



# CHAPTER 53

## Configuring Web-Based Authentication

---

This chapter describes how to configure web-based authentication. Cisco IOS Release 12.2(33)SXH and later releases support web-based authentication.



### Note

For complete syntax and usage information for the commands used in this chapter, see the Cisco IOS Master Command List, Release 12.2SX, at this URL:

[http://www.cisco.com/en/US/docs/ios/mcl/122sxmcl/12\\_2sx\\_mcl\\_book.html](http://www.cisco.com/en/US/docs/ios/mcl/122sxmcl/12_2sx_mcl_book.html)

---



### Tip

For additional information about Cisco Catalyst 6500 Series Switches (including configuration examples and troubleshooting information), see the documents listed on this page:

[http://www.cisco.com/en/US/products/hw/switches/ps708/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html)

---

This chapter consists of these sections:

- [Understanding Web-Based Authentication, page 53-1](#)
- [Configuring Web-Based Authentication, page 53-6](#)
- [Displaying Web-Based Authentication Status, page 53-15](#)

## Understanding Web-Based Authentication

The web-based authentication feature implements web-based authentication, which is also known as Web Authentication Proxy.

You can use the web-based authentication feature to authenticate end users on host systems that do not run the IEEE 802.1X supplicant. You can configure the web-based authentication feature on Layer 2 and Layer 3 interfaces.

When a user initiates an HTTP session, the web-based authentication feature intercepts ingress HTTP packets from the host and sends an HTML login page to the user. The user keys in their credentials, which the web-based authentication feature sends to the AAA server for authentication. If the authentication succeeds, web-based authentication sends a Login-Successful HTML page to the host and applies the access policies returned by the AAA server.

If the authentication fails, web-based authentication feature sends a Login-Fail HTML page to the user, which prompts the user to retry the login attempt. If the user exceeds the maximum number of failed login attempts, web-based authentication sends a Login-Expired HTML page to the host and the user is placed on a watch list for a waiting period.

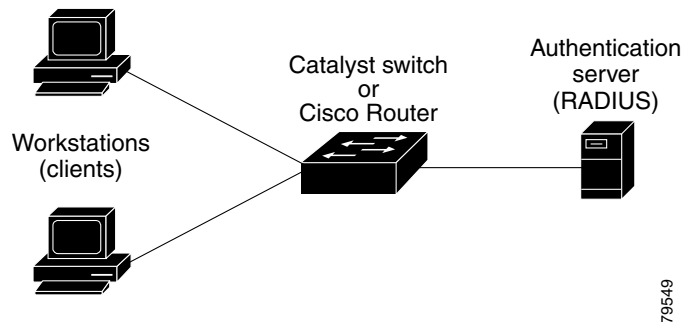
These sections describe the role of web-based authentication as a part of the authentication, authorization, and accounting (AAA) system:

- [Device Roles](#), page 53-2
- [Host Detection](#), page 53-3
- [Session Creation](#), page 53-3
- [Authentication Process](#), page 53-3
- [AAA Fail Policy](#), page 53-4
- [Customization of the Authentication Proxy Web Pages](#), page 53-4
- [Web-based Authentication Interactions with Other Features](#), page 53-5

## Device Roles

With web-based authentication, the devices in the network have specific roles as shown in [Figure 53-1](#).

**Figure 53-1** Web-based Authentication Device Roles



The specific roles shown in [Figure 53-1](#) are as follows:

- *Client*—The device (workstation) that requests access to the LAN and switch services and responds to requests from the switch. The workstation must be running an HTML browser with Java Script enabled.
- *Authentication server*—Performs the actual authentication of the client. The authentication server validates the identity of the client and notifies the switch whether or not the client is authorized to access the LAN and switch services.
- *Switch*—Controls the physical access to the network based on the authentication status of the client. The switch acts as an intermediary (proxy) between the client and the authentication server, requesting identity information from the client, verifying that information with the authentication server, and relaying a response to the client.

## Host Detection

The switch maintains an IP device tracking table to store information about detected hosts.

**Note**

By default, the IP device tracking feature is disabled on a switch. You must enable the IP device tracking feature to use web-based authentication.

For Layer 3 interfaces, web-based authentication sets an HTTP intercept ACL when the feature is configured on the interface (or when the interface is put in service).

