Configuring Web-Based Authentication

The Web-Based Authentication feature, also known as web authentication proxy, authenticates end users on host systems that do not run the IEEE 802.1x supplicant.

Restrictions for Web-Based Authentication

- Web-based authentication and URL-redirect are not supported on the same port at the same time.

Information About Web-Based Authentication

Web-Based Authentication Overview

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.

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.

> **Note** You should use global parameter-map (for method-type, custom, and redirect) only for using the same web authentication methods like consent, web consent, and webauth, for all the clients and SSIDs. This ensures that all the clients have the same web-authentication method.
>
> If the requirement is to use Consent for one SSID and Web-authentication for another SSID, then you should use two named parameter-maps. You should configure Consent in first parameter-map and configure webauth in second parameter-map.

> **Note** The traceback that you receive when webauth client tries to do authentication does not have any performance or behavioral impact. It happens rarely when the context for which FFM replied back to EPM for ACL application is already dequeued (possibly due to timer expiry) and the session becomes 'unauthorized'.

Based on where the web pages are hosted, the local web authentication can be categorized as follows:

- *Internal*: The internal default HTML pages (Login, Success, Fail, and Expire) in the controller are used during the local web authentication.

- *Customized*: The customized web pages (Login, Success, Fail, and Expire) are downloaded onto the controller and used during the local web authentication.

- *External*: The customized web pages are hosted on the external web server instead of using the in-built or custom web pages.

Based on the various web authentication pages, the types of web authentication are as follows:

- *Webauth*: This is a basic web authentication. Herein, the controller presents a policy page with the user name and password. You need to enter the correct credentials to access the network.

- *Consent or web-passthrough*: Herein, the controller presents a policy page with the Accept or Deny buttons. You need to click the Accept button to access the network.

- *Webconsent*: This is a combination of webauth and consent web authentication types. Herein, the controller presents a policy page with Accept or Deny buttons along with user name or password. You need to enter the correct credentials and click the Accept button to access the network.

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.
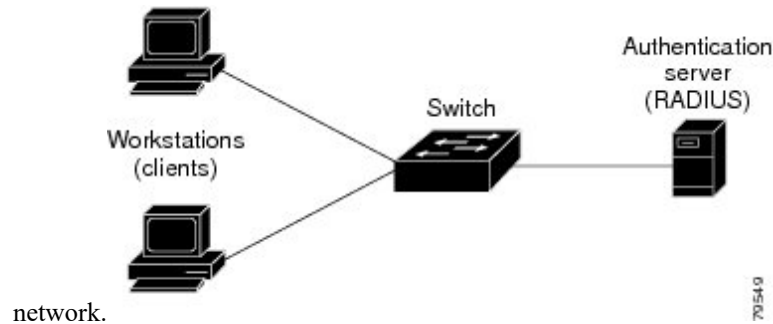
Host Detection

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

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 switch reauthenticates a client when the host does not respond to an ARP probe on a Layer 2 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.

Authentication Proxy Interaction with the Client

The authentication proxy feature requires some user interaction on the client host. The table below describes the interaction of the authentication proxy with the client host.

Table 1: Authentication Proxy Interaction with the Client Host

Authentication Proxy Action with Client	Description
Triggering on HTTP connections	If a user is not currently authenticated at the firewall router, any HTTP connection initiated by the user triggers the authentication proxy. If the user is already authenticated, the authentication proxy is transparent to the user.
Logging in using the login page	Triggering the authentication proxy generates an HTML-based login page. The user must enter a username and password to be authenticated with the AAA server. The Authentication Proxy Login Page figure, in the How the Authentication Proxy Works module, illustrates the authentication proxy login page.

Authentication Proxy Action with Client	Description
Authenticating the user at the client	Following the login attempt, the authentication proxy action can vary depending on whether JavaScript is enabled in the browser. If JavaScript is enabled, and authentication is successful, the authentication proxy displays a message indicating the status of the authentication as shown in the Authentication Proxy Login Status Message figure, in the How the Authentication Proxy Works module. After the authentication status is displayed, the proxy automatically completes the HTTP connection.
	If JavaScript is disabled, and authentication is successful, the authentication proxy generates a popup window with additional instructions for completing the connection. See the Authentication Proxy Login Status Message with JavaScript Disabled figure, in the Secure Authentication module.
	If authentication is unsuccessful in any case, the user must log in again from the login page.

