then select **Access Gateway** from the **Configuration** tab.
2. Click the (⌄) icon from the right corner of the window, and then select **WWN** from the available options.
3. Click the (**+**) icon on the top-right corner of the window. The **Select WWN** window is displayed.
4. Select the WWN or type and add it manually, and then click **Next**. The **Map port** window is displayed.

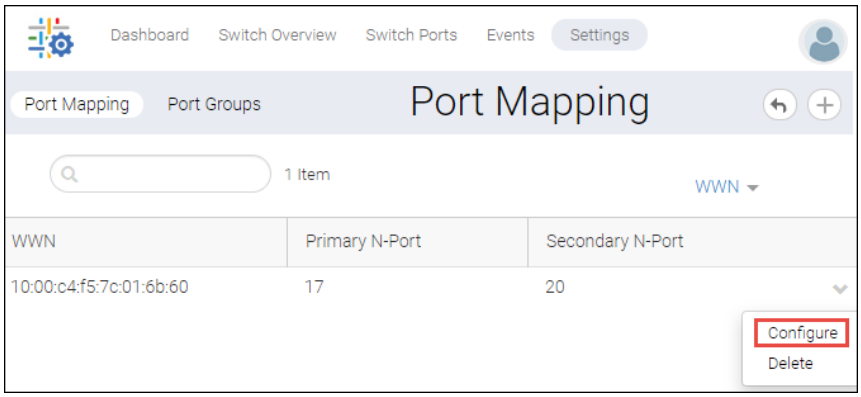


5. Assign primary and secondary N_Port, and then click **Save**.
   - You can assign primary N_Port to the available ports or groups based on the requirements.
   - The WWN fails over to the secondary mapping if the primary mapped port is offline. If a secondary port is not defined, the failover moves to any online ports. The unused WWNs are discarded.

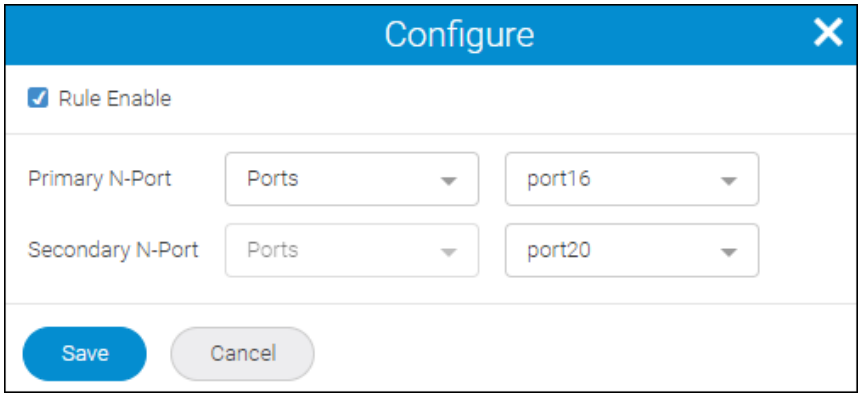
Configuring and Removing Custom Primary and Secondary WWN-N Port Mappings

To configure a port mapping configuration, perform the following steps:

1. Click **Settings** in the navigation bar, and then select **Access Gateway** from the **Configuration** tab.
2. Click the (⌄) icon next to a WWN-N port mapping, and then select **Configure**. The **Configure** window is displayed.



3. Edit the existing mapping based on the requirements The **Rule Enable** option is enabled by default when you perform a WWN-N port mapping.



To delete a WWN-N mapping, click the ( ) icon next to a WWN-N port mapping, and then select **Delete**.

4. Click **Save**.

Advanced Device Security Policy

Advanced Device Security (ADS) is a security policy that restricts access to the fabric at the AG level to a set of authorized devices. Unauthorized access is rejected, and the system logs a RASLOG message.

You can configure the list of allowed devices for each F_Port by specifying their Port WWN (PWWN). The ADS policy secures virtual and physical connections to the SAN.

NOTE
The ADS policy works only when Access Gateway (AG) is enabled.

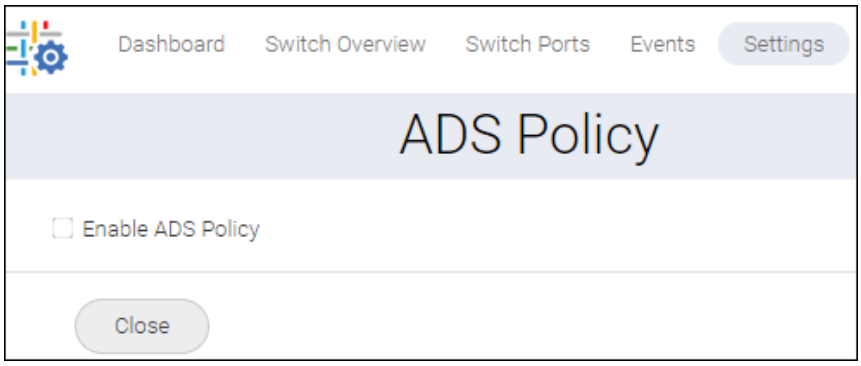
When you enable the ADS policy, it applies to all F_Ports on the AG-enabled device. By default, all devices have access to the fabric on all ports. You can restrict the fabric connectivity to a particular set of devices where the AG device maintains a per-port allow list for the set of devices whose PWWN you define to log in through an F_Port.

Enabling and Disabling the ADS Policy

By default, the ADS policy is disabled. When you manually disable the ADS policy, the allowed lists (global and per-port) are cleared.

