



Configuring TACACS+

This chapter describes how to configure the Terminal Access Controller Access Control System Plus (TACACS+) protocol on Cisco NX-OS devices.

- [About Configuring TACACS+, page 1](#)

About Configuring TACACS+

Information About 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 3000 Series switch. 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 3000 Series switch 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. Cisco Nexus 3000 Series switches provide 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 3000 Series switch 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 3000 Series switch using TACACS+, the following actions occur:

- 1 When the Cisco Nexus 3000 Series switch 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 3000 Series switch will receive one of the following responses from the TACACS+ daemon:
 - ACCEPT—User authentication succeeds and service begins. If the Cisco Nexus 3000 Series switch 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 3000 Series switch. If the Cisco Nexus 3000 Series switch 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 3000 Series switch. Users must first successfully complete TACACS+ authentication before proceeding to TACACS+ authorization.

- 3 If TACACS+ authorization is required, the Cisco Nexus 3000 Series switch 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+ preshared key to authenticate the switch to the TACACS+ server. A preshared key is a secret text string shared between the Cisco Nexus 3000 Series switch 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 3000 Series switch to use.

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

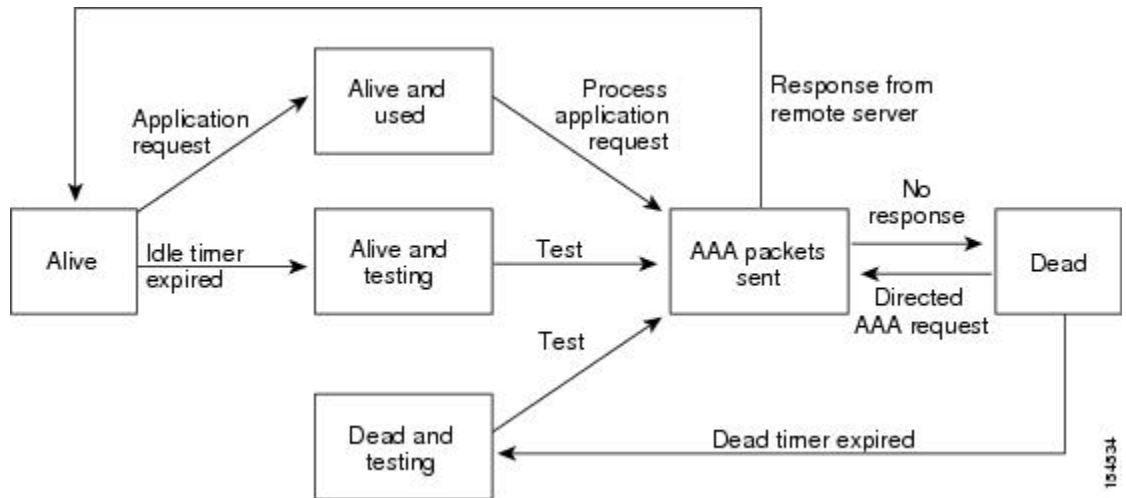
Command Authorization Support for TACACS+ Servers

By default, command authorization is done against a local database in the Cisco NX-OS software when an authenticated user enters a command at the command-line interface (CLI). You can also verify authorized commands for authenticated users using TACACS+.

TACACS+ Server Monitoring

An unresponsive TACACS+ server can delay the processing of AAA requests. A Cisco Nexus 3000 Series switch can periodically monitor an TACACS+ server to check whether it is responding (or alive) to save time in processing AAA requests. The Cisco Nexus 3000 Series switch marks unresponsive TACACS+ servers as dead and does not send AAA requests to any dead TACACS+ servers. A Cisco Nexus 3000 Series switch 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 its way. Whenever an TACACS+ server changes to the dead or alive state, a Simple Network Management Protocol (SNMP) trap is generated and the Cisco Nexus 3000 Series switch displays an error message that a failure is taking place before it can impact performance.

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:

- Obtain the IPv4 addresses or host names for the TACACS+ servers.

- Obtain the preshared keys from the TACACS+ servers, if any.
- Ensure that the Cisco Nexus 3000 Series switch is configured as a TACACS+ client of the AAA servers.

