目 录

1 Password Control

1.1 Password Control简介

Password Control（密码管理）是设备提供的密码安全管理功能，它根据管理员定义的安全策略，对设备管理类的本地用户登录密码、super 密码的设置、老化、更新等方面进行管理，并对用户的登录状态进行控制。

说明

- 本地用户包括两种类型，设备管理类（**manage**）和网络接入类（**network**）。Password Control 功能仅对设备管理类本地用户的登录密码进行控制，对网络接入类本地用户的密码不起作用。关于本地用户类型的详细介绍，请参见“安全配置指导”中的“AAA”。
- 为了防止未授权用户的非法侵入，在进行用户角色切换时，要进行用户身份验证，即需要输入用户角色切换密码，这个密码就被称为 super 密码。关于 super 密码的详细介绍，请参见“基础配置指导”中的“RBAC”。

1.1.1 密码设置控制

1. 密码最小长度限制

管理员可以限制用户密码的最小长度。当设置用户密码时，如果输入的密码长度小于设置的最小长度，系统将不允许设置该密码。

2. 密码的组合检测功能

管理员可以设置用户密码的组成元素的组合类型，以及至少要包含每种元素的个数。密码的组成元素包括以下 4 种类型：

- [A～Z]
- [a～z]
- [0～9]
- 32 个特殊字符（空格~`!@#$%^&*()_+-={}|[]\:";'<>,./）

密码元素的组合类型有 4 种，具体涵义如下：

- 组合类型为 1 表示密码中至少包含 1 种元素；
- 组合类型为 2 表示密码中至少包含 2 种元素；
- 组合类型为 3 表示密码中至少包含 3 种元素；
- 组合类型为 4 表示密码中包含 4 种元素。

当用户设置密码时，系统会检查设定的密码是否符合配置要求，只有符合要求的密码才能设置成功。

3. 密码的复杂度检测功能

密码的复杂度越低，其被破解的可能性就越大，比如包含用户名、使用重复字符等。出于安全性考虑，管理员可以设置用户密码的复杂度检测功能，确保用户的密码具有较高的复杂度。具体实现是：

配置用户密码时，系统检测输入的密码是否符合一定的复杂度要求，只有符合要求的密码才能设置成功。目前，复杂度检测功能对密码的复杂度要求包括以下两项：

- 密码中不能包含用户名或者字符顺序颠倒的用户名。例如，用户名为“abc”，那么“abc982”或者“2cba”之类的密码就不符合复杂度要求。
- 密码中不能包含连续三个或以上的相同字符。例如，密码“a111”就不符合复杂度要求。

1.1.2 密码更新与老化

1. 密码更新管理

管理员可以设置用户登录设备后修改自身密码的最小间隔时间。当用户登录设备修改自身密码时，如果距离上次修改密码的时间间隔小于配置值，则系统不允许修改密码。例如，管理员配置用户密码更新间隔时间为 48 小时，那么用户在上次修改密码后的 48 小时之内都无法成功进行密码修改操作。

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。

2. 密码老化管理

密码老化时间用来限制用户密码的使用时间。当密码的使用时间超过老化时间后，需要用户更换密码。

当用户登录时，如果用户输入已经过期的密码，系统将提示该密码已经过期，需要重新设置密码。如果输入的新密码不符合要求，或连续两次输入的新密码不一致，系统将要求用户重新输入。对于 FTP 用户，密码老化后，只能由管理员修改 FTP 用户的密码；对于 Telnet、SSH、Terminal（通过 Console 口登录设备）用户可自行修改密码。

3. 密码过期提醒

在用户登录时，系统判断其密码距离过期的时间是否在设置的提醒时间范围内。如果在提醒时间范围内，系统会提示该密码还有多久过期，并询问用户是否修改密码。如果用户选择修改，则记录新的密码及其设定时间。如果用户选择不修改或者修改失败，则在密码未过期的情况下仍可以正常登录。对于 FTP 用户，只能由管理员修改 FTP 用户的密码；对于 Telnet、SSH、Terminal（通过 Console 口登录设备）用户可自行修改密码。

