



# Cisco IOS Login Enhancements (Login Block)

---

**Document First Published: August 2005**  
**Last Updated: July 2007**

The Cisco IOS Login Enhancements (Login Block) feature allows users to enhance the security of a router by configuring options to automatically block further login attempts when a possible denial-of-service (DoS) attack is detected.

The login block and login delay options introduced by this feature can be configured for Telnet or SSH virtual connections. By enabling this feature, you can slow down “dictionary attacks” by enforcing a “quiet period” if multiple failed connection attempts are detected, thereby protecting the routing device from a type of denial-of-service attack.

## Feature History for Cisco IOS Login Enhancements

Release	Modification
12.3(4)T	This feature was introduced.
12.2(25)S	This feature was integrated into Cisco IOS Release 12.2 S.
12.2(33)SRA	This feature was integrated into Cisco IOS Release 12.2 SR.

## 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

- [Information About Cisco IOS Login Enhancements, page 1798](#)
- [How to Configure Cisco IOS Login Enhancements, page 1800](#)
- [Configuration Examples for Login Parameters, page 1803](#)
- [Additional References, page 1804](#)
- [Command Reference, page 1805](#)



---

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

Copyright © 2003-2007 Cisco Systems, Inc. All rights reserved.

# Information About Cisco IOS Login Enhancements

To use login enhancements, you should understand the following concepts:

- [Protecting Against Denial of Service and Dictionary Login Attacks](#)
- [Login Enhancements Functionality Overview, page 1798](#)

## Protecting Against Denial of Service and Dictionary Login Attacks

Connecting to a routing device for the purposes of administering (managing) the device, at either the User or Executive level, is most frequently performed using Telnet or SSH (secure shell) from a remote console (such as a PC). SSH provides a more secure connection option because communication traffic between the user's device and the managed device are encrypted. The Login Block capability, when enabled, applies to both Telnet connections and SSH connections.

The automated activation and logging of the Login Block and Quiet Period capabilities introduced by this feature are designed to further enhance the security of your devices by specifically addressing two well known methods that individuals use to attempt to disrupt or compromise networked devices.

If the connection address of a device is discovered and is reachable, a malicious user may attempt to interfere with the normal operations of the device by flooding it with connection requests. This type of attack is referred to as an attempted Denial-of-Service, because it is possible that the device may become too busy trying to process the repeated login connection attempts to properly handle normal routing services or will not be able to provide the normal login service to legitimate system administrators.

The primary intention of a dictionary attack, unlike a typical DoS attack, is to actually gain administrative access to the device. A dictionary attack is an automated process to attempt to login by attempting thousands, or even millions, of username/password combinations. (This type of attack is called a "dictionary attack" because it typically uses, as a start, every word found in a typical dictionary as a possible password.) As scripts or programs are used to attempt this access, the profile for such attempts is typically the same as for DoS attempts; multiple login attempts in a short period of time.

By enabling a detection profile, the routing device can be configured to react to repeated failed login attempts by refusing further connection request (login blocking). This block can be configured for a period of time, called a "quiet period". Legitimate connection attempts can still be permitted during a quiet period by configuring an access-list (ACL) with the addresses that you know to be associated with system administrators.

## Login Enhancements Functionality Overview

To better configure security for virtual login connections, the following requirements have been added to the login process:

- [Delays Between Successive Login Attempts](#)
- [Login Shutdown If DoS Attacks Are Suspected](#)
- [Generation of System Logging Messages for Login Detection](#)

## Delays Between Successive Login Attempts

A Cisco IOS device can accept virtual connections as fast as they can be processed. Introducing a delay between login attempts helps to protect the Cisco IOS software-based device against malicious login connections such as dictionary attacks and DoS attacks. Delays can be enabled in one of the following ways:

- Via the **auto secure** command. If you enable the AutoSecure feature, the default login delay time of one second is automatically enforced.
- Via the **login block-for** command. You must enter this command before issuing the **login delay** command. If you enter only the **login block-for** command, the default login delay time of one second is automatically enforced.
- Via the new global configuration mode command, **login delay**, which allows you to specify a the login delay time to be enforced, in seconds.

## Login Shutdown If DoS Attacks Are Suspected

If the configured number of connection attempts fail within a specified time period, the Cisco IOS device will not accept any additional connections for a “quiet period.” (Hosts that are permitted by a predefined access-control list [ACL] are excluded from the quiet period.)

