

ExtremeSwitching™

## Using CLI and EDM

© 2017, Extreme Networks  
All Rights Reserved.

#### Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Extreme Networks, Inc. assumes no liability for any errors. Extreme Networks, Inc. reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

#### Documentation disclaimer

"Documentation" means information published in varying mediums which may include product information, operating instructions and performance specifications that are generally made available to users of products. Documentation does not include marketing materials. Extreme Networks shall not be responsible for any modifications, additions, or deletions to the original published version of Documentation unless such modifications, additions, or deletions were performed by or on the express behalf of Extreme Networks. End User agrees to indemnify and hold harmless Extreme Networks, Extreme Networks' agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

#### Link disclaimer

Extreme Networks is not responsible for the contents or reliability of any linked websites referenced within this site or Documentation provided by Extreme Networks. Extreme Networks is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Extreme Networks does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

#### Warranty

Extreme Networks provides a limited warranty on Extreme Networks hardware and software. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Extreme Networks' standard warranty language, as well as information regarding support for this product while under warranty is available to Extreme Networks customers and other parties through the Extreme Networks Support website: <http://www.extremenetworks.com/support> under the link "Policies" or such successor site as designated by Extreme Networks. Please note that if You acquired the product(s) from an authorized Extreme Networks Channel Partner outside of the United States and Canada, the warranty is provided to You by said Extreme Networks Channel Partner and not by Extreme Networks.

"Hosted Service" means an Extreme Networks hosted service subscription that You acquire from either Extreme Networks or an authorized Extreme Networks Channel Partner (as applicable) and which is described further in Hosted SAS or other service description documentation regarding the applicable hosted service. If You purchase a Hosted Service subscription, the foregoing limited warranty may not apply but You may be entitled to support services in connection with the Hosted Service as described further in your service description documents for the applicable Hosted Service. Contact Extreme Networks or Extreme Networks Channel Partner (as applicable) for more information.

#### Hosted Service

THE FOLLOWING APPLIES ONLY IF YOU PURCHASE AN EXTREME NETWORKS HOSTED SERVICE SUBSCRIPTION FROM EXTREME NETWORKS OR AN EXTREME NETWORKS CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE EXTREME NETWORKS WEBSITE, <https://extremeportal.force.com> OR SUCH SUCCESSOR SITE AS DESIGNATED BY EXTREME NETWORKS, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU

REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE.

#### Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE EXTREME NETWORKS WEBSITE, <https://extremeportal.force.com> OR SUCH SUCCESSOR SITE AS DESIGNATED BY EXTREME NETWORKS, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS EXTREME NETWORKS SOFTWARE, PURCHASED FROM EXTREME NETWORKS, INC., ANY EXTREME NETWORKS AFFILIATE, OR AN EXTREME NETWORKS CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH EXTREME NETWORKS OR AN EXTREME NETWORKS CHANNEL PARTNER. UNLESS OTHERWISE AGREED TO BY EXTREME NETWORKS IN WRITING, EXTREME NETWORKS DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN EXTREME NETWORKS, AN EXTREME NETWORKS AFFILIATE OR AN EXTREME NETWORKS CHANNEL PARTNER; EXTREME NETWORKS RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND EXTREME NETWORKS, INC. OR THE APPLICABLE EXTREME NETWORKS AFFILIATE ("EXTREME NETWORKS").

Extreme Networks grants You a license within the scope of the license types described below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License as set forth below in the Designated System(s) License (DS) section as applicable. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to You. "Software" means computer programs in object code, provided by Extreme Networks or an Extreme Networks Channel Partner, whether as stand-alone products, pre-installed on hardware products, and any upgrades, updates, patches, bug fixes, or modified versions thereto. "Designated Processor" means a single stand-alone computing device. "Server" means a set of Designated Processors that hosts (physically or virtually) a software application to be accessed by multiple users. "Instance" means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine ("VM") or similar deployment.

#### License type(s)

Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only: 1) on a number of Designated Processors up to the number indicated in the order; or 2) up to the number of Instances of the Software as indicated in the order, Documentation, or as authorized by Extreme Networks in writing. Extreme Networks may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, location or other specific designation, or to be provided by End User to Extreme Networks through electronic means established by Extreme Networks specifically for this purpose.

#### Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, Hosted Service, or hardware provided by Extreme Networks. All content on this site, the documentation, Hosted Service, and the product provided by Extreme Networks including the selection, arrangement and design of the content is owned either by Extreme Networks or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part,

including any code and software unless expressly authorized by Extreme Networks. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Extreme Networks can be a criminal, as well as a civil offense under the applicable law.

### Virtualization

The following applies if the product is deployed on a virtual machine. Each product has its own ordering code and license types. Note, unless otherwise stated, that each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Extreme Networks Channel Partner would like to install two Instances of the same type of products, then two products of that type must be ordered.

### Third Party Components

"Third Party Components" mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements ("Third Party Components"), which contain terms regarding the rights to use certain portions of the Software ("Third Party Terms"). As required, information regarding distributed Linux OS source code (for those products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the products, Documentation or on Extreme Networks' website at: <http://www.extremenetworks.com/support/policies/software-licensing> or such successor site as designated by Extreme Networks. The open source software license terms provided as Third Party Terms are consistent with the license rights granted in these Software License Terms, and may contain additional rights benefiting You, such as modification and distribution of the open source software. The Third Party Terms shall take precedence over these Software License Terms, solely with respect to the applicable Third Party Components to the extent that these Software License Terms impose greater restrictions on You than the applicable Third Party Terms.

The following applies only if the H.264 (AVC) codec is distributed with the product. THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE [HTTP://WWW.MPEGLA.COM](http://WWW.MPEGLA.COM).

### Service Provider

THE FOLLOWING APPLIES TO EXTREME NETWORKS CHANNEL PARTNER'S HOSTING OF EXTREME NETWORKS PRODUCTS OR SERVICES. THE PRODUCT OR HOSTED SERVICE MAY USE THIRD PARTY COMPONENTS SUBJECT TO THIRD PARTY TERMS AND REQUIRE A SERVICE PROVIDER TO BE INDEPENDENTLY LICENSED DIRECTLY FROM THE THIRD PARTY SUPPLIER. AN EXTREME NETWORKS CHANNEL PARTNER'S HOSTING OF EXTREME NETWORKS PRODUCTS MUST BE AUTHORIZED IN WRITING BY EXTREME NETWORKS AND IF THOSE HOSTED PRODUCTS USE OR EMBED CERTAIN THIRD PARTY SOFTWARE, INCLUDING BUT NOT LIMITED TO MICROSOFT SOFTWARE OR CODECS, THE EXTREME NETWORKS CHANNEL PARTNER IS REQUIRED TO INDEPENDENTLY OBTAIN ANY APPLICABLE LICENSE AGREEMENTS, AT THE EXTREME NETWORKS CHANNEL PARTNER'S EXPENSE, DIRECTLY FROM THE APPLICABLE THIRD PARTY SUPPLIER.

WITH RESPECT TO CODECS, IF THE EXTREME NETWORKS CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE G.729 CODEC, H.264 CODEC, OR H.265 CODEC, THE EXTREME NETWORKS CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE EXTREME NETWORKS CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE G.729 CODEC IS LICENSED BY SIPRO LAB TELECOM INC. SEE [WWW.SIPRO.COM/CONTACT.HTML](http://WWW.SIPRO.COM/CONTACT.HTML). THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR

THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (I) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (II) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE [HTTP://WWW.MPEGLA.COM](http://WWW.MPEGLA.COM).

### Compliance with Laws

You acknowledge and agree that it is Your responsibility for complying with any applicable laws and regulations, including, but not limited to laws and regulations related to call recording, data privacy, intellectual property, trade secret, fraud, and music performance rights, in the country or territory where the Extreme Networks product is used.

### Preventing Toll Fraud

"Toll Fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

### Security Vulnerabilities

Information about Extreme Networks' security support policies can be found in the Global Technical Assistance Center Knowledgebase at <https://gtacknowledge.extremenetworks.com/>.

### Downloading Documentation

For the most current versions of Documentation, see the Extreme Networks Support website: <http://documentation.extremenetworks.com>, or such successor site as designated by Extreme Networks.

### Contact Extreme Networks Support

See the Extreme Networks Support website: <http://www.extremenetworks.com/support> for product or Hosted Service notices and articles, or to report a problem with your Extreme Networks product or Hosted Service. For a list of support telephone numbers and contact addresses, go to the Extreme Networks Support website: <http://www.extremenetworks.com/support/contact/> (or such successor site as designated by Extreme Networks), scroll to the bottom of the page, and select Contact Extreme Networks Support.