Guidelines and Limitations for TACACS+

TACACS+ has the following guidelines and limitations:

- You can configure a maximum of 64 TACACS+ servers on the Cisco Nexus 3000 Series switch.

Configuring TACACS+

TACACS+ Server Configuration Process

To configure TACACS+ servers, perform this task:

SUMMARY STEPS

1. Enable TACACS+.
2. Establish the TACACS+ server connections to the Cisco Nexus 3000 Series switch.
3. Configure the preshared secret keys for the TACACS+ servers.
4. If needed, configure TACACS+ server groups with subsets of the TACACS+ servers for AAA authentication methods.
5. If needed, configure any of the following optional parameters:
6. If needed, configure periodic TACACS+ server monitoring.

DETAILED STEPS

-
- | | |
|---------------|--|
| Step 1 | Enable TACACS+. |
| Step 2 | Establish the TACACS+ server connections to the Cisco Nexus 3000 Series switch. |
| 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: <ul style="list-style-type: none"> • Dead-time interval • Allow TACACS+ server specification at login • Timeout interval • TCP port |
| Step 6 | If needed, configure periodic TACACS+ server monitoring. |
-

Enabling TACACS+

By default, the TACACS+ feature is disabled on the Cisco Nexus 3000 Series switch. To explicitly enable the TACACS+ feature to access the configuration and verification commands for authentication, perform this task:

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **feature tacacs+**
3. switch(config)# **exit**
4. (Optional) switch# **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	switch# configure terminal	Enters configuration mode.
Step 2	switch(config)# feature tacacs+	Enables TACACS+.
Step 3	switch(config)# exit	Exits configuration mode.
Step 4	switch# copy running-config startup-config	(Optional) 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 3000 Series switch. 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.

To configure TACACS+ server hosts, perform this task:

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **tacacs-server host** {*ipv4-address* | *host-name*}
3. switch(config)# **exit**
4. (Optional) switch# **show tacacs-server**
5. (Optional) switch# **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	switch# configure terminal	Enters configuration mode.
Step 2	switch(config)# tacacs-server host { <i>ipv4-address</i> <i>host-name</i> }	Specifies the IPv4 address or hostname for a TACACS+ server.
Step 3	switch(config)# exit	Exits configuration mode.
Step 4	switch# show tacacs-server	(Optional) Displays the TACACS+ server configuration.
Step 5	switch# copy running-config startup-config	(Optional) Copies the running configuration to the startup configuration.

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 3000 Series switch. A preshared key is a shared secret text string between the Cisco Nexus 3000 Series switch 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.

To configure global preshared keys, perform this task:

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **tacacs-server key [0 | 7] key-value**
3. switch(config)# **exit**
4. (Optional) switch# **show tacacs-server**
5. (Optional) switch# **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	switch# configure terminal	Enters configuration mode.
Step 2	switch(config)# tacacs-server key [0 7] key-value	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	switch# show tacacs-server	(Optional) 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	switch# copy running-config startup-config	(Optional) Copies the running configuration to the startup configuration.

