Web-Based Authentication

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

- Local Web Authentication Overview, on page 1
- How to Configure Local Web Authentication, on page 8
- Information About Management over Wireless, on page 23
- Configuration Examples for Local Web Authentication, on page 24

Local Web Authentication Overview

Use the local web 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, local web authentication intercepts ingress HTTP packets from the host and sends an HTML login page to the users. The users enter their credentials, which the local web authentication feature sends to the authentication, authorization, and accounting (AAA) server for authentication.

If authentication succeeds, local web authentication sends a Login-Successful HTML page to the host and applies the access policies returned by the AAA server.

If authentication fails, local web 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, local web authentication forwards a Login-Expired HTML page to the host, and the user is excluded with the exclusion reason as Web authentication failure.

Note

You should use either global or named parameter-map under WLAN (for method-type, custom, and redirect) for using the same web authentication methods, such as consent, web consent, and webauth. Global parameter-map is applied by default, if none of the parameter-map is configured under WLAN.
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.

- You can view the webauth parameter-map information using the `show running-config` command output.
- The wireless Web-Authentication feature does not support the bypass type.

**Device Roles**

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

Authentication Process

When you enable local web 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.

*Note*
Beginning with Cisco IOS XE Denali 16.1.1 and later, the default session timeout value for local web authentication on WLC is 1800 seconds. The default session timeout value was infinite seconds, prior to Cisco IOS XE Denali 16.1.1.

- 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 the new-style (Session-aware) CLI mode as follows:

- New-style mode—Use the following global configuration command:
  
  ```
  parameter-map type webauth global
  banner text <text>
  ```

  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**

  ![Authentication Successful Banner](image)

  The banner can be customized as follows:

  - Add a message, such as switch, router, or company name to the banner:
    
    - New-style mode—Use the following global configuration command:
      
      ```
      parameter-map type webauth global
      banner text <text>
      ```
• Add a logo or text file to the banner:
  • New-style mode—Use the following global configuration command:
    parameter-map type webauth global
    banner file <filepath>

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.
Customized Local Web Authentication

During the local web 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.

• 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**

**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.

### How to Configure Local Web Authentication

#### Configuring Default Local Web Authentication

The following table shows the default local web authentication configuration.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAA</td>
<td>Disabled</td>
</tr>
<tr>
<td>RADIUS server</td>
<td></td>
</tr>
<tr>
<td>• IP address</td>
<td>• None specified</td>
</tr>
<tr>
<td>• UDP authentication port</td>
<td>• None specified</td>
</tr>
<tr>
<td>• Key</td>
<td></td>
</tr>
<tr>
<td>Default value of inactivity timeout</td>
<td>3600 seconds</td>
</tr>
<tr>
<td>Inactivity timeout</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

#### Configuring AAA Authentication (GUI)

**Procedure**

1. Choose **Configuration** > **Security** > **AAA**.
2. In the **Authentication** section, click **Add**.
3. In the **Quick Setup: AAA Authentication** window that is displayed, enter a name for your method list.
4. Choose the type of authentication you want to perform before allowing access to the network, in the **Type** drop-down list.
5. Choose if you want to assign a group of servers as your access server, or if you want to use a local server to authenticate access, from the **Group** Type drop-down list.
### Configuring AAA Authentication (CLI)

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>aaa new-model</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# aaa new-model</td>
<td>Enables AAA functionality.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>`aaa authentication login {default</td>
<td>named_authentication_list} group AAA_group_name`</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# aaa authentication login default group group1</td>
<td>Defines the list of authentication methods at login. <code>named_authentication_list</code> refers to any name that is not greater than 31 characters. <code>AAA_group_name</code> refers to the server group name. You need to define the server-group <code>server_name</code> at the beginning itself.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>`aaa authorization network {default</td>
<td>named} group AAA_group_name`</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# aaa authorization network default group group1</td>
<td>Creates an authorization method list for web-based authorization.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><code>tacacs server server-name</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# tacacs server yourserver</td>
<td>Specifies an AAA server.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>`address {ipv4</td>
<td>ipv6}ip_address`</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-server-tacacs)# address ipv4 10.0.1.12</td>
<td>Configures the IP address for the TACACS server.</td>
</tr>
</tbody>
</table>
### Configuring the HTTP/HTTPS Server (GUI)

#### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 6</td>
<td>tacacs-server host {hostname | ip_address}</td>
<td>Specifies an AAA server.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)# tacacs-server host 10.1.1.1</td>
<td></td>
</tr>
</tbody>
</table>

#### Configuring the HTTP/HTTPS Server (GUI)

**Step 1**  
Choose **Administration > Management > HTTP/HTTPS/Netconf**.

**Step 2**  
In the **HTTP/HTTPS Access Configuration** section, enable HTTP Access and enter the port that will listen for HTTP requests. The default port is 80. Valid values are 80, and ports between 1025 and 65535.

**Step 3**  
Enable **HTTPS Access** on the device and enter the designated port to listen for HTTPS requests. The default port is 1025. Valid values are 443, and ports between 1025 and 65535. On a secure HTTP connection, data to and from an HTTP server is encrypted before being sent over the Internet. HTTP with SSL encryption provides a secure connection to allow such functions as configuring a switch from a Web browser.

**Step 4**  
Choose the **Personal Identity Verification** as enabled or disabled.

**Step 5**  
In the **HTTP Trust Point Configuration** section, enable **Enable Trust Point** to use Certificate Authority servers as trustpoints.

**Step 6**  
From the **Trust Points** drop-down list, choose a trust point.

**Step 7**  
In the **Timeout Policy Configuration** section, enter the HTTP timeout policy in seconds. Valid values can range from 1 to 600 seconds.

**Step 8**  
Enter the number of minutes of inactivity allowed before the session times out. Valid values can range from 180 to 1200 seconds.

**Step 9**  
Enter the server life time in seconds. Valid values can range from 1 to 86400 seconds.

**Step 10**  
Enter the maximum number of requests the device can accept. Valid values range from 1 to 86400 requests.

**Step 11**  
Save the configuration.

### Configuring the HTTP Server (CLI)

To use local web authentication, you must enable the HTTP server within the Device. You can enable the server for either HTTP or HTTPS.

#### Note

The Apple pseudo-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:
## Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Device&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> ip http server</td>
<td>Enables the HTTP server. The local web authentication feature uses the HTTP server to communicate with the hosts for user authentication.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config)# ip http server</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> ip http secure-server</td>
<td>Enables HTTPS. You can configure custom authentication proxy web pages or specify a redirection URL for successful login.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config)# ip http secure-server</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config)# end</td>
<td></td>
</tr>
</tbody>
</table>

### Creating Parameter Maps

#### Configuring Local Web Authentication (GUI)

**Procedure**

- **Step 1** Choose Configuration > Security > Web Auth.
- **Step 2** On the Web Auth page, click Add.
Step 3 In the Create Web Auth Parameter window that is displayed, enter a name for the parameter map.

Step 4 In the Maximum HTTP Connections field, enter the maximum number of HTTP connections that you want to allow.

Step 5 In the Init-State Timeout field, enter the time after which the init state timer should expire due to a user's failure to enter valid credentials in the login page.

Step 6 Choose the type of Web Auth parameter.

Step 7 Click Apply to Device.

Step 8 On the Web Auth page, click the name of the parameter map.

Step 9 In the Edit WebAuth Parameter window that is displayed, choose the required Banner Type.
   • If you choose Banner Text, enter the required banner text to be displayed.
   • If you choose File Name, specify the path of the file from which the banner text has to be picked up.

Step 10 Enter the virtual IP addresses as required.

Step 11 Set appropriate status of WebAuth Intercept HTTPS, Captive Bypass Portal, and Watch List Enable.

Step 12 In the Watch List Expiry Timeout field, enter the time in seconds after which the watch list should time out.

Step 13 Set appropriate status for Disable Success Window, Disable Logout Window, and Login Auth Bypass for FQDN.

Step 14 Check the Sleeping Client Status check box to enable authentication of sleeping clients and then specify the Sleeping Client Timeout in minutes. Valid range is between 10 minutes and 43200 minutes.

