



# RADIUS Commands

---

This chapter contains the following sections:

- [allowed-time-range](#), on page 2
- [clear radius server accounting](#), on page 3
- [clear radius server rejected users](#), on page 4
- [clear radius server statistics](#), on page 5
- [clear radius server unknown nas](#), on page 6
- [privilege-level](#), on page 7
- [radius server accounting-port](#), on page 8
- [radius server authentication-port](#), on page 9
- [radius server enable](#), on page 10
- [radius server group](#), on page 11
- [radius server nas secret](#), on page 12
- [radius server traps accounting](#), on page 14
- [radius server traps authentication success](#), on page 15
- [radius server user](#), on page 16
- [show radius server accounting](#), on page 17
- [show radius server configuration](#), on page 19
- [show radius server group](#), on page 20
- [show radius server rejected users](#), on page 21
- [show radius server statistics](#), on page 23
- [show radius server nas secret](#), on page 25
- [show radius server user](#), on page 26
- [show radius server unknown nas](#), on page 27
- [vlan](#), on page 28

# allowed-time-range

To define the time user can connect, use the **allowed-time-range** command in Radius Server Group Configuration mode. To restore the default configuration, use the **no** form of this command.

## Syntax

**allowed-time-range** *time-range-name*

**no allowed-time-range**

## Parameters

- *time-range-name*—Specifies the time range name configured by the time range command.

## Command Mode

Radius Server Group Configuration mode

## User Guidelines

Use the **allowed-time-range** command, to define the time users can connect.

Use the **no** form of the command, to return to the default.

## Example

The following example assigns an periodical time interval:

```
switchxxxxxx(config)# time-range connection-time
switchxxxxxx(config-time-range)# periodic mon 12:00 to wed 12:00
switchxxxxxx(config-time-range)# exit
switchxxxxxx(config)# radius server group developers
switchxxxxxx(config-radser-group)# allowed-time-range connection-time
switchxxxxxx(config-radser-group)# exit
switchxxxxxx(config)#
```

# clear radius server accounting

To clear the Radius Accounting cache, use the **clear radius server accounting** command in Privileged EXEC mode.

## Syntax

**clear radius server accounting**

## Command Mode

Privileged EXEC mode

## User Guidelines

Use the **clear radius server accounting** command, to clear the Radius Accounting cache.

## Example

The following example clears the Radius Accounting cache:

```
switchxxxxxx(config)# clear radius server accounting
```

# clear radius server rejected users

To clear the Radius Rejected Users cache, use the **clear radius server rejected users** command in Privileged EXEC mode.

## Syntax

```
clear radius server rejected users
```

## Command Mode

Privileged EXEC mode

## User Guidelines

Use the **clear radius server rejected users** command, to clear the Radius Rejected Users cache.

## Example

The following example clears the Radius Rejected Users cache:

```
switchxxxxxx(config)# clear radius server rejected users
```

# clear radius server statistics

To clear the Radius server counters, use the **clear radius server statistics** command in Privileged EXEC mode.

## Syntax

**clear radius server statistics** [*ip-address*]

## Parameters

- *ip-address*—Specifies the RADIUS client host IP address. The IP address can be an IPv4, IPv6 or IPv6z address.

## Command Mode

Privileged EXEC mode

## User Guidelines

Use the **clear radius server statistics** command without parameter to clear the all counters.

Use the **clear radius server statistics** command with parameter to clear the counters of a given NAS.

## Example

The following example clears the Radius server counters:

```
switchxxxxxx(config)# clear radius server statistics
```

# clear radius server unknown nas

To clear the Radius Unknown NAS cache, use the **clear radius server unknown nas** command in Privileged EXEC mode.

## Syntax

```
clear radius server unknown nas
```

## Command Mode

Privileged EXEC mode

## User Guidelines

Use the **clear radius server unknown nas** command, to clear the Radius Unknown NAS cache.

## Example

The following example clears the Radius Unknown NAS cache:

```
switchxxxxxx(config)# clear radius server unknown nas
```

# privilege-level

To define the user privilege level, use the **privilege-level** command in Radius Server Group Configuration mode. To restore the default configuration, use the **no** form of this command.

