E

enable password

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

enable password [**level** *level*] {*password*| [*encryption-type*] *encrypted-password*}

no enable password [**level** *level*]

Syntax Description

level *level*	(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).
password	Password users type to enter enable mode.
encryption-type	(Optional) Cisco-proprietary algorithm used to encrypt the password. Currently the only encryption type available is 5. If you specify *encryption-type*, the next argument you supply must be an encrypted password (a password already encrypted by a Cisco router).
encrypted-password	Encrypted password you enter, copied from another router configuration.

Command Default

No password is defined. The default is level 15.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelin

Caution If neither the enable password command nor the enable secret command is configured, and if there is a line password configured for the console, the console line password will serve as the enable password for all VTY (Telnet and Secure Shell [SSH]) sessions.

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** 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 **more nvram: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.
- 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 combinationCrtl-v when you create the password; for example, to create the password *abc?123,* do the following:
  - Enter **abc**.
  - Type **Crtl-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 enables the password " pswd2" for privilege level 2:

```
enable password level 2 pswd2
```

The following example sets the encrypted password "1i5Rkls3LoyxzS8t9", which has been copied from a router configuration file, for privilege level 2 using encryption type 7:

```
enable password level 2 5 $1$i5Rkls3LoyxzS8t9
```

Related Commands

Command	Description
disable	Exits privileged EXEC mode and returns to user EXEC mode.
enable	Enters privileged EXEC mode.
enable secret	Specifies an additional layer of security over the **enable password** command.
privilege	Configures a new privilege level for users and associate commands with that privilege level.
service password-encryption	Encrypts passwords.
show privilege	Displays your current level of privilege.

enable secret

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

enable secret [**level** *level*] {**[0]** *unencrypted-password*| *encryption-type encrypted-password*}

no enable secret [**level** *level*] [*encryption-type encrypted-password*]

Syntax Description

level *level*	(Optional) Specifies the level for which the password applies. You can specify up to 15 privilege levels, using numerals 1 through 15. Level 1 is normal EXEC-mode user privileges. If the *level* argument is not specified in the command or in the **no** form of the command, the privilege level defaults to 15 (traditional enable privileges).
0	(Optional) Specifies an unencrypted clear-text password. The password is converted to a Secure Hash Algorithm (SHA) 256 secret and gets stored in the router.
unencrypted-password	Password for users to enter enable mode. This password should be different from the password created with the **enable password** command.
encryption-type	Cisco-proprietary algorithm used to hash the password. The algorithm types available for this command are **4** and **5**. • **4—**Specifies an SHA-256 encrypted secret string. The SHA256 secret string is copied from the router configuration. **Note** Effective with CSCue95644, the **4** keyword is deprecated. • **5—**Specifies a message digest algorithm 5 (MD5) encrypted secret. • **8—**Specifies a Password-Based Key Derivation Function 2 (PBKDF2) with SHA-256 hashed secret. • **9—**Specifies a scrypt hashed secret.
encrypted-password	Hashed password that is copied from another router configuration.

Command Default No password is defined.

Command Modes Global configuration (config)

Command History

Release	Modification
11.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.0(1)S	This command was integrated into Cisco IOS Release 15.0(1)S. Support for the type **4** algorithm was added.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S. Support for the type **4** algorithm was added.
15.1(4)M	This command was modified. Support for the type **4** algorithm was added.
Cisco IOS Release 3.3SG	This command was modified. Support for the encryption type **5** was removed.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.
Cisco IOS XE Release 3.8S	This command was modified. The warning message for removal of support for the type **5** algorithm was modified.
15.3(3)M	This command was modified. • The **4** keyword was deprecated and support for type **8** and type **9** algorithms were added. • The warning message for the type **5** algorithm was removed. • The warning message for removal of support for the type **4** algorithm was added.
15.3(3)S	The command modifications were integrated into Cisco IOS Release 15.3(3)S.

Usage Guidelin

Caution If neither the **enable password** command or the **enable secret** command is configured, and if a line password is configured for the console, the console line password will serve as the enable password for all vty (Telnet and Secure Shell [SSH]) sessions.

Use the **enable secret** 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 nonreversible 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.

Typically you enter an encryption type only when you paste an encrypted password that you copied from a router configuration file into this command.

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 the **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 the **service password-encryption** command is set, the encrypted form of the password you create is displayed when the **more nvram: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 1 to 25 alphanumeric characters, both uppercase and lowercase.
- 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 combinationCrtl-v when you create the password; for example, to create the password *abc?123,* do the following:
  - Enter **abc**.
  - Press **Crtl-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 enter **abc?123** at the password prompt.

Note During a downgrade from Cisco IOS XE Release 3.3SG to Cisco IOS XE Release 3.2SG, if a SHA256-encrypted enable password is configured, then the SHA256-encrypted password will be lost without any warning, and the secret password will have to be reconfigured.

With CSCue95644, you can use the **enable secret** command to hash the enable secret password with MD5, PBKDF2 with SHA-256, or scrypt hashing algorithms.

Note If you use type 8 or type 9 passwords and then downgrade to an older version of Cisco IOS software that does not support type 8 and type 9 passwords, you must reconfigure the passwords to use type 5 hashing before downgrading. If not, you are locked out of the device and password recovery is required. If you are using an external AAA server to manage privilege levels, you are not locked out of the device.