### Contact Avaya Support

See the Avaya Support website: <https://support.avaya.com> for product or Hosted Service notices and articles, or to report a problem with your Avaya product or Hosted Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: <https://support.avaya.com> (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

### Trademarks

The trademarks, logos and service marks ("Marks") displayed in this site, the Documentation, Hosted Service(s), and product(s) provided by Extreme Networks are the registered or unregistered Marks of Extreme Networks, Inc., its affiliates, its licensors, its suppliers, or other third parties. Users are not permitted to use such Marks without prior written consent from Extreme Networks or such third party which may own the Mark. Nothing contained in this site, the Documentation, Hosted Service(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Extreme Networks or the applicable third party.

Extreme Networks is a registered trademark of Extreme Networks, Inc.

All non-Extreme Networks trademarks are the property of their respective owners. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

For additional information on Extreme Networks trademarks, please see: <http://www.extremenetworks.com/company/legal/>

## Contents

<b>Chapter 1: New in this document</b> .....	7
Notice about feature support.....	7
<b>Chapter 2: Command Line Interface fundamentals</b> .....	8
CLI command modes.....	8
Default user names and passwords.....	11
Documentation convention for the port variable.....	12
Command completion.....	13
<b>Chapter 3: CLI procedures</b> .....	15
Logging on to the software.....	15
Viewing configurations.....	15
Changing user modes in CLI.....	16
Saving the configuration.....	20
Configuring the web server.....	21
Setting the TLS protocol version.....	23
<b>Chapter 4: Enterprise Device Manager fundamentals</b> .....	26
Supported browsers.....	26
Enterprise Device Manager access.....	26
Default user name and password.....	27
Device Physical View.....	27
EDM window.....	28
Navigation pane.....	28
Menu bar.....	31
Toolbar.....	31
Work area.....	32
EDM user session extension.....	32
TLS server for secure HTTPS.....	32
Certificate order priority.....	33
<b>Chapter 5: EDM interface procedures</b> .....	34
Connecting to EDM.....	34
Configuring the web management interface.....	35
Using the chassis shortcut menu.....	36
Using the port shortcut menu.....	37
Using a table-based tab.....	38
Monitoring multiple ports and configuration support.....	39
Opening folders and tabs.....	39
Undocking and docking tabs.....	40
Installing EDM help files.....	41
<b>Chapter 6: File management in EDM</b> .....	42
Copying files.....	42

Contents

Viewing file storage information..... 43  
Displaying internal flash files..... 43  
Displaying USB file information..... 44  
**Glossary**..... 45

# Chapter 1: New in this document

There are no feature changes in this document.

---

## Notice about feature support

This document includes content for multiple hardware platforms across different software releases. As a result, the content can include features not supported by your hardware in the current software release.

If a documented command, parameter, tab, or field does not appear on your hardware, it is not supported.

For information about feature support, see *Release Notes*.

For information about physical hardware restrictions, see your hardware documentation.

# Chapter 2: Command Line Interface fundamentals

This section describes the Command Line Interface (CLI).

CLI is an industry standard command line interface that you can use for single-device management.

---

## CLI command modes

CLI has six major command modes. You start your session on the switch in User EXEC mode. From User EXEC mode, you can enter Privileged EXEC mode. From Privileged EXEC mode, you can enter Global Configuration mode. From Global Configuration mode, you can enter one of the remaining modes.


Each mode provides a specific set of commands. While in a higher mode, you can access most commands from lower modes, except if they conflict with commands of your current mode.

The following table describes the command modes.

Command mode	Description
User EXEC	The initial mode of access.  Only a limited number of commands are available in the User EXEC mode. Most EXEC commands are one-time commands, such as show commands, which show the current configuration status. User EXEC commands are not saved across restarts.
Privileged EXEC	Access this mode from the User EXEC mode.  The user name and password combination determines your access level in the Privileged EXEC mode and higher modes. Enter <code>enable</code> to access this mode from the User EXEC mode. As with the User EXEC mode commands, most EXEC commands are one-time commands, such as show commands, which show the current configuration status. The Privileged EXEC mode commands are also not saved across restarts.
Global Configuration	Access this mode from the Privileged EXEC mode.  Enter <code>config {terminal network}</code> to access the Global Configuration mode. Use this mode to make changes to the running configuration. If you save the configuration, these settings survive a restart of the system.

*Table continues...*



Command mode	Description
Interface Configuration	<p>Access this mode from the Global Configuration mode.</p> <p>Enter <code>interface {GigabitEthernet {slot/port[/sub-port] [-slot/port[/sub-port]][, ...]}&gt;   loopback &lt;1-256&gt;   mgmtEthernet mgmt   mlt &lt;1-512&gt;   vlan &lt;1-4059&gt;}</code> to access the Interface Configuration mode. Use this mode to modify either a logical interface, such as a virtual local area network (VLAN), or a physical interface, such as a port. You can configure the following interfaces:</p> <ul style="list-style-type: none"> <li>• GigabitEthernet</li> <li>• Loopback</li> <li>• mgmtEthernet</li> <li>• MLT</li> <li>• VLAN</li> </ul> <p> <b>Note:</b></p> <p>The mgmtEthernet interface only applies to hardware with a dedicated, physical management interface. For more information, see your hardware documentation.</p>
Router Configuration	<p>Access this mode from the Global Configuration mode.</p> <p>Enter <code>router {bgp isis  ospf  rip  vrf WORD&lt;1-16&gt;   vrrp}</code> to access the Router Configuration mode. Use this mode to modify a protocol. You can configure the following protocols:</p> <ul style="list-style-type: none"> <li>• BGP</li> <li>• IS-IS</li> <li>• OSPF</li> <li>• RIP</li> <li>• VRF</li> <li>• VRRP</li> </ul>
Application Configuration	<p>Access this mode from the Global Configuration mode.</p> <p>Enter <code>application</code> to access the Application Configuration mode.</p>

From either the Global Configuration mode or the Interface Configuration mode, you can save all of the configuration parameters to a file. The default name for the configuration file is `config.cfg`. You can also use alternative file names.

You can enter most of the show commands from the User EXEC mode. In most cases, you can also enter the show commands in all of the upper-level command modes. If you need to enter a particular command mode to access a show command, the procedure will state the required mode.

The following table lists the CLI command modes, the prompt for each mode, and explains how to enter and exit each mode. The prompt is prefaced by the system name, for example:

- `Switch:1#`

## Command Line Interface fundamentals

- LabSwitch:1 (config-isis) #
- NewYork:1 (config) #
- OttawaBranch:1 (config-bgp) #

**Table 1: CLI command modes**

Command mode	Prompt	Command mode or enter/exit mode
User EXEC	>	This mode is the default command mode and does not require an entrance command.  To exit the CLI, enter <code>logout</code> .
Privileged EXEC	#	Enter <code>enable</code> to access the Privileged EXEC mode from the User EXEC mode.  Enter <code>disable</code> to exit the Privileged EXEC mode, and enter the User EXEC mode.  To exit the CLI, enter <code>logout</code> .
Global Configuration	(config)#	From the Privileged EXEC mode, enter <code>configure</code> , followed by either <code>terminal</code> or <code>network</code> to access the Global Configuration mode.  Enter <code>exit</code> to exit the Global Configuration mode, and enter the Privileged EXEC mode.  To exit the CLI, enter <code>logout</code> .
Interface Configuration	(config-if)# (config-mlt)#	Entry into this command mode depends on the type of configured interfaces. From the Global Configuration mode, enter <code>interface {GigabitEthernet {slot/port[/sub-port] [-slot/port[/sub-port]] [, ...]}</code>   <code>loopback &lt;1-256&gt;</code>   <code>mgmtEthernet mgmt   mlt &lt;1-512&gt;</code>   <code>vlan &lt;1-4059&gt;</code> to access the Interface Configuration mode.  <b>* Note:</b>  The <code>mgmtEthernet</code> interface only applies to hardware with a dedicated, physical management interface. For more information, see your hardware documentation.

