



Enhanced Password Security

Feature History

12.0(18)S	This feature was introduced.
12.1(8a)E	This feature was integrated into Cisco IOS Release 12.1(8a)E.
12.2(8)T	This feature was integrated in Cisco IOS Release 12.2(8)T.

This document describes the Enhanced Password Security feature in Cisco IOS Release 12.2(8)T. It includes the following sections:

- [Feature Overview, page 1](#)
- [Supported Platforms, page 2](#)
- [Supported Standards, MIBs, and RFCs, page 4](#)
- [Configuration Tasks, page 4](#)
- [Configuration Examples, page 5](#)
- [Command Reference, page 6](#)

Feature Overview

The Enhanced Password Security feature allows you to configure Message Digest 5 (MD5) encryption for username passwords. Before the introduction of this feature, two types of passwords were associated with usernames: Type 0, which is a clear text password visible to any user who has access to privileged mode on the router, and type 7, that has a password with a weak, exclusive or type encryption. Type 7 passwords can be retrieved from the encrypted text by using publicly available tools.

MD5 encryption is a one-way hash function that makes reversal of an encrypted password impossible, providing strong encryption protection. Using MD5 encryption, you cannot retrieve clear text passwords. Thus, MD5 encrypted passwords cannot be used with protocols that require the clear text password to be retrievable, such as Challenge Handshake Authentication Protocol (CHAP).

Use the **username secret** command to configure a username and an associated MD5-encrypted secret.

Benefits

The Enhanced Password Security feature allows you to configure a strong method of encryption for user passwords.

Restrictions

- Protocols that require the retrieval of clear text passwords, such as CHAP, cannot be used with MD5-encrypted passwords.
- You can specify a username password or a username secret, but not both.

Related Features and Technologies

To establish a username-based authentication system, use the **username** command in global configuration mode. For more information, refer to the chapter “Passwords and Privileges Commands” in the *Cisco IOS Security Command Reference*, Release 12.2.

Related Documents

- *Cisco IOS Security Configuration Guide*, Release 12.2
- *Cisco IOS Security Command Reference*, Release 12.2
- *Improving Security on Cisco Routers*

Supported Platforms

Cisco IOS Releases 12.0(18)S, 12.2(8a)E, and 12.2(8)T

- Cisco 7100 series
- Cisco 7200 series
- Cisco 7500 series

Cisco IOS Release 12.1(8a)E Only

- Cisco 7600 OSR
- Catalyst 6000



Note This feature is supported only on the c6msfc2 and c6msfc images that go into the Catalyst 6000.

Cisco IOS Release 12.2(8)T Only

- Cisco 800 series
- Cisco 805
- Cisco 806
- Cisco 820
- Cisco 828
- Cisco 1400 series
- Cisco 1600 series

- Cisco 1710
- Cisco 1720
- Cisco 1721
- Cisco 1750
- Cisco 1751
- Cisco 2420
- Cisco 2600 series
- Cisco 3620
- Cisco 3631
- Cisco 3640
- Cisco 3660
- Cisco 3725
- Cisco 3745
- Cisco 7700 series
- Cisco CVA120
- Cisco MC3810
- Cisco SOHO78
- Cisco uBR7200 series
- Universal Route Module (URM)
- Cisco VG200

Determining Platform Support Through Cisco Feature Navigator

Cisco IOS software is packaged in feature sets that support specific platforms. To get updated information regarding platform support for this feature, access Cisco Feature Navigator. Cisco Feature Navigator dynamically updates the list of supported platforms as new platform support is added for the feature.

Cisco Feature Navigator is a web-based tool that enables you to quickly determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image. You can search by feature or release. Under the release section, you can compare releases side by side to display both the features unique to each software release and the features in common.

To access Cisco Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions at <http://www.cisco.com/register>.

Cisco Feature Navigator is updated regularly when major Cisco IOS software releases and technology releases occur. For the most current information, go to the Cisco Feature Navigator home page at the following URL:

<http://www.cisco.com/go/fn>

Supported Standards, MIBs, and RFCs

Standards

None

MIBs

None

To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

RFCs

None

Configuration Tasks

See the following sections for configuration tasks for the Enhanced Password Security feature. Each task in the list is identified as either required or optional.

- [Configuring Enhanced Security Password](#) (required)
- [Verifying MD5 Password Encryption](#) (optional)

Configuring Enhanced Security Password

To configure a username and an associated MD5-encrypted secret, use the following command in global configuration mode:

Command	Purpose
Router(config)# username name secret {0 password 5 encrypted-secret}	Encrypts a username with MD5 encryption. 0 enables MD5 encryption on a clear text password. 5 configures a username and enters an MD5-encrypted text string, which is stored as the MD5-encrypted password for the specified username.

