



Configuring TACACS+

This chapter contains the following sections:

- [Information About Configuring TACACS+, on page 1](#)
- [Prerequisites for TACACS+, on page 3](#)
- [Guidelines and Limitations for TACACS+, on page 4](#)
- [Default Settings for TACACS+, on page 4](#)
- [Configuring TACACS+, on page 4](#)
- [Displaying TACACS+ Statistics, on page 14](#)
- [Verifying the TACACS+ Configuration, on page 15](#)
- [Configuration Examples for TACACS+, on page 15](#)

Information About Configuring TACACS+

The Terminal Access Controller Access Control System Plus (TACACS+) security protocol provides centralized validation of users attempting to gain access to a Cisco Nexus device. TACACS+ services are maintained in a database on a TACACS+ daemon typically running on a UNIX or Windows NT workstation. You must have access to and must configure a TACACS+ server before the configured TACACS+ features on your Cisco Nexus device are available.

TACACS+ provides for separate authentication, authorization, and accounting facilities. TACACS+ allows for a single access control server (the TACACS+ daemon) to provide each service (authentication, authorization, and accounting) independently. Each service is associated with its own database to take advantage of other services available on that server or on the network, depending on the capabilities of the daemon.

The TACACS+ client/server protocol uses TCP (TCP port 49) for transport requirements. The Cisco Nexus device provides centralized authentication using the TACACS+ protocol.

TACACS+ Advantages

TACACS+ has the following advantages over RADIUS authentication:

- Provides independent AAA facilities. For example, the Cisco Nexus device can authorize access without authenticating.
- Uses the TCP transport protocol to send data between the AAA client and server, making reliable transfers with a connection-oriented protocol.

- Encrypts the entire protocol payload between the switch and the AAA server to ensure higher data confidentiality. The RADIUS protocol only encrypts passwords.

User Login with TACACS+

When a user attempts a Password Authentication Protocol (PAP) login to a Cisco Nexus device using TACACS+, the following actions occur:

1. When the Cisco Nexus device establishes a connection, it contacts the TACACS+ daemon to obtain the username and password.



Note

TACACS+ allows an arbitrary conversation between the daemon and the user until the daemon receives enough information to authenticate the user. This action is usually done by prompting for a username and password combination, but may include prompts for other items, such as the user's mother's maiden name.

2. The Cisco Nexus device receives one of the following responses from the TACACS+ daemon:
 - ACCEPT—User authentication succeeds and service begins. If the Cisco Nexus device requires user authorization, authorization begins.
 - REJECT—User authentication failed. The TACACS+ daemon either denies further access to the user or prompts the user to retry the login sequence.
 - ERROR—An error occurred at some time during authentication either at the daemon or in the network connection between the daemon and the Cisco Nexus device. If the Cisco Nexus device receives an ERROR response, the switch tries to use an alternative method for authenticating the user.

The user also undergoes an additional authorization phase, if authorization has been enabled on the Cisco Nexus device. Users must first successfully complete TACACS+ authentication before proceeding to TACACS+ authorization.

3. If TACACS+ authorization is required, the Cisco Nexus device again contacts the TACACS+ daemon and it returns an ACCEPT or REJECT authorization response. An ACCEPT response contains attributes that are used to direct the EXEC or NETWORK session for that user and determines the services that the user can access.

Services include the following:

- Telnet, rlogin, Point-to-Point Protocol (PPP), Serial Line Internet Protocol (SLIP), or EXEC services
- Connection parameters, including the host or client IP address (IPv4), access list, and user timeouts

Default TACACS+ Server Encryption Type and Preshared Key

You must configure the TACACS+ that is preshared key to authenticate the switch to the TACACS+ server. A preshared key is a secret text string shared between the Cisco Nexus device and the TACACS+ server host. The length of the key is restricted to 63 characters and can include any printable ASCII characters (white spaces are not allowed). You can configure a global preshared secret key for all TACACS+ server configurations on the Cisco Nexus device to use.

