目 录

1 Password Control

1.1 Password Control配置命令

1.1.1 display password-control

【命令】

display password-control [**super**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

【视图】

任意视图

【缺省级别】

2：系统级

【参数】

super：显示 super 密码的管理信息。如果不指定该参数，将显示全局密码管理的信息。

|：使用正则表达式对显示信息进行过滤。有关正则表达式的详细介绍，请参见“基础配置指导”中的“CLI”。

begin：从包含指定正则表达式的行开始显示。

exclude：只显示不包含指定正则表达式的行。

include：只显示包含指定正则表达式的行。

regular-expression：表示正则表达式，为 1～256 个字符的字符串，区分大小写。

【描述】

display password-control 命令用来显示密码管理的配置信息。

【举例】

显示全局密码管理信息。

```
<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
 User authentication timeout:         60 seconds
 Maximum failed login attempts:       3 times
 Login attempt-failed action:         Lock for 1 minutes
 Minimum password update time:        24 hours
 User account idle-time:              90 days
 Login with aged password:            3 times in 30 days
 Password complexity:                 Disabled (username checking)
```

```
                                        Disabled (repeated characters checking)
```

显示 super 密码管理信息。

```
<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)
```

表1-1 display password-control 命令显示信息描述表

字段	描述
Password control	密码管理功能
Password aging	密码老化功能
Password length	最小密码长度功能
Password composition	组合密码功能
Password history	密码历史功能
Early notice on password expiration	密码老化提醒功能
User authentication timeout	认证超时功能
Maximum failed login attempts	登录失败尝试次数功能
Login attempt-failed action	登录失败尝试次数达到设定次数后的锁定行为功能
Minimum password update time	密码更新的最小时间间隔
User account idle-time	用户帐号闲置时间
Login with aged password	密码过期后允许用户登录功能
Password complexity	密码复杂度检查功能，可检查内容包括：是否包含用户名或者颠倒的用户名；是否包含三个或以上相同字符

1.1.2 display password-control blacklist

【命令】

display password-control blacklist [**user-name** *name* | **ip** *ipv4-address* | **ipv6** *ipv6-address*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

【视图】

任意视图

【缺省级别】

2：系统级

【参数】

user-name *name*：显示密码管理黑名单中指定用户名的用户信息。其中，*name* 表示用户名，为 1～80 个字符的字符串。

ipv4-address：显示密码管理黑名单中指定 IPv4 地址的用户信息。

ipv6-address：显示密码管理黑名单中指定 IPv6 地址的用户信息。

|：使用正则表达式对显示信息进行过滤。有关正则表达式的详细介绍，请参见“基础配置指导”中的“CLI”。

begin：从包含指定正则表达式的行开始显示。

exclude：只显示不包含指定正则表达式的行。

include：只显示包含指定正则表达式的行。

regular-expression：表示正则表达式，为 1～256 个字符的字符串，区分大小写。

【描述】

display password-control blacklist 命令用来显示用户认证失败后，被加入密码管理黑名单中的用户信息。

如果不指定任何参数，则显示密码管理黑名单中的所有用户信息。

【举例】

显示用户尝试失败后，被加入密码管理黑名单中的用户信息。

```
<Sysname> display password-control blacklist
Username: test
   IP: 192.168.44.1        Login failed times: 1      Lock flag: unlock

Total 1 blacklist item(s) matched. 1 listed.
```

表1-2 display password-control blacklist 命令显示信息描述表

字段	描述
Username	用户名
IP	登录IP地址
Login failed times	登录失败的次数
Lock flag	该用户是否被锁定 • unlock：表示未锁定，允许用户再次尝试登录 • lock：表示锁定，暂时或永久禁止用户尝试登录（具体由 **password-control login-attempt** 命令的配置情况决定）

1.1.3 password

【命令】

password

undo password

【视图】

本地用户视图

【缺省级别】

2：系统级

【参数】

无

【描述】

password 命令用来以交互式方式设置本地用户密码，**undo password** 命令用来删除本地用户密码。

需要注意的是：

- 密码可以包含的字符为：[A～Z]、[a～z]、[0～9]以及 32 个特殊字符（空格 ~`!@#$%^&*()_+-={}|[]\:";'<>,./）。
- 以交互式方式设置本地用户密码时，密码必须符合密码管理的相关配置。例如，当密码的最小长度限制为 8 个字符时，输入的密码就必须大于或等于 8 个字符。

【举例】

以交互式方式设置本地用户密码。

```
<Sysname> system-view
[Sysname] local-user test
[Sysname-luser-test] password
Password:**********
Confirm :**********
Updating user(s) information, please wait....
```