For Layer 2 interfaces, web-based authentication detects IP hosts using the following mechanisms:

- ARP based trigger—ARP redirect ACL allows web-based authentication to detect hosts with static IP address or dynamically acquired IP address.
- Dynamic ARP Inspection
- DHCP snooping—Web-based authentication is notified when the switch creates a DHCP binding entry for the host.

## Session Creation

When web-based authentication detects a new host, it creates a session as follows:

- Checks the exception list  
If the host IP is included in the exception list, the policy from the exception list entry is applied, and the session is considered to be established.
- Checks for Auth bypass  
If the host IP is not on the exception list, web-based authentication sends a nonresponsive host (NRH) request to the server.  
If the server response is Access Accepted, authorization is bypassed for this host. The session is considered to be established.
- Sets up the HTTP Intercept ACL  
If the server response to the NRH request is Access Rejected, the HTTP intercept ACL is activated and the session waits for HTTP traffic from the host.

## Authentication Process

When web-based authentication is enabled, the following events occur:

- The user initiates an HTTP session.
- The HTTP traffic is intercepted, and authorization is initiated. The switch sends the login page to the user. The user enters a username and password on the login page, and the switch sends the entries to the authentication server.
- If the client identity is valid and the authentication succeeds, the switch downloads and activates the user's access policy from the authentication server. The login success page is sent to the user.
- If the authentication fails, the switch sends the login fail page. The user retries the login, but if the maximum number of attempts fail, the switch sends the login expired page and the host is placed in a watch list. After a watch list timeout, the user can retry the authentication process.

- If the authentication server does not respond to the switch, and if an AAA fail policy is configured, the switch will apply the failure access policy to the host. The login success page is sent to the user. The AAA fail policy feature is available in Cisco IOS Release 12.2(33)SXI and later releases.

The switch reauthenticates a client when the host does not respond to an ARP probe on a Layer 2 interface, or the host does not send any traffic within the idle timeout on a Layer 3 interface.

- The feature applies the downloaded timeout or the locally configured session timeout.
- If the terminate action is RADIUS, the feature sends a nonresponsive host (NRH) request to the server. The terminate action is included in the response from the server.
- If the terminate action is default, the session is dismantled and the applied policy is removed.

## AAA Fail Policy

The AAA fail policy, supported in Cisco IOS Release 12.2(33)SXI and later releases, is a method for allowing a user to connect or to remain connected to the network if the AAA server is not available. If the AAA server cannot be reached when web-based authentication of a client is needed, instead of rejecting the user (that is, not providing the access to the network), an administrator can configure a default AAA fail policy that can be applied to the user.

This policy is advantageous for the following reasons:

- While AAA is unavailable, the user will still have connectivity to the network, although access may be restricted.
- When the AAA server is again available, a user can be revalidated, and the user's normal access policies can be downloaded from the AAA server.



### Note

When the AAA server is down, the AAA fail policy is applied only if there is no existing policy associated with the user. Typically, if the AAA server is unavailable when a user session requires reauthentication, the policies currently in effect for the user are retained.

While the AAA fail policy is in effect, the session state is maintained as AAA Down.

## Customization of the Authentication Proxy Web Pages

The switch's internal HTTP server hosts four HTML pages for delivery to an authenticating client during the web-based authentication process. The four pages allow the server to notify the user of the following four states of the authentication process:

- Login—The user's credentials are requested
- Success—The login was successful
- Fail—The login has failed
- Expire—The login session has expired due to excessive login failures

In Cisco IOS Release 12.2(33)SXI and later releases, you can substitute your custom HTML pages for the four default internal HTML pages, or you can specify a URL to which the user will be redirected upon successful authentication, effectively replacing the internal Success page.

## Web-based Authentication Interactions with Other Features

These sections describe web-based authentication interactions with these features:

- [Port Security, page 53-5](#)
- [LAN Port IP, page 53-5](#)
- [Gateway IP, page 53-5](#)
- [ACLs, page 53-5](#)
- [IP Source Guard, page 53-6](#)
- [EtherChannel, page 53-6](#)
- [Switchover, page 53-6](#)

### Port Security

You can configure web-based authentication and port security on the same port. (You configure port security on the port by using the **switchport port-security** interface configuration command.) When you enable port security and web-based authentication on a port, web-based authentication authenticates the port, and port security manages network access for all MAC addresses, including that of the client. You can then limit the number or group of clients that can access the network through the port.

For more information about enabling port security, see the [“Configuring Port Security” section on page 54-5](#).

