



# CHAPTER 11

## Configuring Web-Based Authentication

---

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

- [Understanding Web-Based Authentication, page 11-1](#)
- [Configuring Web-Based Authentication, page 11-9](#)
- [Displaying Web-Based Authentication Status, page 11-17](#)



### Note

For complete syntax and usage information for the switch commands used in this chapter, refer to the command reference for this release.

---

## Understanding 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 and Layer 3 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 11-2](#)
- [Session Creation, page 11-3](#)
- [Authentication Process, page 11-3](#)

- [Web Authentication Customizable Web Pages, page 11-6](#)
- [Web-based Authentication Interactions with Other Features, page 11-7](#)

## 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](#) shows the roles of these devices in a network:

**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, 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.

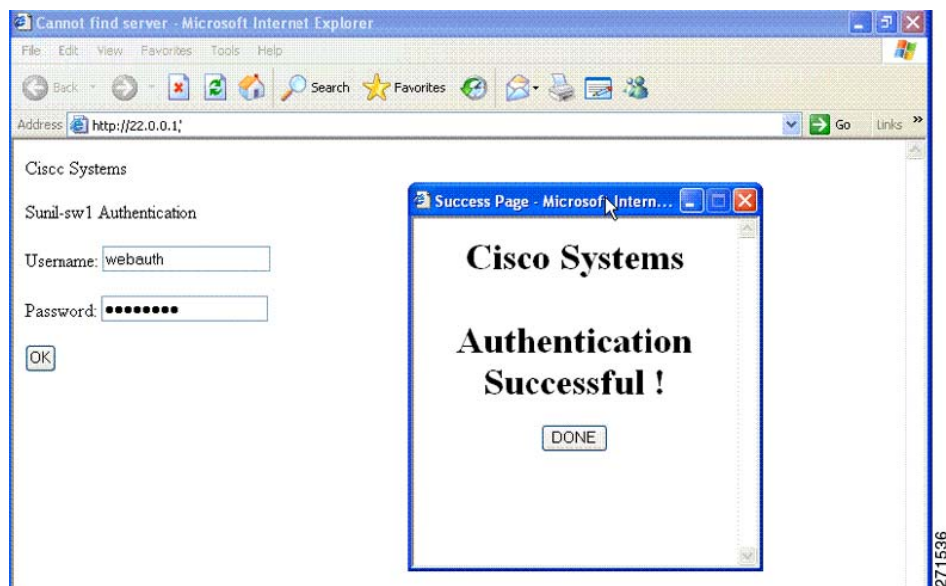
## Local Web Authentication Banner

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*

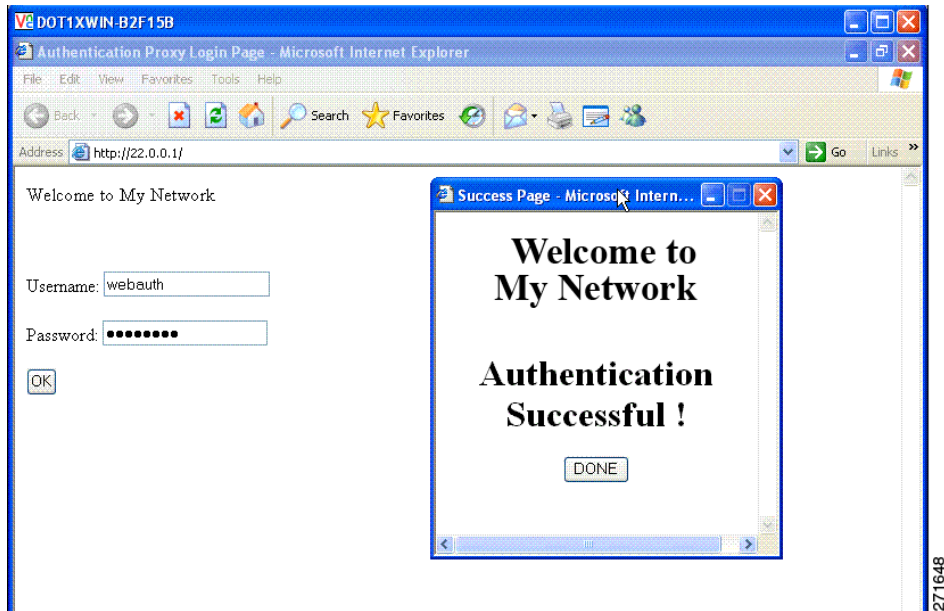
You create a banner by using the **ip admission auth-proxy-banner http** global configuration command. The default banner *Cisco Systems* and *Switch host-name Authentication* appear on the Login Page. *Cisco Systems* appears on the authentication result pop-up page, as shown in [Figure 11-2](#).