Examples

The following example shows how to specify the password with the **enable secret** command:

```
Device> enable
Device# configure terminal
Device(config)# enable secret password
```

After specifying a password with the **enable secret** command, users must enter this password to gain access. Any passwords set through **enable password** command will no longer work.

```
Password: password
```

The following example shows how to enable the encrypted password "1FaD0$Xyti5Rkls3LoyxzS8", which has been copied from a router configuration file, for privilege level 2 using the encryption type 4:

```
Device> enable
Device# configure terminal
Device(config)# enable password level 2 4 $1$FaD0$Xyti5Rkls3LoyxzS8
```

The following example shows the sample warning message that is displayed when a user enters the **enable secret 4** *encrypted-password* command:

```
Device# configure terminal
Device(config)# enable secret 4 tnhtc92DXBhelxjYk8LWJrPV36S2i4ntXrpb4RFmfqY

WARNING: Command has been added to the configuration but Type 4 passwords have been
deprecated.
Migrate to a supported password type

Device(config)# end
Device# show running-config | inc secret

enable secret 4 tnhtc92DXBhelxjYk8LWJrPV36S2i4ntXrpb4RFmfqY
```

Related Commands

Command	Description
enable	Enters privileged EXEC mode.
enable algorithm-type	Sets the algorithm type to hash a user password configured using the **enable secret** command.
enable password	Sets a local password to control access to various privilege levels.
more nvram:startup-config	Displays the startup configuration file contained in NVRAM or specified by the CONFIG_FILE environment variable.

Command	Description
service password-encryption	Encrypt passwords.

enrollment http-proxy

To access the certification authority (CA) by HTTP through the proxy server, use the **enrollment http-proxy** command in ca-trustpoint configuration mode.

enrollment http-proxy *host-name port-num*

Syntax Description

host-name	Defines the proxy server used to get the CA.
port-num	Specifies the port number used to access the CA.

Command Default

If this command is not enabled, the CA will not be accessed via HTTP.

Command Modes

Ca-trustpoint configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SXD.

Usage Guidelines

The **enrollment http-proxy** command must be used in conjunction with the **enrollment** command, which specifies the enrollment parameters for the CA.

Examples

The following example shows how to access the CA named “ka” by HTTP through the bomborra proxy server:

```
crypto ca trustpoint ka
 enrollment url http://kahului
 enrollment http-proxy bomborra 8080
 crl optional
```

Related Commands

Command	Description
crypto ca trustpoint	Declares the CA that your router should use.
enrollment	Specifies the enrollment parameters of your CA.

enrollment url (ca-profile-enroll)

To specify the URL of the certification authority (CA) server to which to send enrollment requests, use the **enrollment url** command in ca-profile-enroll configuration mode. To delete the enrollment URL from your enrollment profile, use the **no** form of this command.

enrollment url *url*[**vrf** *vrf-name*]

no enrollment url *url*[**vrf** *vrf-name*]

Syntax Description

url	URL of the CA server to which your router should send certificate requests.
vrf *vrf-name*	The VRF name.

Command Default

Your router does not recognize the CA URL until you specify it using this command.

Command Modes

Ca-profile-enroll configuration (ca-profile-enroll)#

Command History

Release	Modification
12.2(13)ZH	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
15.1(4)T	This command was modified. The **vrf** *vrf-name* keyword-argument pair was added.

Usage Guidelines

This command allows the user to specify a different URL or a different method for authenticating a certificate and enrolling a certificate; for example, manual authentication and TFTP enrollment.

Note the following when specifying the *url* argument:

- If you are using Simple Certificate Enrollment Protocol (SCEP) for enrollment, the value must be in the form http://CA_name, where CA_name is the host Domain Name System (DNS) name or IP address of the CA.
- If you are using TFTP for enrollment, the value must be in the form tftp://certserver/file_specification. (If the URL does not include a file specification, the fully qualified domain name [FQDN] of the router will be used.)

Examples

The following example shows how to enable certificate enrollment via HTTP for the profile name “E”:

```
crypto pki trustpoint Entrust
  enrollment profile E
  serial
crypto pki profile enrollment E
 authentication url  http://entrust:81
 authentication command  GET /certs/cacert.der
 enrollment url  http://entrust:81/cda-cgi/clientcgi.exe
 enrollment command  POST reference_number=$P2&authcode=$P1
&retrievedAs=rawDER&action=getServerCert&pkcs10Request=$REQ
 parameter 1 value aaaa-bbbb-cccc
 parameter 2 value 5001
```

The following example shows how to configure the enrollment and certificate revocation list (CRL) via the same VRF:

```
crypto pki trustpoint trustpoint1
 enrollment url http://10.10.10.10:80
 vrf vrf1
 revocation-check crl
```

The following example shows how to configure the enrollment and certificate revocation list (CRL) via different VRF:

```
crypto pki profile enrollment pki_profile
 enrollment url  http://10.10.10.10:80  vrf vrf2

crypto pki trustpoint trustpoint1
 enrollment profile pki_profile
 vrf vrf1
 revocation-check crl
```

Related Commands

Command	Description
crypto pki profile enrollment	Defines an enrollment profile.