Extreme SLX-OS Troubleshooting Guide, 20.7.3

Supporting ExtremeRouting and ExtremeSwitching SLX 9740, SLX 9640, SLX 9540, SLX 9250, SLX 9150, Extreme 8820, Extreme 8720, and Extreme 8520

9039538-00 Rev AA
December 2025



Copyright © 2025 Extreme Networks, Inc. All rights reserved.

Legal Notice

Extreme Networks, Inc. reserves the right to make changes in specifications and other information contained in this document and its website without prior notice. The reader should in all cases consult representatives of Extreme Networks to determine whether any such changes have been made.

The hardware, firmware, software or any specifications described or referred to in this document are subject to change without notice.

Trademarks

Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries.

All other names (including any product names) mentioned in this document are the property of their respective owners and may be trademarks or registered trademarks of their respective companies/owners.

For additional information on Extreme Networks trademarks, see: https://www.extremenetworks.com/about-extreme-networks/company/legal/trademarks

Open Source Declarations

Some software files have been licensed under certain open source or third-party licenses. End-user license agreements and open source declarations can be found at: https://www.extremenetworks.com/support/policies/open-source-declaration/

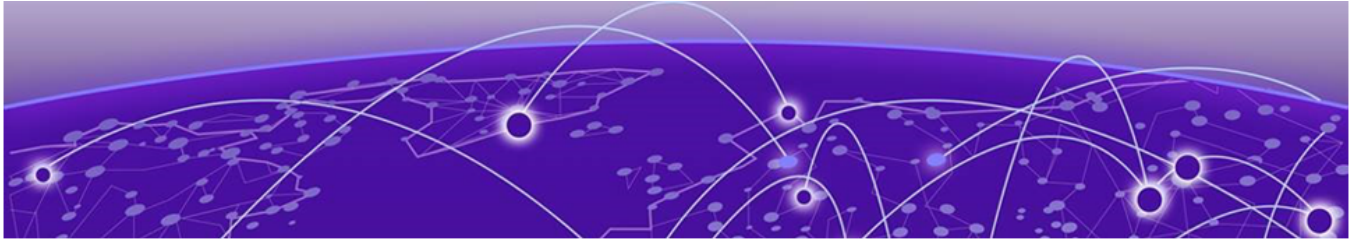


Table of Contents

Preface **5**
- Text Conventions 5
- Documentation and Training 6
  - Open Source Declarations 7
  - Training 7
- Help and Support 7
  - Subscribe to Product Announcements 8
- Send Feedback 8

About this document **9**
- What's New in This Document 9
- Supported Hardware 9
- Regarding Ethernet interfaces and chassis devices 10

Troubleshooting procedures **11**
- Troubleshooting overview 11
  - Gathering troubleshooting information 11
  - Using a troubleshooting methodology 12
  - Understanding troubleshooting hotspots 13
- Troubleshooting standard issues 16
  - Account and Password Recovery 16
  - CPU use is unexpectedly high 20
  - Heavy disk utilization 20
  - Packets are dropped in hardware 21
  - Ping fails 25
  - QoS configuration causes tail drops 26
  - SNMP MIBs report incorrect values 26
  - SNMP traps are missing 26
  - SSH or Telnet operation into the device fails 27
  - Traffic is not being forwarded 28
  - Upgrade fails 28
- Using troubleshooting and diagnostic tools 29
  - Tracing a route with the trace-l2 command 29
  - Using show commands 30
  - Using debug and system diagnostic commands 30
  - Traffic mirroring 31

Supported NTP Regions and Time Zones **32**
- Africa 33
- America 34
- Antarctica 35
- Arctic 35
- Asia 36

Atlantic....36
Australia....37
Europe....37
Indian....37
Pacific....38

Preface

Read the following topics to learn about:

- The meanings of text formats used in this document.
- Where you can find additional information and help.
- How to reach us with questions and comments.

Text Conventions

Unless otherwise noted, information in this document applies to all supported environments for the products in question. Exceptions, like command keywords associated with a specific software version, are identified in the text.

When a feature, function, or operation pertains to a specific hardware product, the product name is used. When features, functions, and operations are the same across an entire product family, such as Extreme Networks switches, the product is referred to as *the switch*.

Table 1: Notes and warnings

Icon	Notice type	Alerts you to...
	Tip	Helpful tips and notices for using the product
	Note	Useful information or instructions
	Important	Important features or instructions
	Caution	Risk of personal injury, system damage, or loss of data
	Warning	Risk of severe personal injury

Table 2: Text

Convention	Description
`screen displays`	This typeface indicates command syntax, or represents information as it is displayed on the screen.
The words *enter* and *type*	When you see the word *enter* in this guide, you must type something, and then press the Return or Enter key. Do not press the Return or Enter key when an instruction simply says *type*.
Key names	Key names are written in boldface, for example **Ctrl** or **Esc**. If you must press two or more keys simultaneously, the key names are linked with a plus sign (+). Example: Press **Ctrl**+**Alt**+**Del**
Words in italicized type	Italics emphasize a point or denote new terms at the place where they are defined in the text. Italics are also used when referring to publication titles.
NEW!	New information. In a PDF, this is searchable text.

Table 3: Command syntax

Convention	Description
bold text	Bold text indicates command names, keywords, and command options.
italic text	Italic text indicates variable content.
`[ ]`	Syntax components displayed within square brackets are optional. Default responses to system prompts are enclosed in square brackets.
`{ x | y | z }`	A choice of required parameters is enclosed in curly brackets separated by vertical bars. You must select one of the options.
x | **y**	A vertical bar separates mutually exclusive elements.
< >	Nonprinting characters, such as passwords, are enclosed in angle brackets.
...	Repeat the previous element, for example, *member*[*member*...].
\	In command examples, the backslash indicates a “soft” line break. When a backslash separates two lines of a command input, enter the entire command at the prompt without the backslash.

Documentation and Training

Find Extreme Networks product information at the following locations:

Current Product Documentation
Release Notes
Hardware and Software Compatibility for Extreme Networks products
Extreme Optics Compatibility
Other Resources such as articles, white papers, and case studies

Open Source Declarations

Some software files have been licensed under certain open source licenses. Information is available on the Open Source Declaration page.

Training

Extreme Networks offers product training courses, both online and in person, as well as specialized certifications. For details, visit the Extreme Networks Training page.

Help and Support

If you require assistance, contact Extreme Networks using one of the following methods:

Extreme Portal

Search the GTAC (Global Technical Assistance Center) knowledge base; manage support cases and service contracts; download software; and obtain product licensing, training, and certifications.

The Hub

A forum for Extreme Networks customers to connect with one another, answer questions, and share ideas and feedback. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.

Call GTAC

For immediate support: (800) 998 2408 (toll-free in U.S. and Canada) or 1 (408) 579 2800. For the support phone number in your country, visit www.extremenetworks.com/support/contact.

Before contacting Extreme Networks for technical support, have the following information ready:

- Your Extreme Networks service contract number, or serial numbers for all involved Extreme Networks products
- A description of the failure
- A description of any actions already taken to resolve the problem
- A description of your network environment (such as layout, cable type, other relevant environmental information)
- Network load at the time of trouble (if known)
- The device history (for example, if you have returned the device before, or if this is a recurring problem)
- Any related RMA (Return Material Authorization) numbers

Subscribe to Product Announcements

You can subscribe to email notifications for product and software release announcements, Field Notices, and Vulnerability Notices.