**Figure 11-2** Authentication Successful Banner

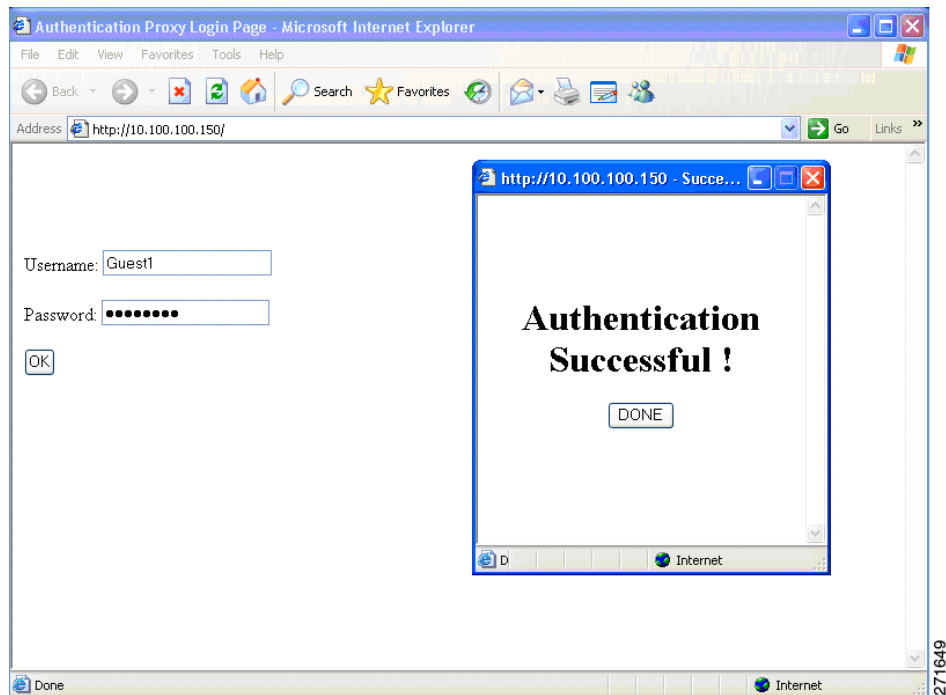


You can also customize the banner, as shown in [Figure 11-3](#).

- 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 11-16.

## 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.

### 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* 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 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 file name.
- The configured authentication proxy feature supports both HTTP and SSL.

You can substitute your HTML pages, as shown in [Figure 11-5 on page 11-7](#), 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** Customizable Authentication Page

**CISCO**

Customized login page

This internet web site is provided as a public service. It is intended for use by the public for viewing and retrieving information only. Unless otherwise indicated, all information on this site is considered public information and may be copied or distributed.

Visitors should know that use of this site is collected for analytical and statistical purposes, such as assessing what information is of most and least interest, determining technical design specifications, and identifying system performance or problem areas. For site security purposes and to ensure that this service remains available to all users, this system employs software programs to monitor network traffic to identify unauthorized attempts to upload or change information, or otherwise cause damage. data logs will only be used to identify individual users and their usage habits for authorized law enforcement investigations or national security purposes. These logs are scheduled for regular destruction in accordance with Company Guidelines.

