traffic-export through zone security

username

To establish a username-based authentication system, use the **username** command in global configuration mode. To remove an established username-based authentication, use the **no** form of this command.

username *name* [**aaa attribute list** *aaa-list-name*]

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

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

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

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

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

username *name* **[dnis]**

username *name* **[mac]**

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

username *name* **[noescape]**

username *name* **[nohangup]**

username *name* [**nopassword**| **password** *password*| **password** *encryption-type encrypted-password*]

username *name* [**one-time** {**password** {**0**| **7**| *password*}| **secret** {**0**| **5**| *password*}}]

username *name* [**password** *secret*]

username *name* [**privilege** *level*]

username *name* [**secret** {**0**| **5**| *password*}]

username *name* [**user-maxlinks** *number*]

username [lawful-intercept] *name* [**privilege** *privilege-level*| **view** *view-name*] **password** *password*

no username *name*

Syntax Description

name	Hostname, server name, user ID, or command name. The *name* argument can be only one word. Blank spaces and quotation marks are not allowed.
aaa attribute list *aaa-list-name*	Uses the specified authentication, authorization, and accounting (AAA) method list.
access-class *access-list-number*	(Optional) Specifies an outgoing access list that overrides the access list specified in the **access-class** command available in line configuration mode. It is used for the duration of the user's session.

autocommand *command*	(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 can contain embedded spaces, commands using the **autocommand** keyword must be the last option on the line.
callback-dialstring *telephone-number*	(Optional) For asynchronous callback only: permits you to specify a telephone number to pass to the DCE device.
callback-line *line-number*	(Optional) For asynchronous callback only: relative number of the terminal line (or the first line in a contiguous group) on which you enable a specific username for callback. Numbering begins with zero.
ending-line-number	(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 line-number and ending-line-number are absolute rather than relative line numbers.
tty	(Optional) For asynchronous callback only: standard asynchronous line.
callback-rotary *rotary-group-number*	(Optional) For asynchronous callback only: permits you to specify a rotary group number on which you want to enable a specific username for callback. The next available line in the rotary group is selected. Range: 1 to 100.
dnis	Does not require a password when obtained via Dialed Number Identification Service (DNIS).
mac	Allows a MAC address to be used as the username for MAC filtering done locally.
nocallback-verify	(Optional) Specifies that the authentication is 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 software from disconnecting the user after an automatic command (set up with the **autocommand** keyword) has completed. Instead, the user gets another EXEC prompt.

nopassword	No password is required for this user to log in. This is usually the most useful keyword to use in combination with the **autocommand** keyword.
password	Specifies the 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.
password	Password that a user enters.
encryption-type	Single-digit number that defines whether the text immediately following is encrypted and if so, what type of encryption is used. 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.
encrypted-password	Encrypted password that a user enters.
one-time	Specifies that the username and password is valid for only one time. This configuration is used to prevent default credentials from remaining in user configurations.
0	Specifies that an unencrypted password or secret (depending on the configuration) follows.
7	Specifies that a hidden password follows.
5	Specifies that a hidden secret follows.
secret	Specifies a secret for the user.
secret	For Challenge Handshake Authentication Protocol (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.
privilege *privilege-level*	(Optional) Sets the privilege level for the user. Range: 1 to 15.
user-maxlinks *number*	Maximum number of inbound links allowed for a user.

lawful-intercept	(Optional) Configures lawful intercept users on a Cisco device.
name	Hostname, server name, user ID, or command name. The *name* argument can be only one word. Blank spaces and quotation marks are not allowed.
view *view-name*	(Optional) For CLI view only: associates a CLI view name, which is specified with the **parser view** command, with the local AAA database.
password *password*	Password to access the CLI view.

Command Default

No username-based authentication system is established.

Command Modes

Global configuration (config)

Command History

Release	Modification
10.0	This command was introduced.
11.1	This command was modified. The following keywords and arguments were added: • **callback-dialstring** *telephone-number* • **callback-rotary** *rotary-group-number* • **callback-line** [**tty**] *line-number* [*ending-line-number* • **nocallback-verify**
12.3(7)T	This command was modified. The following keywords and arguments were added: • **lawful-intercept** • **view** • *view-name*
12.2(33)SRB	This command was modified. The following keywords and arguments were integrated into Cisco IOS Release 12.2(33)SRB: • **lawful-intercept** • **view** • *view-name*

Release	Modification
12.2(33)SB	This command was modified. The following keywords and arguments were integrated into Cisco IOS Release 12.2(33)SB: • **lawful-intercept** • **view** • *view-name*
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
12.4	This command was modified. The following keywords were integrated into Cisco IOS Release 12.4: • **one-time** • **secret** • **0, 5, 7**
15.1(1)S	This command was modified. Support for the **nohangup** keyword was removed from Secure Shell (SSH).
Cisco IOS XE Release 3.2SE	This command was modified. The **mac** keyword was added.

Usage Guidelines

The **username** command provides username or password authentication, or both, for login purposes only.

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

Add a username entry for each remote system with which the local router communicates and from which it requires authentication. 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 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.