When to Use the Authentication Proxy

The following are some situations in which you can use the authentication proxy:

- To manage access privileges on an individual (per-user) basis using the services provided by the authentication servers instead of configuring access control based on host IP address or global access policies. Authenticating and authorizing users from any host IP address also allows network administrators to configure host IP addresses using DHCP.

- To authenticate and authorize local users before permitting access to intranet or Internet services.

- To authenticate and authorize remote users before permitting access to local services.

- To control access for specific extranet users. For example, you might want to authenticate and authorize the financial officer of a corporate partner with one set of access privileges while authorizing the technology officer for that same partner to use another set of access privileges.

- To use the authentication proxy in conjunction with the VPN client software to validate users and to assign specific access privileges.

- To use the authentication proxy in conjunction with AAA accounting to generate start and stop accounting records that can be used for billing, security, or resource allocation purposes, thereby allowing users to track traffic from the authenticated hosts.

Applying Authentication Proxy

Apply the authentication proxy in the inbound direction at any interface on the router where you want per-user authentication and authorization. Applying the authentication proxy inbound at an interface causes it to intercept the initial connection request from an user, before that request is subjected to any other processing. If the user fails to gain authentication with the AAA server, the connection request is dropped.

How you apply the authentication proxy depends on your security policy. For example, you can block all traffic through an interface and enable the authentication proxy feature to require authentication and

authorization for all user-initiated HTTP connections. Users are authorized for services only after successful authentication with the AAA server.

The authentication proxy feature also allows you to use standard access lists to specify a host or group of hosts whose initial HTTP traffic triggers the proxy.

The figure below shows the authentication proxy applied at the LAN interface with all network users required to be authenticated upon the initial connection (all traffic is blocked at each interface).

Figure 2: Applying the Authentication Proxy at the Local Interface
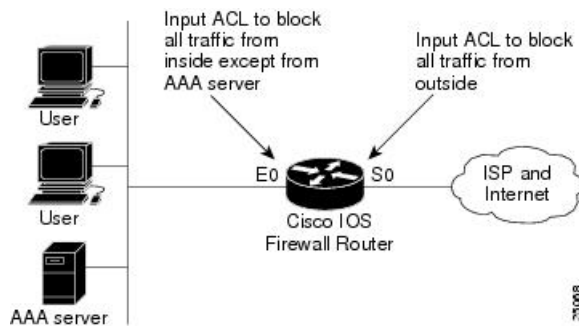
The figure below shows the authentication proxy applied at the dial-in interface with all network traffic blocked at each interface.

Figure 3: Applying the Authentication Proxy at an Outside Interface
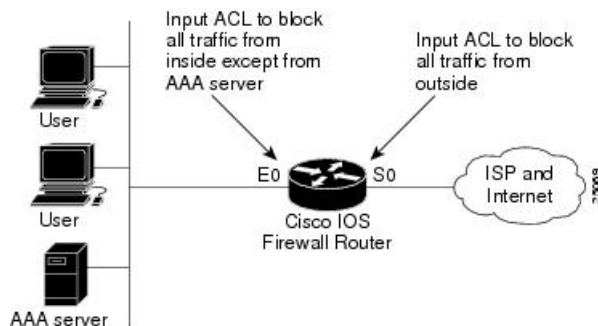
Local Web Authentication Banner

