



Junos[®] OS

Common Criteria Evaluation Configuration Guide for EX4300 Devices

Release

14.1X53-D30



Modified: 2015-11-09

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

Copyright © 2015, Juniper Networks, Inc. All rights reserved.

Juniper Networks, Junos, Steel-Belted Radius, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. The Juniper Networks Logo, the Junos logo, and JunosE are trademarks of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Junos® OS Common Criteria Evaluation Configuration Guide for EX4300 Devices

Release 14.1X53-D30

Copyright © 2015, Juniper Networks, Inc.

All rights reserved.

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 <http://www.juniper.net/support/eula.html>. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Abbreviated Table of Contents

	About the Documentation	xi
Part 1	Introduction to Common Criteria Network Device Protection Profile	
Chapter 1	Common Criteria NDPP Overview	3
Part 2	Preparing Junos OS for Common Criteria NDPP	
Chapter 2	Preparing Junos OS for Common Criteria NDPP	7
Part 3	Configuring Junos OS for Common Criteria NDPP	
Chapter 3	Securing Management Connections	15
Chapter 4	Authorizing Administrators	19
Chapter 5	Configuring System Message	23
Chapter 6	Configuring Idle Timeout and Session Disconnection	25
Chapter 7	Configuring Event Logging	27
Chapter 8	Configuring Firewall Filters	35
Part 4	Additional NDPP Guidance	
Chapter 9	Authorization	39
Chapter 10	Understanding Event Logging	41
Part 5	Index	
	Index	53

Table of Contents

	About the Documentation	xi
	Documentation and Release Notes	xi
	Supported Platforms	xi
	Using the Examples in This Manual	xi
	Merging a Full Example	xii
	Merging a Snippet	xii
	Documentation Conventions	xiii
	Documentation Feedback	xv
	Requesting Technical Support	xvi
	Self-Help Online Tools and Resources	xvi
	Opening a Case with JTAC	xvi
Part 1	Introduction to Common Criteria Network Device Protection Profile	
Chapter 1	Common Criteria NDPP Overview	3
	Understanding Common Criteria	3
	Common Criteria Terms and Acronyms	4
Part 2	Preparing Junos OS for Common Criteria NDPP	
Chapter 2	Preparing Junos OS for Common Criteria NDPP	7
	Identifying Secure Delivery	7
	Downloading Software Packages	8
	Installing Software Packages	9
	Overview of the Software Installation Process	9
	Installing Software Upgrades on the Switch	9
	Verifying the Digital Signature	11
Part 3	Configuring Junos OS for Common Criteria NDPP	
Chapter 3	Securing Management Connections	15
	Using the Console Port	15
	Configuring SSH Service to Protect Remote Connections	16
	Default Management Service Settings	17
Chapter 4	Authorizing Administrators	19
	Authorized Administrator Overview	19
	Configuring Common Criteria NDPP Authorized Administrator	20

Chapter 5	Configuring System Message	23
	Configuring System Message	23
	message	23
Chapter 6	Configuring Idle Timeout and Session Disconnection	25
	Configuring Idle Timeout and Session Disconnection	25
	idle-timeout (System-Login)	26
Chapter 7	Configuring Event Logging	27
	Event Logging Overview	27
	Configuring Event Logging File Locations	28
	Configuring Event Logging to a Local File	28
	Configuring Event Logging to a Remote Server	28
	Configuring Event Logging to a Remote Server When Initiating the Connection from the Remote Server	28
	Configuring Event Logging to a Remote Server When Initiating the Connection from the NDPP Device	30
	Configuring the Client Alive Mechanism	31
	Configuring the System Log Message Timestamp	31
	Setting the Date and Time Locally	32
	time-format	33
	set date	34
Chapter 8	Configuring Firewall Filters	35
	Configuring Firewall Filters	35
	Filtering Default Network Services	35
Part 4	Additional NDPP Guidance	
Chapter 9	Authorization	39
	Choosing and Using Passwords	39
Chapter 10	Understanding Event Logging	41
	Interpreting Event Messages	41
	Logging of Audit Startup and Shutdown	42
	Login and Logout Events Using SSH	42
	Logging Failure to Establish an SSH Session	43
	Logging Establishment or Termination of an SSH session	43
	Logging Changes to the System Time	44
	Logging Initiation of a System Update	45
	Logging Completion of a TSF Self-Test	45
	Logging Attempts at Unlocking an Interactive Session	45
	Logging Termination of a Remote Session by the Session Locking Mechanism	45
	Logging Termination of an Interactive Session	46
	Logging Initiation of a Trusted Channel	46
	Logging Termination of a Trusted Channel	47

Logging Failure of Trusted Channel or Trusted Path Functions	47
System Log Messages	48
SSHD_LOGIN_FAILED	48
UI_AUTH_EVENT	48
UI_CFG_AUDIT_OTHER	48
UI_CLI_IDLE_TIMEOUT	48
UI_CMDLINE_READ_LINE	49
UI_LOGIN_EVENT	49
UI_LOGOUT_EVENT	49

Part 5

Index

Index	53
-----------------	----

List of Tables

	About the Documentation	xi
	Table 1: Supported Platforms and Install Images	xi
	Table 2: Notice Icons	xiii
	Table 3: Text and Syntax Conventions	xiv
Part 4	Additional NDPP Guidance	
Chapter 10	Understanding Event Logging	41
	Table 4: Fields in Event Messages	42

About the Documentation

- Documentation and Release Notes on page xi
- Supported Platforms on page xi
- Using the Examples in This Manual on page xi
- Documentation Conventions on page xiii
- Documentation Feedback on page xv
- Requesting Technical Support on page xvi

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 <http://www.juniper.net/techpubs/>.

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 <http://www.juniper.net/books>.

Supported Platforms

For the features described in this document, and to operate in accordance with the NDPP certification, [Table 1 on page xi](#) shows the platforms that are supported and their install images.

Table 1: Supported Platforms and Install Images

Platform	Install Image
EX4300	jinstall-ex-4300-14.1X53-D30.3-domestic-signed.tgz

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.xml; }
```

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 the *CLI User Guide*.

Documentation Conventions

Table 2 on page xiii defines notice icons used in this guide.

Table 2: 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.

The CLI has two modes, operational mode and configuration mode.

- Operational mode—This mode displays the current status of the device. In operational mode, you enter commands to monitor and troubleshoot the Junos OS, devices, and network connectivity. Operational mode is indicated by the > prompt—for example:

```
user@switch> clear
```

- Configuration mode—A Junos OS device configuration is stored as a hierarchy of statements. In configuration mode, you can define all properties of the Juniper Networks Junos OS, including interfaces, VLANs, Virtual Chassis information, user access, and several system hardware properties. To enter configuration mode, enter the **configure** command. Configuration mode is indicated by the **#** prompt and includes the current location in the configuration hierarchy—for example:

