AAA Commands

This chapter contains the following sections:

aaa authentication login

Use the **aaa authentication login** Global Configuration mode command to set one or more authentication methods to be applied during login. Use the **no** form of this command to restore the default authentication method.

Syntax

aaa authentication login [**authorization**] {**default** | *list-name*} *method1* [*method2...*]

no aaa authentication login {**default** | *list-name*}

Parameters

- **authorization**—Specifies that authentication and authorization are applied to the given list. If the keyword is not configured, then only authentication is applied to the given list.
- **default**—Uses the authentication methods that follow this argument as the default method list when a user logs in (this list is unnamed).
- ***list-name***—Specifies a name of a list of authentication methods activated when a user logs in. (Length: 1–12 characters)
- ***method1*** [*method2...*]—Specifies a list of methods that the authentication algorithm tries (in the given sequence). Each additional authentication method is used only if the previous method returns an error, not if it fails. To ensure that the authentication succeeds even if all methods return an error, specify **none** as the final method in the command line. Select one or more methods from the following list::

Keyword	Description
enable	Uses the enable password for authentication.
line	Uses the line password for authentication.
local	Uses the locally-defined usernames for authentication.
none	Uses no authentication.
radius	Uses the list of all RADIUS servers for authentication.
tacacs	Uses the list of all TACACS+ servers for authentication.

Default Configuration

If no methods are specified, the default are the locally-defined users and passwords. This is the same as entering the command **aaa authentication login local**.

Command Mode

Global Configuration mode

User Guidelines

Create a list of authentication methods by entering this command with the *list-name* parameter where *list-name* is any character string. The method arguments identifies the list of methods that the authentication algorithm tries, in the given sequence.

Note If authorization is enabled for login and the switch receives from a TACACS+ server user level 15, then the enable command is not required and if received level 1 the enable command is required.

The **no aaa authentication login** *list-name* command deletes a list-name only if it has not been referenced by another command.

Example

The following example sets the authentication login methods for the console.

```
switchxxxxxx(config)# aaa authentication login authen-list radius local none
switchxxxxxx(config)# line console
switchxxxxxx(config-line)# login authentication authen-list
```

aaa authentication enable

The **aaa authentication enable** Global Configuration mode command sets one or more authentication methods for accessing higher privilege levels. To restore the default authentication method, use the **no** form of this command.

Syntax

aaa authentication enable [**authorization**] {**default** | *list-name*} *method* [*method2...*]}

no aaa authentication enable {**default** | *list-name*}

Parameters

- **authorization**—Specifies that authentication and authorization are applied to the given list. If the keyword is not configured, then only authentication is applied to the given list.
- **default**—Uses the listed authentication methods that follow this argument as the default method list, when accessing higher privilege levels.
- ***list-name*** —Specifies a name for the list of authentication methods activated when a user accesses higher privilege levels. (Length: 1–12 characters)
- ***method*** [*method2...*]—Specifies a list of methods that the authentication algorithm tries, in the given sequence. The additional authentication methods are used only if the previous method returns an error, not if it fails. Specify **none** as the final method in the command line to ensure that the authentication succeeds, even if all methods return an error. Select one or more methods from the following list:

Keyword	Description
enable	Uses the enable password for authentication.
line	Uses the line password for authentication.
none	Uses no authentication.
radius	Uses the list of all RADIUS servers for authentication.
tacacs	Uses the list of all TACACS+ servers for authentication.

Default Configuration

No Authentication lists exist by default.

Command Mode

Global Configuration mode

User Guidelines

Create a list by entering the **aaa authentication enable** *list-name method1 [method2...]* command where *list-name* is any character string used to name this list. The method argument identifies the list of methods that the authentication algorithm tries, in the given sequence.

All **aaa authentication enable** requests sent by the device to a RADIUS server include the username **$enabx$**, where **x** is the requested privilege level.

All **aaa authentication enable** requests sent by the device to a TACACS+ server include the username that is entered for login authentication.

The additional methods of authentication are used only if the previous method returns an error, not if it fails. Specify **none** as the final method in the command line to ensure that the authentication succeeds even if all methods return an error.

no aaa authentication enable *list-name* deletes list-name if it has not been referenced.

Example

The following example sets the enable password for authentication for accessing higher privilege levels.

```
switchxxxxxx(config)# aaa authentication enable enable-list radius none
switchxxxxxx(config)# line console
switchxxxxxx(config-line)# enable authentication enable-list
```

login authentication

The **login authentication** Line Configuration mode command specifies the login authentication method list for a remote Telnet or console session. Use the **no** form of this command to restore the default authentication method.

Syntax

login authentication {**default** | *list-name*}

no login authentication

Parameters

- **default**—Uses the default list created with the **aaa authentication login** command.
- ***list-name***—Uses the specified list created with the **aaa authentication login** command.

