



Junos[®] OS

System Basics: User Access and Authentication Configuration Guide

Release
12.3



Published: 2012-12-06

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

This product includes the Envoy SNMP Engine, developed by Epilogue Technology, an Integrated Systems Company. Copyright © 1986-1997, Epilogue Technology Corporation. All rights reserved. This program and its documentation were developed at private expense, and no part of them is in the public domain.

This product includes memory allocation software developed by Mark Moraes, copyright © 1988, 1989, 1993, University of Toronto.

This product includes FreeBSD software developed by the University of California, Berkeley, and its contributors. All of the documentation and software included in the 4.4BSD and 4.4BSD-Lite Releases is copyrighted by the Regents of the University of California. Copyright © 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994. The Regents of the University of California. All rights reserved.

GateD software copyright © 1995, the Regents of the University. All rights reserved. Gate Daemon was originated and developed through release 3.0 by Cornell University and its collaborators. Gated is based on Kirton's EGP, UC Berkeley's routing daemon (routed), and DCN's HELLO routing protocol. Development of Gated has been supported in part by the National Science Foundation. Portions of the GateD software copyright © 1988, Regents of the University of California. All rights reserved. Portions of the GateD software copyright © 1991, D. L. S. Associates.

This product includes software developed by Maker Communications, Inc., copyright © 1996, 1997, Maker Communications, Inc.

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.

Products made or sold by Juniper Networks or components thereof might be covered by one or more of the following patents that are owned by or licensed to Juniper Networks: U.S. Patent Nos. 5,473,599, 5,905,725, 5,909,440, 6,192,051, 6,333,650, 6,359,479, 6,406,312, 6,429,706, 6,459,579, 6,493,347, 6,538,518, 6,538,899, 6,552,918, 6,567,902, 6,578,186, and 6,590,785.

Junos® OS System Basics: User Access and Authentication Configuration Guide

12.3

Copyright © 2012, 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.

Table of Contents

	About the Documentation	ix
	Documentation and Release Notes	ix
	Supported Platforms	ix
	Using the Examples in This Manual	ix
	Merging a Full Example	x
	Merging a Snippet	x
	Documentation Conventions	xi
	Documentation Feedback	xiii
	Requesting Technical Support	xiii
	Self-Help Online Tools and Resources	xiii
	Opening a Case with JTAC	xiv
Part 1	Overview	
Chapter 1	User Access Overview	3
	Junos OS Login Classes Overview	3
	Junos OS User Accounts Overview	4
	Junos-FIPS Crypto Officer and User Accounts Overview	6
	Crypto Officer User Configuration	6
	FIPS User Configuration	6
	Understanding Junos OS Access Privilege Levels	7
	Junos OS Login Class Permission Flags	7
	Allowing or Denying Individual Commands for Junos OS Login Classes	10
	Using Regular Expressions on a RADIUS or TACACS+ Server to Allow or Deny Access to Commands	11
	Junos OS Authentication Order for RADIUS, TACACS+, and Password Authentication	13
	Using RADIUS or TACACS+ Authentication	14
	Using Local Password Authentication	14
	Order of Authentication Attempts	15
Chapter 2	User Authentication Overview	19
	Junos OS User Authentication Methods	19
	Special Requirements for Junos OS Plain-Text Passwords	20
	Overview of Template Accounts for RADIUS and TACACS+ Authentication	22
	Junos OS Authentication Methods for Routing Protocols	22
Part 2	Configuration	
Chapter 3	Configuring User Access	27
	Defining Junos OS Login Classes	28
	Configuring Junos OS User Accounts	28

	Limiting the Number of User Login Attempts for SSH and Telnet Sessions	29
	Configuring Time-Based User Access	30
	Configuring Access Privilege Levels	31
	Specifying Access Privileges for Junos OS Operational Mode Commands	32
	Regular Expressions for Allowing and Denying Junos OS Operational Mode Commands	33
	Specifying Access Privileges for Junos OS Configuration Mode Hierarchies	34
	Regular Expressions for Allowing and Denying Junos OS Configuration Mode Hierarchies	35
	Example: Specifying Access Privileges Using allow/deny-configuration-regexps Statements	36
	Specifying Access Privileges Using allow/deny-configuration Statements	40
	Defining Access Privileges Using allow/deny-configuration Statements	42
	Configuring the Timeout Value for Idle Login Sessions	43
	Example: Creating Login Classes with Specific Privileges	43
	Configuring Remote Template Accounts for User Authentication	44
	Configuring Local User Template Accounts for User Authentication	44
	Configuring the Junos OS Authentication Order for RADIUS, TACACS+, and Local Password Authentication	46
	Using Junos OS to Configure Logical System Administrators	47
	Configuring the Junos OS to Display a System Login Message	48
	Configuring the Junos OS to Display a System Login Announcement	49
	Configuring System Alarms to Appear Automatically Upon Login	50
	System Alarms on J Series Routers	50
Chapter 4	Configuring RADIUS and TACACS+ System Authentication	53
	Configuring RADIUS Authentication	53
	Configuring RADIUS Server Details	53
	Configuring MS-CHAPv2 for Password-Change Support	54
	Specifying a Source Address for the Junos OS to Access External RADIUS Servers	55
	Example: Configuring RADIUS Authentication	56
	Example: Configuring RADIUS Template Accounts	57
	Juniper Networks Vendor-Specific RADIUS Attributes	57
	Configuring TACACS+ Authentication	59
	Configuring TACACS+ Server Details	60
	Specifying a Source Address for the Junos OS to Access External TACACS+ Servers	61
	Configuring the Same Authentication Service for Multiple TACACS+ Servers	61
	Configuring Juniper Networks Vendor-Specific TACACS+ Attributes	62
	Juniper Networks Vendor-Specific TACACS+ Attributes	62
	Configuring RADIUS System Accounting	63
	Configuring Auditing of User Events on a RADIUS Server	64
	Specifying RADIUS Server Accounting and Auditing Events	64
	Configuring RADIUS Server Accounting	64
	Example: Configuring RADIUS System Accounting	65

	Configuring TACACS+ System Accounting	66
	Specifying TACACS+ Auditing and Accounting Events	66
	Configuring TACACS+ Server Accounting	67
	Configuring TACACS+ Accounting on a TX Matrix Router	68
	Example: Configuring System Authentication for RADIUS, TACACS+, and Password Authentication	68
Chapter 5	Examples	71
	Example: Configuring User Login Accounts	71
	Example: Configuring User Accounts	72
	Example: Limiting the Number of Login Attempts for SSH and Telnet Sessions	73
	Examples: Configuring Time-Based User Access	73
	Example: Configuring Access Privilege Levels	74
	Example: Configuring Access Privileges for Operational Mode Commands	75
	Example: Configuring the BGP and IS-IS Routing Protocols	75
	Configuring BGP	76
	Configuring IS-IS	77
	Recovering the Root Password	77
Chapter 6	Configuration Statements	81
	System Management Configuration Statements	81
	accounting	88
	access-end	89
	access-start	89
	accounting-port (RADIUS Server)	90
	allow-commands	90
	allow-configuration	91
	allow-configuration-regexps	92
	allowed-days	92
	authentication (Login)	93
	authentication-order	94
	backoff-factor	95
	backoff-threshold	95
	change-type	96
	class (Assigning a Class to an Individual User)	96
	class (Defining Login Classes)	97
	deny-commands	98
	deny-configuration	99
	deny-configuration-regexps	100
	destination (Accounting)	101
	dynamic-profile-options	102
	format	102
	full-name	103
	idle-timeout (System-Login)	103
	load-key-file	104
	login	105
	login-alarms	106
	login-script (Login)	106
	maximum-length	107

	maximum-time	108
	minimum-changes	109
	minimum-length	110
	minimum-lower-cases	111
	minimum-numeric	112
	minimum-punctuations	113
	minimum-time	114
	minimum-upper-cases	115
	password (Login)	116
	permissions	117
	port (RADIUS Server)	117
	port (TACACS+ Server)	118
	radius (System)	119
	radius-options (edit system)	120
	radius-server (System)	121
	retry (RADIUS)	122
	retry-options	123
	secret	124
	server (RADIUS Accounting)	125
	server (TACACS+ Accounting)	125
	single-connection	126
	source-address (NTP, RADIUS, System Logging, or TACACS+)	127
	source-port (Port Addresses)	128
	system	128
	tacplus	129
	tacplus-options	130
	tacplus-server	131
	timeout (System)	132
	tries-before-disconnect	132
	uid	133
	user (Access)	134
	versioning	134
Part 3	Administration	
Chapter 7	Routine Monitoring	137
	show system users	138
	test access profile	142
	test access radius-server	146
Part 4	Index	
	Index	151

List of Tables

	About the Documentation	ix
	Table 1: Notice Icons	xi
	Table 2: Text and Syntax Conventions	xi
Part 1	Overview	
Chapter 1	User Access Overview	3
	Table 3: Predefined System Login Classes	3
	Table 4: Login Class Permission Flags	7
	Table 5: Order of Authentication Attempts	15
Chapter 2	User Authentication Overview	19
	Table 6: Special Requirements for Plain-Text Passwords	20
Part 2	Configuration	
Chapter 3	Configuring User Access	27
	Table 7: Common Regular Expression Operators to Allow or Deny Operational Mode Commands	33
	Table 8: Configuration Mode Hierarchies—Common Regular Expression Operators	35
	Table 9: System Alarms on J Series Routers	50
Chapter 4	Configuring RADIUS and TACACS+ System Authentication	53
	Table 10: Juniper Networks Vendor-Specific RADIUS Attributes	57
	Table 11: Juniper Networks Vendor-Specific TACACS+ Attributes	62
Part 3	Administration	
Chapter 7	Routine Monitoring	137
	Table 12: show system users Output Fields	139
	Table 13: test access profile Output Fields	142
	Table 14: test access radius-server Output Fields	146

About the Documentation

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

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, the following platforms are supported:

- M Series
- MX Series
- T Series
- J Series
- PTX Series

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 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.

Table 2 on page xi 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

Table 2: Text and Syntax Conventions (*continued*)

Convention	Description	Examples
<i>Italic text like this</i>	<ul style="list-style-type: none"> Introduces or emphasizes important new terms. Identifies book 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 System Basics Configuration 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)	Enclose 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 <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)	Enclose a variable for which you can substitute one or more values.	community name members [community-ids]
Indentation and braces ({ })	Identify a level in the configuration hierarchy.	[edit] routing-options { static { route default { nexthop <i>address</i> ; retain; } } }
;(semicolon)	Identifies a leaf statement at a configuration hierarchy level.	
J-Web GUI Conventions		
Bold text like this	Represents J-Web 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 J-Web 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 send your comments to techpubs-comments@juniper.net, or fill out the documentation feedback form at <https://www.juniper.net/cgi-bin/docbugreport/>. If you are using e-mail, be sure to include the following information with your comments:

- Document or topic name
- URL or page number
- Software release 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 JNASC 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: <https://www.juniper.net/alerts/>

- 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

Overview

- [User Access Overview on page 3](#)
- [User Authentication Overview on page 19](#)

CHAPTER 1

User Access Overview

- [Junos OS Login Classes Overview on page 3](#)
- [Junos OS User Accounts Overview on page 4](#)
- [Junos-FIPS Crypto Officer and User Accounts Overview on page 6](#)
- [Understanding Junos OS Access Privilege Levels on page 7](#)
- [Using Regular Expressions on a RADIUS or TACACS+ Server to Allow or Deny Access to Commands on page 11](#)
- [Junos OS Authentication Order for RADIUS, TACACS+, and Password Authentication on page 13](#)

Junos OS Login Classes Overview

All users who can log in to the router or switch must be in a login class. With login classes, you define the following:

- Access privileges that users have when they are logged in to the router or switch
- Commands and statements that users can and cannot specify
- How long a login session can be idle before it times out and the user is logged out

You can define any number of login classes and then apply one login class to an individual user account.

The Junos OS contains a few predefined login classes, which are listed in [Table 3 on page 3](#). The predefined login classes cannot be modified.

Table 3: Predefined System Login Classes

Login Class	Permission Flag Set
operator	clear, network, reset, trace, and view
read-only	view
superuser or super-user	all
unauthorized	None



NOTE:

- You cannot modify a predefined login class name. If you issue the `set` command on a predefined class name, the Junos OS appends `-local` to the login class name. The following message also appears:

warning: '<class-name>' is a predefined class name; changing to
'<class-name>-local'

- You cannot issue the `rename` or `copy` command on a predefined login class. Doing so results in the following error message:

error: target '<class-name>' is a predefined class

**Related
Documentation**

- [Defining Junos OS Login Classes on page 28](#)
- [Defining Junos OS Login Classes](#)
- [Understanding QFabric System Login Classes](#)

Junos OS User Accounts Overview

User accounts provide one way for users to access the router. (Users can access the router without accounts if you configured RADIUS or TACACS+ servers, as described in [“Junos OS User Authentication Methods” on page 19](#).) For each account, you define the login name for the user and, optionally, information that identifies the user. After you have created an account, the software creates a home directory for the user.

For each user account, you can define the following:

- **Username**—Name that identifies the user. It must be unique within the router. Do not include spaces, colons, or commas in the username. The username can be up to 64 characters long.
- **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 must be unique within the router. If you do not assign a UID to a username, the software assigns one when you commit the configuration, preferring the lowest available number.

You must ensure that the UID is unique. However, it is possible to assign the same UID to different users. If you do this, the CLI displays a warning when you commit the configuration and then assigns the duplicate UID.

- **User's access privilege**—(Required) One of the login classes you defined in the `class` statement at the `[edit system login]` hierarchy level, or one of the default classes listed in [“Regular Expressions for Allowing and Denying Junos OS Configuration Mode Hierarchies” on page 35](#).

- Authentication method or methods and passwords that the user can use to access the router—(Optional) You can use SSH or a Message Digest 5 (MD5) password, or you can enter a plain-text password that the Junos OS encrypts using MD5-style encryption before entering it in the password database. For each method, you can specify the user's password. If you configure the **plain-text-password** option, you are prompted to enter and confirm the password:

```
[edit system login user username]
user@host# set authentication plain-text-password
New password: type password here
Retype new password: retype password here
```

The default requirements for plain-text passwords are:

- The password must be between 6 and 128 characters long.
- You can include most character classes in a password (uppercase letters, lowercase letters, numbers, punctuation marks, and other special characters). Control characters are not recommended.
- Valid passwords must contain at least one change of case or character class.

Junos-FIPS and Common Criteria have special password requirements. FIPS and Common Criteria passwords must be between 10 and 20 characters in length. Passwords must use at least three of the five defined character sets (uppercase letters, lowercase letters, digits, punctuation marks, and other special characters). If Junos-FIPS is installed on the router, you cannot configure passwords unless they meet this standard.

For SSH authentication, you can copy the contents of an SSH key file into the configuration or directly configure SSH key information. Use the **load-key-file** *URL filename* command to load an SSH key file that was previously generated, e.g. by using **ssh-keygen**. The *URL filename* is the path to the file's location and name. This command loads RSA (SSH version 1 and SSH version 2) and DSA (SSH version 2) public keys. The contents of the SSH key file are copied into the configuration immediately after you enter the **load-key-file** statement. Optionally, you can use the **ssh-dsa public key <from hostname>** and the **ssh-rsa public key <from hostname>** statements to directly configure SSH keys.

For each user account and for root logins, you can configure more than one public RSA or DSA key for user authentication. When a user logs in using a user account or as root, the configured public keys are referenced to determine whether the private key matches any of them.

To view the SSH keys entries, use the configuration mode **show** command. For example:

```
[edit system login user boojum]
user@host# set authentication load-key-file my-host::ssh/id_dsa.pub
.file.19692 | 0 KB | 0.3 kB/s | ETA: 00:00:00 | 100%
[edit system]
user@host# show
root-authentication {
  ssh-rsa "1024 35 9727638204084251055468226757249864241630322
207404962528390382038690141584534964170019610608358722961563
475784918273603361276441874265946893207739108344813125957722
```

```
625461667999278316123500438660915866283822489746732605661192
181489539813862940327687806538169602027491641637359132693963
44008443 boojum@juniper.net"; # SECRET-DATA
}
```

An account for the user **root** is always present in the configuration. You configure the password for **root** using the root-authentication statement, as described in [Configuring the Root Password](#).

- Related Documentation**
- [Configuring Junos OS User Accounts on page 28](#)
 - [Junos OS Login Classes Overview on page 3](#)

Junos-FIPS Crypto Officer and User Accounts Overview

Junos-FIPS defines a restricted set of user roles. Unlike the Junos OS, which enables a wide range of capabilities to users, FIPS 140-2 defines specific types of users (Crypto Officer, User, and Maintenance). Crypto Officers and FIPS Users perform all FIPS-related configuration tasks and issue all FIPS-related commands. Crypto Officer and FIPS User configurations must follow FIPS 140-2 guidelines. Typically, no user besides a Crypto Officer can perform FIPS-related tasks.

Crypto Officer User Configuration

Junos-FIPS offers finer control of user permissions than those mandated by FIPS 140-2. For FIPS 140-2 conformance, any Junos-FIPS user with the **secret**, **security**, and **maintenance** permission bits set is a Crypto Officer. In most cases, the **super-user** class should be reserved for a Crypto Officer. A FIPS User can be defined as any Junos-FIPS user that does not have the **secret**, **security**, and **maintenance** bits set.

FIPS User Configuration

A Crypto Officer sets up FIPS Users. FIPS Users can be granted permissions normally reserved for a Crypto Officer; for example, permission to zeroize the system and individual AS-II FIPS PICs.

- Related Documentation**
- [Junos OS User Accounts Overview on page 4](#)

Understanding Junos OS Access Privilege Levels

Each top-level command-line interface (CLI) command and each configuration statement have an access privilege level associated with them. Users can execute only those commands and configure and view only those statements for which they have access privileges. The access privileges for each login class are defined by one or more *permission flags*.

For each login class, you can explicitly deny or allow the use of operational and configuration mode commands that would otherwise be permitted or not allowed by a privilege level specified in the **permissions** statement.

The following sections provide additional information about permissions:

- [Junos OS Login Class Permission Flags on page 7](#)
- [Allowing or Denying Individual Commands for Junos OS Login Classes on page 10](#)

Junos OS Login Class Permission Flags

The **permissions** statement specifies one or more of the permission flags listed in [Table 4 on page 7](#). Permission flags are not cumulative, so for each class you must list all the permission flags needed, including **view** to display information and **configure** to enter configuration mode. Two forms of permissions control for individual parts of the configuration are:

- "Plain" form—Provides read-only capability for that permission type. An example is **interface**.
- Form that ends in **-control**—Provides read and write capability for that permission type. An example is **interface-control**.

[Table 4 on page 7](#) lists the Junos[®] operating system (Junos OS) login class permission flags that you can configure by including the **permissions** statement at the **[edit system login class *class-name*]** hierarchy level.

Table 4: Login Class Permission Flags

Permission Flag	Description
access	Can view the access configuration in configuration mode and with the show configuration operational mode command.
access-control	Can view and configure access information at the [edit access] hierarchy level.
admin	Can view user account information in configuration mode and with the show configuration operational mode command.
admin-control	Can view user accounts and configure them at the [edit system login] hierarchy level.

Table 4: Login Class Permission Flags (*continued*)

Permission Flag	Description
all-control	Can access all operational mode commands and configuration mode commands. Can modify configuration in all the configuration hierarchy levels.
clear	Can clear (delete) information learned from the network that is stored in various network databases by using the clear commands.
configure	Can enter configuration mode by using the configure command.
control	Can perform all control-level operations—all operations configured with the -control permission flags.
field	Can view field debug commands. Reserved for debugging support.
firewall	Can view the firewall filter configuration in configuration mode.
firewall-control	Can view and configure firewall filter information at the [edit firewall] hierarchy level.
floppy	Can read from and write to the removable media.
flow-tap	Can view the flow-tap configuration in configuration mode.
flow-tap-control	Can view the flow-tap configuration in configuration mode and can configure flow-tap configuration information at the [edit services flow-tap] hierarchy level.
flow-tap-operation	<p>Can make flow-tap requests to the router or switch. For example, a Dynamic Tasking Control Protocol (DTCP) client must authenticate itself to the Junos OS as an administrative user. That account must have flow-tap-operation permission.</p> <p>NOTE: The flow-tap-operation option is not included in the all-control permissions flag.</p>
idp-profiler-operation	Can view profiler data.
interface	Can view the interface configuration in configuration mode and with the show configuration operational mode command.

Table 4: Login Class Permission Flags (*continued*)

Permission Flag	Description
interface-control	Can view chassis, class of service (CoS), groups, forwarding options, and interfaces configuration information. Can edit configuration at the following hierarchy levels: <ul style="list-style-type: none"> • [edit chassis] • [edit class-of-service] • [edit groups] • [edit forwarding-options] • [edit interfaces]
maintenance	Can perform system maintenance, including starting a local shell on the router and becoming the superuser in the shell by using the su root command, and can halt and reboot the router by using the request system commands.
network	Can access the network by using the ping , ssh , telnet , and traceroute commands.
pgcp-session-mirroring	Can view the pgcp session mirroring configuration.
pgcp-session-mirroring-control	Can modify the pgcp session mirroring configuration.
reset	Can restart software processes by using the restart command and can configure whether software processes are enabled or disabled at the [edit system processes] hierarchy level.
rollback	Can use the rollback command to return to a previously committed configuration other than the most recently committed one.
routing	Can view general routing, routing protocol, and routing policy configuration information in configuration and operational modes.
routing-control	Can view general routing, routing protocol, and routing policy configuration information and can configure general routing at the [edit routing-options] hierarchy level, routing protocols at the [edit protocols] hierarchy level, and routing policy at the [edit policy-options] hierarchy level.
secret	Can view passwords and other authentication keys in the configuration.
secret-control	Can view passwords and other authentication keys in the configuration and can modify them in configuration mode.
security	Can view security configuration in configuration mode and with the show configuration operational mode command.

Table 4: Login Class Permission Flags (*continued*)

Permission Flag	Description
security-control	Can view and configure security information at the [edit security] hierarchy level.
shell	Can start a local shell on the router or switch by using the start shell command.
snmp	Can view Simple Network Management Protocol (SNMP) configuration information in configuration and operational modes.
snmp-control	Can view SNMP configuration information and can modify SNMP configuration at the [edit snmp] hierarchy level.
system	Can view system-level information in configuration and operational modes.
system-control	Can view system-level configuration information and configure it at the [edit system] hierarchy level.
trace	Can view trace file settings and configure trace file properties.
trace-control	Can modify trace file settings and configure trace file properties.
view	Can use various commands to display current system-wide, routing table, and protocol-specific values and statistics. Cannot view the secret configuration.
view-configuration	Can view all of the configuration excluding secrets, system scripts, and event options. NOTE: Only users with the maintenance permission can view commit script, op script, or event script configuration.

Allowing or Denying Individual Commands for Junos OS Login Classes

By default, all top-level CLI commands have associated access privilege levels. Users can execute only those commands and view only those statements for which they have access privileges. For each login class, you can explicitly deny or allow the use of operational and configuration mode commands that would otherwise be permitted or not allowed by a privilege level specified in the **permissions** statement.

- The **all** login class permission bits take precedence over extended regular expressions when a user with **rollback** permission issues the **rollback** command.
- Expressions used to allow and deny commands for users on RADIUS and TACACS+ servers have been simplified. Instead of a single, long expression with multiple commands (**allow-commands=cmd1 cmd2 ... cmdn**), you can specify each command as a separate expression. This new syntax is valid for **allow-configuration-regexps** and

deny-configuration-regexps, **allow-commands** and **deny-commands**, and all user permission bits.

- Users cannot issue the **load override** command when specifying an extended regular expression. Users can only issue the **merge**, **replace**, and **patch** configuration commands.
- If you allow and deny the same commands, the **allow-commands** permissions take precedence over the permissions specified by the **deny-commands**. For example, if you include **allow-commands** "request system software add" and **deny-commands** "request system software add", the login class user is allowed to install software using the **request system software add** command.
- Regular expressions for **allow-commands** and **deny-commands** can also include the **commit**, **load**, **rollback**, **save**, **status**, and **update** commands.
- If you specify a regular expression for **allow-commands** and **deny-commands** with two different variants of a command, the longest match is always executed.

