Password Strength and Management for Common Criteria

The Password Strength and Management for Common Criteria feature is used to specify password policies and security mechanisms for storing, retrieving, and providing rules to specify user passwords.

For local users, the user profile and the password information with the key parameters are stored on the Cisco device, and this profile is used for local authentication of users. The user can be an administrator (terminal access) or a network user (for example, PPP users being authenticated for network access).

For remote users, where the user profile information is stored in a remote server, a third-party authentication, authorization, and accounting (AAA) server may be used for providing AAA services, both for administrative and network access.

- Restrictions for Password Strength and Management for Common Criteria, on page 1
- Information About Password Strength and Management for Common Criteria, on page 1
- How to Configure Password Strength and Management for Common Criteria, on page 3
- Configuration Example for Password Strength and Management for Common Criteria, on page 6
- Additional References for Password Strength and Management for Common Criteria, on page 7
- Feature History for Password Strength and Management for Common Criteria, on page 7

Restrictions for Password Strength and Management for Common Criteria

Only four concurrent users can log on to the system by using vty at any moment.

Information About Password Strength and Management for Common Criteria

The following sections provide information on password strength and management.

Password Composition Policy

The password composition policy allows you to create passwords of any combination of upper and lowercase characters, numbers, and special characters that include “!”, “@”, “#”, “$”, “%”,“^”, “&”, “*”, “(“, and “)”.

Password Length Policy

The administrator has the flexibility to set the password's minimum and maximum length. The recommended minimum password length is 8 characters. The administrator can specify both the minimum (1) and the maximum (64) length for the password.

Password Lifetime Policy

The security administrator can provide a configurable option for a password to have a maximum lifetime. If the lifetime parameter is not configured, the configured password will never expire. The maximum lifetime can be configured by providing the configurable value in years, months, days, hours, minutes, and seconds. The lifetime configuration will survive across reloads as it is a part of the configuration, but every time the system reboots, the password creation time will be updated to the new time. For example, if a password is configured with a lifetime of one month and on the 29th day, the system reboots, then the password will be valid for one month after the system reboots.

Password Expiry Policy

If the user attempts to log on and if the user's password credentials have expired, then the following happens:

1. The user is prompted to set the new password after successfully entering the expired password.
2. When the user enters the new password, the password is validated against the password security policy.
3. If the new password matches the password security policy, then the authentication, authorization, and accounting (AAA) database is updated, and the user is authenticated with the new password.
4. If the new password does not match the password security policy, then the user is prompted again for the password. From AAA perspective, there is no restriction on the number of retries. The number of retries for password prompt in case of unsuccessful authentication is controlled by the respective terminal access interactive module. For example, for telnet, after three unsuccessful attempts, the session will be terminated.

If the password's lifetime is not configured for a user and the user has already logged on and if the security administrator configures the lifetime for that user, then the lifetime will be set in the database. When the same user is authenticated the next time, the system will check for password expiry. The password expiry is checked only during the authentication phase.

If the user has been already authenticated and logged on to the system and if the password expires, then no action will be taken. The user will be prompted to change the password only during the next authentication for the same user.

Password Change Policy

The new password must contain a minimum of 4 character changes from the previous password. A password change can be triggered by the following scenarios:

- The security administrator wants to change the password.
- The user is trying to get authenticated using a profile, and the password for that profile has expired.

When the security administrator changes the password security policy and the existing profile does not meet the password security policy rules, no action will be taken if the user has already logged on to the system. The user will be prompted to change the password only when the user tries to get authenticated using the profile that does not meet the password security restriction.

When the user changes the password, the lifetime parameters set by the security administrator for the old profile will be the lifetime parameters for the new password.

For noninteractive clients such as dot1x, when the password expires, appropriate error messages will be sent to the clients, and the clients must contact the security administrator to renew the password.

User Reauthentication Policy

Users are reauthenticated when they change their passwords.

When users change their passwords on expiry, they will be authenticated against the new password. In such cases, the actual authentication happens based on the previous credentials, and the new password is updated in the database.

Note Users can change their passwords only when they are logging on and after the expiry of the old password; however, a security administrator can change the user's password at any time.

Support for Framed (Noninteractive) Session

When a client such as dot1x uses the local database for authentication, the Password Strength and Management for Common Criteria feature will be applicable; however, upon password expiry, clients will not be able to change the password. An appropriate failure message will be sent to such clients, and the user must request the security administrator to change the password.

How to Configure Password Strength and Management for Common Criteria

The following sections provide information on configuring password strength and management.

