Licensing Guide

Modified: 2018-10-04

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Licensing Guide

The information in this document is current as of the date on the title page.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at https://support.juniper.net/support/eula/. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

List of Tables

About the Documentation

Documentation and Release Notes

To obtain the most current version of all Juniper Networks® technical documentation, see the product documentation page on the Juniper Networks website at https://www.juniper.net/documentation/.

If the information in the latest release notes differs from the information in the documentation, follow the product Release Notes.

Juniper Networks Books publishes books by Juniper Networks engineers and subject matter experts. These books go beyond the technical documentation to explore the nuances of network architecture, deployment, and administration. The current list can be viewed at https://www.juniper.net/books.

Using the Examples in This Manual

If you want to use the examples in this manual, you can use the **load merge** or the **load merge relative** command. These commands cause the software to merge the incoming configuration into the current candidate configuration. The example does not become active until you commit the candidate configuration.

If the example configuration contains the top level of the hierarchy (or multiple hierarchies), the example is a *full example*. In this case, use the **load merge** command.

If the example configuration does not start at the top level of the hierarchy, the example is a *snippet*. In this case, use the **load merge relative** command. These procedures are described in the following sections.

Merging a Full Example

To merge a full example, follow these steps:

1. From the HTML or PDF version of the manual, copy a configuration example into a text file, save the file with a name, and copy the file to a directory on your routing platform.

   For example, copy the following configuration to a file and name the file **ex-script.conf**. Copy the **ex-script.conf** file to the **/var/tmp** directory on your routing platform.

   ```
   system {
     scripts {
       commit {
         file ex-script.xsl;
       }
     }
   }
   interfaces {
     fxp0 {
       disable;
       unit 0 {
         family inet {
           address 10.0.0.1/24;
         }
       }
     }
   }
   ```

2. Merge the contents of the file into your routing platform configuration by issuing the **load merge** configuration mode command:

   ```
   [edit]
   user@host# load merge /var/tmp/ex-script.conf
   load complete
   ```

Merging a Snippet

To merge a snippet, follow these steps:

1. From the HTML or PDF version of the manual, copy a configuration snippet into a text file, save the file with a name, and copy the file to a directory on your routing platform.

   For example, copy the following snippet to a file and name the file **ex-script-snippet.conf**. Copy the **ex-script-snippet.conf** file to the **/var/tmp** directory on your routing platform.

   ```
   commit {
     file ex-script-snippet.xsl; }
   ```

2. Move to the hierarchy level that is relevant for this snippet by issuing the following configuration mode command:

```
[edit]
user@host# edit system scripts
[edit system scripts]
```

3. Merge the contents of the file into your routing platform configuration by issuing the **load merge relative** configuration mode command:

```
[edit system scripts]
user@host# load merge relative /var/tmp/ex-script-snippet.conf
load complete
```

For more information about the **load** command, see CLI Explorer.

Documentation Conventions

Table 1 on page xi defines notice icons used in this guide.

Table 1: Notice Icons

Icon	Meaning	Description
	Informational note	Indicates important features or instructions.
	Caution	Indicates a situation that might result in loss of data or hardware damage.
	Warning	Alerts you to the risk of personal injury or death.
	Laser warning	Alerts you to the risk of personal injury from a laser.
	Tip	Indicates helpful information.
	Best practice	Alerts you to a recommended use or implementation.

Table 2 on page xii defines the text and syntax conventions used in this guide.

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents text that you type.	To enter configuration mode, type the **configure** command: user@host> **configure**
`Fixed-width text like this`	Represents output that appears on the terminal screen.	`user@host>` **show chassis alarms** `No alarms currently active`
Italic text like this	• Introduces or emphasizes important new terms. • Identifies guide names. • Identifies RFC and Internet draft titles.	• A policy *term* is a named structure that defines match conditions and actions. • *Junos OS CLI User Guide* • RFC 1997, *BGP Communities Attribute*
Italic text like this	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# **set system domain-name** *domain-name*
Text like this	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	• To configure a stub area, include the **stub** statement at the **[edit protocols ospf area area-id]** hierarchy level. • The console port is labeled **CONSOLE**.
< > (angle brackets)	Encloses optional keywords or variables.	**stub <default-metric** *metric***>;**
| (pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	**broadcast | multicast** **(*string1* | *string2* | *string3*)**
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	**rsvp { # Required for dynamic MPLS only**
[ ] (square brackets)	Encloses a variable for which you can substitute one or more values.	**community name members [** ***community-ids*** **]**

Indention and braces ({ })	Identifies a level in the configuration hierarchy.	[edit]
		routing-options {
		  static {
		  route default {
		  nexthop *address*;
		  retain;
		  }
		  }
		}

; (semicolon)	Identifies a leaf statement at a configuration hierarchy level.	

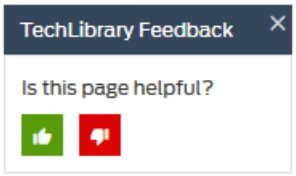
Table 2: Text and Syntax Conventions (continued)

Convention	Description	Examples
GUI Conventions		
Bold text like this	Represents graphical user interface (GUI) items you click or select.	• In the Logical Interfaces box, select **All Interfaces**. • To cancel the configuration, click **Cancel**.
> (bold right angle bracket)	Separates levels in a hierarchy of menu selections.	In the configuration editor hierarchy, select **Protocols>Ospf**.

Documentation Feedback

We encourage you to provide feedback so that we can improve our documentation. You can use either of the following methods:

- Online feedback system—Click TechLibrary Feedback, on the lower right of any page on the Juniper Networks TechLibrary site, and do one of the following:



  - Click the thumbs-up icon if the information on the page was helpful to you.
  - Click the thumbs-down icon if the information on the page was not helpful to you or if you have suggestions for improvement, and use the pop-up form to provide feedback.

- E-mail—Send your comments to **techpubs-comments@juniper.net**. Include the document or topic name, URL or page number, and software version (if applicable).

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or Partner Support Service support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at https://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf.
- Product warranties—For product warranty information, visit https://www.juniper.net/support/warranty/.

- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: https://www.juniper.net/customers/support/
- Search for known bugs: https://prsearch.juniper.net/
- Find product documentation: https://www.juniper.net/documentation/
- Find solutions and answer questions using our Knowledge Base: https://kb.juniper.net/
- Download the latest versions of software and review release notes: https://www.juniper.net/customers/csc/software/
- Search technical bulletins for relevant hardware and software notifications: https://kb.juniper.net/InfoCenter/
- Join and participate in the Juniper Networks Community Forum: https://www.juniper.net/company/communities/
- Open a case online in the CSC Case Management tool: https://www.juniper.net/cm/

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: https://entitlementsearch.juniper.net/entitlementsearch/

Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Management tool in the CSC at https://www.juniper.net/cm/.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see https://www.juniper.net/support/requesting-support.html.

CHAPTER 1

Licensing Overview

Junos OS Software License Overview

Junos OS Feature Licenses

Some Junos OS software features require a license to activate the feature. To enable a licensed feature, you need to purchase, install, manage, and verify a license key that corresponds to each licensed feature. To conform to Junos OS feature licensing requirements, you must purchase one license per feature per device. The presence of the appropriate software license key on your device determines whether you are eligible to configure and use the licensed feature.

To speed deployment of licensed features, Junos OS software implements an honor-based licensing structure and provides you with a 30-day grace period to use a licensed feature without a license key installed. The grace period begins when you configure the feature and your device uses the licensed feature for the first time, but not necessarily when you install the license. After the grace period expires, the system generates system log messages saying that the feature requires a license. To clear the error message and use the licensed feature properly, you must install and verify the required license.

Data center customers, for example those using the QFX platform, use universal licenses. Starting in Junos OS Release 15.1, to ensure that license keys are used properly, Juniper Networks license key generation is enhanced to specify a customer ID in the license key. You can see the customer ID displayed in the output of the **show system license** command.

For information about how to purchase software licenses, contact your Juniper Networks sales representative.

See Also

- Verifying Junos OS License Installation (CLI) on page 41

- show system license on page 44

License Enforcement

For features or scaling levels that require a license, you must install and properly configure the license to meet the requirements for using the licensable feature or scale level. The device enables you to commit a configuration that specifies a licensable feature or scale without a license for a 30-day grace period. The grace period is a short-term grant that enables you to start using features in the pack or scale up to the system limits (regardless of the license key limit) without a license key installed. The grace period begins when the licensable feature or scaling level is actually used by the device (not when it is first committed). In other words, you can commit licensable features or scaling limits to the device configuration, but the grace period does not begin until the device uses the licensable feature or exceeds a licensable scaling level.

NOTE: Configurations might include both licensed and nonlicensed features. For these situations, the license is enforced up to the point where the license can be clearly distinguished. For example, an authentication-order configuration is shared by both Authentication, Authorization, and Accounting (AAA), which is licensed, and by Layer 2 Tunneling Protocol (L2TP), which is not licensed. When the configuration is committed, the device does not issue any license warnings, because it is not yet known whether AAA or L2TP is using the configuration. However, at runtime, the device checks for a license when AAA authenticates clients, but does not check when L2TP authenticates clients.

The device reports any license breach as a warning log message whenever a configuration is committed that contains a feature or scale limit usage that requires a license. Following the 30-day grace period, the device periodically reports the breach to syslog messages until a license is installed and properly configured on the device to resolve the breach.

NOTE: Successful commitment of a licensable feature or scaling configuration does not imply that the required licenses are installed or not required. If a required license is not present, the system issues a warning message after it commits the configuration.

See Also

- Adding New Licenses (CLI Procedure) on page 36
- Deleting License Keys (CLI) on page 52
- Saving License Keys (CLI) on page 43
- Verifying Junos OS License Installation (CLI) on page 41

Junos OS Feature License Keys

This section contains the following topics:

License Key Components

A license key consists of two parts:

- License ID—Alphanumeric string that uniquely identifies the license key. When a license is generated, it is given a license ID.
- License data—Block of binary data that defines and stores all license key objects.

For example, in the following typical license key, the string XXXXXXXXXX is the license ID, and the trailing block of data is the license data:

```
XXXXXXXXXX xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx
           xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx
           xxxxxx xxxxxx xxx
```

The license data defines the device ID for which the license is valid and the version of the license.

License Management Fields Summary

The Licenses page displays a summary of licensed features that are configured on the device and a list of licenses that are installed on the device. The information on the license management page is summarized in Table 3 on page 17.

Table 3: Summary of License Management Fields

Field Name	Definition
Feature Summary	
Feature	Name of the licensed feature: • **Features**—Software feature licenses. • **All features**—All-inclusive licenses
Licenses Used	Number of licenses currently being used on the device. Usage is determined by the configuration on the device. If a feature license exists and that feature is configured, the license is considered used.
Licenses Installed	Number of licenses installed on the device for the particular feature.
Licenses Needed	Number of licenses required for legal use of the feature. Usage is determined by the configuration on the device: If a feature is configured and the license for that feature is not installed, a single license is needed.

Table 3: Summary of License Management Fields (continued)

Field Name	Definition
Installed Licenses	
ID	Unique alphanumeric ID of the license.
State	**Valid**—The installed license key is valid. **Invalid**—The installed license key is not valid.
Version	Numeric version number of the license key.
Group	If the license defines a group license, this field displays the group definition. If the license requires a group license, this field displays the required group definition. NOTE: Because group licenses are currently unsupported, this field is always blank.
Enabled Features	Name of the feature that is enabled with the particular license.
Expiry	Verify that the expiration information for the license is correct. For Junos OS, only permanent licenses are supported. If a license has expired, it is shown as invalid.

See Also

- Generating a License Key on page 165
- Updating License Keys (CLI) on page 166
- Saving License Keys on page 166
- Downloading License Keys on page 165

Software Feature Licenses

Each license is tied to one software feature pack, and that license is valid for only one device.

NOTE: **This is not a complete list of licenses. Contact your Juniper Networks representative for license information.**

For information about how to purchase software licenses, contact your Juniper Networks sales representative at https://www.juniper.net/in/en/contact-us/.

- Software Features That Require Licenses on M Series, MX Series, and T Series Routers on page 19
- Software Features That Require Licenses on M Series Routers Only on page 22
- Software Features That Require Licenses on MX Series Routers Only on page 23
- Software Feature Licenses for SRX Series Devices on page 29

Software Features That Require Licenses on M Series, MX Series, and T Series Routers

Table 4 on page 19 lists the licenses you can purchase for each M Series, MX Series, and T Series software feature. Each license allows you to run the specified software feature on a single device.

NOTE: The DHCP server functionality for Junos OS is part of the subscriber management feature. You must have the S-SA-FP, S-MX80-SA-FP or S-MX104-SA-FP license in order to enable the DHCP server. For service accounting, you must also have S-SSM-FP.

For information about how to purchase a software license, contact your Juniper Networks sales representative at https://www.juniper.net/in/en/contact-us/.

Table 4: Junos OS Feature License Model Number for M Series, MX Series, and T Series Routers

Licensed Software Feature	Supported Devices	Model Number
Generalized Multiprotocol Label Switching (GMPLS) Support on Junos OS	M10i, M7i, M120, M160, M20, M320, M40e, T320, T640, and MX Series Routers	JS-GMPLS
IPv6 Support on Junos OS	M120, M160, M20, M320, M40e, T320, T640, and MX Series Routers	JS-IPv6
Logical Router Support for Junos OS	M10i, M120, M160, M20, M320, M40e, M7i, T320, T640, and MX Series Routers	JS-LR
J-Flow accounting license for Adaptive Services (AS) PIC and Multiservices PIC	M10i, M120, M160, M20, M320, M40e, M7i, T320, M10, M5, T640, and T1600	S-ACCT
Chassis license for Application Traffic Optimization service, policy enforcement and application statistics. This license includes S-AI and S-LDPF fucntionality and 1-year Signature Subscription License	MX104, MX240, MX480, MX960, M Series, and T Series Routers	S-ATO
Software License for Passive Monitoring Flow Collector Application, supporting 100 Kpps throughput; Chassis based license for Multiservices PIC	M320, T640, T320, T1600	S-COLLECTOR-100K
License to use Compressed Real-Time Transport Protocol (CRTP) feature in AS PIC and Multiservices PIC	M10i, M120, M160, M20, M320, M40e, M7i, T320, M10, M5, T640, and T1600	S-CRTP

Table 4: Junos OS Feature License Model Number for M Series, MX Series, and T Series Routers (continued)

Licensed Software Feature	Supported Devices	Model Number
Software License for Passive Monitoring DFC Application, supporting 100Kpps throughput; Chassis based license for Multiservices PIC	M320, T640, T320, and T1600	S-DFC-100K
Security Services license for AS PIC and Multiservices PIC	M10i, M7i, M5, M120, M160, M20, M320, M40e, T320, T640, M10, and T1600	S-ES
Chassis license for IDP service, policy enforcement. This license includes S-AI and S-LDPF fucntionality and 1-year Signature Subscription License	MX104, MX240, MX480, MX960, M Series, and T Series Routers	S-IDP
Junos-FIPS Software License	M10i, M7i, M320, M40e, T320, and T640	S-JUNOS-FIPS
Link Services Software License—up to 1023 ML bundles per Chassis for Multiservices PIC and Multiservices Dense Port Concentrator (DPC)	M5, M7i, M10, M10i, M20, M40e, M120, M320, T320, T640, T1600, MX240, MX480, and MX960	S-LSSL-1023
Link Services Software Ugrade License—from 255 to 1023 ML bundles per Chassis for Multiservices PIC and Multiservices DPC	M5, M7i, M10, M10i, M20, M40e, M120, M320, T320, T640, T1600, MX240, MX480, and MX960	S-LSSL-1023-UPG
Link Services Software Ugrade License—from 64 to 255 ML bundles per Chassis for AS PIC, Multiservices PIC, and Multiservices DPC	M5, M7i, M10, M10i, M20, M40e, M120, M320, T320, T640, T1600, MX240, MX480, and MX960	S-LSSL-255-UPG
Link Services Software License—up to 255 ML bundles per Chassis for AS PIC, Multiservices PIC, and Multiservices DPC	M10, M7i, M5, M120, M20, M320, M40e, T320, T640, M10i, T1600, MX240, MX480, and MX960	S-LSSL-256
Link Services Software License—up to 4 ML bundles per Chassis for AS PIC, Multiservices PIC, and Multiservices DPC	M10i, M120, M20, M320, M40e, M7i, T320, M10, M5, T640, T1600, MX240, MX480, and MX960	S-LSSL-4
Link Services Software License—up to 64 ML bundles per Chassis for AS PIC, MS PIC and MS DPC	M10, M7i, M5, M120, M20, M320, M40e, T320, T640, M10i, T1600, MX240, MX480, and MX960	S-LSSL-64
Link Services Software Upgrade License—from 4 to 64 ML bundles per Chassis for AS PIC, Multiservices PIC, and Multiservices DPC	M5, M7i, M10, M10i, M20, M40e, M120, M320, T320, T640, T1600, MX240, MX480, and MX960	S-LSSL-64-UPG
Software License for Passive Monitoring Flow Monitor Application, supporting 1M flows. Chassis based license for Multiservices PIC	M320, T640, T320, and T1600	S-MONITOR-1M
Network Address Translation (NAT), FW license on AS PIC and Multiservices PIC: Multi-instance	M10, M7i, M5, M120, M160, M20, M320, M40e, T320, T640, M10i, and T1600	S-NAT-FW-MULTI

Table 4: Junos OS Feature License Model Number for M Series, MX Series, and T Series Routers (continued)

Licensed Software Feature	Supported Devices	Model Number
NAT, FW license on AS PIC and Multiservices PIC: Single-instance	M10, M7i, M5, M120, M160, M20, M320, M40e, T320, T640, M10i, and T1600	S-NAT-FW-SINGLE
Software license for Packet trigger subscriber policy	MX240, MX480, MX960, M120, and M320	S-PTSP
Subscriber Access Feature Pack License Scaling (128000)	MX104, MX240, MX480, MX960, M120, and M320	S-SA-128K
Subscriber Access Feature Pack License Scaling (32000)	MX104, MX240, MX480, MX960, M120, and M320	S-SA-32K
Subscriber Access Feature Pack License Scaling (4000)	MX104, MX240, MX480, MX960, M120, M320, and MX80	S-SA-4K
Subscriber Access Feature Pack License Scaling (64000)	MX104, MX240, MX480, MX960, M120, and M320	S-SA-64K
Subscriber Access Feature Pack License Scaling (8000)	MX104, MX240, MX480, MX960, M120, M320, and MX80	S-SA-8K
Subscriber Access Feature Pack License Scaling (96000)	MX104, MX240, MX480, MX960, M120, and M320	S-SA-96K
Subscriber Access Feature Pack license	MX104, MX240, MX480, MX960, M120, and M320	S-SA-FP
Stateful Failover for Services on AS PIC and Multiservices PIC: Multilink PPP (MLPPP) only	M10, M7i, M5, M120, M160, M20, M320, M40e, T320, T640, M10i, and T1600	S-SERVICES-SFO
Subscriber Service Management Feature Packet License (RADIUS/SRC based Service Activation and Deactivation) Per-Service Accounting Features for Subscribers	MX104, MX240, MX480, MX960, M120, and M320	S-SSM-FP
Subscriber Traffic Lawful Intercept Feature Pack License	MX240, MX480, MX960, M120, M320, and MX80	S-SSP-FP
Software license for application aware traffic direct feature	MX240, MX480, MX960, M120, and M320	S-TFDIRECT-APP
Software license for subscriber aware traffic direct feature	MX240, MX480, MX960, M120, and M320	S-TFDIRECT-SUB
Video Services Feature Pack license	M120, M320, MX80, MX104, MX240, MX480, and MX960	S-VIDEO-FP
Port capacity enhancement Feature Pack License for MX5 routers	MX5	mx5-to-mx10-upgrade

Table 4: Junos OS Feature License Model Number for M Series, MX Series, and T Series Routers (continued)

Licensed Software Feature	Supported Devices	Model Number
Port capacity enhancement Feature Pack License for MX10 routers	MX10	mx10-to-mx40-upgrade
Port capacity enhancement Feature Pack License for MX40 routers	MX40	mx40-to-mx80-upgrade

Software Features That Require Licenses on M Series Routers Only

Table 5 on page 22 lists the licenses you can purchase for each M Series software feature. Each license allows you to run the specified software feature on a single device.

For information about how to purchase a software license, contact your Juniper Networks sales representative at https://www.juniper.net/in/en/contact-us/.

Table 5: Junos OS Feature License Model Number for M Series Routers

Licensed Software Feature	Supported Devices	Model Number
J-Flow accounting license on Integrated Adaptive Services Module (ASM) and Integrated Multiservices Module	M7i	S-ACCT-BB
Security Services license on ASM and Integrated Multiservices Module	M7i	S-ES-BB
Layer 2 Tunneling Protocol (L2TP) L2TP Network Server (LNS) license for 16000 sessions on Multiservices PIC	M120	S-LNS-16K
L2TP LNS license Upgrade—from 8000 to 16000 sessions on Multiservices PIC	M120	S-LNS-16K-UPG
L2TP LNS license for 2000 sessions on AS PIC or Integrated Adaptive Services Module and Multiservices PIC	M7i, M10i, and M120	S-LNS-2K
L2TP LNS license for 4000 sessions on AS PIC or Integrated Adaptive Services Module and Multiservices PIC	M7i, M10i, and M120	S-LNS-4K
L2TP LNS license Upgrade—from 2000 to 4000 sessions on AS PIC or Integrated Adaptive Services Module and Multiservices PIC	M7i, M10i, and M120	S-LNS-4K-UPG
L2TP LNS license for 8000 sessions on Multiservices PIC	M7i, M10i, and M120	S-LNS-8K
L2TP LNS license Upgrade—from 4000 to 8000 sessions on AS PIC and Multiservices PIC	M7i, M10i, and M120	S-LNS-8K-UPG
Link services software license on integrated ASM and Integrated Multi Services Module—up to 4 ML bundles	M7i	S-LSSL-BB
NAT, FW license on Integrated ASM and Integrated Multi Services Module: Multi instance	M7i	S-NAT-FW-MULTI-BB

Table 5: Junos OS Feature License Model Number for M Series Routers (continued)

Licensed Software Feature	Supported Devices	Model Number
NAT, FW license on Integrated ASM and Integrated Multi Services Module: Single instance	M7i	S-NAT-FW-SINGLE-BB
Tunnel services software license for AS PIC and Multiservices PIC (chassis license)	M7i and M10i	S-TUNNEL

Software Features That Require Licenses on MX Series Routers Only

Table 6 on page 23 lists the licenses you can purchase for each MX Series software feature. Each license allows you to run the specified software feature on a single device.

NOTE: The DHCP server functionality for Junos OS is part of the subscriber management feature. You must have the S-SA-FP, S-MX80-SA-FP or S-MX104-SA-FP license in order to enable the DHCP server. For service accounting, you must also have S-SSM-FP.

NOTE: This is not a complete list of licenses. Contact your Juniper Networks representative for license information.

For information about how to purchase a software license, contact your Juniper Networks sales representative at https://www.juniper.net/in/en/contact-us/.

Table 6: Junos OS Feature License Model Number for MX Series Routers

Licensed Software Feature	Supported Devices	Model Number
Upgrade license—from MX80-10G-ADV to MX80-40G-ADV	MX80	MX80-10G40G-UPG-ADV-B
Upgrade license—from MX80-10G to MX80-40G	MX80	MX80-10G40G-UPG-B
Upgrade license—from MX80-40G-ADV to full MX80	MX80	MX80-40G-UPG-ADV-B
Upgrade license—from MX80-40G to full MX80	MX80	MX80-40G-UPG-B
Upgrade license--from MX80-5G-ADV to MX80-10G-ADV	MX80	MX80-5G10G-UPG-ADV-B
Upgrade license—from MX80-5G to MX80-10G	MX80	MX80-5G10G-UPG-B
Upgrade license to activate 2x10GE P2&3	MX104	S-MX104-ADD-2X10GE

Table 6: Junos OS Feature License Model Number for MX Series Routers (continued)

Licensed Software Feature	Supported Devices	Model Number
Upgrade license to activate 2X10GE P0&1	MX104	S-MX104-UPG-2X10GE
Upgrade license to activate 4X10GE fixed ports on MX104	MX104	S-MX104-UPG-4X10GE
License to support per VLAN queuing on MX80	MX80	S-MX80-Q
License to support per VLAN queuing on MX104	MX104	S-MX104-Q
Chassis-based software license for inline J-Flow monitoring on MX5, MX10, M40, MX80, and MX104 Series routers	MX5, MX10, M40, MX80, and MX104	S-JFLOW-CH-MX5-104
Chassis-based software license for inline J-Flow monitoring on MX240 routers	MX240	S-JFLOW-CH-MX240
Chassis-based software license for inline J-Flow monitoring on MX480 routers	MX480	S-JFLOW-CH-MX480
Chassis-based software license for inline J-Flow monitoring on MX960 routers	MX960	S-JFLOW-CH-MX960
Chassis-based software license for inline J-Flow monitoring on MX2008 routers	MX2008	S-JFLOW-CH-MX2008
Chassis-based software license for inline J-Flow monitoring on MX2010 routers	MX2010	S-JFLOW-CH-MX2010
Chassis-based software license for inline J-Flow monitoring on MX2020 routers	MX2020	S-JFLOW-CH-MX2020
Flow monitoring and accounting features using J-Flow service on any Modular Port Concentrator (MPC) or MS-DPC	MX240, MX480, and MX960	S-ACCT-JFLOW-CHASSIS
Software License for in-line J-Flow service on Trio MPCs	MX240, MX480, and MX960	S-ACCT-JFLOW-IN

Table 6: Junos OS Feature License Model Number for MX Series Routers (continued)

Licensed Software Feature	Supported Devices	Model Number
Flow monitoring and accounting features using J-Flow service on any MPC limited to 10G of total JFLOW traffic	MX80	S-ACCT-JFLOW-IN-10G
Flow monitoring and accounting features using J-Flow service on any MPC limited to 10G of total JFLOW traffic	MX80	S-ACCT-JFLOW-IN-10G-UPG
Flow monitoring and accounting features using J-Flow service on any MPC limited to 5G of total JFLOW traffic	MX80	S-ACCT-JFLOW-IN-5G
Security services (IPsec, VPN and group VPN) license based on a single NPU for MS-MIC, MS-DPC or MS-MPC	MX Series router	S-ES-NPU
2000 IKE sessions on MS-DPC; Chassis based, limited to 6000 per Chassis	MX240, MX480, and MX960	S-ES-2K
4000 IKE sessions on MS-DPC; Chassis based, limited to 6000 per Chassis	MX240, MX480, and MX960	S-ES-4K
Upgrade from 2000 IKE sessions to 4000 IKE sessions on MS-DPC; Chassis based, limited to 6000 per Chassis	MX240, MX480, and MX960	S-ES-4K-UPG
6000 IKE sessions on MS-DPC; Chassis based, limited to 6000 per Chassis	MX240, MX480, and MX960	S-ES-6K
Upgrade from 4000 IKE sessions to 6000 IKE Sessions on MS-DPC; Chassis based, limited to 6000 per Chassis	MX240, MX480, and MX960	S-ES-6K-UPG
License to run stateful firewall on one NPU per MS-MIC, MS-DPC or MS-MPC	MX Series routers	S-FW-NPU
License to support DS3 Channelization (down to DS0) on each Modular Interface Card (MIC) for MIC-3D-8DS3-E3; also requires license S-MX80-Q when used on the MX80 platform	MX80, MX104, MX240, MX480, and MX960	S-MIC-3D-8CHDS3
License to support full-scale Layer 3 routes and Layer 3 VPN	MX80	S-MX80-ADV-R
License to support 256K routes	MX104	S-MX104-ADV-R1

Table 6: Junos OS Feature License Model Number for MX Series Routers (continued)

Licensed Software Feature	Supported Devices	Model Number
License to support scaling Layer 3 and VPN routes to 1 million or more entries on MX104 platforms	MX104	S-MX104-ADV-R2
License to support full-scale Layer 3 routes and Layer 3 VPN on each slot for MPC-3D-16XGE-SFPP	MX240, MX480, and MX960	S-MPC-3D-16XGE-ADV-R
License to support full-scale Layer 3 routes and Layer 3 VPN on each slot for port queuing MPCs	MX240, MX480, and MX960	S-MPC-3D-PQ-ADV-R
License to support full-scale Layer 3 routes and Layer 3 VPN on each slot for hierarchical quality of service (HQoS) MPCs	MX240, MX480, and MX960	S-MPC-3D-VQ-ADV-R
Subscriber Management Feature Pack License for MX80	MX80	S-MX80-SA-FP
Subscriber Management Feature Pack for MX104 series	MX104	S-MX104-SA-FP
Subscriber Service Management Feature Packet License—RADIUS and SRC-based service activation and deactivation per-service accounting features	MX80	S-MX80-SSM-FP
Subscriber Service Management Feature Packet License	MX104	S-MX104-SSM-FP
Upgrade to Traffic Direct Advanced (per MS-DPC)	MX960	S-MX-TD-UPG
License to run one instance of the NAT software on one NPU per MS-DPC	MX240, MX480, and MX960	S-NAT
License to support inline NAT software on MX5, MX10, MX40, MX80, MX104	MX5, MX10, MX40, MX80, and MX104	S-NAT-IN-MX5-104 (Replaces S-NAT-IN-MX40-MX80 and S-NAT-IN-MX5-MX10)
License to run one instance of the NAT software on one NPU per MS-MIC, MS-DPC, or MS-MPC	MX80, MX104, MX240, MA480, MX960, MX2010, and MX2020	S-NAT-NPU (Replaces S-NAT-IN-MX40-MX80-UPG)
License to run NAT using any MPC in an MX Chassis	MX240, MX480, and MX960	S-NAT-IN-MX-CHASSIS
Subscriber Access Feature Pack License Scaling (4000)	MX240, MX480, MX960, M120, M320, and MX80	S-SA-4K

Table 6: Junos OS Feature License Model Number for MX Series Routers (continued)

Licensed Software Feature	Supported Devices	Model Number
Subscriber Access Feature Pack License Scaling (8000)	MX240, MX480, MX960, M120, M320, and MX80	S-SA-8K
Subscriber Access Feature Pack License Scaling (16,000)	MX240, MX480, MX960, and MX80	S-SA-16K
Subscriber Access Feature Pack License Scaling (32,000)	MX240, MX480, MX960, M120, and M320	S-SA-32K
Subscriber Access Feature Pack License Scaling (64,000)	MX240, MX480, MX960, M120, and M320	S-SA-64K
Subscriber Access Feature Pack License Scaling (96,000)	MX240, MX480, MX960, M120, and M320	S-SA-96K
Subscriber Access Feature Pack License Scaling (128,000)	MX240, MX480, MX960, M120, and M320	S-SA-128K
Subscriber Access Feature Pack License Scaling (256,000)	MX240, MX480, and MX960	S-SA-256K
Subscriber Access Feature Pack License	MX240, MX480, MX960, M120, and M320	S-SA-FP
Software License for Secure Flow Mirroring Service (FlowTap) (does not require MS-DPC)	MX80, MX104, MX240, MX480, and MX960	S-SFM-FLOWTAP-IN
License to run one instance of the SFW and software on a MS-DPC	MX960, MX480, and MX240	S-SFW
Subscriber Service Management Feature Packet License—RADIUS and SRC-based service activation and deactivation per-service accounting features	MX240, MX480, MX960, M120, and M320	S-SSM-FP
Software license for one member of an MX Virtual Chassis	MX960, MX480, and MX240	S-VCR
Upgrade license—from MX10 to equivalent of MX40; allows additional 2x10G fixed ports to be used on the MX10 router	MX10-T	MX10-40-UPG
Upgrade license—from MX10 to equivalent of MX80; allows additional 4x10G fixed ports to be used on the MX10 router	MX10-T	MX10-80-UPG

Table 6: Junos OS Feature License Model Number for MX Series Routers (continued)

Licensed Software Feature	Supported Devices	Model Number
Upgrade license—from MX40 to equivalent of MX80; allows additional 2x10G fixed ports to be used on the MX40 router	MX40-T	MX40-80-UPG
Upgrade license—from MX5 to equivalent of MX10; allows second MIC slot to be used on the MX5 router	MX5-T	MX5-10-UPG
Upgrade license—from MX5 to equivalent of MX40; allows second MIC slot and 2x10G fixed ports to be used on the MX5 router	MX5-T	MX5-40-UPG
Upgrade license—from MX5 to equivalent of MX80. Allows second MIC slot and 4x10G fixed ports to be used on the MX5 router	MX5-T	MX5-80-UPG
Upgrade license—Subscriber Access Feature Pack scaling license upgrade from 4000 through 8000 subscribers	MX80, MX960, MX480, and MX240	S-SA-UP-8K
Upgrade license—Subscriber Access Feature Pack scaling license upgrade from 8000 through 16,000 subscribers	MX80, MX960, MX480, and MX240	S-SA-UP-16K
Upgrade license—Subscriber Access Feature Pack scaling license upgrade from 16,000 through 32,000 subscribers	MX240, MX480, and MX960	S-SA-UP-32K
Upgrade license—Subscriber Access Feature Pack scaling license upgrade from 32,000 through 64,000 subscribers	MX240, MX480, and MX960	S-SA-UP-64K
Upgrade license—Subscriber Access Feature Pack scaling license upgrade from 64,000 through 96,000 subscribers	MX240, MX480, and MX960	S-SA-UP-96K
Upgrade license—Subscriber Access Feature Pack scaling license upgrade from 96,000 through 128,000 subscribers	MX240, MX480, and MX960	S-SA-UP-128K
Upgrade license—Subscriber Access Feature Pack scaling license upgrade from 128,000 through 256,000 subscribers	MX240, MX480, and MX960	S-SA-UP-256K

Table 6: Junos OS Feature License Model Number for MX Series Routers (continued)

Licensed Software Feature	Supported Devices	Model Number
License to use MX as Controller or Aggregation device for Junos Fusion. One license per MX is needed.	MX Series router	S-MX-AD-FUSION-LIC
License to run any supported EX4300 model as a satellite device in Junos Fusion mode. One license per EX4300 is needed	EX4300	S-MX-SAT-EX4300
License to run any supported QFX5100 model as a satellite device in Junos Fusion mode. One license per QFX5100 is needed	QFX5100	S-MX-SAT-QFX5100

See Also

- Junos OS Feature License Keys on page 136
- License Enforcement on page 16
- Configuring the JET Application and its License on a Device Running Junos OS on page 147

Software Feature Licenses for SRX Series Devices

For information about how to purchase a software license, contact your Juniper Networks sales representative at https://www.juniper.net/in/en/contact-us/. Platform support depends on the Junos OS release in your installation.

