Troubleshoot Common Issues for Web Authentication

Troubleshoot Common Issues for Web Authentication

Custom Web Authentication Login Page Fails to Load

Recommended Solution: When adding the customized HTML files to the webauth bundle, add files one at a time to build the package. Adding files incrementally helps you identify the problem. Also as a best practise, customize a bundle that exists instead of creating a new bundle.

Redirection URL does not Work

Recommended Solution: For any redirection issues in custom WebAuth, Cisco recommends to check the WebAuth bundle which has variable within the bundle that allows the redirection. If you enter a redirect URL with += in the WLC Web UI, this could overwrite or add to the URL defined inside the bundle. For example, in the WLC Web UI, the redirectURL field is set to `www.cisco.com`. However, in the bundle it shows as redirectURL+= 'www.google.com'. The += redirects users to `www.cisco.comwww.google.com`, which is an invalid URL.

Guest users cannot connect to the guest WLAN

Recommended Solution: Check the client configuration and security settings on the WLAN, if enabled. Also check if the radios are active and operative.

Users do not Obtain an IP Address

Recommended Solution: Check the DHCP configuration and connectivity. Check if the other WLANs can use the same DHCP server without any problem.

Redirection to the Web Authentication Login Page Fails

Recommended Solution:

In situations where the redirection to the login page does not happen, check the following:

- If a valid DNS server is assigned to the client through DHCP. Run the command **ipconfig/all** and verify the DHCP and DNS server configurations.

- If the DNS server is reachable from the client. Run the command **nslookup www.website.com** in the Command Prompt/Terminal and check if it returns an IP address for the domain.

- If you have entered a valid URL in order to be redirected. For example, if you have entered http://localhost:2002, the redirection will fail as you have entered port 2002 instead of 80.

In scenarios where the web authentication login page does not display even after redirection takes place, you must check if the firewall installed on the client computer is blocking the login page. Disable the firewall and try to access the login page. The firewall can be enabled after web authentication is complete.

This problem can also arise due to non responsive WLC or due to a problem with TLS handshake for the web authentication page. Capture a sniffer trace on the client computer to check if the WLC responds and tries to redirect. For handshake issues, verify if the security settings of the client browser allow SSLv3, and also how stringent the certificate validation settings are.

After Successful Authentication, Guest Users Fail to Get Access to the Internet

Recommended Solution: Remove WebAuth from the security of the WLAN, and change the guest network status to open, as follows:

1. Choose **Configuration** > **Tags and Profiles** > **WLANs**.

2. Click on the guest WLAN name from the list of WLANs and in the Edit WLAN dialog box, go to the **Security** tab.

3. Under **Layer3** tab, clear the **Web Policy** check box and click **Update & Apply to Device**.

Try accessing the internet and if you still experience issues accessing the network, remove WebAuth settings completely and check the interfaces configuration.

Error Extracting WebAuth Files

Verify if all the HTML files and images required for the customized web page are bundled into a .tar file before uploading to the WLC. Ensure that one of the files included in the .tar bundle is `login.html`.