The number of failed connection attempts that trigger the quiet period can be specified via the new global configuration mode command **login block-for**. The predefined ACL that is excluded from the quiet period can be specified via the new global configuration mode command **login quiet-mode access-class**.

This functionality is disabled by default, and it is not enabled if autosecure is enabled.

## Generation of System Logging Messages for Login Detection

After the router switches to and from quiet mode, logging messages are generated. Also, if configured, logging messages are generated upon every successful or failed login request.

Logging messages can be generated for successful login requests via the new global configuration command **login on-success**; the **login on-failure** command generates logs for failed login requests.

Logging messages for failed login attempts are automatically enabled when the **auto secure** command is issued; they are not automatically enabled for successful login attempts via autosecure.



### Note

Currently, only system logging (syslog) messages can be generated for login-related events. Support for SNMP notifications (traps) will be added in a later release.

### System Logging Messages for a Quiet Period

The following logging message is generated after the router switches to quiet-mode:

```
00:04:07:%SEC_LOGIN-1-QUIET_MODE_ON:Still timeleft for watching failures is 158 seconds,
[user:sfd] [Source:10.4.2.11] [localport:23] [Reason:Invalid login], [ACL:22] at 16:17:23
UTC Wed Feb 26 2003
```

The following logging message is generated after the router switches from quiet mode back to normal mode:

```
00:09:07:%SEC_LOGIN-5-QUIET_MODE_OFF:Quiet Mode is OFF, because block period timed out at
16:22:23 UTC Wed Feb 26 2003
```

### System Logging Messages for Successful and Failed Login Requests

The following logging message is generated upon a successful login request:

```
00:04:32:%SEC_LOGIN-5-LOGIN_SUCCESS:Login Success [user:test] [Source:10.4.2.11]
[localport:23] at 20:55:40 UTC Fri Feb 28 2003
```

The following logging message is generated upon a failed login request:

```
00:03:34:%SEC_LOGIN-4-LOGIN_FAILED:Login failed [user:sdfs] [Source:10.4.2.11]
[localport:23] [Reason:Invalid login] at 20:54:42 UTC Fri Feb 28 2003
```

## How to Configure Cisco IOS Login Enhancements

This section contains the following procedures:

- [Configuring Login Parameters, page 1800](#) (Required)
- [Verifying Login Parameters, page 1801](#) (Optional)

## Configuring Login Parameters

Use this task to configure your Cisco IOS device for login parameters that help detect suspected DoS attacks and slow down dictionary attacks.

### Login Parameter Defaults

All login parameters are disabled by default. You must issue the **login block-for** command, which enables default login functionality, before using any other login commands. After the **login block-for** command is enabled, the following defaults are enforced:

- A default login delay of one second
- All login attempts made via Telnet or SSH are denied during the quiet period; that is, no ACLs are exempt from the login period until the **login quiet-mode access-class** command is issued.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **login block-for** *seconds* **attempts** *tries* **within** *seconds*
4. **login quiet-mode access-class** {*acl-name* | *acl-number*}
5. **login delay** *seconds*
6. **login on-failure log** [*every login*]
7. **login on-success log** [*every login*]

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code>  <b>Example:</b> Router> enable	Enables privileged EXEC mode.  • Enter your password if prompted.
Step 2	<code>configure terminal</code>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<code>login block-for seconds attempts tries within seconds</code>  <b>Example:</b> Router(config)# login block-for 100 attempts 2 within 100	Configures your Cisco IOS device for login parameters that help provide DoS detection.  <b>Note</b> This command must be issued before any other login command can be used.
Step 4	<code>login quiet-mode access-class {acl-name   acl-number}</code>  <b>Example:</b> Router(config)# login quiet-mode access-class myacl	(Optional) Specifies an ACL that is to be applied to the router when it switches to quiet mode.  If this command is not enabled, all login requests will be denied during quiet mode.
Step 5	<code>login delay seconds</code>  <b>Example:</b> Router(config)# login delay 10	(Optional) Configures a delay between successive login attempts.
Step 6	<code>login on-failure log [every login]</code>  <b>Example:</b> Router(config)# login on-failure log	(Optional) Generates logging messages for failed login attempts.
Step 7	<code>login on-success log [every login]</code>  <b>Example:</b> Router(config)# login on-success log every 5	(Optional) Generates logging messages for successful login attempts.

## What to Do Next

After you have configured login parameters on your router, you may wish to verify the settings. To complete this task, see the following section [“Verifying Login Parameters.”](#)

## Verifying Login Parameters

Use this task to verify the applied login configuration and present login status on your router.