### LAN Port IP

You can configure LAN port IP (LPIP) and Layer 2 web-based authentication on the same port. The host is authenticated using web-based authentication first, and then LPIP posture validation takes place. The LPIP host policy overrides the web-based authentication host policy.

If the web-based authentication idle timer expires, the NAC policy is removed. The host is authenticated and posture validated again.

### Gateway IP

You cannot configure Gateway IP on a Layer 3 VLAN interface if web-based authentication is configured on any of the switch ports in the VLAN.

You can configure web-based authentication on the same Layer 3 interface as Gateway IP. The host policies for both features are applied in software. The GWIP policy overrides the web-based authentication host policy.

### ACLs

If you configure a VLAN ACL or Cisco IOS ACL on an interface, the ACL is applied to the host traffic only after the web-based authentication host policy is applied.

For Layer 2 web-based authentication, you must configure a port ACL (PACL) as the default access policy for ingress traffic from hosts connected to the port. After authentication, the web-based authentication host policy overrides the PACL.

You cannot configure a MAC ACL and web-based authentication on the same interface.

You cannot configure web-based authentication on a port whose access VLAN has VACL capture configured.

## IP Source Guard

In releases earlier than Cisco IOS Release 12.2(33)SX12, configuring IP Source Guard and web-based authentication on the same interface is not supported.

In Cisco IOS Release 12.2(33)SX12 and later releases, you can configure IP Source Guard and web-based authentication on the same interface. If DHCP snooping is also enabled on the access VLAN, you must enter the **mls acl tcam override dynamic dhcp-snooping** command in global configuration mode to avoid conflict between the two features. Other VLAN-based features are not supported when IP Source Guard and web-based authentication are combined.

## EtherChannel

You can configure web-based authentication on a Layer 2 EtherChannel interface. The web-based authentication configuration applies to all member channels.

## Switchover

On Catalyst 6500 series switches with redundant supervisor engines in RPR mode redundancy, information about currently authenticated hosts is maintained during a switchover. Users will not need to reauthenticate.

# Configuring Web-Based Authentication

These sections describe how to configure web-based authentication:

- [Default Web-Based Authentication Configuration, page 53-7](#)
- [Web-based Authentication Configuration Guidelines and Restrictions, page 53-7](#)
- [Web-based Authentication Configuration Task List, page 53-8](#)
- [Configuring the Authentication Rule and Interfaces, page 53-8](#)
- [Configuring AAA Authentication, page 53-9](#)
- [Configuring Switch-to-RADIUS-Server Communication, page 53-9](#)
- [Configuring the HTTP Server, page 53-11](#)
- [Configuring the Web-based Authentication Parameters, page 53-14](#)
- [Removing Web-based Authentication Cache Entries, page 53-15](#)

## Default Web-Based Authentication Configuration

Table 53-1 shows the default web-based authentication configuration.

**Table 53-1** *Default Web-based Authentication Configuration*

Feature	Default Setting
AAA	Disabled
RADIUS server	<ul style="list-style-type: none"> <li>• None specified</li> <li>• 1812</li> <li>• None specified</li> </ul>
Default value of inactivity timeout	3600 seconds
Inactivity timeout	Enabled

## Web-based Authentication Configuration Guidelines and Restrictions

These are the web-based authentication configuration guidelines:

- Web-based authentication is an ingress-only feature.
- You can configure web-based authentication only on access ports. Web-based authentication is not supported on trunk ports, EtherChannel member ports, or dynamic trunk ports.
- You must configure the default ACL on the interface before configuring web-based authentication. Configure a port ACL for a Layer 2 interface, or a Cisco IOS ACL for a Layer 3 interface.
- On Layer 2 interfaces, you cannot authenticate hosts with static ARP cache assignment. These hosts are not detected by the web-based authentication feature, because they do not send ARP messages.
- By default, the IP device tracking feature is disabled on a switch. You must enable the IP device tracking feature to use web-based authentication.
- You must configure at least one IP address to run the HTTP server on the switch. You must also configure routes to reach each host IP address. The HTTP server sends the HTTP login page to the host.
- Hosts that are more than one hop away may experience traffic disruption if an STP topology change results in the host traffic arriving on a different port. This is because ARP and DHCP updates may not be sent after a Layer 2 (STP) topology change.
- Web-based authentication does not support VLAN assignment as a downloadable host policy.
- Cisco IOS Release 12.2(33)SXI and later releases support downloadable ACLs (DACLS) from the RADIUS server.
- Web-based authentication is not supported for IPv6 traffic.

