



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.

Feature History for Login Password Retry Lockout

Release	Modification
12.3(14)T	This feature was introduced.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

- [Prerequisites for Login Password Retry Lockout, page 1](#)
- [Restrictions for Login Password Retry Lockout, page 2](#)
- [Information About Login Password Retry Lockout, page 2](#)
- [How to Configure Login Password Retry Lockout, page 2](#)
- [Configuration Examples for Login Password Retry Lockout, page 5](#)
- [Additional References, page 6](#)
- [Command Reference, page 7](#)
- [Glossary, page 12](#)

Prerequisites for Login Password Retry Lockout

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



Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Copyright © 2005 Cisco Systems, Inc. All rights reserved.

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

To configure the Login Password Retry Lockout feature, you should understand the following concept:

- [Locking Out a Local AAA User Account, page 2](#)

Locking Out 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. If the user can change to the root privilege (level 15), that user 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

This section contains the following procedures:

- [Configuring Login Password Retry Lockout, page 3](#)
- [Unlocking a Locked-Out User, page 4](#)

- [Clearing the Unsuccessful Attempts of a User, page 4](#)
- [Monitoring and Maintaining Login Password Retry Lockout, page 5](#)

Configuring Login Password Retry Lockout

To configure Login Password Retry Lockout, 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 <i>name</i> [privilege level] password <i>encryption-type password</i> 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.

	Command or Action	Purpose
Step 5	<pre>aaa local authentication attempts max-fail number-of-unsuccessful-attempts</pre> <p>Example: Router (config)# aaa local authentication attempts max-fail 3</p>	Specifies the maximum number of unsuccessful attempts before a user is locked out.
Step 6	<pre>aaa authentication login default method</pre> <p>Example: Router (config)# aaa authentication login default local</p>	Method list for login, specifying to authenticate using the local AAA user database.

Unlocking a Locked-Out User

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



Note

This task can be performed only by users having 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	<pre>enable</pre> <p>Example: Router> enable</p>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	<pre>clear aaa local user lockout {username <i>username</i> all}</pre> <p>Example: Router# clear aaa local user lockout username user1</p>	Unlocks a locked-out user.

Clearing the Unsuccessful Attempts of a User

To clear the unsuccessful 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	<pre>enable</pre> <p>Example: Router> enable </p>	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	<pre>clear aaa local user fail-attempts {username username all}</pre> <p>Example: Router# clear aaa local user fail-attempts username user1 </p>	Clears the unsuccessful attempts of the user. <ul style="list-style-type: none"> 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

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

SUMMARY STEPS

- enable
- show aaa local user locked

DETAILED STEPS

	Command or Action	Purpose
Step 1	<pre>enable</pre> <p>Example: Router> enable </p>	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	<pre>show aaa local user locked</pre> <p>Example: Router# show aaa local user locked </p>	Displays a list of the locked-out users.

Configuration Examples for Login Password Retry Lockout

This section provides the following configuration examples:

- [Login Password Retry Lockout: Example, page 5](#)
- [show aaa local user lockout Command: Example, page 6](#)

Login Password Retry Lockout: Example

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

```

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

```

show aaa local user lockout Command: 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

```

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 , Release 12.3T

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

MIBs	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	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
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	—

Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/public/support/tac/home.shtml

Command Reference

This section documents the following new commands. All other commands used with this feature are documented in the Cisco IOS Release 12.3T command reference publications.

- **aaa local authentication attempts max-fail**
- **clear aaa local user fail-attempts**
- **clear aaa local user lockout**
- **show aaa local user locked**

aaa local authentication attempts max-fail

To specify the maximum number of unsuccessful authentication attempts before a user is locked out, use the **aaa local authentication attempts max-fail** command in global configuration mode. To remove the number of unsuccessful attempts that was set, use the **no** form of this command.

aaa local authentication attempts max-fail *number-of-unsuccessful-attempts*

no aaa local authentication attempts max-fail *number-of-unsuccessful-attempts*

Syntax Description

number-of-unsuccessful-attempts Number of unsuccessful authentication attempts.

Defaults

Login Password Retry Lockout feature is not enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

A system message is generated when a user is either locked by the system or unlocked by the system administrator.

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

An administrator cannot be locked out.



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).



Note

Unconfiguring this command will maintain the status of the user with respect to locked-out or number-of-failed attempts. To clear the existing locked-out or number-of-failed attempts, the system administrator has to explicitly clear the status of the user using **clear** commands.

Examples

The following example illustrates that the maximum number of unsuccessful authentication attempts before a user is locked out has been set for 2:

```
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  
ip subnet-zero
```

Related Commands

Command	Description
clear aaa local user fail-attempts	Clears the unsuccessful login attempts of the user.
clear aaa local user lockout	Unlocks the locked-out user.
show aaa local user locked	Displays a list of all locked-out users.

clear aaa local user fail-attempts

To clear the unsuccessful login attempts of a user, use the **clear aaa local user fail-attempts** command in privileged EXEC mode.

```
clear aaa local user fail-attempts {username username | all}
```

Syntax Description	username <i>username</i>	Name of the user.
	all	Unsuccessful login attempts are cleared for all users.

Defaults Unsuccessful login attempts are not cleared.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.3(14)T	This command was introduced.

Usage Guidelines This command is available only to users having root privilege.

Examples The following example shows that the unsuccessful login attempts for all users will be cleared:

```
Router# clear aaa local user fail-attempts all
```

Related Commands	Command	Description
	aaa local authentication attempts max-fail	Specifies the maximum number of unsuccessful authentication attempts before a user is locked out.
	clear aaa local user lockout	Unlocks the locked-out users.
	show aaa local user locked	Displays a list of all locked-out users.

clear aaa local user logout

To unlock the locked-out users, use the **clear aaa local user logout** command in privileged EXEC mode.

```
clear aaa local user logout {username username | all}
```

Syntax Description

username <i>username</i>	Name of the user to be unlocked.
all	All users are to be unlocked.

Defaults

Locked-out users remain locked out.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

Only a user having root privilege can use this command.

Examples

The following example shows that all locked-out users will be unlocked:

```
Router# clear aaa local user logout all
```

Related Commands

Command	Description
aaa local authentication attempts max-fail	Specifies the maximum number of unsuccessful authentication attempts before a user is locked out.
clear aaa local user fail-attempts	Clears the unsuccessful login attempts of a user.
show aaa local user loced	Displays a list of all locked-out users.

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.

**Note**

Refer to [Internetworking Terms and Acronyms](#) for terms not included in this glossary.

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

Copyright © 2005 Cisco Systems, Inc. All rights reserved.