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 4: Authentication Successful Banner
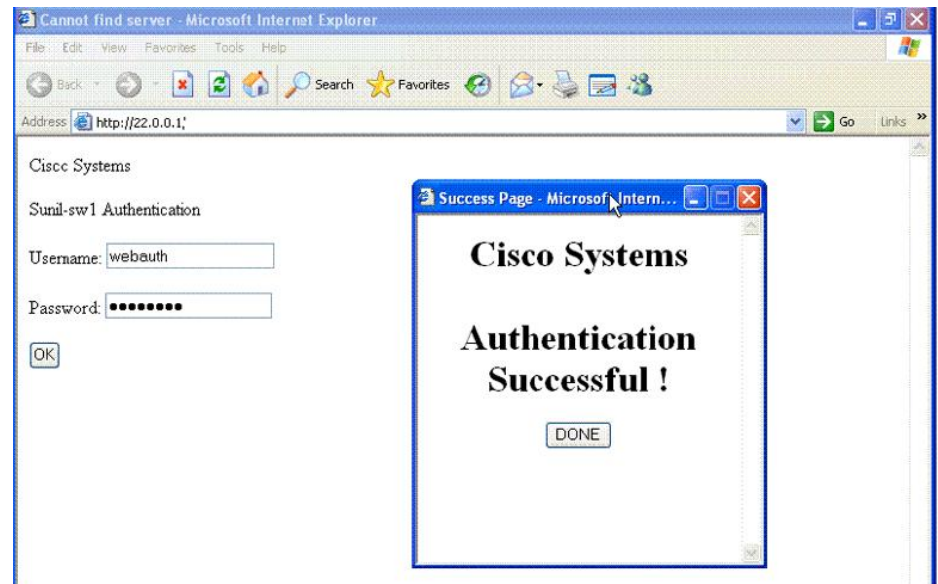
The banner can be customized as follows:

- 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 5: Customized Web Banner
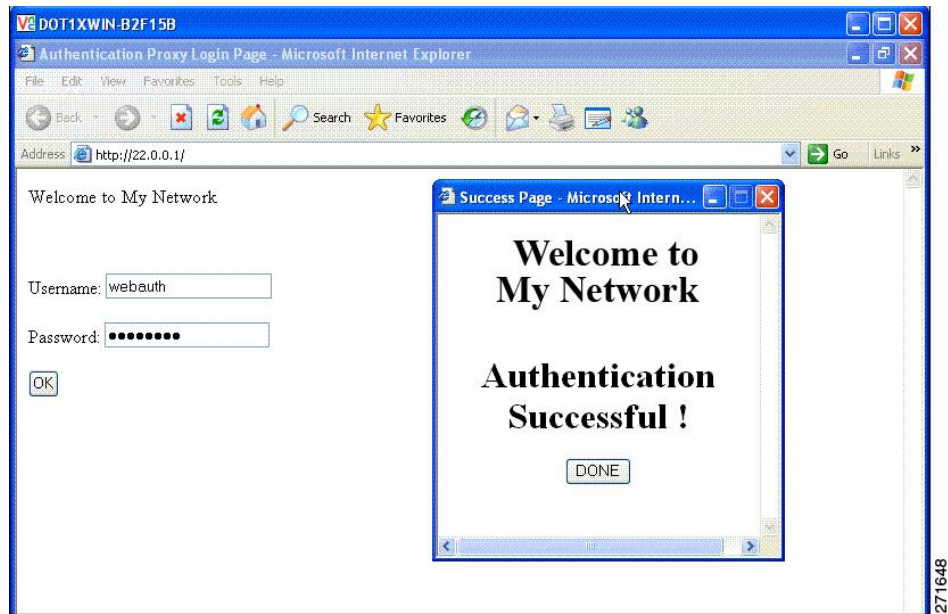
If you do not enable a banner, only the username and password dialog boxes appear in the web authentication login screen, and no banner appears when you log into the switch.

Figure 6: Login Screen With No Banner
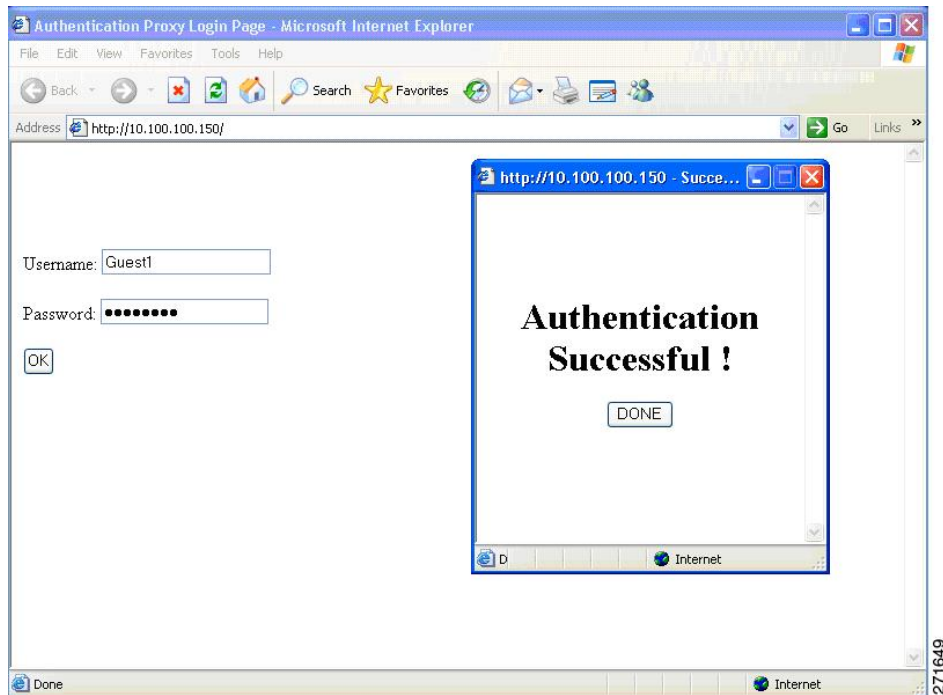
Web Authentication Customizable Web Pages