*Table continues...*

Command mode	Prompt	Command mode or enter/exit mode
		<p>Enter <b>exit</b> to exit the Interface Configuration mode and enter the Global Configuration mode.</p> <p>To return to the Privileged EXEC mode, enter <b>end</b>.</p> <p>To exit the CLI, enter <b>logout</b>.</p>
Router Configuration	(config-bgp)# (config-isis)# (config-ospf)# (config-rip)# (router-vrf)# (config-vrrp)#	<p>Entry into this command mode depends on the configured protocols. Enter <b>router {bgp isis  ospf  rip  vrf WORD&lt;1-16&gt;   vrrp}</b> to access the Router Configuration mode from the Global Configuration mode.</p> <p>Enter <b>exit</b> to exit the Router Configuration mode and enter the Global Configuration mode.</p> <p>To return to the Privileged EXEC mode, enter <b>end</b>.</p> <p>To exit the CLI, enter <b>logout</b>.</p>
Application Configuration	(config-app)#	<p>Enter <b>application</b> to access the Application Configuration mode from the Global Configuration mode.</p> <p>Enter <b>exit</b> to exit the Application Configuration mode, and enter the Global Configuration mode.</p> <p>To return to the Privileged EXEC mode, enter <b>end</b>.</p> <p>To exit the CLI, enter <b>logout</b>.</p>

## Default user names and passwords

The following table contains the default user names and passwords that you can use to log on to the switch using the command line interface (CLI). For more information about how to change passwords, see *Configuring Security*.

**Table 2: CLI default user names and passwords**

User name	Password	Description
rwa	rwa	read-write-all
rw	rw	read-write

*Table continues...*

User name	Password	Description
ro	ro	read-only
l1	l1	layer 1
l2	l2	layer 2
l3	l3	layer 3

If you enable enhanced secure mode, the user names and passwords are different than the default values documented in the preceding table. For more information on enhanced secure mode, see *Administering*.

**! Important:**

The default passwords and community strings are documented and well known. It is strongly recommended that you change the default passwords and community strings immediately after you first log on. For more information about how to change user names and passwords, see *Configuring Security*.

## Documentation convention for the port variable

Commands that require you to enter one or more port numbers on the switch use the parameter `{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}` in the syntax. The following table specifies the rules for using `{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}`.

Syntax	How to use
<code>{slot/port[/sub-port]}</code>	<p>Identifies a single slot and port. If your platform supports channelization and the port is channelized, you must also specify the sub-port in the format <code>slot/port/sub-port</code>.</p> <p>For example, <code>1/1</code> indicates the first port on slot 1. <code>1/41/1</code> indicates the first channel on slot 1, port 41.</p>
<code>{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}</code>	<p>Identifies the slot and port in one of the following formats: a single slot and port (<code>slot/port</code>), a range of slots and ports (<code>slot/port-slot/port</code>), or a series of slots and ports (<code>slot/port,slot/port,slot/port</code>). If your platform supports channelization and the port is channelized, you must also specify the sub-port in the format <code>slot/port/sub-port</code>.</p> <p>For example, <code>1/1-1/3</code> indicates ports 1 to 3 on slot 1, or <code>1/41/1,1/41/3</code> indicates the first and third channels of slot 1, port 41.</p>

## Command completion

The CLI provides potential command completions to the command string. Completions are provided by using a question mark (?) or by using the CLI autocompletion feature.

### ? command completion

The ? command completion is available for any valid command. By typing a command and using a ? as the last argument in the command, the system returns a list of possible command completions from the point of the ?. A short description is provided with each possible completion.

#### Example

If you enter the following command:

```
Switch:1(config-isis)#redistribute ?
```

CLI provides a list of completions for the **redistribute ?** command.

```
Switch:1(config-isis)#redistribute ?
  direct      isis redistribute direct command
  ospf        isis redistribute ospf command
  rip         isis redistribute rip command
  static      isis redistribute static command
```

All the parameters listed under redistribute indicate sub-context commands.

You must use one of the available completions, and if necessary, use the command completion help again to find the next completion.

```
Switch:1(config-isis)#redistribute direct ?
  enable      Enable isis redistribute direct command
  metric      Isis route redistribute metric
  metric-type Set isis redistribute metric type
  route-map   Set isis redistribute direct route-policy
  subnets    Set isis redistribute subnets
<cr>
```

When you see <cr> (Carriage Return/Enter Key) in the list with the additional choices, this means that no additional parameters are required to execute the CLI command. However, the additional choices listed could be peer commands or sub-context commands.

For example, the parameters listed under **redistribute direct ?** are peer commands. You can enter these peer commands on the same line as the root command, for example **redistribute direct enable**. However, the <cr> indicates that you can also enter the **redistribute direct** command only and this command does not require any additional parameters at this level.

### CLI autocompletion

CLI autocompletion is a feature that you can use to automatically fill in the unique parts of a command string rather than typing the entire command. Autocompletion makes the CLI experience easier and prevents mistakes in spelling that force you to re-enter the command.

Autocompletion completes the token in the command as soon as it becomes unique.

The `Tab` key autocompletes the command without executing the command, and places the cursor immediately after the last character. The `Enter` key autocompletes the command and executes it.

### Example

To enable redistribution of ISIS direct routes,

```
Switch:1(config-isis)#redistribute direct
```

When you use `redistribute ?`, you see four possible sub-context commands.

```
direct
static
ospf
rip
```

If you type the following without pressing `Enter`:

```
Switch:1(config-isis)#redistribute direct m
```

and press the `Tab` key, the system completes the command to the following point:

```
redistribute direct metric
```

Two possible completions exist. You can type `-t`, and then press `Tab` to finish the command:

```
Switch:1(config-isis)#redistribute direct metric-type
```

# Chapter 3: CLI procedures

This chapter contains information about common CLI tasks. You can access CLI during runtime to manage the switch.

---

## Logging on to the software

### Before you begin

- The first time you connect to the switch, you must log on to CLI using the direct console port.

### About this task

After you first connect to CLI you can log on to the software using the default user name and password. For more information about the default user names and passwords, see [Default user names and passwords](#) on page 11.

### Procedure

1. At the login prompt, enter the user name.
2. At the password prompt, enter the password.

---

## Viewing configurations

You can view the running configuration using the show command.

### Procedure

1. Enter Privileged EXEC mode:

```
enable
```

2. View running configuration:

```
show running-config
```

### Example

```
Switch:1#show running-config
Preparing to Display Configuration...
#
#
```

## CLI procedures

```
# Thu Feb 05 18:38:02 2016 UTC
# box type           : ProductNameX
# software version   : 4.3.0.0GA
# cli mode           : CLI
#
#
#!end
#
config terminal
#
#
#BOOT CONFIGURATION
#
boot config flags ftpd
boot config flags telnetd
# end boot flags
auto-recover-delay 10
#
#CLI CONFIGURATION
#
telnet-access sessions 3
password password-history 3
#
#SYSTEM CONFIGURATION
#
ip name-server primary 198.51.100.0
sys msg-control control-interval 30
sys msg-control
#
#
```

---

## Changing user modes in CLI

Perform this procedure to change user modes in CLI.

### Before you begin

- You must log on to CLI.

### About this task

You can enter shortened versions of the commands, if the letter combination is unique.

### Procedure

1. Access the Privileged EXEC mode:  
`enable`
2. Access the Global Configuration mode:



```
configure terminal
```

### 3. Access the Interface Configuration mode:

**\* Note:**

The **mgmtEthernet mgmt** command applies only to hardware with a dedicated, physical management interface.

```
interface {GigabitEthernet {slot/port[/sub-port] [-slot/port[/sub-
port]] [,...]} | loopback <1-256> | mgmtEthernet mgmt|mlt <1-512> |
vlan <1-4059>}
```

### 4. Access the Router Configuration mode:

```
router {bgp [0-65535] | isis [enable] | ospf [enable] | rip [enable|
ipv6-enable] | vrf WORD<1-16>| vrrp}
```

### 5. Access the Application Configuration mode:

```
application
```

## Example

Access Privileged EXEC mode:

```
Switch:1> enable
```

Access Global Configuration mode:

```
Switch:1#configure terminal
```

Access Interface Configuration mode for a VLAN:

```
Switch:1(config)#interface vlan 2
```

Access Router Configuration mode for BGP:

```
Switch:1(config-if)# router bgp
```

Exit back to Global Configuration mode:

```
Switch:1(router-bgp) # exit
```

Access Router Configuration mode for isis:

```
Switch:1(config-if)#router isis
```

Exit back to Global Configuration mode:

```
Switch:1(config-isis) #exit
```

Access Router Configuration mode for OSPF:

```
Switch:1(config)#router ospf
```

Exit back to Global Configuration mode:

```
Switch:1(router-ospf) # exit
```

Access Application Configuration mode:

```
Switch:1 (config) # application
```

Exit back to Privileged EXEC mode:

```
Switch:1 (config-app) # end
```

Exit back to User EXEC mode:


```
Switch:1#disable
```

Exit the system:

```
Switch:1>exit
```

## Variable definitions

Use the data in the following table to use the **interface** command.