1. Go to The Hub.
2. In the list of categories, expand the **Product Announcements** list.
3. Select a product for which you would like to receive notifications.
4. Select **Subscribe**.
5. To select additional products, return to the **Product Announcements** list and repeat steps 3 and 4.

You can modify your product selections or unsubscribe at any time.

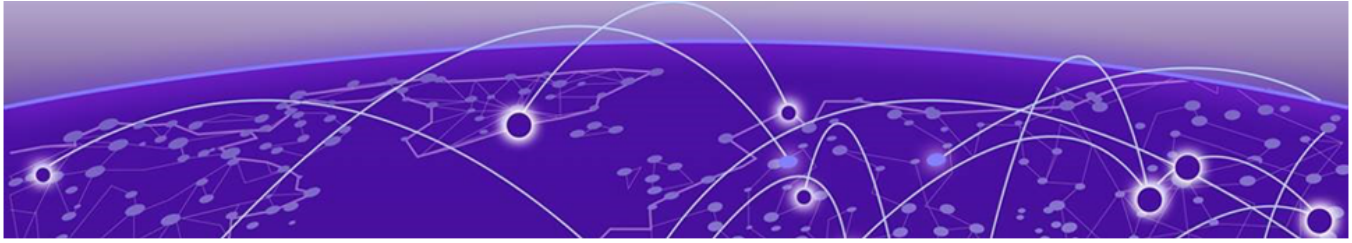
Send Feedback

The User Enablement team at Extreme Networks has made every effort to ensure that this document is accurate, complete, and easy to use. We strive to improve our documentation to help you in your work, so we want to hear from you. We welcome all feedback, but we especially want to know about:

- Content errors, or confusing or conflicting information.
- Improvements that would help you find relevant information.
- Broken links or usability issues.

To send feedback, email us at Product-Documentation@extremenetworks.com.

Provide as much detail as possible including the publication title, topic heading, and page number (if applicable), along with your comments and suggestions for improvement.



About this document

What's New in This Document on page 9
Supported Hardware on page 9
Regarding Ethernet interfaces and chassis devices on page 10

What's New in This Document

This document is released with the SLX-OS 20.7.3 software release. No changes were made to this document for this version.

For additional information, refer to the *Extreme SLX-OS Release Notes* for this version.

Supported Hardware

For instances in which a topic or part of a topic applies to some devices but not to others, the topic specifically identifies the devices.

SLX-OS 20.7.3 supports the following hardware platforms.

- Extreme 8820
- Extreme 8720
- Extreme 8520
- ExtremeSwitching SLX 9540
- ExtremeSwitching SLX 9250
- ExtremeSwitching SLX 9150
- ExtremeRouting SLX 9740
- ExtremeRouting SLX 9640

Note

All configurations and software features that are applicable to SLX 9150 and SLX 9250 devices are also applicable for the Extreme 8520 and Extreme 8720 devices respectively.

All configurations and software features that are applicable to SLX 9740 devices are also applicable for the Extreme 8820 devices.

The "Measured Boot with Remote Attestation" feature is only applicable to the Extreme 8520, Extreme 8720, and Extreme 8820 devices. It is not supported on the SLX 9150 and SLX 9250 devices.

Note
Although many software and hardware configurations are tested and supported for this release, documenting all possible configurations and scenarios is beyond this document's scope.

For information about other releases, see the documentation for those releases.

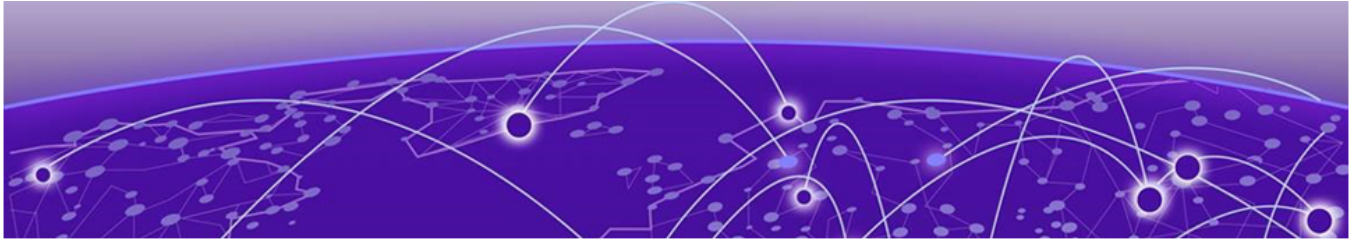
Regarding Ethernet interfaces and chassis devices

The current SLX-OS version does not support any multi-slot (chassis) devices.

The current SLX-OS version does not support any multi-slot (chassis) devices.

However, the Ethernet interface configuration and output *slot/port* examples in this document may appear as either 0/x or n/x, where "n" and "x" are integers greater than 0.

For all currently supported devices, specify **0** for the slot number.



Troubleshooting procedures

Troubleshooting overview on page 11
Troubleshooting standard issues on page 16
Using troubleshooting and diagnostic tools on page 29

Troubleshooting overview

This section provides tips and procedures for troubleshooting issues that may occur while operating a device running Extreme SLX-OS.

It also introduces some of the common troubleshooting tools.

Gathering troubleshooting information

The first step in any successful troubleshooting is to gather the appropriate information (including *supportSave* data).

Capturing supportSave data

Capturing *supportSave* data is key to successful troubleshooting.

The **copy support** command not only runs diagnostic commands, but also gathers core dumps, trace files, and other relevant data. In the same action, the command also copies all this information to a remote host. Once on the remote host, your device provider can proceed to analyze the problem. Meanwhile, your device can be returned to production with minimal downtime.

To capture supportSave data, perform the following steps:

1. Log in to the device.
2. In privileged EXEC mode, enter the **copy support** command to capture the supportSave data.

   Note
   The **copy support** command has options to copy the supportSave files to a remote server using FTP or SCP, or you can save to a local USB device. You can use the command in a single command line, or in interactive mode.

3. If your run of the **copy support** command gets interrupted by a spontaneous reboot, enter the **copy support** command again, after the reboot.

   Submit both runs to your device provider.

The following example uses the single command line mode to copy the supportSave files to a remote host using FTP.

```
device# copy support ftp host 10.38.33.131 user admin directory /home/admin/support
Password: *****
```

The following example uses the interactive form of the command and FTP:

```
device# copy support-interactive
Server Name or IP Address: 10.38.33.131
Protocol (ftp, scp): ftp
User: admin
Password: *****
Directory:/home/admin/support
```

Using information resources

The following information is helpful for incident investigation and resolution when you contact your device-support provider:

- A network diagram and topology information
- A record of the steps and events leading to the incident
- Lists of applications, management agents, and scripts running at the time of the incident
- supportSave files
- Output from the **show media** command if the issue is related to SFP transceivers
- Outputs from any commands run while attempting to troubleshoot the problem yourself
- Any network traces captured using Wireshark software or other network analyzer.
- Terminal Access Controller Access-Control System (TACACS) server version if the issue is related to TACACS.

Using a troubleshooting methodology

Once all relevant information is collected, success is improved significantly with a sound troubleshooting approach.

This section outlines a methodology for troubleshooting issues. It introduces steps that you might consider using, depending on the issue in question.

1. Check whether the device has all of the relevant licenses.
2. After adding or modifying a POD or port-upgrade license, re-enable the ports.
3. Verify the topology and switch configuration as conveyed by the switch
4. Enter the **copy support** command.
5. Run other relevant show commands (for example, **show logging raslog**) to look for clues or triggers of the reported failure.
6. Check the utilization of various resources.
   a. Enter the **show process cpu** command to determine CPU use.
   b. Enter the **show process memory** command to determine memory use.

c. Enter the **show mac-address-table count** command to determine the number of MAC addresses used.
d. Enter the **show media** command to investigate any optics issues.

