



FortiNAC

Captive Network Assistant Automatic Captive Portal Detection

Version: 8.x

Date: August 16, 2022

Rev: H

FORTINET DOCUMENT LIBRARY

<http://docs.fortinet.com>

FORTINET VIDEO GUIDE

<http://video.fortinet.com>

FORTINET KNOWLEDGE BASE

<https://community.fortinet.com/t5/Knowledge-Base/ct-p/knowledgebase>

FORTINET BLOG

<http://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<http://support.fortinet.com>

FORTINET COOKBOOK

<http://cookbook.fortinet.com>

NSE INSTITUTE

<http://training.fortinet.com>

FORTIGUARD CENTER

<http://fortiguard.com>

FORTICAST

<http://forticast.fortinet.com>

END USER LICENSE AGREEMENT

<http://www.fortinet.com/doc/legal/EULA.pdf>

Contents

Overview	4
What it Does	4
How it Works	4
Launching the Portal	4
Self Registration	5
Requirements	5
Considerations	5
Configuration	6
Procedure	6
Modify Allowed Domains List	6
Enable CNA (iOS/macOS/Samsung Android)	7
Enable Guest Login Menu Option	10
Validate	11
Troubleshooting	12
Related KB Articles	12
Appendix	12
Certificate Error Reference Links	12
Disable CNA	12

Overview

What it Does

Using a Valid SSL Certificate for captive portal security will not completely eliminate certificate errors. If the host requests secure access using a URL such as <https://www.google.com>, the request will be redirected to the captive portal for FortiNAC as <https>. This maintains the <https> security level, but ultimately the certificate name will not match (the request will be for [google.com](https://www.google.com) and the response will be from FortiNAC's address) so there is a trust mismatch and the host will translate this to a possible hijacking attempt.

Alternately, if the host requests secure access using a URL, such as <https://www.google.com>, and if FortiNAC did not maintain the security level of <https> and returned <http> instead, this would lead to an encryption error because the request was <https> and the response was <http>. This general conundrum is well-established among vendors who provide captive portals. See [related links in the Appendix](#).

The only way to avoid such errors would be to ensure the browser attempts access to FortiNAC initially. Captive portal solutions address this issue: once the host is isolated, a browser window is automatically opened with the captive portal page presented.

How it Works

Launching the Portal

When a computer connects to the network, requests are sent to certain sites (depending upon the operating system). If the response is anything other than what is expected, it is assumed there is no internet connection. The captive portal automatically launches (presenting the FortiNAC's portal) and the user is notified that they are in a Captive Network. Once the captive portal launches, the user enters information to register.

There are different captive portal detection solutions depending upon the operating system:

Microsoft and Android - Captive Portal Detection (uses full browser)

iOS and macOS - Captive Network Assistant (CNA) (uses mini browser)

Note the following:

- When enabled, this feature is enabled for all portals. It cannot be enabled on a per portal basis.
- This feature should not be used when using Endpoint Compliance Policies for MAC computers. Since macOS launches a mini browser, users cannot download items, such as the agent, from within the Captive Network Assistant.
- Domains used to determine whether or not to launch the browser will differ (see [Edit the Allowed Domains List](#)). In addition, the end user experience can vary between vendor and operating systems.
- This feature only runs a limited scope of Javascript, and HTML requests will not open a new browser window. Clicking a link while using this feature will result in the current browser window being replaced by the new browser window.

Self Registration

The following process occurs:

1. Captive portal is automatically launched once the endpoint is moved to isolation.
2. User fills in the registration request form.
3. Once the request is submitted, the browser is redirected to the Guest Login page.
4. If sponsor approval is required, the user is notified and provided the appropriate credentials once the request is approved.
5. User enters the credentials in the Guest Login page.

If a wireless connection is dropped, the captive network window may automatically close. Interruptions in connectivity causes the established TCP connection between the host and FortiNAC server to be reset. If this occurs, the captive portal will be redirected to the main Login Menu when the endpoint reconnects to the network. If this occurs, the user can complete the registration process by clicking on the Guest Login option from the main menu. For instructions, see [Enable Guest Login Menu Option](#).

Requirements

- FortiNAC version 8.2 and above
- Valid 3rd party SSL certificate installed for the Portal target. For instructions, refer to the [SSL Certificate](#) cookbook recipe in the Fortinet Document Library.
- Portal page Fully-Qualified Host Name cannot use a “.local” domain. See KB article [191201](#) for details.

Considerations

- Samsung phones with newer Android versions do not automatically launch browser when Captive Network Assistant is enabled. See related KB article [195187](#).