Each feature license is tied to exactly one software feature, and that license is valid for exactly one device.

NOTE: **For the most up-to-date license models available, contact your Juniper account team.**

See Also

- Understanding Chassis Cluster Licensing Requirements on page 152
- Verifying Licenses on an SRX Series Device in a Chassis Cluster on page 154
- Installing Licenses on the SRX Series Devices in a Chassis Cluster on page 152
- *Understanding Licenses for Logical Systems and Tenant Systems on SRX Series Devices*

Software Features That Require Licenses on EX Series Switches

The following Junos OS features require an Enhanced Feature License (EFL) or Advanced Feature License (AFL) on EX Series devices:

- (EX2200 only) Bidirectional forwarding detection (BFD)
- (EX2200 only) Connectivity fault management (IEEE 802.lag)
- (EX2200 only) Internet Group Management Protocol version 1 (IGMPv1), IGMPv2, and IGMPv3
- (EX2200 and EX3300) OSPFv1/v2 (with 4 active interfaces)
- (EX2200 only) Protocol Independent Multicast (PIM) dense mode, PIM source-specific mode, PIM sparse mode
- (EX2200 and EX3300) Q-in-Q tunneling (IEEE 802.lad)
- (EX2200 only) Real-time performance monitoring (RPM)
- (EX3200, EX4200, EX4500, EX6200, and EX8200) Border Gateway Protocol (BGP) and multiprotocol BGP (MBGP)
- (EX3200, EX4200, EX4500, EX6200, and EX8200) Intermediate System-to-Intermediate System (IS-IS)
- (EX3200, EX4200, EX4500, EX6200, and EX8200) IPv6 protocols: OSPFv3, PIPng, IS-IS for IPv6, IPv6 BGP
- (EX3200, EX4200, EX4500, EX6200, and EX8200) MPLS with RSVP-based label-switched paths (LSPs) and MPLS-based circuit cross-connects (CCCs)

For more details regarding EX Series feature licenses, see "Understanding Software Licenses for EX Series Switches" on page 66.

For information about how to purchase a software license, contact your Juniper Networks sales representative at https://www.juniper.net/in/en/contact-us/.

Software Features That Require Licenses on the QFX Series

NOTE: If you try to configure a feature that is not licensed, you will receive syslog messages saying that you are using a feature that is licensable and that you do not possess a license for the feature. If you try to commit configuration changes for a feature that is not licensed, you will receive a commit warning saying that you have exceeded the allowed license limit for the feature.

NOTE: Virtual Extensible Local Area Network (VXLAN) is not supported on QFX3500 and QFX3600 devices. When you issue the **show licenses** command, you will see VXLAN in the CLI output, but the feature is not enabled.

NOTE: There is no separate license for Virtual Chassis like there is for Virtual Chassis Fabric.

Table 7 on page 31 lists the standard Junos OS features licenses and supported QFX Series devices. For information on disaggregated Junos OS feature licenses on the QFX5200-32C switch, see "Disaggregated Software Features That Require Licenses on the QFX Series" on page 34.

For information about how to purchase a software license, contact your Juniper Networks sales representative.

Table 7: Standard Junos OS Feature Licenses and Model Numbers for QFX Series Devices

Licensed Software Feature	Supported Devices	Number of Licenses Required	Model Number
QFX Series premium feature license for Border Gateway Protocol (BGP), Intermediate System-to-Intermediate System (IS-IS), and Virtual Extensible Local Area Network (VXLAN), and Open vSwitch Database (OVSDB)	QFX10002-36Q switch	One per switch	QFX10002-36Q-PFL
	QFX10002-60C switch		QFX10002-60C-PFL
	QFX10002-72Q switch		QFX10002-72Q-PFL
	QFX10008 switch		QFX10008-PFL
	QFX10016 switch		QFX10016-PFL

Table 7: Standard Junos OS Feature Licenses and Model Numbers for QFX Series Devices (continued)

Licensed Software Feature	Supported Devices	Number of Licenses Required	Model Number
QFX Series advanced feature license for Border Gateway Protocol (BGP), Intermediate System-to-Intermediate System (IS-IS), Multi-protocol Label Switching (MPLS), and Virtual Extensible Local Area Network (VXLAN), and Open vSwitch Database (OVSDB)	QFX10002-36Q switch QFX10002-60C switch QFX10002-72Q switch QFX10008 switch QFX10016 switch	One per switch	QFX10002-36Q-AFL QFX10002-60C-AFL QFX10002-72Q-AFL QFX10008-AFL QFX10016-AFL
QFX Series premium feature license for Border Gateway Protocol (BGP), Intermediate System-to-Intermediate System (IS-IS), and Virtual Extensible Local Area Network (VXLAN), and Open vSwitch Database (OVSDB)	QFX5110-48S switch QFX5110-32Q switch QFX5200-48Y	One per switch, two per Virtual Chassis, and two per Virtual Chassis Fabric	QFX5K-C1-PFL
QFX Series advanced feature license for Border Gateway Protocol (BGP), Intermediate System-to-Intermediate System (IS-IS), Multi-protocol Label Switching (MPLS), and Virtual Extensible Local Area Network (VXLAN), and Open vSwitch Database (OVSDB)	QFX5110-48S switch QFX5110-32Q switch QFX5200-48Y	One per switch	QFX5K-C1-AFL
QFX Series premium feature license for Border Gateway Protocol (BGP), Intermediate System-to-Intermediate System (IS-IS), and Virtual Extensible Local Area Network (VXLAN), and Open vSwitch Database (OVSDB)	QFX5210-64C switch	One per switch	QFX5K-C2-PFL

Table 7: Standard Junos OS Feature Licenses and Model Numbers for QFX Series Devices (continued)

Licensed Software Feature	Supported Devices	Number of Licenses Required	Model Number
QFX Series advanced feature license for Border Gateway Protocol (BGP), Intermediate System-to-Intermediate System (IS-IS), Multi-protocol Label Switching (MPLS), and Virtual Extensible Local Area Network (VXLAN), and Open vSwitch Database (OVSDB)	QFX5210-64C switch	One per switch, two per Virtual Chassis, and two per Virtual Chassis Fabric	QFX5K-C2-AFL
QFX Series advanced feature license for Border Gateway Protocol (BGP), Intermediate System-to-Intermediate System (IS-IS), Multi-protocol Label Switching (MPLS), and Virtual Extensible Local Area Network (VXLAN), and Open vSwitch Database (OVSDB)	QFX3500, QFX3600, QFX5100-48S, and QFX5100-48T switch	One per switch, two per Virtual Chassis, and two per Virtual Chassis Fabric	QFX-JSL-EDGE-ADV1
QFX Series advanced feature license for Border Gateway Protocol (BGP), Intermediate System-to-Intermediate System (IS-IS), Multi-protocol Label Switching (MPLS), and Virtual Extensible Local Area Network (VXLAN) and Open vSwitch Database (OVSDB)	QFX5100-24Q and QFX5100-96S switch	One per switch, two per Virtual Chassis, and two per Virtual Chassis Fabric	QFX5100-HDNSE-LIC
QFX Series advanced feature license for Border Gateway Protocol (BGP)	QFX3100 Director device	One per Node device in a network Node group	QFX-JSL-DRCTR-ADV1
QFX Series advanced feature license for Fibre Channel	QFX3500 switch	One per switch on which fibre channel ports are configured	QFX-JSL-EDGE-FC

Table 7: Standard Junos OS Feature Licenses and Model Numbers for QFX Series Devices (continued)

Licensed Software Feature	Supported Devices	Number of Licenses Required	Model Number
QFX Series advanced feature license for Fibre Channel	QFX3100 Director device	One per QFX3500 Node device on which fibre channel ports are configured	QFX-JSL-DRCTR-FC
QFX Series advanced feature license for Fibre Channel - Capacity 16	QFX3100 Director device	One for up to 16 QFX3500 Node devices on which fibre channel ports are configured	QFX-JSL-DRCTR-FC-C16
QFX Series feature license for enabling fabric mode	QFX3500 and QFX3600 device	One per device	QFX3000-JSL-EDGE-FAB
QFX Series feature license for base software for QFX3000-G QFabric system	QFX3100 Director device	One per QFX3000-G QFabric system	QFX3008-JSL-DRCTR-FAB
QFX Series feature license for base software for QFX3000-M QFabric system	QFX3100 Director device	One per QFX3000-M QFabric system	QFX3000M-JSL-DRCTR-FAB
QFX and EX Series feature license for enabling Media Access Control security (MACsec)	QFX switches that support MACsec. See "Understanding Media Access Control Security (MACsec)" on page 89.	One per switch, two per Virtual Chassis,	EX-QFX-MACSEC-AGG
Virtual Chassis Fabric (VCF) feature license	Any member device in a Virtual Chassis Fabric (VCF)	Two per Virtual Chassis Fabric (VCF)	QFX-VCF-LIC

Disaggregated Software Features That Require Licenses on the QFX Series

Disaggregated Software Feature Licenses on QFX5200 Switches

NOTE: For information on standard Junos OS feature licenses, see "Software Features That Require Licenses on the QFX Series" on page 31.

The Junos OS software is disaggregated from the hardware. With disaggregated Junos OS, you can purchase the following feature licenses, which are available on a perpetual basis:

- Junos Base Software (JBS) license:

  Includes basic layer 2 switching, basic layer 3 routing, multicast, automation, programmability, Zero Touch Provisioning (ZTP) and basic monitoring.

  NOTE: You must purchase the JBS license to use basic functions, but you do not need to install the license key in Junos OS Release 15.1X53-D30. JBS basic functions work with this release without installing the license key. However, you will need to install the license key in a future release of Junos OS to be determined, so make sure to retain the authorization code you received from the License Management System to generate a license key for the JBS license.

- Junos Advanced Software (JAS) license:

  Includes features supported in JBS license and Border Gateway Protocol (BGP), Intermediate System-to-Intermediate System (IS-IS), and Virtual Extensible Local Area Network (VXLAN). You need to install the license key to use these features.

- Junos Premium Software (JPS) license:

  Includes features supported in JAS license and Multi-protocol Label Switching (MPLS) feature set. You need to install the license key to use these features.

For information about how to purchase a software feature license, contact your Juniper Networks sales representative.

Table 8: Disaggregated Junos OS Feature Licenses and Associated SKU's

Licensed Software Features	SKU's
Junos base software (JBS) license	QFX5000-35-JBS
Junos advanced software (JAS) license	QFX5000-35-JAS
Junos premium software (JPS) license	QFX5000-35-JPS

Add, Delete, and Show Licenses

- Adding New Licenses (CLI Procedure) on page 36
- Verifying Junos OS License Installation (CLI) on page 41
- Saving License Keys (CLI) on page 43
- show system license
- Deleting License Keys (CLI) on page 52
- traceoptions (System License) on page 55
- request system license add
- request system license save
- request system license update

- request system license delete
- license on page 62
- license-type on page 63

Adding New Licenses (CLI Procedure)

Before adding new licenses, complete the following tasks:

- Purchase the required licenses.
- Establish basic network connectivity with the router or switch. For instructions on establishing basic connectivity, see the *Getting Started Guide* or *Quick Start Guide* for your device.

There are two ways to add licenses using the Junos OS CLI:

- The **system license keys key** configuration statement enables you to configure and delete license keys in a Junos OS CLI configuration file.
- The **request system license add** operational command installs a license immediately.

NOTE: On QFabric systems, install your licenses in the default partition of the QFabric system and not on the individual components (Node devices and Interconnect devices).

To add licenses, complete one of the following procedures:

- Installing a License Using a Configuration Statement on page 36
- Installing a License Using an Operational Command on page 40

Installing a License Using a Configuration Statement

Starting with Junos OS Release 15.1, you can configure and delete license keys in a Junos OS CLI configuration file. The **system license keys key** statement at the **[edit]** hierarchy level installs a license by using a configuration statement.

NOTE: The system license keys key configuration statement is not required to install a license. The operational command request system license add installs a license immediately. But because the set system license keys key command is a configuration statement, you can use it to install a license as part of a configuration commit, either directly or by configuration file.

The license keys are validated and installed after a successful commit of the configuration file. If a license key is invalid, the commit fails and issues an error message. You can configure individual license keys or multiple license keys by issuing Junos OS CLI commands or by loading the license key configuration contained in a file. All installed license keys are stored in the **/config/license/** directory.

Select a procedure to install a license using configuration:

- Installing Licenses Using the CLI Directly on page 37
- Installing Licenses Using a Configuration File on page 38

Installing Licenses Using the CLI Directly

To install an individual license key using the Junos OS CLI:

1. Issue the **set system license keys key *name*** statement.

   The ***name*** parameter includes the license ID and the license key. For example:

   ```
   [edit]
   user@device# set system license keys key "JUNOS_TEST_LIC_FEAT xxxxxx xxxxxx
     xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx"
   ```

   To install multiple license keys in the Junos OS CLI, issue the **set system license keys key *name*** statement for each license key to install. For example:

   ```
   [edit]
   user@device# set system license keys key "key_1"
   set system license keys key "key_2"
   set system license keys key "key_2"
   set system license keys key "key_4"
   ```

2. Issue the **commit** command.

   ```
   [edit]
   user@device# commit
   commit complete
   ```

3. Verify that the license key was installed.

   For example:

   ```
   user@device# run show system license
   ```

   ```
   License usage:
                                  Licenses     Licenses    Licenses    Expiry
     Feature name                      used    installed      needed
     sdk-test-feat1                       0            1           0    permanent

   Licenses installed:
     License identifier: JUNOS_TEST_LIC_FEAT
     License version: 2
     Features:
       sdk-test-feat1   - JUNOS SDK Test Feature 1
         permanent
   ```

   Alternatively, you can issue the **show system license** command from operational mode.

Installing Licenses Using a Configuration File

Before you begin, prepare the configuration file. In this example, use the Unix shell **cat** command to write the **license.conf** file:

1. Go to the shell.

```
[edit]
user@device# exit
user@device> exit
%
```

2. Open the new **license.conf** file.

```
% cat > license.conf
```

3. Type the configuration information for the license key or keys:

   - For a single license, for example, type the following content:

```
system {
    license {
        keys {
           key "JUNOS_TEST_LIC_FEAT xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx
xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx";
        }
    }
}
```

   - For multiple license keys, for example, type something like this:

```
system {
 license {
  keys {
   key "key_1"
   key "key_2"
   key "key_3"
   ...
   key "key_n"
   }
 }
}
```

4. Press Ctrl+d to save the file.

To install a license key configuration in a file:

1. Go to the CLI configuration mode.

```
% cli
user@device> configure
[edit]
```

```
user@device#
```

2. Load and merge the license configuration file.

   For example:

```
user@device# load merge license.conf
load complete
```

3. Issue the **show | compare** command to see the configuration.

   For example:

```
[edit]
user@device# show | compare
[edit system]
  +   license {
  +       keys {
  +           key "JUNOS_TEST_LIC_FEAT xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx
  xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx";
  +       }
  +   }
```

4. Issue the **commit** command.

```
[edit]
user@device# commit
```

5. To verify that the license key was installed, issue the **show system license** command.

   For example:

```
root@switch> show system license
```

```
License usage:
                                Licenses     Licenses    Licenses    Expiry
  Feature name                       used    installed      needed
  sdk-test-feat1                        0            1           0    permanent

Licenses installed:
  License identifier: JUNOS_TEST_LIC_FEAT
  License version: 2
  Features:
    sdk-test-feat1   - JUNOS SDK Test Feature 1
      permanent
```

Installing a License Using an Operational Command

Complete the procedure that relates to your system:

- Adding a License to a Device with a Single Routing Engine on page 40
- Adding a License to a Device with Dual Routing Engines on page 40

Adding a License to a Device with a Single Routing Engine

To add a new license key to the device using an operational command:

1. From the CLI operational mode, enter one of the following CLI commands:
   - To add a license key from a file or URL, enter the following command, specifying the filename or the URL where the key is located:

     ```
     user@host> request system license add filename | url
     ```

   - To add a license key from the terminal, enter the following command:

     ```
     user@host> request system license add terminal
     ```

2. When prompted, enter the license key, separating multiple license keys with a blank line.

   If the license key you enter is invalid, an error appears in the CLI output when you press Ctrl+d to exit license entry mode.

3. Go on to "Verifying Junos OS License Installation (CLI)" on page 41.

Adding a License to a Device with Dual Routing Engines

On routers that have graceful Routing Engine switchover (GRES) enabled, after successfully adding the new license on the master Routing Engine, the license keys are automatically synchronized on the backup Routing Engine as well. However, in case GRES is not enabled, the new license is added on each Routing Engine separately. This ensures that the license key is enabled on the backup Routing Engine during changeover of mastership between the Routing Engines.

To add a new license key to a router with dual Routing Engines without GRES:

1. After adding the new license key on the master Routing Engine, use the **request chassis routing-engine master switch** command to have the backup Routing Engine become the master Routing Engine.
2. Log in to the active Routing Engine and add the new license key, repeat the same step.

NOTE: Adding a license key to the router or switch might be delayed if a kernel resynchronization operation is in progress at that time. The following message is displayed on the CLI when the license-adding operation is about to be delayed:
A kernel re-sync operation is in progress. License update may take several minutes to complete.

See Also

- Deleting License Keys (CLI) on page 52
- Junos OS Feature Licenses on page 15
- Verifying Junos OS License Installation (CLI) on page 41
- **request system license add on page 57**

Verifying Junos OS License Installation (CLI)

To verify Junos OS license management, perform the following tasks:

- Displaying Installed Licenses on page 41
- Displaying License Usage on page 42

Displaying Installed Licenses

Purpose Verify that the expected licenses are installed and active on the device.

Action From the CLI, enter the **show system license** command.

Sample Output

```
user@host> show system license
License usage:
                    Licenses     Licenses    Licenses    Expiry
  Feature name         used    installed      needed
  subscriber-acct         0            1           0    permanent
  subscriber-auth         0            1           0    permanent
  subscriber-addr         0            1           0    permanent
  subscriber-vlan         0            1           0    permanent
  subscriber-ip           0            1           0    permanent
  scale-subscriber        0         1000           0    permanent
  scale-l2tp              0         1000           0    permanent
  scale-mobile-ip         0         1000           0    permanent

Licenses installed:
  License identifier: E000185416
  License version: 2
  Features:
    subscriber-acct  - Per Subscriber Radius Accounting
      permanent
    subscriber-auth  - Per Subscriber Radius Authentication
      permanent
```

```
  subscriber-addr  - Address Pool Assignment
    permanent
  subscriber-vlan  - Dynamic Auto-sensed Vlan
    permanent
  subscriber-ip    - Dynamic and Static IP
    permanent
```

Meaning The output shows a list of the license usage and a list of the licenses installed on the device. Verify the following information:

- Each license is present. Licenses are listed in ascending alphanumeric order by license ID.
- The state of each license is **permanent**.

NOTE: A state of invalid indicates that the license key is not a valid license key. Either it was entered incorrectly or it is not valid for the specific device.

- The feature for each license is the expected feature. The features enabled are listed by license. An all-inclusive license has all features listed.
- All configured features have the required licenses installed. The Licenses needed column must show that no licenses are required.

See Also
- Adding New Licenses (CLI Procedure) on page 36

Displaying License Usage

Purpose Verify that the licenses fully cover the feature configuration on the device.

Action From the CLI, enter the **show system license usage** command.

Sample Output

```
user@host> show system license usage
                Licenses     Licenses    Licenses    Expiry
Feature name         used    installed      needed
subscriber-addr         1            0           1    29 days
scale-subscriber        0         1000           0    permanent
scale-l2tp              0         1000           0    permanent
scale-mobile-ip         0         1000           0    permanent
```

Meaning The output shows any licenses installed on the device and how they are used. Verify the following information:

- Any configured licenses appear in the output. The output lists features in ascending alphabetical order by license name. The number of licenses appears in the third column. Verify that you have installed the appropriate number of licenses.
- The number of licenses used matches the number of configured features. If a licensed feature is configured, the feature is considered used. The sample output shows that the subscriber address pooling feature is configured.
- A license is installed on the device for each configured feature. For every feature configured that does not have a license, one license is needed.

  For example, the sample output shows that the subscriber address feature is configured but that the license for the feature has not yet been installed. The license must be installed within the remaining grace period to be in compliance.

See Also
- Adding New Licenses (CLI Procedure) on page 36

Saving License Keys (CLI)

To save the licenses installed on a device:

1. From operational mode, do one of the following tasks
   - To save the installed license keys to a file or URL, enter the following command:

     ```
     user@host> request system license save filename | url
     ```

     For example, the following command saves the installed license keys to a file named **license.config**:

     ```
     user@host>request system license save license.config
     ```

   - To output installed license keys to the terminal, enter the following command:

     ```
     user@host> request system license save terminal
     ```

See Also
- Adding New Licenses (CLI Procedure) on page 36

show system license

Syntax

```
show system license
<installed | key-content filename | keys | revoked-info | usage>
```

Release Information

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 11.1 for the QFX Series.
Command introduced in Junos OS Release 13.3 for the MX104 Universal Routing Platforms.
Customer ID added to output of data center users in Junos OS Release 15.1.
Corrected output for duration of license added in Junos OS Release 17.4R1.

Description

Display licenses and information about how they are used.

Options

none—Display all license information.

key-content *filename*—(Optional) Display license key contents of the specified filename.

installed—(Optional) Display installed licenses only.

keys—(Optional) Display a list of license keys. Use this information to verify that each expected license key is present.

revoked-info—(Optional) Display information about revoked licenses.

usage—(Optional) Display the state of licensed features.

Required Privilege Level

maintenance

See Also

List of Sample Output

show system license keys (MX104 Routers) on page 51
show system license usage (MX104 Routers) on page 51
show system license (QFX Series) on page 51
show system license (QFX5110 Switch with Disaggregated Feature License) on page 51
show system license key-content srx_1year_sub.lic on page 52

Output Fields Table 9 on page 45 lists the output fields for the **show system license** command. Output fields are listed in the approximate order in which they appear.

Table 9: show system license Output Fields

Field Name	Field Description
Feature name	Name assigned to the configured feature. You use this information to verify that all the features for which you installed licenses are present.
Licenses used	Number of licenses used by a router or switch. You use this information to verify that the number of licenses used matches the number configured. If a licensed feature is configured, the feature is considered used. NOTE: In Junos OS Release 10.1 and later, the **Licenses used** column displays the actual usage count based on the number of active sessions or connections as reported by the corresponding feature daemons. This is applicable for scalable license-based features such as Subscriber Access (**scale-subscriber**), L2TP (**scale-l2tp**), Mobile IP (**scale-mobile-ip**), and so on.
Licenses installed	Information about the installed license key: • **License identifier**—Identifier associated with a license key. • **State**—State of the license key:**valid** or **invalid**. An **invalid** state indicates that the key was entered incorrectly or is not valid for the specific device. • **License version**—Version of a license. The version indicates how the license is validated, the type of signature, and the signer of the license key. • **Customer ID**—Name of the customer license is for. Feature added as of Junos OS Release 15.1 for data center customers (for example QFX Series platform users). • **Valid for device**—Device that can use a license key. • **Group defined**—Group membership of a device. • **Features**—Feature associated with a license, such as data link switching (DLSw).
Licenses needed	Number of licenses required for features being used but not yet properly licensed.
Expiry	Amount of time left within the grace period before a license is required for a feature being used.

Sample Output

show system license (vMX Routers with Juniper Agile Licensing)

```
user@host> show system license

License usage:
                                Licenses     Licenses    Licenses    Expiry
  Feature name                       used    installed      needed
  VMX-SCALE                             0            1           0    permanent
  VMX-BANDWIDTH                         0       130000           0    permanent
  mobile-next-DPI-base                  0         1000           0    permanent
```

```
  mobile-next-policy-prepaid-scaling        0      1000          0    permanent
  mobile-next-http-app-scaling              0      1000          0    permanent
  mobile-next-scaling                       0      1000          0    permanent
  logical-system                            0         1          0    permanent
  ax411-wlan-ap                             0         2          0    permanent
  dynamic-vpn                               0         2          0    permanent
  scale-mobile-ip                           0      1000          0    permanent
  scale-l2tp                                0      1000          0    permanent
  scale-subscriber                          0     64010          0    permanent

Licenses installed:
  License identifier: RMS818090001
  License version: 1
  Software Serial Number: AID000000001
  Customer ID: LABJuniperTest
  License count: 1
  Features:
    VMX-SCALE        - Max scale supported by the VMX
      date-based, 2017-03-15 05:30:00 IST - 2017-05-14 05:30:00 IST

  License identifier: RMS818020001
  License version: 1
  Software Serial Number: AID000000001
  Customer ID: vMX-JuniperNetworks
  License count: 1
  Features:
    VMX-SCALE        - Max scale supported by the VMX
      permanent
…
```

show system license

```
user@host> show system license

License usage:
                                Licenses     Licenses    Licenses    Expiry
  Feature name                       used    installed      needed
  subscriber-accounting                 2            2           0    permanent
  subscriber-authentication             1            2           0    permanent
  subscriber-address-assignment         2            2           0    permanent
  subscriber-vlan                       2            2           0    permanent
  subscriber-ip                         0            2           0    permanent
  scale-subscriber                      2            3           0    permanent
  scale-l2tp                            4            5           0    permanent
  scale-mobile-ip                       1            2           0    permanent

Licenses installed:
  License identifier: XXXXXXXXXX
  License version: 2
 Customer ID: ACME CORPORATIOM
  Features:
    subscriber-accounting - Per Subscriber Radius Accounting
      permanent
    subscriber-authentication - Per Subscriber Radius Authentication
      permanent
    subscriber-address-assignment - Radius/SRC Address Pool Assignment
      permanent
    subscriber-vlan  - Dynamic Auto-sensed Vlan
      permanent
```

```
  subscriber-ip    - Dynamic and Static IP
    permanent
```

show system license installed

```
user@host> show system license installed
```

```
License identifier: XXXXXXXXXX
License version: 2
Features:
  subscriber-accounting - Per Subscriber Radius Accounting
    permanent
  subscriber-authentication - Per Subscriber Radius Authentication
    permanent
  subscriber-address-assignment - Radius/SRC Address Pool Assignment
    permanent
  subscriber-vlan  - Dynamic Auto-sensed Vlan
    permanent
  subscriber-ip    - Dynamic and Static IP
    permanent
```

show system license keys

```
user@host> show system license keys
```

```
XXXXXXXXXX xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx
        xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx
        xxxxxx xxxxxx xxx
```

show system license usage

```
user@host> show system license usage
```

```
License usage:
                              Licenses     Licenses    Licenses    Expiry
  Feature name                    used    installed      needed
  subscriber-accounting              2            2           0    permanent
  subscriber-authentication          1            2           0    permanent
  subscriber-address-assignment      2            2           0    permanent
  subscriber-vlan                    2            2           0    permanent
  subscriber-ip                      0            2           0    permanent
  scale-subscriber                   2            3           0    permanent
  scale-l2tp                         4            5           0    permanent
  scale-mobile-ip                    1            2           0    permanent
```

show system license (MX104 Routers)

In the following output, ports 0 and 1 are activated by installing the license to activate the first two built-in ports.

```
user@host> show system license
```

```
License usage:
                              Licenses     Licenses    Licenses    Expiry
  Feature name                    used    installed      needed
  scale-subscriber                   0         1000           0    permanent
  scale-l2tp                         0         1000           0    permanent
  scale-mobile-ip                    0         1000           0    permanent
```

```
  MX104-2x10Gig-port-0-1                0           1           0    permanent

Licenses installed:
  License identifier: XXXXXXXXXX
  License version: 2
  Features:
    MX104-2x10Gig-port-0-1 - MX104 2X10Gig Builtin Port(xe-2/0/0 & xe-2/0/1)
upgrade
      permanent
```

show system license installed (MX104 Routers)

In the following output, ports 0 and 1 are activated by installing the license to activate the first two built-in ports.

```
user@host > show system license installed
```

```
License identifier: XXXXXXXXXX
  License version: 2
  Features:
    MX104-2x10Gig-port-0-1 - MX104 2X10Gig Builtin Port(xe-2/0/0 & xe-2/0/1)
upgrade
      permanent
```

show system license keys (MX104 Routers)

In the following output, ports 0 and 1 are activated by installing the license to activate the first two built-in ports.

```
user@host > show system license keys
```

```
XXXXXXXXXX xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx
           xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx
           xxxxxx xxxx
```

show system license usage (MX104 Routers)

In the following output, ports 0 and 1 are activated by installing the license to activate the first two built-in ports.

```
user@host > show system license usage
```

```
           Licenses     Licenses    Licenses    Expiry
  Feature name                        used    installed      needed
  scale-subscriber                       0         1000           0    permanent
  scale-l2tp                             0         1000           0    permanent
  scale-mobile-ip                        0         1000           0    permanent
  MX104-2x10Gig-port-0-1                 0            1           0    permanent
```

show system license (MX104 Routers)

