CHAPTER 11

Configuring Web-Based Authentication

Finding Feature Information

Your software release may not support all the features documented in this chapter. For the latest feature information and caveats, see the release notes for your platform and software release.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Configuring Web-Based Authentication

- 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 switch HTTP server. You must also configure routes to reach each host IP address. The HTTP server sends the HTTP login page to the host.
- You must configure the default ACL on the interface before configuring web-based authentication. Configure a port ACL for a Layer 2 interface.

Restrictions for Configuring Web-Based Authentication

- 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 cannot authenticate hosts on Layer 2 interfaces with static ARP cache assignment. These hosts are not detected by the web-based authentication feature because they do not send ARP messages.
- Hosts that are more than one hop away might experience traffic disruption if an STP topology change results in the host traffic arriving on a different port. This occurs because the ARP and DHCP updates might not be sent after a Layer 2 (STP) topology change.
- Web-based authentication does not support VLAN assignment as a downloadable-host policy.
- Web-based authentication is not supported for IPv6 traffic.
- Web-based authentication and Network Edge Access Topology (NEAT) are mutually exclusive. You cannot use web-based authentication when NEAT is enabled on an interface, and you cannot use NEAT when web-based authentication is running on an interface.

- Web-based authentication supports only RADIUS authorization servers. You cannot use TACACS+ servers or local authorization.

Information About Configuring Web-Based Authentication

Web-Based Authentication

Use the web-based authentication feature, known as *web authentication proxy*, to authenticate end users on host systems that do not run the IEEE 802.1x supplicant.

Note You can configure web-based authentication on Layer 2 interfaces.

When you initiate an HTTP session, web-based authentication intercepts ingress HTTP packets from the host and sends an HTML login page to the users. The users enter their credentials, which the web-based authentication feature sends to the authentication, authorization, and accounting (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 AAA:

- Device Roles, page 11-2
- Host Detection, page 11-3
- Session Creation, page 11-3
- Authentication Process, page 11-4
- Web Authentication Customizable Web Pages, page 11-6
- Web-Based Authentication Interactions with Other Features, page 11-8

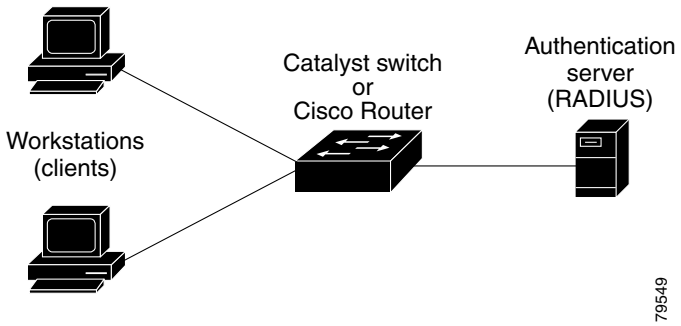
Device Roles

With web-based authentication, the devices in the network have these specific roles:

- Client—The device (workstation) that requests access to the LAN and the services and responds to requests from the switch. The workstation must be running an HTML browser with Java Script enabled.
- Authentication server—Authenticates 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 the 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.

Figure 11-1 Web-Based Authentication Device Roles



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 2 interfaces, web-based authentication detects IP hosts by using these mechanisms:

- ARP-based trigger—ARP redirect ACL allows web-based authentication to detect hosts with a static IP address or a dynamic 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:

- Reviews 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 established.

- Reviews for authorization 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, these 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, and the switch sends the entries to the authentication server.
- If 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 "Local Web Authentication Banner" section on page 11-4.)
- The switch reauthenticates a client when the host does not respond to an ARP probe on a Layer 2 interface, or when 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.