To enable the ADS policy, perform the following steps:

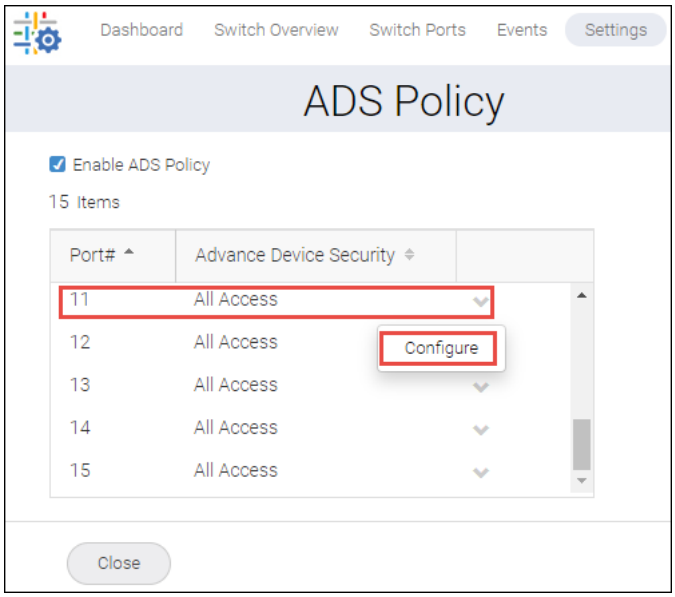
1. Click **Settings** in the navigation bar, and then select **ADS Policy** from the **Security Policies** tab. The **ADS Policy** window is displayed.
2. Select **Enable ADS Policy**, and then select **OK**. Enabling the ADS policy allows all device ports to log in.



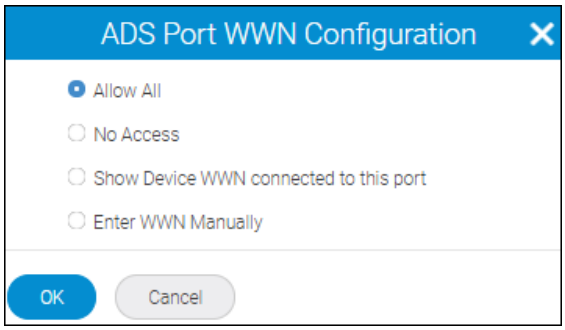
Configuring the ADS Policy

To configure the ADS policy, perform the following steps:

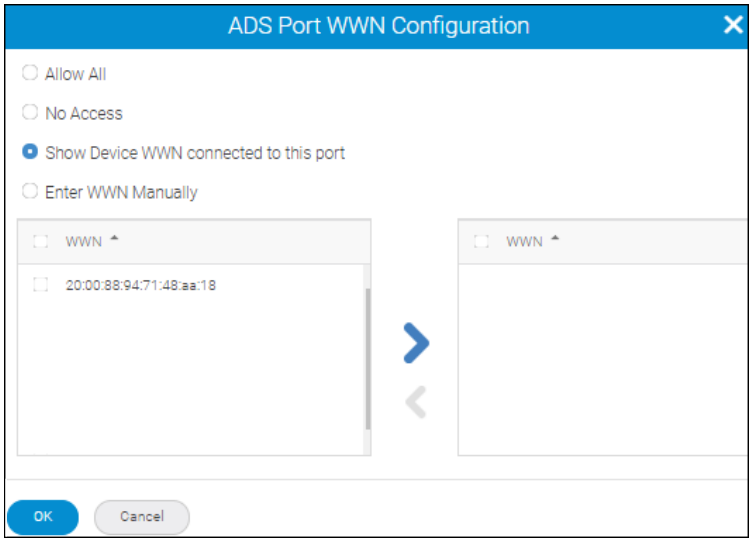
1. Click **Settings** in the navigation bar, and then select **ADS Policy** from the **Security Policies** tab.
   The **ADS Policy** window is displayed.
2. Enable the ADS policy if it is disabled. By default, the ADS policy is disabled.



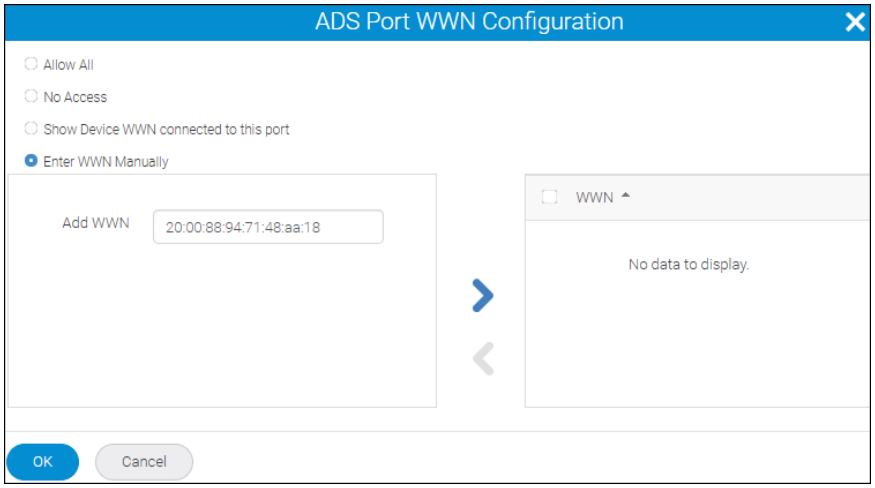
3. Click the (⌄) icon next to the ADS policy, and then select **Configure**. The **ADS Port WWN Configuration** window is displayed.
4. You can configure the ADS policy in four different ways. Select the **Allow All**, **No Access**, **Show Device WWN connected to this port**, or **Enter WWN Manually** option.
   - To allow all devices to log in to the fabric through the F_Port, select the **Allow All** option.



- To allow only the selected WWNs to log in to the fabric through the F_Port, select the **Show Device WWN connected to this port** option. The NPIV-capable device port WWNs can also be added to the allowed list of device port WWNs for the particular F_Port. Select the WWNs and then move them to the WWN list that you want to add.



- To enter the WWN manually, select the **Enter WWN Manually** option. Type the WWN in the **Add WWN** field, and then move it to the WWN list that you want to add.



5. Click **OK**.

Administering FICON CUP Fabrics

This section describes FICON fabrics and the FICON Management Server (FMS).

FICON fabrics require a FICON Logical Switch (LS). FICON channels and control units cannot be attached to a port that is not in a FICON LS. The default switch cannot be used as a FICON LS, so Virtual Fabrics must be enabled and used. To configure a FICON LS, refer to the *Brocade Fabric OS FICON User Guide*.

The Control Unit Port (CUP) provides an in-band management interface from IBM that defines the channel command words (CCWs) that the FICON host can use for managing the switch. A Brocade switch or director that supports CUP can be controlled by one or more host-based management programs or director consoles, such as Brocade Web Tools or Brocade SANnav Management Portal. (Refer to the *Brocade SANnav Management Portal User Guide* for more information about the Brocade SANnav Management Portal.) The director allows control to be shared between host-based management programs and director consoles.

