Administration Guide

FortiIsolator 3.0.0

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

April 16, 2025
FortiIsolator 3.0.0 Administration Guide
51-300-963196-20250416

TABLE OF CONTENTS

Change log

Date	Change Description
2025-03-31	Initial release.

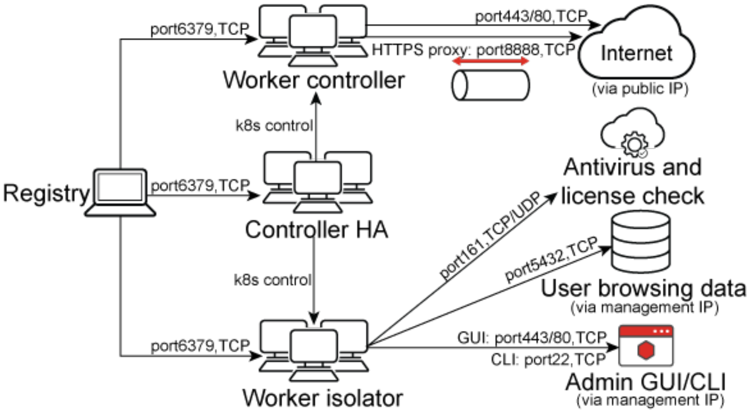
Overview

FortiIsolator 3.0.0 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 FortiIsolator, web content is executed in a remote disposable container and displayed to users visually, isolating any threat.

The FortiIsolator 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.



FortiIsolator 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 FortiIsolator, see the FortiIsolator product page and the FortiIsolator data sheet.

For release information about FortiIsolator 3.0.0, such as new features, upgrade instructions, resolved issues, and known issues, see the FortiIsolator Release Notes.

For instructions about deploying FortiIsolator 3.0.0, refer to the FortiIsolator 3.0 Private Cloud Deployment guide.

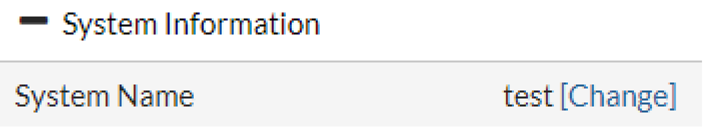
Dashboard

The FortiIsolator 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 FortiIsolator from GUI:

1. From the administration portal, click **Dashboard**, and find the **System Information** widget.
2. In the **System Time** field, click **Change**.
3. In the **Time Zone** drop-down list, select the time zone.
4. Set the time by doing one of the following tasks:
   - To set the time manually, select *Set Time*, and select the time and date options in the drop-down lists.
   - To configure an NTP server, select *Synchronize with NTP Server* and enter the IP address of the NTP server.
5. Click *Apply*.

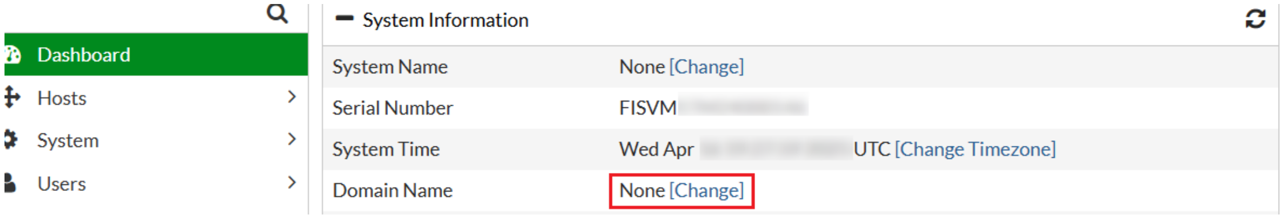
To setup system time from CLI:

```
> 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*.



System Name	None [Change]
Serial Number	FISVM[redacted]
System Time	Wed Apr [redacted] UTC [Change Timezone]
Domain Name	None [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

FortiIsolator 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 FortiIsolator 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 FortiIsolator.

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

Once you successfully configure the FortiIsolator, it is important to back up the configuration. In some cases, you may need to reset the FortiIsolator to factory defaults or perform a TFTP upload of the firmware, which will erase the existing configuration. In these instances, the configuration on the device will have to be recreated, unless a backup can be used to restore it. You should also back up the local certificates as well.

We also recommend to back up the configuration after any changes are made, to ensure you have the most current configuration available. Also, back up the configuration before any upgrades of the FortiIsolator's firmware. Should anything happen to the configuration during the upgrade, you can easily restore the saved configuration.

Always back up the configuration and store it on the management computer or off-site. You have the option to save the configuration file to various locations including the local PC and USB key.

The current version of FortiIsolator is available for configuration backup and restore through GUI only.

Backing up the 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*, it navigates to *System Backup* page.
3. In the *Config File* section, *Click here* to download the configuration file (`isolator.conf`).
   - This will save the configuration file into your local system. To restore the configuration, upload the configuration file in the *Restore System* tab in the Maintenance GUI, which will reboot the FortiIsolator.

Backing up the system

To back up the whole system:

1. From the administration portal, click *Dashboard*, and find the *System Configuration* widget.
2. In the *System Configuration* field, click *Backup/Download Config File*, it navigates to *System Backup* page.
3. In the *Backup* section, *Click here* to save the system backup file (`.tar.xz`).
   - This will save the backup file into your local system. To restore the system, upload the system backup file in the *Restore System* tab in the Maintenance GUI, which will reboot the FortiIsolator.

FortiIsolator certificates

The FortiIsolator CA certificate is required for access to the FortiIsolator. By default, the FortiIsolator 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 FortiIsolator database and a matching management certificate for accessing the FortiIsolator 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 FortiIsolator to visit websites unless you use a global CA certificate that grants global access to websites at browser level.

FortiIsolator 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 FortiIsolator 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 FortiIsolator 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 FortiIsolator 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 FortiIsolator 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 FortiIsolator 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 FortiIsolator using SSH or the FortiIsolator 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. FortiIsolator 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 FortiIsolator 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 FortiIsolator. 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 FortiIsolator. 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 FortiIsolator. 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.

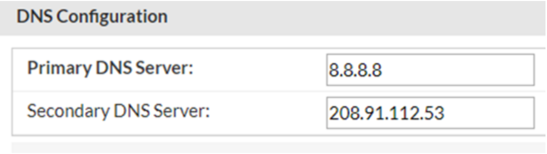
To change the HA IP address from CLI, use the following command:

```
> 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:	8.8.8.8
Secondary DNS Server:	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 FortiIsolator.

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

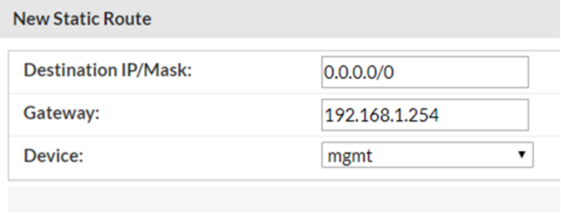
To delete a static route:

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:	0.0.0.0/0
Gateway:	192.168.1.254
Device:	mgmt ▾

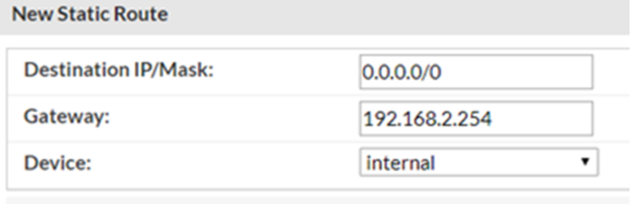
To set up system routing for management IP from CLI:

```
> 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

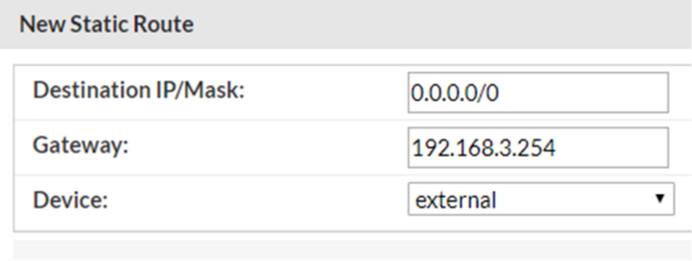
Destination IP/Mask:	0.0.0.0/0
Gateway:	192.168.2.254
Device:	internal

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:	0.0.0.0/0
Gateway:	192.168.3.254
Device:	external

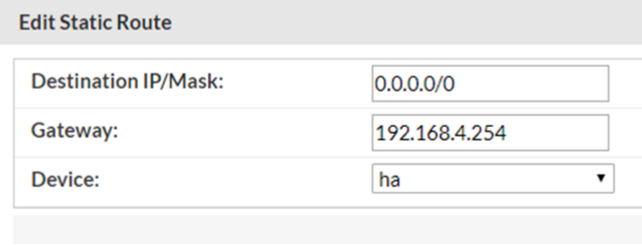
To set up system routing for external IP from CLI:

```
> 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:	0.0.0.0/0
Gateway:	192.168.4.254
Device:	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

FortiIsolator supports multiple routes per interface.

Setting up multiple routes on one interface from CLI

Creating FortiIsolator 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 FortiIsolator covers the following:

- Administrators
- Certificates
- Manage FIS Images
- Login disclaimer

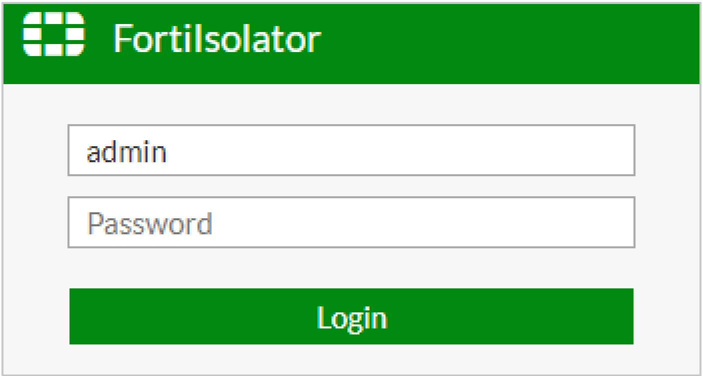
Administrators

Accessing the FortiIsolator administration portal

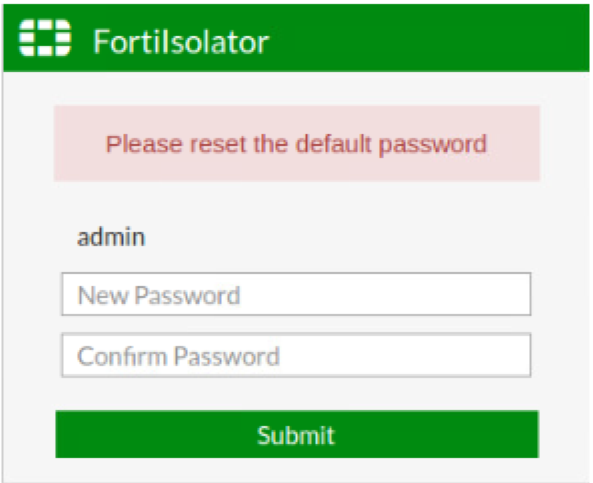
Logging in as administrator

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.



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 FortiIsolator VM license number.
2. Use the maintainer account to log into the FortiIsolator console:
   - **Account name**: `maintainer`
   - **Password**: `bcpb` plus the FortiIsolator 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 FortiIsolator 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 FortiIsolator VM license number.
2. Log into the FortiIsolator console using the maintainer account:
   - **Account name**: `maintainer`
   - **Password**: `bcpb` plus the FortiIsolator 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 FortiIsolator 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.

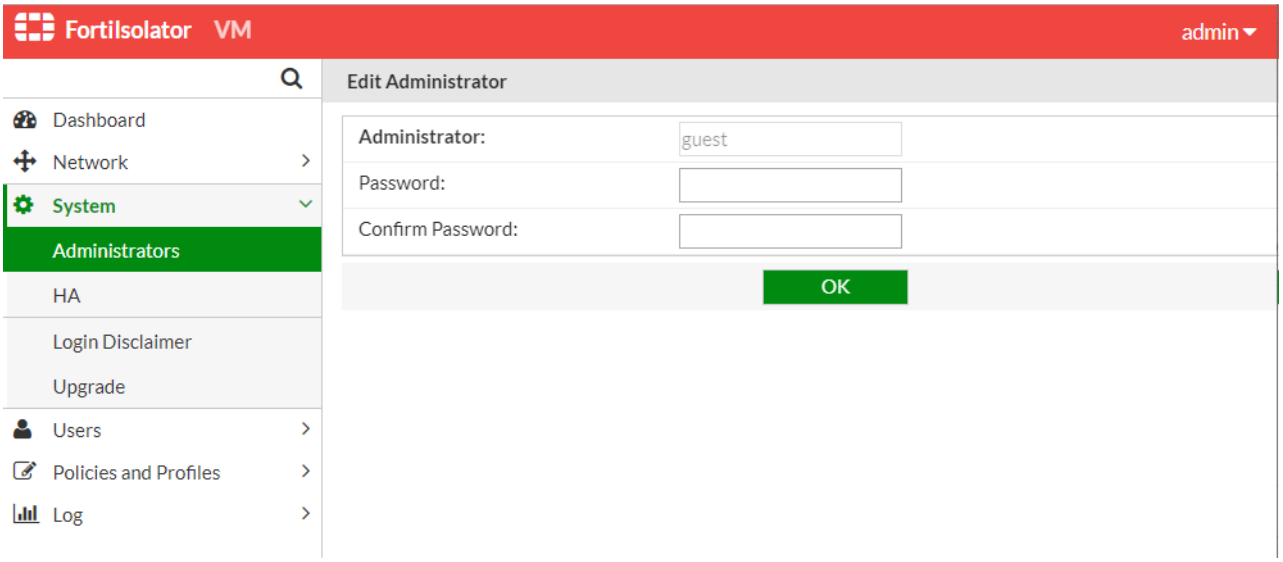
3. Reset the administrator password using the `admin-pwd-reset` command.
4. Reboot the FortiIsolator.

Setting up guest administer account

A guest administor 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 administer 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.



Edit Administrator

Administrator: guest

Password:

Confirm Password:

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

Certificates

The FortiIsolator 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.

FortiIsolator 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
LOCAL_CERT	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, FortiIsolator uses the built-in Isolator CA Certificate.
SAML_CERT	SAML Certificate	Certificate for single-sign-on which is created in *Users* > *Server* > *Create New* > *SAML Server*.
SELF SIGNED CA ROOT CERT	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 *root_ca.crt* 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
INTERMEDIATE CA CERT	Intermediate CA Certificate	This option allows the user to upload subordinate certificates of the root certificate on the FortiIsolator. Subordinate certificates must be uploaded along with the trusted root certificate (`root_ca.crt`) and upper level subordinate certificates (`sub_ca.crt`) in the certificate chain, along with the key files (`sub_ca.key`) 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.
SELF SIGNED SERVER CERT	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* > *Default 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 FortiIsolator and selected in the user's profile.

To regenerate a FortiIsolator CA Certificate:

1. Go to *Dashboard* > *FortiIsolator 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 FortiIsolator 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 FortiIsolator 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 FortiIsolator (see FortiIsolator 3.0 Private Cloud Deployment guide), you must manually upload the following package files in the *System* > *Manage FIS Images* page for full FortiIsolator functionality, such as `fis_wf` for web filtering.

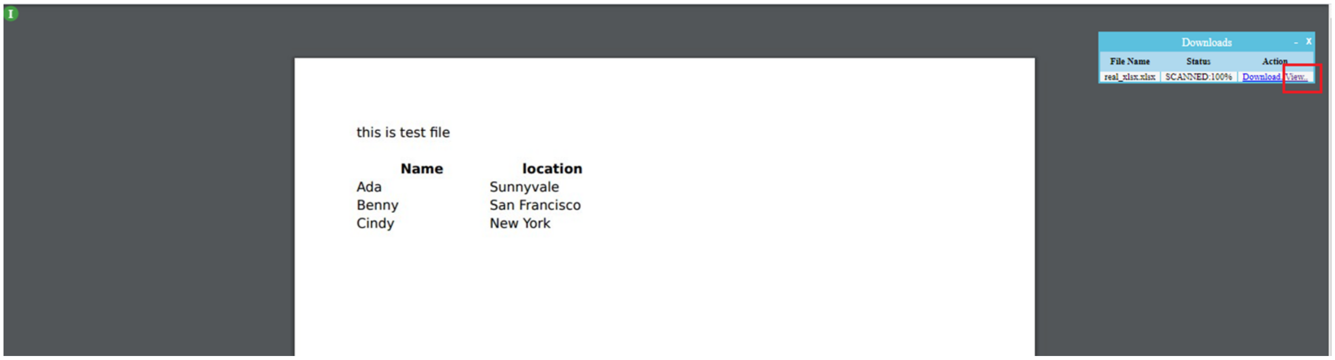
Package file	Purpose	FIS Image
`FIS_auth_DOCKER-v3-build0117.xz`	SAML authentication via FortiAuthenticator	fis_auth
`FIS_fisfs_DOCKER-v3-build0117.xz`	Web browsing	fis_fis
`FIS_log_DOCKER-v3-build0117.xz`	Log collection and management.	fis_log
`office-1.6.tar.gz`	Microsoft Office file viewing (`.doc`, `.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

For instructions about downloading these package files, see Downloading the FortiIsolator firmware and package files in the FortiIsolator 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 FortiIsolator:



File Name	Status	Action
real_xlsx.xlsx	SCANNED:100%	Download View..

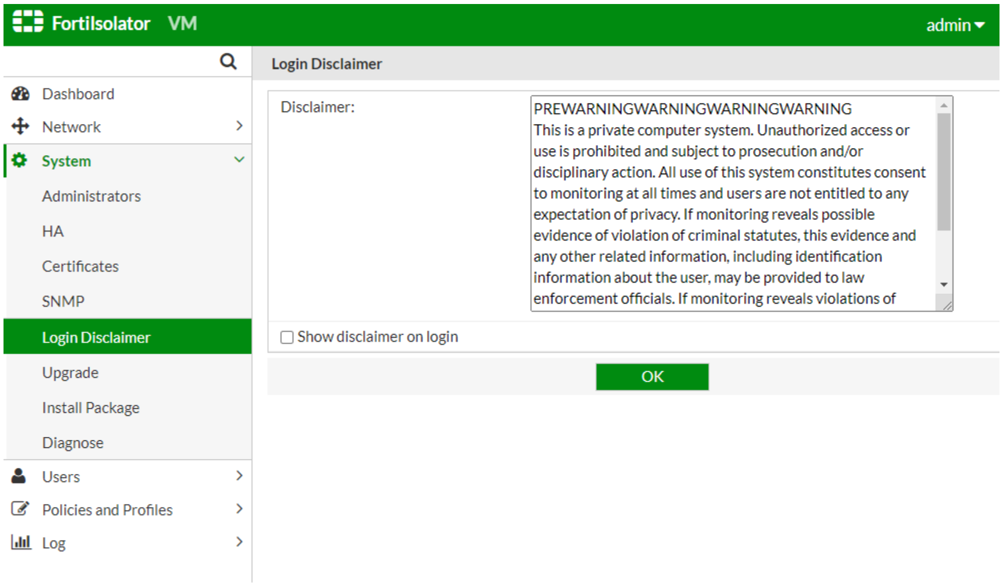
this is test file

Name	location
Ada	Sunnyvale
Benny	San Francisco
Cindy	New York

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.



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

Users

Covers the *Users* section of FortiIsolator.

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 FortiIsolator.

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 FortiIsolator.
- 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 FortiIsolator.

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.

FortiIsolator 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. FortiIsolator 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 26
2. Setup in FortiIsolator on page 29

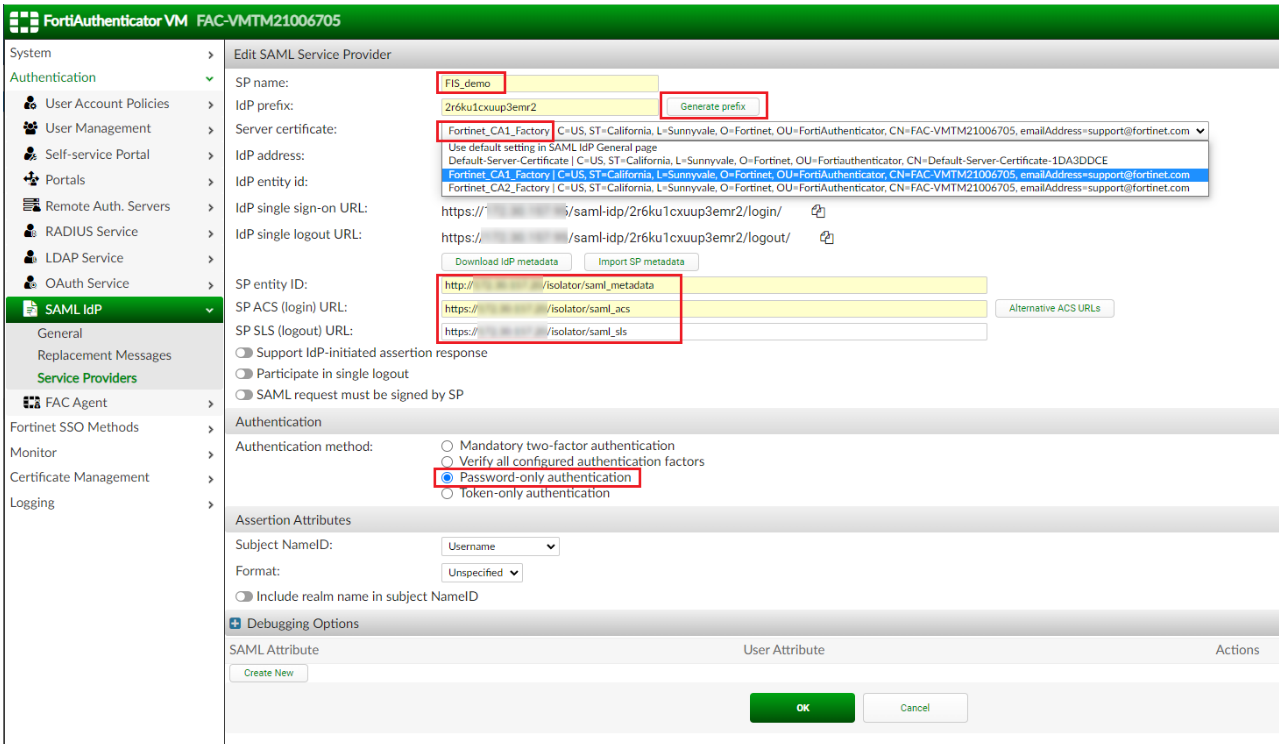
Setup in FortiAuthenticator

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	http://<*FortiIsolator ip or domain name*>/isolator/saml_metadata
SP ACS (login) URL	https://<*FortiIsolator ip or domain name*>/isolator/saml_acs
SP SLS (logout) URL	https://<*FortiIsolator ip or domain name*>/isolator/saml_sls
Authentication method	Password-only authentication