## Web-based Authentication Configuration Task List

To configure the web-based authentication feature, perform the following tasks:

- [Configuring the Authentication Rule and Interfaces, page 53-8](#)
- [Configuring AAA Authentication, page 53-9](#)
- [Configuring Switch-to-RADIUS-Server Communication, page 53-9](#)
- [Configuring the HTTP Server, page 53-11](#)
- [Configuring an AAA Fail Policy, page 53-13](#)
- [Configuring the Web-based Authentication Parameters, page 53-14](#)
- [Removing Web-based Authentication Cache Entries, page 53-15](#)

## Configuring the Authentication Rule and Interfaces

To configure web-based authentication, perform this task:

	Command	Purpose
Step 1	Router(config)# <b>ip admission name name proxy http</b>	Configures an authentication rule for web-based authorization.
Step 2	Router(config)# <b>interface type<sup>1</sup> slot/port</b>	Enters interface configuration mode and specifies the ingress Layer 2 or Layer 3 interface to be enabled for web-based authentication.
Step 3	Router(config-if)# <b>ip access-group name</b>	Applies the default ACL.
Step 4	Router(config-if)# <b>ip admission name</b>	Configures web-based authentication on the specified interface.
Step 5	Router(config-if)# <b>authentication order method1 [method2] [method3]</b>	(Optional) Specifies the fallback order of authentication methods to be used. The three values of <i>method</i> , in the default order, are <b>dot1x</b> , <b>mab</b> , and <b>webauth</b> .  Omitting a method disables that method on the interface.
Step 6	Router(config-if)# <b>exit</b>	Returns to configuration mode.
Step 7	Router(config)# <b>ip device tracking</b>	Enables the IP device tracking table.
Step 8	Router(config)# <b>end</b>	Returns to privileged EXEC mode.
Step 9	Router# <b>show ip admission configuration</b>	Displays the configuration.

1. *type* = fastethernet, gigabitethernet, or tengigabitethernet

This example shows how to enable web-based authentication, while disabling 802.1X or MAB authentication, on Fast Ethernet port 5/1:

```
Router(config)# ip admission name webauth1 proxy http
Router(config)# interface fastethernet 5/1
Router(config-if)# ip admission webauth1
Router(config-if)# authentication order webauth
Router(config-if)# exit
Router(config)# ip device tracking
```

This example shows how to verify the configuration:

```
Router# show ip admission configuration
Authentication Proxy Banner not configured
Authentication global cache time is 60 minutes
Authentication global absolute time is 0 minutes
Authentication global init state time is 2 minutes
Authentication Proxy Watch-list is disabled

Authentication Proxy Rule Configuration
Auth-proxy name webauth1
http list not specified inactivity-time 60 minutes

Authentication Proxy Auditing is disabled
Max Login attempts per user is 5
```

## Configuring AAA Authentication

To enable web-based authentication, you must enable AAA and specify the authentication method. perform this task:

	Command	Purpose
Step 1	Router(config)# <b>aaa new-model</b>	Enables AAA functionality.
Step 2	Router(config)# <b>aaa authentication login default group {tacacs+   radius}</b>	Defines the list of authentication methods at login.
Step 3	Router(config)# <b>aaa authorization auth-proxy default group {tacacs+   radius}</b>	Creates an authorization method list for web-based authorization.
Step 4	Router(config)# <b>tacacs-server host {hostname   ip_address}</b>	Specifies an AAA server. For Radius servers, see the section <a href="#">“Configuring Switch-to-RADIUS-Server Communication”</a> section on page 53-9.
Step 5	Router(config)# <b>tacacs-server key {key-data}</b>	Configures the authorization and encryption key used between the switch and the TACACS server.

This example shows how to enable AAA:

```
Router(config)# aaa new-model
Router(config)# aaa authentication login default group tacacs+
Router(config)# aaa authorization auth-proxy default group tacacs+
```

## Configuring Switch-to-RADIUS-Server Communication

RADIUS security servers are identified by any of the following:

- Host name
- Host IP address
- Host name and specific UDP port numbers
- IP address and specific UDP port numbers

The combination of the IP address and UDP port number creates a unique identifier, which enables RADIUS requests to be sent to multiple UDP ports on a server at the same IP address. If two different host entries on the same RADIUS server are configured for the same service (for example, authentication) the second host entry that is configured functions as the failover backup to the first one. The RADIUS host entries are chosen in the order that they were configured.

