



Passwords and Privileges Commands

This chapter describes the commands used to establish password protection and configure privilege levels. Password protection lets you restrict access to a network or a network device. Privilege levels let you define what commands users can issue after they have logged in to a network device.

For information on how to establish password protection or configure privilege levels, refer to the “Configuring Passwords and Privileges” chapter in the *Security Configuration Guide*. For configuration examples using the commands in this chapter, refer to the “Passwords and Privilege Levels Configuration Examples” section located at the end of the “Configuring Passwords and Privileges” chapter in the *Security Configuration Guide*.

enable

To log on to the router at a specified level, use the **enable** EXEC command.

enable [*level*]

Syntax Description

level (Optional) Defines the privilege level that a user logs in to on the router.

Default

Level 15

Command Mode

EXEC

Usage Guidelines

This command first appeared in Cisco IOS Release 10.0.

Note The enable command is associated with privilege level 0. If you configure AAA authorization for a privilege level greater than 0, this command will not be included in the privilege level command set.

Example

In the following example, the user is logging on to privilege level 5 on a router:

```
enable 5
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

disable

privilege level (global)

privilege level (line)

enable password

To set a local password to control access to various privilege levels, use the **enable password** global configuration command. Use the **no** form of this command to remove the password requirement.

```
enable password [level level] [password | encryption-type encrypted-password]  
no enable password [level level]
```

Syntax Description

level <i>level</i>	(Optional) Level for which the password applies. You can specify up to 16 privilege levels, using numbers 0 through 15. Level 1 is normal EXEC-mode user privileges. If this argument is not specified in the command or the no form of the command, the privilege level defaults to 15 (traditional enable privileges).
<i>password</i>	Password users type to enter enable mode.
<i>encryption-type</i>	(Optional) Cisco-proprietary algorithm used to encrypt the password. Currently the only encryption type available is 7. If you specify <i>encryption-type</i> , the next argument you supply must be an encrypted password (a password already encrypted by a Cisco router).
<i>encrypted-password</i>	Encrypted password you enter, copied from another router configuration.

Default

No password is defined. The default is level 15.

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 10.0.

Use this command with the **level** option to define a password for a specific privilege level. After you specify the level and the password, give the password to the users who need to access this level. Use the **privilege level (global)** configuration command to specify commands accessible at various levels.

You will not ordinarily enter an encryption type. Typically you enter an encryption type only if you copy and paste into this command a password that has already been encrypted by a Cisco router.



Caution If you specify an encryption type and then enter a clear text password, you will not be able to reenter enable mode. You cannot recover a lost password that has been encrypted by any method.

If the **service password-encryption** command is set, the encrypted form of the password you create with the **enable password** command is displayed when a **show startup-config** command is entered.

You can enable or disable password encryption with the **service password-encryption** command.

An enable password is defined as follows:

- Must contain from 1 to 25 uppercase and lowercase alphanumeric characters.
- Must not have a number as the first character.
- Can have leading spaces, but they are ignored. However, intermediate and trailing spaces are recognized.
- Can contain the question mark (?) character if you precede the question mark with the key combination **Ctrl-V** when you create the password; for example, to create the password *abc?123*, do the following:
 - Enter **abc**.
 - Type **Ctrl-V**.
 - Enter **?123**.

When the system prompts you to enter the enable password, you need not precede the question mark with the **Ctrl-V**; you can simply enter **abc?123** at the password prompt.

Examples

In the following example, the password *pswd2* is enabled for privilege level 2:

```
enable password level 2 pswd2
```

In the following example the encrypted password *\$1\$i5Rkls3LoyxzS8t9*, which has been copied from a router configuration file, is set for privilege level 2 using encryption type 7:

```
enable password level 2 7 $1$i5Rkls3LoyxzS8t9
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

disable
enable
enable secret
privilege level (global)
service password-encryption
show privilege
show startup-config

enable secret

To specify an additional layer of security over the **enable password** command, use the **enable secret** global configuration command. Use the **no** form of this command to turn off the enable secret function.

```
enable secret [level level] {password | encryption-type encrypted-password}
no enable secret [level level]
```

