1 Password Policy Commands

Command	Function
password policy life-cycle	Configure a password lifecycle.
password policy min-size	Configure the minimum password length.
password policy no-repeat-times	Prevent repeated use of passwords that are configured in the latest specified number of times.
password policy strong	Enable strong password detection.
password policy forced-password-modify	Enable forcible weak password change.
password policy printable-character-check	Enable the special character detection function.
service password-encryption	Enable encrypted password storage.
show password policy	Display configured password security policies.

1.1 password policy life-cycle

Function

Run the **password policy life-cycle** command to configure a password lifecycle.

Run the **no** form of this command to remove this configuration.

No password lifecycle is configured by default.

Syntax

password policy life-cycle *life-cycle*

no password policy life-cycle

Parameter Description

life-cycle: Password lifecycle, in days. The value range is from 1 to 65535.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

The password lifecycle defines the validity time of a password. If a user enters a password that has already expired during login, the system gives a prompt, indicating that the password has expired, and asks the user to reset the password.

The password lifecycle is valid only for global passwords (configured by running the **enable password** and **enable secret** commands) and local user passwords (configured by running the **username** command). It is invalid for passwords in line configuration mode.

The password lifecycle is affected when the system time is modified.

Examples

The following example sets the password lifecycle to 90 days.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# password policy life-cycle 90
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **enable password** (Basic Configuration/Basic Management)
- **enable secret** (Basic Configuration/Basic Management)
- **Username** (Basic Configuration/Basic Management)

1.2 password policy min-size

Function

Run the **password policy min-size** command to configure the minimum password length.

Run the **no** form of this command to remove this configuration.

The minimum password length is **8** by default.

Syntax

password policy min-size *min-size*

no password policy min-size

Parameter Description

min-size: Minimum password length. The value range is from 1 to 31.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

The minimum password length is used to limit the length of user passwords. If the password entered by a user is shorter than the minimum password length, the system displays an error prompt, asking the user to specify another password of an appropriate length.

Examples

The following example sets the minimum password length to 8.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# password policy min-size 8
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.3 password policy no-repeat-times

Function

Run the **password policy no-repeat-times** command to prevent repeated use of passwords that are configured in the latest specified number of times.

Run the **no** form of this command to remove this configuration.

Repeated password use is allowed by default.

Syntax

password policy no-repeat-times *no-repeat-times*

no password policy no-repeat-times

Parameter Description

No-repeat-times: Number of times in which configured passwords cannot be repeatedly used. The value range is from 1 to 31.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

The repeated password use prevention function prevents users from using historically configured passwords as new passwords. The system records passwords used by a user to a historical password list. If a newly configured password is within the list, the system gives a prompt and asks the user to specify another password. The maximum number of records in the password list can be manually configured. When the number of records in the password list reaches the limit, a new password record will overwrite the earliest password record.

The repeated password use prevention function is valid only for global passwords (configured by running the **enable password** and **enable secret** commands) and local user passwords (configured by running the **username** command). It is invalid for passwords in line configuration mode.

Examples

The following example enables repeated password use prevention function to disallow the use of historical passwords configured in the latest five times.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# password policy no-repeat-times 5
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **enable password** (Basic Configuration/Basic Management)
- **enable secret** (Basic Configuration/Basic Management)
- **username** (Basic Configuration/Basic Management)

1.4 password policy strong

Function

Run the **password policy strong** command to enable strong password detection.

Run the **no** form of this command to disable this feature.

The strong password detection function is enabled by default.

Syntax

password policy strong

no password policy strong

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

Strong password detection is used to detect the complexity of a password and prevent password crackdown due to low complexity. The strong password detection function will send an alarm in the following scenarios:

- The password is the same as the corresponding account.
- The password contains only digits.
- The password contains only uppercase letters.
- The password contains only lowercase letters.

