

Controlling Access to the Switch Using Authentication

This chapter describes how to configure TACACS+ and local authentication to control access to the switch command-line interface (CLI).

Note For complete syntax and usage information for the commands used in this chapter, refer to the *Command Reference* for your switch.

This chapter consists of these sections:

- Understanding the Authentication Methods on page 15-1
- Authentication Default Configuration on page 15-3
- Authentication Configuration Guidelines on page 15-3
- Configuring Local Authentication on page 15-4
- Configuring TACACS+ Authentication on page 15-7

Understanding the Authentication Methods

These sections describe how the different authentication methods work:

- Authentication Overview on page 15-1
- Understanding How Local Authentication Works on page 15-2
- Understanding How TACACS+ Authentication Works on page 15-2

Authentication Overview

You can configure either or both of these authentication methods to control access to the switch:

- TACACS+
- Local authentication

When both authentication methods are enabled local authentication is always attempted last. In supervisor engine software release 4.4 and later, you can specify the authentication method to use for console and Telnet connections independently. For example, you might use local authentication for console connections and TACACS+ authentication for Telnet connections.

Understanding How Local Authentication Works

Local authentication uses locally configured login and enable passwords to authenticate login attempts. The login and enable passwords are local to each switch and are not mapped to individual user names.

Local authentication is enabled by default, but can be disabled if TACACS+ authentication is enabled. If local authentication is disabled and you then disable TACACS+ authentication, local authentication is reenabled automatically.

You can enable local authentication and TACACS+ authentication at the same time. Local authentication is only attempted if TACACS+ authentication fail.

Understanding How TACACS+ Authentication Works

TACACS+ controls access to network devices by exchanging Network Access Server (NAS) information between a network device and a centralized database to determine the identity of a user or entity. TACACS+ is an enhanced version of TACACS, a User Datagram Protocol (UDP)-based access-control protocol specified by RFC 1492. TACACS+ uses TCP to ensure reliable delivery and encrypt all traffic between the TACACS+ server and the TACACS+ daemon on a network device.

TACACS+ works with many authentication types, including fixed password, one-time password, and challenge-response authentication. TACACS+ authentication usually occurs in these instances:

- When you first log onto a machine
- When you send a service request that requires privileged access

When you request privileged or restricted services, TACACS+ encrypts your user password information using the MD5 encryption algorithm and adds a TACACS+ packet header. This header information identifies the packet type being sent (for example, an authentication packet), the packet sequence number, the encryption type used, and the total packet length. The TACACS+ protocol then forwards the packet to the TACACS+ server.

A TACACS+ server can provide authentication, authorization, and accounting functions. These services, while all part of TACACS+, are independent of one another, so that a given TACACS+ configuration can use any or all of the three services. On the Catalyst 5000 series switches, only the authentication feature is supported.

When the TACACS+ server receives the packet, it does the following:

- Authenticates the user information and notifies the client that authentication has either passed or failed.
- Notifies the client that authentication will continue and that the client must provide additional information. This challenge-response process can continue through multiple iterations until authentication either passes or fails.

You can configure a TACACS+ key on the client and server. If you configure a key on the switch, it must be the same as the one configured on the TACACS+ servers. The TACACS+ clients and servers use the key to encrypt all TACACS+ packets transmitted. If you do not configure a TACACS+ key, packets are not encrypted.

You can configure the following TACACS+ parameters on the switch:

- Enable or disable TACACS+ authentication to determine if a user has permission to access the switch
- Enable or disable TACACS+ authentication to determine if a user has permission to enter privileged mode
- Specify a key used to encrypt the protocol packets
- Specify the server on which the TACACS+ server daemon resides
- Set the number of login attempts allowed
- Set the timeout interval for server daemon response
- Enable or disable the directed-request option

TACACS+ authentication is disabled by default. You can enable TACACS+ authentication and local authentication at the same time.

If local authentication is disabled and you then disable TACACS+ authentication, local authentication is reenabled automatically.

Authentication Default Configuration

Table 15-1 shows the default authentication configuration.