For example, if you specify a regular expression for **allow-commands** with the **commit-synchronize** command and a regular expression for **deny-commands** with the **commit** command, users assigned to such a login class would be able to issue the **commit synchronize** command, but not the **commit** command. This is because **commit-synchronize** is the longest match between **commit** and **commit-synchronize** and it is specified for **allow-commands**.

Likewise, if you specify a regular expression for **allow-commands** with the **commit** command and a regular expression for **deny-commands** with the **commit-synchronize** command, users assigned to such a login class would be able to issue the **commit** command, but not the **commit-synchronize** command. This is because **commit-synchronize** is the longest match between **commit** and **commit-synchronize** and it is specified for **deny-commands**.

Related Documentation

- [Configuring Access Privilege Levels on page 31](#)

Using Regular Expressions on a RADIUS or TACACS+ Server to Allow or Deny Access to Commands

Use regular expressions to specify which operational or configuration mode commands are allowed or denied when you use a RADIUS or TACACS+ server for user authentication. You can specify the regular expressions using the appropriate Juniper Networks vendor-specific RADIUS or TACACS+ attributes in your authentication server configuration.

You can specify **allow-configuration**, **deny-configuration**, **allow-commands**, or **deny-commands** in a single extended regular expression, enclosing multiple commands in parentheses and separating them using the pipe symbol. For example, you can specify multiple **allow-commands** parameters using: **allow-commands= (cmd1 | cmd2 | cmdn)**. You can specify **user-permissions** as a list of comma-separated values, and not as a regular expression.

On a RADIUS or TACACS+ server, you can also use a simplified version for regular expressions where you specify each individual expression on a separate line. The simplified

version is valid for **allow-commands**, **deny-commands**, **allow-configuration**, **deny-configuration**, and **permissions** vendor-specific attributes.

For a RADIUS server, specify the individual regular expressions using the following syntax:

```
Juniper-Allow-Commands+= "cmd1"  
Juniper-Allow-Commands+= "cmd2"  
Juniper-Allow-Commands+= "cmdn"  
Juniper-Deny-Commands+= "cmd1"  
Juniper-Deny-Commands+= "cmd2"  
Juniper-Deny-Commands+= "cmdn"  
Juniper-Allow-Configuration+= "regex1"  
Juniper-Allow-Configuration+= "regex2"  
Juniper-Allow-Configuration+= "regexn"  
Juniper-Deny-Configuration+= "regex1"  
Juniper-Deny-Configuration+= "regex2"  
Juniper-Deny-Configuration+= "regexn"  
Juniper-User-Permissions+= "permission-flag1"  
Juniper-User-Permissions+= "permission-flag2"  
Juniper-User-Permissions+= "permission-flagn"
```

For a TACACS+ server, specify the individual regular expressions using the following syntax:

```
allow-commands1="cmd1"  
allow-commands2="cmd2"  
allow-commandsn="cmdn"  
deny-commands1="cmd1"  
deny-commands2="cmd2"  
deny-commandsn="cmdn"  
allow-configuration1="regex1"  
allow-configuration2="regex2"  
allow-configurationn="regexn"  
deny-configuration1="regex1"  
deny-configuration2="regex2"  
deny-configurationn="regexn"  
user-permissions1="permission-flag1"  
user-permissions2="permission-flag2"  
user-permissionsn="permission-flagn "
```

**NOTE:**

- Numeric values 1 to n in the syntax (for a TACACS+ server) must be unique but need not be sequential. For example, the following syntax is valid:

```
allow-commands1="cmd1"
allow-commands3="cmd3"
allow-commands2="cmd2"
deny-commands3="cmd3"
deny-commands2="cmd2"
deny-commands1="cmd1"
```

- The limit on the number of lines of individual regular expressions is imposed by the TACACS+ or RADIUS server.
- When you issue the `show cli authorization` command, the command output displays the regular expression in a single line, even if you specify each individual expression on a separate line.

For more information about Juniper Networks vendor-specific RADIUS and TACACS+ attributes, see [“Juniper Networks Vendor-Specific RADIUS Attributes” on page 57](#) and [“Juniper Networks Vendor-Specific TACACS+ Attributes” on page 62](#).



NOTE: When RADIUS or TACACS+ authentication is configured for a router, regular expressions configured on the RADIUS or TACACS+ server merge with any regular expressions configured on the local router at the [edit system login class] hierarchy level using the `allow-commands`, `deny-commands`, `allow-configuration`, `deny-configuration`, or `permissions` statements. If the final expression has a syntax error, the overall result is an invalid regular expression.

**Related
Documentation**

- [Junos OS Authentication Order for RADIUS, TACACS+, and Password Authentication on page 13](#)

Junos OS Authentication Order for RADIUS, TACACS+, and Password Authentication

Using the **authentication-order** statement, you can prioritize the order in which the Junos OS tries the different authentication methods when verifying user access to a router or switch.

If the **authentication-order** is remote-server then local, Junos OS will retry the local server if the remote-server is unreachable or has timed out. However, if the remote-server rejects the authentication, Junos OS will not retry the authentication.

If none of the configured authentication methods accept the login credentials and if a reject response is received, the login attempt fails. If no response is received from any configured authentication method, the Junos OS consults local password authentication as a last resort.

Using RADIUS or TACACS+ Authentication

You can configure the Junos OS to be both a RADIUS and TACACS+ authentication client.

If an authentication method included in the **[authentication-order]** statement is not available, or if the authentication is available but returns a reject response, the Junos OS tries the next authentication method included in the **authentication-order** statement.

The RADIUS or TACACS+ server authentication might fail because of the following reasons:

- The authentication method is configured, but the corresponding authentication servers are not configured. For instance, the RADIUS and TACACS+ authentication methods are included in the **authentication-order** statement, but the corresponding RADIUS or TACACS+ servers are not configured at the respective **[edit system radius-server]** and **[edit system tacplus-server]** hierarchy levels.
- The RADIUS or TACACS+ server does not respond within the timeout period configured at the **[edit system radius-server]** or **[edit system tacplus-server]** hierarchy levels.
- The RADIUS or TACACS+ server is not reachable because of a network problem.

The RADIUS or TACACS+ server authentication might return a reject response because of the following reasons:

- The user profiles of users accessing a router or switch might not be configured on the RADIUS or TACACS+ server.
- The user enters incorrect logon credentials.

Using Local Password Authentication

You can explicitly configure the password authentication method or use this method as a fallback mechanism when remote authentication servers fail. The password authentication method consults the local user profiles configured at the **[edit system login]** hierarchy level. Users can log in to a router or switch using their local username and password in the following scenarios:

- The password authentication method (password) is explicitly configured as one of the authentication methods in the **[authentication-order authentication-methods]** statement. In this case, the password authentication method is tried if no previous authentication accepts the logon credentials. This is true whether the previous authentication method fails to respond or returns a reject response because of an incorrect username or password.
- The password authentication method is not explicitly configured as one of the authentication methods in the **authentication-order authentication-methods** statement. In this case, the password authentication method is tried only if all configured authentication methods fail to respond. It is not consulted if any configured authentication method returns a reject response because of an incorrect username or password.

Order of Authentication Attempts

Table 5 on page 15 describes how the **authentication-order** statement at the [edit system] hierarchy level determines the procedure that the Junos OS uses to authenticate users for access to a router or switch.

Table 5: Order of Authentication Attempts

Syntax	Order of Authentication Attempts
authentication-order radius;	<ol style="list-style-type: none"> 1. Try configured RADIUS authentication servers. 2. If RADIUS server is available and authentication is accepted, grant access. 3. If RADIUS server is available but authentication is rejected, deny access. 4. If RADIUS servers are not available, try password authentication. <p>NOTE: If a RADIUS server is available, password authentication is not attempted, because it is not explicitly configured in the authentication order.</p>
authentication-order [radius password];	<ol style="list-style-type: none"> 1. Try configured RADIUS authentication servers. 2. If RADIUS servers fail to respond or return a reject response, try password authentication, because it is explicitly configured in the authentication order.
authentication-order [radius tacplus];	<ol style="list-style-type: none"> 1. Try configured RADIUS authentication servers. 2. If RADIUS server is available and authentication is accepted, grant access. 3. If RADIUS servers fail to respond or return a reject response, try configured TACACS+ servers. 4. If TACACS+ server is available and authentication is accepted, grant access. 5. If TACACS+ server is available but authentication is rejected, deny access. 6. If both RADIUS and TACACS+ servers are not available, try password authentication. <p>NOTE: If either RADIUS or TACACS+ servers are available, password authentication is not attempted, because it is not explicitly configured in the authentication order.</p>

Table 5: Order of Authentication Attempts (*continued*)

Syntax	Order of Authentication Attempts
authentication-order [radius tacplus password];	<ol style="list-style-type: none"> 1. Try configured RADIUS authentication servers. 2. If RADIUS server is available and authentication is accepted, grant access. 3. If RADIUS servers fail to respond or return a reject response, try configured TACACS+ servers. 4. If TACACS+ server is available and authentication is accepted, grant access. 5. If TACACS+ servers fail to respond or return a reject response, try password authentication, because it is explicitly configured in the authentication order.
authentication-order tacplus;	<ol style="list-style-type: none"> 1. Try configured TACACS+ authentication servers. 2. If TACACS+ server is available and authentication is accepted, grant access. 3. If TACACS+ server is available but authentication is rejected, deny access. 4. If TACACS+ servers are not available, try password authentication. <p>NOTE: If a TACACS+ server is available, password authentication is not attempted, because it is not explicitly configured in the authentication order.</p>
authentication-order [tacplus password];	<ol style="list-style-type: none"> 1. Try configured TACACS+ authentication servers. 2. If TACACS+ servers fail to respond or return a reject response, try password authentication, because it is explicitly configured in the authentication order.
authentication-order [tacplus radius];	<ol style="list-style-type: none"> 1. Try configured TACACS+ authentication servers. 2. If TACACS+ server is available and authentication is accepted, grant access. 3. If TACACS+ servers fail to respond or return a reject response, try configured RADIUS servers. 4. If RADIUS server is available and authentication is accepted, grant access. 5. If RADIUS server is available but authentication is rejected, deny access. 6. If both TACACS+ and RADIUS servers are not available, try password authentication. <p>NOTE: If either TACACS+ or RADIUS servers are available, password authentication is not attempted, because it is not explicitly configured in the authentication order.</p>

Table 5: Order of Authentication Attempts (*continued*)

Syntax	Order of Authentication Attempts
<code>authentication-order [tacplus radius password];</code>	<ol style="list-style-type: none"> 1. Try configured TACACS+ authentication servers. 2. If TACACS+ server is available and authentication is accepted, grant access. 3. If TACACS+ servers fail to respond or return a reject response, try configured RADIUS servers. 4. If RADIUS server is available and authentication is accepted, grant access. 5. If RADIUS servers fail to respond or return a reject response try password authentication, because it is explicitly configured in the authentication order.
<code>authentication-order password;</code>	<ol style="list-style-type: none"> 1. Try to authenticate the user, using the password configured at the <code>[edit system login]</code> hierarchy level. 2. If the authentication is accepted, grant access. 3. If the authentication is rejected, deny access.



NOTE: If SSH public keys are configured, SSH user authentication first tries to perform public key authentication before using the authentication methods configured in the `authentication-order` statement. If you want SSH logins to use the authentication methods configured in the `authentication-order` statement without first trying to perform public key authentication, do not configure SSH public keys.

In a routing matrix based on a TX Matrix router or a TX Matrix Plus router, the authentication order must be configured only at the configuration groups `re0` and `re1`. The authentication order must not be configured at the `[edit system]` hierarchy on the TX Matrix or TX Matrix Plus router. This is because the authentication order for the routing matrix is controlled on the switch-card chassis (or TX Matrix router) or switch-fabric chassis (or TX Matrix Plus router) only.

In Junos OS Release 10.0 and later, the superuser (belonging to the super-user login class) is also authenticated based on the authentication order that is configured for TACACS+, RADIUS, or password authentication using the `authentication-order` statement. For example, if the only configured authentication order is TACACS+, the superuser can only be authenticated by the TACACS+ server and password authentication cannot be used as an alternative. However, in Junos OS Release 9.6 and earlier, the superuser can use password authentication to login, even if password authentication is not configured explicitly using the `authentication-order` statement.

Related Documentation • [Overview of Template Accounts for RADIUS and TACACS+ Authentication on page 22](#)

- [Configuring the Junos OS Authentication Order for RADIUS, TACACS+, and Local Password Authentication on page 46](#)
- [Limiting the Number of User Login Attempts for SSH and Telnet Sessions on page 29](#)
- [Limiting the Number of User Login Attempts for SSH and Telnet Sessions](#)
- [Example: Configuring System Authentication for RADIUS, TACACS+, and Password Authentication on page 68](#)

CHAPTER 2

User Authentication Overview

- [Junos OS User Authentication Methods on page 19](#)
- [Special Requirements for Junos OS Plain-Text Passwords on page 20](#)
- [Overview of Template Accounts for RADIUS and TACACS+ Authentication on page 22](#)
- [Junos OS Authentication Methods for Routing Protocols on page 22](#)

Junos OS User Authentication Methods

The Junos OS supports three methods of user authentication: local password authentication, Remote Authentication Dial-In User Service (RADIUS), and Terminal Access Controller Access Control System Plus (TACACS+).

With local password authentication, you configure a password for each user allowed to log in to the router or switch.

RADIUS and TACACS+ are authentication methods for validating users who attempt to access the router or switch using telnet. They are both distributed client-server systems—the RADIUS and TACACS+ clients run on the router or switch, and the server runs on a remote network system.

You can configure the router or switch to be both a RADIUS and TACACS+ client, and you can also configure authentication passwords in the Junos OS configuration file. You can prioritize the methods to configure the order in which the software tries the different authentication methods when verifying user access.

Related Documentation

- [Configuring RADIUS Authentication on page 53](#)
- [Configuring TACACS+ Authentication on page 59](#)
- [Junos OS Authentication Order for RADIUS, TACACS+, and Password Authentication on page 13](#)
- [Configuring RADIUS Authentication](#)
- [Configuring TACACS+ Authentication](#)

Special Requirements for Junos OS Plain-Text Passwords

Junos OS has special requirements when you create plain-text passwords on a router or switch. [Table 6 on page 20](#) shows the default requirements.

Table 6: Special Requirements for Plain-Text Passwords

Junos OS	Junos-FIPS
The password must be between 6 and 128 characters long.	FIPS passwords must be between 10 and 20 characters long
You can include most character classes in a password (uppercase letters, lowercase letters, numbers, punctuation marks, and other special characters). Control characters are not recommended.	You can include most character classes in a password (uppercase letters, lowercase letters, numbers, punctuation marks, and other special characters). Control characters are not recommended.
Valid passwords must contain at least one change of case or character class.	Passwords must use at least three of the five defined character classes (uppercase letters, lowercase letters, numbers, punctuation marks, and other special characters).

You can change the requirements for plain-text passwords.

Junos OS supports the following five character classes for plain-text passwords:

- Lowercase letters
- Uppercase letters
- Numbers
- Punctuation
- Special characters: ! @ # \$ % ^ & *, + < > ; ;

Control characters are not recommended.

You can include the **plain-text-password** statement at the following hierarchy levels:

- **[edit system diag-port-authentication]**
- **[edit system pic-console-authentication]**
- **[edit system root-authentication]**
- **[edit system login user *username* authentication]**

The **change-type** statement specifies whether the password is checked for the following:

- The total number of character sets used (**character-set**)
- The total number of character set changes (**set-transitions**)

For example, the following password:

MyPassWd@2

has four character sets (uppercase letters, lowercase letters, special characters, and numbers) and seven character set changes (**M–y**, **y–P**, **P–a**, **s–W**, **W–d**, **d–@**, and **@–2**).

The **change-type** statement is optional. If you omit the **change-type** option, Junos-FIPS plain-text passwords are checked for character sets, and Junos OS plain-text passwords are checked for character set changes.

The **minimum-changes** statement specifies how many character sets or character set changes are required for the password. This statement is optional. If you do not use the **minimum-changes** statement, character sets are not checked for Junos OS. If the **change-type** statement is configured for the **character-set** option, then the **minimum-changes** value must be 5 or less, because Junos OS only supports five character sets.

The **format** statement specifies the hash algorithm (**md5**, **sha1** or **des**) for authenticating plain-text passwords. This statement is optional. For Junos OS, the default format is **md5**. For Junos-FIPS, only **sha1** is supported.

The **maximum-length** statement specifies the maximum number of characters allowed in a password. This statement is optional. By default, Junos OS passwords have no maximum; however, only the first 128 characters are significant. Junos-FIPS passwords must be 20 characters or less. The range for Junos OS maximum-length passwords is from 20 to 128 characters.

The **minimum-length** statement specifies the minimum number of characters required for a password. This statement is optional. By default, Junos OS passwords must be at least 6 characters long, and Junos-FIPS passwords must be at least 10 characters long. The range is from 6 to 20 characters.

Changes to password requirements do not take effect until the configuration is committed. When requirements change, only newly created, plain-text passwords are checked; existing passwords are not checked against the new requirements.

The default configuration for Junos OS plain-text passwords is:

```
[edit system login]
passwords {
  change-type character-sets;
  format md5;
  minimum-changes 1;
  minimum-length 6;
}
```

The default configuration for Junos-FIPS plain-text passwords is:

```
[edit system login]
passwords {
  change-type set-transitions;
  format sha1;
  maximum-length 20;
  minimum-changes 3;
  minimum-length 10;
}
```

- Related Documentation**
- [Changing the Requirements for Junos OS Plain-Text Passwords](#)
 - [Configuring the Root Password](#)
 - [Changing the Requirements for Junos OS Plain-Text Passwords](#)
 - [Configuring the Root Password](#)

Overview of Template Accounts for RADIUS and TACACS+ Authentication

When you use local password authentication, you must create a local user account for every user who wants to access the system. However, when you are using RADIUS or TACACS+ authentication, you can create single accounts (for authorization purposes) that are shared by a set of users. You create these accounts using the remote and local user template accounts. When a user is using a template account, the command-line interface (CLI) username is the login name; however, the privileges, file ownership, and effective user ID are inherited from the template account.

- Related Documentation**
- [Configuring Remote Template Accounts for User Authentication on page 44](#)
 - [Configuring Local User Template Accounts for User Authentication on page 44](#)

Junos OS Authentication Methods for Routing Protocols

Some interior gateway protocols (IGPs)—Intermediate System-to-Intermediate System (IS-IS), Open Shortest Path First (OSPF), and Routing Information Protocol (RIP)—and Resource Reservation Protocol (RSVP) allow you to configure an authentication method and password. Neighboring routers use the password to verify the authenticity of packets sent by the protocol from the router or from a router interface. The following authentication methods are supported:

- Simple authentication (IS-IS, OSPF, and RIP)—Uses a simple text password. The receiving router uses an authentication key (password) to verify the packet. Because the password is included in the transmitted packet, this method of authentication is relatively insecure. We recommend that you *not* use this authentication method.
- MD5 and HMAC-MD5 (IS-IS, OSPF, RIP, and RSVP)—Message Digest 5 (MD5) creates an encoded checksum that is included in the transmitted packet. HMAC-MD5, which combines HMAC authentication with MD5, adds the use of an iterated cryptographic hash function. With both types of authentication, the receiving router uses an authentication key (password) to verify the packet. HMAC-MD5 authentication is defined in RFC 2104, *HMAC: Keyed-Hashing for Message Authentication*.

In general, authentication passwords are text strings consisting of a maximum of 16 or 255 letters and digits. Characters can include any ASCII strings. If you include spaces in a password, enclose all characters in quotation marks (" ").

Junos-FIPS has special password requirements. FIPS passwords must be between 10 and 20 characters in length. Passwords must use at least three of the five defined character sets (uppercase letters, lowercase letters, digits, punctuation marks, and other

special characters). If Junos-FIPS is installed on the router, you cannot configure passwords unless they meet this standard.

**Related
Documentation**

- [Example: Configuring the BGP and IS-IS Routing Protocols on page 75](#)
- [Special Requirements for Junos OS Plain-Text Passwords on page 20](#)

PART 2

Configuration

- [Configuring User Access on page 27](#)
- [Configuring RADIUS and TACACS+ System Authentication on page 53](#)
- [Examples on page 71](#)
- [Configuration Statements on page 81](#)

CHAPTER 3

Configuring User Access

- [Defining Junos OS Login Classes on page 28](#)
- [Configuring Junos OS User Accounts on page 28](#)
- [Limiting the Number of User Login Attempts for SSH and Telnet Sessions on page 29](#)
- [Configuring Time-Based User Access on page 30](#)
- [Configuring Access Privilege Levels on page 31](#)
- [Specifying Access Privileges for Junos OS Operational Mode Commands on page 32](#)
- [Regular Expressions for Allowing and Denying Junos OS Operational Mode Commands on page 33](#)
- [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 34](#)
- [Regular Expressions for Allowing and Denying Junos OS Configuration Mode Hierarchies on page 35](#)
- [Example: Specifying Access Privileges Using allow/deny-configuration-regexps Statements on page 36](#)
- [Specifying Access Privileges Using allow/deny-configuration Statements on page 40](#)
- [Defining Access Privileges Using allow/deny-configuration Statements on page 42](#)
- [Configuring the Timeout Value for Idle Login Sessions on page 43](#)
- [Example: Creating Login Classes with Specific Privileges on page 43](#)
- [Configuring Remote Template Accounts for User Authentication on page 44](#)
- [Configuring Local User Template Accounts for User Authentication on page 44](#)
- [Configuring the Junos OS Authentication Order for RADIUS, TACACS+, and Local Password Authentication on page 46](#)
- [Using Junos OS to Configure Logical System Administrators on page 47](#)
- [Configuring the Junos OS to Display a System Login Message on page 48](#)
- [Configuring the Junos OS to Display a System Login Announcement on page 49](#)
- [Configuring System Alarms to Appear Automatically Upon Login on page 50](#)
- [System Alarms on J Series Routers on page 50](#)

Defining Junos OS Login Classes

To define a login class and its access privileges, include the **class** statement at the **[edit system login]** hierarchy level:

```
[edit system login]
class class-name {
  access-end;
  access-start;
  allow-commands "regular-expression";
  ( allow-configuration | allow-configuration-regexps ) "regular expression 1" "regular
  expression 2";
  allowed-days;
  configuration-breadcrumbs;
  deny-commands "regular-expression";
  ( deny-configuration | deny-configuration-regexps ) "regular expression 1" "regular
  expression 2 ";
  idle-timeout minutes;
  login-script filename;
  login-tip;
  permissions [ permissions ];
}
```

Related Documentation

- [Junos OS Login Classes Overview on page 3](#)
- [Junos OS User Accounts Overview on page 4](#)
- [Example: Creating Login Classes with Specific Privileges on page 43](#)
- [Configuring the Junos OS to Display a System Login Announcement on page 49](#)
- [Disabling Junos OS Processes](#)
- [Using Junos OS to Configure Logical System Administrators on page 47](#)

Configuring Junos OS User Accounts

User accounts provide one way for users to access the router or switch. For each account, you define the login name for the user and, optionally, information that identifies the user. After you have created an account, the software creates a home directory for the user.

To create user accounts, include the **user** statement at the **[edit system login]** hierarchy level:

```
[edit system login]
user username {
  full-name complete-name;
  uid uid-value;
  class class-name;
  authentication {
    (encrypted-password "password" | plain-text-password);
    load-key-file URL filename;
    ssh-dsa "public-key" <from hostname>;
  }
}
```

```

        ssh-rsa "public-key" <from hostname>;
    }
}

```

**Related
Documentation**

- [Example: Configuring User Accounts on page 72](#)
- [Example: Configuring User Login Accounts on page 71](#)
- [Junos OS User Accounts Overview on page 4](#)
- [Limiting the Number of User Login Attempts for SSH and Telnet Sessions on page 29](#)

Limiting the Number of User Login Attempts for SSH and Telnet Sessions

You can limit the number of times a user can attempt to enter a password while logging in through SSH or Telnet. The connection is terminated if a user fails to log in after the number of attempts specified. You can also specify a delay, in seconds, before a user can try to enter a password after a failed attempt. In addition, you can specify the threshold for the number of failed attempts before the user experiences a delay in being able to enter a password again.

