Configuring TACACS+

- Prerequisites for TACACS+, on page 1
- Restrictions for TACACS+, on page 2
- Information About TACACS+, on page 2
- How to Configure TACACS+, on page 5
- Monitoring TACACS+, on page 14
- Additional References for TACACS+, on page 14
- Feature History for TACACS+, on page 15

Prerequisites for TACACS+

The following are the prerequisites for set up and configuration of switch access with TACACS+ (must be performed in the order presented):

1. Configure the switches with the TACACS+ server addresses.
2. Set an authentication key.
3. Configure the key from Step 2 on the TACACS+ servers.
4. Enable authentication, authorization, and accounting (AAA).
5. Create a login authentication method list.
6. Apply the list to the terminal lines.
7. Create an authorization and accounting method list.

The following are the prerequisites for controlling switch access with TACACS+:

- You must have access to a configured TACACS+ server to configure TACACS+ features on your switch. Also, you must have access to TACACS+ services maintained in a database on a TACACS+ daemon typically running on a LINUX or Windows workstation.
- You need a system running the TACACS+ daemon software to use TACACS+ on your switch.
- To use TACACS+, it must be enabled.
- Authorization must be enabled on the switch to be used.

- Users must first successfully complete TACACS+ authentication before proceeding to TACACS+ authorization.
- To use any of the AAA commands listed in this section or elsewhere, you must first enable AAA with the **aaa new-model** command.
- At a minimum, you must identify the host or hosts maintaining the TACACS+ daemon and define the method lists for TACACS+ authentication. You can optionally define method lists for TACACS+ authorization and accounting.
- The method list defines the types of authentication to be performed and the sequence in which they are performed; it must be applied to a specific port before any of the defined authentication methods are performed. The only exception is the default method list (which, by coincidence, is named *default*). The default method list is automatically applied to all ports except those that have a named method list explicitly defined. A defined method list overrides the default method list.
- Use TACACS+ for privileged EXEC access authorization if authentication was performed by using TACACS+.
- Use the local database if authentication was not performed by using TACACS+.

Restrictions for TACACS+

- VRF-aware DNS resolution is not supported if configured with FQDNs.

Information About TACACS+

TACACS+ and Switch Access

This section describes TACACS+. TACACS+ provides detailed accounting information and flexible administrative control over the authentication and authorization processes. It is facilitated through authentication, authorization, accounting (AAA) and can be enabled only through AAA commands.

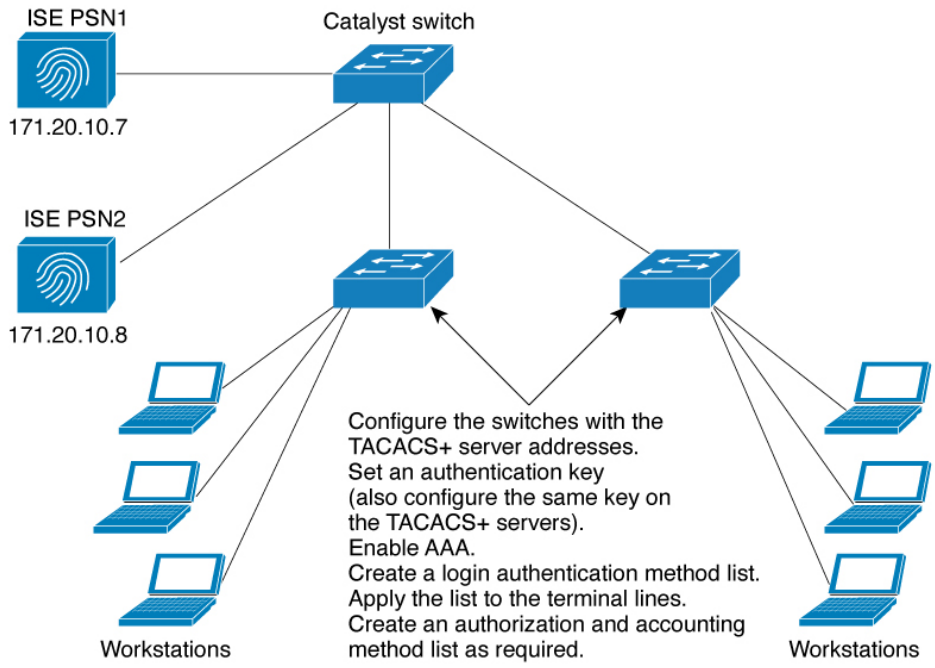
TACACS+ Overview

TACACS+ is a security application that provides centralized validation of users attempting to gain access to your switch.