Table 15-1 Authentication Default Configuration

Feature	Default Value
Local login authentication (console and Telnet)	Enabled
Local enable authentication (console and Telnet)	Enabled
TACACS+ login authentication (console and Telnet)	Disabled
TACACS+ enable authentication (console and Telnet)	Disabled
TACACS+ key	None specified
TACACS+ login attempts	3
TACACS+ server timeout	5 seconds
TACACS+ directed request	Disabled

Authentication Configuration Guidelines

These guidelines apply when configuring authentication on the switch:

- Authentication configuration applies both to console and Telnet connection attempts unless you use the **console** and **telnet** keywords to specify the authentication methods to use for each connection type individually.
- If you configure a TACACS+ key on the switch, make sure you configure an identical key on the TACACS+ server.
- You must specify a TACACS+ server before enabling TACACS+ on the switch.

- If you configure multiple TACACS+ servers, the first server configured is the primary and authentication requests are sent to this server first. You can specify a particular server as primary by using the **primary** keyword.
- TACACS+ supports one privileged mode only (level 1).

Configuring Local Authentication

These sections describe how to configure local authentication on the switch:

- Enabling Local Authentication on page 15-4
- Setting the Login Password on page 15-5
- Setting the Enable Password on page 15-5
- Disabling Local Authentication on page 15-6
- Recovering a Lost Password on page 15-6

Enabling Local Authentication

Note Local login and enable authentication is enabled for both console and Telnet connections by default. You do not need to perform this task unless you want to modify the default configuration or you have disabled local authentication.

To enable local authentication on the switch, perform this task in privileged mode:

Task	Command
Step 1 Enable local login authentication on the switch. Use the console or telnet keywords if you want to enable local authentication only for console port or Telnet connection attempts.	set authentication login local enable [console telnet both]
Step 2 Enable local enable authentication on the switch. Use the console or telnet keywords if you want to enable local authentication only for console port or Telnet connection attempts.	set authentication enable local enable [console telnet both]
Step 3 Verify the local authentication configuration.	show authentication

This example shows how to enable local login and enable authentication for both console and Telnet connections, and how to verify the configuration:

```
Console> (enable) set authentication login local enable
local login authentication set to enable for console and telnet session.
Console> (enable) set authentication enable local enable
local enable authentication set to enable for console and telnet session.
Console> (enable) show authentication
```

```
Login Authentication:  Console Session  Telnet Session
-----
tacacs                disabled      disabled
local                 enabled(primary)  enabled(primary)
```

```

Enable Authentication: Console Session   Telnet Session
-----
tacacs                disabled           disabled
local                 enabled(primary)  enabled(primary)
Console> (enable) show authentication ?

```

Setting the Login Password

The login password controls access to the user mode CLI.

To set the login password for local authentication, perform this task in privileged mode:

Task	Command
Set the login password for access. Enter your old password (press Return on a switch with no password configured), enter your new password, and reenter your new password.	set password

This example shows how to set the login password on the switch:

```

Console> (enable) set password
Enter old password: <old_password>
Enter new password: <new_password>
Retype new password: <new_password>
Password changed.
Console> (enable)

```

Setting the Enable Password

The enable password controls access to the privileged mode CLI.

To set the enable password for local authentication, perform this task in privileged mode:

Task	Command
Set the password for privileged mode. Enter your old password (press Return on a switch with no password configured), enter your new password, and reenter your new password.	set enablepass

This example shows how to set the enable password on the switch:

```

Console> (enable) set enablepass
Enter old password: <old_password>
Enter new password: <new_password>
Retype new password: <new_password>
Password changed.
Console> (enable)

```

Disabling Local Authentication



Caution Make sure that TACACS+ authentication is configured and operating correctly before disabling local login or enable authentication. If you disable local authentication and TACACS+ is not configured correctly, or if the TACACS+ server is not online, you might be unable to log in to the switch.

To disable local authentication on the switch, perform this task in privileged mode:

Task	Command
Step 1 Disable local login authentication on the switch. Use the console or telnet keywords if you want to disable local authentication only for console port or Telnet connection attempts.	set authentication login local disable [console telnet both]
Step 2 Disable local enable authentication on the switch. Use the console or telnet keywords if you want to disable local authentication only for console port or Telnet connection attempts.	set authentication enable local disable [console telnet both]
Step 3 Verify the local authentication configuration.	show authentication