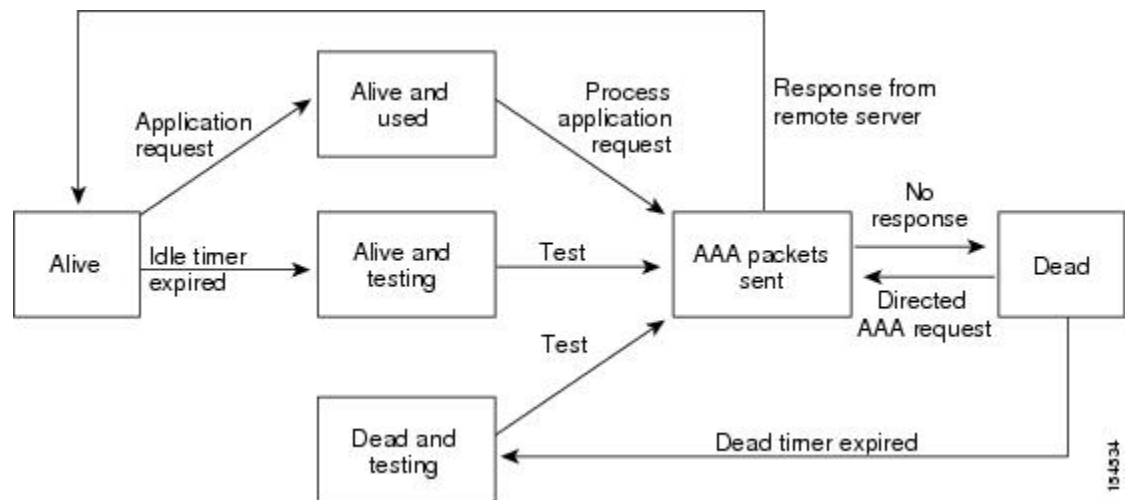
You can override the global preshared key assignment by using the **key** option when configuring an individual TACACS+ server.

TACACS+ Server Monitoring

An unresponsive TACACS+ server can delay the processing of AAA requests. A Cisco Nexus device can periodically monitor an TACACS+ server to check whether it is responding (or alive) to save time in processing AAA requests. The Cisco Nexus device marks unresponsive TACACS+ servers as dead and does not send AAA requests to any dead TACACS+ servers. The Cisco Nexus device periodically monitors dead TACACS+ servers and brings them to the alive state once they are responding. This process verifies that a TACACS+ server is in a working state before real AAA requests are sent to the server. Whenever an TACACS+ server changes to the dead or alive state, a Simple Network Management Protocol (SNMP) trap is generated and the Cisco Nexus device displays an error message that a failure is taking place before it can impact performance.

The following figure shows the different TACACS+ server states:

Figure 1: TACACS+ Server States



Note The monitoring interval for alive servers and dead servers are different and can be configured by the user. The TACACS+ server monitoring is performed by sending a test authentication request to the TACACS+ server.

Prerequisites for TACACS+

TACACS+ has the following prerequisites:

- You must obtain the IPv4 addresses or hostnames for the TACACS+ servers.
- You must obtain the preshared keys from the TACACS+ servers, if any.
- Ensure that the Cisco Nexus device is configured as a TACACS+ client of the AAA servers.

Guidelines and Limitations for TACACS+

TACACS+ has the following configuration guidelines and limitations:

- You can configure a maximum of 64 TACACS+ servers on the Cisco Nexus device.

Default Settings for TACACS+

The following table lists the default settings for TACACS+ parameters.

Table 1: Default TACACS+ Parameters

| Parameters | Default |
|-------------------------------------|-----------|
| TACACS+ | Disabled |
| Dead-time interval | 0 minutes |
| Timeout interval | 5 seconds |
| Idle timer interval | 0 minutes |
| Periodic server monitoring username | test |
| Periodic server monitoring password | test |

Configuring TACACS+

TACACS+ Server Configuration Process

This section describes how to configure TACACS+ servers.

Procedure

- Step 1** Enable TACACS+.
- Step 2** Establish the TACACS+ server connections to the Cisco Nexus device.
- Step 3** Configure the preshared secret keys for the TACACS+ servers.
- Step 4** If needed, configure TACACS+ server groups with subsets of the TACACS+ servers for AAA authentication methods.
- Step 5** If needed, configure any of the following optional parameters:
 - Dead-time interval

- Allow TACACS+ server specification at login
- Timeout interval
- TCP port

Step 6 If needed, configure periodic TACACS+ server monitoring.