1.1.4 password-control aging

【命令】

password-control aging *aging-time*

undo password-control aging

【视图】

系统视图/用户组/本地用户视图

【缺省级别】

2：系统级

【参数】

aging-time：密码的老化时间，取值范围为 1～365，单位为天。

【描述】

password-control aging 命令用来配置密码的老化时间。**undo password-control aging** 命令用来恢复缺省情况。

缺省情况下，全局的密码老化时间为 90 天；用户组的密码老化时间为全局配置的密码老化时间；本地用户的密码老化时间为所属用户组的密码老化时间，若用户组未配置该值，则采用全局配置值。

需要注意的是：

- 系统视图下配置具有全局性，对所有用户组有效，用户组视图下的配置对用户组内所有本地用户有效，本地用户视图下的配置只对当前本地用户有效。

- 本地用户密码老化时间生效的优先级顺序由高到底依次为本地用户视图、用户组视图、全局视图。即，系统优先采用本地用户视图下的配置，若本地用户视图下未配置，则采用用户组视图下的配置，若用户组视图下也未配置，则采用全局视图下的配置。

相关配置可参考命令 **display password-control** 和“安全命令参考/AAA”中的命令 **local-user**、**user-group**。

【举例】

配置全局的密码老化时间为 80 天。

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

配置用户组 test 的密码老化时间为 90 天。

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

配置本地用户 abc 的密码老化时间为 100 天。

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

1.1.5 password-control alert-before-expire

【命令】

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

undo password-control alert-before-expire

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

alert-time：密码过期前的提醒时间，取值范围为 1～30，单位为天。

【描述】

password-control alert-before-expire 命令用来配置密码过期前的提醒时间。**undo password-control alert-before-expire** 命令用来恢复缺省情况。

缺省情况下，密码过期前的提醒时间为 7 天，表示在密码过期之前 7 天提醒用户密码即将老化。

【举例】

设定密码过期前的提醒时间为 10 天。

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

1.1.6 password-control authentication-timeout

【命令】

password-control authentication-timeout *authentication-timeout*

undo password-control authentication-timeout

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

authentication-timeout：用户认证的超时时间，取值范围为 30～120，单位为秒。

【描述】

password-control authentication-timeout 命令用来配置用户认证的超时时间。**undo password-control authentication-timeout** 命令用来恢复缺省情况。

缺省情况下，用户认证的超时时间为 60 秒。

【举例】

设定用户认证的超时时间为 40 秒。

```
<Sysname> system-view
[Sysname] password-control authentication-timeout 40
```

1.1.7 password-control complexity

【命令】

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

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

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

same-character：指定检查密码中是否包含连续三个或以上相同的字符。

user-name：指定检查密码中是否包含用户名或者颠倒的用户名。

【描述】

password-control complexity 命令用来配置用户密码的复杂度检查策略。**undo password-control complexity check** 命令用来取消指定的密码复杂度检查策略。

缺省情况下，不对用户密码进行复杂度检查，允许密码中包含用户名或者颠倒的用户名，也允许包含连续三个或以上的相同字符。

相关配置可参考命令 **display password-control**。

【举例】

配置密码复杂度检测策略，具体要求为：检查配置的密码中是否包含用户名或者颠倒的用户名，若密码不符合复杂度策略，则密码设置不成功。

```
<Sysname> system-view
```

```
[Sysname] password-control complexity user-name check
```

1.1.8 password-control composition

【命令】

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

undo password-control composition

【视图】

系统视图/用户组/本地用户视图

【缺省级别】

2：系统级

【参数】

type-number *type-number*：密码元素的最少组合类型。其中，*type-number* 表示组合类型的个数，取值范围为 1～4。在 FIPS 模式下，*type-number* 取值必须为 4。

type-length *type-length*：密码中至少要包含每种元素的个数。其中，*type-length* 表示元素个数，取值范围为 1～63。

【描述】

password-control composition 命令用来配置用户密码的组合策略。**undo password-control composition** 命令用来恢复缺省情况。

缺省情况下，全局的密码元素的最少组合类型为 1 种，至少要包含每种元素的个数为 1 个；用户组的密码组合策略为全局配置的密码组合策略；本地用户的密码组合策略为所属用户组的密码组合策略，若用户组未配置该值，则采用全局配置值。在 FIPS 模式下，全局的密码原始的最少组合类型必须为 4 种。

