

Administration Guide

Fortisolator 3.0.1



FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO LIBRARY

<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>

FORTINET TRAINING INSTITUTE

<https://training.fortinet.com>

FORTIGUARD LABS

<https://www.fortiguard.com>

END USER LICENSE AGREEMENT

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

FEEDBACK

Email: techdoc@fortinet.com



December 16, 2025

Fortisolator 3.0.1 Administration Guide

51-301-963196-20251216

TABLE OF CONTENTS

Change log	5
Overview	6
Dashboard	8
Changing system name	8
Configuring system time	8
Changing domain name	9
VM license	9
System configuration	10
Fortisolator certificates	11
Hosts	13
Interfaces	13
System DNS	14
System routing	15
System	19
Administrators	19
Accessing the Fortisolator administration portal	19
Certificates	22
Manage FIS Images	24
Login disclaimer	25
Users	27
SAML servers	27
Setup in FortiAuthenticator	27
Setup in Fortisolator	30
User definition	31
User groups	32
Creating user groups from GUI	32
Creating user groups from CLI	33
Policies and profiles	34
Profile	34
Creating a Isolator browsing profile	34
Creating Web Filter profile	40
Creating ICAP profile	43
Policy	44
Global policy	45
Applying global policy and profile settings	46
Applying profile settings to local user account	49
Applying profile settings to user groups	50
Log	51
ISOLATOR	51
ADMIN GUI	52
Remote Server	52
Settings	53

Running web browsers through Fortisolator	54
IP Forwarding mode	54
Using IP Forwarding mode with Mozilla Firefox	54
Using IP Forwarding mode with Google Chrome	56
Using IP Forwarding mode with Edge	61
Proxy mode	64
Using proxy mode with Mozilla Firefox	65
Using proxy mode with Google Chrome	68
Using proxy mode with Edge	77
Logging in as an end user	79
Copying and pasting text	79
Copying and pasting images	80
Downloading files	80
Adding Web Isolation Profile from Fortisolator to FortiProxy	81
Utilities and diagnostics	87
Utilities	87
Diagnostic tools	87

Change log

Date	Change Description
2025-09-29	Initial release.
2025-10-22	Updated Overview on page 6 .
2025-10-24	Updated Overview on page 6 .
2025-12-16	Updated the following: <ul style="list-style-type: none">• Global policy on page 45• Adding Web Isolation Profile from Fortisolator to FortiProxy on page 81• Configuring system time on page 8• Utilities and diagnostics on page 87.

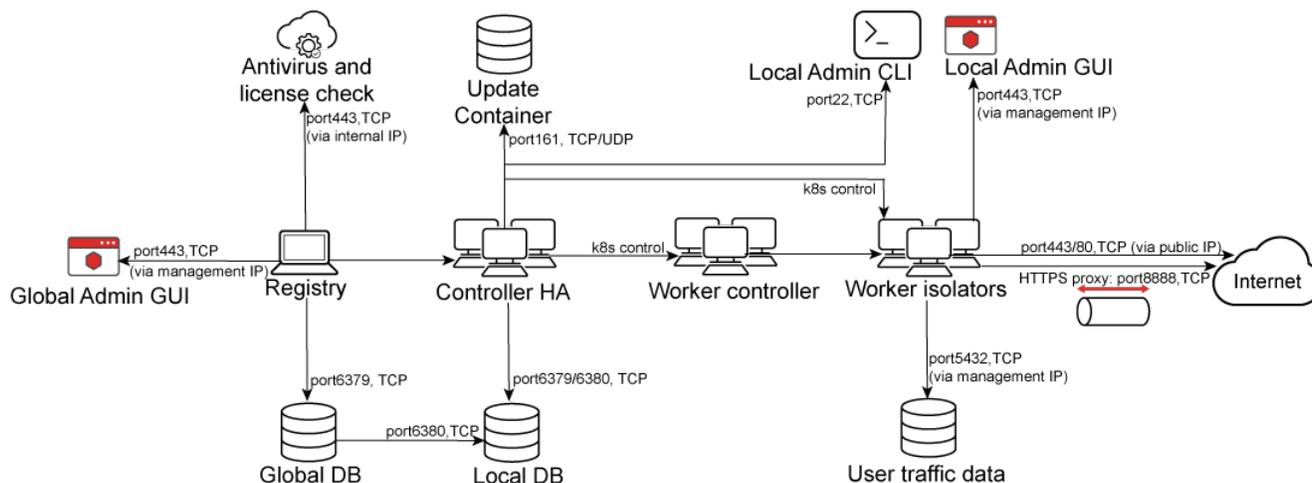
Overview

Fortisolator 3.0.1 is a cloud-based remote browser isolation solution that protects users against zero day malware and phishing threats delivered over the web and email. These threats may result in data loss, compromise, or ransomware. This protection is achieved by creating a visual air gap between users' browsers and websites, which prevents content from breaching the gap. With Fortisolator, web content is executed in a remote disposable container and displayed to users visually, isolating any threat.

The Fortisolator involves the following components:

Component	Description
Registry	Hosting database and all images
Controller HA	Kubernetes control
Worker controller	Web browsing
Worker isolator	Admin GUI, CLI, Kubernetes pods, and supporting containers

The following image illustrates the interaction among the components and the ports used for communication between different components or services.



Fortisolator uses the `fctguard.fortinet.net` server URL to communicate with FortiGuard to query for URL ratings for Web Filter and to download AV and vulnerability scan engine and signature updates.

For more overview information about Fortisolator, see the [Fortisolator product page](#) and the [Fortisolator data sheet](#).

For release information about Fortisolator 3.0.1, such as new features, upgrade instructions, resolved issues, and known issues, see the [Fortisolator Release Notes](#).

For instructions about deploying Fortisolator 3.0.1, refer to the [Fortisolator 3.0 Private Cloud Deployment guide](#).

Dashboard

The Fortisolator dashboard allows you to see information at one glance, including *System Information*, *Host List*, *Service Information*, and so on.

Changing system name

To change the *System Name* from GUI:

1. From the administration portal, click *Dashboard* and find the *System Name* widget.
2. In the *System Name* field, click *Change*.

— System Information

System Name

test [Change]

To change *System Name* from CLI:

```
> set hostname <new_hostname>  
e.g.  
> set hostname test
```



The system name can start with English characters/digits, but must not end with a hyphen. It may contain only the ASCII letters 'a' through 'z' (in a case-insensitive manner), the digits '0' through '9', and the hyphen ('-'). No other symbols, punctuation characters, or white space are permitted.

Configuring system time

To configure time settings for Fortisolator from GUI:

1. From the administration portal, click **Dashboard**, and find the **System Information** widget.
2. In the **System Time** field, click **Change Timezone**.
3. In the **Time Zone** drop-down list, select the time zone.
4. Click *OK*.

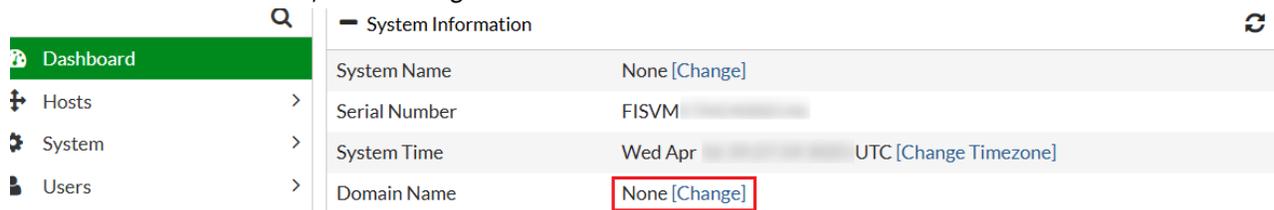
To setup system time from CLI:

```
> set timezone
```

Changing domain name

To change the *Domain Name* from GUI:

1. From the administration portal, click *Dashboard* and locate the *System Information* widget.
2. In the *Domain Name* field, click *Change*.



3. Specify the new domain name and click *Apply* to save the changes.
Domain names are not case-sensitive. Make sure the domain name meets the following requirements:
 - No spaces and or special characters (such as !, \$, &, _)
 - Cannot end with .gov.in
 - Length must be between 3 and 63 characters (excluding extension)

VM license

Fortisolator VM requires a valid license in order to allow all features fully functioning. To obtain a license, please obtain a registration code, go to [Fortinet Service & Support](#) to register the code for Fortisolator VM product, and download the license file.

To upload a license from GUI:

1. From the administration portal, click *Dashboard*, and find the *VM License* widget.
2. In the *VM License* field, click *Upload License*.
3. From *Upload License* page, click *Choose File* to upload the license file.
4. Click *Submit* to finish. This will take several minutes and system will reboot upon finish.



The IP address on the license must to match the Mgmt-ip in the Fortisolator.

Upon completion when the license is successfully uploaded, there will be a green checkmark next to VM License on Dashboard, indicating the license is valid. Mousing over this checkmark shows more details of the license, such as its expiration date.

System configuration

You can back up the system before any major updates and restore it later. You can also migrate the configuration from a previous version (2.4.x or 3.0.x) using a backup file (.tar.xz) from that version and restore it.

The current version of Fortisolator is available for system backup/migration and restore through GUI only.

Backing up and restoring the system

Once you successfully configure the Fortisolator, back up the system after any changes are made to ensure you have the most current configuration available. System backup is especially important in the following cases when the configuration on the device will have to be recreated unless a backup can be used to restore it.

- When you need to reset the Fortisolator to factory defaults or perform a TFTP upload of the firmware, which will erase the existing configuration.
- When you upgrade the Fortisolator firmware—Should anything happen to the configuration during the upgrade, you can easily restore the saved configuration.

To back up the configuration:

1. From the administration portal, click *Dashboard*, and find the *System Configuration* widget.
2. In the *System Configuration* field, click *Backup/Download Config File*.
3. In the *Backup* section of the *System Backup* page, *Click here* to download the backup file (.tar.xz) to your local system.
You can save the backup file to various locations including the local PC and USB key. Always back up the system and store it on the management computer or off-site.
4. To restore the configuration, upload the backup file in the *Restore* section and click *Restore*, which will reboot the Fortisolator.

Migrating the system configuration from earlier versions

While Fortisolator 3.0.1 does not support direct upgrade from any earlier versions, you can migrate your configuration data from 2.4.x or 3.0.0 to 3.0.1 using a backup file from that version and restore it.

To migrate the system configuration from earlier versions:

1. From the administration portal, click *Dashboard*, and find the *System Configuration* widget.
2. In the *System Configuration* field, click *Backup/Download Config File*.
3. In the *Migration* section of the *System Backup* page, *Choose File* to upload the system backup file (.tar.xz) from earlier versions and click *Restore*.
This will restore the configuration of your local system to the previous version.

Fortisolator certificates

The Fortisolator CA certificate is required for access to the Fortisolator. By default, the Fortisolator uses the built-in CA certificate. You can also generate or upload a custom CA certificate to meet your needs. However, you can revert to the default CA certificate anytime.

The CA certificate auto-generates a matching server certificate for accessing the Fortisolator database and a matching management certificate for accessing the Fortisolator GUI. For custom CA certificates, you can also upload a custom server or management certificate that is a match of the custom CA certificate.

By default, the CA certificate must be installed on each device that uses the Fortisolator to visit websites unless you use a global CA certificate that grants global access to websites at browser level.



Fortisolator only supports “Base-64 encoded X.509 (.cer)” format certificates.

To back up, restore, generate, or upload a specific certificate, click *Dashboard* in the administration portal and click the *Backup/Restore* link near *Isolator CA Certificate* in the *System Information* widget, which redirects to the *Isolator CA Certificate* page:

To revert to the default CA certificate:

1. In the *Re-Generate Isolator CA certificate* section, click the link in *Click here to generate Default CA certificate*.

The default CA Certificate will be restored and the Fortisolator will reboot, which might take a few minutes.

To use a custom-generated CA certificate:



If you use a non-default CA certificate, Fortinet recommends that you back up the current CA certificate (see section below) before switching to a new one.

1. In the *Re-Generate Isolator CA certificate* section, click the link in *Click here to generate CA certificate*.
2. Specify the values of the certificate attributes and click *OK*. Bold indicate required attributes.

To back up the current CA certificate:

1. In the *Backup CA certificate* section, click the link in *Click here to save your backup file* to save your backup file.

This will save *ca.tgz* file into your local system; you can store it in a secure place for when you need to restore the system.

To use a local CA certificate:



If you use a non-default CA certificate, Fortinet recommends that you back up the current CA certificate (see section above) before switching to a new one.

1. Depending on the file type of the local certificate, go to the *Restore CA certificates by tgz file* or *Restore CA certificates by files* section.
2. Click *Choose File* to upload the local CA certificate file(s).
3. Specify the password(s), if any.
4. Click *Restore*.
5. Click *OK*.

The local CA certificate will be used and the Fortisolator will be rebooted, which might take a few minutes. If the CA certificate is a global CA certificate that grants global access to websites at browser level, follow the next two sections to upload the corresponding server certificate and management certificate for the whole certificate chain to work.

To use a local server certificate:

1. In the *Restore Server certificates by files*, click *Choose File* to upload the certificate and key. Make sure the server certificate is a match of the current CA certificate.
2. Specify the password and domain name, if any.
3. Click *Restore*.
4. Click *OK*.

The local server certificate will be used and the Fortisolator will be rebooted, which might take a few minutes.

To use a local management certificate:

1. In the *Restore Management certificates by files*, click *Choose File* to upload the certificate and key. Make sure the management certificate is a match of the current CA certificate.
2. Click *Restore*.
3. Click *OK*.

The local management certificate will be used and the Fortisolator will be rebooted, which might take a few minutes.

Hosts

Use this tab to view the network of each host, such as interface, system DNS, and system routing information. To configure the network of each host, visit the maintenance GUI and

The default IP address of the Fortisolator management interface is 192.168.1.99. To perform the initial configuration, connect a device to the management interface and configure the device with an IP address to 192.168.1.0/24 subnet. You can access Fortisolator using SSH or the Fortisolator GUI. The default username is admin and the default password is fortinet.

Interfaces

Physical and virtual interfaces allow traffic to flow between internal networks, and between the internet and internal networks. Fortisolator has options for setting up interfaces and groups of subnet works that can scale as your organization grows.

Setting the management IP address

The default management interface on Fortisolator is set to 192.168.1.99. To change the Management IP address from GUI:

1. Go to *Hosts > Interfaces*.
2. Edit the existing Gateway or create a new one.
3. Select mgmt. interface and then edit it.
4. Follow IPv4 address with subnet format: e.g. 192.168.1.99/255.255.255.0.

To change the Management IP address from CLI, use the following command:

```
> set mgmt-ip <ip_address>/<subnet_mask>  
e.g.  
> set mgmt-ip 192.168.1.99/24
```

Setting the internal IP address and gateway

There is no default Internal interface on Fortisolator. To setup the internal IP address from GUI:

1. Go to *Hosts > Interfaces*.
2. Select Internal interface and then edit it.
3. Follow IPv4 address with subnet format: e.g. 192.168.2.99/255.255.255.0.

To change the internal IP address from CLI, use the following command:

```
> set internal-ip <ip_address>/<subnet_mask>  
e.g.  
> set internal-ip 192.168.2.99/24
```

Setting the external IP address and gateway

There is no default external interface on Fortisolator. To setup the external IP address from GUI:

1. Go to *Hosts > Interfaces*.
2. Select External interface and then edit it.
3. Follow IPv4 address with subnet format: e.g. 192.168.3.99/255.255.255.0.

To change the external IP address from CLI, use the following command:

```
> set external-ip <ip_address>/<subnet_mask>
e.g.
> set external-ip 192.168.3.99/24
```

Setting the HA IP address and gateway

There is no default HA interface on Fortisolator. To setup the HA IP address from GUI:

1. Go to *Hosts > Interfaces*.
2. Select HA interface and then edit it.
3. Follow IPv4 address with subnet format: e.g. 192.168.4.99/255.255.255.0.

To change the HA IP address from CLI, use the following command:

```
> set ha-ip <ip_address>/<subnet_mask>
e.g.
> set ha-ip 192.168.3.99/24
```

System DNS

To setup system DNS from GUI:

1. Go to *Hosts > System DNS*.
2. Fill out *Primary DNS Server* and *Secondary DNS Server*:

DNS Configuration	
Primary DNS Server:	<input type="text" value="8.8.8.8"/>
Secondary DNS Server:	<input type="text" value="208.91.112.53"/>

To setup system DNS from CLI:

```
> set dns <Primary DNS Server> <Secondary DNS Server>
e.g.
> set dns 8.8.8.8 208.91.112.53
```

System routing

Configuring routing settings

Use this procedure to configure routing settings for Fortisolator.

Adding a static route

To add a static route:

1. From the administration portal, go to *Network > System Routing*.
2. To add a new static route, click *Create New*.
3. Type the destination IP address and subnet mask in the *Destination IP/Mask* field.
4. Type the gateway IP address in the *Gateway* field.
5. In the *Device* drop-down list, select the interface for the static route.
6. Click *OK*.

Editing a static route

To edit a static route:

1. From the administration portal, go to *Network > System Routing*.
2. To edit an existing static route, select the interface in the table, and click *Edit*.
3. Type the destination IP address and subnet mask in the *Destination IP/Mask* field.
4. Type the gateway IP address in the *Gateway* field.
5. In the *Device* drop-down list, select the interface for the static route.
6. Click *OK*.

Deleting a static route

To delete a static route:

1. From the administration portal, go to *Network > System Routing*.
2. To delete a static route, select the interface in the table, and click *Delete*.

Setting up system routing for management IP

To set up system routing for management IP from GUI:

1. Go to *Portal > Network > System Routing*.
2. Fill out *Destination IP/Mask*, *Gateway*, and select *mgmt.* from the *Device* dropdown.

3. Click *OK* to save it.

New Static Route	
Destination IP/Mask:	<input type="text" value="0.0.0.0"/>
Gateway:	<input type="text" value="192.168.1.254"/>
Device:	<input type="text" value="mgmt"/>

To set up system routing for management IP from CLI:

```
> set mgmt-gw/<subnet> <gateway>  
e.g.  
> set mgmt-gw 192.168.0.0/24 192.168.0.254
```

Setting up system routing for internal IP

To set up system routing for internal IP from GUI:

1. Go to *Portal > Network > System Routing*.
2. Fill out *Destination IP/Mask*, *Gateway*, and select *Internal* from the *Device* dropdown.
3. Click *OK* to save it.

New Static Route	
Destination IP/Mask:	<input type="text" value="0.0.0.0"/>
Gateway:	<input type="text" value="192.168.2.254"/>
Device:	<input type="text" value="internal"/>

To set up system routing for internal IP from CLI:

```
> set internal-gw/<subnet> <gateway>  
e.g.  
> set internal-gw 0.0.0.0/0 172.30.156.254
```

To setup system routing for external IP from GUI:

1. Go to *Portal > Network > System Routing*.
2. Fill out *Destination IP/Mask*, *Gateway*, and select *External* from the *Device* dropdown.
3. Click *OK* to save it.

New Static Route	
Destination IP/Mask:	<input type="text" value="0.0.0.0"/>
Gateway:	<input type="text" value="192.168.3.254"/>
Device:	<input type="text" value="external"/>

To set up system routing for external IP from CLI:

```
> set external-gw/<subnet> <gateway>
e.g.
> set external-gw 172.30.157.0/24 172.30.157.254
```

To set up system routing for HA IP from GUI:

1. Go to *Portal > Network > System Routing*.
2. Fill out *Destination IP/Mask*, *Gateway*, and select *HA* from *Device* dropdown.
3. Click *OK* to save it.

Edit Static Route	
Destination IP/Mask:	<input type="text" value="0.0.0.0/0"/>
Gateway:	<input type="text" value="192.168.4.254"/>
Device:	<input type="text" value="ha"/>

To set up system routing for HA IP from CLI:

```
> set ha-gw/<subnet> <gateway>
e.g.
> set ha-gw 192.168.4.0/24 192.168.4.254
```

Configuring multiple routing on one interface

Fortisolator supports multiple routes per interface.