Enabling TACACS+

Although by default, the TACACS+ feature is disabled on the Cisco Nexus device. You can enable the TACACS+ feature to access the configuration and verification commands for authentication.

Procedure

| | Command or Action | Purpose |
|---------------|--|--|
| Step 1 | switch# configure terminal | Enters global configuration mode. |
| Step 2 | switch(config)# feature tacacs+ | Enables TACACS+. |
| Step 3 | switch(config)# exit | Exits configuration mode. |
| Step 4 | (Optional) switch# copy running-config startup-config | Copies the running configuration to the startup configuration. |

Configuring TACACS+ Server Hosts

To access a remote TACACS+ server, you must configure the IPv4 address or the hostname for the TACACS+ server on the Cisco Nexus device. All TACACS+ server hosts are added to the default TACACS+ server group. You can configure up to 64 TACACS+ servers.

If a preshared key is not configured for a configured TACACS+ server, a warning message is issued if a global key is not configured. If a TACACS+ server key is not configured, the global key (if configured) is used for that server.

Before you configure TACACS+ server hosts, you should do the following:

- Enable TACACS+.
- Obtain the IPv4 addresses or the hostnames for the remote TACACS+ servers.

Procedure

| | Command or Action | Purpose |
|---------------|--|--|
| Step 1 | switch# configure terminal | Enters global configuration mode. |
| Step 2 | switch(config)# exit | Exits configuration mode. |
| Step 3 | (Optional) switch# show tacacs-server | Displays the TACACS+ server configuration. |
| Step 4 | (Optional) switch# copy running-config startup-config | Copies the running configuration to the startup configuration. |

Example

You can delete a TACACS+ server host from a server group.

Configuring TACACS+ Global Preshared Keys

You can configure preshared keys at the global level for all servers used by the Cisco Nexus device. A preshared key is a shared secret text string between the Cisco Nexus device and the TACACS+ server hosts.

Before you configure preshared keys, you should do the following:

- Enable TACACS+.
- Obtain the preshared key values for the remote TACACS+ servers.

Procedure

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | switch# configure terminal | Enters global configuration mode. |
| Step 2 | switch(config)# tacacs-server key [0 7] <i>key-value</i> | Specifies a preshared key for all TACACS+ servers. You can specify a clear text (0) or encrypted (7) preshared key. The default format is clear text. The maximum length is 63 characters. By default, no preshared key is configured. |
| Step 3 | switch(config)# exit | Exits configuration mode. |
| Step 4 | (Optional) switch# show tacacs-server | Displays the TACACS+ server configuration. Note The preshared keys are saved in encrypted form in the running configuration. Use the show running-config command to display the encrypted preshared keys. |
| Step 5 | (Optional) switch# copy running-config startup-config | Copies the running configuration to the startup configuration. |

Example

The following example shows how to configure global preshared keys:

```
switch# configure terminal
switch(config)# tacacs-server key 0 QsEfThUkO
switch(config)# exit
switch# show tacacs-server
switch# copy running-config startup-config
```

Configuring TACACS+ Server Preshared Keys

You can configure preshared keys for a TACACS+ server. A preshared key is a shared secret text string between the Cisco Nexus device and the TACACS+ server host.

Procedure

| | Command or Action | Purpose |
|---------------|--|--|
| Step 1 | switch# configure terminal | Enters global configuration mode. |
| Step 2 | switch(config)# exit | Exits configuration mode. |
| Step 3 | (Optional) switch# show tacacs-server | Displays the TACACS+ server configuration. Note The preshared keys are saved in encrypted form in the running configuration. Use the show running-config command to display the encrypted preshared keys. |
| Step 4 | (Optional) switch# copy running-config startup-config | Copies the running configuration to the startup configuration. |

Example

The following example shows how to configure the TACACS+ preshared keys:

```
switch# configure terminal
switch(config)# tacacs-server host 10.10.1.1 key 0 PlIjUhYg
switch(config)# exit
switch# show tacacs-server
switch# copy running-config startup-config
```

Configuring TACACS+ Server Groups

You can specify one or more remote AAA servers to authenticate users using server groups. All members of a group must belong to the TACACS+ protocol. The servers are tried in the same order in which you configure them.

