HOW-TO

ENABLE THE CAPTIVE NETWORK ASSISTANT IN FORTINAC 8.2

DATE: 06.18.2018

VERSION: FortiNAC 8.2 and above

Overview

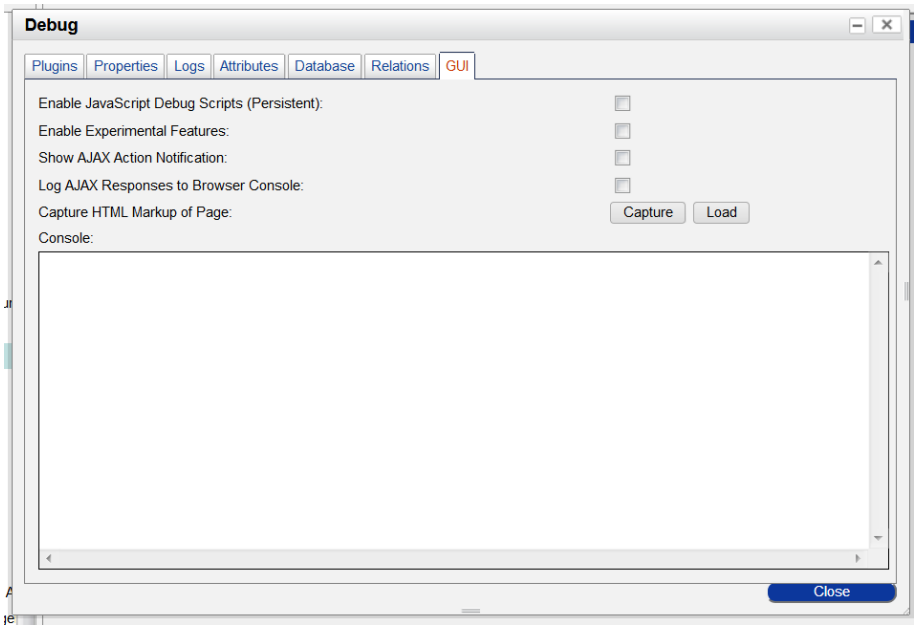
Enabling the Captive Network Assistant (CNA) automatically opens a browser for authentication when a device is isolated. Upon connecting to the network, users will be notified that they are in a Captive Network and must visit the FortiNAC portal to authenticate.

Note the following before enabling CNA:

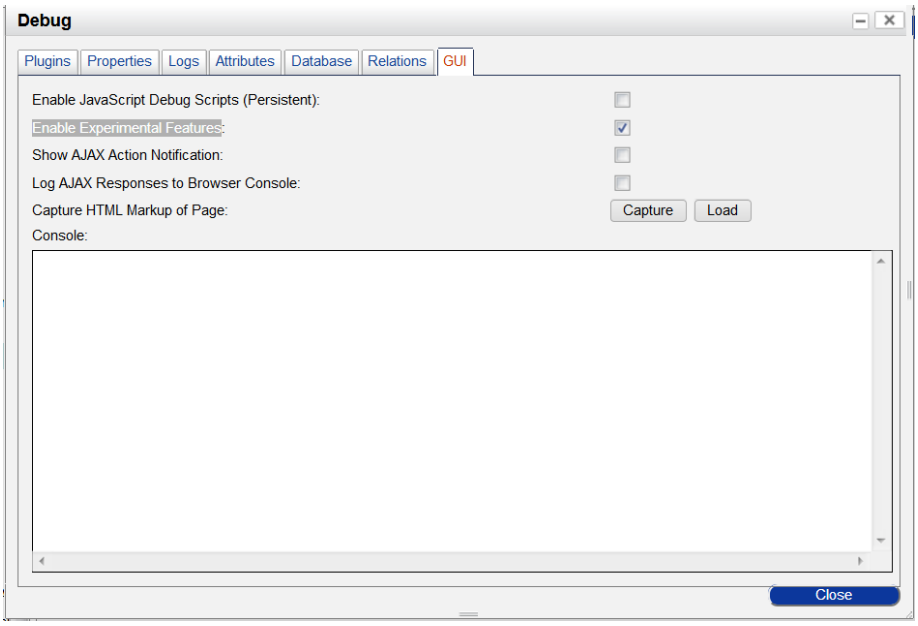
- When CNA is enabled, it is enabled for all portals. It cannot be enabled on a per portal basis.
- The CNA should not be used when using Endpoint Compliance Policies because users cannot download items, such as the agent, from within the CNA.
- CNA implementations vary by vendor. Therefore, domains used to determine whether or not to display the CNA will differ. In addition, the end user experience can vary between vendor and operating systems.
- The CNA only runs a limited scope of Javascript, and HTML requests will not open a new browser window. Clicking a link while using the CNA will result in the current browser window being replaced by the new browser window.
- In order for the CNA to be displayed on iOS and OSX devices, additional FortiNAC configuration is required (see below instrucitons). This is not necessary for any other OS.
- The Allowed Domains (**System > Settings > Allowed Domains**) must not contain any domain that is used by an Operating System where they wish to display the CNA, such as the following:
  Windows: msftncsi.com
  Android: google.com (or clients3.google.com and clients4.google.com)
  iOS/OSX: captive.apple.com, www.apple.com, gsp1.apple.com, akamaiedge.net, akamaitechnologies.com, appleiphonecell.com, www.airport.us, edgekey.net

Enable CNA (iOS and OSX)