## Syntax

**privilege-level** *level*

**no privilege-level**

## Parameters

- *level*—Specifies the user privilege level. (Range: 1-15)

## Default Configuration

1

## Command Mode

Radius Server Group Configuration mode

## User Guidelines

Use the **privilege-level** command, to define the privilege level of users of the given group.

Use the **no** form of the command, to return to the default.

A value of privilege level is passed to a Radius client in the Access-Accept message in the Vendor-Specific(26) attribute. The attribute is only passed to login users.

## Example

The following example specified privilege level 15 for users of the developers group:

```
switchxxxxxx(config)# radius server group developers
switchxxxxxx(config-radser-group)# privilege-level 15
switchxxxxxx(config-radser-group)# exit
switchxxxxxx(config)#
```

# radius server accounting-port

To define the accounting UDP port used for accounting requests, use the **radius server accounting-port** command in Global Configuration mode. To restore the default configuration, use the **no** form of this command.

## Syntax

**radius server accounting-port** udp-port

**no radius server accounting-port**

## Parameters

- *udp-port*—Specifies the UDP port number for accounting requests. (Range: 1–59999)

## Default Configuration

1813

## Command Mode

Global Configuration mode

## User Guidelines

Use the **radius server accounting-port** command, to define an UDP port for accounting requests.

Use the **no radius server accounting-port** command, to restore the default UDP accounting port.

## Example

The following example defines port 2083 as an accounting UDP port:

```
switchxxxxxx(config)# accounting-port 2083
```



# radius server authentication-port

To define the authentication UDP port used for authentication requests, use the **radius server authentication-port** command in Global Configuration mode. To restore the default configuration, use the **no** form of this command.

## Syntax

```
radius server authentication-port udp-port
```

```
no radius server authentication-port
```

## Parameters

- *udp-port*—Specifies the UDP port number for authentication requests. (Range: 1–59999)

## Default Configuration

1812

## Command Mode

Global Configuration mode

## User Guidelines

Use the **radius server authentication-port** command, to define an UDP port for authentication requests.

Use the **no radius server authentication-port** command, to restore the default UDP authentication port.

## Example

The following example defines port 2083 as an authentication UDP port:

```
switchxxxxxx(config)# authentication-port 2083
```

# radius server enable

To enable Embedded Radius server, use the **radius server enable** command in Global Configuration mode. To restore the default configuration, use the **no** form of this command.

## Syntax

**radius server enable**

**no radius server enable**

## Default Configuration

Disabled

## Command Mode

Global Configuration mode

## User Guidelines

Use the **radius server enable** command, to enable Embedded Radius server.

Use the **no radius server enable** command, to disable Embedded Radius server.

## Example

The following example enables Embedded Radius server:

```
switchxxxxx(config)# radius server enable
```

# radius server group

To enter into Radius Server Group Configuration mode and create this group if it does not exist, use the **radius server group** command in Global Configuration mode. To restore the default configuration, use the **no** form of this command.

## Syntax

**radius server group** group-name

**no radius server group** [*group-name*]

## Parameters

- *group-name*—Specifies a name of the group. (Length: 1–32 characters)

## Default Configuration

The group does not exist.

## Command Mode

Global Configuration mode

## User Guidelines

Use the **radius server group** command, to enter into the Radius Server Group Configuration mode. If this group does not exist it is created automatically.

Use the **no radius server group** group-name command, to delete one group.

Use the **no radius server group** command, to delete all groups.

A group cannot be deleted, if there is a user referencing to this group.

The Radius server supports up to 50 groups.

## Example

The following example creates group developers, if it does not exist, and enters into its context:

```
switchxxxxxx(config)# radius server group developers
switchxxxxxx(config-radser-group)#
```

# radius server nas secret

To create a secret key, use the **radius server nas secret key** command in Global Configuration mode. To delete the key, use the **no** form of this command.

## Syntax

```
radius server nas secret key key {default | ip-address}
```

```
radius server nas secret ip-address
```

```
encrypted radius server nas secret key encrypted-key {default | ip-address}
```

```
no radius server nas secret [default | ip-address]
```

## Parameters

- **key**—Specifies the authentication and encryption key for communications between the device and users of the given group. (Range: 0–128 characters)
- **encrypted-key**—Same as the key-string parameter, but the key is in encrypted form.
- **default**—Specifies the default secret key that will be applied to communicate with NASs that do not have a private key.
- **ip-address**—Specifies the RADIUS client host IP address. The IP address can be an IPv4, IPv6 or IPv6z address.