7. Conduct data-path fabric continuity tests:
   a. Issue pings from and to the end-stations or devices.
   b. Check the counters in the output of the **show interface** command to detect if packets are coming in or are being dropped as errors.
   c. Verify that optics used are certified. Enter the **show media interface** command and verify that the Vendor name field shows BROCADE or EXTREME.
   d. Verify that the MAC address table learns the MAC addresses.
   e. Check whether LLDP reports neighbors.
8. 

   Caution
   The following step affects configuration and should be used with care.

   To track certain flows within the network, use permit ACLs and monitor the hit increments.

Understanding troubleshooting hotspots

This section provides background information and guidance related to features where problems have been reported. With this guidance, you should be able to avoid many potential problems.

ACL limits issues

If you keep within the supported limits of ACL usage as shown in the table below, you are unlikely to run into system limits issues. ACLs should instantiate quickly and correctly.

The following software limits apply to ACL names:

- An ACL name must be unique, 1 through 63 characters long, and must begin with a–z, A–Z or 0–9. You can also use underscore (_) or hyphen (-) in an ACL name, but not as the first character.
- Rule sequence numbers can range from 1 through 65535.

The following table displays the maximum numbers of ACLs and ACL rules supported for each device.

Table 4: ACL and rule software limits

ACL type (standard and extended)	Maximum ACLs per type per device	Maximum rules per ACL	Maximum total rules per ACL type
Layer 2	2048	2038	102400
IPv4	2048	2048	102400
IPv6	2048	2048	102400

As you approach or exceed combinations of these limits, you might encounter slow instantiation of ACL rules.

Delays of several minutes can occur in the instantiation of ACL rules and counters if the number of ACLs or VLANs is excessive.

To display the hardware instantiation status (Active/Partial/In Progress/Inactive), run the **`show access-list`** command.

Avoiding oversubscription

Under certain congestion conditions, you may observe incrementing packet drops representing "tail-drops" in the output of the **`show interface stats brief`** command.

```
device# show interface stats brief

                Packets            Error                Discards      CRC
Interface  rx       tx          rx       tx          rx       tx          rx
=========  ===============    ===============    ===============    ===
Po 1       138641  4297936    0        0          0        0          0
Po 2       0        0         0        0          0        0          0
Lo 1       0        0         0        0          0        0          0
Lo 100     0        0         0        0          0        0          0
Eth 0/1    0        0         0        0          0        0          0
Eth 0/2    0        0         0        0          0        0          0
```

In such conditions, you must first identify the bottleneck, and then take action to mitigate the congestion.

Identifying the congestion bottleneck

To identify the network bottleneck, enter the **`show interface`** command at various locations, and identify interfaces with incrementing TX and RX discards.

Depending upon the TX or RX discards, the congestion could be anywhere downstream.

Congestion mitigation

Try the following actions to mitigate congestion.

Note
For further details about congestion control, see the *Extreme SLX-OS QoS and Traffic Management Configuration Guide*.

- Increase bottleneck bandwidth.
  - Add more links to the LAG and ECMP paths.
  - Use higher-speed interfaces.
- Implement flow control on the bottleneck and on neighboring devices.

  Note
  Flow control can increase the number of discards.
- Implement QoS congestion management schemes.
  - Classify, mark, and prioritize critical traffic.
  - Modify scheduling schemes.
  - Random Early Detection (RED)

For the flow control solution, enable flow control either on the ports receiving the traffic from end-devices (servers or personal computers) and the connected end-device itself, or enable flow control on the port-channel as shown in the following example.

```
device(conf-if-eth-0/24)# interface port-channel 100
device(config-Port-channel-100)# qos flowcontrol tx on rx on
```

Once flow control is enabled, enter the **`show interface stats brief`** command again and check the output. It should no longer be reporting packet drops. If the packet drops continue or the ingress rate is considerably lower than expected, contact your device support provider for further investigation.

Note
For TCP sessions with low latency, expect small discards.

Licensing

When a licensed feature does not work, one likely cause is a license issue.

For license-troubleshooting issues, refer to the *Extreme SLX-OS Software Licensing Guide*. Verify that:

- You have a license for the feature.
- The license is correctly installed.

Load balancing distribution

Understanding issues related to load balancing requires some basic knowledge of the criteria used by load balancing algorithms.

The following table provides details for each feature that provides load balancing.

Table 5: Load balancing algorithms

Feature	Algorithm
Port-channels	Provides adaptive load balancing based on up to seven criteria (7-tuple), depending upon what fields are available in the frame.
Trunk	Provides equal packet load balancing (round-robin) among member links.

Under multiple port-channel hops, if confronted with both underutilized and overloaded interfaces, try changing the hashing scheme on one hop to avoid such traffic polarization.

Selecting the MTU

To avoid incompatible adjacencies among network devices, make sure that the maximum transmission unit (MTU) is identical on all network devices.

Some protocols use MTU information to determine:

- Preferred routes
- Protocol-packet size (OSPF, for example)

To allow room for Ethernet headers, make sure that the Ethernet MTU is larger than the IP MTU.

Troubleshooting standard issues

This section describes some potential problems you may encounter and suggestions on how to investigate or resolve each issue.

If these steps do not lead to resolution of the problem, refer to Help and Support on page 7.

Account and Password Recovery

Use these procedures to recover access to your device when normal access to the admin account has been lost.

Caution
Because of the complexity of these procedures, we recommend that you contact support for guidance, especially for recovering the root password. The recovery steps must be followed exactly as presented below. Any variation in the procedure might cause unpredictable results.

Recover the admin password from the root account

If you lose access to the SLX-OS admin account but you have access to the root account for the device, you can recover the password.

Perform the following steps to reset the admin password from the root account.

1. Open a session to access the device.
2. Log in as root.
3. Start the SLX-OS CLI.

```
[root@device]# slxcli
device#
```

4. Access global configuration mode.

```
device# configure terminal
```

5. Reset the admin password.

```
device(config)# username admin password password
```

In this example, the admin password is reset to the default value of `password`.

You can now use the admin account to manage the admin and user passwords by using normal password-management procedures.

Root account and password recovery

By default, the root account on the virtual machine (VM) is disabled. To log into root, you can log into the SLX-OS CLI and enable the root account from global configuration mode by using **`root enable`** command. In rare cases, SLX-OS CLI may not be available to enable the root account.

The ability to enable the root account and recover the root credentials (password) depends on the uboot environment variable. When the variable is set, it executes the root recovery logic based on the parameter set. The variable is not preserved across reboot. Every time a reboot occurs, the root account is disabled by default and this variable has to be set again to enable it unless the root account was not enabled from global configuration mode.

The root account access availability determines the method for password recovery:

- When the root account is disabled and the SLX-OS CLI is not available, you must recover the root login account. The password is also recovered.
  - Recover the root login account on page 18

Note

- For SLX 9540 running SLX-OS 20.1.x and lower, use the steps described in Recover root loging when shell prompt is available. The outputs and steps listed in the topic Recover root login when ONIE is available are not applicable in this case.
- For SLX 9540 running version SLX-OS 20.2.x and higher and all other SLX platforms, such as Extreme 8720, use the steps described in Recover root login when ONIE is available for recovering the root password.

