Contents

Password control commands

The device supports the FIPS mode that complies with NIST FIPS 140-2 requirements. Support for features, commands, and parameters might differ in FIPS mode and non-FIPS mode. For more information about FIPS mode, see *Security Configuration Guide*.

display password-control

Use **display password-control** to display password control configuration.

Syntax

display password-control [**super**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

super: Displays the password control information for the super passwords. If you do not specify this keyword, the command displays the global password control configuration.

Examples

# Display the global password control configuration.

```
<Sysname> display password-control
 Global password control configurations:
 Password control:                     Disabled
 Password aging:                       Enabled (90 days)
 Password length:                      Enabled (10 characters)
 Password composition:                 Enabled (1 types, 1 characters per type)
 Password history:                     Enabled (max history records:4)
 Early notice on password expiration:  7 days
 Maximum login attempts:               3
 Action for exceeding login attempts:  Lock user for 1 minutes
 Minimum interval between two updates: 24 hours
 User account idle time:               90 days
 Logins with aged password:            3 times in 30 days
 Password complexity:                  Disabled (username checking)
                                       Disabled (repeated characters checking)
```

# Display the password control configuration for super passwords.

```
<Sysname> display password-control super
 Super password control configurations:
 Password aging:                       Enabled (90 days)
 Password length:                      Enabled (10 characters)
 Password composition:                 Enabled (1 types, 1 characters per type)
```

Table 1 Command output

Field	Description
Password control	Whether the password control feature is enabled.
Password aging	Whether password expiration is enabled and, if enabled, the aging time.
Password length	Whether the minimum password length restriction feature is enabled and, if enabled, the setting.
Password composition	Whether the password composition restriction feature is enabled and, if enabled, the settings.
Password history	Whether the password history feature is enabled and, if enabled, the setting.
Early notice on password expiration	Number of days during which the user is notified of the pending password expiration.
Maximum login attempts	Allowed maximum number of consecutive failed login attempts for FTP and VTY users.
Action for exceeding login attempts	Action to be taken after a user fails to log in after the specified number of attempts.
Minimum interval between two updates	Minimum password update interval.
Logins with aged password	Number of times and maximum number of days a user can log in using an expired password.
Password complexity	Whether the following password complexity checking is enabled: • **username checking**—Checks whether a password contains the username or the reverse of the username. • **repeated characters checking**—Checks whether a password contains any character that appears consecutively three or more times.

display password-control blacklist

Use **display password-control blacklist** to display password control blacklist information.

Syntax

display password-control blacklist [**user-name** *user-name* | **ip** *ipv4-address* | **ipv6** *ipv6-address*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

user-name *user-name*: Specifies a user by its username, a case-sensitive string of 1 to 55 characters.

ip *ipv4-address*: Specifies the IPv4 address of a user.

ipv6 *ipv6-address*: Specifies the IPv6 address of a user.

Usage guidelines

If you do not specify any parameters, this command displays information about all users in the password control blacklist.

The users' IP addresses and user accounts are added to the password control blacklist when the users fail authentication. You can use this command to view information about blacklisted FTP, Web, and virtual terminal line (VTY) users.

Users accessing the system through the console interface are not blacklisted for the following reasons:

- The system is unable to obtain the IP addresses of these users.
- These users are privileged and, therefore, relatively secure to the system.

Examples

# Display password control blacklist information.

```
<Sysname> display password-control blacklist
 Blacklist items matched: 2.
 Username                     IP address          Login failures   Lock flag
 abcd                         169::168:34:1       4                lock
 admin                        192.168.34.1        1                unlock
```

Table 2 Command output

Field	Description
Blacklist items matched	Number of blacklisted users.
IP address	IP address of the user.
Login failures	Number of login failures.
Lock flag	Whether the user account is locked for the user: • **unlock**—Not limited. • **lock**—Disabled temporarily or permanently, depending on the **password-control login-attempt** command.

password-control { aging | composition | history | length } enable

Use **password-control { aging | composition | history | length } enable** to enable the password expiration, composition restriction, history, or minimum length restriction feature.

Use **undo password-control { aging | composition | history | length } enable** to disable a password control feature.

Syntax

password-control { aging | composition | history | length } enable

undo password-control { aging | composition | history | length } enable

Default

The password control features (**aging**, **composition**, **history**, and **length**) are all enabled.