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



Edit SAML Service Provider

SP name: FIS_demo

IdP prefix: 2r6ku1cxuup3emr2 Generate prefix

Server certificate: Fortinet_CA1_Factory C=US, ST=California, L=Sunnyvale, O=Fortinet, OU=FortiAuthenticator, CN=FAC-VMTM21006705, emailAddress=support@fortinet.com

- Use default setting in SAML IdP General page
- Default-Server-Certificate | C=US, ST=California, L=Sunnyvale, O=Fortinet, OU=Fortiauthenticator, CN=Default-Server-Certificate-1DA3DDCE
- Fortinet_CA1_Factory | C=US, ST=California, L=Sunnyvale, O=Fortinet, OU=FortiAuthenticator, CN=FAC-VMTM21006705, emailAddress=support@fortinet.com
- Fortinet_CA2_Factory | C=US, ST=California, L=Sunnyvale, O=Fortinet, OU=FortiAuthenticator, CN=FAC-VMTM21006705, emailAddress=support@fortinet.com

IdP address:

IdP entity id:

IdP single sign-on URL: https://[redacted]/saml-idp/2r6ku1cxuup3emr2/login/

IdP single logout URL: https://[redacted]/saml-idp/2r6ku1cxuup3emr2/logout/

Download IdP metadata | Import SP metadata

SP entity ID: http://[redacted]/isolator/saml_metadata

SP ACS (login) URL: https://[redacted]/isolator/saml_acs Alternative ACS URLs

SP SLS (logout) URL: https://[redacted]/isolator/saml_sls

Support IdP-initiated assertion response

Participate in single logout

SAML request must be signed by SP

Authentication

Authentication method:
○ Mandatory two-factor authentication
○ Verify all configured authentication factors
● Password-only authentication
○ Token-only authentication

Assertion Attributes

Subject NameID: Username

Format: Unspecified

Include realm name in subject NameID

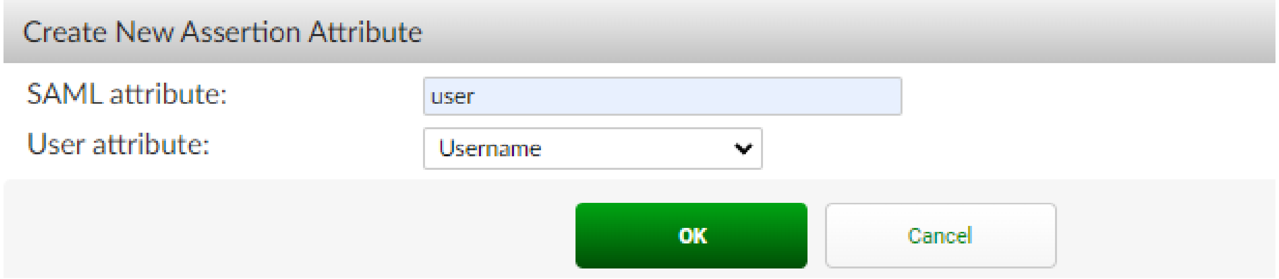
Debugging Options

SAML Attribute	User Attribute	Actions

Create New

OK | Cancel

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



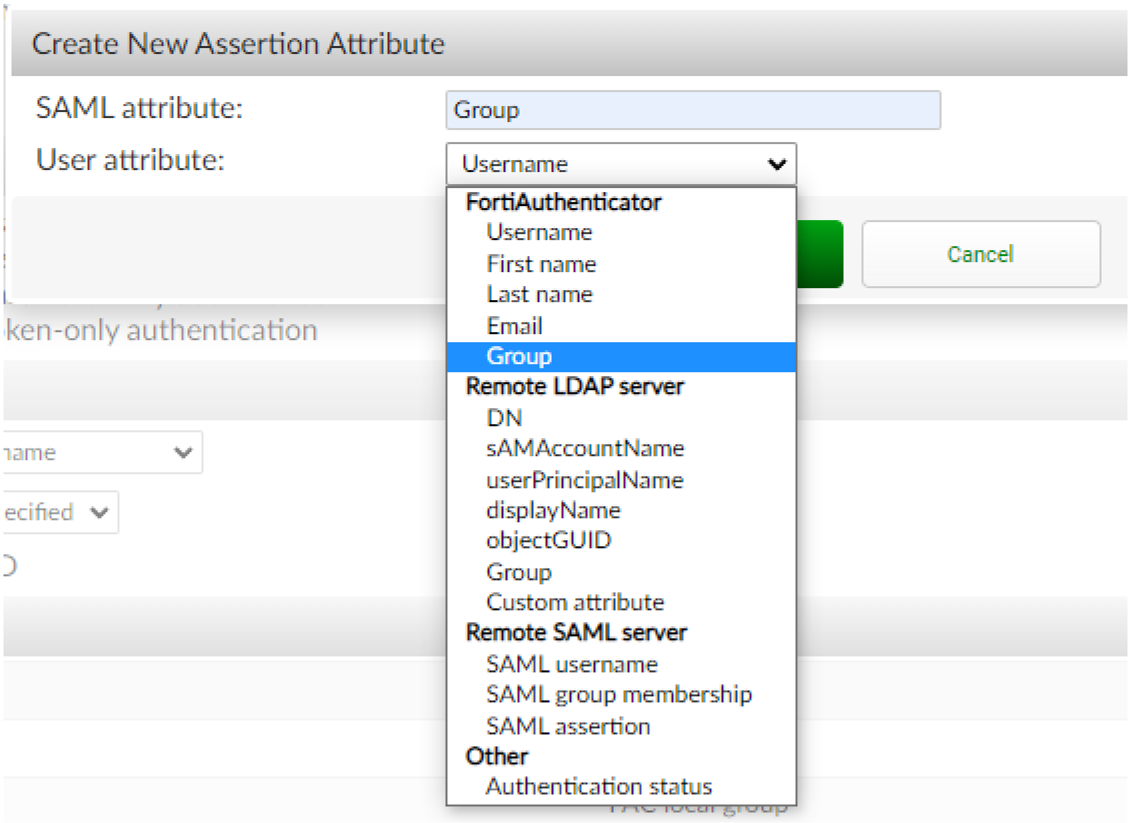
Create New Assertion Attribute

SAML attribute: user

User attribute: Username

OK | Cancel

6. Add SAML Attribute for Group

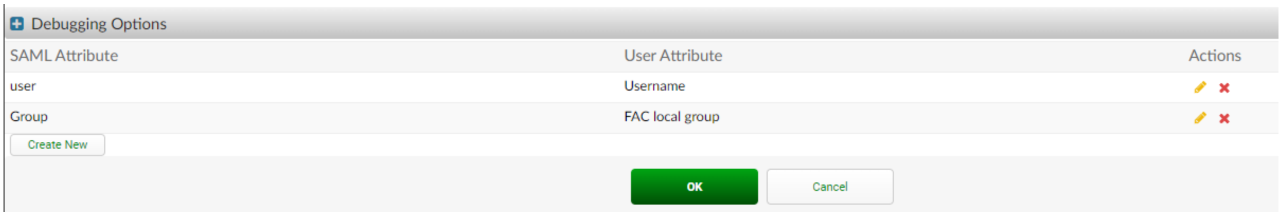


Create New Assertion Attribute

SAML attribute: Group

User attribute: Username

Debugging Options should look like this:



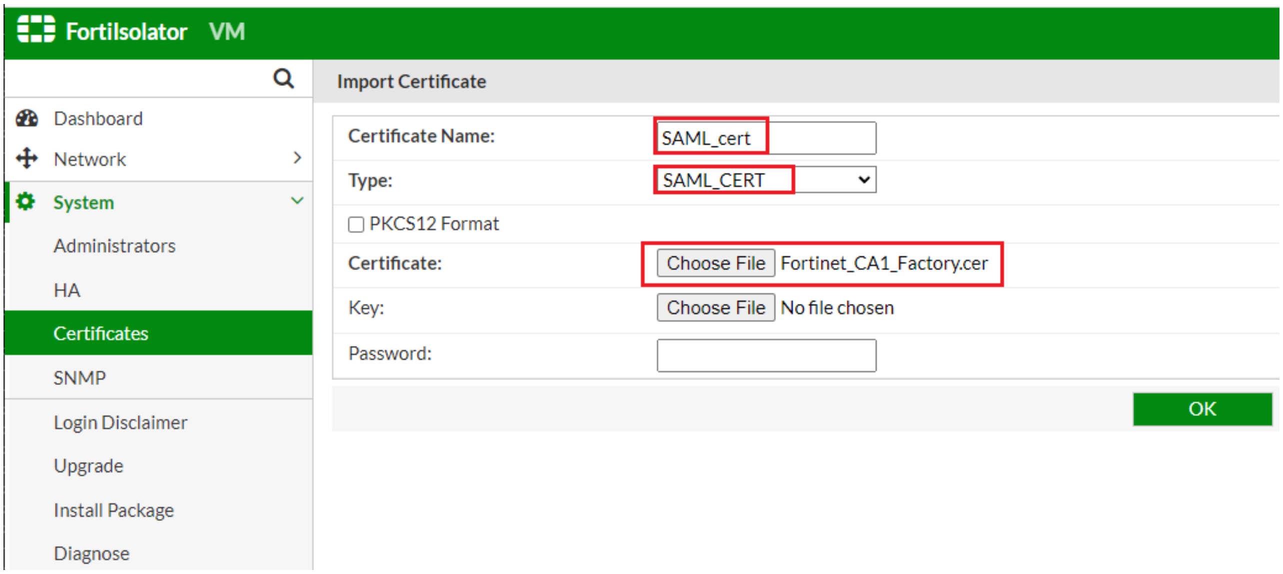
Debugging Options

SAML Attribute	User Attribute	Actions
user	Username	✎ ✖
Group	FAC local group	✎ ✖

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

Setup in FortiIsolator

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



Certificate Name: SAML_cert

Type: SAML_CERT

□ PKCS12 Format

Certificate: Fortinet_CA1_Factory.cer

Key: No file chosen

Password:

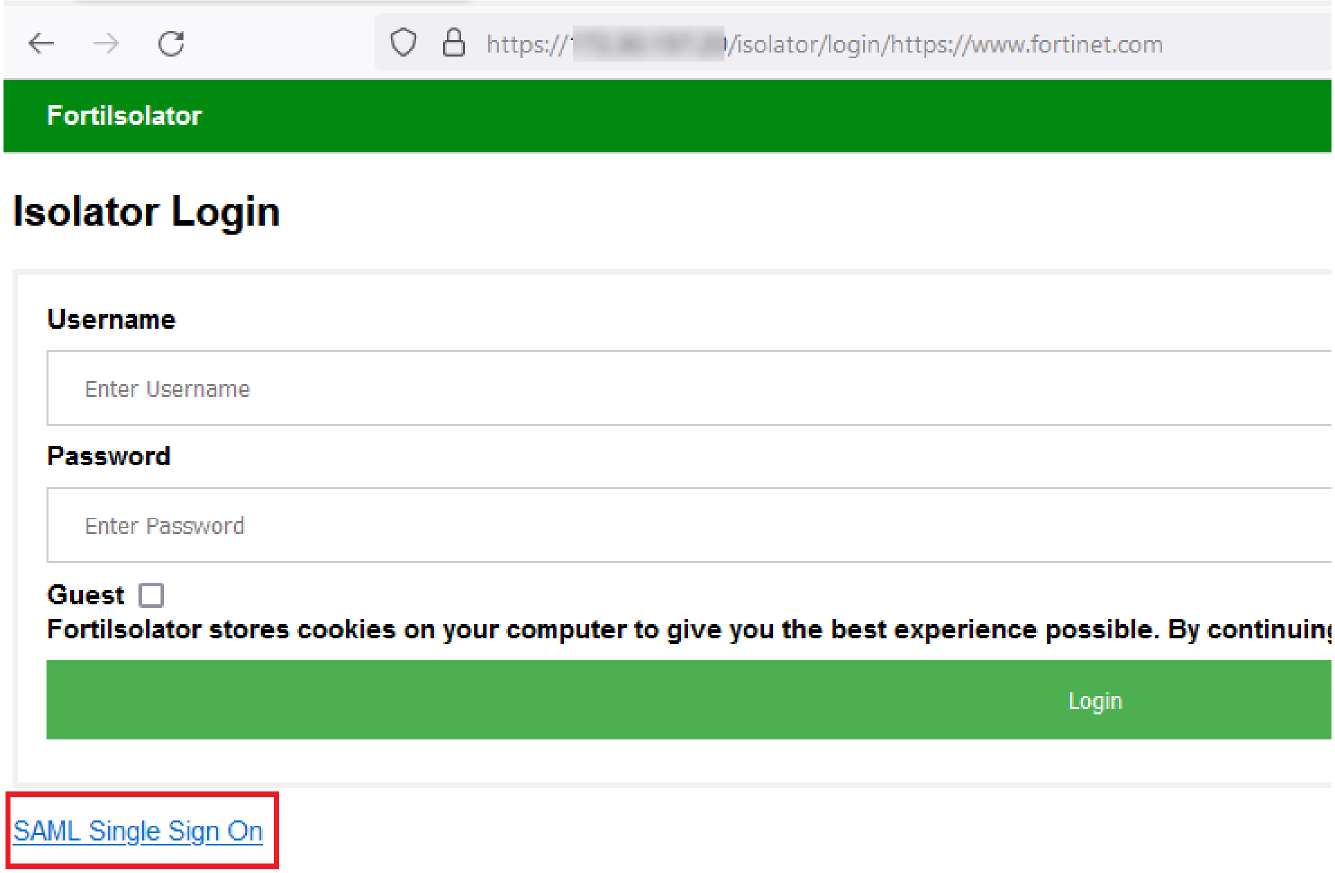
3. Navigate to *Users* > *LDAP Server* > *Create New*.
4. Select *SAML Server* and click *OK*.
5. Configure the following:

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

Run Traffic through FortiIsolator with FortiAuthenticator Users

Example:

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



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

FortiIsolator

Isolator Login

Username

Enter Username

Password

Enter Password

Guest □

FortiIsolator stores cookies on your computer to give you the best experience possible. By continuin

Login

SAML Single Sign On

User definition

End users can browse the web through FortiIsolator 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:

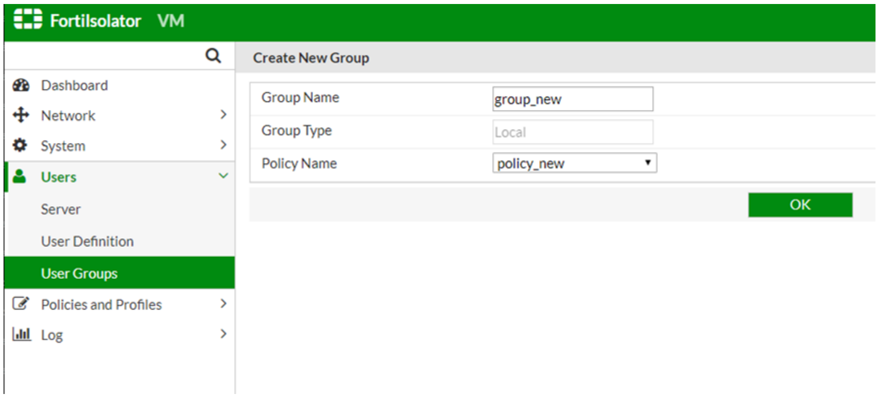
1. From the administration portal, go to *Users* > *User Groups* and click *Create New*.
2. Type in a name for the group and click *OK*.