Setting up multiple routes on one interface from CLI

Creating Fortisolator profile from CLI needs to follow this format:

```
> set <gateway> <SUBNET> <Gateway IP>
```

```
internal-gw <SUBNET> <Gateway IP>
e.g. 192.168.100.0/24 192.168.100.1
```

```
external-gw <SUBNET> <Gateway IP>
e.g. 192.168.100.0/24 192.168.100.1
```

```
mgmt-gw <SUBNET> <Gateway IP>
e.g. 192.168.100.0/24 192.168.100.1
```

```
ha-gw <SUBNET> <Gateway IP>
e.g. 192.168.100.0/24 192.168.100.1
```

Example:

```
> set ha-ip 192.168.122.20/23
> set ha-gw 192.168.122.0/24 192.168.122.254
> set ha-gw 192.168.123.0/24 192.168.123.254
```

```
> show
*****Configured parameters*****
```

```
[Routing Entries]
| SUBNET                GATEWAY                INTERFACE
-----
192.168.122.0/24       192.168.122.254       ha
192.168.123.0/24       192.168.123.254       ha
```

To set multiple routes on one interface from GUI:

1. Go to *Network > System Routing*.
2. Click *Create New* in the toolbar. The *New Static Route* page opens.
3. Provide *Destination, IP/Mask, Gateway, and Device*.
4. Click *OK* to save the input and return to *System Routing* page.

System

The *System* section of Fortisolator covers the following:

- Administrators
- Certificates
- Manage FIS Images
- Login disclaimer

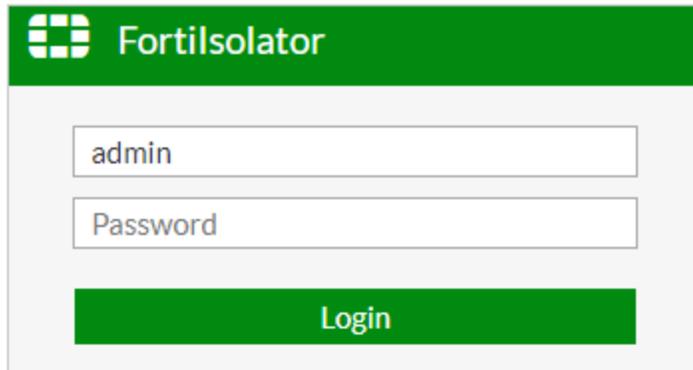
Administrators

Accessing the Fortisolator administration portal

Logging in as administrator

To log in as an administrator:

1. Open a web browser and go to `http://<management IP address>`, where `<management IP address>` is the IP address that you configured for the administrator management portal interface. The default is 192.168.1.99.



The screenshot shows the Fortisolator login interface. It features a green header bar with the Fortisolator logo and the text 'Fortisolator'. Below the header, there is a light gray background containing two input fields. The first field is labeled 'admin' and the second is labeled 'Password'. At the bottom of the form, there is a prominent green button labeled 'Login'.

2. Type in your username and password to access the administration portal. For the first login from a fresh installation, use the default username and password `admin/fortinet`.
3. If prompted, change the default password to include at least 8 characters covering all of the following categories:
 - Uppercase letters (A through Z)
 - Lowercase letters (a through z)
 - Base 10 digits (0 through 9)
 - Non-alphanumeric characters (special characters): `'-!"#$%&()* ,./:;?@[]^_`{|}~+<=>`



4. If you changed the default password in the previous step, click *Submit* and enter the new password.
5. Click *Login*. You will be brought to the dashboard of the administration portal.

To log in as an administrator without an administrator password:

1. Ensure you have the Fortisolator VM license number.
2. Use the maintainer account to log into the Fortisolator console:
 - **Account name:** maintainer
 - **Password:** bcpb plus the Fortisolator serial number or license number, for example: bcpbFIS*****.



The window for entering the maintainer account name and password is 60 seconds, after which you will have to reboot the Fortisolator to be able to log in again. It is recommended that you have the credentials ready in a text editor to copy and paste into the login screen when required. There is no indicator of when the time runs out so it might take more than one attempt to succeed.

Changing the administrator password

To change the administrator password:

1. In the top-right corner of the administration portal, click the admin username.
2. Click *Change Password*.
3. In the *Password* field, type the new password with at least 8 characters covering all of the following categories:
 - Uppercase letters (A through Z)
 - Lowercase letters (a through z)
 - Base 10 digits (0 through 9)
 - Non-alphanumeric characters (special characters): '-! "\$%&()* ,./:;?@[]^_`{|}~+<=>
4. In the *Confirm Password* field, type the new password again.
5. Click *OK*.

To change the administrator password without an administrator password:

1. Ensure you have the Fortisolator VM license number.
2. Log into the Fortisolator console using the maintainer account:
 - **Account name:** maintainer
 - **Password:** bcpb plus the Fortisolator serial number or license number, for example: bcpbFIS*****.



The window for entering the maintainer account name and password is 60 seconds, after which you will have to reboot the Fortisolator to be able to log in again. It is recommended that you have the credentials ready in a text editor to copy and paste into the login screen when required. There is no indicator of when the time runs out so it might take more than one attempt to succeed.

3. Reset the administrator password using the `admin-pwd-reset` command.
4. Reboot the Fortisolator.

Setting up guest administrator account

A guest administrator account is an account with read-only access to the administration portal. The guest user can view, but not edit, the settings and logs in the administration portal.

To set up a guest administrator account:

1. Within the administration portal, go to *System > Administrators* and double-click the *guest* Administrator row, or select the *guest* Administrator row and click *Edit*.
2. The guest administrator account has a preset username of *guest*. You must set up a password.

The screenshot shows the Fortisolator VM administration portal. The top navigation bar is red with the Fortisolator logo and 'VM' on the left, and 'admin' on the right. A search icon is in the center. The left sidebar contains a menu with items: Dashboard, Network, System (expanded), Administrators (highlighted), HA, Login Disclaimer, Upgrade, Users, Policies and Profiles, and Log. The main content area is titled 'Edit Administrator' and contains three input fields: 'Administrator:' with the value 'guest', 'Password:', and 'Confirm Password:'. A green 'OK' button is at the bottom right of the form.

3. Click *OK* to save and apply the settings.

Certificates

The Fortisolator allows users to use self-signed SSL certificates for a specific server or website. Generally, self-signed certificates are very specific and often used for an internal enterprise network. In this page you can import certificates for different purposes.



Fortisolator only supports “Base-64 encoded X.509 (.cer)” format certificates.

To import a certificate:

1. Go to *System > Certificates*. The page shows the types of certificates that you can import.
2. Click *Import* in the toolbar. The *Import Certificate* page opens.
3. Specify *Certificate Name*.
4. Under *Type*, select the type of certificate you are importing.

Option	Certificate Type	Description
<i>LOCAL_CERT</i>	Local Certificate	This option allows users to import a customized local certificate to replace the built-in Isolator CA Certificate. If no local certificate is available, Fortisolator uses the built-in Isolator CA Certificate.
<i>SAML_CERT</i>	SAML Certificate	Certificate for single-sign-on which is created in <i>Users > Server > Create New > SAML Server</i> .
<i>SELF SIGNED CA ROOT CERT</i>	Self Signed CA root Certificate	This option allows the user to upload a self-signed CA root Certificate, which is the origin of a certificate chain that all subordinate certificates stem from. A <i>root_ca.crt</i> file should be uploaded here.



The certificate chain must be complete for the certificate to work. You must also upload the relevant subordinate certificates under the *INTERMEDIATE CA CERT* option.

Option	Certificate Type	Description
<i>INTERMEDIATE CA CERT</i>	Intermediate CA Certificate	This option allows the user to upload subordinate certificates of the root certificate on the Fortisolator. Subordinate certificates must be uploaded along with the trusted root certificate (<i>root_ca.crt</i>) and upper level subordinate certificates (<i>sub_ca.crt</i>) in the certificate chain, along with the key files (<i>sub_ca.key</i>) if necessary. When the certificate chain is complete, which means the root certificate and all relevant subordinate certificates are uploaded, the user only needs to import the lowest level subordinate certificate in the browser.
<i>SELF SIGNED SERVER CERT</i>	Self-signed Server Certificate	A standalone certificate used by the original issuer to verify if a site is legitimate.

5. Enable the *PKCS12 Format* checkbox if it is a PKCS12 certificate.
6. Click *Choose File* to upload a certificate file.
7. Click *Choose file* to upload a key file.
8. Enter the password of the certificate.
9. Click *OK* to return to the certificates list.
10. (Optional) Select the row of the certificate type and click *View* to verify the certificate details.

To view a certificate's details:

1. Go to *System > Certificates*.
2. Select the certificates you need to see details about.
3. Click *View*.

To delete a certificate:

1. Go to *System > Certificates*.
2. Select the certificate you need to delete.
3. Click *Delete* in the toolbar.
4. Click *OK* in the confirmation dialog box to delete the selected certificate.



The Isolator CA Certificate is built-in and cannot be deleted. It takes effect when no local certificate is available.

To assign a certificate to user's profile:

1. Go to *Policies and Profile > Profile*.
2. Select *Isolator profile* and *Edit*.

3. On the bottom of the page, next to *Certificates*, select the certificate that you just imported and click *OK*.
4. Go to *Policies and Profile > Global Policy*, select the profile for Default Isolator Profile, and click *OK*.



If a self-signed SSL certificate is a certificate chain that contains a root certificate and subordinate certificates, both the root certificate and all subordinate certificates must be imported into the Fortisolator and selected in the user's profile.

To regenerate a Fortisolator CA Certificate:

1. Go to *Dashboard > Fortisolator CA Certificate*.
2. Click *Backup/Retore*.
3. Proceed with either of the following options, depending on the type of certificate you are regenerating:
 - To generate a certificate with the default settings, click the link in *Click here to generate Default CA certificate*. The Fortisolator reboots, which takes a few minutes.
 - To generate a certificate with customized settings, click the link in *Click here to generate CA certificate*. Specify the settings and click *OK*.



Once a Fortisolator certificate has been generated or re-generated, it will replace the existing one.

Manage FIS Images

As part of the environment setup while deploying your Fortisolator (see [Fortisolator 3.0 Private Cloud Deployment guide](#)), you must manually upload the following package files in the *System > Manage FIS Images* page for full Fortisolator functionality, such as `fis_wf` for web filtering.

Package file	Purpose	FIS Image
FIS_auth_DOCKER-v3-build0117.xz	SAML authentication via FortiAuthenticator	fis_auth
FIS_fisfs_DOCKER-v3-build0117.xz	Web browsing	fis_fis
FIS_log_DOCKER-v3-build0117.xz	Log collection and management.	fis_log
office-1.6.tar.gz	Microsoft Office file viewing (.doc, .docx, .xls, .xlsx, .ppt)	fis_office
FIS_postgres_DOCKER-v3-build0117.xz	Database support for browsing data storage	fis_postgres
FIS_update_DOCKER-v3-build0117.xz	Antivirus and license check	fis_update
FIS_wf_DOCKER-v3-build0117.xz	Web filtering	fis_wf

Package file	Purpose	FIS Image
	For instructions about downloading these package files, see Downloading the Fortisolator firmware and package files in the Fortisolator 3.0 Private Cloud Deployment guide.	

To upload a package:

1. Go to *System > Manage FIS Images*.
2. In the *Upload Images* section, click *Choose File*.
3. Select the package file and click *Open*.
4. Click *Upload* and then *OK* to confirm.
5. After the upload is complete, verify that the package appears in the image table with the correct version.
6. Click *Apply* in the corresponding package row to use the newly uploaded package.
7. Verify that the state of the package changes to *In Use*.
8. **(Optional)** Delete any existing old packages in the package table that are not in use and you no longer need.

Sample view of a Microsoft Office document in Fortisolator:



Login disclaimer

To configure the login disclaimer:

1. Go to *System > Login Disclaimer*.
2. Enter desired disclaimer and check the box next to *Show disclaimer on login* if you would like the disclaimer to be displayed to the end user upon logging in.

The screenshot shows the Fortisolator VM administration interface. The top header is green with the Fortisolator logo and 'VM' on the left, and 'admin' on the right. A search bar is present. The left sidebar contains a menu with categories: Dashboard, Network, System (expanded), Login Disclaimer (selected), Upgrade, Install Package, Diagnose, Users, Policies and Profiles, and Log. The main content area is titled 'Login Disclaimer' and contains a text area for the disclaimer, a checkbox for 'Show disclaimer on login', and an 'OK' button.

Fortisolator VM admin

Search

Dashboard

Network

System

- Administrators
- HA
- Certificates
- SNMP

Login Disclaimer

- Upgrade
- Install Package
- Diagnose

Users

Policies and Profiles

Log

Disclaimer:

PREWARNINGWARNINGWARNINGWARNING
This is a private computer system. Unauthorized access or use is prohibited and subject to prosecution and/or disciplinary action. All use of this system constitutes consent to monitoring at all times and users are not entitled to any expectation of privacy. If monitoring reveals possible evidence of violation of criminal statutes, this evidence and any other related information, including identification information about the user, may be provided to law enforcement officials. If monitoring reveals violations of

Show disclaimer on login

OK

Users

Covers the *Users* section of Fortisolator.

In Users, you can create new users for clients to browse websites, control the client users with user groups, or connect to SAML servers to allow user accounts on the remote authentication servers to browse websites through the Fortisolator.

All local users can be assigned to one or more user groups. Each user group can associate with one policy. Each policy can associate with Isolator profile, Web Filter profile, and/or ICAP profile. Thus, by assigning individual users to the appropriate user groups you can control how each user accesses websites and what they can browse.

To define local users, user groups, or SAML servers, you can do the following:

- Create local users to access websites through Fortisolator.
- Assign local users to groups with associated with a policy.
- Configure SAML servers to allow user accounts on the remote servers to access websites through Fortisolator.

SAML servers

Security Assertion Markup Language (SAML) is an open standard for exchanging authentication and authorization data between one Identity Provider (IdP) and one or more Service Providers (SP). Both parties exchange messages using the XML protocol as transport.

Fortisolator can integrate with FortiAuthenticator to provide SAML authentication logins with the user identity information that is requested from a third-party Identity Provider (IdP).

In this scenario, the FortiAuthenticator acts as a Service Provider to request user identity information from IdP. Fortisolator can then use this information to sign the user on transparently based on what information the IdP sends.

There are two parts of the setup:

1. [Setup in FortiAuthenticator on page 27](#)
2. [Setup in Fortisolator on page 30](#)

Setup in FortiAuthenticator

1. Go to *FortiAuthenticator > Authentication > SAML IdP > Service Providers > Create New*.
2. Configure the following:

SP Name	Name of the Service Provider
---------	------------------------------

IdP prefix	Generate Prefix
Server Certificate	Fortinet_CA1_Factory
SP Entity ID	<code>http://<Fortisolator ip or domain name>/isolator/saml_metadata</code>
SP ACS (login) URL	<code>https://<Fortisolator ip or domain name>/isolator/saml_acs</code>
SP SLS (logout) URL	<code>https://<Fortisolator ip or domain name>/isolator/saml_sls</code>
Authentication method	Password-only authentication



For the Fortisolator IP, use the external IP if the Fortisolator is set up with one. Otherwise, use the internal IP.

The screenshot shows the configuration page for a SAML Service Provider. Key fields include:

- SP name: FIS_demo
- IdP prefix: 2r6ku1cxuup3emr2
- Server certificate: Fortinet_CA1_Factory
- IdP address: [Redacted]
- IdP entity id: [Redacted]
- IdP single sign-on URL: https://[Redacted]/saml-ldp/2r6ku1cxuup3emr2/login/
- IdP single logout URL: https://[Redacted]/saml-ldp/2r6ku1cxuup3emr2/logout/
- SP entity ID: http://[Redacted]/isolator/saml_metadata
- SP ACS (login) URL: https://[Redacted]/isolator/saml_acs
- SP SLS (logout) URL: https://[Redacted]/isolator/saml_sls

 The 'Authentication' section has 'Password-only authentication' selected.

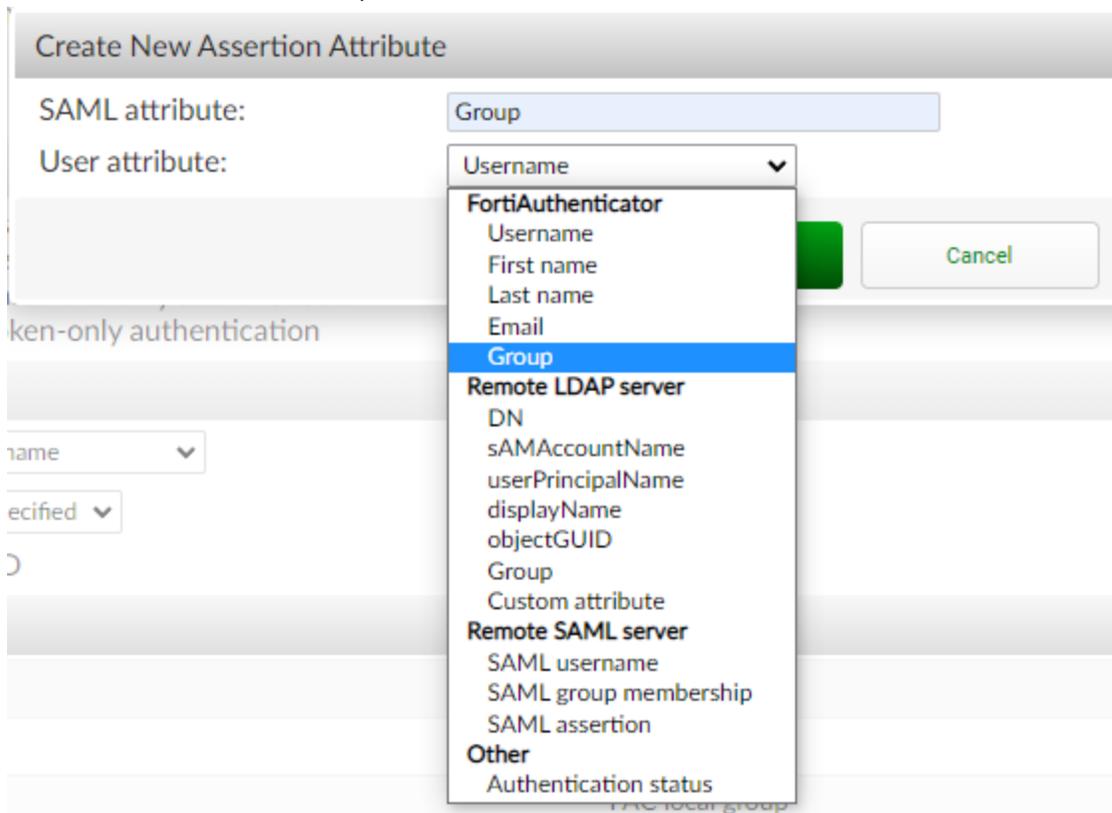
3. Click OK.
4. Click on SP Name then Edit.
5. Add an SAML Attribute for user.

The dialog box is titled 'Create New Assertion Attribute'. It contains two input fields:

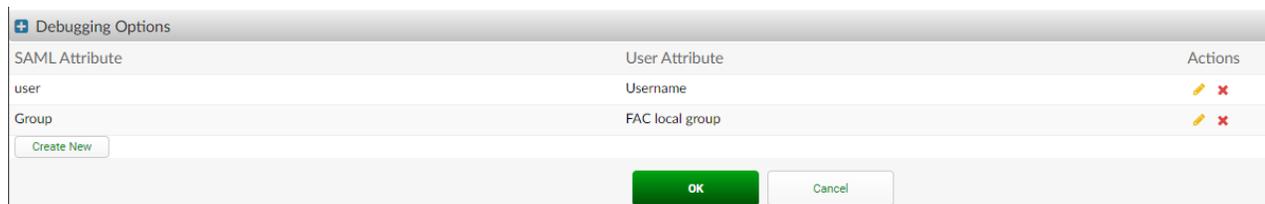
- SAML attribute: user
- User attribute: Username

 At the bottom, there are 'OK' and 'Cancel' buttons.

6. Add SAML Attribute for Group



Debugging Options should look like this:



7. Go to *Certificate Management > End Entities > Local Services* and export the *Fortinet_CA1_Factory* certificate to later import to Fortisolator.
8. Go to *Fortinet SSO Methods > SSO > SSO Users*.
9. Double-check that the SSO Users that Fortisolator will use to log in are imported into FortiAuthenticator. Refer to FortiAuthenticator documents for importing Remote Users.

Setup in Fortisolator

1. Navigate to *System > Certificates > Import*
2. Import the FortiAuthenticator certificate *Fortinet_CA1_Factory* to Fortisolator.