To specify the number of times a user can attempt to enter a password while logging in, include the **retry-options** statement at the **[edit system login]** hierarchy level:

```

[edit system login]
retry-options {
    tries-before-disconnect number;
    backoff-threshold number;
    backoff-factor seconds;
    maximum-time seconds
    minimum-time seconds;
}

```

You can configure the following options:

- **tries-before-disconnect**—Number of times a user can attempt to enter a password when logging in. The connection closes if a user fails to log in after the number specified. The range is from 1 through 10, and the default is 10.
- **backoff-threshold**—Threshold for the number of failed login attempts before the user experiences a delay in being able to enter a password again. Use the **backoff-factor** option to specify the length of the delay in seconds. The range is from 1 through 3, and the default is 2.
- **backoff-factor**—Length of time, in seconds, before a user can attempt to log in after a failed attempt. The delay increases by the value specified for each subsequent attempt after the threshold. The range is from 5 through 10, and the default is 5 seconds.
- **maximum-time seconds**—Maximum length of time, in seconds, that the connection remains open for the user to enter a username and password to log in. If the user remains idle and does not enter a username and password within the configured

maximum-time, the connection is closed. The range is from 20 through 300 seconds, and the default is 120 seconds.

- **minimum-time**—Minimum length of time, in seconds, that a connection remains open while a user is attempting to enter a correct password. The range is from 20 through 60, and the default is 40.

**Related
Documentation**

- [Example: Limiting the Number of Login Attempts for SSH and Telnet Sessions on page 73](#)
- [Configuring Junos OS User Accounts on page 28](#)

Configuring Time-Based User Access

The Junos OS enables you to configure time-based restrictions for user access to log in to a device. This is useful for restricting the time and duration of user logins for all users belonging to a login class. You can specify the days of the week when users can log in, the access start time, and the access end time.

- To configure user access on specific days of the week, without any restrictions on the duration of login, include the **allowed-days** statement only.

```
[edit system]
login {
  class class-name {
    allowed-days [ days-of-the-week ];
  }
}
```

- To configure user access on all the days of the week for a specific duration, include the **access-start** and **access-end** statements only.

```
[edit system]
login {
  class class-name {
    access-start HH:MM;
    access-end HH:MM;
  }
}
```

- To configure user access on specific days of the week for a specified duration, include the **allowed-days**, **access-start**, and **access-end** statements.

```
[edit system]
login {
  class class-name {
    allowed-days [ days-of-the-week ];
    access-start HH:MM;
    access-end HH:MM;
  }
}
```

Specify the start time and end time in **HH:MM** (24-hour) format, where **HH** represents the hours and **MM** represents the minutes.



NOTE: Access start time and end time that spans across 12:00 AM on a specified day results in the user having access until the next day, even if the access day is not explicitly configured. For instance, the following configuration results in the user having access until 6:00 AM on Tuesday and Thursday, although the `allowed-days` statement specifies access only on Monday and Wednesday:

```
[edit system]
login {
  class operator-night-shift {
    allowed-days [ monday wednesday ];
    access-start 2000;
    access-end 0600;
  }
}
```

Related Documentation

- [Examples: Configuring Time-Based User Access on page 73](#)
- [Defining Junos OS Login Classes on page 28](#)
- [access-end on page 89](#)
- [access-start on page 89](#)
- [allowed-days on page 92](#)
- [access-end](#)
- [access-start](#)
- [allowed-days](#)

Configuring Access Privilege Levels

Each top-level command-line interface (CLI) command and each configuration statement have an access privilege level associated with it. Users can execute only those commands and configure and view only those statements for which they have access privileges.

To configure access privilege levels, include the **permissions** statement at the **[edit system login class *class-name*]** hierarchy level:

```
[edit system login class class-name]
permissions [ permissions ];
```

Related Documentation

- [Example: Configuring Access Privilege Levels on page 74](#)
- [Understanding Junos OS Access Privilege Levels on page 7](#)
- [Specifying Access Privileges for Junos OS Operational Mode Commands on page 32](#)
- [permissions on page 117](#)

Specifying Access Privileges for Junos OS Operational Mode Commands

You can specify extended regular expressions by using the **allow-commands** and **deny-commands** statements to define a user's access privileges to individual operational mode commands. Doing so takes precedence over a login class permissions bit set for a user. You can include one **deny-commands** and one **allow-commands** statement in each login class.

To explicitly provide use of an individual operational mode command that would otherwise be denied, include the **allow-commands** statement at the **[edit system login class *class-name*]** hierarchy level:

```
[edit system login class class-name]  
allow-commands "regular-expression";
```

To explicitly deny access to an individual operational mode command that would otherwise be supported, include the **deny-commands** statement at the **[edit system login class *class-name*]** hierarchy level:

```
[edit system login class class-name]  
deny-commands "regular-expression";
```

If the regular expression contains any spaces, operators, or wildcard characters, enclose the expression in quotation marks. Regular expressions are not case-sensitive.

```
allow-commands "show interfaces";
```



NOTE: Modifiers are not supported within the regular expression string to be matched. If a modifier is used, then nothing is matched.

For example, the deny command set **protocols** does not match anything, whereas **protocols** matches *protocols*.

Explicitly providing access to operational mode commands using the **allow-commands** statement adds to the regular permissions set using the **permissions** statement. Likewise, explicitly denying access to operational mode commands using the **deny-commands** statement removes permissions for the specified commands from the default permissions provided by the **permissions** statement.

For example, if a login class has the permission **view** and the **allow-commands** statement includes the **request system software add** command, the specified login class user can install software, in addition to the permissions specified by the **view** permissions flag. Likewise, if a login class has the permission **all** and the **deny-commands** statement includes the **request system software add** command, the specified login class user can perform all operations allowed by the **all** permissions flag, except installing software using the **request system software add** command.

If you allow and deny the same commands, the **allow-commands** permissions take precedence over the permissions specified by **deny-commands**. For example, if you include **allow-commands "request system software add"** and **deny-commands "request system**

software add", the login class user is allowed to install software using the **request system software add** command.

If you specify a regular expression for **allow-commands** and **deny-commands** with two different variants of a command, the longest match is always executed.

For example, if you specify a regular expression for **allow-commands** with the **commit-synchronize** command and a regular expression for **deny-commands** with the **commit** command, users assigned to such a login class would be able to issue the **commit synchronize** command, but not the **commit** command. This is because **commit-synchronize** is the longest match between **commit** and **commit-synchronize**, and it is specified for **allow-commands**.

Likewise, if you specify a regular expression for **allow-commands** with the **commit** command and a regular expression for **deny-commands** with the **commit-synchronize** command, users assigned to such a login class would be able to issue the **commit** command, but not the **commit-synchronize** command. This is because **commit-synchronize** is the longest match between **commit** and **commit-synchronize**, and it is specified for **deny-commands**.

Anchors are required when specifying complex regular expressions with **allow-commands** or **deny-commands** statements. For example, when specifying multiple commands using the pipe (|) symbol for **allow-commands**, the following syntax is incorrect:

allow-commands = "(monitor.*)"|(ping.*)"|(show.*)"|(exit)". Instead, you must specify the expression using the following syntax: **allow-commands = "^(^monitor) | (^ping) | (^show) | (^exit)"** OR **allow-commands = "^(monitor | ping | show | exit)"**

Related Documentation

- [Example: Configuring Access Privileges for Operational Mode Commands on page 75](#)
- [Regular Expressions for Allowing and Denying Junos OS Operational Mode Commands on page 33](#)
- [allow-commands on page 90](#)
- [deny-commands on page 98](#)

Regular Expressions for Allowing and Denying Junos OS Operational Mode Commands

Use extended regular expressions to specify which operational mode commands are denied or allowed. [Table 7 on page 33](#) lists common regular expression operators that can be used in the operational mode commands. Command regular expressions implement the extended (modern) regular expressions as defined in POSIX 1003.2.

Table 7: Common Regular Expression Operators to Allow or Deny Operational Mode Commands

Operator	Match
	One of two or more terms separated by the pipe () symbol. Each term must be a complete standalone expression enclosed in parentheses (), with no spaces between the pipe and the adjacent parentheses. For example, (show system alarms) (show system software) .

Table 7: Common Regular Expression Operators to Allow or Deny Operational Mode Commands (*continued*)

Operator	Match
<code>^</code>	At the beginning of an expression, used to denote where the command begins, and where there might be some ambiguity.
<code>\$</code>	Character at the end of a command. Used to denote a command that must be matched exactly up to that point. For example, allow-commands "show interfaces\$" means that the user can issue the show interfaces command but cannot issue the show interfaces detail or show interfaces extensive command.
<code>[]</code>	Range of letters or digits. To separate the start and end of a range, use a hyphen (-).
<code>()</code>	A group of commands, indicating a complete, standalone expression to be evaluated; the result is then evaluated as part of the overall expression. Parentheses must always be used in conjunction with pipe operators as explained above.

If a regular expression contains a syntax error, it becomes invalid, and although the user can log in, the permission granted or denied by the regular expression does not take effect. When regular expressions configured on TACACS+ or RADIUS servers merge with regular expressions configured on the router or switch, if the final expression has a syntax error, the overall result is an invalid regular expression. If a regular expression does not contain any operators, all varieties of the command are allowed. For example, if the following statement is included in the configuration, the user can issue the commands **show interfaces detail** and **show interfaces extensive** in addition to showing an individual interface:

```
allow-commands "show interfaces";
```

Related Documentation

- [Specifying Access Privileges for Junos OS Operational Mode Commands on page 32](#)

Specifying Access Privileges for Junos OS Configuration Mode Hierarchies

The **allow/deny-configuration** and **allow/deny-configuration-regexps** statements let you explicitly allow or deny users access privileges to portions of the configuration hierarchy. Each of these statements is added to named login classes and configured with one or more regular expressions to be allowed or denied. Each login class is assigned to specific users or user IDs.

The search and match methods differ in the two forms of these statements. You must select which form to use within a login class—you cannot configure **allow-configuration** and **allow-configuration-regexps** together in the same login class. You must select just one. If you have existing configurations using the **allow/deny-configuration** form of the statements, using the same configuration options with the **allow/deny-configuration-regexps** form of the statements might not produce the same results.

- **Allow/deny-configuration** statements perform slower matching, with more flexibility, especially in wildcard matching. However, it can take a very long time to evaluate all of the possible statements if a great number of full path regular expressions or wildcard expressions are configured, possibly impacting performance. These statements were introduced before Junos OS Release 7.4.
- **Allow/deny-configuration-regexps** statements perform faster matching, with less flexibility. You configure a set of strings in which each string is a regular expression, with spaces between the terms of the string. This provides very fast matching. However, it is more tedious to use wildcard expressions in this form of the statement, because you must set up wildcards for each token (term) of the space-delimited string you want to match. These statements were introduced in Junos OS Release 11.2.

Related Documentation

- [Specifying Access Privileges for Junos OS Operational Mode Commands on page 32](#)
- [Example: Configuring Access Privilege Levels on page 74](#)
- [Regular Expressions for Allowing and Denying Junos OS Configuration Mode Hierarchies on page 35](#)
- [Understanding Junos OS Access Privilege Levels on page 7](#)

Regular Expressions for Allowing and Denying Junos OS Configuration Mode Hierarchies

Use extended regular expressions to specify which configuration mode hierarchies are denied or allowed. You specify these regular expressions in the **allow/deny-configuration-regexps** and **allow/deny-configuration** statements at the **[edit system login class]** hierarchy level, or by specifying Juniper Networks vendor-specific TACACS+ or RADIUS attributes in your authentication server's configuration. If regular expressions are received during TACACS+ or RADIUS authentication, they merge with any regular expressions configured on the local router or switch.

[Table 8 on page 35](#) lists common regular expression operators that you can use for allowing or denying configuration mode .

Command regular expressions implement the extended (modern) regular expressions, as defined in POSIX 1003.2.

Table 8: Configuration Mode Hierarchies—Common Regular Expression Operators

Operator	Match
	One of two or more terms separated by the pipe. Each term must be a complete standalone expression enclosed in parentheses (), with no spaces between the pipe and the adjacent parentheses. For example, (show system alarms) (show system software).
^	At the beginning of an expression, used to denote where the command begins, where there might be some ambiguity.

Table 8: Configuration Mode Hierarchies—Common Regular Expression Operators (*continued*)

Operator	Match
\$	Character at the end of a command. Used to denote a command that must be matched exactly up to that point. For example, allow-commands "show interfaces\$" means that the user can issue the show interfaces command but cannot issue show interfaces detail or show interfaces extensive .
[]	Range of letters or digits. To separate the start and end of a range, use a hyphen (-).
()	A group of commands, indicating a complete, standalone expression to be evaluated; the result is then evaluated as part of the overall expression. Parentheses must be used in conjunction with pipe operators as explained.
*	Zero or more terms.
+	One or more terms.
.	Any character except for a space " ".

Related Documentation

- [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 34](#)
- [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies](#)

Example: Specifying Access Privileges Using allow/deny-configuration-regexps Statements

This example shows how to set up configuration access privileges using the **allow-configuration-regexps** and **deny-configuration-regexps** statements.

- [Requirements on page 36](#)
- [Overview on page 37](#)
- [Configuration on page 37](#)
- [Examples on page 37](#)

Requirements

This example uses the following hardware and software components:

- One Juniper Networks J Series, M Series, MX Series, or T Series device
- Junos OS Release 11.2 or later
 - There must be at least one user assigned to a login class.
 - There can be more than one login class, each with varying permission configurations, and more than one user on the device.

Overview

The **allow-configuration-regexps** and **deny-configuration-regexps** statements let you explicitly allow or deny users assigned to named user classes access privileges to portions of the configuration hierarchy, giving the system administrator precision control over who can change specific configurations in the system.



NOTE: The statements **allow-configuration-regexps** and **deny-configuration-regexps** perform similar functions as the statements **allow-configuration** and **deny-configuration**, except you can configure sets of strings in which the strings include spaces when using the first set of statements. You cannot use the two kinds of statements together.

Configuration

To set up configuration access privileges:

1. To explicitly allow one or more individual configuration mode hierarchies that would otherwise be denied, include the **allow-configuration-regexps** statement at the **[edit system login class *class-name*]** hierarchy level, configured with the regular expressions to be allowed.

```
[edit system login class class-name]
user@host# set allow-configuration-regexps "regular expression 1" "regular expression
2" "regular expression 3" "regular expression 4" ...
```

2. To explicitly deny one or more individual configuration hierarchies that would otherwise be allowed, include the **deny-configuration-regexps** statement at the **[edit system login class *class-name*]** hierarchy level, configured with the regular expressions to be denied.

```
[edit system login class class-name]
user@host# set deny-configuration-regexps "regular expression 1" "regular-expression
2" "regular expression 3" "regular expression 4"...
```

3. Assign the login class to one or more users.

```
[edit system login]
user@host# set user username class class-name
```

4. Commit your changes.

Users assigned this login class have the permissions you have set for the class.

Examples

Using Allow or Deny Configurations with Regular Expressions

Purpose This section provides examples of access privilege configurations to give you ideas for creating configurations appropriate for your system. You can use combinations of privilege statements for configuration access and for operational mode commands to give precise control over classes of access privileges.

Allow Configuration Changes The following example login class lets the user make changes at the **[edit system services]** hierarchy level and issue configuration mode commands (such as **commit**), in addition to the permissions specified by the **configure** permissions flag, which allows the user to enter configuration mode using the **configure** command.

```
[edit system login class class-name]
user@host# set permissions configure view view-configuration
user@host# set allow-configuration-regexps "system services"
```

Deny Configuration Changes The following example login class lets the user perform all operations allowed by the **all** permissions flag. However, it denies modifying the configuration at the **[edit system services]** hierarchy level.

```
[edit system login class class-name]
user@host# set permissions all configure view view-configuration
user@host# set deny-configuration-regexps "system services"
```

If the following statement is included in the configuration and the user's login class permission bit is set to **all**, the user cannot configure telnet parameters:

```
[edit system login class class-name]
user@host# set deny-configuration "system services telnet"
```

If the following statement is included in the configuration and the user's login class permission bit is set to **all**, the user cannot issue login class commands within any login class whose name begins with "m":

```
[edit system login class class-name]
user@host# set deny-configuration "system login class m.*"
```

If the following statement is included in the configuration and the user's login class permission bit is set to **all**, the user cannot edit the configuration or issue commands (such as **commit**) at the **[edit system login class]** or the **[edit system services]** hierarchy levels:

```
[edit system login class class-name]
user@host# set deny-configuration "system login class" "system services"
```

Allow and Deny Configuration Changes The following example login class lets the user perform all operations allowed by the **all** permissions flag, and explicitly grants configuration access to **[system "interfaces .* unit .* family inet address .*" protocols]**. However, the user is denied configuration access to the SNMP hierarchy level.



NOTE: You can use the ***** wildcard character when denoting regular expressions. However, it must be used as a portion of a regular expression. You cannot use **[*]** or **[.*]** alone.

```
[edit system login class class-name]
user@host# set permissions all configure view view-configuration
user@host# set allow-configuration-regexps system "interfaces .* unit .* family inet
address .*" protocols
user@host# set deny-configuration-regexps snmp
```

Allow and Deny Multiple Configuration Changes

The following example login class lets the user perform all operations allowed by the **all** permissions flag, and explicitly grants configuration access to multiple hierarchy levels for interfaces. It denies configuration access to the **[edit system]** and **[edit protocols]** hierarchy levels.



NOTE: You can configure as many regular expressions as needed to be allowed or denied. Regular expressions to be denied take precedence over configurations to be allowed.

```
[edit system login class class-name]
user@host# set permissions all configure view view-configuration
user@host# set allow-configuration-regexps "interfaces .* description .*" "interfaces .*
unit .* description .*" "interfaces .* unit .* family inet address .*" "interfaces .* disable"
user@host# set deny-configuration-regexps "system" "protocols"
```

Allow Configuration Changes and Deny Operations Commands

You can combine allow and deny configuration statements with allow and deny operational commands statements to fine-tune access privileges. The following example login class uses a combination of the **deny-commands** operational permissions statement and the **allow-configuration-regexps** configuration permissions statement to let the user configure and commit changes to the OSPF and BGP protocols. However, this class of user cannot issue the **show system statistics** or the **show bgp summary** commands.

```
[edit system login class class-name]
user@host# set permissions all configure view view-configuration
user@host# set deny-commands "(show system statistics)|(show bgp summary)"
user@host# set allow-configuration-regexps "protocols ospf|bgp"
```

The following shows permissions set for individual configuration mode hierarchies:

```
[edit]
system {
  login { # This login class has operator privileges and the additional ability to edit
    # configuration at the system services hierarchy level.
    class only-system-services {
      permissions [ configure ];
      allow-configuration "system services";
    }
    # services commands.
    class all-except-system-services { # This login class has operator privileges but
      # cannot edit any system services configuration.
      permissions [ all ];
      deny-configuration "system services";
    }
  }
}
```

Verification To verify that you have set the access privileges correctly:

1. Configure a login class and commit the changes.
2. Assign the login class to a *username*.
3. Log in as the *username* assigned with the new login class.
4. Attempt to perform the configurations that have been allowed or denied.
 - You should be able to perform configuration changes to hierarchy levels and regular expressions that have been allowed.
 - You should not be able to perform configuration changes to hierarchy levels and regular expressions that have been denied.
 - Denied expressions should take precedence over allowed expressions.
 - Any allowed or denied expressions should take precedence over any permissions granted with the **permissions** statement.

**Related
Documentation**

- [Specifying Access Privileges for Junos OS Operational Mode Commands on page 32](#)
- [Example: Configuring Access Privilege Levels on page 74](#)
- [Regular Expressions for Allowing and Denying Junos OS Configuration Mode Hierarchies on page 35](#)
- [Understanding Junos OS Access Privilege Levels on page 7](#)

Specifying Access Privileges Using allow/deny-configuration Statements

You can specify extended regular expressions by using the **allow-configuration** and **deny-configuration** statements to define user access privileges to parts of the configuration hierarchy. Doing so overrides login class permission bits set for a user. You can also use wildcards to restrict access. When you define access privileges to parts of the configuration hierarchy, do the following:

- Specify the full paths in the extended regular expressions with the **allow-configuration** and **deny-configuration** statements.
- Use parentheses around an extended regular expression that connects two or more expressions with the pipe | symbol. For example:

```
[edit system login class class-name]  
user@host# set deny-configuration "(system login class) | (system services)"
```



NOTE: Each expression separated by a pipe (|) symbol must be a complete standalone expression, and must be enclosed in parentheses (). Do not use spaces between regular expressions separated with parentheses and connected with the pipe (|) symbol. You cannot define access to keywords such as **set**, **edit**, or **activate**.

To explicitly allow an individual configuration mode hierarchy that would otherwise be denied, include the **allow-configuration** statement at the **[edit system login class *class-name*]** hierarchy level:

```
[edit system login class class-name]  
allow-configuration "regular-expression";
```

To explicitly deny an individual configuration hierarchy that would otherwise be allowed, include the **deny-configuration** statement at the **[edit system login class *class-name*]** hierarchy level:

```
[edit system login class class-name]  
deny-configuration "regular-expression";
```

You can include one **deny-configuration** and one **allow-configuration** statement in each login class.



NOTE:

- Explicitly allowing configuration mode hierarchies or regular expressions using the **allow-configuration** statement adds to the regular permissions set using the **permissions** statement. Likewise, explicitly denying configuration mode hierarchies or regular expressions using the **deny-configuration** statement removes permissions for the specified configuration mode hierarchy, from the default permissions provided by the **permissions** statement.

For example, if a login class has permissions **configure** and the **allow-configuration** statement includes the **system services** expression, the specified login class user can edit the configuration at the **[edit system services]** hierarchy level and issue configuration mode commands (such as **commit**), in addition to just entering the configuration mode using the **configure** command (the permissions specified by the **configure** permission flag). Likewise, if a login class has permissions **all** and the **deny-configuration** statement includes **system services**, the specified login class user can perform all operations allowed by the **all** permissions flag, except issuing configuration mode commands (such as **commit**) or modifying the configuration at the **[edit system services]** hierarchy level.

- If you allow and deny the same set of configuration hierarchy levels, regular expressions, or commands, the **allow-configuration** statement permissions take precedence over the permissions specified by the **deny-configuration** statement. For example, if you include **allow-configuration "system services";** and **deny-configuration "system services";**, the login class user can continue to edit the configuration or issue commands at the **[edit system services]** hierarchy level.

Related Documentation

- [Configuring Access Privilege Levels on page 31](#)
- [Defining Access Privileges Using allow/deny-configuration Statements on page 42](#)

- [Regular Expressions for Allowing and Denying Junos OS Configuration Mode Hierarchies on page 35](#)

Defining Access Privileges Using allow/deny-configuration Statements

The following examples show how to configure access privileges for individual configuration mode hierarchy levels.

If the following statement is included in the configuration and the user's login class permission bit is set to **all**, the user cannot configure telnet parameters:

```
[edit system login class class-name]  
user@switch# set deny-configuration "system services telnet"
```

If the following statement is included in the configuration and the user's login class permission bit is set to **all**, the user cannot issue login class commands within any login class whose name begins with "m":

```
[edit system login class class-name]  
user@switch# set deny-configuration "system login class m.*"
```

If the following statement is included in the configuration and the user's login class permission bit is set to **all**, the user cannot edit a configuration or issue commands (such as **commit**) at the login class or system services hierarchy levels:

```
[edit system login class class-name]  
user@switch# set deny-configuration "(system login class) | (system services)"
```

The following example shows how to configure permissions for individual configuration mode hierarchies:

```
[edit]  
system {  
  login { # This login class has operator privileges and the additional ability to edit  
    # configuration at the system services hierarchy level.  
    class only-system-services {  
      permissions [ configure ];  
      allow-configuration "system services";  
    }  
    # services commands.  
    class all-except-system-services { # This login class has operator privileges but  
      # cannot edit any system services configuration.  
      permissions [ all ];  
      deny-configuration "system services";  
    }  
  }  
}
```

Related Documentation

- [Specifying Access Privileges Using allow/deny-configuration Statements on page 40](#)
- [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies](#)

Configuring the Timeout Value for Idle Login Sessions

An idle login session is one in which the CLI operational mode prompt is displayed but there is no input from the keyboard. By default, a login session remains established until a user logs out of the router or switch, even if that session is idle. To close idle sessions automatically, you must configure a time limit for each login class. If a session established by a user in that class remains idle for the configured time limit, the session automatically closes.

To define the timeout value for idle login sessions, include the **idle-timeout** statement at the **[edit system login class *class-name*]** hierarchy level:

```
[edit system login class class-name]  
idle-timeout minutes;
```

Specify the number of minutes that a session can be idle before it is automatically closed.