Views

System view

Predefined user roles

network-admin

Parameters

aging: Enables the password expiration feature.

composition: Enables the password composition restriction feature.

history: Enables the password history feature.

length: Enables the minimum password length restriction feature.

Usage guidelines

For a specific password control feature to take effect, make sure the global password control and the specific password control feature are both enabled. For example, if the global password control and the minimum length restriction feature are not enabled, the **password-control length** command does not take effect.

The system stops recording history passwords after you execute the **undo password-control history enable** command, but it does not delete the prior records.

If the global password control feature is enabled but the minimum password length restriction feature is disabled, the following rules apply:

- In non-FIPS mode, a password must contain a minimum of 4 characters and a minimum of 4 characters must be different.
- In FIPS mode, a password must contain a minimum of 15 characters and a minimum of 4 characters must be different.

Examples

# Enable the password control feature globally.

```
<Sysname> system-view
[Sysname] password-control enable
```

# Enable the password composition restriction feature.

```
[Sysname] password-control composition enable
```

# Enable the password expiration feature.

```
[Sysname] password-control aging enable
```

# Enable the minimum password length restriction feature.

```
[Sysname] password-control length enable
```

# Enable the password history feature.

```
[Sysname] password-control history enable
```

Related commands

display password-control

password-control enable

password-control aging

Use **password-control aging** to set the password aging time.

Use **undo password-control aging** to restore the default.

Syntax

password-control aging *aging-time*

undo password-control aging

Default

A password expires after 90 days. The password aging time for a user group equals the global setting. The password aging time for a local user equals that of the user group to which the local user belongs.

Views

System view

User group view

Local user view

Predefined user roles

network-admin

Parameters

aging-time: Specifies the password aging time in days, in the range of 1 to 365.

Usage guidelines

The aging time depends on the view:

- The time in system view has global significance and applies to all user groups.
- The time in user group view applies to all local users in the user group.
- The time in local user view applies only to the local user.

A password aging time with a smaller application scope has higher priority. The system prefers to use the password aging time in local user view for a local user.

- If no password aging time is configured for the local user, the system uses the password aging time for the user group to which the local user belongs.
- If no password aging time is configured for the user group, the system uses the global password aging time.

Examples

# Globally set the passwords to expire after 80 days.

```
<Sysname> system-view
[Sysname] password-control aging 80
```

# Set the passwords for user group **test** to expire after 90 days.

```
[Sysname] user-group test
[Sysname-ugroup-test] password-control aging 90
[Sysname-ugroup-test] quit
```

# Set the password for device management user **abc** to expire after 100 days.

```
[Sysname] local-user abc class manage
[Sysname-luser-manage-abc] password-control aging 100
```

Related commands

display local-user

display password-control

display user-group

password-control aging enable

password-control alert-before-expire

Use **password-control alert-before-expire** to set the number of days before a user's password expires during which the user is notified of the pending password expiration.

Use **undo password-control alert-before-expire** to restore the default.

Syntax

password-control alert-before-expire *alert-time*

undo password-control alert-before-expire

Default

The default is 7 days.

Views

System view

Predefined user roles

network-admin

Parameters

alert-time: Specifies the number of days before a user password expires during which the user is notified of the pending password expiration. The value range is 1 to 30.

Usage guidelines

This command is effective only for non-FTP users. FTP users can only have their passwords changed by the administrator.

Examples

# Configure the device to notify a user about pending password expiration 10 days before the user's password expires.

```
<Sysname> system-view
[Sysname] password-control alert-before-expire 10
```

Related commands

display password-control

password-control complexity

Use **password-control complexity** to configure the password complexity checking policy.

Use **undo password-control complexity** to remove a password complexity checking item.

Syntax

password-control complexity { **same-character** | **user-name** } **check**

undo password-control complexity { **same-character** | **user-name** } **check**

Default

The global password complexity checking policy is that both username checking and repeated character checking are disabled. The password complexity checking policy for a user group equals the global setting. The password complexity checking policy for a local user equals that of the user group to which the local user belongs.

Views

System view

User group view

Local user view

Predefined user roles

network-admin

Parameters

`same-character`: Refuses a password that contains a minimum of three consecutive identical characters. For example, the password **aaabc** is not complex enough.

`user-name`: Refuses a password that contains the username or the reverse of the username. For example, if the username is **123**, a password such as **abc123** or **321df** is not complex enough.