Syntax Description

level <i>level</i>	(Optional) Level for which the password applies. You can specify up to sixteen privilege levels, using numbers 0 through 15. Level 1 is normal EXEC-mode user privileges. If this argument is not specified in the command or in the no form of the command, the privilege level defaults to 15 (traditional enable privileges). The same holds true for the no form of the command.
<i>password</i>	Password for users to enter enable mode. This password should be different from the password created with the enable password command.
<i>encryption-type</i>	(Optional) Cisco-proprietary algorithm used to encrypt the password. Currently the only encryption type available for this command is 5. If you specify <i>encryption-type</i> , the next argument you supply must be an encrypted password (a password encrypted by a Cisco router).
<i>encrypted-password</i>	Encrypted password you enter, copied from another router configuration.

Default

No password is defined. The default level is 15.

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.0.

Use this command in conjunction with the **enable password** command to provide an additional layer of security over the enable password. The **enable secret** command provides better security by storing the enable secret password using a non-reversible cryptographic function. The added layer of security encryption provides is useful in environments where the password crosses the network or is stored on a TFTP server.

You will not ordinarily enter an encryption type. Typically you enter an encryption type only if you paste into this command an encrypted password that you copied from a router configuration file.



Caution If you specify an encryption-type and then enter a clear text password, you will not be able to reenter enable mode. You cannot recover a lost password that has been encrypted by any method.

If you use the same password for the **enable password** and **enable secret** commands, you receive an error message warning that this practice is not recommended, but the password will be accepted. By using the same password, however, you undermine the additional security the **enable secret** command provides.

Note After you set a password using **enable secret** command, a password set using the **enable password** command works only if the **enable secret** is disabled or an older version of Cisco IOS software is being used, such as when running an older rxboot image. Additionally, you cannot recover a lost password that has been encrypted by any method.

If **service password-encryption** is set, the encrypted form of the password you create here is displayed when a **show startup-config** command is entered.

You can enable or disable password encryption with the **service password-encryption** command.

An enable password is defined as follows:

- Must contain from 1 to 25 uppercase and lowercase alphanumeric characters
- Must not have a number as the first character
- Can have leading spaces, but they are ignored. However, intermediate and trailing spaces are recognized.
- Can contain the question mark (?) character if you precede the question mark with the key combination **Ctrl-V** when you create the password; for example, to create the password *abc?123*, do the following:
 - Enter **abc**.
 - Type **Ctrl-V**.
 - Enter **?123**.

When the system prompts you to enter the enable password, you need not precede the question mark with the **Ctrl-V**; you can simply enter **abc?123** at the password prompt.

Examples

The following example specifies the enable secret password of gobbledegook:

```
enable secret gobbledegook
```

After specifying an enable secret password, users must enter this password to gain access. Any passwords set through enable password will no longer work.

```
Password: gobbledegook
```

In the following example the encrypted password `1FaD0$Xyti5Rkls3LoyxzS8`, which has been copied from a router configuration file, is enabled for privilege level 2 using encryption type 5:

```
enable password level 2 5 $1$FaD0$Xyti5Rkls3LoyxzS8
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

enable

enable password

ip identd

To enable identification support, use the **ip identd** global configuration command. Use the **no** form of this command to disable this feature.

ip identd
no ip identd

Syntax Description

This command has no arguments or keywords.

Default

Identification support is not enabled.

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.1.

The **ip identd** command returns accurate information about the host TCP port; however, no attempt is made to protect against unauthorized queries.

Example

In the following example, identification support is enabled:

```
ip identd
```


password

To specify a password on a line, use the **password** line configuration command. Use the **no** form of this command to remove the password.

password *password*
no password

Syntax Description

password Character string that specifies the line password. The first character cannot be a number. The string can contain any alphanumeric characters, including spaces, up to 80 characters. You cannot specify the *password* in the format *number-space-anything*. The space after the number causes problems. For example, *hello 21* is a legal password, but *21 hello* is not. The password checking is case sensitive. For example, the password *Secret* is different than the password *secret*.

Default

No password is specified.

Command Mode

Line configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 10.0.

When an EXEC process is started on a line with password protection, the EXEC prompts for the password. If the user enters the correct password, the EXEC prints its normal privileged prompt. The user can try three times to enter a password before the EXEC exits and returns the terminal to the idle state.

Example

The following example removes the password from virtual terminal lines 1 to 4:

```
line vty 1 4
no password
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

enable password

privilege level (global)

To set the privilege level for a command, use the **privilege level** global configuration command. Use the **no** form of this command to revert to default privileges for a given command.

```
privilege mode level level command
no privilege mode level level command
```

Syntax Description

<i>mode</i>	Configuration mode. See Table 23 for a list of options for this argument.
<i>level</i>	Privilege level associated with the specified command. You can specify up to sixteen privilege levels, using numbers 0 through 15.
<i>command</i>	Command to which privilege level is associated.

Table 23 shows the acceptable options for the mode argument in the **privilege level** command.

Table 23 Mode Argument Options

Argument Options	Mode
configuration	Global configuration
controller	Controller configuration
exec	EXEC
hub	Hub configuration
interface	Interface configuration
ipx-router	IPX router configuration
line	Line configuration
map-class	Map class configuration
map-list	Map list configuration
route-map	Route map configuration
router	Router configuration

Defaults

Level 15 is the level of access permitted by the **enable** password.
Level 1 is normal EXEC-mode user privileges.

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 10.3.

The password for a privilege level defined using the **privilege level** global configuration command is configured using the **enable password** command.

Level 0 can be used to specify a more-limited subset of commands for specific users or lines. For example, you can allow user “guest” to use only the **show users** and **exit** commands.

Note There are five commands associated with privilege level 0: **disable**, **enable**, **exit**, **help**, and **logout**. If you configure AAA authorization for a privilege level greater than 0, these five commands will not be included.

When you set a command to a privilege level, all commands whose syntax is a subset of that command are also set to that level. For example, if you set the **show ip route** command to level 15, the **show** commands and **show ip** commands are automatically set to privilege level 15—unless you set them individually to different levels.

Example

The commands in the following example set the **configure** command to privilege level 14 and establish SecretPswd14 as the password users must enter to use level 14 commands.

```
privilege exec level 14 configure
enable secret level 14 SecretPswd14
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

enable password

enable secret

privilege level (line)

privilege level (line)

To set the default privilege level for a line, use the **privilege level** line configuration command. Use the **no** form of this command to restore the default user privilege level to the line.

privilege level *level*
no privilege level

Syntax Description

level Privilege level associated with the specified line.

Defaults

Level 15 is the level of access permitted by the enable password.

Level 1 is normal EXEC-mode user privileges.

Command Mode

Line configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 10.3.

Users can override the privilege level you set using this command by logging in to the line and enabling a different privilege level. They can lower the privilege level by using the **disable** command. If users know the password to a higher privilege level, they can use that password to enable the higher privilege level.

You can use level 0 to specify a subset of commands for specific users or lines. For example, you can allow user “guest” to use only the **show users** and **exit** commands.

You might specify a high level of privilege for your console line to restrict who uses the line.

Examples

The commands in the following example configure the auxiliary line for privilege level 5. Anyone using the auxiliary line has privilege level 5 by default.

```
line aux 0
  privilege level 5
```

The command in the following example sets all **show ip** commands, which includes all **show** commands, to privilege level 7:

```
privilege exec level 7 show ip route
```

This is equivalent to the following command:

```
privilege exec level 7 show
```

The commands in the following example set **show ip route** to level 7 and the **show** and **show ip** commands to level 1:

```
privilege exec level 7 show ip route
privilege exec level 1 show ip
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

enable password

privilege level (line)

service password-encryption

To encrypt passwords, use the **service password-encryption** global configuration command. Use the **no** form of this command to disable this service.

service password-encryption
no service password-encryption

Syntax Description

This command has no arguments or keywords.