Configuration

Procedure

Modify Allowed Domains List

1. Navigate to **System > Settings > Allowed Domains**
2. Modify the entries as appropriate based on the Operating System:

Windows

Remove:

msftncsi.com

ipv6.msftncsi.com

ipv6.msftncsi.com.edgesuite.net

www.msftncsi.com

www.msftncsi.com.edgesuite.net

teredo.ipv6.microsoft.com

teredo.ipv6.microsoft.com.nsatc.net

Android

Remove:

clients3.google.com

clients4.google.com

connectivitycheck.google.com

connectivitycheck.gstatic.com

iOS/macOS

Remove:

icloud.com

apple.com

akamaiedge.net

akamaitechnologies.com

appleiphonecell.com

www.airport.us

edgekey.net

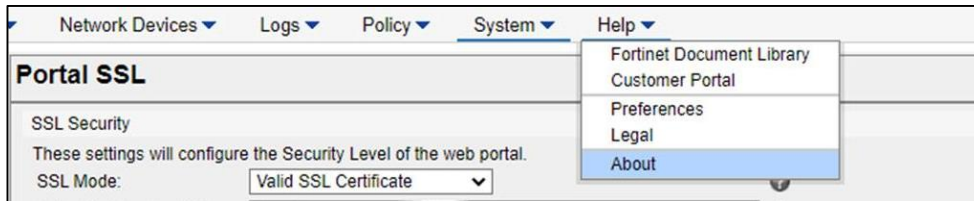
aaplimg.com

akadns.net

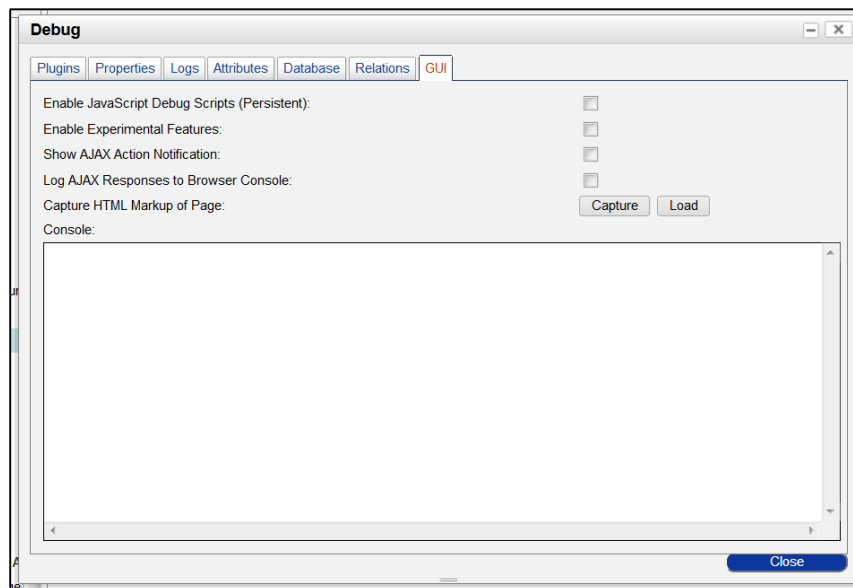
3. Click **Apply**.

Enable CNA (iOS/macOS/Samsung Android)

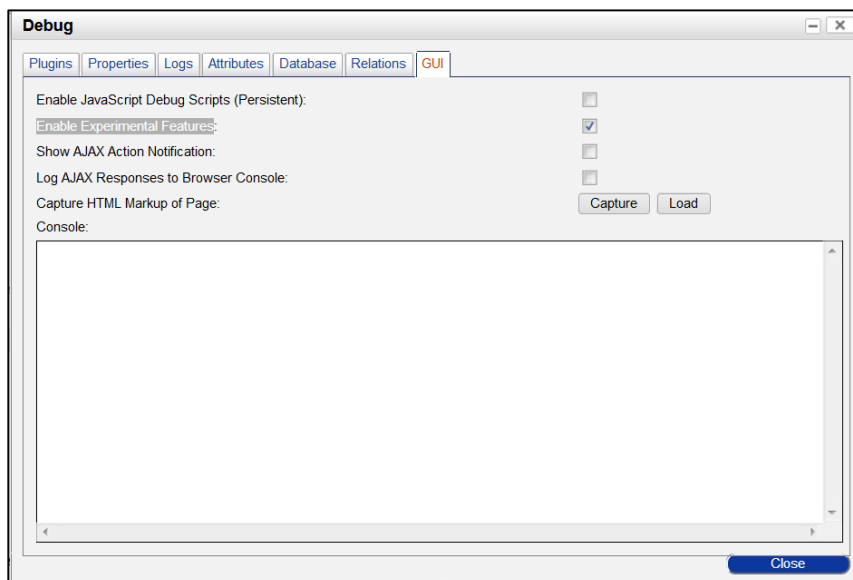
1. Navigate to **System > Settings > Security > Portal SSL**.
2. At the top of the screen, select **Help > About**.