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
```

Related Topics

[Enabling TACACS+ , on page 5](#)

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 3000 Series switch and the TACACS+ server host.

To configure the TACACS+ preshared keys, perform this task:

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **tacacs-server host** {*ipv4-address* | *host-name*} **key** [0 | 7] *key-value*
3. switch(config)# **exit**
4. (Optional) switch# **show tacacs-server**
5. (Optional) switch# **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	switch# configure terminal	Enters configuration mode.
Step 2	switch(config)# tacacs-server host { <i>ipv4-address</i> <i>host-name</i> } key [0 7] <i>key-value</i>	Specifies a preshared key for a specific TACACS+ server. You can specify a clear text (0) or encrypted (7) preshared key. The default format is clear text. The maximum length is 63 characters. This preshared key is used instead of the global preshared key.
Step 3	switch(config)# exit	Exits configuration mode.
Step 4	switch# show tacacs-server	(Optional) 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	switch# copy running-config startup-config	(Optional) Copies the running configuration to the startup configuration.

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 P1IjUhYg
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+.

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **aaa group server tacacs+ group-name**
3. switch(config)# **tacacs-server host {ipv4-address | host-name} key [0 | 7] key-value**
4. (Optional) switch(config-tacacs+)# **deadtime minutes**
5. (Optional) switch(config-tacacs+)# **source-interface interface**
6. switch(config-tacacs+)# **exit**
7. (Optional) switch(config)# **show tacacs-server groups**
8. (Optional) switch(config)# **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	switch# configure terminal	Enters configuration mode.
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	switch(config)# tacacs-server host {ipv4-address host-name} key [0 7] key-value	Specifies a preshared key for a specific TACACS+ server. You can specify a clear text (0) or encrypted (7) preshared key. The default format is clear text. The maximum length is 63 characters. This preshared key is used instead of the global preshared key.
Step 4	switch(config-tacacs+)# deadtime minutes Example:	(Optional) 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 5	switch(config-tacacs+)# source-interface interface Example: switch(config-tacacs+)# source-interface mgmt 0	(Optional) 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 6	switch(config-tacacs+)# exit	Exits configuration mode.
Step 7	switch(config)# show tacacs-server groups	(Optional) Displays the TACACS+ server group configuration.
Step 8	switch(config)# copy running-config startup-config	(Optional) Copies the running configuration to the startup configuration.

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)# deadline 30
switch(config-tacacs)# exit
switch(config)# show tacacs-server groups
switch(config)# copy running-config startup-config
```

Table 1: Related Commands

Command	Description
feature tacacs+	Enables the TACACS+ feature.
ip tacacs source-interface	Configures the global source interface for the TACACS+ groups configured on the Cisco NX-OS device.
show tacacs-server groups	Displays the TACACS+ server group configuration.

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. Refer to Related Commands for additional information.

SUMMARY STEPS

1. **configure terminal**
2. **ip tacacs source-interface** *interface*
3. **exit**
4. (Optional) **show tacacs-server**
5. (Optional) **copy running-config startup config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: switch# configure terminal switch(config)	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.

	Command or Action	Purpose
Step 3	exit Example: <pre>switch(config)# exit switch#</pre>	Exits configuration mode.
Step 4	show tacacs-server Example: <pre>switch# show tacacs-server</pre>	(Optional) Displays the TACACS+ server configuration information.
Step 5	copy running-config startup config Example: <pre>switch# copy running-config startup-config</pre>	(Optional) Copies the running configuration to the startup configuration.

Table 2: Related Commands

Command	Description
aaa group server tacacs group-name	Creates a TACACS+ server group and enters the TACACS+ server group configuration submode for that group. The group-name argument is a case-sensitive alphanumeric string with a maximum length of 127 characters.

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 3000 Series switch 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.

To specify a TACACS+ server at login, perform this task:

SUMMARY STEPS

1. `switch# configure terminal`
2. `switch(config)# tacacs-server directed-request`
3. `switch(config)# exit`
4. (Optional) `switch# show tacacs-server directed-request`
5. (Optional) `switch# copy running-config startup-config`

DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>switch# configure terminal</code>	Enters configuration mode.
Step 2	<code>switch(config)# tacacs-server directed-request</code>	Allows users to specify a TACACS+ server to send the authentication request when logging in. The default is disabled.
Step 3	<code>switch(config)# exit</code>	Exits configuration mode.
Step 4	<code>switch# show tacacs-server directed-request</code>	(Optional) Displays the TACACS+ directed request configuration.
Step 5	<code>switch# copy running-config startup-config</code>	(Optional) Copies the running configuration to the startup configuration.

Configuring AAA Authorization on TACACS+ Servers

You can configure the default AAA authorization method for TACACS+ servers.

Before You Begin

Enable TACACS+.

SUMMARY STEPS

1. `configure terminal`
2. `aaa authorization ssh-certificate default {group group-list [none] | local | none}`
3. `exit`
4. (Optional) `show aaa authorization [all]`
5. (Optional) `copy running-config startup-config`

DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>configure terminal</code> Example: <code>switch# configure terminal</code> <code>switch(config)#</code>	Enters global configuration mode.
Step 2	<code>aaa authorization ssh-certificate default {group group-list [none] local none}</code>	Configures the default AAA authorization method for the TACACS+ servers.