In the following output, ports 2 and 3 are activated by installing the license to activate the next two built-in ports after installing the license to activate the first two built-in ports.

```
user@host > show system license
```

```
License usage:
                                Licenses     Licenses    Licenses    Expiry
  Feature name                       used    installed      needed
  scale-subscriber                      0         1000           0    permanent
  scale-l2tp                            0         1000           0    permanent
  scale-mobile-ip                       0         1000           0    permanent
  MX104-2x10Gig-port-0-1                0            1           0    permanent
  MX104-2x10Gig-port-2-3                0            1           0    permanent

Licenses installed:
  License identifier: XXXXXXXXXX
  License version: 2
  Features:
    MX104-2x10Gig-port-0-1 - MX104 2X10Gig Builtin Port(xe-2/0/0 & xe-2/0/1)
upgrade
      permanent

  License identifier: XXXXXXXXXX
  License version: 2
  Features:
    MX104-2x10Gig-port-2-3 - MX104 2X10Gig Builtin Port(xe-2/0/2 & xe-2/0/3)
upgrade
      permanent
```

show system license installed (MX104 Routers)

In the following output, ports 2 and 3 are activated by installing the license to activate the next two built-in ports after installing the license to activate the first two built-in ports.

```
user@host > show system license installed
```

```
License identifier: XXXXXXXXXX
  License version: 2
  Features:
    MX104-2x10Gig-port-0-1 - MX104 2X10Gig Builtin Port(xe-2/0/0 & xe-2/0/1)
upgrade
      permanent

  License identifier: XXXXXXXXXX
  License version: 2
  Features:
    MX104-2x10Gig-port-2-3 - MX104 2X10Gig Builtin Port(xe-2/0/2 & xe-2/0/3)
upgrade
      permanent
```

show system license keys (MX104 Routers)

In the following output, ports 2 and 3 are activated by installing the license to activate the next two built-in ports after installing the license to activate the first two built-in ports.

```
user@host > show system license keys
```

```
XXXXXXXXXX xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx
           xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx
           xxxxxx xxxx
```

```
XXXXXXXXXX xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx
           xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx
           xxxxxx xxxx
```

show system license usage (MX104 Routers)

In the following output, ports 2 and 3 are activated by installing the license to activate the next two built-in ports after installing the license to activate the first two built-in ports.

```
user@host > show system license usage
```

```
          Licenses     Licenses    Licenses    Expiry
  Feature name                       used    installed      needed
  scale-subscriber                      0         1000           0    permanent
  scale-l2tp                            0         1000           0    permanent
  scale-mobile-ip                       0         1000           0    permanent
  MX104-2x10Gig-port-0-1                0            1           0    permanent
  MX104-2x10Gig-port-2-3                0            1           0    permanent
```

show system license (MX104 Routers)

In the following output, ports 0,1,2, and 3 are activated by installing a single license key to activate all four built-in ports.

```
user@host > show system license
```

```
License usage:
                                Licenses     Licenses    Licenses    Expiry
  Feature name                      used    installed      needed
  scale-subscriber                      0         1000           0    permanent
  scale-l2tp                            0         1000           0    permanent
  scale-mobile-ip                       0         1000           0    permanent
  MX104-2x10Gig-port-0-1                0            1           0    permanent
  MX104-2x10Gig-port-2-3                0            1           0    permanent

Licenses installed:
  License identifier: XXXXXXXXXX
  License version: 2
  Features:
    MX104-2x10Gig-port-0-1 - MX104 2X10Gig Builtin Port(xe-2/0/0 & xe-2/0/1)
upgrade
      permanent
    MX104-2x10Gig-port-2-3 - MX104 2X10Gig Builtin Port(xe-2/0/2 & xe-2/0/3)
upgrade
      permanent
```

show system license installed (MX104 Routers)

In the following output, ports 0,1,2, and 3 are activated by installing a single license key to activate all four built-in ports.

```
user@host > show system license installed
```

```
License identifier: XXXXXXXXXX
  License version: 2
  Features:
```

```
    MX104-2x10Gig-port-0-1 - MX104 2X10Gig Builtin Port(xe-2/0/0 & xe-2/0/1)
upgrade
      permanent
    MX104-2x10Gig-port-2-3 - MX104 2X10Gig Builtin Port(xe-2/0/2 & xe-2/0/3)
upgrade
      permanent
```

show system license keys (MX104 Routers)

In the following output, ports 0,1,2, and 3 are activated by installing a single license key to activate all four built-in ports.

```
user@host > show system license keys

XXXXXXXXX  xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx
           xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx
           xxxxxx xxxxxx x
```

show system license usage (MX104 Routers)

In the following output, ports 0,1,2, and 3 are activated by installing a single license key to activate all four built-in ports.

```
user@host > show system license usage
          Licenses     Licenses    Licenses    Expiry
  Feature name                       used    installed      needed
  scale-subscriber                      0         1000           0    permanent
  scale-l2tp                            0         1000           0    permanent
  scale-mobile-ip                       0         1000           0    permanent
  MX104-2x10Gig-port-0-1                0            1           0    permanent
  MX104-2x10Gig-port-2-3                0            1           0    permanent
```

show system license (QFX Series)

```
user@switch> show system license
License usage:
                  Licenses     Licenses    Licenses    Expiry
  Feature name         used    installed      needed
  qfx-edge-fab            1            1           1    permanent
Licenses installed:
  License identifier: JUNOS417988
  License version: 1
  Features:
    qfx-edge-fab  -        QFX3000 Series QF/Node feature license
      permanent
```

show system license (QFX5110 Switch with Disaggregated Feature License)

```
user@switch> show system license
License usage:
                                 Licenses     Licenses    Licenses    Expiry
  Feature name                       used    installed      needed
  bgp                                   0            1           0    2017-07-05
 00:00:00 UTC
```

```
 isis                                0           1           0    2017-07-05
00:00:00 UTC
 vxlan                               0           1           0    2017-07-05
00:00:00 UTC
 ovsdb                               0           1           0    2017-07-05
00:00:00 UTC
 jbs1                                0           1           0    2017-07-02
00:00:00 UTC
 upgrade1                            0           1           0    2017-07-05
00:00:00 UTC

Licenses installed:
  License identifier: JUNOS797095
  License version: 4
  Software Serial Number: 91730A00223925
  Customer ID: Juniper
  Features:
    JUNOS-BASE-SERVICES-CLASS-1 - QFX Junos Base Services license for Class 1 HW

      date-based, 2016-07-01 00:00:00 UTC - 2017-07-02 00:00:00 UTC

  License identifier: JUNOS797646
  License version: 4
  Software Serial Number: 91730A00224207
  Customer ID: Juniper
  Features:
    CLASS-1-JUNOS-BASE-ADVANCED-UPGRADE - Class 1 Junos Base to Advanced Services
Upgrade
      date-based, 2016-07-04 00:00:00 UTC - 2017-07-05 00:00:00 UTC

{master:0}
```

show system license key-content srx_1year_sub.lic

```
License Key Content:
  License Id: LICENSE-1
  License version: 4
  Valid for device: CW2716AF0740
  Features:
    idp-sig          - IDP Signature
      date-based, 2016-07-03 00:00:00 GMT - 2017-07-03 00:00:00 GMT
```

Deleting License Keys (CLI)

Before deleting a license, ensure that the features enabled by the license will not be needed.

You can use the **request system license delete** operational command, or the **delete** or **deactivate** configuration command to delete a license:

- Using the Operational Command to Delete Licenses on page 53
- Using a Configuration Command to Delete Licenses on page 53

Using the Operational Command to Delete Licenses

To delete licenses using the **request system license delete** command:

1. Display the licenses available to be deleted.

```
user@host> request system license delete license-identifier-list ?
Possible completions:
  E00468XXX4           License key identifier
  JUNOS10XXX1          License key identifier
  JUNOS10XXX2          License key identifier
  JUNOS10XXX3          License key identifier
  JUNOS10XXX4          License key identifier
  [                    Open a set of values
```

2. To delete a license key or keys from a device using the CLI operational mode, select one of the following methods:

   - Delete a single license by specifying the license ID. Using this option, you can delete only one license at a time.

     ```
     user@host> request system license delete license-identifier
     ```

   - Delete all license keys from the device.

     ```
     user@host> request system license delete all
     ```

   - Delete multiple license keys from the device. Specify the license identifier for each key and enclose the list of identifiers in brackets.

     ```
     user@host> request system license delete license-identifier-list [JUNOS10XXX1
       JUNOS10XXX3 JUNOS10XXX4 ...]
     ```

     ```
     Delete license(s) ?
      [yes,no] (no) yes
     ```

3. Verify the license was deleted by entering the **show system license** command.

Using a Configuration Command to Delete Licenses

Starting in Junos OS Release 16.1, to remove licenses from the configuration, you can use either the **delete** or **deactivate** configuration command. The **delete** command deletes a statement or identifier, and all subordinate statements and identifiers contained within the specified statement path are deleted with it. The **deactivate** command adds the **inactive:** tag to a statement, effectively commenting out the statement or identifier from the configuration. Statements or identifiers marked as inactive do not take effect when you issue the **commit** command. To remove the **inactive:** tag from a statement, issue the **activate** command. Statements or identifiers that have been activated take effect when you next issue the **commit** command.

The following procedure uses the **delete** command, but you could use the **deactivate** command as well.

To delete one or all licenses using the **delete** command:

NOTE: You can use the deactivate command instead of the delete command in this procedure.

1. Display the licenses available to be deleted.

   Issue the **run request system license delete license-identifier-list ?** command from the configuration mode of the CLI.

   ```
   [edit]
   user@host# run request system license delete license-identifier-list ?
   ```

   A list of licenses on the device is displayed:

   ```
   Possible completions:
     E00468XXX4           License key identifier
     JUNOS10XXX1          License key identifier
     JUNOS10XXX2          License key identifier
     JUNOS10XXX3          License key identifier
     JUNOS10XXX4          License key identifier
     [                    Open a set of values
   ```

2. Delete the license or licenses you want.

   - To delete a single license, for example:

     ```
     [edit]
     user@host# delete system license keys key “E00468XXX4”
     ```

   - To delete all licenses, for example:

     ```
     [edit]
     user@host# delete system license keys
     ```

3. Commit the configuration by entering the **commit** command.

4. Verify the license was deleted by entering the **show system license** command.

traceoptions (System License)

Syntax

```
traceoptions {
file {
  filename;
  files number;
  match regular-expression;
  size maximum-file-size;
  (world-readable | no-world-readable);
}
flag flag;
no-remote-trace;
}
```

Hierarchy Level

```
[edit system license]
```

Release Information

Statement introduced in Junos OS Release 8.5 for SRX Series and vSRX.
Statement introduced in Junos OS Release 14.1X53-D10 for EX Series and QFX Series.
Statement introduced in Junos OS Release 15.1 for M Series, MX Series, and T Series.

Description

Set trace options for licenses.

Options

file—Configure the trace file information.

filename—Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. All files are placed in the directory **/var/log**. By default, the name of the file is the name of the process being traced.

files *number*—Maximum number of trace files. When a trace file named **trace-file** reaches its maximum size, it is renamed **trace-file.0**, then **trace-file.1**, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

If you specify a maximum number of files, you also must specify a maximum file size with the **size *maximum file-size*** option.

Range: 2 through 1000 files

Default: 10 files

match *regular-expression*—Refine the output to include lines that contain the regular expression.

size *size*—Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). If you specify a maximum file size, you also must specify a maximum number of trace files with the **files *number*** option.

Range: 10 KB through 1 GB

Default: 128 KB

world-readable | no-world-readable—By default, log files can be accessed only by the user who configures the tracing operation. The **world-readable** option enables any user to read the file. To explicitly set the default behavior, use the **no-world-readable** option.

flag *flag*—Specify which tracing operation to perform. To specify more than one tracing operation, include multiple **flag** statements. You can include the following flags.

- **all**—Trace all operations.
- **config**—Trace license configuration processing.
- **events**—Trace licensing events and their processing.

no-remote-trace—Disable the remote tracing.

Required Privilege Level

trace—To view this statement in the configuration.
trace-control—To add this statement to the configuration.

request system license add

Syntax

```
request system license add (filename | terminal)
```

Release Information

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 9.5 for SRX Series devices.
Command introduced in Junos OS Release 11.1 for the QFX Series.
Added additional information section on XML RPC in Junos OS Release 17.4.

Description

Adding a license key to the Junos OS devices to activate the feature.

Options

filename—License key from a file or URL. Specify the filename or the URL where the key is located.

terminal—License key from the terminal.

Additional Information

The **| display xml rpc** filter returns "xml rpc equivalent of this command is not available," the following RPC is supported for license installation:

The following RPC is supported for license installation:

```
<rpc>
<request-license-add>
<key-data> key </key-data>
</request-license-add>
</rpc>
```

Where ***key-data*** is the license key data.

```
<rpc>
<request-license-add>
<filename> key-file </filename>
</request-license-add>
</rpc>
```

Where ***source*** is the URL of the source license key file.

Required Privilege Level

maintenance

List of Sample Output

request system license add on page 58

Output Fields

When you enter this command, you are provided feedback on the status of your request.

Sample Output

request system license add

```
user@host> request system license add terminal

XXXXXXXXXX xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx
         xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx
         xxxxxx xxxxxx xxx

XXXXXXXXXX: successfully added
add license complete (no errors)
```

request system license save

Syntax request system license save (*filename* | terminal)

Release Information
Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 11.1 for the QFX Series.
Command introduced in Junos OS Release 9.5 for SRX Series devices.
Added additional information section on XML RPC in Junos OS Release 17.4.

Description Save installed license keys to a file or URL.

NOTE: Starting in Junos OS Release 18.3R1, the display xml rpc CLI option is supported for request system license add and request system license save commands while installing licenses on Juniper Networks devices.

Options ***filename***—License key from a file or URL. Specify the filename or the URL where the key is located.

terminal—License key from the terminal.

Additional Information The following RPC is supported for saving installed license keys to a file or URL:

```
<rpc>
<request-license-save>
<filename>destination</filename>
</request-license-save>
</rpc>
```

Where ***destination*** is the URL of the destination license key file.

Required Privilege Level maintenance

List of Sample Output request system license save on page 59

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

request system license save

```
user@host> request system license save ftp://user@host/license.conf
```


request system license update

Syntax request system license update

Release Information Command introduced in Junos OS Release 9.5.

Description If your device supports initial install from the EMS server in Products Supporting Juniper Agile Licensing, you can use this command to install all licenses from the EMS server. You can also autoupdate license keys from the LMS or EMS server.

NOTE: The request system license update command always uses the default Juniper license server:

- For Juniper Agile Licensing (JAL) keys: https://license.juniper.net/
- For non-JAL keys: https://ae1.juniper.net

Options **trial**—(For non-Juniper Agile Licensing keys only) Immediately updates trial license keys from the LMS server.

Required Privilege Level maintenance

List of Sample Output
request system license update on page 60
request system license update trial on page 60

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

request system license update

```
user@host> request system license update

Trying to update license keys from https://ae1.juniper.net has been sent, use
show system license to check status.
```

request system license update trial

```
user@host> request system license update trial

Request to automatically update trial license keys from https://ae1.juniper.net
has been sent, use show system license to check status.
```

request system license delete

Syntax

request system license delete (*license-identifier* | license-identifier-list [*licenseid001 licenseid002 licenseid003*] | all)

Release Information

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 11.1 for the QFX Series.
Option **license-identifier-list** introduced in Junos OS Release 13.1.

Description

Delete a license key. You can choose to delete one license at a time, all licenses at once, or a list of license identifiers enclosed in brackets.

Options

license-identifier—Text string that uniquely identifies a license key.

license-identifier-list [*licenseid001 licenseid002 licenseid003....*]—Delete multiple license identifiers as a list enclosed in brackets.

all—Delete all licenses on the device.

Required Privilege Level

maintenance

license

Syntax

```
license {
  autoupdate {
    url url <password password>;
  }
  keys {
    key key
  }
  renew {
    before-expiration number;
    interval interval-hours;
  }
  traceoptions {
    file {
      filename;
      files number;
      match regular-expression;
      size maximum-file-size;
      (world-readable | no-world-readable);
    }
    flag flag;
    no-remote-trace;
  }
}
```

Hierarchy Level

```
[edit system]
```

Release Information

Statement introduced in Junos OS Release 8.5 for SRX Series and vSRX.
Options **keys** introduced in Junos OS Release 14.1X53-D10.
Statement introduced in Junos OS Release 14.1X53-D10 for EX Series and QFX Series, with option **keys** included.
Statement introduced in Junos OS Release 15.1 for M Series, MX Series, PTX Series, and T Series, with option **keys** included.

Description

Specify license information for the device.

Options

autoupdate—Autoupdate license keys from license servers.

before-expiration ***number***—License renewal lead time before expiration, in days.

Range: 0 through 60 days

interval ***interval-hours***—License checking interval, in hours.

Range: 1 through 336 hours

keys key ***key***—Configure one or more license keys. For example,

```
[edit]
user@device# set system license keys key "key_1"
user@device# set system license keys key "key_2"
user@device# set system license keys key "key_3"
user@device# set system license keys key "key_4"
user@device# commit
commit complete
```

renew—License renewal lead time and checking interval.

url—URL of a license server.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level
system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

license-type

Syntax
```
license-type license deployment-scope [ deployments ];
```

Hierarchy Level
```
[edit system extensions providersprovider-id]
```

Release Information
Statement introduced in Junos OS Release 11.1 for FX Series switches.

Description
Configure the license type and the scope of SDK application deployment.

Options
license—Type of license. Obtain correct value from the application's provider.

deployment—Scope of SDK application deployment. You can configure a set of deployments. Obtain correct value from the application's provider.

Required Privilege Level
admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

CHAPTER 2

Understanding Licenses for EX and QFX Series

Understanding Licenses for EX Series

Understanding Software Licenses for EX Series Switches

To enable and use some of the Juniper Networks operating system (Junos OS) features, you must purchase, install, and manage separate software licenses. If the switch has the appropriate software license, you can configure and use these features.

The Junos OS feature license (that is, the purchased authorization code) is universal. However, to conform to Junos OS feature licensing requirements, you must install a unique license key (a combination of the authorization code and the switch's serial number) on each switch.

For a Virtual Chassis deployment, two license keys are recommended for redundancy—one for the device in the master role and the other for the device in the backup role:

- In an EX8200 Virtual Chassis, the devices in the master and backup roles are always XRE200 External Routing Engines.
- In all other Virtual Chassis, the devices in the master and backup roles are switches.

You do not need additional license keys for Virtual Chassis member switches that are in the linecard role or for the redundant Routing Engine (RE) modules or the redundant Switch Fabric and Routing Engine (SRE) modules in an EX8200 member switch.

This topic describes:

Purchasing a Software Feature License

The following sections list features that require separate licenses. To purchase a software license, contact your Juniper Networks sales representative (https://www.juniper.net/us/en/contact-us/sales-offices). You will be asked to supply the chassis serial number of your switch; you can obtain the serial number by running the **show chassis hardware** command.

NOTE: You are required to provide the 12-digit serial number when purchasing a license for an XRE200 External Routing Engine in an EX8200 Virtual Chassis.

The serial number listed on the XRE200 External Routing Engine serial ID label is 16 digits long. Use the last 12 digits of the 16-digit serial number to purchase the license.

You can use the **show chassis hardware** command output to display the 12-digit serial number of the XRE200 External Routing Engine.

Features Requiring a License on EX2200 Switches

For EX2200 switches, the following features can be added to basic Junos OS by installing an enhanced feature license (EFL):

- Bidirectional Forwarding Detection (BFD)
- Connectivity fault management (IEEE 802.1ag)
- IGMP (Internet Group Management Protocol) version 1 (IGMPv1), IGMPv2, and IGMPv3
- OSPFv1/v2 (with four active interfaces)
- Protocol Independent Multicast (PIM) dense mode, PIM source-specific mode, PIM sparse mode
- Q-in-Q tunneling (IEEE 802.1ad)
- Real-time performance monitoring (RPM)
- Virtual Router
- Virtual Router Redundancy Protocol (VRRP)

Table 10 on page 67 lists the EFLs that you can purchase for EX2200 switch models. If you have the license, you can run all of the enhanced software features mentioned above on your EX2200 switch.

Table 10: Junos OS Part Number on EX2200 Switches

Switch Model	Part Number
EX2200-C-12P-2G EX2200-C-12T-2G	EX-12-EFL
EX2200-24T-4G EX2200-24P-4G EX2200-24T-DC-4G	EX-24-EFL
EX2200-48T-4G EX2200-48P-4G	EX-48-EFL

Features Requiring a License on EX2300 Switches

EX2300 switches have enhanced feature licenses (EFLs).

To use the following features on the EX2300 switches, you must install an EFL:

- Bidirectional Forwarding Detection (BFD)
- IGMP (Internet Group Management Protocol) version 1 (IGMPv1), IGMPv2, and IGMPv3
- IPv6 routing protocols: Multicast Listener Discovery version 1 and 2 (MLD v1/v2), OSPFv3, PIM multicast, VRRPv3
- Multicast Source Discovery protocol (MSDP)
- OSPF v2/v3
- Protocol Independent Multicast (PIM) dense mode, PIM source-specific mode, PIM sparse mode
- Real-time performance monitoring (RPM)
- RIPng (RIPng is for RIP IPv6)
- Virtual Router Redundancy Protocol (VRRP)

Table 11 on page 68 lists the EFLs that you can purchase for EX2300 switch models. If you have the license, you can run all of the enhanced software features mentioned above on your EX2300 switch.

Table 11: Junos OS Part Number on EX2300 Switches

Switch Model	Part Number
EX2300-C-12P EX2300-C-12T	EX-12-EFL Note: The EX-12-EFL includes the EX2300-VC license.
EX2300-24T EX2300-24P EX2300-24MP	EX-24-EFL
EX2300-48T EX2300-48P EX2300-48MP	EX-48-EFL

Features Requiring a License on EX3300 Switches

Two types of licenses are available on EX3300 switches: enhanced feature licenses (EFLs) and advanced feature licenses (AFLs).

To use the following features on the EX3300 switches, you must install an EFL:

- Bidirectional Forwarding Detection (BFD)
- IGMP (Internet Group Management Protocol) version 1 (IGMPv1), IGMPv2, and IGMPv3

- IPv6 routing protocols: Multicast Listener Discovery version 1 and 2 (MLD v1/v2), OSPFv3, PIM multicast, VRRPv3, virtual router support for unicast and filter-based forwarding (FBF)
- OSPFv1/v2
- Protocol Independent Multicast (PIM) dense mode, PIM source-specific mode, PIM sparse mode
- Q-in-Q tunneling (IEEE 802.1ad)
- Real-time performance monitoring (RPM)
- Virtual Router
- Virtual Router Redundancy Protocol (VRRP)

Table 12 on page 69 lists the EFLs that you can purchase for EX3300 switch models. If you have the license, you can run all of the enhanced software features mentioned above on your EX3300 switch.

Table 12: Junos OS Part Number on EX3300 Switches

Switch Model	Part Number
EX3300-24T EX3300-24P EX3300-24T-DC	EX-24-EFL
EX3300-48T EX3300-48T-BF EX3300-48P	EX-48-EFL

To use the following feature on EX3300 switches, you must install an AFL:

- Border Gateway Protocol (BGP) and multiprotocol BGP (MBGP)
- IPv6 routing protocols: IPv6 BGP and IPv6 for MBGP
- Virtual routing and forwarding (VRF) BGP

Table 13 on page 69 lists the AFLs that you can purchase for EX3300 switch models. For EX3300 switches, you must purchase and install a corresponding EFL along with the AFL to enable the advanced license features. If you have both these licenses, you can run all of the advanced software features mentioned above on your EX3300 switch.

Table 13: Junos OS AFL Part Number on EX3300 Switches

Switch Model	AFL Part Number
EX3300-24T EX3300-24P EX3300-24T-DC	EX-24-AFL
EX3300-48T EX3300-48T-BF EX3300-48P	EX-48-AFL

Features Requiring a License on EX3400 Switches

EX3400 switches has an enhanced feature licenses (EFLs) and MACSec license.

To use the following features on the EX3400 switches, you must install an EFL:

- Bidirectional Forwarding Detection (BFD)
- IGMP (Internet Group Management Protocol) version 1 (IGMPv1), IGMPv2, and IGMPv3
- IPv6 routing protocols: : Multicast Listener Discovery version 1 and 2 (MLD v1/v2), OSPFv3, PIM multicast, VRRPv3, virtual router support for unicast and filter-based forwarding (FBF)
- Multicast Source Discovery Protocol (MSDP)
- OSPF v2/v3
- Protocol Independent Multicast (PIM) dense mode, PIM source-specific mode, PIM sparse mode
- Real-time performance monitoring (RPM)
- RIPng (RIPng is for RIP IPv6)
- Unicast reverse-path forwarding (RPF)
- Virtual Router
- Virtual Router Redundancy Protocol (VRRP)

Table 14 on page 70 lists the EFLs that you can purchase for EX3400 switch models. If you have the license, you can run all of the enhanced software features mentioned above on your EX3400 switch.

Table 14: Junos OS Part Number on EX3400 Switches

Switch Model	Part Number
EX3400-24T EX3400-24P	EX-24-EFL
EX3400-48P EX3400-48T EX3400-48T-AFI EX3400-48T-DC EX3400-48T-DC-AFI	EX-48-EFL

To use the following features on the EX3400 switches, you must install an AFL:

- Border Gateway Protocol (BGP) and multiprotocol BGP (MBGP)
- Intermediate System-to-Intermediate System (IS-IS)

Table 15 on page 71 lists the AFLs that you can purchase for EX3400 switch models. For EX3400 switches, you must purchase and install a corresponding EFL along with the

AFL to enable the advanced license features. If you have both these licenses, you can run all of the advanced software features mentioned above on your EX3400 switch.

Table 15: Junos OS Part Number on EX3400 Switches

Switch Model	Part Number
EX3400-24T EX3400-24P	EX-24-AFL
EX3400-48P EX3400-48T EX3400-48T-AFI EX3400-48T-DC EX3400-48T-DC-AFI	EX-48-AFL

You must download a MACsec feature license to enable MACsec. The MACsec feature license is an independent feature license; the enhanced feature licenses (EFLs) or advanced feature licenses (AFLs) that must be purchased to enable some features on EX Series switches cannot be purchased to enable MACsec.

To purchase a feature license for MACsec, contact your Juniper Networks sales representative (https://www.juniper.net/us/en/contact-us/sales-offices). The Juniper sales representative will provide you with a feature license file and a license key.

MACsec is supported on EX3400 switches.

Features Requiring a License on EX4300 Switches

Two types of licenses are available on EX4300 switches: enhanced feature licenses (EFLs) and advanced feature licenses (AFLs).

To use the following features on the EX4300 switches, you must install an EFL:

- Bidirectional Forwarding Detection (BFD)
- Connectivity fault management (IEEE 802.1ag)
- IGMP (Internet Group Management Protocol) version 1 (IGMPv1), IGMPv2, and IGMPv3
- Multicast Source Discovery Protocol (MSDP)
- OSPFv2/v3
- Protocol Independent Multicast (PIM) dense mode, PIM source-specific mode, PIM sparse mode
- Real-time perfomance monitoring (RPM)
- RIPng (RIPng is for RIP IPv6)
- Unicast reverse-path forwarding (RPF)
- Virtual Router
- Virtual Router Redundancy Protocol (VRRP)

Table 16 on page 72 lists the EFLs that you can purchase for EX4300 switch models. If you have the license, you can run all of the enhanced software features mentioned above on your EX4300 switch.

Table 16: Junos OS Part Number on EX4300 Switches

Switch Model	Part Number
EX4300-48MP EX4300-48P EX4300-48T EX4300-48T-AFI EX4300-48T-DC EX4300-48T-DC-AFI	EX4300-48-AFL EX4300-48-EFL
EX4300-32F EX4300-32F-DC	EX4300-32F-EFL

To use the following features on EX4300 switches, you must install an AFL:

- Border Gateway Protocol (BGP) and multiprotocol BGP (MBGP)
- Intermediate System-to-Intermediate System (IS-IS)

Table 17 on page 72 lists the AFLs that you can purchase for EX4300 switch models. For EX4300 switches, you must purchase and install a corresponding EFL along with the AFL to enable the advanced license features. If you have both these licenses, you can run all of the advanced software features mentioned above on your EX4300 switch.

Table 17: Junos OS AFL Part Number on EX4300 Switches

Switch Model	AFL Part Number
EX4300-24T EX4300-24P	EX4300-24-AFL
EX4300-48P EX4300-48T EX4300-48T-AFI EX4300-48T-DC EX4300-48T-DC-AFI	EX4300-48-AFL
EX4300-32F EX4300-32F-DC	EX4300-32F-AFL

You must download a MACsec feature license to enable MACsec. The MACsec feature license is an independent feature license; the enhanced feature licenses (EFLs) or advanced feature licenses (AFLs) that must be purchased to enable some features on EX Series switches cannot be purchased to enable MACsec.

To purchase a feature license for MACsec, contact your Juniper Networks sales representative (https://www.juniper.net/us/en/contact-us/sales-offices). The Juniper sales representative will provide you with a feature license file and a license key.

MACsec is supported on EX4300 switches.

Features Requiring a License on EX4600 Switches

To use the following features on EX4600 switches, you must install an advanced feature license:

- Border Gateway Protocol (BGP) and multiprotocol BGP (MBGP)
- Intermediate System-to-Intermediate System (IS-IS)
- Multiprotocol Label Switching (MPLS)

Table 18 on page 73 lists the AFLs that you can purchase for EX4600 switch models.

Table 18: Junos OS AFL Part Number on EX4600 Switches

Switch Model	AFL Part Number
EX4600-40F	EX4600-AFL

You must download a MACsec feature license to enable MACsec. The MACsec feature license is an independent feature license; the enhanced feature licenses (EFLs) or advanced feature licenses (AFLs) that must be purchased to enable some features on EX Series switches cannot be purchased to enable MACsec.

To purchase a feature license for MACsec, contact your Juniper Networks sales representative (https://www.juniper.net/us/en/contact-us/sales-offices). The Juniper sales representative will provide you with a feature license file and a license key.

MACsec is supported on EX4600 switches.

Features Requiring a License on EX3200, EX4200, EX4500, EX4550, EX6200, EX8200, EX9200 and EX9250 Switches

To use the following features on EX3200, EX4200, EX4500, EX4550, EX8200, EX9200 and EX9250 switches, you must install an advanced feature license (AFL):

- Border Gateway Protocol (BGP) and multiprotocol BGP (MBGP)
- Ethernet VPN (available only on EX9200 switches)
- Intermediate System-to-Intermediate System (IS-IS)
- IPv6 routing protocols: IS-IS for IPv6, IPv6 BGP, IPv6 for MBGP
- Logical systems (available only on EX9200 switches)
- MPLS with RSVP-based label-switched paths (LSPs) and MPLS-based circuit cross-connects (CCCs) (Not supported on EX9200 switches)
- Open vSwitch Database (OVSDB) (available only on EX9200 switches)
- Virtual Extensible LAN (VXLAN) (available only on EX9200 switches)

To use the following features on Juniper Networks EX6200 Ethernet Switches, you must install an advanced feature license (AFL):

- Border Gateway Protocol (BGP)
- Intermediate System-to-Intermediate System (IS-IS)
- IPv6 routing protocols: IS-IS for IPv6, IPv6 BGP

To use MACsec feature on Juniper Networks EX9253 Switches, you must install an security feature license (SFL).

To use Forwarding Information Base (FIB) and Address Resolution Protocol (ARP) features on Juniper Networks EX9251 and EX9253 Switches, you must install an mid-scale license (ML).

Table 19 on page 74 lists the AFLs that you can purchase for EX3200, EX4200, EX4500, EX4550, EX6200, EX8200, EX9200 and EX9250 switches. If you have the license, you can run all of the advanced software features mentioned above on your EX3200, EX4200, EX4500, EX4550, EX6200, EX8200, or EX9200 switch. An EFL is not applicable to this range of switches.

