CHAPTER 37

Configuring Web-Based Authentication

This chapter describes how to configure web-based authentication. It consists of these sections:

Note For complete syntax and usage information for the switch commands used in this chapter, look at the *Cisco Catalyst 4500 Series Switch Command Reference* and related publications at this location:

http://www.cisco.com/en/US/products/hw/switches/ps4324/index.html

If the command is not found in the Catalyst 4500 Command Reference, it is located in the larger Cisco IOS library. Refer to the *Catalyst 4500 Series Switch Cisco IOS Command Reference* and related publications at this location:

http://www.cisco.com/en/US/products/ps6350/index.html

About Web-Based Authentication

The web-based authentication feature, known as Web Authentication Proxy, enables you to authenticate end users on host systems that do not run the IEEE 802.1X supplicant.

When you initiate an HTTP session, web-based authentication 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 authentication succeeds, web-based authentication sends a Login-Successful HTML page to the host and applies the access policies returned by the AAA server.

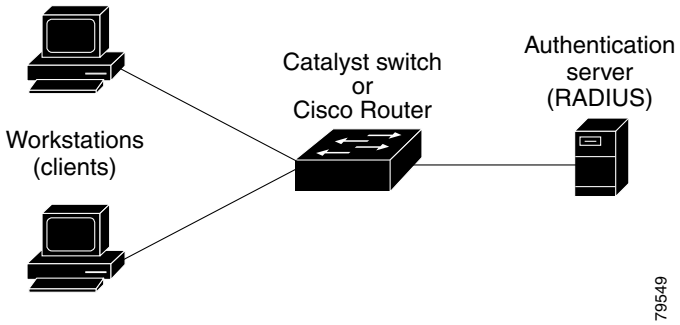
If authentication fails, web-based authentication forwards a Login-Fail HTML page to the user, prompting the user to retry the login. If the user exceeds the maximum number of attempts, web-based authentication forwards a Login-Expired HTML page to the host and the user is placed on a watch list for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

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

Device Roles

With web-based authentication, the devices in the network have specific role (Figure 37-1).

Figure 37-1 Web-Based Authentication Device Roles



The roles 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 that the client is authorized to access the LAN and switch services or that the client is denied.
- *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 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 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 you enable web-based authentication, 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. If the maximum number of attempts fails, the switch sends the login expired page and the host is placed in a watch list. After the watch list times out, 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 applies the failure access policy to the host. The login success page is sent to the user. (See the "Customization of the Authentication Proxy Web Pages" section on page 37-4.)
- 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.

Customization of the Authentication Proxy Web Pages

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

- Login—Your credentials are requested
- Success—The login was successful
- Fail—The login failed
- Expire—The login session has expired because of excessive login failures

You can substitute your custom HTML pages for the four default internal HTML pages, or you can specify a URL to which you are 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 37-4
- LAN Port IP, page 37-4
- ACLs, page 37-5
- Context-Based Access Control, page 37-5
- 802.1X Authentication, page 37-5
- EtherChannel, page 37-5
- Switchover, page 37-5

Port Security

You can configure web-based authentication and port security on the same port. (You configure port security on the port with 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 Chapter 38, “Configuring Port Security.”

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, followed by LPIP posture validation. 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 is validated again.

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 is configured for VACL capture.

Context-Based Access Control

Web-based authentication cannot be configured on a Layer 2 port if context-based access control (CBAC) is configured on the Layer 3 VLAN interface of the port's VLAN.

802.1X Authentication

You cannot configure web-based authentication on the same port as 802.1X authentication except as a fallback authentication method.

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 4500 series switches with redundant supervisor engines in RPR mode, information about currently authenticated hosts is maintained during a switchover. You do not need to reauthenticate.

Configuring Web-Based Authentication

These sections describe how to configure web-based authentication:

Default Web-Based Authentication Configuration

Table 37-1 shows the default web-based authentication configuration.

Table 37-1 Default Web-based Authentication Configuration

Feature	Default Setting
AAA	Disabled
RADIUS server • IP address • UDP authentication port • Key	 • None specified • 1812 • None specified
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 authentication requires two Cisco Attribute-Value (AV) pair attributes:

  The first attribute, priv-lvl=15, must always be set to 15. This sets the privilege level of the user who is logging into the switch.