Default Configuration

default

Command Mode

Line Configuration Mode

Example 1 - The following example specifies the login authentication method as the default method for a console session.

```
switchxxxxxx(config)# line console
switchxxxxxx(config-line)# login authentication default
```

Example 2 - The following example sets the authentication login methods for the console as a list of methods.

```
switchxxxxxx(config)# aaa authentication login authen-list radius local none
switchxxxxxx(config)# line console
switchxxxxxx(config-line)# login authentication authen-list
```

enable authentication

The **enable authentication** Line Configuration mode command specifies the authentication method for accessing a higher privilege level from a remote Telnet or console. Use the **no** form of this command to restore the default authentication method.

Syntax

enable authentication {**default** | *list-name}*

no enable authentication

Parameters

- **default**—Uses the default list created with the **aaa authentication enable** command.
- ***list-name***—Uses the specified list created with the **aaa authentication enable** command.

Default Configuration

default.

Command Mode

Line Configuration Mode

Example 1 - The following example specifies the authentication method as the default method when accessing a higher privilege level from a console.

```
switchxxxxxx(config)# line console
switchxxxxxx(config-line)# enable authentication default
```

Example 2 - The following example sets a list of authentication methods for accessing higher privilege levels.

```
switchxxxxxx(config)# aaa authentication enable enable-list radius none
switchxxxxxx(config)# line console
switchxxxxxx(config-line)# enable authentication enable-list
```

ip http authentication

The **ip http authentication** Global Configuration mode command specifies authentication methods for HTTP server access. Use the **no** form of this command to restore the default authentication method.

Syntax

ip http authentication aaa login-authentication [**login-**authorization] *method1* [*method2...*]

no ip http authentication aaa login-authentication

Parameters

- **login-**authorization—Specifies that authentication and authorization are applied. If the keyword is not configured, then only authentication is applied.
- ***method*** [*method2...*]—Specifies a list of methods that the authentication algorithm tries, in the given sequence. The additional authentication methods are used only if the previous method returns an error, not if it fails. Specify **none** as the final method in the command line to ensure that the authentication succeeds, even if all methods return an error. Select one or more methods from the following list:

Keyword	Description
local	Uses the local username database for authentication.
none	Uses no authentication.
radius	Uses the list of all RADIUS servers for authentication.
tacacs	Uses the list of all TACACS+ servers for authentication.

Default Configuration

The local user database is the default authentication login method. This is the same as entering the **ip http authentication local** command.

Command Mode

Global Configuration mode

User Guidelines

The command is relevant for HTTP and HTTPS server users.

Example

The following example specifies the HTTP access authentication methods.

```
switchxxxxxx(config)# ip http authentication aaa login-authentication radius local none
```

show authentication methods

The **show authentication methods** Privileged EXEC mode command displays information about the authentication methods.

Syntax

show authentication methods

Command Mode

Privileged EXEC mode

Example

The following example displays the authentication configuration:

switchxxxxxx# **show**

```
authentication methods
Login Authentication Method Lists
---------------------------------
Default: Radius, Local, Line
Consl_Login(with authorization): Line, None
Enable Authentication Method Lists
----------------------------------
Default: Radius, Enable
Consl_Enable(with authorization): Enable, None
```

.

```
Line                    Login Method List    Enable Method List
--------------          -----------------    ------------------
Console                 Consl_Login          Consl_Enable
Telnet                  Default              Default
SSH                     Default              Default
```

```
HTTP, HHTPS: Radius, local
Dot1x: Radius
```

login block-for

Login Block-for

Use the following global configuration mode command to configure a quiet mode period followed specified number of failed login attempts. Use the no form of command to return to default settings:

Syntax

login block-for seconds **attempts** tries **within** seconds

no login block-for

Parameters

- **Block for seconds** - Duration (in seconds) of quiet mode period (the time in which login attempts are denied) (range 1 - 65535 (18 hours) seconds).
- **attempts** tries - The number of failed login attempts that triggers the quiet mode period (range 1-100).
- **within** seconds - Duration of time (in seconds) in which the number of failed login attempts must be made before the quiet mode period is triggered (range 1 - 3600 (1 hour) seconds).

Default Configuration

Quiet mode is not configured on device.

Command Mode

Global Configuration mode.

User Guidelines

If the specified number of connection attempts fails (**attempt** tries) within a specified time (**within** seconds), the device will not accept any additional login attempts for a specified period of time (**block-for** seconds).

During the quiet-mode period, management connections to device are restricted by the quiet-mode access-class which allows only the specified connections (command **login quiet-mode access-class**). For devices that support a console connection the “console_only” management access-list is used as the default quiet-mode access-class. In this case, all login attempts over the network (Telnet, SSH, SNMP, HTTP or HTTPS) are denied during the quiet-mode period.

This command can be configured only if a quiet-mode access-class (default or user defined) is configured – see “login quiet-mode access-class”

If the **login block-for** command is already configured on device and the command is reconfigured with new parameters during the “watch period” – then the current count will be terminated, and a new count will begin using new parameters. The Command is rejected if configured during login attack quiet-mode period.

The **no** form of command disables the feature and terminates the quiet mode period, if active.

Examples

Example 1 - The following example shows how to block all login requests for 180 seconds if 18 failed login attempts are exceeded within 180 seconds:

```
switchxxxxxx(config)# login block-for 180 attempts 18 within 180
```

Example 2 -The following example displays an attempt to configure command during device quiet mode period:

```
switchxxxxxx(config)# login block-for 18 attempts 8 within 50
```

Cannot configure login block-for setting while device is in Quiet-Mode.