Table 19: Junos OS AFL Part Number on EX3200, EX4200, EX4500, EX4550, EX6200, EX8200, EX9200 and EX9250 Switches

Switch Model	AFL Part Number
EX3200-24P EX3200-24T EX4200-24F EX4200-24P EX4200-24PX EX4200-24T	EX-24-AFL
EX3200-48P EX3200-48T EX4200-48F EX4200-48P EX4200-48PX EX4200-48T	EX-48-AFL
EX4500-40F-BF EX4500-40F-BF-C EX4500-40F-FB EX4500-40F-FB-C	EX-48-AFL
EX4550	EX4550-AFL
EX6210	EX6210-AFL
EX8208	EX8208-AFL
EX8216	EX8216-AFL
EX-XRE200	EX-XRE200-AFL

Table 19: Junos OS AFL Part Number on EX3200, EX4200, EX4500, EX4550, EX6200, EX8200, EX9200 and EX9250 Switches (continued)

Switch Model	AFL Part Number
EX9204	EX9204-AFL
EX9208	EX9208-AFL
EX9214	EX9214-AFL
EX9251	EX9251-AFL EX9251-ML
EX9253	EX9253-AFL EX9253-ML EX9253-SFL

You must download a MACsec feature license to enable MACsec. The MACsec feature license is an independent feature license; the enhanced feature licenses (EFLs) or advanced feature licenses (AFLs) that must be purchased to enable some features on EX Series switches cannot be purchased to enable MACsec.

To purchase a feature license for MACsec, contact your Juniper Networks sales representative (https://www.juniper.net/us/en/contact-us/sales-offices). The Juniper sales representative will provide you with a feature license file and a license key.

MACsec is supported on EX4200 and EX4550 switches.

License Warning Messages

For using features that require a license, you must install and configure a license key. To obtain a license key, use the contact information provided in your certificate.

If you have not purchased the AFL or EFL and installed the license key, you receive warnings when you try to commit the configuration:

```
[edit protocols]
  'bgp'
    warning: requires 'bgp' license
error: commit failed: (statements constraint check failed)
```

The system generates system log (**syslog**) alarm messages notifying you that the feature requires a license—for example:

```
Sep  3 05:59:11   craftd[806]:  Minor alarm set, BGP Routing Protocol usage
requires a license
Sep  3 05:59:11   alarmd[805]: Alarm set: License color=YELLOW, class=CHASSIS,
```

```
reason=BGP Routing Protocol usage requires a license
Sep  3 05:59:11   alarmd[805]: LICENSE_EXPIRED: License for feature bgp(47) expired
```

Output of the **show system alarms** command displays the active alarms:

```
user@switch> show system alarms
1 alarm currently active
Alarm time               Class  Description
2009-09-03 06:00:11 UTC  Minor  BGP Routing Protocol usage requires a license
```

See Also

- Managing Licenses for the EX Series Switch (CLI Procedure) on page 77
- Monitoring Licenses for the EX Series Switch on page 78
- License Key Components for the EX Series Switch on page 77

Software Features That Require Licenses on EX Series Switches

The following Junos OS features require an Enhanced Feature License (EFL) or Advanced Feature License (AFL) on EX Series devices:

- (EX2200 only) Bidirectional forwarding detection (BFD)
- (EX2200 only) Connectivity fault management (IEEE 802.lag)
- (EX2200 only) Internet Group Management Protocol version 1 (IGMPv1), IGMPv2, and IGMPv3
- (EX2200 and EX3300) OSPFv1/v2 (with 4 active interfaces)
- (EX2200 only) Protocol Independent Multicast (PIM) dense mode, PIM source-specific mode, PIM sparse mode
- (EX2200 and EX3300) Q-in-Q tunneling (IEEE 802.lad)
- (EX2200 only) Real-time performance monitoring (RPM)
- (EX3200, EX4200, EX4500, EX6200, and EX8200) Border Gateway Protocol (BGP) and multiprotocol BGP (MBGP)
- (EX3200, EX4200, EX4500, EX6200, and EX8200) Intermediate System-to-Intermediate System (IS-IS)
- (EX3200, EX4200, EX4500, EX6200, and EX8200) IPv6 protocols: OSPFv3, PIPng, IS-IS for IPv6, IPv6 BGP
- (EX3200, EX4200, EX4500, EX6200, and EX8200) MPLS with RSVP-based label-switched paths (LSPs) and MPLS-based circuit cross-connects (CCCs)

For more details regarding EX Series feature licenses, see “Understanding Software Licenses for EX Series Switches” on page 66.

For information about how to purchase a software license, contact your Juniper Networks sales representative at https://www.juniper.net/in/en/contact-us/.

License Key Components for the EX Series Switch

When you purchase a license for a Junos OS feature that requires a separate license, you receive a license key.

A license key consists of two parts:

- License ID—Alphanumeric string that uniquely identifies the license key. When a license is generated, it is given a license ID.
- License data—Block of binary data that defines and stores all license key objects.

For example, in the following typical license key, the string **Junos204558** is the license ID, and the trailing block of data is the license data:

```
XXXXXXXXXX xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx
xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx
xxxxxx xxxxxx xxx
```

The license data defines the device ID for which the license is valid and the version of the license.

See Also

- Managing Licenses for the EX Series Switch (CLI Procedure) on page 77
- Understanding Software Licenses for EX Series Switches on page 66

Managing Licenses for the EX Series Switch (CLI Procedure)

To enable and use some Junos OS features on an EX Series switch, you must purchase, install, and manage separate software licenses. Each switch requires one license. For a Virtual Chassis deployment, two licenses are recommended for redundancy. After you have configured the features, you see a warning message if the switch does not have a license for the feature.

Before you begin managing licenses, be sure that you have:

- Obtained the needed licenses. For information about how to purchase software licenses, contact your Juniper Networks sales representative.
- Understand what makes up a license key. For more information, see "License Key Components for the EX Series Switch" on page 77.

This topic includes the following tasks:

Adding New Licenses

To add one or more new license keys on the switch, with the CLI:

1. Add the license key or keys:
   - To add one or more license keys from a file or URL, specify the filename of the file or the URL where the key is located:

     `user@switch>` **request system license add *filename* | *url***

   - To add a license key from the terminal:

     `user@switch>` **request system license add terminal**

2. When prompted, enter the license key, separating multiple license keys with a blank line.

   If the license key you enter is invalid, an error appears in the CLI output when you press Ctrl+d to exit the license entry mode.

Deleting Licenses

To delete one or more license keys from the switch with the CLI, specify the license ID:

`user@switch>` **request system license delete *license-id***

You can delete only one license at a time.

Saving License Keys

To save the installed license keys to a file (which can be a URL) or to the terminal:

`user@switch>` **request system license save *filename* | *url***

For example, the following command saves the installed license keys to a file named **license.conf**:

`user@switch>` **request system license save ftp://user@switch/license.conf**

See Also
- Monitoring Licenses for the EX Series Switch on page 78
- Understanding Software Licenses for EX Series Switches on page 66

Monitoring Licenses for the EX Series Switch

To enable and use some Junos OS features on the EX Series switch, you must purchase, install, and manage the appropriate software licenses. Each switch requires one license. For a Virtual Chassis deployment, two licenses are recommended for redundancy.

To monitor your installed licenses, perform the following tasks:

- Displaying Installed Licenses and License Usage Details on page 79
- Displaying Installed License Keys on page 80

Displaying Installed Licenses and License Usage Details

Purpose Verify that the expected license is installed and active on the switch and fully covers the switch configuration.

Action From the CLI, enter the **show system license** command. (To display only the **License usage** list, enter the **show system license usage** command. To display only the **Licenses installed** output, enter **show system license installed**.)

```
user@switch> show system license
License usage:
                                Licenses     Licenses    Licenses    Expiry
  Feature name                       used    installed      needed
  bgp                                   1            1           0    permanent
  isis                                  0            1           0    permanent
  ospf3                                 0            1           0    permanent
  ripng                                 0            1           0    permanent
  mpls                                  0            1           0    permanent


Licenses installed:
  License identifier: XXXXXXXXXX
  License version: 2
  Valid for device: XXXXXXXXXX
  Features:
    ex-series - Licensed routing protocols in ex-series
      permanent
```

Meaning The output shows the license or licenses (for Virtual Chassis deployments) installed on the switch and license usage. Verify the following information:

- If a feature that requires a license is configured (used), a license is installed on the switch. The **Licenses needed**d column must show that no licenses are required.

- The appropriate number of licenses is installed. Each switch requires one license. For a Virtual Chassis deployment, two licenses are recommended for redundancy.
- The expected license is installed.

Displaying Installed License Keys

Purpose Verify that the expected license keys are installed on the switch.

Action From the CLI, enter the **show system license keys** command.

```
user@switch> show system license keys
XXXXXXXXXX xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx
           xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx
           xxxxxx xxxxxx xxx
```

Meaning The output shows the license key or keys (for Virtual Chassis deployments) installed on the switch. Verify that each expected license key is present.

See Also
- Managing Licenses for the EX Series Switch (CLI Procedure) on page 77
- Understanding Software Licenses for EX Series Switches on page 66

Software Features That Require Licenses for QFX Series

- Software Features That Require Licenses on the QFX Series on page 81
- Disaggregated Software Features That Require Licenses on the QFX Series on page 84
- Generating the License Keys for a QFabric System on page 85
- Understanding Junos Fusion Licenses on page 87

Software Features That Require Licenses on the QFX Series

NOTE: If you try to configure a feature that is not licensed, you will receive syslog messages saying that you are using a feature that is licensable and that you do not possess a license for the feature. If you try to commit configuration changes for a feature that is not licensed, you will receive a commit warning saying that you have exceeded the allowed license limit for the feature.

NOTE: Virtual Extensible Local Area Network (VXLAN) is not supported on QFX3500 and QFX3600 devices. When you issue the **show licenses** command, you will see VXLAN in the CLI output, but the feature is not enabled.

NOTE: There is no separate license for Virtual Chassis like there is for Virtual Chassis Fabric.

Table 7 on page 31 lists the standard Junos OS features licenses and supported QFX Series devices. For information on disaggregated Junos OS feature licenses on the QFX5200-32C switch, see "Disaggregated Software Features That Require Licenses on the QFX Series" on page 34.

For information about how to purchase a software license, contact your Juniper Networks sales representative.

Table 20: Standard Junos OS Feature Licenses and Model Numbers for QFX Series Devices

Licensed Software Feature	Supported Devices	Number of Licenses Required	Model Number
QFX Series premium feature license for Border Gateway Protocol (BGP), Intermediate System-to-Intermediate System (IS-IS), and Virtual Extensible Local Area Network (VXLAN), and Open vSwitch Database (OVSDB)	QFX10002-36Q switch	One per switch	QFX10002-36Q-PFL
	QFX10002-60C switch		QFX10002-60C-PFL
	QFX10002-72Q switch		QFX10002-72Q-PFL
	QFX10008 switch		QFX10008-PFL
	QFX10016 switch		QFX10016-PFL

Table 20: Standard Junos OS Feature Licenses and Model Numbers for QFX Series Devices (continued)

Licensed Software Feature	Supported Devices	Number of Licenses Required	Model Number
QFX Series advanced feature license for Border Gateway Protocol (BGP), Intermediate System-to-Intermediate System (IS-IS), Multi-protocol Label Switching (MPLS), and Virtual Extensible Local Area Network (VXLAN), and Open vSwitch Database (OVSDB)	QFX10002-36Q switch QFX10002-60C switch QFX10002-72Q switch QFX10008 switch QFX10016 switch	One per switch	QFX10002-36Q-AFL QFX10002-60C-AFL QFX10002-72Q-AFL QFX10008-AFL QFX10016-AFL
QFX Series premium feature license for Border Gateway Protocol (BGP), Intermediate System-to-Intermediate System (IS-IS), and Virtual Extensible Local Area Network (VXLAN), and Open vSwitch Database (OVSDB)	QFX5110-48S switch QFX5110-32Q switch QFX5200-48Y	One per switch, two per Virtual Chassis, and two per Virtual Chassis Fabric	QFX5K-C1-PFL
QFX Series advanced feature license for Border Gateway Protocol (BGP), Intermediate System-to-Intermediate System (IS-IS), Multi-protocol Label Switching (MPLS), and Virtual Extensible Local Area Network (VXLAN), and Open vSwitch Database (OVSDB)	QFX5110-48S switch QFX5110-32Q switch QFX5200-48Y	One per switch	QFX5K-C1-AFL
QFX Series premium feature license for Border Gateway Protocol (BGP), Intermediate System-to-Intermediate System (IS-IS), and Virtual Extensible Local Area Network (VXLAN), and Open vSwitch Database (OVSDB)	QFX5210-64C switch	One per switch	QFX5K-C2-PFL

Table 20: Standard Junos OS Feature Licenses and Model Numbers for QFX Series Devices (continued)

Licensed Software Feature	Supported Devices	Number of Licenses Required	Model Number
QFX Series advanced feature license for Border Gateway Protocol (BGP), Intermediate System-to-Intermediate System (IS-IS), Multi-protocol Label Switching (MPLS), and Virtual Extensible Local Area Network (VXLAN), and Open vSwitch Database (OVSDB)	QFX5210-64C switch	One per switch, two per Virtual Chassis, and two per Virtual Chassis Fabric	QFX5K-C2-AFL
QFX Series advanced feature license for Border Gateway Protocol (BGP), Intermediate System-to-Intermediate System (IS-IS), Multi-protocol Label Switching (MPLS), and Virtual Extensible Local Area Network (VXLAN), and Open vSwitch Database (OVSDB)	QFX3500, QFX3600, QFX5100-48S, and QFX5100-48T switch	One per switch, two per Virtual Chassis, and two per Virtual Chassis Fabric	QFX-JSL-EDGE-ADV1
QFX Series advanced feature license for Border Gateway Protocol (BGP), Intermediate System-to-Intermediate System (IS-IS), Multi-protocol Label Switching (MPLS), and Virtual Extensible Local Area Network (VXLAN) and Open vSwitch Database (OVSDB)	QFX5100-24Q and QFX5100-96S switch	One per switch, two per Virtual Chassis, and two per Virtual Chassis Fabric	QFX5100-HDNSE-LIC
QFX Series advanced feature license for Border Gateway Protocol (BGP)	QFX3100 Director device	One per Node device in a network Node group	QFX-JSL-DRCTR-ADV1
QFX Series advanced feature license for Fibre Channel	QFX3500 switch	One per switch on which fibre channel ports are configured	QFX-JSL-EDGE-FC

Table 20: Standard Junos OS Feature Licenses and Model Numbers for QFX Series Devices (continued)

Licensed Software Feature	Supported Devices	Number of Licenses Required	Model Number
QFX Series advanced feature license for Fibre Channel	QFX3100 Director device	One per QFX3500 Node device on which fibre channel ports are configured	QFX-JSL-DRCTR-FC
QFX Series advanced feature license for Fibre Channel - Capacity 16	QFX3100 Director device	One for up to 16 QFX3500 Node devices on which fibre channel ports are configured	QFX-JSL-DRCTR-FC-C16
QFX Series feature license for enabling fabric mode	QFX3500 and QFX3600 device	One per device	QFX3000-JSL-EDGE-FAB
QFX Series feature license for base software for QFX3000-G QFabric system	QFX3100 Director device	One per QFX3000-G QFabric system	QFX3008-JSL-DRCTR-FAB
QFX Series feature license for base software for QFX3000-M QFabric system	QFX3100 Director device	One per QFX3000-M QFabric system	QFX3000M-JSL-DRCTR-FAB
QFX and EX Series feature license for enabling Media Access Control security (MACsec)	QFX switches that support MACsec. See "Understanding Media Access Control Security (MACsec)" on page 89.	One per switch, two per Virtual Chassis,	EX-QFX-MACSEC-AGG
Virtual Chassis Fabric (VCF) feature license	Any member device in a Virtual Chassis Fabric (VCF)	Two per Virtual Chassis Fabric (VCF)	QFX-VCF-LIC

Disaggregated Software Features That Require Licenses on the QFX Series

Disaggregated Software Feature Licenses on QFX5200 Switches

NOTE: For information on standard Junos OS feature licenses, see "Software Features That Require Licenses on the QFX Series" on page 31.

The Junos OS software is disaggregated from the hardware. With disaggregated Junos OS, you can purchase the following feature licenses, which are available on a perpetual basis:

- Junos Base Software (JBS) license:

  Includes basic layer 2 switching, basic layer 3 routing, multicast, automation, programmability, Zero Touch Provisioning (ZTP) and basic monitoring.

  NOTE: You must purchase the JBS license to use basic functions, but you do not need to install the license key in Junos OS Release 15.1X53-D30. JBS basic functions work with this release without installing the license key. However, you will need to install the license key in a future release of Junos OS to be determined, so make sure to retain the authorization code you received from the License Management System to generate a license key for the JBS license.

- Junos Advanced Software (JAS) license:

  Includes features supported in JBS license and Border Gateway Protocol (BGP), Intermediate System-to-Intermediate System (IS-IS), and Virtual Extensible Local Area Network (VXLAN). You need to install the license key to use these features.

- Junos Premium Software (JPS) license:

  Includes features supported in JAS license and Multi-protocol Label Switching (MPLS) feature set. You need to install the license key to use these features.

For information about how to purchase a software feature license, contact your Juniper Networks sales representative.

Table 21: Disaggregated Junos OS Feature Licenses and Associated SKU's

Licensed Software Features	SKU's
Junos base software (JBS) license	QFX5000-35-JBS
Junos advanced software (JAS) license	QFX5000-35-JAS
Junos premium software (JPS) license	QFX5000-35-JPS

Generating the License Keys for a QFabric System

When you purchase a Junos OS software feature license for a QFabric system, you receive an e-mail containing an authorization code for the feature license from Juniper Networks. You can use the authorization code to generate a unique license key (a combination of the authorization code and the QFabric system ID) for the QFabric system, and then add the license key on the QFabric system.

Before generating the license keys for a QFabric system:

- Purchase the required licenses for the QFabric system. See "Software Features That Require Licenses on the QFX Series" on page 31.
- Note down the authorization code in the e-mail you received from Juniper Networks when you purchased the license.

- Perform the initial setup of the QFabric system on the Director group. See *Performing the QFabric System Initial Setup on a QFX3100 Director Group*.
- Log in to the QFabric system, issue the **show version** command, and note down the software serial number and QFabric system ID for the QFabric system.

```
user@qfabric> show version
Hostname: qfabric
Model: qfx3000-g
Serial Number: qfsn-0123456789
QFabric System ID: f158527a-f99e-11e0-9fbd-00e081c57cda
JUNOS Base Version [12.2I20111018_0215_dc-builder]
```

To generate the license keys for a QFabric system:

1. In a browser, log in to the Juniper Networks License Management System at https://www.juniper.net/lcrs/license.do.

   The Manage Product Licenses page appears.

   NOTE: To access the licensing site, you must have a service contract with Juniper Networks and an access account. If you need help obtaining an account, complete the registration form at the Juniper Networks website https://www.juniper.net/registration/Register.jsp .

2. On the Generate Licenses tab, select **QFX Series Product** from the drop-down list, and click **Go**.

   The Generate Licenses - QFX Series Product page appears.

3. Select the **QFX Series Product Fabric** option button, and then click **Continue**.

   The Generate Licenses - QFX Series Product Fabrics page appears.

4. In the **Software Serial No** field, enter the software serial number for the QFabric system.

5. In the **QFabric System ID** field, enter the QFabric system ID for the QFabric system.

6. In the **Authorization Code** field, enter the authorization code in the e-mail you received from Juniper Networks when you purchased the license.

7. (Optional) If you want to enter another authorization code for the same device, click **Enter More Authorization Codes** to display a new authorization code field. Enter the authorization code in this field.

8. Click **Confirm**.

The Confirm License Information page appears, displaying a summary of the information you submitted to the License Management System.

9. Review the information to ensure everything is correct and then click **Generate License**.

   The Generate Licenses - QFX Series Product Fabrics page appears, displaying a summary of your license keys, including a link that displays the details of your new license keys.

10. Select the file format in which you want to obtain your new license keys.

11. Select the delivery method you want to use to obtain your new license keys.

    To download the license keys:

    - Select the **Download to this computer** option button, and click **OK**.

    To e-mail the license keys:

    - Select the **Send e-mail to *e-mail ID*** option button, and click **OK**.

See Also

- Software Features That Require Licenses on the QFX Series on page 31
- *Performing the QFabric System Initial Setup on a QFX3100 Director Group*
- *show version*

Understanding Junos Fusion Licenses

Starting with Junos OS Release 17.2R1, you need to install a Junos Fusion license in addition to any other feature licenses that you install to track and activate certain QFX5100-48SH and QFX5100-48TH models that are shipped with satellite software. These models can only be used as satellite devices. For these models, you need to install a Junos Fusion license in addition to any other feature licenses that you install. See Table 22 on page 88 for a list of satellite devices that require Junos Fusion licenses.

NOTE: **You do not need Junos Fusion licenses for satellite device models that were purchased as Junos OS-based top-of-rack switches.**

Install the Junos Fusion licenses on the aggregation device because the aggregation device is the single point of management in a Junos Fusion. If your Junos Fusion is operating in a topology with multiple aggregation devices, you only need to install the licenses on one aggregation device because the license keys are synchronized between the two aggregation devices.

You can install a single-pack license to activate one satellite device, or you can install multi-pack licenses, which can activate up to 128 satellite devices. If the number of satellite devices in a Junos Fusion exceeds the number of Junos Fusion licenses you have installed, the satellite devices are provisioned, but the system will issue a warning saying

that there is a license limit violation. If the satellite device does not have a corresponding Junos Fusion license installed, the satellite device is provisioned, but the system will issue a warning.

Table 22 on page 88 lists the supported aggregation and satellite devices as well as the model numbers of the Junos Fusion license packs.

For information about how to purchase a software license, contact your Juniper Networks sales representative. For information on standard Junos OS feature licenses, see "Software Features That Require Licenses on the QFX Series" on page 31.

Table 22: Junos Fusion License Model Numbers for Satellite Devices

Aggregation Devices Supported	Satellite Devices Requiring Licenses	Model Numbers of License Packs
QFX10002, QFX10008 and QFX10016 switches	• QFX5100-48SH-AFO • QFX5100-48SH-AFI • QFX5100-48TH-AFO • QFX5100-48TH-AFI	QFX10K-C1-JFS-1 QFX10K-C1-JFS-4 QFX10K-C1-JFS-8 QFX10K-C1-JFS-16 QFX10K-C1-JFS-32 QFX10K-C1-JFS-64

See Also

- Junos OS Feature Licenses on page 15
- Junos OS Feature License Keys on page 136
- *Generating License Keys*
- Adding New Licenses (CLI Procedure) on page 36
- Deleting License Keys (CLI) on page 52
- Saving License Keys (CLI) on page 43
- Verifying Junos OS License Installation (CLI) on page 41

Understanding Media Access Control Security (MACsec)

- Understanding Media Access Control Security (MACsec) on page 89
- Configuring Media Access Control Security (MACsec) on page 99

Understanding Media Access Control Security (MACsec)

Media Access Control Security (MACsec) is an 802.1AE IEEE industry-standard security technology that provides secure communication for all traffic on Ethernet links. MACsec provides point-to-point security on Ethernet links between directly connected nodes and is capable of identifying and preventing most security threats, including denial of service, intrusion, man-in-the-middle, masquerading, passive wiretapping, and playback attacks.

MACsec allows you to secure an Ethernet link for almost all traffic, including frames from the Link Layer Discovery Protocol (LLDP), Link Aggregation Control Protocol (LACP), Dynamic Host Configuration Protocol (DHCP), Address Resolution Protocol (ARP), and other protocols that are not typically secured on an Ethernet link because of limitations with other security solutions. MACsec can be used in combination with other security protocols such as IP Security (IPsec) and Secure Sockets Layer (SSL) to provide end-to-end network security.

MACsec is standardized in IEEE 802.1AE. The IEEE 802.1AE standard can be seen on the IEEE organization website at IEEE 802.1: BRIDGING & MANAGEMENT.

Starting in Junos OS Release 18.2R1, MACsec is supported on ACX6360 routers.

How MACsec Works

MACsec provides industry-standard security through the use of secured point-to-point Ethernet links. The point-to-point links are secured after matching security keys— a user-configured pre-shared key when you enable MACsec using static connectivity association key (CAK) security mode, a user-configured static secure association key when you enable MACsec using static secure association key (SAK) security mode, or a dynamic key included as part of the AAA handshake with the RADIUS server when you enable MACsec using dynamic security mode— are exchanged and verified between the interfaces at each end of the point-to-point Ethernet link. Other user-configurable

parameters, such as MAC address or port, must also match on the interfaces on each side of the link to enable MACsec. See "Configuring Media Access Control Security (MACsec)" on page 99.

Once MACsec is enabled on a point-to-point Ethernet link, all traffic traversing the link is MACsec-secured through the use of data integrity checks and, if configured, encryption.

The data integrity checks verify the integrity of the data. MACsec appends an 8-byte header and a 16-byte tail to all Ethernet frames traversing the MACsec-secured point-to-point Ethernet link, and the header and tail are checked by the receiving interface to ensure that the data was not compromised while traversing the link. If the data integrity check detects anything irregular about the traffic, the traffic is dropped.

MACsec can also be used to encrypt all traffic on the Ethernet link. The encryption used by MACsec ensures that the data in the Ethernet frame cannot be viewed by anybody monitoring traffic on the link. MACsec encryption is optional and user-configurable; you can enable MACsec to ensure the data integrity checks are performed while still sending unencrypted data " in the clear" over the MACsec-secured link, if desired.

MACsec is configured on point-to-point Ethernet links between MACsec-capable interfaces. If you want to enable MACsec on multiple Ethernet links, you must configure MACsec individually on each point-to-point Ethernet link.

Understanding Connectivity Associations and Secure Channels

MACsec is configured in connectivity associations. MACsec is enabled when a connectivity association is assigned to an interface.

When you are configuring MACsec using static secure association key (SAK) security mode, you must configure secure channels within a connectivity association. The secure channels are responsible for transmitting and receiving data on the MACsec-enabled link, and also responsible for transmitting SAKs across the link to enable and maintain MACsec. A single secure channel is unidirectional— it can be used to apply MACsec only to either inbound or outbound traffic. A typical connectivity association when MACsec is enabled using SAK security mode contains two secure channels— one secure channel for inbound traffic and another secure channel for outbound traffic.

When you enable MACsec using static CAK or dynamic security mode, you have to create and configure a connectivity association. Two secure channels— one secure channel for inbound traffic and another secure channel for outbound traffic— are automatically created. The automatically-created secure channels do not have any user-configurable parameters; all configuration is done in the connectivity association outside of the secure channels.

Understanding Static Connectivity Association Key Security Mode (Security Mode for Router-to-Router Links)

When you enable MACsec using static connectivity association key (CAK) security mode, two security keys—a connectivity association key (CAK) that secures control plane traffic and a randomly-generated secure association key (SAK) that secures data plane traffic—are used to secure the point-to-point Ethernet link.

You initially establish a MACsec-secured link using a preshared key when you are using static CAK security mode to enable MACsec. A preshared key includes a connectivity association name (CKN) and a connectivity association key (CAK). The CKN and CAK are configured by the user in the connectivity association and must match on both ends of the link to initially enable MACsec.

The preshared keys must be configured on the endpoints of the link and the keys must in agreement with each other. The MACsec Key Agreement (MKA) protocol is responsible for maintaining MACsec on the link, and decides which router on the point-to-point link becomes the key server. The key server then creates an SAK that is shared with the router at the other end of the point-to-point link only, and that SAK is used to secure all data traffic traversing the link. The key server continues to periodically create and share a randomly-created SAK over the point-to-point link for as long as MACsec is enabled.

See *Configuring Media Access Control Security (MACsec) on MX Series Routers* for step-by-step instructions on enabling MACsec by using static CAK security mode.

Understanding MACsec Hardware Requirements for MX Series Routers

You can configure Media Access Control Security (MACsec) on MX Series routers with the enhanced 20-port Gigabit Ethernet MIC (model number MIC-3D-20GE-SFP-E). Starting with Junos OS Release 16.1, you can configure MACsec on MX Series routers with the 40-port 10-Gigabit Ethernet MPC (MPC7E-10G).

Starting with Junos OS Release 17.3R2, you can configure MACsec on MX 10003 routers with the modular MIC (JNP-MIC1-MACSEC).

MACsec can also be configured on supported MX Series router interfaces when those routers are configured in a Virtual Chassis configuration. Encryption and decryption are implemented in the hardware in line-rate mode. An additional overhead of 24 through 32 bytes is required for MACsec if Secure Channel Identifier (SCI) tag is included. On 20-port Gigabit Ethernet MICs, the SCI tag is always included.

For more information regarding MACsec, refer the following IEEE specifications:

- IEEE 802.1AE-2006. Media Access Control (MAC) Security
- IEEE 802.1X-2010. Port-Based Network Access Control. Defines MACSec Key Agreement Protocol

Understanding MACsec Software Requirements for MX Series Routers

Following are some of the key software requirements for MACsec on MX Series Routers:

NOTE: **A feature license is not required to configure MACsec on MX Series routers with the enhanced 20-port Gigabit Ethernet MIC (model number MIC-3D-20GE-SFP-E).**

MACsec is supported on MX Series routers with MACsec-capable interfaces. The SCI tag is always included on MX Series routers.

MACsec supports 128 and 256-bit cipher-suite with and without extended packet numbering (XPN).

MACsec supports MACsec Key Agreement (MKA) protocol with Static-CAK mode using preshared keys.

MACsec supports a single connectivity-association (CA) per physical port or physical interface.

Starting with Junos OS Release 15.1, MACsec is supported on member links of an aggregated Ethernet (**ae-**) interface bundle, and also regular interfaces that are not part of an interface bundle.

Starting with Junos OS Release 17.3R2, MACsec supports 256-bit cipher-suite GCM-AES-256 and GCM-AES-XPN-256 on MX10003 routers with the modular MIC (model number-JNP-MIC1-MACSEC).

Starting in Junos OS Release 18.3R1, the MIC-MACSEC-20GE MIC provides 256-bit cipher-suite GCM-AES-256 and GCM-AES-XPN-256. The MIC-MACSEC-20GE MIC supports MACsec on both twenty 1-Gigabit Ethernet SFP ports and on two 10-Gigabit Ethernet SFP+ ports in the following hardware configurations:

- Installed directly on the MX80 and MX104 routers
- Installed on MPC1, MPC2, MPC3, MPC2E, MPC3E, MPC2E-NG, and MPC3E-NG line cards on the MX240, MX480, and MX960 routers

Refer *Understanding Interface Naming Conventions for MIC-MACSEC-20GE* and *Understanding Rate Selectability* for more information.

Understanding MACsec Security Modes

Understanding Static Connectivity Association Key Security Mode (Recommended Security Mode for Switch-to-Switch Links)

When you enable MACsec using static connectivity association key (CAK) security mode, two security keys— a connectivity association key (CAK) that secures control plane traffic and a randomly-generated secure association key (SAK) that secures data plane traffic— are used to secure the point-to-point Ethernet link. Both keys are regularly exchanged between both devices on each end of the point-to-point Ethernet link to ensure link security.

You initially establish a MACsec-secured link using a pre-shared key when you are using static CAK security mode to enable MACsec. A pre-shared key includes a connectivity association name (CKN) and its own connectivity association key (CAK). The CKN and CAK are configured by the user in the connectivity association and must match on both ends of the link to initially enable MACsec.

Once matching pre-shared keys are successfully exchanged, the MACsec Key Agreement (MKA) protocol is enabled. The MKA protocol is responsible for maintaining MACsec on the link, and decides which switch on the point-to-point link becomes the key server. The key server then creates an SAK that is shared with the switch at the other end of the point-to-point link only, and that SAK is used to secure all data traffic traversing the link.

The key server will continue to periodically create and share a randomly-created SAK over the point-to-point link for as long as MACsec is enabled.