4. 密码老化后允许登录管理

管理员可以设置用户密码过期后在指定的时间内还能登录设备指定的次数。这样，密码老化的用户不需要立即更新密码，依然可以登录设备。例如，管理员设置密码老化后允许用户登录的时间为 15 天、次数为 3 次，那么用户在密码老化后的 15 天内，还能继续成功登录 3 次。

5. 密码历史记录

系统保存用户密码历史记录。当用户修改密码时，系统会要求用户设置新的密码，如果新设置的密码以前使用过，且在当前用户密码历史记录中，系统将给出错误信息，提示用户密码更改失败。另外，用户更改密码时，系统会将新设置的密码逐一与所有记录的历史密码以及当前密码比较，要求新密码至少要与旧密码有 4 字符不同，且这 4 个字符必须互不相同，否则密码更改失败。

可以配置每个用户密码历史记录的最大条数，当密码历史记录的条数超过配置的最大历史记录条数时，新的密码历史记录将覆盖该用户最老的一条密码历史记录。

由于为设备管理类本地用户配置的密码在哈希运算后以密文的方式保存，配置一旦生效后就无法还原为明文密码，因此，设备管理类本地用户的当前登录密码，不会被记录到该用户的密码历史记录中。

1.1.3 用户登录控制

1. 用户首次登录控制

当全局密码管理功能使能后，用户首次登录设备时，系统会输出相应的提示信息要求用户修改密码，否则不允许登录设备。这种情况下的修改密码不受密码更新时间间隔的限制。

2. 密码尝试次数限制

密码尝试次数限制可以用来防止恶意用户通过不断尝试来破解密码。

每次用户认证失败后，系统会将该用户加入密码管理的黑名单。可加入密码管理功能黑名单的用户包括：FTP 用户和通过 VTY 方式访问设备的用户。不会加入密码管理功能黑名单的用户包括：用户名不存在的用户、通过 Console 口连接到设备的用户。

当用户连续尝试认证的失败累加次数达到设置的尝试次数时，系统对用户的后续登录行为有以下三种处理措施：

- 永久禁止该用户登录。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。
- 不对该用户做禁止，允许其继续登录。在该用户登录成功后，该用户会从密码管理的黑名单中删除。
- 禁止该用户一段时间后，再允许其重新登录。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。

3. 用户帐号闲置时间管理

管理员可以限制用户帐号的闲置时间，禁止在闲置时间之内始终处于不活动状态的用户登录。若用户自从最后一次成功登录之后，在配置的闲置时间内再未成功登录过，那么该闲置时间到达之后此用户账号立即失效，系统不再允许使用该账号的用户登录。

1.1.4 密码不回显

出于安全考虑，用户输入密码时，系统将不回显用户的密码。

1.1.5 日志功能

当用户成功修改密码或用户登录失败加入密码管理黑名单时，系统将会记录相应的日志。

1.2 Password Control配置任务简介

本特性的各功能可支持在多个视图下配置，各视图可支持的功能不同。而且，相同功能的命令在不同视图下或针对不同密码时有效范围有所不同，具体情况如下：

- 系统视图下的全局配置对所有本地用户密码都有效；
- 用户组视图下的配置只对当前用户组内的所有本地用户密码有效；
- 本地用户视图下的配置只对当前的本地用户密码有效；

- 为 super 密码的各管理参数所作的配置只对 super 密码有效。

对于本地用户密码的各管理参数，其生效的优先级顺序由高到低依次为本地用户视图、用户组视图、系统视图。

表1-1 Password Control 配置任务简介

配置任务	说明	详细配置
使能密码管理	必选	1.3.1
配置全局密码管理	可选	1.3.2
配置用户组密码管理	可选	1.3.3
配置本地用户密码管理	可选	1.3.4
配置super密码管理	可选	1.3.5