Step 15 Click the Advanced tab.

Step 16 In the Redirect for log-in field, enter the name of the external server to send login request.

Step 17 In the Redirect On-Success field, enter the name of the external server to redirect after a successful login.

Step 18 In the Redirect On-Failure field, enter the name of the external server to redirect after a login failure.

Step 19 To configure external local web authentication, perform these tasks:
   a) Under Redirect to External Server in the Redirect Append for AP MAC Address field, enter the AP MAC address.
   b) In the Redirect Append for Client MAC Address field, enter the client MAC address.
   c) In the Redirect Append for WLAN SSID field, enter the WLAN SSID.
   d) In the Portal IPV4 Address field, enter the IPv4 address of the portal to send redirects.
   e) In the Portal IPV6 Address field, enter the IPv6 address of the portal to send redirects, if IPv6 address is used.

Step 20 To configure customized local web authentication, perform these tasks:
   a) Under Customized Page, specify the following pages:
      • Login Failed Page
      • Login Page
      • Logout Page
      • Login Successful Page

Step 21 Click Update & Apply.
## Configuring the Internal Local Web Authentication (CLI)

Follow the procedure given below to configure the internal local web authentication:

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>parameter-map type webauth {parameter-map-name</td>
<td>global}</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# parameter-map type webauth sample</td>
<td>The parameter-map-name must not exceed 99 characters.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# end</td>
<td></td>
</tr>
</tbody>
</table>

## Configuring the Customized Local Web Authentication (CLI)

Follow the procedure given below to configure the customized local web authentication:

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
<td></td>
</tr>
<tr>
<td>Device# configure terminal</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Step 3**  
**parameter-map type webauth**  
**parameter-map-name**  
*Example:*  
Device(config)# parameter-map type webauth sample  
*Note* You need to configure a virtual IP in the global parameter map to use the customized web authentication bundle.

**Step 4**  
**type** {authbypass | consent | webauth | webconsent}  
*Example:*  
Device(config-params-parameter-map)# type webauth

**Step 5**  
**custom-page login device** *html-filename*  
*Example:*  
Device(config-params-parameter-map)# custom-page login device bootflash:login.html  
Configures the customized login page.

**Step 6**  
**custom-page login expired device** *html-filename*  
*Example:*  
Device(config-params-parameter-map)# custom-page login expired device bootflash:loginexpired.html  
Configures the customized login expiry page.

**Step 7**  
**custom-page success device** *html-filename*  
*Example:*  
Device(config-params-parameter-map)# custom-page success device bootflash:loginsuccess.html  
Configures the customized login success page.

**Step 8**  
**custom-page failure device** *html-filename*  
*Example:*  
Device(config-params-parameter-map)# custom-page failure device bootflash:loginfail.html  
Configures the customized login failure page.

**Step 9**  
**end**  
*Example:*  
Returns to privileged EXEC mode.
### Configuring the External Local Web Authentication (CLI)

Follow the procedure given below to configure the external local web authentication:

#### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 1 | `enable` | Enables privileged EXEC mode.  
Example:  
Device> `enable`  
- Enter your password if prompted. |
| Step 2 | `configure terminal` | Enters global configuration mode.  
Example:  
Device# `configure terminal` |
| Step 3 | `parameter-map type webauth`  
`parameter-map-name` | Configures the webauth type parameter.  
Example:  
Device(config)# `parameter-map type webauth sample` |
| Step 4 | `type {authbypass | consent | webauth | webconsent}` | Configures the webauth sub-types, such as consent, passthru, webauth, or webconsent.  
Example:  
Device(config-params-parameter-map)# `type webauth` |
| Step 5 | `redirect [for-login | on-failure | on-success]`  
`URL` | Configures the redirect URL for the login, failure, and success pages.  
Example:  
Device(config-params-parameter-map)# `redirect for-login`  
`http://9.1.0.100/login.html`  
**Note**  
In the redirect url, you need to press `Ctrl+v` and type `?` to configure the `?` character.  
The `?` character is commonly used in URL when ISE is configured as an external portal. |
### Configuring the External Portal IPv4 Address