NOTE
While enabling FICON Management Server (FMS) mode with online devices connected to ports with addresses of 0xFE or 0xFF, the following error message appears: `FMS mode enable failed due to port(s) with areas 0xFE or 0xFF is (are) connected to device(s).` You must disable the ports or remove the online devices from those ports that are mapped to the 0xFE or 0xFF address.

To use FICON CUP, you must do the following:

- Configure a FICON LS (refer to the *Brocade Fabric OS FICON User Guide)*.
- Install a FICON CUP license on a FICON director (see Adding a License).
- Enable FMS mode on the FICON director (see Enabling or Disabling FICON Management Server Mode).

  NOTE
  You must enable FMS mode before you can access the **FICON Server** tab.
- Install a FICON CUP license on the Brocade switch (see Adding a License).
- Configure CUP attributes (FMS parameters) for the FICON director (see Configuring FMS Mode Parameters).

You can use Web Tools for all of these tasks. You can also use Web Tools to manage FICON directors (when FMS mode is enabled on those directors) to do the following tasks:

- Display the control device Allegiance state (see Viewing the Control Device State).
- Display a code page (see Displaying EBCDIC Code Page Information).
- Manage the port connectivity configuration (see Allow/Prohibit Configuration Matrix).

A FICON CUP license is required to manage port-to-port connectivity through PDCM.

NOTE
If the switch does not have the FICON CUP license installed, Web Tools prevents the enabling of FMS mode and displays the following error message: `Enabling FMS mode requires FICON CUP license installed on the switch. Contact your preferred storage vendor for more details.`

NOTE
Fabric OS v9.0.0 is the last release to support the Prohibit Dynamic Connectivity Mask (PDCM) used for connectivity management as reflected in the Allow/Prohibit Configuration Matrix option in WebTools. The Allow/Prohibit matrix management feature is deprecated in Fabric OS v9.0.0. The Fabric OS zoning feature must be used for connectivity management functions.

NOTE
From Fabric OS v9.2.0, if the FMS is enabled, you can edit the FICON properties in the FICON management page. If FMS is disabled, you can still access the FICON management page but with the limited properties

Enabling or Disabling FICON Management Server Mode

FICON Management Server (FMS) supports switch management using CUP. To use the CUP functionality, all switches in the fabric must have FICON Management Server mode (FMS mode) enabled. FMS mode is a per-switch setting. After FMS mode is enabled, you can activate a CUP license without restarting the director. You can use Web Tools to install a CUP license. For more information on installing licenses, see Adding a License.

When FMS mode is disabled, mainframe management applications, director consoles, or alternate managers cannot communicate with a director with CUP. In addition, when FMS mode is disabled on a director, you cannot configure CUP attributes.

To enable or disable FICON Management Server mode, perform the following steps:

1. Select **Switch Overview** from the navigation bar.
2. Click **Edit** next to the **Switch Details** heading to display the **Edit Switch Details** dialog.
3. Click the **FMS Mode** checkbox.
   Clear the checkbox to disable FMS mode.

   NOTE
   While enabling FMS mode with online devices connected to FE or FF, the following error is shown: `FMS mode enable failed due to port(s) with areas 0xFE or 0xFF is (are) connected to device(s).`
4. Click **Save** to save your changes.

   NOTE
   High Integrity Fabric (HIF) must be enabled to enable FMS mode.

FMS Parameter Overview

FMS parameters control the behavior of the switch with respect to CUP, as well as the behavior of other management interfaces (director console, alternate managers). You can configure FMS parameters for a switch only after FMS mode is enabled on the switch. All FMS parameter settings are persistent across switch power cycles. There are six FMS parameters, as described in the following table.

Table 1: FMS Mode Parameters

Parameter	Description
Programmed Offline State Control	Controls whether host programming is allowed to set the switch offline. The parameter is set as enabled by the hardware after system installation, and it can be reset by Web Tools.
User Alert Mode	UAM user alert mode. If this mode is enabled, a warning message is issued when an action is attempted that will write CUP parameters on the switch. For example, changing the block/unblock state of a port, the port name, or a PDCM by means of the out of band interfaces. This mode can only be modified in-band by the host. The default setting is 0 (off).

Parameter	Description
Active=Saved Mode	Controls the IPL file update. The IPL file saves port connectivity attributes and port names. After a switch restart or power cycle, the switch reads the IPL file and activates its contents as the default configuration. When this mode is enabled, activating a configuration saves a copy to the IPL configuration file. All changes made to the active connectivity attributes or port names by host programming or alternate managers are saved in this IPL file. It keeps the current active configuration persistent across switch restarts and power cycles. You cannot directly modify the IPL file or save a file as an IPL file. When this mode is disabled, the IPL file is not altered for either new configuration activation or any changes made on the current active configuration. This parameter is set as enabled by the hardware after system installation, and it can be reset by Web Tools. **Note:** When FMS mode is enabled and the Active=Saved Mode parameter is disabled, you can enable and disable ports, but the setting is *not* persistent. When the Active=Saved Mode parameter is enabled, you can enable and disable ports and the setting *is* persistent.
Director Clock Alert Mode	Controls behavior for attempts to set the switch timestamp clock through the director console. When this parameter is enabled, the director console (Web Tools, in this case) displays warning indications when the switch timestamp is changed by a user application. When it is disabled, you can activate a function to automatically set the timestamp clock. There is no indication for timestamp clock setting. This parameter is set as disabled by the hardware after system installation, and it can be reset by Web Tools.
Alternate Control Prohibited	Determines whether alternate managers are allowed to modify port connectivity. Enabling this mode prohibits alternate manager control of port connectivity; otherwise, alternate managers can manage port connectivity. This parameter is set as enabled by the hardware after system installation, and it can be reset by Web Tools.
Host Control Prohibited	Determines whether host programming allows modifying port connectivity. Enabling this mode prohibits host programming control of port connectivity; otherwise, host programming can manage port connectivity. This parameter is set as disabled by the hardware after system installation. and it can be reset by Web Tools.