Variable	Value
GigabitEthernet {slot/port[/sub-port] [-slot/port/sub-port]} [...]	<p>Logs on to the GigabitEthernet Interface Configuration mode.</p> <p>Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If your platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.</p>
loopback <1-256>	<p>Logs on to the loopback Interface Configuration mode. Use &lt;1-256&gt; to specify which interface to configure.</p>
mgmtEthernet <i>mgmt</i>	<p>Logs on to the mgmtEthernet Interface Configuration mode. Use <i>mgmt</i> for management configurations.</p> <p> <b>Note:</b></p> <p>The <b>mgmtEthernet mgmt</b> command applies only to hardware with a dedicated, physical management interface.</p>
mlt <1-512>	<p>Logs on to the multi-link trunking (MLT) Interface Configuration mode. Use &lt;1-512&gt; to specify which MLT to configure.</p>
vlan <1-4059>	<p>Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the vrf-scaling and spbm-config-mode boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.</p>

Use the data in the following table to use the `router` command.

Variable	Value
<code>bgp [&lt;0-65535&gt;] [enable]</code>	Enter Border Gateway Protocol (BGP) Router Configuration mode. You can specify a specific autonomous system number. The <code>router bgp</code> command allows you to enter BGP Router Configuration mode. <code>&lt;0-65535&gt;</code> allows you to specify the AS number and the <code>enable</code> option allows you to enable BGP.
<code>bgp [as-4-byte enable]</code>	Enable 4-byte autonomous system numbers globally.
<code>bgp [as-dot enable]</code>	Enable the AS dot representation for 4-byte AS numbers globally.
<code>bgp [WORD &lt;0-11&gt; [enable]]</code>	Specifies the AS number and enables BGP. You cannot enable BGP until you change the local AS to a value other than 0.
<code>isis [enable]</code>	Enter IS-IS Router Configuration mode. The command <code>router isis</code> allows you to enter IS-IS Router Configuration mode. After the configuration, use <code>router isis enable</code> to enable IS-IS globally.
<code>ospf [enable] [ipv6-enable]</code>	Enter Open Shortest Path First (OSPF) Router Configuration mode. You can specify <code>ospf</code> or <code>ipv6</code> . The command <code>router ospf</code> allows you to enter OSPF Router Configuration mode. After the configuration, use <code>router ospf enable</code> to enable OSPF globally.  The options <code>enable</code> or <code>ipv6-enable</code> enable OSPF for the switch.
<code>rip [enable] [vrf &lt;1-255&gt;]</code>	Enter Routing Information Protocol (RIP) Router Configuration mode. You can specify to enable RIP or to enable RIP on a specific Virtual Router Forwarding (VRF) ID. The command <code>router rip</code> allows you to enter RIP Router Configuration mode. After the configuration, use <code>router rip enable</code> to enable RIP globally.
<code>vrf WORD&lt;1-16&gt;</code>	Enter Virtual Router Forwarding (VRF) Router Configuration mode. Specify the VRF name to configure. The command <code>router vrf WORD&lt;1-16&gt;</code> allows you to enter VRF Router Configuration mode.
<code>vrrp</code>	Enter Virtual Router Redundancy Protocol Router Configuration mode.

## Saving the configuration

After you change the configuration, you must save the changes to the module. Save the configuration to a file to retain the configuration settings.

### About this task

File Transfer Protocol (FTP) and Trivial File Transfer Protocol (TFTP) support both IPv4 and IPv6 addresses, with no difference in functionality or configuration.

### Procedure

1. Enter Privileged EXEC mode:

```
enable
```

2. Save the running configuration:

```
save config [backup WORD<1-99>] [file WORD<1-99>] [verbose]
```

### Example

Save the configuration to the default location:

```
Switch:1#save config
```

Identify the file as a backup file and designate a location to save the file:

```
Switch:1#save config backup 198.51.100.1/configs/backup.cfg
```

## Variable definitions

Use the data in the following table to use the `save config` command.

Variable	Value
backup <i>WORD&lt;1-99&gt;</i>	<p>Saves the specified file name and identifies the file as a backup file.</p> <p><i>WORD&lt;1-99&gt;</i> uses one of the following formats:</p> <ul style="list-style-type: none"> <li>• a.b.c.d:&lt;file&gt;</li> <li>• /intflash/&lt;file&gt;</li> </ul> <p>The file name, including the directory structure, up to 1 to 99 characters.</p>
file <i>WORD&lt;1-99&gt;</i>	<p>Specifies the file name in one of the following formats:</p> <ul style="list-style-type: none"> <li>• /intflash/&lt;file&gt;</li> <li>• a.b.c.d:&lt;file&gt;</li> </ul> <p>The file name, including the directory structure, up to 1 to 99 characters.</p>

*Table continues...*

Variable	Value
verbose	Saves the default and current configuration. If you omit this parameter, the command saves only parameters you change.
standby <i>WORD</i> <1-99>	Specifies the standby file name in the following format: <ul style="list-style-type: none"> <li>• /intflash/&lt;file&gt;</li> </ul> The file name, including the directory structure, up to 1 to 99 characters.

---

## Configuring the web server

Perform this procedure to enable and manage the web server using the Command Line Interface (CLI). After you enable the web server, you can connect to EDM.

HTTP and FTP support both IPv4 and IPv6 addresses, with no difference in functionality or configuration. The TFTP server supports both IPv4 and IPv6 addresses. The TFTP client is not supported, only the server.

### About this task

This procedure assumes that you use the default port assignments. You can change the port number used for HTTP and HTTPS.

#### Important:

If you want to allow HTTP access to the device, you must disable the web server secure-only option. If you want to allow HTTPS access to the device, the web server secure-only option is enabled by default.

### Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```
2. Enable the web server:

```
web-server enable
```
3. Disable the secure-only option (for HTTP access) :

```
no web-server secure-only
```
4. Enable the secure-only option (for HTTPS access) :

```
web-server secure-only
```
5. Display the web server status:

```
show web-server
```

### Example

Enable the secure-only web-server, and configure the access level to read-write-all, for a username of smith2 and the password to 90Go2437.

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#web-server enable
Switch:1(config)#web-server secure-only
Switch:1(config)#web-server password rwa smith2 90Go2437
Switch:1(config)#show web-server
```

Web Server Info :

```
Status                : on
Secure-only           : enabled
TLS-minimum-version   : tlsv11
RWA Username          : smith2
RWA Password          : *****
Def-display-rows      : 30
Inactivity timeout    : 900 sec
Html help tftp source-dir :
HttpPort              : 80
HttpsPort             : 443
NumHits               : 232
NumAccessChecks       : 12
NumAccessBlocks       : 0
NumRxErrors           : 178
NumTxErrors           : 0
NumSetRequest         : 0
Minimum password length : 8
Last Host Access Blocked : 0.0.0.0
```

---

## Variable definitions

Use the data in the following table to use the `web-server` command.

Variable	Value
<code>def-display-rows &lt;10-100&gt;</code>	Configures the number of rows each page displays, between 10 and 100.
<code>enable</code>	Enables the Web interface. To disable the web server, use the no form of this command:  <code>no web-server [enable]</code>
<code>help-tftp &lt;WORD/0-256&gt;</code>	Configures the TFTP or FTP directory for Help files, in one of the following formats: <code>a.b.c.d:/  peer:/ [&lt;dir&gt;]</code> . The path can use 0–256 characters. The following example paths illustrate the correct format: <ul style="list-style-type: none"> <li>• <code>192.0.2.1:/help</code></li> <li>• <code>192.0.2.1/</code></li> </ul>

*Table continues...*

Variable	Value
http-port <80-49151>	Configures the web server HTTP port. The default port is 80.
https-port <443-49151>	Configure the web server HTTPS port. The default port is 443.
inactivity-timeout<30-65535>	Configures the web-server session inactivity timeout. The default is 900 seconds (15 minutes).
password {ro   rw   rwa} WORD<1-20> WORD<1-32>	Configures the logon and password for the web interface, where the first WORD<1-20> is the new logon and the second WORD<1-32> is the new password.
password min-passwd-len<1-32>	Configures the minimum password length. By default, the minimum password length is 8 characters.
secure-only	Enables secure-only access for the web server.
tls-min-ver<tlsv10 tlsv11 tlsv12>	Configures the minimum version of the TLS protocol supported by the web-server. You can select among the following: <ul style="list-style-type: none"> <li>• tlsv10 – Configures the version to TLS 1.0.</li> <li>• tlsv11 – Configures the version to TLS 1.1.</li> <li>• tlsv12 – Configures the version to TLS 1.2</li> </ul> The default is tlsv12.

---

## Setting the TLS protocol version

The switch by default supports version TLS 1.2 and above. You can explicitly configure TLS 1.0 and TLS 1.1 version support using CLI.

### About this task

Disable the web server before changing the TLS version. By disabling the web server, other existing users with a connection to the web server are not affected from changing to a different version after you run the `tls-min-ver` command.

### Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. Disable the Web server:

```
no web-server enable
```

3. Set the TLS protocol version:

```
web-server tls-min-ver [tlsv10 | tlsv11 | tlsv12]
```

4. Enable the Web server:

```
web-server enable
```

5. Verify the protocol version:

```
show web-server
```

**Example**

```
Switch> enable
Switch# configure terminal
Switch(config)# web-server tls-min-ver tlsv11
```

Verify the protocol version.