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>redirect portal ipv4</td>
<td>Configures the external portal IPv4 address.</td>
</tr>
</tbody>
</table>

**Example:**

```
Device(config-params-parameter-map)# redirect portal ipv4 23.0.0.1
```

### Configurations

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>redirect portal ipv4</td>
<td>Configures the external portal IPv4 address.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-params-parameter-map)# redirect portal ipv4 23.0.0.1</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)# end</td>
<td></td>
</tr>
</tbody>
</table>

### Configuring the Web Authentication WLANs

Follow the procedure given below to configure WLAN using web auth security and map the authentication list and parameter map:

#### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device&gt; enable</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>wlan profile-name wlan-id ssid-name</td>
<td>Specifies the WLAN name and ID.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)# wlan mywlan 34 mywlan-ssid</td>
<td></td>
</tr>
<tr>
<td></td>
<td>profile-name is the WLAN name which can contain 32 alphanumeric characters.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>wlan-id is the wireless LAN identifier. The valid range is from 1 to 512.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ssid-name is the SSID which can contain 32 alphanumeric characters.</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>no security wpa</td>
<td>Disables the WPA security.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-wlan)# no security wpa</td>
<td></td>
</tr>
</tbody>
</table>
### Command or Action

| Step 5 | security web-auth {authentication-list authentication-list-name | parameter-map parameter-map-name} |
|--------|-----------------------------------------------------------------------------------|
|        | Enables web authentication for WLAN. Here,  
|        | • authentication-list authentication-list-name: Sets the authentication list for IEEE 802.1x.  
|        | • parameter-map parameter-map-name: Configures the parameter map.  

**Example:**  
Device(config-wlan)# security web-auth authentication-list webauthlistlocal  
Device(config-wlan)# security web-auth parameter-map sample

| Step 6 | end  
|--------|------|
|        | Returns to privileged EXEC mode.  

**Example:**  
Device(config)# end

---

### Configuring Pre-Auth Web Authentication ACL (GUI)

**Before you begin**

Ensure that you have configured an access control list (ACL) and a WLAN.

**Procedure**

1. **Step 1**  
   Choose **Configuration > Tags & Profiles > WLANs**.
2. **Step 2**  
   Click the name of the WLAN.
3. **Step 3**  
   In the **Edit WLAN** window, click the **Security** tab and then click the **Layer3** tab.
4. **Step 4**  
   Click **Show Advanced Settings**.
5. **Step 5**  
   In the **Preauthentication ACL** section, choose the appropriate ACL to be mapped to the WLAN.
6. **Step 6**  
   Click **Update & Apply to Device**.

---

### Configuring Pre-Auth Web Authentication ACL (CLI)

Follow the procedure given below to configure pre-auth web authentication ACL:
### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** | `enable` | Enables privileged EXEC mode.  
  **Example:**  
  `Device> enable` |
| **Step 2** | `configure terminal` | Enters global configuration mode.  
  **Example:**  
  `Device# configure terminal` |
| **Step 3** | `access-list access-list-number {deny | permit} source [source-wildcard-bits]` | Creates an ACL list.  
  **Example:**  
  `Device(config)# access-list 2 deny your_host` |
| **Step 4** | `wlan profile-name wlan-id ssid-name` | Creates the WLAN.  
  **Example:**  
  `Device(config)# wlan mywlan 34 mywlan-ssid` |

1. **Purpose:** Enables privileged EXEC mode.  
- Enter your password if prompted.

2. **Purpose:** Enters global configuration mode.

3. **Purpose:** Creates an ACL list.
- **access-list-number** is a decimal number from 1 to 99, 100 to 199, 300 to 399, 600 to 699, 1300 to 1999, 2000 to 2699, or 2700 to 2799.
- Enter `deny` or `permit` to specify whether to deny or permit if the conditions are matched.
- **source** is the source address of the network or host from which the packet is being sent specified as:
  - The 32-bit quantity in dotted-decimal format.
  - The keyword `any` as an abbreviation for `source` and `source-wildcard` of 0.0.0.0 255.255.255.255. You do not need to enter a source-wildcard.
  - The keyword `host` as an abbreviation for `source` and `source-wildcard` of source 0.0.0.0.
- *(Optional)* The `source-wildcard` applies wildcard bits to the source.

