

# Automated Double Authentication

---

## Feature Summary

The automated double authentication feature enhances the existing double authentication feature.

Previously, with the existing double authentication feature, a second level of user authentication is achieved when the user Telnets to the network access server or router and enters a username and password. Now, with automated double authentication, the user does not have to Telnet anywhere but instead responds to a dialog box that requests a username and password or PIN.

(For information about the existing double authentication feature, refer to the “Configuring Authentication” chapter of the Cisco IOS Release 11.3 *Security Configuration Guide*.)

## Benefits

This feature has all the security benefits of double authentication, but provides a simpler, more user-friendly interface for remote users. Users are no longer required to Telnet to a remote device; they can simply respond to on-screen dialogs.

## Restrictions

The remote user hosts must be running a companion client application. As of the first publication of this document, the only client application software available is the Glacier Bay application server software for PCs.

Automated double authentication, like the existing double authentication feature, is for Multilink PPP ISDN connections only. Automated double authentication cannot be used with other protocols such as X.25 or SLIP.

## Platforms

This feature is supported on all Cisco hardware platforms.

## Prerequisites

Before configuring or using automated double authentication, you must accomplish the following:

- You must configure double authentication (as described in the “Configuring Authentication” chapter of the Cisco IOS Release 11.3 *Security Configuration Guide*.)
- You must ensure that participating remote hosts have the appropriate client software loaded—for example, the Glacier Bay PC application server software for PCs.

## Supported MIBs and RFCs

No new MIBs or RFCs are supported by this feature.

## Configuration Tasks

After you have configured double authentication (see “Prerequisites”), you can configure the automation enhancement.

To configure automated double authentication, complete the following tasks, starting in global configuration mode:

Task	Command
Enable automation of double authentication.	<b>ip trigger-authentication</b> [timeout <i>seconds</i> ] [port <i>number</i> ]
Select an ISDN BRI or ISDN PRI interface. (This puts you into interface configuration mode.)	<b>interface bri</b> <i>number</i> or <b>interface serial</b> <i>number:23</i>
Apply automated double authentication to the interface.	<b>ip trigger-authentication</b>

To troubleshoot automated double authentication, perform the following tasks in privileged EXEC mode:

Task	Command
View the list of remote hosts for which automated double authentication has been attempted (successfully or unsuccessfully).	<b>show ip trigger-authentication</b>
Clear the list of remote hosts for which automated double authentication has been attempted. (This clears the table displayed by the <b>show ip trigger-authentication</b> command.)	<b>clear ip trigger-authentication</b>
View <b>debug</b> output related to automated double authentication.	<b>debug ip trigger-authentication</b>

## Configuration Example

This example shows a complete configuration file for a Cisco 2509 router with automated double authentication configured. The configuration commands that apply to automated double authentication are preceded by descriptions with a double asterisk (\*\*).

```
Current configuration:
!
version 11.3
no service password-encryption
!
hostname myrouter
!
!
! **The following AAA commands are used to configure double authentication:
!
! **The following command enables AAA:
aaa new-model
! **The following command enables user authentication via the TACACS+ AAA server:
aaa authentication login default tacacs+
aaa authentication login console none
! **The following command enables device authentication via the TACACS+ AAA server:
aaa authentication ppp default tacacs+
! **The following command causes the remote user's authorization profile
!         to be downloaded from the AAA server to the Cisco 2509 router when required:
aaa authorization exec tacacs+
! **The following command causes the remote device's authorization profile
!         to be downloaded from the AAA server to the Cisco 2509 router when required:
aaa authorization network tacacs+
enable password mypassword
!
ip host blue 172.21.127.226
ip host green 172.21.127.218
ip host red 172.21.127.114
ip domain-name mycompany.com
ip name-server 171.69.2.75
! **The following command globally enables automated double authentication:
ip trigger-authentication timeout 60 port 7500
isdn switch-type basic-5ess
!
!
interface Ethernet0
 ip address 172.21.127.186 255.255.255.248
 no ip route-cache
 no ip mroute-cache
 no keepalive
 ntp disable
 no cdp enable
!
interface Virtual-Template1
 ip unnumbered Ethernet0
 no ip route-cache
 no ip mroute-cache
!
interface Serial0
 ip address 172.21.127.105 255.255.255.248
 encapsulation ppp
 no ip mroute-cache
 no keepalive
 shutdown
 clockrate 2000000
 no cdp enable
!
```

## Configuration Example

```
interface Serial1
  no ip address
  no ip route-cache
  no ip mroute-cache
  shutdown
  no cdp enable
!
! **Automated double authentication occurs via the ISDN BRI interface BRI0:
interface BRI0
  ip unnumbered Ethernet0
! **The following command turns on automated double authentication at this interface:
  ip trigger-authentication
! **PPP encapsulation is required:
  encapsulation ppp
  no ip route-cache
  no ip mroute-cache
  dialer idle-timeout 500
  dialer map ip 172.21.127.113 name myrouter 60074
  dialer-group 1
  no cdp enable
! **The following command specifies that device authentication occurs via PPP CHAP:
  ppp authentication chap
!
router eigrp 109
  network 172.21.0.0
  no auto-summary
!
ip default-gateway 172.21.127.185
no ip classless
ip route 172.21.127.114 255.255.255.255 172.21.127.113
! **Virtual profiles are required for double authentication to work:
virtual-profile virtual-template 1
dialer-list 1 protocol ip permit
no cdp run
! **The following command defines where the TACACS+ AAA server is:
tacacs-server host 171.69.57.35 port 1049
tacacs-server timeout 90
! **The following command defines the key to use with TACACS+ traffic (required):
tacacs-server key mytacacskey
snmp-server community public RO
!
line con 0
  exec-timeout 0 0
  login authentication console
line aux 0
  transport input all
line vty 0 4
  exec-timeout 0 0
  password lab
!
end
```

## Command Reference

This section documents new or modified commands. All other commands used with this feature are documented in the Cisco IOS Release 11.3 command references.

- **clear ip trigger-authentication**
- **ip trigger-authentication (global configuration)**
- **ip trigger-authentication (interface configuration)**
- **show ip trigger-authentication**

## clear ip trigger-authentication

To clear the list of remote hosts for which automated double authentication has been attempted, use the **clear ip trigger-authentication** privileged EXEC configuration command.

**clear ip trigger-authentication**

### Syntax Description

This command has no arguments or keywords.

### Default

Table entries are cleared after a timeout if you do not clear them manually with this command.

### Command Mode

Privileged EXEC

### Usage Guidelines

This command first appeared in Cisco IOS Release 11.3 T.

Use this command when troubleshooting automated double authentication. This command clears the entries in the list of remote hosts displayed by the **show ip trigger-authentication** command.

### Examples

The following example clears the remote host table:

```
router# show ip trigger-authentication
Trigger-authentication Host Table:
Remote Host      Time Stamp
172.21.127.114   2940514234
router# clear ip trigger-authentication
router# show ip trigger-authentication
router#
```

### Related Commands

**show ip trigger-authentication**

## ip trigger-authentication (global configuration)

To enable the automated part of double authentication at a device, use the **ip trigger-authentication** global configuration command. Use the **no** form of this command to disable the automated part of double authentication.

```
ip trigger-authentication [timeout seconds] [port number]  
no ip trigger-authentication
```

### Syntax Description

**timeout** *seconds* (Optional) Specifies how frequently the local device sends a UDP packet to the remote host to request the user's username and password (or PIN). The default is 90 seconds. See "The Timeout Keyword" below for details.

**port** *number* (Optional) Specifies the UDP port to which the local router should send the UPD packet requesting the user's username and password (or PIN). The default is port 7500. See "The Port Keyword" below for details.

### Default

The default timeout is 90 seconds, and the default port number is 7500.

### Command Mode

Global configuration

### Usage Guidelines

This command first appeared in Cisco IOS Release 11.3 T.

Configure this command on the local device (router or network access server) that remote users dial into. Use this command only if the local device has already been configured to provide double authentication; this command enables automation of the second authentication of double authentication.

### The Timeout Keyword

During the second authentication stage of double authentication—when the remote user is authenticated—the remote user must send a username and password (or PIN) to the local device. With automated double authentication, the local device sends a UDP packet to the remote user's host during the second user-authentication stage. This UDP packet triggers the remote host to launch a dialog box requesting a username and password (or PIN).

If the local device does not receive a valid response to the UDP packet within a timeout period, the local device will send another UDP packet. The device will continue to send UDP packets at the timeout intervals until it receives a response and can authenticate the user.

By default, the UDP packet timeout interval is 90 seconds. Use the **timeout** keyword to specify a different interval.

(This timeout also applies to how long entries will remain in the remote host table; see the **show ip trigger-authentication** command for details.)

### The Port Keyword

As described in the previous section, the local device sends a UDP packet to the remote user's host to request the user's username and password (or PIN). This UDP packet is sent to UDP port 7500 by default. (The remote host client software listens to UDP port 7500 by default.) If you need to change the port number because port 7500 is in use by another application, you should change the port number using the **port** keyword. If you change the port number you need to change it in both places—both on the local device and in the remote host client software.

### Examples

The following example globally enables automated double authentication and resets the timeout to 120 seconds:

```
ip trigger-authentication timeout 120
```

### Related Commands

**ip trigger-authentication (interface configuration)**

## ip trigger-authentication (interface configuration)

To specify automated double authentication at an interface, use the **ip trigger-authentication** interface configuration command. Use the **no** form of this command to turn off automated double authentication at an interface.

**ip trigger-authentication**  
**no ip trigger-authentication**

### Syntax Description

This command has no arguments or keywords.

### Default

Automated double authentication is not enabled for specific interfaces.

### Command Mode

Interface configuration

### Usage Guidelines

This command first appeared in Cisco IOS Release 11.3 T.

Configure this command on the local router or network access server that remote users dial into. Use this command only if the local device has already been configured to provide double authentication and if automated double authentication has been enabled with the **ip trigger-authentication (global configuration)** command.

This command causes double authentication to occur automatically when users dial into the interface.

### Examples

The following example turns on automated double authentication at the ISDN BRI interface BRI0:

```
interface BRI0
 ip trigger-authentication
 encapsulation ppp
 ppp authentication chap
```

### Related Commands

**ip trigger-authentication (global configuration)**

## show ip trigger-authentication

To view the list of remote hosts for which automated double authentication has been attempted, use the **show ip trigger-authentication** privileged EXEC command.

**show ip trigger-authentication**

### Syntax Description

This command has no arguments or keywords.

### Command Mode

Privileged EXEC

### Usage Guidelines

This command first appeared in Cisco IOS Release 11.3 T.

Whenever a remote user needs to be user-authenticated in the second stage of automated double authentication, the local device sends a UDP packet to the remote user's host. Whenever such a UDP packet is sent, the user's host IP address is added to a table. If additional UDP packets are sent to the same remote host, a new table entry is not created; instead, the existing entry is updated with a new time stamp. This remote host table contains a cumulative list of host entries; entries are deleted after a timeout period or after you manually clear the table using the **clear ip trigger-authentication** command. You can change the timeout period with the **ip trigger-authentication (global configuration)** command.

Use this command to view the list of remote user's hosts for which automated double authentication has been attempted.

### Sample Display

The following is sample output from the **show ip trigger-authentication** command:

```
myfirewall# show ip trigger-authentication
Trigger-authentication Host Table:
Remote Host      Time Stamp
172.21.127.114   2940514234
```

This output shows that automated double authentication was attempted for a remote user; the remote user's host has the IP address 172.21.127.114. The attempt to automatically double authenticate occurred when the local host (myfirewall) sent the remote host (172.21.127.114) a packet to UDP port 7500. (The default port was not changed in this example.)

### Related Commands

**clear ip trigger-authentication**

## Debug Command

This section documents the new **debug** command introduced for automated double authentication.

### debug ip trigger-authentication

Use the **debug ip trigger-authentication** command to display information related to automated double authentication. The **no** form of this command disables debugging output.

[no] **debug ip trigger-authentication** [verbose]

#### Syntax Description

**verbose** (Optional) Specifies that the complete debugging output be displayed, including information about packets that are blocked before authentication is complete.

#### Usage Guidelines

This command first appeared in Cisco IOS Release 11.3 T.

Use this command when troubleshooting automated double authentication.

This command displays information about the remote host table—whenever entries are added, updated, or removed, a new debugging message is displayed.

What is the remote host table? Whenever a remote user needs to be user-authenticated in the second stage of automated double authentication, the local device sends a UDP packet to the remote user's host. Whenever such a UDP packet is sent, the user's host IP address is added to a table. If additional UDP packets are sent to the same remote host, a new table entry is not created; instead, the existing entry is updated with a new time stamp. This remote host table contains a cumulative list of host entries; entries are deleted after a timeout period or after you manually clear the table using the **clear ip trigger-authentication** command.

If you include the **verbose** keyword, the debugging output also includes information about packet activity.

#### Sample Display

The following example shows sample **debug ip trigger-authentication** output.

In this example, the local device at 172.21.127.186 sends a UDP packet to the remote host at 172.21.127.114. The UDP packet is sent to request the remote user's username and password (or PIN). (The output indicates "New entry added.")

After a timeout period, the local device has not received a valid response from the remote host, so the local device sends another UDP packet. (The output indicates "Time stamp updated.")

**Debug Command**

---

Then the remote user is authenticated, and after a length of time (the timeout period) the entry is removed from the remote host table. (The output indicates “remove obsolete entry.”)

```
myfirewall# debug ip trigger-authentication
TRIGGER_AUTH: UDP sent from 172.21.127.186 to 172.21.127.114, qdata=7C2504
                New entry added, timestamp=2940514234
TRIGGER_AUTH: UDP sent from 172.21.127.186 to 172.21.127.114, qdata=7C2504
                Time stamp updated, timestamp=2940514307
TRIGGER_AUTH: remove obsolete entry, remote host=172.21.127.114
```

The following example shows sample output for **debug ip trigger-authentication verbose**.

In this example, messages about packet activity are included because of the use of the **verbose** keyword.

You can see many packets that are being blocked at the interface because the user has not yet been double authenticated. These packets will be permitted through the interface only after the user has been double authenticated. (You can see packets being blocked when the output indicates “packet enqueued” then “packet ignored.”)

```
TRIGGER_AUTH: packet enqueued, qdata=69FEEC
                remote host=172.21.127.113, local host=172.21.127.186 (if: 0.0.0.0)
TRIGGER_AUTH: UDP sent from 172.21.127.186 to 172.21.127.113, qdata=69FEEC
                Time stamp updated
TRIGGER_AUTH: packet enqueued, qdata=69FEEC
                remote host=172.21.127.113, local host=172.21.127.186 (if: 0.0.0.0)
TRIGGER_AUTH: packet ignored, qdata=69FEEC
TRIGGER_AUTH: packet enqueued, qdata=69FEEC
                remote host=172.21.127.113, local host=172.21.127.186 (if: 0.0.0.0)
TRIGGER_AUTH: packet ignored, qdata=69FEEC
TRIGGER_AUTH: packet enqueued, qdata=69FEEC
                remote host=172.21.127.113, local host=172.21.127.186 (if: 0.0.0.0)
TRIGGER_AUTH: UDP sent from 172.21.127.186 to 172.21.127.113, qdata=69FEEC
                Time stamp updated
TRIGGER_AUTH: packet enqueued, qdata=69FEEC
                remote host=172.21.127.113, local host=172.21.127.186 (if: 0.0.0.0)
TRIGGER_AUTH: packet ignored, qdata=69FEEC
TRIGGER_AUTH: packet enqueued, qdata=69FEEC
                remote host=172.21.127.113, local host=172.21.127.186 (if: 0.0.0.0)
TRIGGER_AUTH: packet ignored, qdata=69FEEC
```