- When the root account is enabled but the root password is not available, perform the relevant task:
  - Recover the root password when shell prompt is available on page 19
  - Recover the root password when ONIE is available on page 20

Note

The default password for the root account on the VM is `fibranne`.

Recover the root login account

If the root account is disabled and SLX-OS CLI is not available, recover the root login account.

Note

These instructions are for all devices except SLX 9540 running SLX-OS 20.1.x and below versions.

For instructions to restore root login/password on SLX 9540 running SLX-OS 20.1.x and below, see Recover the root password when shell prompt is available on page 19.

1. Enter the **reboot** command.
2. Select and enter the ONIE option.
3. Select and enter the ONIE: Rescue option.
4. Define the root login for the root recover environment variable.

```
ONIE:/ # bootenv VM_Root_Recover RootLogin
```

5. Enter the reboot command.

```
ONIE:/ # reboot
ONIE:/ # discover: Rescue mode detected. No discover stopped
Stopping: dropbear ssh daemon... done
```

   The root account is now enabled. You can log in with the default password.
6. If the SLX-OS CLI is available, you can recover the root account by using the SLX-OS CLI **root enable** command.

Recover the root password when shell prompt is available

If you forgot the password for the VM root account and when *shell prompt* is available, you can recover the default password.

Note

To perform the recovery process, you will need access to the shell prompt.

The *shell prompt* is only available in SLX 9540 when the platform is running version SLX-OS 20.1.x and below.

For VM root password recovery, perform the following steps.

1. Reboot the device.

```
# reboot
Press Esc during reboot.
Hit ESC to stop autoboot:  0
FPGA f6000720 -> 0x12

1) Start system.
2) Recover password.
3) Enter command shell.

Option?
```

2. Choose option 3 to access the uboot prompt.

```
Option? 3
=>
```

3. Define the root password value for the root recovery environment variable.

```
=> bootenv VM_Root_Recover RootPasswd
=>
```

This step sets the VM_Root_Recover variable with the RootPasswd value.

4. Save the variable to flash memory.

```
=> saveenv
Saving Environment to SPI Flash...
SF: Detected W25Q128BV @ 0:0 with page size 256 Bytes, erase size 64 KiB, 32 KiB, 4
KiB, total 16 MiB
Erasing SPI flash...Writing to SPI flash...
Erasing SPI flash...Writing to SPI flash...done
=>
```

5. Reboot the device.

```
=> boot
6912784 bytes read in 152 ms (43.4 MiB/s)
Valid Boot Flag
Setup Size = 0x00004400
Magic signature found
Using boot protocol version 2.0c
Linux kernel version 3.14.17 (raop@hq1-ub-ecbld-373) #1 SMP Thu Jul 7 19:43:15 UTC 2016
```

The root account is now enabled. You can log in with the default `fibranne` password.

Recover the root password when ONIE is available

If you forgot the password for the VM root account and ONIE mode is available, you can recover the default password.

Note
ONIE is available for all SLX devices, except for SLX 9540 running SLX-OS version 20.1.x and below.

1. Enter the **reboot** command.
2. Select and enter the **ONIE** option.
3. Select and enter the **ONIE: Rescue** option.
4. Define the root login value for the root recover environment variable.

```
ONIE:/ # bootenv VM_Root_Recover RootPasswd
```

5. Enter the **reboot** command.

```
ONIE:/ # reboot
ONIE:/ # discover: Rescue mode detected. No discover stopped.
Stopping: dropbear ssh daemon... done.
```

The root account is now enabled. You can log in with the default `fibranne` password.

CPU use is unexpectedly high

Unexpectedly high CPU use is usually the result of a process consuming a large percentage of available CPU cycles.

If you suspect high CPU use, complete the following steps.

1. In privileged EXEC mode, enter the **show process cpu** command to determine which process is causing the high CPU reading.
2. Shut down the corresponding interface or delete the configuration suspected of causing the high CPU use.

You might also find the following Linux commands helpful for locating high CPU usage. Run them for every VRF.

- **tcpdump any**
- **top**

Heavy disk utilization

To check disk utilization enter the **show support** command.

To reduce disk utilization, try running the **clear support** command, followed again by **dir**.

From the Linux shell, the **show support** command should also be helpful.

Packets are dropped in hardware

This section discusses how to troubleshoot problems in which loss of packets occurs in all traffic, on specific traffic flows, in specific types of traffic, consistently, or intermittently.

Dropped packets could occur for many reasons, including the following:

- High latency in an end device.
- Broken data path.
- Noise on an optical line caused by too many CRC errors, packet errors, or NIC interoperability errors.

Verifying packets dropped because of high-latency end device

Packets can sometimes be dropped because of buffer overrun within the network caused by end devices taking longer to respond than expected.

For example, an overloaded disk array can cause such latency, as can a host that does not process data as quickly as expected. Devices that stop receiving data for an extended period of time can cause excessive latency.

The ultimate solution to these problems is to fix the end device itself. However, some adjustments to the device and network configuration can help to reduce the problem.

To detect and relieve congestion and dropped packets resulting from latency in end devices, perform the following steps:

1. Enter the **`show lldp neighbors detail`** command to check under "DCBX TLVs" that the end device is DCB-ready and confirm that the end device is also advertising its DCB capabilities.

```
device# show lldp neighbors detail
Neighbors for Interface Eth 0/11

MANDATORY TLVs
===============
Local Interface: Eth 0/11  (Local Interface MAC: 609c.9fde.2621)
Remote Interface: Ethernet 0/1 (Remote Interface MAC: d884.66ea.4b17)
Dead Interval: 120 secs
Remaining Life : 91 secs
Chassis ID: d884.66ea.4b14
LLDP PDU Transmitted: 2153  Received: 2153

OPTIONAL TLVs
==============
Port Interface Description: Eth 0/1
System Name: R60-SN

DCBX TLVs
===========
Version : CEE
DCBX Ctrl OperVersion: 0  MaxVersion: 0  SeqNo: 2 AckNo: 2
DCBX ETS OperVersion: 0  MaxVersion: 0  Enabled: 1  Willing: 0 Error: 0
Enhanced Transmission Selection (ETS)
  Priority-Group ID Map:
    Priority : 0  1  2  3  4  5  6  7
    Group ID : 0  0  0  0  0  0  0  0
  Group ID Bandwidth Map:
```

```
    Group ID  :   0   1   2   3   4   5   6   7
    Percentage:   0   0   0   0   0   0   0   0
    Number of Traffic Classes supported: 8
DCBX PFC OperVersion: 0  MaxVersion: 0  Enabled: 1  Willing: 0 Error: 0
Priority-based Flow Control (PFC)
     Enabled Priorities: none
     Number of Traffic Class PFC supported: 8
LAN LLS OperVersion: 0  MaxVersion: 0  Enabled: 1  Willing: 0 Error: 0
LAN  Logic Link Status: Up
```