Example 3 - The following example displays an failure to configure command. Failure reason: quiet-mode access class (default or user defined) is not configured:

```
switchxxxxxx(config)# login block-for 770 attempts 7 within 613
```

Cannot configure login block-for setting since quiet-mode access-class is not configured.

login delay

Use the **login delay** Global Configuration mode command to configure a delay in device response to a failed login attempts. Use the no form of this command to return to the default setting.

Syntax

login delay seconds

no login delay

Parameters

- seconds - The delay (in seconds) that is imposed between failed login attempts (range 1-10 seconds).

Default Configuration

By default, login delay is disabled.

Command Mode

By default, login delay is disabled.

User Guidelines

The login delay command introduces a delay in device response following a failed login attempt (HTTP, HTTPS, Telnet, SSH and SNMP). The delay provides better protection from possible dictionary attacks.

Examples

Example 1 - The following example sets a delay of 5 seconds following a failed login attempt:

```
switchxxxxxx(config)# login delay 5
```

login quiet-mode access-class

Use the login quiet-mode access-class Global Configuration mode command to to specify a management access control list (MACL) that will be applied when the device transitions to the login quiet-mode. Use the no form of this command to return to the default setting.

Syntax

login quiet-mode access-class name

no login quiet-mode access-class

Parameters

- ***name*** – the name of the management ACL to apply on the device while in login quiet mode.

Default Configuration

By default, the "console-only" management access list is applied as the default quiet-mode access-class. For devices that do not support console - the quiet-mode access-class has no default.

Command Mode

Global configuration mode.

User Guidelines

Use the **login quiet-mode access-class** command to allow selective hosts access to the device management during a login quiet period. Access is allowed based on the specified Management ACL. The management access list needs to be created prior to configuring this command using the management access-list command.

This settings provides the ability to grant access to a client or list of clients even during a quiet-mode period. On devices that support a console connection the "console-only" management access-list is applied by default during a quiet-mode period, meaning all network login connections (telnet, SSH, SNMP, HTTP, HTTPS) are denied, while a connection from the console is allowed. On devices that do not support a console there is no default access-class and the login block-for command cannot be configured if user did not first define a quiet-mode access-class.

The command is rejected if it is configured during a quiet-mode period.

The no form of the command returns quiet-mode access-class to the default setting. On devices without a console the no command cannot be applied if login block-for command is configured.

Examples

Example 1 - The following example shows how to configure the device to accept connection during quiet mode period based on quiet-acl management access list:

```
switchxxxxxx(config)# login quiet-mode access-class quiet-acl
```

show login

Use the following privileged exec mode command to display login setting and status:

Syntax

show login

Parameters

N/A

Default Configuration

N/A

Command Mode

Privileged EXEC mode

User Guidelines

This command displays setting and status related to commands **login delay**, **Login block-for and login quiet-mode access-class**.

Examples

Example 1 - The following example shows output if no login settings have been applied or changed:

```
switchxxxxxx# show login
Login delay: disabled
Login Attacks watch: disabled
Quiet-Mode access list: console-only (the default)
```

Example 2 - The following example shows the show login command output where the user set the login delay to 5 seconds, configured a login block period and the device is not in quiet-mode:

```
switchxxxxxx# show login
Login delay: 5 second
Login Attacks watch: enabled
If more than 4 login failures occur in 60 seconds or less, logins will be disabled for 60
seconds.
Quiet-Mode access list: console-only (the default)
Quiet-Mode: inactive
Watch Window remaining time: 44 seconds.
Present login failure count: 3.
```

Note Login failure count is counted from the earliest failed login that is still valid (within a watching windows)

Example 3 - The following example shows output where user set login delay to 5 seconds, configured a login block period and device is in quiet mode:

```
switchxxxxxx# show login
Login delay: 5 second
Login Attacks watch: enabled
If more than 4 login failures occur in 60 seconds or less, logins will be disabled for 60
seconds.
Quiet-Mode access list: console-only (the default)
Quiet-Mode: active (time remaining: 20 seconds)
```

show login failures

Use the following privileged exec mode command to display information on failed login attempts:

Syntax

Show login failures

Parameters

NA

Default Configuration

NA

Command Mode

Privileged EXEC mode

User Guidelines

This command displays information on last 50 failed login attempts. Information includes the username provided in the failed attempt (if provided as part of attempt), source IP used in failed attempt, service requested in the failed attempt, the number of failed attempts for this connection and the time stamp of last failed attempt for this connection. Entries are sorted from the newest time stamp to the oldest.

Examples

```
switchxxxxxx#  show login failures
```

Information about last 50 login failure's with the device.

