Configuring Web-Based Authentication

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

- Finding Feature Information, on page 1
- Information About Web-Based Authentication, on page 1
- How to Configure Web-Based Authentication, on page 10
- Monitoring Web-Based Authentication Status, on page 34
- Feature Information for Web-Based Authentication, on page 35

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

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.

Information About 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.

Note HTTPS traffic interception for central web authentication redirect is not supported.

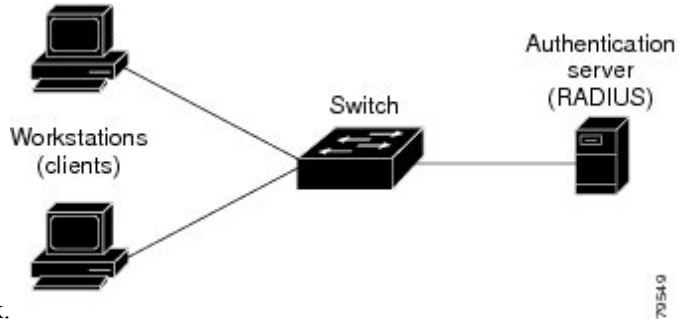
Device Roles

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 1: Web-Based Authentication Device Roles

This figure shows the roles of these devices in a network.



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.
- 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

With Web Authentication, you can create a default and customized web-browser banners that appears when you log in to a switch.

The banner appears on both the login page and the authentication-result pop-up pages. The default banner messages are as follows:

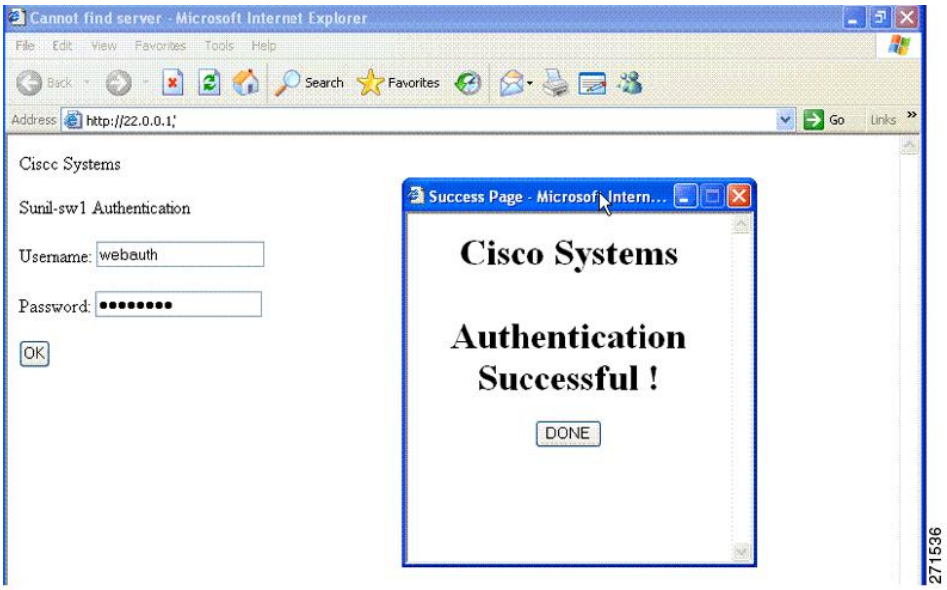
- *Authentication Successful*
- *Authentication Failed*
- *Authentication Expired*

The Local Web Authentication Banner can be configured in legacy and new-style (Session-aware) CLIs as follows:

- Legacy mode—Use the **ip admission auth-proxy-banner http** global configuration command.
- New-style mode—Use the **parameter-map type webauth global banner**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.