Configuring FMS Mode Parameters

To configure FMS mode parameters, perform the following steps:

1. Select **Settings > Configuration > FICON Management**.
2. Click the **FICON Server** tab.

   All attributes on this page are read-only until FMS mode is enabled (see Enabling or Disabling FICON Management Server Mode).
3. Click the **Enable FMS Mode** checkbox.
4. To enable or disable an FMS mode parameter, click the checkbox next to the parameter.

   A checked checkbox indicates that the parameter is enabled. You cannot configure the **User Alert Mode** parameter in Web Tools because it is read-only.

Displaying EBCDIC Code Page Information

Extended Binary Coded Decimal Interchange Code (EBCDIC) is an 8-bit character encoding (code page) used on IBM mainframe operating systems such as z/OS and S/390. Code page 37 is an EBCDIC code page with a full Latin-1 character set.

The EBCDIC code page format identifies the language used to exchange information between the FICON director and host programming. It is a read-only field in Web Tools. When FMS mode is disabled, the code page is displayed as unavailable. Web Tools supports code page 37 only.

To display code page information, perform the following steps:

1. Select **Settings > Configuration > FICON Management**.
2. Click the **FICON Server** tab.

   All attributes on this page are read-only until FMS mode is enabled.

   The code page format displays in the **Language Used** field, as shown in the following example:

   ```
   Language Used (EBCDIC) USA/Canada--00037
   ```

Viewing the Control Device State

The control device is in either a neutral state or a switched state. When it is neutral, the control device accepts commands from any channel that has established a logical path with it and accepts commands from alternate managers. When the control device is switched, it establishes a logical path and accepts commands only from that logical path ("device allegiance"). When the CUP is in allegiance with a host logical path and is processing commands, it causes a FICON CUP busy condition. Most "write" operations from alternate managers are also rejected.

Device allegiance usually lasts for a very short time. However, under abnormal conditions, device allegiance can get "stuck" and fail to terminate. It might cause the switch to be unmanageable with CUP, and you will continue to receive the FICON CUP busy error. In this case, you should check the control device state and the last update time to identify if the device allegiance is stuck.

The **FICON Server** tab displays the control device state. Refresh the browser to get the most recent update.

Web Tools may return a CUP Busy indication when the switch is busy handling configuration updates caused by other management interfaces or the host.

To view the control device state, complete the following steps:

1. Select **Settings > Configuration > FICON Management**.
2. Click the **FICON Server** tab.

   NOTE
   You must enable FMS mode before you can access the **FICON Server** tab (see Enabling or Disabling FICON Management Server Mode).

   The control device state is displayed as neutral or switched in the **Control Device Allegiance** field.

Allow/Prohibit Configuration Matrix

NOTE
Fabric OS 9.0.0 is the last release to support the Prohibit Dynamic Connectivity Mask (PDCM) used for connectivity management as reflected in the Allow/Prohibit Configuration Matrix option in WebTools. Effectively, the Allow/Prohibit matrix management feature is deprecated in Fabric OS 9.0.0. The Fabric OS zoning feature must be used for connectivity management functions.

In the **Configurations** tab, you can manage the configuration files and the active configuration. All configuration files and the active configuration are listed in a table. The active configuration is displayed as "Active Configuration*" and the description in the table is "Current active configuration on switch." The other special configuration file is the IPL. Any other files displayed are user-defined configurations and are stored on the switch.

You can create, activate, copy, or delete saved allow/prohibit configuration matrices. You can also activate, edit, or copy the IPL configuration. You must have FMS mode enabled before you can make any changes to the configurations. Click **F5** or the **Reload this page** icon to get the latest configuration file list from the switch.

When creating a new configuration or editing an existing configuration, the port names are restricted to the printable ASCII character set. Characters beyond printable ASCII characters are displayed as periods.

When initially installed, a switch allows any port to dynamically communicate with any other port. Two connectivity attributes are defined to restrict this any-to-any capability for external ports: Block and Prohibit.

Block is a port connectivity attribute that prevents all communication through a port. Prohibit is a port connectivity attribute that prohibits or allows dynamic communication between ports when a port is not blocked. Each port has a vector specifying its Prohibit attribute with respect to each of the other ports in the switch. This attribute is always set symmetrically in that a pair of ports is either prohibited or allowed to communicate dynamically.

The **Configuration Matrix** (shown in the Configuration Tab Figure) displays the port number (in physical-location format), port name (port address name), and port area ID (port address displayed in hexadecimal) in fixed columns. The right side is a port matrix that lists all ports by area ID and identifies blocked ports (greyed-out) and prohibited port address pairs ( ).

Viewing Allow/Prohibit Configuration Matrices

To display a list of allow/prohibit configuration matrices, perform the following steps:

1. Select **Settings > Configuration > FICON Management**.
2. Click the **Configurations** tab.
   A list of saved configurations is displayed.
3. Click the name of the configuration that you want to view in the table.
   The selected configuration is displayed.

Modifying Allow/Prohibit Configuration Matrices

The allow/prohibit configuration matrix is a FICON port attribute that can be used to prohibit communication between specific ports. Allow/prohibit configuration matrices are not recommended on E_Ports (inter-switch links).

Multiple configurations can be defined, edited, copied, or removed. However, only one configuration can be active per switch.

To create a new allow/prohibit configuration matrix or to edit an existing configuration, perform the following steps:

1. Select **Settings > Configuration > FICON Management**.
2. Click the **Configurations** tab.
   Two default configurations (Active and IPL) are displayed. Any existing user-defined configurations also are displayed.
3. Choose one of the following options:
   - To create a new configuration, click the **Add** icon ( ) in the upper-right side of the **Configurations** tab.
     The **Create New Configurations** window is displayed. Continue with Step 4.
   - To edit an existing configuration, click the name of the configuration you want to edit in the table.
     The selected configuration is displayed. Go to Step 5.