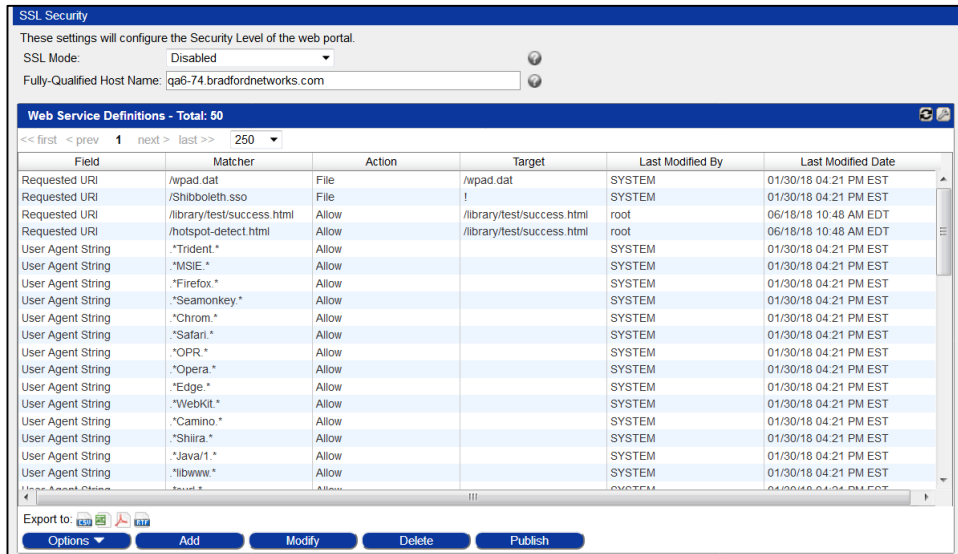
3. Type **d**



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



- Refresh the screen and go back to the **Portal SSL** view. The Web Service Definitions panel should appear:



- Look for entries with the following Matcher values:

`/library/test/success.html`

`/hotspot-detect.html`

`.*gen.*_204.*`

- Highlight the entry and click **Modify**. Edit the entries to match the values in the chart below. If no such entry exists, click **Add** and create the entry.

OS	Field	Regex Matcher	Action	Target
iOS 6 and below	Requested URI	<code>/library/test/success.html</code>	Block Request	N/A
iOS 7 and above	Requested URI	<code>/hotspot-detect.html</code>	Block Request	N/A
Samsung Android	Requested URI	<code>.*gen.*_204.*</code>	Forward to URL	<code>http://<Portal FQDN>/</code>

Examples:

Modify Web Service Definition ✕

Field: Requested URI

Regex Matcher: `/library/test/success.html`

Action: Block Request

Portal SSL	
SSL Security	
These settings will configure the Security Level of the web portal.	
SSL Mode:	Valid SSL Certificate
Fully-Qualified Host Name:	myNAC.mycompany.com

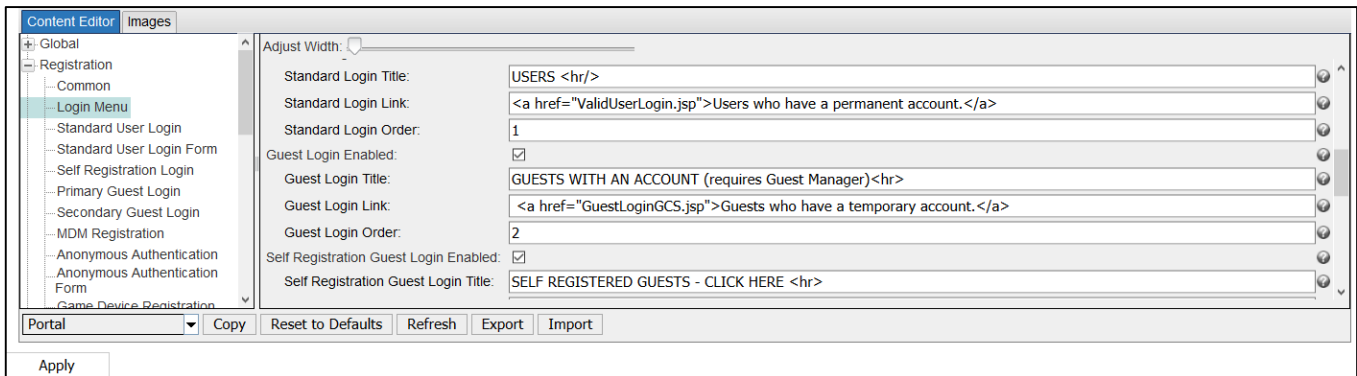
Add Web Service Definition	
Field	Requested URI
Regex Matcher	.*gen.*204.*
Action	Forward to URL
Target	http://myNAC.mycompany.com/
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

