HOW-TO

ENABLE THE CAPTIVE NETWORK ASSISTANT

DATE: 11.14.2016

UPDATED: 06.18.2018

VERSION: FortiNAC 8.1 and below

Overview

The Captive Network Assistant (CNA) Operating System feature automatically opens a "pseudo" browser when a device is connected to an isolated network. Upon connecting, users will be notified through the opening of the "pseudo" browser that they are in a Captive Network and must follow the security policy steps required by the FortiNAC portal.

Note the following security policy limitations with CNA:

- Implementations are Operating System vendor specific and vary significantly. Therefore, DNS 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 pseudo browser runs a limited scope of Javascript, and HTML requests will not open a new browser window. Clicking a link in the pseudo browser results in the current browser window being replaced by a new pseudo browser window.

- Pseudo browser does not support download capabilities required for Endpoint Compliance Policies leveraging FortiNAC agents.

- FortiNAC enablement of the CNA feature is global and cannot be enabled on a per portal basis.

- Cannot be used in BYOD Captive Portal environments where any FortiNAC Endpoint Compliance policy requires the use of agent technology.

In summary, the limitations of the CNA pseudo browsers require that all FortiNAC security policies do not include the use of agent technology.

- In order for the CNA to be displayed on iOS and OSX devices, the Enable the Captive Network Assistant option must be selected (see below for instructions). 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

Instructions to Enable CNA (only required for iOS and OSX):

To display the Enable the Captive Network Assistant option in FortiNAC, do the following:

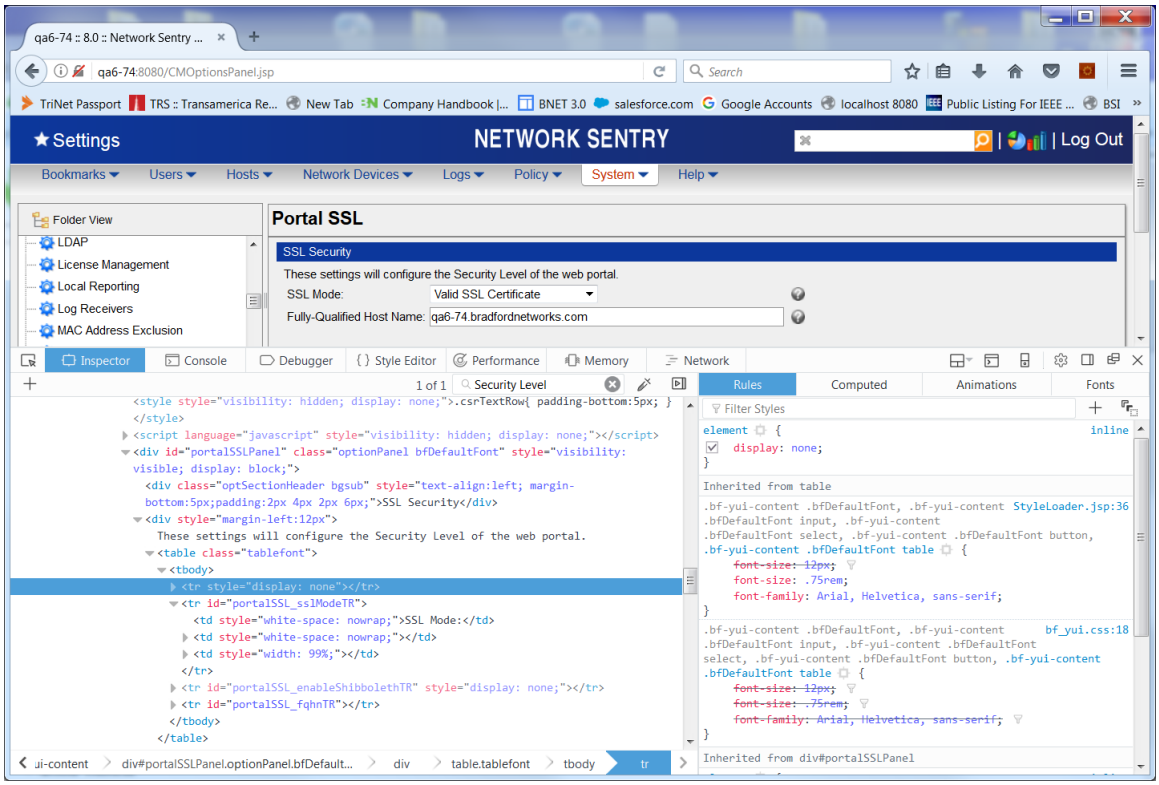
1. Go to **System > Settings**, select the Security node, and then select **Portal SSL**.