3. Navigate to *Users > LDAP Server > Create New*.
4. Select *SAML Server* and click *OK*.
5. Configure the following:

Id	1 - 4
Enable	Checked to enable the server
ID URL	<code>http://<FortiAuthenticator_Port1_ip>/saml-idp/2r6ku1cxuup3emr2/metadata/</code>
Signon URL	<code>https://<FortiAuthenticator_Port1_ip>/saml-idp/2r6ku1cxuup3emr2/login/</code>
Logout URL	<code>https://<FortiAuthenticator_Port1_ip>/saml-idp/2r6ku1cxuup3emr2/logout/</code>
SAML Certificate	SAML_cert

Run Traffic through Fortisolator with FortiAuthenticator Users

Example:

`https://<FortiIsolator ip or domain name>/isolator/login/https://www.fortinet.com`

← → ↻ https://[redacted]/isolator/login/https://www.fortinet.com

Fortisolator

Isolator Login

Username

Enter Username

Password

Enter Password

Guest

Fortisolator stores cookies on your computer to give you the best experience possible. By continuing

Login

[SAML Single Sign On](#)

User definition

End users can browse the web through Fortisolator as a guest or by logging into their user account. The administrator can create local user accounts or allow single sign-on for existing users in your organization. All user info is secured using a database.

This section provides a way to create local users, assign the user to groups with (if desired) a policy.

Creating local user accounts from GUI

To create a local user account from GUI:

1. Open a browser window and navigate to the *Administration Portal* page.
2. Go to *Users > User Definition > Create New*
3. Under *Create New Local User*, fill in the username and password fields and any optional fields as desired, then click *OK*.

- a. To place the user in an existing group, select the boxes for the groups you would like to assign the user to.
- b. To apply an existing policy to the user, select the policy name from the drop-down menu Policy Name.



You can edit existing local user settings by going to *Users > User Definition*. Select the username and click *Edit* or double-click the username to edit.

Creating local user accounts from CLI

To create a local user from CLI, please use CLI command:

```
set user <username> <server-id>
```

(where server-id has to be "0" as for local user)

e.g.

```
> set user fis_user 0
```

Enter the password:

Re-enter the password:

Please enter email: fis_user@fortinet.com

Please enter policy name: policy_new

```
> show user
```

Displaying only local users...

```
name : fis_user
```

```
server_id : 0
```

```
email : fis_user@fortinet.com
```

```
policy_name : policy_new
```

```
encoded password : ffff18ff28ff38ffff60ff3678ff2e03
```

```
>
```

User groups

Local users can be placed into user groups. User group allows you to apply policies to many local users at once rather than one by one individually.

Creating user groups from GUI

To create a user group from GUI:

1. From the administration portal, go to *Users > User Groups* and click *Create New*.
2. Type in a name for the group and click *OK*.

Creating user groups from CLI

To create a user group from CLI:

```
set group <group-name> <server-id> <policy-name>  
(where server-id has to be "0" as for local user)
```

e.g.

```
> set group group_new 0 policy_new
```

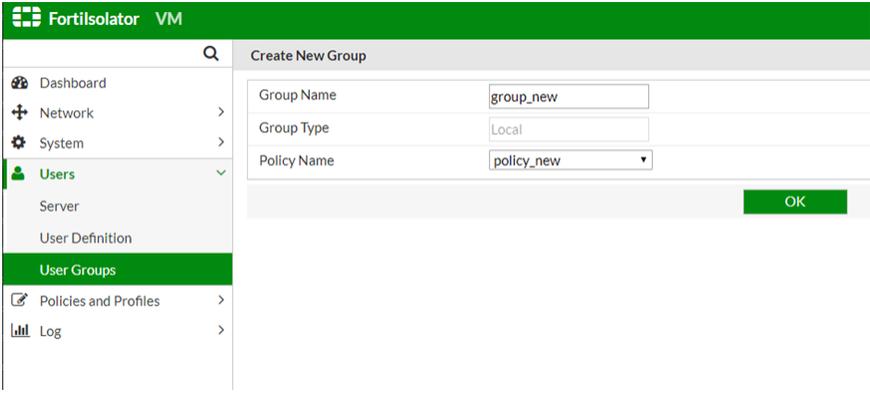
```
> show group
```

```
Group Name : group_new
```

```
Server ID : 0
```

```
Policy : policy_new
```

```
>
```



The screenshot shows the FortiSOLATOR VM web interface. On the left is a navigation menu with items: Dashboard, Network, System, Users (selected), Server, User Definition, User Groups, Policies and Profiles, and Log. The main content area is titled 'Create New Group' and contains a form with the following fields:

- Group Name:
- Group Type:
- Policy Name:

An 'OK' button is located at the bottom right of the form area.

Policies and profiles

In the *Policies and Profiles* section of Fortisolator the following are covered:

- *Profile*—There are three types of profiles you can create: browsing, Web Filter, ICAP.
- *Policies*—Apply created Isolator profile and Web Filter profiles, or global policy.

Profile

Creating a Isolator browsing profile

Configure the Isolator profile to dictate how the end user browses the web through Fortisolator. There are various settings for you to configure, including the bandwidth use and end user privileges.

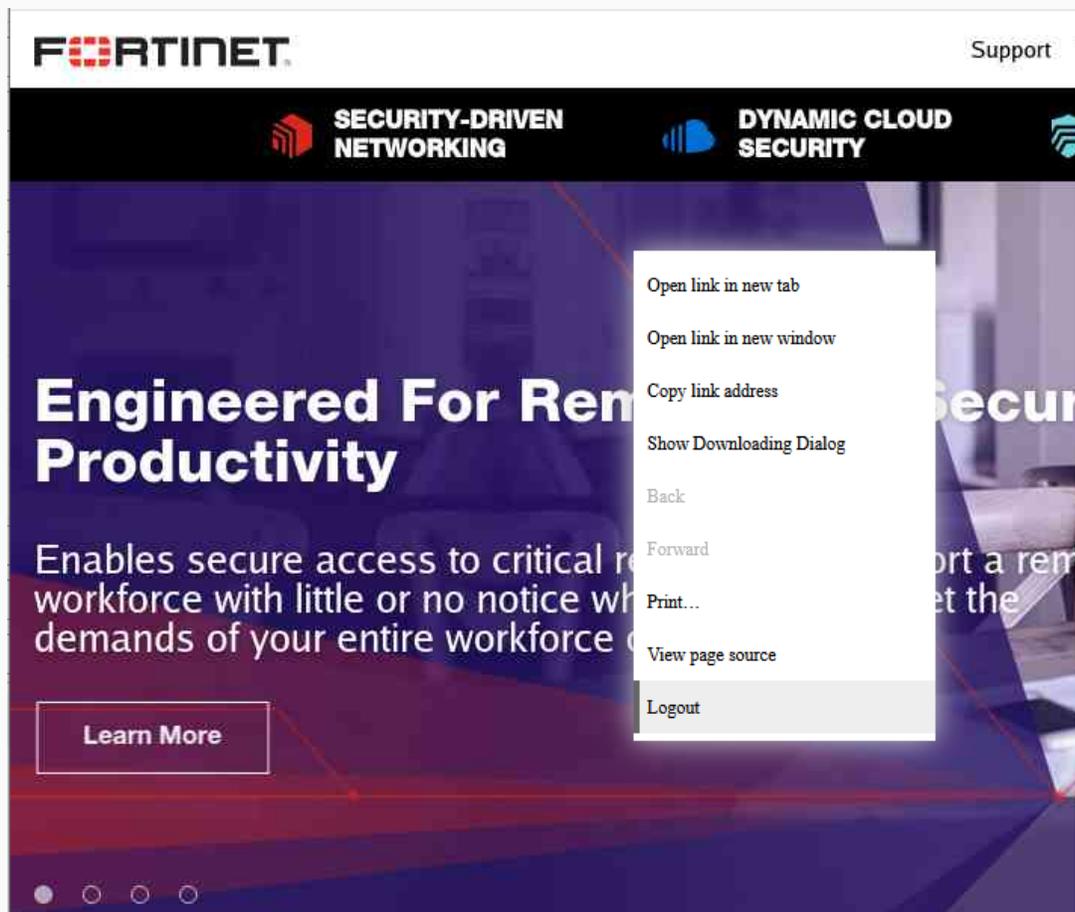
To create an Isolator browsing profile from GUI:

1. From the administration portal, go to *Policies and Profiles > Profiles* and click *Create New*.
2. From the *Profile Type* drop-down menu, select *Isolator Profile* and click *OK*.
3. Fill in the new Isolator profile information with desired settings.

<i>Isolator Profile Name</i>	Name of the Isolator profile. No restrictions.
<i>View-only Mode</i>	Specifies whether to limit the user to view-only access of web pages. The user is restricted from interacting with the pages, such as right-clicking or typing in text.
<i>Image Quality</i>	Specify a percentage within 1-100. A higher percentage means more bandwidth usage.
<i>Video Frame Rate</i>	Video frame rate (high, normal, low). A higher rate means more bandwidth usage.
<i>Scroll Speed</i>	Allows end uses to control the scrolling speed on the mouse wheel while navigating pages. The range is from 1 - 100; 1 is the minimum speed, while 100 is the maximum speed. When the speed is set at 100, one scroll on the mouse wheel will scroll through one full page on the browser window.
<i>Allow Right-click Action</i>	Specifies whether to allow client users to right click on mouse to display a menu.



This option works only if *View-only Mode* is disabled.



Print Users can print the current page as a PDF file.

Logout Log out from the current session.

Allow Copy out from Fortisolator Specifies whether to allow client users to copy content from the Fortisolator to the clipboard using the keyboard or right-click menu. To enable copying content from the Fortisolator using the right-click menu, the *Allow Right-click Action* option must be enabled.

Allow Paste to Fortisolator Specifies whether to allow client users to paste content from the clipboard to the Fortisolator using the keyboard or right-click menu. To enable pasting content to the Fortisolator using the right-click menu, the *Allow Right-click Action* option must be enabled.

Allow Printing Specifies whether to allow client users to print the current page into a PDF file.

User Agent	Customized user agent name. For example, enter the following agent name to enable Fortisolator to pass human verification: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:68.0) FortiIsolatorBrowser/2.0 Gecko/20100101 Firefox/68.0
Show Isolation Icon	Specifies whether to show the Fortisolator icon on the pages when users browse using Fortisolator.

Certificates	Specifies which uploaded certificate(s) to enable for the profile. Fortisolator automatically lists all uploaded Certificates on page 22 of the following types. If no such certificate is uploaded, the list is empty. <ul style="list-style-type: none"> • Self Signed Server Certificate • Self Signed CA Root Certificate • Intermediate CA Certificate
---------------------	---



The certificate chain must be complete for the certificate to work, which means the root certificate and all relevant subordinate certificates (Intermediate CA Certificates) must be enabled at the same time.

Max Download Size (MB)	Specifies the maximum file size in megabytes for downloading files.
-------------------------------	---

Max Upload Size (MB)	Specifies the maximum file size in megabytes for uploading files.
-----------------------------	---

Block File Type Download	Select the file types to block from downloading. You can also add more file types by clicking the <i>Add</i> button. Select <i>Block All</i> to select all file types in the list. <ul style="list-style-type: none"> • <i>exe</i> • <i>doc</i> • <i>ppt</i> • <i>pdf</i> • <i>txt</i> • <i>xls</i> • <i>png</i> • <i>mp3</i>
---------------------------------	---

Block File Type Upload	Select the file types to block from uploading. You can also add more file types by clicking the <i>Add</i> button. Select <i>Block All</i> to select all file types in the list. <ul style="list-style-type: none"> • <i>exe</i> • <i>doc</i> • <i>ppt</i> • <i>pdf</i> • <i>txt</i> • <i>xls</i> • <i>png</i> • <i>mp3</i>
-------------------------------	---

<p><i>Allowlist File Type Download</i></p>	<p>Select the file types to allow for downloading. You can also add more file types by clicking the <i>Add</i> button.</p> <ul style="list-style-type: none"> • <i>exe</i> • <i>doc</i> • <i>ppt</i> • <i>pdf</i> • <i>txt</i> • <i>xls</i> • <i>png</i> • <i>mp3</i>
<p><i>Allowlist File Type Upload</i></p>	<p>Select the file types to allow for uploading. You can also add more file types by clicking the <i>Add</i> button.</p> <ul style="list-style-type: none"> • <i>exe</i> • <i>doc</i> • <i>ppt</i> • <i>pdf</i> • <i>txt</i> • <i>xls</i> • <i>png</i> • <i>mp3</i>
<p><i>File Download Security</i></p>	<p>Configure whether to scan files for virus or malware with the following tools when uploading or downloading files through Fortisolator.</p> <ul style="list-style-type: none"> • If any of the enabled tools detects the file as containing virus or malware, Fortisolator displays the result in the client browser and prevents the user from uploading or downloading the file. • If the file is determined as sanitized by all enabled tools, Fortisolator allows the client user to upload or download the file. <p><i>Send Files with FortiSandbox</i> Specifies whether to send files to FortiSandbox. When enabled, specify the following options to connect to FortiSandbox:</p> <ul style="list-style-type: none"> • <i>FortiSandbox IP</i>—IP address or domain name of the FortiSandbox to connect to. • <i>FortiSandbox Administrator Name</i>—Name of the FortiSandbox administrator. • <i>FortiSandbox Password</i>—Password of FortiSandbox. <p>To verify connection with FortiSandbox, upload a file using Fortisolator. When the following image appears, which means the upload is complete, verify that the file is being scanned in FortiSandbox and view the result of the scan.</p>



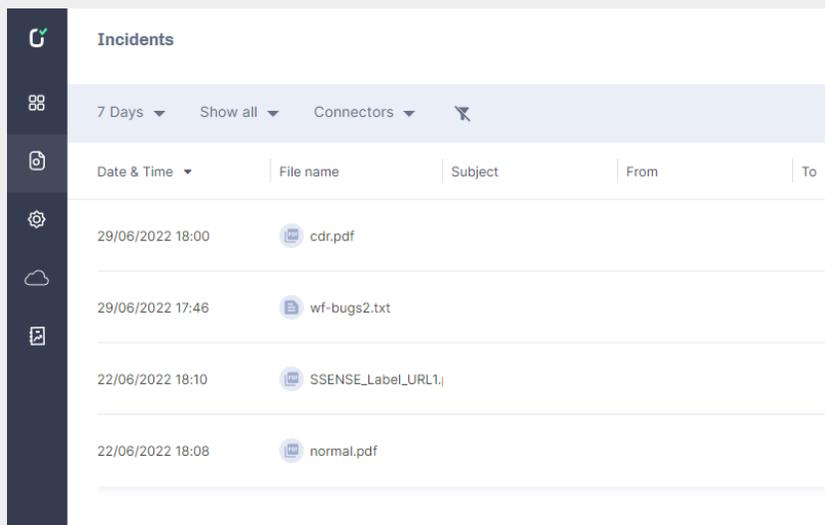
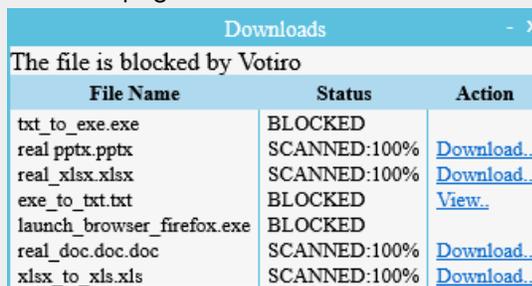
Scan Files with Fortisolator Specifies whether to scan files with Fortisolator. When enabled, further configure the following option:

- *File Content Disarm and Reconstruct with Fortisolator*

File Content Disarm and Reconstruct Integration with Votiro Specifies whether to use **Votiro** for file content disarm and reconstruct. When enabled, specify the following options to connect to Votiro:

- *Votiro URL*—URL of the Votiro application.
- *Votiro Token*—Service token that you created in Votiro which allows Fortisolator to communicate with Votiro.
- *Votiro Channel ID*—ID of the Votiro service token.
- *Votiro Policy Name*—Name of the Votiro policy to use.

To verify connection with Votiro, enable this option and download a file using Fortisolator. When the following image appears, which means the download is complete, verify that the file appears in the *Incidents* page in Votiro.



4. Click OK.

To create a Fortisolator profile from CLI:

```
> set isolator-profile <name> <download> <upload> <viewonly> <avscan> <image-quality> <video-frame-rate> <av-disarm> <right-click> <scroll-speed> <file-type> <permit-of-copy> <permit-of-print> <agent-name> <icon-action> <browser-cookie> <allowlist-file-type> <permit-of-paste>
```

For example,

```
> set isolator-profile system_default 100 100 N Y 100 normal Y Y 10 exe;doc Y Y fortiisolator Y Y png;mp3 Y
```

Parameter	Description
<name>	Name of the Isolator profile.
<download>	Max download size in megabytes (MB).
<upload>	Max upload size in megabytes (MB).
<viewonly>	Limit of view-only (Y/N).
<avscan>	Scan files for malware (Y/N).
<image-quality>	Image quality. Specify a percentage within 1-100.
<video-frame-rate>	Video frame rate (high, normal, low).
<av-disarm>	Use doc-rewrite when scanning file (Y/N).
<right-click>	Permit to right-click (Y/N). This parameter is valid only when <viewonly> is N.
<scroll-speed>	Scrolling speed on the mouse wheel while navigating pages. The range is from 1 - 100 with 1 as the minimum speed and 100 the maximum.
<file-type>	File types to block from downloading and uploading.
<permit-of-copy>	Permit to copy content from the Fortisolator to the clipboard using the keyboard or right-click menu. (Y/N) To enable copying content from the Fortisolator using the right-click menu, the <right-click> option must be enabled (Y).
<permit-of-print>	Permit to print current page into a PDF file. (Y/N)
<agent-name>	Customized user agent name.
<icon-action>	Show the Fortisolator icon on the pages when users browse using Fortisolator (Y/N).
<allowlist-file-type>	File types to allow for downloading and uploading.
<permit-of-paste>	Permit to paste content from the clipboard to the Fortisolator using the keyboard or right-click menu. (Y/N) To enable pasting content to the Fortisolator using the right-click menu, the <right-click> option must be enabled (Y).

To display Isolator browsing profile from CLI:

```
> show isolator-profile system_default
  Remote Render : N
  Download Size(MB) : 100
  Upload Size(MB) : 100
  View-only Mode : N
  Antivirus Scan Enabled : Y
  Content Disarm and Reconstruct: Y
  Allow Right-click Action : Y
  Allow Printing : Y
  Image Quality : 100
  Video Frame Rate : normal
  Scroll Speed : 10
  Block File Type Download : exe;doc
  Block File Type Upload : exe;doc
  Allowlist File Type Download :
  Allowlist File Type Upload :
  Agent Name : fortiisolator
  Show FortiIsolation Icon : Y
  Store Browser's Cookie : N
  Copy-enabled : Y
  Paste-enabled : Y
  FortiSandbox Enabled : N
  FortiSandbox IP : ""
  FortiSandbox Admin : ""
  Votiro Enabled : N
  Votiro IP : ""
  Votiro Policy Name : ""
  Votiro Token : ""
  Votiro Channel ID : ""
>
```

Creating Web Filter profile

Fortisolator supports web filtering, which enables the administrator to control which webpages that end users are allowed to view. You can block specific URLs or websites, which prevents the end user's browser from loading web pages from these websites.

Prerequisites

- Ensure that Fortisolator has a valid license installed.
- Register the device to a production server:
<https://support.fortinet.com/product/RegistrationEntry.aspx>.
- Ensure that the IP address in the Fortisolator license is the same as the Fortisolator management IP address.

To create a Web Filter profile from GUI:

1. From the administration portal, go to *Policies and Profiles > Profiles* and click *Create New*.
2. From the *Profile Type* drop-down menu, select *Web Filter Profile* and click *OK*. You will be brought to the *Edit Web Filter Profile* page.
3. Enter a Web Filter Profile Name.
4. To change web filters for specific categories or subcategories, check the boxes next to the categories or subcategories that you wish to modify. To access the subcategories list, expand the category by clicking the small triangle next to the category.

Edit Web Filter Profile

Webfilter Profile Name

Show

- Potentially Liable
 - ViewOnly
 - Block
 - Allow
 - Discrimination
 - Explicit Violence
 - Extremist Groups
 - Proxy Avoidance
 - Plagiarism
 - Child Abuse
 - Adult/Mature Content

White List

URL	Type

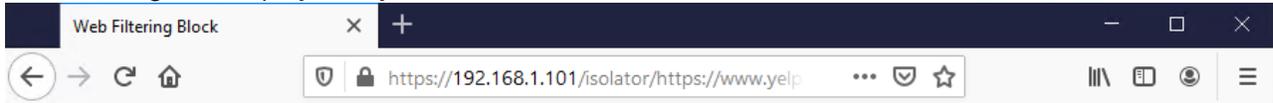
Black List

URL	Type

Right-click on any checked box to select the desired action:

- a. View-only:** End user is restricted to view-only access and is unable to interact with the web page, including clicking links and downloading files.
- b. Block:** End user is restricted from accessing the web page and will be shown a page informing them that the URL has been blocked by the administrator.
- c. Allow:** End user has full access of the website. By default, all web categories are allowed.