You can configure these server groups at any time but they only take effect when you apply them to an AAA service.

Before you begin

You must use the **feature tacacs+** command to enable TACACS+ before you configure TACACS+.

Procedure

| | Command or Action | Purpose |
|---------------|-----------------------------------|-----------------------------------|
| Step 1 | switch# configure terminal | Enters global configuration mode. |

| | Command or Action | Purpose |
|---------------|--|---|
| Step 2 | switch(config)# aaa group server tacacs+ group-name | Creates a TACACS+ server group and enters the TACACS+ server group configuration mode for that group. |
| Step 3 | (Optional) switch(config-tacacs+)# deadtime minutes | Configures the monitoring dead time. The default is 0 minutes. The range is from 0 through 1440. Note If the dead-time interval for a TACACS+ server group is greater than zero (0), that value takes precedence over the global dead-time value. |
| Step 4 | (Optional) switch(config-tacacs+)# source-interface interface | Assigns a source interface for a specific TACACS+ server group. The supported interface types are management and VLAN. Note Use the source-interface command to override the global source interface assigned by the ip tacacs source-interface command. |
| Step 5 | switch(config-tacacs+)# exit | Exits configuration mode. |
| Step 6 | (Optional) switch(config)# show tacacs-server groups | Displays the TACACS+ server group configuration. |
| Step 7 | (Optional) switch(config)# copy running-config startup-config | Copies the running configuration to the startup configuration. |

Example

The following example shows how to configure a TACACS+ server group:

```
switch# configure terminal
switch(config)# aaa group server tacacs+ TacServer
switch(config-tacacs+)# server 10.10.2.2
switch(config-tacacs+)# deadtime 30
switch(config-tacacs+)# exit
switch(config)# show tacacs-server groups
switch(config)# copy running-config startup-config
```


Configuring the Global Source Interface for TACACS+ Server Groups

You can configure a global source interface for TACACS+ server groups to use when accessing TACACS+ servers. You can also configure a different source interface for a specific TACACS+ server group.

Procedure

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | configure terminal | Enters global configuration mode. |
| Step 2 | ip tacacs source-interface <i>interface</i> Example: switch(config)# ip tacacs source-interface mgmt 0 | Configures the global source interface for all TACACS+ server groups configured on the device. The source interface can be the management or the VLAN interface. |
| Step 3 | exit Example: switch(config)# exit switch# | Exits configuration mode. |
| Step 4 | (Optional) show tacacs-server Example: switch# show tacacs-server | Displays the TACACS+ server configuration information. |
| Step 5 | (Optional) copy running-config startup config Example: switch# copy running-config startup-config | Copies the running configuration to the startup configuration. |

Specifying a TACACS+ Server at Login

You can configure the switch to allow the user to specify which TACACS+ server to send the authenticate request by enabling the directed-request option. By default, a Cisco Nexus device forwards an authentication request based on the default AAA authentication method. If you enable this option, the user can log in as *username@hostname*, where *hostname* is the name of a configured RADIUS server.



Note User specified logins are only supported for Telnet sessions.

Procedure

| | Command or Action | Purpose |
|---------------|---|---|
| Step 1 | switch# configure terminal | Enters global configuration mode. |
| Step 2 | switch(config)# tacacs-server directed-request | Allows users to specify a TACACS+ server to send the authentication request when logging in. The default is disabled. |

| | Command or Action | Purpose |
|---------------|---|--|
| Step 3 | switch(config)# exit | Exits configuration mode. |
| Step 4 | (Optional) switch# show tacacs-server directed-request | Displays the TACACS+ directed request configuration. |
| Step 5 | (Optional) switch# copy running-config startup-config | Copies the running configuration to the startup configuration. |

Configuring the Global TACACS+ Timeout Interval

You can set a global timeout interval that the Cisco Nexus device waits for responses from all TACACS+ servers before declaring a timeout failure. The timeout interval determines how long the switch waits for responses from TACACS+ servers before declaring a timeout failure.