If you have configured a timeout value, the CLI displays messages similar to the following when timing out an idle user. It starts displaying these messages 5 minutes before timing out the user.

```
user@host# Session will be closed in 5 minutes if there is no activity.  
Warning: session will be closed in 1 minute if there is no activity  
Warning: session will be closed in 10 seconds if there is no activity  
Idle timeout exceeded: closing session
```

If you configure a timeout value, the session closes after the specified time has elapsed, unless the user is running telnet or monitoring interfaces using the **monitor interface** or **monitor traffic** command.

Related Documentation

- [Defining Junos OS Login Classes on page 28](#)
- [idle-timeout on page 103](#)
- [idle-timeout](#)

Example: Creating Login Classes with Specific Privileges

The following example shows how to create several user classes, each with specific privileges. In this example, you configure timeouts to disconnect the class members after a period of inactivity. Users' privilege levels, and therefore the classes of which they are members, should be dependent on their responsibilities within the organization, and the permissions shown here are only examples.

The first class of users (called "observation") can only view statistics and configuration. They are not allowed to modify any configuration. The second class of users (called "operation") can view and modify the configuration. The third class of users (called "engineering") has unlimited access and control.

```
[edit]  
system {  
  login {
```

```
class observation {
  idle-timeout 5;
  permissions [ view ];
}
class operation {
  idle-timeout 5;
  permissions [ admin clear configure interface interface-control network
reset routing routing-control snmp snmp-control trace-control
firewall-control rollback ];
}
class engineering {
  idle-timeout 5;
  permissions all;
}
}
```

Related Documentation

- [Defining Junos OS Login Classes on page 28](#)

Configuring Remote Template Accounts for User Authentication

By default, the Junos OS uses remote template accounts for user authentication when:

- The authenticated user does not exist locally on the router or switch.
- The authenticated user's record in the authentication server specifies local user, or the specified local user does not exist locally on the router or switch.

To configure the remote template account, include the **user remote** statement at the **[edit system login]** hierarchy level and specify the privileges you want to grant to remote users:

```
[edit system login]
user remote {
  full-name "All remote users";
  uid uid-value;
  class class-name;
}
```

To configure different access privileges for users who share the remote template account, include the **allow-commands** and **deny-commands** statements in the authentication server configuration file.

Related Documentation

- [Overview of Template Accounts for RADIUS and TACACS+ Authentication on page 22](#)
- [user \(Access\) on page 134](#)
- [user \(Access\)](#)

Configuring Local User Template Accounts for User Authentication

You use local user template accounts when you need different types of templates for authentication. Each template can define a different set of permissions appropriate for

the group of users who use that template. These templates are defined locally on the router and referenced by the TACACS+ and RADIUS authentication servers.

When you configure local user templates and a user logs in, the Junos OS issues a request to the authentication server to authenticate the user's login name. If a user is authenticated, the server returns the local username to the Junos OS, which then determines whether a local username is specified for that login name (**local-username** for TACACS+, **Juniper-Local-User** for RADIUS). If so, the Junos OS selects the appropriate local user template locally configured on the router. If a local user template does not exist for the authenticated user, the router defaults to the **remote** template.

To configure different access privileges for users who share the local user template account, include the **allow-commands** and **deny-commands** commands in the authentication server configuration file.

To configure a local user template, include the **user local-username** statement at the **[edit system login]** hierarchy level and specify the privileges you want to grant to the local users to whom the template applies:

```
[edit system login]
user local-username {
  full-name "Local user account";
  uid uid-value;
  class class-name;
}
```

This example configures the **sales** and **engineering** local user templates:

```
[edit]
system {
  login {
    user sales {
      uid uid-value;
      class class-name;
    }
    user engineering {
      uid uid-value;
      class class-name;
    }
  }
}

user = simon {
  ...
  service = junos-exec {
    local-user-name = sales
    allow-commands = "configure"
    deny-commands = "shutdown"
  }
}

user = rob {
  ...
  service = junos-exec {
    local-user-name = sales
    allow-commands = "(request system) | (show rip neighbor)"
  }
}
```

```
        deny-commands = "clear"
    }
}
user = harold {
    ...
    service = junos-exec {
        local-user-name = engineering
        allow-commands = "monitor | help | show | ping | traceroute"
        deny-commands = "configure"
    }
}
user = jim {
    ...
    service = junos-exec {
        local-user-name = engineering
        allow-commands = "show bgp neighbor"
        deny-commands = "telnet | ssh"
    }
}
```

When the login users Simon and Rob are authenticated, the switch applies the sales local user template. When login users Harold and Jim are authenticated, the switch applies the engineering local user template.

**Related
Documentation**

- [Overview of Template Accounts for RADIUS and TACACS+ Authentication on page 22](#)
- [user \(Access\) on page 134](#)
- [user \(Access\)](#)

Configuring the Junos OS Authentication Order for RADIUS, TACACS+, and Local Password Authentication

Using the **authentication-order** statement, you can prioritize the order in which the Junos OS tries the different authentication methods when verifying user access to a router or switch.

To configure the authentication order, include the **authentication-order** statement at the **[edit system]** hierarchy level:

```
[edit system]
authentication-order [ authentication-methods ];
```

Specify one or more of the following authentication methods in the preferred order, from first tried to last tried:

- **radius**—Verify the user using RADIUS authentication services
- **tacplus**—Verify the user using TACACS+ authentication services.
- **password**—Verify the user using the username and password configured locally by including the authentication statement at the **[edit system login user]** hierarchy level.

The CHAP authentication sequence cannot take more than 30 seconds. If it takes longer to authenticate a client, the authentication is abandoned and a new sequence is initiated.

For example, if you configure three RADIUS servers so that the router or switch attempts to contact each server three times, and with each retry the server times out after 3 seconds, then the maximum time given to the RADIUS authentication method before CHAP considers it a failure is 27 seconds. If you add more RADIUS servers to this configuration, they might not be contacted because the authentication process might be abandoned before these servers are tried.

The Junos OS enforces a limit on the number of standing authentication server requests that the CHAP authentication can have at one time. Thus, an authentication server method—RADIUS, for example—might fail to authenticate a client when this limit is exceeded. If it fails, the authentication sequence is reinitiated by the router or switch until authentication succeeds and the link is brought up. However, if the RADIUS servers are not available and if additional authentication methods such as **tacplus** or **password** are configured along with **radius**, the next authentication method is tried.

The following example shows how to configure **radius** and **password** authentication:

```
[edit system]
user@switch# authentication-order [ radius password ];
```

The following example shows how to delete the **radius** statement from the authentication order:

```
[edit system]
user@switch# delete authentication-order radius
```

The following example shows how to insert the **tacplus** statement after the **radius** statement:

```
[edit system]
user@switch# insert authentication-order tacplus after radius
```

Related Documentation

- [Junos OS Authentication Order for RADIUS, TACACS+, and Password Authentication on page 13](#)
- [Using Regular Expressions on a RADIUS or TACACS+ Server to Allow or Deny Access to Commands on page 11](#)
- [Example: Configuring System Authentication for RADIUS, TACACS+, and Password Authentication on page 68](#)
- [authentication-order on page 94](#)

Using Junos OS to Configure Logical System Administrators

Using Junos OS, you can partition a single router or switch into multiple logical devices that perform independent routing or switching tasks. When creating logical systems, you must configure logical system administrators and interfaces, assign logical interfaces to logical systems, and configure various other logical system statements.

The master administrator can assign one or more logical system administrators to each logical system. Once assigned to a logical system, administrators are restricted to viewing only configurations of the logical system to which they are assigned and accessing only the operational commands that apply to that particular logical system. This restriction

means that these administrators cannot access global configuration statements, and all command output is restricted to the logical system to which the administrators are assigned.

To configure logical system administrators, include the **logical-system** *logical-system-name* statement at the **[edit system login class class-name]** hierarchy level and apply the class to the user. For example:

```
[edit]
system {
  login {
    class admin1 {
      permissions all;
      logical-system logical-system-LS1;
    }
    class admin2 {
      permissions view; # Gives users assigned to class admin2 the ability to view
                        # but not to change the configuration.
      logical-system logical-system-LS2;
    }
    user user1 {
      class admin1;
    }
    user user2 {
      class admin2;
    }
  }
}
```

Fully implementing logical systems requires that you also configure any protocols, routing statements, switching statements, and policy statements for the logical system.

- Related Documentation**
- [Defining Junos OS Login Classes on page 28](#)
 - Defining Junos OS Login Classes

Configuring the Junos OS to Display a System Login Message

By default, no login message is displayed. To configure a system login message, include the **message** statement at the **[edit system login]** hierarchy level:

```
[edit system login]
message text;
```

If the message text contains any spaces, enclose it in quotation marks.

You can format the message using the following special characters:

- \n—New line
- \t—Horizontal tab
- \'—Single quotation mark

- \"—Double quotation mark
- \—Backslash

The following is a sample login message configuration:

```
[edit]
system {
  login {
    message "\n\n\n\tUNAUTHORIZED USE OF THIS SYSTEM\n
\tIS STRICTLY PROHIBITED!\n\n\tPlease contact
\t'company-noc@company.com\t' to gain\naccess
to this equipment if you need authorization.\n\n\n";
  }
}
```

The preceding login message configuration example produces a login message similar to the following:

```
server% telnet router1
Trying 1.1.1.1...
Connected to router1.
Escape character is '^['.
```

```
UNAUTHORIZED USE OF THIS SYSTEM
IS STRICTLY PROHIBITED!
```

```
Please contact 'company-noc@company.com' to gain
access to this equipment if you need authorization.
```

```
router1 (tty0)
```

```
login:
```

A system login message appears before the user logs in. A system login announcement appears after the user logs in. See [“Configuring the Junos OS to Display a System Login Announcement” on page 49](#).

Related Documentation

- [Configuring the Junos OS to Display a System Login Announcement on page 49](#)
- [Defining Junos OS Login Classes on page 28](#)

Configuring the Junos OS to Display a System Login Announcement

By default, no login announcement is displayed. To configure a system login announcement, include the **announcement** statement at the **[edit system login]** hierarchy level:

```
[edit system login]
announcement text;
```

If the announcement text contains any spaces, enclose it in quotation marks.

A system login announcement appears after the user logs in. A system login message appears before the user logs in. See [“Configuring the Junos OS to Display a System Login Message” on page 48](#).



TIP: You can use the same special characters described in [“Configuring the Junos OS to Display a System Login Message” on page 48](#) to format your system login announcement.

Related Documentation

- [Configuring the Junos OS to Display a System Login Message on page 48](#)

Configuring System Alarms to Appear Automatically Upon Login

You can configure Juniper Networks routers and switches to run the **show system alarms** command whenever a user with the login class **admin** logs in to the router or switch. To do so, include the **login-alarms** statement at the **[edit system login class admin]** hierarchy level.

```
[edit system login class admin]
login-alarms;
```

For more information on the **show system alarms** command, see the Junos OS Operational Mode Commands.

Related Documentation

- [System Alarms on J Series Routers on page 50](#)
- `show system alarms`

System Alarms on J Series Routers

[Table 9 on page 50](#) describes system alarms that may occur on J Series routers. These alarms are preset and cannot be modified.

Table 9: System Alarms on J Series Routers

Alarm Type	Alarm Summary	Remedy
Configuration	This alarm appears if you have not created a rescue configuration for the router. If you inadvertently commit a configuration that denies management access to the router, you must either connect a console to the router or invoke a rescue configuration. Using a rescue configuration is the recommended method. A rescue configuration is one that you know enables management access to the router.	Create the rescue configuration.
License	This alarm appears if you have configured at least one software feature that requires a feature license, but no valid license for the feature is currently installed.	Install a valid license key.

- Related Documentation**
- [Configuring System Alarms to Appear Automatically Upon Login on page 50](#)

CHAPTER 4

Configuring RADIUS and TACACS+ System Authentication

- [Configuring RADIUS Authentication on page 53](#)
- [Example: Configuring RADIUS Authentication on page 56](#)
- [Example: Configuring RADIUS Template Accounts on page 57](#)
- [Juniper Networks Vendor-Specific RADIUS Attributes on page 57](#)
- [Configuring TACACS+ Authentication on page 59](#)
- [Juniper Networks Vendor-Specific TACACS+ Attributes on page 62](#)
- [Configuring RADIUS System Accounting on page 63](#)
- [Example: Configuring RADIUS System Accounting on page 65](#)
- [Configuring TACACS+ System Accounting on page 66](#)
- [Configuring TACACS+ Accounting on a TX Matrix Router on page 68](#)
- [Example: Configuring System Authentication for RADIUS, TACACS+, and Password Authentication on page 68](#)

Configuring RADIUS Authentication

RADIUS authentication is a method of authenticating users who attempt to access the router or switch. Tasks to configure RADIUS authentication are:

- [Configuring RADIUS Server Details on page 53](#)
- [Configuring MS-CHAPv2 for Password-Change Support on page 54](#)
- [Specifying a Source Address for the Junos OS to Access External RADIUS Servers on page 55](#)

Configuring RADIUS Server Details

To use RADIUS authentication on the router or switch, configure information about one or more RADIUS servers on the network by including one **radius-server** statement at the **[edit system]** hierarchy level for each RADIUS server:

```
[edit system]
radius-server server-address {
    accounting-port port-number;
```

```
port port-number;  
retry number;  
secret password;  
source-address source-address;  
timeout seconds;  
}
```

server-address is the address of the RADIUS server.

You can specify a port on which to contact the RADIUS server. By default, port number 1812 is used (as specified in RFC 2865). You can also specify an accounting port to send accounting packets. The default is 1813 (as specified in RFC 2866).

You must specify a password in the **secret password** statement. If the password contains spaces, enclose it in quotation marks. The secret used by the local router or switch must match that used by the server.

Optionally, you can specify the amount of time that the local router or switch waits to receive a response from a RADIUS server (in the **timeout** statement) and the number of times that the router or switch attempts to contact a RADIUS authentication server (in the **retry** statement). By default, the router or switch waits 3 seconds. You can configure this to be a value from 1 through 90 seconds. By default, the router or switch retries connecting to the server 3 times. You can configure this to be a value from 1 through 10 times.

You can use the **source-address** statement to specify a logical address for individual or multiple RADIUS servers.

To configure multiple RADIUS servers, include multiple **radius-server** statements.

To configure a set of users that share a single account for authorization purposes, you create a template user. To do this, include the **user** statement at the **[edit system login]** hierarchy level, as described in [“Overview of Template Accounts for RADIUS and TACACS+ Authentication” on page 22](#).

Configuring MS-CHAPv2 for Password-Change Support

You can configure the Microsoft implementation of the Challenge Handshake Authentication Protocol version 2 (MS-CHAPv2) on the router or switch to support changing of passwords. This feature provides users accessing a router or switch the option of changing the password when the password expires, is reset, or is configured to be changed at next logon.

Before you configure MS-CHAPv2 for password-change support, ensure that you have done the following:

- Configured RADIUS server authentication parameters.
- Set the first tried option in the authentication order to RADIUS server.

To configure MS-CHAP-v2, include the following statements at the **[edit system radius-options]** hierarchy level:

```
[edit system radius-options]
```

```
password-protocol mschap-v2;
```

The following example shows statements for configuring the MS-CHAPv2 password protocol, password authentication order, and user accounts:

```
[edit]
system {
  authentication-order [ radius password ];
  radius-server {
    192.168.69.149 secret "$9$G-j.5Qz6tpBk.1hrlXxUjiq5Qn/C"; ## SECRET-DATA
  }
  radius-options {
    password-protocol mschap-v2;
  }
  login {
    user bob {
      class operator;
    }
  }
}
```

Specifying a Source Address for the Junos OS to Access External RADIUS Servers

You can specify which source address the Junos OS uses when accessing your network to contact an external RADIUS server for authentication. You can also specify which source address the Junos OS uses when contacting a RADIUS server for sending accounting information.

To specify a source address for a RADIUS server, include the **source-address** statement at the **[edit system radius-server server-address]** hierarchy level:

```
[edit system radius-server server-address]
source-address source-address;
```

source-address is a valid IP address configured on one of the router or switch interfaces.



NOTE: You can configure the Junos OS to select a fixed address as the source address for locally generated IP packets.

Related Documentation

- [Example: Configuring RADIUS Authentication on page 56](#)
- [Example: Configuring System Authentication for RADIUS, TACACS+, and Password Authentication on page 68](#)
- [Juniper Networks Vendor-Specific RADIUS Attributes on page 57](#)
- [Overview of Template Accounts for RADIUS and TACACS+ Authentication on page 22](#)
- [Example: Configuring RADIUS Template Accounts on page 57](#)
- [Using Regular Expressions on a RADIUS or TACACS+ Server to Allow or Deny Access to Commands on page 11](#)
- [Junos OS User Authentication Methods on page 19](#)

- [Example: Configuring RADIUS System Accounting on page 65](#)

Example: Configuring RADIUS Authentication

The Junos OS supports two protocols for central authentication of users on multiple routers: RADIUS and TACACS+. We recommend RADIUS because it is a multivendor IETF standard, and its features are more widely accepted than those of TACACS+ or other proprietary systems. In addition, we recommend using a one-time-password system for increased security, and all vendors of these systems support RADIUS.

The Junos OS uses one or more template accounts to perform user authentication. You create the template account or accounts, and then configure the user access to use that account. If the RADIUS server is unavailable, the fallback is for the login process to use the local account that set up on the router or switch.

The following example shows how to configure RADIUS authentication:

```
[edit]
system {
  authentication-order [ radius password ];
  root-authentication {
    encrypted-password "$9$aH1j8gqQ1gjyghgigiilii"; # SECRET-DATA
  }
  name-server {
    10.1.1.1;
    10.1.1.2;
  }
}
```

The following example shows how to enable RADIUS authentication and define the shared secret between the client and the server. The secret enables the client and server to determine that they are talking to the trusted peer.

Define a timeout value for each server, so that if there is no response within the specified number of seconds, the router can try either the next server or the next authentication mechanism.

```
[edit]
system {
  radius-server {
    10.1.2.1 {
      secret "$9$aH1j8gqQ1sdjerrhser"; # SECRET-DATA
      timeout 5;
    }
    10.1.2.2 {
      secret "$9$aH1j8gqQ1csdoiuardwefoiud"; # SECRET-DATA
      timeout 5;
    }
  }
}
```

**Related
Documentation**

- [Configuring RADIUS Authentication on page 53](#)

Example: Configuring RADIUS Template Accounts

The following example shows how to configure RADIUS template accounts for different users or groups of users:

```
[edit]
system {
  login {
    user observation {
      uid 1001;
      class observation;
    }
    user operation {
      uid 1002;
      class operation;
    }
    user engineering {
      uid 1003;
      class engineering;
    }
  }
}
```

Related Documentation • [Overview of Template Accounts for RADIUS and TACACS+ Authentication on page 22](#)

Juniper Networks Vendor-Specific RADIUS Attributes

Junos OS supports the configuration of Juniper Networks RADIUS vendor-specific attributes (VSAs). These VSAs are encapsulated in a RADIUS vendor-specific attribute with the vendor ID set to the Juniper Networks ID number, 2636. [Table 10 on page 57](#) lists the Juniper Networks VSAs you can configure.

Table 10: Juniper Networks Vendor-Specific RADIUS Attributes

Name	Description	Type	Length	String
Juniper-Local-User-Name	Indicates the name of the user template used by this user when logging in to a device. This attribute is used only in Access-Accept packets.	1	≥3	One or more octets containing printable ASCII characters.
Juniper-Allow-Commands	Contains an extended regular expression that enables the user to run operational mode commands in addition to the commands authorized by the user's login class permission bits. This attribute is used only in Access-Accept packets.	2	≥3	One or more octets containing printable ASCII characters, in the form of an extended regular expression. See “Regular Expressions for Allowing and Denying Junos OS Operational Mode Commands” on page 33 .

Table 10: Juniper Networks Vendor-Specific RADIUS Attributes (*continued*)

Name	Description	Type	Length	String
Juniper-Deny-Commands	Contains an extended regular expression that denies the user permission to run operation mode commands authorized by the user's login class permission bits. This attribute is used only in Access-Accept packets.	3	≥3	One or more octets containing printable ASCII characters, in the form of an extended regular expression. See "Regular Expressions for Allowing and Denying Junos OS Operational Mode Commands" on page 33.
Juniper-Allow-Configuration	Contains an extended regular expression that enables the user to run configuration mode commands in addition to the commands authorized by the user's login class permission bits. This attribute is used only in Access-Accept packets.	4	≥3	One or more octets containing printable ASCII characters, in the form of an extended regular expression. See "Regular Expressions for Allowing and Denying Junos OS Configuration Mode Hierarchies" on page 35.
Juniper-Deny-Configuration	Contains an extended regular expression that denies the user permission to run configuration commands authorized by the user's login class permission bits. This attribute is used only in Access-Accept packets.	5	≥3	One or more octets containing printable ASCII characters, in the form of an extended regular expression. See "Regular Expressions for Allowing and Denying Junos OS Configuration Mode Hierarchies" on page 35.
Juniper-Interactive-Command	Indicates the interactive command entered by the user. This attribute is used only in Accounting-Request packets.	8	≥3	One or more octets containing printable ASCII characters.
Juniper-Configuration-Change	Indicates the interactive command that results in a configuration (database) change. This attribute is used only in Accounting-Request packets.	9	≥3	One or more octets containing printable ASCII characters.

Table 10: Juniper Networks Vendor-Specific RADIUS Attributes (*continued*)

Name	Description	Type	Length	String
Juniper-User-Permissions	<p>Contains information the server uses to specify user permissions. This attribute is used only in Access-Accept packets.</p> <p>NOTE: When the Juniper-User-Permissions attribute is configured to grant the Junos OS maintenance or all permissions on a RADIUS server, the UNIX wheel group membership is not automatically added to a user's list of group memberships. Some operations such as running the su root command from a local shell require wheel group membership permissions. However, when a user is configured locally with the permissions maintenance or all, the user is automatically granted membership to the UNIX wheel group. Therefore, we recommend that you create a template user account with the required permissions and associate individual user accounts with the template user account.</p>	10	≥3	<p>One or more octets containing printable ASCII characters.</p> <p>The string is a list of permission flags separated by a space. The exact name of each flag must be specified in its entirety. See Table 4 on page 7.</p>

For more information about the VSAs, see RFC 2138, *Remote Authentication Dial In User Service (RADIUS)*.

- Related Documentation**
- [Configuring RADIUS Authentication on page 53](#)
 - [Configuring RADIUS Authentication](#)

Configuring TACACS+ Authentication

TACACS+ authentication is a method of authenticating users who attempt to access the router or switch. Tasks to configure TACACS+ configuration are:

- [Configuring TACACS+ Server Details on page 60](#)
- [Specifying a Source Address for the Junos OS to Access External TACACS+ Servers on page 61](#)
- [Configuring the Same Authentication Service for Multiple TACACS+ Servers on page 61](#)
- [Configuring Juniper Networks Vendor-Specific TACACS+ Attributes on page 62](#)

Configuring TACACS+ Server Details

To use TACACS+ authentication on the router or switch, configure information about one or more TACACS+ servers on the network by including the **tacplus-server** statement at the **[edit system]** hierarchy level:

```
[edit system]
tacplus-server server-address {
  port port-number;
  secret password;
  single-connection;
  timeout seconds;
}
```

server-address is the address of the TACACS+ server.

port-number is the TACACS+ server port number.

You must specify a secret (password) that the local router or switch passes to the TACACS+ client by including the **secret** statement. If the password included spaces, enclose the password in quotation marks. The secret used by the local router or switch must match that used by the server.

Optionally, you can specify the length of time that the local router or switch waits to receive a response from a TACACS+ server by including the **timeout** statement. By default, the router or switch waits 3 seconds. You can configure this to be a value in the range from 1 through 90 seconds.

Optionally, you can have the software maintain one open Transmission Control Protocol (TCP) connection to the server for multiple requests, rather than opening a connection for each connection attempt by including the **single-connection** statement.



NOTE: Early versions of the TACACS+ server do not support the **single-connection** option. If you specify this option and the server does not support it, the Junos OS will be unable to communicate with that TACACS+ server.

To configure multiple TACACS+ servers, include multiple **tacplus-server** statements.

On a TX Matrix router, TACACS+ accounting should be configured only under the groups **re0** and **re1**.