	Command or Action	Purpose
	<p>Example:</p> <pre>switch(config)# aaa authorization ssh-certificate default group TACACSServer1 TACACSServer2</pre>	<p>The ssh-certificate keyword configures TACACS+ or local authorization with certificate authentication. The default authorization is local authorization, which is the list of authorized commands for the user's assigned role.</p> <p>The <i>group-list</i> argument consists of a space-delimited list of TACACS+ server group names. Servers belonging to this group are contacted for AAA authorization. The local method uses the local database for authorization, and the none method specifies that no AAA authorization be used.</p>
Step 3	<p>exit</p> <p>Example:</p> <pre>switch(config)# exit switch#</pre>	Exits global configuration mode.
Step 4	<p>show aaa authorization [all]</p> <p>Example:</p> <pre>switch# show aaa authorization</pre>	<p>(Optional)</p> <p>Displays the AAA authorization configuration. The all keyword displays the default values.</p>
Step 5	<p>copy running-config startup-config</p> <p>Example:</p> <pre>switch# copy running-config startup-config</pre>	<p>(Optional)</p> <p>Copies the running configuration to the startup configuration.</p>

Configuring Command Authorization on TACACS+ Servers

You can configure authorization for commands on TACACS+ servers. Command authorization disables user role-based authorization control (RBAC), including the default roles.



Note By default, context sensitive help and command tab completion show only the commands that are supported for a user as defined by the assigned roles. When you enable command authorization, the Cisco NX-OS software displays all commands in the context sensitive help and in tab completion, regardless of the role assigned to the user.

Before You Begin

Enable TACACS+.

Configure TACACS host and server groups before configuring AAA command authorization.

SUMMARY STEPS

1. **configure terminal**
2. **aaa authorization {commands | config-commands} default [group group-list [local] | local]**
3. **exit**
4. (Optional) **show aaa authorization [all]**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
Step 2	aaa authorization {commands config-commands} default [group group-list [local] local] Example: <pre>switch(config)# aaa authorization commands default group TacGroup</pre>	<p>Configures the default authorization method for commands for all roles. The commands keyword configures authorization sources for all EXEC commands, and the config-commands keyword configures authorization sources for all configuration commands. The default authorization for all commands is local authorization, which is the list of authorized commands for the user's assigned role.</p> <p>The <i>group-list</i> argument consists of a space-delimited list of TACACS+ server group names. Servers that belong to this group are contacted for command authorization. The local method uses the local role-based database for authorization..</p> <p>The local method is used only if all the configured server groups fail to respond and you have configured local as the fallback method.</p> <p>The default method is local.</p> <p>If you have not configured a fallback method after the TACACS+ server group method, authorization fails if all server groups fail to respond.</p>
Step 3	exit Example: <pre>switch(config)# exit switch#</pre>	Exits global configuration mode.
Step 4	show aaa authorization [all] Example: <pre>switch(config)# show aaa authorization</pre>	(Optional) Displays the AAA authorization configuration. The all keyword displays the default values.
Step 5	copy running-config startup-config Example: <pre>switch(config)# copy running-config startup-config</pre>	(Optional) Copies the running configuration to the startup configuration.

Testing Command Authorization on TACACS+ Servers

You can test the command authorization for a user on the TACACS+ servers.



Note You must send correct commands for authorization or the results might not be reliable.

Before You Begin

Enable TACACS+.

Ensure that you have configured command authorization for the TACACS+ servers.

SUMMARY STEPS

1. **test aaa authorization command-type {commands | config-commands} user *username* command *command-string***

DETAILED STEPS

	Command or Action	Purpose
Step 1	test aaa authorization command-type {commands config-commands} user <i>username</i> command <i>command-string</i> Example: <pre>switch# test aaa authorization command-type commands user TestUser command reload</pre>	Tests a user's authorization for a command on the TACACS+ servers. The commands keyword specifies only EXEC commands and the config-commands keyword specifies only configuration commands. Note Put double quotes (") before and after the <i>command-string</i> argument if it contains spaces.