```
[edit interfaces ge-0/0/12]
user@switch#
```

In configuration mode, you are actually viewing and changing the candidate configuration file. The candidate configuration allows you to make configuration changes without causing operational changes to the current operating configuration, called the active configuration. When you commit the changes you added to the candidate configuration, the system updates the active configuration. Candidate configurations enable you to alter your configuration without causing potential damage to your current network operations.

To activate your configuration changes, enter the **commit** command.

Table 3 on page xiv defines the text and syntax conventions used in this guide.

Table 3: 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
<i>Italic text like this</i>	<ul style="list-style-type: none"> • Introduces or emphasizes important new terms. • Identifies guide names. • Identifies RFC and Internet draft titles. 	<ul style="list-style-type: none"> • A policy <i>term</i> is a named structure that defines match conditions and actions. • <i>Junos OS CLI User Guide</i> • RFC 1997, <i>BGP Communities Attribute</i>
<i>Italic text like this</i>	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 <i>domain-name</i>
Text like this	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	<ul style="list-style-type: none"> • 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 <i>metric</i> >;

Table 3: Text and Syntax Conventions (*continued*)

Convention	Description	Examples
(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 <i>(string1 string2 string3)</i>
# (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]
Indentation 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.	
GUI Conventions		
Bold text like this	Represents graphical user interface (GUI) items you click or select.	<ul style="list-style-type: none"> 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, comments, and suggestions so that we can improve the documentation. You can provide feedback by using either of the following methods:

- Online feedback rating system—On any page at the Juniper Networks Technical Documentation site at <http://www.juniper.net/techpubs/index.html>, simply click the stars to rate the content, and use the pop-up form to provide us with information about your experience. Alternately, you can use the online feedback form at <http://www.juniper.net/techpubs/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 <http://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf>.
- Product warranties—For product warranty information, visit <http://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: <http://www.juniper.net/customers/support/>
- Search for known bugs: <http://www2.juniper.net/kb/>
- Find product documentation: <http://www.juniper.net/techpubs/>
- Find solutions and answer questions using our Knowledge Base: <http://kb.juniper.net/>
- Download the latest versions of software and review release notes: <http://www.juniper.net/customers/csc/software/>
- Search technical bulletins for relevant hardware and software notifications: <http://kb.juniper.net/InfoCenter/>
- Join and participate in the Juniper Networks Community Forum: <http://www.juniper.net/company/communities/>
- Open a case online in the CSC Case Management tool: <http://www.juniper.net/cm/>

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

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 <http://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 <http://www.juniper.net/support/requesting-support.html>.

PART 1

Introduction to Common Criteria Network Device Protection Profile

- [Common Criteria NDPP Overview on page 3](#)

CHAPTER 1

Common Criteria NDPP Overview

- [Understanding Common Criteria on page 3](#)
- [Common Criteria Terms and Acronyms on page 4](#)

Understanding Common Criteria

The Common Criteria for information security technology is an international agreement signed by 28 countries to permit the evaluation of security products against a common set of standards. In the Common Criteria Recognition Arrangement (CCRA) <http://www.commoncriteriaportal.org/ccra/>, the signatories agree to mutually recognize evaluations of products performed in other countries. All evaluations are performed using a common methodology for Information Technology security evaluation.

The Common Criteria Network Device Protection Profile (NDPP) details the requirements to target several areas of threats and policies that are common to network devices. This guide provides details of how to administer and operate supported platforms running Junos[®] operating system (Junos OS) 14.1X53-D30 to be compliant with the requirements specified in the NDPP. The Junos OS targets several areas of threats and policies that are common to network devices to deliver a Common Criteria Network Device Protection Profile (NDPP) for devices running Junos OS Release 14.1X53-D30. These areas include:

- Providing security functionality that addresses threats to the network device and implements policies that are imposed by law or regulation.
- Protecting communications with remote administrators and external system log servers using SSHv2.
- Offering identification and authentication services that support the composition of moderately complex passwords and that are available both through local login and remote login and support of public key-based authentication for remote login.
- Authorization of administrators, presenting an administrator-configured access consent banner.
- Auditing events associated with security-relevant activity on the target device and storing these events on a device distinct from the target device.
- Providing the ability to verify the source of updates to the device.

Other security functionality of the target device, such as the use of IPsec and firewall filters, is not covered by this evaluation. Likewise, use of cryptographic engines other than

those specified in this guidance is not supported for NDPP compliance, as these engines were not analyzed or tested as part of the evaluation activities.

For more information about Common Criteria, see <http://www.commoncriteriaportal.org/>.

Related Documentation

- [Identifying Secure Delivery on page 7](#)

Common Criteria Terms and Acronyms

EAL	Evaluation Assurance Level. An assurance requirement defined by Common Criteria. For example, EAL2 is Evaluation Assurance Level 2, and EAL3 is Evaluation Assurance Level 3. Higher levels have more stringent requirements.
ECC	Elliptical Curve Cryptography. A public key algorithm technique applied over an elliptical curve (a mathematical expression). Operations over an elliptical curve are known to be faster and more secure, and provide equivalent security using a smaller number of bits.
ECDH	Elliptical Curve Diffie-Hellman. Applies the Diffie-Hellman algorithm over an elliptical curve.
ECDSA	Elliptical curve digital signature algorithm. Applies digital signatures over an elliptical curve.
FIPS	Federal Information Processing Standard. FIPS 140-2 and FIPS 140-3 deal with security and cryptographic modules.
TOE	Target of Evaluation. Used to identify the component under evaluation for compliance.

PART 2

Preparing Junos OS for Common Criteria NDPP

- [Preparing Junos OS for Common Criteria NDPP on page 7](#)

CHAPTER 2

Preparing Junos OS for Common Criteria NDPP

- [Identifying Secure Delivery on page 7](#)
- [Downloading Software Packages on page 8](#)
- [Installing Software Packages on page 9](#)

Identifying Secure Delivery

There are several mechanisms provided in the delivery process to ensure that a customer receives a product that has not been tampered with. The customer should perform the following checks upon receipt of an appliance to verify the integrity of the platform:

- **Shipping label**—Ensure that the shipping label correctly identifies the correct customer name and address as well as the device.
- **Outside packaging**—Inspect the outside shipping box and tape. Ensure that the shipping tape has not been cut or otherwise compromised. Ensure that the box has not been cut or damaged to allow access to the device.
- **Inside packaging**—Inspect the plastic bag and seal. Ensure that the bag is not cut or removed. Ensure that the seal remains intact.

If the customer identifies a problem during the inspection, he or she should immediately contact the supplier. Provide the order number, tracking number, and a description of the identified problem to the supplier.

Additionally, there are several checks that can be performed to ensure that the customer has received a box sent by Juniper Networks and not a different company masquerading as Juniper Networks. The customer should perform the following checks upon receipt of a device to verify the authenticity of the device:

- Verify that the device was ordered using a purchase order. Juniper Networks devices are never shipped without a purchase order.
- When a device is shipped, a shipment notification is sent to the e-mail address provided by the customer when the order is taken. Verify that this e-mail notification was received. Verify that the e-mail contains the following information:

- Purchase order number
- Juniper Networks order number used to track the shipment
- Carrier tracking number used to track the shipment
- List of items shipped including serial numbers
- Address and contacts of both the supplier and the customer
- Verify that the shipment was initiated by Juniper Networks. To verify that a shipment was initiated by Juniper Networks, perform the following tasks:
 - Compare the carrier tracking number of the Juniper Networks order number listed in the Juniper Networks shipping notification with the tracking number on the package received.
 - Log in to the Juniper Networks online customer support portal at <https://www.juniper.net/customers/csc/management> to view the order status. Compare the carrier tracking number or the Juniper Networks order number listed in the Juniper Networks shipment notification with the tracking number on the package received.

Downloading Software Packages

In order to achieve the Common Criteria NDPP environment, your switch must be running Release 14.1X53-D30 for your device, as specified in [Table 1 on page xi](#). Before you begin to download the software, ensure that you have a Juniper Networks Web account and a valid support contract. To obtain an account, complete the registration form at the Juniper Networks website: <https://www.juniper.net/registration/Register.jsp>.

To download software upgrades from Juniper Networks:

1. Using a Web browser, follow the links to the download URL on the Juniper Networks webpage. For EX Series, there are not separate software packages for Canada the U.S. and other locations. Therefore, select **Canada and U.S. Version** regardless of your location:
 - <https://www.juniper.net/support/downloads/junos.html>
2. Log in to the Juniper Networks authentication system using the username (generally your e-mail address) and password supplied by Juniper Networks representatives.
3. Select the EX4300 software package:
jinstall-ex-4300-14.1X53-D30.3-domestic-signed.tgz.
4. Download the software to a local host or to an internal software distribution site.



NOTE: When downloading the Junos install package from the Juniper support site, note the SHA-1 value in the Checksum column. These are used to verify the file integrity of the Junos install package in [“Installing Software Packages” on page 9](#).

After downloading the Junos OS Release 14.1X53 software, you can configure the SSH server to achieve the Common Criteria NDPP environment.

Related Documentation

- [Junos OS 14.1 Installation and Upgrade Guide](#)

Installing Software Packages

- [Overview of the Software Installation Process on page 9](#)
- [Installing Software Upgrades on the Switch on page 9](#)
- [Verifying the Digital Signature on page 11](#)

Overview of the Software Installation Process

An EX Series switch is delivered with a domestic version of Junos OS preinstalled. When you connect power to the switch, it starts (boots) from the installed software. For information about initial configuration of the switch, see [Connecting and Configuring an EX Series Switch](#) in the *System Setup Feature Guide for EX Series Switches*.

As new features and software fixes become available, you must upgrade your software to use them. You upgrade Junos OS on an EX Series switch by copying a software package to your switch or another system on your local network, then use either the J-Web interface or the command-line interface (CLI) to install the new software package on the switch. Finally, you reboot the switch; it boots from the upgraded software. After a successful upgrade, you should back up the new current configuration to a secondary device. You should follow this procedure regardless of whether you are installing a domestic or controlled Junos OS package.

During a successful upgrade, the upgrade package removes all files from `/var/tmp` and completely reinstalls the existing software. It retains configuration files, and similar information, such as secure shell and host keys, from the previous version. The previous software package is preserved in a separate disk partition, and you can manually revert back to it if necessary. If the software installation fails for any reason, such as loss of power during the installation process, the system returns to the originally active installation when you reboot.

Installing Software Upgrades on the Switch

To install software upgrades on the switch:

1. (Optional) Copy the software package to the switch. We recommend that you use FTP to copy the file to the `/var/tmp` directory.

This step is optional because Junos OS can also be upgraded when the software image is stored at a remote location. These instructions describe the software upgrade process for both scenarios.

2. Verify that the SHA-1 checksum value for the Junos install package copied to the Junos device matches the checksum noted on the Juniper support site. This ensures that

the transferred file is ready to use for installation, and that it is not truncated or a corrupted file.

- a. When downloading the Junos install package from the Juniper support site, note the SHA-1 value in the **Checksum** column.
- b. Use the **file checksum sha1** command to verify that the Junos install package is present and that the checksum matches the value on the Juniper support site:

```
user@switch> file checksum sha1
/var/tmp/jinstall-ex-4300-Junos-14.1X53-D30.3-domestic-signed.tgz
SHA1 (/var/tmp/jinstall-ex-4300-Junos-14.1X53-D30-domestic-signed.tgz) =
ba9e47120c7ce55cff29afd73eacd370e162c676
```

3. Install the new package on the switch:

```
user@switch> request system software add package
```

Replace *package* with one of the following paths:

- For a software package in a local directory on the switch—**/var/tmp/package.tgz**.
- For a software package on a remote server:
 - **ftp://hostname/pathname/package.tgz**.
 - **http://hostname/pathname/package.tgz**.

where *package.tgz* is, for example,

jinstall-ex-4300-Junos-14.1X53-D30.3-domestic-signed.tgz.



NOTE: To abort the installation, do not reboot your device; instead, finish the installation and then issue the **request system software delete package.tgz** command, where *package.tgz* is, for example, **jinstall-ex-4300-Junos-14.1X53-D30.3-domestic-signed.tgz**. This is your last chance to stop the installation.

4. Reboot to start the new software:

```
user@switch> request system reboot
```

5. After the reboot has completed, log in and verify that the new version of the software is properly installed by running the **show version** command:

```
user@switch> show version
Hostname: switch
Model: ex4300-48t
Junos: 14.1X53-D30.3
JUNOS EX Software Suite [14.1X53-D30.3]
JUNOS FIPS mode utilities [14.1X53-D30.3]
JUNOS Online Documentation [14.1X53-D30.3]
JUNOS EX 4300 Software Suite [14.1X53-D30.3]
JUNOS Web Management Platform Package [14.1X53-D30.3]
JUNOS py-base-powerpc [14.1X53-D30.3]
```

6. If the switch gets stuck in the boot process and fails to load the Junos OS after upgrade, or if the Junos OS loads but the CLI is not working, see [Troubleshooting Software Installation](#) in the *Junos OS Installation and Upgrade Guide*.

Verifying the Digital Signature

The digital signature is verified by default as part of the installation build process. Successful verification is indicated in the install log as follows:

```
user@switch> request system software add jinstall-14.2-20150812.0-domestic-signed.tgz
no-validate
Installing package '/var/home/regress/jinstall-14.2-20150812.0-domestic-signed.tgz'
...
Verified jinstall-14.2-20150812.0-domestic.tgz signed by PackageDevelopmentEc_2015
Verified jinstall-14.2-20150812.0-domestic.tgz signed by PackageDevelopmentRSA_2015
Pre-checking requirements for jinstall...
```

If verification of the digital signature fails during the build process, the installation will be aborted with following error message:

```
user@switch> request system software add jinstall-14.2-20150812.0-domestic-signed.tgz
no-validate
Installing package '/var/home/regress/jinstall-14.2-20150812.0-domestic-signed.tgz'
...
verify-sig: ERROR: Failed loading signature file
fips-mode-i386-14.2-20150807.0.tgz.esig

Package signature verification failed for fips-mode-i386-14.2-20150807.0.tgz
Installation failed for package '/var/home/regress/build/test.tgz'
```

In the event that verification of the digital signature fails, do not proceed with the installation using that copy of the image. Download the image again as described in [“Downloading Software Packages” on page 8](#), and reattempt the installation. If that fails, then contact Juniper customer support to advise them of the issue (see [“Requesting Technical Support” on page xvi](#)).



NOTE: For Common Criteria NDPP compliance, FIPS mode must not be enabled. You must follow the guidance for using the FIPS mode utilities to configure the SSH server to achieve the Common Criteria NDPP environment (see [“Configuring SSH Service to Protect Remote Connections” on page 16](#)).

- Related Documentation**
- [Junos OS Installation and Upgrade Guide](#)
 - [System Setup Feature Guide for EX Series Switches](#)

PART 3

Configuring Junos OS for Common Criteria NDPP

- [Securing Management Connections on page 15](#)
- [Authorizing Administrators on page 19](#)
- [Configuring System Message on page 23](#)
- [Configuring Idle Timeout and Session Disconnection on page 25](#)
- [Configuring Event Logging on page 27](#)
- [Configuring Firewall Filters on page 35](#)

CHAPTER 3

Securing Management Connections

- [Using the Console Port on page 15](#)
- [Configuring SSH Service to Protect Remote Connections on page 16](#)
- [Default Management Service Settings on page 17](#)

Using the Console Port

By default, the console port on the router or switch is enabled. You can use the console port to connect to the Routing Engine through an RJ-45 cable and use the command-line interface (CLI) to configure the device. For more information about the console connector, see [Connecting a Switch to a Management Console](#).

Before you begin connecting and configuring an EX4300 switch, set the following parameter values on the console server or PC:

- Baud rate—9600
- Flow control—None
- Data—8
- Parity—None
- Stop bits—1
- DCD rate—Disregard

For console port pinout specifications, see [Console Port Connector Pinout Information for an EX Series Switch](#).

For more information about the console connector, see [Connecting a Switch to a Management Console](#).

Related Documentation

- [EX4300 Switch Hardware Guide](#)

Configuring SSH Service to Protect Remote Connections

Use this procedure to configure SSH for NDPP for a router or switch running Junos OS.

1. Specify the set of ciphers that SSH can use to perform encryption and decryption functions.

```
[ edit ]
administrator@host# set system services ssh ciphers [ aes128-cbc aes256-cbc ]
```

2. Specify that the only host-key algorithm enabled is for ECDSA and that algorithms for DSA and RSA are disabled.

```
[ edit ]
administrator@host# set system services ssh hostkey-algorithm ssh-ecdsa
administrator@host# set system services ssh hostkey-algorithm no-ssh-dsa
administrator@host# set system services ssh hostkey-algorithm no-ssh-rsa
```

3. Configure the key exchange method. The supported key exchange methods are Diffie-Hellman group 14 for SHA-1, Elliptical Curve Diffie-Hellman nistp256 for SHA-2, Elliptical Curve Diffie-Hellman nistp384 for SHA-2, and Elliptical Curve Diffie-Hellman nistp521 for SHA-2.

```
[ edit ]
administrator@host# set system services ssh key-exchange dh-group14-sha1
```

```
[ edit ]
administrator@host# set system services ssh key-exchange ecdh-sha2-nistp256
```

```
[ edit ]
administrator@host# set system services ssh key-exchange ecdh-sha2-nistp384
```

```
[ edit ]
administrator@host# set system services ssh key-exchange ecdh-sha2-nistp521
```

4. Specify the set of message authentication code (MAC) algorithms that the SSH server can use to authenticate messages for NDPP. The MAC algorithms that can be used are hmac-sha1, hmac-sha2-256, and hmac-sha2-512.

```
[ edit ]
administrator@host# set system services ssh macs hmac-sha1
```

```
[ edit ]
administrator@host# set system services ssh macs hmac-sha2-256
```

```
[ edit ]
administrator@host# set system services ssh macs hmac-sha2-512
```

5. Log out the console session when the serial cable connected to the console port is unplugged.

```
administrator@host# set system ports console log-out-on-disconnect
```

6. Commit the changes.

```
[ edit ]
administrator@host# commit
```



NOTE: Any SSHv2-compliant client can be used to establish the Remote Administrator connection over the configured SSHv2 service.

Default Management Service Settings

By default, the majority of management services, such as SNMP and DHCP, are disabled on EX4300 switches. Those services disabled by default should not be enabled unless explicitly required for the NDPP configuration.

CHAPTER 4

Authorizing Administrators

- [Authorized Administrator Overview on page 19](#)
- [Configuring Common Criteria NDPP Authorized Administrator on page 20](#)

Authorized Administrator Overview

In Junos OS for NDPP, users who are allowed to make changes to the router or switch are called authorized administrators (or security administrators). An authorized administrator has read and write privileges over key operational components and configuration parameters. An authorized administrator has all permissions, including the ability to change configuration statements and security parameters in addition to other management tasks.

For each authorized administrator account, the following can be defined:

- Username—(Required) Name that identifies the user. It must be unique within the router. Do not include spaces, colons, or commas in the username.
- User's full name—(Optional) If the full name contains spaces, enclose it in quotation marks. Do not include colons or commas.
- User identifier (UID)—(Optional) Numeric identifier that is associated with the user account name. The identifier must be in the range from 100 through 64,000 and should be unique on the router. If you do not assign a UID to a username, the software assigns one when you commit the configuration, using the lowest available number. You should ensure that the UID is unique. However, you can assign the same UID to different users. If you do, the CLI displays a warning when you commit the configuration and then assigns the duplicate UID.
- Authentication methods used to access the router must be either password authentication or public-key authentication.

For SSH authentication, you must copy the contents of an SSH key file into the configuration. Use the **load-key-file** *URL filename* command to load an SSH key file that was previously generated, for example, by using **ssh-keygen**. The *URL filename* is the path to the file's location and name. The contents of the SSH key file are copied into the configuration immediately after you enter the **load-key-file** statement.

Configuring Common Criteria NDPP Authorized Administrator

An account for the user **root** is always present in the configuration. The **root** account is not intended for use in normal operation. For the evaluated configuration, the **root** account is restricted to initial installation and configuration of the evaluated device.

You must configure a Common Criteria NDPP authorized administrator with all permissions, including the ability to change the router configuration.

This procedure shows how to configure an NDPP authorized administrator.

1. The authentication algorithm for plain-text passwords must be configured as sha1 or sha256.

- For sha1:

```
[edit]
administrator@host# set system login password format sha1
```

- For sha256:

```
[edit]
administrator@host# set system login password format sha256
```

2. Commit the changes.

