

A decorative pattern of concentric hexagons in a light blue color, scattered across the top dark blue header area.

FortiNAC - Captive Network Assistant Guide

Version 9.4.5

FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO GUIDE

<https://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTINET TRAINING & CERTIFICATION PROGRAM

<https://www.fortinet.com/training-certification>

NSE INSTITUTE

<https://training.fortinet.com>

FORTIGUARD CENTER

<https://www.fortiguard.com>

END USER LICENSE AGREEMENT

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

FEEDBACK

Email: techdoc@fortinet.com

January 17, 2024

FortiNAC 9.4.5 Captive Network Assistant Guide

49-922-769106-20211216

TABLE OF CONTENTS

Overview	4
What it Does	4
How it Works	4
Launching the Portal	4
Self Registration	5
Requirements	5
Considerations	5
Configuration	6
Modify Allowed Domains List	6
Enable CNA (iOS/macOS/Samsung Android)	7
Enable Guest Login Menu Option	8
Validate	9
Troubleshooting	11
Related KB Articles	11
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` 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

Modify Allowed Domains List

1. Navigate to **System > Settings > Control > 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

aapling.com

akadns.net

3. Click **Apply**.

Enable CNA (iOS/macOS/Samsung Android)

1. Navigate to **Portal > Request Processing Rules**.

Field	Matcher	Action	Target
Request URI	/wpad.dat	File	/wpad.dat
Request URI	/Shibboleth.sso	File	!
Request URI	/library/test/success.html	File	/library/test/success.html
Request URI	/hotspot-detect.html	File	/library/test/success.html
HTTP User Agent	.*Trident.*	Allow	
HTTP User Agent	.*MSIE.*	Allow	
HTTP User Agent	.*Firefox.*	Allow	
HTTP User Agent	.*Seamonkey.*	Allow	
HTTP User Agent	.*Chrom.*	Allow	
HTTP User Agent	.*Safari.*	Allow	

2. Look for entries with the following Matcher values:

/library/test/success.html

/hotspot-detect.html

.*gen.*_204.*

3. Highlight the entry and click **Edit**. Edit the entries to match the values in the chart below. If no such entry exists, click **Create New** and create the entry.

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

Examples:

Edit Request Processing Rule

Field
?
Request URI

Matcher
?
/library/test/success.html

Action
?
Block

Portal SSL

SSL Security

These settings will configure the Security Level of the web portal.

SSL Mode: ?

Fully-Qualified Host Name: ?

Edit Request Processing Rule

Field	?	<input type="text" value="Request URI"/>
Matcher	?	<input type="text" value=".*gen.*_204.*"/>
Action	?	<input type="text" value="Forward"/>
Target	?	<input type="text" value="http://myNAC.mycompany.com/"/>

- Click **OK** to save.
- Once all three entries have been modified, click **Publish** to write the changes to Apache and restart the service.

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.

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

Content Editor | Images

Global

- Registration
 - Common
 - Login Menu**
 - Standard User Login
 - Standard User Login Form
 - Self Registration Login
 - Primary Guest Login
 - Secondary Guest Login
 - MDM Registration
 - Anonymous Authentication
 - Anonymous Authentication Form
 - Game Device Registration

Adjust Width:

Standard Login Title:

Standard Login Link:

Standard Login Order:

Guest Login Enabled: ☒

Guest Login Title:

Guest Login Link:

Guest Login Order:

Self Registration Guest Login Enabled: ☒

Self Registration Guest Login Title:

Portal: Copy Reset to Defaults Refresh Export Import

Apply

- To modify the content of the guest login page, select "Primary Guest Login" in the content editor.

FortiNAC-VM-CA Portal Configuration

Bookmarks Users Hosts Network Devices Logs Policy System Help

Use Portal Version 1

Content Editor Images

Global

Registration

- Common
- Login Menu
- Standard User Login
- Standard User Login Form
- Self Registration Login
- Primary Guest Login**
- Secondary Guest Login
- MDM Registration
- Anonymous Authentication
- Anonymous Authentication Form
- Game Device Registration
- Game Device Help
- Custom Login
- Custom Login Form

Adjust Width:

Left Column Content:

Introduction:

Form Title:

Username Label: Email

Password Label: Password

Missing Fields: Required fields are missing

Instructions: Display Link

Portal Copy Reset to Defaults Refresh Export Import

Apply

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.

Network Access Control

Network Access Control

Registration

Welcome

To gain network access users are required to adhere to our established registration policies.
Select one of the following options:

USERS

[Users who have a permanent account.](#)

GUESTS WITH AN ACCOUNT (requires Guest Manager)

[Guests who have a temporary account.](#)

SELF REGISTERED GUESTS - CLICK HERE

[Self Registration Guest Access](#)

If you need assistance, contact the Help Desk.

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 **Portal > Request Processing Rules**.
2. Look for entries with the following Matcher values:
/library/test/success.html
/hotspot-detect.html
.*gen.*_204.*
3. Highlight the entry and click **Edit**. Change 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

4. Click **OK** to save.
5. Highlight the entry **.*gen.*_204.*** and click **Delete**.
6. Once all three entries have been modified, click **Publish** to write the changes to Apache and restart the service.
7. Navigate **Network > Settings > Control > 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
aaplimg.com
akadns.net

Contact Support for assistance.



Copyright© 2024 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.