Procedure

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | switch# configure terminal | Enters global configuration mode. |
| Step 2 | switch(config)# tacacs-server timeout seconds | Specifies the timeout interval for TACACS+ servers. The default timeout interval is 5 second and the range is from 1 to 60 seconds. |
| Step 3 | switch(config)# exit | Exits configuration mode. |
| Step 4 | (Optional) switch# show tacacs-server | Displays the TACACS+ server configuration. |
| Step 5 | (Optional) switch# copy running-config startup-config | Copies the running configuration to the startup configuration. |

Configuring the Timeout Interval for a Server

You can set a timeout interval that the Cisco Nexus device waits for responses from a TACACS+ server before declaring a timeout failure. The timeout interval determines how long the switch waits for responses from a TACACS+ server before declaring a timeout failure.

Procedure

| | Command or Action | Purpose |
|---------------|--|--|
| Step 1 | switch# configure terminal | Enters global configuration mode. |
| Step 2 | switch(config)# exit | Exits configuration mode. |
| Step 3 | (Optional) switch# show tacacs-server | Displays the TACACS+ server configuration. |
| Step 4 | (Optional) switch# copy running-config startup-config | Copies the running configuration to the startup configuration. |

Configuring TCP Ports

You can configure another TCP port for the TACACS+ servers if there are conflicts with another application. By default, the Cisco Nexus device uses port 49 for all TACACS+ requests.

Procedure

| | Command or Action | Purpose |
|---------------|--|--|
| Step 1 | switch# configure terminal | Enters global configuration mode. |
| Step 2 | switch(config)# exit | Exits configuration mode. |
| Step 3 | (Optional) switch# show tacacs-server | Displays the TACACS+ server configuration. |
| Step 4 | (Optional) switch# copy running-config startup-config | Copies the running configuration to the startup configuration. |

Example

The following example shows how to configure TCP ports:

```
switch# configure terminal
switch(config)# tacacs-server host 10.10.1.1 port 2
switch(config)# exit
switch# show tacacs-server
switch# copy running-config startup-config
```

Configuring Periodic TACACS+ Server Monitoring

You can monitor the availability of TACACS+ servers. These parameters include the username and password to use for the server and an idle timer. The idle timer specifies the interval in which a TACACS+ server receives no requests before the Cisco Nexus device sends out a test packet. You can configure this option to test servers periodically, or you can run a one-time only test.



Note To protect network security, we recommend that you use a username that is not the same as an existing username in the TACACS+ database.

The test idle timer specifies the interval in which a TACACS+ server receives no requests before the Cisco Nexus device sends out a test packet.



Note The default idle timer value is 0 minutes. When the idle time interval is 0 minutes, periodic TACACS+ server monitoring is not performed.

Procedure

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | switch# configure terminal | Enters global configuration mode. |
| Step 2 | switch(config)# tacacs-server dead-time <i>minutes</i> | Specifies the number minutes before the Cisco Nexus device checks a TACACS+ server that was previously unresponsive. The default value is 0 minutes and the valid range is 0 to 1440 minutes. |
| Step 3 | switch(config)# exit | Exits configuration mode. |
| Step 4 | (Optional) switch# show tacacs-server | Displays the TACACS+ server configuration. |
| Step 5 | (Optional) switch# copy running-config startup-config | Copies the running configuration to the startup configuration. |

Example

The following example shows how to configure periodic TACACS+ server monitoring:

```
switch# configure terminal
switch(config)# tacacs-server host 10.10.1.1 test username user1 password Ur2Gd2BH idle-time
3
switch(config)# tacacs-server dead-time 5
switch(config)# exit
switch# show tacacs-server
switch# copy running-config startup-config
```

Configuring the Dead-Time Interval

You can configure the dead-time interval for all TACACS+ servers. The dead-time interval specifies the time that the Cisco Nexus device waits, after declaring a TACACS+ server is dead, before sending out a test packet to determine if the server is now alive.

**Note**

When the dead-time interval is 0 minutes, TACACS+ servers are not marked as dead even if they are not responding. You can configure the dead-time interval per group.