Enabling and Disabling Command Authorization Verification

You can enable and disable command authorization verification on the command-line interface (CLI) for the default user session or for another username.



Note The commands do not execute when you enable authorization verification.

SUMMARY STEPS

1. **terminal verify-only [username *username*]**
2. **terminal no verify-only [username *username*]**

DETAILED STEPS

	Command or Action	Purpose
Step 1	terminal verify-only [username <i>username</i>] Example: switch# terminal verify-only	Enables command authorization verification. After you enter this command, the Cisco NX-OS software indicates whether the commands you enter are authorized or not.
Step 2	terminal no verify-only [username <i>username</i>] Example: switch# terminal no verify-only	Disables command authorization verification.

Configuring Privilege Level Support for Authorization on TACACS+ Servers

You can configure privilege level support for authorization on TACACS+ servers.

Unlike Cisco IOS devices, which use privilege levels to determine authorization, Cisco NX-OS devices use role-based access control (RBAC). To enable both types of devices to be administered by the same TACACS+ servers, you can map the privilege levels configured on TACACS+ servers to user roles configured on Cisco NX-OS devices.

When a user authenticates with a TACACS+ server, the privilege level is obtained and used to form a local user role name of the format "priv-*n*," where *n* is the privilege level. The user assumes the permissions of this local role. Sixteen privilege levels, which map directly to corresponding user roles, are available. The following table shows the user role permissions that correspond to each privilege level.

Privilege Level	User Role Permissions
15	network-admin permissions
13 - 1	<ul style="list-style-type: none"> Standalone role permissions, if the feature privilege command is disabled. Same permissions as privilege level 0 with cumulative privileges for roles, if the feature privilege command is enabled.
0	Permission to execute show commands and exec commands (such as ping , trace , and ssh).



Note When the **feature privilege** command is enabled, privilege roles inherit the permissions of lower level privilege roles.

SUMMARY STEPS

1. **configure terminal**
2. **[no] feature privilege**
3. **[no] enable secret [0 | 5] password [priv-lvl priv-lvl | all]**
4. **[no] username username priv-lvl n**
5. (Optional) **show privilege**
6. (Optional) **copy running-config startup-config**
7. **exit**
8. **enable level**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
Step 2	[no] feature privilege Example: <pre>switch(config)# feature privilege</pre>	Enables or disables the cumulative privilege of roles. Users can see the enable command only if this feature is enabled. The default is disabled.
Step 3	[no] enable secret [0 5] password [priv-lvl priv-lvl all] Example: <pre>switch(config)# enable secret 5 def456 priv-lvl 15</pre>	<p>Enables or disables a secret password for a specific privilege level. Users are prompted to enter the correct password upon each privilege level escalation. The default is disabled.</p> <p>You can enter 0 to specify that the password is in clear text or 5 to specify that the password is in encrypted format. The <i>password</i> argument can be up to 64 alphanumeric characters. The <i>priv-lvl</i> argument is from 1 to 15.</p> <p>Note To enable the secret password, you must have enabled the cumulative privilege of roles by entering the feature privilege command.</p>
Step 4	[no] username username priv-lvl n Example: <pre>switch(config)# username user2 priv-lvl 15</pre>	<p>Enables or disables a user to use privilege levels for authorization. The default is disabled.</p> <p>The priv-lvl keyword specifies the privilege level to which the user is assigned. There is no default privilege level. Privilege levels 0 to 15 (priv-lvl 0 to priv-lvl 15) map to user roles priv-0 to priv-15.</p>
Step 5	show privilege Example: <pre>switch(config)# show privilege</pre>	<p>(Optional)</p> <p>Displays the username, current privilege level, and status of cumulative privilege support.</p>

	Command or Action	Purpose
Step 6	copy running-config startup-config Example: <pre>switch(config)# copy running-config startup-config</pre>	(Optional) Copies the running configuration to the startup configuration.
Step 7	exit Example: <pre>switch(config)# exit switch#</pre>	Exits global configuration mode.
Step 8	enable level Example: <pre>switch# enable 15</pre>	Enables a user to move to a higher privilege level. This command prompts for the secret password. The <i>level</i> argument specifies the privilege level to which the user is granted access. The only available level is 15.