2. Enter the **show qos flowcontrol interface** command to check for pause frames.
3. Enter the **show qos interface** command to check the QoS configuration.

```
SLX# show qos interface ethernet 0/2
[Note: CoS = Class of Service, TC = Traffic Class, DP = Drop Precedence]
Interface Ethernet 0/2
  Provisioning Mode: none
  Default TC: 0

  CoS-to-TC Map: default
             In-CoS: 0  1  2  3  4  5  6  7
        -------------------------------------
             Out-TC: 0  1  2  3  4  5  6  7
             Out-DP: 0  0  0  0  0  0  0  0

  TC-to-CoS Map: default
              In-TC: 0  1  2  3  4  5  6  7
        -------------------------------------
        Out-CoS(DP=0): 0  1  2  3  4  5  6  7
        Out-CoS(DP=1): 0  1  2  3  4  5  6  7
        Out-CoS(DP=2): 0  1  2  3  4  5  6  7
        Out-CoS(DP=3): 0  1  2  3  4  5  6  7

  DSCP Mutation Map: default (DSCP = d1d2)
        d1 :  d2 0  1  2  3  4  5  6  7  8  9
        -------------------------------------
         0 :    00 01 02 03 04 05 06 07 08 09
         1 :    10 11 12 13 14 15 16 17 18 19
         2 :    20 21 22 23 24 25 26 27 28 29
         3 :    30 31 32 33 34 35 36 37 38 39
         4 :    40 41 42 43 44 45 46 47 48 49
         5 :    50 51 52 53 54 55 56 57 58 59
         6 :    60 61 62 63

  DSCP-to-TC Map: default (x/y: TC = x, DP = y, DSCP = d1d2)
        d1 :  d2  0   1   2   3   4   5   6   7   8   9
        -------------------------------------------------
         0 :     0/0 0/0 0/0 0/0 0/0 0/0 0/0 0/0 1/0 1/0
         1 :     1/0 1/0 1/0 1/0 1/0 1/0 2/0 2/0 2/0 2/0
         2 :     2/0 2/0 2/0 2/0 3/0 3/0 3/0 3/0 3/0 3/0
         3 :     3/0 3/0 4/0 4/0 4/0 4/0 4/0 4/0 4/0 4/0
         4 :     5/0 5/0 5/0 5/0 5/0 5/0 5/0 5/0 6/0 6/0
         5 :     6/0 6/0 6/0 6/0 6/0 6/0 7/0 7/0 7/0 7/0
         6 :     7/0 7/0 7/0 7/0

  DSCP-to-CoS Map: default (DSCP = d1d2)
        d1 :  d2 0  1  2  3  4  5  6  7  8  9
        -------------------------------------
         0 :    00 00 00 00 00 00 00 00 01 01
         1 :    01 01 01 01 01 01 02 02 02 02
         2 :    02 02 02 02 03 03 03 03 03 03
         3 :    03 03 04 04 04 04 04 04 04 04
         4 :    05 05 05 05 05 05 05 05 06 06
         5 :    06 06 06 06 06 06 07 07 07 07
         6 :    07 07 07 07
```

```
  Per Traffic-Class Tail Drop Threshold (bytes)
             TC:      0      1      2      3      4      5      6      7
      ------------------------------------------------------------------
      Threshold:      0      0      0      0      0      0      0      0

  Flow control mode Off

  Traffic Class Scheduler configured for 8 Strict Priority queues
```

4. (If needed) Reconfigure QoS.

   For detailed information, refer to the QoS sections of the *Extreme SLX-OS Layer 2 Switching Configuration Guide* and the *Extreme SLX-OS Layer 3 Routing Configuration Guide*.

Verifying the data path

This procedure checks whether network continuity might be the reason for dropped packets.

1. Enter the **ping** command to test for a complete path to the end device

```
device# ping 10.24.81.2
PING 10.24.81.2 (10.24.81.2): 56 octets data
64 octets from 10.24.81.2: icmp_seq=0 ttl=128 time=9.4 ms
64 octets from 10.24.81.2: icmp_seq=1 ttl=128 time=0.3 ms
64 octets from 10.24.81.2: icmp_seq=2 ttl=128 time=0.3 ms
64 octets from 10.24.81.2: icmp_seq=3 ttl=128 time=0.3 ms
64 octets from 10.24.81.2: icmp_seq=4 ttl=128 time=0.3 ms
--- 10.24.81.2 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.3/2.1/9.4 ms
```

2. Enter the **show interface** command to display whether packets are coming in or are dropped as errors.

```
device# show interface eth 0/1
Ethernet 0/1 is admin down, line protocol is down (admin down)
Hardware is Ethernet, address is 0000.aaaa.bbbb
    Current address is 0000.aaaa.bbbb
Pluggable media present
Interface index (ifindex) is 203431936 (0xc202000)
MTU 1548 bytes
10G Interface
LineSpeed Actual     : Nil
LineSpeed Configured : Auto, Duplex: Full
Priority Tag disable
Forward LACP PDU: Disable
Route Only: Disabled
Tag-type: 0x8100
Last clearing of show interface counters: 11:18:42
Queueing strategy: fifo
Receive Statistics:
    0 packets, 0 bytes
    Unicasts: 0, Multicasts: 0, Broadcasts: 0
    64-byte pkts: 0, Over 64-byte pkts: 0, Over 127-byte pkts: 0
    Over 255-byte pkts: 0, Over 511-byte pkts: 0, Over 1023-byte pkts: 0
    Over 1518-byte pkts(Jumbo): 0
    Runts: 0, Jabbers: 0, CRC: 0, Overruns: 0
    Errors: 0, Discards: 0
Transmit Statistics:
    0 packets, 0 bytes
    Unicasts: 0, Multicasts: 0, Broadcasts: 0
    Underruns: 0
```

```
    Errors: 0, Discards: 0
Rate info:
    Input 0.000000 Mbits/sec, 0 packets/sec, 0.00% of line-rate
    Output 0.000000 Mbits/sec, 0 packets/sec, 0.00% of line-rate
Route-Only Packets Dropped: 0
Time since last interface status change: 11:18:42
```

3. Enter the **show media interface** command to check that the optics used are Brocade- or Extreme Networks-certified and that the Power fields are not zero.

```
device# show media interface ethernet 0/1
  Interface      Ethernet 0/1
  Identifier     3    SFP
  Connector      7    LC
  Transceiver           0000000000000010 10_GB/s
  Name           sw
  Encoding       6
  Baud Rate      103 (units 100 megabaud)
  Length 9u      0   (units km)
  Length 9u      0   (units 100 meters)
  Length 50u     8   (units 10 meters)
  Length 62.5u   3   (units 10 meters)
  Length Cu      0   (units 1 meter)
  Vendor Name    BROCADE
  Vendor OUI     00:05:1e
  Vendor PN      57-0000075-01    (10GE SR SFP+)
  Vendor Rev     A
  Wavelength     850 (units nm)
  Options        001a
  BR Max         0
  BR Min         0
  Serial No      AAF313060000MV6
  Date Code      130206
  Optical Monitor Yes
  Temperature    20 Centigrade
  Voltage        3286.2  (mVolts)
  Current        0.278  (mAmps)
  TX Power       13.3  (uWatts) / -18.761 (dBm)
  RX Power       2.7  (uWatts)
```



Note
Some devices do not display TX Power.

4. Enter the **show arp vrf** command.
5. Enter the **show mac-address-table** command to verify that the MAC address table learns new values.

   The new MAC address should appear here.
6. Enter the **show lldp neighbors** command to verify that LLDP reports all neighbors.

   If the output does not show all neighbors, contact your device support provider.
7. Enter the **show mac-address-table** command to detect whether MAC addresses learned from other network devices are present.

   Enter this command on other network devices to ensure that those devices can detect this MAC address.

Checking for noise on an optical line

Excessive noise on an optical line can result in dropped packets because of excessive CRC errors, NIC interoperability errors, or other conditions.