To configure the RADIUS server parameters, perform this task:

	Command	Purpose
Step 1	Router(config)# <b>ip radius source-interface</b> <i>interface_name</i>	Specifies that the RADIUS packets have the IP address of the indicated interface.
Step 2	Router(config)# <b>radius-server host</b> { <i>hostname</i>   <i>ip-address</i> } <b>test username</b> <i>username</i>	Specifies the host name or IP address of the remote RADIUS server.  The <b>test username</b> <i>username</i> option enables automated testing of the RADIUS server connection. The specified <i>username</i> does not need to be a valid user name.  The <b>key</b> option specifies an authentication and encryption key to be used between the switch and the RADIUS server.  To use multiple RADIUS servers, reenter this command.
Step 3	Router(config)# <b>radius-server key</b> <i>string</i>	Configures the authorization and encryption key used between the switch and the RADIUS daemon running on the RADIUS server.
Step 4	Router(config)# <b>radius-server vsa send authentication</b>	Enables downloading of an ACL from the RADIUS server. This feature is supported in Cisco IOS Release 12.2(33)SXI and later releases.
Step 5	Router(config)# <b>radius-server dead-criteria tries</b> <i>num-tries</i>	Specifies the number of unanswered transmits to a RADIUS server before considering the server to be dead. The range of <i>num-tries</i> is 1 to 100.

When you configure the RADIUS server parameters, note the following information:

- Specify the **key string** on a separate command line.
- For **key string**, specify the authentication and encryption key used between the switch and the RADIUS daemon running on the RADIUS server. The key is a text string that must match the encryption key used on the RADIUS server.
- When you specify the **key string**, spaces within and at the end of the key are used. If you use spaces in the key, do not enclose the key in quotation marks unless the quotation marks are part of the key. This key must match the encryption used on the RADIUS daemon.
- You can globally configure the timeout, retransmission, and encryption key values for all RADIUS servers by using the **radius-server host** global configuration command. If you want to configure these options on a per-server basis, use the **radius-server timeout**, **radius-server retransmit**, and the **radius-server key** global configuration commands. For more information, see the *Cisco IOS Security Configuration Guide*, Release 12.2, publication and the *Cisco IOS Security Command Reference*, Release 12.2, publication at this URL:  
[http://www.cisco.com/en/US/docs/ios/12\\_2/security/command/reference/fsecur\\_r.html](http://www.cisco.com/en/US/docs/ios/12_2/security/command/reference/fsecur_r.html)
- Cisco IOS Release 12.2(33)SXI and later releases support downloadable ACLs (DACLS) from the RADIUS server.

**Note**

You also need to configure some settings on the RADIUS server. These settings include the IP address of the switch, the key string to be shared by both the server and the switch, and the downloadable ACL. For more information, see the RADIUS server documentation.

This example shows how to configure the RADIUS server parameters on the switch:

```
Router(config)# ip radius source-interface Vlan80
Router(config)# radius-server host 172.120.39.46 test username user1
Router(config)# radius-server key rad123
Router(config)# radius-server dead-criteria tries 2
```

## Configuring the HTTP Server

To use web-based authentication, you must enable the HTTP server within the switch. You can enable the server for either HTTP or HTTPS. To enable the server, perform one of these tasks in global configuration mode:

Command	Purpose
Router(config)# <b>ip http server</b>	Enables the HTTP server. The web-based authentication feature uses the HTTP server to communicate with the hosts for user authentication.
Router(config)# <b>ip http secure-server</b>	Enables HTTPS.

With Cisco IOS Release 12.2(33)SX1 and later releases, you can optionally configure custom authentication proxy web pages or specify a redirection URL for successful login, as described in the following sections:

- [Customizing the Authentication Proxy Web Pages](#)
- [Specifying a Redirection URL for Successful Login](#)

## Customizing the Authentication Proxy Web Pages

With Cisco IOS Release 12.2(33)SX1 and later releases, you have the option to provide four substitute HTML pages to be displayed to the user in place of the switch's internal default HTML pages during web-based authentication.

