# Enhanced Password Security - Phase I

**Feature History**

| | |
|---|---|
| 12.0(18)S | This feature was introduced. |

This document describes the Enhanced Password Security feature in Cisco IOS Release 12.0(18)S. It includes the following sections:

## Feature Overview

Using the Enhanced Password Security feature, you can configure MD5 encryption for username passwords. Before the introduction of this feature there were two types of passwords associated with usernames. Type 0 is a clear text password visible to any user who has access to privileged mode on the router. Type 7 is 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. MD5 encrypted passwords cannot be used with protocols that require that the clear text password be retrievable, such as Challenge Handshake Authentication Protocol (CHAP).

Use the **username (secret)** command to configure a user name and an associated MD5 encrypted secret.

### Benefits

Enhanced Password Security provides a strong method of encryption for user passwords.

# Restrictions

- Protocols which 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. See *Passwords and Privileges Commands* for more details.

# Related Documents

- *Cisco IOS Release 12.0 Security Configuration Guide*

- *Cisco IOS Release 12.0 Security Command Reference*

- *Improving Security on Cisco Routers*

# Supported Platforms

- Cisco 7200 routers

- Cisco 7500 series

### Platform Support Through 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 Feature Navigator. Feature Navigator dynamically updates the list of supported platforms as new platform support is added for the feature.

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.

To access 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.

Feature Navigator is updated when major Cisco IOS software releases and technology releases occur. As of May 2001, Feature Navigator supports M, T, E, S, and ST releases. You can access Feature Navigator at the following URL:

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

# Supported Standards, MIBs, and RFCs

### Standards

No new or modified standards are supported by this feature.

**MIBs**

No new or modified MIBs are supported by this feature.

To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB web site on Cisco.com at the following URL: http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml.

**RFCs**

No new or modified RFCs are supported by this feature.

# Configuration Tasks

The following section details the configuration task necessary for the Enhanced Password Security feature.

- Configuring Enhanced Security Password, page 3 (required)

# Configuring Enhanced Security Password

| | Command | Purpose |
|---|---|---|
| **Step 1** | Router(config)# **username** *name* **secret 0** *password* | Configures a username and encrypts a clear text password with MD5 encryption. |
| | or | |
| | Router(config)# **username** *name* **secret 5** *encrypted-secret* | Configures a username and enters an MD5 encrypted text string which is stored as theMD5 encrypted password for the specified username. |

# Verifying MD5 Password Encryption

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

**Step 1** Configure an encrypted MD5 user password in global configuration mode.

**Step 2** Exit configuration mode and enter the **login local** command.

**Step 3** Verify that a valid user is able to log in through the console.

# Monitoring and Maintaining Enhanced Password Security

Use the following command to monitor and maintain Enhanced Password Security.

| Command | Purpose |
|---|---|
| Router# **show running-config** | Enter the **show running-config** command to verify that MD5 password encryption has been enabled. If the "`username name secret 5`" line appears in the command output, the Enhanced Password Security feature is enabled. |

# Configuration Examples

This section provides the following configuration example:

# Configuring MD5 Encryption on a Clear Text Password Example

The following example configures username "abc" with the MD5 encrypted password "xyz". Output from the **show running-config** confirms that the MD5 encrypted password has been configured. Note that the password itself is not displayed.

```
Router# configure terminal
Router(config)# username abc secret 0 xyz
Router(config)# exit
Router# show running-config
!
version 12.0
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 configures username "cde" and enters an MD5 encryption text string as the user password. Output from the **show running-config** confirms that the MD5 encrypted password has been configured. Note that the password itself is not displayed.

```
Router# configure terminal
Router(config)# username cde secret 5 $1$feb0$a104Qd9UZ./Ak00KTggPD0
Router(config)# exit
Router# show running-config
!
version 12.0
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 modified command that configures the Enhanced Password Security feature. All other commands used with this feature are documented in the Cisco IOS Release 12.0 command reference publications.

- **username (secret)**

# username (secret)

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

**username** *name* **secret** {**0** *password* | **5** *encrypted-secret*}

**Syntax Description**

| | |
|---|---|
| *name* | Specifies the user name. |
| **0** *password* | Specifies a clear text password, which will be MD5 encrypted. |
| **5** *encrypted-secret* | 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 |
|---|---|
| 10.0 | This command was introduced. |
| 11.1 | The following keywords and arguments were added: |
| | • **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**] |
| 12.0(18)S | The following keywords were added: |
| | • **secret 0** |
| | • **secret 5** |

**Usage Guidelines**

Use the **username secret** command to configure a user name and MD5 encrypted user password.Use the **0** keyword to enable MD5 encryption on a clear text password. Use the **5** keyword to enter an MD5 encryption string and save it as the userMD5 encrypted secret. MD5 encryption is a strong encryption method which is not retrievable. You cannot use MD5 encryption with protocols such as CHAP that require clear-text passwords.

Use the **username secret** command to provide an additional layer of security over the username password. The **username secret** command provides better security by encrypting the password using non-reversible MD5 encryption, and storing the encrypted text. The added layer of MD5 encryption is useful in environments where 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.

⚠
**Caution**      If you specify MD5 encryption 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 **username 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 **username secret** command provides.

**Examples**      The following example configures username "abc" and enables MD5 encryption on the clear text password "xyz":

```
username abc secret 0 xyz
```

The following example configures username "cde" and enters an MD5 encrypted text string that is stored as the user name 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. |

# Glossary

**CHAP**—Challenge-Handshake Authentication Protocol

**MD5**—Message Digest 5. Algorithm used for message authentication in SNMP v.2. MD5 verifies the integrity of the communication, authenticates the origin, and checks for timeliness.