5. To allow or block specific websites, click the corresponding *Create New* button in the *Allow List* or *Block List* section. Enter the URL details and click *OK*. The allow list and block list filters accept simple URLs, regular expressions, wildcards, and exemptions as URL filter criteria.
6. To finish creating the Web Filter Profile, click *Submit*.
7. To verify that the web filter is working, try browsing to one of the blocked web pages. You should see the following text displayed in your browser:



The URL is blocked by Fortinet Isolator Web Filtering

Your Isolator administrator has blocked the URL

To create a Webfilter profile from CLI:

```
set wf-allow-list <name> <url> <type>
```

TYPE

- 0: Simple
- 1: Regular Expression
- 2: Wildcard
- 3: Exempt

e.g.

```
> set wf-allow-list allow_list_new website.com 0
```

```
> show wf-allow-list
```

```
allow_list-allow_list_new testsite.com 0
```

```
set wf-block-list <name> <url> <type>
```

e.g.

```
> set wf-block-list block_list_new blocksite.com 0
```

TYPE

- 0: Simple
- 1: Regular Expression
- 2: Wildcard
- 3: Exempt

```
> show wf-block-list
```

```
block_list-block_list_new blocksite.com 0
```

```
set wf-profile <name> <allow-list> <block-list> <actions>
```

```
e.g.
> set wf-profile webprofile_new allow_list_new block_list_new 0

> show wf-profile

Web Filter Profile:webprofile_new
  allowlist : allow_list_new
  blocklist : block_list_new
  action profile : 0
```

Creating ICAP profile

Internet Content Adaptation Protocol (ICAP) is an application layer protocol that is used to offload tasks from the firewall to separate, specialized servers.

Fortisolator supports ICAP web filtering, which allows the administrator to use third-party ICAP servers to control which webpages the end users are allowed to view. You can block specific URLs or websites, which prevents the end user's browser from loading web pages from these websites.

If you enable ICAP in a policy, HTTP and HTTPS traffic that is intercepted by the policy is transferred to the ICAP server specified by the selected ICAP profile. Responses from the ICAP server are returned to the Fortisolator, and then forwarded to their destination.

ICAP profiles can be applied to policies that use Proxy-based or IP Forwarding mode.

Prerequisites

- Ensure that an ICAP server is alive and can block web sites from its local server.
- Ensure the ICAP server can ping to Fortisolator and vice versa.

To create an ICAP profile from GUI:

1. From the administration portal, go to *Policies and Profiles > Profiles* and click *Create New*.
2. From the *Profile Type* drop-down menu, select ICAP Profile and click *OK*.
3. Fill in the new ICAP profile information with desired settings:

ICAP Profile Name	Name of the ICAP profile
IP Address	IP Address of the ICAP server
Port	Port number that the ICAP server running the service on
Service	Service name of the ICAP server
Action when server fails	Actions on Fortisolator if fails to connect to ICAP <ul style="list-style-type: none"> • Allow • Block • View only

To create an ICAP profile from CLI:

```
set icap-profile <name> <ip> <port> <service> <fail-action>
```

```
<name> : ICAP Profile Name
<ip> : IP Address
<port> : Port
<service> : Service
<fail-action> : Action when server fails (Block = 1, allow = 2, viewonly = 3)
```

e.g.

```
> set icap-profile icap_new 172.30.157.208 1344 url_check 1
```

```
> show icap-profile
```

```
ICAP Profile:icap_new
```

```
    IP Address : 172.30.157.208
```

```
    Port : 1344
```

```
    Service Name : url_check
```

Edit Profile	
ICAP Profile Name	<input type="text" value="icap_new"/>
IP address	<input type="text" value="172.30.157.208"/>
Port	<input type="text" value="1344"/>
Service	<input type="text" value="url_check"/>
Action when server fails	<input type="text" value="Block"/>
<input type="button" value="OK"/>	

Policy

A policy provides a convenient way to apply a certain Isolator profile and/or Web Filter profile to local individual users or user groups. Policies are not active until they are applied.

To create a policy from GUI:

1. Go to *Policies and Profiles* > *Policies* and click *Create New*.
2. Type in a name for the policy.
3. Select the desired Isolator and/or Web Filter profiles, and/or ICAP Filter profile to be used in the policy.
4. Specify the value for *Max Session Per User*, which is the maximum number of sessions (tabs) allowed for requests from a same local user.
5. Specify the value for *Max Session Per IP*, which is the maximum number of sessions (tabs) allowed for requests from a unique IP address.
6. Specify the *Auth Cookie Lifetime* setting, which is the number of hours after which the authorization cookie expires and the user needs to re-login. Enter an integer within the range of 1-240.



This setting does not take effect when the user is in guest mode.

7. Click *OK* to finish.

To create a Fortisolator policy from CLI:

```
> set policy <policy-name> <isolator-profile-name> <webfilter-profile-name> <icap-profile-name>
    <max-session-per-user> <max-session-per-ip> <auth-cookie-lifetime>
```

e.g.

```
> set policy policy_new system_default webfilter_profile ICAP_profile 50 30 96
```

<policy-name >	Policy name
<isolator-profile-name >	Isolator profile name
<webfilter-profile-name >	Web Filter profile name
<icap-profile-name >	ICAP profile name
<max-session-per-user>	Maximum number of sessions (tabs) allowed for requests from a same local user
<max-session-per-ip>	Maximum number of sessions (tabs) allowed for requests from a unique IP address
<auth-cookie-lifetime>	Number of hours after which the authorization cookie expires and the user needs to re-login. This parameter accepts integers within the range of 1-240.



This parameter does not take effect when the user is in guest mode.

To display a Fortisolator policy from CLI:

```
> show policy
    Policy : policy_new
    Isolator Profile : system_default
    WebFilter Profile : webfilter_profile
    ICAP Profile : ICAP_profile
    Max Session Per User : 50
    Max Session Per IP : 30
    Auth Cookie Lifetime : 96
```

Global policy

There are several ways you can apply Isolator profile and Web Filter profile settings to end users. Isolator profiles and Web Filter profiles can be applied to the guest account, individual local user accounts, and/or local user groups.

Applying global policy and profile settings

The Fortisolator provides a global policy to local users and guest that do not have assigned groups with selected policy. Global policy is a way to apply a certain Isolator profile, Web Filter profile, and/or ICAP profile to local individual users or guest.

To apply profiles to the global policy from GUI:

1. Go to *Policies and Profiles > Global Policy* and select the desired *Guest Type*. This option determines the way of [Logging in as an end user on page 79](#).

*guest
disable*

A user has to log in with a user account of one of the following types:

- **Local user** - The user can log in by entering the designated username and password configured in [User definition on page 31](#) if *Login Option* is *Local User or SAML User Only*.
- **SAML user** - If a SAML server is configured through FortiAuthenticator in [SAML servers on page 27](#), the user can log in with single-sign-on by clicking the *SAML Single Sign On* link and entering the credentials.

*guest
enable*

A user can log in with either a user account or as a guest.

- To log in with a user account, the user enters the credentials of one of the following account types:
 - **Local user** - The user enters the designated username and password configured in [User definition on page 31](#).
 - **SAML user** - If a SAML server is configured through FortiAuthenticator in [SAML servers on page 27](#), the user can single-sign-on by clicking the *SAML Single Sign On* link and entering the credentials.
- To log in as a guest, the user leaves the username and password empty and selects *Guest*.

guest only

A user has to log in as a guest.



With *guest only*, the login page will not show. Users can browse sites without being prompted to log in.

2. Select the Isolator profile, Web Filter profile, and/or ICAP Filter profile to be used in the policy. Also set *Max Session Per User*, *Max Session Per IP*, *Auth Cookie Lifetime*, and *Login Option* to be used in the global policy.

<i>Default Isolator Profile Name</i>	Select an Isolator profile for Global Policy.
<i>Default WebFilter Profile Name</i>	Select a Web Filter profile for Global Policy.
<i>Default ICAP Profile Name</i>	Select an ICAP profile for Global Policy.
<i>Max Session Per User</i>	Maximum number of sessions (tabs) allowed for requests from a same local user
<i>Max Session Per IP</i>	Maximum number of sessions (tabs) allowed for requests from a unique IP address
<i>Auth Cookie Lifetime</i>	Number of hours after which the authorization cookie expires and the user needs to re-login. Enter an integer within the range of 1-240.



This setting does not take effect when the user is in guest mode.

3. Click OK to finish.

Global Policy	
Guest Type:	guest enable
Default Isolator Profile Name:	system_default
Default WebFilter Profile Name:	<None>
Default ICAP Profile Name:	<None>
Default Forwarding Profile Name:	<None>
Max Session Per User:	50
Max Session Per IP:	100
Auth Cookie Lifetime:	24

To apply profiles to global policy from CLI:

```
> set guest-type 0|1|2
(disabled = 0, enabled = 1, guest-only = 2)
```

For example:

```
> set guest-type 0
> show guest-type
guest type : Disabled
> set guest-type 1
> show guest-type
guest type : Enabled
> set guest-type 2
> show guest-type
guest type : Guest Only
```

```
> set global-policy <isolator-profile-name> <webfilter-profile-name> <icap-profile-name> <guest-type> <max-session-per-user> <max-session-per-ip> <auth-cookie-lifetime>
```

e.g.

```
> set global-policy system_default webfilter_profile ICAP_profile 1 50 30 96 1
```

<isolator-profile-name >	Isolator profile name
<webfilter-profile-name >	Web Filter profile name
<icap-profile-name >	ICAP profile name
<guest-type>	Login mode of the user:

	1	<i>guest disable</i> : A user must log in with the following types of credentials: <ul style="list-style-type: none"> Local user account—Only if <i>Login Option</i> is <i>Local User</i> or <i>SAML User</i>. SAML credentials—Only if a SAML server is configured through FortiAuthenticator in SAML servers on page 27.
	2	<i>guest enable</i> : A user can log in with a user account, SAML/NTLM authentication, or as a guest.
	0	<i>guest only</i> : A user has to log in as a guest. No credentials are required.
<max-session-per-user>		Maximum number of sessions (tabs) allowed for requests from a same local user
<max-session-per-ip>		Maximum number of sessions (tabs) allowed for requests from a unique IP address
<auth-cookie-lifetime>		Number of hours after which the authorization cookie expires and the user needs to re-login. This parameter accepts integers within the range of 1-240.
 <p>This parameter does not take effect when the user is in guest mode.</p>		

To display the global policy profile from CLI:

```
> show global-policy
Global Policy:
Guest Type : 1
Isolator Profile : system_default
WebFilter Profile : webfilter_profile
ICAP Profile : ICAP_profile
Max Session Per User : 50
Max Session Per IP : 30
Auth Cookie Lifetime : 96
```

Applying profile settings to local user account

To apply profile settings to local user account:

1. From the administration portal, go to *Policies and Profiles* > *Policies* and make sure the policy you want to apply exists. If not, create a new policy with the desired profiles.
2. Go to *Users* > *User Definition*. Select the user you wish to apply the profile settings to and click *Edit*.
3. From the *Policy Name* drop-down menu, select the policy you wish to apply to the local user.

4. Click *OK* to finish.

Applying profile settings to user groups

To apply profile settings to user groups:

1. From the administration portal, go to *Policies and Profiles > Policies* and make sure the policy you want to apply exists. If not, create a new policy with the desired profiles.
2. Go to *Users > User Groups*. Select the user group you wish to apply the profile settings and click *Edit*.
3. From the *Policy Name* drop-down menu, select the policy you wish to apply to the user group.
4. Click *OK* to finish.

Log



The *FIS_log* package must be manually installed and applied for logs to show correctly:

- See the [Fortisolator 3.0 Private Cloud Deployment Guide](#) for instructions of downloading the package.
 - See [Manage FIS Images on page 24](#) for instructions of uploading and applying the package in Fortisolator.
-

Logging is a useful component to help you understand what is happening on your Fortisolator and on networks, and to inform you about certain activities, such as:

- Daemons running on the Fortisolator
- Connectivity with FDN server, internal database, Anti-Virus servers, etc.
- Heartbeat information among the nodes when have HA cluster setup
- Detections of virus when uploading or downloading files
- Web filtering activities on sites to passing through or blocking by Fortisolator for client users
- Forwarding logs to remote log servers

You can view logs by the following categories:

- [ISOLATOR on page 51](#)
- [ADMIN GUI on page 52](#)

You can also configure Fortisolator to send the log to a third-party [Remote Server on page 52](#), including FortiAnalyzer.

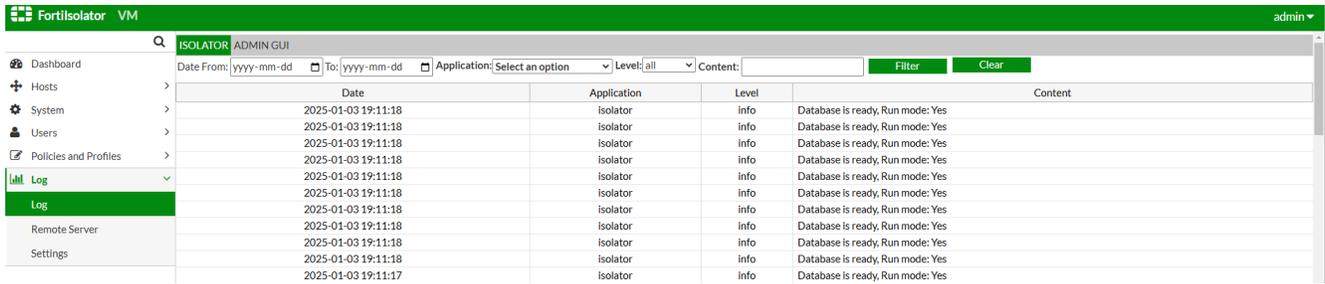
- FortiAnalyzer—Fortisolator routes the log to FortiAnalyzer for display, processing, or reporting. Fortisolator no longer displays the logs under the log categories. See the [FortiAnalyzer Administration Guide](#) for more information.
- Third-party remote server—Fortisolator sends a copy of the raw log to the remote server while keeping the log display under the log categories.

You can also configure the log backup behavior for the Fortisolator in the [Settings on page 53](#) tab.

Refer to the [Fortisolator Log Message Reference Guide](#) for more information about how to interpret the log messages.

ISOLATOR

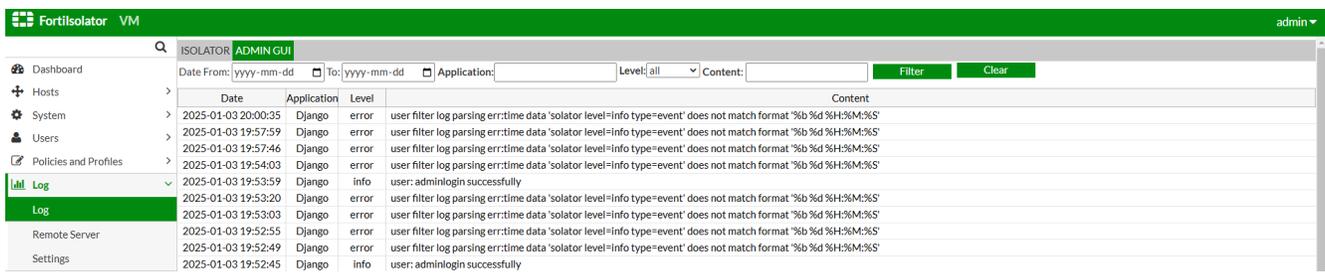
The *ISOLATOR* tab includes browsing traffic logs for all traffic flowing through your Fortisolator.



- To filter the log messages, enter the desired filter criteria using the date, application name, level, and/or content and click *Filter*. To view debug logs, you must enable debug logs using the following command: `set global-debuglog-enabled 1`.
- To clear the log window of messages, click *Clear*.

ADMIN GUI

The ADMIN GUI tab includes all event logs.



- To filter the log messages, enter the desired filter criteria using the date, application name, level, and/or content and click *Filter*.
- To clear the log window of messages, click *Clear*.

Remote Server

To send syslog messages to FortiAnalyzer or a remote server:

1. From the administration portal, go to *Log > Remote Server*.
2. Specify the information for your remote server.

<i>Logging Protocol</i>	Syslog
<i>Network Protocol</i>	<ul style="list-style-type: none"> • udp • tcp

Log Server IP Address	Remote server IP that receives the logs.
Port	Port number of the remote server that receives the logs. Enter 514 for FortiAnalyzer remote servers.

3. Configure the types of logs to send to the remote server.
 - a. Click *+ Create New* to add a new log type or select an existing type and click *Edit* or *Delete* to modify the type.
 - b. When adding or editing a type, select the *Category* and *Severity*. See the descriptions in [Log on page 51](#).
 - c. Click *OK*.
4. Click *Submit*.



If you configure a FortiAnalyzer remote server, Fortisolator routes the log to FortiAnalyzer for display, processing, or reporting and no longer displays the logs under the log categories. See the [FortiAnalyzer Administration Guide](#) for more information.

However, for third-party remote servers, Fortisolator sends a copy of the raw log to the remote server while keeping the log display under the log categories.

Settings

To back up or clean up log messages on the Fortisolator:

From the administration portal, go to *Log > Settings*.

- To save your current log messages as a file, click the *Click here* link inside the *Backup Logs* section.
- To configure the Fortisolator to back up log files on a regular basis:
 - a. Select the *Schedule to backup log files periodically* option.
 - b. Fill in the settings.

Log File Size (MB)	Specify the log file size in megabytes.
Log time	Specify the intervals (in hours) to save log files.
Log Retention Period (days)	Specify the retention period (in days) of the saved logs.

- c. Click *Submit*.