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.

- 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 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 redirecting users to specific URL after authentication occurs is entered and then the command configuring web pages is entered, the CLI redirecting users to a specific URL does not take effect.

- Configured web pages can be copied to the switch boot flash or flash.

- 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's active switch 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 7: Customizable Authentication Page
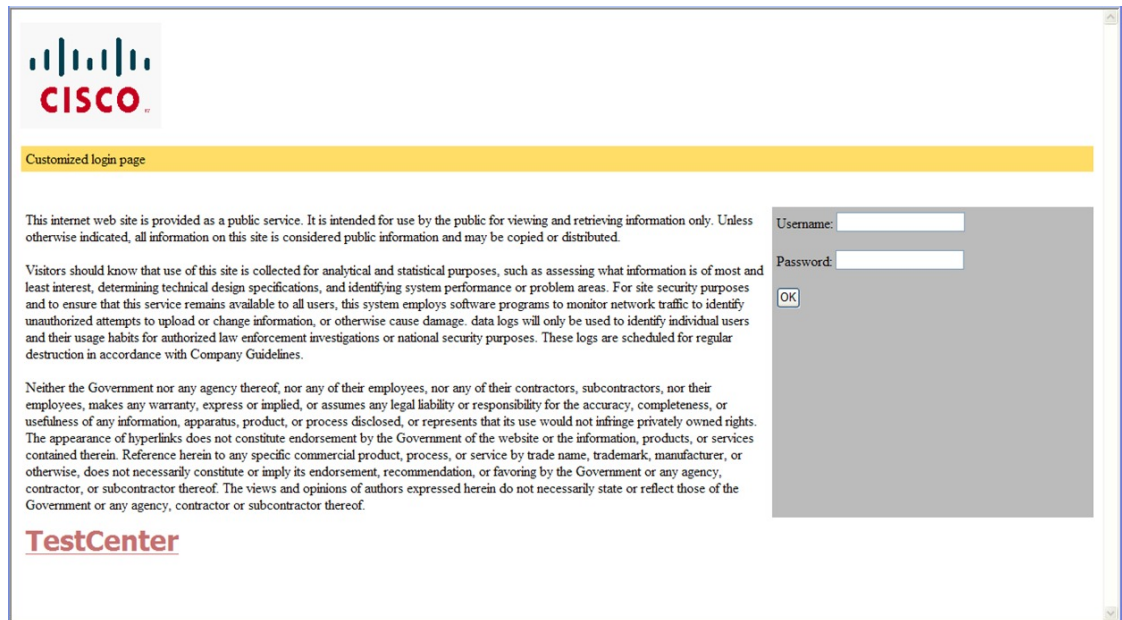
Authentication Proxy Web Page Guidelines

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.

Web-Based Authentication Interactions with Other Features

AAA Accounting with Authentication Proxy

Using the authentication proxy, you can generate start and stop accounting records with enough information to be used for billing and security auditing purposes. Thus, you can monitor the actions of authenticated hosts that use the authentication proxy service.

When an authentication proxy cache expires and is deleted, additional data, such as elapsed time, is added to the accounting information and a stop record is sent to the server. At this point, the information is deleted from the data structure.