## Default Configuration

The secret key does not exist.

## Command Mode

Global Configuration mode

## User Guidelines

Use the **radius server nas secret key key default** command, to defines a key that will be applied to communicate with NASs that do not have a private key.

Use the **radius server nas secret key key ip-address** command, to defines a key that will be applied to communicate with the specified NAS.

Use the **radius server nas secret ip-address** command, to defines that the default secret key will be applied to communicate with the specified NAS.

If a NAS is not defined by this command all messages received from this NAS will be dropped.

The Radius server supports up to 50 NASs.

Use the **no radius server nas secret default** command, to delete the default key.

Use the **no radius server nas secret ip-address** command, to remove the given NAS and its secret key.

Use the **no radius server nas secret** command, to delete all NASs and all secret keys.

**Example 1.** The following example defines a default secret key:

```
switchxxxxxx(config)# radius server nas secret key qrBut56$#qw default
```

**Example 2.** The following example defines a default secret key:

```
switchxxxxxx(config)# radius server nas secret key qrBut56$#qw default
```

**Example 3.** The following example defines a NAS using the default secret key:

```
switchxxxxxx(config)# radius server nas secret 10.05.10.1
```

# radius server traps accounting

To enable sending accounting traps, use the **radius server traps accounting** command in Global Configuration mode. To disable the traps, use the **no** form of this command.

## Syntax

**radius server traps accounting**

**no radius server traps accounting**

## Default Configuration

Accounting traps are disabled.

## Command Mode

Global Configuration mode

## User Guidelines

A rate limit is applied to the traps: not more than one trap of this type can be sent in 10 seconds.

## Example

The following example enables sending accounting traps:

```
switchxxxxxx(config)# radius server traps accounting
```

# radius server traps authentication success

To enable sending traps when a user is successfully authorized, use the **radius server traps authentication success** command in Global Configuration mode. To disable the traps, use the **no** form of this command.

## Syntax

**radius server traps authentication success**

**no radius server traps authentication success**

## Default Configuration

Success traps are disabled.

## Command Mode

Global Configuration mode

## User Guidelines

A rate limit is applied to the traps: not more than one trap of this type can be sent in 10 seconds.

## Example

The following example enables sending traps when a user is successfully authorized:

```
switchxxxxxx(config)# radius server traps authentication success
```

# radius server user

To create a user, use the **radius server user** command in Global Configuration mode. To restore the default configuration, use the **no** form of this command.

## Syntax

```
radius server user username user-name group group-name password unencrypted-password
encrypted radius server user username user-name group group-name passwordencrypted-password
no radius server user [username user-name | group group-name]
```

## Parameters

- **user-name**—Specifies the user name. (Length: 1–32 characters)
- **group-name**—Specifies the user group name. (Length: 1–32 characters)
- **unencrypted-password**—Specifies the user password. (Length: 1–64 characters)
- **encrypted-password**—Same as the *unencrypted-password* parameter, but the password is in the encrypted form.

## Default Configuration

The user does not exist.

The Radius server supports up to 1024 users.

## Command Mode

Global Configuration mode

## User Guidelines

Use the **radius server user** command, to create a new user.

Use the **no radius server user username** user-name command to delete one user.

Use the **no radius server user group** group-name command to delete users of the given group.

Use the **no radius server user** command to delete all users.

## Example

Example 1. The following example creates a new user with name bob of group developer with password Aerv#136dSsT:

```
switchxxxxxx(config)# radius server user username bob group developers password Aerv#136dSsT
```

Example 2. The following example creates a new user with name bill of group finance and the password is provided in the encrypted format:

```
switchxxxxxx(config)# encrypted radius server user username bill group
finance password bCWG7DnKMNUaik4S0TkLDkJVYIsQcwQkRFVYj7VNvAI=
```



# show radius server accounting

To display user accounting information, use the **show radius server accounting** command in Privileged EXEC mode.

## Syntax

```
show radius server accounting [username user-name]
```

## Parameters

- *user-name*—Specifies the user name. (Length: 1–32 characters)

## Command Mode

Privileged EXEC mode

## User Guidelines

The Radius server saves the last 1024 accounting logs in a cycle file on FLASH.

Use the **show radius server accounting username user-name** command, to display accounting information of one user.