  The second attribute is an access list to be applied for web-authenticated hosts. The syntax is similar to 802.1x per-user access control lists (ACLs). However, instead of ip:inacl, this attribute must begin with proxyacl, and the source field in each entry must be any. (After authentication, the client IP address replaces the any field when the ACL is applied.)

  For example:

```
proxyacl# 10=permit ip any 10.0.0.0 0.255.255.255
proxyacl# 20=permit ip any 11.1.0.0 0.0.255.255
proxyacl# 30=permit udp any any eq syslog
proxyacl# 40=permit udp any any eq tftp
```

Note The proxyacl entry determines the type of allowed network access.

- 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.
- 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.
- Starting with Cisco IOS Release 12.2(50)SG , you can apply 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 37-7
- Configuring AAA Authentication, page 37-8
- Configuring Switch-to-RADIUS-Server Communication, page 37-8
- Configuring the HTTP Server, page 37-10
- Configuring the Web-Based Authentication Parameters, page 37-13
- Removing Web-Based Authentication Cache Entries, page 37-13

Configuring the Authentication Rule and Interfaces

To configure web-based authentication, perform this task:

	Command	Purpose
Step 1	`Switch(config)# ip admission name name proxy http`	Configures an authentication rule for web-based authorization.
	`Switch(config)# no ip admission name name`	Removes the authentication rule.
Step 2	`Switch(config)# interface type slot/port`	Enters interface configuration mode and specifies the ingress Layer 2 or Layer 3 interface to be enabled for web-based authentication. *type* can be fastethernet, gigabit ethernet, or tengigabitethernet
Step 3	`Switch(config-if)# ip access-group name`	Applies the default ACL.
Step 4	`Switch(config-if)# ip admission name`	Configures web-based authentication on the specified interface.
Step 5	`Switch(config-if)# exit`	Returns to configuration mode.
Step 6	`Switch(config)# ip device tracking`	Enables the IP device tracking table.
Step 7	`Switch(config)# end`	Returns to privileged EXEC mode.
Step 8	`Switch# show ip admission configuration`	Displays the configuration.

This example shows how to enable web-based authentication on Fast Ethernet port 5/1:

```
Switch(config)# ip admission name webauth1 proxy http
Switch(config)# interface fastethernet 5/1
```

```
Switch(config-if)# ip admission webauth1
Switch(config-if)# exit
Switch(config)# ip device tracking
```

This example shows how to verify the configuration:

```
Switch# 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, perform this task:

	Command	Purpose
Step 1	`Switch(config)# aaa new-model`	Enables AAA functionality.
	`Switch(config)# no aaa new-model`	Disables AAA functionality.
Step 2	`Switch(config)# aaa authentication login default group {tacacs+ | radius}`	Defines the list of authentication methods at login.
Step 3	`Switch(config)# aaa authorization auth-proxy default group {tacacs+ | radius}`	Creates an authorization method list for web-based authorization.
	`Switch(config)# no aaa authorization auth-proxy default group {tacacs+ | radius}`	Clears the configured method list.
Step 4	`Switch(config)# tacacs-server host {hostname | ip_address}`	Specifies an AAA server. For RADIUS servers, see the section "Configuring Switch-to-RADIUS-Server Communication" section on page 37-8.
Step 5	`Switch(config)# tacacs-server key {key-data}`	Configures the authorization and encryption key used between the switch and the TACACS server.

This example shows how to enable AAA:

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

Configuring Switch-to-RADIUS-Server Communication

RADIUS security servers are identified by one 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	`Switch(config)# ip radius source-interface interface_name`	Specifies that the RADIUS packets have the IP address of the indicated interface.
	`Switch(config)# no ip radius source-interface`	Prevents the RADIUS packets from having the IP address of the previously indicated interface.
Step 2	`Switch(config)# radius-server host {hostname | ip-address} test username username`	Specifies the host name or IP address of the remote RADIUS server. The **test username** *username* option enables automated testing of the RADIUS server connection. The specified *username* does not need to be a valid user name. The **key** 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.
	`Switch(config)# no radius-server host {hostname | ip-address}`	Deletes the specified RADIUS server.
Step 3	`Switch(config)# radius-server key string`	Configures the authorization and encryption key used between the switch and the RADIUS daemon running on the RADIUS server.
Step 4	`Switch(config)# radius-server vsa send authentication`	Enables downloading of an ACL from the RADIUS server. This feature was introduced in Cisco IOS Release 12.2(50)SG.
Step 5	`Switch(config)# radius-server dead-criteria tries num-tries`	Specifies the number of unanswered transmits to a RADIUS server before considering the server to be inactive. The range of *num-tries* is 1 to 100.

When you configure the RADIUS server parameters, do the following:

- 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*, use spaces within and at the end of the key. 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 with 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

Note You need to configure some settings on the RADIUS server, including: the IP address of the switch, the key string to be shared by both the server and the switch, and the downloadable ACL (DACL). (Starting with Cisco IOS Release 12.2(50)SG, Catalyst 4500 series switches support DACLs.) For more information, see the RADIUS server documentation.

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