8. Click **OK** to save.
9. Once all three entries have been modified, click **Publish** to write the changes to Apache and restart the service.
10. Hide the Web Service Definitions panel. **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.

Enable Guest Login Menu Option

If Self-Registration is used, ensure the Guest Login is accessible from the main Login Menu. This will allow users to register if they have been redirected to the main Login Menu.

1. Navigate to **System > Portal Configuration**.
2. Select the Portal to modify from the portal drop down.
3. In the Content Editor, navigate to **Registration > Login Menu**.
4. Enable by selecting the check box next to **Guest Login Enabled**.

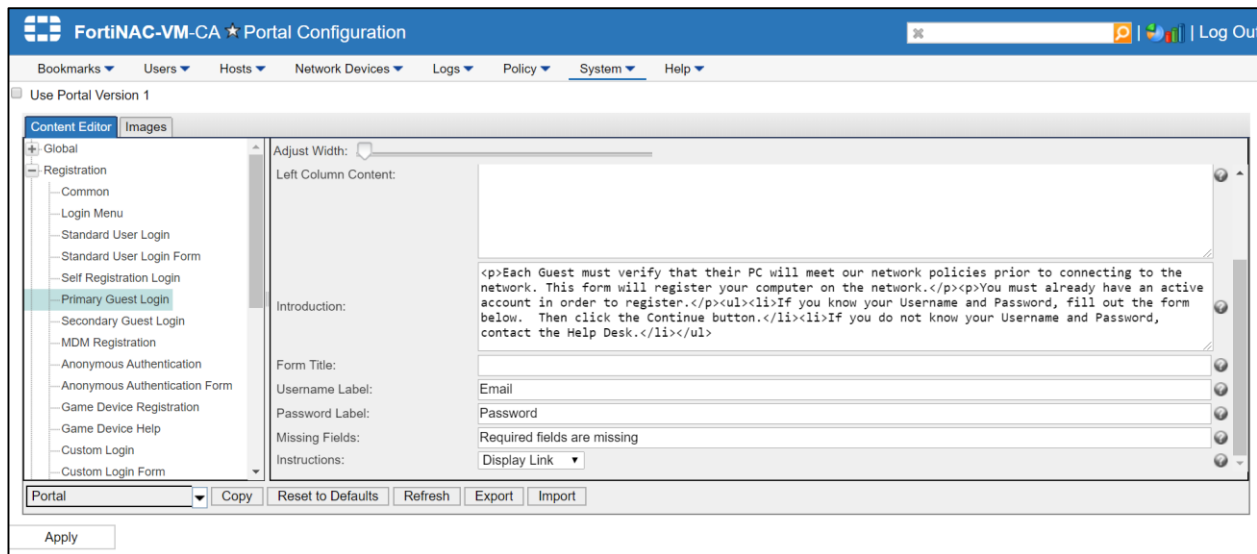


The screenshot shows the 'Content Editor' interface for the 'Login Menu' configuration. The left sidebar shows a tree view with 'Login Menu' selected. The main area contains the following configuration fields:

- Standard Login Title: USERS <hr/>
- Standard Login Link: Users who have a permanent account.
- Standard Login Order: 1
- Guest Login Enabled:
- Guest Login Title: GUESTS WITH AN ACCOUNT (requires Guest Manager)<hr>
- Guest Login Link: Guests who have a temporary account.
- Guest Login Order: 2
- Self Registration Guest Login Enabled:
- Self Registration Guest Login Title: SELF REGISTERED GUESTS - CLICK HERE <hr>

At the bottom, there is a 'Portal' dropdown menu and buttons for 'Copy', 'Reset to Defaults', 'Refresh', 'Export', and 'Import'. An 'Apply' button is located below the main editor area.