Usage guidelines

The password complexity checking policy depends on the view:

- The policy in system view has global significance and applies to all user groups.
- The policy in user group view applies to all local users in the user group.
- The policy in local user view applies only to the local user.

A password complexity checking policy with a smaller application scope has higher priority. The system prefers to use the password complexity checking policy in local user view for a local user.

- If no policy is configured for the local user, the system uses the policy for the user group to which the local user belongs.
- If no policy is configured for the user group, the system uses the global policy.

You can enable both username checking and repeated character checking.

Examples

# Configure the password complexity checking policy, refusing any password that contains the username or the reverse of the username.

```
<Sysname> system-view
[Sysname] password-control complexity user-name check
```

Related commands

`display local-user`

`display password-control`

`display user-group`

password-control composition

Use **`password-control composition`** to configure the password composition policy.

Use **`undo password-control composition`** to restore the default.

Syntax

`password-control composition type-number` *`type-number`* [**`type-length`** *`type-length`*]

`undo password-control composition`

Default

In non-FIPS mode:

The password using the global composition policy must contain a minimum of one character type and a minimum of one character for each type.

In FIPS mode:

The password using the global composition policy must contain a minimum of four character types and a minimum of one character for each type.

In both non-FIPS and FIPS modes:

The password composition policy for a user group is the same as the global policy. The password composition policy for a local user is the same as that of the user group to which the local user belongs.

Views

System view

User group view

Local user view

Predefined user roles

network-admin

Parameters

`type-number` *`type-number`*: Specifies the minimum number of character types that a password must contain. The value range for the *`type-number`* argument is 1 to 4 in non-FIPS mode and fixed at 4 in FIPS mode.

`type-length` *`type-length`*: Specifies the minimum number of characters that are from each type in the password. The value range for the *`type-length`* argument is 1 to 63 in non-FIPS mode, and 1 to 15 in FIPS mode.

Usage guidelines

The password composition policy depends on the view:

- The policy in system view has global significance and applies to all user groups.
- The policy in user group view applies to all local users in the user group.
- The policy in local user view applies only to the local user.

A password composition policy with a smaller application scope has higher priority. The system prefers to use the password composition policy in local user view for a local user.

- If no policy is configured for the local user, the system uses the policy for the user group to which the local user belongs.
- If no policy is configured for the user group, the system uses the global policy.

The product of the minimum number of character types and minimum number of characters for each type must be smaller than the maximum length of passwords.

Examples

# Specify that all passwords must each contain a minimum of four character types and a minimum of five characters for each type.

```
<Sysname> system-view
[Sysname] password-control composition type-number 4 type-length 5
```

# Specify that passwords in user group **test** must contain a minimum of four character types and a minimum of five characters for each type.

```
[Sysname] user-group test
[Sysname-ugroup-test] password-control composition type-number 4 type-length 5
[Sysname-ugroup-test] quit
```

# Specify that the password of device management user **abc** must contain a minimum of four character types and a minimum of five characters for each type.

```
[Sysname] local-user abc class manage
```

```
[Sysname-luser-manage-abc] password-control composition type-number 4 type-length 5
```

Related commands

display local-user

display password-control

display user-group

password-control composition enable

password-control enable

Use **password-control enable** to enable the password control feature globally.

Use **undo password-control enable** to disable the password control feature globally.

Syntax

password-control enable

undo password-control enable

Default

In non-FIPS mode:

The password control feature is disabled globally.

In FIPS mode:

The password control feature is enabled globally and cannot be disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

A specific password control feature takes effect only after the global password control feature is enabled.

After the global password control feature is enabled, you cannot display the password and super password configurations for device management users by using the corresponding **display** commands. The configuration for network access user passwords can be displayed. The first password configured for device management users must contain a minimum of four different characters.

Examples

# Enable the password control feature globally.

```
<Sysname> system-view
[Sysname] password-control enable
```

Related commands

display password-control

password-control { **aging** | **composition** | **history** | **length** } **enable**

password-control expired-user-login

Use **password-control expired-user-login** to set the maximum number of days and maximum number of times that a user can log in after the password expires.

Use **undo password-control expired-user-login** to restore the defaults.