To specify the use of your custom authentication proxy web pages, first store your custom HTML files on the switch's internal disk or flash memory, then perform this task in global configuration mode:

	Command	Purpose
<b>Step 1</b>	Router(config)# <b>ip admission proxy http login page file</b> <i>device:login-filename</i>	Specifies the location in the switch memory file system of the custom HTML file to be used in place of the default login page. The <i>device:</i> is either disk or flash memory, such as disk0:.
<b>Step 2</b>	Router(config)# <b>ip admission proxy http success page file</b> <i>device:success-filename</i>	Specifies the location of the custom HTML file to be used in place of the default login success page.

	Command	Purpose
Step 3	Router(config)# <b>ip admission proxy http failure page file</b> <i>device:fail-filename</i>	Specifies the location of the custom HTML file to be used in place of the default login failure page.
Step 4	Router(config)# <b>ip admission proxy http login expired page file</b> <i>device:expired-filename</i>	Specifies the location of the custom HTML file to be used in place of the default login expired page.

When configuring the use of customized authentication proxy web pages, consider the following guidelines:

- To enable the custom web pages feature, you must specify all four custom HTML files. If fewer than four files are specified, the internal default HTML pages will be used.
- The four custom HTML files must be present on the disk or flash of the switch.
- An image file has a size limit of 256 KB.
- All image files must have a filename that begins with “web\_auth\_” (like “web\_auth\_logo.jpg” instead of “logo.jpg”).
- All image file names must be less than 33 characters.
- Any images on the custom pages must be located on an accessible HTTP server. An intercept ACL must be configured within the admission rule to allow access to the HTTP server.
- Any external link from a custom page will require configuration of an intercept ACL within the admission rule.
- Any name resolution required for external links or images will require configuration of an intercept ACL within the admission rule to access a valid DNS server.
- If the custom web pages feature is enabled, a configured auth-proxy-banner will not be used.
- If the custom web pages feature is enabled, the redirection URL for successful login feature will not be available.
- To remove the specification of a custom file, use the **no** form of the command.

Because the custom login page is a public web form, consider the following guidelines for this page:

- The login form must accept user input for the username and password and must POST the data as **uname** and **pwd**.
- The custom login page should follow best practices for a web form, such as page timeout, hidden password, and prevention of redundant submissions.

The following example shows how to configure custom authentication proxy web pages:

```
Router(config)# ip admission proxy http login page file disk1:login.htm
Router(config)# ip admission proxy http success page file disk1:success.htm
Router(config)# ip admission proxy http fail page file disk1:fail.htm
Router(config)# ip admission proxy http login expired page file disk1:expired.htm
```

The following example shows how to verify the configuration of custom authentication proxy web pages:

```
Router# show ip admission configuration

Authentication proxy webpage
Login page           : disk1:login.htm
Success page        : disk1:success.htm
Fail Page           : disk1:fail.htm
Login expired Page  : disk1:expired.htm

Authentication global cache time is 60 minutes
Authentication global absolute time is 0 minutes
```

```

Authentication global init state time is 2 minutes
Authentication Proxy Session ratelimit is 100
Authentication Proxy Watch-list is disabled
Authentication Proxy Auditing is disabled
Max Login attempts per user is 5

```

## Specifying a Redirection URL for Successful Login

With Cisco IOS Release 12.2(33)SXI and later releases, you have the option to specify a URL to which the user will be redirected upon successful authentication, effectively replacing the internal Success HTML page.

To specify a redirection URL for successful login, perform this task in global configuration mode:

Command	Purpose
Router(config)# <b>ip admission proxy http success redirect url-string</b>	Specifies a URL for redirection of the user in place of the default login success page.

When configuring a redirection URL for successful login, consider the following guidelines:

- If the custom authentication proxy web pages feature is enabled, the redirection URL feature is disabled and will not be available in the CLI. You can perform redirection in the custom login success page.
- If the redirection URL feature is enabled, a configured auth-proxy-banner will not be used.
- To remove the specification of a redirection URL, use the **no** form of the command.

The following example shows how to configure a redirection URL for successful login:

```
Router(config)# ip admission proxy http success redirect www.cisco.com
```

The following example shows how to verify the redirection URL for successful login:

```

Router# show ip admission configuration

Authentication Proxy Banner not configured
Customizable Authentication Proxy webpage not configured
HTTP Authentication success redirect to URL: http://www.cisco.com
Authentication global cache time is 60 minutes
Authentication global absolute time is 0 minutes
Authentication global init state time is 2 minutes
Authentication Proxy Watch-list is disabled
Authentication Proxy Max HTTP process is 7
Authentication Proxy Auditing is disabled
Max Login attempts per user is 5

```

## Configuring an AAA Fail Policy

The AAA fail policy for web-based authentication is supported in Cisco IOS Release 12.2(33)SXI and later releases.