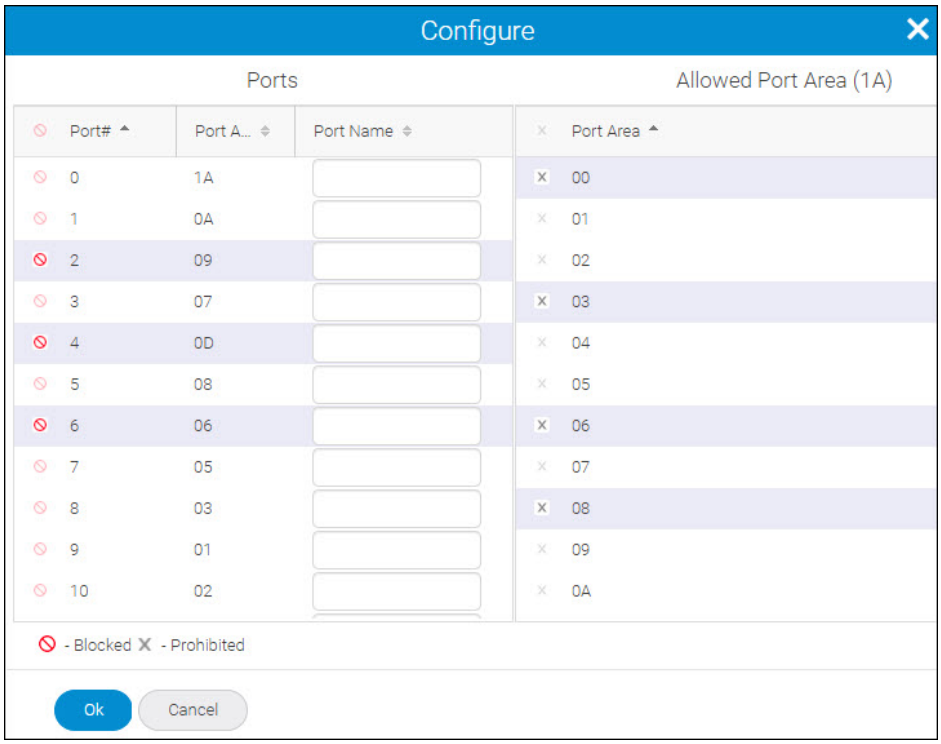
4. Enter a name and description for the new configuration.

   The file name must be in uppercase characters and numbers and can contain only dashes or underscores as special characters.

5. Click **Configure**.

   The **Configure** dialog is displayed.

   Figure 12: Configure Dialog



6. To block a port, select the **Blocked** icon (⊘) next to the port number in the **Ports** table.

   Repeat this step for each port that you want to block. To block all ports, select the **Ports# Blocked** icon (⊘) in the table header.

   When you block a port, data and control traffic are not allowed on that port.

7. To prohibit a connection between two ports, perform the following steps:

   a) Select a port number or port area in the **Ports** table to display a list of port areas in the **Allowed Port Area** list.

      Do not select the **Blocked** icon (⊘) for the row.

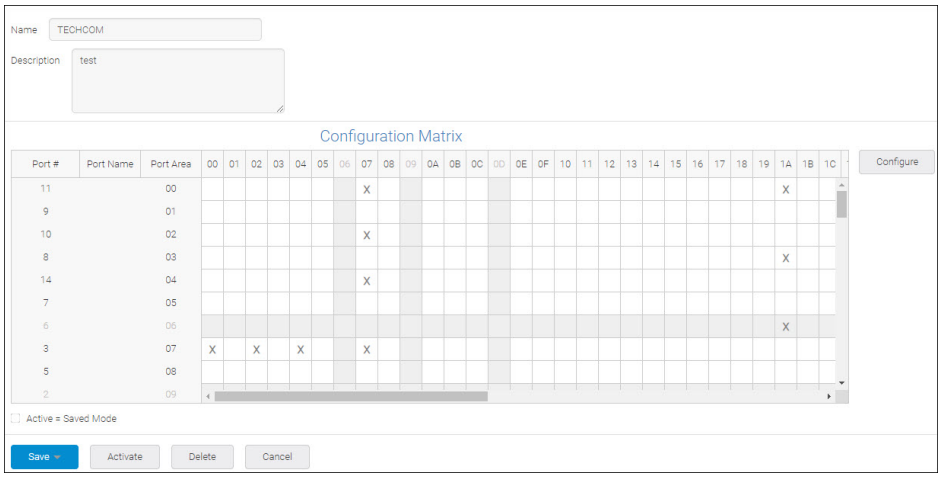
   b) Select the Prohibited icon (X) corresponding to a port that you want to prohibit in the **Allowed Port Area** list.

      This prohibits the selected port from all the other ports. Repeat this step for each port that you want to prohibit. To prohibit all ports, select the **Port Area** Prohibited icon (X) in the header.

8. Click **Ok** to save the allow/prohibit configuration matrix.

   The **Configuration** tab is displayed.

Figure 13: Configuration Tab



The **Configuration Matrix** displays in the **Configuration** tab. The switch port numbers are displayed on the horizontal axis, and the port areas are displayed on both the vertical axis and the horizontal axis.

Clear cells indicate that communication is allowed between the ports.

A Prohibited icon (X) displays at the intersection point to identify prohibited ports.

Greyed-out cells display to identify blocked ports.

9. After you have finished making changes, perform one of the following:
   - Click **Activate** to save the changes and make the configuration active immediately, as described in Activating an Allow/Prohibit Configuration Matrix.
   - Click **Save** to save the changes but not make the configuration active.
   - Click **Save As** to save the configuration to a new configuration file, as described in Copying an Allow/Prohibit Configuration Matrix.
   - Click **Cancel** to cancel all changes without saving.

Activating an Allow/Prohibit Configuration Matrix

When you activate a saved allow/prohibit configuration matrix on the switch, the preceding configuration (currently activated) is overwritten.

To activate an allow/prohibit configuration matrix, perform the following steps:

1. Select **Settings > Configuration > FICON Management**.
2. Click the **Configurations** tab.
3. Click the name of the saved configuration that you want to activate in the table.
   The selected configuration is displayed.
4. Optional: Click the **Active=Saved Mode** checkbox to enable (selected) or disable (not selected) the **Active=Saved Mode** parameter after the configuration is activated.
5. Click **Activate**.

   The confirmation dialog is displayed. The message reminds you that the current configuration will be overwritten upon activation.

6. Click **Yes** to activate the configuration, or click **No** to cancel the activation.

Copying an Allow/Prohibit Configuration Matrix

To copy an allow/prohibit configuration matrix to a new configuration, perform the following steps:

1. Select **Settings > Configuration > FICON Management**.
2. Click the **Configurations** tab.
3. Click the name of the configuration that you want to copy in the table.
   The selected configuration is displayed.
4. Choose one of the following options:
   - If you selected the Active configuration or IPL configuration, click **Save As**.
   - If you selected a user-defined configuration, click **Save > Save As**.
5. Enter a name and description for the new configuration, and click **Save** to save the configuration to the target file.