Examples

The following example enables the strong password detection function.

```
Hostname> enable
Hostname# configure terminal
```

```
Hostname(config)# password policy strong
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.5 password policy forced-password-modify

Function

Run the **password policy forced-password-modify** command to enable forcible weak password change.

Run the **no** form of this command to disable this feature.

Forcible weak password change is disabled by default.

Syntax

password policy forced-password-modify

no password policy forced-password-modify

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

The forcible weak password change function is used together with another password policy (such as the minimum password length or strong password detection).

After the forcible weak password change function is enabled, a warning prompt will be displayed if a user uses a weak password (containing less than 8 bytes or only digits, uppercase letters, or lowercase letters) during login or configuration. If both the forcible weak password change function and another password policy are enabled, the password will continue to be checked according to the other password policy during user login. If the password does not meet requirements of the other password policy, a prompt for changing the password will be displayed. The user is allowed to log in only after the new password meets requirements of the password policy.

The forcible weak password change function is valid only for global passwords (configured by running the **enable password** and **enable secret** commands) and local user passwords (configured by running the **username** command). It is invalid for passwords in line configuration mode.

Examples

The following example enables forcible weak password change.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# password policy forced-password-modify
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **enable password** (Basic Configuration/Basic Management)
- **enable secret** (Basic Configuration/Basic Management)
- **username** (Basic Configuration/Basic Management)

1.6 password policy printable-character-check

Function

Run the **password policy printable-character-check** command to enable the special character detection function.

Run the **no** form of this command to disable this feature.

Special character detection is disabled by default.

Syntax

password policy printable-character-check

no password policy printable-character-check

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

After strong password detection and special character detection are configured, passwords that contain only special characters are invalid and cannot be configured successfully. Special characters include space, tilde (~), backtick (`), exclamation mark (!), at sign (@), number sign (#), dollar sign ($), percent sign (%), caret (^), ampersand (&), asterisk (*), brackets (()), underscore (_), plus sign (+), minus sign (–), equal sign (=), braces ({}), vertical bar (|), square brackets ([]), backslash (\), colon (:), quotation mark ("), semicolon (;), apostrophe ('), angle brackets (<>), comma (,), period (.), and slash (/).

Examples

The following example enables special character detection.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# password policy strong
Hostname(config)# password policy printable-character-check
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.7 service password-encryption

Function

Run the **service password-encryption** command to enable encrypted password storage.

Run the **no** form of this command to disable this feature.

Encrypted password storage is enabled by default.

Syntax

service password-encryption

no service password-encryption

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

When encrypted password storage is disabled, all passwords used in the configuration process are displayed and stored in plaintext format unless the passwords are configured in ciphertext format. For security purposes, encrypted password storage should be enabled. When encrypted password storage is enabled and the **show running-config** command is run to display configurations or the **write** command is run to save configuration files, passwords configured by users are displayed in ciphertext format. If encrypted password storage is disabled again, passwords displayed in ciphertext format will not be restored to the plaintext format.

Examples

The following example enables encrypted password storage.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# service password-encryption
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.8 show password policy

Function

Run the **show password policy** command to display configured password security policies.

Syntax

show password policy

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

This command is used to display password security policies configured on a device.

Examples

The following example displays configured password security policies.

```
Hostname> enable
Hostname# show password policy
Global password policy configurations:
 Password encryption:                 Enabled
 Password strong-check:               Enabled
Password secret-dictionary-check:    Enabled
 Password min-size:                   Enabled (6 characters)
 Password life-cycle:                 Enabled (90 days)
 Password no-repeat-times:            Enabled (max history record: 5)
```

Table 1-1Output Fields of the show password policy Command

Field	Description
Password encryption	Whether passwords are stored in encrypted mode
Password strong-check	Whether strong password detection is enabled
Password secret-dictionary-check	Whether password dictionary check is enabled
Password min-size	Minimum password length
Password life-cycle	Password lifecycle
Password no-repeat-times	Number of latest configured passwords that cannot be used repeatedly

Notifications

N/A

Platform Description

N/A

Related Commands

N/A