1.3 配置Password Control

注意

设备存储空间不足会造成以下两个影响：

- 不能使能全局密码管理功能；
- 全局密码管理功能处于使能的状态下，用户登录设备失败。

1.3.1 使能密码管理

使能全局密码管理功能，是密码管理所有配置生效的前提。若要使得具体的密码管理功能（密码老化、密码最小长度、密码历史记录、密码组合检测）生效，还需使能指定的密码管理功能。

需要注意的是，使能全局密码管理功能后：

- 设备管理类本地用户密码以及 super 密码的配置将不被显示，即无法通过相应的 **display** 命令查看到设备管理类本地用户密码以及 super 密码的配置。网络接入类本地用户密码不受密码管理功能控制，其配置显示也不受影响。
- 首次设置的设备管理类本地用户密码必须至少由四个不同的字符组成。

表1-2 使能密码管理

操作	命令	说明
进入系统视图	**system-view**	-
使能全局密码管理功能	**password-control enable**	缺省情况下，全局密码管理功能处于未使能状态
（可选）使能指定的密码管理功能	**password-control { aging | composition | history | length } enable**	缺省情况下，各密码管理功能均处于使能状态

说明

开启全局密码管理功能后，Password Control 会记录用户配置密码时的 UTC 时间。如果因设备断电重启等原因，UTC 时间与 Password Control 记录的 UTC 时间不一致，可能导致密码老化管理功能出错。因此，为保证密码老化管理功能的正常工作，建议设备通过 NTP（Network Time Protocol，网络时间协议）协议获取 UTC 时间。关于 NTP 的详细介绍，请参见“网络管理和监控配置指导”中的“NTP”。

1.3.2 配置全局密码管理

系统视图下的全局密码管理参数对所有设备管理类的本地用户生效。对于密码老化时间、密码最小长度以及密码组合策略这三个功能，可分别在系统视图、用户组视图、本地用户视图下配置相关参数，其生效优先级从高到低依次为：本地用户视图->用户组视图->系统视图。

除用户登录尝试失败后的行为配置属于即时生效的配置，会在配置生效后立即影响密码管理黑名单中当前用户的锁定状态以及这些用户后续的登录之外，其它全局密码管理配置生效后仅对后续登录的用户以及后续设置的用户密码有效，不影响当前用户。

表1-3 配置全局密码管理

操作	命令	说明
进入系统视图	**system-view**	-
配置密码的老化时间	**password-control aging** *aging-time*	缺省情况下，密码的老化时间为90天
配置密码更新的最小时间间隔	**password-control update-interval** *interval*	缺省情况下，密码更新的最小时间间隔为24小时
配置密码的最小长度	**password-control length** *length*	缺省情况下，密码的最小长度为10个字符
配置用户密码的组合策略	**password-control composition type-number** *type-number* [**type-length** *type-length*]	缺省情况下，密码元素的组合类型至少为1种，至少要包含每种元素的个数为1个
配置用户密码的复杂度检查策略	**password-control complexity** { **same-character** | **user-name** } **check**	缺省情况下，不对用户密码进行复杂度检查
配置每个用户密码历史记录的最大条数	**password-control history** *max-record-number*	缺省情况下，每个用户密码历史记录的最大条数为4条
配置用户登录尝试次数以及登录尝试失败后的行为	**password-control login-attempt** *login-times* [**exceed** { **lock** | **lock-time** *time* | **unlock** }]	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
配置密码过期前的提醒时间	**password-control alert-before-expire** *alert-time*	缺省情况下，密码过期前的提醒时间为7天
配置密码过期后允许用户登录的时间和次数	**password-control expired-user-login delay** *delay* **times** *times*	缺省情况下，密码过期后的30天内允许用户登录3次
配置用户帐号的闲置时间	**password-control login idle-time** *idle-time*	缺省情况下，用户帐号的闲置时间为90天

