Contents

1 Configuring Password Policies

1.1 Introduction

1.1.1 Overview

A password policy provides the password detection function for applications that need to configure accounts and passwords (for example, creating local users) on a device to ensure that users use passwords that meet security specifications and prevent password crackdown due to low password complexity.

1.2 Restrictions and Guidelines

The password lifecycle, repeated password use prevention, and forcible weak password change functions take effect only to global passwords (**enable password** and **enable secret**) and local user passwords (**username** *username* **password** *password*) and are invalid to passwords in line configuration mode.

1.3 Configuration Task Summary

All the configuration tasks below are optional. Select the configuration tasks as required.

(1) Configuring the Minimum Password Length

(2) Enabling Strong Password Detection

(3) Enabling Forcible Weak Password Change

(4) Configuring a Password Lifecycle

(5) Configuring Repeated Password Use Prevention

(6) Configuring Encrypted Password Storage

(7) Enabling Special Character Detection

1.4 Configuring the Minimum Password Length

1.4.1 Overview

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.

1.4.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the minimum password length.

password policy min-size *min-size*

No minimum length is configured for passwords by default.

1.5 Enabling Strong Password Detection

1.5.1 Overview

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 and disallow the user to configure the password 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.

1.5.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable the strong password detection function.

password policy strong

The strong password detection function is enabled by default.

1.6 Enabling Forcible Weak Password Change

1.6.1 Overview

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.

1.6.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable forcible weak password change.

password policy forced-password-modify

Forcible weak password change is disabled by default.

1.7 Configuring a Password Lifecycle

1.7.1 Overview

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.

1.7.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the password lifecycle.

password policy life-cycle *life-cycle*

No password lifecycle is configured by default.

1.8 Configuring Repeated Password Use Prevention

1.8.1 Overview

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.

1.8.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Prevent repeated use of passwords configured in the latest specified number of times.

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

Repeated password use is allowed by default.

1.9 Configuring Encrypted Password Storage

1.9.1 Overview

Encrypted password storage is used to store passwords after encryption.

When administrators run the **show running-config** command to display configurations or run the **write** command to save configuration files, passwords configured by users are displayed in ciphertext format if encrypted password storage is enabled and displayed in plaintext format if encrypted password storage is disabled.

1.9.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable encrypted password storage.

service password-encryption

Encrypted password storage is disabled by default.

1.10 Enabling Special Character Detection

1.10.1 Overview

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 (/).

1.10.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable special character detection.

password policy printable-character-check

Special character detection is disabled by default.

1.11 Monitoring

Run the **show** commands to check the running status of a configured function to verify the configuration effect.

Table 1-1 Monitoring

Command	Purpose
show password policy	Displays configured password security policies.

1.12 Configuration Examples

1.12.1 Requirements

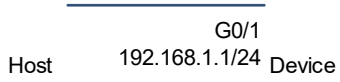
To ensure password complexity, you can configure password policies on a device to limit users' passwords.

Password security requirements are as follows:

- A password must be a string of at least eight characters.
- A password cannot be the same as the account.
- A password cannot contain only digits, uppercase letters, or lowercase letters.
- A password is valid for 90 days.
- Passwords must be stored in encrypted mode.
- A password cannot be the same as historical passwords configured in the latest three times.

1.12.2 Topology

Figure 1-1 Configuring Password Policies



1.12.3 Notes

- Set the minimum password length to 8.
- Enable strong password detection.
- Set the password lifecycle to 90 days.
- Enable encrypted password storage.
- Configure repeated password use prevention to disable the use of historical passwords configured in the latest three times.

1.12.4 Procedure

Enter the global configuration mode.

```
Device> enable
```

```
Device# configure terminal
```

Set the minimum password length to 8.

```
Device(config)# password policy min-size 8
```

Enable strong password detection.

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

Set the password lifecycle to 90 days.

```
Device(config)# password policy life-cycle 90
```

Enable encrypted password storage.

```
Device(config)# service password-encryption
```

Configure repeated password use prevention to disable the use of historical passwords configured in the latest three times.

```
Device(config)# password policy no-repeat-times 3
```

1.12.5 Verification

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

```
Device> enable
Device# show password policy
Global password policy configurations:
 Password encryption:                 Enabled
 Password strong-check:               Enabled
 Password forced-password-modify:     Disabled
 Password min-size:                   Enabled (8 characters)
 Password life-cycle:                 Enabled (90 days)
 Password no-repeat-times:            Enabled (max history record: 3)
 Password printable-character-check:  Disabled
```

1.12.6 Configuration Files

```
!
password policy life-cycle 90
password policy no-repeat-times 3
password policy min-size 8
password policy strong
service password-encryption
```