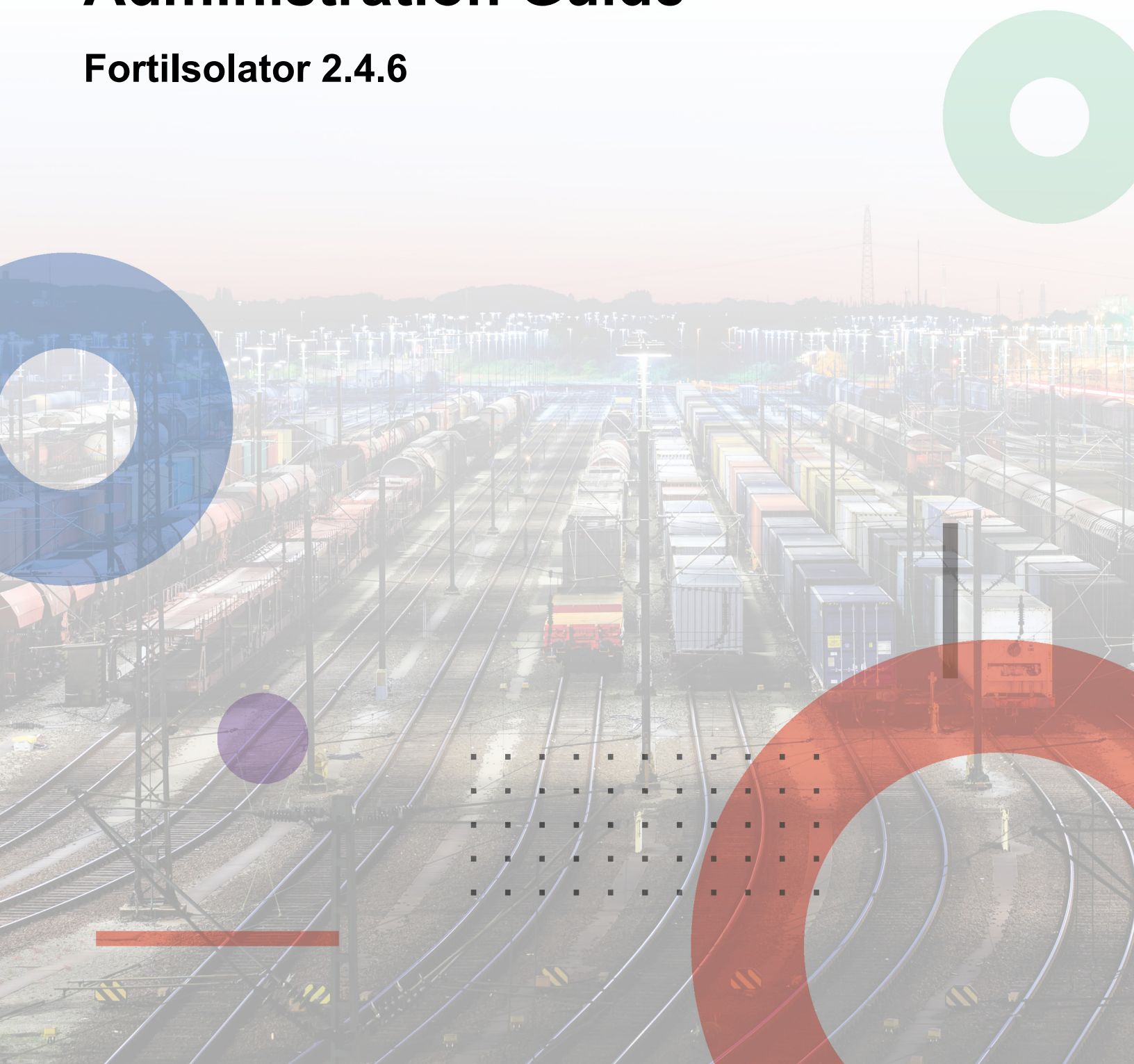
FORTINET

# Administration Guide

## FortiIsolator 2.4.6



**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 2.4.6 Administration Guide
51-246-1032191-20250416

# TABLE OF CONTENTS

# Change log

| Date | Change Description |
| --- | --- |
| 2024-07-08 | Initial release. |
| 2025-04-16 | Updated High Availability on page 46 and SAML servers on page 61. |

# Overview

FortiIsolator is a 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.

For more overview information about FortiIsolator, see the FortiIsolator product page and the FortiIsolator data sheet.

For release information about FortiIsolator 2.4.6, such as new features, installation and upgrade instructions, resolved issues, and known issues, see the FortiIsolator Release Notes.

# Port information

The following table lists the ports for inbound traffic of each FortiIsolator service by interface. You must enable the ports for communication between FortiIsolator and servers running associated services. For outbound traffic, FortiIsolator uses a random port picked by the kernel on the internal interface.

| Interface | Service | Protocol | Port |
|---|---|---|---|
| **Interface_internal** | Web access | TCP | 443/80/8800 |
| | HTTPS proxy | TCP | 8888 |
| | Management of FortiIsolator VMs on AWS | TCP | 8080 |
| | SNMP | UDP | 161 |
| | HA synchronization | TCP | 1443/1080/1887/1888 |
| **Interface_mgmt** | SSH | TCP | 22 |

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.

# Setting up IP mapping

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 192.168.1.1/24. You can access FortiIsolator using SSH or the FortiIsolator GUI. The default username is `admin` and the default password is `fortinet`.

Use the FortiIsolator GUI or CLI to set the permanent IP address configuration.

You can perform the initial configuration using the serial console. For more information, see the FortiIsolator 1000F QuickStart Guide.

### Topology

FortiIsolator supports IP mapping, which allows you to configure access to FortiIsolator through port forwarding. Port forwarding maps external IP addresses to FortiIsolator internal IP addresses. You can configure port forwarding in high availability (HA) or regular mode.

For example, given two networks connected to a FortiGate device, one external and the other internal, when IP addresses on the external network are accessed, traffic is redirected to the internal IP addresses on FortiIsolator. The configuration information in this section follows an example setup with the following values:

| | |
|---|---|
| External IP address of router | <external_IP_address> |
| Internal IP address of FortiIsolator | 192.168.0.99 |
| Router redirections | <external_IP_address>:12443 > 192.168.0.99:443 |


IP mapping supports only IP forwarding mode, not Proxy mode.

## Configuring IP mapping in regular mode

Configuring IP Mapping in regular mode (non-HA) requires configurations in three systems:

1. FortiIsolator configuration
2. FortiGate configuration
3. Client system configuration

## FortiIsolator configuration

In the FortiIsolator CLI, configure port forwarding mappings using the `fis-ipmap` command in the following format:

```
set fis-ipmap <port_map_to_443> <external_IP_address>
```

For example,

```
set fis-ipmap 12443 172.30.147.207
```

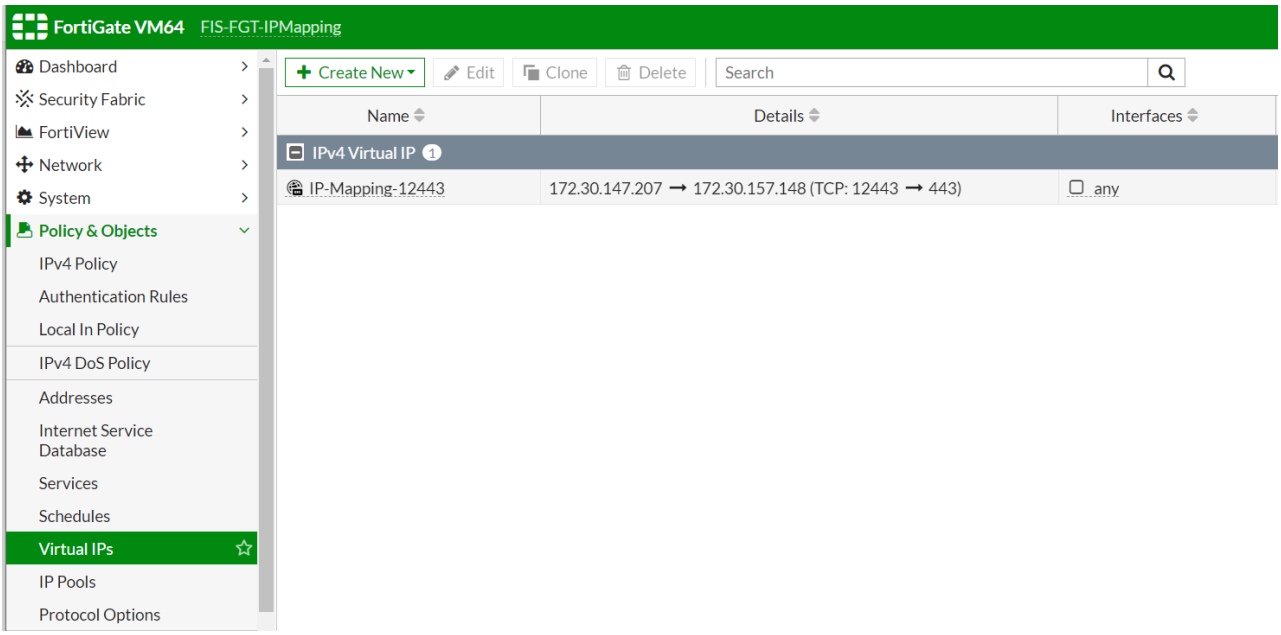
```
[IP Address]
      INTERFACE                IPv4                    MAC
--------------------    --------------------    --------------------
            internal    172.30.157.148/24       00:0C:29:63:17:33
                mgmt    172.30.156.148/24       00:0C:29:63:17:47

[Routing Entries]
         SUBNET              GATEWAY               INTERFACE
--------------------    --------------------    --------------------
           0.0.0.0/0    172.30.157.254          internal

hostname                        : FISVM1TM21000288
dns server                      : 8.8.8.8
dns server                      : 208.91.112.52
build number                    : 0488(interim)
date time                       : 2022-06-14 15:10:09 PDT

[SNMP Configurations]
Agent Listening Interface       : mgmt
Agent Community                 : fis_public
Trap Host-IP                    :
Trap Host Community             :
Session Threashold(%)           : 70
SNMP V3 User Status             : Disabled
SNMP V3 Username                : fis_user
V3 Query Port Status            : Disabled
V3 Query Port Num               : 0
V3 Trap Port Status             : Disabled
V3 Trap Local Port Num          : 162
V3 Trap Remote Port Num         : 162
SNMP V3 Hosts:
Security Level                  : noauth
Authentication Status           : Disabled
Authentication Method           :
Authentication Password         :
Private Status                  : Disabled
Encrypt Method                  :
Encrypt Password                :
SNMP V3 Trap Events:
       check_session_threshold:  Disabled
       send_mgmt_ip_off_days:  Disabled

ip mapping                      : 172.30.147.207
mapping for port 443            : 12443
[IPMAP HA Settings]
priority        IP      IP mapping      Port 443
```

## FortiGate configuration

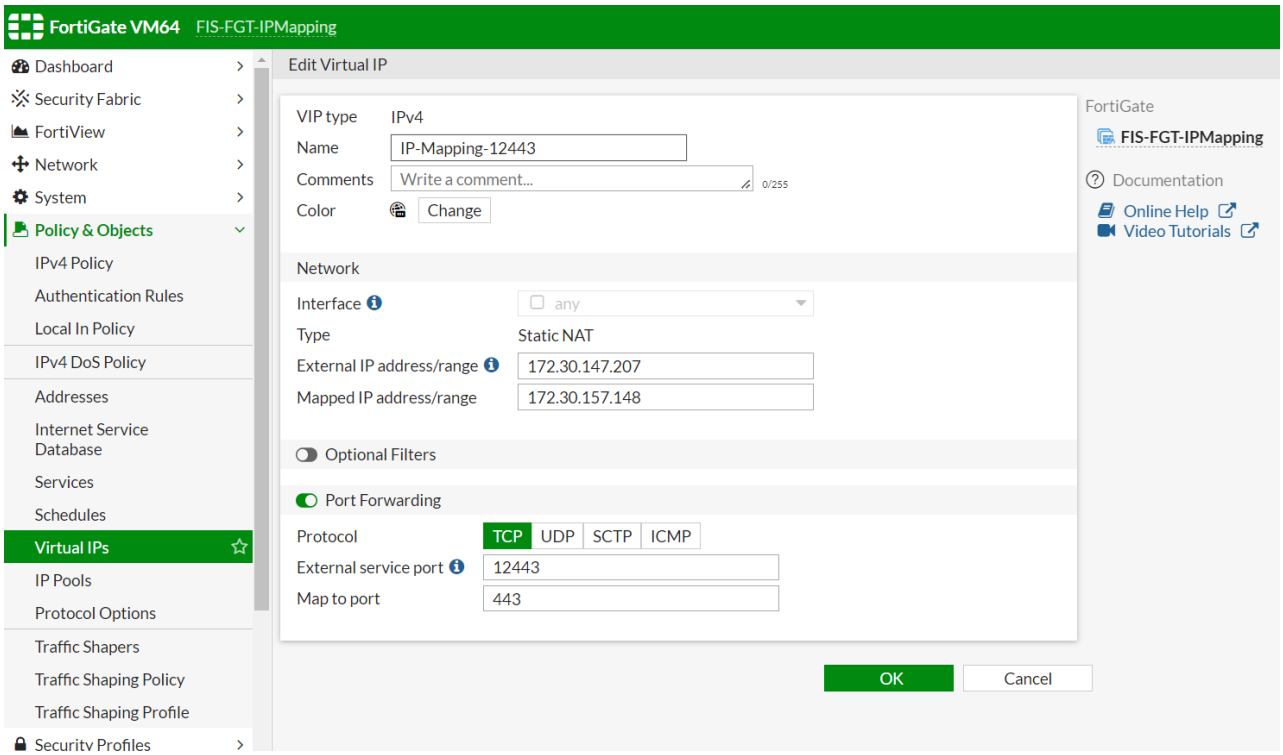
Complete the following steps in the FortiGate UI.