Permitting or Denying Commands for Users of Privilege Roles

As a network administrator, you can modify the privilege roles to permit users to execute specific commands or to prevent users from running those commands.

You must follow these guidelines when changing the rules of privilege roles:

- You cannot modify the priv-14 and priv-15 roles.
- You can add deny rules only to the priv-0 role.
- These commands are always permitted for the priv-0 role: **configure**, **copy**, **dir**, **enable**, **ping**, **show**, **ssh**, **telnet**, **terminal**, **traceroute**, **end**, and **exit**.

SUMMARY STEPS

1. **configure terminal**
2. **[no] role name priv-*n***
3. **rule *number* {deny | permit} command *command-string***
4. **exit**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.

	Command or Action	Purpose
Step 2	<p>[no] role name priv-<i>n</i></p> <p>Example: <pre>switch(config)# role name priv-5 switch(config-role)#</pre></p>	Enables or disables a privilege role and enters role configuration mode. The <i>n</i> argument specifies the privilege level and is a number between 0 and 13.
Step 3	<p>rule number {deny permit} command <i>command-string</i></p> <p>Example: <pre>switch(config-role)# rule 2 permit command pwd</pre></p>	<p>Configures a command rule for users of privilege roles. These rules permit or deny users to execute specific commands. You can configure up to 256 rules for each role. The rule number determines the order in which the rules are applied. Rules are applied in descending order. For example, if a role has three rules, rule 3 is applied before rule 2, which is applied before rule 1.</p> <p>The <i>command-string</i> argument can contain spaces.</p> <p>Note Repeat this command for 256 rules.</p>
Step 4	<p>exit</p> <p>Example: <pre>switch(config-role)# exit switch(config)#</pre></p>	Exits role configuration mode.
Step 5	<p>copy running-config startup-config</p> <p>Example: <pre>switch(config)# copy running-config startup-config</pre></p>	(Optional) 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 3000 Series switch 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.

To specify a TACACS+ global timeout interval, perform this task:

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **tacacs-server timeout** *seconds*
3. switch(config)# **exit**
4. (Optional) switch# **show tacacs-server**
5. (Optional) switch# **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	switch# configure terminal	Enters 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	switch# show tacacs-server	(Optional) Displays the TACACS+ server configuration.
Step 5	switch# copy running-config startup-config	(Optional) 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 3000 Series switch 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.

To configure the timeout interval for a server, perform this task:

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# switch(config)# **tacacs-server host {ipv4-address | host-name} timeout seconds**
3. switch(config)# **exit**
4. (Optional) switch# **show tacacs-server**
5. (Optional) switch# **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	switch# configure terminal	Enters configuration mode.
Step 2	switch(config)# switch(config)# tacacs-server host {ipv4-address host-name} timeout seconds	Specifies the timeout interval for a specific server. The default is the global value. Note The timeout interval value specified for a TACACS+ server overrides the global timeout interval value specified for all TACACS+ servers.
Step 3	switch(config)# exit	Exits configuration mode.

	Command or Action	Purpose
Step 4	switch# show tacacs-server	(Optional) Displays the TACACS+ server configuration.
Step 5	switch# copy running-config startup-config	(Optional) 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, Cisco Nexus 3000 Series switches use port 49 for all TACACS+ requests.

To configure TCP ports, perform this task:

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **tacacs-server host {ipv4-address | host-name} port tcp-port**
3. switch(config)# **exit**
4. (Optional) switch# **show tacacs-server**
5. (Optional) switch# **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	switch# configure terminal	Enters configuration mode.
Step 2	switch(config)# tacacs-server host {ipv4-address host-name} port tcp-port	Specifies the UDP port to use for TACACS+ accounting messages. The default TCP port is 49. The range is from 1 to 65535.
Step 3	switch(config)# exit	Exits configuration mode.
Step 4	switch# show tacacs-server	(Optional) Displays the TACACS+ server configuration.
Step 5	switch# copy running-config startup-config	(Optional) Copies the running configuration to the startup configuration.

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 3000 Series switch 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 user name 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 3000 Series switch 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.