Running web browsers through Fortisolator

You can run web browsers through Fortisolator in the following modes:

- IP Forwarding mode
- Proxy mode

IP Forwarding mode

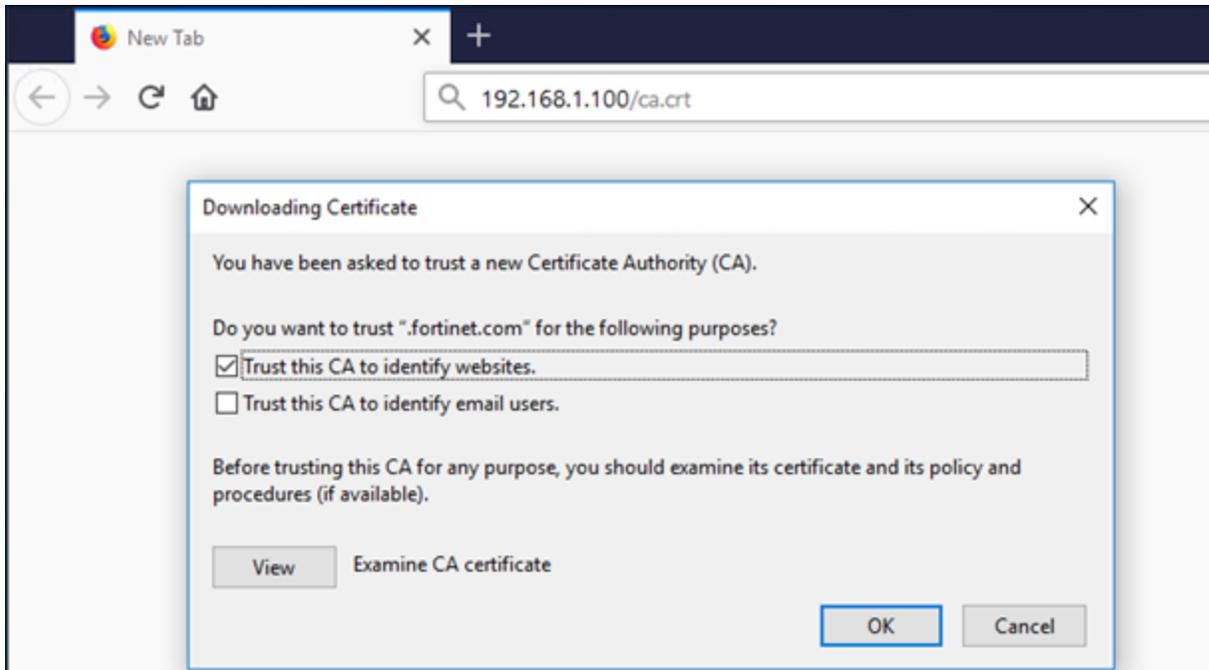
You can configure Fortisolator to run in IP Forwarding mode using the following types of browsers:

- Using IP Forwarding mode with Mozilla Firefox on page 54
- Using IP Forwarding mode with Google Chrome on page 56
- Using IP Forwarding mode with Edge on page 61

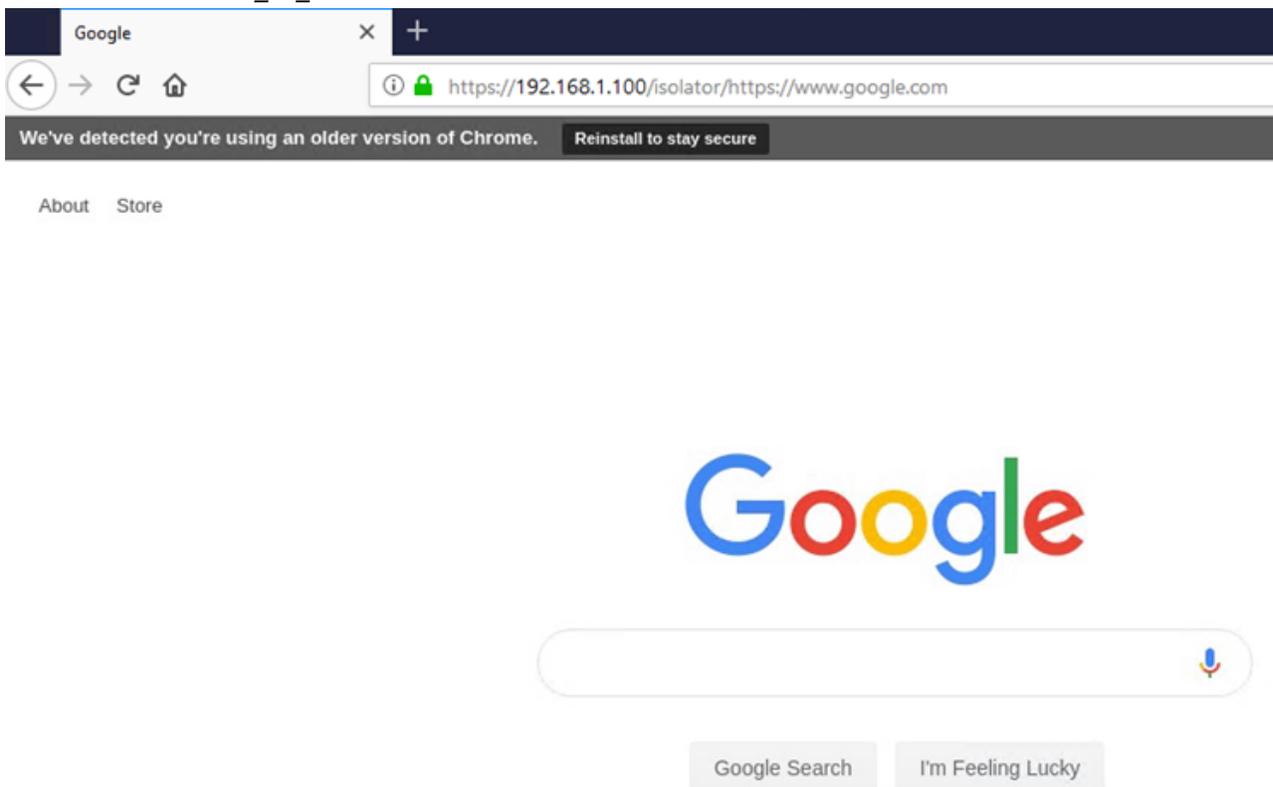
Using IP Forwarding mode with Mozilla Firefox

To configure IP Forwarding mode with Mozilla Firefox:

1. Download the Fortisolator certificate (ca.crt) and import it into the Mozilla Firefox browser:
 - a. In the Mozilla Firefox browser address bar, type `http://<internal_IP_address>/ca.crt` (for example, `http://192.168.1.100/ca.crt`).
 - where `<internal_IP_address>` is the IP address of the Fortisolator internal interface.
 - b. In the *Downloading Certificate* window, select the *Trust this CA to identify websites* checkbox.
 - c. Click *OK*.



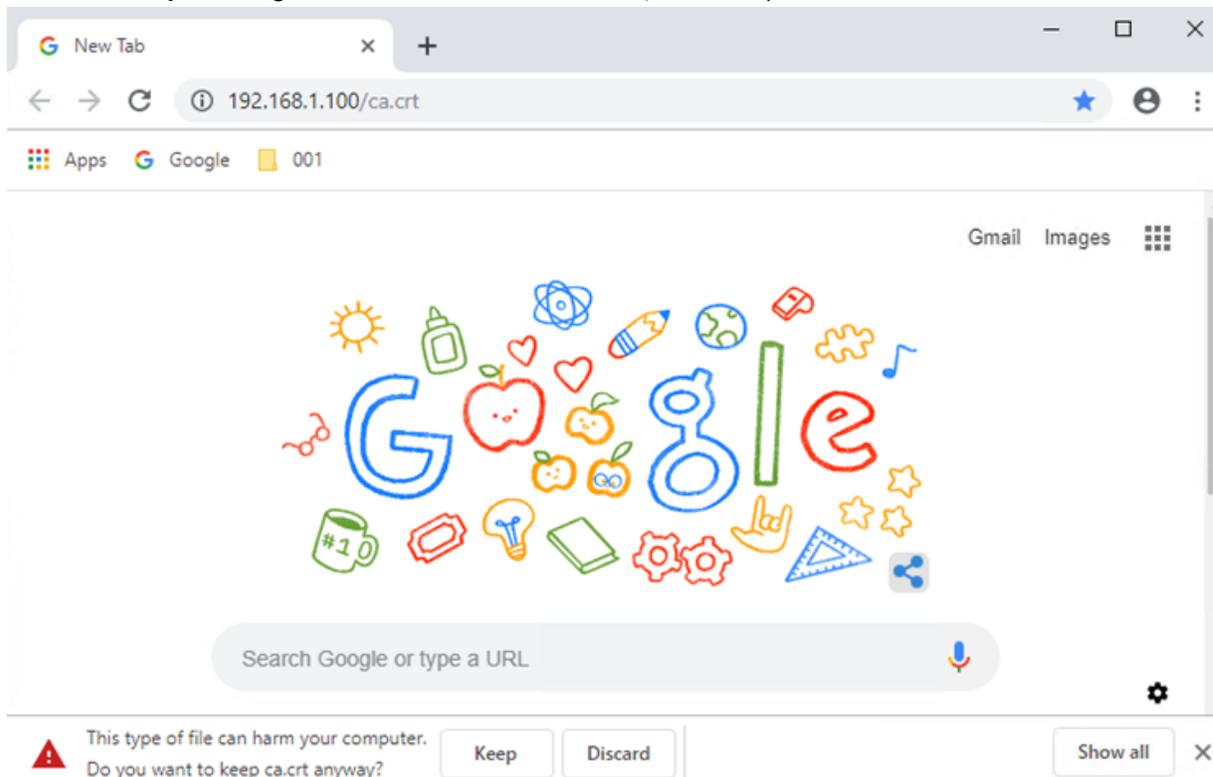
2. In the Mozilla Firefox browser address bar, type `https://<internal_IP_address>/isolator/https://www.<website-url>.com` (for example, `https://192.168.1.100/isolator/https://www.google.com`).
 - where `<internal_IP_address>` value is the IP address of the Fortisolator internal interface.



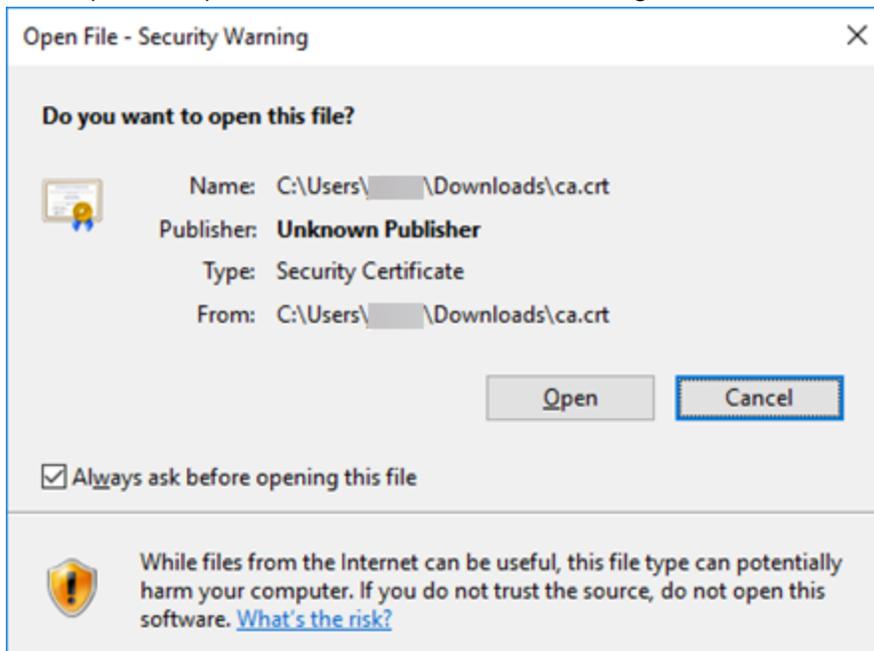
Using IP Forwarding mode with Google Chrome

To configure IP Forwarding mode with Google Chrome:

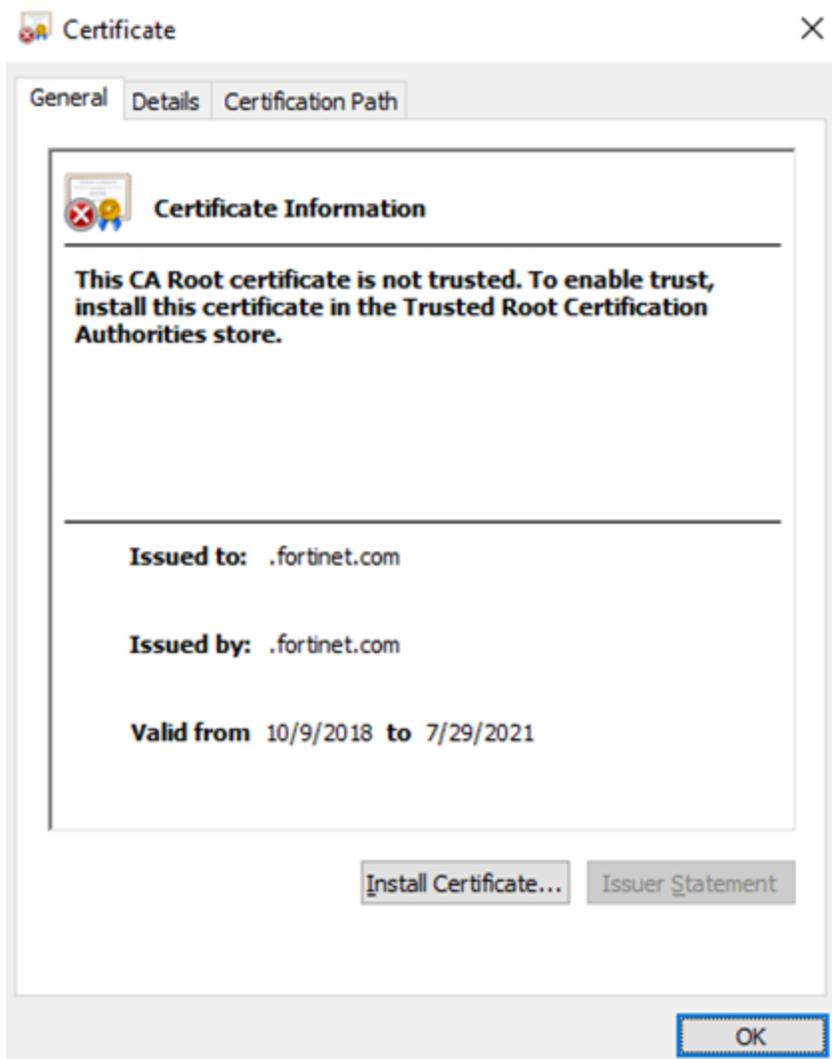
1. Download the Fortisolator certificate (ca.crt) and import it into your Google Chrome browser:
 - a. In the Google Chrome browser address bar, type `http://<internal_IP_address>/ca.crt` (for example, `http://192.168.1.100/ca.crt`).
 - where `<internal_IP_address>` value is the IP address of the Fortisolator internal interface.
 - b. In the security warning at the bottom of the browser, click **Keep** to download the certificate.



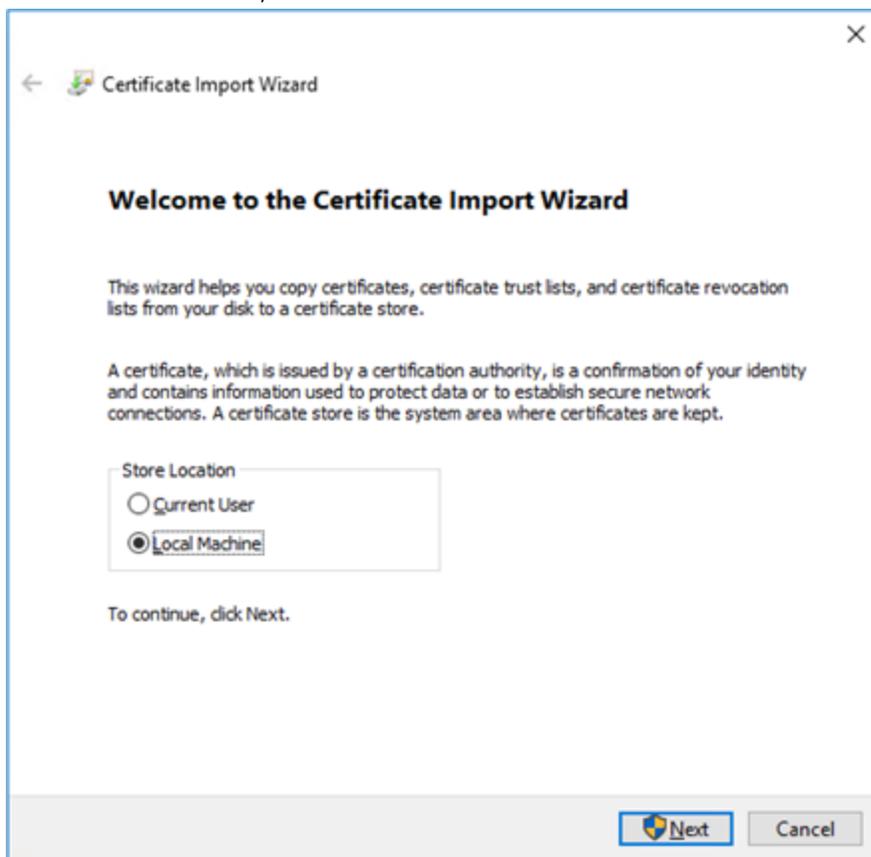
- c. Click *Open* to import the ca.crt certificate into Google Chrome.



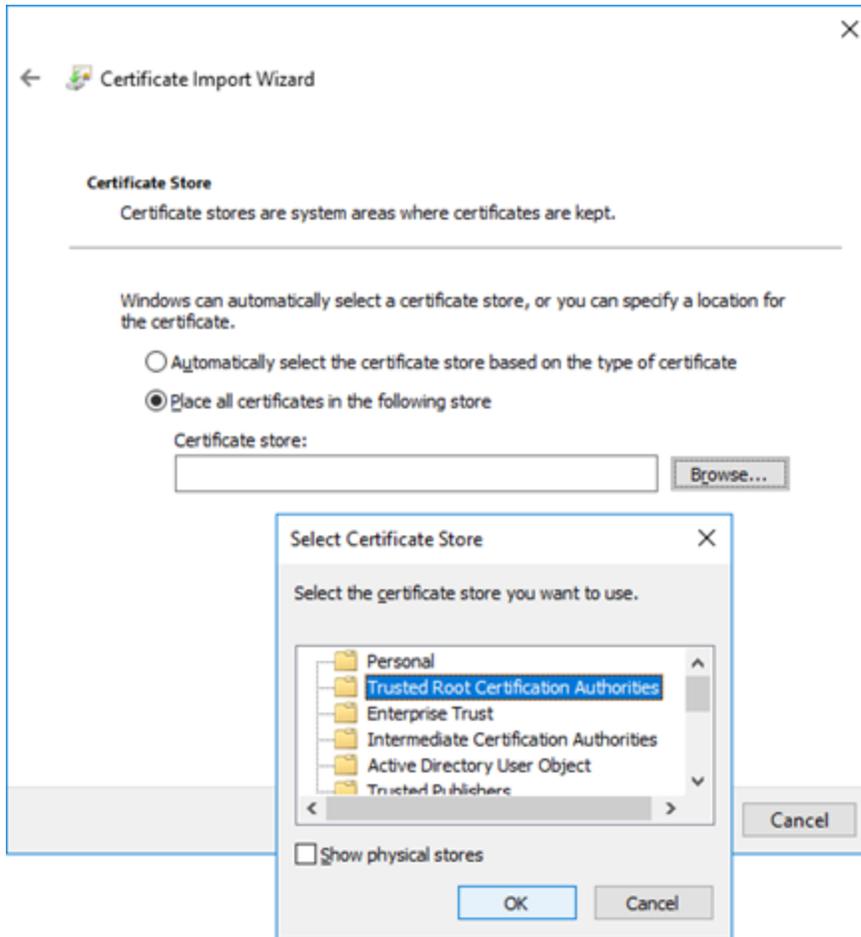
- d. Click *Install Certificate*.



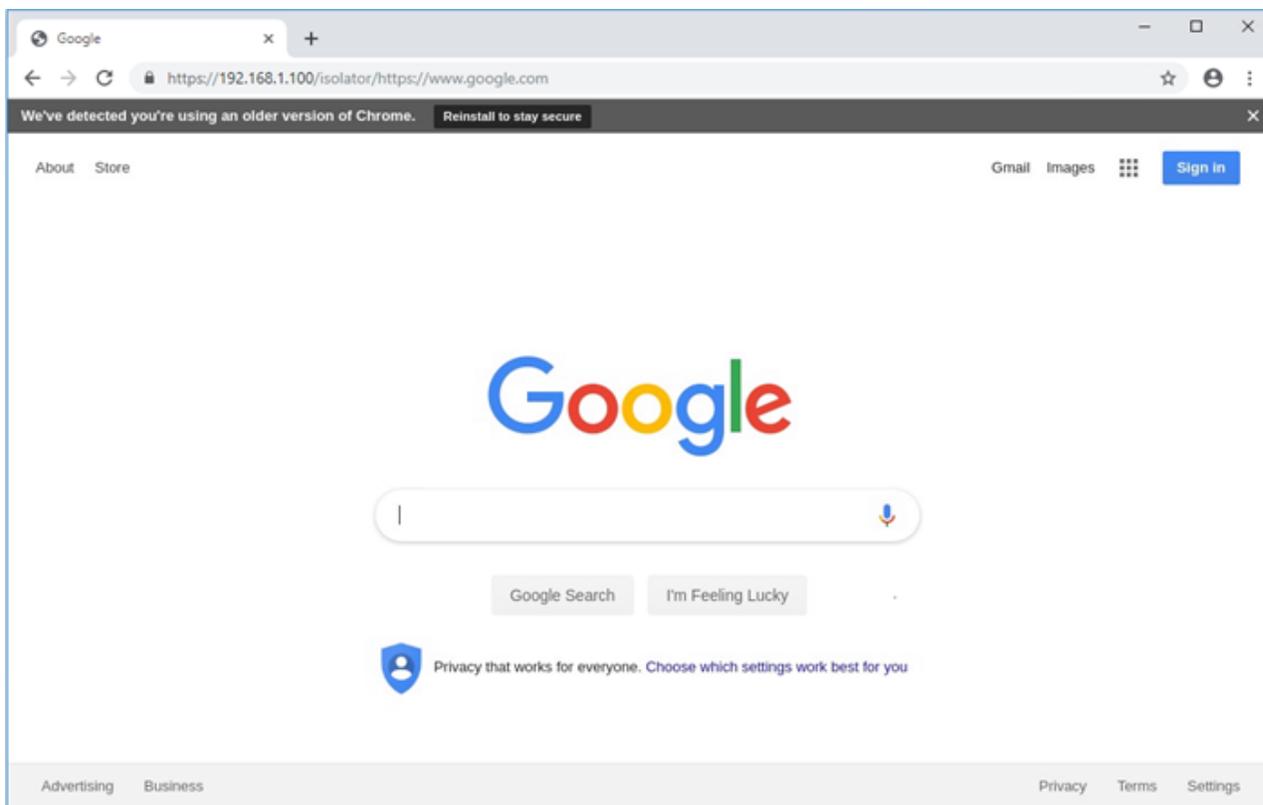
- e. Select *Local Machine*, and click *Next*.