1. Enter the **show interface** command and check the output for CRC errors or TX discards.

```
device# show interface eth 0/1
Ethernet 0/1 is admin down, line protocol is down (admin down)
Hardware is Ethernet, address is 0000.aaaa.bbbb
    Current address is 0000.aaaa.bbbb
Pluggable media present
Interface index (ifindex) is 203431936 (0xc202000)
MTU 1548 bytes
10G Interface
LineSpeed Actual     : Nil
LineSpeed Configured : Auto, Duplex: Full
Priority Tag disable
Forward LACP PDU: Disable
Route Only: Disabled
Tag-type: 0x8100
Last clearing of show interface counters: 11:18:42
Queueing strategy: fifo
Receive Statistics:
    0 packets, 0 bytes
    Unicasts: 0, Multicasts: 0, Broadcasts: 0
    64-byte pkts: 0, Over 64-byte pkts: 0, Over 127-byte pkts: 0
    Over 255-byte pkts: 0, Over 511-byte pkts: 0, Over 1023-byte pkts: 0
    Over 1518-byte pkts(Jumbo): 0
    Runts: 0, Jabbers: 0, CRC: 0, Overruns: 0
    Errors: 0, Discards: 0
Transmit Statistics:
    0 packets, 0 bytes
    Unicasts: 0, Multicasts: 0, Broadcasts: 0
    Underruns: 0
    Errors: 0, Discards: 0
Rate info:
    Input 0.000000 Mbits/sec, 0 packets/sec, 0.00% of line-rate
    Output 0.000000 Mbits/sec, 0 packets/sec, 0.00% of line-rate
Route-Only Packets Dropped: 0
Time since last interface status change: 11:18:42
```

2. If errors are reported in the previous step, check the SFP transceiver and cable on the local switch and on the peer switch at the other end of the cable.
   a. Enter the **show media interface** command on each device and check the Vendor Name field to check that the optics are Brocade- or Extreme Networks-certified.
   b. Try replacing the SFP transceiver.
   c. Try replacing the cable.
3. If needed, enter the **show media optical-monitoring interface ethernet** command.

Ping fails

If pings do not successfully traverse the device, try the following operations.

1. Trace the packet flow and check whether ARP or ICMP packets are getting dropped.

2. Trace which direction is failing by using interface statistics.
3. Locate the device that is dropping the packets.
4. Look for any error counters incrementing on that device.
5. Check the MAC address table to determine whether the MAC addresses are learned on the correct port or port-channel:
   a. Enter the **show ip route** command, which will indicate what MAC address to look for.
   b. Enter the **show arp vrf** command.
   c. Enter the **show mac-address-table** command to verify that the MAC address table learns new values.

QoS configuration causes tail drops

Tail-drop queueing is the most basic form of congestion control. Normal operation is first-in, first-out (FIFO) until all buffers are exhausted. After that, new frames are dropped.

To monitor and configure tail drops, refer to the *Extreme SLX-OS Command Reference* topics for the following commands:

- **show interface stats brief**
- **show qos rx-queue**
- **show qos tx-queue**
- **qos rx-queue limit**
- **qos tx-queue limit**

SNMP MIBs report incorrect values

If SNMP MIBs report incorrect values, complete the following steps.

1. Ensure you are using a supported MIB browser.
2. Ensure that the issue is seen consistently.
3. Ensure that the SNMP configuration is correct.
4. If the MIB browser is supported, the SNMP configuration is correct, and you still see the issue consistently, contact your device support provider.

SNMP traps are missing

If SNMP traps are missing, complete the following procedure.

1. Ensure that the correct SNMP configuration is enabled. For details, see the “SNMP” section of the *Extreme SLX-OS Management Configuration Guide*.
2. To ensure that the trap being considered is supported, see the *Extreme SLX-OS MIB Reference*.
3. Ensure that the SNMP trap or inform receiver is reachable.
4. If the problem persists, contact your device support provider.

SSH or Telnet operation into the device fails

Assuming a correct IP address and correct login credentials, failure to access the device using SSH or Telnet could be for one of the following reasons:

- SSH or Telnet is disabled. (Verify by entering **show telnet server status** or **show ssh server status**.)
- The management port is down.
- Access to the management interface is denied by an ACL.
- The device CPU is overloaded.

Verifying the status of the management port

1. On the system console, enter the **show system** command to check the status of the management port.

```
device# show system
Stack MAC                     : b8:25:62:00:00:00

  -- UNIT 0 --
Unit Name                     : SLX
Up Time                       : up 17 days
Current Time                  : 11:54:11 GMT
SLX-OS Version                : 20.1.1
Jumbo Capable                 : yes
Burned In MAC                 : HWaddr
Management IP                 : 198.51.100.0
Management Port Status        : DOWN

  -- Power Supplies --
PS1 is faulty
PS2 is OK

  -- Fan Status --
Fan 1 is Ok, speed is 17945 RPM
Fan 2 is Ok, speed is 18125 RPM
Fan 3 is Ok, speed is 17945 RPM
Fan 4 is Ok, speed is 18125 RPM
Fan 5 is Ok, speed is 18125 RPM
```

2. If the status of the management port is DOWN, enter the **interface management** command to configure the management port correctly. Refer to the "Ethernet management interface" section of the *Extreme SLX-OS Management Configuration Guide*.
3. If the problem persists, contact your device support provider.

Checking for a deny ACL

On the system console, enter the **show running-config interface management** command and check the output to determine whether an ACL is denying access to the management port.

Checking for overloaded CPU

An overloaded device CPU can prevent SSH or Telnet access.

See CPU use is unexpectedly high on page 20.

Traffic is not being forwarded

If the traffic is not being forwarded, you may need to examine packets in transit across links to understand the traffic pattern on a specific port.

On most platforms, you can use insight interfaces to mirror traffic to an interface associated with third-party VM. For details, refer to the "Guest OS for TPVM" > "Insight interface and TPVM" section of the *Extreme SLX-OS Management Configuration Guide*.

Upgrade fails

If firmware upgrade fails, troubleshooting varies if the failure was before or after device reload.

Upgrade failure prior to device reload

Perform these steps if upgrade fails prior to device reload.

1. Examine your installation details:
   - Verify the command arguments and the upgrade path options.
   - Is there a requirement to install intermediate firmware before installing the desired firmware?
   - Is there a command option requirement?
2. Examine if the build downloaded correctly—by comparing **`md5sum`** for the downloaded `*.tar` file with the source.
3. Redo your extraction of the `*.tar` file, preferably under Linux.

   Note
   If you need to extract the `*.tar` file unders MS Windows, use the 7-Zip shareware utility.

4. Perform the upgrade.

   Note
   If the same failure occurs, contact your device support provider.

Upgrade failure during device reload

Perform these steps if upgrade fails during device reload.

1. Prepare a logged serial port connection to the device.

   Note
   This connection might be required by your support provider during the troubleshooting.

2. Verify that the device is reachable by SSH or TELNET.
3. If the device is reachable, enter the **`show version`** command.

```
device# show version
SLX-OS Operating System Version: 20.1.01
```

```
Copyright (c) 1995-2019 Extreme Networks, Inc.
Firmware name:      20.1.01
Build Time:         13:35:38 Jun 24, 2019
Install Time:       19:32:30 Jun 24, 2019
Kernel:             4.14.67

Control Processor:   GenuineIntel
Memory Size:        SLXVM: 8371 MB   System Total: 16070 MB

System Uptime:   0days 21hrs 47mins 30secs
Name      Primary/Secondary Versions
------------------------------------
SLX-OS    20.1.01
          20.1.01a
```

4. If **show version** does not display the new firmware as the primary version, prepare output logs of the following commands, and contact your device support provider.
   - **show firmwaredownloadhistory**
   - **show firmwaredownloadstatus**

Using troubleshooting and diagnostic tools

This section describes the various troubleshooting and diagnostic tools available with SLX-OS, and provides some guidelines for their use.