1.3.3 配置用户组密码管理

表1-4 配置用户组密码管理

操作	命令	说明
进入系统视图	**system-view**	-
创建用户组，并进入用户组视图	**user-group** *group-name*	缺省情况下，不存在任何用户组 用户组的相关配置请参见“安全配置指导”中的“AAA”
配置用户组的密码老化时间	**password-control aging** *aging-time*	缺省情况下，采用全局密码老化时间
配置用户组的密码最小长度	**password-control length** *length*	缺省情况下，采用全局密码最小长度
配置用户组的密码组合策略	**password-control composition type-number** *type-number* [**type-length** *type-length*]	缺省情况下，采用全局密码组合策略
配置用户密码的复杂度检查策略	**password-control complexity** { **same-character** | **user-name** } **check**	缺省情况下，采用全局密码复杂度检查策略
配置用户登录尝试次数以及登录尝试失败后的行为	**password-control login-attempt** *login-times* [**exceed** { **lock** | **lock-time** *time* | **unlock** }]	缺省情况下，采用全局的用户登录尝试限制策略

1.3.4 配置本地用户密码管理

表1-5 配置本地用户密码管理

操作	命令	说明
进入系统视图	**system-view**	-
创建设备管理类本地用户，并进入本地用户视图	**local-user** *user-name* **class manage**	缺省情况下，不存在任何本地用户 本地用户密码管理功能仅对设备管理类的本地用户生效，对于网络接入类本地用户不起作用 本地用户的相关配置请参见“安全配置指导”中的“AAA”
配置本地用户的密码老化时间	**password-control aging** *aging-time*	缺省情况下，采用本地用户所属用户组的密码老化时间
配置本地用户的密码最小长度	**password-control length** *length*	缺省情况下，采用本地用户所属用户组的密码最小长度
配置本地用户的密码组合策略	**password-control composition type-number** *type-number* [**type-length** *type-length*]	缺省情况下，采用本地用户所属用户组的密码组合策略
配置用户密码的复杂度检查策略	**password-control complexity** { **same-character** | **user-name** } **check**	缺省情况下，采用本地用户所属用户组的密码复杂度检查策略
配置用户登录尝试次数以及登录尝试失败后的行为	**password-control login-attempt** *login-times* [**exceed** { **lock** | **lock-time** *time* | **unlock** }]	缺省情况下，采用本地用户所属用户组的用户登录尝试限制策略

1.3.5 配置super密码管理

表1-6 配置 super 密码管理

操作	命令	说明
进入系统视图	**system-view**	-
配置super密码的老化时间	**password-control super aging** *aging-time*	缺省情况下，密码的老化时间为90天
配置super密码的最小长度	**password-control super length** *length*	缺省情况下，密码的最小长度为10个字符
配置super密码的组合策略	**password-control super composition type-number** *type-number* [**type-length** *type-length*]	缺省情况下，密码元素的组合类型至少为1种，至少要包含每种元素的个数为1个

1.4 Password Control显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后 Password Control 的运行情况，通过查看显示信息验证配置的效果。

在用户视图下执行 **reset** 命令可以清除 Password Control 统计信息。

表1-7 Password Control 显示和维护

操作	命令
显示密码管理的配置信息	**display password-control** [**super**]
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	**display password-control blacklist** [**user-name** *user-name* | **ip** *ipv4-address* | **ipv6** *ipv6-address*]
清除密码管理黑名单中的用户	**reset password-control blacklist** [**user-name** *user-name*]
清除用户的密码历史记录	**reset password-control history-record** [**user-name** *user-name* | **super** [**role** *role-name*]]

说明

当密码历史记录功能未启动时，**reset password-control history-record** 命令同样可以清除全部或者某个用户的密码历史记录。

1.5 Password Control典型配置举例

1. 组网需求

有以下密码管理需求：

- 全局密码管理策略：用户 2 次登录失败后就永久禁止登录；最小密码长度为 16 个字符，密码老化时间为 30 天；允许用户进行密码更新的最小时间间隔为 36 小时；密码过期后 60 天内允许登录 5 次；用户帐号的闲置时间为 30 天；不允许密码中包含用户名或者字符顺序颠倒的用户名；不允许密码中包含连续三个或以上相同字符；密码元素的最少组合类型为 4 种，至少要包含每种元素的个数为 4 个。
- 切换到用户角色 network-operator 时使用的 super 密码管理策略：最小密码长度为 24 个字符，密码元素的最少组合类型为 4 种，至少要包含每种元素的个数为 5 个。
- 本地 Telnet 用户 test 的密码管理策略：最小密码长度为 24 个字符，密码元素的最少组合类型为 4 种，至少要包含每种元素的个数为 5 个，密码老化时间为 20 天。