Use the **show radius server accounting** command, to display accounting information of all users.

**Example 1.** The following example displays accounting information of all users:

```
switchxxxxxx# show radius server accounting
29-Jun-14, 16:00, Stop
  User: Bob
  Accounting Session Time: 6 hours,15 minutes
  Authenticated by: local
  NAS Address: 10.23.1.3
  User Address: 160.134.7.8
  Termination Reason: User Request
29-Jun-14, 12:04, Start
  User: Alisa
  Authenticated by: Radius
  NAS Address: 10.23.1.3
  User Address: 00:12:cf:00:1c:25
  NAS Port: 10
29-Jun-14, 12:04, Stop
  User: Alisa
  Accounting Session Time: 2 days,2 hours,10 minutes
  Authenticated by: Radius
  NAS Address: 10.23.1.3
  User Address: 00:12:cf:00:1c:25
  Termination Reason: User Request
*20-Feb-2008, 9:20, Date and Time were updated to 29-Jun-14, 11:00
20-Feb-2014, 9:05, Start
  User: Bob
  Authenticated by: local
  NAS Address: 10.23.1.3
  User Address: 160.134.7.8
*20-Feb-2008, 9:00, Reboot
```

**Example 2.** The following example displays accounting information of one user Bob:

```
switchxxxxx# show radius server accounting username Bob:
29-Jun-14, 16:00, Stop
  User: Bob
  Accounting Session Time: 6 hours,15 minutes
  Authenticated by: Radius
  NAS Address: 10.23.1.3
  User Address: 160.134.7.8
  Termination Reason: User Request
*20-Feb-2008, 9:20, Date and Time were updated to 29-Jun-14, 11:00
20-Feb-2014, 9:05, Start
  User: Bob
  Authenticated by: Radius
  NAS Address: 10.23.1.3
  User Address: 160.134.7.8
*20-Feb-2008, 9:00, Reboot
```

# show radius server configuration

To display Radius Server global configuration, use the **show radius server configuration** command in Privileged EXEC mode.

## Syntax

**show radius server configuration**

## Command Mode

Privileged EXEC mode

## User Guidelines

Use the **show radius server configuration** command, to display Radius server global configuration.

## Example

The following example displays radius server global configuration:

```
switchxxxxxx# show radius server configuration
Radius Server Status: Enabled
Authentication UDP port: 1812 (default)
Accounting UDP port: 1813 (default)
Authentication failure traps are enabled
Authentication success traps are enabled
Accounting traps are enabled
```

# show radius server group

To display a Radius Server group configuration, use the **show radius server group** command in Privileged EXEC mode.

## Syntax

```
show radius server group [group-name]
```

## Parameters

- *group-name*—Specifies a name of the group. (Length: 1–32 characters)

## Command Mode

Privileged EXEC mode

## User Guidelines

Use the **show radius server group** *group-name* command, to display one group.

Use the **show radius server group** command, to display all groups.

## Example

The following example displays radius server groups.

```
switchxxxxxx# show radius server group
Group gr1
  VLAN: 124
  Privilege Level: 15
  Time Range: ConnectionTime
  Group Users: develop, designers
Group gr2
  Privilege Level: 1 (default)
  Group Users: bob
```

# show radius server rejected users

To display rejected users, use the **show radius server rejected users** command in Privileged EXEC mode.

## Syntax

```
show radius server rejected users [username user-name]
```

## Parameters

- *user-name*—Specifies the user name. (Length: 1–32 characters)

## Command Mode

Privileged EXEC mode

## User Guidelines

The Radius server saves the last 1024 rejected authentication requests in a cycle file on FLASH.

The Radius server saves the last 1024 accounting logs in a cycle file on FLASH.

Use the **show radius server rejected users** *user-name* command, to display one rejected user.

Use the **show radius server rejected users** command, to display all rejected users.