TACACS+ provides for separate and modular 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 can be tied into 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 goal of TACACS+ is to provide a method for managing multiple network access points from a single management service. Your switch can be a network access server along with other Cisco routers and access servers.

Figure 1: Network Configuration of Typical TACACS+



TACACS+, administered through the AAA security services, can provide these services:

- Authentication: Provides complete control of authentication through login and password dialog, challenge and response, and messaging support.

  The authentication facility can conduct a dialog with the user (for example, after a username and password are provided, to challenge a user with several questions, such as home address, mother's maiden name, service type, and social security number). The TACACS+ authentication service can also send messages to user screens. For example, a message could notify users that their passwords must be changed because of the company's password aging policy.

- Authorization: Provides fine-grained control over user capabilities for the duration of the user's session, including but not limited to setting autocommands, access control, session duration, or protocol support. You can also enforce restrictions on what commands a user can execute with the TACACS+ authorization feature.

- Accounting: Collects and sends information used for billing, auditing, and reporting to the TACACS+ daemon. Network managers can use the accounting facility to track user activity for a security audit or to provide information for user billing. Accounting records include user identities, start and stop times, executed commands (such as PPP), number of packets, and number of bytes.

The TACACS+ protocol provides authentication between the switch and the TACACS+ daemon, and it ensures confidentiality because all protocol exchanges between the switch and the TACACS+ daemon are encrypted.

TACACS+ Operation

When a user attempts a simple ASCII login by authenticating to a switch using TACACS+, this process occurs:

1. When the connection is established, the switch contacts the TACACS+ daemon to obtain a username prompt to show to the user. The user enters a username, and the switch then contacts the TACACS+ daemon to obtain a password prompt. The switch displays the password prompt to the user, the user enters a password, and the password is then sent to the TACACS+ daemon.

   TACACS+ allows a dialog between the daemon and the user until the daemon receives enough information to authenticate the user. The daemon prompts for a username and password combination, but can include other items, such as the user's mother's maiden name.

2. The switch eventually receives one of these responses from the TACACS+ daemon:

   - ACCEPT: The user is authenticated and service can begin. If the switch is configured to require authorization, authorization begins at this time.
   - REJECT: The user is not authenticated. The user can be denied access or is prompted to retry the login sequence, depending on the TACACS+ daemon.
   - ERROR: An error occurred at some time during authentication with the daemon or in the network connection between the daemon and the switch. If an ERROR response is received, the switch typically tries to use an alternative method for authenticating the user.
   - CONTINUE: The user is prompted for additional authentication information.

   After authentication, the user undergoes an additional authorization phase if authorization has been enabled on the switch. Users must first successfully complete TACACS+ authentication before proceeding to TACACS+ authorization.

3. If TACACS+ authorization is required, the TACACS+ daemon is again contacted, and it returns an ACCEPT or REJECT authorization response. If an ACCEPT response is returned, the response contains data in the form of attributes that direct the EXEC or NETWORK session for that user and the services that the user can access:

   - Telnet, Secure Shell (SSH), rlogin, or privileged EXEC services
   - Connection parameters, including the host or client IP address, access list, and user timeouts

Method List

A method list defines the sequence and methods to be used to authenticate, to authorize, or to keep accounts on a user. You can use method lists to designate one or more security protocols to be used, thus ensuring a backup system if the initial method fails. The software uses the first method listed to authenticate, to authorize, or to keep accounts on users; if that method does not respond, the software selects the next method in the list. This process continues until there is successful communication with a listed method or the method list is exhausted.