Syntax

password-control expired-user-login delay *delay* **times** *times*

undo password-control expired-user-login

Default

A user can use an expired password to log in three times within 30 days after the password expires. If all the three attempts fail or the user makes a login attempt after 30 days, the system prompts the user to set a new password.

Views

System view

Predefined user roles

network-admin

Parameters

delay *delay*: Specifies the maximum number of days during which a user can log in using an expired password. The value range for the *delay* argument is 1 to 90.

times *times*: Specifies the maximum number of times a user can log in after the password expires. The value range is 0 to 10. For a user to set a new password at the system prompt immediately after the password expires, set the value to 0.

Usage guidelines

This command is effective only on non-FTP login users. An FTP user cannot continue to log in after its password expires.

Examples

# Allow a user to log in five times within 60 days after the password expires.

```
<Sysname> system-view
[Sysname] password-control expired-user-login delay 60 times 5
```

Related commands

display password-control

password-control history

Use **password-control history** to set the maximum number of history password records for each user.

Use **undo password-control history** to restore the default.

Syntax

password-control history *max-record-number*

undo password-control history

Default

The maximum number of history password records for each user is 4.

Views

System view

Predefined user roles

network-admin

Parameters

max-record-number: Specifies the maximum number of history password records for each user. The value range is 2 to 15.

Usage guidelines

When the number of history password records reaches the maximum number, the subsequent history record overwrites the earliest one.

The system stops recording passwords after you execute the **undo password-control history enable** command, but it does not delete the prior records.

To delete the existing records, use one of the following methods:

- Use the **undo password-control enable** command to disable the password control feature globally.
- Use the **reset password-control history-record** command to clear the passwords manually.

Examples

# Set the maximum number of history password records for each user to 10.

```
<Sysname> system-view
[Sysname] password-control history 10
```

Related commands

display password-control

password-control history enable

reset password-control blacklist

password-control length

Use **password-control length** to set the minimum password length.

Use **undo password-control length** to restore the default.

Syntax

password-control length *length*

undo password-control length

Default

In non-FIPS mode:

The global minimum password length is 10 characters.

In FIPS mode:

The global minimum password length is 15 characters.

In both non-FIPS and FIPS modes:

The minimum password length for a user group equals the global setting. The minimum password length for a local user equals that of the user group to which the local user belongs.

Views

System view

User group view

Local user view

Predefined user roles

network-admin

Parameters

length: Specifies the minimum password length in characters. The value range for this argument is 4 to 32 in non-FIPS mode, and 15 to 32 in FIPS mode.

Usage guidelines

The minimum length setting depends on the view:

- The setting in system view has global significance and applies to all user groups.
- The setting in user group view applies to all local users in the user group.
- The setting in local user view applies only to the local user.

A minimum password length with a smaller application scope has higher priority. The system prefers to use the minimum password length in local user view for a local user.

- If no minimum password length is configured for the local user, the system uses the minimum password length for the user group to which the local user belongs.
- If no minimum password length is configured for the user group, the system uses the global minimum password length.

Examples

# Set the global minimum password length to 16 characters.

```
<Sysname> system-view
[Sysname] password-control length 16
```

# Set the minimum password length to 16 characters for the user group **test**.

```
[Sysname] user-group test
[Sysname-ugroup-test] password-control length 16
[Sysname-ugroup-test] quit
```

# Set the minimum password length to 16 characters for the device management user **abc**.

```
[Sysname] local-user abc class manage
[Sysname-luser-manage-abc] password-control length 16
```

Related commands

display local-user

display password-control

display user-group

password-control length enable

password-control login idle-time

Use **password-control login idle-time** to set the maximum account idle time.

Use **undo password-control login idle-time** to restore the default.

Syntax

password-control login idle-time *idle-time*

undo password-control login idle-time

Default

The maximum account idle time is 90 days.

Views

System view

Predefined user roles

network-admin

Parameters

idle-time: Specifies the maximum account idle time in days. The value range is 0 to 365. 0 means no restriction for account idle time.

Usage guidelines

If a user account is idle for this period of time, the account becomes invalid and can no longer be used to log in to the device.

The account might become invalid if the system time changes after your last successful login. You cannot use an invalid account to log in. To disable the account idle time restriction, set the idle time value to 0.