NOTE: Accounting should not be configured at the **[edit system]** hierarchy level; on a TX Matrix router, control is done under the switch-card chassis only.

To configure a set of users that share a single account for authorization purposes, you create a template user. To do this, include the **user** statement at the **[edit system login]**

hierarchy level, as described in “Overview of Template Accounts for RADIUS and TACACS+ Authentication” on page 22.

Specifying a Source Address for the Junos OS to Access External TACACS+ Servers

You can specify which source address the Junos OS uses when accessing your network to contact an external TACACS+ server for authentication. You can also specify which source address the Junos OS uses when contacting a TACACS+ server for sending accounting information.

To specify a source address for a TACACS+ server for authentication, include the **source-address** statement at the **[edit system tacplus-server server-address]** hierarchy level:

```
[edit system tacplus-server server-address]
source-address source-address;
```

source-address is a valid IP address configured on one of the router or switch interfaces.

To specify a source address for a TACACS+ server for system accounting, include the **source-address** statement at the **[edit system accounting destination tacplus server server-address]** hierarchy level:

```
[edit system accounting destination tacplus server server-address]
source-address source-address;
```

source-address is a valid IP address configured on one of the router or switch interfaces.

Configuring the Same Authentication Service for Multiple TACACS+ Servers

To configure the same authentication service for multiple TACACS+ servers, include statements at the **[edit system tacplus-server]** and **[edit system tacplus-options]** hierarchy levels.

To assign the same authentication service to multiple TACACS+ servers, include the **service-name** statement at the **[edit system tacplus-options]** hierarchy level:

```
[edit system tacplus-options]
service-name service-name;
```

service-name is the name of the authentication service. By default, the service name is set to **junos-exec**.

The following example shows how to configure the same authentication service for multiple TACACS+ servers:

```
[edit system]
tacplus-server {
  10.2.2.2 secret "$9$2dgoJGDiqP5ZG9A"; ## SECRET-DATA
  10.3.3.3 secret "$9$2dgoJGDiqP5ZG9A"; ## SECRET-DATA
}
tacplus-options {
  service-name bob;
}
```

Configuring Juniper Networks Vendor-Specific TACACS+ Attributes

The Juniper Networks Vendor-Specific TACACS+ Attributes enable you to configure access privileges for users on a TACACS+ server. They are specified in the TACACS+ server configuration file on a per-user basis. The Junos OS retrieves these attributes through an authorization request of the TACACS+ server after authenticating a user. You do not need to configure these attributes to run the Junos OS with TACACS+.

To specify these attributes, include a **service** statement of the following form in the TACACS+ server configuration file:

```
service = junos-exec {
  local-user-name = <username-local-to-router>
  allow-commands = "<allow-commands-regex>"
  allow-configuration-regexps = "<allow-configuration-regex>"
  deny-commands = "<deny-commands-regex>"
  deny-configuration-regexps = "<deny-configuration-regex>"
}
```

This **service** statement can appear in a **user** or **group** statement.

Related Documentation

- [Example: Configuring System Authentication for RADIUS, TACACS+, and Password Authentication on page 68](#)
- [Juniper Networks Vendor-Specific TACACS+ Attributes on page 62](#)
- [Overview of Template Accounts for RADIUS and TACACS+ Authentication on page 22](#)
- [Using Regular Expressions on a RADIUS or TACACS+ Server to Allow or Deny Access to Commands on page 11](#)
- [Junos OS User Authentication Methods on page 19](#)

Juniper Networks Vendor-Specific TACACS+ Attributes

Junos OS supports the configuration of Juniper Networks TACACS+ vendor-specific attributes (VSAs). These VSAs are encapsulated in a TACACS+ vendor-specific attribute with the vendor ID set to the Juniper Networks ID number, 2636. [Table 11 on page 62](#) lists the Juniper Networks VSAs you can configure.

Table 11: Juniper Networks Vendor-Specific TACACS+ Attributes

Name	Description	Length	String
local-user-name	Indicates the name of the user template used by this user when logging in to a device.	≥3	One or more octets containing printable ASCII characters.
allow-commands	Contains an extended regular expression that enables the user to run operational mode commands in addition to those commands authorized by the user's login class permission bits.	≥3	One or more octets containing printable ASCII characters, in the form of an extended regular expression. See Table 7 on page 33 .

Table 11: Juniper Networks Vendor-Specific TACACS+ Attributes (*continued*)

Name	Description	Length	String
allow-configuration-regexps	Contains an extended regular expression that enables the user to run configuration mode commands in addition to those commands authorized by the user's login class permission bits.	≥3	One or more octets containing printable ASCII characters, in the form of an extended regular expression. See “Regular Expressions for Allowing and Denying Junos OS Configuration Mode Hierarchies” on page 35 .
deny-commands	Contains an extended regular expression that denies the user permission to run operational mode commands authorized by the user's login class permission bits.	≥3	One or more octets containing printable ASCII characters, in the form of an extended regular expression. See Table 7 on page 33 .
deny-configuration-regexps	Contains an extended regular expression that denies the user permission to run configuration mode commands authorized by the user's login class permission bits.	≥3	One or more octets containing printable ASCII characters, in the form of an extended regular expression. See Table 8 on page 35 .
user-permissions	<p>Contains information the server uses to specify user permissions.</p> <p>NOTE: When the user-permissions attribute is configured to grant the Junos OS maintenance or all permissions on a TACACS+ server, the UNIX wheel group membership is not automatically added to a user's list of group memberships. Some operations such as running the su root command from a local shell require wheel group membership permissions. However, when a user is configured locally with the permissions maintenance or all, the user is automatically granted membership to the UNIX wheel group. Therefore, we recommend that you create a template user account with the required permissions and associate individual user accounts with the template user account.</p>	≥3	One or more octets containing printable ASCII characters. See Table 4 on page 7 .

- Related Documentation**
- [Configuring Juniper Networks Vendor-Specific TACACS+ Attributes on page 62](#)
 - [Configuring TACACS+ Authentication](#)

Configuring RADIUS System Accounting

With RADIUS accounting enabled, Juniper Networks routers or switches, acting as RADIUS clients, can notify the RADIUS server about user activities such as software logins, configuration changes, and interactive commands. The framework for RADIUS accounting is described in RFC 2866.

Tasks for configuring RADIUS system accounting are:

1. [Configuring Auditing of User Events on a RADIUS Server on page 64](#)
2. [Specifying RADIUS Server Accounting and Auditing Events on page 64](#)
3. [Configuring RADIUS Server Accounting on page 64](#)

Configuring Auditing of User Events on a RADIUS Server

To audit user events, include the following statements at the **[edit system accounting]** hierarchy level:

```
[edit system accounting]
events [ events ];
destination {
  radius {
    server {
      server-address {
        accounting-port port-number;
        secret password;
        source-address address;
        retry number;
        timeout seconds;
      }
    }
  }
}
```

Specifying RADIUS Server Accounting and Auditing Events

To specify the events you want to audit when using a RADIUS server for authentication, include the **events** statement at the **[edit system accounting]** hierarchy level:

```
[edit system accounting]
events [ events ];
```

events is one or more of the following:

- **login**—Audit logins
- **change-log**—Audit configuration changes
- **interactive-commands**—Audit interactive commands (any command-line input)

Configuring RADIUS Server Accounting

To configure RADIUS server accounting, include the **server** statement at the **[edit system accounting destination radius]** hierarchy level:

```
server {
  server-address {
    accounting-port port-number;
    secret password;
    source-address address;
    retry number;
    timeout seconds;
```

```
}
}
```

server-address specifies the address of the RADIUS server. To configure multiple RADIUS servers, include multiple **server** statements.



NOTE: If no RADIUS servers are configured at the [edit system accounting destination radius] statement hierarchy level, the Junos OS uses the RADIUS servers configured at the [edit system radius-server] hierarchy level.

accounting-port port-number specifies the RADIUS server accounting port number.

The default port number is 1813.



NOTE: If you enable RADIUS accounting at the [edit access profile profile-name accounting-order] hierarchy level, accounting is triggered on the default port of 1813 even if you do not specify a value for the accounting-port statement.

You must specify a secret (password) that the local router or switch passes to the RADIUS client by including the **secret** statement. If the password contains spaces, enclose the entire password in quotation marks (" ").

In the **source-address** statement, specify a source address for the RADIUS server. Each RADIUS request sent to a RADIUS server uses the specified source address. The source address is a valid IPv4 address configured on one of the router or switch interfaces.

Optionally, you can specify the number of times that the router or switch attempts to contact a RADIUS authentication server by including the **retry** statement. By default, the router or switch retries three times. You can configure the router or switch to retry from 1 through 10 times.

Optionally, you can specify the length of time that the local router or switch waits to receive a response from a RADIUS server by including the **timeout** statement. By default, the router or switch waits 3 seconds. You can configure the timeout to be from 1 through 90 seconds.

Example: Configuring RADIUS System Accounting

The following example shows three servers (10.5.5.5, 10.6.6.6, and 10.7.7.7) configured for RADIUS accounting.

```
system {
  accounting {
    events [ login change-log interactive-commands ];
    destination {
      radius {
        server {
          10.5.5.5 {
            accounting-port 3333;
```

```
        secret $9$dkafeqwrew;
        source-address 10.1.1.1;
        retry 3;
        timeout 3;
    }
    10.6.6.6 secret $9$fe3erqwrez;
    10.7.7.7 secret $9$f34929ftby;
}
}
}
```

Related Documentation

- [Configuring RADIUS System Accounting on page 63](#)

Configuring TACACS+ System Accounting

You can use TACACS+ to track and log software logins, configuration changes, and interactive commands. To audit these events, include the following statements at the **[edit system accounting]** hierarchy level:

```
[edit system accounting]
events [ events ];
destination {
  tacplus {
    server {
      server-address {
        port port-number;
        secret password;
        single-connection;
        timeout seconds;
      }
    }
  }
}
```

Tasks for configuring TACACS+ system accounting are:

1. [Specifying TACACS+ Auditing and Accounting Events on page 66](#)
2. [Configuring TACACS+ Server Accounting on page 67](#)

Specifying TACACS+ Auditing and Accounting Events

To specify the events you want to audit when using a TACACS+ server for authentication, include the **events** statement at the **[edit system accounting]** hierarchy level:

```
[edit system accounting]
events [ events ];
```

events is one or more of the following:

- **login**—Audit logins
- **change-log**—Audit configuration changes

- **interactive-commands**—Audit interactive commands (any command-line input)

Configuring TACACS+ Server Accounting

To configure TACACS+ server accounting, include the **server** statement at the **[edit system accounting destination tacplus]** hierarchy level:

```
[edit system accounting destination tacplus]
server {
  server-address {
    port port-number;
    secret password;
    single-connection;
    timeout seconds;
  }
}
```

server-address specifies the address of the TACACS+ server. To configure multiple TACACS+ servers, include multiple **server** statements.



NOTE: If no TACACS+ servers are configured at the **[edit system accounting destination tacplus]** statement hierarchy level, the Junos OS uses the TACACS+ servers configured at the **[edit system tacplus-server]** hierarchy level.

port-number specifies the TACACS+ server port number.

You must specify a secret (password) that the local router or switch passes to the TACACS+ client by including the **secret** statement. If the password contains spaces, enclose the entire password in quotation marks (" "). The password used by the local router or switch must match that used by the server.

Optionally, you can specify the length of time that the local router or switch waits to receive a response from a TACACS+ server by including the **timeout** statement. By default, the router or switch waits 3 seconds. You can configure this to be a value in the range from 1 through 90 seconds.

Optionally, you can maintain one open TCP connection to the server for multiple requests, rather than opening a connection for each connection attempt, by including the **single-connection** statement.

To ensure that start and stop requests for accounting of login events are correctly logged in the Accounting file instead of the Administration log file on a TACACS+ server, include either the **no-cmd-attribute-value** statement or the **exclude-cmd-attribute** at the **[edit system tacplus-options]** hierarchy level.

If you use the **no-cmd-attribute-value** statement, the value of the **cmd** attribute is set to a null string in the start and stop requests. If you use the **exclude-cmd-attribute** statement, the **cmd** attribute is totally excluded from the start and stop requests. Both statements support the correct logging of accounting requests in the Accounting file, instead of the Administration file.

```
[edit system tacplus-options]
(no-cmd-attribute-value | exclude-cmd-attribute);
```

**Related
Documentation**

- [Configuring TACACS+ Accounting on a TX Matrix Router on page 68](#)
- [Configuring TACACS+ Authentication on page 59](#)

Configuring TACACS+ Accounting on a TX Matrix Router

On a TX Matrix router, TACACS+ accounting should be configured only under the groups **re0** and **re1**.



NOTE: Accounting should *not* be configured at the **[edit system]** hierarchy; on a TX Matrix router, control is done under the switch-card chassis only.

**Related
Documentation**

- [Configuring TACACS+ System Accounting on page 66](#)

Example: Configuring System Authentication for RADIUS, TACACS+, and Password Authentication

The following example shows how to configure system authentication for RADIUS, TACACS+, and password authentication.

In this example, only the user Philip and users authenticated by a remote RADIUS server can log in. If a user logs in and is not authenticated by the RADIUS server, the user is denied access to the router or switch. If the RADIUS server is not available, the user is authenticated using the **password** authentication method and allowed access to the router or switch. For more information about the password authentication method, see [“Using Local Password Authentication” on page 14](#).

When Philip tries to log in to the system, if the RADIUS server authenticates him, he is given access and privileges for the **super-user** class. Local accounts are not configured for other users. When they log in to the system and the RADIUS server authenticates them, they are given access using the same user ID (UID) 9999 and the privileges associated with the **operator** class.

```
[edit]
system {
  authentication-order radius;
  login {
    user philip {
      full-name "Philip";
      uid 1001;
      class super-user;
    }
    user remote {
      full-name "All remote users";
      uid 9999;
      class operator;
    }
  }
}
```

```

    }
  }
}

```



NOTE: For authorization purposes, you can use a template account to create a single account that can be shared by a set of users at the same time. For example, when you create a remote template account, a set of remote users can concurrently share a single UID. For more information about template accounts, see [“Overview of Template Accounts for RADIUS and TACACS+ Authentication” on page 22](#).

When a user logs in to a device, the user's login name is used by the RADIUS or TACACS+ server for authentication. If the user is authenticated successfully by the authentication server and the user is not configured at the **[edit system login user]** hierarchy level, the device uses the default remote template user account for the user, provided a remote template account is configured at the **edit system login user remote** hierarchy level. The remote template account serves as a default template user account for all users that are authenticated by the authentication server but not having a locally configured user account on the device. Such users share the same login class and UID.

To configure an alternate template user, specify the **user-name** parameter returned in the RADIUS authentication response packet. Not all RADIUS servers allow you to change this parameter. The following shows a sample Junos OS configuration:

```

[edit]
system {
  authentication-order radius;
  login {
    user philip {
      full-name "Philip";
      uid 1001;
      class super-user;
    }
    user operator {
      full-name "All operators";
      uid 9990;
      class operator;
    }
    user remote {
      full-name "All remote users";
      uid 9999;
      class read-only;
    }
  }
}

```

Assume your RADIUS server is configured with the following information:

- User Philip with password “olympia”
- User Alexander with password “bucephalus” and username “operator”

- User Darius with password “redhead” and username “operator”
- User Roxane with password “athena”

Philip would be given access as a superuser (**super-user**) because he has his own local user account. Alexander and Darius share UID 9990 and have access as operators. Roxane has no template-user override, so she shares access with all the other remote users, getting read-only access.

**Related
Documentation**

- [Configuring the Junos OS Authentication Order for RADIUS, TACACS+, and Local Password Authentication on page 46](#)

CHAPTER 5

Examples

- [Example: Configuring User Login Accounts on page 71](#)
- [Example: Configuring User Accounts on page 72](#)
- [Example: Limiting the Number of Login Attempts for SSH and Telnet Sessions on page 73](#)
- [Examples: Configuring Time-Based User Access on page 73](#)
- [Example: Configuring Access Privilege Levels on page 74](#)
- [Example: Configuring Access Privileges for Operational Mode Commands on page 75](#)
- [Example: Configuring the BGP and IS-IS Routing Protocols on page 75](#)
- [Recovering the Root Password on page 77](#)

Example: Configuring User Login Accounts

The following example shows how to configure the local administrator account (**user admin**). If RADIUS fails or becomes unreachable, the login process reverts to password authentication on the local accounts on the router or switch.

```
[edit]
system {
  login {
    user admin {
      uid 1000;
      class engineering;
      authentication {
        encrypted-password "<PASSWORD>"; # SECRET-DATA
      }
    }
  }
}
```

Related Documentation

- [Configuring Junos OS User Accounts on page 28](#)

Example: Configuring User Accounts

The following example shows how to create accounts for four router or switch users, and create an account for the template user **remote**. All users use one of the default system login classes. User **alexander** also has two digital signal algorithm (DSA) public keys configured for SSH authentication.

```
[edit]
system {
  login {
    user philip {
      full-name "Philip of Macedonia";
      uid 1001;
      class super-user;
      authentication {
        encrypted-password "$1$poPPeY";
      }
    }
    user alexander {
      full-name "Alexander the Great";
      uid 1002;
      class view;
      authentication {
        encrypted-password "$1$14c5.$sBopasdFFdssdfFFdsdfs0";
        ssh-dsa "8924 37 5678 5678@gaugamela.per";
        ssh-dsa "6273 94 9283@boojum.per";
      }
    }
    user darius {
      full-name "Darius King of Persia";
      uid 1003;
      class operator;
      authentication {
        ssh-rsa "1024 37 12341234@ecbatana.per";
      }
    }
    user anonymous {
      class unauthorized;
    }
    user remote {
      full-name "All remote users";
      uid 9999;
      class read-only;
    }
  }
}
```

Related Documentation

- [Junos OS User Accounts Overview on page 4](#)
- [Limiting the Number of User Login Attempts for SSH and Telnet Sessions on page 29](#)

Example: Limiting the Number of Login Attempts for SSH and Telnet Sessions

The following example shows how to limit the user to four attempts when the user enters a password while logging in through SSH or Telnet. Set the **backoff-threshold** to 2, the **back-off-factor** to 5 seconds, and the **minimum-time** to 40 seconds. The user experiences a delay of 5 seconds after the second attempt to enter a correct password fails. After each subsequent failed attempt, the delay increases by 5 seconds. After the fourth and final failed attempt to enter a correct password, the user experiences an additional 10-second delay, and the connection closes after a total of 40 seconds.

The additional variables **maximum-time** and **lockout-period** are not set in this example.

```
[edit]
system {
  login {
    retry-options {
      backoff-threshold 2;
      backoff-factor 5;
      minimum-time 40;
      tries-before-disconnect 4;
    }
    password {
    }
  }
}
```



NOTE: This sample only shows the portion off the [edit system login] hierarchy level being modified.

Related Documentation

- [Limiting the Number of User Login Attempts for SSH and Telnet Sessions on page 29](#)
- [login on page 105](#)
- [login](#)

Examples: Configuring Time-Based User Access

The following example shows how to configure user access for the **operator-round-the-clock-access** login class from Monday through Friday without any restriction on access time or duration of login:

```
[edit system]
login {
  class operator-round-the-clock-access {
    allowed-days [ monday tuesday wednesday thursday friday ];
  }
}
```

The following example shows how to configure user access for the **operator-day-shift** login class on Monday, Wednesday, and Friday from 8:30 AM to 4:30 PM:

```
[edit system]
```

```
login {  
  class operator-day-shift {  
    allowed-days [ monday wednesday friday ];  
    access-start 0830;  
    access-end 1630;  
  }  
}
```

Alternatively, you can also specify the login start time and end time for the **operator-day-shift** login class to be from 8:30 AM to 4:30 PM in the following format:

```
[edit system]  
login {  
  class operator-day-shift {  
    allowed-days [ monday wednesday friday ];  
    access-start 08:30am;  
    access-end 04:30pm;  
  }  
}
```

The following example shows how to configure user access for the **operator-day-shift-all-days-of-the-week** login class to be on all days of the week from 8:30 AM to 4:30 PM:

```
[edit system]  
login {  
  class operator-day-shift-all-days-of-the-week {  
    access-start 0830;  
    access-end 1630;  
  }  
}
```

Related Documentation • [Configuring Time-Based User Access on page 30](#)

Example: Configuring Access Privilege Levels

Create two access privilege classes on the router or switch, one for configuring and viewing user accounts only and the second for configuring and viewing SNMP parameters only:

```
[edit]  
system {  
  login {  
    class user-accounts {  
      permissions [ configure admin admin-control ];  
    }  
    class network-mgmt {  
      permissions [ configure snmp snmp-control ];  
    }  
  }  
}
```

Related Documentation • [Configuring Access Privilege Levels on page 31](#)

Example: Configuring Access Privileges for Operational Mode Commands

The following example shows how to configure access privileges for different login classes for individual operational mode commands:

```
[edit]
system {
  # This login class has operator privileges and the additional ability
  # to reboot the router.
  login {
    # This login class has operator privileges and the additional ability to reboot the
    # router or switch.
    class operator-and-boot {
      permissions [ clear network reset trace view ];
      allow-commands "request system reboot";
    }
    # This login class has operator privileges but can't use any commands beginning
    # with "set".
    # This login class has operator privileges
    # but cannot use any commands beginning with "set"
    class operator-no-set {
      permissions [ clear network reset trace view ];
      deny-commands "^set";
    }
    # This login class has operator privileges and can install software but not view
    # BGP information, and can issue the show route command, without specifying
    # commands or arguments under it.
    class operator-and-install-but-no-bgp {
      permissions [ clear network reset trace view ];
      allow-commands "(request system software add)|(show route$)";
      deny-commands "show bgp";
    }
  }
}
```

Related Documentation • [Specifying Access Privileges for Junos OS Operational Mode Commands on page 32](#)

Example: Configuring the BGP and IS-IS Routing Protocols

The main task of a router is to use its routing and forwarding tables to forward user traffic to its intended destination. Attackers can send forged routing protocol packets to a router with the intent of changing or corrupting the contents of its routing table or other databases, which in turn can degrade the functionality of the router and the network. To prevent such attacks, routers must ensure that they form routing protocol relationships (peering or neighboring relationships) to trusted peers. One way of doing this is by authenticating routing protocol messages. We strongly recommend using authentication when configuring routing protocols. The Junos OS supports HMAC-MD5 authentication for BGP, Intermediate System-to-Intermediate System (IS-IS), Open Shortest Path First (OSPF), Routing Information Protocol (RIP), and Resource Reservation Protocol (RSVP). HMAC-MD5 uses a secret key that is combined with the data being transmitted to compute a hash. The computed hash is transmitted along with the data. The receiver

uses the matching key to recompute and validate the message hash. If an attacker has forged or modified the message, the hash will not match and the data will be discarded.

In the following examples, we configure BGP as the exterior gateway protocol (EGP) and IS-IS as the interior gateway protocol (IGP). If you use OSPF, configure it similarly to the IS-IS configuration shown.

Configuring BGP

The following example shows the configuration of a single authentication key for the BGP peer group internal peers. You can also configure BGP authentication at the neighbor or routing instance levels, or for all BGP sessions. As with any security configuration, there is a trade-off between the degree of granularity (and to some extent the degree of security) and the amount of management necessary to maintain the system. This example also configures a number of tracing options for routing protocol events and errors, which can be good indicators of attacks against routing protocols. These events include protocol authentication failures, which might point to an attacker that is sending spoofed or otherwise malformed routing packets to the router in an attempt to elicit a particular behavior.

```
[edit]
protocols {
  bgp {
    group ibgp {
      type internal;
      traceoptions {
        file bgp-trace size 1m files 10;
        flag state;
        flag general;
      }
      local-address 10.10.5.1;
      log-updown;
      neighbor 10.2.1.1;
      authentication-key "$9$aH1j8gqQ1gJyJghgJgIiiii";
    }
    group ebgp {
      type external;
      traceoptions {
        file ebgp-trace size 10m files 10;
        flag state;
        flag general;
      }
      local-address 10.10.5.1;
      log-updown;
      peer-as 2;
      neighbor 10.2.1.2;
      authentication-key "$9$aH1j8gqQ1gJyJghgJgIiiii";
    }
  }
}
```

Configuring IS-IS

Although all IGPs supported by the Junos OS support authentication, some are inherently more secure than others. Most service providers use OSPF or IS-IS to allow fast internal convergence and scalability and to use traffic engineering capabilities with Multiprotocol Label Switching (MPLS). Because IS-IS does not operate at the network layer, it is more difficult to spoof than OSPF, which is encapsulated in IP and is therefore subject to remote spoofing and DoS attacks.