To configure periodic TACACS+ server monitoring, perform this task:

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **tacacs-server host** {*ipv4-address* | *host-name*} **test** {*idle-time minutes* | **password** *password* [*idle-time minutes*] | **username** *name* [**password** *password* [*idle-time minutes*]]}
3. switch(config)# **tacacs-server dead-time** *minutes*
4. switch(config)# **exit**
5. (Optional) switch# **show tacacs-server**
6. (Optional) switch# **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	switch# configure terminal	Enters configuration mode.
Step 2	switch(config)# tacacs-server host { <i>ipv4-address</i> <i>host-name</i> } test { <i>idle-time minutes</i> password <i>password</i> [<i>idle-time minutes</i>] username <i>name</i> [password <i>password</i> [<i>idle-time minutes</i>]]}	Specifies parameters for server monitoring. The default username is test and the default password is test. The default value for the idle timer is 0 minutes and the valid range is 0 to 1440 minutes. Note For periodic TACACS+ server monitoring, the idle timer value must be greater than 0.
Step 3	switch(config)# tacacs-server dead-time <i>minutes</i>	Specifies the number minutes before the Cisco Nexus 3000 Series switch checks a TACACS+ server that was previously unresponsive. The default value is 0 minutes and the valid range is 0 to 1440 minutes.

	Command or Action	Purpose
Step 4	switch(config)# exit	Exits configuration mode.
Step 5	switch# show tacacs-server	(Optional) Displays the TACACS+ server configuration.
Step 6	switch# copy running-config startup-config	(Optional) Copies the running configuration to the startup configuration.

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 3000 Series switch 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-timer interval is 0 minutes, TACACS+ servers are not marked as dead even if they are not responding. You can configure the dead-timer per group.

To configure the dead-time interval for all TACACS+ servers, perform this task:

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **tacacs-server deadtime** *minutes*
3. switch(config)# **exit**
4. (Optional) switch# **show tacacs-server**
5. (Optional) switch# **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	switch# configure terminal	Enters 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.

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

Manually Monitoring TACACS+ Servers or Groups

To manually issue a test message to a TACACS+ server or to a server group, perform this task:

SUMMARY STEPS

1. switch# test aaa server tacacs+ {ipv4-address | ipv6-address | host-name} [vrf vrf-name] username password
2. switch# test aaa group group-name username password

DETAILED STEPS

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

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.

To disable TACACS+, perform this task:

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **no feature tacacs+**
3. switch(config)# **exit**
4. (Optional) switch# **copy running-config startup-config**

DETAILED STEPS

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

Displaying TACACS+ Statistics

To display the statistics the Cisco Nexus 3000 Series switch maintains for TACACS+ activity, perform this task:

SUMMARY STEPS

1. switch# **show tacacs-server statistics** {hostname | ipv4-address | ipv6-address}

DETAILED STEPS

	Command or Action	Purpose
Step 1	switch# show tacacs-server statistics {hostname ipv4-address ipv6-address}	Displays the TACACS+ statistics.

For detailed information about the fields in the output from this command, see the *Cisco Nexus 3000 Series Command Reference*.

Verifying TACACS+ Configuration

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

SUMMARY STEPS

1. switch# show tacacs+ {status | pending | pending-diff}
2. switch# show running-config tacacs [all]
3. switch# show startup-config tacacs
4. switch# show tacacs-serve [host-name | ipv4-address] [directed-request | groups | sorted | statistics]

DETAILED STEPS

	Command or Action	Purpose
Step 1	switch# show tacacs+ {status pending pending-diff}	Displays the TACACS+ Cisco Fabric Services distribution status and other details.
Step 2	switch# show running-config tacacs [all]	Displays the TACACS+ configuration in the running configuration.
Step 3	switch# show startup-config tacacs	Displays the TACACS+ configuration in the startup configuration.
Step 4	switch# show tacacs-serve [host-name ipv4-address] [directed-request groups sorted statistics]	Displays all configured TACACS+ server parameters.

Configuration Examples for TACACS+

The following 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
```

The following 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# config t
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
```

Default TACACS+ Settings

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

Table 3: Default TACACS+ Parameters

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