```
Switch(config)# ip radius source-interface Vlan80
Switch(config)# radius-server host 172.120.39.46 test username user1
Switch(config)# radius-server key rad123
Switch(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:

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

Starting with Cisco IOS Release 12.2(50)SG, 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(50)SG, you can display four substitute HTML pages to the user rather than the switch's switch 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
Step 1	`Switch(config)# ip admission proxy http login page file device:login-filename`	Specifies the location in the switch memory file system of the custom HTML file to use in place of the default login page. The *device:* is either disk or flash memory, such as *disk0:*.
Step 2	`Switch(config)# ip admission proxy http success page file device:success-filename`	Specifies the location of the custom HTML file to use in place of the default login success page.
Step 3	`Switch(config)# ip admission proxy http failure page file device:fail-filename`	Specifies the location of the custom HTML file to use in place of the default login failure page.
Step 4	`Switch(config)# ip admission proxy http login expired page file device:expired-filename`	Specifies the location of the custom HTML file to use in place of the default login expired page.

When configuring customized authentication proxy web pages, observe the following guidelines:

- To enable the custom web pages feature, specify all four custom HTML files. If you specify fewer than four files, the internal default HTML pages are used.
- The four custom HTML files must be present on the disk or flash of the switch. The maximum size of each HTML file is 8 KB.
- 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 requires configuration of an intercept ACL within the admission rule.
- Any name resolution required for external links or images requires 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 is not used.
- If the custom web pages feature is enabled, the redirection URL for successful login feature is not 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:

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

```
Switch# 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(50)SG, you have the option to specify a URL to which the user is redirected upon successful authentication, effectively replacing the internal Success HTML page.

To specify a redirection URL for successful login, perform this task:

Command	Purpose
`Switch(config)# ip admission proxy http success redirect` *url-string*	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 is not 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 is not 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:

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

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

```
Switch# 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 the Web-Based Authentication Parameters

You can configure the maximum number of failed login attempts allowed 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	`Switch(config)# ip admission max-login-attempts` *number*	Sets the maximum number of failed login attempts. The range is 1 to 2147483647 attempts; the default is 5.
Step 2	`Switch(config)# end`	Returns to privileged EXEC mode.
Step 3	`Switch# show ip admission configuration`	Displays the authentication proxy configuration.
Step 4	`Switch# show ip admission cache`	Displays the list of authentication entries.

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

```
Switch(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
`Switch# clear ip auth-proxy cache {* | host ip address}`	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.
`Switch# clear ip admission cache {* | host ip address}`	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 IP address 209.165.201.1:

```
Switch# 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
Step 1	`Switch# show authentication sessions [interface` *type slot/port*`]`	Displays the web-based authentication settings. type = fastethernet, gigabitethernet, or tengigabitethernet (Optional) Use the **interface** keyword to display the web-based authentication settings for a specific interface.

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

```
Switch# show authentication sessions
```

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

```
Switch# show authentication sessions interface gigabitethernet 3/27
```