1. Go to *Policy & Objects* > *Virtual IPs*.
2. Create an IPv4 virtual IP with the following information:
   - **IP-Mapping-443**: <external_IP_address> -> FIS_IP (TCP: 12443 > 443)
     For example, 172.30.147.207 -> 172.30.157.148 (TCP: 12443 > 443)

This example uses the following:
- External_IP_address: 172.30.147.207
- FIS_IP: 172.30.157.148

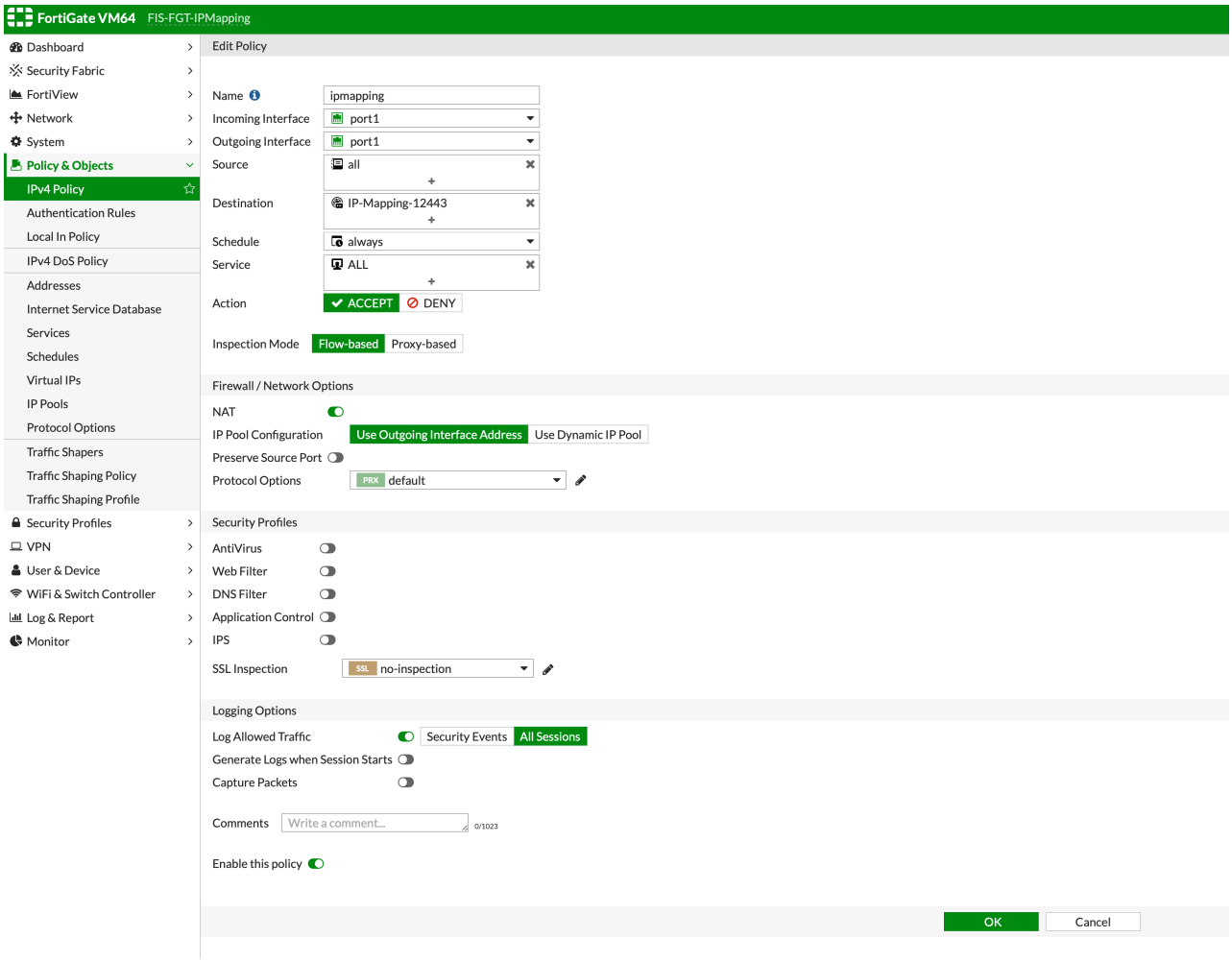



Settings of **ip-mapping-443**:




3. Go to *Policy & Objects* > *IPv4 Policy* > *Create New*.

4. Create an IPv4 policy that includes the virtual IP (443) that you created.




## Client system configuration

Complete the following steps on the client system (for example, Windows 10).

1. In Windows 10, launch CMD as administrator.
2. Use the following commands to add the FortiGate IP address to the routing table on the client system:
   a. At the command prompt, type

   ```
   route -p ADD <external_IP_address> Mask 255.255.255.255 <FGT_IP_address>
   ```

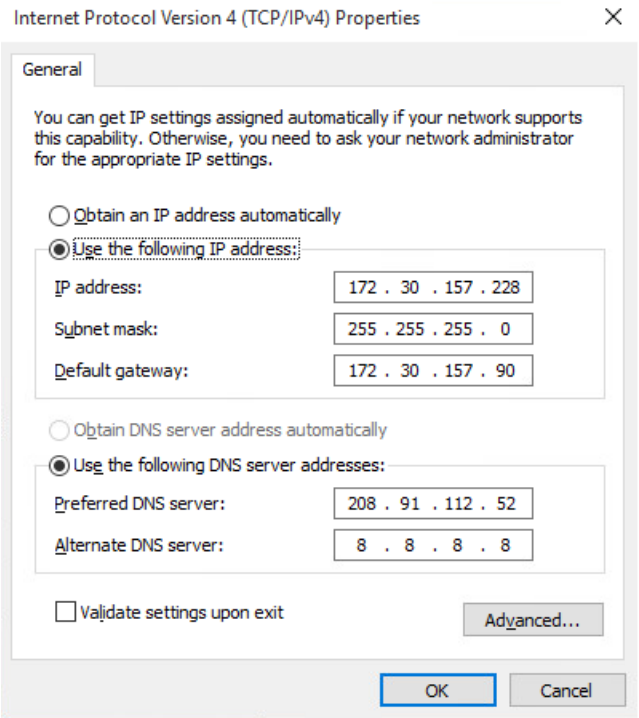
   For example,

   ```
   route -p ADD 172.30.147.207 MASK 255.255.255.255 172.30.157.90
   ```

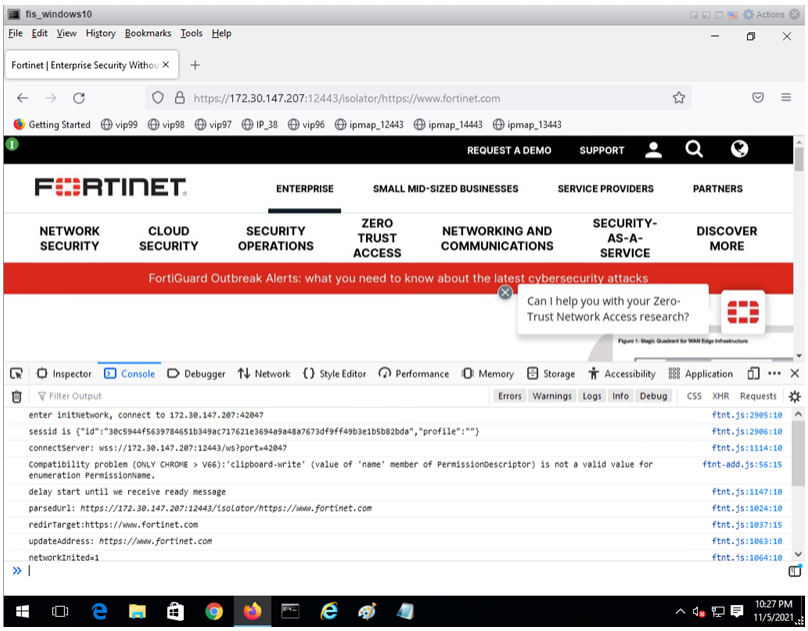
**b.** To confirm the setup, type `route print`.

```
Interface List
  5...00 0c 29 be 3a da ......Intel(R) 82574L Gigabit Network Connection #2
  7...00 0c 29 be 3a d0 ......Intel(R) PRO/1000 MT Network Connection
  1...........................Software Loopback Interface 1
  9...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter
  6...00 00 00 00 00 00 00 e0 Microsoft Teredo Tunneling Adapter
  4...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #2
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0    172.30.157.90   172.30.157.228    266
          0.0.0.0          0.0.0.0    172.30.156.90   172.30.156.227    266
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    306
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    306
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    306
   172.30.147.206  255.255.255.255    172.30.157.90   172.30.157.228     11
   172.30.147.207  255.255.255.255    172.30.157.90   172.30.157.228     11
    172.30.156.0    255.255.255.0         On-link    172.30.156.227    266
   172.30.156.227  255.255.255.255         On-link    172.30.156.227    266
   172.30.156.255  255.255.255.255         On-link    172.30.156.227    266
    172.30.157.0    255.255.255.0         On-link    172.30.157.228    266
   172.30.157.228  255.255.255.255         On-link    172.30.157.228    266
   172.30.157.255  255.255.255.255         On-link    172.30.157.228    266
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    306
        224.0.0.0        240.0.0.0         On-link    172.30.157.228    266
        224.0.0.0        240.0.0.0         On-link    172.30.156.227    266
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    306
  255.255.255.255  255.255.255.255         On-link    172.30.157.228    266
  255.255.255.255  255.255.255.255         On-link    172.30.156.227    266
===========================================================================
Persistent Routes:
  Network Address          Netmask  Gateway Address  Metric
   172.30.147.206  255.255.255.255    172.30.157.90       1
   172.30.147.207  255.255.255.255    172.30.157.90       1
          0.0.0.0          0.0.0.0    172.30.157.90  Default
          0.0.0.0          0.0.0.0    172.30.157.90  Default
          0.0.0.0          0.0.0.0    172.30.156.90  Default
===========================================================================

C:\Users\admin.FORTIENT>
```

3. Check the Client IPv4 setting. Make sure default gateway is the FortiGate IP.




4. Configure your browser by following the steps in IP Forwarding mode on page 89, depending on your browser type.
5. Verify that it works by browsing to the following address:
   `https://<external_IP_address>:<port_map_to_443>/isolator/https://www.fortinet.com`
   e.g.:
   `https://172.30.147.207:12443/isolator/https://www.fortinet.com`



# Configuring IP mapping in HA mode

**Prerequisites:**

Please follow High Availability to make sure native HA mode works before configuring IP Mapping in HA mode.

Configuring IP Mapping in HA mode includes the following steps:

1. FortiIsolator configuration
2. FortiGate configuration
3. Client system configuration

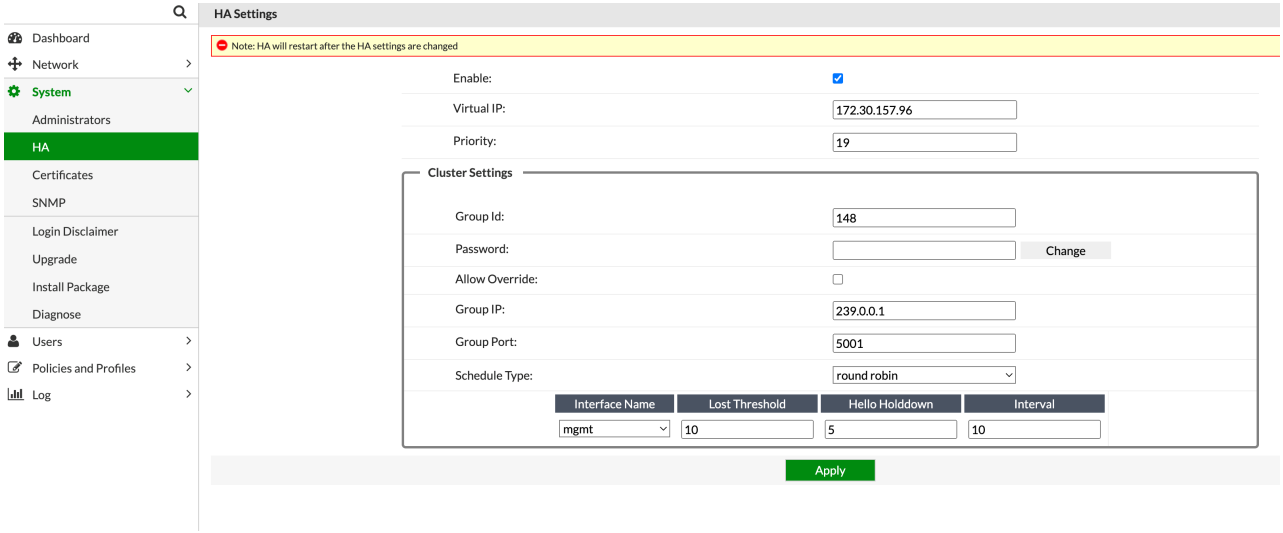
## Single-node setting (one-primary only)

