Configuring Web Redirect with 8021.X Authentication

Web Redirect with 802.1X Authentication

You can configure a WLAN to redirect a user to a particular web page after 802.1X authentication has completed successfully. You can configure the web redirect to give the user partial or full access to the network.

This section contains the following subsections:

Conditional Web Redirect

If you enable conditional web redirect, the user can be conditionally redirected to a particular web page after 802.1X authentication has completed successfully. You can specify the redirect page and the conditions under which the redirect occurs on your RADIUS server. Conditions might include the user's password reaching expiration or the user needing to pay his or her bill for continued usage.

If the RADIUS server returns the Cisco AV-pair "url-redirect," then the user is redirected to the specified URL upon opening a browser. If the server also returns the Cisco AV-pair "url-redirect-acl," the specified access control list (ACL) is installed as a preauthentication ACL for this client. The client is not considered fully authorized at this point and can only pass traffic allowed by the preauthentication ACL.

After the client completes a particular operation at the specified URL (for example, changing a password or paying a bill), the client must reauthenticate. When the RADIUS server does not return a "url-redirect," the client is considered fully authorized and allowed to pass traffic.

Note The conditional web redirect feature is available only for WLANs that are configured for 802.1X or WPA+WPA2 Layer 2 security.

After you configure the RADIUS server, you can then configure the conditional web redirect on the controller using either the controller GUI or CLI.

Splash Page Web Redirect

If you enable splash page web redirect, the user is redirected to a particular web page after 802.1X authentication has completed successfully. After the redirect, the user has full access to the network. You can specify the redirect page on your RADIUS server and the corresponding ACL to allow access to this server in "url-redirect-acl". If the RADIUS server returns the Cisco AV-pair “url-redirect,” then the user is redirected to the specified URL upon opening a browser. The client is considered fully authorized at this point and is allowed to pass traffic, even if the RADIUS server does not return a “url-redirect.”

Note The splash page web redirect feature is available only for WLANs that are configured for 802.1X or WPA+WPA2 Layer 2 security with 802.1x key management. Preshared key management is not supported with any Layer 2 security method.

Suppose there are backend applications running on the wireless clients and they use HTTP or HTTPS port for their communication. If the applications start communicating before the actual web page is opened, the redirect functionality does not work with web passthrough.

After you configure the RADIUS server, you can then configure the splash page web redirect on the controller using either the controller GUI or CLI.

Configuring the RADIUS Server (GUI)

Note These instructions are specific to the CiscoSecure ACS; however, they should be similar to those for other RADIUS servers.

Step 1 From the CiscoSecure ACS main menu, choose **Group Setup**.

Step 2 Click **Edit Settings**.

Step 3 From the Jump To drop-down list, choose **RADIUS (Cisco IOS/PIX 6.0)**.

Step 4 Select the **[009\001] cisco-av-pair** check box.

Step 5 Enter the following Cisco AV-pairs in the [009\001] cisco-av-pair edit box to specify the URL to which the user is redirected and, if configuring conditional web redirect, the conditions under which the redirect takes place, respectively:

url-redirect=http://url

url-redirect-acl=acl_name

Configuring Web Redirect

Configuring Web Redirect (GUI)

Step 1 Choose **WLANs** to open the WLANs page.

Step 2 Click the ID number of the desired WLAN. The WLANs > Edit page appears.

Step 3 Choose the **Security** and **Layer 2** tabs to open the WLANs > Edit (Security > Layer 2) page.

Step 4 From the Layer 2 Security drop-down list, choose **802.1X** or **WPA+WPA2**.

Step 5 Set any additional parameters for 802.1X or WPA+WPA2.

Step 6 Choose the **Layer 3** tab to open the WLANs > Edit (Security > Layer 3) page.

Step 7 From the Layer 3 Security drop-down list, choose **None**.

Step 8 Check the **Web Policy** check box.

Step 9 Choose one of the following options to enable conditional or splash page web redirect: **Conditional Web Redirect** or **Splash Page Web Redirect**. The default value is disabled for both parameters.

Step 10 If the user is to be redirected to a site external to the controller, choose the ACL that was configured on your RADIUS server from the Preauthentication ACL drop-down list.

Step 11 Click **Apply** to commit your changes.

Step 12 Click **Save Configuration** to save your changes.

Configuring Web Redirect (CLI)

Step 1 Enable or disable conditional web redirect by entering this command:

config wlan security cond-web-redir {**enable** | **disable**} *wlan_id*

Step 2 Enable or disable splash page web redirect by entering this command:

config wlan security splash-page-web-redir {**enable** | **disable**} *wlan_id*

Step 3 Save your settings by entering this command:

save config

Step 4 See the status of the web redirect features for a particular WLAN by entering this command:

show wlan *wlan_id*

Information similar to the following appears:

```
WLAN Identifier................................ 1
Profile Name................................... test
Network Name (SSID)............................ test
...
Web Based Authentication....................... Disabled
Web-Passthrough................................ Disabled
```

```
Conditional Web Redirect..................... Disabled
Splash-Page Web Redirect..................... Enabled
...
```

Disabling Accounting Servers per WLAN (GUI)

Note Disabling accounting servers disables all accounting operations and prevents the controller from falling back to the default RADIUS server for the WLAN.

Step 1 Choose **WLANs** to open the WLANs page.

Step 2 Click the ID number of the WLAN to be modified. The WLANs > Edit page appears.

Step 3 Choose the **Security** and **AAA Servers** tabs to open the WLANs > Edit (Security > AAA Servers) page.

Step 4 Unselect the **Enabled** check box for the Accounting Servers.

Step 5 Click **Apply** to commit your changes.

Step 6 Click **Save Configuration** to save your changes.

Disabling Coverage Hole Detection per WLAN

Note Coverage hole detection is enabled globally on the controller.

Note You can disable coverage hole detection on a per-WLAN basis. When you disable coverage hole detection on a WLAN, a coverage hole alert is still sent to the controller, but no other processing is done to mitigate the coverage hole. This feature is useful for guest WLANs where guests are connected to your network for short periods of time and are likely to be highly mobile.

This section contains the following subsections:

Disabling Coverage Hole Detection on a WLAN (GUI)

Step 1 Choose **WLANs** to open the WLANs page.

Step 2 Click the profile name of the WLAN to be modified. The WLANs > Edit page appears.

Step 3 Choose the **Advanced** tab to display the WLANs > Edit (Advanced) page.

Step 4 Uncheck the **Coverage Hole Detection Enabled** check box.

Note OEAP 600 Series Access Points do not support coverage hole detection.

Step 5 Click **Apply**.

Step 6 Click **Save Configuration**.

Disabling Coverage Hole Detection on a WLAN (CLI)

Step 1 Disable coverage hole detection on a by entering this command:

config wlan chd *wlan-id* **disable**

Note OEAP 600 Series Access Points do not support coverage hole detection.

Step 2 Save your settings by entering this command:

save config

Step 3 See the coverage hole detection status for a particular WLAN by entering this command:

show wlan *wlan-id*

Information similar to the following appears:

```
WLAN Identifier................................ 2
Profile Name................................... wlan2
Network Name (SSID)............................ 2
. . .
CHD per WLAN................................ Disabled
```