   Click **Cancel** to cancel copying the configuration.

   The file name must be in uppercase characters, and numbers and can contain only dashes or underscores as special characters.

Deleting an Allow/Prohibit Configuration Matrix

You can delete only user-defined allow/prohibit configuration matrices. To delete a saved allow/prohibit configuration matrix, perform the following steps:

1. Select **Settings > Configuration > FICON Management**.
2. Click the **Configurations** tab.
3. Click the name of the configuration that you want to delete in the **Configurations** table.
   The selected configuration is displayed.
4. Click **Delete**.

   NOTE
   There is no confirmation message. Web Tools immediately deletes the allow/prohibit configuration matrix.

CUP Logical Path Configuration

The **CUP Logical Paths** table details the operational state along with the reporting path of the FICON configured logical switch. The logical reporting path is a CUP mechanism for sending FRU-failure type reports to a FICON logical path through the FICON protocol.

Viewing CUP Logical Path Configurations

To display a list of CUP logical path configurations, perform the following steps:

1. Select **Settings > Configuration > FICON Management**.
2. Click the **FICON Server** tab.
   All attributes on this page are read-only until FMS mode is enabled. The list of CUP logical path configurations displays in the **CUP Logical Paths** table.

Configuring CUP Logical Paths

To configure a CUP logical path, perform the following steps:

1. Select **Settings > Configuration > FICON Management**.
2. Click the **FICON Server** tab.

   All attributes on this page are read-only until FMS mode is enabled. The list of CUP logical path configurations displays in the **CUP Logical Paths** table.
3. Select a logical path, and select **Set Current** from the action menu.
4. Click **Save**.

Link Incident Registered Recipient Configuration

The Link Incident Registered Recipient (LIRR) receives Link Incident Reports (LIRs) on the source N_Port. The LIRR database is stored on the switch. The **Link Incident Registered Recipient** table displays the payload format, port type, PID, listener port WWN, listener type, switch port WWN, and path status for each LIRR configuration.

Viewing LIRR Configurations

To display a list of Link Incident Registered Recipient (LIRR) configurations, perform the following steps:

1. Select **Settings > Configuration > FICON Management**.
2. Click the **FICON Server** tab.

   All attributes on this page are read-only until FMS mode is enabled. The list of LIRR configurations displays in the **Link Incident Registered Recipients** table.

Configuring LIRRs

To configure the Link Incident Registered Recipients (LIRRs), perform the following steps:

1. Select **Settings > Configuration > FICON Management**.
2. Click the **FICON Server** tab.

   All attributes on this page are read-only until FMS mode is enabled. The list of LIRR configurations displays in the **CUP Logical Paths** table.
3. Select an LIRR configuration, and select **Set Current** from the action menu.
4. Click **Save**.
5. Optional: Reset the selected LIRR using the **Reset** button.

Displaying Request Node Identification Data

Web Tools displays Request Node Identification Data (RNID) information for the local switch and for attached FICON devices and FICON channel paths. RNID information for the switch displays in the **Switch Overview** tab.

To display the RNID data, perform the following steps:

1. Click the **Switch Overview** tab.
2. Click **Show more** at the bottom of the **Switch Details** area.

   The RNID data displays at the bottom of the area.

   Ports that completed an RNID exchange display **FICON** in the **Capability** column. For those ports, the following information specific to RNID is displayed:

- Type
- Model
- Tag
- Sequence Number
- Insistent Domain ID Mode
- Manufacturer
- Manufacturer Plant

Maintenance and Support

This section describes features such as switch configuration backup and restore, trace dump, and Web Tools support data collection.

Switch Configuration Backup and Restore

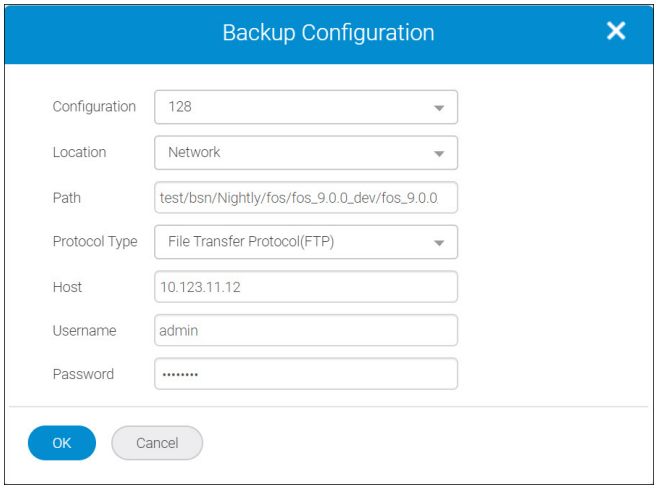
You can back up and restore the configuration file for all switches in the fabric to avoid the loss of configuration files due to a failure. This also helps you to maintain a similar configuration across the switches in a fabric.

Backing Up the Switch Configuration

You must back up the individual configuration files regularly before performing an upgrade or downgrade of the Fabric OS software or making significant changes to the configuration. You must avoid copying configurations from one switch to another.

To create a configuration backup file, perform the following steps:

1. Click **Switch Overview** in the navigation bar.
2. Click the more icon on the top-right corner of the window, and select **Backup Configuration** from the options. The **Backup Configuration** window is displayed.
3. Select the configuration type and the source of the location from the options: **Network** or **USB**. If **Network** is chosen as the location of the configuration file, perform the following steps:
   a. Enter the configuration file with a fully qualified path, or select the configuration file type from the **Configuration** field.
   b. Enter the host name or IP address, user name, and password. You can enter the IP address in either IPv4 or IPv6 format.
   c. Select the protocol type in the **Protocol Type** field from the options: **Secure Copy Protocol (SCP)**, **Secure File Transfer Protocol (SFTP)**, or **File Transfer Protocol (FTP)**.



4. If **USB** is chosen as the location of the configuration file, the network parameters are not needed and are not displayed. Specify the firmware file path in the USB drive.
5. Click **OK**. A warning message appears that the successful initiation and the time to complete the backup.