NOTE: If the MACsec session is terminated due to a link failure, when the link is restored, the MKA key server elects a key server and generates a new SAK.

You enable MACsec using static CAK security mode by configuring a connectivity association on both ends of the link. All configuration is done within the connectivity association but outside of the secure channel. Two secure channels— one for inbound traffic and one for outbound traffic— are automatically created when using static CAK security mode. The automatically-created secure channels do not have any user-configurable parameters that cannot already be configured in the connectivity association.

We recommend enabling MACsec on switch-to-switch links using static CAK security mode. Static CAK security mode ensures security by frequently refreshing to a new random security key and by sharing only the security key between the two devices on the MACsec-secured point-to-point link. Additionally, some optional MACsec features— replay protection, SCI tagging, and the ability to exclude traffic from MACsec— are available only when you enable MACsec using static CAK security mode.

NOTE: The switches on each end of a MACsec-secured switch-to-switch link must either both be using Junos OS Release 14.1X53-D10 or later, or must both be using an earlier version of Junos, in order to establish a MACsec-secured connection when using static CAK security mode.

See "Configuring Media Access Control Security (MACsec)" on page 99 for step-by-step instructions on enabling MACsec using static CAK security mode.

Understanding Dynamic Secure Association Key Security Mode (Switch-to-Host Links)

Dynamic secure association key (SAK) security mode is used to enable MACsec on a switch-to-host link.

To enable MACsec on a link connecting an endpoint device— such as a server, phone, or personal computer— to a switch, the endpoint device must support MACsec and must be running software that allows it to enable a MACsec-secured connection. When configuring MACsec on a switch-to-host link, the MACsec Key Agreement (MKA) keys, which are included as part of 802.1X authentication, are retrieved from a RADIUS server as part of the AAA handshake. A master key is passed from the RADIUS server to the switch and from the RADIUS server to the host in independent authentication transactions. The master key is then passed between the switch and the host to create a MACsec-secured connection.

A secure association using dynamic secure association security mode must be configured on the switch' s Ethernet interface that connects to the host in order for the switch to create a MACsec-secured connection after receiving the MKA keys from the RADIUS server.

The RADIUS server must be using Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) in order to support MACsec. The RADIUS servers that support other widely-used authentication frameworks, such as password-only or md5, cannot be used to support MACsec. In order to enable MACsec on a switch to secure a connection to a host, you must be using 802.1X authentication on the RADIUS server. MACsec must be configured into dynamic mode. MACsec is still enabled using connectivity associations when enabled on a switch-to-host link, as it is on a switch-to-switch link.

Understanding Static Secure Association Key Security Mode (Supported for Switch-to-Switch Links)

When you enable MACsec using static secure association key (SAK) security mode, one of up to two manually configured SAKs is used to secure data traffic on the point-to-point Ethernet link. All SAK names and values are configured by the user; there is no key server or other tool that creates SAKs. Security is maintained on the point-to-point Ethernet link by periodically rotating between the two security keys. Each security key name and value must have a corresponding matching value on the interface at the other end of the point-to-point Ethernet link to maintain MACsec on the link.

You configure SAKs within secure channels when you enable MACsec using static SAK security mode. You configure secure channels within connectivity associations. A typical connectivity association for MACsec using static SAK security mode contains two secure channels— one for inbound traffic and one for outbound traffic— that have each been configured with two manually-configured SAKs. You must attach the connectivity association with the secure channel configurations to an interface to enable MACsec using static SAK security mode.

We recommend enabling MACsec using static CAK security mode. Use static SAK security mode only if you have a compelling reason to use it instead of static CAK security mode.

See "Configuring Media Access Control Security (MACsec)" on page 99 for step-by-step instructions on enabling MACsec using SAKs.

Understanding the Requirements to Enable MACsec on a Switch-to-Host Link

When configuring MACsec on a switch-to-host link, the MACsec Key Agreement (MKA) keys, which are included as part of 802.1X authentication, are retrieved from a RADIUS server as part of the AAA handshake. A master key is passed from the RADIUS server to the switch and from the RADIUS server to the host in independent authentication transactions. The master key is then passed between the switch and the host to create a MACsec-secured connection.

The following requirements must be met in order to enable MACsec on a link connecting a host device to a switch.

The host device:

- must support MACsec and must be running software that allows it to enable a MACsec-secured connection with the switch.

The switch:

- must support MACsec (see Table 23 on page 96).

- must be configured into dynamic secure association key security mode.
- must be using 802.1X authentication to communicate with the RADIUS server.

The RADIUS server:

- must be using the Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) authentication framework.

NOTE: RADIUS servers that support other widely-used authentication frameworks, such as password-only or md5, cannot be used to support MACsec.

- must be using 802.1X authentication.
- can be multiple hops from the switch and the host device.

MACsec Software Image Requirements for EX Series and QFX Series Switches

Junos OS Release 16.1 and Later

For Junos OS Release 16.1 and later, you must download the standard Junos image to enable MACsec. MACsec is not supported in the limited image. See the "MACsec Hardware and Software Support Summary" on page 96 to determine the correct release for your device.

The standard version of Junos OS software contains encryption and is, therefore, not available to customers in all geographies. The export and re-export of this Junos OS software is strictly controlled under United States export laws. The export, import, and use of this Junos OS software is also subject to controls imposed under the laws of other countries. If you have questions about acquiring this version of your Junos OS software, contact Juniper Networks Trade Compliance group at compliance_helpdesk@juniper.net.

Junos OS Releases Prior to 16.1

For releases prior to Junos OS Release 16.1, you must download the controlled version of your Junos OS software to enable MACsec. MACsec support is not available in the domestic version of Junos OS software in releases prior to Junos OS Release 16.1. See the "MACsec Hardware and Software Support Summary" on page 96 to determine the correct release for your device.

The controlled version of Junos OS software includes all features and functionality available in the domestic version of Junos OS, while also supporting MACsec. The domestic version of Junos OS software is shipped on all switches that support MACsec, so you must download and install a controlled version of Junos OS software for your switch before you can enable MACsec.

The controlled version of Junos OS software contains encryption and is, therefore, not available to customers in all geographies. The export and re-export of the controlled version of Junos OS software is strictly controlled under United States export laws. The export, import, and use of the controlled version of Junos OS software is also subject to controls imposed under the laws of other countries. If you have questions about acquiring

the controlled version of your Junos OS software, contact Juniper Networks Trade Compliance group at compliance_helpdesk@juniper.net.

MACsec Hardware and Software Support Summary

Table 23 on page 96 summarizes MACsec hardware and software support for EX Series and QFX Series switches.

See Feature Explorer for a full listing of Junos OS releases and platforms that support MACsec.

Table 23: MACsec Hardware and Software Support Summary for EX Series and QFX Series Switches

Switch	MACsec-capable Interfaces	Switch-to-Switch Support Introduction	Switch-to-Host Support Introduction	Encryption
EX3400	10GbE fiber interfaces and 1GbE copper interfaces.	15.1X53-D50	15.1X53-D50	AES-128 NOTE: MACsec is not available on the limited Junos OS image package.
EX4200	All uplink port connections on the SFP+ MACsec uplink module.	13.2X50-D15	14.1X53-D10	AES-128
EX4300	All access and uplink ports.	13.2X50-D15	14.1X53-D10	AES-128
EX4550	All EX4550 optical interfaces that use the *LC* connection type. See *Pluggable Transceivers Supported on EX4550 Switches*.	13.2X50-D15	14.1X53-D10	AES-128
EX4600	All twenty-four fixed 1GbE SFP/10GbE SFP+ interfaces and all interfaces that support the copper Gigabit Interface Converter (GBIC). All eight SFP+ interfaces on the EX4600-EM-8F expansion module.	14.1X53-D15 NOTE: MACsec is not supported on EX4600 in Junos OS Release 15.1.	Not supported	AES-128

Table 23: MACsec Hardware and Software Support Summary for EX Series and QFX Series Switches (continued)

Switch	MACsec-capable Interfaces	Switch-to-Switch Support Introduction	Switch-to-Host Support Introduction	Encryption
EX9200	All forty SFP interfaces on the EX9200-40F-M line card. All twenty SFP interfaces on the EX9200-20F-MIC installed in an EX9200-MPC line card. NOTE: You can install up to two EX9200-20F-MIC MICs in an EX9200-MPC line card for a maximum of forty MACsec-capable interfaces. All forty SFP+ interfaces on the EX9200-40XS.	15.1R1	15.1R1	AES-128 NOTE: Starting in Junos OS Release 18.2R1, AES-256 is supported on the EX9200-40XS line card.
QFX5100	All eight SFP+ interfaces on the EX4600-EM-8F expansion module installed in a QFX5100-24Q switch.	14.1X53-D15 NOTE: MACsec is not supported on QFX5100-24Q switches in Junos OS Release 15.1.	Not supported	AES-128

Table 23: MACsec Hardware and Software Support Summary for EX Series and QFX Series Switches (continued)

Switch	MACsec-capable Interfaces	Switch-to-Switch Support Introduction	Switch-to-Host Support Introduction	Encryption
QFX10008 and QFX10016	All six interfaces on the QFX10000-6C-DWDM line card.	17.2R1 NOTE: Static CAK mode only.	Not supported	AES-128 and AES-256 NOTE: When enabling MACsec on the QFX10000-6C-DWDM line card, we recommend using a cipher suite with extended packet numbering (XPN). Supported XPN cipher suites are GCM-AES-XPN-128 and GCM-AES-XPN-256.
	All 30 interfaces on the QFX10000-30C-M line card.	17.4R1 NOTE: Static CAK mode only.	Not supported	AES-128 and AES-256 NOTE: When enabling MACsec on the QFX10000-30C-M line card, we recommend using a cipher suite with extended packet numbering (XPN). Supported XPN cipher suites are GCM-AES-XPN-128 and GCM-AES-XPN-256.

Understanding MACsec in a Virtual Chassis

MACsec can be configured on supported switch interfaces when those switches are configured in a Virtual Chassis or Virtual Chassis Fabric (VCF), including when MACsec-supported interfaces are on member switches in a mixed Virtual Chassis or VCF that includes switch interfaces that do not support MACsec. MACsec, however, cannot be enabled on Virtual Chassis ports (VCPs) to secure traffic travelling between member switches in a Virtual Chassis or VCF.

Understanding the MACsec Feature License Requirement

A feature license is required to configure MACsec on EX Series and QFX series switches, with the exception of the QFX10000-6C-DWDM and QFX10000-30C-M line cards. If the MACsec licence is not installed, MACsec functionality cannot be activated.

To purchase a feature license for MACsec, contact your Juniper Networks sales representative (https://www.juniper.net/us/en/contact-us/sales-offices). The Juniper sales representative will provide you with a feature license file and a license key. You will

be asked to supply the chassis serial number of your switch; you can obtain the serial number by running the **show chassis hardware** command.

The MACsec feature license is an independent feature license; the feature licenses that must be purchased to enable other groups of features on your switches cannot be purchased to enable MACsec.

MACsec Limitations

- All types of Spanning Tree Protocol frames cannot currently be encrypted using MACsec.
- MACsec traffic drops are expected during GRES switchover.

See Also
- Configuring Media Access Control Security (MACsec) on page 99

Configuring Media Access Control Security (MACsec)

Media Access Control Security (MACsec) is an industry-standard security technology that provides secure communication for almost all types of traffic on Ethernet links. MACsec provides point-to-point security on Ethernet links between directly-connected nodes and is capable of identifying and preventing most security threats, including denial of service, intrusion, man-in-the-middle, masquerading, passive wiretapping, and playback attacks. MACsec is standardized in IEEE 802.1AE.

You can configure MACsec to secure point-to-point Ethernet links connecting EX Series or QFX Series switches, or on Ethernet links connecting a switch to a host device such as a PC, phone, or server. Each point-to-point Ethernet link that you want to secure using MACsec must be configured independently. You can enable MACsec on switch-to-switch links using static secure association key (SAK) security mode or static connectivity association key (CAK) security mode. Both processes are provided in this document.

BEST PRACTICE: We recommend enabling MACsec using static CAK security mode on switch-to-switch links. Static CAK security mode ensures security by frequently refreshing to a new random secure association key (SAK) and by only sharing the SAK between the two devices on the MACsec-secured point-to-point link. Additionally, some optional MACsec features—replay protection, SCI tagging, and the ability to exclude traffic from MACsec—are only available for MACsec-secured switch-to-switch connections that are enabled using static CAK security mode.

The configuration steps for both processes are provided in this document.

BEST PRACTICE: When enabling MACsec, we recommend that when you examine your interface MTU, adjusting it for MACsec overhead, which is 32 bytes.

NOTE: This topic pertains to switches that support MACsec. Any specifics about a particular switch are identified as such.

Acquiring and Downloading the Junos OS Software

For Junos OS Release 16.1 and later, you must download the standard Junos image to enable MACsec. MACsec is not supported in the limited image.

For releases prior to Junos OS Release 16.1, you must download the controlled version of your Junos OS software to enable MACsec. MACsec support is not available in the domestic version of Junos OS software in releases prior to Junos OS Release 15.1.

You can identify whether a software package is the standard or controlled version of Junos OS by viewing the package name. A software package for a controlled version of Junos OS is named using the following format:

***package-name-m.nZx.y*-controlled-signed.tgz**

A software package for a standard version of Junos OS is named using the following format:

***package-name-m.nZx.y*-.tgz**

If you are unsure which version of Junos OS is running on your switch, enter the **show version** command. If the **JUNOS Crypto Software Suite** description appears in the output, you are running the controlled version of Junos OS. If you are running a controlled version of Junos OS, enter the **show system software** command to display the version. The output also shows the version of all loaded software packages.

The controlled version of Junos OS software for EX Series or QFX Series switches contains encryption and is, therefore, not available to customers in all geographies. The export and re-export of the controlled version of Junos OS software is strictly controlled under United States export laws. The export, import, and use of the controlled version of Junos OS software is also subject to controls imposed under the laws of other countries. If you

have questions about acquiring the controlled version of your Junos OS software, contact Juniper Networks Trade Compliance group at **compliance_helpdesk@juniper.net**.

The standard version of Junos OS software for EX Series and QFX Series switches contains encryption and is, therefore, not available to customers in all geographies. The export and re-export of this Junos OS software is strictly controlled under United States export laws. The export, import, and use of this Junos OS software is also subject to controls imposed under the laws of other countries. If you have questions about acquiring this version of your Junos OS software, contact Juniper Networks Trade Compliance group at **compliance_helpdesk@juniper.net**.

The process for installing the controlled or standard version of Junos OS software onto your switch is identical to installing any other version of Junos OS software. You must enter the **request system software add** statement to download the Junos OS image, and the **request system reboot** statement to reboot the switch to complete the upgrade procedure.

See "Understanding Media Access Control Security (MACsec)" on page 89 for additional information on the versions of Junos OS software that are required for MACsec.

Acquiring and Downloading the MACsec Feature License

A feature license is required to configure MACsec on an EX Series or a QFX Series switch, with the exception of the QFX10000-6C-DWDM and QFX10000-30C-M line cards. If the MACsec licence is not installed, MACsec functionality cannot be activated.

The MACsec feature license is an independent feature license; the enhanced feature licenses (EFLs) or advanced feature licenses (AFLs) that must be purchased to enable some features on EX Series or QFX Series switches cannot be purchased to enable MACsec.

To purchase a software license for MACsec, contact your Juniper Networks sales representative (https://www.juniper.net/us/en/contact-us/sales-offices). The Juniper sales representative will provide you with a feature license file and a license key. You will be asked to supply the chassis serial number of your switch; you can obtain the serial number by running the **show chassis hardware** command.

For a Virtual Chassis deployment, two MACsec license keys are recommended for redundancy—one for the device in the master role and the other for the device in the backup role

To add one or more new MACsec license keys on the switch, follow this procedure:

1. Add the license key or keys:
   - To add one or more license keys from a file or URL, specify the filename of the file or the URL where the key is located:

     ```
     user@switch> request system license add filename |url
     ```

   - To add a license key from the terminal:

     ```
     user@switch> request system license add terminal
     ```


2. When prompted, enter the license key, separating multiple license keys with a blank line.

   If the license key you enter is invalid, an error appears in the CLI output when you press Ctrl+d to exit the license entry mode.

A MACsec feature license is installed and maintained like any other switch license. See "Managing Licenses for the EX Series Switch (CLI Procedure)" on page 77 or "Adding New Licenses (CLI Procedure)" on page 36 for more detailed information on configuring and managing your MACsec software license.

Configuring the PIC Mode of the MACsec-capable Interfaces (EX4200 switches only)

To configure MACsec on an EX4200 switch, you must install the SFP+ MACsec uplink module. The interfaces on the SFP+ MACsec uplink module are the only MACsec-capable interfaces available for EX4200 switches. All four ports on the uplink module are MACsec-capable.

The SFP+ MACsec uplink module provides two ports for 10-gigabit small form-factor pluggable (SFP+) transceivers when configured to operate in 10-gigabit mode or four ports for 1-gigabit small form-factor pluggable (SFP) transceivers when configured to operate in 1-gigabit mode.

The PIC mode is set to **10g**, by default. You only need to perform this procedure if you want to operate your uplink in 1-gigabit mode, or if you previously set the uplink module to 1-gigabit mode and would like to return it to 10-gigabit mode.

To configure the PIC mode:

```
[edit chassis]
user@switch# set fpc fpc-slot-number pic 1 sfpplus pic-mode (1g | 10g)
```

where ***fpc-slot-number*** is the FPC slot number, ***pic-slot-number*** is the PIC slot number, and the **[1g | 10g]** option configures the MACsec capability of the four SFP+ ports on the MACsec uplink module.

The ***fpc-slot-number*** is always 0 on standalone EX4200 switches, and is the member ID of the member switch in an EX4200 Virtual Chassis.

The PIC slot number is always 1 for the uplink module port slot on an EX4200 switch, so **pic 1** is always the specified PIC slot number.

The PIC mode is set to **10g** by default. When the PIC mode is set to **10g**, uplink ports 0 and 2 on the MACsec uplink module support MACsec at 10-Gbps speeds. Ports 1 and 3 cannot be used to send any traffic.

When the PIC mode is set to **1g**, all four SFP+ ports on the MACsec uplink module support MACsec at 1-Gbps speeds.

Configuring MACsec Using Static Connectivity Association Key Security Mode (Recommended for Enabling MACsec on Switch-to-Switch Links)

You can enable MACsec using static connectivity association key (CAK) security mode or static secure association keys (SAK) security mode on a point-to-point Ethernet link connecting switches. This procedure shows you how to configure MACsec using static CAK security mode.

BEST PRACTICE: We recommend enabling MACsec using static CAK security mode on switch-to-switch links. Static CAK security mode ensures security by frequently refreshing to a new random secure association key (SAK) and by only sharing the SAK between the two devices on the MACsec-secured point-to-point link. Additionally, some optional MACsec features—replay protection, SCI tagging, and the ability to exclude traffic from MACsec—are only available for MACsec-secured switch-to-switch connections that are enabled using static CAK security mode.

When you enable MACsec using static CAK security mode, a pre-shared key is exchanged between the switches on each end of the point-to-point Ethernet link. The pre-shared key includes a connectivity association name (CKN) and a connectivity association key (CAK). The CKN and CAK are configured by the user in the connectivity association and must match on both ends of the link to initially enable MACsec.

After the pre-shared keys are exchanged and verified, the MACsec Key Agreement (MKA) protocol, which enables and maintains MACsec on the link, is enabled. The MKA is responsible for selecting one of the two switches on the point-to-point link as the key server. The key server then creates a randomized security key that is shared only with the other device over the MACsec-secured link. The randomized security key enables and maintains MACsec on the point-to-point link. The key server will continue to periodically create and share a randomly-created security key over the point-to-point link for as long as MACsec is enabled.

NOTE: If the MACsec session is terminated due to a link failure, when the link is restored, the MKA key server elects a key server and generates a new SAK.

You enable MACsec using static CAK security mode by configuring a connectivity association on both ends of the link. All configuration is done within the connectivity association but outside of the secure channel. Two secure channels—one for inbound traffic and one for outbound traffic—are automatically created when using static CAK security mode. The automatically-created secure channels do not have any user-configurable parameters that cannot already be configured in the connectivity association.

To configure MACsec using static CAK security mode to secure a switch-to-switch Ethernet link:

1. Create a connectivity association. You can skip this step if you are configuring an existing connectivity association.

   ```
   [edit security macsec]
   user@switch# set connectivity-association connectivity-association-name
   ```

   For instance, to create a connectivity association named **ca1**, enter:

   ```
   [edit security macsec]
   user@switch# set connectivity-association ca1
   ```

2. Configure the MACsec security mode as **static-cak** for the connectivity association:

   ```
   [edit security macsec]
   user@switch# set connectivity-association connectivity-association-name security-mode
   static-cak
   ```

   For instance, to configure the MACsec security mode to **static-cak** on connectivity association ca1:

   ```
   [edit security macsec]
   user@switch# set connectivity-association ca1 security-mode static-cak
   ```

3. Create the pre-shared key by configuring the connectivity association key name (CKN) and connectivity association key (CAK):

   ```
   [edit security macsec]
   user@switch# set connectivity-association connectivity-association-name pre-shared-key
   ckn hexadecimal-number
   user@switch# set connectivity-association connectivity-association-name pre-shared-key
   cak hexadecimal-number
   ```

   A pre-shared key is exchanged between directly-connected links to establish a MACsec-secure link. The pre-shared-key includes the CKN and the CAK. The CKN is a 64-digit hexadecimal number and the CAK is a 32-digit hexadecimal number. The CKN and the CAK must match on both ends of a link to create a MACsec-secured link.

   NOTE: To maximize security, we recommend configuring all 64 digits of a CKN and all 32 digits of a CAK.

   If you do not configure all 64 digits of a CKN or all 32 digits of a CAK, all remaining digits will be auto-configured to 0. However, you will receive a warning message when you commit the configuration.

   After the pre-shared keys are successfully exchanged and verified by both ends of the link, the MACsec Key Agreement (MKA) protocol is enabled and manages the secure link. The MKA protocol then elects one of the two directly-connected switches as the key server. The key server then shares a random security with the other device over the MACsec-secure point-to-point link. The key server will continue to periodically create and share a random security key with the other device over the MACsec-secured point-to-point link as long as MACsec is enabled.

To configure a CKN of **37c9c2c45ddd012aa5bc8ef284aa23ff6729ee2e4acb66e91fe34ba2cd9fe311** and CAK of **228ef255aa23ff6729ee664acb66e91f** on connectivity association ca1:

```
[edit security macsec]
user@switch# set connectivity-association ca1 pre-shared-key ckn
37c9c2c45ddd012aa5bc8ef284aa23ff6729ee2e4acb66e91fe34ba2cd9fe311
user@switch# set connectivity-association ca1 pre-shared-key cak
228ef255aa23ff6729ee664acb66e91f
```

NOTE: MACsec is not enabled until a connectivity association is attached to an interface. See the final step of this procedure to attach a connectivity association to an interface.

4. (Required on non-EX4300 switches when connecting to EX4300 switches only) Enable SCI tagging:

   ```
   [edit security macsec connectivity-association connectivity-association-name]
   user@switch# set include-sci
   ```

   You must enable SCI tagging on a switch that is enabling MACsec on an Ethernet link connecting to an EX4300 switch.

   SCI tags are automatically appended to packets leaving a MACsec-enabled interface on an EX4300 switch. This option is, therefore, not available on EX4300 switches.

   You should only use this option when enabling MACsec on a link a to an EX4300 switch. SCI tags are eight octets long, so appending an SCI tag to all traffic on the link adds a significant amount of unneeded overhead.

5. (Optional) Set the MKA key server priority:

   ```
   [edit security macsec connectivity-association connectivity-association-name]
   user@switch# set mka key-server-priority priority-number
   ```

   Specifies the key server priority used by the MKA protocol to select the key server. The switch with the lower *priority-number* is selected as the key server.

   The default *priority-number* is 16.

   If the **key-server-priority** is identical on both sides of the point-to-point link, the MKA protocol selects the interface with the lower MAC address as the key server. Therefore, if this statement is not configured in the connectivity associations at each end of a MACsec-secured point-to-point link, the interface with the lower MAC address becomes the key server.

   To change the key server priority to 0 to increase the likelihood that the current device is selected as the key server when MACsec is enabled on the interface using connectivity association **ca1**:

   ```
   [edit security macsec connectivity-association ca1]
   ```

```
user@switch# set mka key-server-priority 0
```

To change the key server priority to 255 to decrease the likelihood that the current device is selected as the key server in connectivity association ca1:

```
[edit security macsec connectivity-association ca1]
user@switch# set mka key-server-priority 255
```

6. (Optional) Set the MKA transmit interval:

```
[edit security macsec connectivity-association connectivity-association-name]
user@switch# set mka transmit-interval interval
```

The MKA transmit interval setting sets the frequency for how often the MKA protocol data unit (PDU) is sent to the directly connected device to maintain MACsec connectivity on the link. A lower *interval* increases bandwidth overhead on the link; a higher *interval* optimizes MKA protocol communication.

The default *interval* is 2000ms. We recommend increasing the interval to 6000 ms in high-traffic load environments. The transmit interval settings must be identical on both ends of the link when MACsec using static CAK security mode is enabled.

For instance, if you wanted to increase the MKA transmit interval to 6000 milliseconds when connectivity association ca1 is attached to an interface:

```
[edit security macsec connectivity-association ca1]
user@switch# set mka transmit-interval 6000
```

7. (Optional) Disable MACsec encryption:

```
[edit security macsec connectivity-association connectivity-association-name]
user@switch# set no-encryption
```

Encryption is enabled for all traffic entering or leaving the interface when MACsec is enabled using static CAK security mode, by default.

When encryption is disabled, traffic is forwarded across the Ethernet link in clear text. You are able to view unencrypted data in the Ethernet frame traversing the link when you are monitoring it. The MACsec header is still applied to the frame, however, and all MACsec data integrity checks are run on both ends of the link to ensure the traffic sent or received on the link has not been tampered with and does not represent a security threat.

8. (Optional) Set an offset for all packets traversing the link:

```
[edit security macsec connectivity-association connectivity-association-name]
user@switch# set offset (0 | 30 | 50)
```

For instance, if you wanted to set the offset to 30 in the connectivity association named **ca1**:

```
[edit security macsec connectivity-association ca1]
user@switch# set offset 30
```

The default offset is 0. All traffic in the connectivity association is encrypted when encryption is enabled and an **offset** is not set.

When the offset is set to 30, the IPv4 header and the TCP/UDP header are unencrypted while encrypting the rest of the traffic. When the offset is set to 50, the IPv6 header and the TCP/UDP header are unencrypted while encrypting the rest of the traffic.

You would typically forward traffic with the first 30 or 50 octets unencrypted if a feature needed to see the data in the octets to perform a function, but you otherwise prefer to encrypt the remaining data in the frames traversing the link. Load balancing features, in particular, typically need to see the IP and TCP/UDP headers in the first 30 or 50 octets to properly load balance traffic.

9. (Optional) Enable replay protection.

```
[edit security macsec connectivity-association connectivity-association-name]
user@switch# set replay-protect replay-window-size number-of-packets
```

When MACsec is enabled on a link, an ID number is assigned to each packet on the MACsec-secured link.

When replay protection is enabled, the receiving interface checks the ID number of all packets that have traversed the MACsec-secured link. If a packet arrives out of sequence and the difference between the packet numbers exceeds the replay protection window size, the packet is dropped by the receiving interface. For instance, if the replay protection window size is set to five and a packet assigned the ID of 1006 arrives on the receiving link immediately after the packet assigned the ID of 1000, the packet that is assigned the ID of 1006 is dropped because it falls outside the parameters of the replay protection window.

Replay protection is especially useful for fighting man-in-the-middle attacks. A packet that is replayed by a man-in-the-middle attacker on the Ethernet link will arrive on the receiving link out of sequence, so replay protection helps ensure the replayed packet is dropped instead of forwarded through the network.

Replay protection should not be enabled in cases where packets are expected to arrive out of order.

You can require that all packets arrive in order by setting the replay window size to 0.

To enable replay protection with a window size of five on connectivity association **ca1**:

```
[edit security macsec connectivity-association ca1]
user@switch# set replay-protect replay-window-size 5
```

10. (Optional) Exclude a protocol from MACsec:

```
[edit security macsec connectivity-association connectivity-association-name]
user@switch# set exclude-protocol protocol-name
```

For instance, if you did not want Link Level Discovery Protocol (LLDP) to be secured using MACsec:

```
[edit security macsec connectivity-association connectivity-association-name]
```

```
user@switch# set exclude-protocol lldp
```

When this option is enabled, MACsec is disabled for all packets of the specified protocol—in this case, LLDP—that are sent or received on the link.

11. Assign the connectivity association to an interface:

```
[edit security macsec]
user@switch# set interfaces interface-names connectivity-association
connectivity-association-name
```

Assigning the connectivity association to an interface is the final configuration step to enabling MACsec on an interface.

For instance, to assign connectivity association ca1 to interface xe-0/0/1:

```
[edit security macsec]
user@switch# set interfaces xe-0/1/0 connectivity-association ca1
```

NOTE: On an EX4300 uplink module, the first transceiver plugged into the uplink module determines the PIC mode, as the PIC recognizes the SFP type and programs all of the ports to be either ge- or xe-. Make sure the MACsec configuration on the interface matches the link speed for the uplink module ports.

MACsec using static CAK security mode is not enabled until a connectivity association on the opposite end of the link is also configured, and contains pre-shared keys that match on both ends of the link.

See Also

- Understanding Media Access Control Security (MACsec) on page 89

Configuring MACsec on the Switch Using Dynamic Secure Association Key Security Mode to Secure a Switch-to-Host Link

Before you begin to enable MACsec on a switch-to-host link:

- Confirm that MACsec on switch-to-host links is supported on your switch. See "Understanding Media Access Control Security (MACsec)" on page 89.
- Configure a RADIUS server. The RADIUS server:
  - must be configured as the user database for 802.1X authentication.
  - Starting in Junos OS Release 15.1, the Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) authentication framework is required for MACsec on a switch-to-host link.
  - must have connectivity to the switch and to the host. The RADIUS server can be multiple hops from the switch or the host.

  See *Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch*.

- Enable MACsec on the host device.

  The procedures for enabling MACsec on the host device varies by host device, and is beyond the scope of this document.

To configure MACsec using dynamic security mode to secure a switch-to-host Ethernet link:

1. Create a connectivity association. You can skip this step if you are configuring an existing connectivity association.

   ```
   [edit security macsec]
   user@switch# set connectivity-association connectivity-association-name
   ```

   For instance, to create a connectivity association named ca-dynamic1, enter:

   ```
   [edit security macsec]
   user@switch# set connectivity-association ca-dynamic1
   ```

2. Configure the MACsec security mode as dynamic for the connectivity association:

   ```
   [edit security macsec]
   user@switch# set connectivity-association connectivity-association-name security-mode
   dynamic
   ```

   For instance, to configure the MACsec security mode to dynamic on connectivity association ca-dynamic1:

   ```
   [edit security macsec]
   user@switch# set connectivity-association ca-dynamic1 security-mode dynamic
   ```

3. (Optional) Configure the **must-secure** option:

   ```
   [edit security macsec]
   user@switch# set connectivity-association connectivity-association-name mka must-secure
   ```

   When the **must-secure** option is enabled, all traffic that is not MACsec-secured that is received on the interface is dropped.

   When the **must-secure** option is disabled, all traffic from devices that support MACsec is MACsec-secured while traffic received from devices that do no support MACsec is forwarded through the network.

   The **must-secure** option is particularly useful in scenarios where multiple devices, such as a phone and a PC, are accessing the network through the same Ethernet interface. If one of the devices supports MACsec while the other device does not support MACsec, the device that doesn't support MACsec can continue to send and receive traffic over the network—provided the **must-secure** option is disabled—while traffic to and from the device that supports MACsec is MACsec-secured. In this scenario, traffic to the device that is not MACsec-secured must be VLAN-tagged.