```
Switch> show web-server

Web Server Info :

      Status                : on
      Secure-only           : disabled
      TLS-minimum-version   : tlsv11
      RWA Username          : admin
      RWA Password          : *****
      Def-display-rows     : 30
      Inactivity timeout    : 900 sec
      Html help tftp source-dir :
      HttpPort              : 80
      HttpsPort             : 443
      NumHits                : 198
      NumAccessChecks       : 8
      NumAccessBlocks       : 0
      NumRxErrors           : 198
      NumTxErrors           : 0
      NumSetRequest         : 0
      Minimum password length : 8
      Last Host Access Blocked : 0.0.0.0
```

---

## Variable definitions

Use the data in the following table to use the **web-server** command.

Variable	Value
def-display-rows <10-100>	Configures the number of rows each page displays, between 10 and 100.
enable	Enables the Web interface. To disable the web server, use the no form of this command:  no web-server [enable]
help-tftp <WORD/0-256>	Configures the TFTP or FTP directory for Help files, in one of the following formats: a.b.c.d:/  peer:/

*Table continues...*



Variable	Value
	[<dir>]. The path can use 0–256 characters. The following example paths illustrate the correct format: <ul style="list-style-type: none"> <li>• 192.0.2.1:/help</li> <li>• 192.0.2.1/</li> </ul>
http-port <80-49151>	Configures the web server HTTP port. The default port is 80.
https-port <443-49151>	Configure the web server HTTPS port. The default port is 443.
inactivity-timeout<30–65535>	Configures the web-server session inactivity timeout. The default is 900 seconds (15 minutes).
password {ro   rw   rwa} WORD<1-20> WORD<1-32>	Configures the logon and password for the web interface, where the first WORD<1-20> is the new logon and the second WORD<1-32> is the new password.
password min-passwd-len<1–32>	Configures the minimum password length. By default, the minimum password length is 8 characters.
secure-only	Enables secure-only access for the web server.
tls-min-ver<t/1sv10 t/1sv11 t/1sv12>	Configures the minimum version of the TLS protocol supported by the web-server. You can select among the following: <ul style="list-style-type: none"> <li>• t/1sv10 – Configures the version to TLS 1.0.</li> <li>• t/1sv11 – Configures the version to TLS 1.1.</li> <li>• t/1sv12 – Configures the version to TLS 1.2</li> </ul> The default is t/1sv12.

# Chapter 4: Enterprise Device Manager fundamentals

This section details Enterprise Device Manager (EDM).

EDM is a web-based graphical user interface (GUI) you can use to configure a single switch. EDM runs from the switch and you can access it from a web browser. You do not need to install additional client software, and you can access it with all operating systems.

---

## Supported browsers

Use the following recommended browser versions to access Enterprise Device Manager (EDM):

- Microsoft Edge 38.14393
- Microsoft Internet Explorer 11
- Mozilla Firefox 50+

 **Note:**

The following earlier browser versions can be used to access EDM (although not recommended):

- Microsoft Internet Explorer 9 and 10
- Mozilla Firefox 37 through 49

---

## Enterprise Device Manager access

To access EDM, open `http://<deviceip>/login.html` or `https://<deviceip>/login.html` from Microsoft Edge, Microsoft Internet Explorer or Mozilla Firefox. Ensure you use a supported browser version.

 **Important:**

- You must enable the web server from CLI (see [Configuring the Web server using CLI](#) on page 21) to enable HTTP access to the EDM. If you want HTTP access to the device, you must also disable the web server secure-only option. The web server secure-only option,

allowing for HTTPS access to the device, is enabled by default. It is recommended that you take the appropriate security precautions within the network if you use HTTP

- EDM access is available to read-write users only

If you experience issues while connecting to the EDM, check the proxy settings. Proxy settings can affect EDM connectivity to the switch. Clear the browser cache and do not use proxy when connecting to the device.

---

## Default user name and password

The following table contains the default user name and password that you can use to log on to the switch using EDM. For more information about changing the passwords, see *Configuring Security*.

**Table 3: EDM default username and password**

Username	Password
admin	password

### Important:

The default passwords and community strings are documented and well known. It is strongly recommended that you change the default passwords and community strings immediately after you first log on. For more information about changing user names and passwords, see *Configuring Security*.

---

## Device Physical View

After you access EDM, the system displays a real-time physical view of the front panel of the device. From the front panel view, you can view fault, configuration, and performance information for the device or a single port. You can open this tab by clicking the Device Physical View tab above the device view.

You can use the device view to determine the operating status of the various ports in your hardware configuration. You can also use the device view to perform management tasks on specific objects. In the device view, you can select a port or the entire chassis. To select an object, click the object. EDM outlines the selected object in yellow, indicating your selection.

The conventions on the device view are similar to the actual device appearance. The port LEDs and the ports are color-coded to provide status. Green indicates the module or port is up and running, red indicates the module or port is disabled, dark pink indicates a protocol is down, and amber indicates an enabled port that is not connected to anything. For information about LED behavior, see your hardware documentation.

## EDM window

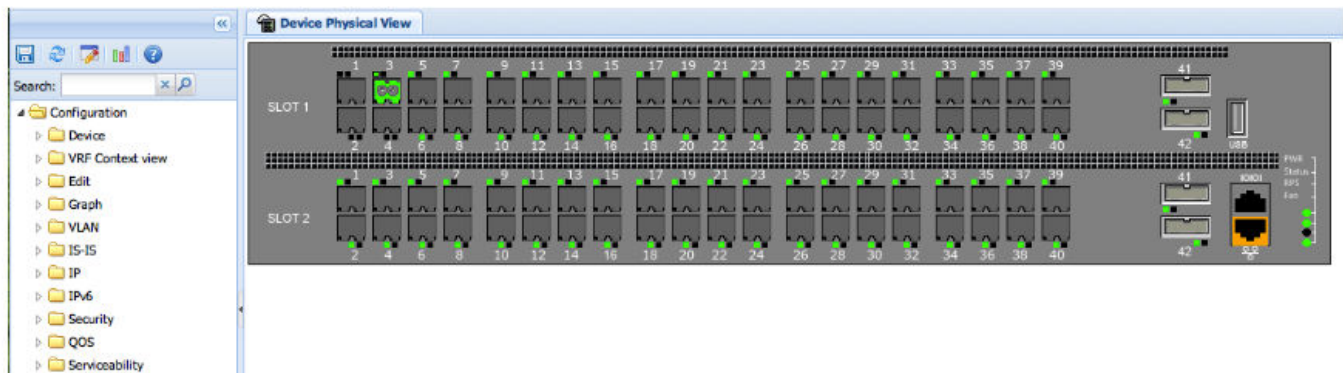
The following figure shows the different sections of the EDM window:

- Navigation pane—Located on the left side of the window, the navigation pane displays all the available command tabs in a tree format. A row of buttons at the top of the navigation pane provides a quick method to perform common functions.
- Menu bar—Located at the top of the window, the menu bar shows the most recently accessed primary tabs and their respective secondary tabs.
- Toolbar—Located just below the menu bar, the toolbar gives you quick access to the most common operational commands such as Apply, Refresh, and Help.