The following example also shows how to configure a number of tracing options for routing protocol events and errors, which can be good indicators of attacks against routing protocols. These events include protocol authentication failures, which might point to an attacker that is sending spoofed or otherwise malformed routing packets to the router in an attempt to elicit a particular behavior.

```
[edit]
protocols {
  isis {
    authentication-key "$9$aHlj8gqQ1givyjhgjgiiii"; # SECRET-DATA
    authentication-type md5;
    traceoptions {
      file isis-trace size 10m files 10;
      flag normal;
      flag error;
    }
    interface at-0/0/0.131 {
      lsp-interval 50;
      level 2 disable;
      level 1 {
        metric 3;
        hello-interval 5;
        hold-time 60;
      }
    }
    interface lo0.0 {
      passive;
    }
  }
}
```

Related Documentation

- [Configuring the Authentication Key Update Mechanism for BGP and LDP Routing Protocols](#)

Recovering the Root Password

If you forget the root password for the router, you can use the password recovery procedure to reset the root password.



NOTE: You need console access to recover the root password.



VIDEO: Recovering the Root Password

To recover the root password:

1. Power off the router by pressing the power button on the front panel.
2. Turn off the power to the management device, such as a PC or laptop computer, that you want to use to access the CLI.
3. Plug one end of the Ethernet rollover cable supplied with the router into the RJ-45-to-DB-9 serial port adapter supplied with the router.
4. Plug the RJ-45-to-DB-9 serial port adapter into the serial port on the management device.
5. Connect the other end of the Ethernet rollover cable to the console port on the router.
6. Turn on the power to the management device.
7. On the management device, start your asynchronous terminal emulation application (such as Microsoft Windows Hyperterminal) and select the appropriate **COM** port to use (for example, **COM1**).
8. Configure the port settings as follows:
 - Bits per second: 9600
 - Data bits: 8
 - Parity: None
 - Stop bits: 1
 - Flow control: None
9. Power on the router by pressing the power button on the front panel. Verify that the POWER LED on the front panel turns green.

The terminal emulation screen on your management device displays the router's boot sequence.
10. When the following prompt appears, press the Spacebar to access the router's bootstrap loader command prompt:

Hit [Enter] to boot immediately, or space bar for command prompt.
Booting [kernel] in 9 seconds...
11. At the following prompt, enter **boot -s** to start up the system in single-user mode.

ok **boot -s**
12. At the following prompt, enter **recovery** to start the root password recovery procedure.

Enter full pathname of shell or 'recovery' for root password recovery or RETURN for /bin/sh: **recovery**
13. Enter configuration mode in the CLI.
14. Set the root password. For example:

```
user@host# set system root-authentication plain-text-password
```

15. At the following prompt, enter the new root password. For example:

```
New password: juniper1
Retype new password:
```

16. At the second prompt, reenter the new root password.
17. After you have finished configuring the password, commit the configuration.

```
root@host# commit
commit complete
```

18. Exit configuration mode in the CLI.
19. Exit operational mode in the CLI.
20. At the prompt, enter **y** to reboot the router.

```
Reboot the system? [y/n] y
```

Related Documentation

- [Configuring the Root Password](#)

Configuration Statements

- [System Management Configuration Statements on page 81](#)

System Management Configuration Statements

This topic lists all the configuration statements that you can include at the **[edit system]** hierarchy level to configure system management features:

```
system {
  accounting {
    events [ login change-log interactive-commands ];
    destination {
      radius {
        server {
          server-address {
            accounting-port port-number;
            retry number;
            secret password;
            source-address address;
            timeout seconds;
          }
        }
      }
    }
    tacplus {
      server {
        server-address {
          port port-number;
          secret password;
          single-connection;
          timeout seconds;
        }
      }
    }
  }
  archival {
    configuration {
      archive-sites {
        ftp://<username>:<password>@<host>:<port>/<url-path>;
        ftp://<username>:<password>@<host>:<port>/<url-path>;
      }
      transfer-interval interval;
    }
  }
}
```

```

        transfer-on-commit;
    }
}
allow-v4mapped-packets;
arp {
    aging-timer minutes;
    gratuitous-arp-delay;
    gratuitous-arp-on-ifup;
    interfaces;
    passive-learning;
    purging;
}
authentication-order [ authentication-methods ];
backup-router address <destination destination-address>;
commit synchronize;
(compress-configuration-files | no-compress-configuration-files);
default-address-selection;
dump-device (compact-flash | remove-compact | usb);
diag-port-authentication (encrypted-password "password" | plain-text-password);
dynamic-profile-options {
    versioning;
}
domain-name domain-name;
domain-search [ domain-list ];
host-name hostname;
inet6-backup-router address <destination destination-address>;
internet-options {
    tcp-mss mss-value;
    (gre-path-mtu-discovery | no-gre-path-mtu-discovery);
    icmpv4-rate-limit bucket-size bucket-size packet-rate packet-rate;
    icmpv6-rate-limit bucket-size bucket-size packet-rate packet-rate;
    (ipip-path-mtu-discovery | no-ipip-path-mtu-discovery);
    (ipv6-path-mtu-discovery | no-ipv6-path-mtu-discovery);
    ipv6-path-mtu-discovery-timeout;
    no-tcp-rfc1323-paws;
    no-tcp-rfc1323;
    (path-mtu-discovery | no-path-mtu-discovery);
    source-port upper-limit <upper-limit>;
    (source-quench | no-source-quench);
    tcp-drop-synfin-set;
}
location {
    altitude feet;
    building name;
    country-code code;
    floor number;
    hcoord horizontal-coordinate;
    lata service-area;
    latitude degrees;
    longitude degrees;
    npa-nxx number;
    postal-code postal-code;
    rack number;
    vcoord vertical-coordinate;
}
login {

```



```

announcement text;
class class-name {
    access-end;
    access-start;
    allow-commands "regular-expression";
    ( allow-configuration | allow-configuration-regexps ) "regular expression 1" "regular
        expression 2";
    allowed-days;
    deny-commands "regular-expression";
    ( deny-configuration | deny-configuration-regexps ) "regular expression 1" "regular
        expression 2 ";
    idle-timeout minutes;
    login-script
    login-tip;
    permissions [ permissions ];
}
message text;
password {
    change-type (set-transitions | character-set);
    format (md5 | sha1 | des);
    maximum-length length;
    minimum-changes number;
    minimum-length length;
}
retry-options {
    backoff-threshold number;
    backoff-factor seconds;
    minimum-time seconds;
    tries-before-disconnect number;
}
user username {
    full-name complete-name;
    uid uid-value;
    class class-name;
    authentication {
        (encrypted-password "password" | plain-text-password);
        ssh-rsa "public-key";
        ssh-dsa "public-key";
    }
}
}
login-tip number;
mirror-flash-on-disk;
name-server {
    address;
}
no-multicast-echo;
no-redirects;
no-ping-record-route;
no-ping-time-stamp;
ntp {
    authentication-key key-number type type value password;
    boot-server address;
    broadcast <address> <key key-number> <version value> <ttl value>;
    broadcast-client;
    multicast-client <address>;
}

```

```
peer address <key key-number> <version value> <prefer>;
source-address source-address;
server address <key key-number> <version value> <prefer>;
trusted-key [ key-numbers ];
}
ports {
  auxiliary {
    type terminal-type;
  }
  pic-console-authentication {
    encrypted-password encrypted-password;
    plain-text-password;
    console {
      insecure;
      log-out-on-disconnect;
      type terminal-type;
      disable;
    }
  }
}
processes {
  process--name (enable | disable) failover (alternate-media | other-routing-engine);
  timeout seconds;
}
}
radius-server server-address {
  accounting-port port-number;
  port port-number;
  retry number;
  secret password;
  source-address source-address;
  timeout seconds;
}
radius-options {
  password-protocol mschap-v2;
}
attributes {
  nas-ip-address ip-address;
}
root-authentication {
  (encrypted-password "password" | plain-text-password);
  ssh-rsa "public-key";
  ssh-dsa "public-key";
}
(saved-core-context | no-saved-core-context);
saved-core-files saved-core-files;
scripts {
  commit {
    allow-transients;
    file filename {
      optional;
      refresh;
      refresh-from url;
      source url;
    }
  }
  traceoptions {
    file <filename> <files number> <size size> <world-readable | no-world-readable>;
    flag flag;
  }
}
```

```

        no-remote-trace;
    }
    op {
        file filename {
            arguments {
                argument-name {
                    description descriptive-text;
                }
            }
            command filename-alias;
            description descriptive-text;
            refresh;
            refresh-from url;
            source url;
        }
        refresh;
        refresh-from url;
        traceoptions {
            file <filename> <files number> <size size> <world-readable | no-world-readable>;
            flag flag;
            no-remote-trace;
        }
    }
}
services {
    finger {
        connection-limit limit;
        rate-limit limit;
    }
    flow-tap-dtcp {
        ssh {
            connection-limit limit;
            rate-limit limit;
        }
    }
    ftp {
        connection-limit limit;
        rate-limit limit;
    }
    service-deployment {
        servers server-address {
            port port-number;
        }
        source-address source-address;
    }
    ssh {
        root-login (allow | deny | deny-password);
        protocol-version [v1 v2];
        connection-limit limit;
        rate-limit limit;
    }
    telnet {
        connection-limit limit;
        rate-limit limit;
    }
    web-management {

```

```
http {
    interfaces [ interface-names ];
    port port;
}
https {
    interfaces [ interface-names ];
    local-certificate name;
    port port;
}
session {
    idle-timeout [ minutes ];
    session-limit [ session-limit ];
}
}
xnm-clear-text {
    connection-limit limit;
    rate-limit limit;
}
xnm-ssl {
    connection-limit limit;
    local-certificate name;
    rate-limit limit;
}
}
static-host-mapping {
    hostname {
        alias [ alias ];
        inet [ address ];
        sysid system-identifier;
    }
}
syslog {
    archive <files number> <size size> <world-readable | no-world-readable>;
    console {
        facility severity;
    }
    file filename {
        facility severity;
        archive <archive-sites {ftp-url <password password>}> <files number> <size size>
            <start-time "YYYY-MM-DD.hh:mm"> <transfer-interval minutes> <world-readable |
            no-world-readable>;
        explicit-priority;
        match "regular-expression";
        structured-data {
            brief;
        }
    }
}
host (hostname | other-routing-engine | scc-master) {
    facility severity;
    explicit-priority;
    facility-override facility;
    log-prefix string;
    match "regular-expression";
    source-address source-address;
    structured-data {
        brief;
    }
}
```

```
    }  
  }  
  source-address source-address;  
  time-format (year | millisecond | year millisecond);  
  user (username | *) {  
    facility severity;  
    match "regular-expression";  
  }  
}  
tacplus-options {  
  service-name service-name;  
  (no-cmd-attribute-value | exclude-cmd-attribute);  
}  
tacplus-server server-address {  
  secret password;  
  single-connection;  
  source-address source-address;  
  timeout seconds;  
}  
time-zone (GMThour-offset | time-zone);  
}  
tracing {  
  destination-override {  
    syslog host;  
  }  
}  
use-imported-time-zones;  
}
```

accounting

Syntax

```
accounting {
  events [ login change-log interactive-commands ];
  destination {
    radius {
      server {
        server-address {
          accounting-port port-number;
          secret password;
          source-address address;
          retry number;
          timeout seconds;
        }
      }
    }
    tacplus {
      server {
        server-address {
          port port-number;
          secret password;
          single-connection;
          timeout seconds;
        }
      }
    }
  }
}
```

Hierarchy Level [edit [system](#)]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Configure audit of TACACS+ or RADIUS authentication events, configuration changes, and interactive commands.

Options The remaining statements are explained separately.

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

Related Documentation

- [Configuring RADIUS System Accounting on page 63](#)
- [Configuring TACACS+ System Accounting on page 66](#)

access-end

Syntax	access-end <i>HH:MM</i> ;
Hierarchy Level	[edit system login class]
Release Information	Statement introduced in Junos OS Release 10.1.
Description	Configure the end time for login access.
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">• Configuring Time-Based User Access on page 30

access-start

Syntax	access-start <i>HH:MM</i> ;
Hierarchy Level	[edit system login class]
Release Information	Statement introduced in Junos OS Release 10.1.
Description	Configure the start time for login access.
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">• Configuring Time-Based User Access on page 30

accounting-port (RADIUS Server)

Syntax	<code>accounting-port <i>port-number</i>;</code>
Hierarchy Level	[edit system accounting destination radius server <i>server-address</i>], [edit system radius-server <i>server-address</i>]
Release Information	Statement introduced in Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Configure the accounting port number on which to contact the RADIUS server.
Options	<i>number</i> —Port number on which to contact the RADIUS server. Default: 1813
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring RADIUS Authentication on page 53• Configuring RADIUS System Accounting on page 63

allow-commands

Syntax	<code>allow-commands "<i>regular-expression</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	Specify the operational mode commands that members of a login class can use.
Default	If you omit this statement and the deny-commands statement, users can issue only those commands for which they have access privileges through the permissions statement.
Options	<i>regular-expression</i> —Extended (modern) regular expression as defined in POSIX 1003.2. If the regular expression contains any spaces, operators, or wildcard characters, enclose it in quotation marks.
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">• Specifying Access Privileges for Junos OS Operational Mode Commands on page 32• deny-commands on page 98• user on page 134

allow-configuration

Syntax	<code>allow-configuration "regular-expression";</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	Explicitly allow configuration access to the specified levels in the hierarchy even if the permissions set with the permissions statement do not grant such access by default.
Default	If you omit this statement and the deny-configuration statement, users can edit only those commands for which they have access privileges through the permissions statement.
Options	regular-expression —Extended (modern) regular expression as defined in POSIX 1003.2. If the regular expression contains any spaces, operators, or wildcard characters, enclose it in quotation marks.
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"> • Specifying Access Privileges Using allow/deny-configuration Statements on page 40 • Regular Expressions for Allowing and Denying Junos OS Configuration Mode Hierarchies on page 35 • deny-configuration on page 99 • user on page 134

allow-configuration-regexps

Syntax	<code>allow-configuration-regexps "regular expression 1" "regular expression 2";</code>
Hierarchy Level	[edit system login class <i>class-name</i>]
Release Information	Statement introduced in Junos OS Release 11.2.
Description	<p>Explicitly allow configuration access to specified hierarchies using regular expressions even if the permissions set with the permissions statement allow that access. .</p> <p>The statement deny-configuration-regexps takes precedence if it is used in the same login class definition.</p>
Default	If you do not configure this statement or the deny-configuration-regexps statement, users can edit only those commands for which they have access privileges set with the permissions statement.
Options	<p>regular expression—Extended (modern) regular expression as defined in POSIX 1003.2. If the regular expression contains any spaces, operators, or wildcard characters, enclose it in quotation marks. Enter as many expressions as needed..</p>
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 34• Regular Expressions for Allowing and Denying Junos OS Configuration Mode Hierarchies on page 35• deny-configuration-regexps on page 100• user on page 134

allowed-days

Syntax	<code>allowed-days [<i>days-of-the-week</i>];</code>
Hierarchy Level	[edit system login class <i>class-name</i>]
Release Information	Statement introduced in Junos OS Release 10.1.
Description	Specify the days of the week when users can log in.
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• Configuring Time-Based User Access on page 30

authentication (Login)

Syntax	<pre>authentication { (encrypted-password "password" plain-text-password); load-key-file URL filename; ssh-dsa "public-key"; ssh-ecdsa "public-key"; ssh-rsa "public-key"; }</pre>
Hierarchy Level	[edit system login user <i>username</i>]
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>
Description	Authentication methods that a user can use to log in to the router or switch. You can assign multiple authentication methods to a single user.
Options	<p>encrypted-password "password"—Message Digest 5 (MD5) or other encrypted authentication. Specify the MD5 or other password. You can specify only one encrypted password for each user.</p> <p>You cannot configure a blank password for encrypted-password using blank quotation marks (" "). You must configure a password whose number of characters range from 1 through 128 characters and enclose the password in quotation marks.</p> <p>load-key-file URL filename—Load previously-generated RSA (SSH version 1 and SSH version 2) and DSA (SSH version 2) public keys from a named file at a specified URL location. The file contains one or more SSH keys.</p> <p>plain-text-password—When using this option, the command-line interface (CLI) prompts you for the password and then encrypts it.</p> <p>ssh-dsa "public-key"—SSH version 2 authentication. Specify the DSA public key. You can specify one or more public keys for each user.</p> <p>ssh-ecdsa "public-key"—SSH version 2 authentication. Specify the ECDSA public key. You can specify one or more public keys for each user.</p> <p>ssh-rsa "public-key"—SSH version 1 and SSH version 2 authentication. Specify the RSA public key. You can specify one or more public keys for each user.</p>
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Junos OS User Accounts on page 28 • root-authentication

authentication-order

Syntax	<code>authentication-order [<i>authentication-methods</i>];</code>
Hierarchy Level	[edit system]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Configure the order in which the software tries different user authentication methods when attempting to authenticate a user. For each login attempt, the software tries the authentication methods in order, starting with the first one, until the password matches.
Default	If you do not include the authentication-order statement, users are verified based on their configured passwords.
Options	<i>authentication-methods</i> —One or more authentication methods, listed in the order in which they should be tried. The method can be one or more of the following: <ul style="list-style-type: none">• password—Use the password configured for the user with the authentication statement at the [edit system login user] hierarchy level.• radius—Use RADIUS authentication services.• tacplus—Use TACACS+ authentication services.
Required Privilege Level	system —To view this statement in the configuration. system-control —To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring the Junos OS Authentication Order for RADIUS, TACACS+, and Local Password Authentication on page 46• authentication on page 93

backoff-factor

Syntax	<code>backoff-factor <i>seconds</i>;</code>
Hierarchy Level	<code>[edit system login retry-options]</code>
Release Information	Statement introduced in Junos OS Release 8.0.
Description	Configure the length of delay after each failed login attempt, which increases for each subsequent login attempt after the value specified in the backoff-threshold statement.
Options	<p><i>seconds</i>—Length of delay after each failed login attempt. The length of delay increases by this value for each subsequent login attempt after the value specified in the backoff-threshold option.</p> <p>Range: 5 through 10</p> <p>Default: 5</p>
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Limiting the Number of User Login Attempts for SSH and Telnet Sessions on page 29 • retry-options on page 123

backoff-threshold

Syntax	<code>backoff-threshold <i>number</i>;</code>
Hierarchy Level	<code>[edit system login retry-options]</code>
Release Information	Statement introduced in Junos OS Release 8.0.
Description	Configure the threshold for the number of failed login attempts on the router before the user experiences a delay when attempting to reenter a password.
Options	<p><i>number</i>—Threshold for the number of failed login attempts before the user experiences a delay when attempting to reenter a password. Use the backoff-factor option to specify the length of delay, in seconds.</p> <p>Range: 1 through 3</p> <p>Default: 2</p>
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Limiting the Number of User Login Attempts for SSH and Telnet Sessions on page 29 • retry-options on page 123

change-type

Syntax	<code>change-type (character-sets set-transitions);</code>
Hierarchy Level	[edit system login password]
Release Information	Statement introduced in Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Set requirements for using character sets in plain-text passwords. When you combine this statement with the minimum-changes statement, you can check for the total number of character sets included in the password or for the total number of character-set changes in the password. Newly created passwords must meet these requirements.
Options	Specify one of the following: <ul style="list-style-type: none">• character-sets—The number of character sets in the password. Valid character sets include uppercase letters, lowercase letters, numbers, punctuation, and other special characters.• set-transitions—The number of transitions between character sets.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Special Requirements for Junos OS Plain-Text Passwords on page 20• minimum-changes on page 109

class (Assigning a Class to an Individual User)

Syntax	<code>class class-name;</code>
Hierarchy Level	[edit system login user <i>username</i>]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Configure a user's login class. You must configure one class for each user.
Options	class-name —One of the classes defined at the [edit system login class] hierarchy level.
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">• Configuring Junos OS User Accounts on page 28

class (Defining Login Classes)

Syntax	<pre> class <i>class-name</i> { allow-commands "<i>regular-expression</i>"; (allow-configuration allow-configuration-regexps) "<i>regular expression 1</i>" "<i>regular expression 2</i>"; configuration-breadcrumbs; deny-commands "<i>regular-expression</i>"; (deny-configuration deny-configuration-regexps) "<i>regular expression 1</i>" "<i>regular expression 2</i>"; idle-timeout <i>minutes</i>; login-script <i>filename</i>; login-tip; permissions [<i>permissions</i>]; } </pre>
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	Define a login class.
Options	<p><i>class-name</i>—A name you choose for the login class.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Defining Junos OS Login Classes on page 28 • user on page 134

deny-commands

Syntax	<code>deny-commands "regular-expression";</code>
Hierarchy Level	[edit system login class]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Specify the operational mode commands that the user is denied permission to issue even though the permissions set with the permissions statement would allow it.
Default	If you omit this statement and the allow-commands statement, users can issue only those commands for which they have access privileges through the permissions statement.
Options	regular-expression —Extended (modern) regular expression as defined in POSIX 1003.2. If the regular expression contains any spaces, operators, or wildcard characters, enclose it in quotation marks.
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">• Specifying Access Privileges for Junos OS Operational Mode Commands on page 32• allow-commands on page 90• user on page 134

deny-configuration

Syntax	<code>deny-configuration "regular-expression";</code>
Hierarchy Level	[edit system login class]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Explicitly deny configuration access to the specified levels in the hierarchy even if the permissions set with the permissions statement grant such access by default.
Default	If you omit this statement and the allow-configuration statement, users can edit those levels in the configuration hierarchy for which they have access privileges through the permissions statement.
Options	regular-expression —Extended (modern) regular expression as defined in POSIX 1003.2. If the regular expression contains any spaces, operators, or wildcard characters, enclose it in quotation marks.
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"> • Specifying Access Privileges Using allow/deny-configuration Statements on page 40 • allow-configuration on page 91 • user on page 134

deny-configuration-regexps

Syntax	<code>deny-configuration-regexps "regular expression 1" "regular expression 2";</code>
Hierarchy Level	[edit system login class <i>class-name</i>]
Release Information	Statement introduced in Junos OS Release 11.2.
Description	<p>Explicitly deny configuration access to specified hierarchies using regular expressions even if the permissions set with the permissions statement allow that access.</p> <p>Expressions configured with this statement take precedence over allow-configuration-regexps if the two statements are used in the same login class definition.</p>
Default	If you do not configure this statement or the deny-configuration-regexps statement, users can edit only those commands for which they have access privileges set with the permissions statement.
Options	<p>regular expression—Extended (modern) regular expression as defined in POSIX 1003.2.</p> <p>If the regular expression contains any spaces, operators, or wildcard characters, enclose it in quotation marks. Enter as many expressions as needed.</p>
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 34• allow-configuration-regexps on page 92• user on page 134

destination (Accounting)

```
Syntax destination {
    radius {
        server {
            server-address {
                accounting-port port-number;
                secret password;
                source-address address;
                retry number;
                timeout seconds;
            }
        }
    }
    tacplus {
        server {
            server-address {
                port port-number;
                secret password;
                single-connection;
                timeout seconds;
            }
        }
    }
}
```

Hierarchy Level [edit system [accounting](#)]

Release Information Statement introduced before Junos OS Release 7.4.
radius statement added in Junos OS Release 7.4.
 Statement introduced in Junos OS Release 9.0 for EX Series switches.
 Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description Configure the authentication server.

Options The remaining statements are explained separately.