   The **must-secure** option is disabled, by default.

4. (Required only if the host device requires SCI tagging) Enable SCI tagging:


```
[edit security macsec connectivity-association connectivity-association-name]
user@switch# set include-sci
```

You should only use this option when connecting a switch to a host that requires SCI tags. SCI tags are eight octets long, so appending an SCI tag to all traffic on the link adds a significant amount of unneeded overhead.

5. (Optional) Set the MKA key server priority:

```
[edit security macsec connectivity-association connectivity-association-name]
user@switch# set mka key-server-priority priority-number
```

Specifies the key server priority used by the MKA protocol to select the key server. The switch with the lower *priority-number* is selected as the key server.

The default *priority-number* is 16. If the **key-server-priority** is identical on both sides of the point-to-point link, the MKA protocol selects the interface with the lower MAC address as the key server. Therefore, if this statement is not configured in the connectivity associations at each end of a MACsec-secured point-to-point link, the interface with the lower MAC address becomes the key server.

To change the key server priority to 0 to increase the likelihood that the current device is selected as the key server when MACsec is enabled on the interface using connectivity association ca1:

```
[edit security macsec connectivity-association ca-dynamic1]
user@switch# set mka key-server-priority 0
```

To change the key server priority to 255 to decrease the likelihood that the current device is selected as the key server in connectivity association ca-dynamic1:

```
[edit security macsec connectivity-association ca-dynamic1]
user@switch# set mka key-server-priority 255
```

6. (Optional) Set the MKA transmit interval:

```
[edit security macsec connectivity-association connectivity-association-name]
user@switch# set mka transmit-interval interval
```

The MKA transmit interval setting sets the frequency for how often the MKA protocol data unit (PDU) is sent to the directly connected device to maintain MACsec connectivity on the link. A lower interval increases bandwidth overhead on the link; a higher interval optimizes MKA protocol communication.

The default interval is 2000ms. We recommend increasing the interval to 6000 ms in high-traffic load environments. The transmit interval settings must be identical on both ends of the link.

For instance, if you wanted to increase the MKA transmit interval to 6000 milliseconds when connectivity association ca-dynamic1 is attached to an interface:

```
[edit security macsec connectivity-association ca-dynamic1]
user@switch# set mka transmit-interval 6000
```

7. (Optional) Disable MACsec encryption:

   ```
   [edit security macsec connectivity-association connectivity-association-name]
   user@switch# set no-encryption
   ```

   Encryption is enabled for all traffic entering or leaving the interface when MACsec is enabled using dynamic security mode, by default. When encryption is disabled, traffic is forwarded across the Ethernet link in clear text. You are able to view unencrypted data in the Ethernet frame traversing the link when you are monitoring it. The MACsec header is still applied to the frame, however, and all MACsec data integrity checks are run on both ends of the link to ensure the traffic sent or received on the link has not been tampered with and does not represent a security threat.

8. (Optional) Set an offset for all packets traversing the link:

   ```
   [edit security macsec connectivity-association connectivity-association-name]
   user@switch# set offset (0 | 30 | 50)
   ```

   For instance, if you wanted to set the offset to 30 in the connectivity association named ca-dynamic1:

   ```
   [edit security macsec connectivity-association ca-dynamic1]
   user@switch# set offset 30
   ```

   The default offset is 0. All traffic in the connectivity association is encrypted when encryption is enabled and an offset is not set.

   When the offset is set to 30, the IPv4 header and the TCP/UDP header are unencrypted while encrypting the rest of the traffic. When the offset is set to 50, the IPv6 header and the TCP/UDP header are unencrypted while encrypting the rest of the traffic.

   You would typically forward traffic with the first 30 or 50 octets unencrypted if a feature needed to see the data in the octets to perform a function, but you otherwise prefer to encrypt the remaining data in the frames traversing the link. Load balancing features, in particular, typically need to see the IP and TCP/UDP headers in the first 30 or 50 octets to properly load balance traffic.

9. (Optional) Enable replay protection.

   ```
   [edit security macsec connectivity-association connectivity-association-name]
   user@switch# set replay-protect replay-window-size number-of-packets
   ```

   When MACsec is enabled on a link, an ID number is assigned to each packet on the MACsec-secured link. When replay protection is enabled, the receiving interface checks the ID number of all packets that have traversed the MACsec-secured link. If a packet arrives out of sequence and the difference between the packet numbers exceeds the replay protection window size, the packet is dropped by the receiving interface. For instance, if the replay protection window size is set to five and a packet assigned the ID of 1006 arrives on the receiving link immediately after the packet assigned the ID of 1000, the packet that is assigned the ID of 1006 is dropped because it falls outside the parameters of the replay protection window.

Replay protection is especially useful for fighting man-in-the-middle attacks. A packet that is replayed by a man-in-the-middle attacker on the Ethernet link will arrive on the receiving link out of sequence, so replay protection helps ensure the replayed packet is dropped instead of forwarded through the network.

Replay protection should not be enabled in cases where packets are expected to arrive out of order.

You can require that all packets arrive in order by setting the replay window size to 0.

To enable replay protection with a window size of five on connectivity association ca-dynamic1:

```
[edit security macsec connectivity-association ca-dynamic1]
user@switch# set replay-protect replay-window-size 5
```

10. (Optional) Exclude a protocol from MACsec:

```
[edit security macsec connectivity-association connectivity-association-name]
user@switch# set exclude-protocol protocol-name
```

For instance, if you did not want Link Level Discovery Protocol (LLDP) to be secured using MACsec:

```
[edit security macsec connectivity-association ca-dynamic1]
user@switch# set exclude-protocol lldp
```

When this option is enabled, MACsec is disabled for all packets of the specified protocol—in this case, LLDP—that are sent or received on the link.

BEST PRACTICE: We recommend that any protocol other than MACsec being used on the MACsec connection, such as LLDP, LACP, STP, or layer 3 routing protocols, should be excluded and moved outside of the MACsec tunnel.

11. Assign the connectivity association to an interface:

```
[edit security macsec]
user@switch# set interfaces interface-names connectivity-association
connectivity-association-name
```

Assigning the connectivity association to an interface is the final configuration step to enabling MACsec on an interface. For instance, to assign connectivity association ca-dynamic1 to interface xe-0/0/1:

```
[edit security macsec]
user@switch# set interfaces xe-0/1/0 connectivity-association ca-dynamic1
```

NOTE: On an EX4300 uplink module, the first transceiver plugged into the uplink module determines the PIC mode, as the PIC recognizes the SFP type and programs all of the ports to be either ge- or xe-. Make sure the MACsec configuration on the interface matches the link speed for the uplink module ports.

Configuring MACsec Using Static Secure Association Key Security Mode to Secure a Switch-to-Switch Link

When you enable MACsec using static secure association key (SAK) security mode, one of up to two manually configured security keys is used to secure the point-to-point Ethernet link between the switches. All security key names and values are configured by the user; there is no key server or other tool that creates security keys. Security is maintained on the point-to-point Ethernet link by periodically rotating the security keys. Each security key name and value must have a corresponding matching value on the interface at the other end of the point-to-point Ethernet link to maintain MACsec on the link.

You configure static SAKs within secure channels when you are enabling MACsec using static SAK security mode. You configure secure channels within connectivity associations. A typical connectivity association for MACsec using static SAK security mode contains two secure channels—one for inbound traffic and one for outbound traffic—that have each been configured with two static SAKs. You must attach the connectivity association with the secure channel configurations to an interface to enable MACsec using static SAK security mode.

To configure MACsec on a switch-to-switch Ethernet link using static SAK security mode:

1. Create a connectivity association. You can skip this step if you are configuring an existing connectivity association.

   ```
   [edit security macsec]
   user@switch# set connectivity-association connectivity-association-name
   ```

   For instance, to create a connectivity association named **ca1**, enter:

   ```
   [edit security macsec]
   user@switch# set connectivity-association ca1
   ```

2. Configure the MACsec security mode as **static-sak** for the connectivity association:

   ```
   [edit security macsec]
   user@switch# set connectivity-association connectivity-association-name security-mode
   static-sak
   ```

   For instance, to configure the MACsec security mode to **static-sak** on connectivity association ca1:

   ```
   [edit security macsec]
   user@switch# set connectivity-association ca1 security-mode static-sak
   ```

3. Create a secure channel within the connectivity association. You can skip this step if you are configuring an existing secure channel.

   ```
   [edit security macsec]
   user@switch# set connectivity-association connectivity-association-name secure-channel
   secure-channel-name
   ```

   For instance, to create secure channel **sc1** in connectivity association **ca1**, enter:

   ```
   [edit security macsec]
   user@switch# set connectivity-association ca1 secure-channel sc1
   ```

4. Define the security associations and the static SAKs for the secure channel:

   ```
   [edit security macsec]
   user@switch# set connectivity-association connectivity-association-name secure-channel
   secure-channel-name security-association number key key-string
   ```

   where the **security-association** ***number*** is a number between 0 and 3, and the *key-string* is a 32-digit key defined statically by the network administrator.

   The key string is a 32-digit hexadecimal number. The key string and the security association must match on both sides of an Ethernet connection to secure traffic using MACsec.

   A secure channel must have at least two security associations with unique key strings. MACsec uses a security associations to establish a secure communications link, and periodically rotates to a new security association to keep the link secure. MACsec, therefore, must have at least one backup security association and key at all times.

   To create one secure channel with two security associations and keys, for example:

   ```
   [edit security macsec]
   user@switch# set connectivity-association ca1 secure-channel sc1 security-association 0 key
   d183c4002fa6fe3d2d9a852c20ab8412
   user@switch# set connectivity-association ca1 secure-channel sc1 security-association 1 key
   b976c7494ab6fe2f2d4c432a90fd90a8
   ```

5. Specify whether the secure channel should be applied to traffic entering or leaving the switch:

   ```
   [edit security macsec]
   user@switch# set connectivity-association connectivity-association-name secure-channel
   secure-channel-name direction [inbound | outbound]
   ```

   where **inbound** applies the secure channel to traffic entering the switch, and **outbound** applies the secure channel to traffic leaving the switch.

NOTE: A secure channel can only be applied to traffic entering (**inbound**) or leaving (**outbound**) an interface on the switch.

If you need to configure MACsec using SAKs on inbound and outbound traffic on the same interface, you must configure a connectivity association with one secure channel for inbound traffic and a second secure channel for outbound traffic. The connectivity association is assigned to an interface later in this process.

For instance, to configure secure channel **sc1** to apply MACsec to incoming traffic:

```
[edit security macsec]
user@switch# set connectivity-association ca1 secure-channel sc1 direction inbound
```

To configure secure channel **sc2** to apply MACsec to outgoing traffic:

```
[edit security macsec]
user@switch# set connectivity-association ca1 secure-channel sc2 direction outbound
```

6. Specify a MAC address:

```
[edit security macsec]
user@switch# set connectivity-association connectivity-association-name secure-channel
secure-channel-name id mac-address mac-address
```

If you are configuring a MAC address on a secure channel in the outbound direction, you should specify the MAC address of the interface as the **mac-address**.

If you are configuring a MAC address on a secure channel in the inbound direction, you should specify the MAC address of the interface at the other end of the link as the **mac-address**.

The **mac-address** variables must match on the sending and receiving secure channel on each side of a link to enable MACsec using static SAK security mode.

NOTE: You can see the MAC address of an interface in the **show interfaces** output.

To configure MACsec to accept frames from MAC address **12:34:56:ab:cd:ef** on secure channel **sc1**:

```
[edit security macsec]
user@switch# set connectivity-association ca1 secure-channel sc1 id mac-address
12:34:56:ab:cd:ef
```

7. Specify a port:

```
[edit security macsec]
user@switch# set connectivity-association connectivity-association-name secure-channel
secure-channel-name id port-id port-id-number
```

The **port-id-number** variables must match on a sending and receiving secure channel on each side of a link to enable MACsec.

NOTE: The only requirement for port numbers in this implementation of MACsec is that they match on the sending and receiving ends of an Ethernet link. When the port numbers match, MACsec is enabled for all traffic on the connection.

To specify port ID 4 on secure channel **sc1**:

```
[edit security macsec]
user@switch# set connectivity-association ca1 secure-channel sc1 id port-id 4
```

8. (Optional) Enable encryption:

```
[edit security macsec]
user@switch# set connectivity-association connectivity-association-name secure-channel
secure-channel-name encryption
```

You can enable MACsec without enabling encryption. If a secure channel is configured on an interface without encryption, traffic is forwarded across the Ethernet link in clear text, and you will be able to view unencrypted data in the Ethernet frame traversing the link when you are monitoring it. The MACsec header is still applied to the frame, however, and all MACsec data integrity checks are run on both ends of the link to ensure the traffic on the link does not represent a security threat.

Encryption is disabled by default when you are enabling MACsec using static SAK security mode. To ensure all traffic traversing secure-channel **sc1** is encrypted:

```
[edit security macsec]
user@switch# set connectivity-association ca1 secure-channel sc1 encryption
```

9. (Optional) Set an offset to send the first 30 or 50 octets in unencrypted plain text when encryption is enabled.

```
[edit security macsec]
user@switch# set connectivity-association connectivity-association-name secure-channel
secure-channel-name offset [0 | 30 | 50]
```

When the offset is set to 30, the IPv4 header and the TCP/UDP header are unencrypted while encrypting the rest of the traffic. When the offset is set to 50, the IPv6 header and the TCP/UDP header are unencrypted while encrypting the rest of the traffic.

You would typically forward traffic with the first 30 or 50 octets unencrypted if a feature needed to see the data in the octets to perform a function, but you otherwise prefer to encrypt the remaining data in the frames traversing the link. Load balancing features, in particular, typically need to see the IP and TCP/UDP headers in the first 30 or 50 octets to properly load balance traffic.

The default offset is 0, so all traffic on the link is encrypted when the **encryption** option is enabled and an **offset** is not set.

To change the offset to 30 for secure channel **sc1**:

```
[edit security macsec]
user@switch# set connectivity-association ca1 secure-channel sc1 offset 30
```

10. Assign the connectivity association to an interface:

    ```
    [edit security macsec]
    user@switch# set interfaces interface-names connectivity-association
    connectivity-association-name
    ```

    Assigning the connectivity association to an interface is the final configuration step to enabling MACsec on an interface.

    For instance, to assign connectivity association ca1 to interface xe-0/0/1:

    ```
    [edit security macsec]
    user@switch# set interfaces xe-0/1/0 connectivity-association ca1
    ```

    NOTE: On an EX4300 uplink module, the first transceiver plugged into the uplink module determines the PIC mode, as the PIC recognizes the SFP type and programs all of the ports to be either ge- or xe-. Make sure the MACsec configuration on the interface matches the link speed for the uplink module ports.

MACsec using static SAK security mode is not enabled until a connectivity association on the opposite end of the link is also configured, and the configuration match on both ends of the link.

See Also

- Understanding Media Access Control Security (MACsec) on page 89

CHAPTER 3

Understanding Licensing Requirement and Configuration for PTX and MX Series

Software Licensing Requirements

Software Features That Require Licenses on MX Series Routers Only

Table 6 on page 23 lists the licenses you can purchase for each MX Series software feature. Each license allows you to run the specified software feature on a single device.

NOTE: The DHCP server functionality for Junos OS is part of the subscriber management feature. You must have the S-SA-FP, S-MX80-SA-FP or S-MX104-SA-FP license in order to enable the DHCP server. For service accounting, you must also have S-SSM-FP.

NOTE: This is not a complete list of licenses. Contact your Juniper Networks representative for license information.

For information about how to purchase a software license, contact your Juniper Networks sales representative at https://www.juniper.net/in/en/contact-us/.

Table 24: Junos OS Feature License Model Number for MX Series Routers

Licensed Software Feature	Supported Devices	Model Number
Upgrade license—from MX80-10G-ADV to MX80-40G-ADV	MX80	MX80-10G40G-UPG-ADV-B
Upgrade license—from MX80-10G to MX80-40G	MX80	MX80-10G40G-UPG-B
Upgrade license—from MX80-40G-ADV to full MX80	MX80	MX80-40G-UPG-ADV-B
Upgrade license—from MX80-40G to full MX80	MX80	MX80-40G-UPG-B
Upgrade license-–from MX80-5G-ADV to MX80-10G-ADV	MX80	MX80-5G10G-UPG-ADV-B
Upgrade license—from MX80-5G to MX80-10G	MX80	MX80-5G10G-UPG-B
Upgrade license to activate 2x10GE P2&3	MX104	S-MX104-ADD-2X10GE
Upgrade license to activate 2X10GE P0&1	MX104	S-MX104-UPG-2X10GE
Upgrade license to activate 4X10GE fixed ports on MX104	MX104	S-MX104-UPG-4X10GE
License to support per VLAN queuing on MX80	MX80	S-MX80-Q
License to support per VLAN queuing on MX104	MX104	S-MX104-Q
Chassis-based software license for inline J-Flow monitoring on MX5, MX10, M40, MX80, and MX104 Series routers	MX5, MX10, M40, MX80, and MX104	S-JFLOW-CH-MX5-104
Chassis-based software license for inline J-Flow monitoring on MX240 routers	MX240	S-JFLOW-CH-MX240

Table 24: Junos OS Feature License Model Number for MX Series Routers (continued)

Licensed Software Feature	Supported Devices	Model Number
Chassis-based software license for inline J-Flow monitoring on MX480 routers	MX480	S-JFLOW-CH-MX480
Chassis-based software license for inline J-Flow monitoring on MX960 routers	MX960	S-JFLOW-CH-MX960
Chassis-based software license for inline J-Flow monitoring on MX2008 routers	MX2008	S-JFLOW-CH-MX2008
Chassis-based software license for inline J-Flow monitoring on MX2010 routers	MX2010	S-JFLOW-CH-MX2010
Chassis-based software license for inline J-Flow monitoring on MX2020 routers	MX2020	S-JFLOW-CH-MX2020
Flow monitoring and accounting features using J-Flow service on any Modular Port Concentrator (MPC) or MS-DPC	MX240, MX480, and MX960	S-ACCT-JFLOW-CHASSIS
Software License for in-line J-Flow service on Trio MPCs	MX240, MX480, and MX960	S-ACCT-JFLOW-IN
Flow monitoring and accounting features using J-Flow service on any MPC limited to 10G of total JFLOW traffic	MX80	S-ACCT-JFLOW-IN-10G
Flow monitoring and accounting features using J-Flow service on any MPC limited to 10G of total JFLOW traffic	MX80	S-ACCT-JFLOW-IN-10G-UPG
Flow monitoring and accounting features using J-Flow service on any MPC limited to 5G of total JFLOW traffic	MX80	S-ACCT-JFLOW-IN-5G
Security services (IPsec, VPN and group VPN) license based on a single NPU for MS-MIC, MS-DPC or MS-MPC	MX Series router	S-ES-NPU
2000 IKE sessions on MS-DPC; Chassis based, limited to 6000 per Chassis	MX240, MX480, and MX960	S-ES-2K
4000 IKE sessions on MS-DPC; Chassis based, limited to 6000 per Chassis	MX240, MX480, and MX960	S-ES-4K

Table 24: Junos OS Feature License Model Number for MX Series Routers (continued)

Licensed Software Feature	Supported Devices	Model Number
Upgrade from 2000 IKE sessions to 4000 IKE sessions on MS-DPC; Chassis based, limited to 6000 per Chassis	MX240, MX480, and MX960	S-ES-4K-UPG
6000 IKE sessions on MS-DPC; Chassis based, limited to 6000 per Chassis	MX240, MX480, and MX960	S-ES-6K
Upgrade from 4000 IKE sessions to 6000 IKE Sessions on MS-DPC; Chassis based, limited to 6000 per Chassis	MX240, MX480, and MX960	S-ES-6K-UPG
License to run stateful firewall on one NPU per MS-MIC, MS-DPC or MS-MPC	MX Series routers	S-FW-NPU
License to support DS3 Channelization (down to DS0) on each Modular Interface Card (MIC) for MIC-3D-8DS3-E3; also requires license S-MX80-Q when used on the MX80 platform	MX80, MX104, MX240, MX480, and MX960	S-MIC-3D-8CHDS3
License to support full-scale Layer 3 routes and Layer 3 VPN	MX80	S-MX80-ADV-R
License to support 256K routes	MX104	S-MX104-ADV-R1
License to support scaling Layer 3 and VPN routes to 1 million or more entries on MX104 platforms	MX104	S-MX104-ADV-R2
License to support full-scale Layer 3 routes and Layer 3 VPN on each slot for MPC-3D-16XGE-SFPP	MX240, MX480, and MX960	S-MPC-3D-16XGE-ADV-R
License to support full-scale Layer 3 routes and Layer 3 VPN on each slot for port queuing MPCs	MX240, MX480, and MX960	S-MPC-3D-PQ-ADV-R
License to support full-scale Layer 3 routes and Layer 3 VPN on each slot for hierarchical quality of service (HQoS) MPCs	MX240, MX480, and MX960	S-MPC-3D-VQ-ADV-R
Subscriber Management Feature Pack License for MX80	MX80	S-MX80-SA-FP
Subscriber Management Feature Pack for MX104 series	MX104	S-MX104-SA-FP

Table 24: Junos OS Feature License Model Number for MX Series Routers (continued)

Licensed Software Feature	Supported Devices	Model Number
Subscriber Service Management Feature Packet License—RADIUS and SRC-based service activation and deactivation per-service accounting features	MX80	S-MX80-SSM-FP
Subscriber Service Management Feature Packet License	MX104	S-MX104-SSM-FP
Upgrade to Traffic Direct Advanced (per MS-DPC)	MX960	S-MX-TD-UPG
License to run one instance of the NAT software on one NPU per MS-DPC	MX240, MX480, and MX960	S-NAT
License to support inline NAT software on MX5, MX10, MX40, MX80, MX104	MX5, MX10, MX40, MX80, and MX104	S-NAT-IN-MX5-104 (Replaces S-NAT-IN-MX40-MX80 and S-NAT-IN-MX5-MX10)
License to run one instance of the NAT software on one NPU per MS-MIC, MS-DPC, or MS-MPC	MX80, MX104, MX240, MA480, MX960, MX2010, and MX2020	S-NAT-NPU (Replaces S-NAT-IN-MX40-MX80-UPG)
License to run NAT using any MPC in an MX Chassis	MX240, MX480, and MX960	S-NAT-IN-MX-CHASSIS
Subscriber Access Feature Pack License Scaling (4000)	MX240, MX480, MX960, M120, M320, and MX80	S-SA-4K
Subscriber Access Feature Pack License Scaling (8000)	MX240, MX480, MX960, M120, M320, and MX80	S-SA-8K
Subscriber Access Feature Pack License Scaling (16,000)	MX240, MX480, MX960, and MX80	S-SA-16K
Subscriber Access Feature Pack License Scaling (32,000)	MX240, MX480, MX960, M120, and M320	S-SA-32K
Subscriber Access Feature Pack License Scaling (64,000)	MX240, MX480, MX960, M120, and M320	S-SA-64K
Subscriber Access Feature Pack License Scaling (96,000)	MX240, MX480, MX960, M120, and M320	S-SA-96K
Subscriber Access Feature Pack License Scaling (128,000)	MX240, MX480, MX960, M120, and M320	S-SA-128K
Subscriber Access Feature Pack License Scaling (256,000)	MX240, MX480, and MX960	S-SA-256K

Table 24: Junos OS Feature License Model Number for MX Series Routers (continued)

Licensed Software Feature	Supported Devices	Model Number
Subscriber Access Feature Pack License	MX240, MX480, MX960, M120, and M320	S-SA-FP
Software License for Secure Flow Mirroring Service (FlowTap) (does not require MS-DPC)	MX80, MX104, MX240, MX480, and MX960	S-SFM-FLOWTAP-IN
License to run one instance of the SFW and software on a MS-DPC	MX960, MX480, and MX240	S-SFW
Subscriber Service Management Feature Packet License—RADIUS and SRC-based service activation and deactivation per-service accounting features	MX240, MX480, MX960, M120, and M320	S-SSM-FP
Software license for one member of an MX Virtual Chassis	MX960, MX480, and MX240	S-VCR
Upgrade license—from MX10 to equivalent of MX40; allows additional 2x10G fixed ports to be used on the MX10 router	MX10-T	MX10-40-UPG
Upgrade license—from MX10 to equivalent of MX80; allows additional 4x10G fixed ports to be used on the MX10 router	MX10-T	MX10-80-UPG
Upgrade license—from MX40 to equivalent of MX80; allows additional 2x10G fixed ports to be used on the MX40 router	MX40-T	MX40-80-UPG
Upgrade license—from MX5 to equivalent of MX10; allows second MIC slot to be used on the MX5 router	MX5-T	MX5-10-UPG
Upgrade license—from MX5 to equivalent of MX40; allows second MIC slot and 2x10G fixed ports to be used on the MX5 router	MX5-T	MX5-40-UPG
Upgrade license—from MX5 to equivalent of MX80. Allows second MIC slot and 4x10G fixed ports to be used on the MX5 router	MX5-T	MX5-80-UPG
Upgrade license—Subscriber Access Feature Pack scaling license upgrade from 4000 through 8000 subscribers	MX80, MX960, MX480, and MX240	S-SA-UP-8K

Table 24: Junos OS Feature License Model Number for MX Series Routers (continued)

Licensed Software Feature	Supported Devices	Model Number
Upgrade license—Subscriber Access Feature Pack scaling license upgrade from 8000 through 16,000 subscribers	MX80, MX960, MX480, and MX240	S-SA-UP-16K
Upgrade license—Subscriber Access Feature Pack scaling license upgrade from 16,000 through 32,000 subscribers	MX240, MX480, and MX960	S-SA-UP-32K
Upgrade license—Subscriber Access Feature Pack scaling license upgrade from 32,000 through 64,000 subscribers	MX240, MX480, and MX960	S-SA-UP-64K
Upgrade license—Subscriber Access Feature Pack scaling license upgrade from 64,000 through 96,000 subscribers	MX240, MX480, and MX960	S-SA-UP-96K
Upgrade license—Subscriber Access Feature Pack scaling license upgrade from 96,000 through 128,000 subscribers	MX240, MX480, and MX960	S-SA-UP-128K
Upgrade license—Subscriber Access Feature Pack scaling license upgrade from 128,000 through 256,000 subscribers	MX240, MX480, and MX960	S-SA-UP-256K
License to use MX as Controller or Aggregation device for Junos Fusion. One license per MX is needed.	MX Series router	S-MX-AD-FUSION-LIC
License to run any supported EX4300 model as a satellite device in Junos Fusion mode. One license per EX4300 is needed	EX4300	S-MX-SAT-EX4300
License to run any supported QFX5100 model as a satellite device in Junos Fusion mode. One license per QFX5100 is needed	QFX5100	S-MX-SAT-QFX5100

See Also

- Junos OS Feature License Keys on page 136
- License Enforcement on page 16
- Configuring the JET Application and its License on a Device Running Junos OS on page 147

License Modes for PTX Series Routers

PTX Series routers are available in two license variants: IR and R. Depending on the license purchased, the router offers full IP or LSR.

NOTE: The license-mode statement is only supported on the PTX3000 and PTX5000 Series routers with third-generation FPCs.

Table 25 on page 127 describes the two license variants for the PTX3000 and PTX5000.

Table 25: License Variants for the PTX3000 and PTX5000 FPCs

License	Description	Scale Restrictions
IR	Scaled up LSR and peering	• Up to 2 million routes in the forwarding information base (FIB) • Up to 6 million routes in the routing information base (RIB) • Up to 256 routing instances of the virtual routing and forwarding (VRF) instance type • Up to 128 thousand LSPs
R	Full IP core	None

Table 26 on page 127 describes the two license variants for the PTX1000.

Table 26: License Variants for the PTX1000

License	Description	Scale Restictions
IR	Scaled up LSR and peering	• Up to 1 million routes in the forwarding information base (FIB) • Up to 6 million routes in the routing information base (RIB) • Up to 256 routing instances of the virtual routing and forwarding (VRF) instance type • Up to 128 thousand LSPs
R	Full IP core	None

For the PTX3000 and PTX5000, If you purchase two FPCs: one with an IR license and one with an R license. After the FPCs are installed on a router, both FPCs appear identical. To distinguish between an FPC with an IR license and an FPC with an R license after the FPC is installed on the router, you must configure the license mode based on the license purchased. For instance, if you purchased an FPC with the IR license, you must configure the license mode for that FPC as IR. The license mode settings are set specific to each FPC slot. If the FPC is installed in a different slot, or moved to another device, the license mode settings must be reconfigured on the new slot or device. Also, the license mode settings previously configured must be deleted.

NOTE: The license mode settings are used only to provide information. You cannot set or alter the license of the FPC by configuring the license mode.

To view the current license mode settings, from the configuration mode, use the **show chassis fpc** command. To view the current license mode settings, from the operational mode, use the **show chassis hardware extensive** command. To delete the existing license mode settings, use the **delete chassis fpc** command.

See Also

- Junos OS Feature License Keys on page 136
- License Enforcement on page 16
- Configuring the JET Application and its License on a Device Running Junos OS on page 147

License Modes for Enhanced MPCs Overview

Enhanced MPCs are available in three license variants. Before Junos OS Release 16.1, there were two variants: infrastructure routing (IR) and routing (R). Starting in Junos OS Release 16.1, there is also a base variant, making a total of three licence variants. All variants support an identical feature set, but with a few scale differences.Table 27 on page 129 describes the three license variants.

Table 27: License Variants for MPCs

License	How to Identify	Description
base	No special suffix in the license name.	• All Layer 2, Layer 2.5, and Layer 3 features. • Up to 32 Layer 3 routing instances of the virtual routing and forwarding (VRF) instance. The VRF support includes Layer 3 VPN (L3VPN). • Up to 2 million routes in the forwarding information base (FIB), provided there is hardware support. (FIB is also known as forwarding table.) • Up to 6 million routes in the routing information base (RIB), also known as routing table.
IR	-IR suffix in the license name.	• All Layer 2, Layer 2.5, and Layer 3 features. • Up to 32 Layer 3 routing instances of the virtual routing and forwarding (VRF) instance. The VRF support includes Layer 3 VPN (L3VPN).
R	-R suffix in the license name.	Full-scale Layer 2, Layer 2.5, and Layer 3 features. Scale is determined by the hardware capabilities.

Suppose you have purchased two MPC4Es: one with IR license and one with R license. After the MPCs are installed on a router, both MPCs appear identical. To distinguish between an MPC with an IR license and an MPC with an R license after the MPC is installed on the router, you must configure the license mode based on the license purchased. For instance, if you have purchased an MPC with the IR license, you must configure the license mode for that MPC as IR. The license mode settings are set specific to each MPC slot. If the MPC is installed in a different slot, or moved to another device, the license mode settings must be reconfigured on the new slot or device. Also, the license mode settings previously configured must be deleted.

NOTE: **The license mode settings are used only to provide information. You cannot set or alter the license of the MPC by configuring the license mode.**

To view the current license mode settings on an MPC, from the configuration mode, use the **show chassis fpc** command. To view the current license mode settings on an MPC, from the operational mode, use the **show chassis hardware extensive** command. To delete the existing license mode settings on an MPC, use the **delete chassis fpc** command.

See Also
- Junos OS Feature License Keys on page 136

- License Enforcement on page 16
- Configuring the JET Application and its License on a Device Running Junos OS on page 147

Configuring the License Mode for Specific Enhanced MPCs on MX Series Routers

Starting with Junos OS Release 14.2, you can set the license mode for enhanced MPCs such as MPC4E, MPC5E, and MPC6. Configuring the license mode enables you to distinguish between an MPC with an IR license and an MPC with an R license after the MPC is installed on the router. An MPC with an R license supports all the Layer 2, Layer 2.5, and Layer 3 features. An MPC with an IR license offers partial support for these features. For more information about the license variants, see "License Modes for Enhanced MPCs Overview" on page 129

NOTE: **The license mode settings are used only to provide information. You cannot set or alter the license of the MPC when you configure the license mode.**

Before you configure the license mode of the MPC, verify the license of the MPC. You will need this information do configure the license mode.