4. **Purpose:** Creates the WLAN.
- **profile-name** is the WLAN name which can contain 32 alphanumeric characters.
- **wlan-id** is the wireless LAN identifier. The valid range is from 1 to 512.
- **ssid-name** is the SSID which can contain 32 alphanumeric characters.
**Purpose**

**Command or Action**

<table>
<thead>
<tr>
<th>Step 5</th>
<th>ip access-group web access-list-name</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Device(config-wlan)# ip access-group web name</td>
</tr>
</tbody>
</table>

Maps the ACL to the web auth WLAN. *access-list-name* is the IPv4 ACL name or ID.

<table>
<thead>
<tr>
<th>Step 6</th>
<th>end</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Device(config)# end</td>
</tr>
</tbody>
</table>

Returns to privileged EXEC mode.

---

### Configuring the Maximum Web Authentication Request Retries

Follow these steps to configure the maximum web authentication request retries:

#### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> wireless security web-auth retries number</td>
<td><em>number</em> is the maximum number of web auth request retries. The valid range is 0 to 20.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config)# wireless security web-auth retries 2</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config)# end</td>
<td></td>
</tr>
</tbody>
</table>
Configuring a Local Banner in Web Authentication Page (GUI)

**Procedure**

**Step 1** Choose **Configuration > Security > Web Auth.**

**Step 2** In the **Webauth Parameter Map** tab, click the parameter map name. The **Edit WebAuth Parameter** window is displayed.

**Step 3** In the **General** tab and choose the required Banner Type:

- If you choose **Banner Text**, enter the required banner text to be displayed.
- If you choose **File Name**, specify the path of the file from which the banner text has to be picked up.

**Step 4** Click **Update & Apply**.

Configuring a Local Banner in Web Authentication Page (CLI)

Follow the procedure given below to configure a local banner in web authentication pages.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Device&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Device# configure terminal</td>
<td></td>
</tr>
</tbody>
</table>

**Step 3** `ip admission auth-proxy-banner http [banner-text | file-path]`

**Example:**

Device(config)# ip admission auth-proxy-banner http C My Switch C

(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:**

Returns to privileged EXEC mode.
### Configuring Webpassthrough

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device # configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> parameter-map type webauth parameter-map name</td>
<td>Configures the webauth type parameter.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device (config) # parameter-map type webauth webparalocal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> type consent</td>
<td>Configures webauth type as consent.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device (config-params-parameter-map) # type consent</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device (config-params-parameter-map) # end</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> show running-config</td>
<td>Displays the configuration details.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
</tbody>
</table>
### Configuring Preauthentication ACL

#### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Device# <code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td><code>wlan wlan-name</code></td>
<td>For <code>wlan-name</code>, enter the profile name.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Device (config)# <code>wlan ramban</code></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td><code>shutdown</code></td>
<td>Disables the WLAN.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Device (config-wlan)# <code>shutdown</code></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td><code>ip access-group web preauthrule</code></td>
<td>Configures ACL that has to be applied before authentication.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Device (config-wlan)# <code>ip access-group web preauthrule</code></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td><code>no shutdown</code></td>
<td>Enables the WLAN.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Device (config)# <code>no shutdown</code></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td><code>end</code></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Device (config-wlan)# <code>end</code></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td><code>show wlan name wlan-name</code></td>
<td>Displays the configuration details.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Device# <code>show wlan name ramban</code></td>
<td></td>
</tr>
</tbody>
</table>
Information About Management over Wireless

The management over wireless feature allows you to monitor and configure local controllers using a wireless client. You can perform all the management tasks except uploads to and downloads from (transfers to and from) the controller.

Restrictions on Management over Wireless
- Management over wireless can be disabled only if clients are on central switching.

Configuring Management over Wireless (GUI)

Procedure

1. Choose Administration > Device > Wireless.
2. Check the Management Via Wireless check box to enable the feature.
3. Save the configuration.