- To avoid the situation of a privilege level 1 user entering into a higher privilege level, configure a per-user privilege level other than 1 (for example, 0 or 2 through 15).

- Per-user privilege levels override virtual terminal privilege levels.

In Cisco IOS Release 15.1(1)S and later releases, the **nohangup** keyword is not supported with SSH. If the **username** *user* **autocommand** *command-name* command is configured and SSH is used, the session disconnects after executing the configured command once. This behavior with SSH is opposite to the Telnet behavior, where Telnet continuously asks for authentication and keeps executing the command until the user exits Telnet manually.

CLI and Lawful Intercept Views

Both CLI views and lawful intercept views restrict access to specified commands and configuration information. A lawful intercept view allows a user to secure access to lawful intercept commands that are held within the TAP-MIB, which is a special set of Simple Network Management Protocol (SNMP) commands that stores information about calls and users.

Users who are specified via the **lawful-intercept** keyword are placed in the lawful-intercept view, by default, if no other privilege level or view name has been explicitly specified.

If no value is specified for the *secret* argument and the **debug serial-interface** command is enabled, an error is displayed when a link is established and the CHAP challenge is not implemented. The 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 *Cisco IOS Debug Command Reference* .

Examples

The following example shows how 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:

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

The following example shows how 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
```

The following example shows how to implement an ID that works even if all the TACACS+ servers break. The command takes the following form:

```
username superuser password superpassword
```

The following example shows how to enable CHAP on interface serial 0 of "server_l." It also defines a password for a remote server named "server_r."

```
hostname server_l
username server_r password theirsystem
interface serial 0
 encapsulation ppp
 ppp authentication chap
```

The following is output from the **show running-config** command displaying the passwords that are encrypted:

```
hostname server_l
username server_r password 7 121F0A18
interface serial 0
 encapsulation ppp
 ppp authentication chap
```

In the following example, a privilege level 1 user is denied access to privilege levels higher than 1:

```
username user privilege 0 password 0 cisco
username user2 privilege 2 password 0 cisco
```

The following example shows how to remove the username-based authentication for user2:

```
no username user2
```

Related Commands

Command	Description
arap callback	Enables an ARA client to request a callback from an ARA client.
callback forced-wait	Forces the Cisco IOS software to wait before initiating a callback to a requesting client.
debug ppp negotiation	Displays PPP packets sent during PPP startup, where PPP options are negotiated.
debug serial-interface	Displays information about a serial connection failure.
debug serial-packet	Displays more detailed serial interface debugging information than you can obtain using **debug serial interface** command.
ppp callback (DDR)	Enables a dialer interface that is not a DTR interface to function either as a callback client that requests callback or as a callback server that accepts callback requests.
ppp callback (PPP client)	Enables a PPP client to dial into an asynchronous interface and request a callback.
show users	Displays information about the active lines on the router.

username secret

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

username *name* **secret** {**0** *password* | **5** *secret-string* | **4** *secret-string* | **8** *secret-string* | **9** *secret-string*}

Syntax Description

name	Username.
0	Specifies an unencrypted secret.
password	Clear-text password.
5 *secret-string*	message digest alogrithm5 (MD5) encrypted secret text string, which is stored as the encrypted user password.
4 *secret-string*	Secure Hash Algorithm, 26-bits (SHA-256) encrypted secret text string, which is stored as the encrypted user password. **Note** NOTE: Effective with CSCue95644, the **4** keyword is deprecated.
8 *secret-string*	Password-Based Key Derivation Function 2 (PBKDF2) with SHA-256 hashed secret text string, which is stored as the hashed user password.
9 *secret-string*	Scrypt hashed secret text string, which is stored as the hashed user password.

Command Default

No username-based authentication system is established.

Command Modes

Global configuration (config)

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.
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.

Release	Modification
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Cisco IOS Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
15.0(1)S	This command was integrated into Cisco IOS Release 15.0(1)S. Algorithm types **0**, **4**, and **5** were added.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.
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 Guidelines

Use the **username secret** command to configure a username and MD5-encrypted user password. MD5 encryption is a strong encryption method that is not retrievable; thus, you cannot use MD5 encryption with protocols that require clear-text passwords, such as Challenge Handshake Authentication Protocol (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 non reversible 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.

Use this command to enable Enhanced Password Security for the specified, unretrievable username. This command enables MD5 encryption on the password. MD5 encryption is a strong encryption method. You cannot use MD5 encryption with protocols, such as CHAP, that require clear-text passwords.

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.

With CSCue95644, you can use the **username secret** command to configure a username and hash the user 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.

The **username** command provides username or secret authentication for login purposes only. The *name* argument can be one word only. Spaces and quotation marks are not allowed. You can use multiple **username** commands to specify options for a single user.

Examples

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

```
username abc secret 0 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
```

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

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

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

```
Device# configure terminal
Device(config)# username demo 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 username

username demo secret 4 tnhtc92DXBhelxjYk8LWJrPV36S2i4ntXrpb4RFmfqY
```

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.
username algorithm-type	Sets the algorithm type to hash a user password configured using the **username secret** command.