Figure 2: Authentication Successful Banner

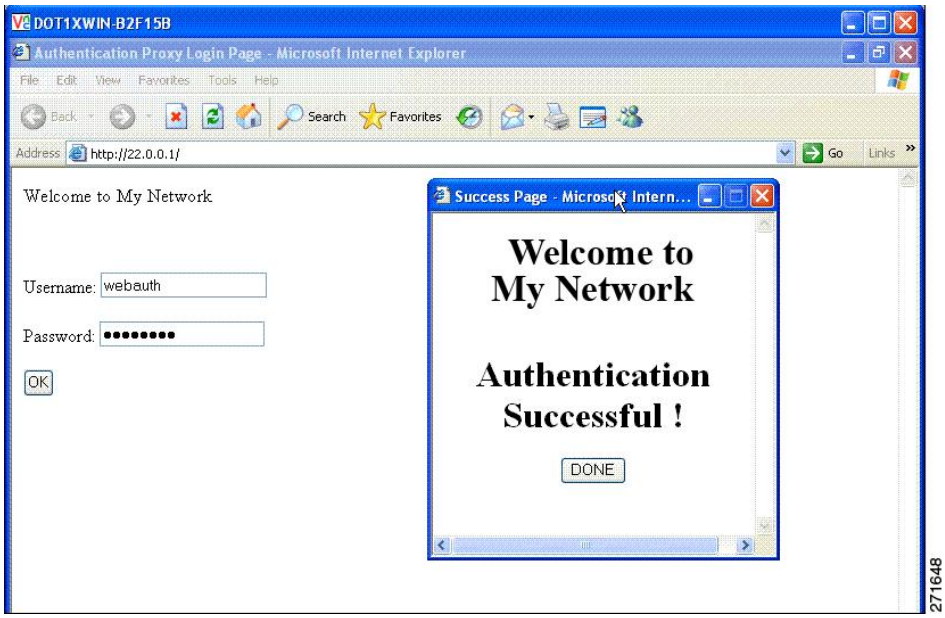


The banner can be customized as follows:

- Add a message, such as switch, router, or company name to the banner:
  - Legacy mode—Use the **ip admission auth-proxy-banner http** *banner-text*global configuration command.
  - New-style mode—Use the **parameter-map type webauth global banner**global configuration command
- Add a logo or text file to the banner :

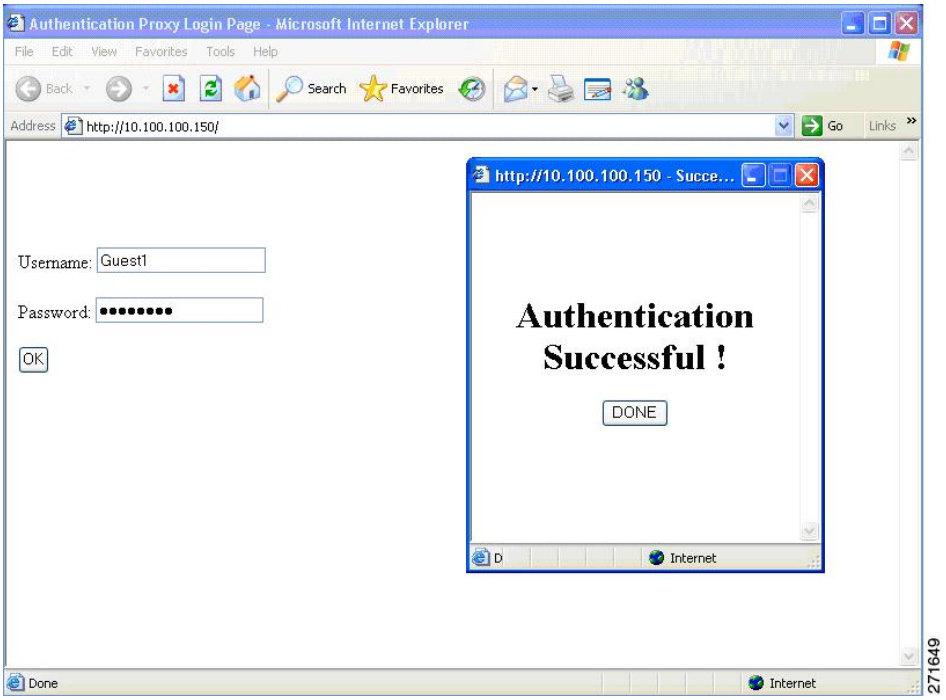
- Legacy mode—Use the **ip admission auth-proxy-banner http** *file-path* global configuration command.
- New-style mode—Use the **parameter-map type webauth global banner** global configuration command

Figure 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.

Figure 4: Login Screen With No Banner



For more information, see the *Session Aware Networking Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches) Session Aware Networking Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)* and the *Web Authentication Enhancements - Customizing Authentication Proxy Web Pages*.

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.