The accounting records for the authentication proxy user session are related to the cache and the dynamic ACL usage.

ACLs

You must configure port ACLs on interfaces for web-based authentication.

Ensure that sufficient TCAM space is available to enable web-based authentication.

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.

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.

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.

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.

Default Web-Based Authentication Configuration

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

Table 2: 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.

- External web authentication, where the switch redirects a client to a particular host or web server for displaying login message, is not supported.

- 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.

- 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 key**, and **radius-server retransmit** global configuration commands.

> **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.

How to Configure Web-Based Authentication

Configuring the Authentication Rule and Interfaces

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**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** Device> **enable**	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Device# **configure terminal**	Enters global configuration mode.
Step 3	**ip admission name** *name* **proxy http** **Example:** Device(config)# **ip admission name webauth1 proxy http**	Configures an authentication rule for web-based authorization.
Step 4	**interface** *type slot/port* **Example:** Device(config)# **interface gigabitethernet 0/2**	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, GigabitEthernet, or TenGigabitEthernet.
Step 5	**ip access-group** *name* **Example:** Device(config-if)# **ip access-group webauthag**	Applies the default ACL.
Step 6	**ip admission name** **Example:** Device(config)# **ip admission name**	Configures an authentication rule for web-based authorization for the interface.
Step 7	**exit** **Example:**	Exits interface configuration mode and returns to global configuration mode.

	Command or Action	Purpose
	Device(config-if)# **exit**	
Step 8	**ip device tracking** **Example:** Device(config)# **ip device tracking**	Enables the IP device tracking table.
Step 9	**end** **Example:** Device(config)# **end**	Exits global configuration mode and returns to privileged EXEC mode.
Step 10	**show ip admission** **Example:** Device# **show ip admission**	Displays the network admission cache entries and information about web authentication sessions.

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 host** {*hostname* | *ip_address*}
7. **tacacs-server key** {*key-data*}
8. **end**

DETAILED STEPS

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

Command or Action	Purpose
Device# **configure terminal**	
Step 3 **aaa new-model** **Example:** Device(config)# **aaa new-model**	Enables AAA functionality.
Step 4 **aaa authentication login default group** {**tacacs+** | **radius**} **Example:** Device(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.
Step 5 **aaa authorization auth-proxy default group** {**tacacs+** | **radius**} **Example:** Device(config)# **aaa authorization auth-proxy default group tacacs+**	Creates an authorization method list for web-based authorization.
Step 6 **tacacs-server host** {*hostname* | *ip_address*} **Example:** Device(config)# **tacacs-server host 10.1.1.1**	Specifies an AAA server.
Step 7 **tacacs-server key** {*key-data*} **Example:** Device(config)# **tacacs-server key**	Configures the authorization and encryption key used between the device and the TACACS server.
Step 8 **end** **Example:** Device(config)# **end**	Exits global configuration mode and returns to privileged EXEC mode.

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**
4. **radius-server host** {*hostname* | *ip-address*} **test username** *username*
5. **radius-server key** *string*
6. **radius-server dead-criteria tries** *num-tries*
7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** Device> **enable**	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Device# **configure terminal**	Enters global configuration mode.
Step 3	**ip radius source-interface** **Example:** Device(config)# **ip radius source-interface vlan 80**	Specifies that the RADIUS packets have the IP address of the indicated interface.
Step 4	**radius-server host** {*hostname*	*ip-address*} **test username** *username* **Example:** Device(config)# **radius-server host 172.120.39.46 test username user1**	Specifies the host name or IP address of the remote RADIUS server. • The **test username** *username* option enables automated testing of the RADIUS server connection. The specified *username* does not need to be a valid user name. • To use multiple RADIUS servers, reenter this command for each server.
Step 5	**radius-server key** *string* **Example:** Device(config)# **radius-server key rad123**	Configures the authorization and encryption key used between the switch and the RADIUS daemon running on the RADIUS server.

	Command or Action	**Purpose**
Step 6	**radius-server dead-criteria tries** *num-tries* **Example:** Device(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 7	**end** **Example:** Device(config)# **end**	Exits global configuration mode and returns to privileged EXEC mode.