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
>
```



Create New Group

Group Name: group_new

Group Type: Local

Policy Name: policy_new

Policies and profiles

In the *Policies and Profiles* section of FortiIsolator 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 Default policy.

Profile

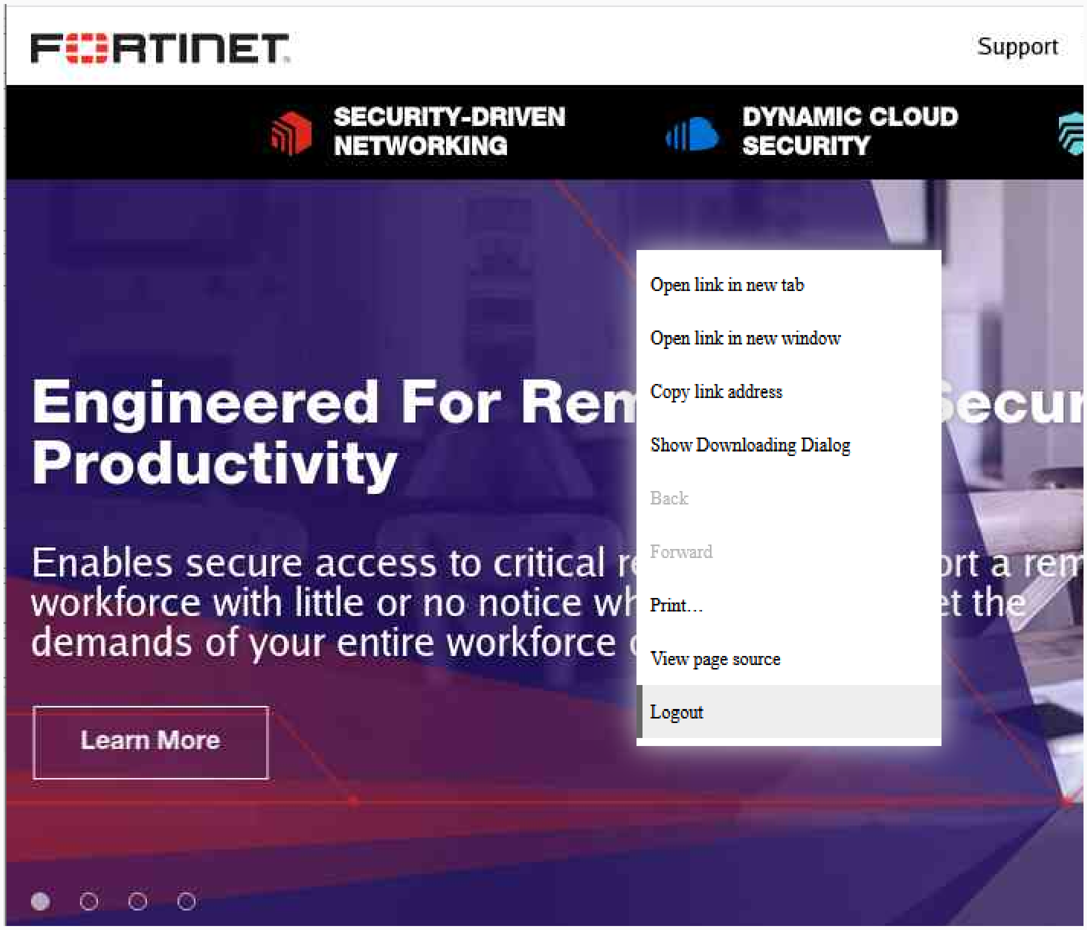
Creating a Isolator browsing profile

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

To create an Isolator browsing profile from GUI:

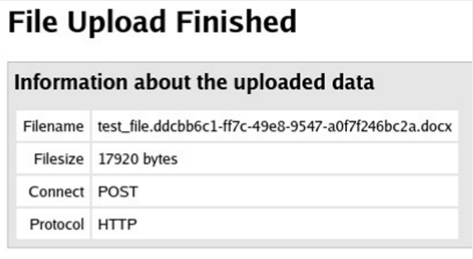
1. From the administration portal, go to *Policies and Profiles* > *Profiles* and click *Create New*.
2. From the *Profile Type* drop-down menu, select *Isolator Profile* and click *OK*.
3. Fill in the new Isolator profile information with desired settings.

Isolator Profile Name	Name of the Isolator profile. No restrictions.
View-only Mode	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.
Image Quality	Specify a percentage within 1-100. A higher percentage means more bandwidth usage.
Video Frame Rate	Video frame rate (high, normal, low). A higher rate means more bandwidth usage.
Scroll Speed	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.
Allow Right-click Action	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.

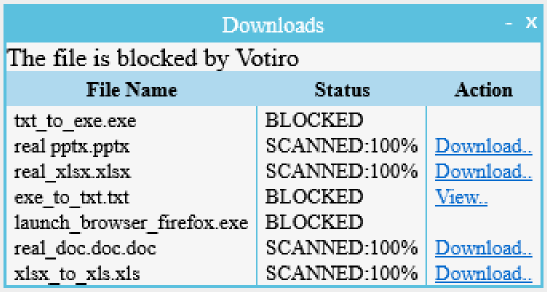
<table>
<tr><td></td><td>

<table>
<tr><td>Print</td><td>Users can print the current page as a PDF file.</td></tr>
<tr><td>Logout</td><td>Log out from the current session.</td></tr>
</table></td></tr>
<tr><td><i>Allow Copy out from FortiIsolator</i></td><td>Specifies whether to allow client users to copy content from the FortiIsolator to the clipboard using the keyboard or right-click menu.
To enable copying content from the FortiIsolator using the right-click menu, the <i>Allow Right-click Action</i> option must be enabled.</td></tr>
<tr><td><i>Allow Paste to FortiIsolator</i></td><td>Specifies whether to allow client users to paste content from the clipboard to the FortiIsolator using the keyboard or right-click menu.
To enable pasting content to the FortiIsolator using the right-click menu, the <i>Allow Right-click Action</i> option must be enabled.</td></tr>
<tr><td><i>Allow Printing</i></td><td>Specifies whether to allow client users to print the current page into a PDF file.</td></tr>
<tr><td><i>User Agent</i></td><td>Customized user agent name. For example, enter the following agent name to enable FortiIsolator to pass human verification:
<code>Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:68.0) FortiIsolatorBrowser/2.0 Gecko/20100101 Firefox/68.0</code></td></tr>
</table>

Show Isolation Icon	Specifies whether to show the FortiIsolator icon on the pages when users browse using FortiIsolator.
Certificates	Specifies which uploaded certificate(s) to enable for the profile. FortiIsolator automatically lists all uploaded Certificates on page 21 of the following types. If no such certificate is uploaded, the list is empty. • 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 *Add* button. Select *Block All* to select all file types in the list. • *exe* • *doc* • *ppt* • *pdf* • *txt* • *xls* • *png* • *mp3*
Block File Type Upload	Select the file types to block from uploading. You can also add more file types by clicking the *Add* button. Select *Block All* to select all file types in the list. • *exe* • *doc* • *ppt* • *pdf* • *txt* • *xls* • *png* • *mp3*
Allowlist File Type Download	Select the file types to allow for downloading. You can also add more file types by clicking the *Add* button. • *exe* • *doc* • *ppt*

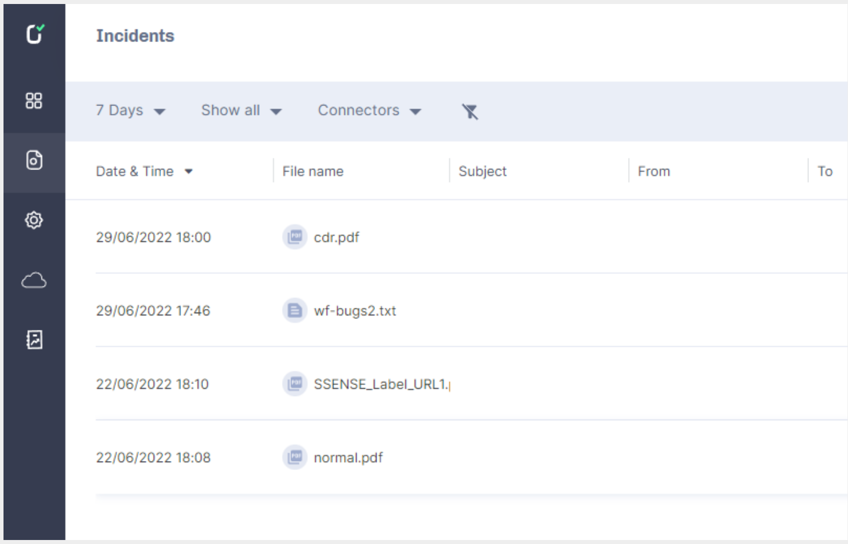
		• *pdf* • *txt* • *xls* • *png* • *mp3*
Allowlist File Type Upload		Select the file types to allow for uploading. You can also add more file types by clicking the *Add* button. • *exe* • *doc* • *ppt* • *pdf* • *txt* • *xls* • *png* • *mp3*
File Download Security		Configure whether to scan files for virus or malware with the following tools when uploading or downloading files through FortiIsolator. • If any of the enabled tools detects the file as containing virus or malware, FortiIsolator 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, FortiIsolator allows the client user to upload or download the file.
	Send Files with FortiSandbox	Specifies whether to send files to FortiSandbox. When enabled, specify the following options to connect to FortiSandbox: • *FortiSandbox IP*—IP address or domain name of the FortiSandbox to connect to. • *FortiSandbox Administrator Name*—Name of the FortiSandbox administrator. • *FortiSandbox Password*—Password of FortiSandbox. To verify connection with FortiSandbox, upload a file using FortiIsolator. 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.  **File Upload Finished** **Information about the uploaded data** Filename test_file.ddcbb6c1-ff7c-49e8-9547-a0f7f246bc2a.docx Filesize 17920 bytes Connect POST Protocol HTTP
	Scan Files with FortiIsolator	Specifies whether to scan files with FortiIsolator. When enabled, further configure the following option: • *File Content Disarm and Reconstruct with FortiIsolator*

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 FortiIsolator 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 FortiIsolator. When the following image appears, which means the download is complete, verify that the file appears in the *Incidents* page in Votiro.



The file is blocked by Votiro

File Name	Status	Action
txt_to_exe.exe	BLOCKED	
real pptx.pptx	SCANNED:100%	Download..
real_xlsx.xlsx	SCANNED:100%	Download..
exe_to_txt.txt	BLOCKED	View..
launch_browser_firefox.exe	BLOCKED	
real_doc.doc.doc	SCANNED:100%	Download..
xlsx_to_xls.xls	SCANNED:100%	Download..



Date & Time	File name	Subject	From	To
29/06/2022 18:00	cdr.pdf			
29/06/2022 17:46	wf-bugs2.txt			
22/06/2022 18:10	SSENSE_Label_URL1.(			
22/06/2022 18:08	normal.pdf			

4. Click *OK*.

To create a FortiIsolator 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 with1 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 FortiIsolator to the clipboard using the keyboard or right-click menu. (Y/N) To enable copying content from the FortiIsolator 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 FortiIsolator icon on the pages when users browse using FortiIsolator (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 FortiIsolator using the keyboard or right-click menu. (Y/N) To enable pasting content to the FortiIsolator 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

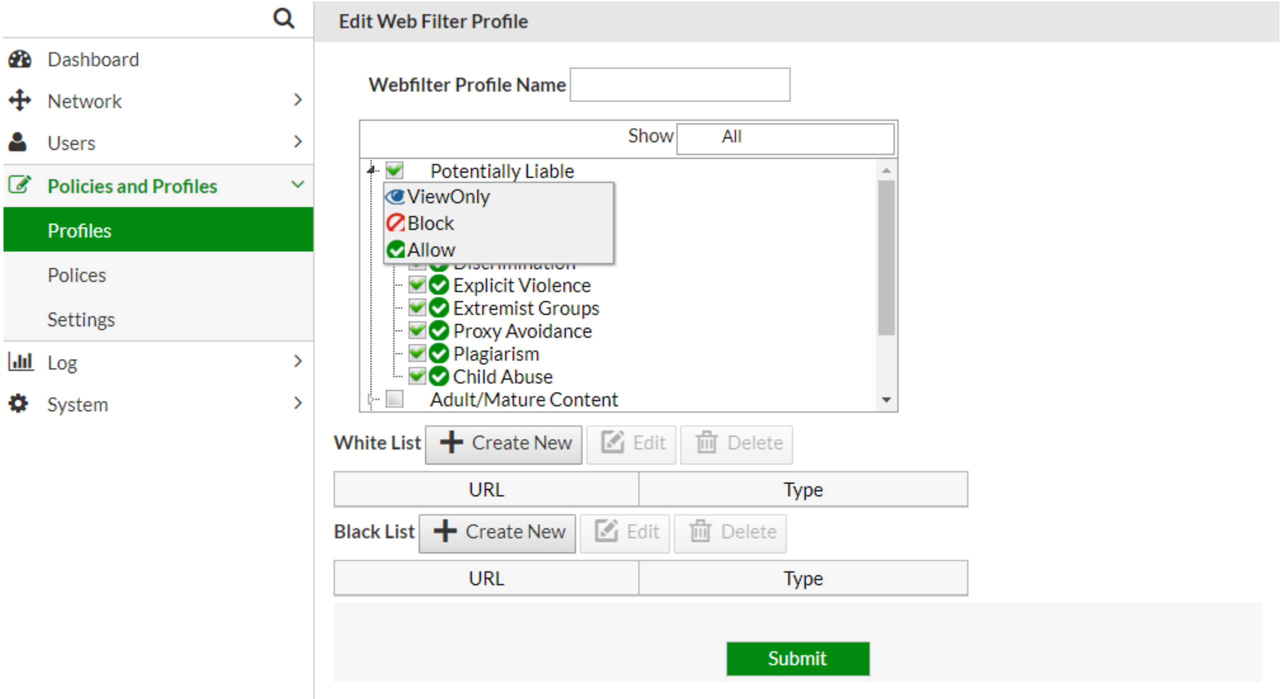
FortiIsolator supports web filtering, which enables the administrator to control which webpages that end users are allowed to view. You can block specific URLs or websites, which prevents the end user's browser from loading web pages from these websites.

Prerequisites

- Ensure that FortiIsolator 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 FortiIsolator license is the same as the FortiIsolator 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.



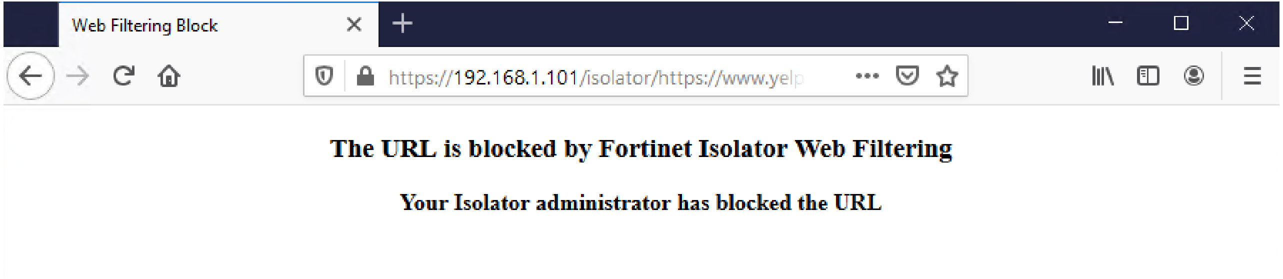
Right-click on any checked box to select the desired action:

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.

FortiIsolator 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 FortiIsolator, 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 FortiIsolator 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 FortiIsolator if fails to connect to ICAP • Allow • Block • View only

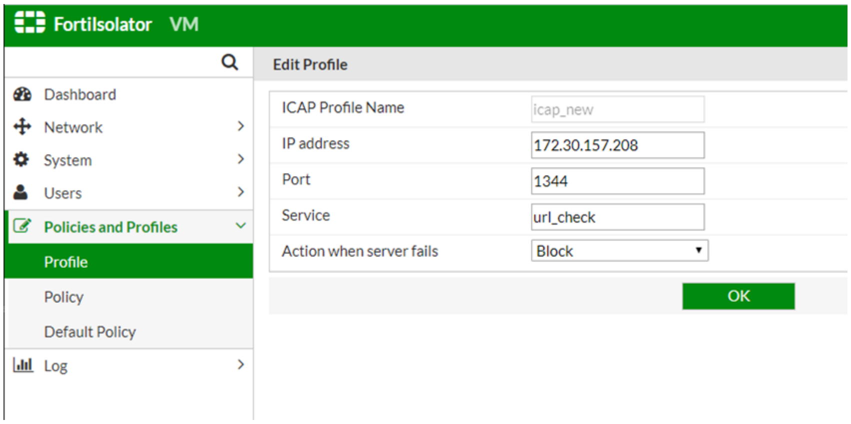
To create an ICAP profile from CLI:

```
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	icap_new
IP address	172.30.157.208
Port	1344
Service	url_check
Action when server fails	Block

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 Policy*.
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 FortiIsolator 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 FortiIsolator 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
```

Default 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 default policy and profile settings

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

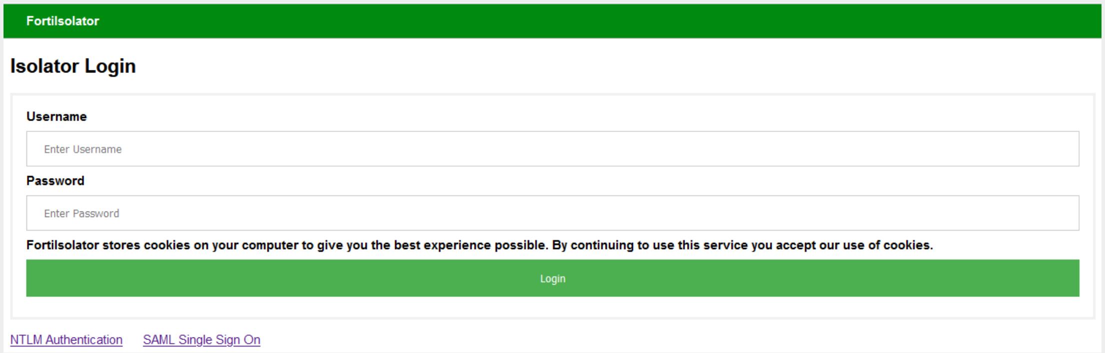
To apply profiles to default policy from GUI:

1. Go to *Policies and Profiles* > *Default Policy* and select the desired *Guest Type*. This option determines the way of Logging in as an end user on page 84.

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 30 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 26, the user can log in with single-sign-on by clicking the *SAML Single Sign On* link and entering the credentials.

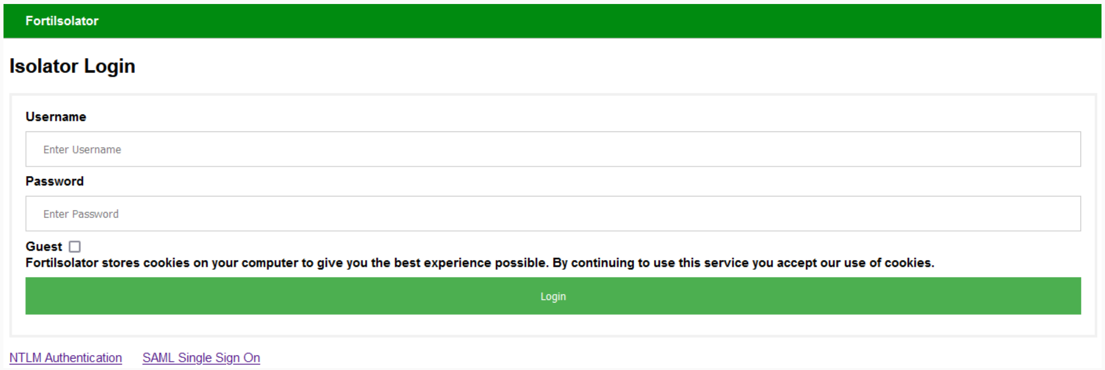


FortiIsolator stores cookies on your computer to give you the best experience possible. By continuing to use this service you accept our use of cookies.

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 30.
  - **SAML user** - If a SAML server is configured through FortiAuthenticator in SAML servers on page 26, 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*.



FortiIsolator stores cookies on your computer to give you the best experience possible. By continuing to use this service you accept our use of cookies.

guest only

A user has to log in as a guest.

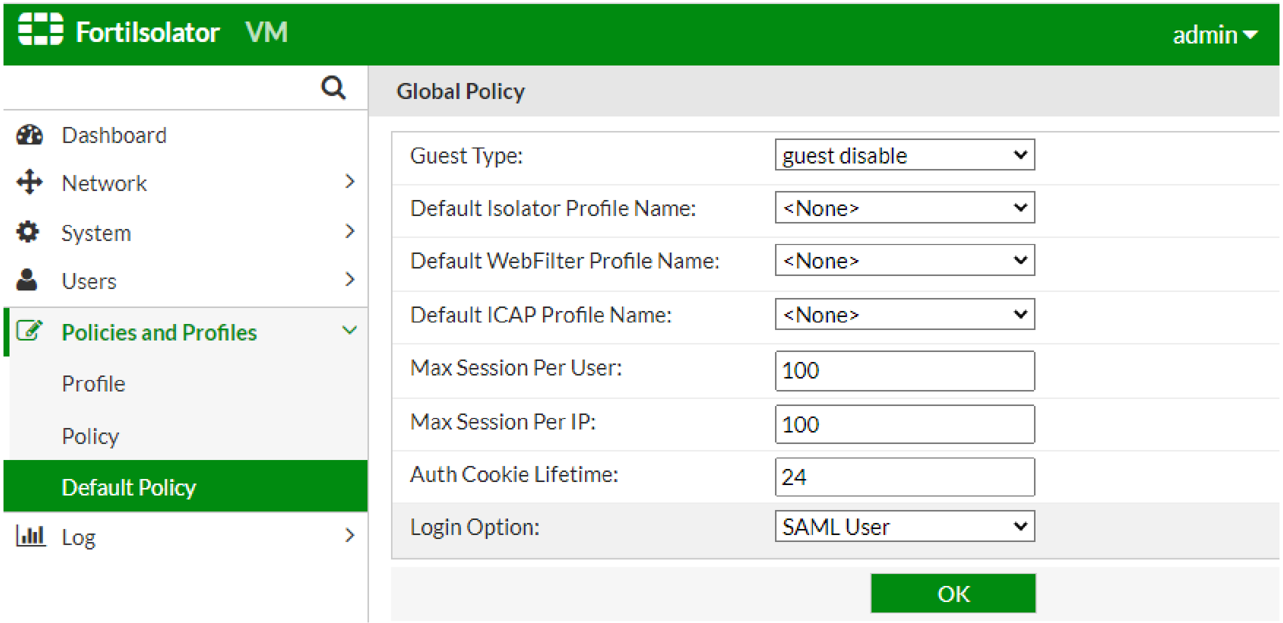
With *guest only*, the login page will not show. Users can browse sites without being prompted to log in.

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 default policy.

Default Isolator Profile Name	Select an Isolator profile for Default Policy.
Default WebFilter Profile Name	Select a Web Filter profile for Default Policy.

Default ICAP Profile Name	Select an ICAP profile for Default Policy.
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. Enter an integer within the range of 1-240. This setting does not take effect when the user is in guest mode.
Login Option	Select the options that the user can log in. This option is available only if *Guest Type* is *guest disable* and a SAML server is configured through FortiAuthenticator in SAML servers on page 26. • *Local User or SAML User*—Allow the user to log in using a local user account or SAML credentials. • *SAML User*—Allow the user to log in using the SAML credentials only. Local user accounts are not allowed.

3. Click *OK* to finish.



Global Policy

Guest Type: guest disable

Default Isolator Profile Name: <None>

Default WebFilter Profile Name: <None>

Default ICAP Profile Name: <None>

Max Session Per User: 100

Max Session Per IP: 100

Auth Cookie Lifetime: 24

Login Option: SAML User

To apply profiles to default 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 default-policy <isolator-profile-name> <webfilter-profile-name> <icap-profile-name>
     <guest-type> <max-session-per-user> <max-session-per-ip> <auth-cookie-lifetime>
     <global-policy-login-option>
e.g.

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

<table>
<tr><td><code>&lt;isolator-profile-name &gt;</code></td><td>Isolator profile name</td></tr>
<tr><td><code>&lt;webfilter-profile-name &gt;</code></td><td>Web Filter profile name</td></tr>
<tr><td><code>&lt;icap-profile-name &gt;</code></td><td>ICAP profile name</td></tr>
<tr><td><code>&lt;guest-type&gt;</code></td><td>Login mode of the user:
<table>
<tr><td>1</td><td><i>guest disable</i>: A user must log in with the following types of credentials:
• Local user account—Only if <i>Login Option</i> is <i>Local User or SAML User</i>.
• SAML credentials—Only if a SAML server is configured through FortiAuthenticator in SAML servers on page 26.</td></tr>
<tr><td>2</td><td><i>guest enable</i>: A user can log in with a user account, SAML/NTML authentication, or as a guest.</td></tr>
<tr><td>0</td><td><i>guest only</i>: A user has to log in as a guest. No credentials are required.</td></tr>
</table></td></tr>
<tr><td><code>&lt;max-session-per-user&gt;</code></td><td>Maximum number of sessions (tabs) allowed for requests from a same local user</td></tr>
<tr><td><code>&lt;max-session-per-ip&gt;</code></td><td>Maximum number of sessions (tabs) allowed for requests from a unique IP address</td></tr>
<tr><td><code>&lt;auth-cookie-lifetime&gt;</code></td><td>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.</td></tr>
<tr><td><code>&lt;global-policy-login-option&gt;</code></td><td>Login option allowed for the user. This option is available only if <i>Guest Type</i> is <i>guest disable</i> and a SAML server is configured through FortiAuthenticator in SAML servers on page 26.</td></tr>
</table>

	1	*Local User or SAML User*: A user can log in with a local user account or SAML credentials.
	0	*SAML User*: A user can only log in using SAML credentials. Local user accounts are not allowed.

To display the default policy profile from CLI:

```
> show default-policy
      Default 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
      Global Policy Login Option : 1
```

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 FortiIsolator 3.0 Private Cloud Deployment Guide for instructions of downloading the package.
- See Manage FIS Images on page 23 for instructions of uploading and applying the package in FortiIsolator.

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

- Daemons running on the FortiIsolator
- 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 FortiIsolator for client users
- Forwarding logs to remote log servers

You can view logs by the following categories:

- ISOLATOR on page 49
- ADMIN GUI on page 50

You can also configure FortiIsolator to send the log to a third-party Remote Server on page 50, including FortiAnalyzer.

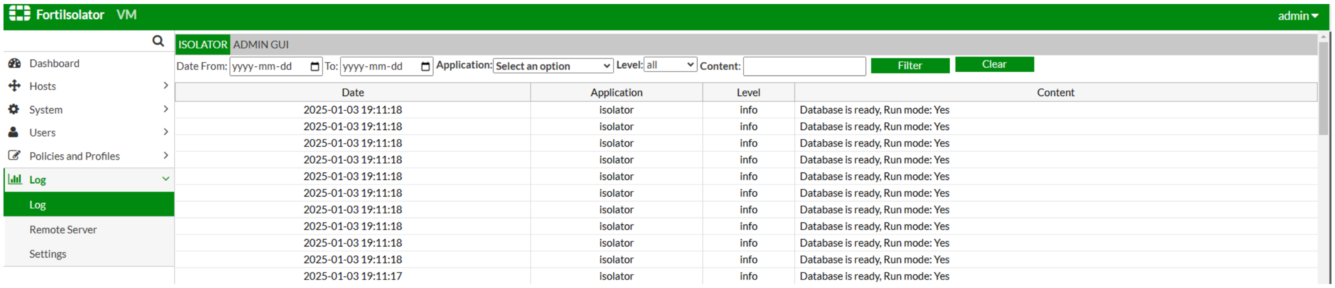
- FortiAnalyzer— FortiIsolator routes the log to FortiAnalyzer for display, processing, or reporting. FortiIsolator no longer displays the logs under the log categories. See the FortiAnalyzer Administration Guide for more information.
- Third-party remote server—FortiIsolator sends a copy of the raw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

You can also configure the log backup behavior for the FortiIsolator in the Settings on page 51 tab.

Refer to the FortiIsolator 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 FortiIsolator.



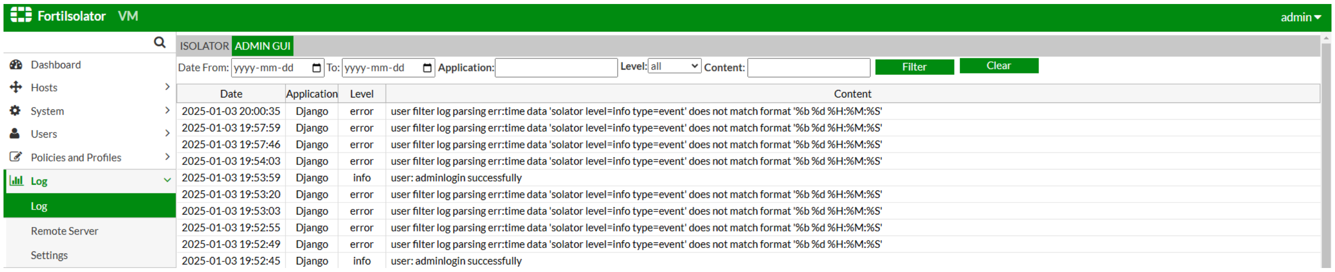
Date From: yyyy-mm-dd To: yyyy-mm-dd Application: Select an option Level: all Content:

Date	Application	Level	Content
2025-01-03 19:11:18	isolator	info	Database is ready, Run mode: Yes
2025-01-03 19:11:18	isolator	info	Database is ready, Run mode: Yes
2025-01-03 19:11:18	isolator	info	Database is ready, Run mode: Yes
2025-01-03 19:11:18	isolator	info	Database is ready, Run mode: Yes
2025-01-03 19:11:18	isolator	info	Database is ready, Run mode: Yes
2025-01-03 19:11:18	isolator	info	Database is ready, Run mode: Yes
2025-01-03 19:11:18	isolator	info	Database is ready, Run mode: Yes
2025-01-03 19:11:18	isolator	info	Database is ready, Run mode: Yes
2025-01-03 19:11:18	isolator	info	Database is ready, Run mode: Yes
2025-01-03 19:11:18	isolator	info	Database is ready, Run mode: Yes
2025-01-03 19:11:17	isolator	info	Database is ready, Run mode: Yes

- 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.



Date	Application	Level	Content
2025-01-03 20:00:35	Django	error	user filter log parsing err:time data 'solator level=info type=event' does not match format '%b %d %H:%M:%S'
2025-01-03 19:57:59	Django	error	user filter log parsing err:time data 'solator level=info type=event' does not match format '%b %d %H:%M:%S'
2025-01-03 19:57:46	Django	error	user filter log parsing err:time data 'solator level=info type=event' does not match format '%b %d %H:%M:%S'
2025-01-03 19:54:03	Django	error	user filter log parsing err:time data 'solator level=info type=event' does not match format '%b %d %H:%M:%S'
2025-01-03 19:53:59	Django	info	user: adminlogin successfully
2025-01-03 19:53:20	Django	error	user filter log parsing err:time data 'solator level=info type=event' does not match format '%b %d %H:%M:%S'
2025-01-03 19:53:03	Django	error	user filter log parsing err:time data 'solator level=info type=event' does not match format '%b %d %H:%M:%S'
2025-01-03 19:52:55	Django	error	user filter log parsing err:time data 'solator level=info type=event' does not match format '%b %d %H:%M:%S'
2025-01-03 19:52:49	Django	error	user filter log parsing err:time data 'solator level=info type=event' does not match format '%b %d %H:%M:%S'
2025-01-03 19:52:45	Django	info	user: adminlogin successfully

- 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.

Logging Protocol	Syslog
Network Protocol	• 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 a editing a type, select the *Category* and *Severity*. See the descriptions in Log on page 49.
   c. Click *OK*.
4. Click *Submit*.

If you configure a FortiAnalyzer remote server, FortiIsolator 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, FortiIsolator 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 FortiIsolator:

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 FortiIsolator 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 FortiIsolator

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

- IP Forwarding mode
- Proxy mode

IP Forwarding mode

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

- Using IP Forwarding mode with Mozilla Firefox on page 52
- Using IP Forwarding mode with Google Chrome on page 54
- Using IP Forwarding mode with Internet Explorer on page 59
- Using IP Forwarding mode with Edge on page 63

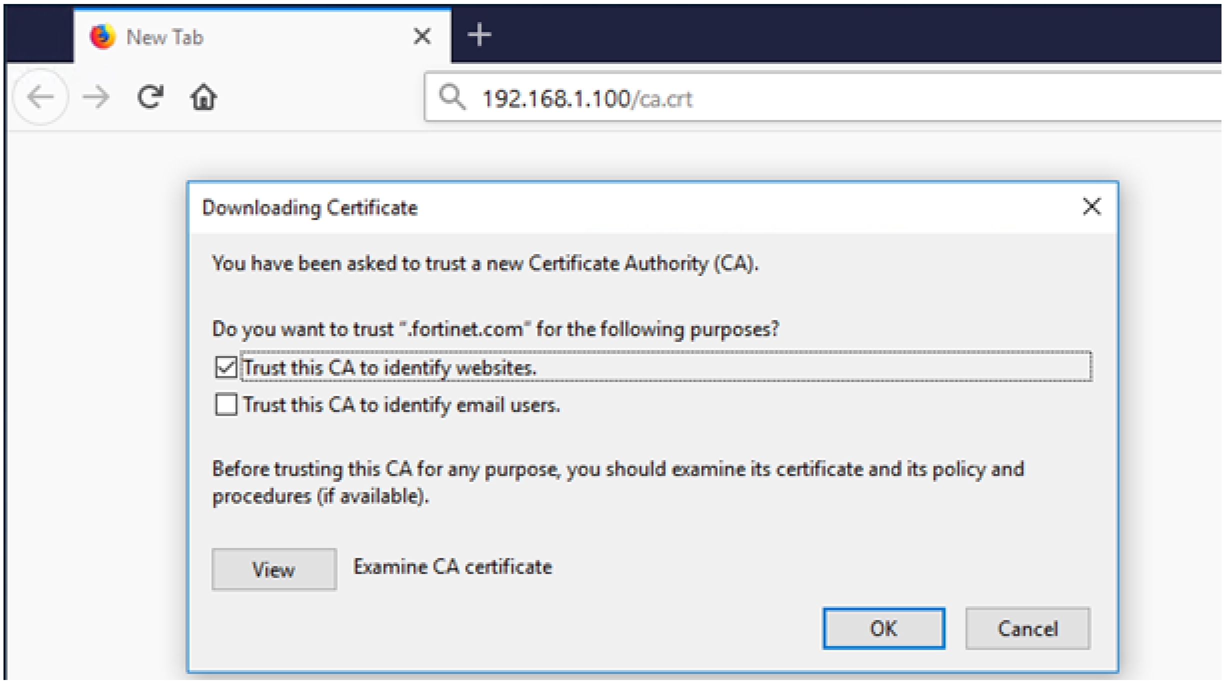
Using IP Forwarding mode with Mozilla Firefox

To configure IP Forwarding mode with Mozilla Firefox:

1. Download the FortiIsolator 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 FortiIsolator internal interface.

    b. In the *Downloading Certificate* window, select the *Trust this CA to identify websites* checkbox.

    c. Click *OK*.



Downloading Certificate

You have been asked to trust a new Certificate Authority (CA).

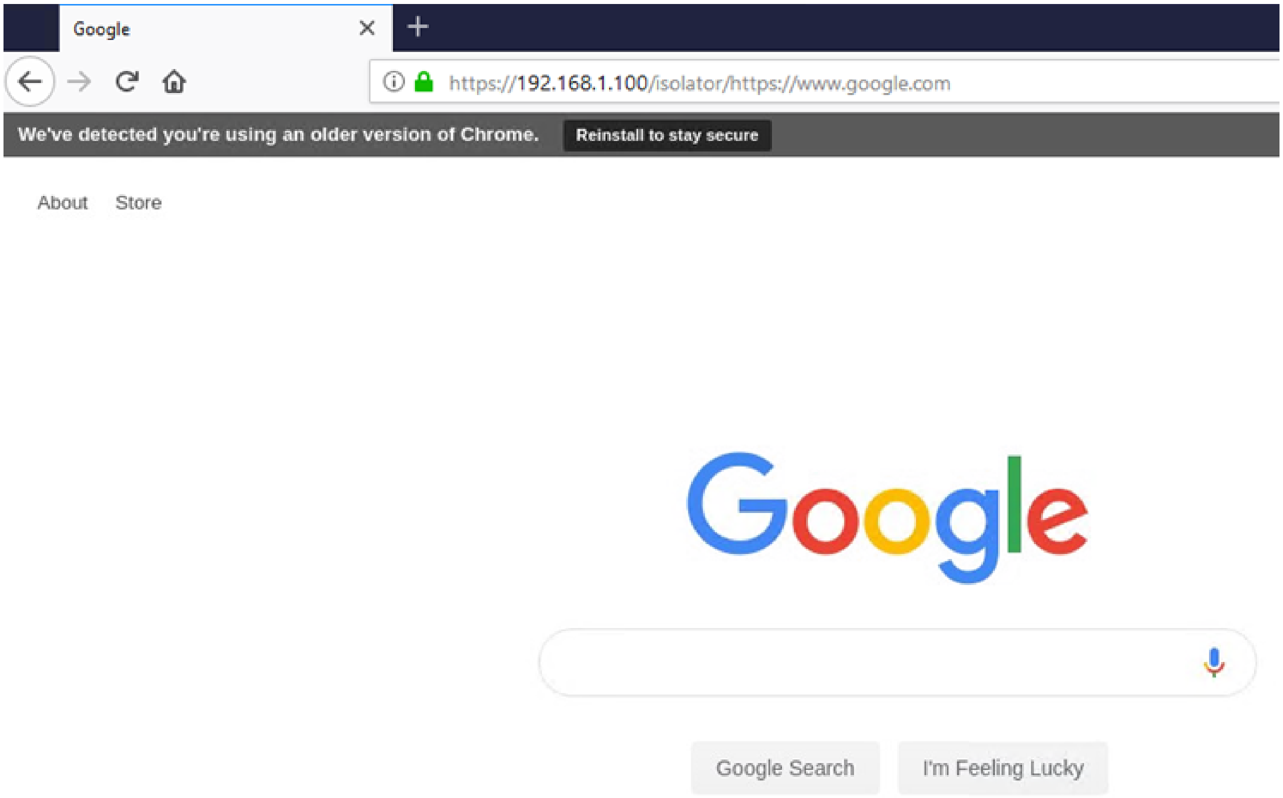
Do you want to trust ".fortinet.com" for the following purposes?

☑ Trust this CA to identify websites.

□ Trust this CA to identify email users.

Before trusting this CA for any purpose, you should examine its certificate and its policy and procedures (if available).

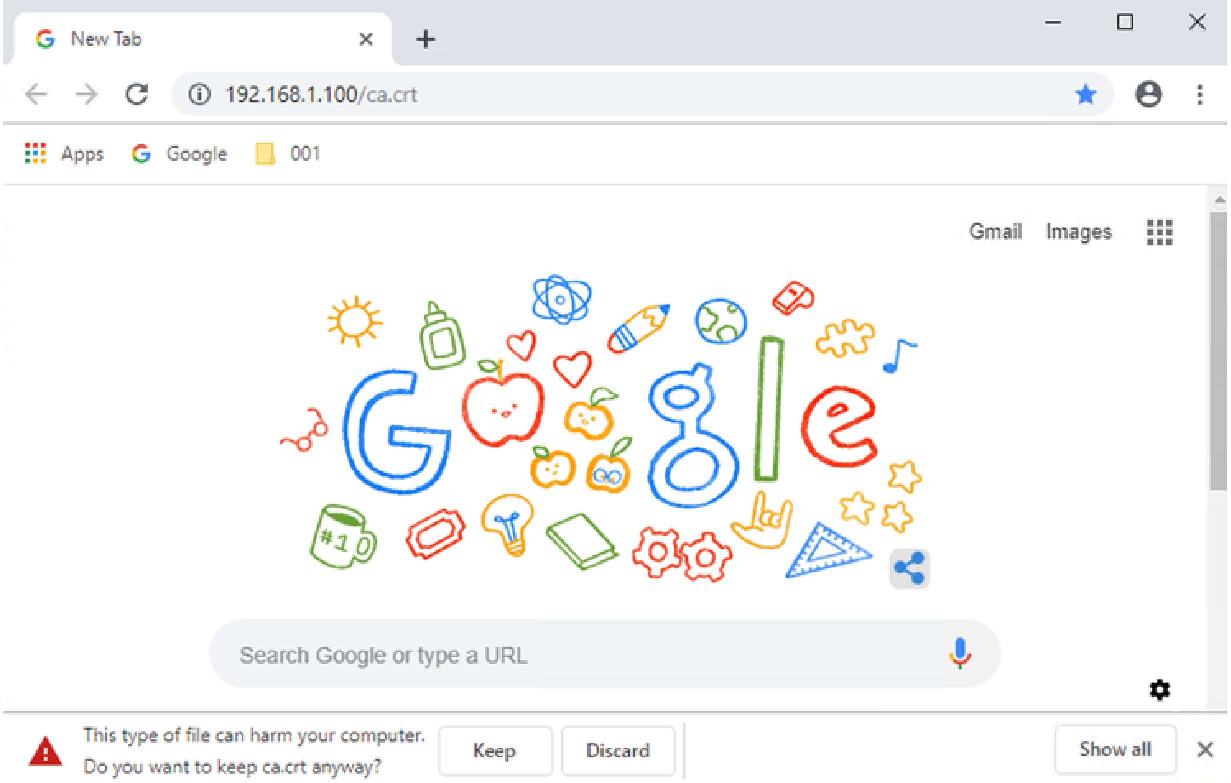
2. In the Mozilla Firefox browser address bar, type `https://<internal_IP_address>/isolator/https://www.<website-url>.com` (for example, `https://192.168.1.100/isolator/https://www.google.com`).
   - where `<internal_IP_address>` value is the IP address of the FortiIsolator internal interface.


Google
https://192.168.1.100/isolator/https://www.google.com
We've detected you're using an older version of Chrome.
Reinstall to stay secure
About
Store
Google
Google Search
I'm Feeling Lucky

Using IP Forwarding mode with Google Chrome

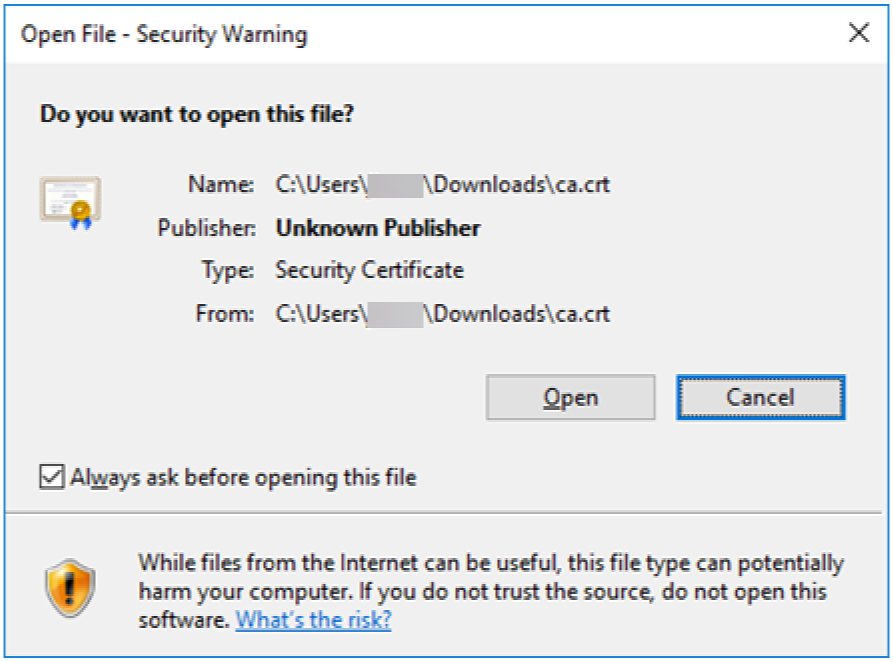
To configure IP Forwarding mode with Google Chrome:

1. Download the FortiIsolator 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 FortiIsolator internal interface.
   - **b.** In the security warning at the bottom of the browser, click *Keep* to download the certificate.



This type of file can harm your computer. Do you want to keep ca.crt anyway?

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



Open File - Security Warning

Do you want to open this file?

Name: C:\Users\[redacted]\Downloads\ca.crt

Publisher: **Unknown Publisher**

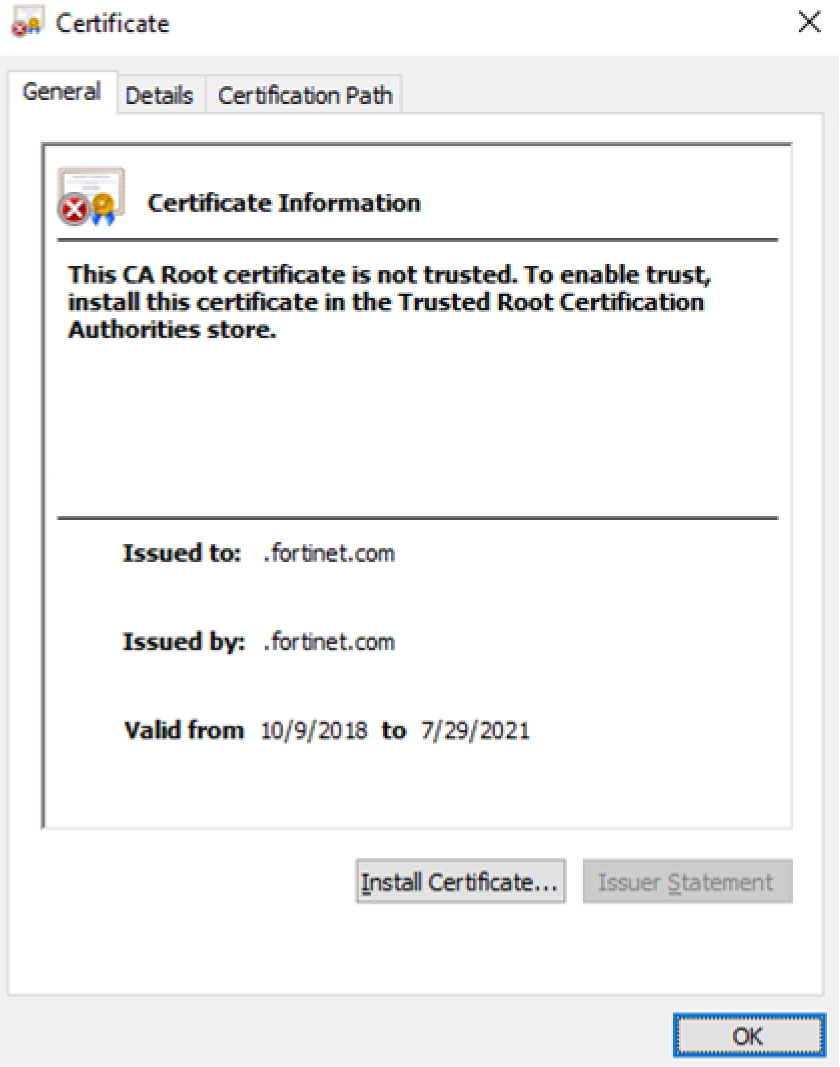
Type: Security Certificate

From: C:\Users\[redacted]\Downloads\ca.crt

☑ Always ask before opening this file

While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not open this software. What's the risk?

d. Click *Install Certificate*.



Certificate Information

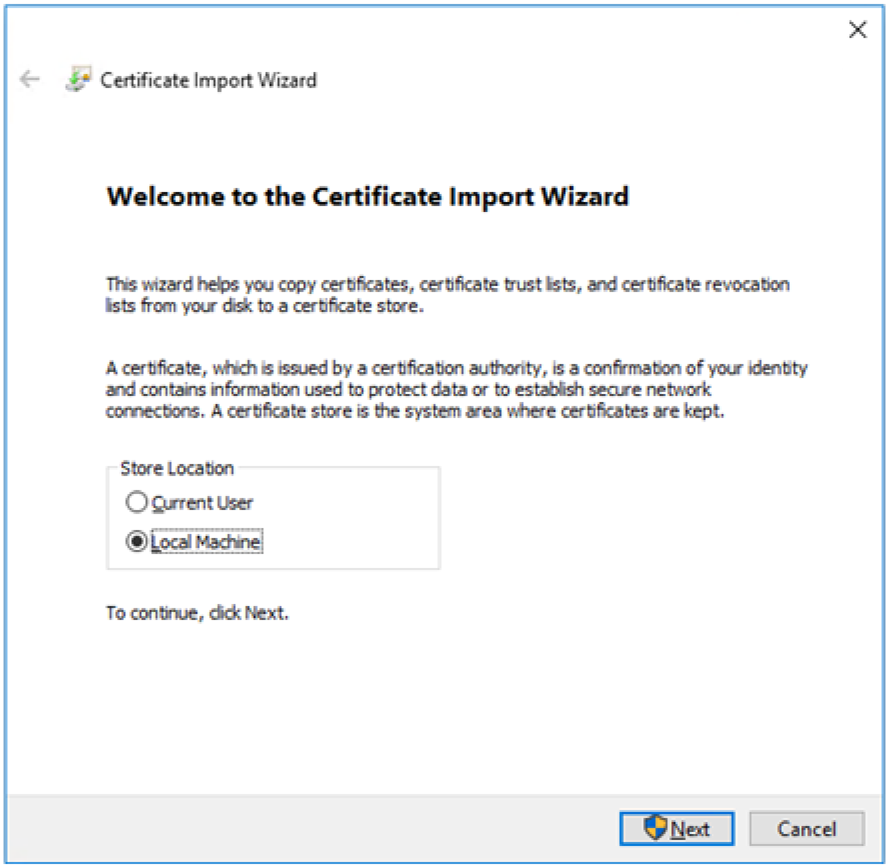
This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

Issued to: .fortinet.com

Issued by: .fortinet.com

Valid from 10/9/2018 to 7/29/2021

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



Certificate Import Wizard

Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

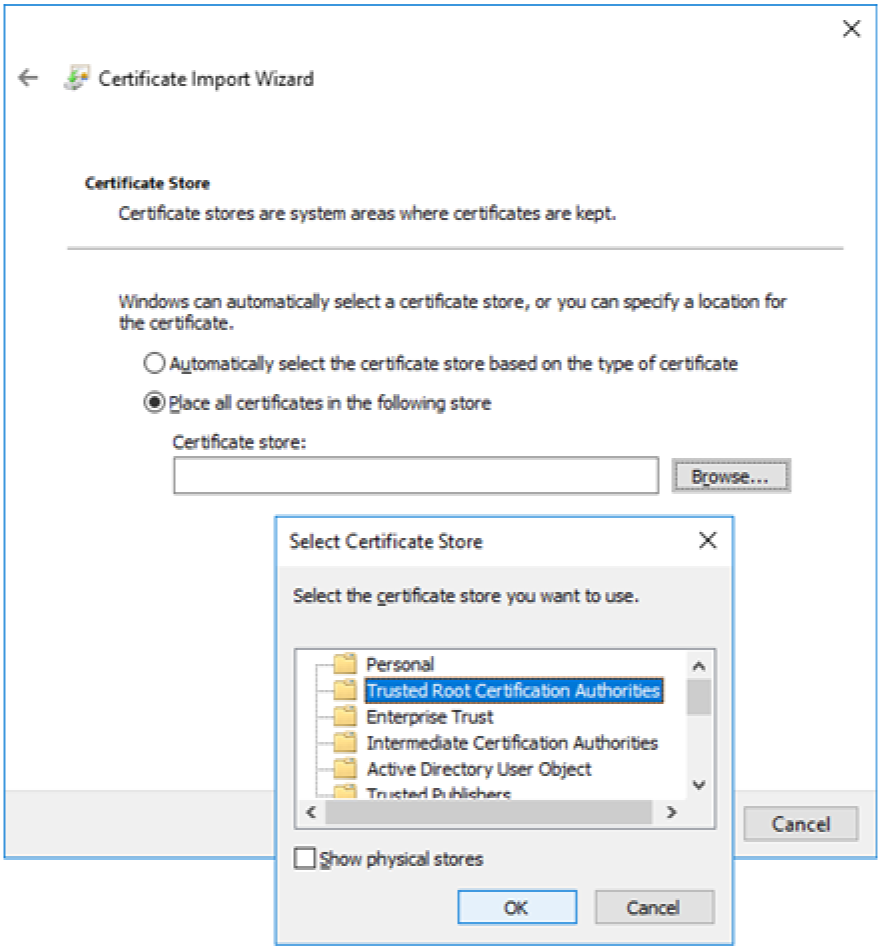
Store Location

○ Current User

● Local Machine

To continue, click Next.

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



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store:

Select Certificate Store

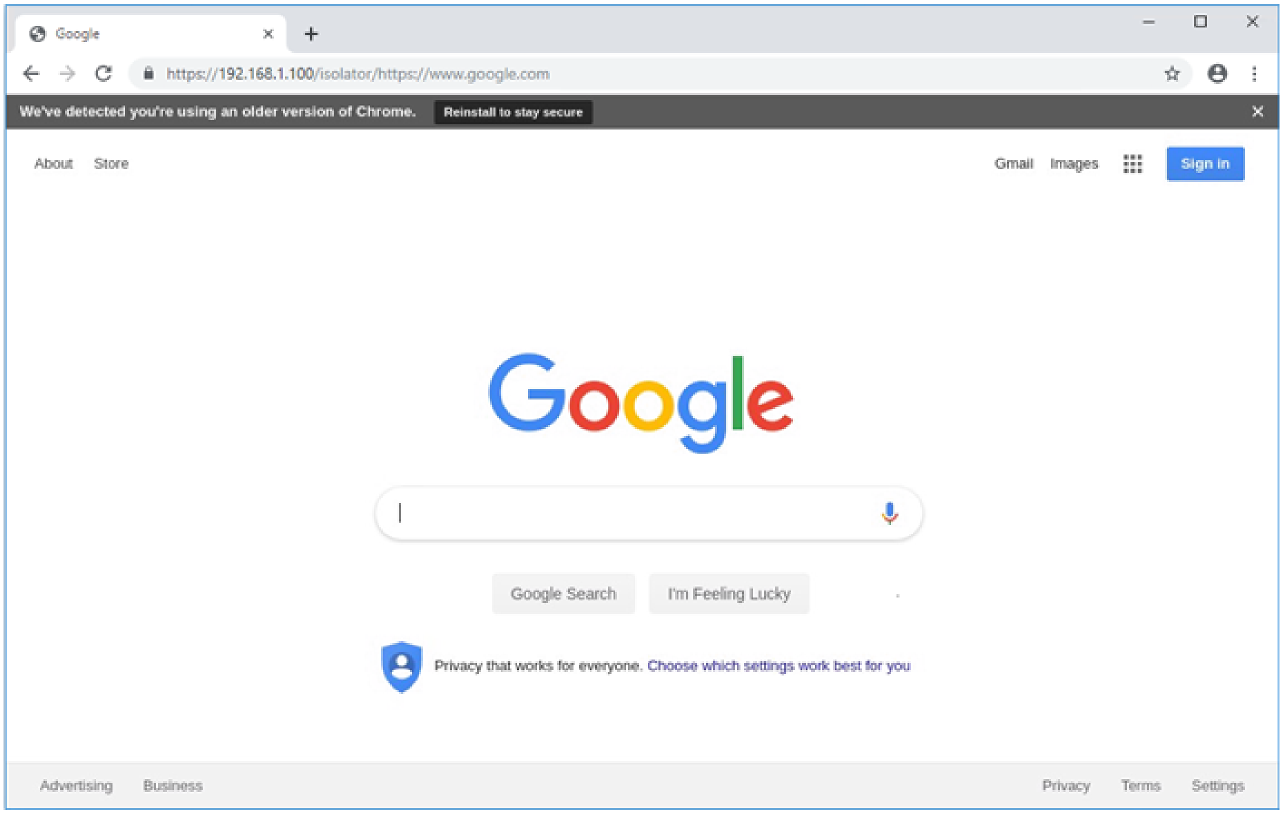
Select the certificate store you want to use.

- Personal
- Trusted Root Certification Authorities
- Enterprise Trust
- Intermediate Certification Authorities
- Active Directory User Object
- Trusted Publishers

□ Show physical stores

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 FortiIsolator internal interface.



https://192.168.1.100/isolator/https://www.google.com

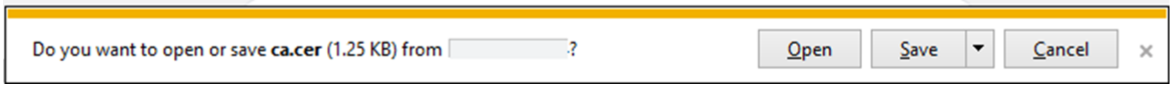
We've detected you're using an older version of Chrome.

Privacy that works for everyone. Choose which settings work best for you

Using IP Forwarding mode with Internet Explorer

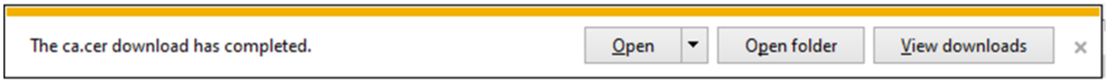
To configure IP Forwarding mode with Internet Explorer:

1. Download the FortiIsolator certificate (`ca.crt`) and import it into your Internet Explorer browser:
   - **a.** In the Internet Explorer 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 FortiIsolator internal interface.
   - **b.** In the security warning at the bottom of the browser, click *Save* to download the certificate.



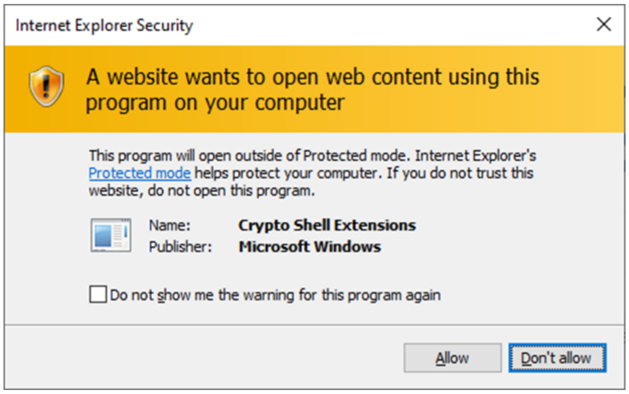
Do you want to open or save **ca.cer** (1.25 KB) from ?

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



The ca.cer download has completed.

d. Click *Allow* to install certificate.



Internet Explorer Security

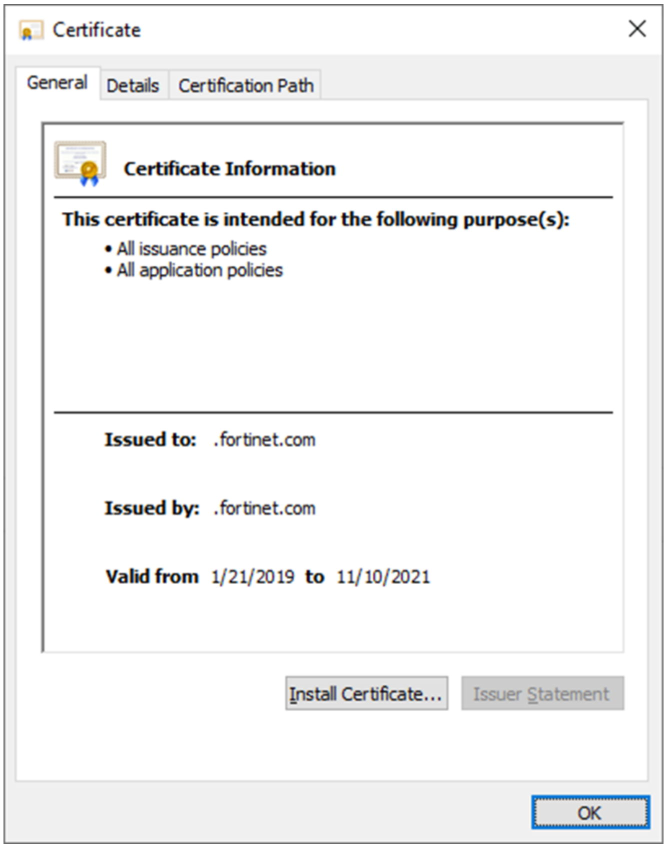
A website wants to open web content using this program on your computer

This program will open outside of Protected mode. Internet Explorer's Protected mode helps protect your computer. If you do not trust this website, do not open this program.

Name: **Crypto Shell Extensions**
Publisher: **Microsoft Windows**

□ Do not show me the warning for this program again

e. Click *Install Certificate*.



Certificate

Certificate Information

This certificate is intended for the following purpose(s):

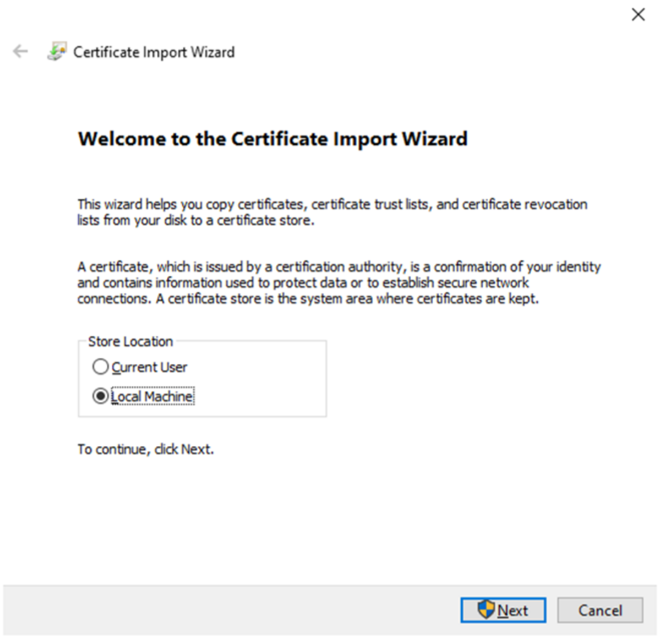
- All issuance policies
- All application policies

Issued to: .fortinet.com

Issued by: .fortinet.com

Valid from 1/21/2019 **to** 11/10/2021

f. Select *Local Machine*, and click *Next*.



Certificate Import Wizard

Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

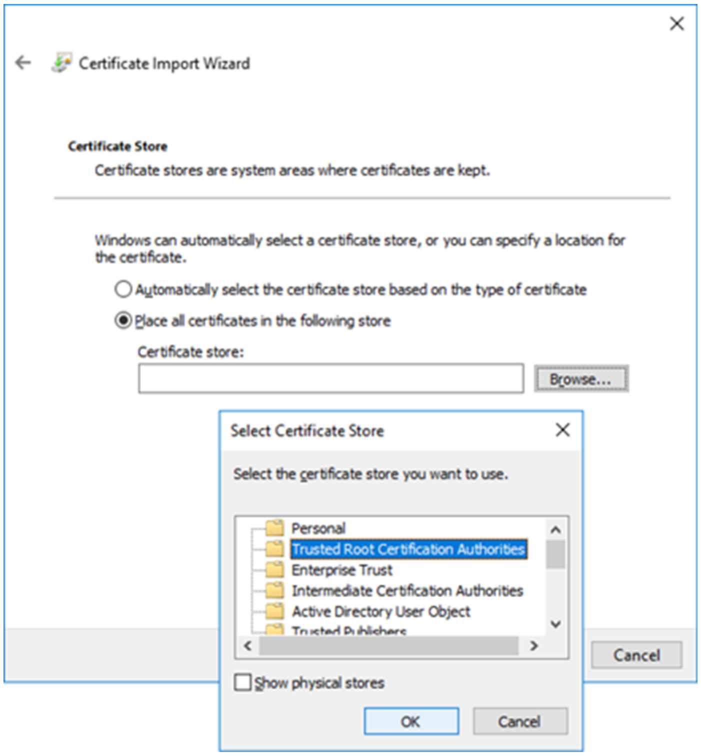
Store Location

○ Current User

● Local Machine

To continue, click Next.

g. Select *Trusted Root Certification Authorities*, and click *OK*.



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store:

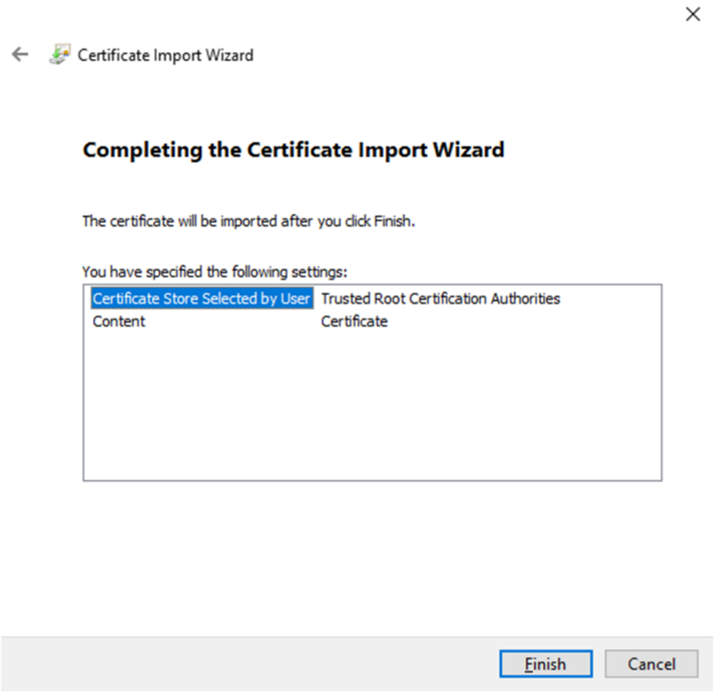
Select Certificate Store

Select the certificate store you want to use.

- Personal
- Trusted Root Certification Authorities
- Enterprise Trust
- Intermediate Certification Authorities
- Active Directory User Object
- Trusted Publishers

□ Show physical stores

h. Completing the Certificate Import Wizard.



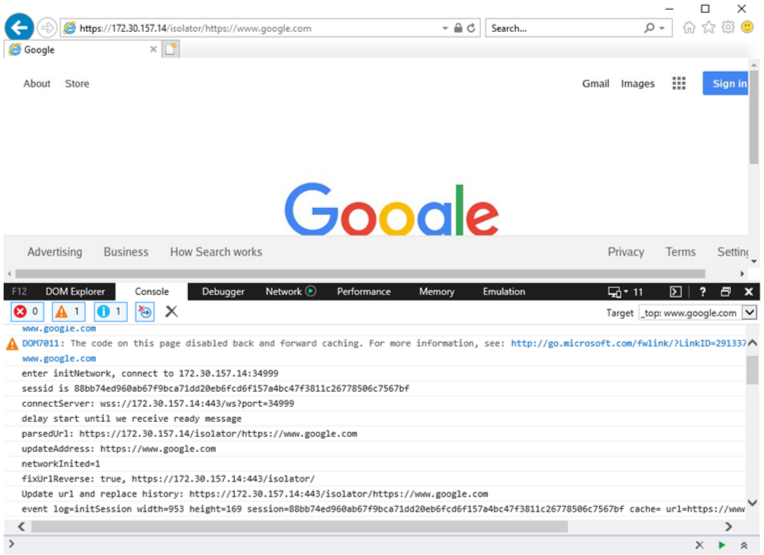
Completing the Certificate Import Wizard

The certificate will be imported after you click Finish.

You have specified the following settings:

Certificate Store Selected by User	Trusted Root Certification Authorities
Content	Certificate

2. In the Internet Explorer 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 FortiIsolator internal interface.

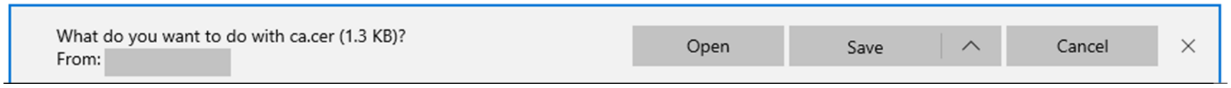


