



# Firewall Authentication Proxy for FTP and Telnet Sessions

---

Before the introduction of the Firewall Authentication Proxy for FTP and Telnet Sessions feature, users could enable only HTTP when configuring authentication proxy. This feature introduces support for FTP and Telnet, providing users with three protocol options when configuring authentication proxy.

## Feature Specifications for the Firewall Authentication Proxy for FTP and Telnet Sessions Feature

---

### Feature History

Release	Modification
12.3(1)	This feature was introduced.

---

### Supported Platforms

For platforms supported in Cisco IOS Release 12.3(1), consult Cisco Feature Navigator.

---

## 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

- [Restrictions for Firewall Authentication Proxy for FTP and Telnet Sessions, page 2](#)
- [Information About Firewall Authentication Proxy for FTP and Telnet Sessions, page 2](#)
- [How to Configure FTP or Telnet Authentication Proxy, page 7](#)
- [Configuration Examples for FTP and Telnet Authentication Proxy, page 12](#)
- [Additional References, page 15](#)
- [Command Reference, page 17](#)



---

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

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

# Restrictions for Firewall Authentication Proxy for FTP and Telnet Sessions

- Authentication proxy is an IP-only feature; thus, it comes with only -o3 images.
- “proxyacl#<n>” is the only supported attribute in the authentication, authorization, and accounting (AAA) server’s user configuration.
- Authentication proxy is subjected only to the traffic that passes through the router; traffic that is destined for the router continues to be authenticated by the existing authentication methods that are provided by Cisco IOS.

## Information About Firewall Authentication Proxy for FTP and Telnet Sessions

To configure the Authentication Proxy for FTP and Telnet Sessions feature, you must understand the following concepts:

- [Feature Design for FTP and Telnet Authentication Proxy, page 2](#)
- [Absolute Timeout, page 7](#)

## Feature Design for FTP and Telnet Authentication Proxy

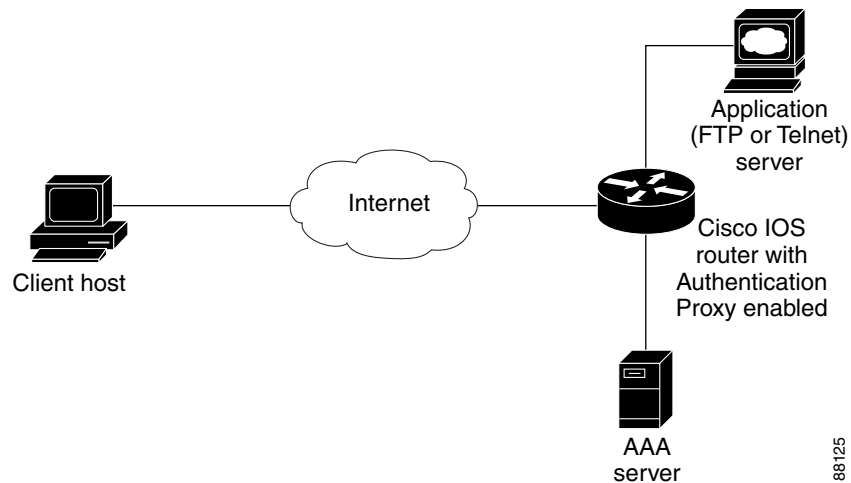
Authentication proxy for FTP and Telnet Sessions functions like authentication proxy for HTTP; that is, FTP and Telnet are independent components in the Cisco IOS software and can be enabled or disabled on the interface of an unauthenticated host.

Many of the authentication proxy for FTP or Telnet functions are similar to those used with HTTP, such as the interaction between the authentication proxy router and the AAA server during authentication. However, because of protocol differences, FTP and Telnet login methods are different from HTTP.

## FTP and Telnet Login Methods

[Figure 1](#) displays a typical authentication proxy topology.

**Figure 1** Typical Authentication Proxy Topology



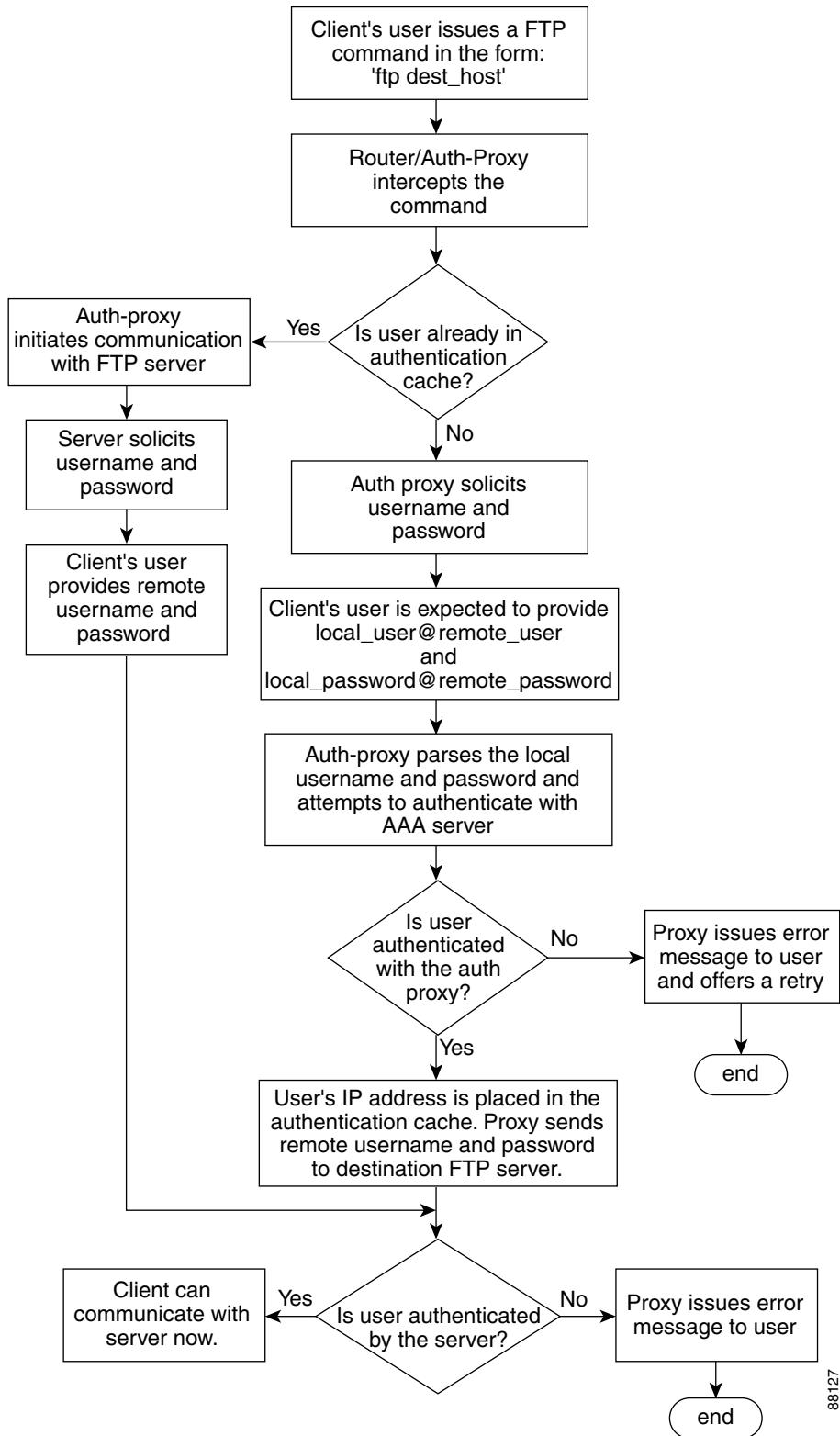
Just as with HTTP, the authentication proxy router intercepts traffic that is sent from the client host. Upon receiving a FTP or Telnet packet, the router will look into its authentication cache to check whether the client host has already been authenticated. If it has been authenticated, the router will forward the client host's traffic to the FTP or Telnet server for additional authentication. If the IP address of the client host is not in the cache of the router, the router will try to authenticate the client host with the AAA server using the username and password of the router.

## FTP Login

For FTP login, the client host will be prompted (by the authentication proxy router) for the username and password of the router; the client must respond with the username and password in the following format: "login: proxy\_username@ftp\_username" and "password: proxy\_passwd@ftp\_passwd:". The authentication proxy will use the proxy\_username and password to verify the client's profile against the AAA server's user database. After the client is successfully authenticated with the AAA server, the authentication proxy will pass the FTP (remote) username and password to the FTP server (destination server) for the application server authentication.

A flow chart that depicts an overview of the FTP authentication proxy process is shown in [Figure 2](#).

Figure 2 FTP Authentication Proxy Overview



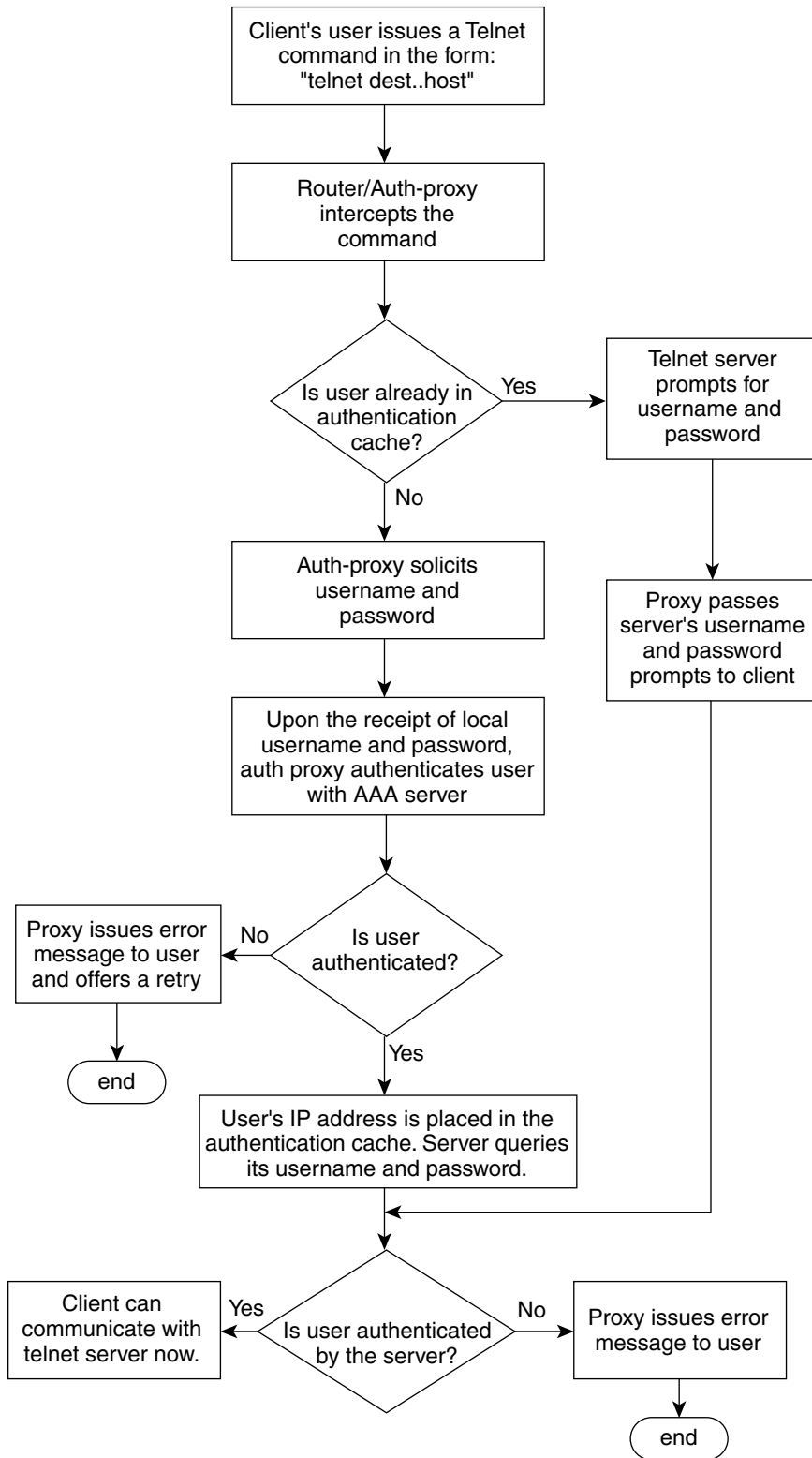
88127

## Telnet Login

For Telnet login, the client host will be prompted (by the authentication proxy router) for the username, followed by the password; the client must respond with the username and password in the following format: “login: proxy\_username:” and “password: proxy\_passwd:”. The username and password will be verified against the AAA server’s user database. After the client is successfully authenticated with the AAA server, the Telnet server (destination server) will prompt the client for the username and password of the Telnet server.

A flow chart that depicts an overview of the Telnet authentication proxy process is shown in [Figure 3](#).

Figure 3 Telnet Authentication Proxy Overview



88126

If authentication with the AAA server fails, the proxy will inform the client accordingly. With Telnet, the proxy does not have any interest in the Telnet server's username and password. If the client is authenticated with the AAA server but fails with the Telnet server, the client will not have to authenticate with the AAA server the next time he or she logs into the network; the client's IP address will be stored in the authentication cache. The client will have to authenticate only with the Telnet server.

**Note**

With FTP, the client must always reenter the local and remote username and password combination every time he or she tries to log into the network—regardless of a successful AAA server authentication.

## Absolute Timeout

An absolute timeout value has been added to allow users to configure a window during which the authentication proxy on the enabled interface is active. After the absolute timer expires, the authentication proxy will be disabled regardless of any activity. The absolute timeout value can be configured per protocol (via the **ip auth-proxy name** command) or globally (via the **ip auth-proxy** command). The default value of the absolute timeout is zero; that is, the absolute timer is turned off by default, and the authentication proxy is enabled indefinitely and is subject only to the timeout specified by the **inactivity-timer** keyword.

**Note**

The **inactivity-timer** keyword deprecates the **auth-cache-time** keyword in the **ip auth-proxy name** and the **ip auth-proxy** commands.

## How to Configure FTP or Telnet Authentication Proxy

To enable FTP or Telnet authentication proxy, you must enable AAA services, configure the FTP or Telnet server, and enable authentication proxy. This section contains the following procedures:

- [Configuring AAA, page 7](#)
- [Configuring the Authentication Proxy, page 9](#)
- [Verifying FTP or Telnet Authentication Proxy, page 11](#)
- [Monitoring and Maintaining FTP or Telnet Authentication Proxy Sessions, page 12](#)

## Configuring AAA

To use authentication proxy, you must configure a AAA server for authentication. The authentication proxy service of the AAA server must also be configured for authorization. To configure these tasks, perform the following steps:

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa authentication login default group tacacs+ group radius**

5. **aaa authorization auth-proxy default** [[group tacacs+] [group radius]]
6. **aaa authorization exec default** [group tacacs+] [group radius]
7. **aaa accounting auth-proxy default stop-only** [group tacacs+] [group radius]
8. **access-list** *access-list-number* {permit | deny} {tcp | ip | icmp} host *source* eq *tacacs* host *destination*

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables higher privilege levels, such as privileged EXEC mode.  Enter your password if prompted.
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>aaa new-model</b>  <b>Example:</b> Router (config)# aaa new-model	Enables the AAA functionality on the router.
Step 4	<b>aaa authentication login default group tacacs+ group radius</b>  <b>Example:</b> Router (config)# aaa authentication login default group tacacs+ group radius	Defines the list of authentication methods at login.
Step 5	<b>aaa authorization auth-proxy default</b> [[group tacacs+] [group radius]]  <b>Example:</b> Router (config)# aaa authorization auth-proxy default group tacacs+ group radius	Uses the <b>auth-proxy</b> keyword to enable authorization proxy for AAA methods.
Step 6	<b>aaa authorization exec default</b> [group tacacs+] [group radius]  <b>Example:</b> Router (config)# aaa authorization exec default group tacacs+ group radius	Enables authorization for TACACS+ and RADIUS.

	Command or Action	Purpose
Step 7	<pre>aaa accounting auth-proxy default stop-only [group tacacs+] [group radius]</pre> <p><b>Example:</b></p> <pre>Router (config)# aaa accounting auth-proxy default stop-only group tacacs+ group radius</pre>	Activates authentication proxy accounting and uses the <b>auth-proxy</b> keyword to set up the authorization policy as dynamic access control lists (ACLs) that can be downloaded.
Step 8	<pre>access-list access-list-number {permit   deny} {tcp   ip   icmp} host source eq tacacs host destination</pre> <p><b>Example:</b></p> <pre>Router (config)# access-list 111 permit tcp host 209.165.200.225 eq tacacs host 209.165.200.254</pre> <p>or</p> <pre>Router (config)# access-list 111 deny ip any any</pre> <p>or</p> <pre>Router (config)# access-list 111 permit icmp any any</pre>	<p>Creates an ACL entry to allow the AAA server to return traffic to the firewall.</p> <p>The source address is the IP address of the AAA server, and the destination is the IP address of the router interface where the AAA server resides.</p>

## What to Do Next

Ensure that your FTP or Telnet server is enabled and that the user credentials of the client (the username and password) are stored in the server's database.

## Configuring the Authentication Proxy

To configure the authentication proxy, perform the following steps:

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip auth-proxy** {inactivity-timer *min* | absolute-timer *min*}
4. **ip auth-proxy auth-proxy-banner** {ftp | http | telnet} [*banner-text*]
5. **ip auth-proxy name** *auth-proxy-name* {ftp | http | telnet} [inactivity-timer *min* | absolute-timer *min*] [list {*acl* | *acl-name*}]
6. **interface** *type*
7. **ip auth-proxy** *auth-proxy-name*

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<p><b>enable</b></p> <p><b>Example:</b> Router&gt; enable</p>	<p>Enables higher privilege levels, such as privileged EXEC mode.</p> <p>Enter your password if prompted.</p>
Step 2	<p><b>configure terminal</b></p> <p><b>Example:</b> Router# configure terminal</p>	<p>Enters global configuration mode.</p>
Step 3	<p><b>ip auth-proxy {inactivity-timer min   absolute-timer min}</b></p> <p><b>Example:</b> Router (config)# ip auth-proxy inactivity-timer 30</p>	<p>Sets the global authentication proxy idle timeout values in minutes.</p> <ul style="list-style-type: none"> <li>• <b>inactivity-timer min</b>—Specifies the length of time in minutes that an authentication cache entry is managed after a period of inactivity. Enter a value in the range 1 to 2,147,483,647. The default value is 60 minutes.</li> <li>• <b>absolute-timer min</b>—Specifies a window in which the authentication proxy on the enabled interface is active. Enter a value in the range 1 to 65,535 minutes (45 and a half days). The default value is 0 minutes.</li> </ul>
Step 4	<p><b>ip auth-proxy auth-proxy-banner {ftp   http   telnet} [banner-text]</b></p> <p><b>Example:</b> Router (config)# ip auth-proxy auth-proxy-banner ftp hello</p>	<p>Optional) Displays the name of the firewall router in the authentication proxy login page. Disabled by default.</p> <ul style="list-style-type: none"> <li>• <b>ftp</b>—Specifies the FTP protocol.</li> <li>• <b>http</b>—Specifies the HTTP protocol.</li> <li>• <b>telnet</b>—Specifies the Telnet protocol.</li> <li>• <b>banner-text</b>—(Optional) A text string that replaces the default banner.</li> </ul>
Step 5	<p><b>ip auth-proxy name auth-proxy-name {ftp   http   telnet} [inactivity-timer min] [absolute-timer min] [list {acl   acl-name}]</b></p> <p><b>Example:</b> Router (config)# ip auth-proxy name ftp_list1 ftp absolute-timer 60 ftp list 102</p>	<p>Configures authentication proxy on an interface.</p> <ul style="list-style-type: none"> <li>• <b>ftp</b>—Specifies FTP to trigger that authentication proxy.</li> <li>• <b>http</b>—Specifies HTTP to trigger that authentication proxy.</li> <li>• <b>telnet</b>—Specifies Telnet to trigger that authentication proxy.</li> <li>• <b>inactivity-timer min</b>—Overrides global authentication proxy cache timer for a specific authentication proxy name.</li> <li>• <b>absolute-timer min</b>— Overrides the global value specified via the <b>ip auth-proxy</b> command.</li> <li>• <b>list {acl   acl-name}</b>—Specifies a standard (1–99), extended (1–199), or named access list to use with the authentication proxy.</li> </ul>

	Command or Action	Purpose
Step 6	<b>interface</b> <i>type</i>  <b>Example:</b> Router (config)# interface e0	Enters interface configuration mode by specifying the interface type on which to apply the authentication proxy.
Step 7	<b>ip auth-proxy</b> <i>auth-proxy-name</i>  <b>Example:</b> Router(config-if)# ip auth-proxy authproxyrule	In interface configuration mode, applies the named authentication proxy rule at the interface.  This command enables the authentication proxy rule with that name.

## Verifying FTP or Telnet Authentication Proxy

To verify your FTP or Telnet authentication proxy configuration, perform the following optional steps:

### SUMMARY STEPS

1. **enable**
2. **show ip auth-proxy configuration**
3. **show ip auth-proxy cache**

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables higher privilege levels, such as privileged EXEC mode.  Enter your password if prompted.
Step 2	<b>show ip auth-proxy configuration</b>  <b>Example:</b> Router# show ip auth-proxy configuration	Displays the current authentication proxy configuration.
Step 3	<b>show ip auth-proxy cache</b>  <b>Example:</b> Router# show ip auth-proxy cache	Displays the list of user authentication entries.  The authentication proxy cache lists the host IP address, the source port number, the timeout value for the authentication proxy, and the state of the connection. If the authentication proxy state is ESTAB or INTERCEPT, the user authentication was successful.

## Monitoring and Maintaining FTP or Telnet Authentication Proxy Sessions

To monitor FTP or Telnet authentication proxy sessions, perform the following optional steps:

### SUMMARY STEPS

1. `enable`
2. `debug ip auth-proxy {detailed | ftp | function-trace | object-creation | object-deletion | telnet | timers}`

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code>  <b>Example:</b> Router> enable	Enables higher privilege levels, such as privileged EXEC mode.  Enter your password if prompted.
Step 2	<code>debug ip auth-proxy {detailed   ftp   function-trace   object-creation   object-deletion   telnet   timers}</code>  <b>Example:</b> Router# debug ip auth-proxy ftp	Displays the authentication proxy configuration information on the router.

## Configuration Examples for FTP and Telnet Authentication Proxy

This section provides the following configuration examples:

- [Authentication Proxy Configuration Example, page 12](#)
- [AAA Server User Profile Examples, page 13](#)

### Authentication Proxy Configuration Example

The following example shows how to configure your router for authentication proxy:

```
aaa new-model
aaa authentication login default group tacacs+
aaa authorization exec default group tacacs+
aaa authorization auth-proxy default group tacacs+
enable password lab
!
ip inspect name pxy_test ftp
ip auth-proxy name pxy auth-cache-time 1
!
interface Ethernet0/0
 ip address 209.165.200.225 255.255.255.224
 ip access-group 105 in
 no ip directed-broadcast
 ip inspect pxy_test in
 ip auth-proxy pxy
```

```

no shut
!
interface Ethernet0/1
 ip address 209.165.200.225 255.255.255.224
 ip access-group 102 in
 no ip directed-broadcast
no shut
!
ip http authentication aaa
!
access-list 102 permit any
access-list 102 permit tcp host 209.165.200.234 eq tacacs any
access-list 102 deny tcp any any
access-list 102 deny udp any any
access-list 102 permit ip any any
access-list 105 permit tcp any any eq www
access-list 105 permit ip any any
access-list 105 deny tcp any any
access-list 105 deny udp any any
dialer-list 1 protocol ip permit
dialer-list 1 protocol ipx permit
!
tacacs-server host 209.165.200.234
tacacs-server key cisco
!
line con 0
 transport input none
 login authentication special
line aux 0
line vty 0 4
 password lab

```

## AAA Server User Profile Examples

This section includes examples of the authentication proxy user profile entries on the AAA servers. The “proxyacl” entries define the user access privileges. After the user has successfully used the authentication proxy to log in, these entries are transferred to the firewall router. Each entry in the profile must specify “permit” access for the service or application. The source address in each entry is set to “any”, which is replaced with the IP address of the authenticating host when the profile is downloaded to the firewall. The privilege level must be set to 15 for all AAA users.

This section contains the following examples:

- [TACACS+ User Profiles Example](#)
- [Livingston RADIUS User Profiles Example](#)
- [Ascend RADIUS User Profiles Example](#)

### TACACS+ User Profiles Example

The following example are sample TACACS+ user profiles:

```

default authorization = permit
key = cisco
user = http_1 {
  default service = permit
  login = cleartext test
  service = exec
  {

```

```

        priv-lvl = 15
        inacl#4="permit tcp any host 209.165.200.234 eq 23"
        inacl#5="permit tcp any host 209.165.200.234 eq 20"
        inacl#6="permit tcp any host 209.165.200.234 eq 21"
        inacl#3="deny -1"
    }
    service = auth-proxy
    {
        priv-lvl=15
        proxyacl#4="permit tcp any host 209.165.201.1 eq 23"
        proxyacl#5="permit tcp any host 209.165.201.1 eq 20"
        proxyacl#6="permit tcp any host 209.165.201.1 eq 21"
        proxyacl#7="permit tcp any host 209.165.201.1 eq 25"
    }
}
user = http {
    login = cleartext test
    service = auth-proxy
    {
        priv-lvl=15
        proxyacl#4="permit tcp any host 209.165.201.1 eq 23"
        proxyacl#5="permit tcp any host 209.165.201.1 eq 20"
        proxyacl#6="permit tcp any host 209.165.201.1 eq 21"
    }
}
user = proxy_1 {
    login = cleartext test
    service = auth-proxy
    {
        priv-lvl=14
    }
}
user = proxy_3 {
    login = cleartext test
    service = auth-proxy
    {
        priv-lvl=15
    }
}

```

## Livingston RADIUS User Profiles Example

The following examples are sample user profiles for the Livingston RADIUS server:

```

#----- Proxy user -----
http          Password = "test" User-Service-Type=Outbound-User
cisco-avpair = "auth-proxy:priv-lvl=15",
cisco-avpair = "auth-proxy:proxyacl#3=permit tcp any any eq 23"

http_1       Password = "test"
User-Service-Type = Shell-User,
User-Service-Type=Dialout-Framed-User,
cisco-avpair = "shell:priv-lvl=15",
cisco-avpair = "shell:inacl#4=permit tcp any host 209.165.200.234
eq 23
cisco-avpair = "auth-proxy:priv-lvl=15",
cisco-avpair = "auth-proxy:proxyacl#3=permit tcp any any eq 23"

```

```

http_fail          Password = "test" User-Service-Type=Outbound-User
                  cisco-avpair = "auth-proxy:priv-lvl=14",
                  cisco-avpair = "auth-proxy:proxyacl#3=permit tcp any any eq 23"

proxy Password = "cisco" User-Service-Type=Outbound-User      cisco-avpair =
"auth-proxy:proxyacl#4=permit tcp any any eq 20"

```

## Ascend RADIUS User Profiles Example

The following examples are sample user profiles for the Ascend RADIUS server:

```

#----- Proxy user -----

http          Password = "test" User-Service=Dialout-Framed-User
            cisco-avpair = "auth-proxy:priv-lvl=15",
            cisco-avpair = "auth-proxy:proxyacl#3=permit tcp any any eq 23"

http_2          Password = "test"
User-Service=Dialout-Framed-User
            cisco-avpair = "auth-proxy:priv-lvl=15",
            cisco-avpair = "auth-proxy:proxyacl#3=permit tcp any any eq 23",
            cisco-avpair = "shell:inacl#4=permit tcp any host 209.165.200.234 eq 25"

http_1          Password = "test"
User-Service=Dialout-Framed-User,
            cisco-avpair = "shell:inacl#4=permit tcp any host 209.165.200.234 eq 23",
            cisco-avpair = "auth-proxy:priv-lvl=15",
            cisco-avpair = "auth-proxy:proxyacl#3=permit tcp any any eq 23"

http_fail          Password = "test" User-Service=Dialout-Framed-User
            cisco-avpair = "auth-proxy:priv-lvl=14",
            cisco-avpair = "auth-proxy:proxyacl#3=permit tcp any any eq 23"

            cisco-avpair = "auth-proxy:proxyacl#1=permit tcp any any eq 23",
            cisco-avpair = "auth-proxy:proxyacl#3=permit tcp any any eq ftp",
            cisco-avpair = "auth-proxy:proxyacl#4=permit tcp any any eq 20"

#-----

proxy Password = "cisco" User-Service = Dialout-Framed-User

            cisco-avpair = "auth-proxy:priv-lvl=15",

            cisco-avpair = "auth-proxy:priv-lvl=15",
            cisco-avpair = "auth-proxy:proxyacl#1=permit tcp any any eq 26",
            cisco-avpair = "auth-proxy:proxyacl#3=permit tcp any any eq ftp",

```

## Additional References

The following sections provide additional references related to the Firewall Authentication Proxy for FTP and Telnet Sessions feature:

- [Related Documents, page 16](#)
- [Standards, page 16](#)
- [MIBs, page 16](#)

## Additional References

- [RFCs, page 16](#)
- [Technical Assistance, page 17](#)

## Related Documents

Related Topic	Document Title
Additional authentication proxy configuration tasks	The chapter “Configuring Authentication Proxy” in the <i>Cisco IOS Security Configuration Guide</i> , Release 12.3
Additional authentication proxy commands	<i>Cisco IOS Security Command Reference</i> , Release 12.3
RADIUS and TACACS+ configuration information	The section “Security Server Protocols” in the <i>Cisco IOS Security Configuration Guide</i> , Release 12.3
RADIUS and TACACS+ attribute information	The chapters “RADIUS Attributes” and “TACACS+ Attribute-Value Pairs” in the <i>Cisco IOS Security Configuration Guide</i> , Release 12.3
Additional authentication proxy information	<i>Firewall Support of HTTPS Authentication Proxy</i> , Cisco IOS Release 12.2(15)T feature module

## 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: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

## RFCs

RFCs	Title
None	—

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

## Command Reference

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

- [debug ip auth-proxy](#)
- [ip auth-proxy](#)
- [ip auth-proxy auth-proxy-banner](#)
- [ip auth-proxy name](#)

# debug ip auth-proxy

To display the authentication proxy configuration information on the router, use the **debug ip auth-proxy** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

```
debug ip auth-proxy {detailed | ftp | function-trace | object-creation | object-deletion | telnet |
timers}
```

```
no debug ip auth-proxy
```

## Syntax Description

<b>detailed</b>	Displays details of the TCP events during an authentication proxy process. The details are generic to all FTP, HTTP, and Telnet protocols.
<b>ftp</b>	Displays FTP events related to the authentication proxy.
<b>function-trace</b>	Displays the authentication proxy functions.
<b>object-creation</b>	Displays additional entries to the authentication proxy cache.
<b>object-deletion</b>	Displays deletion of cache entries for the authentication proxy.
<b>telnet</b>	Displays Telnet-related authentication proxy events.
<b>timers</b>	Displays authentication proxy timer-related events.

## Command History

Release	Modification
12.0(5)T	This command was introduced.
12.3(1)	The <b>detailed</b> keyword was added.

## Command Modes

Privileged EXEC

## Usage Guidelines

Use the **debug ip auth-proxy** command to display authentication proxy activity. See the “Examples” section for more information about the debug options.



### Note

The **function-trace** debugging information provides low-level software information for Cisco technical support representatives. No output examples are provided for this keyword option.

## Examples

The following examples illustrate the output of the **debug ip auth-proxy** command. In these examples, debugging is on for object creations, object deletions, HTTP, and TCP.

In this example, the client host at 192.168.201.1 is attempting to make an HTTP connection to the web server located at 192.168.21.1. The HTTP debugging information is on for the authentication proxy. The following output shows that the router is setting up an authentication proxy entry for the login request:

```
00:11:10: AUTH-PROXY creates info:
  cliaddr - 192.168.21.1, cliport - 36583
  seraddr - 192.168.201.1, serport - 80
  ip-srcaddr 192.168.21.1
  pak-srcaddr 0.0.0.0
```

Following a successful login attempt, the debugging information shows the authentication proxy entries created for the client. In this example, the client is authorized for SMTP (port 25), FTP data (port 20), FTP control (port 21), and Telnet (port 23) traffic. The dynamic ACL entries are included in the display.

```
00:11:25:AUTH_PROXY OBJ_CREATE:acl item 61AD60CC

00:11:25:AUTH-PROXY OBJ_CREATE:create acl wrapper 6151C7C8 -- acl item 61AD60CC
00:11:25:AUTH-PROXY Src 192.168.162.216 Port [0]
00:11:25:AUTH-PROXY Dst 192.168.162.220 Port [25]
00:11:25:AUTH_PROXY OBJ_CREATE:acl item 6151C908

00:11:25:AUTH-PROXY OBJ_CREATE:create acl wrapper 6187A060 -- acl item 6151C908
00:11:25:AUTH-PROXY Src 192.168.162.216 Port [0]
00:11:25:AUTH-PROXY Dst 192.168.162.220 Port [20]
00:11:25:AUTH_PROXY OBJ_CREATE:acl item 61A40B88

00:11:25:AUTH-PROXY OBJ_CREATE:create acl wrapper 6187A0D4 -- acl item 61A40B88
00:11:25:AUTH-PROXY Src 192.168.162.216 Port [0]
00:11:25:AUTH-PROXY Dst 192.168.162.220 Port [21]
00:11:25:AUTH_PROXY OBJ_CREATE:acl item 61879550

00:11:25:AUTH-PROXY OBJ_CREATE:create acl wrapper 61879644 -- acl item 61879550
00:11:25:AUTH-PROXY Src 192.168.162.216 Port [0]
00:11:25:AUTH-PROXY Dst 192.168.162.220 Port [23]
```

The next example shows the debug output following a **clear ip auth-proxy cache** command to clear the authentication entries from the router. The dynamic ACL entries are removed from the router.

```
00:12:36:AUTH-PROXY OBJ_DELETE:delete auth_proxy cache 61AD6298
00:12:36:AUTH-PROXY OBJ_DELETE:delete create acl wrapper 6151C7C8 -- acl item 61AD60CC
00:12:36:AUTH-PROXY OBJ_DELETE:delete create acl wrapper 6187A060 -- acl item 6151C908
00:12:36:AUTH-PROXY OBJ_DELETE:delete create acl wrapper 6187A0D4 -- acl item 61A40B88
00:12:36:AUTH-PROXY OBJ_DELETE:delete create acl wrapper 61879644 -- acl item 61879550
```

The following example shows the timer information for a dynamic ACL entry. All times are expressed in milliseconds. The *first laststart* is the time that the ACL entry is created relative to the startup time of the router. The *lastref* is the time of the last packet to hit the dynamic ACL relative to the startup time of the router. The *exptime* is the next expected expiration time for the dynamic ACL. The *delta* indicates the remaining time before the dynamic ACL expires. After the timer expires, the debugging information includes a message indicating that the ACL and associated authentication proxy information for the client have been removed.

```
00:19:51:first laststart 1191112

00:20:51:AUTH-PROXY:delta 54220 lastref 1245332 exptime 1251112
00:21:45:AUTH-PROXY:ACL and cache are removed
```

The following example is sample output with the **detailed** keyword enabled:

```
00:37:50:AUTH-PROXY:proto_flag=5, dstport_index=1
00:37:50: SYN SEQ 245972 LEN 0
00:37:50:dst_addr 192.168.127.2 src_addr 192.168.27.1 dst_port 21 src_port 4347
00:37:50:AUTH-PROXY:auth_proxy_half_open_count++ 1
00:37:50:AUTH-PROXY:proto_flag=5, dstport_index=1
00:37:50: ACK 1820245643 SEQ 245973 LEN 0
00:37:50:dst_addr 192.168.127.2 src_addr 192.168.27.1 dst_port 21 src_port 4347
00:37:50:clientport 4347 state 0
00:37:50:AUTH-PROXY:incremented proxy_proc_count=1
00:37:50:AUTH-PROXY:proto_flag=5, dstport_index=1
00:37:50: ACK 1820245674 SEQ 245973 LEN 0
00:37:50:dst_addr 192.168.127.2 src_addr 192.168.27.1 dst_port 21 src_port 4347
00:37:50:clientport 4347 state 0
00:37:57:AUTH-PROXY:proto_flag=5, dstport_index=1
```

## debug ip auth-proxy

```

00:37:57: PSH ACK 1820245674 SEQ 245973 LEN 16
00:37:57:dst_addr 192.168.127.2 src_addr 192.168.27.1 dst_port 21 src_port 4347
00:37:57:clientport 4347 state 0
00:37:57:AUTH-PROXY:proto_flag=5, dstport_index=1
00:37:57: ACK 1820245699 SEQ 245989 LEN 0
00:37:57:dst_addr 192.168.127.2 src_addr 192.168.27.1 dst_port 21 src_port 4347
00:37:57:clientport 4347 state 0
00:38:01:AUTH-PROXY:proto_flag=5, dstport_index=1
00:38:01: PSH ACK 1820245699 SEQ 245989 LEN 16
00:38:01:dst_addr 192.168.127.2 src_addr 192.168.27.1 dst_port 21 src_port 4347
00:38:01:clientport 4347 state 0
00:38:01:AUTH-PROXY:Authenticating user ryan
00:38:01:AUTH-PROXY:Session state is INIT.Not updating stats
00:38:01:AUTH-PROXY:Session state is INIT.Not updating stats
00:38:01:AUTH-PROXY:Sent AAA request successfully
00:38:01:AUTH-PROXY:Sent password successfully
00:38:01:AUTH-PROXY:processing authorization data
00:38:01:AUTH-PROXY:Sending accounting start.unique-id 2
00:38:01:AUTH-PROXY:Session state is INIT.Not updating stats
00:38:01:AUTH-PROXY:Session state is INIT.Not updating stats
00:38:01:AUTH-PROXY:wait complete on watched boolean stat=0
00:38:01:AUTH-PROXY:src ip addr is 192.168.127.2, dstaddr=192.168.27.1
00:38:01: SYN ACK 2072458992 SEQ 4051022445 LEN 0
00:38:01:AUTH-PROXY:src ip addr is 192.168.127.2, dstaddr=192.168.27.1
00:38:01: PSH ACK 2072458992 SEQ 4051022446 LEN 49
00:38:02:AUTH-PROXY:src ip addr is 192.168.127.2, dstaddr=192.168.27.1
00:38:02: ACK 2072459003 SEQ 4051022495 LEN 0
00:38:02:AUTH-PROXY:src ip addr is 192.168.127.2, dstaddr=192.168.27.1
00:38:02: PSH ACK 2072459003 SEQ 4051022495 LEN 33
00:38:02:AUTH-PROXY:src ip addr is 192.168.127.2, dstaddr=192.168.27.1
00:38:02: ACK 2072459014 SEQ 4051022528 LEN 0
00:38:02:AUTH-PROXY:src ip addr is 192.168.127.2, dstaddr=192.168.27.1
00:38:02: PSH ACK 2072459014 SEQ 4051022528 LEN 26
00:38:03:AUTH-PROXY:proto_flag=5, dstport_index=1
00:38:03: ACK 1820245725 SEQ 246005 LEN 0
00:38:03:dst_addr 192.168.127.2 src_addr 192.168.27.1 dst_port 21 src_port 4347
00:38:03:clientport 4347 state 3
7200b#

```

## Related Commands

Command	Description
show debug	Displays the debug options set on the router.

## ip auth-proxy

To set the authentication proxy idle timeout value (the length of time an authentication cache entry, along with its associated dynamic user access control list, is managed after a period of inactivity), use the **ip auth-proxy** command in global configuration mode. To set the default value, use the **no** form of this command.

```
ip auth-proxy {inactivity-timer min | absolute-timer min}
```

```
no ip auth-proxy {inactivity-timer | absolute-timer}
```

Syntax Description		
<b>inactivity-timer</b> <i>min</i>		Specifies the length of time in minutes that an authentication cache entry, along with its associated dynamic user access control list (ACL), is managed after a period of inactivity. Enter a value in the range 1 to 2,147,483,647. The default value is 60 minutes.
		<b>Note</b> This option deprecates the <b>auth-cache-time</b> <i>min</i> option.
<b>absolute-timer</b> <i>min</i>		Specifies a window in which the authentication proxy on the enabled interface is active. Enter a value in the range 1 to 65,535 minutes (45 and a half days). The default value is 0 minutes.

### Defaults

The default value of the **inactivity-timer** *min* option is 60 minutes.

The default value of the **absolute-timer** *min* option is zero.

### Command Modes

Global configuration

### Command History

Release	Modification
12.0(5)T	This command was introduced.
12.3(1)	The <b>inactivity-timer</b> <i>min</i> and <b>absolute-timer</b> <i>min</i> options were added.

### Usage Guidelines

Use this command to set the global idle timeout value for the authentication proxy. You must set the value of the **inactivity-timer** *min* option to a higher value than the idle timeout of any Context-Based Access Control (CBAC) protocols. Otherwise, when the authentication proxy removes the user profile along associated dynamic user ACLs, there might be some idle connections monitored by CBAC. Removing these user-specific ACLs could cause those idle connections to hang. If the CBAC idle timeout value is shorter, CBAC resets these connections when the CBAC idle timeout expires, which is before the authentication proxy removes the user profile.

The **absolute-timer** *min* option allows users to configure a window during which the authentication proxy on the enabled interface is active. Once the absolute timer expires, the authentication proxy will be disabled regardless of any activity. The global absolute timeout value can be overridden by the local (per protocol) value, which is enabled via the **ip auth-proxy name** command. The absolute timer is turned off by default, and the authentication proxy is enabled indefinitely.

---

**Examples**

The following example sets the inactivity timeout to 30 minutes:

```
ip auth-proxy inactivity-timer 30
```

---

**Related Commands**

Command	Description
<a href="#">ip auth-proxy name</a>	Creates an authentication proxy rule.
<b>show ip auth-proxy configuration</b>	Displays the authentication proxy entries or the running authentication proxy configuration.

# ip auth-proxy auth-proxy-banner

To display a banner, such as the router name, in the authentication proxy login page, use the **ip auth-proxy auth-proxy-banner** command in global configuration mode. To disable display of the banner, use the **no** form of this command.

```
ip auth-proxy auth-proxy-banner {ftp | http | telnet} [banner-text]
```

```
no ip auth-proxy auth-proxy-banner {ftp | http | telnet}
```

## Syntax Description

<b>ftp</b>	Specifies the FTP protocol.
<b>http</b>	Specifies the HTTP protocol.
<b>telnet</b>	Specifies the Telnet protocol.
<i>banner-text</i>	(Optional) Specifies a text string to replace the default banner, which is the name of the router. The text string should be written in the following format: "C banner-text C," where "C" is a delimiting character.

## Defaults

This command is not enabled, and a banner is not displayed on the authentication proxy login page.

## Command Modes

Global configuration

## Command History

Release	Modification
12.0(5)T	This command was introduced.
12.3(1)	The following keywords were added: <b>ftp</b> , <b>http</b> , and <b>telnet</b> .

## Usage Guidelines

The **ip auth-proxy auth-proxy-banner** command allows users to configure one of two possible scenarios:

- The **ip auth-proxy auth-proxy-banner** command is enabled.  
In this scenario, the administrator has not supplied any text. Thus, a default banner that states the following: "Cisco Systems, <router's hostname> Authentication" will be displayed in the authentication proxy login page. This scenario is most commonly used.
- The **ip auth-proxy auth-proxy-banner** command with the *banner-text* argument is enabled.  
In this scenario, the administrator can supply multiline text that will be converted to HTML by the auth-proxy parser code. Thus, *only* the multiline text will displayed in the authentication proxy login page. You will *not* see the default banner, "Cisco Systems, <router's hostname> Authentication."



### Note

If the **ip auth-proxy auth-proxy-banner** command is not enabled, there will not be any banner configuration. Thus, nothing will be displayed to the user on authentication proxy login page except a text box to enter the username and a text box to enter the password.

---

**Examples**

The following example causes the router name to be displayed in the authentication proxy login page:

```
ip auth-proxy auth-proxy-banner ftp
```

The following example shows how to specify the custom banner “whozat” to be displayed in the authentication proxy login page:

```
ip auth-proxy auth-proxy-banner telnet ^Cwhozat^C
```

---

**Related Commands**

Command	Description
<a href="#">ip auth-proxy name</a>	Creates an authentication proxy rule.

---

## ip auth-proxy name

To create an authentication proxy rule, use the **ip auth-proxy name** command in global configuration mode. To remove the authentication proxy rules, use the **no** form of this command.

```
ip auth-proxy name auth-proxy-name { ftp | http | telnet } [inactivity-timer min] [absolute-timer min] [list { acl | acl-name }]
```

```
no ip auth-proxy name auth-proxy-names
```

Syntax Description	
<i>auth-proxy-name</i>	Associates a name with an authentication proxy rule. Enter a name of up to 16 alphanumeric characters.
<b>ftp</b>	Specifies FTP to trigger the authentication proxy.
<b>http</b>	Specifies HTTP to trigger the authentication proxy.
<b>telnet</b>	Specifies Telnet to trigger the authentication proxy.
<b>inactivity-timer</b> <i>min</i>	(Optional) Overrides the global authentication proxy cache timer for a specific authentication proxy name, offering more control over timeout values. Enter a value in the range 1 to 2,147,483,647. The default value is equal to the value set with the <b>ip auth-proxy</b> command.  <b>Note</b> This option deprecates the <b>auth-cache-time</b> <i>min</i> option.
<b>absolute-timer</b> <i>min</i>	(Optional) Specifies a window in which the authentication proxy on the enabled interface is active. Enter a value in the range 1 to 65,535 minutes (45 and a half days). The default value is 0 minutes.
<b>list</b> { <i>acl</i>   <i>acl-name</i> }	(Optional) Specifies a standard (1–99), extended (1–199), or named access list to use with the authentication proxy. With this option, the authentication proxy is applied only to those hosts in the access list. If no list is specified, all connections initiating HTTP, FTP, or Telnet traffic arriving at the interface are subject to authentication.

**Defaults** The default value is equal to the value set with the **ip auth-proxy auth-cache-time** command.

**Command Modes** Global configuration

Command History	Release	Modification
	12.0(5)T	This command was introduced.
	12.2	Support for named and extend access lists was introduced.
	12.3(1)	The following keywords were introduced: <ul style="list-style-type: none"> <li><b>ftp</b></li> <li><b>telnet</b></li> <li><b>inactivity-timer</b> <i>min</i></li> <li><b>absolute-timer</b> <i>min</i></li> </ul>

**Usage Guidelines**

This command creates a named authentication proxy rule, and it allows you to associate that rule with an access control list (ACL), providing control over which hosts use the authentication proxy. The rule is applied to an interface on a router using the **ip auth-proxy** command.

Use the **inactivity-timer** *min* option to override the global the authentication proxy cache timer. This option provides control over timeout values for specific authentication proxy rules. The authentication proxy cache timer monitors the length of time (in minutes) that an authentication cache entry, along with its associated dynamic user access control list, is managed after a period of inactivity. When that period of inactivity (idle time) expires, the authentication entry and the associated dynamic access lists are deleted.

Use the **list** option to associate a set of specific IP addresses or a named ACL with the **ip auth-proxy name** command.

Use the **no** form of this command with a rule name to remove the authentication proxy rules. If no rule is specified, the **no** form of this command removes all the authentication rules on the router, and disables the proxy at all interfaces.

**Note**

You must use the **aaa authorization auth-proxy** command together with the **ip auth-proxy name** command. Together these commands set up the authorization policy to be retrieved by the firewall. Refer to the **aaa authorization auth-proxy** command for more information.

**Examples**

The following example creates the HQ\_users authentication proxy rule. Because an access list is not specified in the rule, all connection-initiating HTTP traffic is subjected to authentication.

```
ip auth-proxy name HQ_users http
```

The following example creates the Mfg\_users authentication proxy rule and applies it to hosts specified in ACL 10:

```
access-list 10 192.168.7.0 0.0.0.255
ip auth-proxy name Mfg_users http list 10
```

The following example sets the timeout value for Mfg\_users to 30 minutes:

```
access-list 15 any
ip auth-proxy name Mfg_users http inactivity-timer 30 list 15
```

The following example disables the Mfg\_users rule:

```
no ip auth-proxy name Mfg_users
```

The following example disables the authentication proxy at all interfaces and removes all the rules from the router configuration:

```
no ip auth-proxy
```

**Related Commands**

Command	Description
<b>aaa authorization</b>	Sets parameters that restrict network access to a user.
<b>ip auth-proxy</b>	Sets the authentication proxy idle timeout value (the length of time an authentication cache entry, along with its associated dynamic user ACL, is managed after a period of inactivity).

Command	Description
<b>ip auth-proxy (interface)</b>	Applies an authentication proxy rule at a firewall interface.
<b>show ip auth-proxy configuration</b>	Displays the authentication proxy entries or the running authentication proxy configuration.

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 © 2003 Cisco Systems, Inc. All rights reserved

■ ip auth-proxy name