Web-Based Authentication

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

• Authentication Overview, on page 1
• How to Configure Local Web Authentication, on page 7
• Information About Management over Wireless, on page 13
• Configuration Examples for Local Web Authentication, on page 14

Authentication Overview

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

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

If authentication fails, 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, authentication forwards a Login-Expired HTML page to the host, and the user is...

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

---

**Note**

• 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.

• Change in web authentication parameter map redirect login URL does not occur until a AP rejoin happens. You must enable and disable the WLAN to apply the new URL redirection.

---

**Note**

We recommend that you follow the Cisco guidelines to create a customized web authentication login page. If you have upgraded to the latest versions of Google Chrome or Mozilla Firefox browsers, ensure that your webauth bundle has the following line in the `login.html` file:

```html
<body onload="loadAction();"> 
```
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.
- 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 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*

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>
    ```
If you do not enable a banner, only the username and password dialog boxes appear in the web authentication login screen, and no banner appears when you log into the switch.

**Figure 4: Login Screen With No Banner**
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 primary stack 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.
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>
</tbody>
</table>
### Configuring AAA Authentication (GUI)

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Choose <strong>Configuration &gt; Security &gt; AAA</strong>.</td>
</tr>
<tr>
<td>Step 2</td>
<td>In the <strong>Authentication</strong> section, click <strong>Add</strong>.</td>
</tr>
<tr>
<td>Step 3</td>
<td>In the <strong>Quick Setup: AAA Authentication</strong> window that is displayed, enter a name for your method list.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Choose the type of authentication you want to perform before allowing access to the network, in the <strong>Type</strong> drop-down list.</td>
</tr>
<tr>
<td>Step 5</td>
<td>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 <strong>Group</strong> Type drop-down list.</td>
</tr>
<tr>
<td>Step 6</td>
<td>To configure a local server to act as a fallback method when servers in the group are unavailable, check the <strong>Fallback</strong> to local check box.</td>
</tr>
<tr>
<td>Step 7</td>
<td>Choose the server groups you want to use to authenticate access to your network, from the <strong>Available Server Groups</strong> list and click &gt; icon to move them to the <strong>Assigned Server Groups</strong> list.</td>
</tr>
<tr>
<td>Step 8</td>
<td>Click <strong>Save &amp; Apply to Device</strong>.</td>
</tr>
</tbody>
</table>

### Configuring AAA Authentication (CLI)

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>aaa new-model</code></td>
<td>Enables AAA functionality.</td>
</tr>
<tr>
<td><em>Example:</em></td>
<td><code>Device(config)# aaa new-model</code></td>
<td></td>
</tr>
</tbody>
</table>

---

#### Default Setting

**Feature** | **Default Setting**
---|---
RADIUS server | • None specified
  - IP address
  - UDP authentication port
  - Key
Default value of inactivity timeout | 3600 seconds
Inactivity timeout | Enabled
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 2</strong></td>
<td>Defines the list of authentication methods at login.</td>
</tr>
<tr>
<td>aaa authentication login {default</td>
<td>named_authentication_list} group AAA_group_name</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config)# aaa authentication login default group group1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Creates an authorization method list for web-based authorization.</td>
</tr>
<tr>
<td>aaa authorization network {default</td>
<td>named} group AAA_group_name</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config)# aaa authorization network default group group1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Specifies a AAA server.</td>
</tr>
<tr>
<td>tacacs-server host {hostname</td>
<td>ip_address}</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config)# tacacs-server host 10.1.1.1</td>
<td></td>
</tr>
</tbody>
</table>

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

**Procedure**

**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>
</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** ip http server | Enables the HTTP server. The local web authentication feature uses the HTTP server to communicate with the hosts for user authentication.  
  Example:  
  Device(config)# ip http server |
| **Step 4** ip http secure-server | Enables HTTPS.  
  You can configure custom authentication proxy web pages or specify a redirection URL for successful login.  
  Example:  
  Device(config)# ip http secure-server |

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.
### Creating a Parameter Map (GUI)

**Procedure**

**Step 1**  Choose **Configuration > Security > Local Policy**.
**Step 2**  Click **Add**.
**Step 3**  Click **Policy Map**.
**Step 4**  Enter **Policy Map Name**.
**Step 5**  In the **Match Criteria List** settings, click **Add**.
**Step 6**  In the **Add Match Criteria** settings, choose the service template from the **Service Template** drop-down list.
**Step 7**  Choose the filters from **Device Type**, **User Role**, **User Name**, **OUI** and **MAC Address** drop-down lists.
**Step 8**  Click **Add Criteria**.
**Step 9**  Click **Apply to Device**.