Examples

# Set the maximum account idle time to 30 days.

```
<Sysname> system-view
[Sysname] password-control login idle-time 30
```

Related commands

display password-control

password-control login-attempt

Use **password-control login-attempt** to configure the login attempt limit. The settings include the maximum number of consecutive login failures and the action to be taken when the maximum number is reached.

Use **undo password-control login-attempt** to restore the default.

Syntax

password-control login-attempt *login-times* [**exceed** { **lock** | **lock-time** *time* | **unlock** }]

undo password-control login-attempt

Default

The global login-attempt settings:

- The maximum number of consecutive login failures is 3.
- The locking period is 1 minute.

The login-attempt settings for a user group equal the global settings.

The login-attempt settings for a local user equal those for the user group to which the local user belongs.

Views

System view

User group view

Local user view

Predefined user roles

network-admin

Parameters

login-times: Specifies the maximum number of consecutive login failures. The value range is 2 to 10.

exceed: Specifies an action to be taken for the user who fails to log in after making the maximum number of attempts.

- **lock**: Disables the user account permanently.
- **lock-time** *time*: Disables the user account for a period of time. The user can uses this user account when the timer expires. The value range for the *time* argument is 1 to 360 minutes.
- **unlock**: Allows the user account to continue using this account to perform login attempts.

Usage guidelines

The login-attempt policy depends on the view:

- The policy in system view has global significance and applies to all user groups.
- The policy in user group view applies to all local users in the user group.
- The policy in local user view applies only to the local user.

A login-attempt policy with a smaller application scope has higher priority. The system prefers to use the login-attempt policy in local user view for a local user.

- If no policy is configured for the local user, the system uses the policy for the user group to which the local user belongs.
- If no policy is configured for the user group, the system uses the global policy.

If an FTP or VTY user fails to log in, the system adds the user account and the user's IP address to the password control blacklist. When the maximum number of consecutive login failures is reached, the login attempt limit feature is triggered.

Whether a blacklisted user and user account are locked depends on the locking setting:

- If a user account is permanently locked for a user, the user cannot use this account unless this account is removed from the password control blacklist. To remove the user account, use the **reset password-control blacklist** command.
- To use a temporarily locked user account, the user can perform either of the following tasks:
  - Wait until the locking timer expires.
  - Remove the user account from the password control blacklist.
- If the user account and the user are blacklisted but not locked, the user can continue using this account to log in. The account and the user's IP address are removed from the password control blacklist when the user uses the account to successfully log in to the device.

NOTE:

This account is locked only for this user. Other users can still use this account, and the blacklisted user can use other user accounts.

The **password-control login-attempt** command takes effect immediately after being executed, and can affect the users already in the password control blacklist.

Examples

# Allow a maximum of four consecutive login failures on a user account, and disable the user account if the limit is reached.

```
<Sysname> system-view
[Sysname] password-control login-attempt 4 exceed lock
```

# Use the user account **test** to log in to the device, and enter incorrect password for four times.

# Display the password control blacklist. The output shows that the user account is on the blacklist, and its status is **lock**.

```
[Sysname] display password-control blacklist

 Username: test
    IP: 192.168.44.1        Login failures: 4      Lock flag: lock

 Blacklist items matched: 1.
```

# Verify that the user at 192.168.44.1 cannot use this user account to log in.

# Allow a maximum of two consecutive login failures on a user account, and disable the account for 3 minutes if the limit is reached.

```
<Sysname> system-view
[Sysname] password-control login-attempt 2 exceed lock-time 3
```

# Use the user account **test** to log in to the device, and enter incorrect password for two attempts.

# Display the password control blacklist. The output shows that the user account is on the blacklist and its status is **lock**.

```
[Sysname] display password-control blacklist

 Username: test
    IP: 192.168.44.1        Login failures: 2      Lock flag: lock

 Blacklist items matched: 1.
```

# Verify that after 3 minutes, the user account is removed from the password control blacklist and the user at 192.168.44.1 can use this account.

Related commands

display local-user

display password-control

display password-control blacklist

display user-group

reset password-control blacklist

password-control super aging

Use **password-control super aging** to set the aging time for super passwords.

Use **undo password-control super aging** to restore the default.

Syntax

password-control super aging *aging-time*

undo password-control super aging

Default

A super password expires after 90 days.

Views

System view

Predefined user roles

network-admin

Parameters

aging-time: Specifies the super password aging time in days, in the range of 1 to 365.