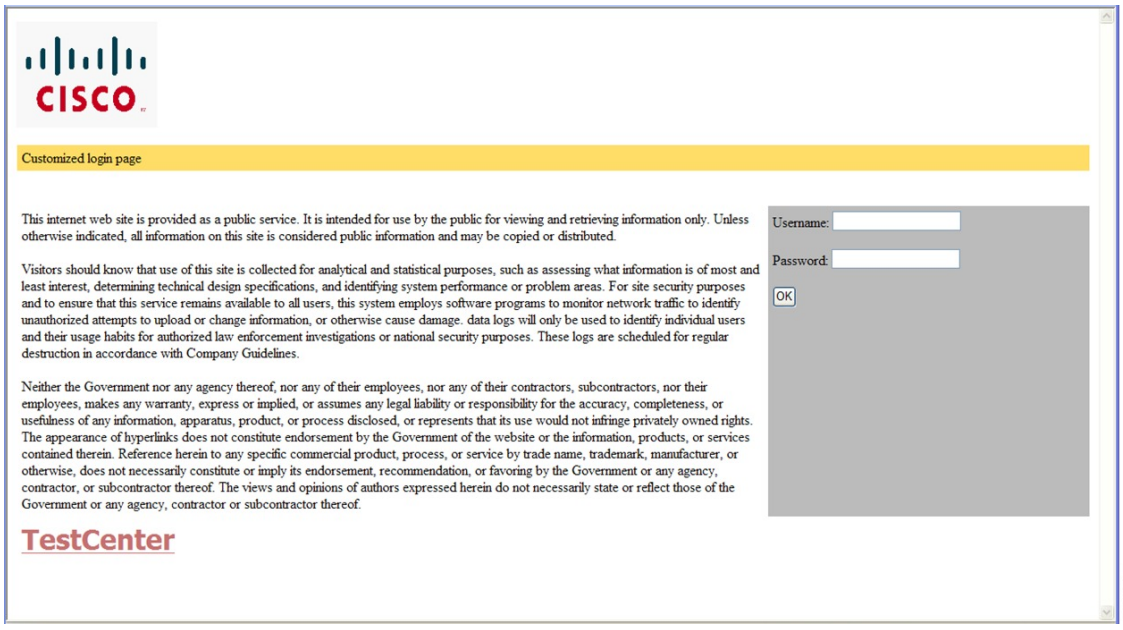
Guidelines

- 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.
- On stackable switches, 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 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 5: Customizable Authentication Page



Authentication Proxy Web Page Guidelines

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.

Related Topics

Customizing the Authentication Proxy Web Pages, on page 18

Redirection URL for Successful Login Guidelines

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.
- If the redirection URL is required after the web-based authentication client is successfully authenticated, then the URL string must start with a valid URL (for example, http://) followed by the URL information. If only the URL is given without http://, then the redirection URL on successful authentication might cause page not found or similar errors on a web browser.

Related Topics

Specifying a Redirection URL for Successful Login, on page 20

Custom Web Authentication Guidelines

- You cannot specify a directory path of a file when downloading a tar bundle from the controller GUI. The tar file is stored in the default flash path.
- You can provide any image name for web authentication and the image name need not be **webauth**.

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.

Related Topics

Enabling and 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 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, it is more secure, though not required, to 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. The Policy ACL is applied to the session even if there is no ACL configured on the port.

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.

EtherChannel

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

How to Configure Web-Based Authentication

Default Web-Based Authentication Configuration

The following table shows the default web-based authentication configuration.

Table 1: Default Web-based Authentication Configuration

Feature	Default Setting
AAA	Disabled
RADIUS server • IP address • UDP authentication port • Key	• None specified • 1645 • 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 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 supports IPv6 in Session-aware policy mode. IPv6 Web-authentication requires at least one IPv6 address configured on the switch and IPv6 Snooping configured on the switchport.
- 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 NRH (Non-Responsive Host) is not supported for voice devices.
- Only the Password Authentication Protocol (PAP) is supported for web-based RADIUS authentication on controllers. The Challenge Handshake Authentication Protocol (CHAP) is not supported for web-based RADIUS authentication on controllers.
- Identify the following RADIUS security server settings that will be used while configuring switch-to-RADIUS-server communication:
  - 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.
- 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 transmit, and the radius-server key global configuration commands. For more information, see the *Cisco IOS Security Configuration Guide*, Release 12.4 and the *Cisco IOS Security Command Reference*, Release 12.4.

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.

Web-Based Authentication Configuration Task List

Configuring the Authentication Rule and Interfaces

Examples in this section are legacy-style configurations. For new-style configurations, see the *Session Aware Networking Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)*

Follow these steps to configure the authentication rule and interfaces:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip admission name** *name* **proxy http**
4. **interface** *type slot/port*
5. **ip access-group** *name*
6. **ip admission** *name*
7. **exit**
8. **ip device tracking**
9. **end**
10. **show ip admission status**
11. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**ip admission name** *name* **proxy http** **Example:** `Switch(config)# ip admission name webauth1 proxy http`	Configures an authentication rule for web-based authorization.

	Command or Action	Purpose
Step 4	**interface** *type slot/port* **Example:** `Switch(config)# interface gigabitEthernet1/0/1`	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 5	**ip access-group** *name* **Example:** `Switch(config-if)# ip access-group webauthag`	Applies the default ACL.
Step 6	**ip admission** *name* **Example:** `Switch(config-if)# ip admission webauth1`	Configures web-based authentication on the specified interface.
Step 7	**exit** **Example:** `Switch(config-if)# exit`	Returns to configuration mode.
Step 8	**ip device tracking** **Example:** `Switch(config)# ip device tracking`	Enables the IP device tracking table.
Step 9	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.
Step 10	**show ip admission status** **Example:** `Switch# show ip admission status`	Displays the configuration.
Step 11	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Configuring AAA Authentication