Username	Source IP	Service	Count	TimeStamp
___________	___________	___________	___________	___________
ffff	10.5.44.25	telnet	3	00:01:23 edt Wed Jul 7 2021
fff	10.5.44.25	telnet	4	08:37:08 edt Thu Jul 8 2021
bb	10.5.44.25	ssh	2	00:17:59 edt Wed Jul 7 2021
fff	10.5.44.25	ssh	2	00:20:37 edt Wed Jul 7 2021
ffff	10.5.44.25	ssh	2	00:21:12 edt Wed Jul 7 2021

Username	Source IP	Service	Count	TimeStamp
aaaa	fe80::1111	ssh	2	00:21:26 edt Wed Jul 7 2021
	10.5.44.25	telnet	3	00:38:14 edt Wed Jul 7 2021
aaa	10.5.44.22	telnet	1	08:37:16 edt Thu Jul 8 2021
555	10.5.44.23	telnet	1	08:37:26 edt Thu Jul 8 2021

clear login failures

Use the following privileged exec mode command to clear login failure database:

Syntax

clear login failures

Parameters

NA

Default Configuration

NA

Command Mode

Privileged EXEC mode

User Guidelines

Use this command to clear all entries in login failure database (command **show login failures**).

Examples

```
switchxxxxxx#  clear login failures
```

clear login quiet-mode

Use the following privileged exec mode command to immediately terminate an active quiet-mode period:

Syntax

clear login quiet-mode

Parameters

NA

Default Configuration

NA

Command Mode

Privileged EXEC mode

User Guidelines

Use this command to terminate an active quiet-period, without disabling the feature (command **login block-for**). Quiet mode period will be terminated even if the quiet mode period timer did not expire.

Examples

```
switchxxxxxx#  clear login quiet-mode
11-Aug-2021 10:33:12 :%ABC-I-XXX: Quiet-Mode is OFF, terminated by user
```

password

Use the **password** Line Configuration mode command to specify a password on a line (also known as an access method, such as a console or Telnet). Use the **no** form of this command to return to the default password.

Syntax

password {*unencrypted-password* [**method** *hash-method***]** | *encrypted-password* **encrypted**}

password generate-password [**method** hash-method]

no password

Parameters

- ***unencrypted-password***—The authentication password for the user. (Range: 1–64)
- [**method** *hash-method***]** — (optional) specifies the method used for encrypting the clear-text password. Supported values:
  - **sha512** - PBKDF2 encryption with HMAC using the SHA512 as the underlying Hashing Algorithm. This is the default method if the **method** parameter is not specified.
- **encrypted** encrypted-password—Specifies that the password is encrypted and hashed using a salt. Use this keyword to enter a password that is already encrypted (for instance, a password that was copied from the configuration file of another device). The *encrypted-password* is specified in the format of *$<type>$<salt>$<encrypted-password >*, where:
  - **<*type*>** - is an integer value that indicates the type of hash algorithm used to generate the hash
  - **<salt>** - The base64 encoding of the 96 bits used for salt (length – 16 bytes)
  - **<*encrypted-password*>** - The base64 encoding of the encrypted hash output (length - 86 bytes)

Default Configuration

No password is defined.

Command Mode

Line Configuration Mode

User Guidelines

The *unencrypted-password* must comply to password complexity requirements.

If the **generate-password** option is selected, the user does not need to input a password. Instead, the device will automatically generate a random based password suggestion. This suggestion will be displayed to the user, and the user will be presented with an option to accept or reject the proposed password. If user selected to accept the proposed password, then the specified username with this password (in encrypted format) will be added to device configuration file. If user rejects the proposed password then a new command needs to be entered by the user.

Example

Example 1 -The following example specifies the password ‘secreT123!’ on the console line.

```
switchxxxxxx(config)# line console
switchxxxxxx(config-line)# password secreT123!
```

Example 2 - The command in this example includes the generate-password key word. in this case the device will propose a randomly generated password to be used. in the example below the user selects to accept the proposed password.

```
switchxxxxxx(config)# line console
switchxxxxxx(config-line)# password generate-password
Generated password: aBgrT9!59Hq$
Accept generated password (y/n) [Y] y
“Configuration and password are added to device configuration. Please Note
password for future use.”
```

Example 3 - The command in this example includes the generate-password key word. in this case the device will propose a randomly generated password to be used. in the example below the user selects to reject the proposed password.

```
switchxxxxxx(config)# line console
switchxxxxxx(config-line)# password generate-password
Generated password: aBgrT9!59Hq$
Accept generated password (y/n) [Y] n
“Auto generated password rejected by user. Password configuration is not added to
device configuration”
```

enable password

Use the **enable password** Global Configuration mode command to set a local password to control access to normal and privilege levels. Use the **no** form of this command to return to the default password.

Syntax

enable password [**level** *privilege-level*] {[**method** *hash-method*] *unencrypted-password* | **encrypted** *encrypted-password*}

enable [**level** *privilege-level*] [**method** *hash-method*] **generate-password**

enable masked-secret [**level** *privilege-level*] [**method** *hash-method*]

no enable password [**level** *privilege-level*]

Parameters

- **level** privilege-level—Level for which the password applies. If not specified, the level is 15. (Range: 1–15)
- [**method** *hash-method*] — (optional) specifies the method used for encrypting the clear-text password. Supported values:
  - **sha512** - PBKDF2 encryption with HMAC using the SHA512 as the underlying Hashing Algorithm. This is the default method if the **method** parameter is not specified.
- *unencrypted-password*—Password for this level. (Range: 0–159 chars)
- **encrypted** encrypted-password—Specifies that the password is encrypted and hashed using a salt. Use this keyword to enter a password that is already encrypted (for instance, a password that was copied from the configuration file of another device). The *encrypted-password* is specified in the format of *$<type>$<salt>$<encrypted-password* >, where:
  - ***<type>*** - is an integer value that indicates the type of hash algorithm used to generate the hash
  - **<salt>** - The base64 encoding of the 96 bits used for salt (length – 16 bytes)
  - ***<encrypted-password>*** - The base64 encoding of the encrypted hash output (length - 86 bytes)

Default Configuration

Default for **level** is 15.