TACACS+ Configuration Options

You can configure the switch to use a single server or AAA server groups to group existing server hosts for authentication. You can group servers to select a subset of the configured server hosts and use them for a particular service. The server group is used with a global server-host list and contains the list of IP addresses of the selected server hosts.

TACACS+ Login Authentication

A method list describes the sequence and authentication methods to be queried to authenticate a user. You can designate one or more security protocols to be used for authentication, thus ensuring a backup system for authentication in case the initial method fails. The software uses the first method listed to authenticate users; if that method fails to respond, the software selects the next authentication method in the method list. This process continues until there is successful communication with a listed authentication method or until all defined methods are exhausted. If authentication fails at any point in this cycle—meaning that the security server or local username database responds by denying the user access—the authentication process stops, and no other authentication methods are attempted.

TACACS+ Authorization for Privileged EXEC Access and Network Services

AAA authorization limits the services available to a user. When AAA authorization is enabled, the switch uses information retrieved from the user's profile, which is located either in the local user database or on the security server, to configure the user's session. The user is granted access to a requested service only if the information in the user profile allows it.

TACACS+ Accounting

The AAA accounting feature tracks the services that users are accessing and the amount of network resources that they are consuming. When AAA accounting is enabled, the switch reports user activity to the TACACS+ security server in the form of accounting records. Each accounting record contains accounting attribute-value (AV) pairs and is stored on the security server. This data can then be analyzed for network management, client billing, or auditing.

TACACS+ over TLS

TACACS+ over Transport Layer Security (TLS) enhances security and provides stronger certificate-based AAA services. It sends device authentication traffic over encrypted channels.

Default TACACS+ Configuration

TACACS+ and AAA are disabled by default.

To prevent a lapse in security, you cannot configure TACACS+ through a network management application. When enabled, TACACS+ can authenticate users accessing the switch through the CLI.

Note Although TACACS+ configuration is performed through the CLI, the TACACS+ server authenticates HTTP connections that have been configured with a privilege level of 15.

How to Configure TACACS+

This section describes how to configure your switch to support TACACS+.

Identifying the TACACS+ Server Host and Setting the Authentication Key

Follow these steps to identify the TACACS+ server host and set the authentication key:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**tacacs server** *server-name* **Example:** `Device(config)# tacacs server yourserver`	Configures a TACACS+ public server by specifying a server name and enters TACACS+ server configuration mode. This command allows you to define the TACACS+ server settings such as IP address, encryption key, port, timeout, and other parameters for AAA services. For *server-name*, specify the server name.
Step 4	**address** {**ipv4** | **ipv6**} *ip address* **Example:** `Device(config-server-tacacs)# address ipv4 10.0.1.12`	Configures the IP address for the TACACS server.
Step 5	**key** [*encryption-type*] [*key-string*] **Example:** `Device(config-server-tacacs)# key 0 auth-key`	Sets the authentication encryption key used for all TACACS+ communications between the access server and the TACACS+ daemon. This encryption key must match the key used on the TACACS+ daemon. *encryption-type* is optional, and if nothing is specified it is considered as clear text. Enter **0** to specify that an unencrypted key will follow. Enter **6** to specify that an encrypted key will follow. Enter **7** to specify that a hidden key will follow.
Step 6	**exit** **Example:** `Device(config-server-tacacs)# exit`	Exits the TACACS server mode and enters the global configuration mode.
Step 7	**aaa new-model** **Example:**	Enables AAA.

	Command or Action	Purpose
	`Device(config)# aaa new-model`	
Step 8	**aaa group server tacacs+** *group-name* **Example:** `Device(config)# aaa group server tacacs+ your_server_group`	(Optional) Defines the AAA server-group with a group name, and enters server group configuration mode.
Step 9	**server name** *server-name* **Example:** `Device(config-sg-tacacs)# server name yourserver`	(Optional) Associates a particular TACACS+ server with the defined server group. Repeat this step for each TACACS+ server in the AAA server group. Each server in the group must be previously defined in Step 3.
Step 10	**end** **Example:** `Device(config-sg-tacacs)# end`	Exits server group configuration mode and returns to privileged EXEC mode.