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa authentication login default group** {**tacacs+** | **radius**}
5. **aaa authorization auth-proxy default group** {**tacacs+** | **radius**}
6. **tacacs server** *server-name*
7. **address** {**ipv4** | **ipv6**} *ip address*
8. **key** *string*
9. **exit**
10. **end**
11. **show running-config**
12. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**aaa new-model** **Example:** `Switch(config)# aaa new-model`	Enables AAA functionality.
Step 4	**aaa authentication login default group** {**tacacs+** | **radius**} **Example:** `Switch(config)# aaa authentication login default group tacacs+`	Defines the list of authentication methods at login. **named_authentication_list** refers to any name that is not greater than 31 characters. **AAA_group_name** refers to the server group name. You need to define the server-group **server_name** at the beginning itself.

	Command or Action	Purpose
Step 5	**aaa authorization auth-proxy default group** {**tacacs+** | **radius**} **Example:** `Switch(config)# aaa authorization auth-proxy default group tacacs+`	Creates an authorization method list for web-based authorization.
Step 6	**tacacs server** *server-name* **Example:** `Switch(config)# tacacs server yourserver`	Specifies an AAA server.
Step 7	**address** {**ipv4** | **ipv6**} *ip address* **Example:** `Switch(config-server-tacacs)# address ipv4 10.0.1.12`	Configures the IP address for the TACACS server.
Step 8	**key** *string* **Example:** `Switch(config-server-tacacs)# key cisco123`	Configures the authorization and encryption key used between the switch and the TACACS server.
Step 9	**exit** **Example:** `Switch(config-server-tacacs)# exit`	Exits the TACACS server mode and enters the global configuration mode.
Step 10	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.
Step 11	**show running-config** **Example:** `Switch# show running-config`	Verifies your entries.
Step 12	**copy running-config startup-config** **Example:**	(Optional) Saves your entries in the configuration file.

	Command or Action	Purpose
	`Switch# copy running-config startup-config`	

Configuring Switch-to-RADIUS-Server Communication

Follow these steps to configure the RADIUS server parameters:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip radius source-interface vlan** *vlan interface number*
4. **radius server** *server name*
5. **address** {**ipv4** | **ipv6**} *ip address*
6. **key** *string*
7. **exit**
8. **radius-server dead-criteria tries** *num-tries*
9. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**ip radius source-interface vlan** *vlan interface number* **Example:** `Switch(config)# ip radius source-interface vlan 80`	Specifies that the RADIUS packets have the IP address of the indicated interface.
Step 4	**radius server** *server name* **Example:** `Switch(config)# radius server rsim address ipv4`	(Optional) Specifies the IP address of the RADIUS server.

	Command or Action	Purpose
	`124.2.2.12`	
Step 5	**address** {**ipv4** | **ipv6**} *ip address* **Example:** `Switch(config-radius-server)# address ipv4 10.0.1.2 auth-port 1550 acct-port 1560`	Configures the IP address for the RADIUS server.
Step 6	**key** *string* **Example:** `Switch(config-radius-server)# key rad123`	(Optional) Specifies the authentication and encryption key used between the switch and the RADIUS daemon running on the RADIUS server.
Step 7	**exit** **Example:** `Switch(config-radius-server)# exit`	Exits the RADIUS server mode and enters the global configuration mode.
Step 8	**radius-server dead-criteria tries** *num-tries* **Example:** `Switch(config)# radius-server dead-criteria tries 30`	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.
Step 9	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.

Related Topics

Switch-to-RADIUS-Server Communication

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.

Note The Apple psuedo-browser will not open if you configure only the **ip http secure-server** command. You should also configure the **ip http server** command.

Follow these steps to enable the server for either HTTP or HTTPS:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip http server**
4. **ip http secure-server**
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**ip http server** **Example:** `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.
Step 4	**ip http secure-server** **Example:** `Switch(config)# ip http secure-server`	Enables 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.
Step 5	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.

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.

For the equivalent Session Aware Networking configuration example for this feature, see the section "Configuring a Parameter Map for Web-Based Authentication" in the chapter, "Configuring Identity Control Policies." of the book, "*Session Aware Networking Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)*."

Follow these steps to specify the use of your custom authentication proxy web pages:

Before you begin

Store your custom HTML files on the Switch flash memory.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip admission proxy http login page file** *device:login-filename*
4. **ip admission proxy http success page file** *device:success-filename*
5. **ip admission proxy http failure page file** *device:fail-filename*
6. **ip admission proxy http login expired page file** *device:expired-filename*
7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**ip admission proxy http login page file** *device:login-filename* **Example:** `Switch(config)# ip admission proxy http login page file disk1:login.htm`	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 4	**ip admission proxy http success page file** *device:success-filename* **Example:** `Switch(config)# ip admission proxy http success page file disk1:success.htm`	Specifies the location of the custom HTML file to use in place of the default login success page.