需要注意的是：

- 系统视图下配置具有全局性，对所有用户组有效，用户组视图下的配置对用户组内所有本地用户有效，本地用户视图下的配置只对当前本地用户有效。
- 本地用户密码组合策略生效的优先级顺序由高到底依次为本地用户视图、用户组视图、全局视图。即，系统优先采用本地用户视图下的配置，若本地用户视图下未配置，则采用用户组视图下的配置，若用户组视图下也未配置，则采用全局视图下的配置。

相关配置可参考命令 **display password-control** 和“安全命令参考/AAA”中的命令 **local-user**、**user-group**。

【举例】

配置全局的密码元素的最少组合类型为 3 种，至少要包含每种元素的个数为 5 个。

```
<Sysname> system-view
[Sysname] password-control composition type-number 3 type-length 5
```

配置用户组 test 的密码元素的最少组合类型为 3 种，至少要包含每种元素的个数为 5 个。

```
[Sysname] user-group test
[Sysname-ugroup-test] password-control composition type-number 3 type-length 5
[Sysname-ugroup-test] quit
```

配置本地用户 abc 的密码元素的最少组合类型为 3 种，至少要包含每种元素的个数为 5 个。

```
[Sysname] local-user abc
[Sysname-luser-abc] password-control composition type-number 3 type-length 5
```

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

【命令】

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

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

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

aging：使能密码老化管理功能。

composition：使能密码的组合检测管理功能。

history：使能密码历史记录管理功能。

length：使能密码最小长度管理功能。

【描述】

password-control { **aging** | **composition** | **history** | **length** } **enable** 命令用来使能指定的密码管理的相关功能。**undo password-control** { **aging** | **composition** | **history** | **length** } **enable** 命令用来关闭指定的密码管理的相关功能。

缺省情况下，各密码管理功能均处于使能状态。

需要注意的是：

- 要使相关的密码管理功能生效，必须保证全局密码管理功能处于使能状态。
- 如果没有使能指定的密码管理功能，则它对应的密码管理策略配置将不起作用。例如，若密码最小长度管理功能处于未使能状态，则 **password-control length** 命令配置的具体长度限制就不生效。
- 如果执行命令 **undo password-control history enable**，在此之前的历史记录依然保存，命令执行之后将不再记录历史密码。

相关配置可参考命令 **password-control enable** 和 **display password-control**。

【举例】

使能全局密码管理功能。

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

使能密码组合检测管理功能。

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

使能密码老化功能。

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

使能密码最小长度功能。

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

使能密码历史记录功能。

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

1.1.10 password-control enable

【命令】

password-control enable

undo password-control enable

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

无

【描述】

password-control enable 命令用来使能全局密码管理功能。**undo password-control enable** 命令用来关闭全局密码管理功能。

缺省情况下，全局的密码管理能处于未使能状态。

只有在使能了全局密码管理功能的情况下，其它相关的密码管理功能才能生效。

相关配置可参考命令 **display password-control**。

【举例】

使能全局密码管理功能。

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

1.1.11 password-control expired-user-login

【命令】

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

undo password-control expired-user-login

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

delay：密码过期后允许用户登录的时长，取值范围为 1～90，单位为天。

times：密码过期后允许用户登录的最大次数，取值范围为 0～10。0 表示密码过期后不允许用户登录。

【描述】

password-control expired-user-login 命令用来配置密码过期后允许登录的时间和次数。**undo password-control expired-user-login** 命令用来恢复缺省情况。

缺省情况下，密码过期后允许登录的时间为 30 天，允许登录的次数为 3 次，表示如果密码过期，那么系统还允许用户在 30 天内登录 3 次。

相关配置可参考命令 **display password-control**。

【举例】

设定允许用户在密码过期之后的 60 天内登录 5 次。

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

1.1.12 password-control history

【命令】

password-control history *max-record-num*

undo password-control history

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

max-record-num：每个用户密码历史记录的最大条数，取值范围为 2～15。

【描述】

password-control history 命令用来配置每个用户密码历史记录的最大条数。**undo password-control history** 命令用来恢复缺省情况。

缺省情况下，每个用户密码历史记录的最大条数为 4 条。

【举例】

设定每个用户密码历史记录的最大条数为 10 条。

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

1.1.13 password-control length

【命令】

password-control length *length*

undo password-control length

【视图】

系统视图/用户组/本地用户视图

【缺省级别】

2：系统级

【参数】

length：密码的最小长度，在 FIPS 模式下取值范围为 8～32，在非 FIPS 模式下取值范围为 4～32。

【描述】

password-control length 命令用来配置密码的最小长度。**undo password-control length** 命令用来恢复缺省情况。

