

Chapter 21

Configuring System Authentication

You can configure the router to use RADIUS or TACACS+ authentication, or both, to validate users who attempt to access the router. If you set up both authentication methods, you also can configure which the router will try first.

When configuring system authentication, you can do the following:

- Configuring RADIUS Authentication on page 360

- Configuring TACACS+ Authentication on page 362

- Specifying a Source Address for RADIUS and TACACS+ Servers on page 364

- Configuring Template Accounts for RADIUS and TACACS+ Authentication on page 366

- Configuring the Authentication Order on page 369

For examples of configuring system authentication, see “Examples: Configuring System Authentication” on page 370.

Configuring RADIUS Authentication

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

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

server-address is the address of the RADIUS server.

You can specify a port number on which to contact the RADIUS server. By default, port number 1812 is used (as specified in RFC 2138).

You must specify a password in the `secret` statement. Passwords can contain spaces. The secret used by the local router must match that used by the server.

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

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 “Configuring Template Accounts for RADIUS and TACACS+ Authentication” on page 366.

Configuring Juniper Networks-Specific RADIUS Attributes

The JUNOS software supports the configuration of Juniper Networks-specific RADIUS attributes. These attributes are known as vendor-specific attributes and are described in RFC 2138, *Remote Authentication Dial In User Service (RADIUS)*. These Juniper Networks-specific attributes are encapsulated in a RADIUS vendor-specific attribute with the vendor ID set to the Juniper Networks ID number, 2636. Table 11 lists the Juniper Networks-specific attributes you can configure.

Table 11: Juniper Networks-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 allows 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.
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.
Juniper-Allow-Configuration	Contains an extended regular expression that allows 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.
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.

Configuring TACACS+ Authentication

To use TACACS+ authentication on the router, 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 passes to the TACACS+ client by including the `secret` statement. Secrets can contain spaces. The secret used by the local router must match that used by the server.

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

You can optionally 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 software will be unable to communicate with that TACACS+ server.

To configure multiple TACACS+ servers, include multiple `tacplus-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 “Configuring Template Accounts for RADIUS and TACACS+ Authentication” on page 366.

Configuring Juniper Networks-Specific TACACS+ Attributes

The TACACS attributes listed in Table 12 are specific to Juniper Networks. They are specified in the TACACS+ server configuration file on a per-user basis. The JUNOS software 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 JUNOS 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-regexp>"
  allow-configuration = "<allow-configuration-regexp>"

  deny-commands = "<deny-commands-regexp>"
  deny-configuration = "<deny-configuration-regexp>"
}
```

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

Table 12: Juniper Networks-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 allows 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.
allow-configuration	Contains an extended regular expression that allows 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.
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.
deny-configuration	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.

Specifying a Source Address for RADIUS and TACACS+ Servers

You can specify which source address the JUNOS software uses when accessing your network to contact an external TACACS+ or RADIUS server for authentication. You can also specify which source address the JUNOS software 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 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 interfaces.

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 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. For information about how to configure a TACACS+ server at the [edit system tacplus-server] hierarchy level, see, “Configuring TACACS+ Authentication” on page 362.

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.

Example: Configuring Multiple TACACS+ Servers

Configure the same authentication service for multiple TACACS+ servers:

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

Configuring 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.

This section discusses the following topics:

Using Remote Template Accounts on page 366

Using Local User Template Accounts on page 366

Using Remote Template Accounts

By default, the JUNOS software uses the remote template accounts when:

The authenticated user does not exist locally on the router

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

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 commands in the authentication server configuration file. For information about how to define access privileges on the authentication server, see “Configuring Juniper Networks-Specific RADIUS Attributes” on page 361 and “Configuring Juniper Networks-Specific TACACS+ Attributes” on page 363.

For information about creating user accounts, see “Configuring User Accounts” on page 387. For an example of how to configure a template account, see “Examples: Configuring System Authentication” on page 370.

Using Local User Template Accounts

You use local user template accounts when you need different types of templates. 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 software 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 software, 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 software 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. For information about how to configure access privileges on the authentication server, see “Configuring Juniper Networks-Specific RADIUS Attributes” on page 361 and “Configuring Juniper Networks-Specific TACACS+ Attributes” on page 363.

For information about creating user accounts, see “Configuring User Accounts” on page 387. For an example of how to configure a template account, see “Examples: Configuring System Authentication” on page 370.

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;
}
```

Using Local User Template Example

In this example, you configure 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;
    }
  }
}
```

Now you configure users on the TACACS+ authentication server:

```

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, they use the sales local user template. When login users Harold and Jim are authenticated, they use the engineering local user template.