This example shows how to disable local login and enable authentication for both console and Telnet connections, and how to verify the configuration (you must have TACACS+ authentication enabled before you disable local authentication):

```

Console> (enable) set authentication login local disable
local login authentication set to disable for console and telnet session.
Console> (enable) set authentication enable local disable
local enable authentication set to disable for console and telnet session.
Console> (enable) show authentication

Login Authentication: Console Session  Telnet Session
-----
tacacs                enabled(primary)  enabled(primary)
local                 disabled           disabled

Enable Authentication: Console Session  Telnet Session
-----
tacacs                enabled(primary)  enabled(primary)
local                 disabled           disabled
Console> (enable)
    
```

Recovering a Lost Password

To recover a lost local authentication password, perform this task. You must complete steps 3–7 within 30 seconds or the recovery will fail. If you lost both the login and enable passwords, repeat the process for each password.

- Step 1** Connect to the switch through the supervisor engine console port (you cannot recover the password if you are connected through a Telnet connection).
- Step 2** Enter the **reset system** command to reboot the switch.
- Step 3** At the “Enter Password” prompt, press **Return** (the login password is null for 30 seconds when you are connected to the console port).
- Step 4** Enter privileged mode using the **enable** command.

- Step 5** At the “Enter Password” prompt, press **Return** (the enable password is null for 30 seconds when you are connected to the console port).
- Step 6** Enter the **set password** or **set enablepass** command, as appropriate.
- Step 7** When prompted for your old password, press **Return**.
- Step 8** Enter and confirm your new password.

Configuring TACACS+ Authentication

These sections describe how to configure TACACS+ authentication on the switch:

- Specifying TACACS+ Servers on page 15-7
- Enabling TACACS+ Authentication on page 15-8
- Specifying the TACACS+ Key on page 15-9
- Setting the TACACS+ Timeout Interval on page 15-10
- Setting the TACACS+ Login Attempts on page 15-10
- Enabling TACACS+ Directed Request on page 15-11
- Disabling TACACS+ Directed Request on page 15-12
- Clearing TACACS+ Servers on page 15-12
- Clearing the TACACS+ Key on page 15-12
- Disabling TACACS+ Authentication on page 15-13

Specifying TACACS+ Servers

Specify one or more TACACS+ servers before you enable TACACS+ authentication on the switch. The first server you specify is the primary server, unless you explicitly make one server the primary using the **primary** keyword.

To specify one or more TACACS+ servers, perform this task in privileged mode:

Task	Command
Step 1 Specify the IP address of one or more TACACS+ servers.	set tacacs server <i>ip_addr</i> [primary]
Step 2 Verify the TACACS+ configuration.	show tacacs

This example shows how to specify TACACS+ servers and verify the configuration:

```

Console> (enable) set tacacs server 172.20.52.3
172.20.52.3 added to TACACS server table as primary server.
Console> (enable) set tacacs server 172.20.52.7 primary
172.20.52.7 added to TACACS server table as primary server.
Console> (enable) set tacacs server 172.20.52.10
172.20.52.10 added to TACACS server table as backup server.
Console> (enable) show tacacs

Login Authentication:  Console Session  Telnet Session
-----
tacacs                disabled          disabled
local                 enabled(primary) enabled(primary)

```

```

Enable Authentication: Console Session  Telnet Session
-----
tacacs          disabled                disabled
local          enabled(primary)             enabled(primary)
Tacacs key:
Tacacs login attempts: 3
Tacacs timeout: 5 seconds
Tacacs direct request: disabled

Tacacs-Server                                     Status
-----
172.20.52.3
172.20.52.7                                     primary
172.20.52.10
Console> (enable)

```

Enabling TACACS+ Authentication

Note Specify at least one TACACS+ server before enabling TACACS+ authentication on the switch. For information on specifying a TACACS+ server, see the “Specifying TACACS+ Servers” section on page 15-7.

You can enable TACACS+ authentication for login and enable access to the switch. If desired, you can use the **console** and **telnet** keywords to specify that TACACS+ authentication be used only on console or Telnet connections.