2. 配置步骤

使能全局密码管理功能。

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

配置用户 2 次登录失败后就永久禁止该用户登录。

```
[Sysname] password-control login-attempt 2 exceed lock
```

配置全局的密码老化时间为 30 天。

```
[Sysname] password-control aging 30
```

配置全局的密码的最小长度为 16。

```
[Sysname] password-control length 16
```

配置密码更新的最小时间间隔为 36 小时。

```
[Sysname] password-control update-interval 36
```

配置用户密码过期后的 60 天内允许登录 5 次。

```
[Sysname] password-control expired-user-login delay 60 times 5
```

配置用户帐号的闲置时间为 30 天。

```
[Sysname] password-control login idle-time 30
```

使能在配置的密码中检查包含用户名或者字符顺序颠倒的用户名的功能。

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

使能在配置的密码中检查包含连续三个或以上相同字符的功能。

```
[Sysname] password-control complexity same-character check
```

#配置全局的密码元素的最少组合类型为 4 种，至少要包含每种元素的个数为 4 个。

```
[Sysname] password-control composition type-number 4 type-length 4
```

配置 super 密码的最小长度为 24。

```
[Sysname] password-control super length 24
```

配置 super 密码元素的最少组合类型为 4 种，至少要包含每种元素的个数为 5 个。

```
[Sysname] password-control super composition type-number 4 type-length 5
```

配置切换到用户角色 network-operator 时使用的 super 密码为明文 123456789ABGFTweuix@#$%!。

```
[Sysname] super password role network-operator simple 123456789ABGFTweuix@#$%!
```

添加设备管理类本地用户 test。

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

配置本地用户的服务类型为 Telnet。

```
[Sysname-luser-manage-test] service-type telnet
```

配置本地用户的最小密码长度为 24 个字符。

```
[Sysname-luser-manage-test] password-control length 24
```

配置本地用户的密码元素的最少组合类型为 4 种，至少要包含每种元素的个数为 5 个。

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

配置本地用户的密码老化时间为 20 天。

```
[Sysname-luser-manage-test] password-control aging 20
```

以交互式方式配置本地用户密码。

```
[Sysname-luser-manage-test] password
Password:
Confirm :
Updating user information. Please wait ... ...
[Sysname-luser-manage-test] quit
```

3. 验证配置结果

可通过如下命令查看全局密码管理的配置信息。

```
<Sysname> display password-control
 Global password control configurations:
 Password control:                       Enabled
 Password aging:                         Enabled (30 days)
 Password length:                        Enabled (16 characters)
 Password composition:                   Enabled (4 types, 4 characters per type)
 Password history:                       Enabled (max history record:4)
 Early notice on password expiration:  7 days
 Maximum login attempts:                 2
 Action for exceeding login attempts:  Lock
 Minimum interval between two updates: 36 hours
 User account idle time:                 30 days
 Logins with aged password:              5 times in 60 days
 Password complexity:                    Enabled (username checking)
                                         Enabled (repeated characters checking)
```

可通过如下命令查看 super 密码管理的配置信息。

```
<Sysname> display password-control super
 Super password control configurations:
 Password aging:                         Enabled (90 days)
 Password length:                        Enabled (24 characters)
 Password composition:                   Enabled (4 types, 5 characters per type)
```

可通过如下命令查看到本地用户密码管理的配置信息。

```
<Sysname> display local-user user-name test class manage
Total 1 local users matched.

Device management user test:
 State:                    Active
 Service type:             Telnet
 User group:               system
 Bind attributes:
 Authorization attributes:
  Work directory:          flash:
```

```
 User role list:          network-operator
Password control configurations:
 Password aging:          20 days
 Password length:         24 characters
 Password composition:    4 types, 5 characters per type
```