NOTE: Permission bits override allow and deny commands.

Configuring the Authentication Order

If you configure the router to be both a RADIUS and TACACS+ client (by including the radius-server and tacplus-server statements), you can prioritize the order in which the software tries the different authentication methods when verifying that a user can access the router. For each login attempt, the JUNOS software tries the authentication methods in order, starting with the first one, until the password matches.

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

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

In *authentication-methods*, specify one or more of the following 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 password configured for the user with the authentication statement at the [edit system login user] hierarchy level.

If you do not include the authentication-order statement, users are verified based on their configured passwords.

Example: Removing an Order Set from the Authentication Order

Delete the radius statement from the authentication order:

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

For more information about how to remove a statement from the configuration, see “Removing a Statement from the Configuration” on page 226.

Example: Inserting an Order Set in the Authentication Order

Insert the tacplus statement after the radius statement:

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

For more information about how to modify a portion of the configuration in which the statement order matters, see “Inserting a New Identifier” on page 231.

Examples: Configuring System Authentication

The following example allows logins only by the individual user Philip, and by users who have been authenticated by a remote RADIUS server. If a user logs in and is not authenticated by the RADIUS server, the user is denied access to the router. However, if the RADIUS server is not available, the user's login name has a local password, and the user enters that password, the user is authenticated (using the password authentication method) and allowed access to the router. For more information about the password authentication method, see "Example: Defaulting to Local User Password Authentication, RADIUS" on page 372.

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 same privileges for 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 "Configuring Template Accounts for RADIUS and TACACS+ Authentication" on page 366.

Configuring a single remote user template account requires that all users without individual configuration entries share the same class and UID. When you are using RADIUS and telnet or RADIUS and SSH together, you can specify a different template user other than the remote user.

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 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.

Using the Local User Fallback Mechanism

The JUNOS software provides a local user fallback mechanism (password authentication method) that enables users to log in to the router when no TACACS+ or RADIUS authentication servers is available. The following examples illustrate how this mechanism works.

Example: Inserting Password into the Authentication Order

If you specify the following authentication order:

```
[edit]
system authentication-order [tacplus password];
```

the JUNOS software first uses the authentication method TACACS+ to authenticate users when they attempt to log in to the router. The authentication servers are tried in the order specified at the [edit system tacplus-server] hierarchy level. If no TACACS+ authentication server is available, the JUNOS software will try the next authentication method listed, password. The password option also allows users that fail to authenticate with TACACS+ to log in to the router by means of UNIX password authentication.

In effect, this configuration provides a local user fallback mechanism (traditional UNIX password) when all TACACS+ servers are unavailable, but does not restrict authentication to TACACS+ authentication only (all users will be able to try the traditional UNIX password as well).

Example: Defaulting to Local User Password Authentication, TACACS +

If you specify the following authentication order:

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

and none of the TACACS+ servers configured at the [edit system tacplus-server] hierarchy are available, the JUNOS software will try to use the password authentication method. If a TACACS+ server is available, the JUNOS software will not try to use the password authentication method.

Example: Defaulting to Local User Password Authentication, RADIUS

If you specify the following authentication order:

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

and none of the RADIUS servers configured at the [edit system radius-server] hierarchy level are available, the JUNOS software will try to use the password authentication method. If a RADIUS server is available, the JUNOS software will not try to use the password authentication method.

Example: Defaulting to Local User Password Authentication, TACACS + and RADIUS

If you specify the following authentication order:

```
[edit]  
system authentication-order [tacplus radius];
```

and no TACACS+ authentication server is available but at least one RADIUS authentication server responds (but fails to authenticate), the JUNOS software will try to use the local user fallback mechanism (password authentication method).



NOTE: If any one authentication method (RADIUS or TACACS+) fails to communicate with all of its configured servers, the JUNOS software will use the local user fallback mechanism (password authentication method).