Command Mode

Global Configuration mode

User Guidelines

The *unencrypted-password* must comply to password complexity requirements

When the administrator configures a new **enable** password, this password is encrypted automatically and saved to the configuration file. No matter how the password was entered, it appears in the configuration file with the keyword **encrypted** and the encrypted value. The administrator is required to use the **encrypted** keyword only when actually entering an encrypted keyword.

If the administrator wants to manually copy a password that was configured on one switch (for instance, switch B) to another switch (for instance, switch A), the administrator must add **encrypted** in front of this encrypted password when entering the **enable** command in switch A. In this way, the two switches will have the same password.

The administrator is required to use the **encrypted** keyword only when actually entering an encrypted keyword.

If the **generate-password** option is used, instead of entering a password the user will be presented with a randomly generated password suggestion. This suggestion will comply with all current password strength settings

The user will be given the choice to accept or reject the proposed password. If the user elects to accept the password, then this password will be added for the configured enable level (in encrypted format) in the configuration file.

If the user rejects the password suggestion, the command will need to be entered again to configure this enable level.

Example

Example 1 - The command sets a password that has already been encrypted. It will be copied to the configuration file just as it is entered. To login to device using this password, the user must know its unencrypted form.

```
switchxxxxxx(config)# enable password encrypted
$15$TqKC13RgV/QJb2Ma$4JmeD7wgRGH2iwGKMM+g4M53uQxpOMlhkUN56UMAEUuMqhw0bsRH27zakc7
2hLxt/YhEknPA6LX7fTgqwZn6Vw==
```

Example 2 - The command sets an unencrypted password for level 1 (it will be encrypted in the configuration file).

```
switchxxxxxx(config)# enable password level 1 let-me-In
```

Example 3 - The command in this example includes the **generate-password** key word. in this case the device will propose a randomly generated password to be used. in the example below the user selects to **accept** the proposed password.

```
switchxxxxxx(config)# enable password generate-password
Generated password: aBgrT9!59Hq$
Accept generated password (y/n) [Y] y
“Configuration and password are added to device configuration. Please Note
password for future use”
```

Example 4 - The command in this example includes the generate-password key word. in this case the device will propose a randomly generated password to be used. in the example below the user selects to rejects the proposed password.

```
switchxxxxxx(config)# enable password generate-password
Generated password: aBgrT9!59Hq$
Accept generated password (y/n) [Y] n
“Auto generated password rejected by user. Password configuration is not added to
device configuration”
```

service password-recovery

Use the **service password-recovery** Global Configuration mode command to enable the password-recovery mechanism. This mechanism allows an end user, with physical access to the console port of the device, to enter the boot menu and trigger the password recovery process. Use the **no service password-recovery** command to disable the password-recovery mechanism. When the password-recovery mechanism is disabled, accessing the boot menu is still allowed and the user can trigger the password recovery process. The difference is, that in this case, all the configuration files and all the user files are removed. The following log message is generated to the terminal: “All the configuration and user files were removed”.

Syntax

service password-recovery

no service password-recovery

Default Configuration

The service password recovery is enabled by default.

Command Mode

Global Configuration mode

User Guidelines

- If password recovery is enabled, the user can access the boot menu and trigger the password recovery in the boot menu. All configuration files and user files are kept.
- If password recovery is disabled, the user can access the boot menu and trigger the password recovery in the boot menu. The configuration files and user files are removed.
- If a device is configured to protect its sensitive data with a user-defined passphrase for (Secure Sensitive Data), then the user cannot trigger the password recovery from the boot menu even if password recovery is enabled.

Example

The following command disables password recovery:

```
switchxxxxxx(config)# no service password recovery
Note that choosing to use Password recovery option in the Boot Menu during the boot process
 will remove the configuration files and the user files. Would you like to continue ? Y/N.
```

username

Use the **username** Global Configuration mode command to create or edit a username based user authentication account. Use the **no** form to remove a user account.