```
[edit]
root@host# commit
```

3. Create a login class named **security-admin** with **permissions all**.

```
[edit]
root@host# set system login class security-admin permissions all
```

4. Use the newly-created **security-admin** class to define your NDPP user authorized administrator named NDPP-admin.

```
[edit]
root@host# set system login user NDPP-admin full-name "Common Criteria NDPP
Authorized Administrator" class security-admin authentication plain-text-password
<password>
New password: type password here
Retype new password: retype password here
```

5. (Optional) Configure public key authentication for remote administrators.

```
[edit]
root@host# set system login user NDPP-admin authentication ssh-ecdsa <public-key>
```

6. Commit the changes.

```
[edit]
root@host# commit
```



NOTE: The root user password should be reset following the change to sha1 or sha256 for the password storage format. This ensures the new password is protected using a sha1 hash, rather than the default password hashing algorithm. To reset the root user password use the `set system login user root authentication plain-text-password password` command, and confirm the new password when prompted.

7. Verify your user setup.

```
[edit system login user NDPP-admin]
root@host# show
full-name "Common Criteria NDPP Authorized Administrator";
uid 001;
class security-admin;
authentication {
    encrypted-password "$ABC123"; # SECRET-DATA; ssh-eccdsa
    "eccdsa-sha2-nistp256
    AAAAEZVjZHNhLXNoYTItbmlkdHAyNTYAAAAIbmlkdHAyNTYAAABBBBCSGe4pk5SCOLzNH0I/Ngwc
    +QUvISTokbBFHdgpwhc15Pljw0Mm+AiB9UO72D+HZc8lAd/5082NA1imk7QSYuog=
    shanbhag@nms5-vm-linux3";
}
```


CHAPTER 5

Configuring System Message

- [Configuring System Message on page 23](#)
- [message on page 23](#)

Configuring System Message

The security administrator must configure a banner with an advisory notice to be displayed before the identification and authentication screen.

The **message** system login option defines the system login message. This message appears before a user logs in.

message

Syntax	<code>message text;</code>
Hierarchy Level	[edit system login]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	<p>Configure a system login message. This message appears before a user logs in.</p> <p>You can format the message using the following special characters:</p> <ul style="list-style-type: none">• \n—New line• \t—Horizontal tab• \'—Single quotation mark• \"—Double quotation mark• \\—Backslash
Options	text —Text of the message.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration

CHAPTER 6

Configuring Idle Timeout and Session Disconnection

- [Configuring Idle Timeout and Session Disconnection on page 25](#)
- [idle-timeout \(System-Login\) on page 26](#)

Configuring Idle Timeout and Session Disconnection

The security administrator can configure a period of time after which an inactive session will be locked and require re-authentication to be unlocked. This helps to protect the device from being idle for a long period before the session times out.

The **idle-timeout** system login option defines the length of time the CLI operational mode prompt remains active before the session times out.

```
administrator@host# set system login class class-name idle-timeout minutes
```

The administrator can also configure the console session to logout when the serial cable connected to the console port is unplugged using the **log-out-on-disconnect** option at the **[edit system ports console]** hierarchy level.

```
administrator@host# set system ports console log-out-on-disconnect
```

Related
Documentation

- [idle-timeout \(System-Login\) on page 26](#)

idle-timeout (System-Login)

Syntax	<code>idle-timeout <i>minutes</i>;</code>
Hierarchy Level	[edit system login class <i>class-name</i>]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	For a login class, configure the maximum time that a session can be idle before the user is logged out of the router or switch. The session times out after remaining at the CLI operational mode prompt for the specified time.
Default	If you omit this statement, a user is never forced off the system after extended idle times.
Options	<i>minutes</i> —Maximum idle time. Range: 0 through 4294967295 minutes



NOTE: The timeout feature is disabled if the value of *minutes* is set to 0.

Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Configuring the Timeout Value for Idle Login Sessions</i>• <i>user</i>

CHAPTER 7

Configuring Event Logging

- [Event Logging Overview on page 27](#)
- [Configuring Event Logging File Locations on page 28](#)
- [Configuring the System Log Message Timestamp on page 31](#)
- [Setting the Date and Time Locally on page 32](#)
- [time-format on page 33](#)
- [set date](#)

Event Logging Overview

A secure Junos OS environment requires the auditing of events listed below, and storing them in a local audit file. The recorded events are simultaneously sent to an external syslog server.

A syslog server is required to receive the syslog messages streamed from the switch. The syslog server must have an SSH client with NETCONF support configured to receive the streamed syslog messages.

The logging for NDPP captures the following events:

- Changes to secret data in the configuration.
- Committed changes.
- System startup.
- Login/logout of users.
- Failure to establish an SSH session.
- Establishment/termination of an SSH session.
- Changes to the (system) time.
- Initiation of a system update.
- Completion of TOE Security Functions (TSF) self-tests.
- Attempts at unlocking an interactive session.
- Termination of a remote session by the session locking mechanism.
- Termination of an interactive session.

- Initiation of a trusted channel.
- Termination of a trusted channel.
- Failure of functions of a trusted channel or a trusted path.

Configuring Event Logging File Locations

- [Configuring Event Logging to a Local File on page 28](#)
- [Configuring Event Logging to a Remote Server on page 28](#)

Configuring Event Logging to a Local File

You configure the storing of audit information to a local file and the level of detail to be recorded with the **syslog** statement. The following must be used to ensure all events detailed in NDPP are logged and are stored in a local file (named **Audit-File** in this example):

```
[edit system]
syslog {
  file Audit-File {
    any any;
  }
}
```



NOTE: The log file should be set to a maximum size of 250 MB. To configure the log file size, use the size statement at the [edit system syslog file *filename* archive] hierarchy level.

Configuring Event Logging to a Remote Server

You configure the export of audit information to a secure, remote server by setting up an event trace monitor that sends event log messages by using NETCONF over SSH to the remote system event logging server (see [“Configuring SSH Service to Protect Remote Connections” on page 16](#)).

The following procedures show the configuration needed to send system log messages to a secure external server by using NETCONF over SSH.

- [Configuring Event Logging to a Remote Server When Initiating the Connection from the Remote Server on page 28](#)
- [Configuring Event Logging to a Remote Server When Initiating the Connection from the NDPP Device on page 30](#)
- [Configuring the Client Alive Mechanism on page 31](#)

Configuring Event Logging to a Remote Server When Initiating the Connection from the Remote Server

To configure event logging to a remote server when the SSH connection to the NDPP device is initiated from the remote system log server.

1. On the remote system log server, generate an ECDSA public key.

```
$ ssh-keygen -b 256 -t ecdsa -C 'syslog-monitor key pair' -f ~/.ssh/syslog-monitor
```

You are prompted to enter a passphrase. The storage locations for the **syslog-monitor** key pair are shown.

2. On the NDPP device, create a class named **monitor** that has permission to trace events.

```
[edit system login]
root@host# set class monitor permissions trace
```

3. Create a user named **syslog-mon** with the class **monitor**, and with authentication that uses the **syslog-monitor** key pair from the key pair file located on the remote system log server.

```
[edit system login]
root@host# set user syslog-mon class monitor authentication ssh-ecdsa "ssh-ecdsa
xxxxx syslog-monitor key pair"
```

4. Set up NETCONF for use with SSH.

```
[edit system services]
root@host# set netconf ssh
```

5. Configure the system log to log everything to **/var/log/messages**.

```
[edit system ]
root@host# set syslog file messages any any
```

6. Commit the changes.

```
[edit ]
root@host# commit
```

7. On the remote system log server, start up the SSH agent **ssh-agent(1)**.

```
$ eval `ssh-agent -s`
```

8. On the remote system log server, add the **syslog-monitor** key pair to **ssh-agent(1)**.

```
$ ssh-add ~/.ssh/syslog-monitor
```

You are prompted to enter the predetermined passphrase. Enter the *same* passphrase that you used in Step 1.

9. While you are logged in to the **external_syslog_server** session, establish a tunnel to the Junos OS device and start NETCONF.

```
$ ssh syslog-mon@1NDPP_TOE -s netconf
```

10. With NETCONF established, configure a system log events message stream.

```
<rpc><get-syslog-events><stream>messages</stream></get-syslog-events></rpc>
```

You should see examples of system log messages (**<syslog>**) being received, for example:

```
<syslog>
May 7 11:40:46 test0 mgd[1522]: UI_CMDLINE_READ_LINE: User 'root', command 'quit'
</syslog>
```

For more information about configuring event logging, see *Junos OS 14.1 Administration Library for Routing Devices*.

Configuring Event Logging to a Remote Server When Initiating the Connection from the NDPP Device

To configure event logging to a remote server when the SSH connection to the remote system log server is initiated from the NDPP device:

1. On the remote system log server, generate an ECDSA public key.

```
$ ssh-keygen -b 256 -t ecdsa -C 'syslog-monitor key pair' -f ~/.ssh/syslog-monitor
```

You are prompted to enter a passphrase. The storage locations for the **syslog-monitor** key pair are shown.

2. On the NDPP device, create a class named **monitor** that has permission to trace events.