Procedure

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | switch# configure terminal | Enters global configuration mode. |
| Step 2 | switch(config)# tacacs-server deadtime <i>minutes</i> | Configures the global dead-time interval. The default value is 0 minutes. The range is from 1 to 1440 minutes. |
| Step 3 | switch(config)# exit | Exits configuration mode. |

| | Command or Action | Purpose |
|---------------|--|--|
| Step 4 | (Optional) switch# show tacacs-server | Displays the TACACS+ server configuration. |
| Step 5 | (Optional) switch# copy running-config startup-config | Copies the running configuration to the startup configuration. |

Configuring ASCII Authentication

You can enable ASCII authentication on the TACACS+ server.

Before you begin

Enable TACACS+.

Procedure

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | configure terminal Example: switch# configure terminal switch(config)# | Enters global configuration mode. |
| Step 2 | aaa authentication login ascii-authentication Example: switch(config)# aaa authentication login ascii-authentication | Enables ASCII authentication. The default is disabled. |
| Step 3 | exit Example: switch(config)# exit switch# | Exits configuration mode. |
| Step 4 | (Optional) show tacacs-server Example: switch# show tacacs-server | Displays the TACACS+ server configuration. |
| Step 5 | (Optional) copy running-config startup-config Example: switch# copy running-config startup-config | Copies the running configuration to the startup configuration. |

Manually Monitoring TACACS+ Servers or Groups

Procedure

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | switch# test aaa server tacacs+ { <i>ipv4-address</i> <i>ipv6-address</i> <i>host-name</i> } [vrf <i>vrf-name</i>] <i>username password</i> | Sends a test message to a TACACS+ server to confirm availability. |
| Step 2 | switch# test aaa group <i>group-name username password</i> | Sends a test message to a TACACS+ server group to confirm availability. |

Example

The following example shows how to manually issue a test message:

```
switch# test aaa server tacacs+ 10.10.1.1 user1 Ur2Gd2BH
switch# test aaa group TacGroup user2 As3He3CI
```

Disabling TACACS+

You can disable TACACS+.



Caution

When you disable TACACS+, all related configurations are automatically discarded.

Procedure

| | Command or Action | Purpose |
|---------------|--|--|
| Step 1 | switch# configure terminal | Enters global configuration mode. |
| Step 2 | switch(config)# no feature tacacs+ | Disables TACACS+. |
| Step 3 | switch(config)# exit | Exits configuration mode. |
| Step 4 | (Optional) switch# copy running-config startup-config | Copies the running configuration to the startup configuration. |

Displaying TACACS+ Statistics

To display the statistics, the switch maintains for TACACS+ activity, perform this task:

Example

For detailed information about the fields in the output from this command, see the *Command Reference* for your Nexus switch.

Verifying the TACACS+ Configuration

To display TACACS+ information, perform one of the following tasks:

| Command | Purpose |
|--|---|
| <code>show tacacs+ {status pending pending-diff}</code> | Displays the TACACS+ Cisco Fabric Services distribution status and other details. |
| <code>show running-config tacacs [all]</code> | Displays the TACACS+ configuration in the running configuration. |
| <code>show startup-config tacacs</code> | Displays the TACACS+ configuration in the startup configuration. |
| <code>show tacacs-serve [host-name ipv4-address ipv6-address] [directed-request groups sorted statistics]</code> | Displays all configured TACACS+ server parameters. |

Configuration Examples for TACACS+

This example shows how to configure TACACS+:

```
switch# configure terminal
switch(config)# feature tacacs+
switch(config)# tacacs-server key 7 "ToIkLhPpG"
switch(config)# tacacs-server host 10.10.2.2 key 7 "ShMoMhTl"
switch(config)# aaa group server tacacs+ TacServer
switch(config-tacacs+)# server 10.10.2.2
switch(config-tacacs+)# use-vrf management
```

This example shows how to enable tacacs+ and how to configure the tacacs+ server preshared keys to specify remote AAA servers to authenticate server group TacServer1:

```
switch# configure terminal
switch(config)# feature tacacs+
switch(config)# tacacs-server key 7 "ikvhw10"
switch(config)# tacacs-server host 1.1.1.1
switch(config)# tacacs-server host 1.1.1.2

switch(config)# aaa group server tacacs+ TacServer1
switch(config-tacacs+)# server 1.1.1.1
switch(config-tacacs+)# server 1.1.1.2
```

