Login Password Retry Lockout

The Login Password Retry Lockout feature allows system administrators to lock out a local authentication, authorization, and accounting (AAA) user account after a configured number of unsuccessful attempts by the user to log in.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Login Password Retry Lockout

- You must be running a Cisco IOS image that contains the AAA component.

Restrictions for Login Password Retry Lockout

- Authorized users can lock themselves out because there is no distinction between an attacker who is guessing passwords and an authorized user who is entering the password incorrectly multiple times.
- A denial of service (DoS) attack is possible; that is, an authorized user could be locked out by an attacker if the username of the authorized user is known to the attacker.

Information About Login Password Retry Lockout

Lock Out of a Local AAA User Account

The Login Password Retry Lockout feature allows system administrators to lock out a local AAA user account after a configured number of unsuccessful attempts by the user to log in using the username that corresponds to the AAA user account. A locked-out user cannot successfully log in again until the user account is unlocked by the administrator.

A system message is generated when a user is either locked by the system or unlocked by the system administrator. The following is an example of such a system message:

```
%AAA-5-USER_LOCKED: User user1 locked out on authentication failure.
```

The system administrator cannot be locked out.

Note The system administrator is a special user who has been configured using the maximum privilege level (root privilege--level 15). A user who has been configured using a lesser privilege level can change the privilege level using the **enable** command. A user that can change to the root privilege (level 15) is able to act as a system administrator.

This feature is applicable to any login authentication method, such as ASCII, Challenge Handshake Authentication Protocol (CHAP), and Password Authentication Protocol (PAP).

Note No messages are displayed to users after authentication failures that are due to the locked status (that is, there is no distinction between a normal authentication failure and an authentication failure due to the locked status of the user).

How to Configure Login Password Retry Lockout

Configuring Login Password Retry Lockout

To configure the Login Password Retry Lockout feature, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **username** *name* [**privilege** *level*] **password** *encryption-type password*
4. **aaa new-model**
5. **aaa local authentication attempts max-fail** *number-of-unsuccessful-attempts*
6. **aaa authentication login default method**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**username** *name* [**privilege** *level*] **password** *encryption-type password* **Example:** `Router(config)# username user1 privilege 15 password 0 cisco`	Establishes a username-based authentication system.
Step 4	**aaa new-model** **Example:** `Router(config)# aaa new-model`	Enables the AAA access control model.
Step 5	**aaa local authentication attempts max-fail** *number-of-unsuccessful-attempts* **Example:** `Router(config)# aaa local authentication attempts max-fail 3`	Specifies the maximum number of unsuccessful attempts before a user is locked out.

	Command or Action	Purpose
Step 6	**aaa authentication login default method** **Example:** `Router(config)# aaa authentication login default local`	Sets the authentication, authorization, and accounting (AAA) authentication method at login. For example, **aaa authentication login default** *local* specifies the local AAA user database.

Unlocking a Login Locked-Out User

To unlock a login locked-out user, perform the following steps.

Note This task can be performed only by users having the root privilege (level 15).

SUMMARY STEPS

1. **enable**
2. **clear aaa local user lockout** {**username** *username* | **all**}

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**clear aaa local user lockout** {**username** *username*	**all**} **Example:** `Router# clear aaa local user lockout username user1`	Unlocks a locked-out user.

Clearing the Unsuccessful Login Attempts of a User

This task is useful for cases in which the user configuration was changed and the unsuccessful login attempts of a user that are already logged must be cleared.

To clear the unsuccessful login attempts of a user that have already been logged, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **clear aaa local user fail-attempts** {**username** *username* | **all**}

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**clear aaa local user fail-attempts** {**username** *username* | **all**} **Example:** `Router# clear aaa local user fail-attempts username user1`	Clears the unsuccessful attempts of the user. • This command is useful for cases in which the user configuration was changed and the unsuccessful attempts that are already logged must be cleared.

Monitoring and Maintaining Login Password Retry Lockout Status

To monitor and maintain the status of the Login Password Retry Lockout configuration, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **show aaa local user lockout**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**show aaa local user lockout** **Example:** `Router# show aaa local user lockout`	Displays a list of the locked-out users for the current login password retry lockout configuration.

Example

The following output shows that user1 is locked out:

```
Router# show aaa local user lockout
           Local-user          Lock time
           user1               04:28:49 UTC Sat Jun 19 2004
```

Configuration Examples for Login Password Retry Lockout

Displaying the Login Password Retry Lockout Configuration Example

The following **show running-config** command output illustrates that the maximum number of failed user attempts has been set for 2 as the login password retry lockout configuration:

```
Router # show running-config
Building configuration...
Current configuration : 1214 bytes
!
version 12.3
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname LAC-2
!
boot-start-marker
boot-end-marker
!
!
username sysadmin
username sysad privilege 15 password 0 cisco
username user1 password 0 cisco
aaa new-model
aaa local authentication attempts max-fail 2
!
!
aaa authentication login default local
aaa dnis map enable
aaa session-id common
```

Additional References

The following sections provide references related to Login Password Retry Lockout.

Related Documents

Related Topic	Document Title
Cisco IOS security commands	*Cisco IOS Security Command Reference*

Standards

Standards	Title
None	--

MIBs

MIBs	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
None	--

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

Feature Information for Login Password Retry Lockout

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1: Feature Information for Login Password Retry Lockout

Feature Name	Releases	Feature Information
Login Password Retry Lockout	Cisco IOS 15.2(1)E	The Login Password Retry Lockout feature allows system administrators to lock out a local AAA user account after a configured number of unsuccessful attempts by the user to log in. This feature was introduced in Cisco IOS Release 12.3(14)T. This feature was integrated into Cisco IOS Release 12.2(33)SRE. The following commands were introduced or modified: **aaa local authentication attempts max-fail**, **clear aaa local user fail-attempts**, **clear aaa local user lockout**.

Glossary

- **local AAA method** --Method by which it is possible to configure a local user database on a router and to have AAA provision authentication or authorization of users from this database.
- **local AAA user** --User who is authenticated using the local AAA method.