Configuring TACACS+ Login Authentication

Follow these steps to configure TACACS+ login authentication:

Before you begin

To configure AAA authentication, you define a named list of authentication methods and then apply that list to various ports.

Note To secure the device for HTTP access by using AAA methods, you must configure the device with the **ip http authentication aaa** global configuration command. Configuring AAA authentication does not secure the device for HTTP access by using AAA methods.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**aaa new-model** **Example:** `Device(config)# aaa new-model`	Enables AAA.
Step 4	**aaa authentication login** {**default** | *list-name*} *method1* [*method2...*] **Example:** `Device(config)# aaa authentication login default tacacs+ local`	Creates a login authentication method list. • To create a default list that is used when a named list is *not* specified in the **login authentication** command, use the **default** keyword followed by the methods that are to be used in default situations. The default method list is automatically applied to all ports. • For *list-name*, specify a character string to name the list you are creating. • For *method1...*, specify the actual method the authentication algorithm tries. The additional methods of authentication are used only if the previous method returns an error, not if it fails. Select one of these methods: • *enable*: Use the enable password for authentication. Before you can use this authentication method, you must define an enable password by using the **enable** *password* global configuration command. • *group tacacs+*: Uses TACACS+ authentication. Before you can use this authentication method, you must configure the TACACS+ server. • *line* : Use the line password for authentication. Before you can use this authentication method, you must define a line password. Use the **password** *password* line configuration command. • *local*: Use the local username database for authentication. You must enter username information in the database. Use the **username** *password* global configuration command. • *local-case*: Use a case-sensitive local username database for authentication. You must enter username information in the

	Command or Action	Purpose
		database by using the **username** *name* **password** global configuration command. • *none*: Do not use any authentication for login.
Step 5	**line** [**console** | **tty** | **vty**] *line-number* [*ending-line-number*] **Example:** `Device(config)# line 2 4`	Enters line configuration mode, and configures the lines to which you want to apply the authentication list.
Step 6	**login authentication** {**default** | *list-name*} **Example:** `Device(config-line)# login authentication default`	Applies the authentication list to a line or set of lines. • If you specify **default**, use the default list created with the **aaa authentication login** command. • For *list-name*, specify the list created with the **aaa authentication login** command.
Step 7	**end** **Example:** `Device(config-line)# end`	Exits line configuration mode and returns to privileged EXEC mode.

Configuring TACACS+ Authorization for Privileged EXEC Access and Network Services

You can use the **aaa authorization** global configuration command with the **tacacs+** keyword to set parameters that restrict a user's network access to privileged EXEC mode.

Note Authorization is bypassed for authenticated users who log in through the CLI even if authorization has been configured.

Follow these steps to specify TACACS+ authorization for privileged EXEC access and network services:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**aaa authorization network***authorization-list* **tacacs+** **Example:** `Device(config)# aaa authorization network list1 tacacs+`	Configures the switch for user TACACS+ authorization for all network-related service requests.
Step 4	**aaa authorization exec** *default***tacacs+** **Example:** `Device(config)# aaa authorization exec default tacacs+`	Configures the switch for user TACACS+ authorization if the user has privileged EXEC access. The **exec** keyword might return user profile information (such as **autocommand** information).
Step 5	**end** **Example:** `Device(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.

Starting TACACS+ Accounting

Follow these steps to start TACACS+ Accounting:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**aaa accounting network** *authorization-list* **start-stop tacacs+** **Example:** `Device(config)# aaa accounting network list1 start-stop tacacs+`	Enables TACACS+ accounting for all network-related service requests.
Step 4	**aaa accounting exec** *default* **start-stop tacacs+** **Example:**	Enables TACACS+ accounting to send a start-record accounting notice at the beginning

	Command or Action	Purpose
	`Device(config)# aaa accounting exec default start-stop tacacs+`	of a privileged EXEC process and a stop-record at the end.
Step 5	**end** **Example:** `Device(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.

What to do next

To establish a session with a device if the AAA server is unreachable, use the **aaa accounting system guarantee-first** command. It guarantees system accounting as the first record, which is the default condition. In some situations, users might be prevented from starting a session on the console or terminal connection until after the system reloads, which can take more than 3 minutes.

To establish a console or Telnet session with the router if the AAA server is unreachable when the router reloads, use the **no aaa accounting system guarantee-first** command.

Establishing a Session with a Device if the AAA Server is Unreachable

To establishing a session with a device if the AAA server is unreachable, use the **aaa accounting system guarantee-first** command. It guarantees system accounting as the first record, which is the default condition. In some situations, users might be prevented from starting a session on the console or terminal connection until after the system reloads, which can take more than 3 minutes.

To establish a console or Telnet session with the device if the AAA server is unreachable when the device reloads, use the **no aaa accounting system guarantee-first** command.

Configuring TACACS Source-Interface Under a TACACS Server-Group

The TACACS source-interface can be configured under a TACACS server-group in either of the following methods:

- Configure a TACACS source-interface under the TACACS server-group using the **ip tacacs source-interface** *interface-name* command.
- Configure a VRF using the **vrf** *vrf-name* command under the TACACS server-group, and then associate the configured VRF globally to a source-interface using the **ip tacacs source interface** *interface-name* **vrf** *vrf-name* command.

Priority will be given to the source-interface under the server-group configuration in case both methods are configured.

Either public servers or private servers can be configured under a server-group. We recommend that you configure public servers as described in the Identifying the TACACS+ Server Host and Setting the Authentication Key, on page 6 procedure.

To configure TACACS source-interface under a TACACS server-group, perform the following:

Before you begin

You must configure a VRF routing table and associate VRF to an interface

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	{ **ip** | **ipv6** }**tacacs source-interface** *interface-number* **vrf** *vrf-name* **Example:** `Device(config)# ip tacacs source-interface GigabitEthernet1/0/23 vrf vrf17`	Forces TACACS to use the IP address of a specified interface for all outgoing TACACS packets, and enables the specification on a per-VRF basis. • *interface-name*: Specifies the name of the interface that TACACS+ uses for all of its outgoing packets. • **vrf** *vrf-name*: Specifies the per-VRF configuration.
Step 4	**aaa group server tacacs** *group_name* **Example:** `Device(config-sg-tacacs+)# aa group server tacacs rad-grp`	Groups different TACACS server hosts into distinct lists and distinct methods and enters server-group configuration mode.

Step 5	• **server-private** {*ip-address* | *name*} [**nat**] [**single-connection**] [**port** *port-number*] [**timeout** *seconds*] [**key** [**0** | **7** | **6**] *string*]
	• **server** {*ip-address* | *name*}
	Example:
	`Device(config-sg-tacacs+)# server-private 10.1.1.1 port 19 key cisco`
	Or
	`Device(config-sg-tacacs+)# server 10.11.11.11`
		Configures the IP address of the private TACACS+ server for the group server.
		Or
		Configures the IP address of the public TACACS+ server for the group server. This is the IP address assigned to the TACACS+ server defined in global configuration mode.

Step 6	**ip vrf forwarding** *vrf-name* **Example:** `Device(config-sg-tacacs+)# ip vrf forwarding vrf17`	(Optional) Configures the VRF reference of a AAA TACACS+ server group.
Step 7	{ **ip** | **ipv6** } **tacacs source-interface** *interface-number* **Example:**	(Optional) Forces TACACS+ to use the IP address of a specified interface for all outgoing TACACS packets from the TACACS+ group server.

	Command or Action	Purpose
	`Device(config-sg-tacacs+)# ip tacacs source-interface loopback0`	*interface-name*: Specifies the name of the interface that TACACS uses for all of its outgoing packets.
Step 8	**end** **Example:** `Device(config-sg-tacacs+)# end`	Returns to privileged EXEC mode.