5. To modify the content of the guest login page, select “Primary Guest Login” in the content editor.



The screenshot shows the 'Content Editor' interface for the 'Primary Guest Login' configuration. The left sidebar shows a tree view with 'Primary Guest Login' selected. The main area contains the following configuration fields:

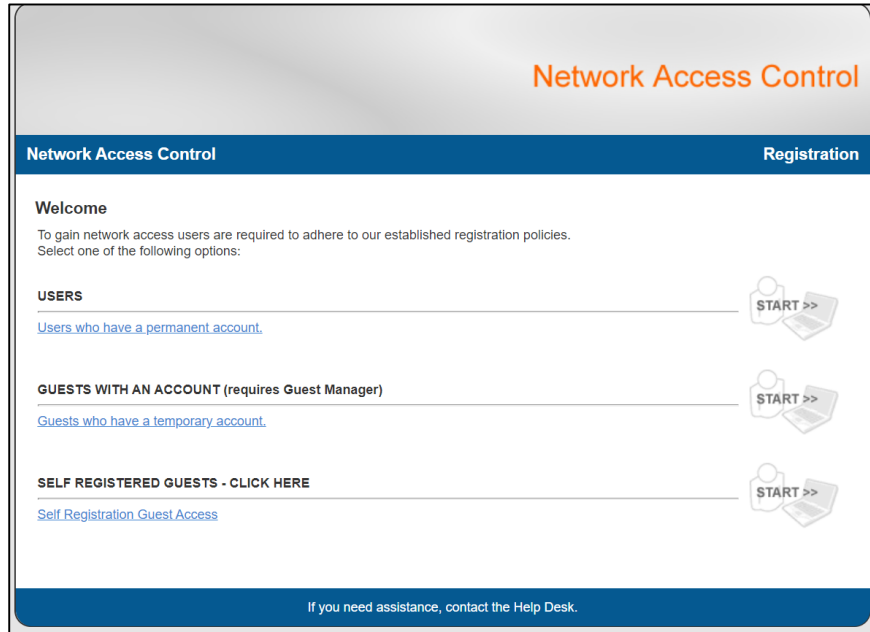
- Left Column Content: (Empty text area)
- Introduction: <p>Each Guest must verify that their PC will meet our network policies prior to connecting to the network. This form will register your computer on the network.</p><p>You must already have an active account in order to register.</p>If you know your Username and Password, fill out the form below. Then click the Continue button.If you do not know your Username and Password, contact the Help Desk.
- Form Title: (Empty text field)
- Username Label: Email
- Password Label: Password
- Missing Fields: Required fields are missing
- Instructions: Display Link

At the bottom, there is a 'Portal' dropdown menu and buttons for 'Copy', 'Reset to Defaults', 'Refresh', 'Export', and 'Import'. An 'Apply' button is located below the main editor area.

6. Click **Apply**.

Validate

1. Connect rogue device and verify popup appears prompting for credentials.
2. If Self-Registration is an option, confirm the Guest Login link is available in the mail Login Menu.



Troubleshooting

Related KB Articles

[Troubleshooting Captive Network Assistant](#)

[Samsung Android Web Service Definition Target URL displays incorrectly](#)

Appendix

Certificate Error Reference Links

<http://serverfault.com/questions/596844/ssl-certificate-errors-in-captive-portals>

<http://forum.m0n0.ch/forum/topic.5988.0.html>

<https://forums.untangle.com/feedback/31539-captive-portal-session-redirect-https.html>

<https://supportforums.cisco.com/discussion/11940491/how-redirect-https-traffic-captive-portal>

Disable CNA

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. The Web Service Definitions panel should appear.
6. Look for entries with the following Matcher values:
/library/test/success.html
/hotspot-detect.html
.*gen.*_204.*
7. Highlight the entry and click **Modify**. Edit the entries to match the values in the chart below.

OS	Field	Regex Matcher	Action	Target
iOS 6 and below	Requested URI	/library/test/success.html	Allow Request	N/A
iOS 7 and above	Requested URI	/hotspot-detect.html	Allow Request	N/A

8. Click **OK** to save.
9. Highlight the entry **.*gen.*_204.*** and click **Delete**.

10. Once all three entries have been modified, click **Publish** to write the changes to Apache and restart the service.
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.
12. Select **Help > About**.
13. Type **d**.
14. De-select **Enable Experimental Features** and click **Close**.
15. Refresh view to verify the Portal SSL view no longer displays the Web Service Definitions.
16. Navigate **System > Settings > Allowed Domains** and undo modifications:

Windows

Add:

msftncsi.com

Android

Add:

clients3.google.com

clients4.google.com

connectivitycheck.google.com

connectivitycheck.gstatic.com

iOS/macOS

Add:

icloud.com

apple.com

akamaiedge.net

akamaitechnologies.com

appleiphonecell.com

www.airport.us

edgekey.net

aapling.com

akadns.net

Contact Support for assistance.



FORTINET[®]



Copyright© 2020 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.