Syntax

username name {[**method** *hash-method*] **password** {*unencrypted-password* | {**encrypted** encrypted-password}} | {**privilege** privilege-level {[**method** *hash-method*] *unencrypted-password* | {**encrypted** encrypted-password}}}}

username name {[**method** hash-method] **generate-password** | {**privilege** privilege-level{[**method** hash-method] **generate-password**}

username *name* {[**method** hash-method] **masked-secret** | {**privilege** privilege-level {[**method** hash-method] **masked-secret**}

no username name

Parameters

- ***name***—The name of the user. (Range: 1–20 characters)
- [**method** *hash-method*] — (optional) specifies the method used for encrypting the clear-text password. Supported values:
    - **sha512** - PBKDF2 encryption with HMAC using the SHA512 as the underlying Hashing Algorithm. This is the default method if the **method** parameter is not specified.
- **password**—Specifies the password for this username.
- unencrypted-password—The authentication password for the user. (Range: 1–64)
- **encrypted** encrypted-password—Specifies that the password is encrypted and hashed using a salt. Use this keyword to enter a password that is already encrypted (for instance, a password that was copied from the configuration file of another device). The *encrypted-password* is specified in the format of *$<type>$<salt>$<encrypted-password >*, where:
    - **<*type*>** - is an integer value that indicates the type of hash algorithm used to generate the hash.
    - **<*salt*>** - The base64 encoding of the 96 bits used for salt (length – 16 bytes)
    - **<*encrypted-password*>** - The base64 encoding of the encrypted hash output (length - 86 bytes)
- **generate-password** - The device automatically generates a random based password suggestion. The user has an option to accept or reject the proposed password.
- **privilege** privilege-level —User account privilege level. If not specified the level is 1. (Range: 1–15).

Default Configuration

No user is defined.

Command Mode

Global Configuration mode

Usage Guidelines

The *unencrypted-password* must comply to password complexity requirements.

If the generate-password option is used, instead of entering a password the user will be presented with a randomly generated password suggestion. This suggestion will comply with all current password strength settings. The user will be given the choice to accept or reject the proposed password. If the user elects to accept the password, then this password will be added for the configured user name (in encrypted format) in the configuration file.

If the user rejects the password suggestion, the command will need to be entered again to configure this user.

The knowledge of the current password is required if the user requests to modify the password of the account used to login to the current session (while maintaining the current username). The user will be prompted to provide the current password in clear-text format. The password change will succeed only if the user correctly provided the current password.

The last level 15 user cannot be removed and cannot be a remote user

Example

Example 1- Sets an unencrypted password for user tom (level 15). It will be encrypted in the configuration file.

```
switchxxxxxx(config)# username tom password 1234Ab$5678
```

Example 2 - Sets a password for user jerry (level 15) that has already been encrypted. It will be copied to the configuration file just as it is entered. To use it, the user must know its unencrypted form.

```
switchxxxxxx(config)# username jerry privilege 15 encrypted
$15$TqKC13RgV/QJb2Ma$4JmeD7wgRGH2iwGKMM+g4M53uQxpOMlhkUN56UMAEUuMqhw0bsRH27zakc72hLxt/YhEknPA6LX7fTgqwZn6Vw==
```

Example 3 - The command in this example includes the generate-password key word. in this case the device will propose a randomly generated password to be used. in the example below the user selects to accept the proposed password.

```
switchxxxxxx(config)# username tom generate-password privilege 15
Generated password: aBgrT9!59Hq$
Accept generated password (y/n) [Y] y
"Configuration and password are added to device configuration. Please Note
password for future use."
```

Example 4 - The command in this example includes the generate-password key word. in this case the device will propose a randomly generated password to be used. in the example below the user selects to reject the proposed password.

```
switchxxxxxx(config)# username tom generate-password privilege 15
Generated password: aBgrT9!59Hq$
Accept generated password (y/n) [Y] n
"Auto generated password rejected by user. Password configuration is not added to
device configuration."
```

show users accounts

The **show users accounts** Privileged EXEC mode command displays information about the users local database.

Syntax

show users accounts

Command Mode

Privileged EXEC mode

Example

The following example displays information about the users local database:

```
switchxxxxxx# show users accounts

Username          Privilege         Password
--------          ---------         Expiry date
Bob               15                ----------
Robert            15                Jan 18 2005
Smith             15                Jan 19 2005
```

The following table describes the significant fields shown in the display:

Field	Description
Username	The user name.
Privilege	The user’s privilege level.
Password Expiry date	The user's password expiration date.

passwords complexity keyboard-pattern

Use the passwords complexity keyboard-pattern Global Configuration mode command to enable QWERTY keyboard pattern related restriction as part of password complexity settings.

Use the no form of the command to disable the QWERTY keyboard pattern related restriction.

Syntax

passwords complexity keyboard-pattern

no passwords complexity keyboard-pattern

Parameters

N/A

Default Configuration

Keyboard-pattern Password complexity setting is Disabled by default.

Command Mode

Global Configuration mode

User Guidelines

Use the **passwords complexity keyboard-pattern** command to define that a password cannot contain more than 3 consecutive characters on a QWERTY keyboard. The restriction applies only to letters and numbers on the keyboard and not to symbols. Both forward and reverse character sequences are prohibited.

The restriction is applied to the password defined using one of the following command:

- username
- enable password
- password

Example

The following example enables the key-board-pattern based password restriction.

```
switchxxxxxx(config)# passwords complexity keyboard-pattern
```

aaa accounting login start-stop

Use the **aaa accounting login start-stop** command in Global Configuration mode to enable accounting of device management sessions. Use the **no** form of this command to disable accounting.