Refer also to Gathering troubleshooting information on page 11, which provides information about supportSave files.

Tracing a route with the trace-l2 command

To specify the Layer 2 path for traceroute packets, use the **trace-l2** command.

```
F4# trace-l2 ?
Possible completions:
  show   show L2 topology
  vlan   trace VLAN
F4# trace-l2 vlan ?
Possible completions:
  1-4090vlan number
F4# trace-l2 vlan 1 ?
Possible completions:
  A.B.C.Ddestination IP address
  ASCII string destination host name
  HHHH.HHHH.HHHHdestination MAC address
  |
  <cr>
```

Using show commands

The table below lists some **show** commands that are often used for troubleshooting.

Table 6: show commands used for troubleshooting

Command group	Commands	Specific fields or purpose
System commands	show chassis show environment show firmwaredownloadstatus show license show logging raslog show mac-address-table show process cpu show process memory show running-config show system show version show vlan brief	
Interface commands	show interface show ip int brief show media show qos flowcontrol interface show qos queue interface show qos int	Check pause-frames Check the CoS statistics Check packet drops, buffer consumption, real-time queue statistics
Feature commands	show port-channel detail show lacp counter show lldp neighbors detail show lldp statistics show qos interface all show udld statistics	

Using debug and system diagnostic commands

Diagnostic commands, such as "debug" and "show system internal" commands, are developed and intended for specialized troubleshooting. We recommend that

you work closely with Extreme technical support in executing such commands and interpreting their results.

You can perform the following operations related to debugging features:

- To enable debugging on a feature, use the **debug** command in privileged EXEC mode.
  ```
  device# debug feature required-keywords
  ```
- To check whether debugging is enabled on a feature, use the **show debug** command in privileged EXEC mode.
  ```
  device# show debug feature
  ```
- To disable debugging, use the **no debug** command.
  ```
  device# no debug feature required-keywords
  ```

Use caution when debugging in real time on a production device, because real-time debugging is CPU-intensive.

We recommend checking the command output on a lab device first, and then if the output looks acceptable, enable it on the production device to get more data. In addition, to reduce CPU load, we recommend using keywords such as events and summary that limit the extent of debugging rather than more comprehensive options such as detail and all.

Debugging operations are used mainly for debugging control plane protocols such as LACP and LLDP. For example, to view received LLDP packets on the console, use the following command:

```
device# debug lldp packets all rx
```

If the device is accessed through Telnet, enable logging using a terminal monitor.

The following are the most frequently used debug commands:

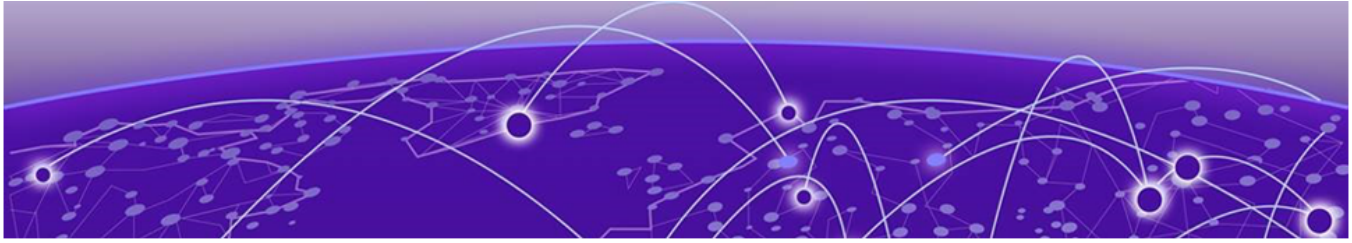
- **debug dot1x packet**
- **debug lacp pdu** [rx | tx]
- **debug lldp packet** { **all | ethernet** *slot/port* }
- **debug spanning-tree bpdu** [rx | tx]

Traffic mirroring

In certain instances, you may need to examine packets in transit across links to understand the traffic pattern on a specific port.



Note
Refer to the "Guest OS for TPVM" > "Insight interface and TPVM" section of the *Extreme SLX-OS Management Configuration Guide*.



Supported NTP Regions and Time Zones

Africa on page 33
America on page 34
Antarctica on page 35
Arctic on page 35
Asia on page 36
Atlantic on page 36
Australia on page 37
Europe on page 37
Indian on page 37
Pacific on page 38

Africa

The table below lists region and city time zones supported in the Africa region.

Table 7: Region/city time zones in Africa region

Africa/Luanda	Africa/Banjul	Africa/Mogadishu
Africa/Ouagadougou	Africa/Conakry	Africa/Sao_Tome
Africa/Bujumbura	Africa/Malabo	Africa/Mbabane
Africa/Porto-Novo	Africa/Bissau	Africa/Ndjamena
Africa/Gaborone	Africa/Nairobi	Africa/Lome
Africa/Kinshasa	Africa/Monrovia	Africa/Tunis
Africa/Lubumbashi	Africa/Maseru	Africa/Dar_es_Salaam
Africa/Bangui	Africa/Tripoli	Africa/Kampala
Africa/Brazzaville	Africa/Casablanca	Africa/Johannesburg
Africa/Abidjan	Africa/Bamako	Africa/Lusaka
Africa/Douala	Africa/Nouakchott	Africa/Harare
Africa/Djibouti	Africa/Blantyre	
Africa/Algiers	Africa/Maputo	
Africa/Cairo	Africa/Windhoek	
Africa/El_Aaiun	Africa/Niamey	
Africa/Asmara	Africa/Lagos	
Africa/Ceuta	Africa/Kigali	
Africa/Addis_Ababa	Africa/Khartoum	
Africa/Libreville	Africa/Freetown	
Africa/Accra	Africa/Dakar	

America

The table below lists region and city time zones supported in the America region.

Table 8: Region/city time zones in America region

America/Antigua America/Anguilla America/Curacao America/Argentina/Buenos_Aires America/Argentina/Cordoba America/Argentina/San_Luis America/Argentina/Jujuy America/Argentina/Tucuman America/Argentina/Catamarca America/Argentina/La_Rioja America/Argentina/San_Juan America/Argentina/Mendoza America/Argentina/Rio_Gallegos America/Argentina/Ushuaia America/Aruba	America/Guatemala America/Guyana America/Tegucigalpa America/Port-au-Prince America/Guadeloupe America/Jamaica America/St_Kitts America/Cayman America/St_Lucia America/Marigot America/Adak America/Martinique America/Montserrat America/Mexico_City America/Cancun	America/Edmonton America/Cambridge_Bay America/Yellowknife America/Inuvik America/Dawson_Creek America/Vancouver America/Whitehorse America/Thunder_Bay America/Iqaluit America/Pangnirtung America/Resolute America/Rankin_Inlet America/Winnipeg America/Rainy_River America/Regina
America/Barbados America/St_Barthelemy America/La_Paz America/Noronha America/Belem America/Fortaleza America/Recife America/Araguaina America/Maceio America/Bahia America/Sao_Paulo America/Campo_Grande America/Cuiaba America/Santarem America/Porto_Velho	America/Merida America/Monterrey America/Mazatlan America/Chihuahua America/Hermosillo America/Tijuana America/Managua America/Panama America/Lima America/Miquelon America/Puerto_Rico America/Asuncion America/Paramaribo America/El_Salvador America/Grand_Turk	America/Montevideo America/St_Vincent America/Caracas America/Tortola America/St_Thomas America/New_York America/Detroit America/Kentucky/Monticello America/Indiana/Indianapolis America/Indiana/Vincennes America/Indiana/Knox America/Indiana/Winamac America/Indiana/Marengo America/Indiana/Vevay America/Chicago
America/Boa_Vista America/Manaus America/Eirunepe America/Rio_Branco America/Nassau America/Belize	America/Swift_Current America/Dawson America/Santiago America/Bogota America/Costa_Rica America/Havana	America/Indiana/Tell_City America/Indiana/Petersburg America/Menominee America/North_Dakota/Center America/North_Dakota/New_Salem