### To configure IP mapping of FortiIsolator in HA mode with one single primary node:

1. Configure port forwarding mappings using the following commands in the FortiIsolator CLI:
   - `set fis-ipmap <port_map_to_443> <external_IP_address>`
     For example, `set fis-ipmap 12443 172.30.147.207`
   - `set fis-ipmap-vip <external IP> <vip_port_map_to_443>`
     For example, `set fis-ipmap-vip 172.30.147.207 14443`
   - `set fis-ipmap-ha <priority> <external_IP_address> <internal_IP_address:primary> <port_map_to_443>`
     For example, `set fis-ipmap-ha 19 172.30.147.207 172.30.157.148 12443`

```
**********Configured parameters**********

[IP Address]
      INTERFACE                IPv4                      MAC
--------------------    --------------------    --------------------
            internal    172.30.157.148/24       00:0C:29:63:17:33
                mgmt    172.30.156.148/24       00:0C:29:63:17:47

[Routing Entries]
         SUBNET              GATEWAY               INTERFACE
--------------------    --------------------    --------------------
           0.0.0.0/0    172.30.157.254          internal

hostname                        : FISVM1TM21000288
dns server                      : 8.8.8.8
dns server                      : 208.91.112.52
build number                    : 0488(interim)
date time                       : 2022-06-15 10:37:02 PDT

[SNMP Configurations]
Agent Listening Interface       : mgmt
Agent Community                 : fis_public
Trap Host-IP                    :
Trap Host Community             :
Session Threashold(%)           : 70
SNMP V3 User Status             : Disabled
SNMP V3 Username                : fis_user
V3 Query Port Status            : Disabled
V3 Query Port Num               : 0
V3 Trap Port Status             : Disabled
V3 Trap Local Port Num          : 162
V3 Trap Remote Port Num         : 162
SNMP V3 Hosts:
Security Level                  : noauth
Authentication Status           : Disabled
Authentication Method           :
Authentication Password         :
Private Status                  : Disabled
Encrypt Method                  :
Encrypt Password                :
SNMP V3 Trap Events:
       check_session_threshold:  Disabled
       send_mgmt_ip_off_days:  Disabled

ip mapping                      : 172.30.147.207
mapping for port 443            : 12443
ip mapping (VIP)                : 172.30.147.207
mapping for port 443 (VIP)      : 14443
[IPMAP HA Settings]
priority        IP      IP mapping      Port 443
19      172.30.157.148  172.30.147.207  12443
```

2. Make sure HA is Enabled in Fortilsolator.



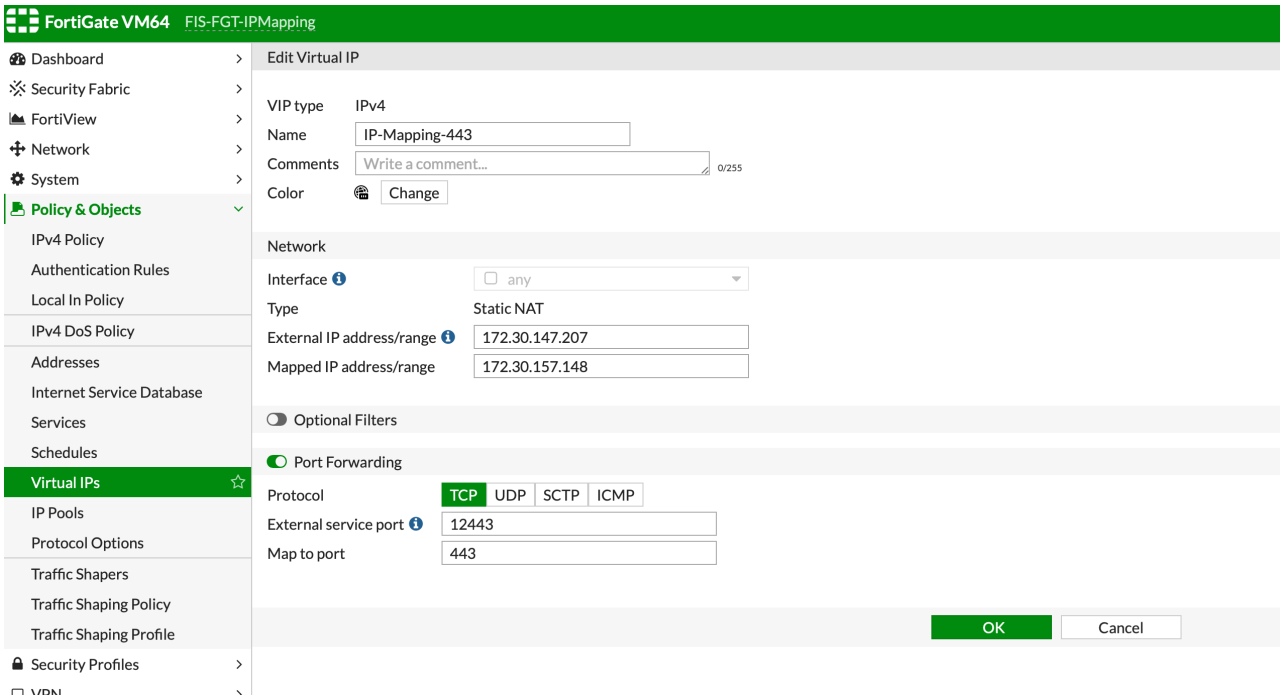

## FortiGate configuration

Complete the following steps in the FortiGate UI.

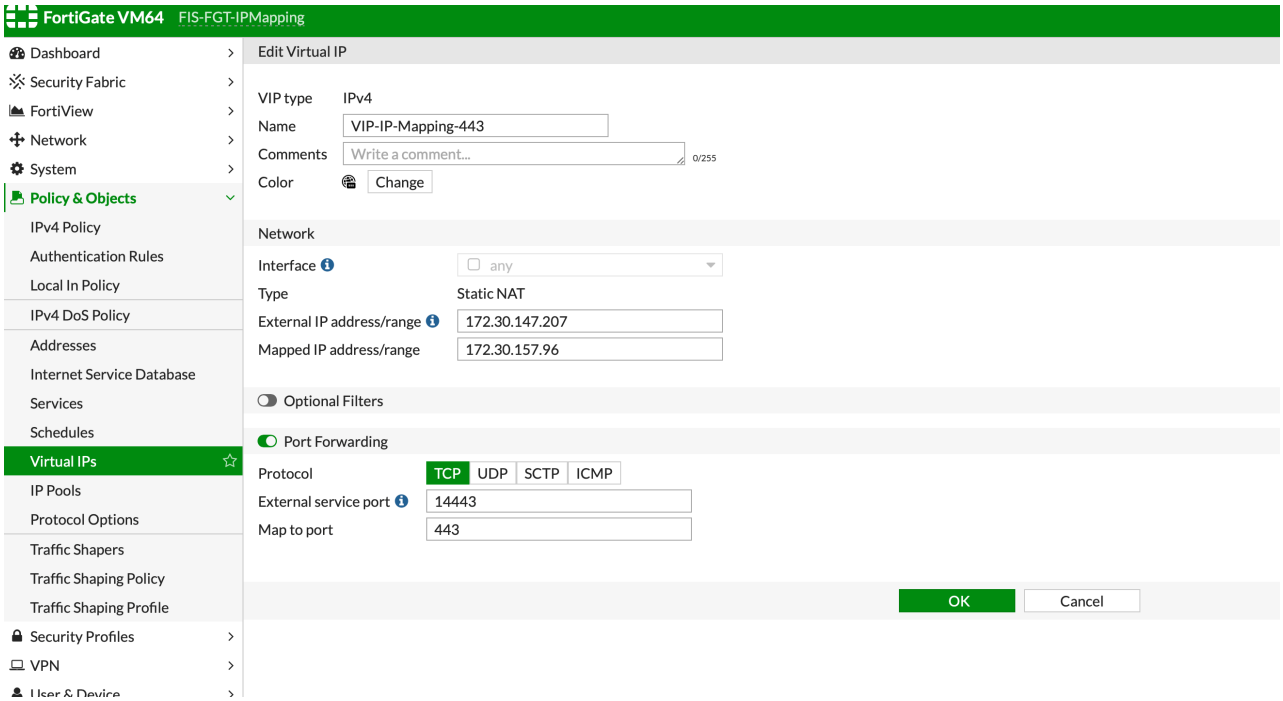
1. Go to *Policy & Objects* > *Virtual IPs*.
2. Create an IPv4 virtual IP with the following information:
   - **IP-Mapping-HA-443**: external_IP_address **->** FIS_IP (TCP: 12443 > 443)
     For example, 172.30.147.207 **->** 172.30.157.96 (TCP: 12443 > 443).

In this example, we are using:
- External_IP_address: 172.30.147.207
- FIS HA Virtual IP: 172.30.157.96
- FIS_IP: 172.30.157.148

Settings of **IP-Mapping-443**:

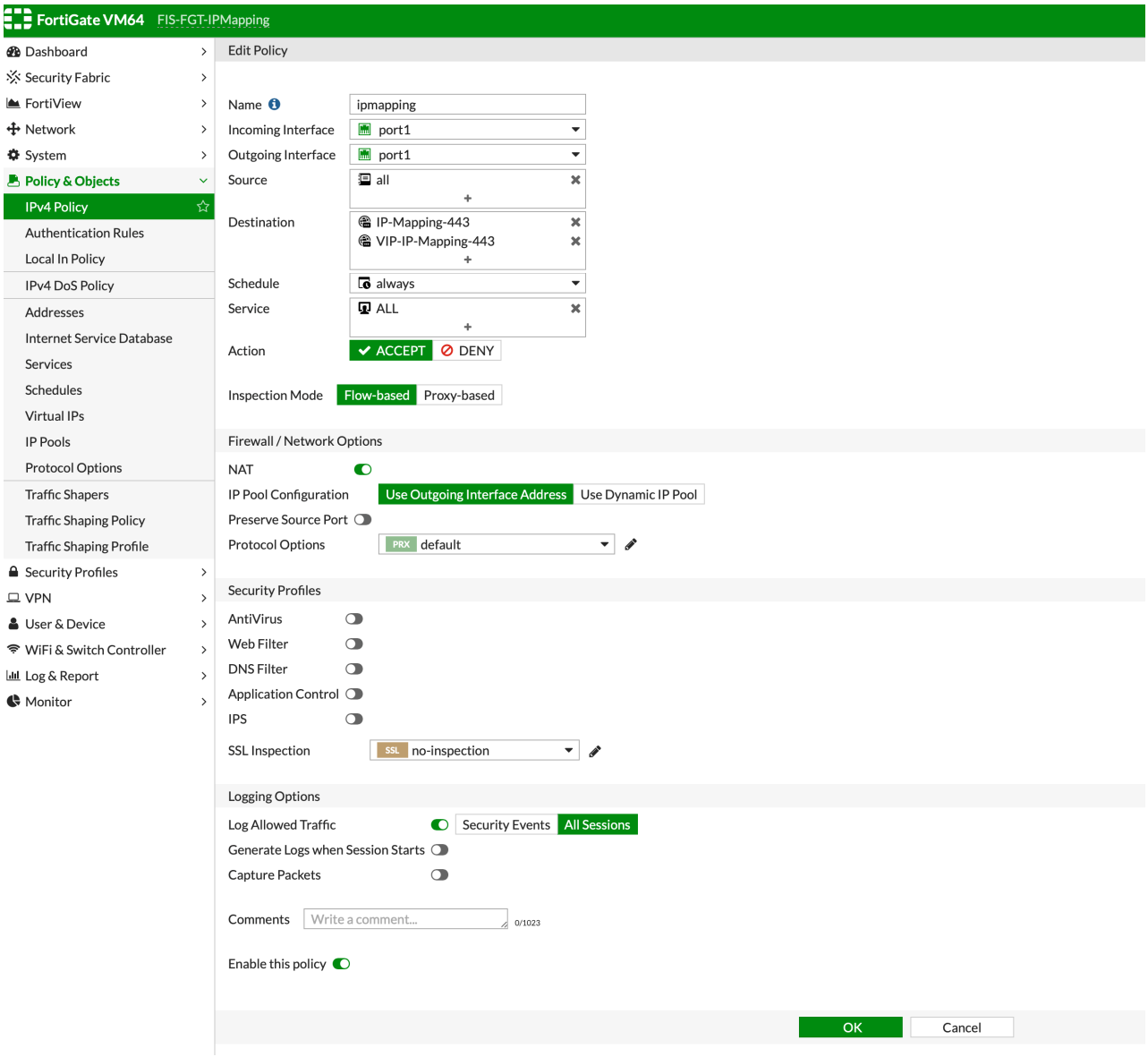



Settings of **IP-Mapping-HA-443**:




3. Go to *Policy & Objects* > *IPv4 Policy* > *Create New*.

4. Create an IPv4 policy that includes the virtual IP that you created.




## Client system configuration

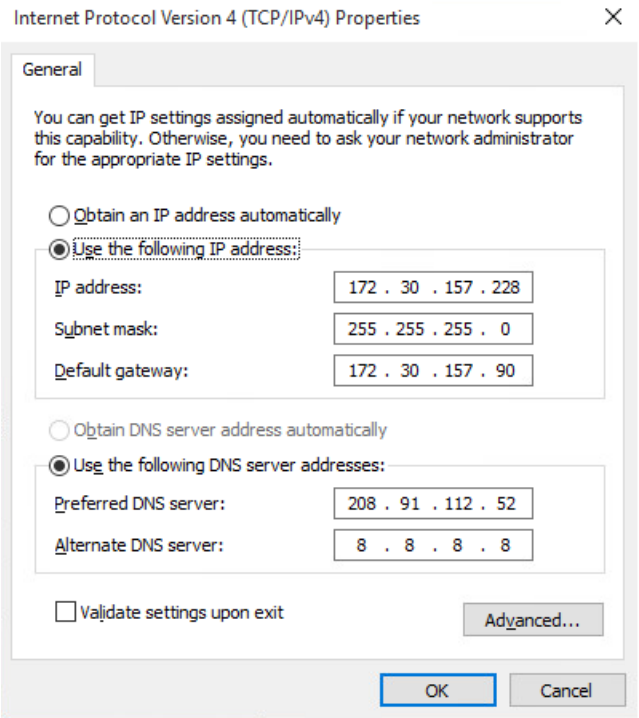
Complete the following steps on the client system (for example, Windows 10).