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

Related Documentation

- [Configuring RADIUS System Accounting on page 63](#)
- [Configuring TACACS+ System Accounting on page 66](#)

dynamic-profile-options

Syntax	<code>dynamic-profile-options { versioning; }</code>
Hierarchy Level	[edit system]
Release Information	Statement introduced in Junos OS Release 11.4.
Description	Configure global dynamic profile options. The remaining statement is explained separately.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">Enabling Dynamic Profiles to use Multiple Versions

format

Syntax	<code>format (md5 sha1);</code>
Hierarchy Level	[edit system login password]
Release Information	Statement introduced in Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Configure the authentication algorithm for plain-text passwords.
Default	For Junos OS, the default encryption format is md5 . For Junos-FIPS software, the default encryption format is sha1 .
Options	The hash algorithm that authenticates the password can be one of these algorithms: <ul style="list-style-type: none">md5—Produces a 128-bit digest.sha1—Produces a 160-bit digest.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">Special Requirements for Junos OS Plain-Text Passwords on page 20

full-name

Syntax	<code>full-name <i>complete-name</i>;</code>
Hierarchy Level	[edit system login user]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. Statement introduced in Junos OS Release 11.1 for the QFX Series.
Description	Configure the complete name of a user.
Options	<i>complete-name</i> —Full name of the user. If the name contains spaces, enclose it in quotation marks.
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"> • Configuring Junos OS User Accounts on page 28 • user on page 134 • user

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
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"> • Configuring the Timeout Value for Idle Login Sessions on page 43 • user on page 134

load-key-file

Syntax	<code>load-key-file URL filename;</code>
Hierarchy Level	[edit system root-authentication], [edit system login user <i>username</i> authentication]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. Statement introduced in Junos OS Release 11.1 for the QFX Series.
Description	Load RSA (SSH version 1 and SSH version 2) and DSA or ECDSA (SSH version 2) public keys from a previously-generated named file at a specified URL location. The file contains one or more SSH keys that are copied into the configuration when the command is issued.
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">• Configuring the Root Password• Configuring the Root Password• Configuring Junos OS User Accounts on page 28• Configuring Junos OS User Accounts

login

```
Syntax login {
    announcement text;
    class class-name {
        allow-commands "regular-expression";
        allow-configuration-regexps "regular expression 1" "regular expression 2";
        configuration-breadcrumbs;
        deny-commands "regular-expression";
        ( deny-configuration | deny-configuration-regexps ) "regular expression 1" "regular
            expression 2 ";
        idle-timeout minutes;
        login-script filename;
        login-tip;
        permissions [ permissions ];
    }
    message text;
    password {
        change-type (set-transitions | character-set);
        format (md5 | sha1 | des);
        maximum-length length;
        minimum-changes number;
        minimum-length length;
    }
    retry-options {
        backoff-threshold number;
        backoff-factor seconds;
        minimum-time seconds;
        tries-before-disconnect number;
    }
    user username {
        full-name complete-name;
        uid uid-value;
        class class-name;
        authentication authentication;
        (encrypted-password "password" | plain-text-password);
        ssh-rsa "public-key";
        ssh-dsa "public-key";
    }
}
```

Hierarchy Level [edit system]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Configure user access to the router or switch.



NOTE: The remaining statements are explained separately.

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

Related Documentation

- [Defining Junos OS Login Classes on page 28](#)

login-alarms

Syntax login-alarms;

Hierarchy Level [edit system login class *class-name*]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description Show system alarms automatically when an **admin** user logs in to the router or switch.

Options *class-name*—Login class name.

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

Related Documentation

- [Configuring System Alarms to Appear Automatically Upon Login on page 50](#)

login-script (Login)

Syntax login-script *filename*;

Hierarchy Level [edit system [login class](#) *class-name*]

Release Information Statement introduced in Junos OS Release 9.5.

Description Execute the specified op script when a user belonging to the class logs in to the CLI. The script must be enabled in the configuration.

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

Related Documentation

- [Executing an Op Script](#)

maximum-length

Syntax	maximum-length <i>length</i> ;
Hierarchy Level	[edit system login passwords]
Release Information	Statement introduced in Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Specify the maximum number of characters allowed in plain-text passwords. Newly created passwords must meet this requirement.
Default	For Junos-FIPS software, the maximum number of characters for plain-text passwords is 20. For Junos OS, no maximum is set.
Options	length —The maximum number of characters the password can include. Range: 1 to 64 characters
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Special Requirements for Junos OS Plain-Text Passwords on page 20 • Example: Changing the Requirements for Junos OS Plain-Text Passwords • password (Login) on page 116

maximum-time

Syntax	<code>maximum-time <i>seconds</i>;</code>
Hierarchy Level	<code>[edit system login retry-options]</code>
Release Information	Statement introduced in Junos OS Release 9.6.
Description	Configure the maximum time available for the user to enter the username and password for logging on to a router before the connection is closed.
Options	<p><i>seconds</i>—Maximum length of time that the connection remains open for the user to enter a username and password to log in. If the user remains idle and does not enter a username and password within the configured maximum-time, the connection is closed.</p> <p>Range: 20 through 300</p> <p>Default: 120</p>
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• Limiting the Number of User Login Attempts for SSH and Telnet Sessions on page 29• retry-options on page 123

minimum-changes

Syntax	<code>minimum-changes <i>number</i>;</code>
Hierarchy Level	[edit system login passwords]
Release Information	Statement introduced in Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	<p>Specify the minimum number of character sets (or character set changes) required in plain-text passwords. Newly created passwords must meet this requirement.</p> <p>This statement is used in combination with the change-type statement. If the change-type is character-sets, then the number of character sets included in the password is checked against the specified minimum. If change-type is set-transitions, then the number of character set changes in the password is checked against the specified minimum.</p>
Default	For Junos OS, the minimum number of changes is 1. For Junos-FIPS Software, the minimum number of changes is 3.
Options	<i>number</i> —The minimum number of character sets (or character set changes) required for the password.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Special Requirements for Junos OS Plain-Text Passwords on page 20 • change-type on page 96

minimum-length

Syntax	minimum-length <i>length</i> ;
Hierarchy Level	[edit system login passwords]
Release Information	Statement introduced in Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	<p>Specify the minimum number of characters required in plain-text passwords. Newly created passwords must meet this requirement.</p> <p>This statement can be used in combination with all of the other requirement options for plain-text passwords, such as minimum-upper-cases, minimum-punctuations, minimum-lower-cases, and so on.</p> <p>Using several password minimum requirement options will cause the minimum-length to be reset if the total sum of the required minimums exceeds the minimum-length setting.</p>
Default	For Junos OS, the minimum number of characters for plain-text passwords is six. For Junos-FIPS software, the minimum number of characters for plain-text passwords is 10.
Options	length —The minimum number of characters the password must include. Range: 6 to 20 characters
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Special Requirements for Junos OS Plain-Text Passwords on page 20• Example: Changing the Requirements for Junos OS Plain-Text Passwords• maximum-length on page 107

minimum-lower-cases

Syntax	<code>minimum-lower-cases <i>number</i>;</code>
Hierarchy Level	[edit system login password]
Release Information	Statement introduced in Junos OS Release 12.1.
Description	<p>Specify the minimum number of lower-case letters required in plain-text passwords. Newly created passwords must meet this requirement.</p> <p>This statement can be used in combination with all of the other requirement options for plain-text passwords, such as minimum-length, minimum-punctuations, minimum-upper-cases, and so on.</p> <p>Using several password minimum requirement options will cause the minimum-length to be reset if the total sum of the required minimums exceeds the minimum-length setting.</p>
Options	<i>number</i> —The minimum number of lower-case letters required for the password.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Special Requirements for Junos OS Plain-Text Passwords on page 20 • Example: Changing the Requirements for Junos OS Plain-Text Passwords • password (Login) on page 116

minimum-numeric

Syntax	<code>minimum-numeric <i>number</i>;</code>
Hierarchy Level	[edit system login password]
Release Information	Statement introduced in Junos OS Release 12.1.
Description	<p>Specify the minimum number of numeric class characters required in plain-text passwords. Newly created passwords must meet this requirement.</p> <p>This statement can be used in combination with all of the other requirement options for plain-text passwords, such as minimum-length, minimum-punctuations, minimum-lower-cases, and so on.</p> <p>Using several password minimum requirement options will cause the minimum-length to be reset if the total sum of the required minimums exceeds the minimum-length setting.</p>
Options	<i>number</i> —The minimum number of numeric class characters required for the password.
Required Privilege Level	<code>system</code> —To view this statement in the configuration. <code>system-control</code> —To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Special Requirements for Junos OS Plain-Text Passwords on page 20• Example: Changing the Requirements for Junos OS Plain-Text Passwords• password (Login) on page 116

minimum-punctuations

Syntax	<code>minimum-punctuations <i>number</i>;</code>
Hierarchy Level	[edit system login password]
Release Information	Statement introduced in Junos OS Release 12.1.
Description	<p>Specify the minimum number of punctuation class characters required in plain-text passwords. Newly created passwords must meet this requirement.</p> <p>This statement can be used in combination with all of the other requirement options for plain-text passwords, such as minimum-length, minimum-upper-cases, minimum-lower-cases, and so on.</p> <p>Using several password minimum requirement options will cause the minimum-length to be reset if the total sum of the required minimums exceeds the minimum-length setting.</p>
Options	<i>number</i> —The minimum number of punctuation class characters required for the password.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Special Requirements for Junos OS Plain-Text Passwords on page 20 • Example: Changing the Requirements for Junos OS Plain-Text Passwords • password (Login) on page 116

minimum-time

Syntax	minimum-time <i>seconds</i> ;
Hierarchy Level	[edit system login retry-options]
Release Information	Statement introduced in Junos OS Release 8.0.
Description	Configure the minimum time available for the user to enter a password to log on to a router before the connection is closed.
Options	<p><i>seconds</i>—Minimum length of time that the connection remains open while the user is attempting to enter a password to log in.</p> <p>Range: 20 through 60</p> <p>Default: 20</p>
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• Limiting the Number of User Login Attempts for SSH and Telnet Sessions on page 29• retry-options on page 123

minimum-upper-cases

Syntax	minimum-upper-cases <i>number</i> ;
Hierarchy Level	[edit system login password]
Release Information	Statement introduced in Junos OS Release 12.1.
Description	<p>Specify the minimum number of upper-case letters required in plain-text passwords. Newly created passwords must meet this requirement.</p> <p>This statement can be used in combination with all of the other requirement options for plain-text passwords, such as minimum-length, minimum-punctuations, minimum-lower-cases, and so on.</p> <p>Using several password minimum requirement options will cause the minimum-length to be reset if the total sum of the required minimums exceeds the minimum-length setting.</p>
Options	<i>number</i> —The minimum number of upper-case letters required for the password.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Special Requirements for Junos OS Plain-Text Passwords on page 20 • Example: Changing the Requirements for Junos OS Plain-Text Passwords • password (Login) on page 116

password (Login)

Syntax	<pre>password { change-type (set-transitions character-set); format (md5 sha1); maximum-length length; minimum-changes number; minimum-length length; minimum-lower-cases number; minimum-nums number; minimum-punctuations number; minimum-upper-cases number; }</pre>
Hierarchy Level	[edit system login]
Release Information	Statement introduced in Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	<p>Configure special requirements such as character length and encryption format for plain-text passwords. Newly created passwords must meet these requirements.</p> <p>Using several password minimum requirement options will cause the minimum-length to be reset if the total sum of the required minimums exceeds the minimum-length setting.</p> <p>The individual statements are explained separately.</p>
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Special Requirements for Junos OS Plain-Text Passwords on page 20• Example: Changing the Requirements for Junos OS Plain-Text Passwords

permissions

Syntax	<code>permissions [<i>permissions</i>];</code>
Hierarchy Level	[edit system login class]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Configure the login access privileges to be provided on the router or switch.
Options	<i>permissions</i> —Privilege type. For a list of permission flag types, see Table 4 on page 7 .
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"> • Configuring Access Privilege Levels on page 31 • user on page 134

port (RADIUS Server)

Syntax	<code>port <i>port-number</i>;</code>
Hierarchy Level	[edit system radius-server <i>address</i>], [edit system accounting destination radius server <i>address</i>]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. Statement introduced in Junos OS Release 11.1 for the QFX Series.
Description	Configure the port number on which to contact the RADIUS server.
Options	<i>number</i> —Port number on which to contact the RADIUS server. Default: 1812 (as specified in RFC 2865)



NOTE: The [edit system accounting] hierarchy is not available on QFabric systems.

Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring RADIUS Authentication on page 53 • Configuring RADIUS Authentication


port (TACACS+ Server)

Syntax	<code>port <i>port-number</i>;</code>
Hierarchy Level	[edit system accounting destination tacplus server <i>server-address</i>]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Configure the port number on which to contact the TACACS+ server.
Options	<i>number</i> —Port number on which to contact the TACACS+ server. Default: 49
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring TACACS+ System Accounting on page 66

radius (System)

Syntax	<pre>radius { server { server-address { accounting-port port-number; secret password; source-address address; retry number; timeout seconds; } } }</pre>
Hierarchy Level	[edit system accounting destination]
Release Information	<p>Statement introduced in 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>
Description	Configure the RADIUS accounting server.
Options	<p>server-address—Address of the RADIUS accounting server.</p> <p>The remaining statements are explained separately.</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"> • Configuring RADIUS System Accounting on page 63

radius-options (edit system)

Syntax	<pre>radius-options { attributes { nas-ip-address <i>ip-address</i>; } password-protocol <i>mschap-v2</i>; }</pre>
Hierarchy Level	[edit system]
Release Information	<p>Statement introduced in Junos OS Release 8.3.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>MS-CHAPv2 password protocol configuration option introduced in Junos OS Release 9.2.</p> <p>MS-CHAPv2 password protocol configuration option introduced in Junos OS Release 9.2 for EX Series switches.</p> <p>Statement introduced in Junos OS Release 11.1 for the QFX Series.</p>
	<div> NOTE: The <code>radius-options</code> statement is not available on QFabric systems.</div>
Description	Configure RADIUS options for the NAS-IP address for outgoing RADIUS packets and password protocol used in RADIUS packets.
Options	<p><code>nas-ip-address <i>ip-address</i></code>—IP address of the network access server (NAS) that requests user authentication.</p> <p><code>password-protocol <i>mschap-v2</i></code>—Protocol MS-CHAPv2, used for password authentication and password changing.</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">• Configuring MS-CHAPv2 for Password-Change Support on page 54• Configuring RADIUS Authentication

radius-server (System)

Syntax	<pre>radius-server server-address { accounting-port port-number; port number; retry number; secret password; source-address source-address; timeout seconds; }</pre>
Hierarchy Level	[edit system]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	<p>Configure a RADIUS server for Point-to-Point Protocol (PPP).</p> <p>To configure multiple RADIUS servers, include multiple radius-server statements. The servers are tried in order and in a round-robin fashion until a valid response is received from one of the servers or until all the configured retry limits are reached.</p>
Options	<p>server-address—Address of the RADIUS authentication server.</p> <p>The remaining statements are explained separately.</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"> • Configuring RADIUS Authentication on page 53

retry (RADIUS)

Syntax	<code>retry number;</code>
Hierarchy Level	[edit system radius-server server-address], [edit system accounting destination radius server <i>server-address</i>]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Number of times the router or switch is allowed to try to contact a RADIUS authentication or accounting server.
Options	<i>number</i> —Number of retries allowed for contacting a RADIUS server. Range: 1 through 10 Default: 3
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring RADIUS Authentication on page 53• Configuring RADIUS System Accounting on page 63• timeout on page 132

retry-options

Syntax	<pre> retry-options { backoff-factor <i>seconds</i>; backoff-threshold <i>number</i>; maximum-time <i>seconds</i>; minimum-time <i>seconds</i>; tries-before-disconnect <i>number</i>; } </pre>
Hierarchy Level	[edit system login]
Release Information	<p>Statement introduced in Junos OS Release 8.0.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>maximum-time option introduced in Junos OS Release 9.6.</p> <p>maximum-time option introduced in Junos OS Release 9.6 for EX Series switches.</p>
Description	Maximum number of times a user can attempt to enter a password while logging in through SSH or Telnet before being disconnected.
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Limiting the Number of User Login Attempts for SSH and Telnet Sessions on page 29 • rate-limit

secret

Syntax	<code>secret <i>password</i>;</code>
Hierarchy Level	[edit system accounting destination radius server <i>server-address</i>], [edit system accounting destination tacplus server <i>server-address</i>], [edit system radius-server <i>server-address</i>], [edit system tacplus-server <i>server-address</i>]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Configure the password to use with the RADIUS or TACACS+ server. The secret password used by the local router or switch must match that used by the server.
Options	<i>password</i> —Password to use; can include spaces included in quotation marks.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring RADIUS Authentication on page 53• Configuring TACACS+ Authentication on page 59• Configuring TACACS+ System Accounting on page 66• Configuring RADIUS System Accounting on page 63

server (RADIUS Accounting)

Syntax	<pre>server { server-address { accounting-port port-number; retry number secret password; source-address address; timeout seconds; } }</pre>
Hierarchy Level	[edit system accounting destination radius]
Release Information	Statement introduced in Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Configure RADIUS logging. The remaining statements are explained separately.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring RADIUS System Accounting on page 63

server (TACACS+ Accounting)

Syntax	<pre>server { server-address { port port-number; secret password; single-connection; timeout seconds; } }</pre>
Hierarchy Level	[edit system accounting destination tacplus]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Configure TACACS+ logging. The remaining statements are explained separately.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring TACACS+ System Accounting on page 66

single-connection

Syntax	single-connection;
Hierarchy Level	[edit system accounting destination tacplus-server <i>server-address</i>] [edit system tacplus-server <i>server-address</i>],
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Optimize attempts to connect to a TACACS+ server. The software maintains one open TCP connection to the server for multiple requests rather than opening a connection for each connection attempt.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring TACACS+ Authentication on page 59• Configuring TACACS+ System Accounting on page 66

source-address (NTP, RADIUS, System Logging, or TACACS+)

Syntax	<code>source-address <i>source-address</i>;</code>
Hierarchy Level	<p>[edit system accounting destination radius server <i>server-address</i>],</p> <p>[edit system accounting destination tacplus server <i>server-address</i>],</p> <p>[edit system ntp],</p> <p>[edit system radius-server <i>server-address</i>],</p> <p>[edit system syslog],</p> <p>[edit system tacplus-server <i>server-address</i>]</p>
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>
Description	Specify a source address for each configured TACACS+ server, RADIUS server, NTP server, or the source address to record in system log messages that are directed to a remote machine.
Options	<p><i>source-address</i>—A valid IP address configured on one of the router or switch interfaces.</p> <p>For system logging, the address is recorded as the message source in messages sent to the remote machines specified in all host <i>hostname</i> statements at the [edit system syslog] hierarchy level, but not for messages directed to the other Routing Engine or to the TX Matrix router or TX Matrix Plus router in a routing matrix based on a TX Matrix router or TX Matrix Plus router.</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"> • Specifying a Source Address for the Junos OS to Access External RADIUS Servers on page 55 • Synchronizing and Coordinating Time Distribution Using NTP • Specifying an Alternative Source Address for System Log Messages

source-port (Port Addresses)

Syntax	source-port upper-limit <upper-limit>;
Hierarchy Level	[edit system internet-options]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 11.1 for the QFX Series.
Description	Configure the range of port addresses.
Options	upper-limit <i>upper-limit</i> —(Optional) The range of port addresses and can be a value from 5000 through 65,355.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">Configuring the Junos OS to Extend the Default Port Address Range

system

Syntax	system { ... }
Hierarchy Level	[edit]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Configure system management properties.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">System Management Configuration Statements on page 81

tacplus

Syntax	<pre> tacplus { server { server-address { port <i>port-number</i>; secret <i>password</i>; single-connection; timeout <i>seconds</i>; } } } </pre>
Hierarchy Level	[edit system accounting destination]
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>
Description	Configure the Terminal Access Controller Access Control System Plus (TACACS+).
Options	<p><i>server-address</i>—Address of the TACACS+ authentication server.</p> <p>The remaining statements are explained separately.</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"> • Configuring TACACS+ System Accounting on page 66

tacplus-options

Syntax	<pre>tacplus-options { (exclude-cmd-attribute no-cmd-attribute-value); service-name <i>service-name</i>; timestamp-and-timezone; }</pre>
Hierarchy Level	[edit system]
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>Options for no-cmd-attribute-value and exclude-cmd-attribute introduced in Junos OS Release 9.3.</p> <p>Statement introduced in Junos OS Release 11.1 for QFX Series.</p> <p>Option for timestamp-and-timezone introduced in Junos OS Release 12.2.</p>
Description	Configure TACACS+ options for authentication and accounting.
Options	<p>exclude-cmd-attribute—Exclude the cmd attribute value completely from start and stop accounting records to enable logging of accounting records in the correct log file on a TACACS+ server.</p> <p>no-cmd-attribute-value—Set the cmd attribute value to an empty string in the TACACS+ accounting start and stop requests to enable logging of accounting records in the correct log file on a TACACS+ server.</p> <p>service-name <i>service-name</i>—Name of the authentication service used when you configure multiple TACACS+ servers to use the same authentication service.</p> <p>Default: junos-exec</p> <p>timestamp-and-timezone—Include this statement if you want start time, stop time, and timezone attributes included in start/stop accounting records.</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">• Configuring the Same Authentication Service for Multiple TACACS+ Servers on page 61• Configuring TACACS+ Server Accounting on page 67• Junos OS Authentication Order for RADIUS, TACACS+, and Password Authentication on page 13• Configuring TACACS+ Authentication• Configuring TACACS+ System Accounting

tacplus-server

Syntax	<pre>tacplus-server server-address { secret password; single-connection; source-address source-address; timeout seconds; }</pre>
Hierarchy Level	[edit system]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Configure the TACACS+ server.
Options	server-address —Address of the TACACS+ authentication server. The remaining statements are explained separately.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring TACACS+ Authentication on page 59

timeout (System)

Syntax	<code>timeout <i>seconds</i>;</code>
Hierarchy Level	[edit system radius-server <i>server-address</i>], [edit system tacplus-server <i>server-address</i>], [edit system accounting destination radius server <i>server-address</i>], [edit system accounting destination tacplus server <i>server-address</i>]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Configure the amount of time that the local router or switch waits to receive a response from a RADIUS or TACACS+ server.
Options	<i>seconds</i> —Amount of time to wait. Range: 1 through 90 seconds Default: 3 seconds
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring RADIUS Authentication on page 53• Configuring TACACS+ Authentication on page 59• retry on page 122

tries-before-disconnect

Syntax	<code>tries-before-disconnect <i>number</i>;</code>
Hierarchy Level	[edit system login retry-options]
Release Information	Statement introduced in Junos OS Release 8.0.
Description	Configure the maximum number of times the user is allowed to enter a password to attempt to log in to the router through SSH or Telnet.
Options	<i>number</i> —Maximum number of times a user is allowed to attempt to enter a password to log in through SSH or Telnet. Range: 1 through 10 Default: 10
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">• Limiting the Number of User Login Attempts for SSH and Telnet Sessions on page 29• retry-options on page 123

uid

Syntax	<code>uid <i>uid-value</i>;</code>
Hierarchy Level	[edit system login user]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Numeric identifier associated with the user account name, either assigned by an administrator or assigned automatically when you commit the user configuration. It is used by applications that request numeric identifiers, such as some RADIUS queries or secure applications such as flow-tap monitoring.
Options	<i>uid-value</i> —Number associated with the login account. This value must be unique on the router or switch. Range: 100 through 64000
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">• Configuring Junos OS User Accounts on page 28

user (Access)

Syntax	<pre>user username { authentication { class class-name; (encrypted-password "password" plain-text-password); full-name complete-name; load-key-file URL filename; ssh-dsa "public-key" <from hostname>; ssh-rsa "public-key" <from hostname>; uid uid-value; } }</pre>
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	Configure access permission for individual users.
Options	The remaining statements are explained separately.
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">• Configuring Junos OS User Accounts on page 28• class on page 96

versioning

Syntax	versioning;
Hierarchy Level	[edit system dynamic-profile-options]
Release Information	Statement introduced in Junos OS Release 11.4.
Description	Enable version support for dynamic profiles on the system.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Enabling Dynamic Profiles to use Multiple Versions

PART 3

Administration

- [Routine Monitoring on page 137](#)

CHAPTER 7

Routine Monitoring

show system users

Syntax	show system users <no-resolve>
Syntax (TX Matrix Router)	show system users <all-chassis all-lcc <i>lccnumber</i> scc> <no-resolve>
Syntax (TX Matrix Plus Router)	show system users <detail> <all-chassis all-lcc <i>lcc number</i> <i>sfc number</i> > <no-resolve>
Syntax (MX Series Router)	show system users <all-members> <local> <member <i>member-id</i> > <no-resolve>
Release Information	Command introduced before Junos OS Release 7.4. Command introduced in Junos OS Release 9.0 for EX Series switches. sfc option introduced for the TX Matrix Plus router in JUNOS Release 9.6. Command introduced in Junos OS Release 11.1 for the QFX Series.
Description	List information about the users who are currently logged in to the router or switch.