Table 8: Region/city time zones in America region (continued)

America/St_Johns	America/Dominica	America/Denver
America/Halifax	America/Santo_Domingo	America/Boise
America/Glace_Bay	America/Guayaquil	America/Shiprock
America/Moncton	America/Grenada	America/Phoenix
America/Goose_Bay	America/Cayenne	America/Los_Angeles
America/Blanc-Sablon	America/Godthab	America/Anchorage
America/Montreal	America/Danmarkshavn	America/Juneau
America/Toronto	America/Scoresbysund	America/Yakutat
America/Nipigon	America/Thule	America/Nome
		America/Port_of_Spain

Antarctica

The table below lists region and city time zones supported in the Antarctica region.

Table 9: Region/city time zones in Antarctica region

Antarctica/McMurdo	Antarctica/Mawson	Antarctica/Vostok
Antarctica/South_Pole	Antarctica/Davis	Antarctica/DumontDUrville
Antarctica/Rothera	Antarctica/Casey	Antarctica/Syowa

Arctic

The table below lists region and city time zones supported in the Arctic region.

Table 10: Region/city time zone in Arctic region

Arctic/Longyearbyen		

Asia

The table below lists region and city time zones supported in the Asia region.

Table 11: Region/city time zones in Asia region

Asia/Dubai	Asia/Tokyo	Asia/Gaza
Asia/Kabul	Asia/Bishkek	Asia/Qatar
Asia/Yerevan	Asia/Phnom_Penh	Asia/Yekaterinburg
Asia/Baku	Asia/Pyongyang	Asia/Omsk
Asia/Dhaka	Asia/Seoul	Asia/Novosibirsk
Asia/Bahrain	Asia/Kuwait	Asia/Krasnoyarsk
Asia/Brunei	Asia/Almaty	Asia/Irkutsk
Asia/Thimphu	Asia/Qyzylorda	Asia/Yakutsk
Asia/Shanghai	Asia/Aqtobe	Asia/Vladivostok
Asia/Harbin	Asia/Aqtau	Asia/Sakhalin
Asia/Chongqing	Asia/Oral	Asia/Magadan
Asia/Urumqi	Asia/Vientiane	Asia/Kamchatka
Asia/Kashgar	Asia/Beirut	Asia/Anadyr
Asia/Nicosia	Asia/Colombo	Asia/Riyadh
Asia/Tbilisi	Asia/Rangoon	Asia/Singapore
Asia/Hong_Kong	Asia/Ulaanbaatar	Asia/Damascus
Asia/Jakarta	Asia/Hovd	Asia/Bangkok
Asia/Pontianak	Asia/Choibalsan	Asia/Dushanbe
Asia/Makassar	Asia/Macau	Asia/Dili
Asia/Jayapura	Asia/Kuala_Lumpur	Asia/Ashgabat
Asia/Jerusalem	Asia/Kuching	Asia/Taipei
Asia/Kolkata	Asia/Katmandu	Asia/Samarkand
Asia/Baghdad	Asia/Muscat	Asia/Tashkent
Asia/Tehran	Asia/Manila	Asia/Ho_Chi_Minh
Asia/Amman	Asia/Karachi	Asia/Aden
		Asia/Srednekolymsk

Atlantic

The table below lists region and city time zones supported in the Atlantic region.

Table 12: Region/city time zones in Atlantic region

Atlantic/Bermuda	Atlantic/Faroe	Atlantic/Azores
Atlantic/Cape_Verde	Atlantic/South_Georgia	Atlantic/St_Helena
Atlantic/Canary	Atlantic/Reykjavik	
Atlantic/Stanley	Atlantic/Madeira	

Australia

The table below lists region and city time zones supported in the Australia region.

Table 13: Region/city time zones in Australia region

Australia/Lord_Howe	Australia/Sydney	Australia/Darwin
Australia/Hobart	Australia/Brisbane	Australia/Perth
Australia/Currie	Australia/Lindeman	Australia/Eucla
Australia/Melbourne	Australia/Adelaide	

Europe

The table below lists region and city time zones supported in the Europe region.

Table 14: Region/city time zones in Europe region

Europe/Andorra	Europe/Gibraltar	Europe/Warsaw
Europe/Tirane	Europe/Athens	Europe/Lisbon
Europe/Vienna	Europe/Zagreb	Europe/Bucharest
Europe/Mariehamn	Europe/Budapest	Europe/Belgrade
Europe/Sarajevo	Europe/Dublin	Europe/Kaliningrad
Europe/Brussels	Europe/Isle_of_Man	Europe/Moscow
Europe/Sofia	Europe/Rome	Europe/Volgograd
Europe/Minsk	Europe/Jersey	Europe/Samara
Europe/Zurich	Europe/Vaduz	Europe/Stockholm
Europe/Prague	Europe/Vilnius	Europe/Ljubljana
Europe/Berlin	Europe/Luxembourg	Europe/Bratislava
Europe/Copenhagen	Europe/Riga	Europe/San_Marino
Europe/Tallinn	Europe/Monaco	Europe/Istanbul
Europe/Madrid	Europe/Chisinau	Europe/Kiev
Europe/Helsinki	Europe/Podgorica	Europe/Uzhgorod
Europe/Paris	Europe/Skopje	Europe/Zaporozhye
Europe/London	Europe/Malta	Europe/Simferopol
Europe/Guernsey	Europe/Amsterdam	Europe/Vatican
Europe/Oslo		

Indian

The table below lists region and city time zones supported in the Indian region.

Table 15: Region/city time zones in Indian region

Indian/Cocos	Indian/Antananarivo	Indian/Mahe
Indian/Christmas	Indian/Mauritius	Indian/Kerguelen
Indian/Chagos	Indian/Maldives	Indian/Mayotte
Indian/Comoro	Indian/Reunion	

Pacific

The table below lists region and city time zones supported in the Pacific region.

Table 16: Region/city time zones in Pacific region

Pacific/Pago_Pago	Pacific/Kwajalein	Pacific/Palau
Pacific/Rarotonga	Pacific/Saipan	Pacific/Guadalcanal
Pacific/Easter	Pacific/Noumea	Pacific/Fakaofo
Pacific/Galapagos	Pacific/Norfolk	Pacific/Tongatapu
Pacific/Fiji	Pacific/Nauru	Pacific/Funafuti
Pacific/Truk	Pacific/Niue	Pacific/Johnston
Pacific/Ponape	Pacific/Auckland	Pacific/Midway
Pacific/Kosrae	Pacific/Chatham	Pacific/Wake
Pacific/Guam	Pacific/Tahiti	Pacific/Honolulu
Pacific/Tarawa	Pacific/Marquesas	Pacific/Efate
Pacific/Enderbury	Pacific/Gambier	Pacific/Wallis
Pacific/Kiritimati	Pacific/Port_Moresby	Pacific/Apia
Pacific/Majuro	Pacific/Pitcairn	