**Example 1.** The following example displays all rejected users:

```
switchxxxxxx# show radius server rejected users
30-Jun-14 16:44
  User Name: Jack
  User Type: Login
  NAS Address: 10.1.1.1
  User Address: 10.23.4.3
  Reason: Unknown user
30-Jun-14 16:04
  User Name: Bob
  User Type: Login
  NAS Address: 10.1.1.1
  User Address: 10.23.4.3
  Reason: Illegal password
*20-Feb-2008, 9:20, Date and Time were updated to 29-Jun-14, 11:00
20-Feb-08 16:24
  User Name: Robert
  User Type: 802.1x
  NAS Address: 10.1.1.1
  NAS Port: 2
  User Address: 00:67:67:96:ac:21
  Reason: Not Supported EAP method
20-Feb-08 14:14
  User Name: Alisa
  User Type: 802.1x
  NAS Address: 10.1.1.1
  NAS Port: 2
  User Address: 00:67:67:96:ac:21
  Reason: Not allowed at this time
*20-Feb-2008, 9:00, Reboot
```

**Example 2.** The following example displays one rejected user Bob:

```
switchxxxxx# show radius server rejected users 30-Jun-14 16:04
  User Name: Bob
  User Type: Login
  NAS Address: 10.1.1.1
  User Address: 10.23.4.3
  Reason: Illegal password
*20-Feb-2008, 9:20, Date and Time were updated to 29-Jun-14, 11:00
*20-Feb-2008, 9:00, Reboot
```

# show radius server statistics

To display the Radius server counters, use the **show radius server statistics** command in User EXEC mode.

## Syntax

```
show radius server statistics [ip-address]
```

## Parameters

- *ip-address*—Specifies the RADIUS client host IP address. The IP address can be an IPv4, IPv6 or IPv6z address.

## Command Mode

User EXEC mode

## User Guidelines

Use the **show radius server statistics** command to display the Radius server counters defined in RFC4669 and RFC4671.

Use the **show radius server statistics** command without parameter to display the global counters.

Use the **show radius server statistics** command with parameter to display the counters of the given NAS.

**Example 1.** The following example displays the Radius server global counters:

```
switchxxxxxx# show radius server statistics
Number of incoming packets on the authentication port: 120
Number of incoming Access-Requests from unknown addresses: 0
Number of duplicate incoming Access-Requests: 3
Number of sent Access-Accepts: 100
Number of sent Access-Rejects: 17
Number of sent Access-Challenges: 0
Number of incoming malformed Access-Requests: 0
Number of incoming Authentication-Requests with Bad Authenticator: 0
Number of incoming Authentication packets with other mistakes: 0
Number of incoming Authentication packets of unknown type: 0
Number of incoming packets on the accounting port: 80
Number of incoming Accounting-Requests from unknown addresses: 12
Number of incoming Accounting-Requests from unknown addresses: 0
Number of incoming duplicate Accounting-Requests: 0
Number of sent Accounting-Responses: 0
Number of incoming malformed Accounting-Requests: 0
Number of incoming Accounting-Requests with Bad Authenticator: 0
Number of incoming Accounting packets with other mistakes: 0
Number of incoming not recorded Accounting-Requests: 0
Number of incoming Accounting packets of unknown type: 0
```

**Example 2.** The following example displays the Radius server counters of the given SNA: secret keys:

```
switchxxxxxx# show radius server statistics 1.1.1.1
NAS: 1.1.1.1
Number of incoming packets on the authentication port: 120
Number of duplicate incoming Access-Requests: 3
Number of sent Access-Accepts: 100
```

```
Number of sent Access-Rejects: 17
Number of sent Access-Challenges: 0
Number of incoming malformed Access-Requests: 0
Number of incoming Authentication-Requests with Bad Authenticator: 0
Number of incoming Authentication packets with other mistakes: 0
Number of incoming Authentication packets of unknown type: 0
Number of incoming packets on the accounting port: 80
Number of incoming Accounting-Requests from unknown addresses: 0
Number of incoming duplicate Accounting-Requests: 0
Number of sent Accounting-Responses: 0
Number of incoming malformed Accounting-Requests: 0
Number of incoming Accounting-Requests with Bad Authenticator: 0
Number of incoming Accounting packets with other mistakes: 0
Number of incoming not recorded Accounting-Requests: 0
Number of incoming Accounting packets of unknown type: 0
```



# show radius server nas secret

To display secret keys, use the **show radius server nas secret** command in Privileged EXEC mode.

## Syntax

```
show radius server nas secret [default | ip-address]
```

## Parameters

- **default**—Specifies the default secret key that will be applied to communicate with NASs that do not have a private key.
- **ip-address**—Specifies the RADIUS client host IP address. The IP address can be an IPv4, IPv6 or IPv6z address.