缺省情况下，全局的密码最小长度为 10 个字符，本地用户的密码最小长度为全局配置。用户组的密码最小长度为全局配置的密码最小长度；本地用户的密码最小长度为所属用户组的密码最小长度，若用户组未配置该值，则采用全局配置值。

需要注意的是：

- 系统视图下配置具有全局性，对所有用户组有效，用户组视图下的配置对用户组内所有本地用户有效，本地用户视图下的配置只对当前本地用户有效。
- 本地用户密码最小长度生效的优先级顺序由高到底依次为本地用户视图、用户组视图、全局视图。即，系统优先采用本地用户视图下的配置，若本地用户视图下未配置，则采用用户组视图下的配置，若用户组视图下也未配置，则采用全局视图下的配置。

相关配置可参考命令 **display password-control** 和“安全命令参考/AAA”中的命令 **local-user**、**user-group**。

【举例】

配置全局的密码最小长度为 9 个字符。

```
<Sysname> system-view
[Sysname] password-control length 9
```

配置用户组 test 的密码最小长度为 9 个字符。

```
[Sysname] user-group test
[Sysname-ugroup-test] password-control length 9
[Sysname-ugroup-test] quit
```

配置本地用户 abc 的密码最小长度为 9 个字符。

```
[Sysname] local-user abc
[Sysname-luser-abc] password-control length 9
```

1.1.14 password-control login idle-time

【命令】

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

undo password-control login idle-time

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

idle-time：用户帐号的闲置时间，取值范围为 0～365，单位为天。0 表示对用户帐号闲置时间无限制。

【描述】

password-control login idle-time 命令用来配置用户帐号的闲置时间。**undo password-control login idle-time** 命令用来恢复缺省情况。

缺省情况下，用户帐号的闲置时间为 90 天，表示如果用户自最后一次成功登录后，在 90 天内再未成功登录过设备，那么该用户帐号将会失效。

相关配置可参考命令 **display password-control**。

【举例】

设定用户帐号的闲置时间为 30 天，表示自最后一次成功登录后，若用户在 30 天内再未成功登录过设备，那么将该用户帐号将会失效。

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

1.1.15 password-control login-attempt

【命令】

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

undo password-control login-attempt

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

login-times：用户登录尝试次数，取值范围为 2～10。

exceed：用户登录尝试失败后的行为。

lock：表示永久禁止该用户登录。

lock-time *time*：表示禁止该用户一段时间后，再允许该用户重新登录。其中，*time* 为禁止该用户的时间，取值范围为 1～360，单位为分钟。

unlock：表示不禁止该用户，允许其继续登录。

【描述】

password-control login-attempt 命令用来配置用户登录尝试次数以及登录尝试失败后的行为。**undo password-control login-attempt** 命令用来恢复缺省情况。

缺省情况下，用户登录尝试次数为 3 次；如果用户登录失败，则 1 分钟后再允许该用户重新登录。

需要注意的是：

- 对于被永久禁止登录的用户，只有管理员把该用户从密码管理的黑名单中删除后，该用户才能重新登录。

- 对于被禁止一段时间内登录的用户，当配置的禁止时间超时或者管理员将其从密码管理的黑名单中删除，该用户才可以重新登录。
- 对于不禁止登录的用户，只要用户登录成功或者密码管理的黑名单的老化时间（系统规定为 1 分钟）超时后，该用户就会从该黑名单中被删除。

相关配置可参考命令 **display password-control**、**display password-control blacklist** 和 **reset password-control blacklist**。

【举例】

管理员设定用户登录尝试次数为 4 次，并且永久禁止该用户登录。

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

之后，若有用户连续尝试认证的失败累加次数达到 4 次，管理员可通过命令查看到被加入密码管理黑名单中的用户锁定状态由之前的 **unlock** 切换为 **lock**，且该用户无法再次成功登录。

```
[Sysname] display password-control blacklist
Username: test
   IP: 192.168.44.1        Login failed times: 4      Lock flag: lock

Total 1 blacklist item(s) matched. 1 listed.
```

管理员设定用户登录尝试次数为 2 次，并且禁止该用户 3 分钟后，再允许该用户重新登录。

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

之后，若有用户连续尝试认证的失败累加次数达到 2 次，管理员可通过命令查看到被加入密码管理黑名单中的用户锁定状态由之前的 **unlock** 切换为 **lock**。

```
[Sysname] display password-control blacklist
Username: test
   IP: 192.168.44.1        Login failed times: 2      Lock flag: lock

Total 1 blacklist item(s) matched. 1 listed.
```