Do not try to set the license mode while the card is rebooting or the following error message will appear: **Card not online or TRIO/DPC based.**

To configure the license mode for MPCs on MX Series routers:

1. Configure the license mode for the MPC in a specified MPC slot.

   If the MPC has an IR license, configure the license mode as IR. If the MPC has an R license, configure the license mode of the MPC as R.

   ```
   [edit]
   user@host# set chassis fpc slot-number ir-mode ir-mode
   ```

2. In configuration mode, verify the configuration, for example:

   ```
   [edit]
   user@host# show chassis
   fpc 1 {
     ir-mode IR;
   }
   ```

3. After verifying the license mode, commit the changes by using the **commit** statement.

   ```
   [edit]
   user@host# commit
   ```

See Also

- Junos OS Feature License Keys on page 136
- License Enforcement on page 16
- Configuring the JET Application and its License on a Device Running Junos OS on page 147

Example: Configuring the License Mode for MPC5E

This example describes how to configure the license mode for MPC5E on the MX480 router. It also describes how to remove the license mode settings and reconfigure the license mode settings on a new slot.

Requirements

This example uses the following hardware and software components:

- Junos OS Release 14.2 or later for MX Series routers
- A single MX480 router with MPC5E with R license

Overview

Configuring the license mode for an MPC enables you to distinguish between an MPC with an IR license and an MPC with an R license after the MPC is installed on the router.

NOTE: **The license mode settings are used only to provide information. You cannot set or alter the license of the MPC when you configure the license mode.**

The license mode settings are set specific to each MPC slot. If the MPC is installed in a different slot, or moved to another device, the license mode settings must be reconfigured on the new slot or device. Also, the license mode settings configured previously must be removed. You can view the license mode settings from both configuration mode and operational mode.

Topology

In this example, an MPC5E is installed in slot 4 of an MX480 router and has an R license. The R license indicates that all Layer 2, Layer 2.5, and Layer 3 features are supported on the MPC. You first configure the license mode of the MPC5E in slot 4 to R. After configuring the license mode, you can verify the license mode settings. You then install the MPC5E in slot 2 of the same router. License mode settings are set specific to each MPC slot. Therefore, the license mode setting must be reconfigured. After you move the MPC5E,

delete the license mode setting on slot 4 and then reconfigure the license mode setting on slot 2.

Configuration

To configure the license mode for the MPC5E according to the topology specified in the overview section, perform these tasks:

- Configuring the License Mode for MPC5E in Slot 4 on page 132
- Deleting the License Mode for MPC5E in Slot 4 on page 132
- Configuring the License Mode for MPC5E in Slot 2 on page 133

Configuring the License Mode for MPC5E in Slot 4

Step-by-Step Procedure

To configure the license mode for the MPC5E in slot 4:

1. Configure the license mode R for the MPC5E in slot 4:

```
[edit]
user@host# set chassis fpc 4 ir-mode R
```

2. In configuration mode, verify the configuration.

```
user@host# show chassis fpc 4
pic 0 {
    power off;
}
pic 1 {
    power off;
}
ir-mode R;
```

3. After verifying the license mode, commit the changes by using the **commit** statement.

```
[edit]
user@host# commit
```

Deleting the License Mode for MPC5E in Slot 4

Step-by-Step Procedure

To delete the license mode R for the MPC5E in slot 4:

1. Delete the license mode for the MPC5E.

```
[edit]
user@host# delete chassis fpc 4 ir-mode R
```

2. In configuration mode, verify the configuration.

```
user@host# show chassis fpc 4
```

```
pic 0 {
   power off;
}
pic 1 {
   power off;
}
```

3. After verifying the license mode, commit the changes by using the **commit** statement.

```
[edit]
user@host# commit
```

Configuring the License Mode for MPC5E in Slot 2

Step-by-Step Procedure

To configure the license mode for the MPC5E in slot 2:

1. Configure the license mode R for the MPC5E.

```
[edit]
user@host# set chassis fpc 2 ir-mode R
```

2. In configuration mode, verify the configuration.

```
user@host# show chassis fpc 2
pic 0 {
   power off;
}
pic 1{
   power off;
}
ir-mode R;
```

3. After verifying the license mode, commit the changes by using the **commit** statement.

```
[edit]
user@host# commit
```

Verification

To confirm that you have accurately configured the license mode settings on MPC5E, perform these tasks:

- Verifying That License Mode Is Configured for MPC5E in Slot 4 on page 134
- Verifying That the Configured License Mode Is Deleted on page 134
- Verifying That the License Mode Is Configured for MPC5E in Slot 2 on page 135

Verifying That License Mode Is Configured for MPC5E in Slot 4

Purpose To verify that license mode R is configured for the MPC5E in slot 4.

Action From operational mode, enter the **show chassis hardware extensive** command.

```
user@host> show chassis hardware extensive
...
FPC 4            REV 30   750-045715   CABM2612          MPC5E 3D Q 24XGE+6XLGE
 Jedec Code:   0x7fb0            EEPROM Version:    0x02
 P/N:          750-045715        S/N:               CABM2612
 Assembly ID:  0x0b8a            Assembly Version:  01.30
 Date:         08-27-2013        Assembly Flags:    0x00
 Version:      REV 30            CLEI Code:         PROTOXCLEI
 ID: MPC5E 3D Q 24XGE+6XLGE      FRU Model Number:  PROTO-ASSEMBLY
 Board Information Record:
  Address 0x00: ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff
 I2C Hex Data:
  Address 0x00: 7f b0 02 fe 0b 8a 01 1e 52 45 56 20 33 30 00 00
  Address 0x10: 00 00 00 00 37 35 30 2d 30 34 35 37 31 35 00 00
  Address 0x20: 53 2f 4e 20 43 41 42 4d 32 36 31 32 00 1b 08 07
  Address 0x30: dd ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff
  Address 0x40: ff ff ff ff 01 50 52 4f 54 4f 58 43 4c 45 49 50
  Address 0x50: 52 4f 54 4f 2d 41 53 53 45 4d 42 4c 59 00 00 00
  Address 0x60: 00 00 00 00 00 00 41 30 30 ff ff ff ff ff ff ff
  Address 0x70: ff ff ff c2 ff ff ff ff ff ff ff ff ff ff ff ff
 R/IR Mode: R
...
```

Meaning License mode **R** is configured for the MPC5E in slot **4**.

Verifying That the Configured License Mode Is Deleted

Purpose To verify that the configured license mode is deleted.

Action From operational mode, enter the **show chassis hardware extensive** command.

```
user@host> show chassis hardware extensive
...
FPC 4            REV 30   750-045715   CABM2612          MPC5E 3D Q 24XGE+6XLGE
 Jedec Code:   0x7fb0            EEPROM Version:    0x02
 P/N:          750-045715        S/N:               CABM2612
 Assembly ID:  0x0b8a            Assembly Version:  01.30
 Date:         08-27-2013        Assembly Flags:    0x00
 Version:      REV 30            CLEI Code:         PROTOXCLEI
 ID: MPC5E 3D Q 24XGE+6XLGE      FRU Model Number:  PROTO-ASSEMBLY
 Board Information Record:
  Address 0x00: ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff
 I2C Hex Data:
  Address 0x00: 7f b0 02 fe 0b 8a 01 1e 52 45 56 20 33 30 00 00
  Address 0x10: 00 00 00 00 37 35 30 2d 30 34 35 37 31 35 00 00
  Address 0x20: 53 2f 4e 20 43 41 42 4d 32 36 31 32 00 1b 08 07
```

```
 Address 0x30: dd ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff
 Address 0x40: ff ff ff ff 01 50 52 4f 54 4f 58 43 4c 45 49 50
 Address 0x50: 52 4f 54 4f 2d 41 53 53 45 4d 42 4c 59 00 00 00
 Address 0x60: 00 00 00 00 00 00 41 30 30 ff ff ff ff ff ff ff
 Address 0x70: ff ff ff c2 ff ff ff ff ff ff ff ff ff ff ff ff
...
```

Meaning The license mode setting has been removed for the MPC5E in slot **4**.

Verifying That the License Mode Is Configured for MPC5E in Slot 2

Purpose To verify that license mode R is configured for the MPC5E in slot 2.

Action From operational mode, enter the **show chassis hardware extensive** command.

```
user@host> show chassis hardware extensive
...
FPC 2            REV 30   750-045715   CABM2612          MPC5E 3D Q 24XGE+6XLGE
 Jedec Code:   0x7fb0            EEPROM Version:    0x02
 P/N:          750-045715        S/N:               CABM2612
 Assembly ID:  0x0b8a            Assembly Version:  01.30
 Date:         08-31-2013        Assembly Flags:    0x00
 Version:      REV 30            CLEI Code:         PROTOXCLEI
 ID: MPC5E 3D Q 24XGE+6XLGE      FRU Model Number:  PROTO-ASSEMBLY
 Board Information Record:
  Address 0x00: ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff
 I2C Hex Data:
  Address 0x00: 7f b0 02 fe 0b 8a 01 1e 52 45 56 20 33 30 00 00
  Address 0x10: 00 00 00 00 37 35 30 2d 30 34 35 37 31 35 00 00
  Address 0x20: 53 2f 4e 20 43 41 42 4d 32 36 31 32 00 1b 08 07
  Address 0x30: dd ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff
  Address 0x40: ff ff ff ff 01 50 52 4f 54 4f 58 43 4c 45 49 50
  Address 0x50: 52 4f 54 4f 2d 41 53 53 45 4d 42 4c 59 00 00 00
  Address 0x60: 00 00 00 00 00 00 41 30 30 ff ff ff ff ff ff ff
  Address 0x70: ff ff ff c2 ff ff ff ff ff ff ff ff ff ff ff ff
 R/IR Mode: R
...
```

Meaning License mode **R** is configured for the MPC5E in slot **2**.

See Also

- Junos OS Feature License Keys on page 136
- License Enforcement on page 16
- Configuring the JET Application and its License on a Device Running Junos OS on page 147

Junos OS Feature License Keys

Some Junos OS software features require a license to be activated. To enable each licensed feature, you must purchase, install, manage, and verify a license key that corresponds to the licensed feature.

Release-Tied License Keys and Upgrade Licenses on MX Series Routers

The Junos OS licensing infrastructure currently associates a license feature with attributes such as date, platform, and validity. In addition to these attributes, for MX Series routers running Junos OS Release 12.2 and later, a licensed feature can be associated with a release number at the time of generating the license key. This type of release-tied license key is used to validate a particular licensed feature while attempting a software upgrade. The upgrade process aborts if the release number in the license key is earlier than the Junos OS release number to which the system is being upgraded.

Additionally, an upgrade license key can be generated for a release-tied licensed feature. An upgrade license key is used for carrying forward a capacity license to the upgrade release. Although an upgrade license might be an acceptable license on the current release, it does not add to the existing capacity limit. The capacity added in the upgrade license key is valid for the upgrade software release only.

The release number embedded in the license key indicates the maximum release number up to which Junos OS can be upgraded.

As an example, assume that your system is running Junos OS Release 12.2 and is using the **scale-subscriber** licensed feature with a later release-tied upgrade license key installed. If you request a software upgrade to the later release of Junos OS, the software upgrade operation fails and the following error message is displayed:

```
mgd: error: No valid upgrade license found for feature 'scale-subscriber'.
Aborting Software upgrade.
Validation failed
```

In this example, to successfully upgrade to the later release of Junos OS, the release number included in the upgrade license key should be greater than or equal to the later release number. Also, you can perform software upgrades up to the previous release without any additional license keys to retain the existing scale limit.

NOTE:

When you install a release-tied license, the following apply:

- You can purchase an upgrade capacity license only if a base capacity license for the same scale-tier has already been generated or purchased.
- You cannot install an upgrade license if the capacity does not match any of the existing base capacity licenses on the system.
- The license installation fails when you install a lower release number license key on a higher software release number.
- A release-tied license can be installed on a Junos OS release number that is lower than or equal to the release number included in the license key. For example, a 12.2 license key is valid on Junos OS Release 12.1.
- An upgrade license is valid only on the target release number specified in the license key, but can be installed on an earlier Junos OS release. For example, a 4 K scale-tier upgrade license for Junos OS Release 12.2 can be installed on an earlier release, and the installed count of licenses remains unaltered.
- Release-tied licenses of the previous release are not deleted on upgrading Junos OS to a newer release version.

Licensable Ports on MX5, MX10, and MX40 Routers

Starting with Junos OS Release 12.2, license keys are available to enhance the port capacity on MX5, MX10, and MX40 routers up to the port capacity of an MX80 router. The MX5, MX10, and MX40 routers are derived from the modular MX80 chassis with similar slot and port assignments, and provide all functionality available on an MX80 router, but at a lower capacity. Restricting port capacity is achieved by making a set of MIC slots and ports licensable. MICs without a license are locked, and are unlocked or made usable by installing appropriate upgrade licenses.

The base capacity of a router is identified by the Ideeprom assembly ID (I2C ID), which defines the board type. However, the Junos OS licensing infrastructure allows the use of restricted ports without a license for a grace period of 30 days. After the grace period expires, the router reverts back to the base capacity if no upgrade license is purchased and installed for the locked ports. The I2C ID along with an upgrade license determine the final capacity of an MX5, MX10, or MX40 router.

The MX5, MX10, MX40, and MX80 routers support the following types of MICs:

- A built-in 10-Gigabit Ethernet MIC with four 10-Gigabit Ethernet ports
- Two front-pluggable MICs

A feature ID is assigned to every license upgrade for enhancing port capacity. Table 28 on page 138 displays the chassis types and their associated port capacity, I2C ID, base capacity, feature ID, feature name, and the final capacity after a license upgrade.

Table 28: Upgrade Licenses for Enhancing Port Capacity

Chassis Type	Port Capacity	I2C ID	Base Capacity	Feature ID and Feature Name	Upgrade Capacity
MX5	20G	0x556	Slot 1 • 1/MIC0	f1—MX5 to MX10 upgrade	Slot 1 and 2 • 1/MIC0 • 1/MIC1
MX10	40G	0x555	Slot 1 and 2 • 1/MIC0 • 1/MIC1	f2—MX10 to MX40 upgrade	Slot 2 and first 2 ports on Slot 0 • 1/MIC1 • First 2 ports on 0/MIC0
MX40	60G	0x554	Slot 1, SLot 2 and first 2 ports on Slot 0 • 1/MIC0 • 1/MIC1 • First 2 ports on 0/MIC0	f3—MX40 to MX80 upgrade	Slot 2 and all ports on Slot 0 • 1/MIC1 • All 4 ports on 0/MIC0

When installing an upgrade license for enhancing port capacity on MX5, MX10 and MX40 routers, consider the following:

- To upgrade an MX5 router to MX80 router capacity, licenses for all three features (f1, f2, f3) must be installed. All three features can be provided in a single license key.
- To upgrade an MX10 router to MX40 router capacity, installing a license key with f2 feature is sufficient.
- Non-applicable feature IDs in a license key reject the upgrade license. For example:
  - An f1 feature ID on an MX10 upgrade license key rejects the license.
  - Feature IDs f1 and f2 on an MX40 upgrade license key reject the entire license.

Port Activation on MX104 Routers

Starting with Junos OS Release 13.3, license keys are available to activate the ports on the MX104 router. MX104 routers have four built-in ports. By default, in the absence of valid licenses, all four built-in ports are deactivated. By installing licenses, you can activate any two of the four or all of the four built-in ports. For instance, you can install a license to activate the first two built-in ports (xe-2/0/0 and xe-2/0/1) or you can install a license to activate the next two built-in ports (xe-2/0/2 and xe-2/0/3). You can also install a license to activate all four built-in ports (xe-2/0/0, xe-2/0/1, xe-2/0/2, and xe-2/0/3). If you have already activated two of the built-in ports, you can install an additional license to activate the other two built-in ports on the MX104 router.

A feature ID is assigned to every license for activating the built-in ports on the MX104 router. The port license model with the feature ID is described in Table 29 on page 139.

Table 29: Port Activation License Model for MX104 Routers

Feature ID	Feature Name	Functionality
F1	MX104 2X10G Port Activate (0 and 1)	Ability to activate first two built-in ports (xe-2/0/0 and xe-2/0/1)
F2	MX104 2X10G Port Activate (2 and 3)	Ability to activate next two built-in ports (xe-2/0/2 and xe-2/0/3)

Both the features are also provided in a single license key for ease of use. To activate all four ports, you must either install the licenses for both the features listed in Table 29 on page 139 or the single license key for both features. If you install the single license key when feature IDs F1 and F2 are already installed, the license does not get rejected. Also, MX104 routers do not support the graceful license expiry policy. A graceful license expiry policy allows the use of a feature for a certain period of time (usually a grace period of 30 days), and reverts if the license for that feature is not installed after the grace period.

See Also

- License Enforcement on page 16
- Software Feature Licenses on page 18
- Verifying Junos OS License Installation (CLI) on page 41
- **show system license on page 44**

License Server Management for Throughput Data Export on MX Series Routers for NAT, Firewall, and Inline Flow Monitoring Services

To support our transition to software defined networking (SDN), Juniper Networks supports the Software Business Model Transformation, which includes new licensing, pricing, and branding strategies that make it easier for users to extract value from Juniper software solutions. This value of this approach is known as the Juniper Software Advantage (JSA), which provides the following benefits:

- Simple—Simple to buy, use, and manage rights
- Repeatable—License models which facilitates repeatable use among multiple hardware platforms and usage scenarios.
- Measurable—License fees based on easy to measure usage

Although the licensing of JSA products is trust-based, Juniper Networks might periodically audit the usage of its products. License Measurement Tool (LMT) is a technique that is used to compute the usage of individual Network Edge Products under JSA. MX Series routers need to define the mechanism for updating the LMT tool with information such as per-service throughput. For example, for services such as carrier-grade NAT and inline flow monitoring, the router needs to calculate per service throughput and update it in LMT.

On MX Series routers, the Routing Engine periodically sends query messages to every Service PIC on which the service, for which throughput collection is being performed, is configured to run. This polling is performed for all the services for which throughput measurement is enabled. Service PICs, upon receiving the query for a particular service, reply with the throughput measured during the last query interval, for that service. If a service PIC hosts multiple services, the Routing Engine sends separate throughput queries to that service PIC for all the services. If a service is configured on multiple services PICs, the Routing Engine aggregates the throughput values received from all of them and exports the aggregated throughput to the log collector in the predefined log format. The LMT application analyze these values from log collector, performs aggregation on values collected from all routers, and displays them in the LMT application.

You can configure the capability to transmit the throughput details per service for the Junos Address Aware (carrier-grade NAT) and Junos Traffic Vision (previously known as Jflow) in the last time interval to an external log collector. The default time interval at which the throughput data is sent is 300 seconds, which you can configure to suit your network needs. Multiple instances of the same service running on different PICs within a router are supported. If the same service is running on different PICs within a router, the router transmits the consolidated final throughput to the log collector or server. This functionality is supported on MX Series routers with MS-MCPs and MS-MICs, and also in the MX Series Virtual Chassis configuration. To configure the license server properties for throughput data to be transmitted for the defined services, such as NAT or stateful firewall, from the service PIC on the router to the external log collector, include the license-server statement at the [edit] hierarchy level. To specify the IP address of the license log server, include the **ip-address *address*** statement at the **[edit license-server]** hierarchy level. To configure the frequency of transmission of throughput date, include the **log-interval *seconds*** statement at the [edit license-server] hierarchy level. To specify

the services for which throughput data collection must be performed, include the **services (jflow | cgnat | firewall)** statement at the **[edit license-server]** hierarchy level.

Throughput Measurement and Export

Throughput is defined as: "The network traffic throughput processed by juniper software in a second. It is represented as Mb/Sec (Megabits per second) or GB/sec (Gigabits per second). Throughput is measured as the 95th percentile of all the peaks measured in a quarter." Service PICs keep track of the amount of data (in bits) processed by the various service plugins running on them. When a throughput query arrives from the Routing Engine, for a particular service, the Service PIC returns the value D/T mbps, in its reply, where:

- D is the amount of data (megabits) processed by that service since the previous query was received. If the query interval happens to be 300 seconds, for example, then D refers to the amount of data that was processed during the last 300 second interval. If the current query happens to be the very first query, for a particular service, then D represents the cumulative data bits processed so far, by that service.
- T is the time (seconds) that elapsed since the previous query was received. This is the query interval configured using the CLI interface. If the current query happens to be the very first query, for a particular service, then T represents the time that elapsed since that service started processing packets. For all subsequent queries, T equals the query interval.

The Routing Engine aggregates the throughput measured (in mbps) across all the Service PICs on which a particular Service is configured and exports it to the Log collector which performs the 95th percentile calculation.

See Also

- License Enforcement on page 16
- Software Feature Licenses on page 18
- Verifying Junos OS License Installation (CLI) on page 41
- **show system license on page 44**

Junos Node Slicing Overview

Junos Node Slicing enables service providers and large enterprises to create a network infrastructure that consolidates multiple routing functions into a single physical device. It helps leverage the benefits of virtualization without compromising on performance. In particular, Junos Node Slicing enables the convergence of multiple services on a single physical infrastructure while avoiding the operational complexity involved. It provides operational, functional, and administrative separation of functions on a single physical infrastructure that enables the network to implement the same virtualization principles the compute industry has been using for years.

Using Junos Node Slicing, you can create multiple partitions in a single physical MX Series router. These partitions are referred to as guest network functions (GNFs). Each GNF behaves as an independent router, with its own dedicated control plane, data plane, and management plane. This enables you to run multiple services on a single converged MX

Series router, while still maintaining operational isolation between them. You can leverage the same physical device to create parallel partitions that do not share the control plane or the forwarding plane, but only share the same chassis, space, and power.

You can also send traffic between GNFs through the switch fabric by using an Abstracted Fabric (AF) interface, a pseudo interface that behaves as a first class Ethernet interface. An AF interface facilitates routing control, data, and management traffic between GNFs.

Junos Node Slicing supports multi-version software compatibility, thereby allowing the GNFs to be independently upgraded.

Benefits of Junos Node Slicing

- **Converged network**—With Junos Node Slicing, service providers can consolidate multiple network services, such as video edge and voice edge, into a single physical router, while still maintaining operational separation between them. You can achieve both horizontal and vertical convergence. Horizontal convergence consolidates router functions of the same layer to a single router, while vertical convergence collapses router functions of different layers into a single router.
- **Improved scalability**—Focusing on virtual routing partitions, instead of physical devices, improves the programmability and scalability of the network, enabling service providers and enterprises to respond to infrastructure requirements without having to buy additional hardware.
- **Easy risk management**—Though multiple network functions converge on a single chassis, all the functions run independently, benefiting from operational, functional, and administrative separation. Partitioning a physical system, such as Broadband Network Gateway (BNG), into multiple independent logical instances ensures that failures are isolated. The partitions do not share the control plane or the forwarding plane, but only share the same chassis, space, and power. This means failure in one partition does not cause any widespread service outage.
- **Reduced network costs**—Junos Node Slicing enables interconnection of GNFs through internal switching fabrics, which leverages Abstracted Fabric (AF) interface, a pseudo interface that represents a first class Ethernet interface behavior. With AF interface in place, companies no longer need to depend on physical interfaces to connect GNFs, resulting in significant savings.
- **Reduced time-to-market for new services and capabilities**—Each GNF can operate on a different Junos software version. This advantage enables companies to evolve each GNF at its own pace. If a new service or a feature needs to be deployed on a certain GNF, and it requires a new software release, only the GNF involved requires an update. Additionally, with the increased agility, Junos Node Slicing enables service providers and enterprises to introduce highly flexible Everything-as-a-service business model to rapidly respond to ever-changing market conditions.

See Also

- License Enforcement on page 16
- Software Feature Licenses on page 18
- Verifying Junos OS License Installation (CLI) on page 41

- show system license on page 44

Subscriber Access Licensing Overview

To enable some Juniper Networks Junos OS features or router scaling levels, you might have to purchase, install, and manage separate software license packs. The presence on the router of the appropriate software license keys (passwords) determines whether you can configure and use certain features or configure a feature to a predetermined scale.

NOTE: For the latest information about subscriber access licensing, contact your Juniper Networks sales representative at https://www.juniper.net/in/en/contact-us/.

See Also

- Configuring the Router to Strictly Enforce the Subscriber Scaling License on page 149
- Software Features That Require Licenses on MX Series Routers Only on page 23
- Software Feature Licenses on page 18

Address-Assignment Pools Licensing Requirements

The address-assignment pool feature is part of the Junos OS Subscriber Management Feature Pack license. You must install and properly configure the license to meet the requirements for using the address-assignment pool feature.

License Configuration

- Guidelines for Configuring an MX Series Router to Transmit Per-Service Throughput to an External Log Collector on page 143
- Installing Junos OS Licenses on Virtual Chassis Member Routers on page 144
- Configuring the JET Application and its License on a Device Running Junos OS on page 147
- Configuring the Router to Strictly Enforce the Subscriber Scaling License on page 149

Guidelines for Configuring an MX Series Router to Transmit Per-Service Throughput to an External Log Collector

Observe the following guidelines while configuring this functionality on MX Series routers with MS-MPCs and MS-MICs:

- If the syslog server is unreachable, the router cannot send information to the log collector.
- After a graceful Routing Engine switchover (GRES) procedure, the newly functioning active Routing Engine starts sending the data to the server after the configured time interval, which is similar to a reset operation. The time elapsed in the active interval and data before GRES are not preserved.

- The time range must be from 60 through 86400 seconds (24 hours).
- If the timer is not configured, the default value of 300 seconds is assumed.
- The throughput data can be sent only if a service is up and running.
- Only maximum throughput is transmitted for the last 300 seconds or the configured time interval.
- The throughput value must not be less than zero to enable transmission. The data is sent based on the timezone of the router.
- An acknowledgment mechanism for data sent to the log collector is not supported. The router does not receive any acknowledgement regarding whether the data is already written into the log collector.
- The router does not maintain throughput data beyond the configurable time interval.
- No mechanisms exist to track if the log collector is successfully receiving the sent data or if the log server is reachable.
- The time interval and log collector are common for all the services; you cannot configure a different period for collection of logs for each service or a different log collector for each service.
- You cannot clear the system throughput value using a CLI command. It is assumed that the throughput value is not cleared or changed from outside. Throughput must be calculated internally by services and must not be manually modified by a CLI.
- SNMP support for these values is not available.
- The log collector performs a 95 percentile calculation of throughput data. Syslogs are sent even in scaled system conditions to the log collector for the throughput data related to the configured services.
- The following is the format of the syslogs configured to be sent at the prescribed frequency:

```
<Date> <Time> < time-zone> <Router_name> <Service_name> <Throughput_value>
Throughput = <Unit_Mbps/Gbps> in last <Time_Interval>
```

An example is as follows:

```
Jan  8 08:49:57  America/Adak deuterium  CGNAT Throughput = 1500000 Mbps in
last 300Sec
```

Installing Junos OS Licenses on Virtual Chassis Member Routers

To enable some Junos OS features or router scaling levels, you might have to purchase, install, and manage separate software license packs. The presence on the router of the appropriate software license keys (passwords) determines whether you can configure and use certain features or configure a feature to a predetermined scale.

Before you configure an MX Series Virtual Chassis, install the following Junos OS software licenses on each MX Series router to be configured as a member of the Virtual Chassis:

- MX Virtual Chassis Redundancy Feature Pack—You must purchase and install a unique MX Virtual Chassis Redundancy Feature Pack for each member router in the Virtual Chassis. If you issue the **request virtual-chassis member-id set**, **request virtual-chassis member-id delete**, **request virtual-chassis vc-port set**, or **request virtual-chassis vc-port delete** command to set or delete member IDs or Virtual Chassis ports without first installing an MX Virtual Chassis Redundancy Feature Pack on both member routers, the software displays a warning message that you are operating without a valid Virtual Chassis software license.
- Junos OS feature licenses—Purchase and install the appropriate Junos OS feature licenses to enable use of a particular software feature or scaling level in your network. You must install the required feature licenses on each member router in the Virtual Chassis.

Sometimes, if a Virtual Chassis member is newly installed, the licenses are lost, creating a situation in which any new license installed in master Routing Engine will get synced across all members, but any previously installed license (any license installed before the newly installed member) does not get synced. In this case, you must reinstall (delete and add) licenses in the master Routing Engine if a Virtual Chassis member is replaced. This procedure will sync all installed licenses to all members.

This topic covers the following procedures:

- Installing Junos OS Licenses on Members on page 145
- Reinstalling Junos OS Licenses on New Members on page 146

Installing Junos OS Licenses on Members

Before you begin:

- Prepare your site for the Virtual Chassis configuration.

  See *Preparing for a Virtual Chassis Configuration*.

- Familiarize yourself with the procedures for installing and managing Junos OS licenses.

  See *Software Installation and Upgrade Guide*.

To install Junos OS licenses on each member router in the Virtual Chassis:

1. Install the required licenses on the MX Series router to be designated as the protocol master for the Virtual Chassis.
   a. Install the MX Virtual Chassis Redundancy Feature Pack.
   b. Install the Junos OS feature licenses required for your software feature or scaling level.
2. Install the required licenses on the MX Series router to be designated as the protocol backup for the Virtual Chassis.
   a. Install the MX Virtual Chassis Redundancy Feature Pack.

b. Install the Junos OS feature licenses required for your software feature or scaling level.

3. (Optional) Verify the license installation on each member router.

   For example:

```
user@host> show system license
License usage:
                                Licenses     Licenses    Licenses    Expiry
  Feature name                       used    installed      needed
  subscriber-accounting                 0            1           0    permanent
  subscriber-authentication             0            1           0    permanent
  subscriber-address-assignment         0            1           0    permanent
  subscriber-vlan                       0            1           0    permanent
  subscriber-ip                         0            1           0    permanent
  scale-subscriber                      0       256000           0    permanent
  scale-l2tp                            0         1000           0    permanent
  scale-mobile-ip                       0         1000           0    permanent
  virtual-chassis                       0            1           0    permanent
```

Reinstalling Junos OS Licenses on New Members

When you need to install a new Virtual Chassis member router, use this procedure to ensure all installed licenses are synced to all members.

Before adding the new Routing Engine to the Virtual Chassis, install required operational packages. This is like the first procedure, Installing Junos OS Licenses on Members.

To sync Junos OS licenses from master to newly replaced virtual chassis members:

1. On the master router, exit the CLI to switch to user **root**.

```
{master:member0-re1}
```

```
user@host> start shell user root
{master:member0-re1}
Password:
```

2. Enter the root password and go back into the CLI.

```
root@host% cli
```

3. Copy the licenses from the master member to the Routing Engine that does not have licenses installed (that is, the newly installed Routing Engine).

```
{master:member0-re1}
```

```
user@host> file copy /config/license/*.lic member0-re0:/config/license/
{master:member0-re1}
user@host>
```

See Also

- License Enforcement on page 16
- License Modes for Enhanced MPCs Overview on page 129
- Configuring the License Mode for Specific Enhanced MPCs on MX Series Routers on page 130
- Software Features That Require Licenses on MX Series Routers Only on page 23

Configuring the JET Application and its License on a Device Running Junos OS

Before you can start a JET application on a device running Junos OS, first determine if you must configure the license. License configuration for JET applications is required only if you are deploying on-box applications written in C or C++ and built using the Juniper Extension Toolkit (JET) development environment. For simple Python JET applications, which do not require licensing, this task is not required.

This topic contains two examples of configuring JET applications to run on Junos OS:

- Configuring a Python Application to Run on a Device on page 147
- Configuring a C or C++ Application to Run on a Device on page 148

Configuring a Python Application to Run on a Device

To configure a JET Python application and its license on a device:

1. (Optional if Python application is signed) Issue the **set system scripts language python** command.