To configure an AAA fail policy, perform this task in global configuration mode:

	Command	Purpose
Step 1	Router(config)# <b>ip admission name</b> <i>rule-name</i> <b>proxy http event timeout</b> <b>aaa policy identity</b> <i>identity_policy_name</i>	Creates an AAA fail rule and associates an identity policy to be applied to sessions when the AAA server is unreachable.  To remove the rule on the switch, use the <b>no ip admission name</b> <i>rule-name</i> <b>proxy http event timeout aaa policy identity</b> global configuration command.
Step 2	Router(config)# <b>ip admission ratelimit aaa-down</b> <i>number_of_sessions</i>	(Optional) To avoid flooding the AAA server when it returns to service, you can rate limit the authentication attempts from hosts in the AAA Down state.

The following example shows how to apply an AAA fail policy:

```
Router(config)# ip admission name AAA_FAIL_POLICY proxy http event timeout aaa policy
identity GLOBAL_POLICY1
```

The following example shows how to determine whether any hosts are connected in the AAA Down state:

```
Router# show ip admission cache
Authentication Proxy Cache
  Client IP 209.165.201.11 Port 0, timeout 60, state ESTAB (AAA Down)
```

The following example shows how to view detailed information about a particular session based on the host IP address:

```
Router# show ip admission cache 209.165.201.11
Address          : 209.165.201.11
MAC Address     : 0000.0000.0000
Interface       : Vlan333
Port            : 3999
Timeout         : 60
Age             : 1
State           : AAA Down
AAA Down policy : AAA_FAIL_POLICY
```

## Configuring the Web-based Authentication Parameters

You can configure the maximum number of failed login attempts before the client is placed in a watch list for a waiting period.

To configure the web-based authentication parameters, perform this task:

	Command	Purpose
Step 1	Router(config)# <b>ip admission max-login-attempts</b> <i>number</i>	Sets the maximum number of failed login attempts. The range is 1 to 2147483647 attempts; the default is 5.
Step 2	Router(config)# <b>end</b>	Returns to privileged EXEC mode.
Step 3	Router# <b>show ip admission configuration</b>	Displays the authentication proxy configuration.
Step 4	Router# <b>show ip admission cache</b>	Displays the list of authentication entries.

This example shows how to set the maximum number of failed login attempts to 10:

```
Router(config)# ip admission max-login-attempts 10
```

## Removing Web-based Authentication Cache Entries

To delete existing session entries, perform either of these tasks:

Command	Purpose
Router# <b>clear ip auth-proxy cache</b> {*   <i>host ip address</i> }	Deletes authentication proxy entries. Use an asterisk to delete all cache entries. Enter a specific IP address to delete the entry for a single host.
Router# <b>clear ip admission cache</b> {*   <i>host ip address</i> }	Deletes authentication proxy entries. Use an asterisk to delete all cache entries. Enter a specific IP address to delete the entry for a single host.

This example shows how to remove the web-based authentication session for the client at a specific IP address:

```
Router# clear ip auth-proxy cache 209.165.201.1
```

## Displaying Web-Based Authentication Status

To display the web-based authentication settings for all interfaces or for specific ports, perform this task:

Command	Purpose
<b>Step 1</b> Router# <b>show fm ip-admission l2http</b> [ <b>all</b>   <b>interface</b> <i>type</i> <sup>1</sup> <i>slot/port</i> ]	Displays the web-based authentication settings.  (Optional) Use the <b>all</b> keyword to display the settings for all interfaces using web-based authentication.  (Optional) Use the <b>interface</b> keyword to display the web-based authentication settings for a specific interface.

1. *type* = fastethernet, gigabitethernet, or tengigabitethernet

This example shows how to view only the global web-based authentication status:

```
Router# show fm ip-admission l2http all
```

This example shows how to view the web-based authentication settings for interface GigabitEthernet 3/27:

```
Router# show fm ip-admission l2http interface gigabitethernet 3/27
```

For detailed information about the fields in these displays, see the Cisco IOS Master Command List, Release 12.2SX.

**Tip**

---

For additional information about Cisco Catalyst 6500 Series Switches (including configuration examples and troubleshooting information), see the documents listed on this page:

[http://www.cisco.com/en/US/products/hw/switches/ps708/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html)

---