- f. Select *Trusted Root Certification Authorities*, and click *OK*.



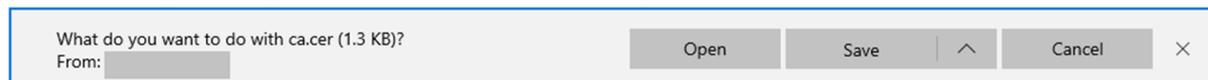
2. In the Google Chrome browser address bar, type `https://<internal_IP_address>/isolator/https://www.<website-url>.com` (for example, `https://192.168.1.100/isolator/https://www.google.com`).
- where `<internal_IP_address>` value is the IP address of the Fortisolator internal interface.



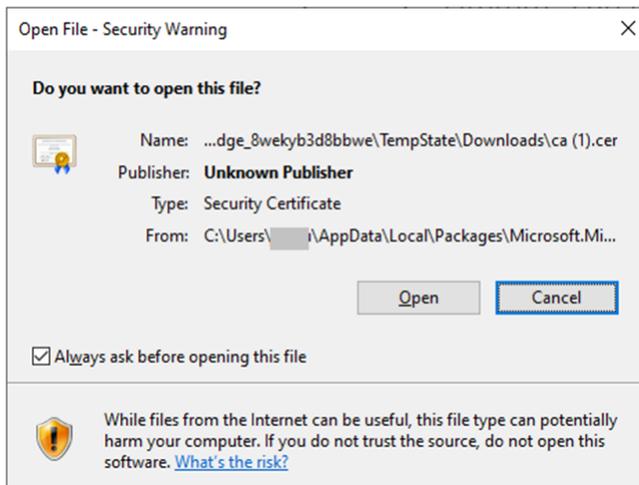
Using IP Forwarding mode with Edge

To configure IP Forwarding mode with Edge browser:

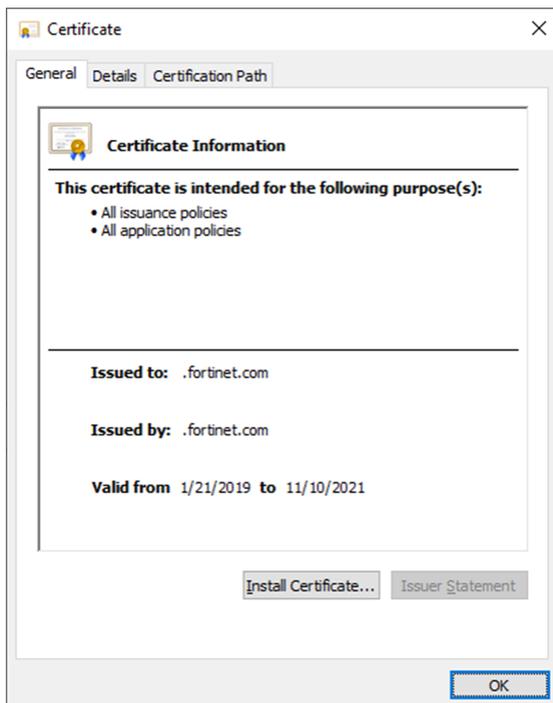
1. Download the Fortisolator certificate (ca.crt) and import it into your Edge browser:
 - a. In the Edge browser address bar, type `http://<internal_IP_address>/ca.crt` (for example, `http://192.168.1.100/ca.crt`).
 - where `<internal_IP_address>` value is the IP address of the Fortisolator internal interface.
 - b. In the security warning at the bottom of the browser, click **Save** to download the certificate.



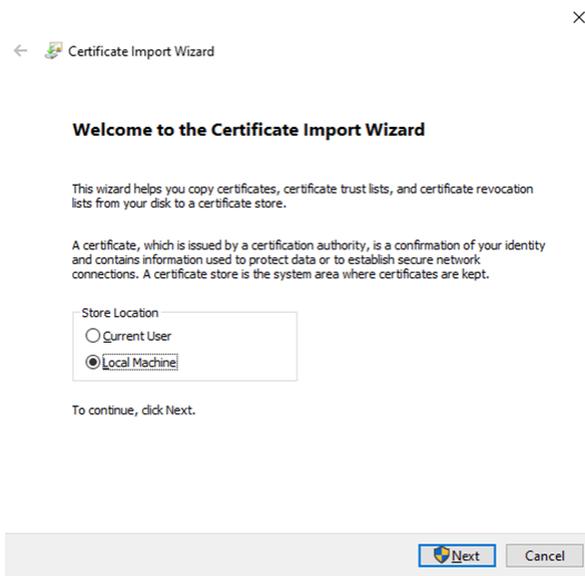
- c. Click *Open* to import the ca.crt certificate into Edge.



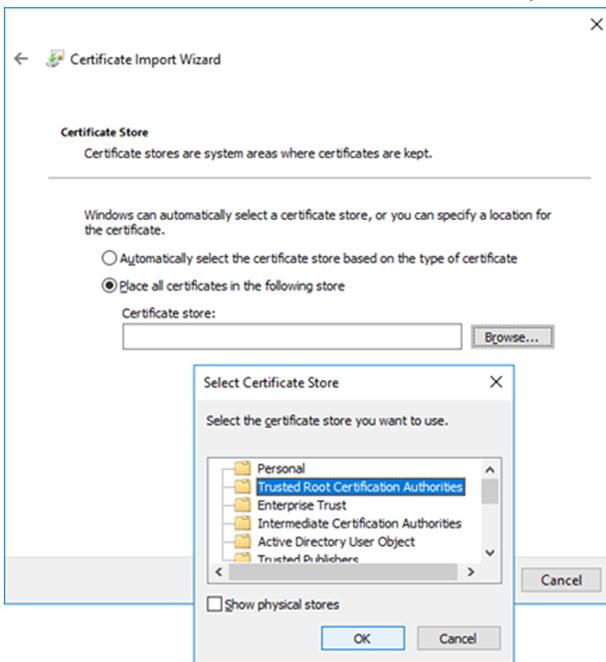
- d. Click *Install Certificate*.



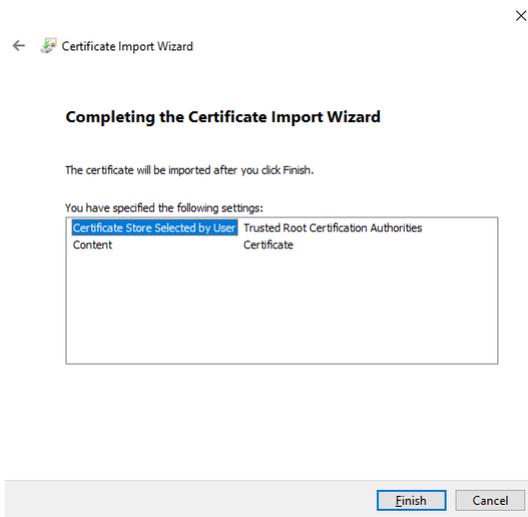
- e. Select *Local Machine*, and click *Next*.



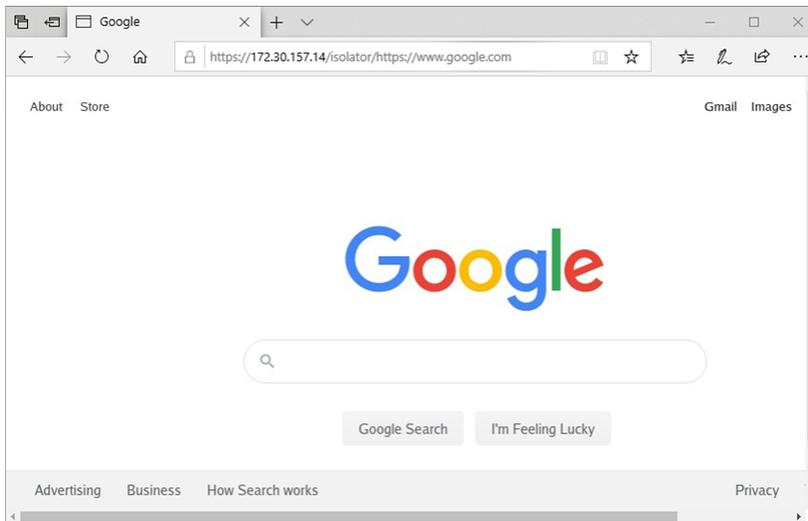
- f. Select *Trusted Root Certification Authorities*, and click *OK*.



g. Completing the Certificate Import Wizard.



- In the Edge browser address bar, type `https://<internal_IP_address>/isolator/https://www.<website-url>.com` (for example, `https://172.30.157.14/isolator/https://www.google.com`) where `<internal_IP_address>` value is the IP address of the Fortisolator internal interface.



Proxy mode

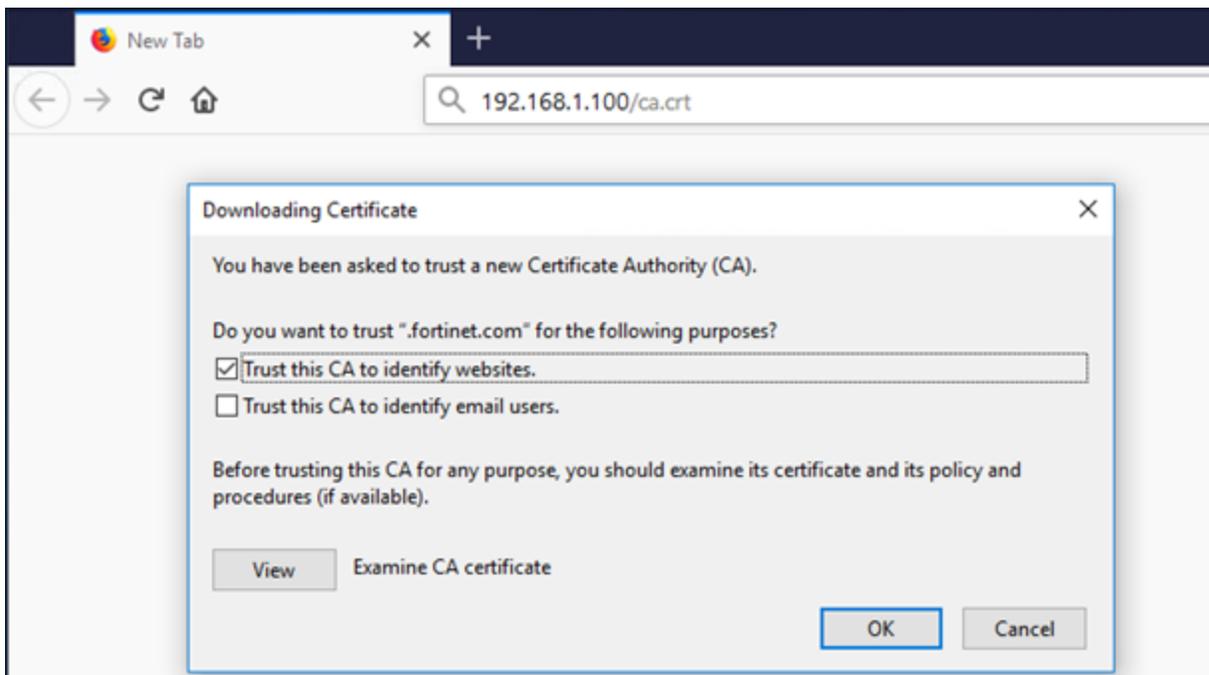
You can configure Fortisolator to run in Proxy mode using the following types of browsers:

- [Using proxy mode with Mozilla Firefox on page 65](#)
- [Using proxy mode with Google Chrome on page 68](#)
- [Using proxy mode with Edge on page 77](#)

Using proxy mode with Mozilla Firefox

To configure proxy mode with Mozilla Firefox:

1. Download the Fortisolator certificate (ca.crt) and import it into the Mozilla Firefox browser:
 - a. In the Mozilla Firefox browser address bar, type `http://<internal_IP_address>/ca.crt` (for example, `http://192.168.1.100/ca.crt`).
 - where `<internal_IP_address>` is the IP address of the Fortisolator internal interface.
 - b. In the *Downloading Certificate* window, select the *Trust this CA to identify websites* checkbox.
 - c. Click *OK*.



2. Open the Mozilla Firefox browser.
3. In the menu, click *Options*.
4. Click *General*.
5. In the *Network Settings* section, click *Settings*.
6. In the *Connection Settings* window, select *Manual proxy configuration*, and enter the following settings (values shown here are examples):
 - **HTTP Proxy:** 192.168.1.100, **Port:** 8888
 - **SSL Proxy:** 192.168.1.100, **Port:** 8888
 - **No Proxy for:** "localhost, 127.0.0.1, <internal_IP_address>/24", where `<internal_IP_address>` is the IP address of the Fortisolator internal interface.
7. Click *OK*.

Connection Settings [X]

Configure Proxy Access to the Internet

- No proxy
- Auto-detect proxy settings for this network
- Use system proxy settings
- Manual proxy configuration**

HTTP Proxy: 192.168.1.100 Port: 8888

Use this proxy server for all protocols

SSL Proxy: 192.168.1.100 Port: 8888

FTP Proxy: Port: 0

SOCKS Host: Port: 0

SOCKS v4 **SOCKS v5**

Automatic proxy configuration URL

[] Reload

No proxy for

localhost, 127.0.0.1, 192.168.1.0/24

Example: .mozilla.org, .net.nz, 192.168.1.0/24

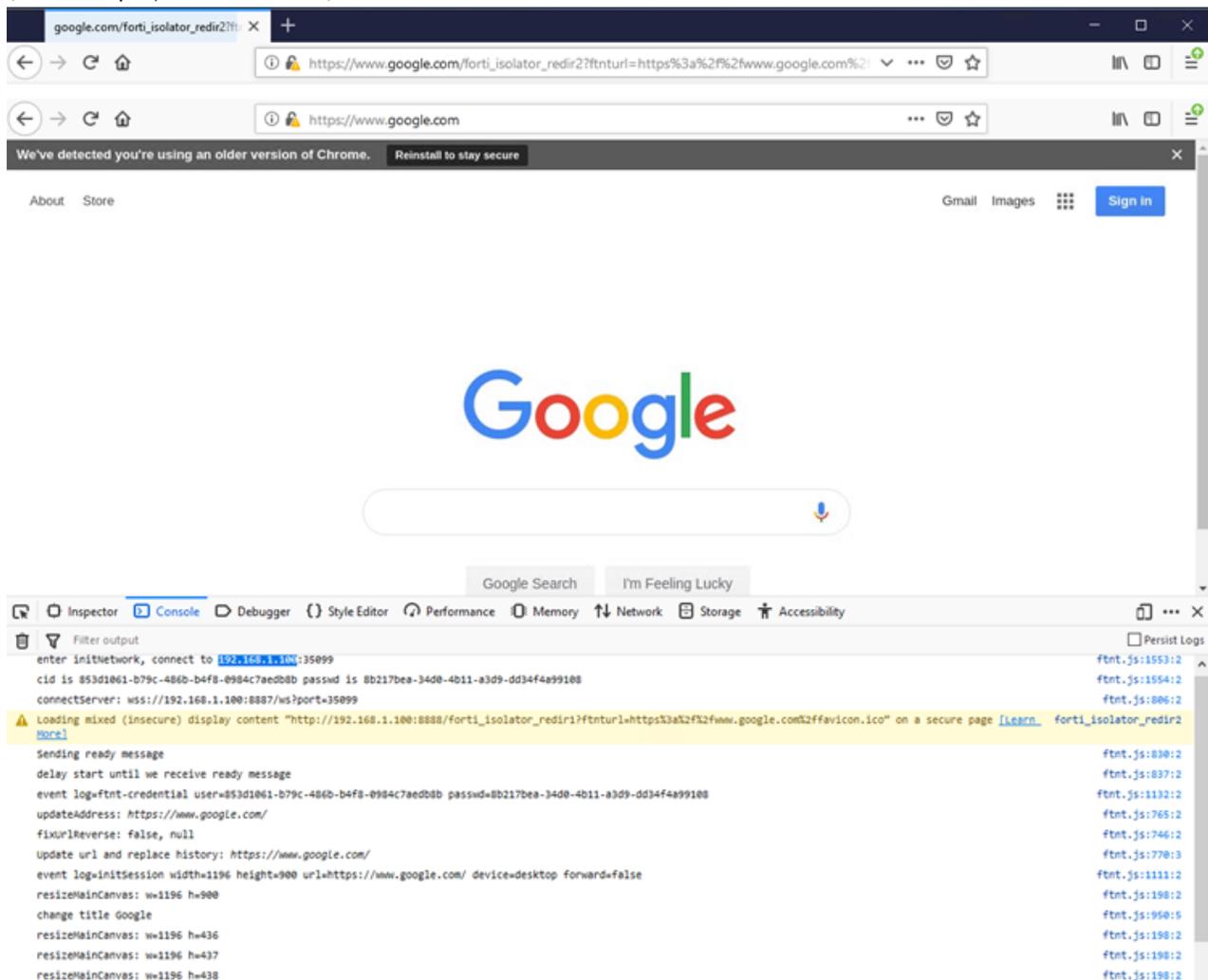
- Do not prompt for authentication if password is saved
- Proxy DNS when using SOCKS v5
- Enable DNS over HTTPS
- Use default (https://mozilla.cloudflare-dns.com/dns-query)**
- Custom []

OK Cancel Help

Verifying Fortisolator proxy mode with Mozilla Firefox

To verify that Fortisolator proxy mode is working correctly with Mozilla Firefox:

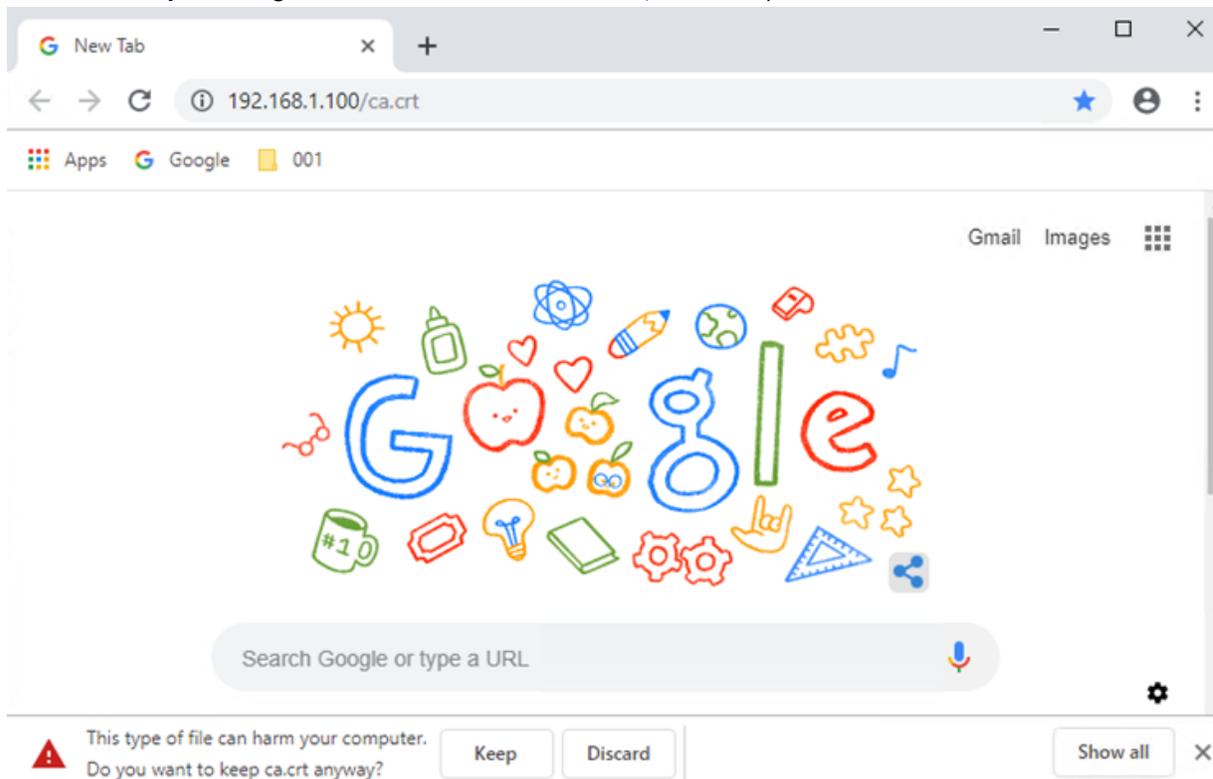
1. In the Mozilla Firefox browser, type `https://www.google.com..`
The URL redirects the browser to `forti_isolator` for a short period of time. For example, `https://www.google.com/forti_isolator_redir2?ftnturl=https%3a%2f%2fwww.google.com%2f&ftntcid=5f4084e8-7978-4c89-97c5-31ef3640600c&ftntpasswd=35026d03-9a1c-42e9-959e-fca18d67e4c0`. The page should load successfully with the URL displayed as you typed it (`https://www.google.com`).
2. Check the browser console to make sure that it is connecting to the internal IP address of Fortisolator (for example, `192.168.1.100`).