Default

No encryption

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 10.0.

The actual encryption process occurs when the current configuration is written or when a password is configured. Password encryption is applied to all passwords, including username passwords, authentication key passwords, the privileged command password, console and virtual terminal line access passwords, and BGP neighbor passwords. This command is primarily useful for keeping unauthorized individuals from viewing your password in your configuration file.

When password encryption is enabled, the encrypted form of the passwords is displayed when a **show running-config** command is entered.



Caution This command does not provide a high level of network security. If you use this command, you should also take additional network security measures.

Note You cannot recover a lost encrypted password. You must clear NVRAM and set a new password.

Example

The following example causes password encryption to take place:

```
service password-encryption
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

enable password
key-string
neighbor password

show privilege

To display your current level of privilege, use the **show privilege** EXEC command.

show privilege

Syntax Description

This command has no arguments or keywords.

Command Mode

EXEC

Usage Guidelines

This command first appeared in Cisco IOS Release 10.3.

Sample Display

The following is sample output from the **show privilege** command. The current privilege level is 15.

```
Router# show privilege
Current privilege level is 15
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

enable password

enable secret

username

To establish a username-based authentication system, enter the **username** global configuration command.

```
username name { nopassword | password password | password encryption-type
encrypted-password }
username name password secret
username name [access-class number]
username name [autocommand command]
username name [callback-dialstring telephone-number]
username name [callback-rotary rotary-group-number]
username name [callback-line [tty] line-number [ending-line-number]]
username name [nocallback-verify]
username name [noescape] [nohangup]
username name [privilege level]
```

Syntax Description

<i>name</i>	Host name, server name, user ID, or command name. The <i>name</i> argument can be only one word. White spaces and quotation marks are not allowed.
nopassword	No password is required for this user to log in. This is usually most useful in combination with the autocommand keyword.
password	Specifies a possibly encrypted password for this username.
<i>password</i>	Password a user enters.
<i>encryption-type</i>	(Optional) Single-digit number that defines whether the text immediately following is encrypted, and, if so, what type of encryption is used. Currently defined encryption types are 0, which means that the text immediately following is not encrypted, and 7, which means that the text is encrypted using a Cisco-defined encryption algorithm.
<i>encrypted-password</i>	Encrypted password a user enters.
password	(Optional) Password to access the name argument. A password must be from 1 to 25 characters, can contain embedded spaces, and must be the last option specified in the username command.
<i>secret</i>	For CHAP authentication: specifies the secret for the local router or the remote device. The secret is encrypted when it is stored on the local router. The secret can consist of any string of up to 11 ASCII characters. There is no limit to the number of username and password combinations that can be specified, allowing any number of remote devices to be authenticated.
access-class	(Optional) Specifies an outgoing access list that overrides the access list specified in the access-class line configuration command. It is used for the duration of the user's session.
<i>number</i>	Access list number.

autocommand	(Optional) Causes the specified command to be issued automatically after the user logs in. When the command is complete, the session is terminated. Because the command can be any length and contain embedded spaces, commands using the autocommand keyword must be the last option on the line.
<i>command</i>	The command string. Because the command can be any length and contain embedded spaces, commands using the autocommand keyword must be the last option on the line.
callback-dialstring	(Optional) For asynchronous callback only: permits you to specify a telephone number to pass to the DCE device.
<i>telephone-number</i>	For asynchronous callback only: telephone number to pass to the DCE device.
callback-rotary	(Optional) For asynchronous callback only: permits you to specify a rotary group number. The next available line in the rotary group is selected.
<i>rotary-group-number</i>	For asynchronous callback only: integer between 1 and 100 that identifies the group of lines on which you want to enable a specific username for callback.
callback-line	(Optional) For asynchronous callback only: specific line on which you enable a specific username for callback.
tty	(Optional) For asynchronous callback only: standard asynchronous line.
<i>line-number</i>	For asynchronous callback only: relative number of the terminal line (or the first line in a contiguous group) on which you want to enable a specific username for callback. Numbering begins with zero.
<i>ending-line-number</i>	(Optional) Relative number of the last line in a contiguous group on which you want to enable a specific username for callback. If you omit the keyword (such as tty), then <i>line-number</i> and <i>ending-line-number</i> are absolute rather than relative line numbers.
nocallback-verify	(Optional) Authentication not required for EXEC callback on the specified line.
noescape	(Optional) Prevents a user from using an escape character on the host to which that user is connected.
nohangup	(Optional) Prevents Cisco IOS from disconnecting the user after an automatic command (set up with the autocommand keyword) has completed. Instead, the user gets another EXEC prompt.
privilege	(Optional) Sets the privilege level for the user.
<i>level</i>	(Optional) Number between 0 and 15 that specifies the privilege level for the user.