Configuring Management over Wireless (CLI)

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Example: Device(config)# wireless mgmt-via-wireless</td>
<td></td>
</tr>
<tr>
<td>Step 3 end</td>
<td>Exits the global configuration mode and returns to the privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 4 show running-config</td>
<td>Verifies the status of management access over wireless clients.</td>
</tr>
<tr>
<td>Example: Device# show running-config</td>
<td></td>
</tr>
</tbody>
</table>
Configuration Examples for Local Web Authentication

Example: Obtaining Web Authentication Certificate

This example shows how to obtain web authentication certificate.

```plaintext
Device# configure terminal
Device(config)# crypto pki import cert pkcs12 tftp://9.1.0.100/ldapserver-cert.p12 cisco
Device(config)# end
Device# show crypto pki trustpoints cert
Trustpoint cert:
  Subject Name:
  e=rkannajr@cisco.com
cn=sthaliya-lnx
ou=WNBU
o=Cisco
l=SanJose
st=California
c=US
  Serial Number (hex): 00
  Certificate configured.

Device# show crypto pki certificates cert
Certificate
  Status: Available
  Certificate Serial Number (hex): 04
  Certificate Usage: General Purpose
  Issuer:
    e=rkannajr@cisco.com
cn=sthaliya-lnx
ou=WNBU
o=Cisco
l=SanJose
st=California
c=US
  Subject:
    Name: ldapserver
e=rkannajr@cisco.com
cn=ldapserver
ou=WNBU
o=Cisco
st=California
c=US
  Validity Date:
    start date: 07:35:23 UTC Jan 31 2012
    end date: 07:35:23 UTC Jan 28 2022
  Associated Trustpoints: cert ldap12
  Storage: nvram:rkannajrscisc#4.cer

CA Certificate
  Status: Available
  Certificate Serial Number (hex): 00
  Certificate Usage: General Purpose
  Issuer:
    e=rkannajr@cisco.com
cn=sthaliya-lnx
ou=WNBU
o=Cisco
l=SanJose
st=California
```
Example: Displaying a Web Authentication Certificate

This example shows how to display a web authentication certificate.

Device# show crypto ca certificate verb
Certificate
Status: Available
Version: 3
Certificate Serial Number (hex): 2A9636AC00000000858B
Certificate Usage: General Purpose
Issuer:
cn=Cisco Manufacturing CA
o=Cisco Systems
Subject:
Name: WS-C3780-6DS-S-2037064C0E80
Serial Number: PID:WS-C3780-6DS-S SN:FOC1534X12Q
CRL Distribution Points:
Validity Date:
start date: 15:43:22 UTC Aug 21 2011
end date: 15:53:22 UTC Aug 21 2021
Subject Key Info:
Public Key Algorithm: rsaEncryption
RSA Public Key: (1024 bit)
Signature Algorithm: sha1WithRSAEncryption
Fingerprint MD5: A310B856 A41565F1 1D9410B5 7284CB21
Fingerprint SHA1: 04F180F6 CA1A67AF 9D7F561A 2BB397A1 0F5EB3C9
X509v3 extensions:
Digital Signature
Non Repudiation
Key Encipherment
Data Encipherment
X509v3 Subject Key ID: B9EEB123 5A3764B4 5E9C54A7 46E6EECA 02D283F7
X509v3 Authority Key ID: D0C52226 AB4F4660 ECAE0591 C7DC5AD1 B0471F76C
Authority Info Access:
Associated Trustpoints: CISCO_IDEVID_SUDI
Key Label: CISCO_IDEVID_SUDI
Example: Choosing the Default Web Authentication Login Page

This example shows how to choose a default web authentication login page.