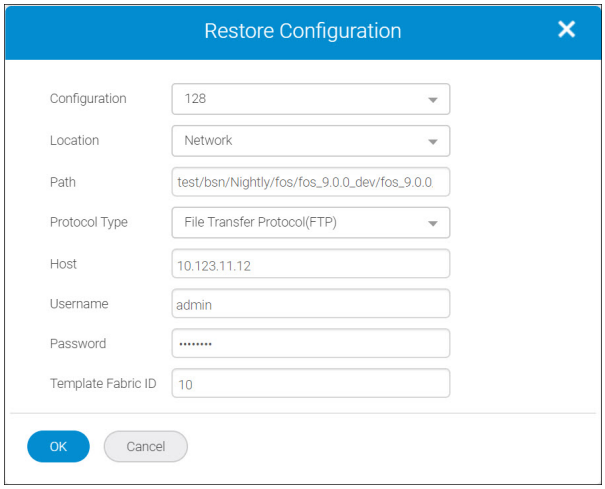
You can monitor the progress by watching the Upload/Download Progress bar.

Restoring the Switch Configuration

Restoring a configuration involves overwriting the configuration on the switch by downloading a previously saved backup configuration file. Perform this procedure during planned downtime. Make sure that the configuration file you are downloading is compatible with your switch model. Configuration files from other model switches might cause your switch to fail.

To restore the switch configuration, perform the following steps:

1. Click **Switch Overview** in the navigation bar.
2. Click the more icon on the top-right corner of the window, and select **Restore Configuration** from the options. The **Restore Configuration** window appears.



3. Select the configuration type and the source of the location from the options: **Network** or **USB**. If **Network** is chosen as the location of the configuration file, perform the following steps:
   a. Enter the configuration file with a fully qualified path, or select the configuration file type from the **Configuration** field.
   b. Enter the host name or IP address, user name, and password. You can enter the IP address in either IPv4 or IPv6 format.
   c. Select the protocol type in the **Protocol Type** field from the options: **Secure Copy Protocol (SCP)**, **Secure File Transfer Protocol (SFTP)**, or **File Transfer Protocol (FTP)**.
4. If you select **USB** as the location of the configuration file source, the network parameters are not needed and are not displayed. Enter the fabric ID of the logical switch in **Template Fabric ID**.
5. Click **OK**. A warning message appears that the successful initiation and the time to restore the backup.

Configuring Trace Dump

A trace dump is a snapshot of the running behavior within a Brocade switch. The dump can be used by developers and troubleshooters at Brocade to help understand what might be contributing to a specific switch behavior when certain internal events are seen. For example, a trace dump can be created each time a certain error message is logged to the system error log. Developers can then examine what led up to the message event by studying the traces.

Tracing is always "on". As software runs on the switch, the trace information is placed into a circular buffer in system RAM. Periodically, the trace buffer is "frozen" and saved. This saved information is called a "trace dump".

A trace dump is generated when the following events occur:

- It is triggered manually (use the `tracedump` command).
- A critical-level log message occurs.
- A particular log message occurs.
- A kernel panic occurs.
- The hardware watchdog timer expires.

For information about the `tracedump` command, refer to the *Brocade Fabric OS Command Reference Manual*.

When a trace dump is generated, it is automatically uploaded to an FTP host if automatic FTP uploading is enabled. Using the **Trace Dump** option, you can view and configure the trace FTP host target and enable or disable automatic trace uploads.

How a Trace Dump Is Used

The generation of a trace dump causes a CRITICAL message to be logged to the system error log. When a trace dump is detected, Fabric OS runs the `supportsave` command on the affected switch. This command packages all error logs, the `supportshow` output, and the trace dump into a single file, and if automatic trace dump transfers are enabled, it moves the file to your FTP server.

In addition to the automatic generation of trace dumps on faults, you can also generate a trace dump manually or when certain system error messages are logged. This is normally done with assistance from Brocade customer support when diagnosing switch behavior.

For details on the `supportsave` command, refer to the *Brocade Fabric OS Command Reference Manual*.

Setting Up Automatic Trace Dump Transfers

You can set up a switch so that diagnostic information is transferred automatically to a remote server. Then, if a problem occurs, you can provide your customer support representative with the most detailed information possible. To ensure the best service, you should set up automatic transfer as part of the standard switch configuration, before a problem occurs.

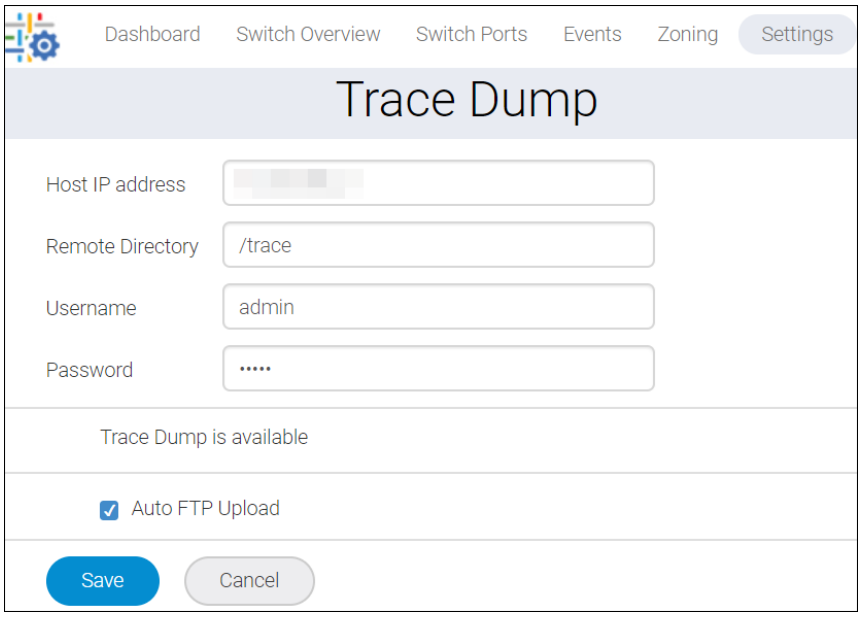
Setting up the automatic transfer of diagnostic files involves the following tasks:

- Specifying a remote server to store the files.
- Enabling the automatic transfer of trace dumps to the server. (Trace dumps overwrite each other by default; sending them to preserve information that may be lost.)