- Work area—Located on the right side of the window, the work area displays the dialog boxes where you can view or configure parameters on the switch.

The following figure shows an example of the Device Physical View window.

**\* Note:**

The Device Physical View on your hardware can appear differently than the following example.



**Figure 1: EDM window**

## Navigation pane






You can use the navigation pane to see what commands are available and to quickly browse through the command hierarchy. A row of buttons at the top of the navigation pane provides a quick method to perform common functions.

**! Important:**

For module-based chassis, menu options related to a specific module are activated only after you install and select the required module.

The following table describes the buttons that appear at the top of the navigation pane.

**Table 4: Navigation pane buttons**

Button	Name	Description
	Save Config	Saves the running configuration.
	Refresh Status	Refreshes the Device Physical View.
	Edit	Edits the selected item in the Device Physical View.
	Graph	Opens the graph options for the selected item in the Device Physical View.
	Help Setup Guide	Opens instructions about how to install the Help files and configure EDM to use the Help files.

Expand a folder by clicking it. Some folders have subfolders such as the Edit folder, which has the Port, Diagnostics, and SNMPv3 subfolders.

Within each folder and subfolder, there are numerous tabs. To open a tab, click it. The selected tab appears in the menu bar and opens in the work area. The following table describes the main folders in the navigation pane.

**Table 5: Navigation pane folders**

Menu	Description
Device	<p>Use the Device menu to refresh and update device information or enable polling.</p> <ul style="list-style-type: none"> <li>• Preference Setting — Enable polling or hot swap detection. Configure the frequency to poll the device.</li> <li>• Refresh Status — Use this option to refresh the device view.</li> <li>• Rediscover Device — Use this to trigger a rediscovery to update all of the device information.</li> </ul>
VRF Context view	<p>Use the VRF Context view to switch to another VRF context when you use the embedded EDM. GlobalRouter is the default view at log in. You can configure both Global Router (GRT) and Virtual Routing and Forwarding (VRF) instances when you</p>

*Table continues...*

Menu	Description
	launch a VRF context view. You can open only five tabs for each EDM session.
Edit	<p>Use the Edit menu to view and configure parameters for the chassis or for the currently selected object. The selected object can be a port. You can also use the Edit menu to perform the following tasks:</p> <ul style="list-style-type: none"> <li>• check and update security settings for the device</li> <li>• run diagnostic tests</li> <li>• change the configuration of the file system, NTP, service delivery, Fabric Attach, and SNMPv3 settings for the device</li> </ul>
Graph	Use the Graph menu to view and configure EDM statistics and to produce graphs of the chassis or port statistics.
VLAN	Use the VLAN menu to view and configure VLANs, spanning tree groups (STG), MultiLink Trunks/LACP, SMLT, and SLPP.
IS-IS	Use the IS-IS menu to view and configure IS-IS, Shortest Path Bridging MAC (SPBM), statistics and ISID.
IP	Use the IP menu to view and configure IP routing functions for the system, including VRF, IP-VPN, IP-MVPN, IP, TCP/UDP, OSPF, RIP, VRRP, RSMLT, BGP, Multicast, MSDP, IGMP, PIM, SPB-PIM-GW, DHCP Relay, DHCP Snooping, ARP Inspection, Source Guard, UDP Forwarding, IS-IS, Policy.
IPv6	Use the IPv6 menu to view and configure IPv6 routing functions, including IPv6, TCP/UDP, Tunnel, OSPF, VRRP, BGP+, RSMLT, DHCP Relay, Policy, IPSec, FHS, IPv6 RIPng, IPv6 PIM, IPv6 MLD, IPv6 Mroute.
Security	Use the Security menu to view and configure policies, filters, and protocols such as RADIUS, SSH, TACACS+ and EAPoL.
QOS	Use the QOS menu to view and configure QoS mapping tables, filters, profiles, and policy statistics.
Serviceability	Use the Serviceability menu to enable and view statistics for RMON, and enable and configure sFlow and SLA Monitor.

## Menu bar

The menu bar is above the work area and consists of two rows of tabs.

- The top row displays the tabs you can open through the navigation pane. These primary tabs appear in the sequence that you open them.
- After you click a primary tab, the secondary tabs associated with it appear in the bottom row. Click a secondary tab to open it in the work area.

In both the top and bottom rows of the menu bar, if the number of tabs exceeds the available space on the desktop, the system displays left- and right-pointing arrows. Click an arrow to scroll to the required tab.

To reduce the number of tabs on the top row, you can click the X on the upper-right corner of a tab to remove it from the row. The following figure shows a sample menu bar.

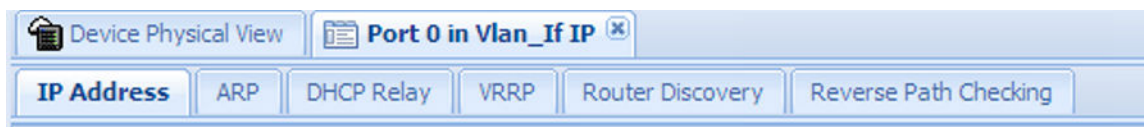


Figure 2: Menu bar

## Toolbar

The toolbar buttons provide quick access to commonly used operational commands. The buttons that appear vary depending on the tab you select. However, the Apply, Refresh, and Help buttons are on almost every screen. Other common buttons are Insert and Delete. The following list detail the common toolbar buttons.

- Apply—Use this button to execute all edits that you make.
- Refresh—Use this button to refresh all data on the screen.
- Help—Use this button to display online help that is context sensitive to the current dialog box.
- Insert—Use this button to display a secondary dialog box related to the selected tab. After you edit the configurable parameters, click the Insert button in the dialog box. This causes a new entry to appear in the dialog box of the selected tab.
- Delete—Use this button to delete a selected entry.

The following figure shows a sample toolbar.



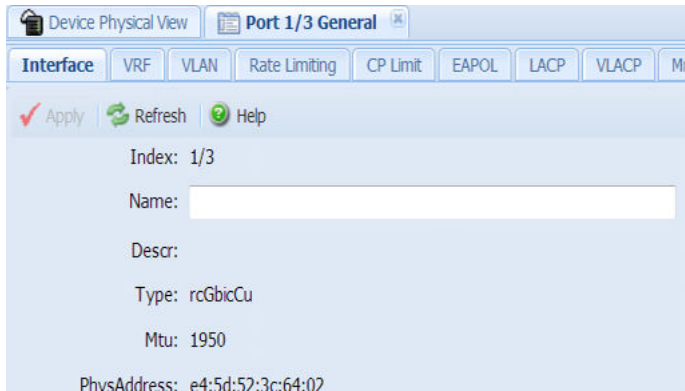
Figure 3: Toolbar

---

## Work area

The work area is the main area on the right side of the window that displays the configuration dialog boxes. Use the work area to view or configure parameters on the switch.

The following figure is a sample work area showing the work area for the Port 1/3 General, Interface tab. If you want to compare the information in two tabs, you can undock one, then open another tab. For more information about undocking a tab, see [Undocking and docking tabs](#) on page 40.



**Figure 4: Work area**

---

## EDM user session extension

If the EDM user session remains unused for a duration of ten minutes, the system displays the following message:

```
Your session will expire in about 5 minute(s). Would you like to extend
the session?
```

If you do not respond, EDM automatically ends the session with the following message: *Your session has expired.*

You can log on again if you want to continue to use EDM.

---

## TLS server for secure HTTPS

This feature enhances communications security by implementing Mocana NanoSSL to secure HTTPS server using Transport Layer Security (TLS) cryptographic protocol.

The following are the key properties of Secure Web server with TLS:

- This feature can be implemented on a maximum of only 10 concurrent client connections.



- The switch supports version TLS 1.2 and above by default. You can explicitly configure TLS 1.0 and TLS 1.1 version support using CLI or EDM.
- This feature replaces SSL 3.0 with TLS. SSL 3.0 is not supported.
- TLS server does not support RC4, DES, TDES, and MD5 based cipher suites.
- The minimum password length for the web server is 8 characters, by default. You can change this using CLI or EDM.

---

## Certificate order priority

Use the following information to understand the certificate order priority when the TLS server and switch connect.

The TLS server selects the server certificate in the following order:

1. A CA-signed certificate if the certificate is already present in the `/intflash/.cert/` folder on the switch.
2. A self-signed certificate if the certificate is already present in the `/intflash/.cert/` folder on the switch.

If the server certificates are not available, TLS server generates a new self-signed certificate on boot and uses that by default. The self-signed certificate is available in `./intflash/.cert/.ssl`. You can choose to use an online or offline CA signed certificate which will take precedence over the self-signed one.

### SSL-based self-signed certificate

Some earlier releases use the default certificate available in the `/intflash/.ssh` folder, which is the open SSL-based self-signed certificate that is named `host.cert`.

To use the Mocana stack based self-signed certificate, delete the open SSL self-signed certificate prior to upgrading your software release. The Mocana certificate offers better and stronger encryption.

If a user does not delete the `host.cert` file in the `/intflash/.ssh` folder used in earlier releases, forcefully generates a self-signed certificate automatically during upgrade or post upgrade using the command `config ssl certificate`.

If you have a subscribed CA-signed certificate renamed as `host.cert` in folder `/intflash/.ssh` in the previous release, it cannot be reused now.

To use your subscribed CA-signed certificate, upgrade with the Mocana-based self-signed certificate, and then use the digital certificates feature to install a CA-signed certificate through the online or offline method.

You cannot obtain a CA-signed certificate and rename the certificate as `host.cert`. You must use the online or offline method to obtain certificate.

# Chapter 5: EDM interface procedures

This chapter contains procedures for starting and using Enterprise Device Manager (EDM). The software is built-in to the switch, and you do not need to install additional software.

---

## Connecting to EDM

### Before you begin

- Ensure that the switch is running.
- Note the IP address of the switch.
- Ensure that you use a supported browser version.
- Ensure that you enable the web server using CLI.

### About this task

Perform this procedure to connect to EDM to configure and maintain your network through a graphical user interface.

### Procedure

1. In the address field, enter the IP address of the system using the following formats: **https://<IP\_address>** (default) or **http://<IP\_address>**.

 **Note:**

By default the Web server is configured with the secure-only option, which requires you to use HTTPS to access EDM. To access EDM using HTTP, you must disable the secure-only option.

2. In the **User Name** field, type the user name. The default is admin.
3. In the **Password** field, type a password. The default is password.
4. Click **Log On**.

For information about how to change the Log On credentials, see *Configuring Security*.

## Configuring the web management interface

### Before you begin

- The web server is enabled.

### About this task

Configure the web management interface to change the usernames and passwords for management access to the switch using a web browser.

HTTP, FTP, and TFTP server supports both IPv4 and IPv6 addresses, with no difference in functionality or configuration.

### Procedure

1. In the navigation pane, open the **Configuration > Security > Control Path** folders.
2. Click **General**.
3. Click the **Web** tab.
4. Complete the **WebUserName** and **WebUserPassword** fields to specify the user name and password for access to the web interface. You use the other fields to specify the path and file name for the web Help files and to assign the number of rows in the web display.
5. Click **Apply**.

## Web field descriptions

Use the data in the following table to use the Web tab.

Name	Description
<b>WebUserName</b>	Specifies the username from 1–20 characters. The default is admin.
<b>WebUserPassword</b>	Specifies the password from 1–32 characters. The default is password.
<b>MinimumPasswordLength</b>	Configures the minimum password length. By default, the minimum password length is 8 characters.
<b>HttpPort</b>	Specifies the HTTP port for web access. The default value is 80.
<b>HttpsPort</b>	Specifies the HTTPS port for web access. The default value is 443.
<b>SecureOnly</b>	Controls whether the secure-only option is enabled. The default is enabled.
<b>InactivityTimeout</b>	Specifies the idle time (in seconds) to wait before the EDM login session expires. The default value is 900 seconds (15 minutes).

*Table continues...*

Name	Description
<b>TlsMinimumVersion</b>	Configures the minimum version of the TLS protocol supported by the web-server. You can select from the following options: <ul style="list-style-type: none"> <li>• tlsv10 – Configures the version to TLS 1.0.</li> <li>• tlsv11 – Configures the version to TLS 1.1.</li> <li>• tlsv12 – Configures the version to TLS 1.2</li> </ul> The default is tlsv12.
<b>HelpTftp/Ftp_SourceDir</b>	Configures the TFTP or FTP directory for Help files, in one of the following formats: a.b.c.d:/  peer:/ [<dir>]. The path can use 0–256 characters. The following example paths illustrate the correct format: <ul style="list-style-type: none"> <li>• 192.0.2.1:/Help</li> <li>• 192.0.2.1:/</li> </ul>
<b>DefaultDisplayRows</b>	Configures the web server display row width between 10–100. The default is 30.
<b>LastChange</b>	Shows the last web-browser initiated configuration change.
<b>NumHits</b>	Shows the number of hits to the web server.
<b>NumAccessChecks</b>	Shows the number of access checks performed by the web server.
<b>NumAccessBlocks</b>	Shows the number of access attempts blocked by the web server.
<b>LastHostAccessBlocked</b>	Shows the IP address of the last host access blocked the web server.
<b>NumRxErrors</b>	Shows the number of receive errors the web server encounters.
<b>NumTxErrors</b>	Shows the number of transmit errors the web server encounters.
<b>NumSetRequest</b>	Shows the number of set-requests sent to the web server.

---

## Using the chassis shortcut menu

### About this task

Perform the following procedure to display the chassis shortcut menu.

### Procedure

1. In the Device Physical View, select the chassis.

2. Right-click the chassis.

---

## Chassis shortcut menu field descriptions

Use the data in the following table to use the Chassis shortcut menu.

Name	Description
<b>Edit</b>	Edits chassis parameters.
<b>Graph</b>	Graphs chassis statistics.
<b>Refresh Status</b>	Refreshes the status of the chassis and MDAs.
<b>Refresh Port Tooltips</b>	Refreshes the port tooltip data of the system. The port tooltip data contains the following variables: Slot/Port, PortName, and PortOperSpeed.

---

## Using the port shortcut menu

### About this task

Perform this procedure to display the port shortcut menu.

### Procedure

1. In the Device Physical View, select a port.
2. Right-click the selected port.

---

## Port shortcut menu field descriptions

Use the data in the following table to use the port shortcut menu.

Name	Description
<b>Edit General</b>	Configures the general options for the port.
<b>Edit IP</b>	Configures the IP options for the port.
<b>Edit IPv6</b>	Configures the IPv6 options for the port.