Neither the Government nor any agency thereof, nor any of their employees, nor any of their contractors, subcontractors, nor their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. The appearance of hyperlinks does not constitute endorsement by the Government of the website or the information, products, or services contained therein. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the Government or any agency, contractor, or subcontractor thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the Government or any agency, contractor or subcontractor thereof.

**TestCenter**

Username:

Password:

206603

For more information, see the [“Customizing the Authentication Proxy Web Pages”](#) section on page 11-13.

## Web-based Authentication Interactions with Other Features

- [Port Security, page 11-7](#)
- [LAN Port IP, page 11-8](#)
- [Gateway IP, page 11-8](#)
- [ACLs, page 11-8](#)
- [Context-Based Access Control, page 11-8](#)
- [802.1x Authentication, page 11-8](#)
- [EtherChannel, page 11-8](#)

### 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 25-9.

## 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.

# Configuring Web-Based Authentication

- [Default Web-Based Authentication Configuration, page 11-9](#)
- [Web-Based Authentication Configuration Guidelines and Restrictions, page 11-9](#)
- [Web-Based Authentication Configuration Task List, page 11-10](#)
- [Configuring the Authentication Rule and Interfaces, page 11-10](#)
- [Configuring AAA Authentication, page 11-11](#)
- [Configuring Switch-to-RADIUS-Server Communication, page 11-11](#)
- [Configuring the HTTP Server, page 11-13](#)
- [Configuring the Web-Based Authentication Parameters, page 11-15](#)
- [Removing Web-Based Authentication Cache Entries, page 11-16](#)

## Default Web-Based Authentication Configuration

Table 11-1 shows the default web-based authentication configuration.

**Table 11-1**      **Default Web-based Authentication Configuration**

| Feature                             | Default Setting  |
|-------------------------------------|------------------|
| AAA                                 | Disabled         |
| RADIUS server                       |                  |
| • IP address                        | • None specified |
| • UDP authentication port           | • 1812           |
| • Key                               | • None specified |
| Default value of inactivity timeout | 3600 seconds     |
| Inactivity timeout                  | Enabled          |

## Web-Based Authentication Configuration Guidelines and Restrictions

- 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.
- 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.
- 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.

- 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 Configuration Task List

- [Configuring the Authentication Rule and Interfaces, page 11-10](#)
- [Configuring AAA Authentication, page 11-11](#)
- [Configuring Switch-to-RADIUS-Server Communication, page 11-11](#)
- [Configuring the HTTP Server, page 11-13](#)
- [Configuring an AAA Fail Policy, page 11-15](#)
- [Configuring the Web-Based Authentication Parameters, page 11-15](#)
- [Removing Web-Based Authentication Cache Entries, page 11-16](#)

## Configuring the Authentication Rule and Interfaces

|        | Command                                                | Purpose                                                                                                                                                                                                            |
|--------|--------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>ip admission name</b> <i>name</i> <b>proxy http</b> | Configure an authentication rule for web-based authorization.                                                                                                                                                      |
| Step 2 | <b>interface</b> <i>type slot/port</i>                 | Enter interface configuration mode and specifies the ingress Layer 2 or Layer 3 interface to be enabled for web-based authentication.<br><i>type</i> can be fastethernet, gigabit ethernet, or tengigabitethernet. |
| Step 3 | <b>ip access-group</b> <i>name</i>                     | Apply the default ACL.                                                                                                                                                                                             |
| Step 4 | <b>ip admission</b> <i>name</i>                        | Configures web-based authentication on the specified interface.                                                                                                                                                    |
| Step 5 | <b>exit</b>                                            | Return to configuration mode.                                                                                                                                                                                      |
| Step 6 | <b>ip device tracking</b>                              | Enables the IP device tracking table.                                                                                                                                                                              |
| Step 7 | <b>end</b>                                             | Return to privileged EXEC mode.                                                                                                                                                                                    |
| Step 8 | <b>show ip admission configuration</b>                 | Display the configuration.                                                                                                                                                                                         |
| Step 9 | <b>copy running-config startup-config</b>              | (Optional) Save your entries in the configuration file.                                                                                                                                                            |