Default

No username-based authentication system is established.

Command Mode

Global configuration

Usage Guidelines

The following commands first appeared in Cisco IOS Release 10.0:

username *name* {**nopassword** | **password** *password* | **password** *encryption-type* *encrypted-password*}

username *name* **password** *secret*

username *name* [**access-class** *number*]

username *name* [**autocommand** *command*]

username *name* [**noescape**] [**nohangup**]

username *name* [*privilege level*]

The following commands first appeared in Cisco IOS Release 11.1:

username *name* [**callback-dialstring** *telephone-number*]

username *name* [**callback-rotary** *rotary-group-number*]

username *name* [**callback-line** [**tty**] *line-number* [*ending-line-number*]]

username *name* [**nocallback-verify**]

The **username** command provides username and/or password authentication for login purposes only. (Note that it does not provide username and/or password authentication for enable mode when the **enable use-tacacs** command is also configured.)

Multiple **username** commands can be used to specify options for a single user.

Add a **username** entry for each remote system that the local router communicates with and requires authentication from. The remote device must have a **username** entry for the local router. This entry must have the same password as the local router's entry for that remote device.

This command can be useful for defining usernames that get special treatment. For example, you can use this command to define an "info" username that does not require a password, but connects the user to a general purpose information service.

The **username** command is required as part of the configuration for the Challenge Handshake Authentication Protocol (CHAP). Add a **username** entry for each remote system from which the local router requires authentication.

Note To enable the local router to respond to remote CHAP challenges, one **username** *name* entry must be the same as the **hostname** entry that has already been assigned to the other router.

If there is no *secret* specified and the **debug serial-interface** command is enabled, an error is displayed when a link is established and the CHAP challenge is not implemented. CHAP debugging information is available using the **debug ppp negotiation**, **debug serial-interface**, and **debug serial-packet** commands. For more information about **debug** commands, refer to the *Debug Command Reference*.

Examples

To implement a service similar to the UNIX **who** command, which can be entered at the login prompt and lists the current users of the router, the **username** command takes the following form:

```
username who nopassword nohangup autocommand show users
```

To implement an information service that does not require a password to be used, the command takes the following form:

```
username info nopassword noescape autocommand telnet nic.ddn.mil
```

To implement an ID that works even if the TACACS servers all break, the command takes the following form:

```
username superuser password superpassword
```

The following example enables CHAP on interface serial 0 of “server_1.” It also defines a password for a remote server named “server_r”.

```
hostname server_1
username server_r password their system
interface serial 0
 encapsulation ppp
 ppp authentication chap
```

When you look at your configuration file, the password will be encrypted and the display will look similar to the following:

```
hostname server_1
username server_r password 7 02120C5E02144F32555D1D1c08
interface serial 0
 encapsulation ppp
 ppp authentication chap
```

The username command is required as part of the configuration file for CHAP. Add a username entry for each remote system from which the local router requires authentication.

Related Commands

You can use the master indexes or search online to find documentation of related commands.

arap callback
callback-forced-wait
ppp callback

username