## SUMMARY STEPS

1. **enable**
2. **show login [failures]**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>show login [failures]</b>  <b>Example:</b> Router# show login	Displays login parameters. <ul style="list-style-type: none"> <li>• <b>failures</b>—Displays information related only to failed login attempts.</li> </ul>

## Examples

The following sample output from the **show login** command verifies that no login parameters have been specified:

```
Router# show login

No login delay has been applied.
No Quiet-Mode access list has been configured.
All successful login is logged and generate SNMP traps.
All failed login is logged and generate SNMP traps

Router NOT enabled to watch for login Attacks
```

The following sample output from the **show login** command verifies that the **login block-for** command is issued. In this example, the command is configured to block login hosts for 100 seconds if 16 or more login requests fail within 100 seconds; five login requests have already failed.

```
Router# show login

A default login delay of 1 seconds is applied.
No Quiet-Mode access list has been configured.
All successful login is logged and generate SNMP traps.
All failed login is logged and generate SNMP traps.

Router enabled to watch for login Attacks.
If more than 15 login failures occur in 100 seconds or less, logins will be disabled for
100 seconds.

Router presently in Watch-Mode, will remain in Watch-Mode for 95 seconds.
Present login failure count 5.
```

The following sample output from the **show login** command verifies that the router is in quiet mode. In this example, the **login block-for** command was configured to block login hosts for 100 seconds if 3 or more login requests fail within 100 seconds.

```
Router# show login

A default login delay of 1 seconds is applied.
```

```
No Quiet-Mode access list has been configured.
All successful login is logged and generate SNMP traps.
All failed login is logged and generate SNMP traps.
```

```
Router enabled to watch for login Attacks.
If more than 2 login failures occur in 100 seconds or less, logins will be disabled for
100 seconds.
```

```
Router presently in Quiet-Mode, will remain in Quiet-Mode for 93 seconds.
Denying logins from all sources.
```

The following sample output from **show login failures** command shows all failed login attempts on the router:

```
Router# show login failures
```

```
Information about login failure's with the device
```

Username	Source IPAddr	lPort	Count	TimeStamp
try1	10.1.1.1	23	1	21:52:49 UTC Sun Mar 9 2003
try2	10.1.1.2	23	1	21:52:52 UTC Sun Mar 9 2003

The following sample output from **show login failures** command verifies that no information is presently logged:

```
Router# show login failures
```

```
*** No logged failed login attempts with the device.***
```

## Configuration Examples for Login Parameters

This section includes the following example:

- [Setting Login Parameters: Example, page 1803](#)

### Setting Login Parameters: Example

The following example shows how to configure your router to enter a 100 second quiet period if 15 failed login attempts is exceeded within 100 seconds; all login requests will be denied during the quiet period except hosts from the ACL "myacl." Also, logging messages will be generated for every 10th failed login and every 15th successful login.

```
Router(config)# login block-for 100 attempts 15 within 100
Router(config)# login quiet-mode access-class myacl
Router(config)# login on-failure log every 10
Router(config)# login on-success log every 15
```

## Additional References

The following sections provide references related to Cisco IOS Login Enhancements.

### Related Documents

Related Topic	Document Title
AutoSecure	<ul style="list-style-type: none"> <li>• <i>AutoSecure</i> (Cisco IOS Release 12.3(1) feature module)</li> <li>• Cisco IOS Security Configuration Guides, Release 12.4.</li> </ul>
Secure Management/Administrative Access	Role-Based CLI Access

### Standards

Standards	Title
None	—

### MIBs

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

### RFCs

RFCs	Title
None	—

### Technical Assistance

Description	Link
<p>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.</p>	<p><a href="http://www.cisco.com/public/support/tac/home.shtml">http://www.cisco.com/public/support/tac/home.shtml</a></p>



# Command Reference

The following new commands are pertinent to this feature. To see the command pages for these commands and other commands used with this feature, go to the *Cisco IOS Master Commands List*, Release 12.4, at <http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124mindx/124index.htm>.

- **login block-for**
- **login delay**
- **login on-failure**
- **login on-success**
- **login quiet-mode access-class**
- **show login**

---

CCVP, the Cisco logo, and the Cisco Square Bridge logo 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, BPX, 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, Networking Academy, Network Registrar, Packet, 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. (0705R)

h\_login.fm-v10 © 2003-2007 Cisco Systems, Inc. All rights reserved.