Specifying a Remote Server

To specify a remote server, perform the following steps:

1. Click **Settings** in the navigation bar, and then select **Services** > **Trace Dump**.
   The **Trace Dump** window is displayed.
2. To collect the trace, enter the FTP host IP address, the path of the remote directory for the trace dump files, the FTP user name, and the FTP password in the appropriate fields.



NOTE

- The IP address can be in IPv4 or IPv6 format, or it can be a DNS name.
- The path for Windows is `Folder Name/FileName.txt` or `FileName.txt`.
- The path for Linux is `Directory Name/FileName.txt` or `FileName.txt`.
- The password is optional if you log in as an anonymous user.

3. Click **Save**.
   The trace is collected in the specified remote server.

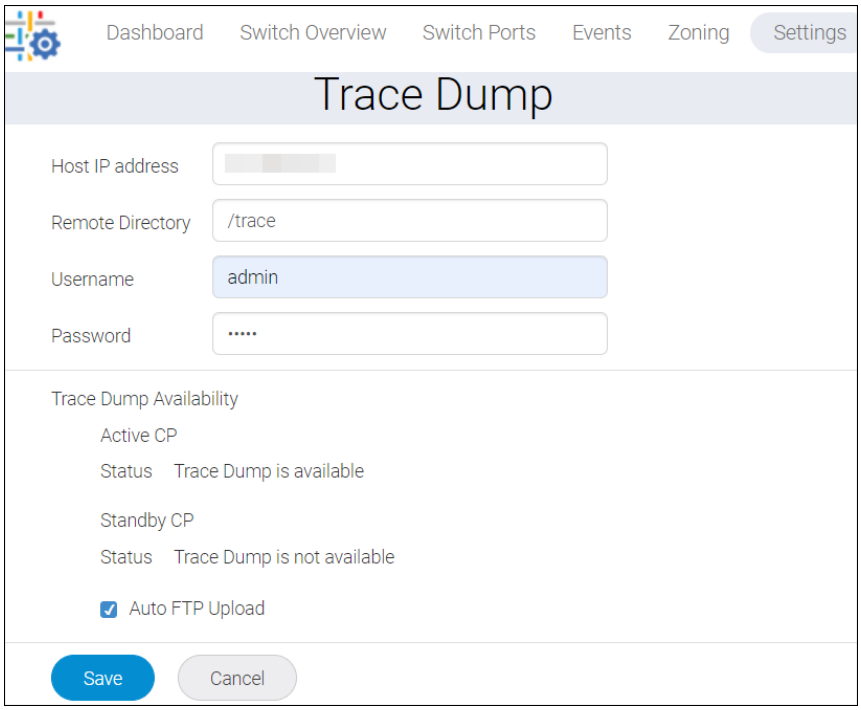
Enabling Automatic Transfer of Trace Dumps

Web Tools allows automatic transfer of trace dumps by providing an option to enable **Auto FTP Upload**. You can view the availability of the trace dump status under the **Trace Dump Availability** option. If a trace dump is not available for a specific server, the `Trace Dump is not available` status appears.

To enable the automatic transfer of trace dumps, perform the following steps:

NOTE
You cannot enable the **Auto FTP Upload** option until you have specified a remote server and the trace dump is available.

1. Click **Settings** in the navigation bar, and then select **Services** > **Trace Dump**.
   The **Trace Dump** window is displayed.
2. Select the **Auto FTP Upload** option under **Trace Dump Availability** both for the active and standby CP. The **Active CP** and **Standby CP** options are available for chassis.

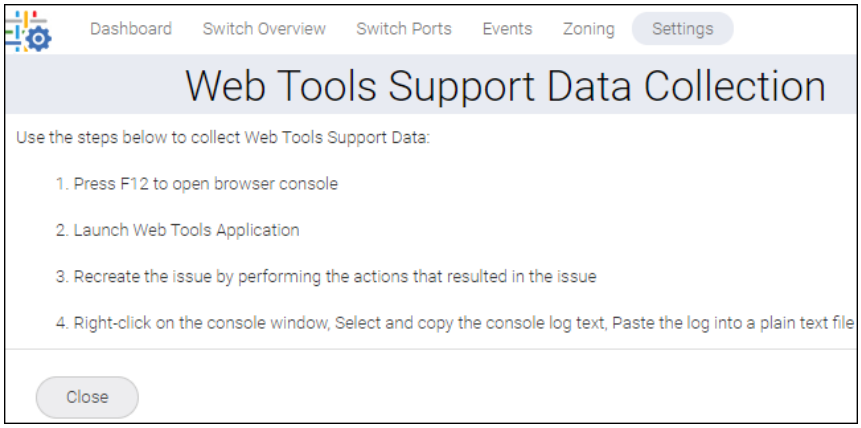


3. Click **Save**.
   The trace dump is automatically uploaded to the FTP server.

Web Tools Support Data Collection

Web Tools Support Data Collection allows you to collect log information to troubleshoot any issue.

1. Press **F12** to open browser console.
2. Launch Web Tools.
3. Click **Settings** in the navigation bar, and then select **Services** > **Web Tools Support Data Collection**. The **Web Tools Support Data Collection** window is displayed.
4. Re-create the issue by performing the actions that resulted in the issue.
5. Right-click the console window, and then select, copy, and paste the console log text into a plain text file.



Revision History

The revision history provides a list of the significant changes made in each version of the document.

FOS-92x-WebTools-UG100; April 28, 2023

Initial document release.

Documentation Legal Notice

This notice provides copyright and trademark information as well as legal disclaimers.

Broadcom reserves the right to make changes without further notice to any products or data herein to improve reliability, function, or design. Information furnished by Broadcom is believed to be accurate and reliable. However, Broadcom does not assume any liability arising out of the application or use of this information, nor the application or use of any product or circuit described herein, neither does it convey any license under its patent rights nor the rights of others.

The product described by this document may contain open source software covered by the GNU General Public License or other open source license agreements. To find out which open source software is included in Brocade products or to view the licensing terms applicable to the open source software, please download the open source attribution disclosure document in the Broadcom Support Portal. If you do not have a support account or are unable to log in, please contact your support provider for this information.


BROADCOM®