Local Web Authentication Banner

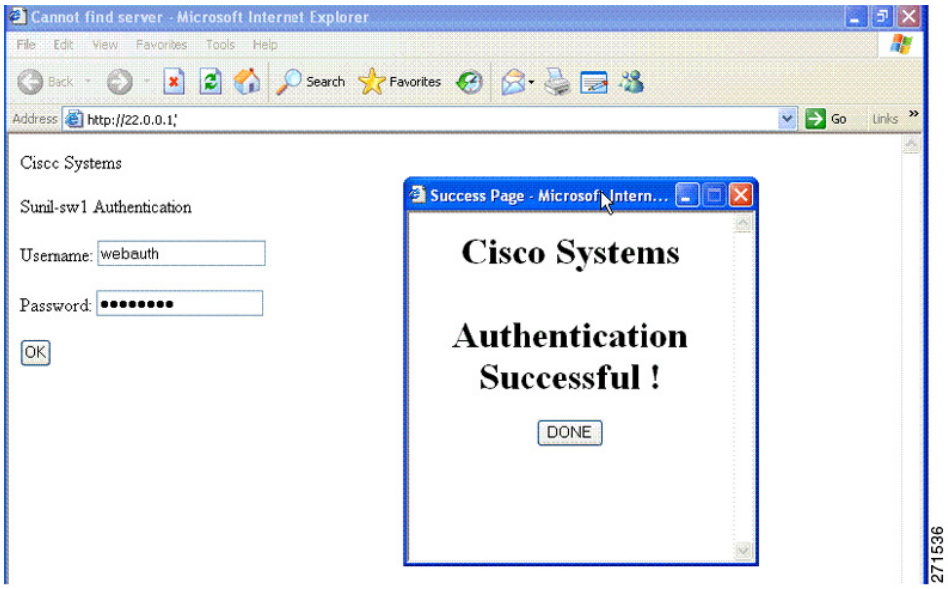
You can create a banner that will appear when you log in to a switch by using web authentication.

The banner appears on both the login page and the authentication-result pop-up pages:

- Authentication Successful
- Authentication Failed
- Authentication Expired

You create a banner by using the **ip admission auth-proxy-banner http** global configuration command. The default banner Cisco Systems and Switch host-name Authentication appear on the Login Page. Cisco Systems appears on the authentication result pop-up page, as shown in Figure 11-2.

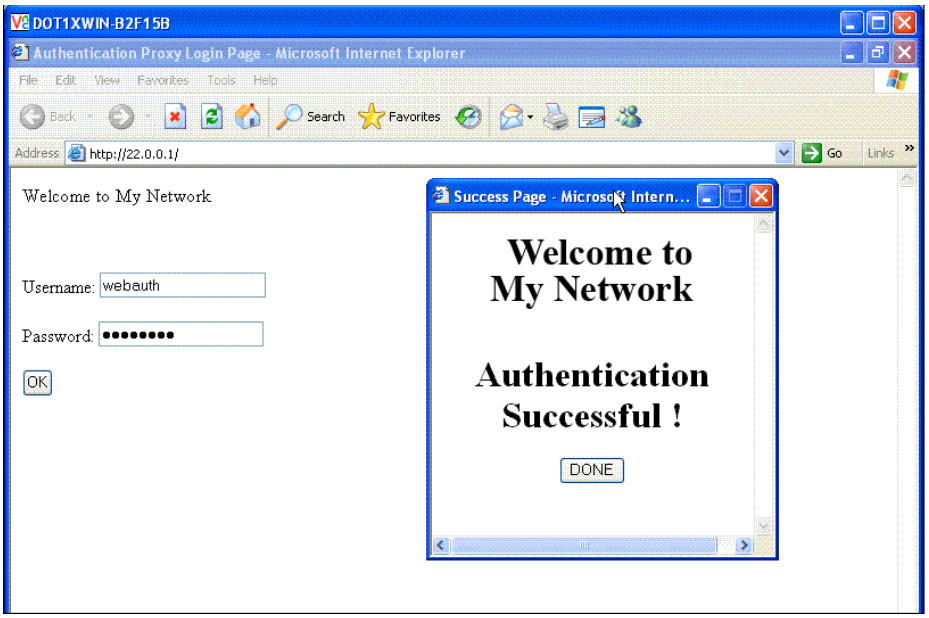
Figure 11-2 Authentication Successful Banner



You can also customize the banner, as shown in Figure 11-3.