<b>Channelization Enable</b>	Enables channelization for the port.  Not all hardware platforms support the same port speeds or the channelization feature. For more information about feature support, see Release Notes.
<b>Channelization Disable</b>	Disables channelization for the port.

*Table continues...*

Name	Description
Graph	Displays the statistics for the port.
Enable	Enables the port.
Disable	Disables the port.

## Using a table-based tab

### About this task

Change an existing configuration using a table-based tab. You cannot edit grey-shaded fields in the table. The following procedure is an illustration on how to use a table-based tab.

#### \* Note:

You can expand the appropriate folders for any feature you configure and select a table-based tab.

### Procedure

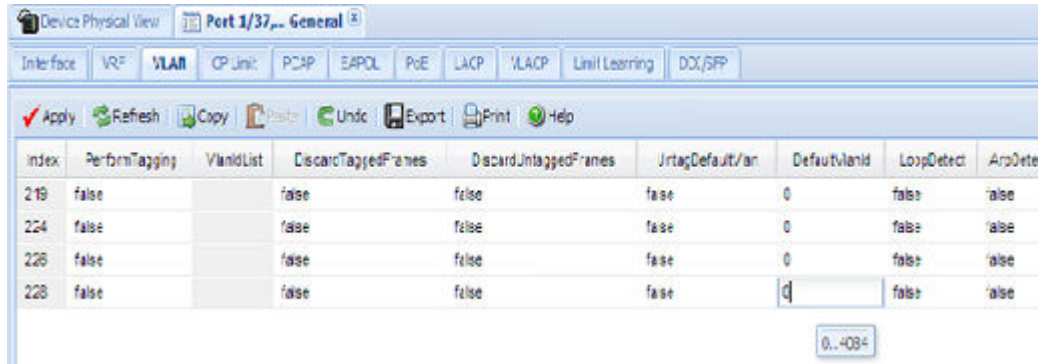
1. In the Device Physical View, select multiple ports.
2. In the navigation pane, expand the **Configuration > Edit > Port > General** folders.
3. Click the **VLAN** tab.

The system displays a table-based tab with the VLAN information.

4. Select a table-based tab.
5. Double-click a white-shaded field to edit the value.
6. Click the arrow in the list field to view the options, and then select the appropriate value.

Index	PerformTagging	VlanList	DiscardTaggedFrames	DiscardUntaggedFrames	UntagDefaultVlan	DefaultVlanId	LoopD
219	false		false	false	false	0	false
224	false		false	false	false	0	false
226	false		false	false	false	0	false
228	false		false	false	false	0	false

7. In a text-entry field, double-click, and then edit the value.



8. Click **Apply** to save the configuration changes.

---

## Monitoring multiple ports and configuration support

### About this task

You can monitor or apply the same configuration changes to more than one port by using the multiple port selection function. You can use the standard menu or the shortcut menu to edit the configuration settings for multiple ports.

#### + Tip:

A selected port shows a yellow outline around the port.

### Procedure

1. Click the **Device Physical View** tab.
2. To select multiple ports, press the `Control` key, and then click the required ports.

#### \* Note:

When you use the Enterprise Device Manager (EDM) embedded in the software, you can select a maximum of 24 ports.

---

## Opening folders and tabs

### About this task

Perform this procedure to navigate in EDM.

### Procedure

1. In the navigation pane, expand the **Configuration** folder.
2. Click the subfolder, for example, the **VLAN** folder.

3. In a folder or subfolder, click a tab to open that tab.

---

## Undocking and docking tabs

### About this task

Perform this procedure to undock a tab. You can undock tabs to have more than one tab visible at a time.

### Procedure

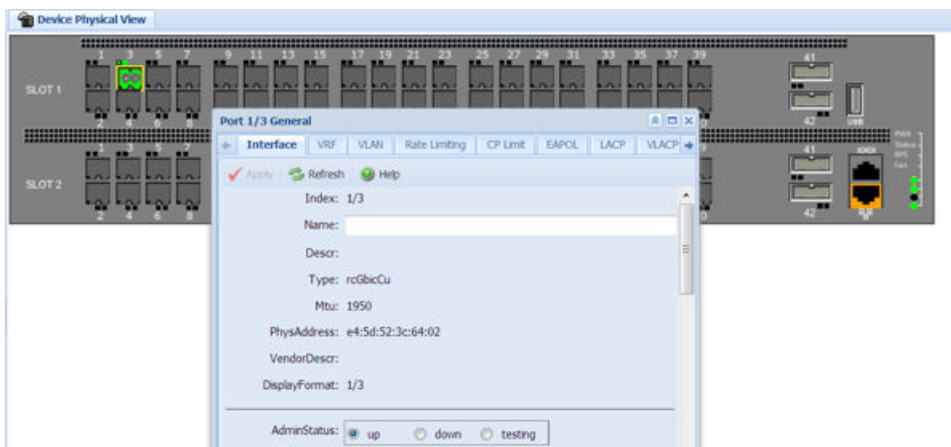
1. In the navigation pane, click a tab.
2. In the menu bar, click and drag a tab to undock it.
3. In the top right corner of the tab, click **pages** to dock the tab.


---

## Example of undocking and docking tabs

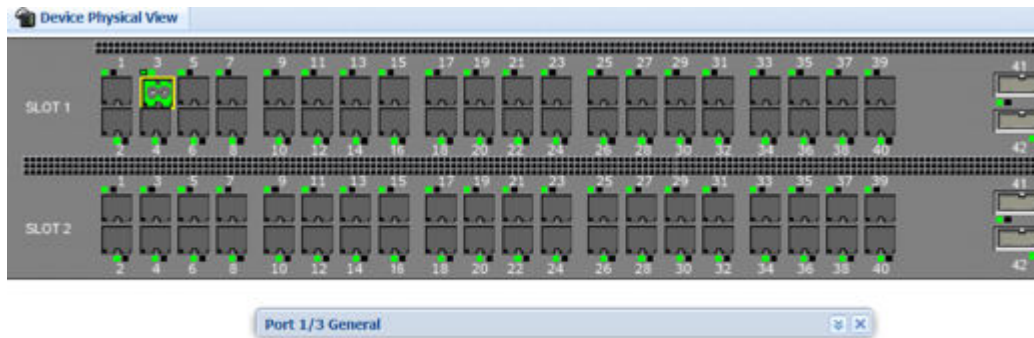
### Procedure

1. Click the **Device Physical View** tab.
2. In the Device Physical View, select a port. In this example, right-click port 3.
3. In the Port shortcut menu, click **Edit General**.
4. Click and drag the Port 1/3 General tab wherever you want on the screen as shown in the following figure.



5. To reposition the tab anywhere on the screen, click and drag the title bar.
6. To manipulate the tab, click on the buttons in the top-right of the dialog box.  

7. Click the up arrowhead to minimize the tab as shown in the following figure.





8. Click the down arrowhead to restore the tab to its original size.
9. Click the pages to dock the tab back into the menu bar.
10. Click the X to close the tab.

---

## Installing EDM help files

While the EDM GUI is bundled with the switch software, the associated EDM help files are not. To access the help files from the EDM GUI, you must install the EDM help files on a TFTP or FTP server in your network.

Use the following procedure to install the EDM help files on a TFTP or FTP server, and configure EDM to use the help files

### Procedure

1. Download the EDM help file.
2. On a TFTP or FTP server reachable from the switch, create a directory called **Help**.
  - + Tip:**  
Ensure that you configure the switch with the host user name and password if you use FTP.
  - You can name the directory anything that will help you remember its purpose.
3. Unzip the EDM help zip file into the directory created in the preceding step.
4. In the EDM navigation pane, expand the **Configuration > Security > Control Path** folders.
5. Click **General**.
6. Click **Web**.
7. In the **HelpTftp/Ftp\_SourceDir** field, enter the IP address of the file server and the path to the help files, for example, 192.0.2.15:/home/Help/.

# Chapter 6: File management in EDM

This chapter contains procedures for managing files with Enterprise Device Manager (EDM).

Use the File System tab to perform the following tasks:

- Copy a file.
- Check the amount of memory used and the number of files stored in the internal flash memory.
- Verify the name, size, and storage date of each file present in the internal flash memory.

---


## Copying files

### About this task

Perform this procedure to copy a file.

### Procedure

1. In the navigation pane, expand the **Configuration > Edit** folders.
2. Click **File System**.
3. In the **Source** field, specify the file you want to copy. Use one of the following options:
  - /intflash/<file>
  - /usb/<file>

 **Note:**

The USB option does not apply to all hardware platforms. For more information, see your hardware documentation.

  - x:x:x:x:x:x:x:<file>
  - <A.B.C.D>:<file>
4. In the **Destination** field, specify the file you want to copy. Use one of the following options:
  - /intflash/<file>
  - /usb/<file>

**\* Note:**

The USB option does not apply to all hardware platforms. For more information, see your hardware documentation.

- x:x:x:x:x:x:<file>
- <A.B.C.D>:<file>

5. In the **Action** field, click **start**.
6. Click **Apply** to start copying the files.

The system displays the results of the copy action in the Result field.

---

## Viewing file storage information

Perform this procedure to view the file storage information for the switch.

### About this task

This procedure displays the name of the storage, the number of bytes used, and the number of bytes free.

### Procedure

1. In the navigation pane, expand the **Configuration > Edit** folders.
2. Click **File System**.
3. Click the **Storage Usage** tab.

---

## Displaying internal flash files

Display information about the files on the internal flash.

**\* Note:**

This tab does not appear on all hardware platforms.

### Procedure

1. In the navigation pane, expand the **Configuration > Edit** folders.
2. Click **Chassis**.
3. Click the **Flash Files** tab.

---

## Flash Files field descriptions

Use the data in the following table to use the Flash Files tab.

Name	Description
Name	Specifies the directory name of the flash file.
Date	Specifies the creation or modification date of the flash file.
Size	Specifies the size of the flash file.

---

## Displaying USB file information

### About this task

Display information about the files on a USB flash device to view general file information.

### Procedure

1. In the navigation pane, expand the **Configuration > Edit** folders.
2. Click **Chassis**.
3. Click the **USB Files** tab.

---

## USB Files field descriptions

Use the data in the following table to use the USB Files tab.

Name	Description
Slot	Specifies the slot number.
Name	Specifies the directory name of the file.
Date	Specifies the creation or modification date of the file.
Size	Specifies the size of the file.

# Glossary

**command line interface (CLI)**

A textual user interface. When you use CLI, you respond to a prompt by typing a command. After you enter the command, you receive a system response.

**Enterprise Device Manager (EDM)**

A web-based embedded management system to support single-element management. EDM provides complete configuration management functionality for the supported devices and is supplied to the customer as embedded software in the device.

**graphical user interface (GUI)**

A graphical (rather than textual) computer interface.

**Trivial File Transfer Protocol (TFTP)**

A protocol that governs transferring files between nodes without protection against packet loss.