Configuring the HTTP Server

To use web-based authentication, you must enable the HTTP server within the device. 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 the procedure given below 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:** Device> **enable**	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Device# **configure terminal**	Enters global configuration mode.

	Command or Action	Purpose
Step 3	ip http server **Example:** Device(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:** Device(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:** Device(config)# **end**	Exits global configuration mode and 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 device default HTML pages during web-based authentication.

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

Before you begin

Store your custom HTML files on the device 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:**	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	**Purpose**
	Device> **enable**	
Step 2	**configure terminal** **Example:** Device# **configure terminal**	Enters global configuration mode.
Step 3	**ip admission proxy http login page file** *device:login-filename* **Example:** Device(config)# **ip admission proxy http login page file disk1:login.htm**	Specifies the location in the device 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:** Device(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.
Step 5	**ip admission proxy http failure page file** *device:fail-filename* **Example:** Device(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:** Device(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:** Device(config)# **end**	Exits global configuration mode and returns to privileged EXEC mode.

Configuring 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**

DETAILED STEPS

	Command or Action	**Purpose**
Step 1	**enable** **Example:** Device> **enable**	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Device# **configure terminal**	Enters global configuration mode.
Step 3	**ip admission max-login-attempts** *number* **Example:** Device(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:** Device(config)# **end**	Exits global configuration mode and returns to privileged EXEC mode.

Configuring a Web Authentication Local Banner

Beginning in privileged EXEC mode, follow the procedure given below to configure a local banner on a device that has web authentication configured.

SUMMARY STEPS

1. **enable**
2. **configure terminal**

3. **ip auth-proxy auth-proxy-banner http** [*banner-text* | *file-path*]
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** Device> **enable**	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Device# **configure terminal**	Enters global configuration mode.
Step 3	**ip auth-proxy auth-proxy-banner http** [*banner-text* | *file-path*] **Example:** Device(config)# **aaa ip auth-proxy auth-proxy-banner 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 a file-path indicates a file (for example, a logo or text file) that appears in the banner.
Step 4	**end** **Example:** Device(config)# **end**	Exits global configuration mode and returns to privileged EXEC mode.

Configuring Central Web Authentication

Central Web Authentication (CWA) is a process where a policy server, like Cisco Identity Services Engine (ISE), is used to centrally authenticate users via Web Authentication. Having a central policy server for Web Authentication makes it easier to implement operationally. CWA supports both ACL and VLAN-based enforcement. Additionally, RADIUS CoA is also supported. This allows for posture assessment and enforcement based on profiling.

Note CWA is introduced for the Catalyst 2960-L switch from Cisco IOS Release 15.2(5)E1.

For details on how to configure Central Web Authentication for all Catalyst switches, refer to the Central Web Authentication with a Switch and Identity Services Engine Configuration Example document.

Removing Web-Based Authentication Cache Entries

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

SUMMARY STEPS

1. **enable**

2. **clear ip admission cache** {* | *host ip address*}

DETAILED STEPS

	Command or Action	**Purpose**
Step 1	**enable** **Example:** Device> **enable**	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**clear ip admission cache** {*	*host ip address*} **Example:** Device# **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.

Verifying 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 3: 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.

Displaying Web-Based Authentication Status

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

SUMMARY STEPS

1. **show authentication sessions** {**interface***type/ slot*}

DETAILED STEPS

	Command or Action	**Purpose**
Step 1	**show authentication sessions** {**interface***type/ slot*} **Example:**	Displays the web-based authentication settings.

	Command or Action	Purpose
	This example shows how to view only the global web-based authentication status: Device# **show authentication sessions** **Example:** This example shows how to view the web-based authentication settings for GigabitEthernet interface 3/27: Device# **show authentication sessions interface gigabitethernet 3/27**	• (Optional) Use the **interface** keyword to display the web-based authentication settings for a specific interface • The *type* argument can be FastEthernet, GigabitEthernet, or TenGigabitEthernet

Monitoring HTTP Authentication Proxy

Perform the following task to troubleshoot your HTTP authentication proxy configuration:

SUMMARY STEPS

1. **enable**
2. **debug ip admission all**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** Device> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**debug ip admission all** **Example:** Device# debug ip admission all	Displays all IP admission debugging information for web-based authentication.