```
www.google.com
DOM7011: The code on this page disabled back and forward caching. For more information, see: http://go.microsoft.com/fwlink/?LinkID=291337
www.google.com
enter initNetwork, connect to 172.30.157.14:34999
sessid is 88bb74ed960ab67f9bca71dd20eb6fcd6f157a4bc47f3811c26778506c7567bf
connectServer: wss://172.30.157.14:443/ws?port=34999
delay start until we receive ready message
parsedUrl: https://172.30.157.14/isolator/https://www.google.com
updateAddress: https://www.google.com
networkInited=1
fixUrlReverse: true, https://172.30.157.14:443/isolator/
Update url and replace history: https://172.30.157.14:443/isolator/https://www.google.com
event log=initSession width=953 height=169 session=88bb74ed960ab67f9bca71dd20eb6fcd6f157a4bc47f3811c26778506c7567bf cache= url=https://www
```

Using IP Forwarding mode with Edge

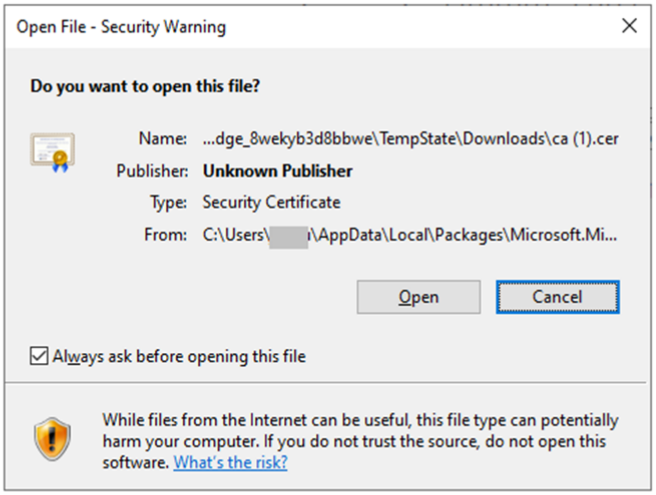
To configure IP Forwarding mode with Edge browser:

1. Download the FortiIsolator 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 FortiIsolator internal interface.
   - **b.** In the security warning at the bottom of the browser, click *Save* to download the certificate.



What do you want to do with ca.cer (1.3 KB)?
From: [redacted]

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



Open File - Security Warning

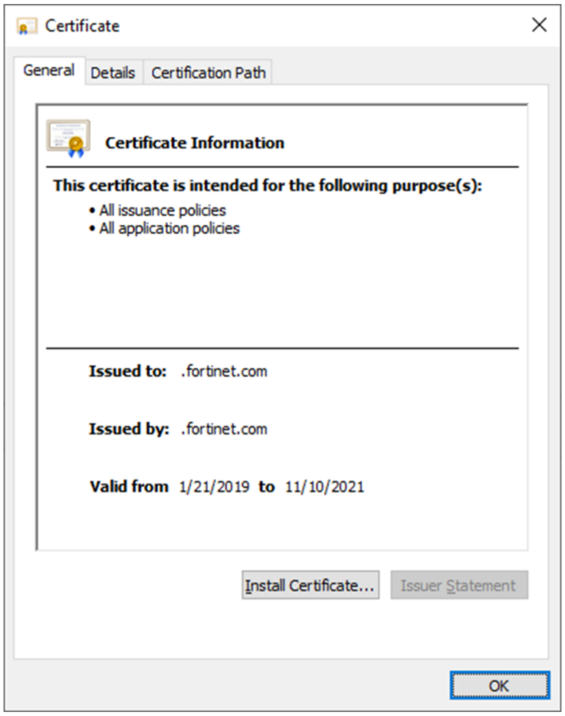
Do you want to open this file?

Name: ...dge_8wekyb3d8bbwe\TempState\Downloads\ca (1).cer
Publisher: **Unknown Publisher**
Type: Security Certificate
From: C:\Users\[redacted]\AppData\Local\Packages\Microsoft.Mi...

☑ Always ask before opening this file

While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not open this software. What's the risk?

d. Click *Install Certificate*.



Certificate Information

This certificate is intended for the following purpose(s):

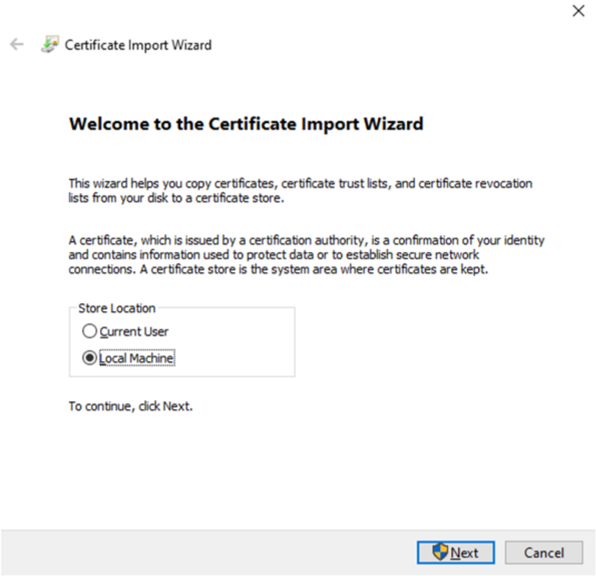
- All issuance policies
- All application policies

Issued to: .fortinet.com

Issued by: .fortinet.com

Valid from 1/21/2019 **to** 11/10/2021

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



Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

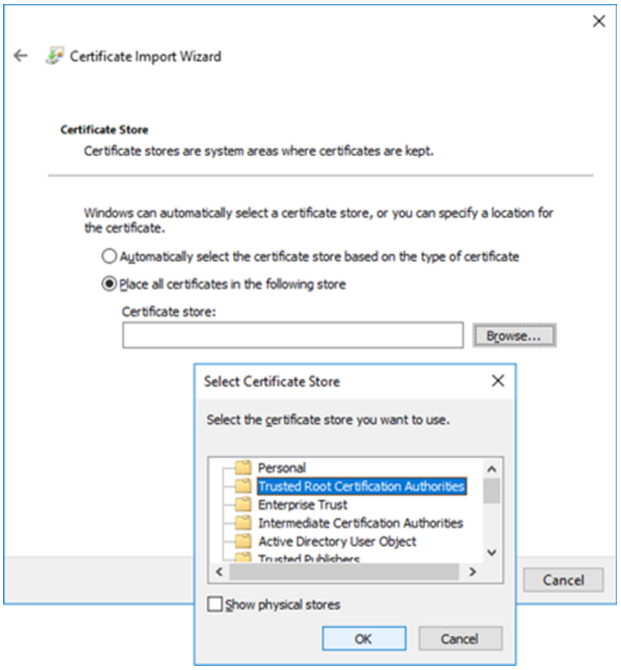
Store Location

○ Current User

● Local Machine

To continue, click Next.

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


Certificate Import Wizard
Browse...
Cancel
Select Certificate Store
Personal
Trusted Root Certification Authorities
Enterprise Trust
Intermediate Certification Authorities
Active Directory User Object
Trusted Publishers
OK
Cancel

Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

○ Automatically select the certificate store based on the type of certificate

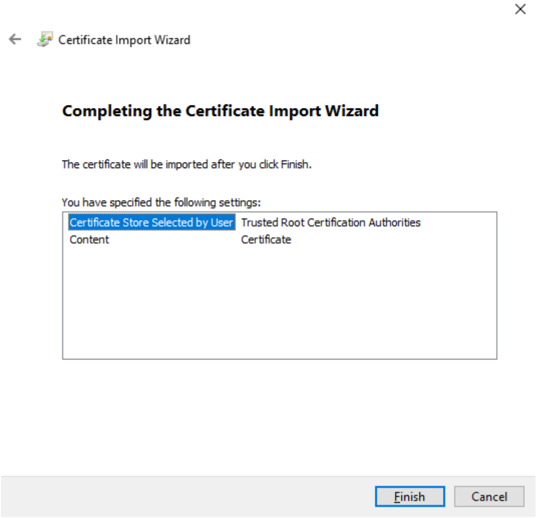
● Place all certificates in the following store

Certificate store:

Select the certificate store you want to use.

☐ Show physical stores

g. Completing the Certificate Import Wizard.



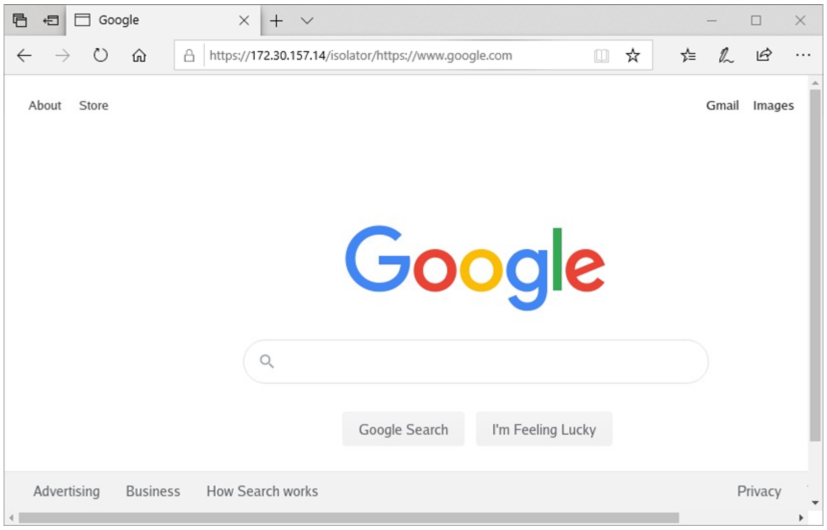
Completing the Certificate Import Wizard

The certificate will be imported after you click Finish.

You have specified the following settings:

Certificate Store Selected by User	Trusted Root Certification Authorities
Content	Certificate

- 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 FortiIsolator internal interface.



Proxy mode

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

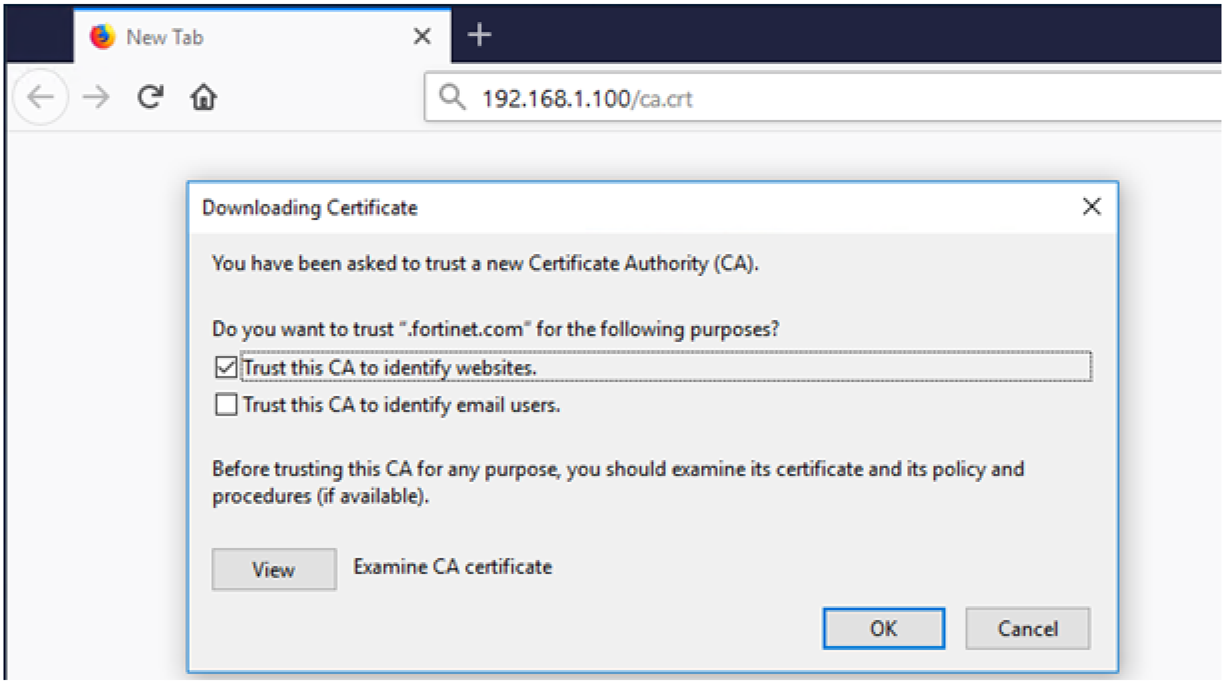
- Using proxy mode with Mozilla Firefox on page 66
- Using proxy mode with Google Chrome on page 70
- Using proxy mode with Internet Explorer on page 78
- Using proxy mode with Edge on page 82

Using proxy mode with Mozilla Firefox

To configure proxy mode with Mozilla Firefox:

1. Download the FortiIsolator 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 FortiIsolator internal interface.

   b. In the *Downloading Certificate* window, select the *Trust this CA to identify websites* checkbox.
   c. Click *OK*.



You have been asked to trust a new Certificate Authority (CA).

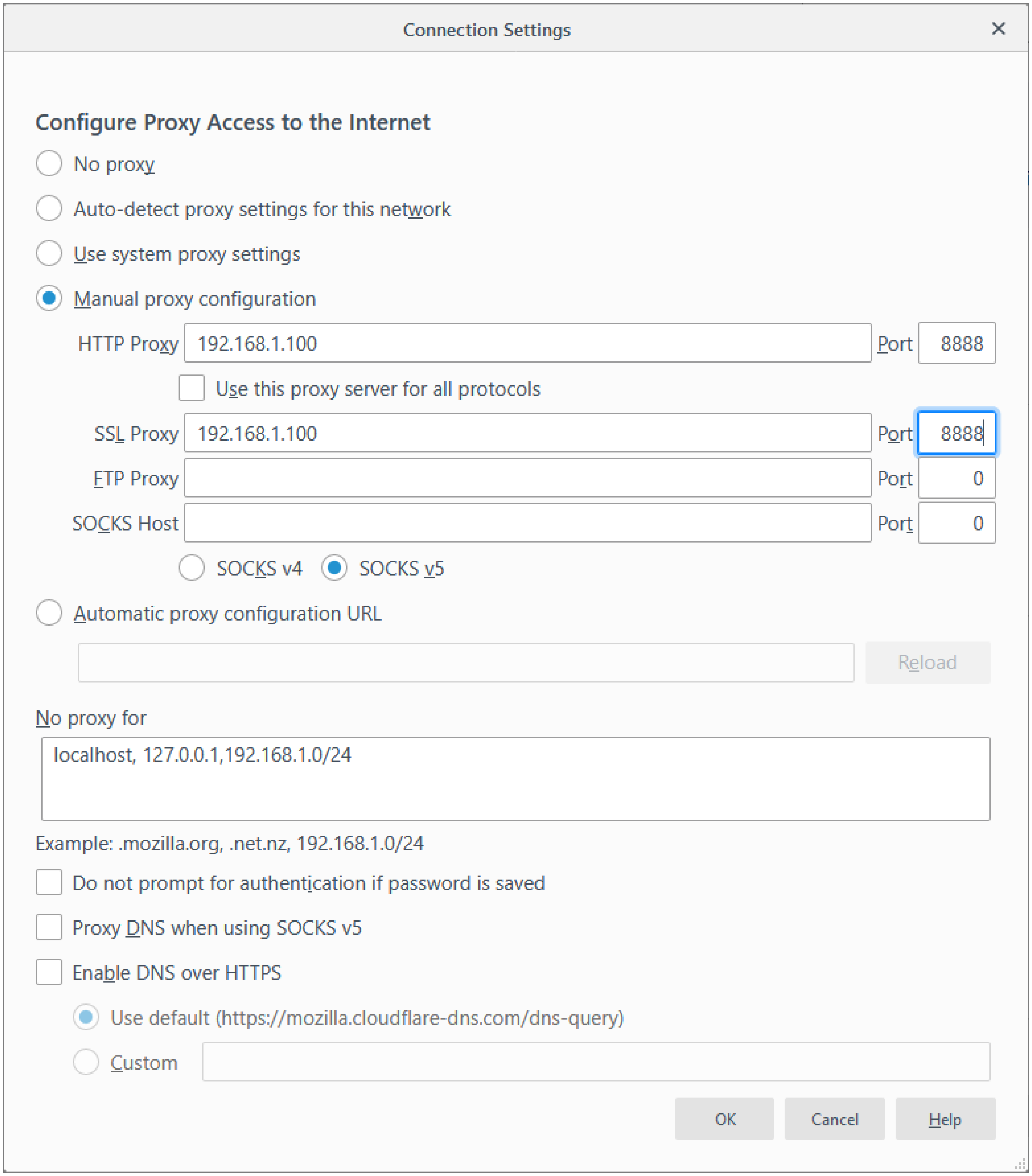
Do you want to trust ".fortinet.com" for the following purposes?

☑ Trust this CA to identify websites.

☐ Trust this CA to identify email users.

Before trusting this CA for any purpose, you should examine its certificate and its policy and procedures (if available).

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 FortiIsolator internal interface.
7. Click *OK*.



Connection Settings

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)

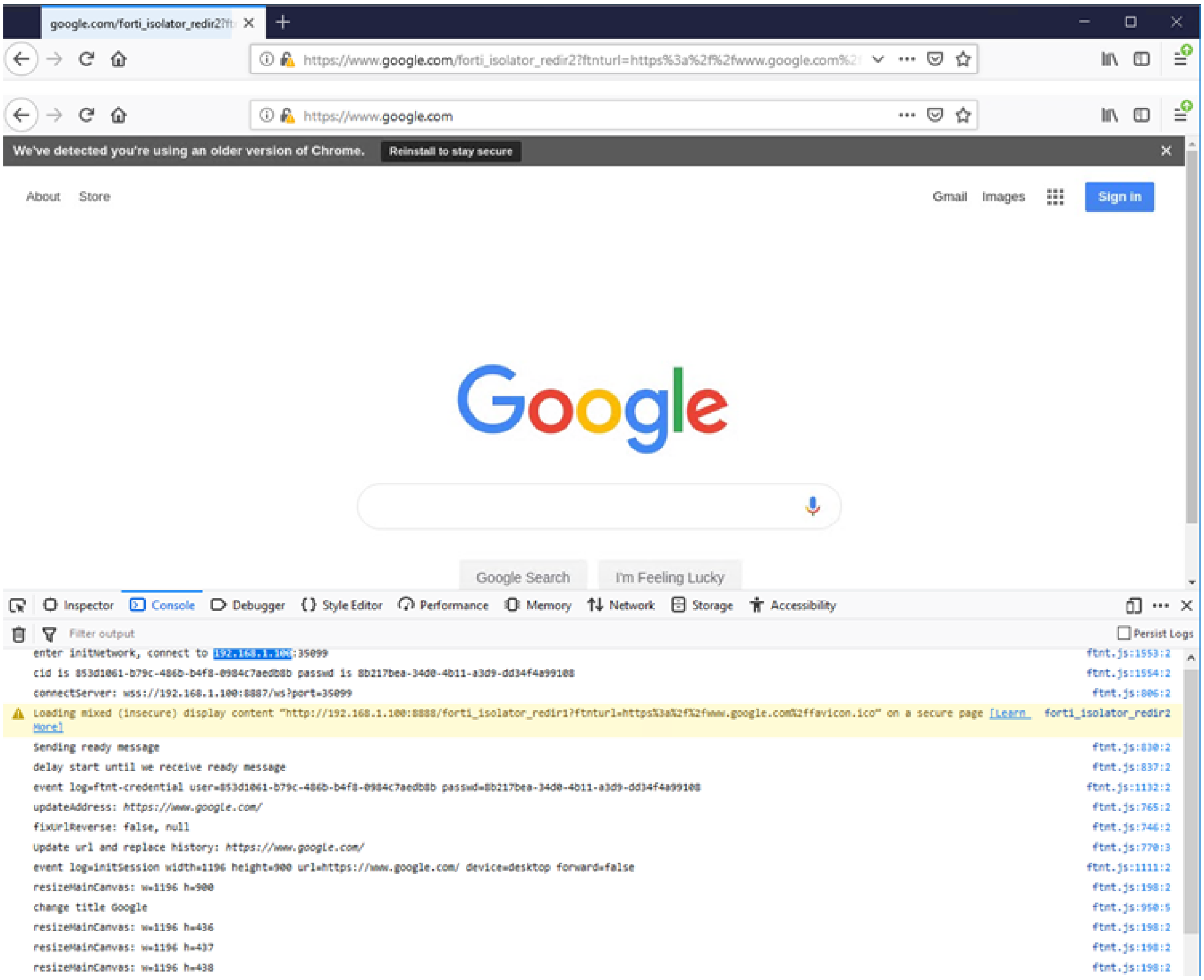
○ Custom

OK Cancel Help

Verifying FortiIsolator proxy mode with Mozilla Firefox

To verify that FortiIsolator 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 FortiIsolator (for example, 192.168.1.100).



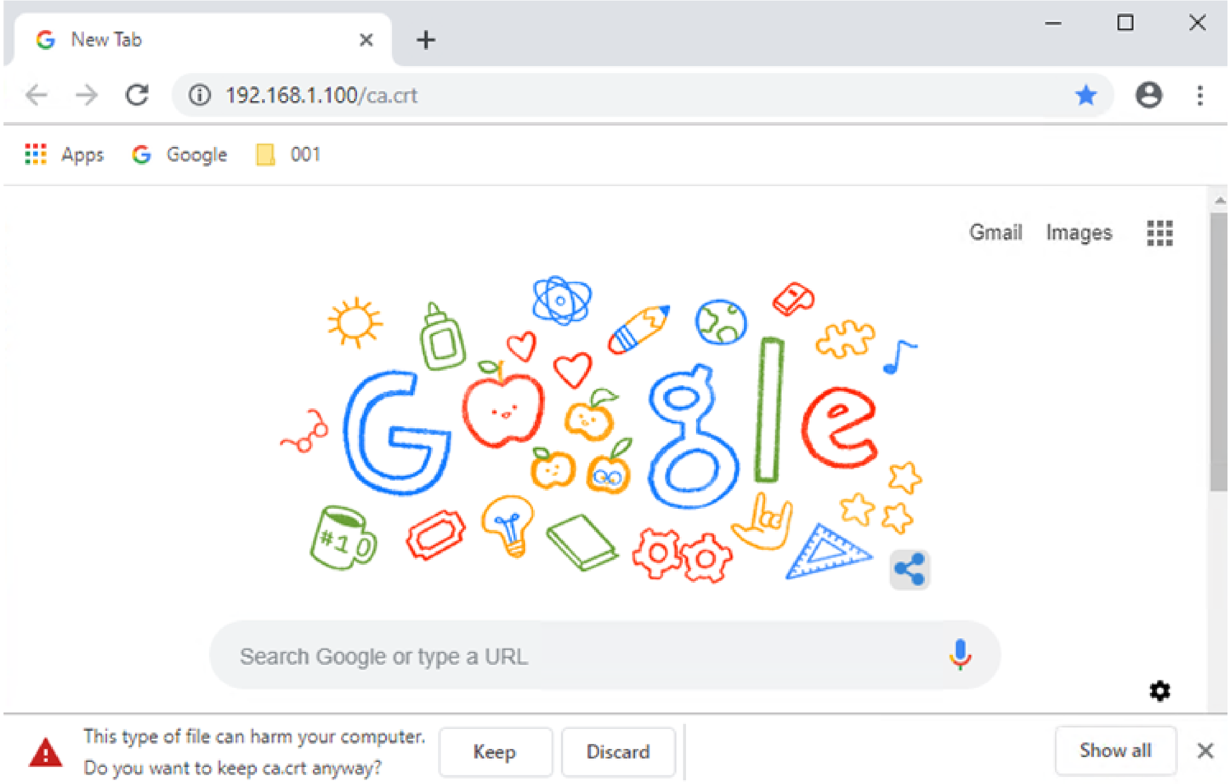
We've detected you're using an older version of Chrome.