Syntax

aaa accounting login start-stop group {**radius** | **tacacs+**}

no aaa accounting login start-stop

Parameters

- **group radius**—Uses a RADIUS server for accounting.
- **group tacacs+**—Uses a TACACS+ server for accounting.

Default Configuration

Disabled

Command Mode

Global Configuration mode

User Guidelines

This command enables the recording of device management sessions (Telnet, serial and WEB but not SNMP).

It records only users that were identified with a username (e.g. a user that was logged in with a line password is not recorded).

If accounting is activated, the device sends a “start”/“stop” messages to a RADIUS server when a user logs in / logs out respectively.

The device uses the configured priorities of the available RADIUS/TACACS+ servers in order to select the RADIUS/TACACS+ server.

The following table describes the supported RADIUS accounting attributes values, and in which messages they are sent by the switch.

Name	Start Message	Stop Message	Description
User-Name (1)	Yes	Yes	User’s identity.
NAS-IP-Address (4)	Yes	Yes	The switch IP address that is used for the session with the RADIUS server.
Class (25)	Yes	Yes	Arbitrary value is included in all accounting packets for a specific session.
Called-Station-ID (30)	Yes	Yes	The switch IP address that is used for the management session.

Name	Start Message	Stop Message	Description
Calling-Station-ID (31)	Yes	Yes	The user IP address.
Acct-Session-ID (44)	Yes	Yes	A unique accounting identifier.
Acct-Authentic (45)	Yes	Yes	Indicates how the supplicant was authenticated.
Acct-Session-Time (46)	No	Yes	Indicates how long the user was logged in.
Acct-Terminate-Cause (49)	No	Yes	Reports why the session was terminated.

The following table describes the supported TACACS+ accounting arguments and in which messages they are sent by the switch.

Name	Description	Start Message	Stop Message
task_id	A unique accounting session identifier.	Yes	Yes
user	username that is entered for login authentication	Yes	Yes
rem-addr	IP address of the user	Yes	Yes
elapsed-time	Indicates how long the user was logged in.	No	Yes
reason	Reports why the session was terminated.	No	Yes

Example

```
switchxxxxxx(config)# aaa accounting login start-stop group radius
```

aaa accounting dot1x

To enable accounting of 802.1x sessions, use the **aaa accounting dot1x** Global Configuration mode command. Use the **no** form of this command to disable accounting.

Syntax

aaa accounting dot1x start-stop group radius

no aaa accounting dot1x start-stop group radius

Default Configuration

Disabled

Command Mode

Global Configuration mode

User Guidelines

This command enables the recording of 802.1x sessions.

If accounting is activated, the device sends start/stop messages to a RADIUS server when a user logs in / logs out to the network, respectively. The device uses the configured priorities of the available RADIUS servers in order to select the RADIUS server.

If a new supplicant replaces an old supplicant (even if the port state remains authorized), the software sends a stop message for the old supplicant and a start message for the new supplicant.

In multiple sessions mode (dot1x multiple-hosts authentication), the software sends start/stop messages for each authenticated supplicant.

In multiple hosts mode (dot1x multiple-hosts), the software sends start/stop messages only for the supplicant that has been authenticated. The software does not send start/stop messages if the port is force-authorized.

The software does not send start/stop messages for hosts that are sending traffic on the guest VLAN or on the unauthenticated VLANs.

The following table describes the supported Radius accounting Attributes Values and when they are sent by the switch.

Name	Start	Stop	Description
User-Name (1)	Yes	Yes	Supplicant’s identity.
NAS-IP-Address (4)	Yes	Yes	The switch IP address that is used for the session with the RADIUS server.
NAS-Port (5)	Yes	Yes	The switch port from where the supplicant has logged in.

Name	**Start**	**Stop**	**Description**
Class (25)	Yes	Yes	The arbitrary value that is included in all accounting packets for a specific session.
Called-Station-ID (30)	Yes	Yes	The switch MAC address.
Calling-Station-ID (31)	Yes	Yes	The supplicant MAC address.
Acct-Session-ID (44)	Yes	Yes	A unique accounting identifier.
Acct-Authentic (45)	Yes	Yes	Indicates how the supplicant was authenticated.
Acct-Session-Time (46)	No	Yes	Indicates how long the supplicant was logged in.
Acct-Terminate-Cause (49)	No	Yes	Reports why the session was terminated.
Nas-Port-Type (61)	Yes	Yes	Indicates the supplicant physical port type.

Example

```
switchxxxxxx(config)# aaa accounting dot1x start-stop group radius
```

show accounting

The **show accounting** EXEC mode command displays information as to which type of accounting is enabled on the switch.

Syntax

show accounting

Command Mode

User EXEC mode

Example

The following example displays information about the accounting status.

```
switchxxxxxx# show accounting
Login: Radius
802.1x: Disabled
```

passwords complexity

Use the **passwords complexity** Global Configuration mode commands to control the minimum requirements from a password when password complexity is enabled. Use the **no** form of these commands to return to default.