1. In Windows 10, launch CMD as administrator.
2. Use the following commands to add the FortiGate IP address to the routing table on the client system:
   a. At the command prompt, type `route -p ADD <external_IP_address> Mask 255.255.255.255 <FGT_IP_address>`.
   For example, `route -p ADD 172.30.147.207 MASK 255.255.255.255 172.30.157.90`

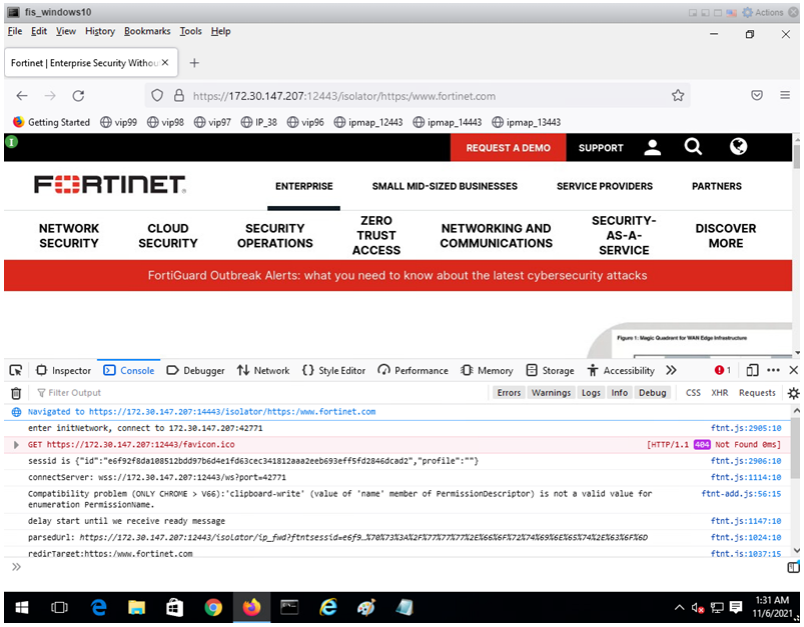
**b.** To confirm the setup, type `route print`.

```
Interface List
  5...00 0c 29 be 3a da ......Intel(R) 82574L Gigabit Network Connection #2
  7...00 0c 29 be 3a d0 ......Intel(R) PRO/1000 MT Network Connection
  1...........................Software Loopback Interface 1
  9...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter
  6...00 00 00 00 00 00 00 e0 Microsoft Teredo Tunneling Adapter
  4...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #2
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0    172.30.157.90   172.30.157.228    266
          0.0.0.0          0.0.0.0    172.30.156.90   172.30.156.227    266
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    306
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    306
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    306
   172.30.147.206  255.255.255.255    172.30.157.90   172.30.157.228     11
   172.30.147.207  255.255.255.255    172.30.157.90   172.30.157.228     11
     172.30.156.0    255.255.255.0         On-link    172.30.156.227    266
   172.30.156.227  255.255.255.255         On-link    172.30.156.227    266
   172.30.156.255  255.255.255.255         On-link    172.30.156.227    266
     172.30.157.0    255.255.255.0         On-link    172.30.157.228    266
   172.30.157.228  255.255.255.255         On-link    172.30.157.228    266
   172.30.157.255  255.255.255.255         On-link    172.30.157.228    266
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    306
        224.0.0.0        240.0.0.0         On-link    172.30.157.228    266
        224.0.0.0        240.0.0.0         On-link    172.30.156.227    266
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    306
  255.255.255.255  255.255.255.255         On-link    172.30.157.228    266
  255.255.255.255  255.255.255.255         On-link    172.30.156.227    266
===========================================================================
Persistent Routes:
  Network Address          Netmask  Gateway Address  Metric
   172.30.147.206  255.255.255.255    172.30.157.90       1
   172.30.147.207  255.255.255.255    172.30.157.90       1
          0.0.0.0          0.0.0.0    172.30.157.90  Default
          0.0.0.0          0.0.0.0    172.30.157.90  Default
          0.0.0.0          0.0.0.0    172.30.156.90  Default
===========================================================================

C:\Users\admin.FORTIENT>
```

3. Check the Client IPv4 setting. Make sure default gateway is the FortiGate IP.




4. Configure your browser by following the steps in IP Forwarding mode on page 89, depending on your browser type.
5. Verify that it works by browsing to the following address:
   `https://<external_IP_address>:<port_map_to_HA_443>/isolator/https://www.fortinet.com`
   e.g.:
   `https://172.30.147.207:14443/isolator/https://www.fortinet.com`
   (It will now redirect to: `https://172.30.147.207:12443/isolator/https://www.fortinet.com`)



## Multiple-nodes setting (one-primary-one-secondary)

### To configure IP mapping of FortiIsolator in HA mode with one primary node and one secondary node:

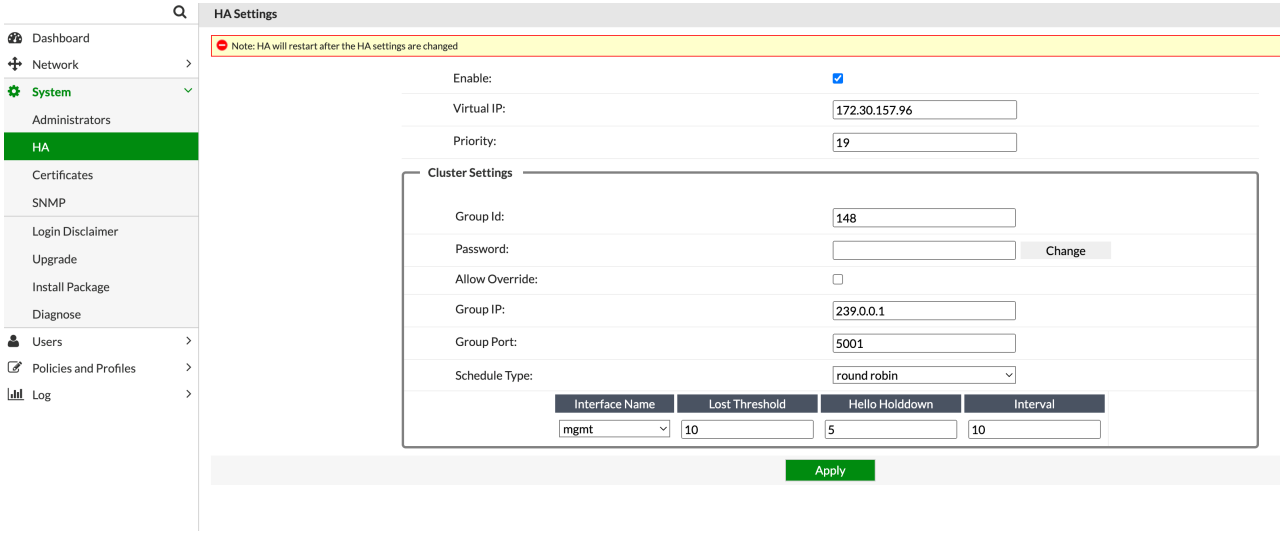
1. In the primary node, configure port forwarding mappings using the following commands in the FortiIsolator CLI:
   - `set fis-ipmap <port_map_to_443> <external_IP_address>`
     For example, `set fis-ipmap 12443 172.30.147.207`
   - `set fis-ipmap-vip <external IP> <vip_port_map_to_443>`
     For example, `set fis-ipmap-vip 172.30.147.207 14443`
   - `set fis-ipmap-ha <priority> <external_IP_address> <internal_IP_address:primary> <port_map_to_443>`
     For example, `set fis-ipmap-ha 19 172.30.147.207 172.30.157.148 12443`
   - `set fis-ipmap-ha <priority> <external_IP_address> <internal_IP_address:secondary1> <port_map_to_443>`
     For example, `set fis-ipmap-ha 20 172.30.147.207 172.30.157.149 13443`

```
**********Configured parameters**********

[IP Address]
      INTERFACE                IPv4                    MAC
--------------------    --------------------    --------------------
            internal    172.30.157.148/24       00:0C:29:63:17:33
                mgmt    172.30.156.148/24       00:0C:29:63:17:47

[Routing Entries]
         SUBNET              GATEWAY               INTERFACE
--------------------    --------------------    --------------------
           0.0.0.0/0    172.30.157.254          internal

hostname                      : FISVM1TM21000288
dns server                    : 8.8.8.8
dns server                    : 208.91.112.52
build number                  : 0488(interim)
date time                     : 2022-06-15 13:00:31 PDT

[SNMP Configurations]
Agent Listening Interface     : mgmt
Agent Community               : fis_public
Trap Host-IP                  :
Trap Host Community           :
Session Threashold(%)         : 70
SNMP V3 User Status           : Disabled
SNMP V3 Username              : fis_user
V3 Query Port Status          : Disabled
V3 Query Port Num             : 0
V3 Trap Port Status           : Disabled
V3 Trap Local Port Num        : 162
V3 Trap Remote Port Num       : 162
SNMP V3 Hosts:
Security Level                : noauth
Authentication Status         : Disabled
Authentication Method         :
Authentication Password       :
Private Status                : Disabled
Encrypt Method                :
Encrypt Password              :
SNMP V3 Trap Events:
       check_session_threshold:  Disabled
       send_mgmt_ip_off_days:  Disabled

ip mapping                    : 172.30.147.207
mapping for port 443          : 12443
ip mapping (VIP)              : 172.30.147.207
mapping for port 443 (VIP)    : 14443
[IPMAP HA Settings]
priority        IP      IP mapping      Port 443
19      172.30.157.148  172.30.147.207  12443
20      172.30.157.149  172.30.147.207  13443
```

2. In the secondary node, configure port forwarding mappings using the following commands in the FortiIsolator CLI:
   - `set fis-ipmap <port_map_to_443> <external_IP_address>`
     For example, `set fis-ipmap 13443 172.30.147.207`

```
**********Configured parameters**********

[IP Address]
      INTERFACE                IPv4                    MAC
--------------------    --------------------    --------------------
           internal    172.30.157.149/22       00:0C:29:D7:AD:26
               mgmt    172.30.156.149/24       00:0C:29:D7:AD:3A

[Routing Entries]
         SUBNET              GATEWAY               INTERFACE
--------------------    --------------------    --------------------
          0.0.0.0/0    172.30.157.254          internal

hostname                      : FISVM1TM21000289
dns server                    : 8.8.8.8
dns server                    : 208.91.112.52
build number                  : 0488(interim)
date time                     : 2022-06-15 12:59:26 PDT

[SNMP Configurations]
Agent Listening Interface     : mgmt
Agent Community               : fis_public
Trap Host-IP                  :
Trap Host Community           :
Session Threashold(%)         : 70
SNMP V3 User Status           : Disabled
SNMP V3 Username              : fis_user
V3 Query Port Status          : Disabled
V3 Query Port Num             : 0
V3 Trap Port Status           : Disabled
V3 Trap Local Port Num        : 162
V3 Trap Remote Port Num       : 162
SNMP V3 Hosts:
Security Level                : noauth
Authentication Status         : Disabled
Authentication Method         :
Authentication Password       :
Private Status                : Disabled
Encrypt Method                :
Encrypt Password              :
SNMP V3 Trap Events:
       check_session_threshold:  Disabled
       send_mgmt_ip_off_days:  Disabled

ip mapping                    : 172.30.147.207
mapping for port 443          : 13443
```

3. Make sure the primary and secondary nodes have different HA priority but the same group id.




Below is a summary of the example:

- **Primary:** `172.30.156.148`
  - `set fis-ipmap 12443 172.30.147.207`
  - `set fis-ipmap-vip 172.30.147.207 14443`
  - `set fis-ipmap-ha 19 172.30.147.207 172.30.157.148 12443`
  - `set fis-ipmap-ha 20 172.30.147.207 172.30.157.149 13443`
- **Secondary:** `172.30.156.149`
  - `set fis-ipmap 13443 172.30.147.207`

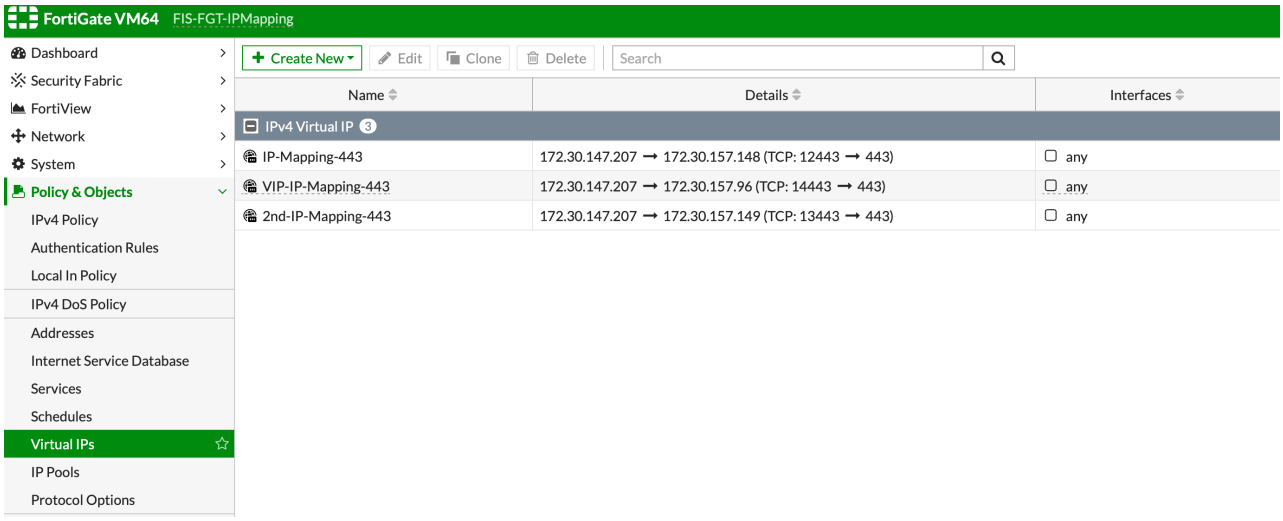
## FortiGate configuration

Complete the following steps in the FortiGate UI.