Examples

# Set the super passwords to expire after 10 days.

```
<Sysname> system-view
[Sysname] password-control super aging 10
```

Related commands

display password-control

password-control aging

password-control super composition

Use **password-control super composition** to configure the composition policy for super passwords.

Use **undo password-control super composition** to restore the default.

Syntax

password-control super composition type-number *type-number* [**type-length** *type-length*]

undo password-control super composition

Default

In non-FIPS mode:

A super password must contain a minimum of one character type and a minimum of one character for each type.

In FIPS mode:

A super password must contain a minimum of four character types and a minimum of one character for each type.

Views

System view

Predefined user roles

network-admin

Parameters

type-number *type-number*: Specifies the minimum number of character types that a super password must contain. The value range for the *type-number* argument is 1 to 4 in non-FIPS mode and fixed at 4 in FIPS mode.

type-length *type-length*: Specifies the minimum number of characters that are from each character type. The value range for the *type-length* argument is 1 to 63 in non-FIPS mode, and 1 to 15 in FIPS mode.

Usage guidelines

The product of the minimum number of character types and minimum number of characters for each type must be smaller than the maximum length of the super password.

Examples

# Specify that a super password must contain a minimum of four character types and a minimum of five characters for each type.

```
<Sysname> system-view
[Sysname] password-control super composition type-number 4 type-length 5
```

Related commands

display password-control

password-control composition

password-control super length

Use **password-control super length** to set the minimum length for super passwords.

Use **undo password-control super length** to restore the default.

Syntax

password-control super length *length*

undo password-control super length

Default

In non-FIPS mode:

The minimum super password length is 10 characters.

In FIPS mode:

The minimum super password length is 15 characters.

Views

System view

Predefined user roles

network-admin

Parameters

length: Specifies the minimum length of super passwords in characters. The value range for this argument is 4 to 63 in non-FIPS mode, and 15 to 63 in FIPS mode.

Examples

# Set the minimum length of super passwords to 16 characters.

```
<Sysname> system-view
[Sysname] password-control super length 16
```

Related commands

display password-control

password-control length

password-control update-interval

Use **password-control update-interval** to set the minimum password update interval, which is the minimum interval at which users can change their passwords.

Use **undo password-control update-interval** to restore the default.

Syntax

password-control update-interval *interval*

undo password-control update-interval

Default

The minimum password update interval is 24 hours.

Views

System view

Predefined user roles

network-admin

Parameters

interval: Specifies the minimum password update interval in hours, in the range of 0 to 168. 0 means no requirements for password update interval.

Usage guidelines

The set minimum interval is not effective on a user who is prompted to change the password at the first login or after the password expires.

Examples

# Set the minimum password update interval to 36 hours.

```
<Sysname> system-view
[Sysname] password-control update-interval 36
```

Related commands

display password-control

reset password-control blacklist

Use **reset password-control blacklist** to remove blacklisted users.

Syntax

reset password-control blacklist [**user-name** *user-name*]

Views

User view

Predefined user roles

network-admin

Parameters

user-name *user-name*: Specifies the username of a user account to be removed from the password control blacklist. The username is a case-sensitive string of 1 to 55 characters.

Usage guidelines

You can use this command to remove a user account that is blacklisted due to excessive login failures. Then the blacklisted user can use this user account to log in.

Examples

# Remove the user account named **test** from the password control blacklist.

```
<Sysname> reset password-control blacklist user-name test
Are you sure to delete the specified user in blacklist? [Y/N]:
```

Related commands

display password-control blacklist

reset password-control history-record

Use **reset password-control history-record** to delete history password records.

Syntax

reset password-control history-record [**super** [**role** *role name*] | **user-name** *user-name*]

Views

User view

Predefined user roles

network-admin

Parameters

super: Deletes the history records of the specified super password or all super passwords.

role *role name*: Specifies a user role name, a case-sensitive string of 1 to 63 characters. If you do not specify this option, the command deletes the history records of all super passwords.

user-name *user-name*: Specifies the username of the user whose password records are to be deleted. The *user-name* argument is a case-sensitive string of 1 to 55 characters.

Usage guidelines

If you do not specify any parameters, this command deletes the history password records of all local users.

Examples

# Clear the history password records of all local users.

```
<Sysname> reset password-control history-record
Are you sure to delete all local user's history records? [Y/N]:y
```

Related commands

password-control history