### 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></td>
<td>enable</td>
</tr>
<tr>
<td>Example:</td>
<td>Device&gt; enable</td>
</tr>
<tr>
<td></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td>Example:</td>
<td>Device# configure terminal</td>
</tr>
<tr>
<td></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>wireless security web-auth retries &lt;number&gt;</td>
</tr>
<tr>
<td>Example:</td>
<td>number is the maximum number of web auth request retries. The valid range is 0 to 20.</td>
</tr>
</tbody>
</table>
Configuring a Local Banner in Web Authentication Page (GUI)

**Procedure**

1. **Step 1**: Choose **Configuration > Security > Web Auth**.
2. **Step 2**: In the **Webauth Parameter Map** tab, click the parameter map name. The **Edit WebAuth Parameter** window is displayed.
3. **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.
4. **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><strong>Example:</strong></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><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device# configure terminal</td>
<td></td>
</tr>
</tbody>
</table>

---

<table>
<thead>
<tr>
<th>PurposeCommand or Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device(config)# wireless security</td>
</tr>
<tr>
<td>web-auth retries 2</td>
</tr>
</tbody>
</table>

**Step 4** end

**Example:**

Device(config)# end

Returns to privileged EXEC mode.
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 3</strong></td>
<td>Enables the local banner.</td>
</tr>
<tr>
<td>`ip admission auth-proxy-banner http [banner-text</td>
<td>file-path]`</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Device(config)# ip admission auth-proxy-banner http C My Switch C</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><code>end</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Device(config)# end</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Verifies your entries.</td>
</tr>
<tr>
<td><code>show running-config</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Device# show running-config</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
<tr>
<td><code>copy running-config startup-config</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Device# copy running-config startup-config</code></td>
<td></td>
</tr>
</tbody>
</table>

### Information About Management over Wireless

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

**Step 1** Choose **Configuration > Wireless > Wireless Global**.

**Step 2** Check the **Management Via Wireless** check box to enable the feature.
Step 3 \quad \text{Click \ Apply.}

---

**Configuring Management over Wireless (CLI)**

**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>Example: Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> [no] wireless mgmt-via-wireless</td>
<td>Enables management access over wireless clients.</td>
</tr>
<tr>
<td>Example: Device(config)# wireless mgmt-via-wireless</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> end</td>
<td>Exits the global configuration mode and returns to the privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 4</strong> show running-config</td>
<td>Verifies the status of management access over wireless clients.</td>
</tr>
<tr>
<td>include mgmt-via-wireless</td>
<td></td>
</tr>
<tr>
<td>Example: Device# show running-config include mgmt-via-wireless</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.

```
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=WNBUS
     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
l=SanJose
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:rkannajrcisc#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
c=US
Subject:
  e=rkannajr@cisco.com
cn=sthaliya-lnx
ou=WNBU
o=Cisco
l=SanJose
st=California
c=US
Validity Date:
  start date: 07:27:56 UTC Jan 31 2012
  end date: 07:27:56 UTC Jan 28 2022
Associated Trustpoints: cert ldap12 ldap
Storage: nvram:rkannajrcisc#0CA.cer

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
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
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
Device(config-params-parameter-map)# 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 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 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.

```plaintext
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:loginsucess.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:loginsucess.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.

```plaintext
Device# configure terminal
Device(config)# wlan fff
Device(config-wlan)# shutdown
Device(config-wlan)# ip access-group web preauthrule
Device(config-wlan)# no shutdown
Device(config-wlan)# end
Device# show wlan name fff
```

**Example: Configuring Webpassthrough**

This example shows how to configure webpassthrough.

```plaintext
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
```