Verifying HTTPS Authentication Proxy

To verify your HTTPS authentication proxy configuration, perform the following optional steps:

SUMMARY STEPS

1. **enable**
2. **show ip auth-proxy cache**
3. **show ip admission { status | cache }**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show ip auth-proxy cache** **Example:** `Device# show ip auth-proxy cache`	Displays the list of user authentication entries. The authentication proxy cache lists the host IP address, the source port number, the timeout value for the authentication proxy, and the state of the connection. If the authentication proxy state is HTTP_ESTAB, the user authentication was successful.
Step 3	**show ip admission { status	cache }** **Example:** `Device# show ip admission cache`	Display the network admission configuration status and cache entries for web authentication sessions.

Configuration Examples for Web-Based Authentication

Example: Configuring the Authentication Rule and Interfaces

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

```
Device> enable
Device# configure terminal
Device(config)# ip admission name webauth1 proxy http
Device(config)# interface fastethernet 5/1
Device(config-if)# ip admission webauth1
Device(config-if)# exit
Device(config)# ip device tracking
Device(config)# end
```

This example shows how to verify the configuration:

```
Device# show ip admission
IP admission status:
  Enabled interfaces          0
  Total sessions              0
  Init sessions               0     Max init sessions allowed     100
    Limit reached             0     Hi watermark                  0
  TCP half-open connections   0     Hi watermark                  0
  TCP new connections         0     Hi watermark                  0
  TCP half-open + new         0     Hi watermark                  0
  HTTPD1 Contexts             0     Hi watermark                  0

  Parameter Map: Global
    Custom Pages
      Custom pages not configured
```

```
     Banner
       Banner not configured
```

Example: AAA Configuration

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa authentication login default group tacacs group radius
! Set up the aaa new model to use the authentication proxy.
Device(config)# aaa authorization auth-proxy default group tacacs group radius
! Define the AAA servers used by the device.
Device(config)# aaa accounting auth-proxy default start-stop group tacacs+
! Set up authentication proxy with accounting.
Device(config)# tacacs-server host 172.31.54.143
Device(config)# tacacs-server key cisco
Device(config)# radius-server host 172.31.54.143
Device(config)# radius-server key cisco
Device(config)# end
```

Example: HTTP Server Configuration

```
Device> enable
Device# configure terminal
! Enable the HTTP server on the device.
Device(config)# ip http server
! Set the HTTP server authentication method to AAA.
Device(config)# ip http authentication aaa
! Define standard access list 61 to deny any host.
Device(config)# access-list 61 deny any
! Use ACL 61 to deny connections from any host to the HTTP server.
Device(config)# ip http access-class 61
Device(config)# end
```

Example: Customizing the Authentication Proxy Web Pages

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

```
Device> enable
Device# configure terminal
Device(config)# ip admission proxy http login page file flash:login.htm
Device(config)# ip admission proxy http success page file flash:success.htm
Device(config)# ip admission proxy http fail page file flash:fail.htm
Device(config)# ip admission proxy http login expired page flash flash:expired.htm
Device(config)# end
```

The following output displays the host IP addresses, the session timeout, and the posture states. If the posture statue is POSTURE ESTAB, the host validation was successful.

```
Device# show ip admission cache eapoudp
Posture Validation Proxy Cache
Total Sessions: 3 Init Sessions: 1
 Client IP 10.0.0.112, timeout 60, posture state POSTURE ESTAB
 Client IP 10.0.0.142, timeout 60, posture state POSTURE INIT
 Client IP 10.0.0.205, timeout 60, posture state POSTURE ESTAB
```

Example: Specifying a Redirection URL for Successful Login

Configuring redirection URL for successful login

```
Device> enable
Device# configure terminal
Device(config)# ip admission proxy http success redirect www.cisco.com
Device(config)# end
```

Additional References for Web-Based Authentication

Related Documents

Related Topic	Document Title
For complete syntax and usage information for the commands used in this chapter.	Consolidated Platform Command Reference, Cisco IOS Release 15.2(7)Ex (Catalyst 2960-L Switches)

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature Information for Web-Based Authentication

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 4: Feature Information for Web-Based Authentication

Feature Name	Releases	Feature Information
Web-Based Authentication	Cisco IOS Release 15.2(5)ECisco IOS Release 15.2(7)E1	This feature was introduced.