```
enter initNetwork, connect to 192.168.1.100:35099                                                ftnt.js:1553:2
cid is 853d1061-b79c-486b-b4f8-0984c7aedb8b passwd is 8b217bea-34d0-4b11-a3d9-dd34f4a99108       ftnt.js:1554:2
connectServer: wss://192.168.1.100:8887/ws?port=35099                                             ftnt.js:806:2
Loading mixed (insecure) display content "http://192.168.1.100:8888/forti_isolator_redir1?ftnturl=https%3a%2f%2fwww.google.com%2ffavicon.ico" on a secure page [Learn   forti_isolator_redir2
More]
Sending ready message                                                                             ftnt.js:830:2
delay start until we receive ready message                                                        ftnt.js:837:2
event log=ftnt-credential user=853d1061-b79c-486b-b4f8-0984c7aedb8b passwd=8b217bea-34d0-4b11-a3d9-dd34f4a99108   ftnt.js:1132:2
updateAddress: https://www.google.com/                                                            ftnt.js:765:2
fixUrlReverse: false, null                                                                        ftnt.js:746:2
Update url and replace history: https://www.google.com/                                           ftnt.js:770:3
event log=initSession width=1196 height=900 url=https://www.google.com/ device=desktop forward=false   ftnt.js:1111:2
resizeMainCanvas: w=1196 h=900                                                                    ftnt.js:198:2
change title Google                                                                               ftnt.js:950:5
resizeMainCanvas: w=1196 h=436                                                                    ftnt.js:198:2
resizeMainCanvas: w=1196 h=437                                                                    ftnt.js:198:2
resizeMainCanvas: w=1196 h=438                                                                    ftnt.js:198:2
```

Using proxy mode with Google Chrome

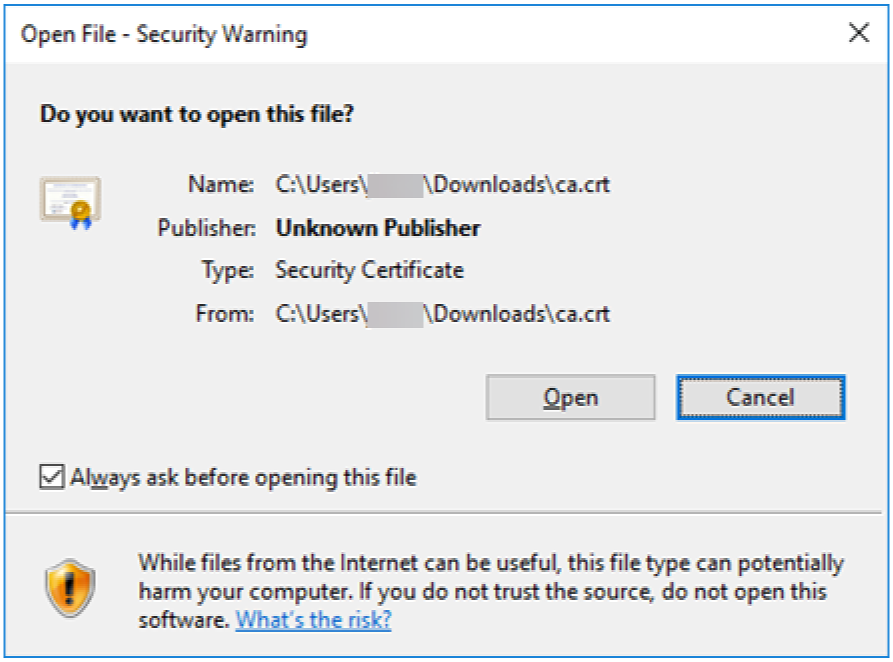
To configure proxy mode with Google Chrome:

1. Download the FortiIsolator 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 FortiIsolator internal interface.
   b. In the security warning at the bottom of the browser, click *Keep* to download the certificate.



This type of file can harm your computer. Do you want to keep ca.crt anyway?

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



Do you want to open this file?

Name: C:\Users\[redacted]\Downloads\ca.crt

Publisher: **Unknown Publisher**

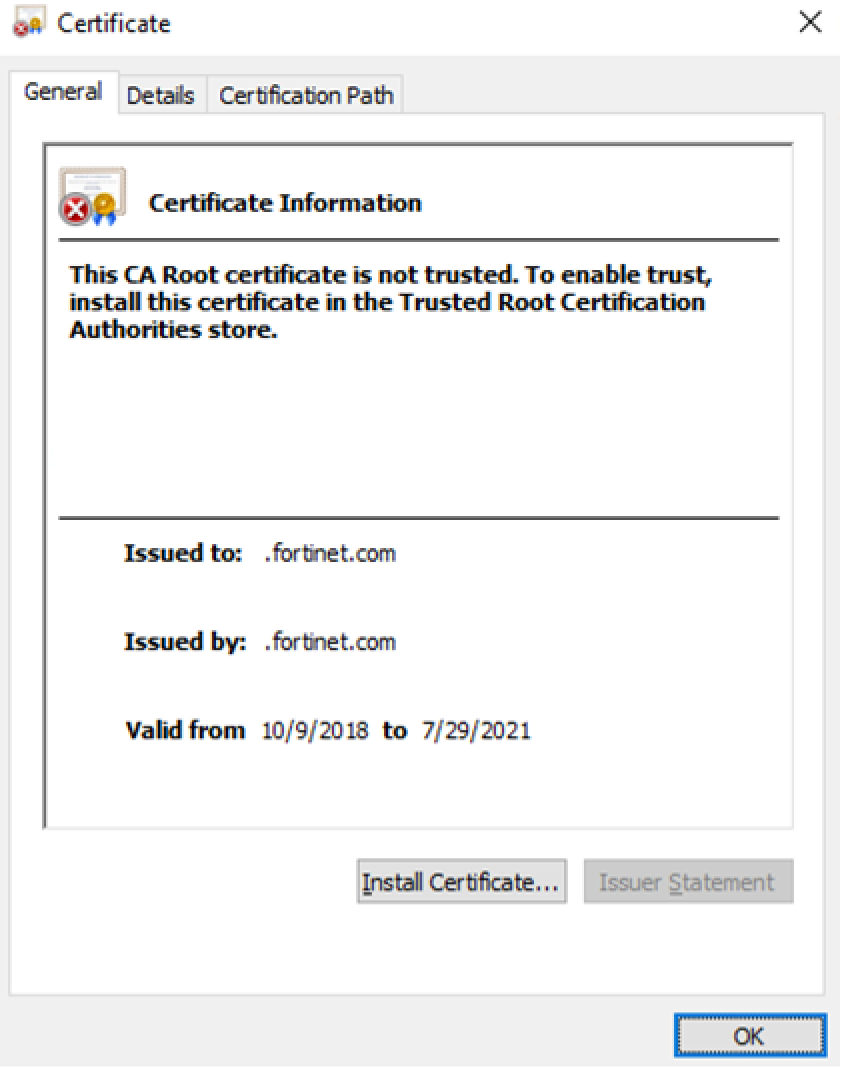
Type: Security Certificate

From: C:\Users\[redacted]\Downloads\ca.crt

☑ Always ask before opening this file

While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not open this software. What's the risk?

d. Click *Install Certificate*.



Certificate Information

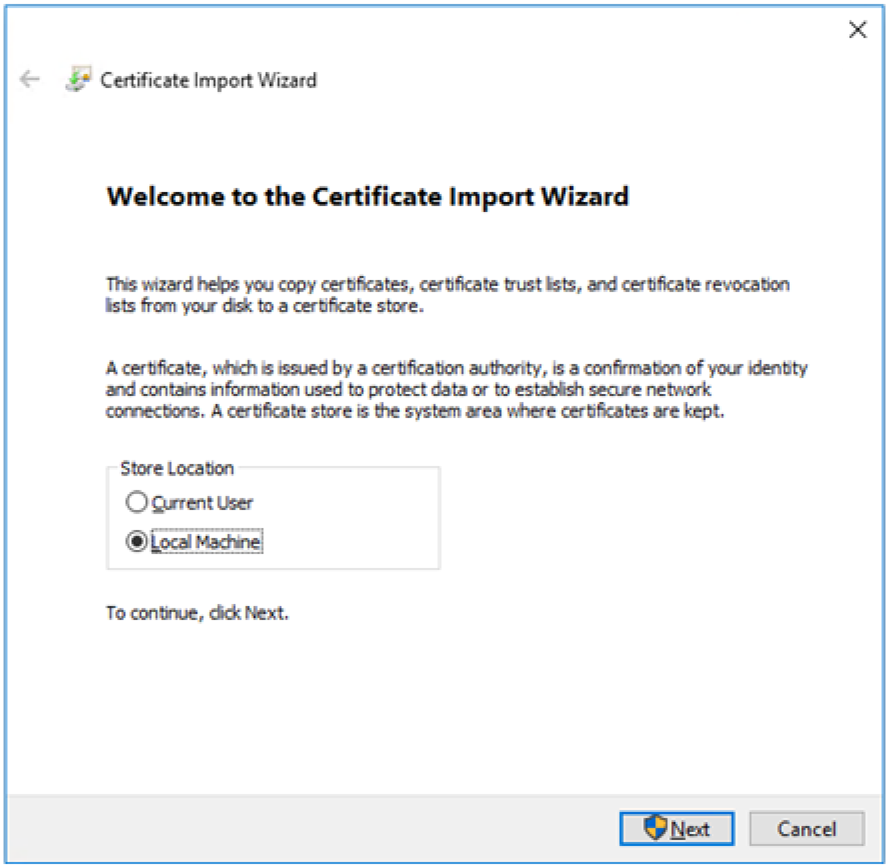
This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

Issued to: .fortinet.com

Issued by: .fortinet.com

Valid from 10/9/2018 **to** 7/29/2021

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



Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

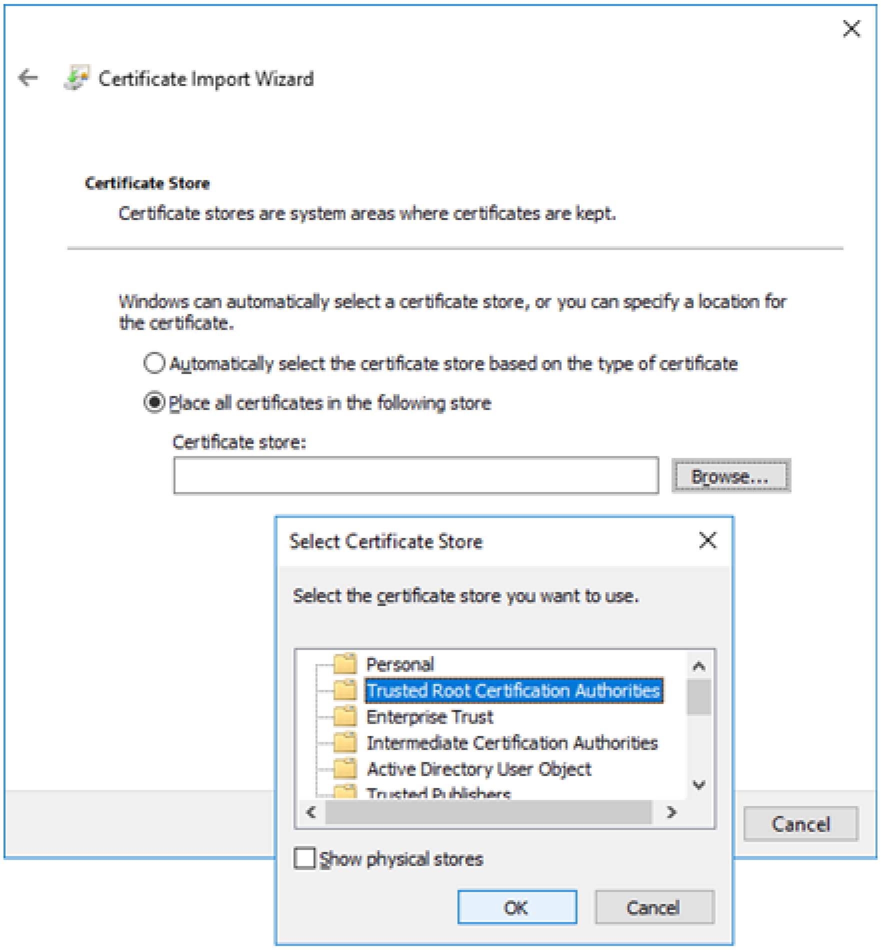
Store Location

○ Current User

● Local Machine

To continue, click Next.

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



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store:

Select Certificate Store

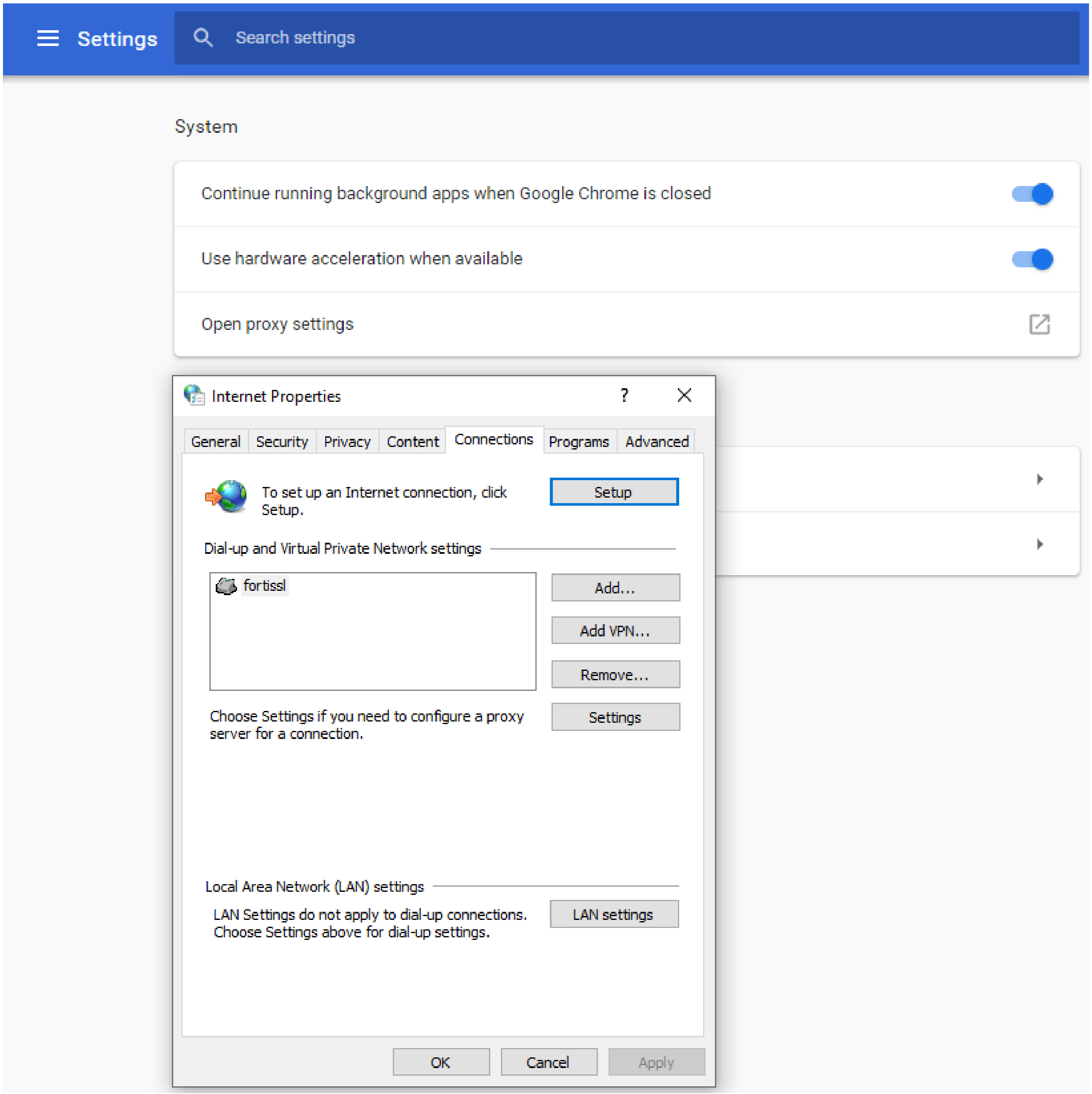
Select the certificate store you want to use.

- Personal
- Trusted Root Certification Authorities
- Enterprise Trust
- Intermediate Certification Authorities
- Active Directory User Object
- Trusted Publishers

☐ Show physical stores

2. Open the Google Chrome browser.

3. In the menu, click *Settings*.



Continue running background apps when Google Chrome is closed

Use hardware acceleration when available

Open proxy settings

To set up an Internet connection, click Setup.

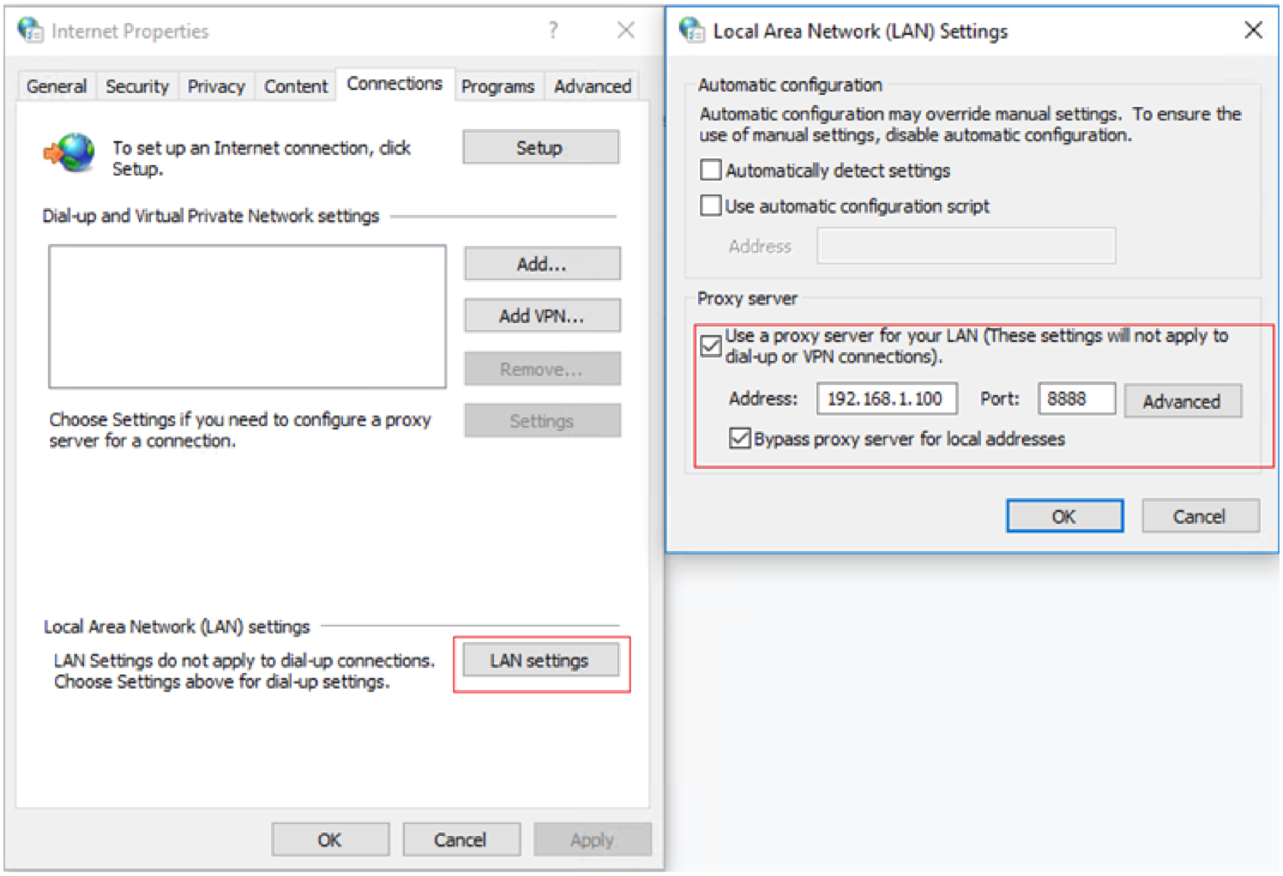
Dial-up and Virtual Private Network settings

Choose Settings if you need to configure a proxy server for a connection.

Local Area Network (LAN) settings

LAN Settings do not apply to dial-up connections. Choose Settings above for dial-up 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



To set up an Internet connection, click Setup.

Dial-up and Virtual Private Network settings

Choose Settings if you need to configure a proxy server for a connection.

Local Area Network (LAN) settings

LAN Settings do not apply to dial-up connections. Choose Settings above for dial-up settings.

Automatic configuration

Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.

☐ Automatically detect settings

☐ Use automatic configuration script

Address

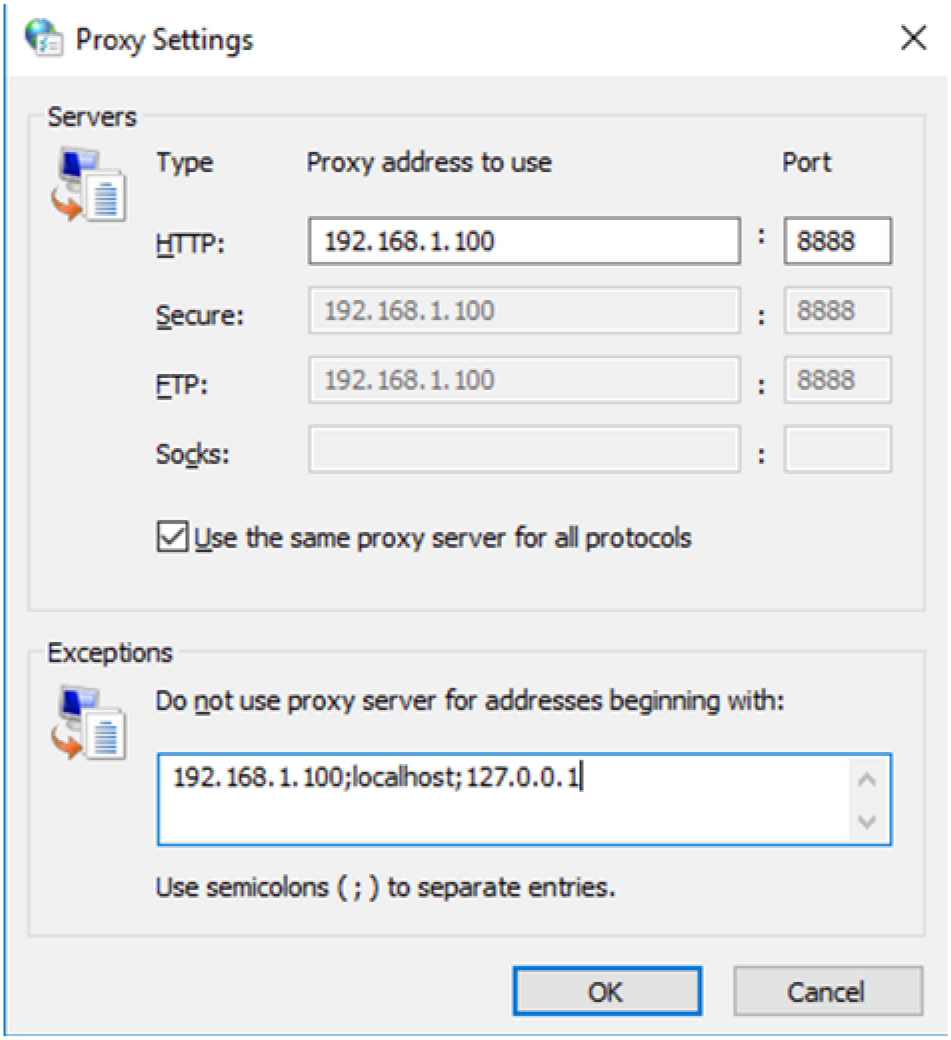
Proxy server

☑ Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).

Address: 192.168.1.100 Port: 8888

☑ Bypass proxy server for local addresses

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).



Proxy Settings

Servers

Type	Proxy address to use		Port
HTTP:	192.168.1.100	:	8888
Secure:	192.168.1.100	:	8888
FTP:	192.168.1.100	:	8888
Socks:		:	

☑ Use the same proxy server for all protocols

Exceptions

Do not use proxy server for addresses beginning with:

192.168.1.100;localhost;127.0.0.1

Use semicolons (;) to separate entries.

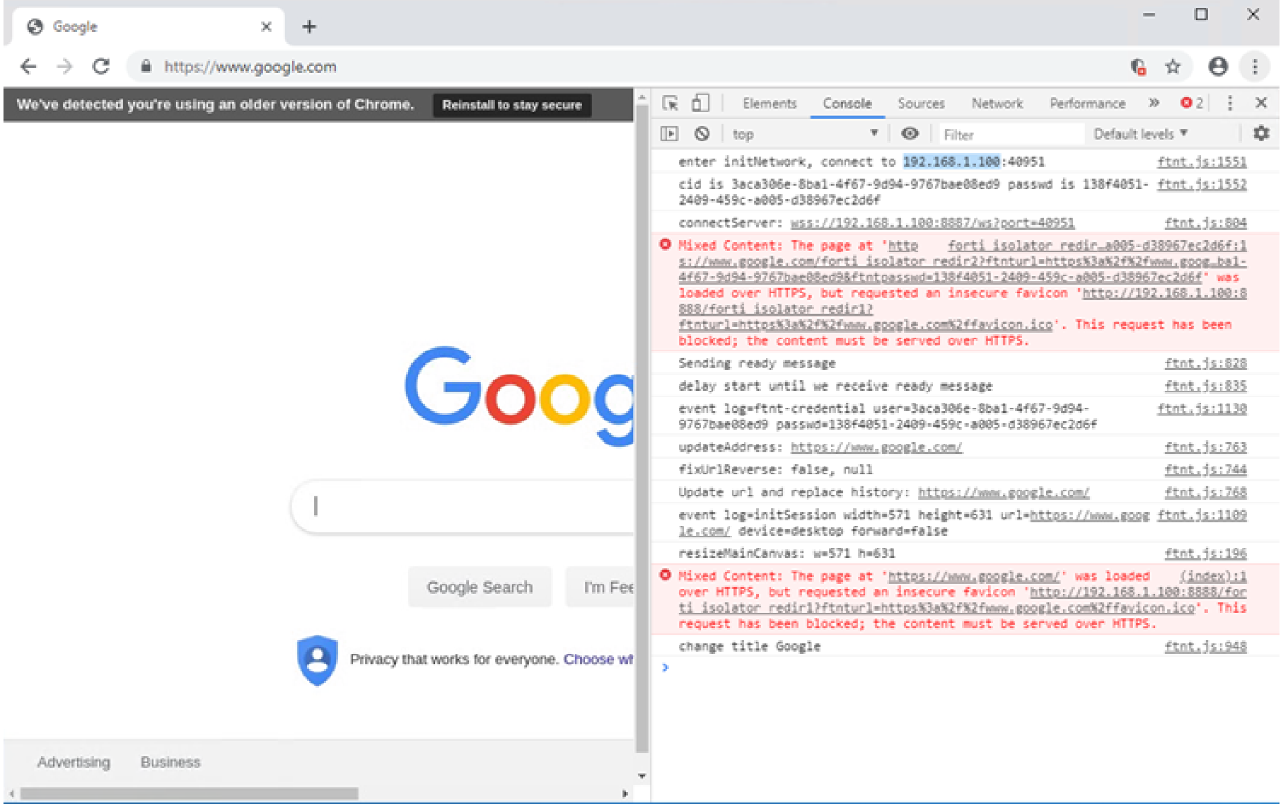
11. Click *OK* to accept the settings in all windows.

Verifying FortiIsolator proxy mode with Google Chrome

To verify that FortiIsolator 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 FortiIsolator (for example,

192.168.1.100).