Syntax

passwords complexity {**min-length** number} | {**min-classes** number} | {**no-repeat** number} | **not-current** | **not-username** | **not-manufacturer-name**

no passwords complexity min-length | **min-classes** | **no-repeat** | **not-current** | **not-username** | **not-manufacturer-name**

Parameters

- **min-length** number—Sets the minimal length of the password. (Range: 8–64)
- **min-classes** number—Sets the minimal character classes (uppercase letters, lowercase letters, numbers, and special characters available on a standard keyboard). (Range: 1–4)
- **no-repeat** number—Specifies the maximum number of characters in the new password that can be repeated consecutively. (Range: 1–16)
- **not-current**—Specifies that the new password cannot be the same as the current password.
- **not-username**—Specifies that the password cannot repeat or reverse the user name or any variant reached by changing the case of the characters.
- **not-manufacturer-name**—Specifies that the password cannot repeat or reverse the manufacturer's name or any variant reached by changing the case of the characters.

Default Configuration

The minimal length is 8.

The number of classes is 3.

The default for no-repeat is 3.

All the other controls are enabled by default.

Command Mode

Global Configuration mode

Example

The following example configures the minimal required password length to 10 characters.

```
switchxxxxxx(config)# passwords complexity min-length 10
```

passwords aging

Use the **passwords aging** Global Configuration mode command to enforce password aging. Use the **no** form of this command to return to default.

Syntax

passwords aging *days*

no passwords aging

Parameters

- ***days***—Specifies the number of days before a password change is forced. You can use 0 to disable aging. (Range: 0–365).

Default Configuration

Password aging is disabled by default.

Command Mode

Global Configuration mode

User Guidelines

The password aging setting is relevant to local database users, enable passwords and line passwords.

If password aging is enabled, when a user logs into the device within the 10 days preceding the password expiration date, a warning will be displayed alerting the user that the password will expire soon. The user is granted access to the device without changing the password. At this stage it is the user's responsibility to change the password before the expiration date.

Is the user logs into the device after the password expiration date, they are prompted to enter a new password and are not allowed access to the device management until a new password has been configured.

To disable password aging, use **passwords aging 0**.

Example

The following example configures the aging time to be 24 days.

```
witchxxxxxx(config)# passwords aging 24
```

password complexity history

The passwords complexity history Global Configuration mode command configures the number of password changes required before a password can be reused. Use the no form of this command to return to the default setting

Syntax

passwords complexity history *number*

no passwords complexity history

Parameters

number—Specifies the number of password changes required before a password can be reused. (Range: 3–12).

Default Configuration

By default the number of passwords changes that are needed before password reuse is 12.

Command Mode

Global configuration mode.

User Guidelines

The setting is relevant to local users' passwords, line passwords and enable passwords.

The local user history is maintained for users up to the number of local users supported on the device.

Password history is not checked during a configuration download.

The password history is kept even if the password history check is disabled.

Example

The following example sets the number of password changes required before a password can be reused to 10.

```
switchxxxxxx(config)# passwords complexity history 10
```

aaa login-history file

The aaa login-history file Global Configuration mode command enables writing to the login history file. Use the no form of this command to disable writing to the login history file.

Syntax

aaa login-history file

no aaa login-history file

Default Configuration

Writing to the login history file is enabled.

Command Mode

Global Configuration mode.

User Guidelines

The login history is stored in the device internal buffer.

Example

The following example enables writing to the login history file.

```
switchxxxxxx(config)# aaa login-history file
```

show passwords configuration

The **show passwords configuration** Privileged EXEC mode command displays information about the password management configuration.

Syntax

show passwords configuration

Parameters

N/A

Default Configuration

N/A

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# show passwords configuration
Passwords aging is enabled with aging time 180 days.
Passwords history is enabled, the number of previous passwords to check is 12
Passwords complexity is enabled with the following attributes:
 Minimal length: 8 characters
 Minimal classes: 3
 Maximum consecutive same characters: 3
 Password cannot include more than 2 sequential numbers or characters
Password cannot contain the username, manufacturer name or product name
Password must be different from current password
Password cannot contain commonly used passwords or known breached passwords
```

show users login-history

The show users **login-history** Privileged EXEC mode command displays information about the user’s login history.

Syntax

show users login-history [**username** name]

Parameters

- name—Name of the user. (Range: 1–20 characters).

Default Configuration

N/A

Command Mode

Privileged EXEC mode.

User Guidelines

This command displays information on users authenticated using the local AAA database and not on users authenticated using remote AAA servers like Radius and TACACS.

Example

The following example displays information about the users’ login history.

Example 1 - The following example shows how to block all login requests for 180 seconds if 18 failed login attempts are exceeded within 180 seconds:

```
switchxxxxxx# show users login-history
File save: Enabled.
Login Time              Username  Protocol    Location
--------------------
Jan 18 2004 23:58:17    Robert    HTTP        172.16.1.8
Jan 19 2004 07:59:23    Robert    HTTP        172.16.1.8
Jan 19 2004 08:23:48    Bob       Serieal
Jan 19 2004 08:29:29    Robert    HTTP        172.16.1.8
Jan 19 2004 08:42:31    John      SSH         172.16.0.1
Jan 19 2004 08:49:52    Betty     Telnet      172.16.1.7
```