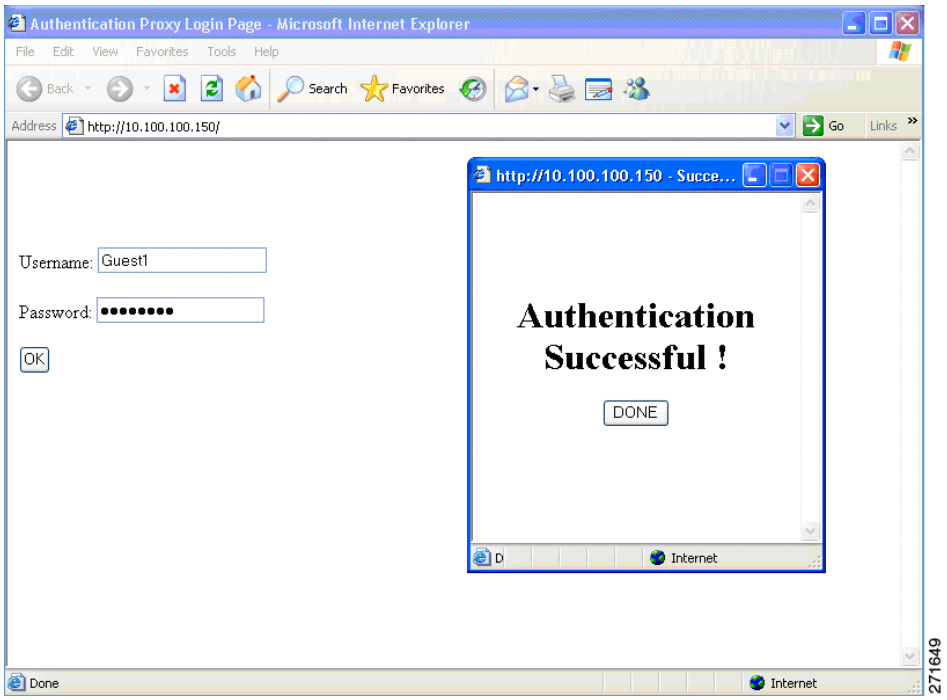
- Add a switch, router, or company name to the banner by using the **ip admission auth-proxy-banner http** *banner-text* global configuration command.
- Add a logo or text file to the banner by using the **ip admission auth-proxy-banner http** *file-path* global configuration command.

Figure 11-3 Customized Web Banner



If you do not enable a banner, only the username and password dialog boxes appear in the web authentication login screen, and no banner appears when you log into the switch, as shown in Figure 11-4.

Figure 11-4 Login Screen with No Banner



For more information, see the *Cisco IOS Security Command Reference* and the "Configuring a Web Authentication Local Banner" section on page 11-14.

Web Authentication Customizable Web Pages

During the web-based authentication process, the switch internal HTTP server hosts four HTML pages to deliver to an authenticating client. The server uses these pages to notify you of these four-authentication process states:

- 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.

Web Authentication Guidelines

- You can substitute your own HTML pages for the default internal HTML pages.
- You can use a logo or specify text in the login, success, failure, and expire web pages.
- On the banner page, you can specify text in the login page.
- The pages are in HTML.
- You must include an HTML redirect command in the success page to access a specific URL.
- The URL string must be a valid URL (for example, http://www.cisco.com). An incomplete URL might cause page not found error or similar errors on a web browser.

- If you configure web pages for HTTP authentication, they must include the appropriate HTML commands (for example, to set the page time out, to set a hidden password, or to confirm that the same page is not submitted twice).
- The CLI command to redirect users to a specific URL is not available when the configured login form is enabled. The administrator should ensure that the redirection is configured in the web page.
- If the CLI command redirecting users to a specific URL after authentication occurs is entered and then the command configuring web pages is entered, the CLI command redirecting users to a specific URL does not take effect.
- Configured web pages can be copied to the switch boot flash or flash.
- Configured pages can be accessed from the flash on the stack master or members.
- The login page can be on one flash, and the success and failure pages can be another flash (for example, the flash on the stack master or a member).
- You must configure all four pages.
- The banner page has no effect if it is configured with the web page.
- All of the logo files (image, flash, audio, video, and so on) that are stored in the system directory (for example, flash, disk0, or disk) and that must be displayed on the login page must use web_auth_*filename* as the filename.
- The configured authentication proxy feature supports both HTTP and SSL.

When configuring customized authentication proxy web pages, follow these guidelines:

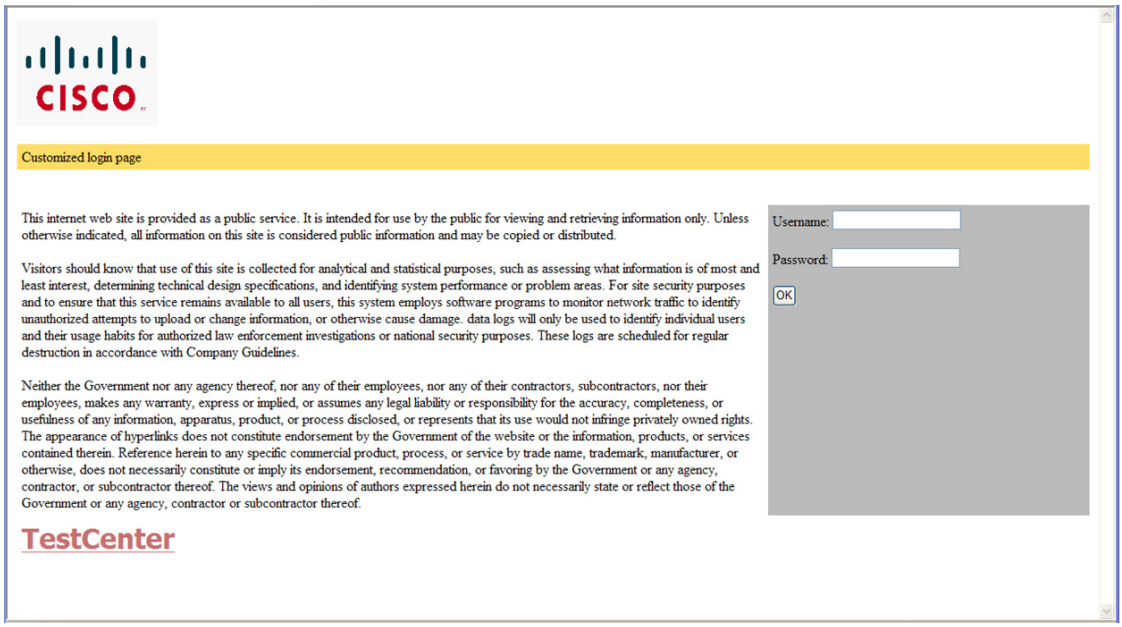
- To enable the custom web pages feature, specify all four custom HTML files. If you specify fewer than four files, the internal default HTML pages are used.
- The four custom HTML files must be present on the flash memory of the switch. The maximum size of each HTML file is 8 KB.
- Any images on the custom pages must be on an accessible HTTP server. Configure an intercept ACL within the admission rule.
- Any external link from a custom page requires configuration of an intercept ACL within the admission rule.
- To access a valid DNS server, any name resolution required for external links or images requires configuration of an intercept ACL within the admission rule.
- 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 these guidelines for the page:

- The login form must accept user entries for the username and password and must show them 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.

You can substitute your HTML pages, as shown in Figure 11-5, for the default internal HTML pages. You can also specify a URL to which users are redirected after authentication occurs, which replaces the internal Success page.

Figure 11-5 Customizeable Authentication Page



Web-Based Authentication Interactions with Other Features

Port Security

You can configure web-based authentication and port security on the same 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 26-11.

LAN Port IP

You can configure LAN port IP (LPIP) and Layer 2 web-based authentication on the same port. The host is authenticated by 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.

Gateway IP

You cannot configure Gateway IP (GWIP) 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 a 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.

Note When a proxy ACL is configured for a web-based authentication client, the proxy ACL is downloaded and applied as part of the authorization process. Hence, the PACL displays the proxy ACL access control entry (ACE).

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 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.

Default Web-Based Authentication Settings

Table 11-1 Default Web-Based Authentication Settings

Feature	Default Settings
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

Configuring Switch-to-RADIUS-Server Communication

RADIUS security servers identification:

- 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, that 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.

How to Configure Web-Based Authentication

Configuring the Authentication Rule and Interfaces

	Command	Purpose
Step 1	**ip admission name** *name* **proxy http**	Configures an authentication rule for web-based authorization.
Step 2	**interface** *type slot/port*	Enters interface configuration mode and specifies the ingress Layer 2 interface to be enabled for web-based authentication. *type* can be Fast Ethernet, Gigabit Ethernet, or 10-Gigabit Ethernet.
Step 3	**ip access-group** *name*	Applies the default ACL.
Step 4	**ip admission** *name*	Configures web-based authentication on the specified interface.
Step 5	**exit**	Returns to configuration mode.
Step 6	**ip device tracking**	Enables the IP device tracking table.
Step 7	**end**	Returns to privileged EXEC mode.
Step 8	**show ip admission configuration**	Displays the configuration.

Configuring AAA Authentication

	Command	Purpose
Step 1	**aaa new-model**	Enables AAA functionality.
Step 2	**aaa authentication login default group** {*tacacs+* | *radius*}	Defines the list of authentication methods at login.
Step 3	**aaa authorization auth-proxy default group** {*tacacs+* | *radius*}	Creates an authorization method list for web-based authorization.
Step 4	**radius-server host** {*hostname* | *ip-address*} **test username** *username*	Specifies an AAA server. 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.
Step 5	**radius-server key** *string*	Configures the authorization and encryption key used between the switch and the RADIUS daemon running on the RADIUS server. To use multiple RADIUS servers, reenter this command for each server.