To enable TACACS+ authentication, perform this task in privileged mode:

Task	Command
Step 1 Enable TACACS+ authentication for login mode. Use the console or telnet keywords if you want to enable TACACS+ only for console port or Telnet connection attempts.	set authentication login tacacs enable [console telnet both] [primary]
Step 2 Enable TACACS+ authentication for enable mode. Use the console or telnet keywords if you want to enable TACACS+ only for console port or Telnet connection attempts.	set authentication enable tacacs enable [console telnet both] [primary]
Step 3 Verify the TACACS+ configuration.	show tacacs show authentication

This example shows how to enable TACACS+ authentication for console and Telnet connections and how to verify the configuration:

```

Console> (enable) set authentication login tacacs enable
tacacs login authentication set to enable for console and telnet session.
Console> (enable) set authentication enable tacacs enable
tacacs enable authentication set to enable for console and telnet session.
Console> (enable) show authentication

Login Authentication: Console Session  Telnet Session
-----
tacacs          enabled(primary)             enabled(primary)
local          enabled                            enabled

Enable Authentication: Console Session  Telnet Session

```

```

-----
tacacs          enabled(primary)  enabled(primary)
local          enabled             enabled
Console> (enable)

```

This example shows how to enable TACACS+ authentication for Telnet connections only and how to verify the configuration:

```

Console> (enable) set authentication login tacacs enable telnet
tacacs login authentication set to enable for telnet session.
Console> (enable) set authentication enable tacacs enable telnet
tacacs enable authentication set to enable for telnet session.
Console> (enable) show authentication

```

```

Login Authentication: Console Session  Telnet Session
-----
tacacs          disabled             enabled(primary)
local          enabled(primary)  enabled

```

```

Enable Authentication: Console Session  Telnet Session
-----
tacacs          disabled             enabled(primary)
local          enabled(primary)  enabled
Console> (enable)

```

Specifying the TACACS+ Key

Note If you configure a TACACS+ key on the switch, make sure you configure an identical key on the TACACS+ server.

To specify the TACACS+ key, perform this task in privileged mode:

Task	Command
Step 1 Configure the key used to encrypt packets.	set tacacs key <i>key</i>
Step 2 Verify the TACACS+ configuration.	show tacacs

This example shows how to specify the TACACS+ key and verify the configuration:

```

Console> (enable) set tacacs key Secret_String
The tacacs key has been set to Secret_String.
Console> (enable) show tacacs

```

```

Login Authentication: Console Session  Telnet Session
-----
tacacs          enabled(primary)  enabled(primary)
local          enabled             enabled

```

```

Enable Authentication: Console Session  Telnet Session
-----
tacacs          enabled(primary)  enabled(primary)
local          enabled             enabled

```

```

Tacacs key: Secret_String
Tacacs login attempts: 3
Tacacs timeout: 5 seconds
Tacacs direct request: disabled

```

```
Tacacs-Server                               Status
-----
172.20.52.3
172.20.52.7                                primary
172.20.52.10
Console> (enable)
```

Setting the TACACS+ Timeout Interval

You can specify the timeout interval between retransmissions to the TACACS+ server. The default timeout is 5 seconds.

To specify the TACACS+ timeout interval, perform this task in privileged mode:

Task	Command
Step 1 Configure the TACACS+ timeout interval.	set tacacs timeout <i>seconds</i>
Step 2 Verify the TACACS+ configuration.	show tacacs

This example shows how to set the server timeout interval and verify the configuration:

```
Console> (enable) set tacacs timeout 30
Tacacs timeout set to 30 seconds.
Console> (enable) show tacacs

Login Authentication: Console Session Telnet Session
-----
tacacs                enabled(primary) enabled(primary)
local                 enabled           enabled

Enable Authentication: Console Session Telnet Session
-----
tacacs                enabled(primary) enabled(primary)
local                 enabled           enabled

Tacacs key: Secret_String
Tacacs login attempts: 3
Tacacs timeout: 30 seconds
Tacacs direct request: disabled

Tacacs-Server                               Status
-----
172.20.52.3
172.20.52.7                                primary
172.20.52.10
Console> (enable)
```

Setting the TACACS+ Login Attempts

You can specify the number of failed login attempts allowed.