	Command or Action	Purpose
Step 5	**ip admission proxy http failure page file** *device:fail-filename* **Example:** `Switch(config)# ip admission proxy http fail page file disk1:fail.htm`	Specifies the location of the custom HTML file to use in place of the default login failure page.
Step 6	**ip admission proxy http login expired page file** *device:expired-filename* **Example:** `Switch(config)# ip admission proxy http login expired page file disk1:expired.htm`	Specifies the location of the custom HTML file to use in place of the default login expired page.
Step 7	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.

Related Topics

Authentication Proxy Web Page Guidelines, on page 8

Specifying a Redirection URL for Successful Login

Follow these steps to specify a URL to which the user is redirected after authentication, effectively replacing the internal Success HTML page:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip admission proxy http success redirect** *url-string*
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:**	Enters the global configuration mode.

	Command or Action	Purpose
	`Switch# configure terminal`	
Step 3	**ip admission proxy http success redirect** *url-string* **Example:** `Switch(config)# ip admission proxy http success redirect www.example.com`	Specifies a URL for redirection of the user in place of the default login success page.
Step 4	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.

Related Topics

Redirection URL for Successful Login Guidelines, on page 8

Configuring the Web-Based Authentication Parameters

Follow these steps to configure the maximum number of failed login attempts before the client is placed in a watch list for a waiting period:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip admission max-login-attempts** *number*
4. **end**
5. **show running-config**
6. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.

	Command or Action	Purpose
Step 3	**ip admission max-login-attempts** *number* **Example:** `Switch(config)# ip admission max-login-attempts 10`	Sets the maximum number of failed login attempts. The range is 1 to 2147483647 attempts. The default is 5.
Step 4	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.
Step 5	**show running-config** **Example:** `Switch# show running-config`	Verifies your entries.
Step 6	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Configuring a Web Authentication Local Banner

Follow these steps to configure a local banner on a switch that has web authentication configured.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip admission auth-proxy-banner http** [*banner-text* | *file-path*]
4. **end**
5. **show running-config**
6. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**ip admission auth-proxy-banner http** [*banner-text* | *file-path*] **Example:** `Switch(config)# ip admission auth-proxy-banner http C My Switch C`	Enables the local banner. (Optional) Create a custom banner by entering *C banner-text C* (where *C* is a delimiting character), or *file-path* that indicates a file (for example, a logo or text file) that appears in the banner.
Step 4	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.
Step 5	**show running-config** **Example:** `Switch# show running-config`	Verifies your entries.
Step 6	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Configuring Web-Based Authentication without SVI

You configure the web-based authentication without SVI feature to redirect the HTML login page to the client without creating an IP address in the routing table. These steps are optional.

You configure the web-based authentication without SVI feature to redirect the HTML login page to the client. This is done without creating an IP address in the SVI interface which then would be applied to the WebAuth enabled interface. These steps are optional.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **parameter-map type webauth global**
4. **l2-webauth-enabled**
5. **end**

6. **show running-config**
7. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**parameter-map type webauth global** **Example:** `Switch (config)# parameter-map type webauth global`	Creates a parameter map and enters parameter-map webauth configuration mode. The specific configuration commands supported for a global parameter map defined with the global keyword differ from the commands supported for a named parameter map defined with the parameter-map-name argument.
Step 4	**l2-webauth-enabled** **Example:** `Switch (config-params-parameter-map)# l2-webauth-enabled`	Enables the web-based authentication without SVI feature
Step 5	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.
Step 6	**show running-config** **Example:** `Switch# show running-config`	Verifies your entries.
Step 7	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Configuring Web-Based Authentication with VRF Aware

You configure the web-based authentication with VRF aware to redirect the HTML login page to the client. These steps are optional.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **parameter-map type webauth global**
4. **webauth-vrf-aware**
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**parameter-map type webauth global** **Example:** `Switch (config)# parameter-map type webauth global`	Creates a parameter map and enters parameter-map webauth configuration mode. The specific configuration commands supported for a global parameter map defined with the global keyword differ from the commands supported for a named parameter map defined with the parameter-map-name argument.
Step 4	**webauth-vrf-aware** **Example:** `Switch (config-params-parameter-map)# webauth-vrf-aware`	Enables the web-based authentication VRF aware feature on SVI.
Step 5	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.

	Command or Action	Purpose
Step 6	**show running-config** **Example:** `Switch# show running-config`	Verifies your entries.
Step 7	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Removing Web-Based Authentication Cache Entries

Follow these steps to remove web-based authentication cache entries:

SUMMARY STEPS

1. **enable**
2. **clear ip auth-proxy cache** {* | *host ip address*}
3. **clear ip admission cache** {* | *host ip address*}

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**clear ip auth-proxy cache** {*	*host ip address*} **Example:** `Switch# clear ip auth-proxy cache 192.168.4.5`	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.
Step 3	**clear ip admission cache** {*	*host ip address*} **Example:** `Switch# clear ip admission cache 192.168.4.5`	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.