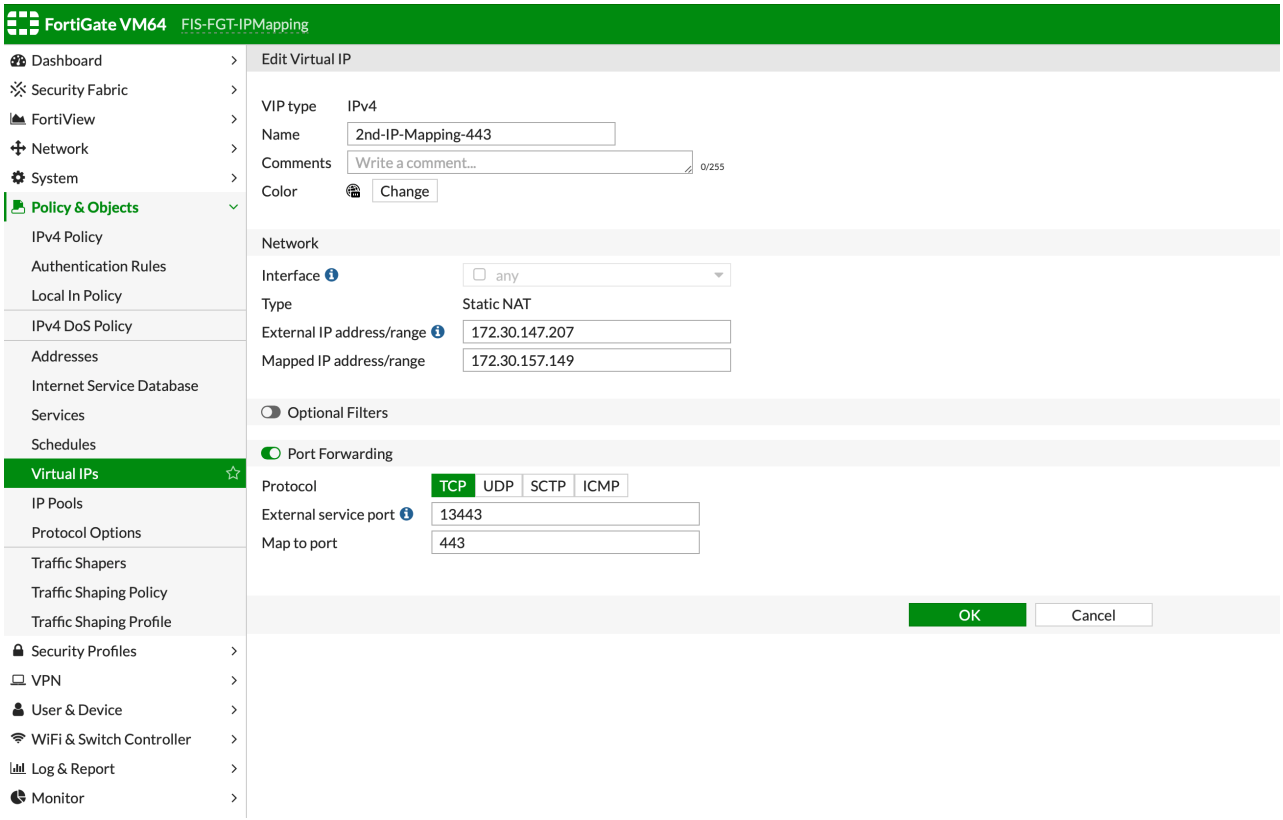
1. Go to *Policy & Objects* > *Virtual IPs*.
2. Create an IPv4 virtual IP for the secondary node with the following information:
   - **IP-Mapping-HA-443**: <external_IP_address> -> FIS_IP (TCP: 14443 > 443)
     For example, 172.30.147.207 -> 172.30.157.96 (TCP: 14443 > 443)

This example uses the following:

- External_IP_address: 172.30.147.207
- FIS HA Virtual IP: 172.30.157.96
- FIS_IP_Primary: 172.30.157.148
- FIS_IP_Secondary: 172.30.157.149

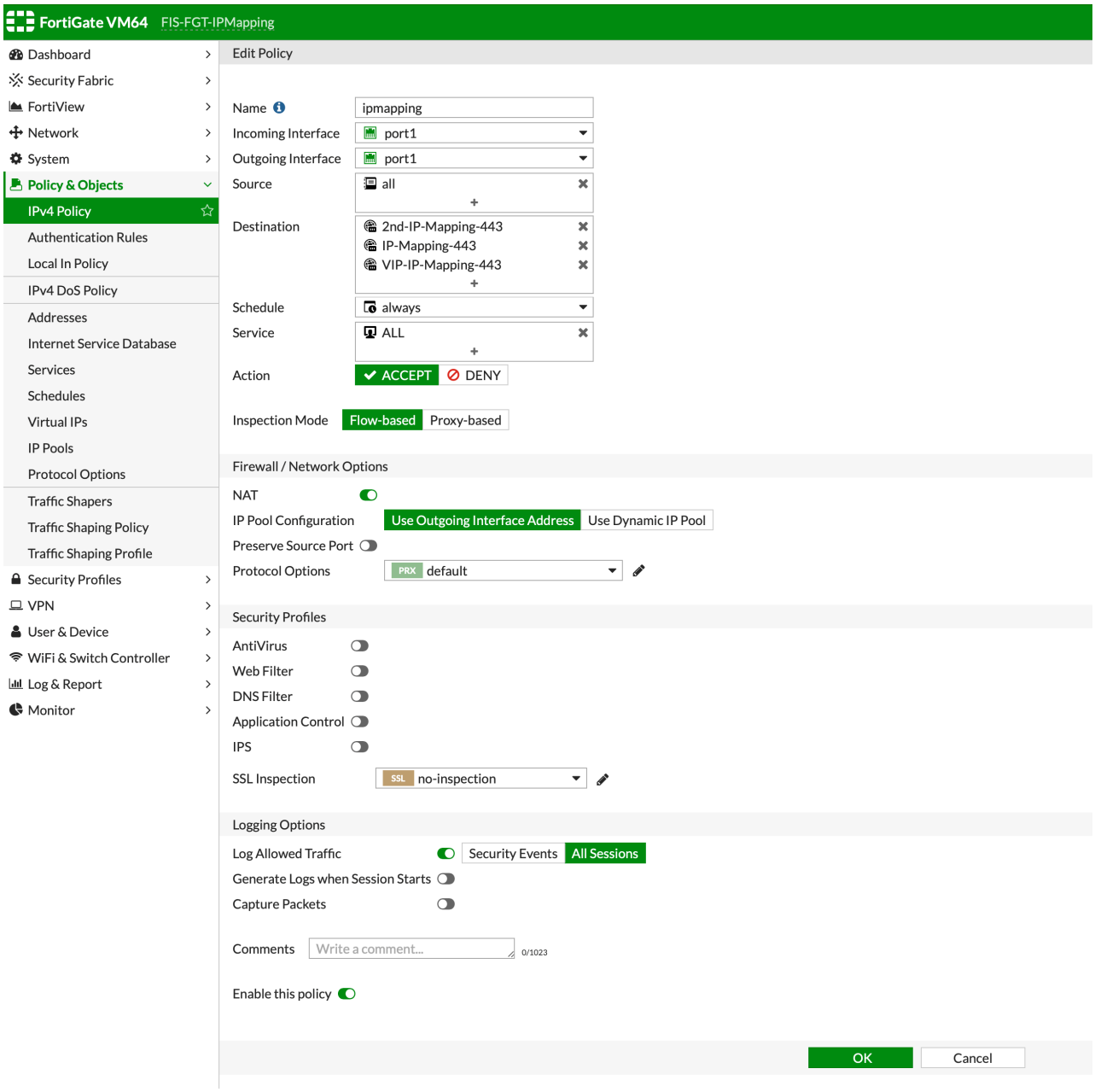



Settings of second **ip-mapping-443**:




3. Go to *Policy & Objects* > *IPv4 Policy* > *Create New*.

4. Create an IPv4 policy that includes the virtual IP that you created.




## Client system configuration

Complete the following steps on the client system (for example, Windows 10).

1. In Windows 10, launch CMD as administrator.
2. Use the following commands to add the FortiGate IP address to the routing table on the client system:
   - At the command prompt, type

     ```
     route -p ADD <external_IP_address> Mask 255.255.255.255 <FGT_IP_address>
     ```