```
[edit system login]
root@host# set class monitor permissions trace
```

3. Create a user named **syslog-mon** with the class **monitor**, and with authentication that uses the **syslog-monitor** key pair from the key pair file located on the remote system log server.

```
[edit system login]
root@host# set user syslog-mon class monitor authentication ssh-ecdsa "ssh-ecdsa
xxxxx syslog-monitor key pair"
```

4. In system services, set up NETCONF for use with SSH.

```
[edit system services]
root@host# set netconf ssh
```

5. Configure the system log to log everything to **/var/log/messages**.

```
[edit system ]
root@host# set syslog file messages any any
```

6. Commit the changes.

```
[edit ]
root@host# commit
```

7. Initiate an SSH session to the external system log server from the NDPP device.

```
$ ssh -R 127.0.0.1:2222:127.0.0.1:22 USER_X@external_syslog_server
```

8. While you are logged in, on the remote system log server, start up the SSH agent **ssh-agent(1)**.

```
$ eval `ssh-agent -s`
```

9. On the remote system log server, add the **syslog-monitor** key pair to **ssh-agent(1)**.

```
$ ssh-add ~/.ssh/syslog-monitor
```

You are prompted to enter the predetermined passphrase. Enter the *same* passphrase that you used in Step 1.

10. While you are logged in to the **external_syslog_server** session, establish a tunnel to the Junos OS device and start NETCONF.

```
$ ssh -p2222 syslog-mon@127.0.0.1 -s netconf
```

11. With NETCONF established, configure a system log events message stream.

```
<rpc><get-syslog-events><stream>messages</stream></get-syslog-events></rpc>
```

You should see examples of system log messages (`<syslog></syslog>`) being received, for example:

```
<syslog>
May 7 11:40:46 test0 mgd[1522]: UI_CMDLINE_READ_LINE: User 'root', command 'quit'
</syslog>
```

For more information about configuring event logging, see [Junos OS 14.1 Administration Library for Routing Devices](#).

Configuring the Client Alive Mechanism

If the connection to the remote syslog server drops, the session can be re-established automatically using the client alive mechanism. The client alive mechanism is not enabled at default. To enable it, configure the **client-alive-interval** and the **client-alive-count-max** statements at the `[edit system services ssh]` hierarchy level.

In the following example, the session will be re-established automatically if connectivity is restored within the period (**client-alive-interval seconds * client-alive-count-max seconds**), or 100 seconds (20 x 5).

```
[edit system services ssh]
client-alive-count-max 5;
client-alive-interval 20;
```

If the connection is dropped beyond this period, there will be no automatic re-establishment of the session and the administrator will need to re-establish the session manually.

Configuring the System Log Message Timestamp

By default, the timestamp recorded in a standard-format system log message specifies the month, date, hour, minute, and second when the message was logged, as in the following example:

```
Aug 21 12:36:30
```

To achieve compliance with NDPP, the timestamp must also include the year, as in the following example:

```
Aug 21 12:36:30 2014
```

To include the year in the timestamp, include the **time-format** statement at the `[edit system syslog]` hierarchy level:

```
[edit system syslog]
time-format year
```



NOTE: Messages logged in structured-data format include the year and millisecond by default. If you include the structured-data statement at the [edit system syslog file *filename*] hierarchy level along with the time-format statement, the time-format statement is ignored and messages are logged in structured-data format.

Related Documentation • [time-format on page 33](#)

Setting the Date and Time Locally

You can set the date and time on a device running Junos OS by using the **set date** operational mode command:

To enter the date and time locally:

1. From operational mode, manually set the date and time.

Because this is an operational-mode command, there is no need to perform a commit operation.

```
user@host> set date YYYYMMDDhhmm.ss
```

For example:

```
user@host> set date 201307251632
Thu Jul 25 16:32:00 PDT 2013
```


2. Verify the time.

The **show system uptime** command provides the following information: current time, last boot time, protocols start time, last configuration commit time.

```
user@host> show system uptime
Current time: 2013-07-25 16:33:38 PDT
System booted: 2013-07-11 17:14:25 PDT (1w6d 23:19 ago)
Protocols started: 2013-07-11 17:16:35 PDT (1w6d 23:17 ago)
Last configured: 2013-07-23 12:32:42 PDT (2d 04:00 ago) by user
4:33PM up 13 days, 23:19, 1 user, load averages: 0.00, 0.01, 0.00
```

Related Documentation • [set date on page 34](#)

time-format

Syntax	<code>time-format (year millisecond year millisecond);</code>
Hierarchy Level	<code>[edit system syslog]</code>
Release Information	<p>Statement introduced before Junos OS Release 7.4.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>Statement introduced in Junos OS Release 11.1 for the QFX Series.</p> <p>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.</p>
Description	<p>Include the year, the millisecond, or both, in the timestamp on every standard-format system log message. The additional information is included for messages directed to each destination configured by a file, console, or user statement at the <code>[edit system syslog]</code> hierarchy level. As of Junos OS Release 11.4, the additional time information is also sent to destinations configured by a host statement.</p> <p>By default, the timestamp specifies the month, date, hour, minute, and second when the message was logged—for example, Aug 21 12:36:30. However, the timestamp for traceoption messages is specified in milliseconds by default, and is independent of the <code>[edit system syslog time-format]</code> statement.</p>
	<p> NOTE: When the <code>structured-data</code> statement is included at the <code>[edit system syslog file filename]</code> hierarchy level, this statement is ignored for the file.</p>
Options	<p>millisecond—Include the millisecond in the timestamp.</p> <p>year—Include the year in the timestamp.</p>
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • <i>Including the Year or Millisecond in Timestamps</i> • <i>Junos OS System Log Messages Reference</i> • <i>structured-data</i>

set date

Syntax	set date (<i>date-time</i>)
Release Information	Command introduced before Junos OS Release 7.4.
Description	<p>Set the date and time manually.</p> <pre>user@host> set date 201307251632 Thu Jul 25 16:32:00 PDT 2013</pre>
Options	<ul style="list-style-type: none">• <i>date-time</i>—Specify date and time in one of the following formats:<ul style="list-style-type: none">• <i>YYYYMMDDHHMM.SS</i>• “<i>month DD, YYYY HH:MM(am pm)</i>”
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none">• <i>Setting the Date and Time Locally</i>

CHAPTER 8

Configuring Firewall Filters

- [Configuring Firewall Filters on page 35](#)

Configuring Firewall Filters

In the Junos OS, management traffic is isolated from other types of traffic, such as user transit traffic, in several ways. The Junos OS maintains a separate virtual address space for every authorized manager. Traffic separation is also accomplished when a separate management network is connected to the dedicated management port.

You should deploy firewall filters on management ports to limit access to authorized locations. For more information about firewall filters, see the [Junos OS Policy Framework Configuration Guide](#).

This section provides examples for configuring firewall filters:

Filtering Default Network Services

This firewall filter should be applied to ensure that only the services detailed in the Security Target respond in the NDPP configuration. This filters the unsecured syslog connection between the Routing Engines (UDP/514) and also filters the JVAS PTSP application connection (which is an RE/PIC application for internal routing instance IRI1, UDP/49155).



NOTE: This firewall filter is only an example. Do not copy the addressing specifics and use them on an actual system.

Configure the firewall filter:

```
[edit firewall family inet]
filter NDPP-filter {
  term block {
    from {
      protocol udp;
      destination-port [ 514 49155 ];
    }
    reject port-unreachable;
  }
  term allow {
    then accept;
  }
}
```

```
}  
}
```

Configure the **NDPP-filter** filter as an input filter to **lo0**:

```
[edit interfaces lo0 unit 0 family inet]  
filter {  
    input NDPP-filter;  
}
```

PART 4

Additional NDPP Guidance

- [Authorization on page 39](#)
- [Understanding Event Logging on page 41](#)

CHAPTER 9

Authorization

- [Choosing and Using Passwords on page 39](#)

Choosing and Using Passwords

The following guidelines and configuration options should be considered when configuring the requirements for passwords and when selecting passwords for authorized administrator accounts:

- The password should be easy to remember so that users are not tempted to write it down.
- The password should be changed periodically.
- The password should not be divulged to anyone.
- The following password requirements can be configured:
 - Contain a minimum of 15 characters or more. The minimum length can be set to more than 15 characters by the authorized administrator if needed.

[edit]

administrator@host# set system login password minimum-length 15

Include both alphanumeric and punctuation characters, composed of any combination of upper and lowercase letters, numbers, and special characters (which include !, @, #, \$, %, ^, &, *, (, and)). There should be at least one change of case, one or more digits, and one or more punctuation marks.

- Contain character sets in the password. Valid character sets include uppercase letters, lowercase letters, numbers, punctuation, and other special characters.

[edit]

administrator@host# set system login password change-type character-sets

- Contain the minimum number of character sets or character set changes. The minimum number of character sets required in plain-text passwords in Junos OS is 3.

[edit]

administrator@host# set system login password minimum-changes 3

Weak passwords are:

- Words that might be found in or exist as a permuted form in a system file such as `/etc/passwd`.
- The host name of the system (always a first guess).
- Any word that appears in a dictionary. This includes dictionaries other than English, and words found in works such as Shakespeare, Lewis Carroll, Roget's Thesaurus, and so on. This prohibition includes common words and phrases from sports, sayings, movies, and television shows.
- Permutations on any of the above. For example, a dictionary word with vowels replaced with digits (for example f00t) or with digits added to the end.
- Any machine-generated password. Algorithms reduce the search space of password-guessing programs and so should not be used.

Strong reusable passwords can be based on letters from a favorite phrase or word, and then concatenated with other, unrelated words, along with additional digits and punctuation.



NOTE: Passwords should be changed from time to time.

CHAPTER 10

Understanding Event Logging

- [Interpreting Event Messages on page 41](#)
- [Logging of Audit Startup and Shutdown on page 42](#)
- [Login and Logout Events Using SSH on page 42](#)
- [Logging Failure to Establish an SSH Session on page 43](#)
- [Logging Establishment or Termination of an SSH session on page 43](#)
- [Logging Changes to the System Time on page 44](#)
- [Logging Initiation of a System Update on page 45](#)
- [Logging Completion of a TSF Self-Test on page 45](#)
- [Logging Attempts at Unlocking an Interactive Session on page 45](#)
- [Logging Termination of a Remote Session by the Session Locking Mechanism on page 45](#)
- [Logging Termination of an Interactive Session on page 46](#)
- [Logging Initiation of a Trusted Channel on page 46](#)
- [Logging Termination of a Trusted Channel on page 47](#)
- [Logging Failure of Trusted Channel or Trusted Path Functions on page 47](#)
- [System Log Messages on page 48](#)

Interpreting Event Messages

The following is a sample event message.

```
Jul 24 17:43:28 router1 mgd[4163]: UI_CFG_AUDIT_SET_SECRET: User 'admin' set: [system  
radius-server 1.2.3.4 secret]
```

[Table 4 on page 42](#) describes the fields for an event message. If the system logging utility cannot determine the value in a particular field, a hyphen (-) appears instead.

Table 4: Fields in Event Messages

Field	Description	Examples
timestamp	Time when the message was generated, in one of two representations: <ul style="list-style-type: none"> MMM-DD HH:MM:SS.MS+/-HH:MM, is the month, day, hour, minute, second and millisecond in local time. The hour and minute that follows the plus sign (+) or minus sign (-) is the offset of the local time zone from Coordinated Universal Time (UTC). YYYY-MM-DDTHH:MM:SS.MSZ is the year, month, day, hour, minute, second and millisecond in UTC. 	Jul 24 17:43:28 is the timestamp expressed as local time in the United States. 2012-07-24T09:17:15.719Z is 9:17 AM UTC on 24 July 2012.
hostname	Name of the host that originally generated the message.	router1
process	Name of the Junos OS process that generated the message.	mgd
processID	UNIX process ID (PID) of the Junos OS process that generated the message.	4153
TAG	Junos OS system log message tag, which uniquely identifies the message.	UI_DBASE_LOGOUT_EVENT
username	Username of the user initiating the event.	"admin"
message-text	English-language description of the event .	set: [system radius-server 1.2.3.4 secret]

Logging of Audit Startup and Shutdown

The audit information logged includes both startup and shutdown events of Junos OS. This in turn identifies the startup and shutdown events of the audit system, which cannot be independently disabled or enabled. For example, if Junos OS is restarted, the audit log contains the following information:

```
Oct 21 17:28:28 2015 yeti eventd[845]: SYSTEM_OPERATIONAL: System is operational
Oct 21 17:25:53 2015 yeti shutdown: reboot by sec-officer:
```

Login and Logout Events Using SSH

System log messages are generated whenever a user successfully or unsuccessfully attempts SSH access. Logout events are also recorded. For example, the following logs are the result of one failed authentication attempt, a successful password authentication attempt followed by a logout, and finally a successful public key authentication attempt:

```
Oct 21 17:30:54 2015 yeti sshd: SSHD_LOGIN_FAILED: Login failed for user 'sec-officer' from host '10.92.232.107'

Oct 21 17:31:11 2015 yeti sshd[1409]: Accepted keyboard-interactive/pam for sec-officer from 10.92.232.107
```

```

port 60216 ssh2
Oct 21 17:31:12 2015 yeti mgd[1414]: UI_AUTH_EVENT: Authenticated user 'sec-officer' at permission level
'j-sec-admin'
Oct 21 17:31:12 2015 yeti mgd[1414]: UI_LOGIN_EVENT: User 'sec-officer' login, class 'j-sec-admin' [1414],
ssh-connection '10.92.232.107 60216 192.168.38.166 22', client-mode 'cli'
Oct 21 17:31:12 2015 yeti mgd[1414]: UI_CMDLINE_READ_LINE: User 'sec-officer', command 'exit '
Oct 21 17:31:12 2015 yeti mgd[1414]: UI_LOGOUT_EVENT: User 'sec-officer' logout
Oct 21 17:31:12 2015 yeti sshd[1409]: Received disconnect from 10.92.232.107: 11: disconnected by user

Oct 21 17:32:05 2015 yeti sshd[2528]: Accepted publickey for syslog-mon from 10.92.232.107 port 59211
ssh2: ECDSA 9f:e3:14:b2:a2:52:3d:92:ad:d7:f6:47:e9:a1:a0:23
Oct 21 17:32:05 2015 yeti sshd[2528]: subsystem request for netconf by user syslog-mon
Oct 21 17:32:05 2015 yeti mgd[2532]: UI_AUTH_EVENT: Authenticated user 'syslog-mon' at permission level
'j-monitor'
Oct 21 17:32:05 2015 yeti mgd[2532]: UI_LOGIN_EVENT: User 'syslog-mon' login, class 'j-monitor' [2532],
ssh-connection '10.92.232.107 59211 192.168.38.166 22', client-mode 'cli'

```

Logging Failure to Establish an SSH Session

System log messages are generated whenever a user attempts to establish an SSH session. For example, the following logs are generated as a result of failure to establish a remote administrator connection over SSH:

```

Jan 20 14:03:24 starfire sshd: SSHD_LOGIN_FAILED: Login failed for user 'sec-admin' from host
'10.209.11.24'

```

Logging Establishment or Termination of an SSH session

System log messages are generated whenever a user successfully or unsuccessfully attempts to establish an SSH session. For example, the following logs are generated when an SSH session has been established:

```

Oct 21 17:31:11 2015 yeti sshd[1409]: Accepted keyboard-interactive/pam for sec-officer from 10.92.232.107
port 60216 ssh2
Oct 21 17:31:12 2015 yeti mgd[1414]: UI_AUTH_EVENT: Authenticated user 'sec-officer' at permission level
'j-sec-admin'
Oct 21 17:31:12 2015 yeti mgd[1414]: UI_LOGIN_EVENT: User 'sec-officer' login, class 'j-sec-admin' [1414],
ssh-connection '10.92.232.107 60216 192.168.38.166 22', client-mode 'cli'
Oct 21 17:31:12 2015 yeti mgd[1414]: UI_CMDLINE_READ_LINE: User 'sec-officer', command 'exit '
Oct 21 17:31:12 2015 yeti mgd[1414]: UI_LOGOUT_EVENT: User 'sec-officer' logout
Oct 21 17:31:12 2015 yeti sshd[1409]: Received disconnect from 10.92.232.107: 11: disconnected by user

Oct 21 17:32:05 2015 yeti sshd[2528]: Accepted publickey for syslog-mon from 10.92.232.107 port 59211
ssh2: ECDSA 9f:e3:14:b2:a2:52:3d:92:ad:d7:f6:47:e9:a1:a0:23
Oct 21 17:32:05 2015 yeti sshd[2528]: subsystem request for netconf by user syslog-mon
Oct 21 17:32:05 2015 yeti mgd[2532]: UI_AUTH_EVENT: Authenticated user 'syslog-mon' at permission level
'j-monitor'
Oct 21 17:32:05 2015 yeti mgd[2532]: UI_LOGIN_EVENT: User 'syslog-mon' login, class 'j-monitor' [2532],
ssh-connection '10.92.232.107 59211 192.168.38.166 22', client-mode 'cli'

```

The following logs are generated when an SSH session has been terminated because the packet size is too large:

```

Oct 2 13:37:32 veo sshd[9387]: Potential replay attack detected on SSH connection initiated from
192.168.38.246:16111
Oct 2 13:37:32 veo sshd[9387]: SSH_MSG_REPLAY_DETECT: Potential replay attack detected on SSH connection
initiated from 192.168.38.246:16111

```

```
Oct  2 13:37:32  veo sshd[9387]: Bad packet length 262172.
Oct  2 13:37:32  veo sshd[9387]: Disconnecting: Packet corrupt
Oct  2 13:37:32  veo inetd[2009]: /usr/sbin/sshd[9387]: exited, status 255
```

The following logs are generated when termination of the SSH session is initiated by the remote endpoint due to timeout of the connection:

```
Aug  6 00:49:55  bm-a sshd[14391]: Received disconnect from 10.209.11.20: 11: disconnected by user
Aug  6 00:49:55  bm-a inetd[1929]: /usr/sbin/sshd[14391]: exited, status 255
Aug  6 00:49:56  bm-a file[14395]: UI_CHILD_STATUS: Cleanup child '/usr/sbin/syslog-filter', PID 14397,
status 0x100
Aug  6 00:49:56  bm-a file[14395]: UI_CHILD_EXITED: Child exited: PID 14397, status 1, command
'/usr/sbin/syslog-filter'
Aug  6 00:49:56  bm-a file[14395]: UI_LOGOUT_EVENT: User 'syslog-mon' logout
```

The following logs are generated when termination of the SSH session is initiated by the remote endpoint due to closure of the connection:

```
Aug  7 12:21:24 2015 bm-a mgd[27304]: UI_LOGOUT_EVENT: User 'regress' logout
Aug  7 12:21:25 2015 bm-a sshd[27298]: Received disconnect from 10.209.11.25: 11: disconnected by user
Aug  7 12:21:25 2015 bm-a inetd[1929]: /usr/sbin/sshd[27298]: exited, status 255
```



NOTE: By default, syslog over NETCONF using SSH is run in continuous mode, so there is no normal termination. NETCONF over SSH supports the option to run syslog with a termination condition. The following logs are generated when the session is terminated as a result of the termination condition:

```
Oct 10 12:02:42 2015 chessie sshd[3467]: Received disconnect from 10.92.232.33: 11: disconnected by user
Oct 10 12:02:42 2015 chessie inetd[1979]: /usr/sbin/sshd[3467]: exited, status 255
Oct 10 12:02:43 2015 chessie file[3470]: UI_CHILD_STATUS: Cleanup child '/usr/sbin/syslog-filter', PID
3472, status 0x100
Oct 10 12:02:43 2015 chessie file[3470]: UI_CHILD_EXITED: Child exited: PID 3472, status 1, command
'/usr/sbin/syslog-filter'
Oct 10 12:02:43 2015 chessie file[3470]: UI_LOGOUT_EVENT: User 'syslog-mon' logout
```

Logging Changes to the System Time

System log messages are generated when the time or date on the NDPP device is changed. For example, the following messages are generated as a result of date change on the Junos OS device:

```
Aug  7 04:32:36 2015 bm-a mgd[26660]: UI_CMDLINE_READ_LINE: User 'regress', command 'set date
20150807120000 '
Aug  7 04:32:44 2015 bm-a mgd[26660]: UI_CMDLINE_READ_LINE: User 'regress', command 'set date
201508071200.00 '
Aug  7 04:32:44 2015 bm-a mgd[26660]: UI_CHILD_START: Starting child '/bin/date'
Aug  7 12:00:00 2015 bm-a date: date set by root
Aug  7 12:00:00 2015 bm-a mgd[26660]: UI_CHILD_STATUS: Cleanup child '/bin/date', PID 27144, status 0x200
```

Logging Initiation of a System Update

System log messages are generated on initiation of a system update. For example, the following messages are generated as a result of a system update on the Junos OS device:

```
Jan 20 17:33:19 starfire mgd[5321]: UI_CMDLINE_READ_LINE: User 'sec-admin', command 'request system
software add jinstall-12.1R4.5-domestic-signed.tgz '
Jan 20 17:33:19 starfire mgd[5321]: /usr/libexec/ui/package -X update
/var/home/sec-admin/jinstall-12.1R4.5-domestic-signed.tgz
Jan 20 17:33:19 starfire mgd[5321]: UI_CHILD_START: Starting child '/usr/libexec/ui/package'
Jan 20 17:33:54 starfire mgd[5321]: UI_CHILD_STATUS: Cleanup child '/usr/libexec/ui/package', PID 5327,
status 0
```

Logging Completion of a TSF Self-Test

System log messages are generated when a TOE Security Functions (TSF) self-test is completed. For example, the following message is generated as a result of successful completion of a TSF self-test:

```
Jan 20 13:38:45 starfire /kernel: mgd: FIPS Self-tests Passed
```

Failure of the TSF self-test will generate system log message in the following format, based on the type of self-test failure:

```
Apr 9 12:59:14 nms5-m10i-a fips-error[13766]: FIPS Error 6: RSA conversion failed
Apr 9 13:00:03 nms5-m10i-a fips-error[13801]: FIPS Error 6: Nitrox RSA public encrypt failed
Apr 9 13:04:42 nms5-m10i-a fips-error[13871]: FIPS Error 1: HMAC-SHA2-512 Known Answer Test: Failed
```

Logging Attempts at Unlocking an Interactive Session

System log messages are generated whenever a user attempts to unlock an interactive session. For example, the following messages are generated as a result of an attempt to unlock an interactive session:

```
Oct 2 09:53:04 veo login[24935]: LOGIN_INFORMATION: User NDPP-admin logged in from host [unknown] on
device ttyu0
Oct 2 09:53:04 veo mgd[24937]: UI_AUTH_EVENT: Authenticated user 'NDPP-admin' at permission level
'j-security-admin'
Oct 2 09:53:04 veo mgd[24937]: UI_LOGIN_EVENT: User 'NDPP-admin' login, class 'j-security-admin' [24937],
ssh-connection '', client-mode 'cli'
Oct 2 09:55:00 veo /usr/sbin/cron[24939]: (root) CMD ( /usr/libexec/atrun)
Oct 2 09:55:04 veo UI_CLI_IDLE_TIMEOUT: Idle timeout for user 'NDPP-admin' exceeded and session terminated
Oct 2 09:55:04 veo mgd[24937]: UI_LOGOUT_EVENT: User 'NDPP-admin' logout
```

Logging Termination of a Remote Session by the Session Locking Mechanism

System log messages are generated whenever a remote session is terminated by the session locking mechanism. For example, the following messages are generated as a result of termination of a remote session by the session locking mechanism:

```
Jul 21 20:22:40 starfire sshd[8216]: Accepted password for sec-admin from 10.209.11.24 port 55535 ssh2
Jul 21 20:22:40 starfire mgd[8220]: UI_AUTH_EVENT: Authenticated user 'sec-admin' at permission level
'j-administrator'
Jul 21 20:22:40 starfire mgd[8220]: UI_LOGIN_EVENT: User 'sec-admin' login, class 'j-administrator'
```

```
[8220], ssh-connection '10.209.11.24 55535 10.209.14.92 22', client-mode 'cli'
```

```
Jul 21 20:32:40 starfire UI_CLI_IDLE_TIMEOUT: Idle timeout for user 'sec-admin' exceeded and session
terminated
Jul 21 20:32:40 starfire mgd[8220]: UI_LOGOUT_EVENT: User 'sec-admin' logout
Jul 21 20:32:40 starfire sshd[8216]: Received disconnect from 10.209.11.24: 11: disconnected by user
```

Logging Termination of an Interactive Session

System log messages are generated whenever an interactive session is terminated. For example, the following log messages display the termination of a local interactive session:

```
Jul 21 20:38:12 starfire login[8424]: LOGIN_INFORMATION: User sec-admin logged in from host [unknown]
on device ttyd0
Jul 21 20:38:13 starfire rshd[8427]: root@re1 as root: cmd='/sbin/sysctl net.inet.ip_control_plane'
Jul 21 20:38:13 starfire mgd[8429]: UI_AUTH_EVENT: Authenticated user 'sec-admin' at permission level
'j-administrator'
Jul 21 20:38:13 starfire mgd[8429]: UI_LOGIN_EVENT: User 'sec-admin' login, class 'j-administrator'
[8429], ssh-connection '', client-mode 'cli'
Jul 21 20:38:19 starfire mgd[8429]: UI_CMDLINE_READ_LINE: User 'sec-admin', command 'show system users
'
Jul 21 20:48:20 starfire UI_CLI_IDLE_TIMEOUT: Idle timeout for user 'sec-admin' exceeded and session
terminated
Jul 21 20:48:20 starfire mgd[8429]: UI_LOGOUT_EVENT: User 'sec-admin' logout
```

The following log messages display the termination of a remote interactive session:

```
Oct 2 10:53:08 veo sshd[25341]: Accepted password for NDPP-admin from 192.168.38.252 port 3254 ssh2
Oct 2 10:53:08 veo mgd[25345]: UI_AUTH_EVENT: Authenticated user 'NDPP-admin' at permission level
'j-security-admin'
Oct 2 10:53:08 veo mgd[25345]: UI_LOGIN_EVENT: User 'NDPP-admin' login, class 'j-security-admin' [25345],
ssh-connection '192.168.38.252 3254 192.168.38.77 22', client-mode 'cli'
Oct 2 10:53:11 veo mgd[25345]: UI_CMDLINE_READ_LINE: User 'NDPP-admin', command 'quit '
Oct 2 10:53:11 veo mgd[25345]: UI_LOGOUT_EVENT: User 'NDPP-admin' logout
```

Logging Initiation of a Trusted Channel

System log messages are generated upon initiation of a trusted channel. For example, the following messages are generated as a result of initiation of a trusted channel:

```
Dec 23 02:01:54 nms5-m10i-a sshd[92615]: Accepted publickey for syslog-mon from 10.209.11.25 port 51142
ssh2
Dec 23 02:01:54 nms5-m10i-a sshd[92615]: subsystem request for netconf by user syslog-mon
Dec 23 02:01:54 nms5-m10i-a mgd[92619]: UI_AUTH_EVENT: Authenticated user 'syslog-mon' at permission
level 'j-monitor'
Dec 23 02:01:54 nms5-m10i-a mgd[92619]: UI_LOGIN_EVENT: User 'syslog-mon' login, class 'j-monitor'
[92619], ssh-connection '10.209.11.25 51142 10.209.10.197 22', client-mode 'cli'
Dec 23 02:01:54 nms5-m10i-a mgd[92619]: UI_CMDLINE_READ_LINE: User 'syslog-mon', command 'xml-mode netconf
need-trailer '
Dec 23 02:01:54 nms5-m10i-a mgd[92619]: UI_LOGOUT_EVENT: User 'syslog-mon' logout
Dec 23 02:01:54 nms5-m10i-a file[92618]: auto-snapshot is not configured
Dec 23 02:01:54 nms5-m10i-a file[92618]: UI_AUTH_EVENT: Authenticated user 'syslog-mon' at permission
level 'j-monitor'
Dec 23 02:01:54 nms5-m10i-a file[92618]: UI_LOGIN_EVENT: User 'syslog-mon' login, class 'j-monitor'
[92618], ssh-connection '10.209.11.25 51142 10.209.10.197 22', client-mode 'netconf'
Dec 23 02:02:25 nms5-m10i-a file[92618]: UI_NETCONF_CMD: User 'syslog-mon' used NETCONF client to run
```

```
command 'get-syslog-events stream=messages'
```

```
Dec 23 02:02:25 nms5-m10i-a file[92618]: UI_CHILD_START: Starting child '/usr/sbin/syslog-filter'
```

Logging Termination of a Trusted Channel

System log messages are generated upon termination of a trusted channel. For example, the following messages are generated when a trusted channel is terminated:

```
Dec 23 02:03:55 nms5-m10i-a sshd[92615]: error: Received disconnect from 10.209.11.25: 11: disconnected
by user
Dec 23 02:03:55 nms5-m10i-a inetd[1739]: /usr/sbin/sshd[92615]: exited, status 255
Dec 23 02:03:56 nms5-m10i-a file[92618]: UI_CHILD_STATUS: Cleanup child '/usr/sbin/syslog-filter', PID
92626, status 0x100
Dec 23 02:03:56 nms5-m10i-a file[92618]: UI_CHILD_EXITED: Child exited: PID 92626, status 1, command
'/usr/sbin/syslog-filter'
Dec 23 02:03:56 nms5-m10i-a file[92618]: UI_LOGOUT_EVENT: User 'syslog-mon' logout
```

Logging Failure of Trusted Channel or Trusted Path Functions

System log messages are generated whenever the functions of a trusted channel or a trusted path fail. For example, the following messages are generated upon failure of functions of a trusted channel:

```
Dec 23 02:14:50 nms5-m10i-a inetd[1739]: /usr/sbin/sshd[92655]: exited, status 255
Dec 23 02:14:51 nms5-m10i-a file[92658]: UI_CHILD_STATUS: Cleanup child '/usr/sbin/syslog-filter', PID
92660, status 0x100
Dec 23 02:14:51 nms5-m10i-a file[92658]: UI_CHILD_EXITED: Child exited: PID 92660, status 1, command
'/usr/sbin/syslog-filter'
Dec 23 02:14:51 nms5-m10i-a file[92658]: UI_LOGOUT_EVENT: User 'syslog-mon' logout
```

```
Jan 20 17:16:53 starfire sshd[4731]: Accepted publickey for syslog-mon from 10.209.11.24 port 55572
ssh2
Jan 20 17:16:53 starfire sshd[4731]: subsystem request for netconf by user syslog-mon
Jan 20 17:16:53 starfire sshd[4731]: subsystem request for netconf failed, subsystem not found
```

System log messages are also generated upon failure to establish trusted connection to the remote syslog server for remote administration over SSH due to SSH protocol failures. For example, the following message is generated as a result of protocol version mismatch:

```
Aug 6 03:38:44 bm-a sshd[16251]: Did not receive identification string from 10.209.11.20
```

The following message is generated as a result of cipher mismatch between client and server:

```
Aug 6 03:40:03 bm-a sshd[16265]: fatal: no matching cipher found: client 3des-cbc server
aes128-cbc,aes256-cbc [preauth]
```

The following message is generated as a result of mac algorithm mismatch:

```
Aug 6 03:42:22 bm-a sshd[16282]: fatal: no matching mac found: client hmac-md5 server
hmac-sha1,hmac-sha2-256,hmac-sha2-512 [preauth]
```

The following message is generated as a result of SSH hostkey mismatch:

```
Aug 6 03:46:22 bm-a sshd[16315]: fatal: no hostkey alg [preauth]
```

The following message is generated as a result of SSH key-exchange mismatch:

```
Aug  6 03:47:55  bm-a sshd[16326]: fatal: Unable to negotiate a key exchange method [preauth]
```

System Log Messages

Descriptions of system log messages are in the [Junos OS System Log Messages Reference](#). Additionally, you might encounter the following messages.

SSHD_LOGIN_FAILED

System Log Message	Login failed for user ' <i>username</i> ' from host ' <i>source-address</i> '
Description	A login attempt failed for the indicated username.
Type	Event: This message reports an event, not an error
Severity	notice
Facility	ANY

UI_AUTH_EVENT

System Log Message	Authenticated user ' <i>username</i> ' at permission level ' <i>authentication-level</i> '
Description	The management process (mgd) authenticated the indicated user.
Type	Event: This message reports an event, not an error
Severity	info
Facility	LOG_AUTH

UI_CFG_AUDIT_OTHER

System Log Message	User ' <i>username</i> ' action: <i>pathname delimitervalue</i>
Description	The indicated user deleted, activated, or deactivated a configuration object, as indicated. The Junos OS configuration log facility logged the change.
Type	Event: This message reports an event, not an error
Severity	info
Facility	ANY

UI_CLI_IDLE_TIMEOUT

System Log Message	Idle timeout for user ' <i>username</i> ' exceeded and session terminated
Description	The indicated user's session was ended after a period of prolonged inactivity.
Type	Event: This message reports an event, not an error
Severity	info
Facility	LOG_USER

UI_CMDLINE_READ_LINE

System Log Message	User ' <i>username</i> ', command ' <i>command</i> '
Description	The indicated user typed the indicated command at the CLI prompt and pressed the Enter key, sending the command string to the management process (mgd).
Type	Event: This message reports an event, not an error
Severity	info
Facility	LOG_AUTH

UI_LOGIN_EVENT

System Log Message	User ' <i>username</i> ' login, class ' <i>class-name</i> ' <i>local-peer[pid]</i> , ssh-connection ' <i>ssh-connection</i> ', client-mode ' <i>client-mode</i> '
Description	The indicated user started a Junos OS CLI session.
Type	Event: This message reports an event, not an error
Severity	info
Facility	ANY

UI_LOGOUT_EVENT

System Log Message	User ' <i>username</i> ' logout
Description	The indicated user exited from a Junos OS CLI session.
Type	Event: This message reports an event, not an error
Severity	info
Facility	ANY

PART 5

Index

- [Index on page 53](#)

Index

Symbols

#, comments in configuration statements.....	xv
(), in syntax descriptions.....	xv
< >, in syntax descriptions.....	xiv
[], in configuration statements.....	xv
{ }, in configuration statements.....	xv
(pipe), in syntax descriptions.....	xv

B

braces, in configuration statements.....	xv
brackets	
angle, in syntax descriptions.....	xiv
square, in configuration statements.....	xv

C

CLI	
date	
setting.....	34
comments, in configuration statements.....	xv
Common Criteria	
local file logging.....	28
remote server logging.....	28
user types.....	19
Common Criteria Recognition Arrangement	
CCRA.....	3
conventions	
text and syntax.....	xiv
curly braces, in configuration statements.....	xv
customer support.....	xvi
contacting JTAC.....	xvi

D

date	
setting from CLI.....	34
date and time	
setting locally.....	32
documentation	
comments on.....	xv

E

EAL.....	
----------	--

ECC.....	
ECDH.....	
ECDSA.....	
event logging	
overview.....	27

F

FIPS.....	
font conventions.....	xiv

I

idle-timeout statement.....	26
-----------------------------	----

L

logging	
audit startup.....	42
interactive session	
terminate.....	46
unlock.....	45
login and logout events.....	42
remote session.....	45
self-test.....	45
ssh session	
failure.....	43
terminate, establish.....	43
time.....	44
to local file.....	28
to remote server.....	28
trusted channel	
failure.....	47
initiation.....	46
terminate.....	47
trusted path	
failure.....	47
update.....	45
logging out.....	42

M

manuals	
comments on.....	xv
message statement.....	23

P

parentheses, in syntax descriptions.....	xv
--	----

S

set date command.....	32, 34
SSH service	
configuring.....	16

ssh statement	
usage guidelines.....	16
support, technical See technical support	
syntax conventions.....	xiv
system services	
SSH.....	16

T

technical support	
contacting JTAC.....	xvi
terms.....	
time-format statement.....	33
TOE.....	

U

users	
types in Common Criteria.....	19