```
enter initNetwork, connect to 192.168.1.100:40951                              ftnt.js:1551
cid is 3aca306e-8ba1-4f67-9d94-9767bae08ed9 passwd is 138f4051-                ftnt.js:1552
2409-459c-a005-d38967ec2d6f
connectServer: wss://192.168.1.100:8887/ws?port=40951                           ftnt.js:804
Mixed Content: The page at 'http    forti isolator redir…a005-d38967ec2d6f:1
s://www.google.com/forti isolator redir2?ftnturl=https%3a%2f%2fwww.goog…ba1-
4f67-9d94-9767bae08ed9&ftntpasswd=138f4051-2409-459c-a005-d38967ec2d6f' was
loaded over HTTPS, but requested an insecure favicon 'http://192.168.1.100:8
888/forti isolator redir1?
ftnturl=https%3a%2f%2fwww.google.com%2ffavicon.ico'. This request has been
blocked; the content must be served over HTTPS.
Sending ready message                                                           ftnt.js:828
delay start until we receive ready message                                      ftnt.js:835
event log=ftnt-credential user=3aca306e-8ba1-4f67-9d94-                        ftnt.js:1130
9767bae08ed9 passwd=138f4051-2409-459c-a005-d38967ec2d6f
updateAddress: https://www.google.com/                                          ftnt.js:763
fixUrlReverse: false, null                                                      ftnt.js:744
Update url and replace history: https://www.google.com/                         ftnt.js:768
event log=initSession width=571 height=631 url=https://www.goog ftnt.js:1109
le.com/ device=desktop forward=false
resizeMainCanvas: w=571 h=631                                                   ftnt.js:196
Mixed Content: The page at 'https://www.google.com/' was loaded      (index):1
over HTTPS, but requested an insecure favicon 'http://192.168.1.100:8888/for
ti isolator redir1?ftnturl=https%3a%2f%2fwww.google.com%2ffavicon.ico'. This
request has been blocked; the content must be served over HTTPS.
change title Google                                                             ftnt.js:948
```

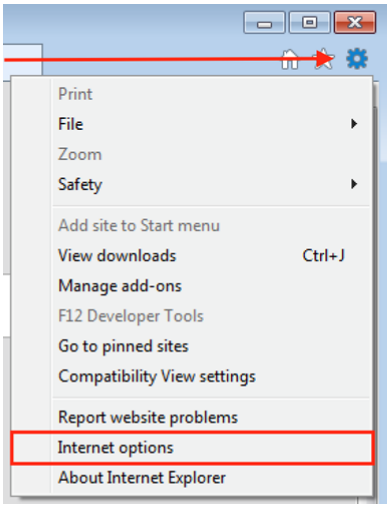
Using proxy mode with Internet Explorer

Pre-requisites:

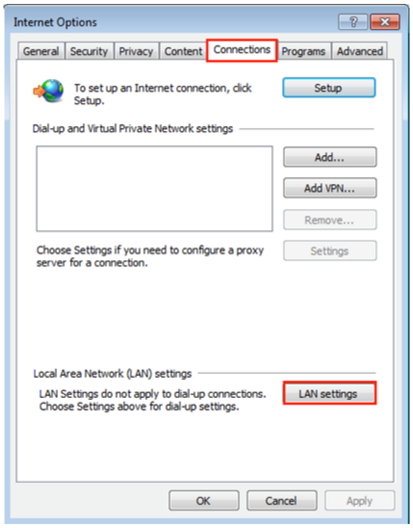
Please follow step 1 in Using IP Forwarding mode with Internet Explorer on page 59 to install FortiIsoaltor `ca.crt` certificate prior to using proxy mode.

To configure proxy mode with Internet Explorer:

1. Open an Internet Explorer browser window and click the gear icon at the top right corner to open browser settings.
2. Select *Internet options* from the settings menu.



3. Navigate to the *Connections* tab and select the *LAN settings* button.

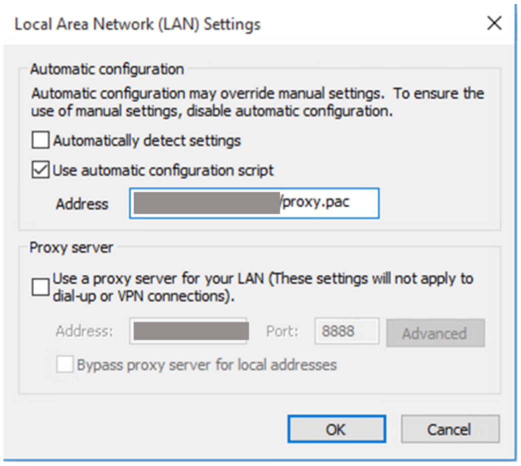


To set up an Internet connection, click Setup.

Choose Settings if you need to configure a proxy server for a connection.

LAN Settings do not apply to dial-up connections. Choose Settings above for dial-up settings.

4. Make sure the *Automatically detect settings* box is not checked. (If it is checked, uncheck it).
5. Check the *Use automatic configuration script* box and paste your proxy IP address into the *Address* field and click *OK*.



Local Area Network (LAN) Settings

Automatic configuration

Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.

□ Automatically detect settings

☑ Use automatic configuration script

Address [redacted]/proxy.pac

Proxy server

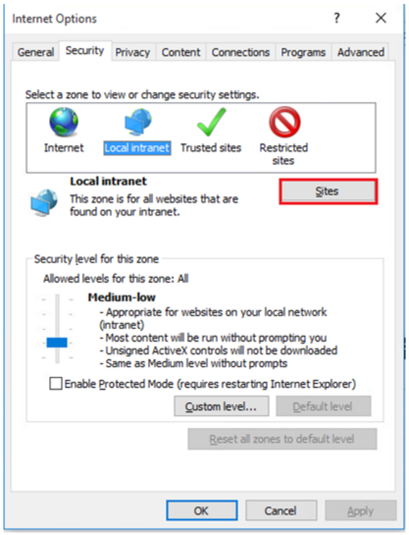
□ Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).

Address: [redacted] Port: 8888 Advanced

□ Bypass proxy server for local addresses

OK Cancel

6. Navigate to the *Security* tab and select the *Local intranet* zone.



Internet Options

General | Security | Privacy | Content | Connections | Programs | Advanced

Select a zone to view or change security settings.

Internet | Local intranet | Trusted sites | Restricted sites

Local intranet

This zone is for all websites that are found on your intranet.

Sites

Security level for this zone

Allowed levels for this zone: All

Medium-low

- Appropriate for websites on your local network (intranet)
- Most content will be run without prompting you
- Unsigned ActiveX controls will not be downloaded
- Same as Medium level without prompts

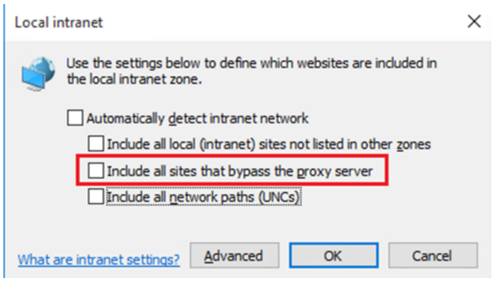
□ Enable Protected Mode (requires restarting Internet Explorer)

Custom level... Default level

Reset all zones to default level

OK Cancel Apply

7. Click the *Sites* button to configure how Intranet sites are detected.
8. Make sure that at the very least the *Include all sites that bypass the proxy server* box is not checked. We recommend that all the options for these settings are not checked when possible. Click *OK*.



Local intranet

Use the settings below to define which websites are included in the local intranet zone.

□ Automatically detect intranet network

□ Include all local (intranet) sites not listed in other zones

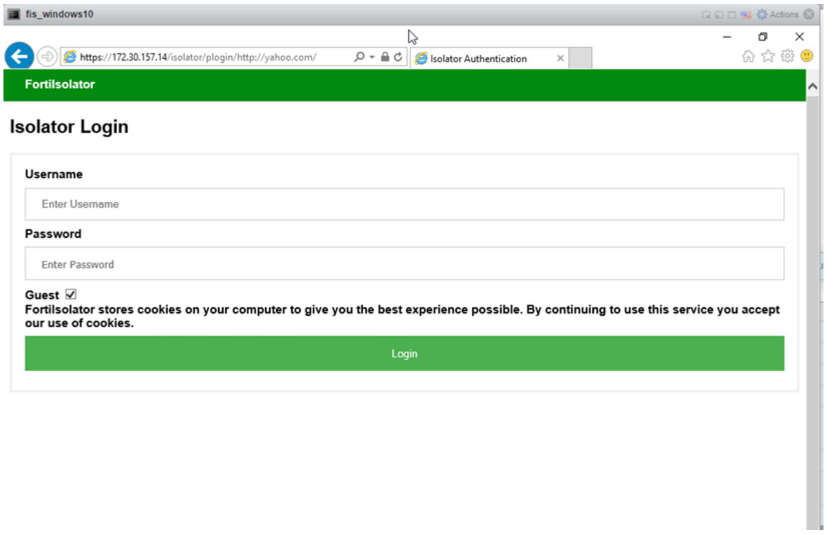
□ Include all sites that bypass the proxy server

□ Include all network paths (UNCs)

What are intranet settings? Advanced OK Cancel

9. Close and restart Internet Explorer.

Verifying FortiIsolator proxy mode with Internet Explorer



Isolator Login

Username

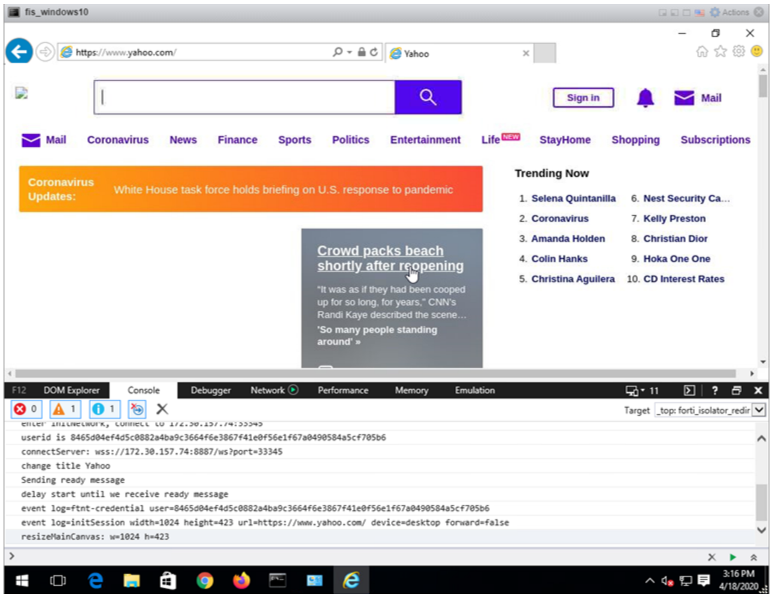
Enter Username

Password

Enter Password

Guest ☑
FortiIsolator stores cookies on your computer to give you the best experience possible. By continuing to use this service you accept our use of cookies.

Login



Coronavirus Updates: White House task force holds briefing on U.S. response to pandemic

Trending Now

1. Selena Quintanilla
2. Coronavirus
3. Amanda Holden
4. Colin Hanks
5. Christina Aguilera
6. Nest Security Ca...
7. Kelly Preston
8. Christian Dior
9. Hoka One One
10. CD Interest Rates

Crowd packs beach shortly after reopening

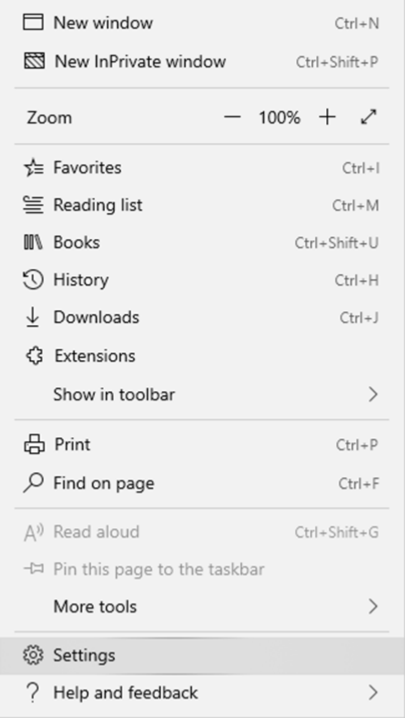
"It was as if they had been cooped up for so long, for years," CNN's Randi Kaye described the scene... 'So many people standing around' »