## Command Mode

Privileged EXEC mode

## User Guidelines

Use the **show radius server nas secret default** command, to display the default secret key.

Use the **show radius server nas secret ip-address** command, to display the given NAS secret key.

Use the **show radius server nas secret** command, to display all secret keys.

**Example 1.** The following example displays all secret keys:

```
switchxxxxx# show radius server nas secret
Default Secret Key's MD5:1238af77aaca17568f1298cced1255cc
      NAS Address                Secret Key's MD5
-----
10.1.35.3                        1238af77aaca17568f1298cced165fec
10.2.37.6                        default
3000:1231:1230:9cab:1384         1238af77aaca17568f12988601fcabed
3001:ab11::9cda:0981            1238af77aaca17568f1298bc5476ddad
```

**Example 2.** The following example displays the default secret key:

```
switchxxxxx# show radius server nas secret default
Default Secret Key's MD5:1238af77aaca17568f1298cced1255cc
```

**Example 3.** The following example displays the secret key of one given NAS:

```
switchxxxxx# show radius server nas secret 10.1.35.3
      NAS ID                Secret Key's MD5
-----
10.1.35.3                    1238af77aaca17568f1298cced165fec
```

# show radius server user

To display a Radius Server user configuration, use the **show radius server user** command in Privileged EXEC mode.

## Syntax

```
show radius server user [username user-name] | [group group-name]
```

## Parameters

- *user-name*—Specifies the user name. (Length: 1–32 characters)
- *group-name*—Specifies a name of the group. (Length: 1–32 characters)

## Command Mode

Privileged EXEC mode

## User Guidelines

Use the **show radius server user username** *user-name* command, to display one user.

Use the **show radius server user group** *group-name* command, to display all users of the given group.

Use the **show radius server user** command, to display all users.

## Examples

The following example displays one user bob:

```
switchxxxxx# show radius server user username bob
User bob
  Group: developers
  Password's MD5: 1238af77aacal7568f1298cced1255cc
```

# show radius server unknown nas

To display unknown NASes, use the **show radius server unknown nas** command in Privileged EXEC mode.

## Syntax

```
show radius server unknown nas
```

## Command Mode

Privileged EXEC mode

## User Guidelines

The Radius server saves the last 100 unknown NASes in a cycle cache.

## Example

The following example displays Radius requests received from unknown NASes:

```
switchxxxxx# show radius server unknown nas
30-Jun-14 16:44 NAS Address: 10.1.1.1
30-Jun-14 16:04 NAS Address: 10.1.1.1
*20-Feb-08, 9:20, Date and Time were updated to 29-Jun-14, 11:00
20-Feb-08 16:24 NAS Address: 10.1.1.1
20-Feb-08 14:14 NAS Address: 10.1.1.1
*20-Feb-08, 9:00, Reboot
```

# vlan

To define Radius Assigned VLAN, use the **vlan** command in Radius Server Group Configuration mode. To restore the default configuration, use the **no** form of this command.

## Syntax

```
vlan {id vlan-id | name vlan-name}
```

```
no vlan
```

## Parameters

- *vlan-id*—Specifies a VLAN ID. (Range: 1-4094)
- *vlan-name*—Specifies a name of the VLAN. (Length: 1–32characters)

## Default Configuration

No Radius Assigned VLAN.

## Command Mode

Radius Server Group Configuration mode

## User Guidelines

Use the **vlan** command, to assign the VLAN to a radius client. This Radius Assigned VLAN is passed to a Radius client in the Access-Accept message in the following attributes:

- Tunnel-Type(64)
- Tunnel-Medium-Type(65)
- Tunnel-Private-Group-ID(81)

If a VLAN is not assigned these attributes are not included in the Access-Accept message.

Use the **no** form of the command, to delete VLAN assignment.

## Example

The following example assigns VLAN 100 to users of the developers group and VLAN with name management of users of the managers group:

```
switchxxxxxx(config)# radius server group developers
switchxxxxxx(config-radser-group)# vlan id 100
switchxxxxxx(config-radser-group)# exit
switchxxxxxx(config)# radius server group managers
switchxxxxxx(config-radser-group)# vlan name management
switchxxxxxx(config-radser-group)# exit
switchxxxxxx(config)#
```