NOTE: The **show system users** command lists the information about administrative users that are logged in to a router or switch using the CLI, J-Web, or an SSH client. The output does not list information about web users or automated users that are logged in from a remote client application using Junos XML APIs, such as NETCONF.

Options	<p>none—List information about the users who are currently logged in to the router or switch.</p> <p>all-chassis—(TX Matrix and TX Matrix Plus routers only) (Optional) Show users currently logged in to all the routers in the chassis.</p> <p>all-lcc—(TX Matrix and TX Matrix Plus routers only) (Optional) On a TX Matrix router, show users currently logged in to all T640 routers (or line-card chassis) connected to the TX Matrix router. On a TX Matrix Plus router, show users currently logged in to all T1600 routers (or line-card chassis) connected to the TX Matrix Plus router.</p> <p>all-members—(MX Series routers only) (Optional) Display users currently logged in to all members of the Virtual Chassis configuration.</p> <p>lccnumber—(TX Matrix and TX Matrix Plus routers only) (Optional) On a TX Matrix router, show users currently logged in to a specific T640 router that is connected to the TX Matrix router. On a TX Matrix Plus router, show users currently logged in to a specific</p>
----------------	---

T1600 router that is connected to the TX Matrix Plus router. Replace **number** with a value from 0 through 3.

local—(MX Series routers only) (Optional) Display users currently logged in to the local Virtual Chassis member.

member member-id—(MX Series routers only) (Optional) Display users currently logged in to the specified member of the Virtual Chassis configuration. Replace **member-id** with a value of 0 or 1.

no-resolve—(Optional) Do not attempt to resolve IP addresses to hostnames.

scc—(TX Matrix routers only) (Optional) Show users currently logged in to the TX Matrix router (or switch-card chassis).

sfc number—(TX Matrix Plus routers only) (Optional) Show users currently logged in to the TX Matrix Plus router (or switch-fabric chassis). Replace **number** with 0.

Additional Information By default, when you issue the **show system users** command on a TX Matrix or TX Matrix Plus master Routing Engine, the command is broadcast to all the T640 (in a routing matrix based on a TX Matrix router) or T1600 (in a routing matrix based on a TX Matrix Plus router) master Routing Engines connected to it. Likewise, if you issue the same command on the TX Matrix or TX Matrix Plus backup Routing Engine, the command is broadcast to all the T640 (in a routing matrix based on a TX Matrix router) or T1600 (in a routing matrix based on a TX Matrix Plus router) backup Routing Engines that are connected to it.

Required Privilege Level view

List of Sample Output [show system users on page 140](#)
[show system users lcc no-resolve \(TX Matrix and TX Matrix Plus Router\) on page 140](#)
[show system users \(TX Matrix Plus Router\) on page 140](#)
[show system users \(QFX Series\) on page 141](#)
[show system users no-resolve \(QFX Series\) on page 141](#)

Output Fields [Table 12 on page 139](#) describes the output fields for the **show system users** command. Output fields are listed in the approximate order in which they appear.

Table 12: show system users Output Fields

Field Name	Field Description
time and up	Current time, in the local time zone, and how long the router or switch has been operational.
users	Number of users logged in to the router or switch.
load averages	Load averages for the last 1 minute, 5 minutes, and 15 minutes.
USER	Username.
TTY	Terminal through which the user is logged in.

Table 12: show system users Output Fields (*continued*)

Field Name	Field Description
FROM	System from which the user has logged in. A hyphen indicates that the user is logged in through the console.
LOGIN@	Time when the user logged in.
IDLE	How long the user has been idle.
WHAT	Processes that the user is running.

Sample Output

```

show system users user@host> show system users
7:30PM up 4 days, 2:26, 2 users, load averages: 0.07, 0.02, 0.01
USER   TTY FROM          LOGIN@  IDLE WHAT
root   d0  -              Fri05PM 4days -csh (csh)
blue   p0  level5.company.net 7:30PM  - cli

```

```

show system users lcc user@host> show system users lcc 2 no-resolve
no-resolve (TX Matrix lcc2-re0:
and TX Matrix Plus Router)
10:34AM PDT up 1 day, 7:11, 5 users, load averages: 0.03, 0.01, 0.00
USER   TTY FROM          LOGIN@  IDLE WHAT
root   d0  -              3:21AM  7:12 /bin/csh
regress p0  scc-re0        10:15AM  - telnet hostA
regress p1  scc-re0        10:16AM  - telnet hostA
regress p2  scc-re0        10:19AM  - telnet hostA
regress p3  scc-re0        10:24AM  - telnet hostA

```

```

show system users (TX user@host> show system users
Matrix Plus Router) sfc0-re0:
-----
1:41AM up 26 mins, 3 users, load averages: 0.08, 0.04, 0.03
USER   TTY FROM          LOGIN@  IDLE WHAT
regress p0  10.209.208.123 1:18AM  21 cli
regress p1  172.17.29.207 1:37AM  2 cli
regress p2  172.17.28.19 1:40AM  - cli

lcc0-re0:
-----
1:41AM up 26 mins, 0 users, load averages: 0.00, 0.00, 0.03

lcc1-re0:
-----
1:41AM up 26 mins, 0 users, load averages: 0.00, 0.02, 0.03

lcc2-re0:
-----
1:41AM up 26 mins, 0 users, load averages: 0.16, 0.06, 0.02

lcc3-re0:
-----
1:41AM up 26 mins, 0 users, load averages: 0.12, 0.04, 0.04

```

```
regress@aj> show system users
sfc0-re0:
```

```
-----
1:42AM up 28 mins, 4 users, load averages: 0.02, 0.03, 0.02
USER      TTY      FROM                                LOGIN@  IDLE WHAT
regress   p0        pssraj-t61.jnpr.net                1:18AM   22 cli
regress   p1        eng-shell4.juniper.net              1:37AM   - cli
regress   p2        bigpink.juniper.net                 1:40AM   - cli
regress   p3        sv-cutty-01.englab.juniper.net      1:42AM   - -csh (csh)
```

```
lcc0-re0:
```

```
-----
1:42AM up 28 mins, 0 users, load averages: 0.02, 0.01, 0.03
```

```
lcc1-re0:
```

```
-----
1:42AM up 28 mins, 0 users, load averages: 0.07, 0.04, 0.03
```

```
lcc2-re0:
```

```
-----
1:42AM up 27 mins, 0 users, load averages: 0.07, 0.06, 0.02
```

```
lcc3-re0:
```

```
-----
1:42AM up 28 mins, 0 users, load averages: 0.05, 0.04, 0.04
```

**show system users
(QFX Series)**

```
user@switch> show system users
USER      TTY      FROM                                LOGIN@  IDLE WHAT
tlewis    p0        172.22.18.117                      2:54AM   39 -cli (cli)
tlewis    p1        172.22.18.117                      3:01AM   - -cli (cli)
tcheng    p2        172.22.17.197                      3:08AM   11 -cli (cli)
```

**show system users
no-resolve (QFX
Series)**

```
user@switch> show system users no-resolve
USER      TTY      FROM                                LOGIN@  IDLE WHAT
tlewis    p0        172.22.18.117                      2:54AM   39 -cli (cli)
tlewis    p1        172.22.18.117                      3:01AM   - -cli (cli)
tcheng    p2        172.22.17.197                      3:08AM   11 -cli (cli)
```

test access profile

Syntax	<code>test access profile <i>profile-name</i> user <i>username</i> password <i>password</i> <detail></code>
Release Information	Command introduced in Junos OS Release 9.1.
Description	Specify a profile to use to get information from a RADIUS server, which includes all the information from the test access radius-server command.
Options	<p>detail—(Optional) Show the RADIUS attributes returned by the server.</p> <p>profile-name—Access profile name configured.</p> <p>password—Password for the username.</p> <p>username—User name to be authenticated to the RADIUS server.</p>
Required Privilege Level	view
List of Sample Output	<p>test access profile on page 143</p> <p>test access profile detail on page 143</p>
Output Fields	Table 13 on page 142 lists the output fields for the test access profile command. Output fields are listed in the approximate order in which they appear.

Table 13: test access profile Output Fields

Field Name	Field Description
Profile Name	Name of the configured access profile.
Client Username	The user name authenticated by the RADIUS server.
Client Password	The user password authenticated by the RADIUS server.
Num Servers	Number of RADIUS servers in the configured access profile.
Server List	List of RADIUS servers in the configure access profile.
IP Address	The IP address of the RADIUS server authenticated.
UDP Port	The RADIUS server port utilized during the authentication test.
Source Address	The source IP address of the client making the RADIUS request. If no address is shown, it defaults to the address of the outgoing interface.
Timeout	The RADIUS server timeout period.
Retry Count	The number of authentication attempts allowed by the RADIUS server.

Table 13: test access profile Output Fields (*continued*)

Field Name	Field Description
Secret	The shared secret used for authentication with the RADIUS server.
Status	The test result status (Accepted or Rejected) and the number of retransmits utilized during authentication.
Attempts	The number of authentication attempts on the RADIUS server.
Attribute List	The list of returned RADIUS attributes, sorted by the attribute name, and including parameter length and value. See your RADIUS server documentation for attribute descriptions.
(Attribute) Name	The name of the attribute.
(Attribute) Length	The attribute length in bytes.
(Attribute) Value	The attribute value.

Sample Output

test access profile The following example uses the **test access profile** command to access and display basic information about the RADIUS server(s) shown in the resulting output:

```

user@host> test access profile alpha user TEST password TEST
user@host> test access profile alpha user TEST password TEST
Test Radius Profile Access
  Profile Name       : alpha
  Client Username    : TEST
  Client Password    : TEST
  Num Servers        : 5
      Server List
    IP Address      UDP   Source      Retry
    Attempts        Port  Address      Timeout Count Secret  Status
1.1.1.1            1812  10.10.10.10  2        1    TEST   Timeout
2
1.2.3.4            1812  Default      1        2    TEST   Timeout
3
192.168.10.10     1812  Default      3        3    TEST   Accepted
1

```

test access profile detail The following example uses the **test access profile detail** command to access and display detailed information about the RADIUS server(s) shown in the resulting output:

```

user@host> test access profile alpha user TEST password TEST detail
user@host> test access profile alpha user TEST password TEST detail
Test Radius Profile Access Detailed
  Profile Name       : alpha
  Client Username    : TEST
  Client Password    : TEST
  Num Servers        : 5
      Radius Server List

```

```

IP Address      : 1.2.3.4
UDP Port        : 1812
Source Address  : 192.168.10.10
Timeout        : 2
Retry Count     : 1
Secret          : TEST
Status         : Timeout
Attempts       : 2

```

```

IP Address      : 1.2.3.5
UDP Port        : 1812
Source Address  : Default
Timeout        : 1
Retry Count     : 2
Secret          : TEST
Status         : Timeout
Attempts       : 3

```

```

IP Address      : 192.168.10.10
UDP Port        : 1812
Source Address  : Default
Timeout        : 3
Retry Count     : 3
Secret          : TEST
Status         : Accepted
Attempts       : 1

```

Attribute List

Name	Length	Value
Class	52	SBR2CLÍ%¿ð0%¿
Acct-Interim-Interval	4	5
Callback-Id	12	123-456-789
Callback-Number	13	555-555-1212
Class	15	Class information
Filter-Id	4	999
Filter-Id	6	12345
Framed-Compression	4	0
Framed-IP-Address	4	1:2:3:4
Framed-IP-Netmask	4	255:255:255:255
Framed-IPv6-Route	15	1:2:3:4:5:6:7:8
Framed-MTU	4	1024
Framed-Pool	9	pool sbr
Framed-Protocol	4	1
Framed-Route	8	iproute
Framed-Routing	4	0
Vendor-Specific	11	583
Idle-Timeout	4	3
Vendor-Specific	10	a4c
Vendor-Specific	14	a4c
Login-IP-Host	4	10:1:1:1
Login-LAT-Group	10	lat group
Login-LAT-Node	9	lat node
Login-LAT-Port	9	lat port
Login-LAT-Service	12	lat service
Login-Service	4	0
Login-TCP-Port	4	1812
Vendor-Specific	10	137
Vendor-Specific	38	137
Vendor-Specific	10	137

Vendor-Specific	9	137
Vendor-Specific	16	137
Vendor-Specific	10	137
Vendor-Specific	10	137
Vendor-Specific	10	137
Vendor-Specific	9	137
Vendor-Specific	10	137
Vendor-Specific	10	137
Vendor-Specific	10	137
Vendor-Specific	10	137
Password-Retry	4	3
Port-Limit	4	100
Prompt	4	
Reply-Message	18	Radius Server SB
Service-Type	4	2
Session-Timeout	4	10
Termination-Action	4	1
Tunnel-Assignment-ID	4	
Tunnel-Client-Auth-ID	6	
Tunnel-Client-Endpoint	4	
Tunnel-Password	19	
Tunnel-Type	4	12
MS BAP Usage	4	0
MS-CHAP MPPE-Keys	32	-1234567890
MS-CHAP2 Success	3	123456789
MS Filter	10	ms-filter
MS Link Drop Time Limit	4	5
MS Link Utilization Threshold	4	6
MS MPPE Encryption Policy	4	1
MS MPPE Encryption Types	3	-556677889
MS Primary DNS Server	4	1:1:1:1
MS Primary NBNS Server	4	2:2:2:2
MS Secondary DNS Server	4	3:3:3:3
MS Secondary NBNS Server	4	4:4:4:4

test access radius-server

Syntax `test access radius-server address user username password password secret secret
<authentication-port port>
<retry number>
<source-address address>
<timeout number>`

Release Information Command introduced in Junos OS Release 9.1.

Description Verify RADIUS server authentication parameters.

Options *address*—RADIUS server under test IP address.

password—Password for the user.

secret—Secret shared with the RADIUS server.

user—User name to be authenticated to the RADIUS server.

authentication-port—(Optional) RADIUS server authentication port number (1through 65535).

retry—(Optional) Retry attempts (1through 10).

source-address—(Optional) Use an alternate address as the source address.

timeout—(Optional) Request timeout period (1through 90 seconds).

Required Privilege Level view

List of Sample Output [test access radius-server user password secret on page 147](#)

Output Fields [Table 14 on page 146](#) lists the output fields for the **test access radius-server** command. Output fields are listed in the approximate order in which they appear.

Table 14: test access radius-server Output Fields

Field Name	Field Description
Server	The IP address of the RADIUS server authenticated.
UDP port	The RADIUS server port utilized during the authentication test.
Source IP Address	"Default" is shown if the IP address is the same as that of the RADIUS server. Alternatively, an IP address specified for authentication is shown.
Server timeout	The RADIUS server timeout period.
Sever retry count	The number of authentication attempts allowed by the RADIUS server.

Table 14: test access radius-server Output Fields (*continued*)

Field Name	Field Description
Secret	The shared secret used for authentication with the RADIUS server.
Client Username	The user name authenticated by the RADIUS server.
Client Password	The user password authenticated by the RADIUS server.
Status	The test result status (Accepted or Rejected) and the number of retransmits utilized during authentication.

Sample Output

test access radius-server user password secret The following example command tests RADIUS authentication with a specific server (172.28.30.95), user (JOHNDOE), secret (No1Knows), and password (JohnPass); and displays the resulting output:

```
user@host> test access radius-server 172.28.30.95 user JOHNDOE password JohnPass secret No1Knows
```

```
Test Radius Server Access
  Server           : 172.28.30.95
  UDP port         : 1812
  Source IP Address : Default
  Server timeout   : 3
  Sever retry count : 3
  Secret           : No1Knows
  Client Username   : JOHNDOE
  Client Password   : JohnPass
  Status            : Accepted, retransmits: 0
```


PART 4

Index

- [Index on page 151](#)

Index

Symbols

!	regular expression operator.....	33, 35
#	comments in configuration statements.....	xii
\$	regular expression operator.....	34, 36
()	regular expression operator.....	34, 36
(),	in syntax descriptions.....	xii
*	regular expression operator.....	36
+	regular expression operator.....	36
.	regular expression operator.....	36
< >	in syntax descriptions.....	xii
[]	in configuration statements.....	xii
\	regular expression operator.....	34, 36
^	regular expression operator.....	34, 35
{ }	in configuration statements.....	xii
(pipe)	in syntax descriptions.....	xii

A

access privilege levels	
configuration example.....	74
configuration mode hierarchies.....	36
operational mode commands.....	75
configuring.....	31
configuration mode hierarchies.....	34
operational mode commands.....	32
login classes.....	7
user accounts.....	4
access-end statement.....	89
access-start statement.....	89
accounting statement.....	88
authentication	
usage guidelines.....	63, 66
accounting-port statement	
RADIUS servers.....	90

allow-commands statement.....	90
usage guidelines.....	10
allow-configuration statement.....	91
allow-configuration-regexps statement.....	92
usage guidelines.....	10
allowed-days statement.....	92
allowing commands to login classes.....	10
announcement statement	
usage guidelines.....	49
announcements	
system login.....	49
authentication	
order.....	13, 46
protocol.....	22
RADIUS.....	19, 22, 44, 53
root password.....	20
shared user accounts.....	22, 44
TACACS+	19, 22, 44, 59
users.....	19
authentication statement	
login.....	93
usage guidelines.....	4, 28
authentication-order statement.....	94
usage guidelines.....	13, 46

B

backoff-factor statement.....	95
backoff-threshold statement.....	95
BGP	
security configuration example.....	76
braces, in configuration statements.....	xii
brackets	
angle, in syntax descriptions.....	xii
square, in configuration statements.....	xii

C

cables	
console port, connecting.....	78
Ethernet rollover, connecting.....	78
change-type statement.....	96
usage guidelines.....	20
class statement	
assigning to user.....	96
login.....	97
usage guidelines.....	3, 4, 28
commands	
allowing or denying to login classes.....	10
comments, in configuration statements.....	xii

console port	
adapter.....	78
conventions	
text and syntax.....	xi
Crypto Officer.....	6
user configuration.....	6
curly braces, in configuration statements.....	xii
customer support.....	xiii
contacting JTAC.....	xiii

D

deny-commands statement.....	98
usage guidelines.....	10
deny-configuration statement.....	99
deny-configuration-regexps statement	
usage guidelines.....	10
denying commands to login classes.....	10
destination statement.....	101
usage guidelines.....	63, 66
documentation	
comments on.....	xiii
dynamic-profile-options statement.....	102

E

encrypted passwords.....	20
encrypted-password option.....	20
Ethernet rollover cable, connecting the router to a	
management device.....	78
events statement	
usage guidelines.....	64, 66
exclude-cmd-attribute statement.....	130

F

FIPS.....	6
user configuration.....	6
<i>See also</i> Junos-FIPS	
flags	
login class.....	7
user permissions.....	7
font conventions.....	xi
format statement.....	102
full names, in user accounts.....	4
full-name statement.....	103
usage guidelines.....	4, 28

H

HMAC-MD5 authentication.....	22
------------------------------	----

I

idle timeout values	
login classes.....	43
idle-timeout statement.....	103
usage guidelines.....	43
IS-IS	
security configuration example.....	77

J

Juniper-Allow-Commands attribute (RADIUS).....	57
Juniper-Allow-Configuration attribute	
(RADIUS).....	58
Juniper-Configuration-Change attribute	
(RADIUS).....	58
Juniper-Deny-Commands attribute (RADIUS).....	58
Juniper-Deny-Configuration attribute	
(RADIUS).....	58
Juniper-Interactive-Command attribute	
(RADIUS).....	58
Juniper-Local-User-Name attribute (RADIUS).....	57
Juniper-User-Permissions attribute (RADIUS).....	59
Junos-FIPS	
password requirements.....	5, 22
user accounts.....	6

L

laptop <i>See</i> management device	
load-key-file command	
usage guidelines.....	4, 28
load-key-file statement.....	104
usage guidelines.....	4, 20, 28
local password authentication.....	44
local user	
template accounts.....	44
login announcements, system.....	49
login classes	
access privilege levels.....	7
commands, allowing or denying.....	10
defining.....	3
idle timeout values.....	43
security configuration example.....	43
login messages, system.....	48
login statement.....	105
usage guidelines.....	3, 4, 28, 29
login-alarms statement.....	106
usage guidelines.....	50
login-script statement.....	106

M

management device	
recovering root password from.....	77
manuals	
comments on.....	xiii
maximum-length statement.....	107
usage guidelines.....	20
maximum-time statement.....	108
MD5 authentication.....	22
message statement	
usage guidelines.....	48
messages	
system login.....	48
minimum-changes statement.....	109
usage guidelines.....	20
minimum-length statement.....	110
usage guidelines.....	20
minimum-lower-cases statement.....	111
minimum-nums statement.....	112
minimum-punctuations statement.....	113
minimum-time statement.....	114
minimum-upper-cases statement.....	115
ms-chapv2	
changing password ms-chapv2.....	54

N

no-cmd-attribute-value statement.....	130
---------------------------------------	-----

O

operators, regular expression.....	33, 35
------------------------------------	--------

P

parentheses, in syntax descriptions.....	xii
password statement	
login.....	116
passwords	
RADIUS.....	53
root.....	20
root password, recovering.....	77
shared user.....	44
passwords statement	
usage guidelines.....	20
PC See management device	
permission flags	
login class.....	7
user.....	7
permissions statement.....	117
usage guidelines.....	7

plain-text passwords	
for user accounts.....	5
root password.....	20
plain-text-password option.....	20
port statement	
RADIUS.....	117
TACACS+.....	118
usage guidelines.....	59
usage guidelines.....	53
ports	
RADIUS servers.....	53
protocols	
authentication.....	22

R

RADIUS accounting.....	63
RADIUS authentication.....	19, 53
security configuration example.....	56
TACACS+	44
RADIUS authorization See RADIUS authentication	
radius statement	
accounting.....	119
RADIUS templates	
security configuration example.....	57
radius-options statement	120
radius-server statement.....	121
usage guidelines.....	53
regular expression operators.....	33, 35
remote	
template account.....	44
retry statement.....	122
usage guidelines.....	53
retry-options statement.....	123
usage guidelines.....	29
RJ-45-to-DB-9 serial port adapter.....	78
rollover cable, connecting the console port.....	78
root password.....	20
root password recovery.....	77
root-authentication statement	
usage guidelines.....	20
routers	
login classes.....	3
ports	
RADIUS servers.....	53
user accounts.....	4, 28
routing-instance statement	
usage guidelines.....	53

S

secret statement	
authentication.....	124
usage guidelines, RADIUS.....	53
usage guidelines, TACACS+	59
server statement	
RADIUS accounting.....	125
TACPLUS+.....	125
service-name statement.....	130
show system users command.....	138
simple authentication.....	22
single-connection statement.....	126
usage guidelines.....	59
source-address statement	
NTP.....	127
RADIUS	
usage guidelines.....	55
RADIUS and TACACS+.....	127
system logging.....	127
usage guidelines	
usage guidelines, RADIUS.....	53
source-port statement.....	128
SSH key files.....	20
SSH service	
limiting login attempts.....	29
support, technical See technical support	
syntax conventions.....	xi
system authentication	
authentication order.....	13, 46
RADIUS	
configuring.....	53
remote template accounts.....	44
TACACS+.....	59
system login.....	48, 49
system statement.....	128
usage guidelines.....	81

T

TACACS+ accounting.....	66
usage guidelines, TX Matrix router.....	68
TACACS+ authentication	
configuring.....	59
overview.....	19
tacplus statement.....	129
tacplus-options statement.....	130
usage guidelines.....	61
tacplus-server statement.....	131
usage guidelines.....	59

technical support	
contacting JTAC.....	xiii
telnet	
service, limiting login attempts.....	29
template accounts.....	44
test access profile command.....	142
test access radius-server command.....	146
timeout statement	
authentication	
usage guidelines, RADIUS.....	53
usage guidelines, TACACS+	59
RADIUS and TACACS+.....	132
timestamp-and-timezone statement.....	130
tries-before-disconnect statement.....	132
troubleshooting	
root password recovery.....	77

U

uid statement.....	133
usage guidelines.....	4, 28
UIDs.....	4
user access	
login classes.....	3
user accounts.....	4, 6, 28
user accounts	
configuring.....	4, 28
in Junos-FIPS.....	6
security configuration example.....	71
shared user accounts.....	44
user authentication	
methods for.....	19
user identifiers See UIDs	
user permission flags.....	7
user statement	
access.....	134
usage guidelines.....	4, 28
users	
logged in, displaying.....	138

V

versioning statement.....	134
---------------------------	-----