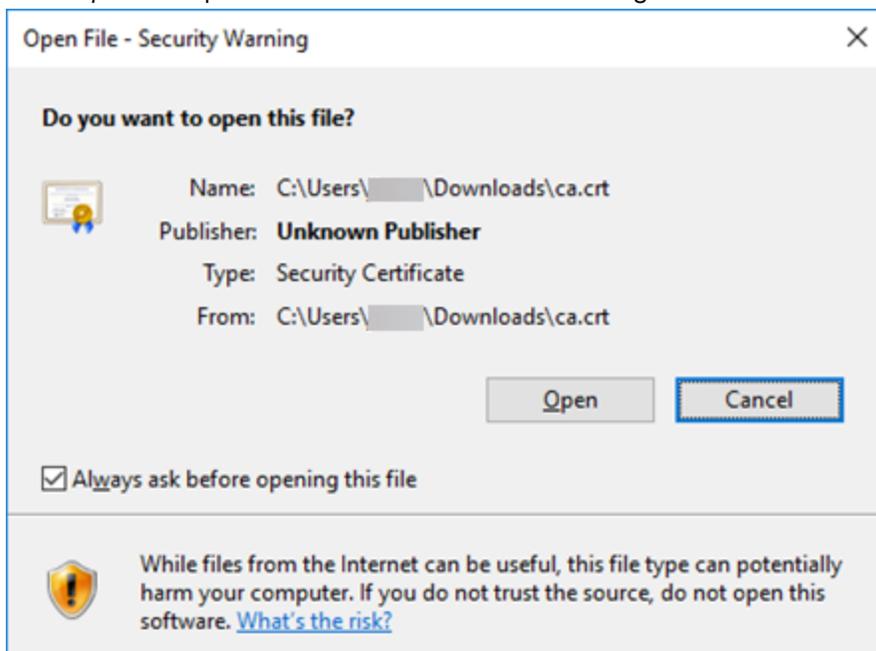
Using proxy mode with Google Chrome

To configure proxy mode with Google Chrome:

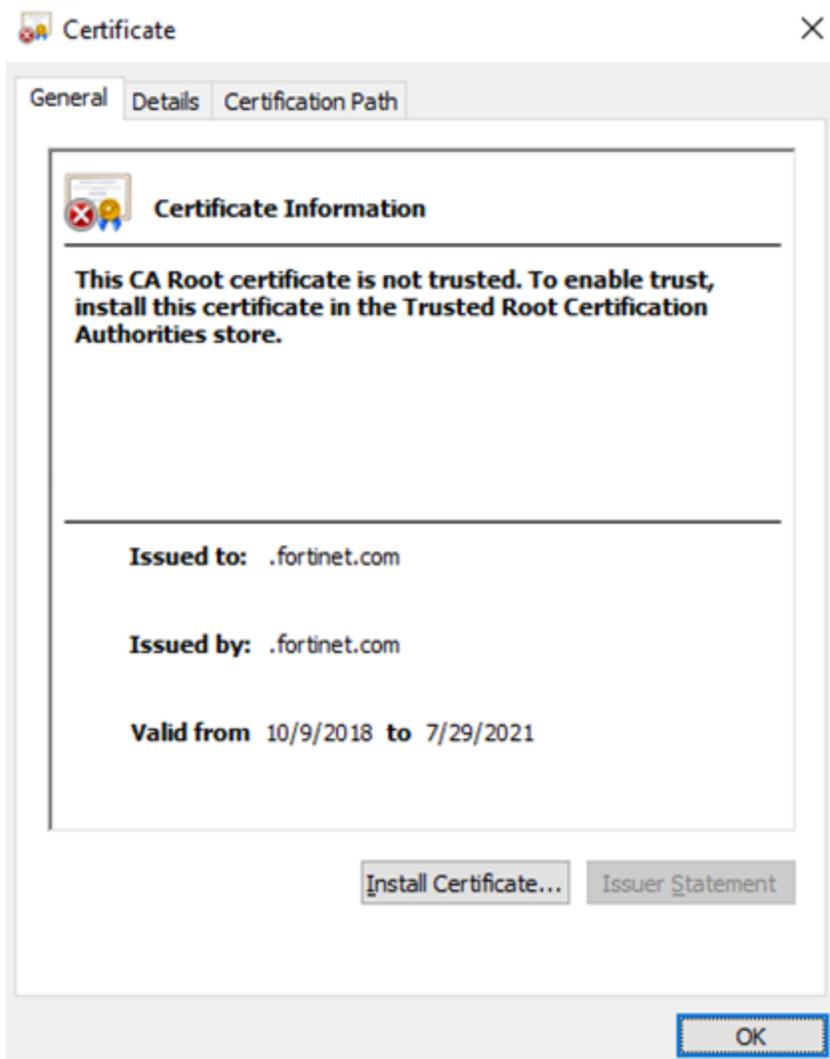
1. Download the Fortisolator certificate (ca.crt) and import it into your Google Chrome browser:
 - a. In the Google Chrome browser address bar, type `http://<internal_IP_address>/ca.crt` (for example, `http://192.168.1.100/ca.crt`).
 - where `<internal_IP_address>` value is the IP address of the Fortisolator internal interface.
 - b. In the security warning at the bottom of the browser, click **Keep** to download the certificate.



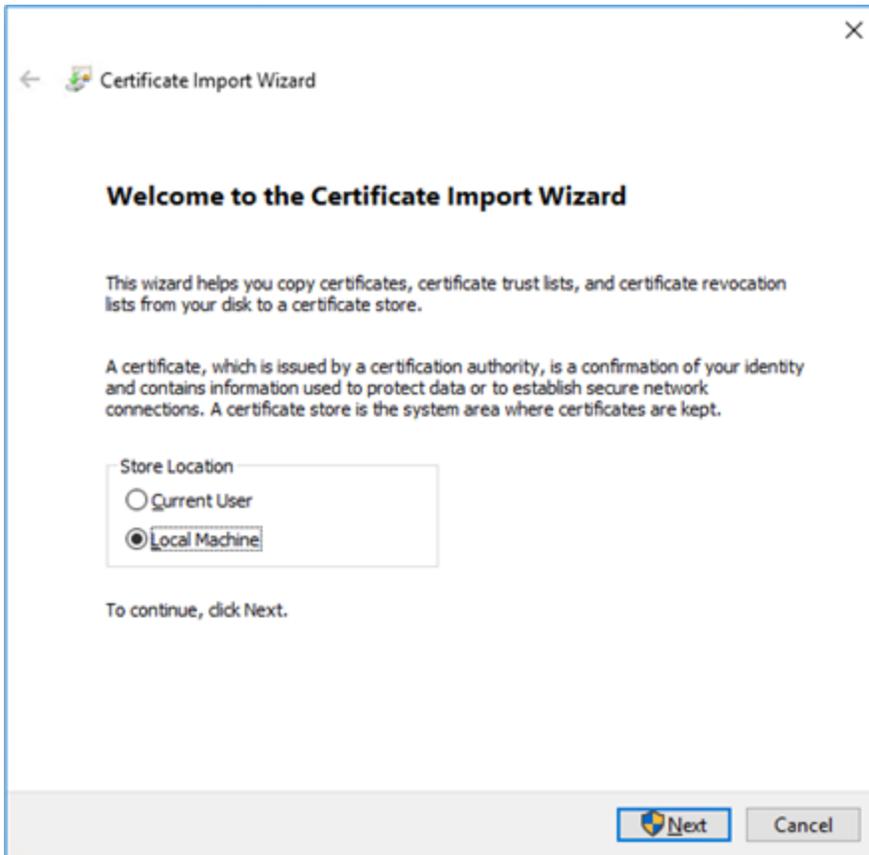
- c. Click *Open* to import the ca.crt certificate into Google Chrome.



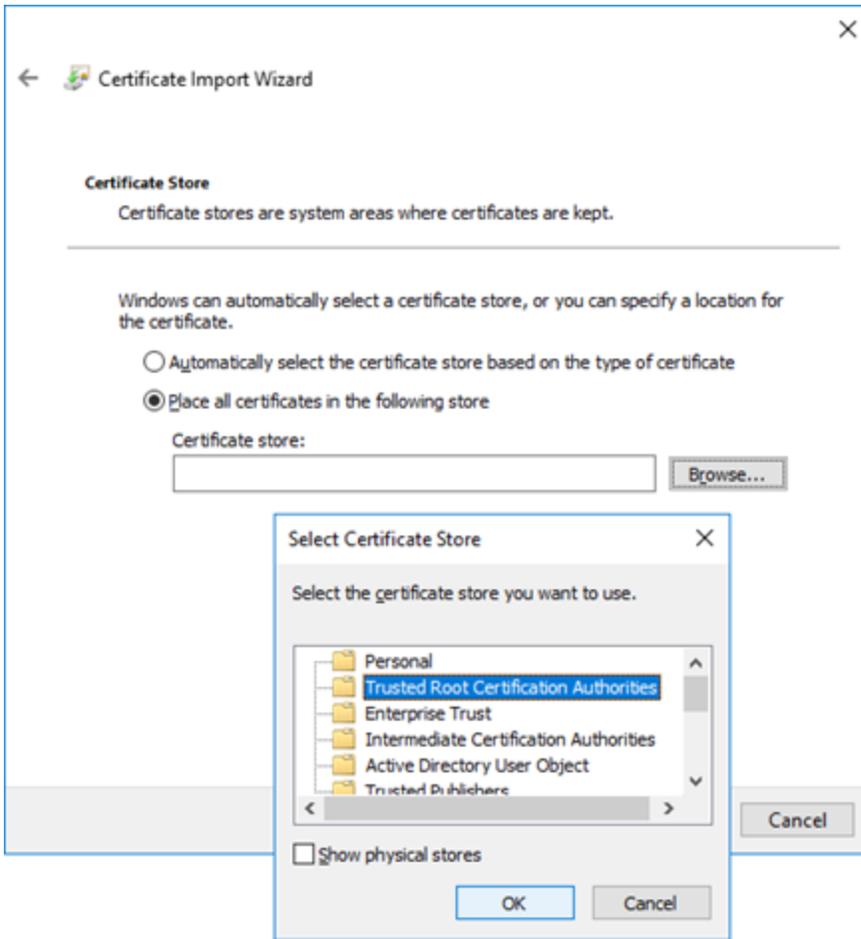
- d. Click *Install Certificate*.



- e. Select *Local Machine*, and click *Next*.

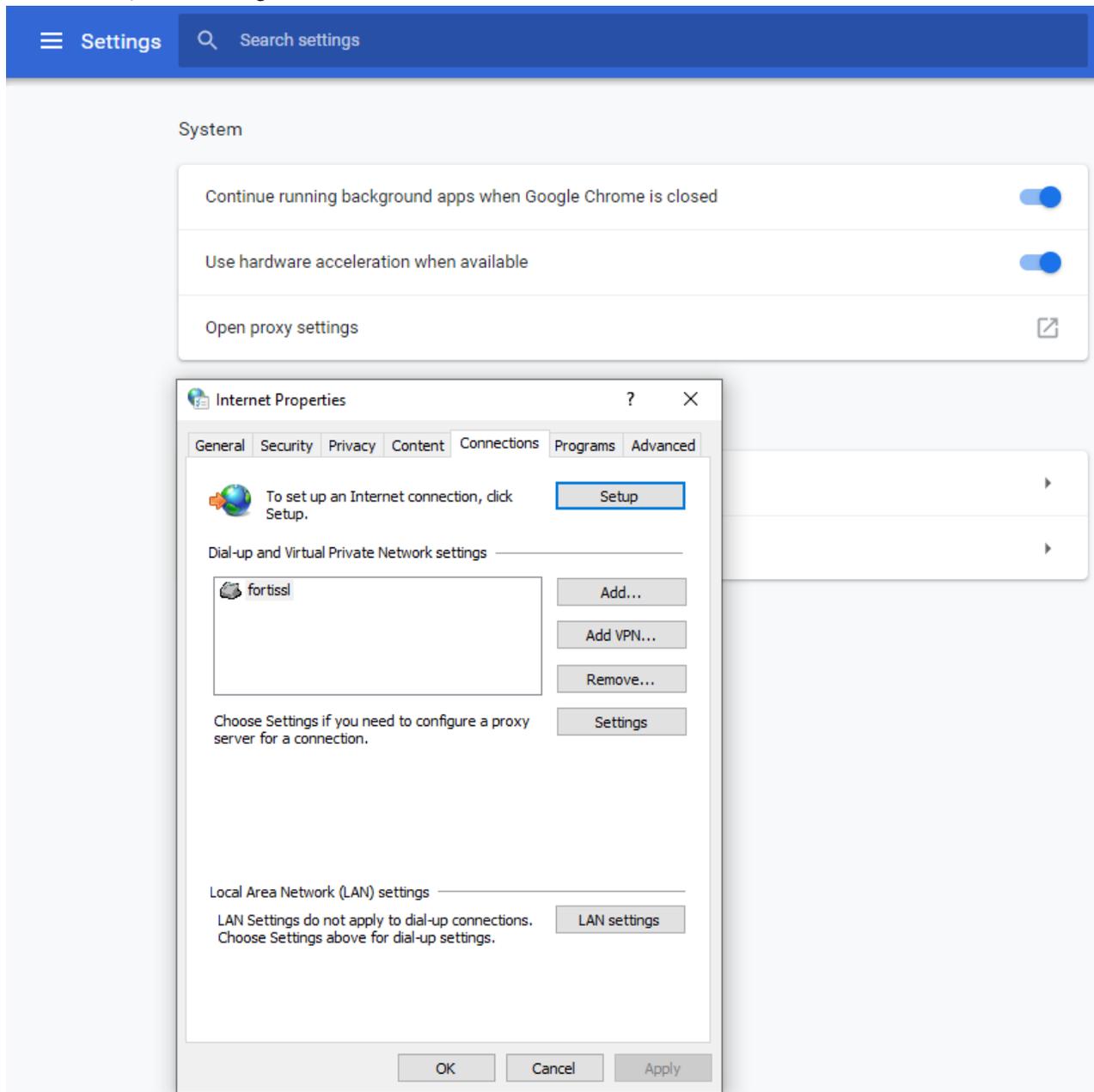


- f. Select *Trusted Root Certificate Authorities*, and click *OK*.

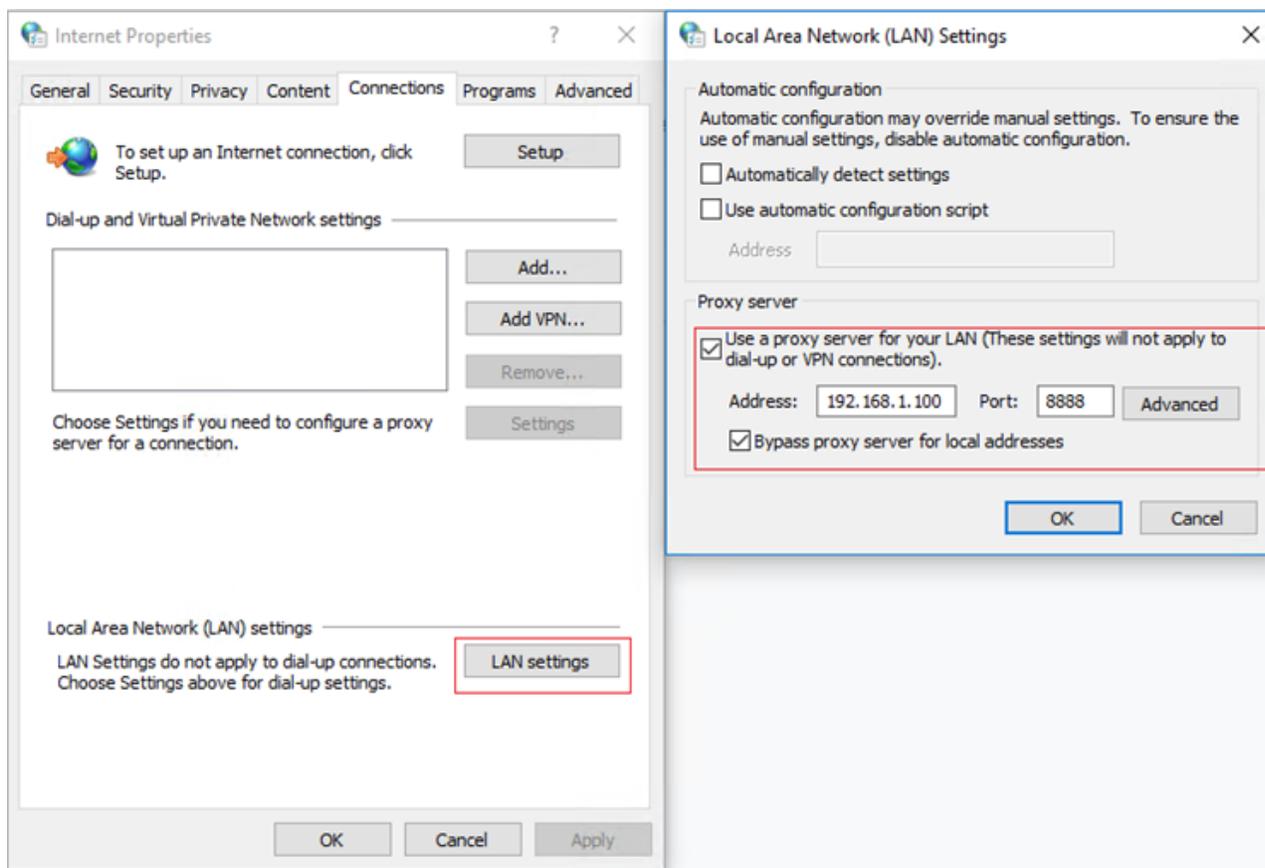


- 2. Open the Google Chrome browser.

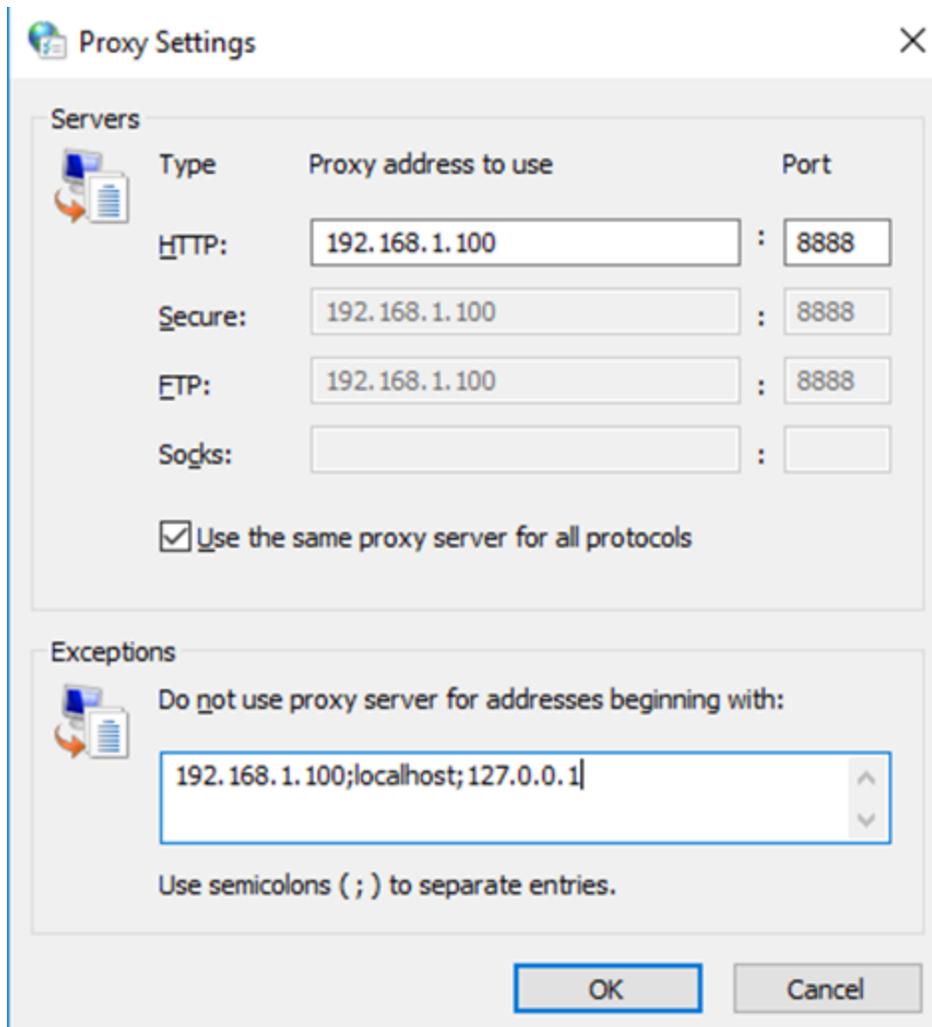
3. In the menu, click *Settings*.