用户被禁止登录 3 分钟后，将被从密码管理黑名单中删除，且可以重新登录。

1.1.16 password-control password update interval

【命令】

password-control password update interval *interval*

undo password-control password update interval

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

interval：密码更新的最小时间间隔，取值范围为 0～168，单位为小时。0 表示对密码更新的时间间隔无限制。

【描述】

password-control password update interval 命令用来配置密码更新的最小时间间隔。**undo password-control password update interval** 命令用来恢复缺省情况。

缺省情况下，密码更新的最小时间间隔为 24 小时。

需要注意的是，有两种情况下的密码更新并不受该功能的约束：用户首次登录设备时系统要求用户修改密码；密码老化后系统要求用户修改密码。

相关配置可参考命令 **display password-control**。

【举例】

设定密码更新的最小时间间隔为 36 小时。

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

1.1.17 password-control super aging

【命令】

password-control super aging *aging-time*

undo password-control super aging

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

aging-time：super 密码的老化时间，取值范围为 1～365，单位为天。

【描述】

password-control super aging 命令用来配置 super 密码的老化时间。**undo password-control super aging** 命令用来恢复缺省情况。

缺省情况下，super 密码的老化时间为全局密码老化时间。

需要注意的是，对于 super 密码的各管理参数来说，系统优先采用为 super 密码的单独配置；当没有为 super 密码进行单独配置时，采用全局配置。

相关配置请参考命令 **password-control aging**。

【举例】

设定 super 密码的老化时间为 10 天。

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

1.1.18 password-control super composition

【命令】

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

undo password-control super composition

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

type-number *type-number*：super 密码的最少组合类型。其中，*type-number* 表示组合类型，取值范围为 1～4。在 FIPS 模式下，*type-number* 取值必须为 4。

type-length *type-length*：super 密码中每种类型的最少字符个数。其中，*type-length* 表示字符个数，取值范围为 1～16。

【描述】

password-control super composition 命令用来配置 super 密码的组合策略。**undo password-control super composition** 命令用来恢复缺省情况。

缺省情况下，super 密码组合策略为全局密码组合策略。在 FIPS 模式下，super 密码的最少组合类型必须为 4。

需要注意的是，对于 super 密码的各管理参数来说，系统优先采用为 super 密码的单独配置；当没有为 super 密码进行单独配置时，采用全局配置。

相关配置请参考命令 **password-control composition**。

【举例】

配置 super 密码的最少组合类型为 3 种，每种类型的最少字符个数为 5 个。

```
<Sysname> system-view
[Sysname] password-control super composition type-number 3  type-length 5
```

1.1.19 password-control super length

【命令】

password-control super length *length*

undo password-control super length

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

length：super 密码的最小字符长度，在 FIPS 模式下取值范围为 8～16，在非 FIPS 模式下 4～16。

【描述】

password-control super length 命令用来配置 super 密码的最小长度。**undo password-control super length** 命令用来恢复缺省情况。

缺省情况下，super 密码的最小长度为全局密码最小长度。

需要注意的是，对于 super 密码的各管理参数来说，系统优先采用为 super 密码的单独配置；当没有为 super 密码进行单独配置时，采用全局配置。

相关配置请参考命令 **password-control length**。

【举例】

设定 super 密码的最小长度为 10 个字符。

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

1.1.20 reset password-control blacklist

【命令】

reset password-control blacklist { **all** | **user-name** *name* }

【视图】

用户视图

【缺省级别】

3：管理级

【参数】

all：清除密码管理黑名单中所有用户。

user-name *name*：清除密码管理黑名单中指定的用户。其中，*name* 表示用户名，为 1～80 个字符的字符串，区分大小写。

【描述】

reset password-control blacklist 命令用来清除密码管理黑名单中的用户。

相关配置请参考命令 **display password-control blacklist**。

【举例】

清除密码管理黑名单中的用户 test。

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

1.1.21 reset password-control history-record

【命令】

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

【视图】

用户视图

【缺省级别】

3：管理级

【参数】

user-name *name*：删除指定用户名的密码历史记录。其中，*name* 表示用户名，为 1～80 个字符的字符串，区分大小写。

super：删除 super 密码的历史记录。

level *level*：指定用户级别。其中，*level* 表示用户级别，取值范围为 1～3。

【描述】

reset password-control history-record 命令用来清除用户的密码历史记录。

需要注意的是：

- 如果不指定任何参数，将删除所有本地用户的密码历史记录。
- 如果不指定参数 *level*，将删除所有 super 密码的历史记录。

【举例】

清除所有本地用户的密码历史记录。当用户输入 Y，系统删除所有本地用户的密码历史记录。

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