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

|        | Command                                                                       | Purpose                                                                                                                                       |
|--------|-------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>aaa new-model</b>                                                          | Enables AAA functionality.                                                                                                                    |
| Step 2 | <b>aaa authentication login default group</b> { <i>tacacs+   radius</i> }     | Defines the list of authentication methods at login.                                                                                          |
| Step 3 | <b>aaa authorization auth-proxy default group</b> { <i>tacacs+   radius</i> } | Create an authorization method list for web-based authorization.                                                                              |
| Step 4 | <b>tacacs-server host</b> { <i>hostname   ip_address</i> }                    | Specify an AAA server. For RADIUS servers, see the <a href="#">“Configuring Switch-to-RADIUS-Server Communication”</a> section on page 11-11. |
| Step 5 | <b>tacacs-server key</b> { <i>key-data</i> }                                  | Configure the authorization and encryption key used between the switch and the TACACS server.                                                 |
| Step 6 | <b>copy running-config startup-config</b>                                     | (Optional) Save your entries in the configuration file.                                                                                       |

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 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.

To configure the RADIUS server parameters, perform this task:

|        | Command                                                                                                          | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|--------|------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>ip radius source-interface</b> <i>interface_name</i>                                                          | Specify that the RADIUS packets have the IP address of the indicated interface.                                                                                                                                                                                                                                                                                                                                                                                   |
| Step 2 | <b>radius-server host</b> { <i>hostname</i>   <i>ip-address</i> } <b>test</b><br><b>username</b> <i>username</i> | Specify the host name or IP address of the remote RADIUS server.<br><br>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.<br><br>The <b>key</b> option specifies an authentication and encryption key to use between the switch and the RADIUS server.<br><br>To use multiple RADIUS servers, reenter this command for each server. |
| Step 3 | <b>radius-server key</b> <i>string</i>                                                                           | Configure the authorization and encryption key used between the switch and the RADIUS daemon running on the RADIUS server.                                                                                                                                                                                                                                                                                                                                        |
| Step 4 | <b>radius-server vsa send authentication</b>                                                                     | Enable downloading of an ACL from the RADIUS server. This feature is supported in Cisco IOS Release 12.2(50)SG.                                                                                                                                                                                                                                                                                                                                                   |
| Step 5 | <b>radius-server dead-criteria tries</b> <i>num-tries</i>                                                        | Specify the number of unanswered sent messages to a RADIUS server before considering the server to be inactive. The range of <i>num-tries</i> is 1 to 100.                                                                                                                                                                                                                                                                                                        |

When you configure the RADIUS server parameters:

- 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 by using 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* and the *Cisco IOS Security Command Reference, Release 12.2*:  
[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)

**Note**

You need to configure some settings on the RADIUS server, including: the switch IP address, the key string to be shared by both the server and the switch, and the downloadable ACL (DACL). 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.

|        | Command                      | Purpose                                                                                                                                  |
|--------|------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>ip http server</b>        | Enable the HTTP server. The web-based authentication feature uses the HTTP server to communicate with the hosts for user authentication. |
| Step 2 | <b>ip http secure-server</b> | Enable HTTPS.                                                                                                                            |

You can configure custom authentication proxy web pages or specify a redirection URL for successful login.

**Note**

To ensure secure authentication when you enter the **ip http secure-server** command, the login page is always in HTTPS (secure HTTP) even if the user sends an HTTP request.