Configuring TACACS+ over TLS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**tacacs server** *tacacs-server-name* **Example:** `Device(config)# tacacs server yourserver`	Configures a TACACS+ server and enters TACACS server configuration mode.

Step 4	**tls** [**connectiontimeout** *connection-timeout-value*] [**idletimeout** *idle-timeout-value*] [[**ip** | **ipv6**] {**tacacs source-interface** *interface-name* |**vrf forwarding** *forwarding-table-name*}] [**match-server-identity** {**dns-id** *dns-id* | **ip-address** *ip-address* | **srv-id** *srv-id*}] [**port** *port-number*] [**retries** *number-of-connection-retries*] [**trustpoint** {**client** *trustpoint name* | **server** *trustpoint name*}]
	Example:
	`Device(config-server-tacacs)# tls connectiontimeout 10`
	`Device(config-server-tacacs)# tls idletimeout 75`
	`Device(config-server-tacacs)# tls ip tacacs source-interface GigabitEthernet 1/0/1`
	`Device(config-server-tacacs)# tls ipv6 vrf forwarding table-1`
		Configures the TLS parameters. You can configure the following parameters:
		• **connectiontimeout**: Configures TLS connection timeout value. The default is 5 seconds.
		• **idletimeout**: Configures the TLS idle timeout value. The default is 60 seconds.
		• **ip**: Configures IP source parameters.
		• **ipv6**: Configures IPv6 source parameters.
		• **match-server-identity**: Configures TLS certification validation parameters.
		Note This is a mandatory configuration.
		• **port**: Configures the TLS port number. The default is 2083.

	Command or Action	Purpose

	`Device(config-server-tacacs)# tls match-server-identity ip-address 10.1.1.10`
	`Device(config-server-tacacs)# tls port 10`
	`Device(config-server-tacacs)# tls retries 15`
	`Device(config-server-tacacs)# tls trustpoint client TP-self-signed-12345`
	`Device(config-server-tacacs)# tls trustpoint server isetp`
		• **retries**: Configures the number of TLS connection retries. The default is 5.
		• **trustpoint**: Configures the TLS trustpoint for a client and a server. If the TLS trustpoint for the client and server are the same, the trustpoint name should also be the same for both.

Step 5	**end** **Example:** `Device(config-server-tacacs)# end`	Exits TACACS server configuration mode and returns to privileged EXEC mode.

Monitoring TACACS+

Table 1: Commands for Displaying TACACS+ Information

Command	Purpose
show tacacs	Displays TACACS+ server statistics.

Additional References for TACACS+

Related Documents

Related Topic	Document Title
AAA configuration	Configuring Authentication, Configuring Authorization, and Configuring Accounting chapters of the *Security Configuration Guide*

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature History for TACACS+

This table provides release and related information for the features explained in this module.

These features are available in all the releases subsequent to the one they were introduced in, unless noted otherwise.

Release	Feature	Feature Information
Cisco IOS XE Everest 16.5.1a	TACACS+	TACACS+ provides detailed accounting information and flexible administrative control over authentication and authorization processes. TACACS+ is facilitated through AAA and can be enabled only through AAA commands. Support for this feature was introduced on the C9500-12Q, C9500-16X, C9500-24Q, C9500-40X models of the Cisco Catalyst 9500 Series Switches.
Cisco IOS XE Fuji 16.8.1a	TACACS+	Support for this feature was introduced on the C9500-24Y4C, C9500-32C, C9500-32QC, and C9500-48Y4C models of the Cisco Catalsyt 9500 Series Switches.
Cisco IOS XE Cupertino 17.7.1	TACACS+	This feature was implemented on the C9500X-28C8D model.
Cisco IOS XE Dublin 17.10.1b	TACACS+	This feature was implemented on the C9500X-60L4D model.
Cisco IOS XE 17.18.1	TACACS+ over TLS	TACACS+ over TLS enhances security and provides stronger certificate-based AAA services.

Use the Cisco Feature Navigator to find information about platform and software image support. To access Cisco Feature Navigator, go to https://cfnng.cisco.com/.