Downloading Web Authentication Tar Bundle (CLI)

You can download a tar bundle (.tar) containing all personalized files from the FTP or TFTP server.

SUMMARY STEPS

1. **archive tar /xtract <transfer mode> ://<IP> /<location>/<login filename> < DIRECTORY>**
2. **archive tar /xtract <transfer mode> ://<IP> /<location>/<login filename> < DIRECTORY> flash-1:**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**archive tar /xtract <transfer mode> ://<IP> /<location>/<login filename> < DIRECTORY>**
	Example:
	`Switch# archive tar /xtract tftp://9.1.0.100/user1/login.tar  flash2`
	`Switch# show flash:`
	`59  4096 Jan 08 2014 13:19:33.0000000000 +00:00 flash`
	`60  2574 Jan 08 2014 13:19:51.0000000000 +00:00 flash2/aup.html`
	`61  4082 Jan 08 2014 13:19:51.0000000000 +00:00 flash2/login.html`
	`62  70123 Jan 08 2014 13:19:52.0000000000 +00:00 flash2/yourlogo.jpg`
	`63  344 Jan 08 2014 13:19:51.0000000000 +00:00 flash2/failed.html`
	`64  1653 Jan 08 2014 13:19:52.0000000000 +00:00 flash2/logout.html`
	`64  1653 Jan 08 2014 13:19:52.0000000000 +00:00 flash2/expired.html`
		Specifies to download a tar bundle (.tar) from the FTP or TFTP server.

Step 2	**archive tar /xtract <transfer mode> ://<IP> /<location>/<login filename> < DIRECTORY> flash-1:**
	Example:
	`Switch# archive tar /xtract tftp://10.20.10.10/asd/login.tar abc flash-1:`
	`Switch# show flash-1:`
	`29  4096 Jan 09 2014 17:08:49.0000000000 +00:00`
	`30  2574 Jan 09 2014 17:08:49.0000000000 +00:00 aup.html`
	`31  344 Jan 09 2014 17:08:49.0000000000 +00:00 abc/failed.html`
	`32  4082 Jan 09 2014 17:08:49.0000000000 +00:00 alogin.html`
	`33  1653 Jan 09 2014 17:08:49.0000000000 +00:00 logout.html`
	`34  70123 Jan 09 2014 17:08:49.0000000000 +00:00 yourlogo.jpg`
		Specifies to download a tar bundle (.tar) from the FTP or TFTP server in high availability environment.

Downloading Web Authentication Tar Bundle (GUI)

Step 1 Choose **Configuration** > **Commands** > **Download File** to open the Download File to Controller page.

Step 2 From the **File Type** drop-down list, choose Webauth Bundle.

Step 3 From the **Transfer Mode** drop-down list, choose from the following options:

- **TFTP**
- **FTP**

Step 4 In the**IP Address** text box, enter the IP address of the server.

Step 5 In the**File Path** text box, enter the directory path of the software.

Step 6 In the**File Name** text box, enter the name of the controller software file (**filename.aes**).

Integrating Customized Web Authentication Pages into a Parameter Map (CLI)

You can configure the personalized pages into a parameter map. Using the parameter map, you can configure all the personalized pages in one shot. This minimizes the need of configuring all the four custom pages separately. Even if you want to configure only some pages, the others pages use the defaults.

SUMMARY STEPS

1. **configure terminal**
2. **parameter-map type webauth** *name* **type** *webauth*
3. **custom-page login device flash:flash2/login.html**
4. **custom-page success device flash: flash2/logout.html**
5. **custom-page failure device flash: flash2/failed.html**
6. **custom-page login expired device flash: flash2/expired.html**
7. **end**
8. **show parameter-map type webauth name** *name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**parameter-map type webauth** *name* **type** *webauth* **Example:** `Switch(config)# parameter-map type webauth WEB type webauth`	Creates a parameter map.
Step 3	**custom-page login device flash:flash2/login.html** **Example:** `Switch(config-params-parameter-map)# custom-page login device flash:flash2/login.html`	Configures the personalized pages into a parameter map.
Step 4	**custom-page success device flash: flash2/logout.html** **Example:**	Configures the personalized pages into a parameter map.