2. Right-click next to the **SSL Mode** field, and select **Inspect** from the right-click menu.

3. In the Developer Tool, enter “Security Level” in the search field and enter.

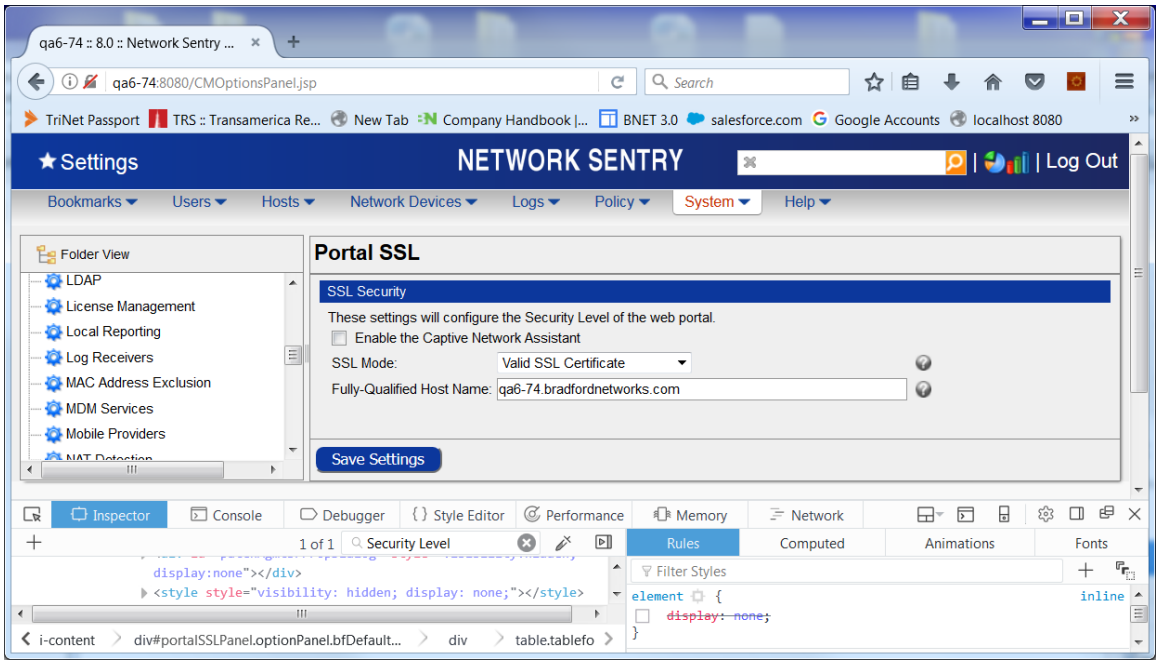
4. Arrow down and select the “**display; none;**” table row style.

5. Hover the cursor next to "display; none;" in the upper right panel. A check box should display (as shown in the following image):



6. Clear the check box. The **display: none;** element style will be crossed-out.

The **Enable the Captive Network Assistant** option will now display in the Portal SSL window.



7. Close the Developer Tool by clicking on the “X” in the upper right corner of the panel.

8. In FortiNAC, select the **Enable the Captive Network Assistant** check box. When enabled, Apache will no longer capture requests from the CNA.