Configuring the Password Security Policy

To create a password security policy and to apply the policy to a specific user profile, perform this procedure.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**aaa new-model** **Example:** `Device(config)# aaa new-model`	Enables AAA globally.
Step 4	**aaa common-criteria policy** *policy-name* **Example:** `Device(config)# aaa common-criteria policy policy1`	Creates the AAA security password policy and enters common criteria configuration policy mode.
Step 5	**char-changes** *number* **Example:** `Device(config-cc-policy)# char-changes 4`	(Optional) Specifies the number of changed characters between old and new passwords.
Step 6	**max-length** *number* **Example:** `Device(config-cc-policy)# max-length 25`	(Optional) Specifies the maximum length of the password.
Step 7	**min-length** *number* **Example:** `Device(config-cc-policy)# min-length 8`	(Optional) Specifies the minimum length of the password.
Step 8	**numeric-count** *number* **Example:** `Device(config-cc-policy)# numeric-count 4`	(Optional) Specifies the number of numeric characters in the password.
Step 9	**special-case** *number* **Example:** `Device(config-cc-policy)# special-case 3`	(Optional) Specifies the number of special characters in the password.
Step 10	**exit** **Example:** `Device(config-cc-policy)# exit`	(Optional) Exits common criteria configuration policy mode and returns to global configuration mode.

	Command or Action	Purpose

Step 11	**username** *username* **common-criteria-policy** *policy-name* **password** *password*
	Example:
	`Device(config)# username user1 common-criteria-policy policy1 password password1`
		(Optional) Applies a specific policy and password to a user profile.
		Note A single numerical character is not accepted as password. The following console message is displayed if you try to configure a password with a single numerical character.
		`username user2 common-criteria-policy Hay_passwd_policy_2 password 3`
		`% Incomplete command.`

Step 12	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.

Verifying the Common Criteria Policy

To verify all the common criteria security policies, perform this procedure.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode.

Step 2	**show aaa common-criteria policy name** *policy-name*
	Example:
	`Device# show aaa common-criteria policy name policy1`
	
	`Policy name: policy1`
	`Minimum length: 1`
	`Maximum length: 64`
	`Upper Count: 20`
	`Lower Count: 20`
	`Numeric Count: 5`
	`Special Count: 2`
	`Number of character changes 4`
	`Valid forever. User tied to this policy will not expire.`
		Displays the password security policy information for a specific policy.

Step 3	**show aaa common-criteria policy all** **Example:**	Displays password security policy information for all the configured policies.

	Command or Action	Purpose
	Device# **show aaa common-criteria policy all** ========== Policy name: policy1 Minimum length: 1 Maximum length: 64 Upper Count: 20 Lower Count: 20 Numeric Count: 5 Special Count: 2 Number of character changes 4 Valid forever. User tied to this policy will not expire. ========== Policy name: policy2 Minimum length: 1 Maximum length: 34 Upper Count: 10 Lower Count: 5 Numeric Count: 4 Special Count: 2 Number of character changes 2 Valid forever. User tied to this policy will not expire. ==========	

Configuration Example for Password Strength and Management for Common Criteria

The following section provides a configuration example for password strength and management for common criteria.

Example: Password Strength and Management for Common Criteria

The following example shows how to create a common criteria security policy and apply the specific policy to a user profile:

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa common-criteria policy policy1
Device(config-cc-policy)# char-changes 4
Device(config-cc-policy)# max-length 20
Device(config-cc-policy)# min-length 6
Device(config-cc-policy)# numeric-count 2
Device(config-cc-policy)# special-case 2
Device(config-cc-policy)# exit
Device(config)# username user1 common-criteria-policy policy1 password password1
Device(config)# end
```

Additional References for Password Strength and Management for Common Criteria

Related Documents

Related Topic	Document Title
For complete syntax and usage information for the commands used in this chapter.	Consolidated Platform Command Reference, Cisco IOS Release 15.2(7)E (Catalyst 1000 Switches)

RFCs

RFC	Title
RFC 2865	*Remote Authentication Dial-in User Service*
RFC 3576	*Dynamic Authorization Extensions to RADIUS*

Feature History for Password Strength and Management for Common Criteria

This table provides release and related information for features explained in this module.

These features are available on all releases subsequent to the one they were introduced in, unless noted otherwise.

Release	Feature	Feature Information
Cisco IOS Release 15.2(7)E1	Password Strength and Management for Common Criteria	The Password Strength and Management for Common Criteria feature is used to specify password policies and security mechanisms for storing, retrieving, and providing rules to specify user passwords.

Use Cisco Feature Navigator to find information about platform and software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn.