



Authentication Proxy Commands

This chapter describes the commands used to configure authentication proxy. The Cisco IOS Firewall authentication proxy feature allows network administrators to apply specific security policies on a per-user basis. Without authentication proxy, user identity and related authorized access was associated with a user's IP address, or a single security policy had to be applied to an entire user group or subnet. Configuring authentication proxy enables users to be identified and authorized on the basis of their per-user policy; access privileges tailored on an individual basis are possible, as opposed to general policy applied across multiple users.

With the authentication proxy feature, users can log in to the network or access the Internet via HTTP, and their specific access profiles are automatically retrieved and applied from a CiscoSecure ACS or other RADIUS or TACACS+ authentication server. The user profiles are active only when there is active traffic from the authenticated users.

For information on how to configure authentication proxy, refer to the “Configuring Authentication Proxy” chapter in the *Cisco IOS Security Configuration Guide*. For configuration examples using the commands in this chapter, refer to the “Authentication Proxy Configuration Examples” section located at the end of the “Configuring Authentication Proxy” chapter in the *Cisco IOS Security Configuration Guide*.

clear ip auth-proxy cache

To clear authentication proxy entries from the router, use the **clear ip auth-proxy cache** command in EXEC mode.

```
clear ip auth-proxy cache { * | host-ip-address }
```

Syntax Description

*	Clears all authentication proxy entries, including user profiles and dynamic access lists.
<i>host-ip-address</i>	Clears the authentication proxy entry, including user profiles and dynamic access lists, for the specified host.

Command Modes

EXEC

Command History

Release	Modification
12.0(5)T	This command was introduced.

Usage Guidelines

Use this command to clear entries from the translation table before they time out.

Examples

The following example deletes all authentication proxy entries:

```
clear ip auth-proxy cache *
```

The following example deletes the authentication proxy entry for the host with IP address 192.168.4.5:

```
clear ip auth-proxy cache 192.168.4.5
```

Related Commands

Command	Description
show ip auth-proxy	Displays the authentication proxy entries or the running authentication proxy configuration.

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 auth-cache-time *min*

no ip auth-proxy auth-cache-time

Syntax Description	auth-cache-time <i>min</i>	Specifies the length of time in minutes that an authentication cache entry, along with its associated dynamic user 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.
---------------------------	-----------------------------------	--

Defaults	60 minutes
-----------------	------------

Command Modes	Global configuration
----------------------	----------------------

Command History	Release	Modification
	12.0(5)T	This command was introduced.

Usage Guidelines	Use this command to set the global idle timeout value for the authentication proxy. You must set the auth-cache-time timeout <i>min</i> 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.
-------------------------	---

Examples	The following example sets the authorization cache timeout to 30 minutes: <pre>ip auth-proxy auth-cache-time 30</pre>
-----------------	--

Related Commands	Command	Description
	ip auth-proxy name show ip auth-proxy	Creates an authentication proxy rule. Displays the authentication proxy entries or the running authentication proxy configuration.

ip auth-proxy (interface configuration)

To apply an authentication proxy rule at a firewall interface, use the **ip auth-proxy** command in interface configuration mode. To remove the authentication proxy rules, use the **no** form of this command.

ip auth-proxy *auth-proxy-name*

no ip auth-proxy *auth-proxy-name*

Syntax Description

<i>auth-proxy-name</i>	Specifies the name of the authentication proxy rule to apply to the interface configuration. The authentication proxy rule is established with the ip auth-proxy name command.
------------------------	---

Defaults

No default behavior or values.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.

Usage Guidelines

Use the **ip auth-proxy** command to enable the named authentication proxy rule at the firewall interface. Traffic passing through the interface from hosts with an IP address matching the standard access list and protocol type (HTTP) is intercepted for authentication if no corresponding authentication cache entry exists. If no access list is defined, the authentication proxy intercepts traffic from all hosts whose connection initiating packets are received at the configured interface.

Use the **no** form of this command with a rule name to disable the authentication proxy for a given rule on a specific interface. If a rule is not specified, the **no** form of this command disables the authentication proxy on the interface.

Examples

The following example configures interface Ethernet0 with the HQ_users rule:

```
interface e0
  ip address 172.21.127.210 255.255.255.0
  ip access-group 111 in
  ip auth-proxy HQ_users
  ip nat inside
```

Related Commands

Command	Description
ip auth-proxy name	Creates an authentication proxy rule.

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 [*banner-text*]

no ip auth-proxy auth-proxy-banner [*banner-text*]

Syntax Description

banner-text (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.

Usage Guidelines

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

- 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 the 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
```

ip auth-proxy auth-proxy-banner

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 ^Cwhozat^C
```

Related Commands

Command	Description
ip auth-proxy name	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 http [list {acl | acl-name}] [auth-cache-time min]
```

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

Syntax Description		
<i>auth-proxy-name</i>		Associates a name with an authentication proxy rule. Enter a name of up to 16 alphanumeric characters.
http		Specifies the protocol that triggers the authentication proxy. The only supported protocol is HTTP.
list { <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 traffic arriving at the interface are subject to authentication.
auth-cache-time <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 ip auth-proxy auth-cache-time command.

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.

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 **auth-cache-time** 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 auth-cache-time 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
aaa authorization	Sets parameters that restrict network access to a user.
ip auth-proxy	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).
ip auth-proxy (interface configuration)	Applies an authentication proxy rule at a firewall interface.
show ip auth-proxy	Displays the authentication proxy entries or the running authentication proxy configuration.

show ip auth-proxy

To display the authentication proxy entries or the running authentication proxy configuration, use the **show ip auth-proxy** command in privileged EXEC mode.

```
show ip auth-proxy { cache | configuration }
```

Syntax Description

cache	Display the current list of the authentication proxy entries.
configuration	Display the running authentication proxy configuration.

Command Modes

EXEC

Command History

Release	Modification
12.0(5)T	This command was introduced.

Usage Guidelines

Use the **show ip auth-proxy** to display either the authentication proxy entries or the running authentication proxy configuration. Use the **cache** keyword to list the host IP address, the source port number, the timeout value for the authentication proxy, and the state for connections using authentication proxy. If authentication proxy state is HTTP_ESTAB, the user authentication was successful.

Use the **configuration** keyword to display all authentication proxy rules configured on the router.

Examples

The following example shows sample output from the **show ip auth-proxy cache** command after one user authentication using the authentication proxy:

```
Router# show ip auth-proxy cache

Authentication Proxy Cache
  Client IP 192.168.25.215 Port 57882, timeout 1, state HTTP_ESTAB
```

The following example shows how the **show ip auth-proxy configuration** command displays the information about the authentication proxy rule **pxy**. The global idle timeout value is 60 minutes. The idle timeouts value for this named rule is 30 minutes. No host list is specified in the rule, meaning that all connection initiating HTTP traffic at the interface is subject to the authentication proxy rule.

```
Router# show ip auth-proxy configuration

Authentication cache time is 60 minutes
Authentication Proxy Rule Configuration
Auth-proxy name pxy
http list not specified auth-cache-time 30 minutes
```

show ip auth-proxy

Related Commands	Command	Description
	clear ip auth-proxy cache	Clears authentication proxy entries from the router.
	ip auth-proxy	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).
	ip auth-proxy (interface configuration)	Applies an authentication proxy rule at a firewall interface.
	ip auth-proxy name	Creates an authentication proxy rule.