Device# configure terminal
Device(config)# parameter-map type webauth test
This operation will permanently convert all relevant authentication commands to their CPL control-policy equivalents. As this conversion is irreversible and will disable the conversion CLI 'authentication display [legacy|new-style]', you are strongly advised to back up your current configuration before proceeding.
Do you wish to continue? [yes]: yes
Device(config)# wlan wlan50
Device(config-wlan)# shutdown
Device(config-wlan)# security web-auth authentication-list test
Device(config-wlan)# security web-auth parameter-map test
Device(config-wlan)# no shutdown
Device(config-wlan)# end
Device# show running-config | section wlan50
wlan wlan50 50 wlan50
security wpa akm cckm
security wpa wpa1
security wpa wpa1 ciphers aes
security wpa wpa1 ciphers tkip
security web-auth authentication-list test
security web-auth parameter-map test
session-timeout 1800
no shutdown

Device# show running-config | section parameter-map type webauth test
parameter-map type webauth test
type webauth

Example: Choosing a Customized Web Authentication Login Page from an IPv4 External Web Server

This example shows how to choose a customized web authentication login page from an IPv4 external web server.

Device# configure terminal
Device(config)# parameter-map type webauth global
Device(config-params-parameter-map)# virtual-ip ipv4 1.1.1.1
Device(config-params-parameter-map)# parameter-map type webauth test
type webauth
Device(config-params-parameter-map)# redirect for-login http://9.1.0.100/login.html
Device(config-params-parameter-map)# redirect portal ipv4 9.1.0.100
Device(config-params-parameter-map)# end
Device# show running-config | section parameter-map
parameter-map type webauth global
virtual-ip ipv4 1.1.1.1
parameter-map type webauth test
type webauth
redirect for-login http://9.1.0.100/login.html
redirect portal ipv4 9.1.0.100
security web-auth parameter-map rasagna-auth-map
security web-auth parameter-map test
Example: Choosing a Customized Web Authentication Login Page from an IPv6 External Web Server

This example shows how to choose a customized web authentication login page from an IPv6 external web server.

Device# configure terminal
Device(config)# parameter-map type webauth global
Device(config-params-parameter-map)# virtual-ip ipv6 1:1:1::1
Device(config-params-parameter-map)# parameter-map type webauth test
Device(config-params-parameter-map)# type webauth
Device(config-params-parameter-map)# redirect for-login http://9:1:1::100/login.html
Device(config-params-parameter-map)# redirect portal ipv6 9:1:1::100
Device(config-params-parameter-map)# end
Device# show running-config | section parameter-map
parameter-map type webauth global
virtual-ip ipv6 1:1:1::1
parameter-map type webauth test
type webauth
redirect for-login http://9:1:1::100/login.html
redirect portal ipv6 9:1:1::100
security web-auth parameter-map rasagna-auth-map
security web-auth parameter-map test

Example: Assigning Login, Login Failure, and Logout Pages per WLAN

This example shows how to assign login, login failure and logout pages per WLAN.

Device# configure terminal
Device(config)# parameter-map type webauth test
Device(config-params-parameter-map)# custom-page login device flash:loginsantosh.html
Device(config-params-parameter-map)# custom-page login expired device flash:loginexpire.html
Device(config-params-parameter-map)# custom-page failure device flash:loginfail.html
Device(config-params-parameter-map)# custom-page success device flash:loginsuccess.html
Device(config-params-parameter-map)# end
Device# show running-config | section parameter-map type webauth test
parameter-map type webauth test
type webauth
redirect for-login http://9.1.0.100/login.html
redirect portal ipv4 9.1.0.100
custom-page login device flash:loginsantosh.html
custom-page success device flash:loginsuccess.html
custom-page failure device flash:loginfail.html
custom-page login expired device flash:loginexpire.html

Example: Configuring Preauthentication ACL

This example shows how to configure preauthentication ACL.

Device# configure terminal
Device(config)# wlan fff
Device(config-wlan)# shutdown
Device(config-wlan)# ip access-group web preauthrule
Device(config-wlan)# no shutdown
Example: Configuring Webpassthrough

This example shows how to configure webpassthrough.

```
Device# configure terminal
Device(config)# parameter-map type webauth webparalocal
Device(config-params-parameter-map)# type consent
Device(config-params-parameter-map)# end
Device# show running-config | section parameter-map type webauth test
parameter-map type webauth test
  type webauth
  redirect for-login http://9.1.0.100/login.html
  redirect portal ipv4 9.1.0.100
```