Verifying MD5 Password Encryption

To verify that MD5 password encryption has been enabled, use the **show running-config** command. If the “username name secret 5” line appears in the command output, enhanced password security is enabled.

Follow the steps below to verify MD5 encryption on a username password:

-
- Step 1** Configure an encrypted MD5 username password in global configuration mode.
 - Step 2** Exit global configuration mode and enter the **login local** command.
 - Step 3** Verify that a valid user is able to log in through the console.
-

Configuration Examples

This section provides the following configuration examples:

- [Configuring MD5 Encryption on a Clear Text Password Example](#)
- [Configuring MD5 Encryption on a MD5 Encrypted Text String Example](#)

Configuring MD5 Encryption on a Clear Text Password Example

The following example shows how to configure username “abc” with the MD5 encrypted password “xyz”. Output from the **show running-config** command confirms that the MD5 encrypted password has been configured. Note that the password itself is not displayed.

```
Router(config)# username abc secret 0 xyz
Router(config)# exit
Router# show running-config
!
version 12.1
no service single-slot-reload-enable
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname CE
!
logging rate-limit console 10 except errors
no logging console
enable secret 0 $1$53Ew$Dp8.E4JGpg7rKxQa49BF9/
!
username abc secret 5 $1$fBYK$rH5/OChyx/      !--Note that password 'xyz' is not displayed.
ip subnet-zero
.
.
.
```

Configuring MD5 Encryption on a MD5 Encrypted Text String Example

The following example shows how to configure username “cde” and enter an MD5 encryption text string as the user password. Output from the **show running-config** command confirms that the MD5 encrypted password has been configured. Note that the password itself is not displayed.

```
Router(config)# username cde secret 5 $1$feb0$a104Qd9UZ./Ak00KTggPD0
Router(config)# exit
Router# show running-config
!
version 12.1
no service single-slot-reload-enable
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname CE
!
logging rate-limit console 10 except errors
no logging console
enable secret 5 $1$feb0$a104Qd9UZ./Ak00KTggPD0
!
username cde secret 5
!
ip subnet-zero
.
.
.
```

Command Reference

This section documents the new command that configures the Enhanced Password Security feature. All other commands used with this feature are documented in the Cisco IOS Release 12.2 command reference publications.

- [username secret](#)

username secret

To encrypt a user password with Message Digest 5 (MD5) encryption, use the **username secret** command in global configuration mode.

```
username name secret {[0] password | 5 encrypted-secret}
```

Syntax Description		
	<i>name</i>	Specifies the username.
	0	(Optional) Specifies a clear text password, which will be MD5 encrypted.
	<i>password</i>	Clear text password.
	5 <i>encrypted-secret</i>	Specifies an MD5-encrypted text string, which will be stored as the encrypted user password.

Defaults No default behavior or values.

Command Modes Global configuration

Command History	Release	Modification
	12.0(18)S	This command was introduced.
	12.1(8a)E	This command was integrated into Cisco IOS Release 12.1(8a)E.
	12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.

Usage Guidelines Use the **username secret** command to configure a username and MD5-encrypted user password. The optional **0** keyword enables MD5 encryption on a clear text password; the **5** keyword enters an MD5 encryption string and saves it as the user MD5-encrypted secret. MD5 encryption is a strong encryption method which is not retrievable; thus, you cannot use MD5 encryption with protocols that require clear text passwords, such as CHAP.

The **username secret** command provides an additional layer of security over the username password. It also provides better security by encrypting the password using nonreversible MD5 encryption and storing the encrypted text. The added layer of MD5 encryption is useful in environments in which the password crosses the network or is stored on a TFTP server.

Use MD5 as the encryption type if you paste into this command an encrypted password that you copied from a router configuration file.

Examples The following example shows how to configure username “abc” and enable MD5 encryption on the clear text password “xyz”:

```
username abc secret xyz
```

The following example shows how to configure username “cde” and enter an MD5 encrypted text string that is stored as the username password:

```
username cde secret 5 $1$feb0$a104Qd9UZ./Ak00KTggPD0
```

Related Commands

Command	Description
enable password	Sets a local password to control access to various privilege levels.
enable secret	Specifies an additional layer of security over the enable password command.
username	Establishes a username-based authentication system.