Configuring Switch-to-RADIUS-Server Communication

	Command	Purpose
Step 1	**ip radius source-interface** *interface_name*	Specifies that the RADIUS packets have the IP address of the indicated interface.
Step 2	**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 use between the switch and the RADIUS server. To use multiple RADIUS servers, reenter this command for each server.
Step 3	**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	**radius-server vsa send authentication**	Enables downloading of an ACL from the RADIUS server. This feature is supported in Cisco IOS Release 12.2(50)SG.
Step 5	**radius-server dead-criteria tries** *num-tries*	Specifies the number of unanswered sent messages to a RADIUS server before considering the server to be inactive. The range of *num-tries* is 1 to 100.

Configuring the HTTP Server

	Command	Purpose
Step 1	**ip http server**	Enables the HTTP server. The web-based authentication feature uses the HTTP server to communicate with the hosts for user authentication.
Step 2	**ip http secure-server**	Enables HTTPS.

Customizing the Authentication Proxy Web Pages

Before You Begin

You can configure web authentication to display four substitute HTML pages to the user in place of the switch 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 flash memory, then perform this task in global configuration mode:

	Command	Purpose
Step 1	**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 flash memory.
Step 2	**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	**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	**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.

Specifying a Redirection URL for Successful Login

You can specify a URL to which the user is redirected after authentication, effectively replacing the internal S*uccess* HTML page.

Command	Purpose
ip admission proxy http success redirect *url-string*	Specifies a URL for redirection of the user in place of the default login success page.

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.

	Command	Purpose
Step 1	**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	**end**	Returns to privileged EXEC mode.
Step 3	**show ip admission configuration**	Displays the authentication proxy configuration.
Step 4	**show ip admission cache**	Displays the list of authentication entries.
Step 5	**copy running-config startup-config**	(Optional) Saves your entries in the configuration file.

Configuring a Web Authentication Local Banner

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**ip admission auth-proxy-banner http** [*banner-text* | *file-path*]	Enables the local banner. (Optional) Creates a custom banner by entering *C banner-text C*, where *C* is a delimiting character or a file-path indicates a file (for example, a logo or text file) that appears in the banner.
Step 3	**end**	Returns to privileged EXEC mode.
Step 4	**copy running-config startup-config**	(Optional) Saves your entries in the configuration file.

Removing Web-Based Authentication Cache Entries

Enter a specific IP address to delete the entry for a single host. Use an asterisk to delete all cache entries.

Command	Purpose
clear ip auth-proxy cache {* | *host ip address*}	Clears authentication proxy entries from the switch.
clear ip admission cache {* | *host ip address*}	Clears IP admission cache entries from the switch.

Monitoring and Maintaining Web-Based Authentication

Command	Purpose
show authentication sessions	Displays the web-based authentication settings.
show ip admission configuration	Displays the authentication proxy configuration.
show ip admission cache	Displays the list of authentication entries.

Configuration Examples for Configuring Web-Based Authentication

Enabling and Displaying Web-Based Authentication: Examples

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
```

Enabling AAA: Example

This example shows how to enable AAA:

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

Configuring the RADIUS Server Parameters: Example

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 a Custom Authentication Proxy Web Page: Example

This example shows how to configure custom authentication proxy web pages:

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

Verifying a Custom Authentication Proxy Web Page: Example

This example shows how to verify the configuration of a custom authentication proxy web pages:

```
Switch# show ip admission configuration
Authentication proxy webpage
 Login page           : flash:login.htm
 Success page         : flash:success.htm
 Fail Page            : flash:fail.htm
 Login expired Page   : flash: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
```

Configuring a Redirection URL: Example

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

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

Verifying a Redirection URL: Example

This 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 a Local Banner: Example

This example shows how to configure a local banner with the custom message *My Switch*:

```
Switch(config) configure terminal
Switch(config)# aaa new-model
Switch(config)# aaa ip auth-proxy auth-proxy-banner C My Switch C
Switch(config) end
```

Clearing the Web-Based Authentication Session: Example

This example shows how to remove the web-based authentication session for the client at the IP address 209.165.201.1:

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

Additional References

The following sections provide references related to switch administration:

Related Documents

Related Topic	Document Title
Cisco IE 2000 commands	*Cisco IE 2000 Switch Command Reference*, Release 15.0(2)EC
Cisco IOS basic commands	*Cisco IOS Configuration Fundamentals Command Reference*
Authentication proxy commands Radius server commands	*Cisco IOS Security Command Reference*
Authentication proxy configuration Radius server configuration	*Cisco IOS Security Configuration Guide*

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

MIBs	MIBs Link
—	To locate and download MIBs using Cisco IOS XR software, use the Cisco MIB Locator found at the following URL and choose a platform under the Cisco Access Products menu: http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

RFCs

RFCs	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	—

Technical Assistance

Description	Link
The Cisco Technical Support website contains thousands of 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.	http://www.cisco.com/techsupport