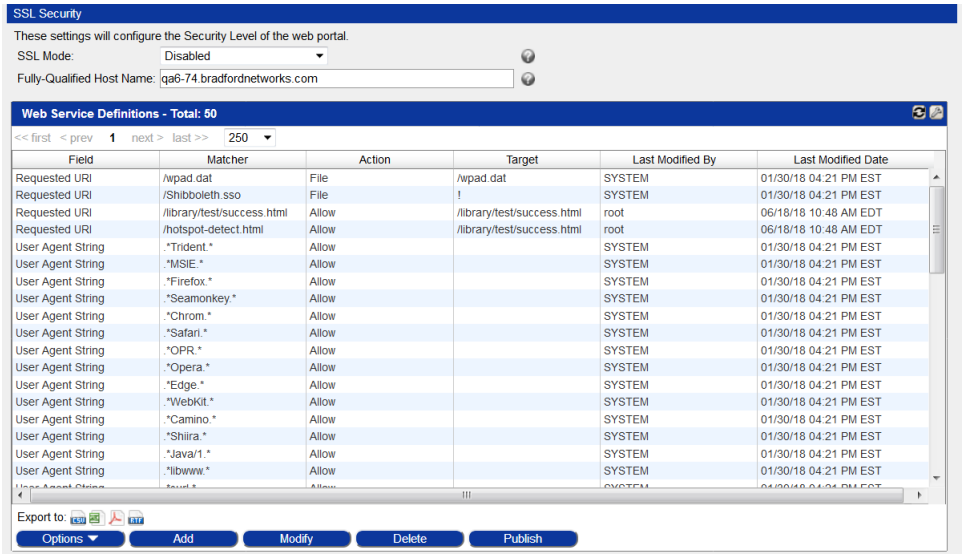
1. Navigate to **System > Settings**, select the Security node, and then select **Portal SSL**.
2. Select **Help > About.**
3. Type **d**



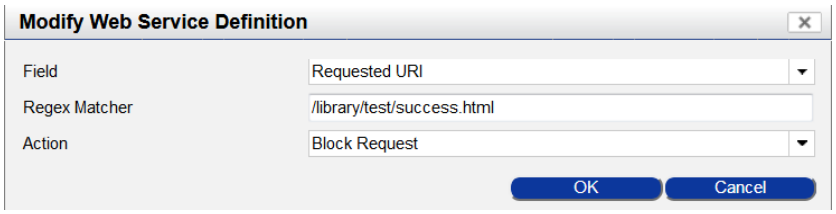
4. Click the **GUI** tab and select the checkbox next to **Enable Experimental Features** and click **Close.**



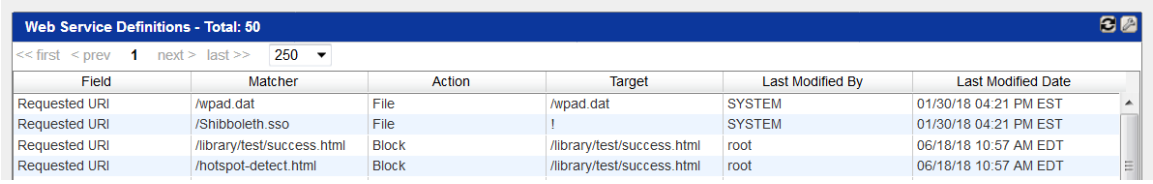
5. Refresh the screen and go back to the **Portal SSL** view.



6. Highlight **/library/test/success.html** (iOS 6 devices and below) and click **Modify**.
7. Change the Action to **Block Request:**



8. Click **OK**.
9. Repeat for **/hotspot-detect.html (**iOS 7 devices and above). The view should now look like the following:

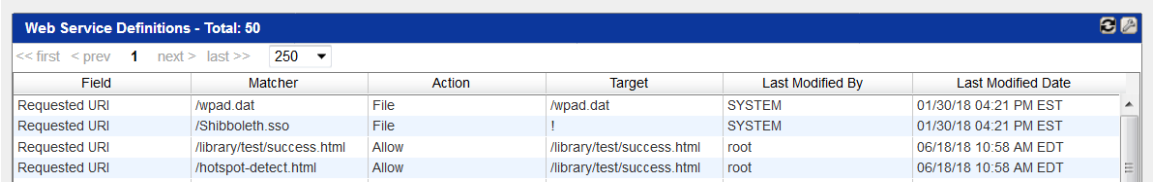


10. Click **Publish.** CNA is now enabled and Apache will no longer capture requests from the CNA.
11. Hide the web services again. **Important:** Web Service Definitions control how FortiNAC responds to devices in the Portal. It is advised that no further edits be made to this view.
    a. Select **Help > About.**
    b. Type **d.**

c. Click the GUI tab and de-select **Enable Experimental Features** and click **Close**.
d. Refresh view to verify the Portal SSL view no longer displays the Web Service Definitions.

Disable CNA (iOS and OSX)

1. Navigate to **System > Settings**, select the Security node, and then select **Portal SSL**.
2. Select **Help > About.**
3. Type **d**
4. Click the **GUI** tab and select the checkbox next to **Enable Experimental Features** and click **Close.**
5. Refresh the screen and go back to the **Portal SSL** view.
6. Highlight **/library/test/success.html** (iOS 6 devices and below) and click **Modify**.
7. Change the Action to **Allow Request.**
8. Click **OK**.
9. Repeat for **/hotspot-detect.html (**iOS 7 devices and above). The view should now look like the following:



10. Click **Publish.** CNA is now disabled.
11. Hide the web services again. **Important:** Web Services controls how FortiNAC responds to devices in the Portal. It is advised that no further edits be made to this view.
    a. Select **Help > About.**
    b. Type **d.**
    c. De-select **Enable Experimental Features** and click **Close**.
    d. Refresh view to verify the Portal SSL view no longer displays the Web Service Definitions.