```
enter initNetwork, connect to 172.30.157.74:33345
userid is 8465d04ef4d5c0882a4ba9c3664f6e3867f41e0f56e1f67a0490584a5cf705b6
connectServer: wss://172.30.157.74:8887/ws?port=33345
change title Yahoo
Sending ready message
delay start until we receive ready message
event log=ftnt-credential user=8465d04ef4d5c0882a4ba9c3664f6e3867f41e0f56e1f67a0490584a5cf705b6
event log=initSession width=1024 height=423 url=https://www.yahoo.com/ device=desktop forward=false
resizeMainCanvas: w=1024 h=423
```

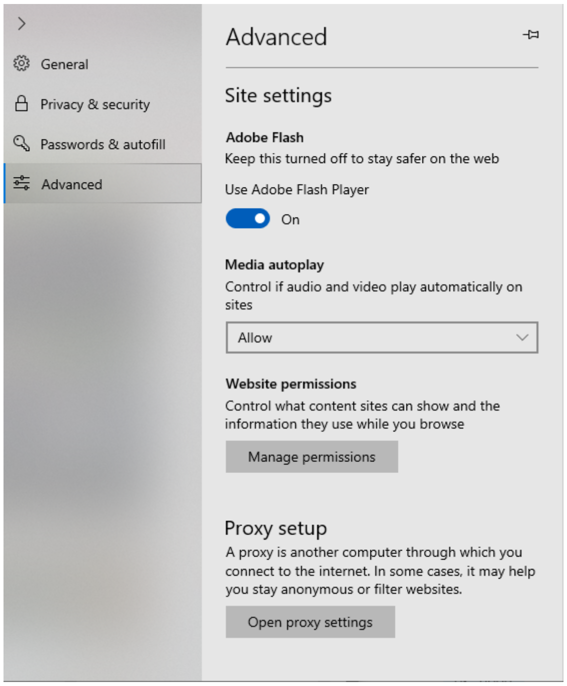
Using proxy mode with Edge

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*.



Advanced

Site settings

Adobe Flash
Keep this turned off to stay safer on the web

Use Adobe Flash Player
On

Media autoplay
Control if audio and video play automatically on sites

Allow

Website permissions
Control what content sites can show and the information they use while you browse

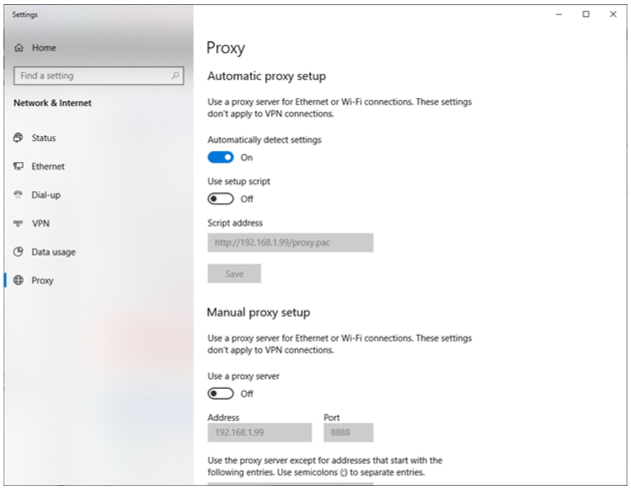
Manage permissions

Proxy setup

A proxy is another computer through which you connect to the internet. In some cases, it may help you stay anonymous or filter websites.

Open proxy settings

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



Proxy

Automatic proxy setup

Use a proxy server for Ethernet or Wi-Fi connections. These settings don't apply to VPN connections.

Automatically detect settings
On

Use setup script
Off

Script address
http://192.168.1.99/proxy.pac

Save

Manual proxy setup

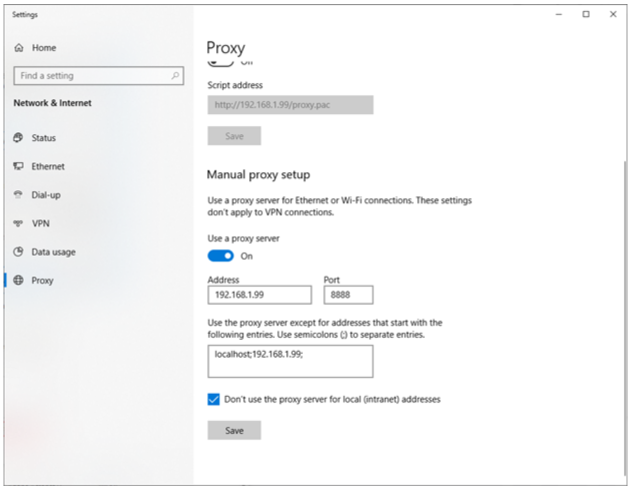
Use a proxy server for Ethernet or Wi-Fi connections. These settings don't apply to VPN connections.

Use a proxy server
Off

Address: 192.168.1.99
Port: 8888

Use the proxy server except for addresses that start with the following entries. Use semicolons (;) to separate entries.

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



Proxy

Script address
http://192.168.1.99/proxy.pac

Save

Manual proxy setup

Use a proxy server for Ethernet or Wi-Fi connections. These settings don't apply to VPN connections.

Use a proxy server
On

Address: 192.168.1.99
Port: 8888

Use the proxy server except for addresses that start with the following entries. Use semicolons (;) to separate entries.

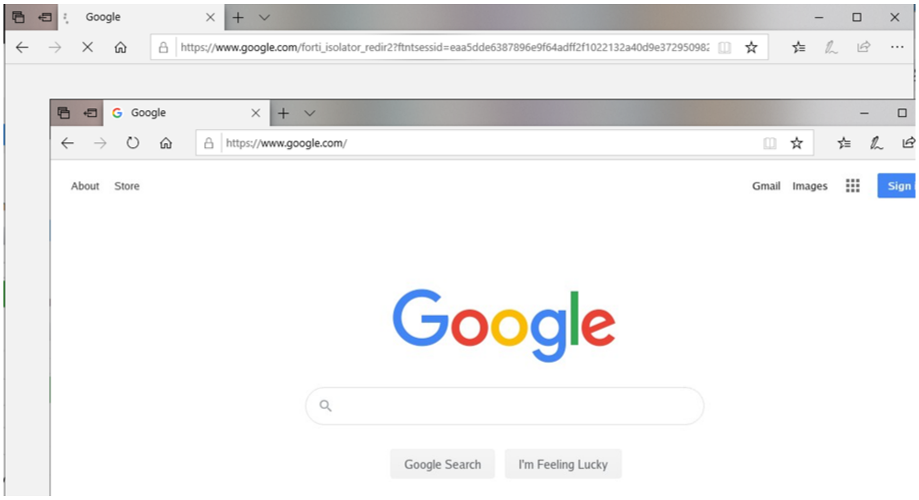
localhost;192.168.1.99;

☑ Don't use the proxy server for local (intranet) addresses

Save

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

Verifying FortiIsolator proxy mode with Edge



https://www.google.com/forti_isolator_redir2?ftntsessid=eaa5dde6387896e9f64adff2f1022132a40d9e37295098z

https://www.google.com/

Logging in as an end user

Depending on the Default policy on page 44 that applies to the end user, the user can log into FortiIsolator in one of the following ways:

- **Local user** - The user enters the designated username and password configured in User definition on page 30. This option is available only if *Guest Type* of the default 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 default 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 26, 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 default policy is *guest enable* or *guest disable*.

Copying and pasting text

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

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 FortiIsolator:

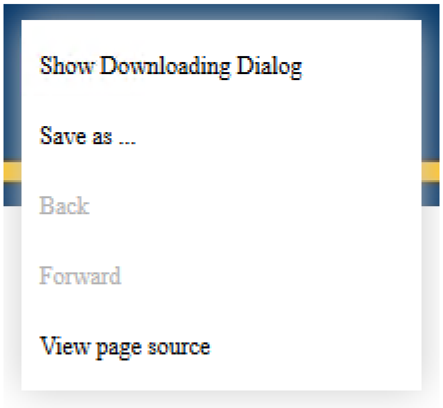
1. In a browser, right-click on the images that you want to save.
2. Click *Copy Image to clipboard*.
3. Open MS Word, MS Excel, or MS Powerpoint
4. Press `Ctrl+V` or right-click to paste the image.

Downloading files

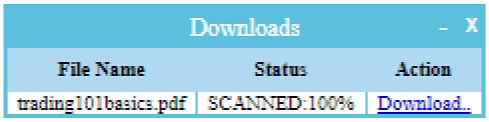
End users are able to download files up to a certain file size while browsing through FortiIsolator if the administrator has configured the Isolator Profile settings to allow it.

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 FortiIsolator to FortiProxy

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

FortiIsolator setup

To download FortiIsolator CA certificate:

1. Connect to FortiIsolator.
2. Go to *Dashboard* > *System Information* > *Isolator CA Certificate* > *Backup/Restore*.
3. Backup the CA Certificates by pressing *Click here*. Save the `ca.tgz` file to your local system.
4. Unzip `ca.tgz`, you get 3 files under a new folder; these files will be use later when configuring FortiProxy.

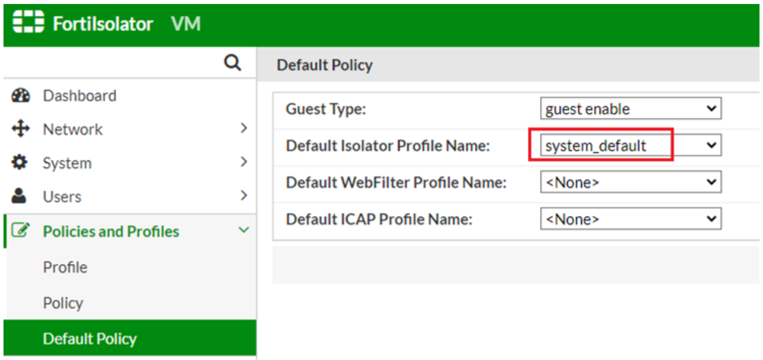
To configure default policy:

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 FortiIsolator Profile name that is selected in FortiIsolator Default Policy setting.

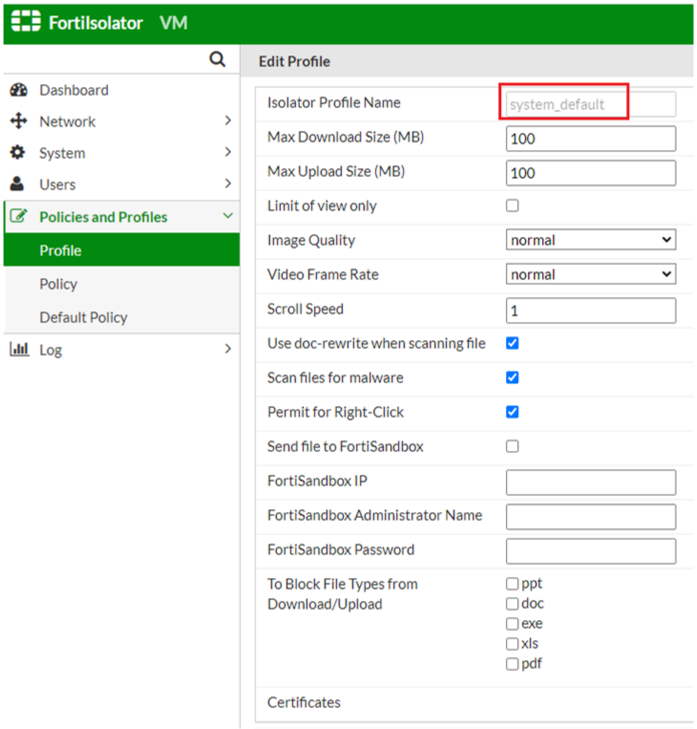
Currently the profile name "system_default" is being used in the example below. All settings, as in FortiProxy header content, FortiIsolator Isolator Profile Name, and FortiIsolator Default Isolator Profile, are using the same profile name "system_default."

Example



Default Policy

Guest Type:	guest enable
Default Isolator Profile Name:	system_default
Default WebFilter Profile Name:	<None>
Default ICAP Profile Name:	<None>



Isolator Profile Name	system_default
Max Download Size (MB)	100
Max Upload Size (MB)	100
Limit of view only	☐
Image Quality	normal
Video Frame Rate	normal
Scroll Speed	1
Use doc-rewrite when scanning file	☑
Scan files for malware	☑
Permit for Right-Click	☑
Send file to FortiSandbox	☐
FortiSandbox IP	
FortiSandbox Administrator Name	
FortiSandbox Password	
To Block File Types from Download/Upload	☐ppt ☐doc ☐exe ☐xls ☐pdf
Certificates	

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 FortiIsolator CA certificate and create a new SSL/SSH inspection profile:

1. Import FortiIsolator CA Certificate:
   a. Connect to FortiProxy portal GUI by going to *System* > *Certificates* > *Import* > *CA Certificate*.
   b. Set *Type* as *File*.
   c. Upload: `ca.crt` browser to where you save the FortiIsolator CA certificate.
   d. Click *OK*

   Doing do ensures that FortiProxy will trust FortiIsolator when dealing with HTTPS traffic.

   e. Go to *System* > *Certificates* > *Import* > *Local Certificate*.
   f. Type: *Certificate*
   g. Certificate file: `ca.crt`
   h. Key file: `ca.key`
   i. Certificate name: *FIS_CA_Cert*

   j. Leave eveything else as it is.
   k. 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: FortiIsolator
   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-nic	Display general network interface setting
diagnose-wf	Test and show WF action for an URL

FORTINET®

www.fortinet.com