   ```
   [edit]
   user@device# set system scripts language python
   ```

   If you do not include the **language python** statement, you cannot execute unsigned Python scripts on the device.

   NOTE: Junos OS supports using symbolic links for files in the /var/db/scripts/jet directory, but the device will only execute the script at the target location if it is signed.

2. At the **[edit system extensions]** hierarchy level, configure the application's provider's ID, for example:

   ```
   [edit system extensions]
   user@device# set providers xyzcompany
   ```

   NOTE: The same provider license must be used to configure a JET application to run on Junos OS as was used to package it.

3. Configure the license type and deployment scope.

```
[edit system extensions]
user@device# set providers xyzcompany license-type juniper deployment-scope
  commercial
```

4. Commit the configuration.

```
[edit system extensions]
user@device# top
[edit]
user@device# commit
```

Configuring a C or C++ Application to Run on a Device

To configure a JET C or C++ application:

1. Configure the application's provider's ID, license type, and deployment scope.

   The following application example was packaged using **chef** as the provider license:

```
[edit]
user@device# set system extensions providers chef license-type juniper
  deployment-scope commercial
```

NOTE: The same provider license must be used to configure a JET application to run on Junos OS as was used to package it.

2. Commit the configuration and exit to operational mode.

```
[edit]
user@device# commit
commit complete
```

```
[edit]
user@device# exit
user@device>
```

See Also

- License Modes for Enhanced MPCs Overview on page 129
- Configuring the License Mode for Specific Enhanced MPCs on MX Series Routers on page 130
- Software Features That Require Licenses on MX Series Routers Only on page 23

Configuring the Router to Strictly Enforce the Subscriber Scaling License

You can configure the router to strictly enforce the subscriber scaling feature, which is part of the Junos Subscriber Access Feature Pack license. The subscriber scaling feature specifies the maximum number of subscribers that can be logged in at any one time.

When you configure strict scaling license support, the router performs the following actions:

- Strictly enforces the subscriber scaling license and does not allow any grace period. When the number of logged-in subscriber reaches the number allowed by the scaling license, no additional subscribers are allowed to log in.
- Creates the informational log message, "90 percent of installed subscriber scale licenses in use" in **/var/log/messages**, to inform you when you have 10 percent of the total allowed licenses remaining. The router clears this condition when license usage falls below 90 percent. The log message is created again if the 90 percent usage is later reached.

To configure the router to strictly enforce the subscriber scaling license:

1. Specify that you want to configure subscriber management.

```
[edit system services]
user@host# edit subscriber-management
```

2. Configure the router to enforce the scaling license.

```
[edit system services subscriber-management]
user@host# set enforce-strict-scale-limit-license
```

See Also

- Subscriber Access Licensing Overview on page 143
- Junos OS Feature Licenses on page 15
- Verifying Junos OS License Installation (CLI) on page 41

CHAPTER 4

Understanding and Managing Licenses for SRX Series

Understanding Licenses for SRX Series Devices

Software Feature Licenses for SRX Series Devices

For information about how to purchase a software license, contact your Juniper Networks sales representative at https://www.juniper.net/in/en/contact-us/. Platform support depends on the Junos OS release in your installation.

Each feature license is tied to exactly one software feature, and that license is valid for exactly one device.

NOTE: For the most up-to-date license models available, contact your Juniper account team.

See Also

- Understanding Chassis Cluster Licensing Requirements on page 152

- Verifying Licenses on an SRX Series Device in a Chassis Cluster on page 154
- Installing Licenses on the SRX Series Devices in a Chassis Cluster on page 152
- *Understanding Licenses for Logical Systems and Tenant Systems on SRX Series Devices*

Understanding Chassis Cluster Licensing Requirements

There is no separate license required for chassis cluster. However, some Junos OS software features require a license to activate the feature. To configure and use the licensed feature in a chassis cluster setup, you must purchase one license per feature per device and the license needs to be installed on both nodes of the chassis cluster. Both devices (which are going to form a chassis cluster) must have the valid, identical features licenses installed on them. If both devices do not have an identical set of licenses, then after a failover, a particular feature (that is, a feature that is not licensed on both devices) might not work or the configuration might not synchronize in chassis cluster formation. Licensing is usually ordered when the device is purchased, and this information is bound to the chassis serial number. For example, Intrusion Detection and Prevention (IDP) is a licensed feature and the license for this specific feature is tied to the serial number of the device. For information about how to purchase software licenses, contact your Juniper Networks sales representative at https://www.juniper.net/in/en/contact-us/.

For information about how to purchase software licenses, contact your Juniper Networks sales representative at https://www.juniper.net/in/en/contact-us/.

Installing Licenses on the SRX Series Devices in a Chassis Cluster

You can add a license key from a file or a URL, from a terminal, or from the J-Web user interface. Use the ***filename*** option to activate a perpetual license directly on the device. Use the ***url*** option to send a subscription-based license key entitlement (such as unified threat management [UTM]) to the Juniper Networks licensing server for authorization. If authorized, the server downloads the license to the device and activates it.

Before adding new licenses, complete the following tasks:

- Purchase the required licenses.
- Set the chassis cluster node ID and the cluster ID. See *Example: Setting the Node ID and Cluster ID for SRX Series Devices in a Chassis Cluster* .
- Ensure that your SRX Series device has a connection to the Internet (if particular feature requires Internet or if (automatic) renewal of license through internet is to be used). For instructions on establishing basic connectivity, see the Getting Started Guide or Quick Start Guide for your device.

To install licenses on the primary node of an SRX Series device in a chassis cluster:

1. Run the **show chassis cluster status** command and identify which node is primary for redundancy group 0 on your SRX Series device.

   {primary:node0}
   user@host> show chassis cluster status redundancy-group 0

   ```
   Cluster ID: 9
   Node                  Priority          Status    Preempt  Manual failover

   Redundancy group: 0 , Failover count: 1
       node0                   254         primary        no       no
       node1                   1           secondary      no       no
   ```

   Output to this command indicates that node 0 is primary and node 1 is secondary.

2. From CLI operational mode, enter one of the following CLI commands:

   - To add a license key from a file or a URL, enter the following command, specifying the filename or the URL where the key is located:

     user@host> **request system license add *filename* | *url***

   - To add a license key from the terminal, enter the following command:

     user@host> **request system license add terminal**

3. When prompted, enter the license key, separating multiple license keys with a blank line.

   If the license key you enter is invalid, an error appears in the CLI output when you press Ctrl+d to exit license entry mode.

4. Verify the installed licenses.

   For more details, see Adding New Licenses (CLI Procedure).

To install licenses on the secondary node of an SRX Series device in a chassis cluster:

1. Initiate a failover to change node 1 (secondary node) to be the primary node:

   {primary:node0}

   user@host> request chassis cluster failover redundancy-group 0 node 1

   ```
    - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
   - -
   Initiated manual failover for redundancy group 0
   ```

NOTE: Initiating a failover to the secondary node is not required if you are installing licenses manually on the device. However, if you are installing the license directly from the Internet, you must initiate a failover.

2. Repeat the steps described in "Step-by-Step Procedure" on page 153 to install licenses on the secondary node.

3. Reboot the device for licenses to take effect.

NOTE: You must install the updated license on both nodes of the chassis cluster before the existing license expires.

NOTE: In a chassis cluster configuration, when one device has a license installed, and the other device does not have the same license installed, an error message is displayed when you try to configure that specific feature as shown in the following example:

[edit security utm feature-profile web-filtering type]

```
  'type juniper-enhanced'
    warning: requires 'wf_key_websense_ewf' license
<<<<<<<<<<<<<<<<<<<<<<<
configuration check succeeds
```

TIP: If you are not using any specific feature or license , you can delete the license from both devices in a chassis cluster. You need to connect to each node separately to delete the licenses. For details, see "Example: Deleting a License Key" on page 171.

Verifying Licenses on an SRX Series Device in a Chassis Cluster

Purpose You can verify the licenses installed on both the devices in a chassis cluster setup by using the **show system license installed** command to view license usage.

Action Licenses details on node 0.

user@host> show system license installed

```
{primary:node0}
user@host> show system license
License usage:
                                Licenses     Licenses    Licenses    Expiry
  Feature name                       used    installed      needed
  logical-system                        1           26           0    permanent
  services-offload                      0            1           0    permanent

Licenses installed:
  License identifier: JUNOS363684
  License version: 2
  Valid for device: JN111A654AGB
  Features:
    services-offload - services offload mode
      permanent

  License identifier: JUNOS531744
  License version: 4
  Valid for device: JN111A654AGB
  Features:
    services-offload - services offload mode
      permanent

  License identifier: JUNOS558173
  License version: 4
  Valid for device: JN111A654AGB
  Features:
    logical-system-25 - Logical System Capacity
      permanent
```

Licenses details on node 1.

```
{secondary-hold:node1}
user@host> show system license
License usage:
                                Licenses     Licenses    Licenses    Expiry
  Feature name                       used    installed      needed
  idp-sig                               0            1           0    permanent
  logical-system                        1           26           0    permanent
  services-offload                      0            1           0    permanent

Licenses installed:
  License identifier: JUNOS209661
  License version: 2
  Valid for device: JN111AB4DAGB
  Features:
    idp-sig          - IDP Signature
      permanent

  License identifier: JUNOS336648
  License version: 2
  Valid for device: JN111AB4DAGB
  Features:
    logical-system-25 - Logical System Capacity
```

```
    permanent

License identifier: JUNOS363685
License version: 2
Valid for device: JN111AB4DAGB
Features:
  services-offload - services offload mode
    permanent

License identifier: JUNOS531745
License version: 4
Valid for device: JN111AB4DAGB
Features:
  services-offload - services offload mode
    permanent
```

Meaning Use the fields **License version** and **Features** to make sure that licenses installed on both the nodes are identical.

Understanding Licenses for Logical Systems and Tenant Systems on SRX Series Devices

This topic provides licensing information for SRX Series devices running logical systems and tenant systems.

Starting in Junos OS Release 18.3R1, an SRX Series device running logical systems or tenant systems includes three licenses by default. One license for a master logical system and the other two licenses for user-defined logical system or tenant system. The system does not allow you to configure additional logical systems or tenant systems if the number of logical systems and tenant systems exceeds the number of available licenses. In the earlier releases, the system allowed you to configure an additional logical system even if the number of logical systems exceeds the number of available licenses, but with a warning message of non-licensed logical-systems do not pass traffic. You can purchase licenses for additional logical systems and tenant systems that you intend to create. If you intend to configure an interconnect logical system or interconnect tenant system to use as a switch, it also requires separate licenses.

We enforce that you do not configure more logical systems or tenant systems than the number of licenses you have purchased. If the number of logical systems or tenant systems that you attempt to configure exceeds the number of licenses that you have purchased, then the system displays an error message similar to the following:

```
user@host> commit
```

```
error: 2 more multitenancy license(s) are needed!
error: configuration check-out failed
```

You can use the **show system license status all-logical-systems-tenants** or **show system license usage** commands to view the active logical systems and tenant systems on the device.

```
user@host> show system license status all-logical-systems-tenants
```

```
logical system name  license status
root-logical-system  enabled
LSYS2                enabled
LSYS0                enabled
LSYS11               enabled
LSYS12               enabled
LSYS23               enabled
TSYS1                enabled
TSYS2                enabled
TSYS3                enabled
```

```
user@host> show system license usage
```

```
                    Licenses  Licenses     Licenses   Expiry
 Feature name       used      installed    needed
 logical-system       9          11          0        2019-05-18
                                                      08:00:00 CST
```

When you use SRX Series devices running logical systems or tenant systems in a chassis cluster, you must purchase and install the same number of licenses for each node in the chassis cluster. Logical systems or tenant systems licenses pertain to a single chassis, or node, within a chassis cluster and not to the cluster collectively.

See Also

- *Understanding Logical Systems for SRX Series Services Gateways*
- *Understanding Tenant Systems*
- Understanding Chassis Cluster Licensing Requirements on page 152
- Installing Licenses on the SRX Series Devices in a Chassis Cluster on page 152
- Verifying Licenses on an SRX Series Device in a Chassis Cluster on page 154

Understanding UTM Licensing

The majority of UTM features function as a subscription service requiring a license. You can redeem this license once you have purchased your subscription license SKUs. You redeem your license by entering your authorization code and chassis serial number into the Customer Service License Management System (LMS) interface. Once your entitlement is generated, you can use the CLI from your device to send a license update request to the LMS server. The LMS server then sends your subscription license directly to the device.

NOTE: UTM requires 1 GB of memory.

Table 30: UTM Feature Subscription Service License Requirements

UTM Feature	Requires License
Antispam	Yes
Antivirus: sophos	Yes
Content Filtering	No
Web Filtering: integrated	Yes
Web Filtering: redirect	No
Web Filtering: local	No
Web Filtering: enhanced	Yes

NOTE: License enforcement is supported on all SRX Series devices. Licensed features including anti-virus or Enhanced Web Filtering will not function until a license has been installed. The license must be installed after installing or upgrading to a new Junos OS Release version. Unlicensed features such as UTM blacklists and whitelists will continue to function without a license.

Updating UTM Licenses (CLI Procedure)

To apply the UTM subscription license to SRX Series devices, use the following CLI command:

```
user@host> request system license update
```

After you install the license for SRX300, SRX320, SRX340, SRX345, SRX550M, and SRX1400 devices, reboot the device. The device reserves additional memory for UTM features and hence decreases the session capacity.

For SRX3400, SRX3600, SRX4600, SRX5600 and SRX5800 devices, use the following command to manually reallocate the memory for UTM features:

```
user@host>set security forwarding-process application-services enable-utm-memory
```

Reboot the device for the configuration to take effect.

NOTE: SRX1500, SRX4100 and SRX4200 devices have enough memory for UTM. These devices do not require any command for memory allocation.

See Also

- Understanding Chassis Cluster Licensing Requirements on page 152
- Verifying Licenses on an SRX Series Device in a Chassis Cluster on page 154
- Installing Licenses on the SRX Series Devices in a Chassis Cluster on page 152
- *Understanding Licenses for Logical Systems and Tenant Systems on SRX Series Devices*

Installing the IPS License (CLI)

You can either download an IPS license from the license server, or manually install IPS if you received a license from Juniper Networks.

Access the SRX Series device console through the serial cable plugged into the console port on the device or by using a terminal session such as SSH.

To apply your IPS subscription license to the device, use the following CLI command:

```
user@host> request system license update
```

If you received a license for manual installation, perform the following tasks:

1. Access the SRX Series Services Gateway console either by plugging the serial cable into the console port on the device or by using a terminal session such as SSH.

2. Check for an IPS license (required for all IPS updates):

   ```
   user@host> show system license
   ```

   ```
   License usage:
                                  Licenses     Licenses    Licenses    Expiry
     Feature name                      used    installed      needed
     logical-system                       0          0           0    permanent
   ```

3. If there are no licenses installed, obtain the chassis serial number by using the following CLI command:

   ```
   user@host> show chassis hardware
   ```

4. A serial number is needed to generate the IPS license. You can add a license key from a file or URL or from the terminal.

   - From a file or URL:

     ```
     user@host> request system license add <file name>
     ```

   - From the terminal:

     ```
     user@host> request system license add terminal
     ```

5. When prompted, enter the license key, separating multiple license keys with a blank line. If the license key you enter is invalid, an error is generated when you press Ctrl-D to exit license entry mode.

6. Verify the system license by entering the **show system license** command.

```
user@host> show system license
```

```
License usage:
                    Licenses     Licenses    Licenses   Expiry
  Feature name         used    installed      needed
  idp-sig               4            1           0  permanent


Licenses installed:
  License identifier: JUNOS208639
  License version: 2
  Valid for device: AA4508AD0005
  Features:
    idp-sig   - IDP Signature
     date-based, 2009-0406 08:00:00 GMT-8 - 2010-04-06 08:00:00 GMT-8
```

See Also

- Understanding Chassis Cluster Licensing Requirements on page 152
- Verifying Licenses on an SRX Series Device in a Chassis Cluster on page 154
- Installing Licenses on the SRX Series Devices in a Chassis Cluster on page 152
- *Understanding Licenses for Logical Systems and Tenant Systems on SRX Series Devices*

Installing and Verifying Licenses for an Application Signature Package

The Junos OS application signature package update is a separately licensed subscription service. You must install the application signature package update license key on your device to download and install the signature database updates provided by Juniper Networks. If your license key expires, you can continue to use the locally stored application signature package content.

Licensing is usually ordered when the device is purchased, and this information is bound to the chassis serial number. These instructions assume that you already have the license. If you did not order the license during the purchase of the device, contact your account team or Juniper customer care for assistance. For more information, refer to the Knowledge Base article KB9731 at https://kb.juniper.net/InfoCenter/index?page=home.

NOTE: Starting from Junos OS 15.1X49-D30 and Junos OS Release 17.3R1, on SRX1500 devices, AppSecure is part of Juniper Networks Secure Edge software (a default shipping software package on the SRX1500). A separate license key is not required on your device to download and install the AppID signature database updates, or to use other AppSecure features such as AppFW, AppQoS, and AppTrack.

NOTE: Starting from Junos OS 15.1X49-D30 and Junos OS Release 17.3R1, on SRX300, SRX320, SRX340, and SRX345 devices, AppSecure is part of Juniper Networks Secure Edge software or IPS subscription license. A separate license key is not required on your device to download and install the AppID signature database updates, or to use other AppSecure features such as AppFW, AppQoS, and AppTrack.

NOTE: Starting from 15.1X49-D65 and Junos OS Release 17.3R1, on SRX4100, and SRX4200 devices, AppSecure is part of Juniper Networks Secure Edge software (a default shipping software package). A separate license key is not required on your device to download and install the AppID signature database updates, or to use other AppSecure features such as AppFW, AppQoS, and AppTrack.

NOTE: Starting from Junos OS Release 17.4R1, on SRX4600, AppSecure is part of Juniper Networks Secure Edge software (a default shipping software package). A separate license key is not required on your device to download and install the AppID signature database updates, or to use other AppSecure features such as AppFW, AppQoS, and AppTrack.

You can install the license on the SRX Series device using either the automatic method or manual method as follows:

- Install your license automatically on the device.

  To install or update your license automatically, your device must be connected to the Internet .

  ```
  user@host> request system license update
  ```

  ```
  Trying to update license keys from https://ae1.juniper.net, use 'show system
  license' to check status.
  ```

- Install the licenses manually on the device.

  ```
  user@host> request system license add terminal
  ```

  ```
  [Type ^D at a new line to end input,
   enter blank line between each license key]
  ```

  Paste the license key and press Enter to continue.

- Verify the license is installed on your device.

Use the **show system license command** command to view license usage, as shown in the following example:

```
License usage:
                                Licenses     Licenses    Licenses    Expiry
  Feature name                      used    installed      needed
  logical-system                       4            1           3    permanent


 License identifier: JUNOSXXXXXX
  License version: 2
  Valid for device: AA4XXXX005
  Features:
    appid-sig        - APPID Signature
      date-based, 2014-02-17 08:00:00 GMT-8 - 2015-02-11 08:00:00 GMT-8
```

The output sample is truncated to display only license usage details.

See Also
- Adding New Licenses (CLI Procedure) on page 36

Understanding Integrity Check and Autorecovery of Configuration, Licenses, and Disk Information on SRX Series Devices

This topic includes the following sections:

Overview

The autorecovery feature is supported on dual-partitioned SRX Series devices. With this feature, information on disk partitioning, configuration, and licenses is recovered automatically in the event it becomes corrupted.

Autorecovery provides the following functions:

- Detect corruption in disk partitioning during system bootup and attempt to recover partitions automatically
- Detect corruption in the Junos OS rescue configuration during system bootup and attempt to recover the rescue configuration automatically
- Detect corruption in Junos OS licenses during system bootup and attempt to recover licenses automatically

How Autorecovery Works

The feature works in the following ways:

- The feature provides the **request system autorecovery state save** command, which backs up important data such as disk partitioning information, licenses, and Junos OS rescue configuration.
- Once the backup copies are saved, they are used to check the integrity of the working copies of the data on every bootup.
- The working copies are automatically recovered if any corruption is detected.

How to Use Autorecovery

You use autorecovery in the following ways:

- Prepare the router for deployment with the necessary licenses and configuration.
- After you finalize the state, execute the **request system autorecovery state save** command to back up the state.
- After you save the state, integrity check and recovery actions (if any) occur automatically on every bootup.
- If subsequent maintenance activities change the state of the router by adding licenses or updating the configuration, you need to execute the **request system autorecovery state save** command again to update the saved state.
- Execute the **show system autorecovery state** command any time to view the status of the saved information and the integrity check status of each saved item.
- Execute the **request system autorecovery state clear** command to delete all backed up data and disable autorecovery, if required.

Data That Is Backed Up in an Autorecovery

The following data is backed up during the autorecovery process:

- Rescue configuration (regenerated from the current configuration)
- License keys
- BSD lables (disk-partitioning information)

Data is backed up only when you execute the **request system autorecovery state save** command. Disk-partitioning information is backed up automatically from factory defaults (for new systems), on installation from the boot loader, and on snapshot creation.

Troubleshooting Alarms

Table 31 on page 164 lists types of autorecovery alarms, descriptions, and required actions.

Table 31: Autorecovery Alarms

Alarm	Alarm Type	Description	Action Required
Autorecovery information needs to be saved	Minor	This alarm indicates: • Unsaved data needs to be saved, or saved data contains problems and another save is required.	• Ensure that the system has all required licenses and configuration. • Execute the **request system autorecovery state save** command.
Autorecovery has recovered corrupted information	Minor	This alarm indicates: • Boot time integrity check failed for certain items; however, the items have been recovered successfully.	• No action is required. • Alarm is cleared on next bootup.
Autorecovery was unable to recover data completely	Major	This alarm indicates: • Boot time integrity check failed for certain items, which could not be recovered successfully.	• The system might be experiencing a fatal malfunction.

Considerations

- Devices must have dual-root partitioning for autorecovery to work.
- The **request system configuration rescue save** command regenerates the rescue configuration from the current Junos OS configuration and then saves it. Therefore, executing the **save** command overwrites any existing rescue configuration.
- In general, the saved contents of the rescue configuration are not updated automatically. If you add licenses, you must execute the **request system autorecovery state save** command again.

NOTE: The rescue configuration is backed up. If /config is corrupted, the system boots from the rescue configuration.

See Also

- *Example: Creating a Snapshot and Using It to Boot an SRX Series Device*
- *Example: Installing Junos OS Upgrade Packages on SRX Series Devices*
- *Reverting the Junos OS Software Image Back to the Previous Version*

Managing Junos OS Licenses

- Updating License Keys (CLI) on page 166
- Example: Adding a New License Key on page 167
- Example: Deleting a License Key on page 171

Displaying License Keys in J-Web

To display license keys installed on the device:

1. In the J-Web interface, select **Maintain>Licenses**.
2. Under Installed Licenses, click **Display Keys** to display all the license keys installed on the device.

   A screen displaying the license keys in text format appears. Multiple licenses are separated by a blank line.

See Also

- Junos OS Feature License Keys on page 17

Downloading License Keys

To download license keys installed on the device:

1. In the J-Web interface, select **Maintain>Licenses**.
2. Under Installed Licenses, click **Download Keys** to download all the license keys installed on the device to a single file.
3. Select **Save it to disk** and specify the file to which the license keys are to be written.

See Also

- Junos OS Feature License Keys on page 17
- Generating a License Key on page 165
- Example: Adding a New License Key on page 167
- Example: Deleting a License Key on page 171

Generating a License Key

To generate a license key:

1. Gather the authorization code that you received when you purchased your license as well as your device serial number.
2. Go to the Juniper Networks licensing page at:

   https://www.juniper.net/lcrs/generateLicense.do

3. Enter the device serial number and authorization code in the webpage and click **Generate**. Depending on the type of license you purchased, you will receive one of the following responses:

   - License key—If you purchased a perpetual license, you will receive a license key from the licensing management system. You can enter this key directly into the system to activate the feature on your device.
   - License key entitlement—If you purchased a subscription-based license, you will receive a license key entitlement from the licensing management system. You can use this entitlement to validate your license on the Juniper Networks licensing server and download the feature license from the server to your device.

See Also

- Example: Adding a New License Key on page 167
- Example: Deleting a License Key on page 171
- Updating License Keys (CLI) on page 166
- Downloading License Keys on page 165

Saving License Keys

To save license keys installed on the device:

1. From operational mode, save the installed license keys to a file or URL.

```
user@host>request system license save filename | url
```

For example, the following command saves the installed license keys to a file named **license.config**:

```
request system license save ftp://user@host/license.conf
```

See Also

- Junos OS Feature License Keys on page 17
- Generating a License Key on page 165
- Example: Adding a New License Key on page 167
- Example: Deleting a License Key on page 171
- Downloading License Keys on page 165

Updating License Keys (CLI)

Use this task to update a subscription license or a trial license. You can do immediate update from command mode or set up automatic updates using the CLI.

You can set up a proxy server to allow indirect access to the Juniper Networks License Management System (LMS). To set up a proxy server for license updates, see *Example: Configuring a Proxy Server for License Updates*.

To do immediate update of a license key from command mode:

1. From operational mode, do one of the following tasks:

   - Update the license keys immediately from the LMS server. You can only use this command to update subscription-based licenses (such as UTM).

     ```
     user@host> request system license update
     ```

     NOTE: The request system license update command always uses the default Juniper license server: https://ae1.juniper.net.

   - Update the trial license keys immediately from the LMS server.

     ```
     user@host>request system license update trial
     ```

To enable automatic license updates from the CLI:

1. Contact your account team or Juniper Networks Customer Care to extend the validity period of existing license keys and obtain the URL for a valid update server.

2. Once you have successfully extended your license key and received the update server URL, configure the auto-update parameter:

   ```
   user@host> set system license autoupdate url https://ae1.juniper.net/
   ```

3. (Optional) Configure renew options. The following sample allows the device to contact the license server 30 days before the current license expires and sends an automatic update request every 6 hours.

   ```
   user@host> set system license renew before-expiration 30
   user@host> set system license renew interval 6
   ```

See Also

- Understanding Chassis Cluster Licensing Requirements on page 152
- Verifying Licenses on an SRX Series Device in a Chassis Cluster on page 154
- Installing Licenses on the SRX Series Devices in a Chassis Cluster on page 152
- Understanding Licenses for Logical Systems and Tenant Systems on SRX Series Devices on page 156

Example: Adding a New License Key

This example shows how to add a new license key.

- Requirements on page 168
- Overview on page 168

Requirements

Before you begin, confirm that your Junos OS feature requires you to purchase, install, and manage a separate software license.

Overview

You can add a license key from a file or URL, from a terminal, or from the J-Web user interface. Use the ***filename*** option to activate a perpetual license directly on the device. (Most feature licenses are perpetual.) Use the ***url*** to send a subscription-based license key entitlement (such as UTM) to the Juniper Networks licensing server for authorization. If authorized, the server downloads the license to the device and activates it.

In this example, the file name is bgp-reflection.

Configuration

CLI Quick Configuration

To quickly configure this section of the example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

From operational mode, you can add a license key in either way:

- From a file or URL:

```
user@hostname> request system license add bgp-reflection
```

- From the terminal:

```
user@hostname> request system license add terminal
```

GUI Step-by-Step Procedure

To add a new license key:

1. In the J-Web user interface, select **Maintain>Licenses**.
2. Under Installed Licenses, click **Add** to add a new license key.
3. Do one of the following, using a blank line to separate multiple license keys:
   - In the **License File URL** box, type the full URL to the destination file containing the license key to be added.
   - In the **License Key Text** box, paste the license key text, in plain-text format, for the license to be added.
4. Click **OK** to add the license key.

NOTE: If you added the SRX100 Memory Upgrade license, the device reboots immediately and comes back up as a high-memory device.

5. Click **OK** to check your configuration and save it as a candidate configuration.

6. If you are done configuring the device, click **Commit Options>Commit**.

Step-by-Step Procedure

To add a new license key:

1. From operational mode, add a license key in either way:

   - From a file or URL:

     ```
     user@host> request system license add bgp-reflection
     ```

   - From the terminal:

     ```
     user@host>request system license add terminal
     ```

2. When prompted, enter the license key, separating multiple license keys with a blank line. If the license key you enter is invalid, an error is generated when you press Ctrl-D to exit license entry mode.

NOTE: If you added the SRX100 Memory Upgrade license, the device reboots immediately and comes back up as a high-memory device.

Results

From operational mode, confirm your configuration by entering the **show system license** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
user@hostname> show system license
```

```
License usage:
                    Licenses     Licenses    Licenses   Expiry
  Feature name         used    installed      needed
  bgp-reflection          0            1           0  permanent


Licenses installed:
  License identifier: G0300000xxxx
  License version: 2
  Valid for device: JN001875AB
  Features:
```

```
  bgp-reflection   - Border Gateway Protocol route reflection
permanent

  License identifier: G0300000xxxx
License version: 2
Valid for device: JN001875AB
```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

Confirm that the configuration is working properly.

Verifying Installed Licenses

Purpose Verify that the expected licenses have been installed and are active on the device.

Action From operational mode, enter the **show system license** command.

The output shows a list of the licenses used and a list of the licenses installed on the device and when they expire.

Verifying License Usage

Purpose Verify that the licenses fully cover the feature configuration on the device.

Action From operational mode, enter the **show system license usage** command.

```
user@hostname> show system license usage
```

```
                        Licenses     Licenses    Licenses    Expiry
Feature name             used       installed      needed
bgp-reflection              1            1           0     permanent
```

The output shows a list of the licenses installed on the device and how they are used.

Verifying Installed License Keys

Purpose Verify that the license keys were installed on the device.

Action From operational mode, enter the **show system license keys** command.

```
user@hostname> show system license keys
```

```
XXXXXXXXXX xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx
           xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx
           xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx
           xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx
```

The output shows a list of the license keys installed on the device. Verify that each expected license key is present.

See Also

- Junos OS Feature License Keys on page 17
- Generating a License Key on page 165
- Example: Deleting a License Key on page 171
- Updating License Keys (CLI) on page 166
- Downloading License Keys on page 165

Example: Deleting a License Key

This example shows how to delete a license key.

- Requirements on page 171
- Overview on page 171
- Configuration on page 171
- Verification on page 172

Requirements

Before you delete a license key, confirm that it is no longer needed.

Overview

You can delete a license key from the CLI or J-Web user interface. In this example, the license ID is G0300000xxxx.

Configuration

CLI Quick Configuration

To quickly configure this section of the example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
user@host> request system license delete G0300000xxxx
```

GUI Step-by-Step Procedure

To delete a license key:

1. In the J-Web user interface, select **Maintain>Licenses**.
2. Select the check box of the license or licenses you want to delete.
3. Click **Delete**.

NOTE: If you deleted the SRX100 Memory Upgrade license, the device reboots immediately and comes back up as a low-memory device.

4. Click **OK** to check your configuration and save it as a candidate configuration.
5. If you are done configuring the device, click **Commit Options>Commit**.

Step-by-Step Procedure

To delete a license key:

1. From operational mode, for each license, enter the following command and specify the license ID. You can delete only one license at a time.

```
user@host> request system license delete G0300000xxxx
```

NOTE: If you deleted the SRX100 Memory Upgrade license, the device reboots immediately and comes back up as a low-memory device.

Results

From configuration mode, confirm your deletion by entering the **show system license** command. The license key you deleted will be removed. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

If you are done configuring the device, enter **commit** from configuration mode.

Verification

Confirm that the configuration is working properly.

- Verifying Installed Licenses on page 172

Verifying Installed Licenses

Purpose

Verify that the expected licenses have been removed from the device.

Action From operational mode, enter the **show system license** command.

See Also

- Generating a License Key on page 165
- Example: Adding a New License Key on page 167
- Updating License Keys (CLI) on page 166
- Downloading License Keys on page 165