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

## Customizing the Authentication Proxy Web Pages

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 | <b>ip admission proxy http login page file</b><br><i>device:login-filename</i>     | Specify the location in the switch memory file system of the custom HTML file to use in place of the default login page. The <i>device:</i> is flash memory. |
| Step 2 | <b>ip admission proxy http success page file</b><br><i>device:success-filename</i> | Specify the location of the custom HTML file to use in place of the default login success page.                                                              |

|        | Command                                                                                  | Purpose                                                                                         |
|--------|------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------|
| Step 3 | <b>ip admission proxy http failure page file</b><br><i>device:fail-filename</i>          | Specify the location of the custom HTML file to use in place of the default login failure page. |
| Step 4 | <b>ip admission proxy http login expired page file</b><br><i>device:expired-filename</i> | Specify the location of the custom HTML file to use in place of the default login expired page. |

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.

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
```

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
```

## Specifying a Redirection URL for Successful Login

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

| Command                                                           | Purpose                                                                               |
|-------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| <b>ip admission proxy http success redirect</b> <i>url-string</i> | Specify a URL for redirection of the user in place of the default login success page. |

When configuring a redirection URL for successful login, consider these 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.

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

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

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 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                                                                                                   |
|---------------|------------------------------------------------------|-----------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | <b>ip admission max-login-attempts</b> <i>number</i> | Set the maximum number of failed login attempts. The range is 1 to 2147483647 attempts. The default is 5. |
| <b>Step 2</b> | <b>end</b>                                           | Returns to privileged EXEC mode.                                                                          |
| <b>Step 3</b> | <b>show ip admission configuration</b>               | Display the authentication proxy configuration.                                                           |
| <b>Step 4</b> | <b>show ip admission cache</b>                       | Display the list of authentication entries.                                                               |
| <b>Step 5</b> | <b>copy running-config startup-config</b>            | (Optional) Save your entries in the configuration file.                                                   |

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

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

## Configuring a Web Authentication Local Banner

Beginning in privileged EXEC mode, follow these steps to configure a local banner on a switch that has web authentication configured.

|        | Command                                                                                 | Purpose                                                                                                                                                                                                                                        |
|--------|-----------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>configure terminal</b>                                                               | Enter global configuration mode.                                                                                                                                                                                                               |
| Step 2 | <b>ip admission auth-proxy-banner http</b><br>[ <i>banner-text</i>   <i>file-path</i> ] | Enable the local banner.<br><br>(Optional) Create a custom banner by entering <i>C banner-text C</i> , where <i>C</i> 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 | <b>end</b>                                                                              | Return to privileged EXEC mode.                                                                                                                                                                                                                |
| Step 4 | <b>copy running-config startup-config</b>                                               | (Optional) Save your entries in the configuration file.                                                                                                                                                                                        |

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
```

For more information about the **ip auth-proxy auth-proxy-banner** command, see the “Authentication Proxy Commands” section of the [Cisco IOS Security Command Reference](#) on Cisco.com.

## Removing Web-Based Authentication Cache Entries

| Command                                                         | Purpose                                                                                                                                              |
|-----------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>clear ip auth-proxy cache</b> { *   <i>host ip address</i> } | Delete authentication proxy entries. Use an asterisk to delete all cache entries. Enter a specific IP address to delete the entry for a single host. |
| <b>clear ip admission cache</b> { *   <i>host ip address</i> }  | Delete 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 the IP address 209.165.201.1:

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

# Displaying Web-Based Authentication Status

Perform this task to display the web-based authentication settings for all interfaces or for specific ports:

|        | Command                                                                           | Purpose                                                                                                                                                                                                                                          |
|--------|-----------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>show authentication sessions</b><br>[ <b>interface</b> <i>type slot/port</i> ] | Displays the web-based authentication settings.<br><br>type = fastethernet, gigabitethernet, or tengigabitethernet<br><br>(Optional) Use the <b>interface</b> 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 gigabit interface 3/27:

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