To specify the number of login attempts allowed, perform this task in privileged mode:

Task	Command
Step 1 Configure the number of allowed login attempts.	set tacacs attempts <i>number</i>
Step 2 Verify the TACACS+ configuration.	show tacacs

This example shows how to set the number of login attempts and verify the configuration:

```

Console> (enable) set tacacs attempts 5
Tacacs number of attempts set to 5.
Console> (enable) show tacacs

Login Authentication: Console Session  Telnet Session
-----
tacacs                enabled(primary)  enabled(primary)
local                 enabled            enabled

Enable Authentication: Console Session  Telnet Session
-----
tacacs                enabled(primary)  enabled(primary)
local                 enabled            enabled

Tacacs key: Secret_String
Tacacs login attempts: 5
Tacacs timeout: 30 seconds
Tacacs direct request: disabled

Tacacs-Server                               Status
-----
172.20.52.3
172.20.52.7                                primary
172.20.52.10
Console> (enable)

```

Enabling TACACS+ Directed Request

When TACACS+ directed request is enabled, users must specify the hostname of a configured TACACS+ server (in the form *username@server_hostname*) or the authentication request will fail after the @ sign.

To enable TACACS+ directed request, perform this task in privileged mode:

Task	Command
Step 1 Enable TACACS+ directed request on the switch.	set tacacs directedrequest enable
Step 2 Verify the TACACS+ configuration.	show tacacs

This example shows how to enable TACACS+ directed request and verify the configuration:

```

Console> (enable) set tacacs directedrequest enable
Tacacs direct request has been enabled.
Console> (enable) show tacacs

Login Authentication: Console Session  Telnet Session
-----
tacacs                enabled(primary)  enabled(primary)
local                 enabled            enabled

Enable Authentication: Console Session  Telnet Session
-----
tacacs                enabled(primary)  enabled(primary)
local                 enabled            enabled

Tacacs key: Secret_String
Tacacs login attempts: 5
Tacacs timeout: 30 seconds
Tacacs direct request: enabled

```

```
Tacacs-Server                               Status
-----
172.20.52.3
172.20.52.7                                primary
172.20.52.10
Console> (enable)
```

Disabling TACACS+ Directed Request

To disable TACACS+ directed request, perform this task in privileged mode:

Task	Command
Step 1 Disable TACACS+ directed request on the switch.	set tacacs directedrequest disable
Step 2 Verify the TACACS+ configuration.	show tacacs

This example shows how to disable TACACS+ directed request:

```
Console> (enable) set tacacs directedrequest disable
Tacacs direct request has been disabled.
Console> (enable)
```

Clearing TACACS+ Servers

To clear one or more TACACS+ servers, perform this task in privileged mode:

Task	Command
Step 1 Specify the IP address of the TACACS+ server to clear from the configuration. Use the all keyword to clear all of the servers from the configuration.	clear tacacs server [ip_addr all]
Step 2 Verify the TACACS+ server configuration.	show tacacs

This example shows how to clear a TACACS+ server from the configuration:

```
Console> (enable) clear tacacs server 172.20.52.3
172.20.52.3 cleared from TACACS table
Console> (enable)
```

Clearing the TACACS+ Key

To clear the TACACS+ key, perform this task in privileged mode:

Task	Command
Step 1 Clear the TACACS+ key.	clear tacacs key
Step 2 Verify the TACACS+ configuration.	show tacacs

This example shows how to clear the TACACS+ key:

```
Console> (enable) clear tacacs key
TACACS server key cleared.
Console> (enable)
```

Disabling TACACS+ Authentication

If local authentication is disabled and you disable TACACS+ authentication, local authentication is automatically enabled on the switch.

To disable TACACS+ authentication, perform this task in privileged mode:

Task	Command
Step 1 Disable TACACS+ authentication for login mode. Use the console or telnet keywords if you want to disable TACACS+ only for console port or Telnet connection attempts.	set authentication login tacacs disable [console telnet both]
Step 2 Disable TACACS+ authentication for enable mode. Use the console or telnet keywords if you want to disable TACACS+ only for console port or Telnet connection attempts.	set authentication enable tacacs disable [console telnet both]
Step 3 Verify the TACACS+ configuration.	show tacacs show authentication

This example shows how to disable TACACS+ authentication for console and Telnet connections and how to verify the configuration:

```

Console> (enable) set authentication login tacacs disable
tacacs login authentication set to disable for console and telnet session.
Console> (enable) set authentication enable tacacs disable
tacacs enable authentication set to disable for console and telnet session.
Console> (enable) show authentication

Login Authentication: Console Session  Telnet Session
-----
tacacs                disabled                disabled
local                 enabled(primary)       enabled(primary)

Enable Authentication: Console Session  Telnet Session
-----
tacacs                disabled                disabled
local                 enabled(primary)       enabled(primary)
Console> (enable)

```