	Command or Action	Purpose
	`Switch(config-params-parameter-map)# custom-page success device flash: flash2/logout.html`	
Step 5	**custom-page failure device flash: flash2/failed.html** **Example:** `Switch(config-params-parameter-map)# custom-page failure device flash: flash2/failed.html`	Configures the personalized pages into a parameter map.
Step 6	**custom-page login expired device flash: flash2/expired.html** **Example:** `Switch(config-params-parameter-map)# custom-page login expired device flash: flash2/expired.html`	Configures the personalized pages into a parameter map.
Step 7	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Step 8	**show parameter-map type webauth name** *name*
	Example:
	`Switch# show parameter-map type webauth name WEB`
	`Parameter Map Name : WEB`
	`Type : webauth`
	`Custom Page:`
	`Auth-proxy login : flash: flash2/login.html`
	`Auth-proxy Init State time : 120 sec`
	`Auth-proxy Fin Wait time : 3000 milliseconds`
	`Webauth max-http connection : 30`
	`Webauth logout-window : Enabled`
	`Consent Email : Disabled`
		Configures the personalized pages into a parameter map.

Linking Image in Custom Pages

In custom pages, you can also send back images.

In releases earlier to software release 3E, the custom page had to contain the link to the image as an entire path, in the form of: **<img src="http://<ip-addresss>/flash:web_auth_image.jpg" alt="name">**. The IP address is the management IP address of the controller.

SUMMARY STEPS

1. **<img src="./flash:web_auth_image.jpg" alt="name”>**
2. **<img src="./flash:web_auth_image.jpg" alt="name”>**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**<img src="./flash:web_auth_image.jpg" alt="name”>** **Example:** `Switch# <img src="./flash:web_auth_image.jpg" alt="name”>`	Specifies to link image to the custom page. The virtual IP address is automatically used as a source. The logical link implies that you define the virtual IP address in the global parameter map. **Note** You can still define the image full path (with controller IP address). In such case, the IP address is either the management IP or the virtual IP (if configured).

Step 2	**<img src="./flash:web_auth_image.jpg" alt="name”>**
	Example:
	`Switch# show run | sec parameter-map`
	`parameter-map type webauth global`
	`virtual-ip ipv4 192.0.2.1`
	`Sample Webauth_login HTML`
		Specifies to link image to the custom page. The virtual IP address is automatically used as a source. The logical link implies that you define the virtual IP address in the global parameter map.
		Note You can still define the image full path (with controller IP address). In such case, the IP address is either the management IP or the virtual IP (if configured).

Sample Web Authentication Login HTML

You can use the sample web authentication login page (**webauth_login**). If you want to modify or customize the sample page, you need to involve a developer who knows HTML, which is not covered by the Cisco Technical Assistance Center.

```
<HTML><HEAD>
<TITLE>Authentication Proxy Login Page</TITLE>
<script type="text/javascript">
var pxypromptwindow1;
var pxysubmitted = false;
function submitreload() {
    if (pxysubmitted == false) {
        pxypromptwindow1=window.open('', 'pxywindow1', 'resizable=no,width=350,
         height=350,scrollbars=yes');
        pxysubmitted = true;
        return true;
    } else {
        alert("This page can not be submitted twice.");
        return false;
    }
}
</script>
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
<style type="text/css">
body {
    background-color: #ffffff;
}
</style>
</HEAD>
<BODY>
<H1><img src="http://192.168.2.91/flash:web_auth_logo.png" width="75" height="50"
```

```
alt="Cisco Logo" longdesc="http://www.cisco.com"></H1>
<center>
<H2> Wireless Guest Access Web Authentication</H2>
<center>
<iframe src="http://192.168.2.91/flash:web_auth_aup.html" width="950" height="250"
scrolling="auto"></iframe><BR><BR>

<FORM method=post action="/" target="pxywindow1">
  Username: <input type=text name=uname><BR><BR>
  Password: <input type=password name=pwd><BR><BR>
  <input type=submit name=ok value=OK   onClick="return submitreload();">
</FORM><noscript>
<BR>
<UL>
  <H2><FONT COLOR="red">Warning!</FONT></H2>
  <p>JavaScript should be enabled in your Web browser
     for secure authentication</p>
  <LI>Follow the instructions of your Web browser to enable
      JavaScript if you would like to have JavaScript enabled
      for secure authentication</LI>
  <BR>OR<BR><BR>
  <LI> Follow these steps if you want to keep JavaScript
       disabled or if your browser does not support JavaScript
    <OL><BR>
      <LI> Close this Web brower window</LI>
      <LI> Click on Reload button of the original browser window</LI>
    </OL></LI>
</UL>
</noscript>
<center>
<p> </p>
<img src="http://192.168.2.91/flash:web_auth_cisco.png" alt="Cisco Powered" width="215"
height="136" align="middle" longdesc="http://www.cisco.com">
</center>
</BODY></HTML>
```

Configuring a Parameter Map for Local Web Authentication (CLI)

SUMMARY STEPS

1. **configure terminal**
2. **parameter-map type webauth global**
3. **banner** {*file* | *text*}
4. **custom-page**
5. **max-http-conns**
6. **intercept-https-enable**
7. **ratelimit**
8. **redirect**
9. **timeout**
10. **watch-list**
11. **virtual-ip ipv4** *virtual -IP-address*
12. **exit**
13. **no**
14. **parameter-map type webauth** *name* **type** *webauth test*
15. **banner** *bannet-text*