4. Expand *Advanced*.
5. In the *System* section, click *Open proxy settings*.
6. In the *Internet Properties* window, click the *Connections* tab.
7. Click *LAN settings*.
8. In the *Proxy server* section, select *Use a proxy server for your LAN*, and enter the following setting (values shown here are examples):
 - **Address:** 192.168.1.100, **Port:** 8888



9. Click *Advanced*.
10. In the *Proxy Settings* window, in the *Exceptions* section, type `192.168.1.100;localhost;127.0.0.1` (values used here are examples).

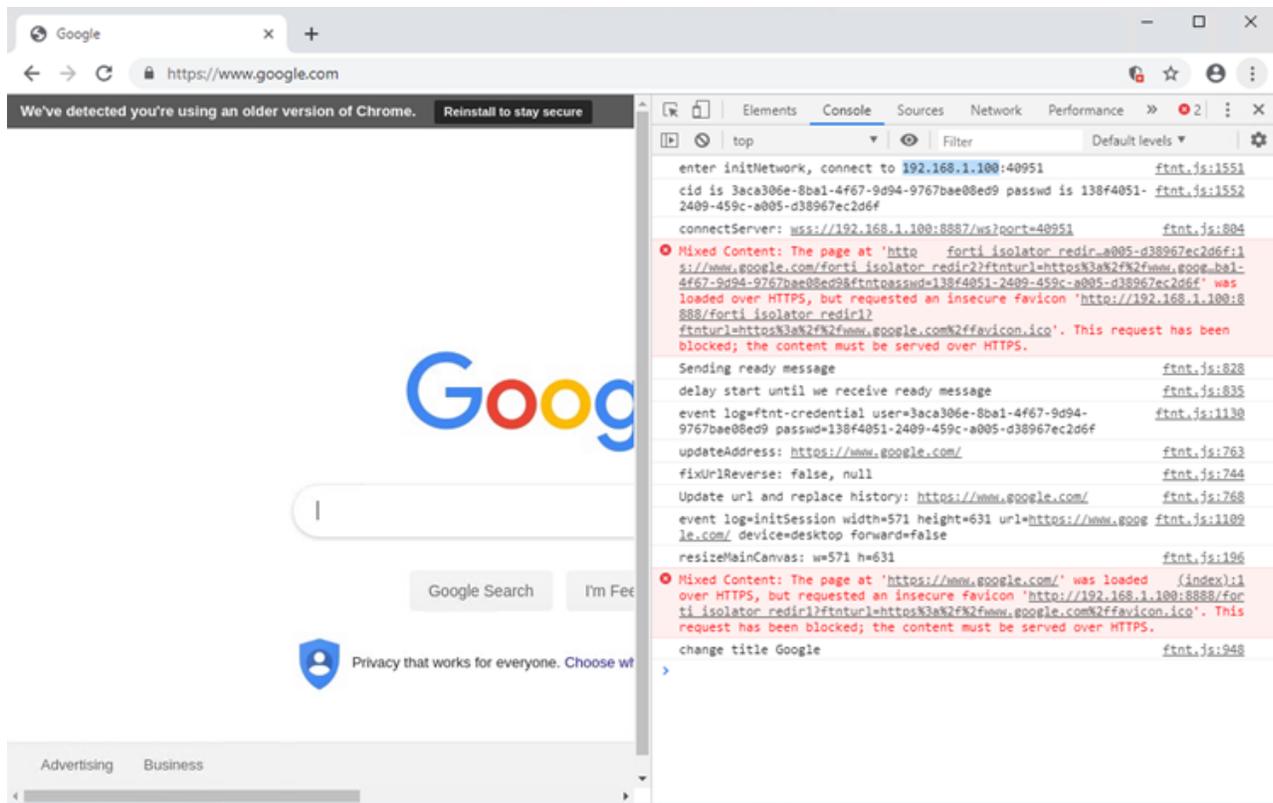


11. Click **OK** to accept the settings in all windows.

Verifying Fortisolator proxy mode with Google Chrome

To verify that Fortisolator proxy mode is working correctly with Google Chrome:

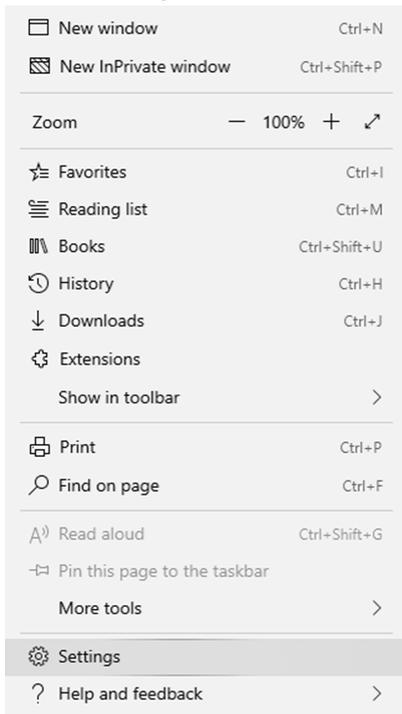
1. In the Google Chrome browser, type `https://www.google.com`.
The URL redirects the browser to `forti_isolator` for a short period of time. For example, `https://www.google.com/forti_isolator_redir2?ftnturl=https%3a%2f%2fwww.google.com%2f&ftntcid=3aca306e-8ba1-4f67-9d94-9767bae08ed9&ftntpasswd=138f4051-2409-459c-a005-d38967ec2d6f`. The page should load successfully with the URL displayed as you typed it (`https://www.google.com`).
2. Check the browser console to make sure that it is connecting to the internal IP address of Fortisolator (for example, `192.168.1.100`).



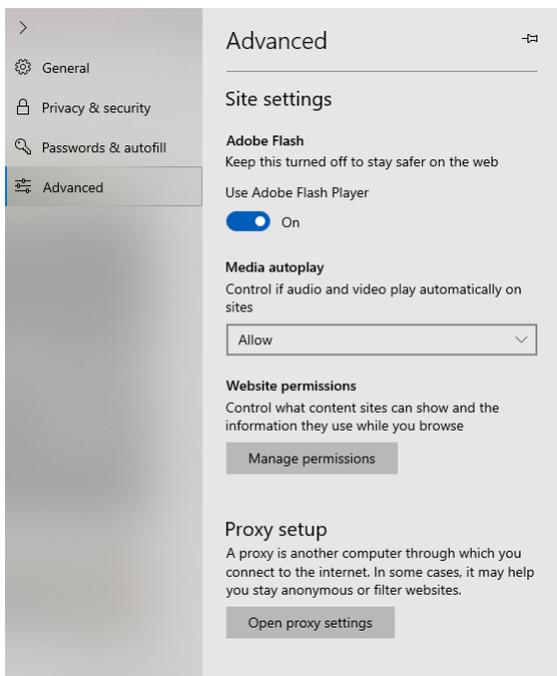
Using proxy mode with Edge

To configure proxy mode with Edge:

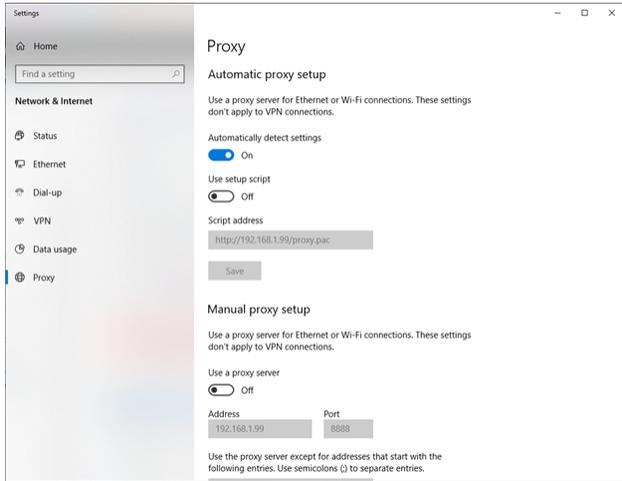
1. Open an Edge browser and click the gear icon at the top right corner to open browser settings.
2. Select *Settings* from the menu.



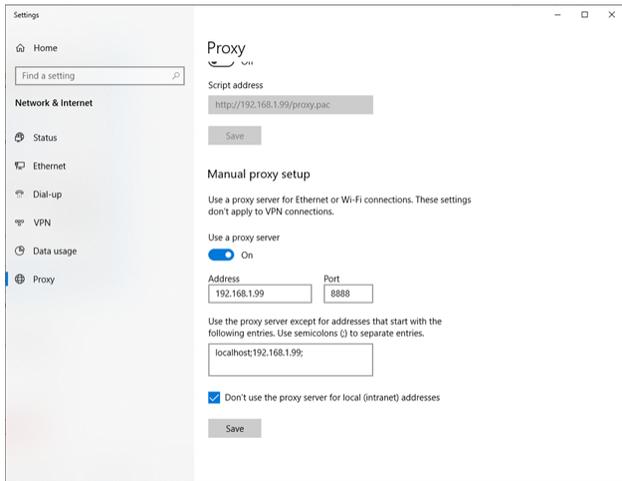
3. Click *Advanced*.



4. Under *Proxy setup*, click on *Open proxy settings*.

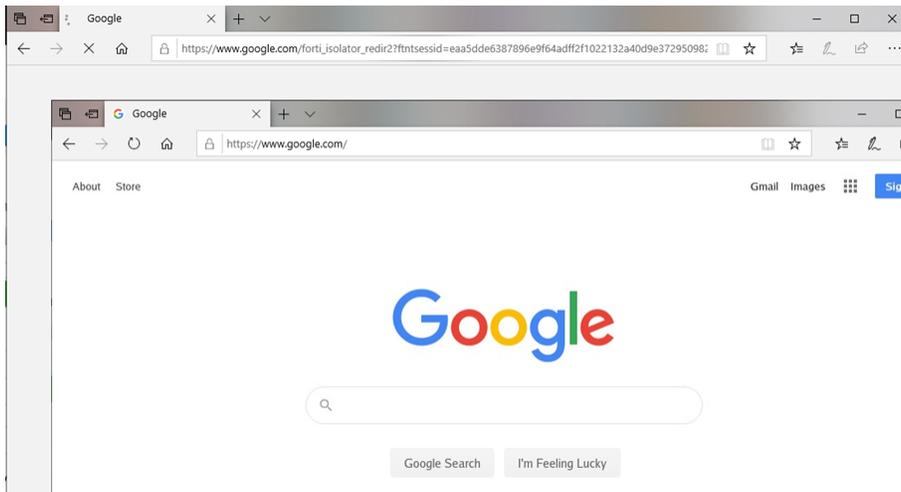


5. Enable *Manual proxy setup*, paste your proxy IP address into the *Address* field with *port 8888* and exception list:



6. Click *Save* to exit from Settings, and restart Edge browser.

Verifying Fortisolator proxy mode with Edge



Logging in as an end user

Depending on the [Global policy on page 45](#) that applies to the end user, the user can log into Fortisolator in one of the following ways:

- **Local user** - The user enters the designated username and password configured in [User definition on page 31](#). This option is available only if *Guest Type* of the global policy is *guest enable* or *guest disable*.
- **Guest user** - The user logs in as a guest without the need to enter a username or password. This option is available only if *Guest Type* of the global policy is *guest enable* or *guest only*.
 - In *guest enable* mode, the user leaves *Username* and *Password* fields blank and checks the *Guest* box to log in as a guest.
 - In *guest only* mode, the user can browse sites without being prompted to log in.
- **SAML Single Sign On** - If a SAML server is configured through FortiAuthenticator in [SAML servers on page 27](#), the user can log in with single-sign-on by clicking the *SAML Single Sign On* link and entering the credentials. This option is available only if *Guest Type* of the global policy is *guest enable* or *guest disable*.

Copying and pasting text

To copy and paste text in a browser that is running through Fortisolator:

1. In a browser, select text that you want to copy, and then right-click.
2. Click *Copy*.
3. Navigate to the location where you want to paste the text, and then right-click.
4. Click *Paste*.

Copying and pasting images

To save images from in a browser that is running through Fortisolator:

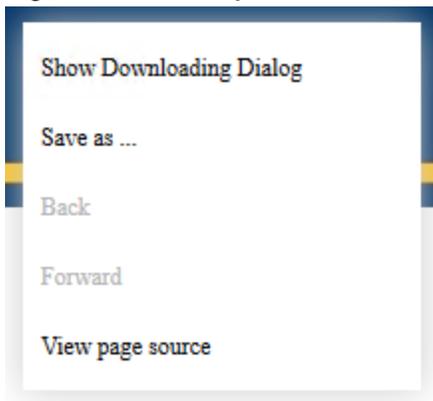
1. In a browser, right-click on the images that you want to save.
2. Click *Copy Image to clipboard*.
3. Open MS Word, MS Excel, or MS Powerpoint
4. Press Ctrl+V or right-click to paste the image.

Downloading files

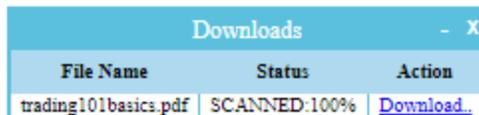
End users are able to download files up to a certain file size while browsing through Fortisolator if the administrator has configured the Isolator Profile settings to allow it.

To download a file:

1. Right-click the file you want to download and a menu appears.



2. Click *Save as...* and the *Downloads* dialog box pops up, displaying the file name and a link to download the file. If the vscanner capability is enabled on the Isolator profile settings by the administrator, the dialog will show the scanning status of the file.



File Name	Status	Action
trading101basics.pdf	SCANNED:100%	Download..

3. Once the file has been scanned, the file is now safe to download. Click the *Download* link under *Action* to download the file.

Adding Web Isolation Profile from Fortisolator to FortiProxy

Fortisolator supports adding a web isolation profile from Fortisolator to FortiProxy.

Fortisolator setup

To download Fortisolator CA certificate:

1. Connect to Fortisolator.
2. Go to *Dashboard > System Information > Isolator CA Certificate > Backup/Restore*.
3. Backup the CA Certificates by pressing *Click here*. Save the `ca_cert.tgz` file to your local system.
4. Unzip `ca_cert.tgz` and save the files, which will be use later when configuring FortiProxy.

To configure the global policy:

1. Set the Guest Type to *guest only*.
2. Set Default Isolator Profile Name to *system_default*.
3. Click *OK*.



FortiProxy Header content must be named consistently with the Fortisolator Profile name that is selected in Fortisolator Global Policy setting.

Currently the profile name "`system_default`" is being used in the example below. All settings, as in FortiProxy header content, Fortisolator Isolator Profile Name, and Fortisolator Default Isolator Profile, are using the same profile name "`system_default`".

Example

The screenshot shows the Fortisolator VM interface. On the left is a navigation menu with the following items: Dashboard, System, Users, Policies and Profiles (highlighted in green), Profile, Policy, and Global Policy (highlighted in green). The main content area is titled 'Global Policy' and contains several configuration fields:

Guest Type:	guest enable
Default Isolator Profile Name:	system_default
Default WebFilter Profile Name:	<None>
Default ICAP Profile Name:	<None>
Default Forwarding Profile Name:	<None>
Max Session Per User:	50
Max Session Per IP:	100
Auth Cookie Lifetime:	24

Fortisolator VM

Edit Profile

Isolator Profile Name:

View-only Mode:

Image Quality:

Video Frame Rate:

Scroll Speed:

Allow Right-click Action:

Allow Copy:

Allow Paste:

Allow Printing:

User Agent:

Show Isolation Icon:

Idle Timeout:

Timeout Minutes:

Broadcast Mode:

Certificates:

Max Download Size (MB):

Max Upload Size (MB):

Block File Type Download: Block All

- exe
- doc;docx
- ppt;pptx
- pdf
- txt
- xls;xlsx
- png
- mp3

FortiProxy setup

To enable explicit web proxy on FortiProxy:

1. Connect to FortiProxy portal GUI: *Network > Interfaces > Port2*.
2. Enable Explicit Web Proxy: *Enable*.
3. Click *OK*.

To import Fortisolator CA certificate and create a new SSL/SSH inspection profile:

1. Import Fortisolator CA Certificate:
 - a. Connect to FortiProxy portal GUI by going to *System > Certificates > Import > CA Certificate*.
 - b. Set *Type* as *File*.
 - c. Click *Upload* and browse to select the Fortisolator CA certificate (*ca.crt*) you saved earlier.
 - d. Click *OK*
-



Doing so ensures that FortiProxy will trust Fortisolator when dealing with HTTPS traffic.

- e. Go to *System > Certificates > Import > Local Certificate*.
 - f. Select the *Certificate* type and upload the certificate file (*ca.crt*) and key file (*ca.key*) you saved earlier.
 - g. Certificate name: *FIS_CA_Cert*.
 - h. Leave everything else as it is.
 - i. Click *OK*
-



Doing so ensures that FortiProxy can use SSL Deep Inspection.

2. Create Web Proxy Profile:
 - a. Go to *Policy & Objects > Web Proxy Profile > Create New*.
Name: *FIS-read-only*
Header Client IP: *pass*
Header Via Request: *pass*
Header Via Response: *pass*
Header X Forwarded For: *add*
Header Front End Https: *pass*
Header X Authenticated User: *pass*
Header X Authenticated Groups: *pass*
Strip Encoding: *Disable*
Log Header Change: *Disable*
 - b. Go to *Header > Create New*.
ID: *1*

Name: fis-isolator-profile
Action: add-to-request
Header Content: system_default
Base64 Encoding: Disable
Add Option: new
Protocol: HTTP HTTPS

3. Create SSL/SSH Inspection Profile:

- a.** Go to *Security Profiles > SSL/SSH Inspection > Create New*.

Name: **deep_inspection2**
CA Certificate: **FIS_CA_Cert**
Leave everything else as is.

- b.** Click *OK*.

Create Isolator Server

- 1.** Go to *Policy & Objects > Isolator Server > Create New*.

Name: FIS
Comments: Fortisolator
Address Type: IP
IP: 192.168.1.18
Port: 8888

- 2.** Click *OK*.

Create Explicit Web Proxy Policy

To create a policy to isolate Unrated/Malicious websites:

- 1.** Go to *Policy & Objects > Policy > Create New*.

Type: Explicit
Name: FortiProxy_FIS
Explicit Web Proxy: web-proxy
Outgoing Interface: Internet(port1)
Source: all
Destination: all
Schedule: always
Application/Service: webproxy1
Action: ISOLATE
Isolator Server: FIS
Webproxy Profile: FIS-read-only
SSL/SSH Inspection: deep_inspection2
Log Allow Traffic: All Sessions
Log HTTP Transaction: Enable
Enable this policy: Enable
Leave the rest as it is.

- 2.** Click *OK*.

For more information about FortiProxy setup, see the following topics in the [FortiProxy Administration Guide](#):

- [Create or edit an isolator server](#)
- [Create or edit a policy](#)

Utilities and diagnostics

Utilities

Utility	Definition
nslookup	Basic tool for DNS debugging
ping	Test network connectivity to another network host
fnsysctl disp	Display conf, category or log
fnsysctl tail	Display the last part of conf, category or log

Diagnostic tools

Tool	Definition
diagnose-wf	Test and show WF action for an URL



www.fortinet.com

Copyright© 2025 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., 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 Chief Legal Officer, 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. 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.