16. **consent email**
17. **custom-page**
18. **max-http-conns**
19. **redirect**
20. **timeout**
21. **type**
22. **exit**
23. **no**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**parameter-map type webauth global** **Example:** `Switch(config)# parameter-map type webauth global`	Creates a parameter map and enters parameter-map webauth configuration mode. The specific configuration commands supported for a global parameter map defined with the global keyword differ from the commands supported for a named parameter map defined with the parameter-map-name argument.
Step 3	**banner** {*file* | *text*} **Example:** `Switch(config-params-parameter-map)# banner`	Displays a banner on the local web-authentication login web page.
Step 4	**custom-page** **Example:** `Switch(config-params-parameter-map)# custom-page`	Specifies the custom page such as login, expired, success, or failure page.
Step 5	**max-http-conns** **Example:** `Switch(config-params-parameter-map)# max-http-conns`	Specifies the maximum number of HTTP connections per clients.
Step 6	**intercept-https-enable** **Example:** `Switch(config-params-parameter-map)# intercept-https-enable`	Specifies to enable intercept of HTTPS traffic.
Step 7	**ratelimit** **Example:** `Switch(config-params-parameter-map)# ratelimit`	Specifies to rate limit on the number of web authentication sessions.
Step 8	**redirect** **Example:**	Specifies to redirect the URL.

	Command or Action	Purpose
	`Switch(config-params-parameter-map)# redirect`	
Step 9	**timeout** **Example:** `Switch(config-params-parameter-map)# timeout`	Specifies to timeout for the initial state of web authentication.
Step 10	**watch-list** **Example:** `Switch(config-params-parameter-map)# watch-list`	Specifies the watch list of web authentication clients.
Step 11	**virtual-ip ipv4** *virtual -IP-address* **Example:** `Switch(config-params-parameter-map)# virtual-ip ipv4 172.16.16.16`	(Optional) Specifies a virtual IP address for web-based authentication clients. This command is supported in the global parameter map only.
Step 12	**exit** **Example:** `Switch(config-params-parameter-map)# exit`	Specifies to exit from **parameter-map params** configuration mode.
Step 13	**no** **Example:** `Switch(config-params-parameter-map)# no`	Specifies to negate a command or set its defaults.
Step 14	**parameter-map type webauth** *name* **type** *webauth test* **Example:** `Switch(config)# parameter-map type webauth user1 type webauth test`	Specifies parameter map user-defined name for local web-based authentication clients. This command is supported in the global parameter map only.
Step 15	**banner** *bannet-text* **Example:** `Switch(config-params-parameter-map)# banner`	(Optional) Displays a banner on the local web-authentication login web page.
Step 16	**consent email** **Example:** `Switch(config-params-parameter-map)# consent email`	(Optional) Requests a user's e-mail address on the local web-authentication login web page. This command is supported in named parameter maps only.
Step 17	**custom-page** **Example:** `Switch(config-params-parameter-map)# custom-page`	Specifies the custom page such as login, expired, success, or failure page.
Step 18	**max-http-conns** **Example:** `Switch(config-params-parameter-map)# max-http-conns`	Specifies the maximum number of HTTP connections per clients.

	Command or Action	Purpose
Step 19	**redirect** **Example:** `Switch(config-params-parameter-map)# redirect`	Specifies to redirect the URL.
Step 20	**timeout** **Example:** `Switch(config-params-parameter-map)# timeout`	Specifies to timeout for the initial state of web authentication.
Step 21	**type** **Example:** `Switch(config-params-parameter-map)# virtual-ip ipv4 172.16.16.16`	(Optional) Specifies the parameter type such as web authentication or consent, or both.
Step 22	**exit** **Example:** `Switch(config-params-parameter-map)# exit`	Specifies to exit from **parameter-map params** configuration mode.
Step 23	**no** **Example:** `Switch(config-params-parameter-map)# no`	Specifies to negate a command or set its defaults.

Monitoring Web-Based Authentication Status

Use the commands in this topic to display the web-based authentication settings for all interfaces or for specific ports.

Table 2: Privileged EXEC show Commands

Command	Purpose
show authentication sessions method webauth	Displays the web-based authentication settings for all interfaces for fastethernet, gigabitethernet, or tengigabitethernet
show authentication sessions interface *type slot/port*[**details**]	Displays the web-based authentication settings for the specified interface for fastethernet, gigabitethernet, or tengigabitethernet. In Session Aware Networking mode, use the **show access-session interface** command.

Feature Information for Web-Based Authentication

Release	Feature Information
Cisco IOS XE 3.2SECisco IOS XE 3.2SE Cisco IOS XE 3.3SE	This feature is introduced.