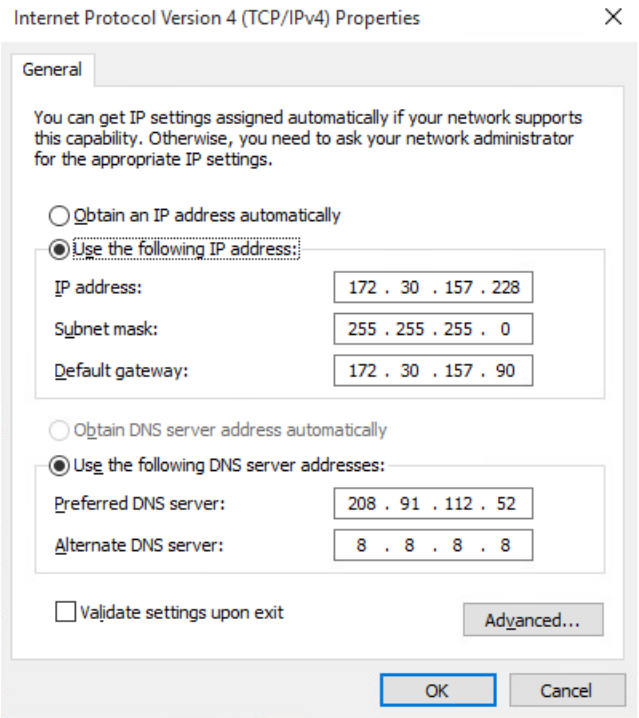
     For example,

     ```
     route -p ADD 172.30.147.207 MASK 255.255.255.255 172.30.157.90
     ```

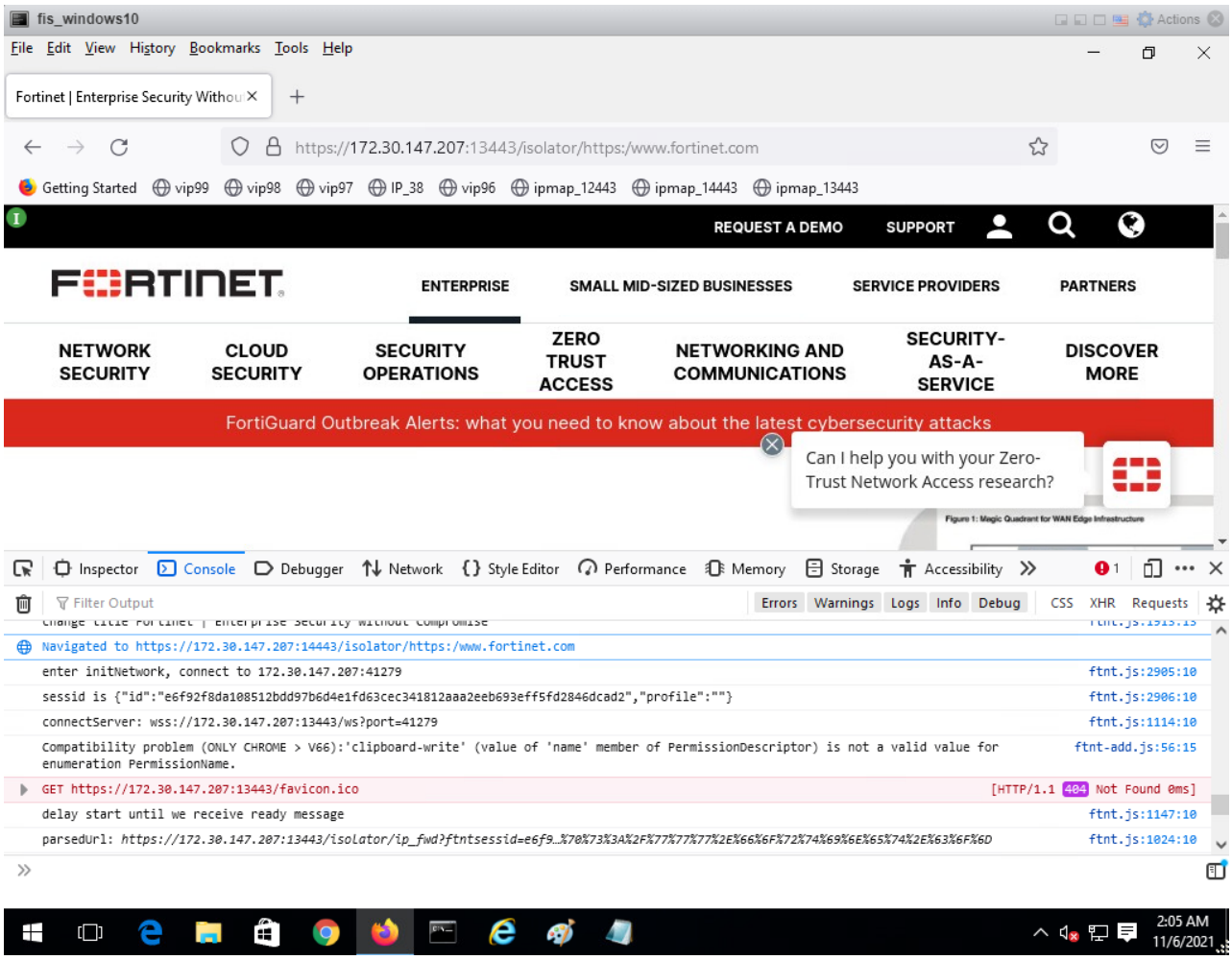
- To confirm the setup, type `route print`.

```
Interface List
  5...00 0c 29 be 3a da ......Intel(R) 82574L Gigabit Network Connection #2
  7...00 0c 29 be 3a d0 ......Intel(R) PRO/1000 MT Network Connection
  1...........................Software Loopback Interface 1
  9...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter
  6...00 00 00 00 00 00 00 e0 Microsoft Teredo Tunneling Adapter
  4...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #2
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0    172.30.157.90   172.30.157.228    266
          0.0.0.0          0.0.0.0    172.30.156.90   172.30.156.227    266
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    306
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    306
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    306
   172.30.147.206  255.255.255.255    172.30.157.90   172.30.157.228     11
   172.30.147.207  255.255.255.255    172.30.157.90   172.30.157.228     11
     172.30.156.0    255.255.255.0         On-link    172.30.156.227    266
   172.30.156.227  255.255.255.255         On-link    172.30.156.227    266
   172.30.156.255  255.255.255.255         On-link    172.30.156.227    266
     172.30.157.0    255.255.255.0         On-link    172.30.157.228    266
   172.30.157.228  255.255.255.255         On-link    172.30.157.228    266
   172.30.157.255  255.255.255.255         On-link    172.30.157.228    266
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    306
        224.0.0.0        240.0.0.0         On-link    172.30.157.228    266
        224.0.0.0        240.0.0.0         On-link    172.30.156.227    266
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    306
  255.255.255.255  255.255.255.255         On-link    172.30.157.228    266
  255.255.255.255  255.255.255.255         On-link    172.30.156.227    266
===========================================================================
Persistent Routes:
  Network Address          Netmask  Gateway Address  Metric
   172.30.147.206  255.255.255.255    172.30.157.90       1
   172.30.147.207  255.255.255.255    172.30.157.90       1
          0.0.0.0          0.0.0.0    172.30.157.90  Default
          0.0.0.0          0.0.0.0    172.30.157.90  Default
          0.0.0.0          0.0.0.0    172.30.156.90  Default
===========================================================================

C:\Users\admin.FORTIENT>
```

3. Check the Client IPv4 setting. Make sure default gateway is the FortiGate IP.




4. Configure your browser by following the steps in IP Forwarding mode on page 89, depending on your browser type.
5. Verify that it works by browsing to the following address:
   `https://<external_IP_address>:<port_map_to_HA_443>/isolator/https://www.fortinet.com`
   e.g.:
   `https://172.30.147.207:14443/isolator/https://www.fortinet.com`
   The address will now redirect to the primary node:
   `https://172.30.147.207:12443/isolator/https://www.fortinet.com`
   or the secondary node:
   `https://172.30.147.207:13443/isolator/https://www.fortinet.com`


fis_windows10
File Edit View History Bookmarks Tools Help
Fortinet | Enterprise Security Without
https://172.30.147.207:13443/isolator/https:/www.fortinet.com
Getting Started vip99 vip98 vip97 IP_38 vip96 ipmap_12443 ipmap_14443 ipmap_13443
REQUEST A DEMO SUPPORT
FORTINET
ENTERPRISE SMALL MID-SIZED BUSINESSES SERVICE PROVIDERS PARTNERS
NETWORK SECURITY CLOUD SECURITY SECURITY OPERATIONS ZERO TRUST ACCESS NETWORKING AND COMMUNICATIONS SECURITY-AS-A-SERVICE DISCOVER MORE
FortiGuard Outbreak Alerts: what you need to know about the latest cybersecurity attacks
Can I help you with your Zero-Trust Network Access research?
Inspector Console Debugger Network Style Editor Performance Memory Storage Accessibility
Filter Output
Errors Warnings Logs Info Debug CSS XHR Requests
Navigated to https://172.30.147.207:14443/isolator/https:/www.fortinet.com
enter initNetwork, connect to 172.30.147.207:41279 ftnt.js:2905:10
sessid is {"id":"e6f92f8da108512bdd97b6d4e1fd63cec341812aaa2eeb693eff5fd2846dcad2","profile":""} ftnt.js:2906:10
connectServer: wss://172.30.147.207:13443/ws?port=41279 ftnt.js:1114:10
Compatibility problem (ONLY CHROME > V66):'clipboard-write' (value of 'name' member of PermissionDescriptor) is not a valid value for enumeration PermissionName. ftnt-add.js:56:15
GET https://172.30.147.207:13443/favicon.ico [HTTP/1.1 404 Not Found 0ms]
delay start until we receive ready message ftnt.js:1147:10
parsedUrl: https://172.30.147.207:13443/isolator/ip_fwd?ftntsessid=e6f9…%70%73%3A%2F%77%77%77%2E%66%6F%72%74%69%6E%65%74%2E%63%6F%6D ftnt.js:1024:10
2:05 AM
11/6/2021

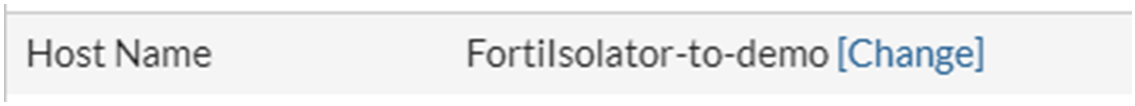
# Dashboard

The FortiIsolator dashboard allows you to see information at one glance, including System Information, System Resources, and so on. You can also reboot and shut down the system from the dashboard, as well as check your licenses.

## Changing host name

To change the *Host Name* from GUI:

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




To change *Host Name* from CLI:

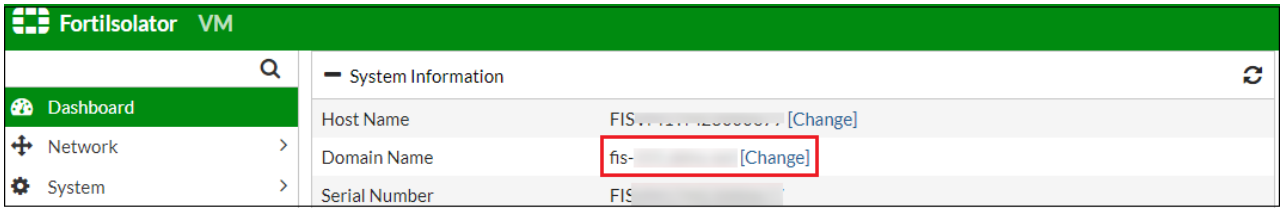
```
> set hostname <new_hostname>
e.g.
> set hostname FortiIsolator-to-demo
```

The host name can start with English characters or 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.

## Changing domain name

To change the *Domain Name* from GUI:

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




3. Specify the new domain name and click *Apply* to save the changes.
   Domain names are not case-sensitive. Make sure the domain name meets the following requirements:

- No spaces and or special characters (such as !, $, &, _)
- Cannot end with `.gov.in`
- Length must be between 3 and 63 characters (excluding extension)

# 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
```

# 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 backup 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 backup the configuration:

1. From the administration portal, click *Dashboard*, and find the *System Configuration* widget.
2. In the *System Configuration* field, click *Backup/Restore*, it navigates to *System Recovery* page.
3. In *System Recovery* page, under *Backup* section, *Click here* to save your backup file.
   - This will save the `backup.tgz` file into your local system; you can store it in a secure place for when you need to restore the system.

## Restoring a configuration

### To restore the FortiIsolator configuration:

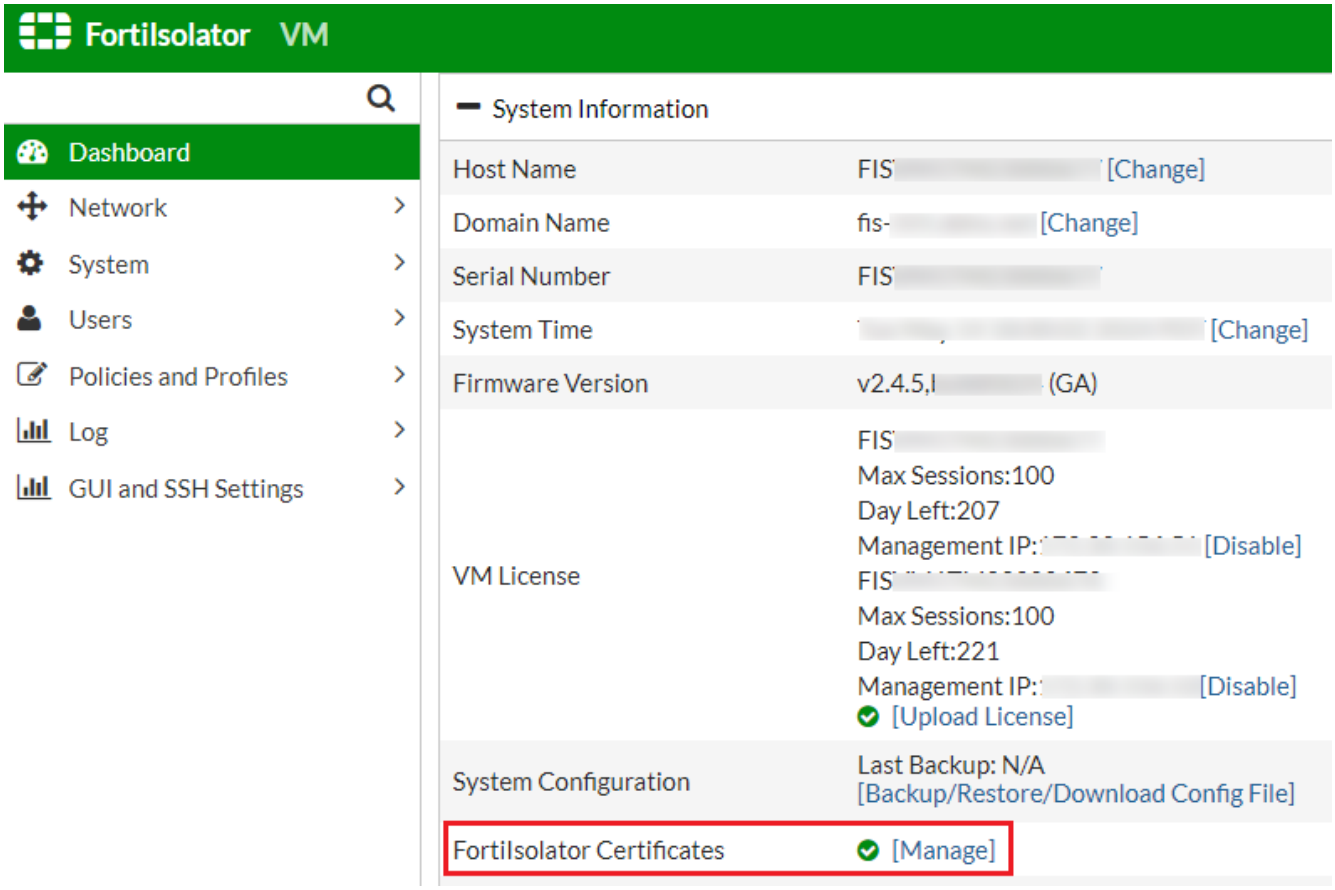
1. From the administration portal, click *Dashboard*, and find the *System Configuration* widget.
2. In the *System Configuration* field, click *Backup/Restore*, it navigates to *System Recovery* page.
3. In *System Recovery* page, under *Restore* section, *Choose File* to locate the configuration file.
   - The source of the configuration file to be restored: your Local PC or a USB Disk.
4. Click *Restore*, *OK* on the pop-up to confirm.
   - This will restore the configuration file and reboot the FortiIsolator. It takes few minutes.

# FortiIsolator certificates

The FortiIsolator CA certificate is required for access to the FortiIsolator from the browser. The CA certificate then auto-generates a matching server certificate for accessing the FortiIsolator database and a matching management certificate for accessing the FortiIsolator GUI. By default, the built-in FortiIsolator CA certificate is used. You can also generate or upload a custom CA certificate to meet your needs. However, you can revert to the default CA certificate anytime. For custom CA certificates, you can also upload a custom server or management certificate that is a match of the custom CA certificate.

The FortiIsolator 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.

You can manage the FortiIsolator CA certificate and the associated server and management certificates in the *Dashboard* of the administration portal by clicking the *Manage* link near *FortiIsolator Certificates* in the *System Information* widget.




**To revert to the default CA certificate and the matching server and management certificates:**

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

**To back up the current CA certificate or the matching server or management certificates:**

1. In the *Backup CA certificate* section, depending on the certificate you want to back up, click the link in one of the following:
   - *Click here to save CA certificate*
   - *Click here to save Isolator Server certificate*
   - *Click here to save Management Server certificate*

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

**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).
   Only “Base-64 encoded X.509 (`.cer`)” format certificates are supported.
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. Only “Base-64 encoded X.509 (`.cer`)” format certificates are supported.
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. Only “Base-64 encoded X.509 (`.cer`)” format certificates are supported.
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.

For information about other certificate types, such as self-signed SSL certificates for a specific server or website or certificates used between FortiIsolator and FortiProxy or SAML servers, see Certificates on page 51.

# Network

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`.

Use the FortiIsolator GUI or CLI to set the permanent IP address configuration.

You can perform the initial configuration using the serial console. For more information, see the FortiIsolator 1000F QuickStart Guide.

## 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 Portal > Network > Interface.
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 *Portal* > *Network* > *Interface*.
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 *Portal* > *Network* > *Interface*.
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 *Portal* > *Network* > *Interface*.
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.

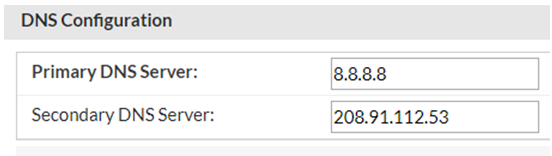
To change the HA IP address from CLI, use the following command:

```
> 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 *Portal* > *Network* > *System DNS*.
2. Fill out *Primary DNS Server* and *Secondary DNS Server*:




### 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

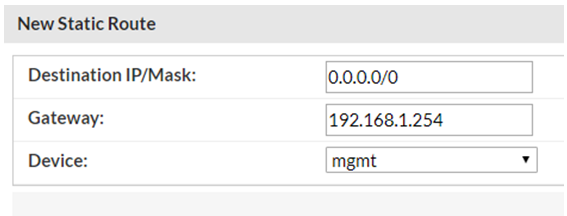
### To delete a static route:

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.



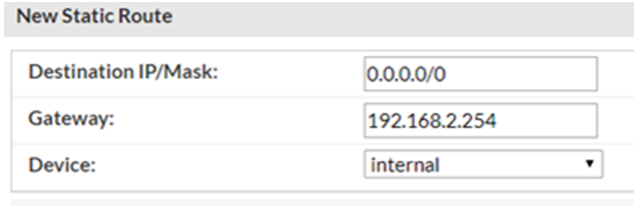
### To set up system routing for management IP from CLI:

```
> 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.

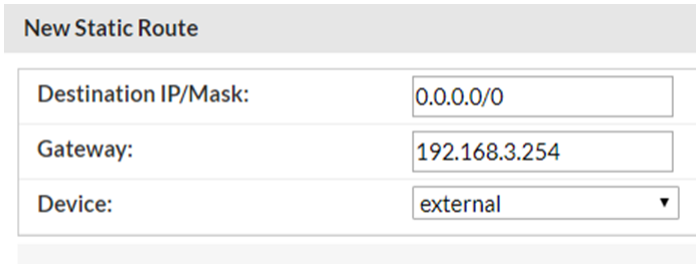



### To set up system routing for internal IP from CLI:

```
> 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.



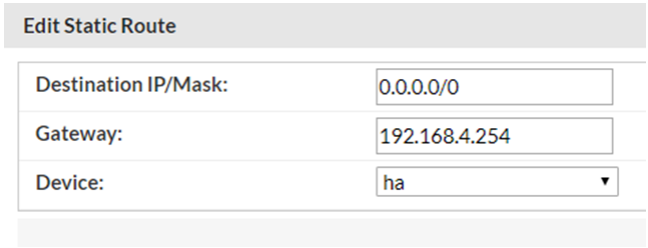

### To set up system routing for external IP from CLI:

```
> 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.




### 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.

# Forwarding server

This feature provides a method for identifying the original IP address of a client browser connecting to the FortiIsolator server.

If X-Forward is enabled, the HTTP request header shows the information of the original IP address of the client browser. If X-Forward is disabled, the HTTP request header does not show the information.

## Configuring forwarding server from GUI

**To configure forwarding server from GUI:**

1. Go to *Network* > *Forwarding Server*.
2. Enable *X-forward*.
3. Set *Proxy Type* to *Manual Proxy Configuration*.
4. Set the http/https proxy ip/port of the manual proxy.
5. Set the bypass list
6. Click *OK*.

## Configuring forwarding server from CLI

### To configure forwarding server from CLI:

```
> set proxy-http-xforwarded 1
> set proxy-mode 1
> set proxy-server <protocol> <ip-address> <port>
(e.g. set proxy-server http 12.34.56.78 8080)
> set proxy-server <protocol> <ip-address> <port>
(e.g. set proxy-server https 12.34.56.78 8080)
```

# System

The *System* section of FortiIsolator covers the following:



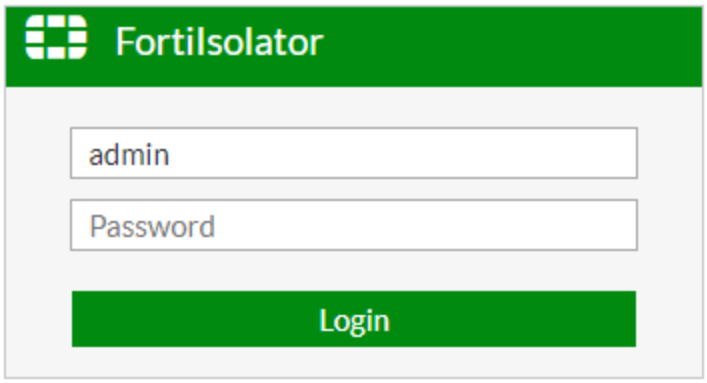
# Administrators

## Accessing the FortiIsolator administration portal

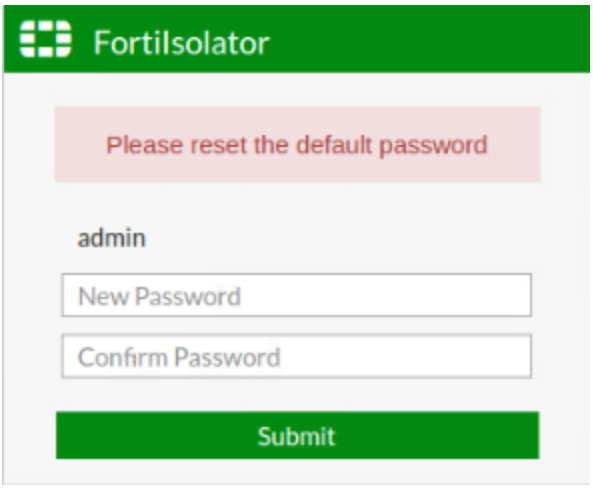
### Logging in as administrator

#### 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. For FortiIsolator appliances, ensure you have physical access to the FortiIsolator with a serial number and a console cable. For FortiIsolator VMs, ensure you have the 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. For FortiIsolator appliances, ensure you have physical access to the FortiIsolator with a serial number and a console cable. For FortiIsolator VMs, ensure you have the 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.

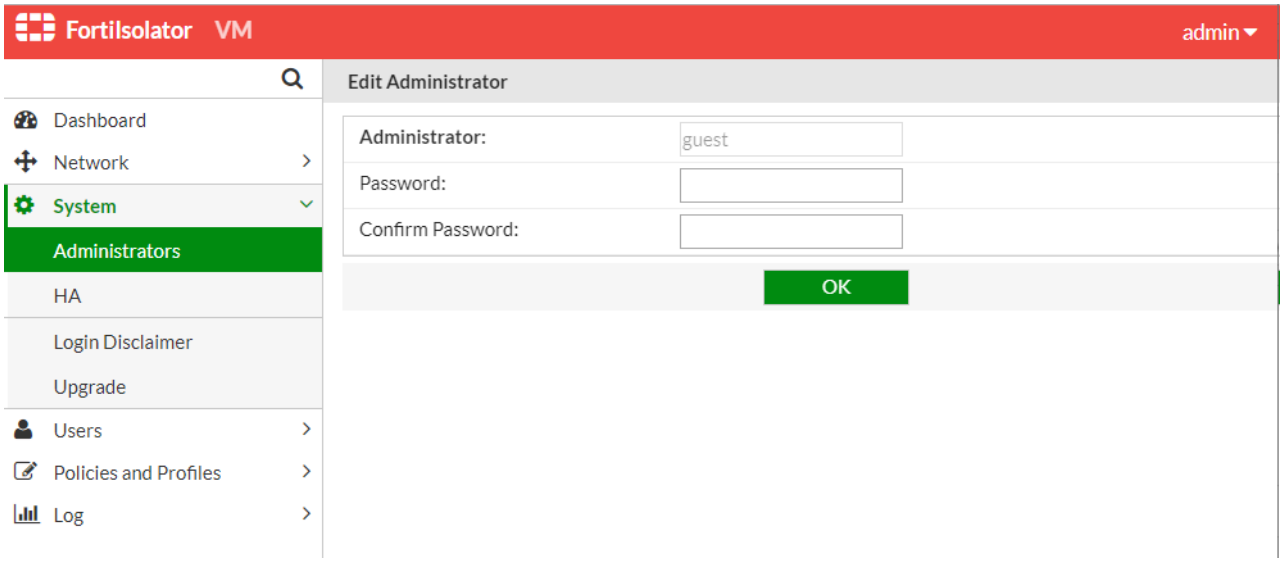
3. Reset the administrator password using the `admin-pwd-reset` command.
4. Reboot the FortiIsolator.

## 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.



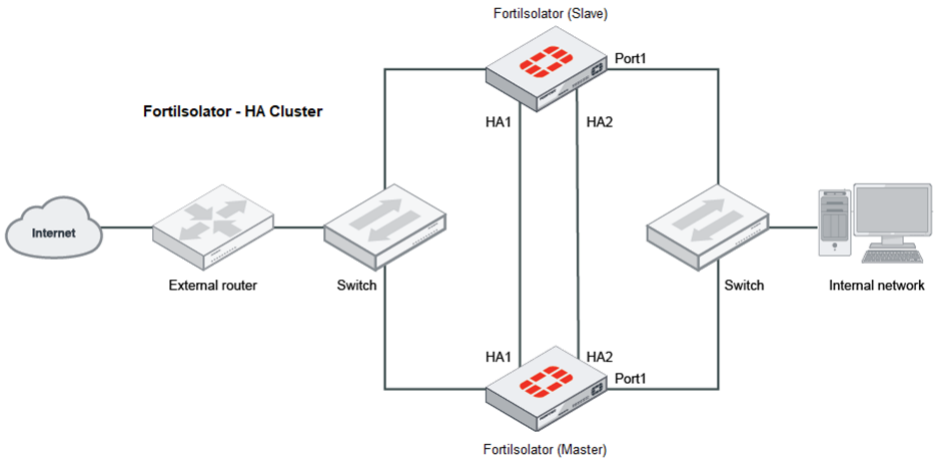

3. Click *OK* to save and apply the settings.

# High Availability

High availability (HA) is usually required in a system where there is high demand for little downtime. There are usually hot-swaps, backup routes, or standby backup units and as soon as the active entity fails, backup entities will start functioning. This results in minimal interruption for the users.

## Architecture

FortiIsolator provides an HA solution whereby FortiIsolator can find other member FortiIsolators to negotiate and create a cluster, which consists of 2 to 255 FortiIsolator members/nodes configured for HA operation. The cluster works like a device but always has a hot backup device.




## Configuration

The nodes in the cluster do not have to be the same model (e.g. FIS 1000F, KVM, or ESXi) and their IP addresses can vary. However, the same firmware must be installed on all nodes and some HA setting (bold in table below) must be the same.

When you use domain names instead of IP addresses in HA mode, make sure your DNS server has load balancing capabilities. Otherwise, all requests will go to the primary node.

### GUI

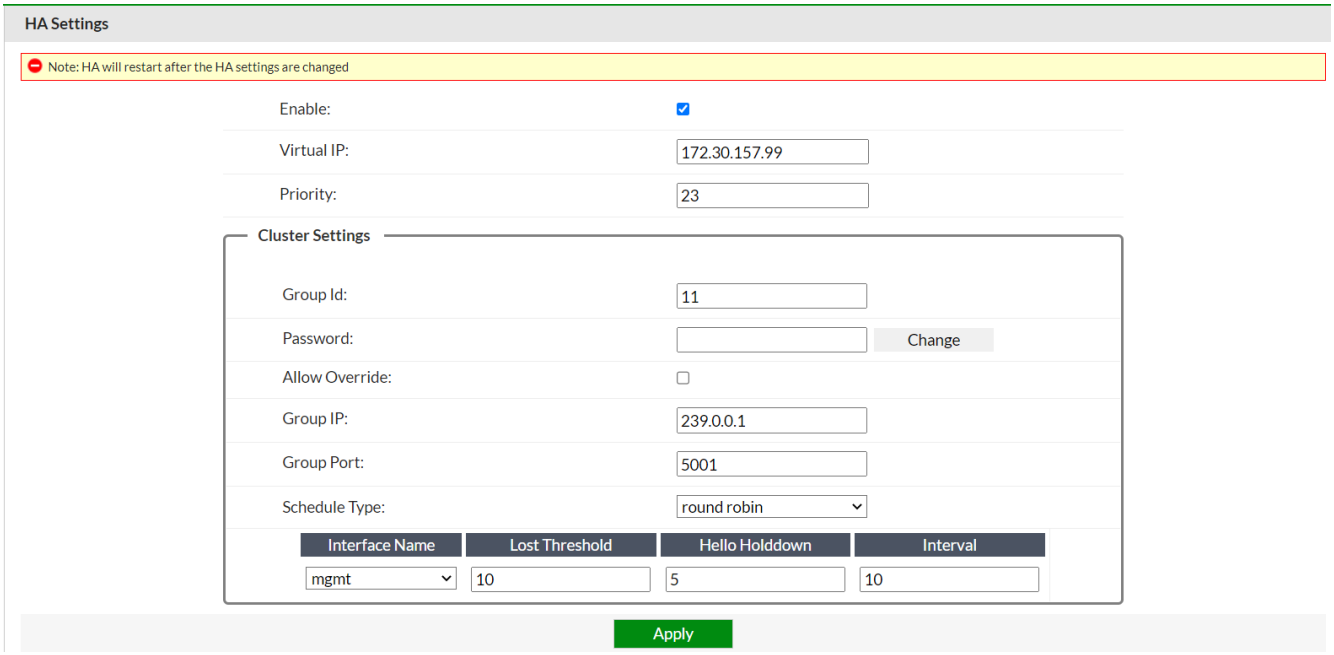
Under *System* > *HA*, configure the following options.

| Parameter | Description |
|---|---|
| ***Enable*** | Specifies whether to enable HA mode for this node. |

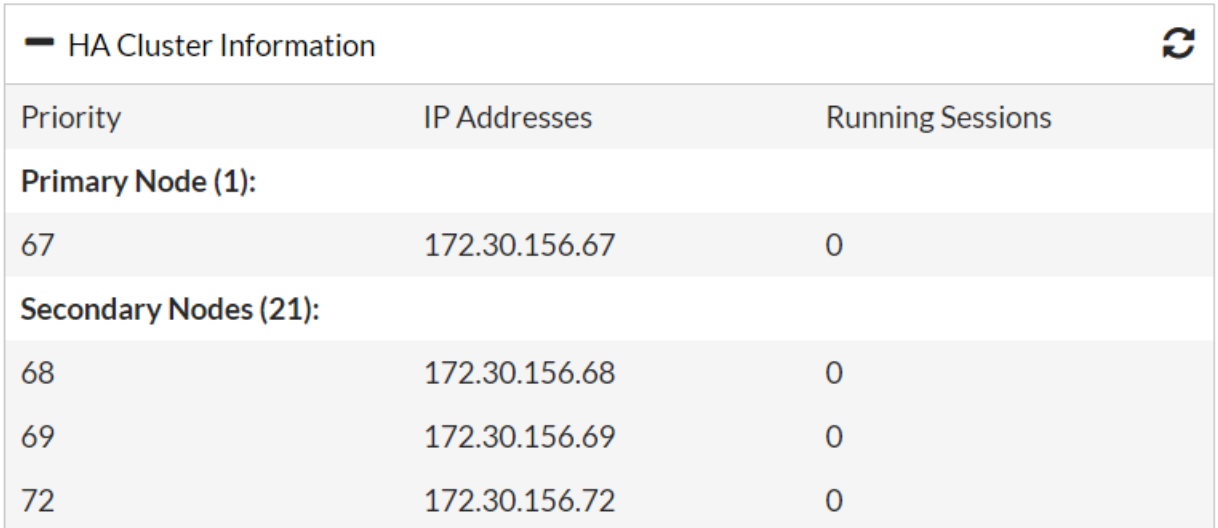
| Parameter | Description |
|---|---|
| ***Virtual IP*** | IP for web browsers access from all nodes in the cluster. Only the primary device has virtual IP address, which is shared among all nodes within the cluster so all nodes can use this same virtual IP address to access sites. The virtual IP address must be the same subnet as the internal interface.<br>In HA mode, web browsers access the virtual IP address in the following modes:<br>• *IP Forwarding*—The web browser first connects to the virtual IP address of the primary node which then forwards the request to itself or another node in the cluster through the internal IP of the recipient node in the cluster, which can be the primary node itself or a secondary node.<br>• *Proxy*—The web browser connects to the virtual IP address of the primary node and keeps communicating with the primary node, which then connects to a node (can be the primary node itself) on its internal IP through web socket connection. The web browser then runs the session on that node. |
| *Priority* | Priority of the node indicated with an integer between 0 to 254, where 0 means the highest priority.<br>You must assign a unique priority ID to each node. The node with the highest priority ID automatically becomes the primary device of the HA cluster. |
| ***Group Id*** | A unique number to identify the cluster. One Group ID number represents one cluster, while different Group ID numbers represent different clusters. Group ID must be an integer between 1 – 255. |
| ***Password*** | Password for the group, which protects the cluster from unauthorized access. |
| *Allow Override* | Specifies whether to allow other nodes to override as a primary node when this node is primary. This option does not take effect when the node is secondary. |
| ***Group IP*** | IP multicast in the range of 224.0.0.0 and 239.255.255.255. |
| ***Group Port*** | Port of the group IP address. |
| ***Schedule Type*** | • *round robin*—Send URL requests can to all member nodes in circular order one by one. All handlings have equal priority.<br>• *weighted round robin*: Round robin scheduling with a fixed number as configured weight which allows member nodes to deal with more than one URL requests in one circular order. |
| *FQDN* | Full qualified domain name of the HA cluster, which is a combination of the host name and domain name. When defined, you can log into the FortiIsolator using the FQDN instead of the IP address of the HA cluster.<br>For example, if the host name is `fisisolator` and the domain name is `ddns.com`, the FQDN will be `fisisolator.ddns.com`. See Changing host name on page 31 and Changing domain name on page 31. |
| ***Interface Name*** | Name of the network interface for network traffic, such as the heartbeats to detect whether the member nodes are alive, and communication among all member nodes within the cluster. |

| Parameter | Description |
|---|---|
| ***Lost Threshold*** | Maximum number of successive heartbeat packets that can be missed from other nodes within the cluster. The HA cluster fails as soon as the number of successive missing packets exceeds *Lost Threshold*. |
| ***Hello Holddown*** | Duration (in seconds) of the transition from HA in Hello state to HA in work state. This parameter accepts integers between 5 - 300. |
| ***Interval*** | Duration (in seconds) between two successive packets. |

The following is an example of an HA cluster setup. After you apply the HA settings, reboot the FortiIsolator and close all existing tabs before opening new ones to avoid any web page display issues.




To verify HA cluster information, go to the Dashboard of the GUI and check the *HA Cluster Information* section. See example below.



## CLI

### To configure HA from CLI:

```
set ha-enabled 1
set ha-virtual-ip 172.30.157.99
set ha-priority 2
set ha-group-id 31
set ha-interface mgmt
set ha-password password
```

### To verify HA cluster Information from CLI:

```
show ha-all
     enabled : Enabled
     gid : 11
     lost-threshold : 10
     interval : 10
     holddown : 5
     priority : 68
     allow-override : 0
     schedule : Round Robin
     vip : 172.30.157.99
     password : ffff18ff28ff38ffff60ff3678ff2e03
     interface : mgmt
     ha-group-ip : 239.0.0.1
     ha-group-port : 5001

Cluster Information
   Number of Machine : 4

   Primary node
   (Primary) IP Priority running session
   172.30.157.67 : 67 0

   Secondary node Priority running session
   172.30.157.68 : 68 0
   172.30.157.69 : 69 0
   172.30.157.72 : 72 0
```

## Database

FortiIsolator saves the following HA-related information and configuration in an internal database:

- User groups on page 66
- Profile on page 68
  - Web Filter profile
  - ICAP Profile
- Default policy on page 79
- Agent server
- Polling server

By default, FortiIsolator saves the information in an internal database on the primary node, which gets synchronized to the database of all secondary nodes each time the primary node has changes. Each secondary node then reads from its own local database. To avoid the performance overhead of multiple databases running concurrently, you can set up a dedicated database server for the whole system:

1. Configure a node to be the dedicated database server by running the `set remote-database-enabled 1` command.
2. Connect to the dedicated database server by running the `set database-server <server IP> 6397 <server name> <server password>` command on each node that you want to connect to the database.
3. Verify the server connection by running the `show database-server` command.

### Batch Upgrade

FortiIsolator supports batch upgrade in HA mode. Upgrading one FortiIsolator appliance or VM in the cluster automatically batch upgrades all FortiIsolator appliances or VMs in the cluster. Each appliance or VM automatically reboots after it gets upgraded. The appliance or VM that triggers the batch upgrade is upgraded last. The reboot might take a few minutes.

For more information about how to upgrade a FortiIsolator appliance or VM, see Upgrade on page 57.

## License sharing

FortiIsolator allows licenses to be shared among all members of the same HA setup. A license file can be uploaded from any member and will then be applied to the entire HA setup. Each license is entitled with a certain number of sessions. All session entitlements within the HA setup are shared and split among the members, depending on when the session limit is reached. For example, for an HA setup of five members with a total entitlement of 500 sessions, the 500 sessions are shared among the members and each member can have up to 500 sessions.

### Configuring maximum number of sessions

To optimize license usage and ensure fair distribution of sessions among the members, you can configure a limit for the number of sessions allowed for each user or IP address.

**To configure the limit in the GUI:**

Use the following options under *Policies and Profiles* > *Default Policy*:

- *Max Session Per User*: assigns a session limit to each local user.
- *Max Session Per IP*: assigns a session limit to each unique IP address.

**To configure the limit in the CLI:**

**Default policy:**

- `set default-policy-max-session-per-ip   100`
- `set default-policy-max-session-per-user 100`

**User-created policy:**

- `set policy-max-session-per-user policy_name 100`
- `set policy-max-session-per-ip   policy_name 100`

# Certificates

Use this page to manage the following types of certificates:

- Self-signed SSL certificates for a specific server or website, often used for an internal enterprise network
- Certificates used between FortiIsolator and FortiProxy or SAML servers

For information about FortiIsolator certificates required for access to the FortiIsolator from the browser, see FortiIsolator certificates on page 33.

**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 |
|---|---|---|
| *SAML_CERT* | SAML Certificate | Certificate for single-sign-on which is created in *LDAP Server* > *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.<br><br>  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.
   Only “Base-64 encoded X.509 (`.cer`)” format certificates are supported.
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 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, the root certificate and all subordinate certificates must be imported into the FortiIsolator and selected in the user’s profile.

# SNMP

SNMP enables FortiIsolator administrators to monitor hardware on client's network.

An admin user can configure the hardware, such as the FortiIsolator SNMP agent, to report system information and send traps (alarms or event messages) to SNMP managers. SNMP traps alert admin users to events that happen, such as the session limit is about to reach.

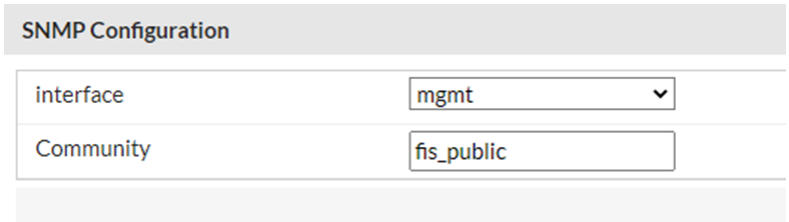
The FortiIsolator SNMP implementation is read-only. SNMP managers have read-only access to FortiIsolator system information through queries, and can receive trap messages from the FortiIsolator unit.

**SNMP configuration**

Before a remote SNMP manager can connect to the FortiIsolator SNMP agent, configurations must be made on FortiIsolator interface and community string in order to accept SNMP connections.

## To configure a FortiIsolator interface and Community string to accept SNMP connections in the GUI:

1. Go to *System* > *SNMP*.
2. Under *interface* dropdown list, select an interface.
3. In the *Community* box, enter SNMP community string.
4. Click *OK*.




## To configure a FortiIsolator interface to accept SNMP connections in the CLI:

```
set snmpd-interface <internal|external|mgmt|ha>
     set snmpd-interface mgmt
```

## To configure a Community string to accept SNMP connections in the CLI:

```
set snmpd-community <fis_community>
     set snmpd-community fis_public
          File: /var/log/syslog/snmpd.conf
          rocommunity fis_public default -V systemonly
```

## To configure SNMP traps:

- For SNMP v1 and v2:

```
set session-threshold [1-100]
     set session-threshold 5
set trap-host-ip <host-ip>
     set trap-host-ip 192.168.1.100
set trap-host-community <host-community>
     set trap-host-community public
```

```
            File: /etc/snmp/ snmptrapd.conf
            authCommunity log,execute,net public
```

- For SNMP v3:

```
set session-threshold [1-100]
     set session-threshold 5
set trap-host-ip <host-ip>
     set trap-host-ip 192.168.1.100
set trap-host-community <host-community>
     set trap-host-community fis_public
          File: /etc/snmp/ snmptrapd.conf
          authCommunity log,execute,net fis_public
set snmpd-v3-user <user name> <disabled | enabled>
     set snmpd-v3-user fis_user 1
set snmpd-auth-method-pwd <1|2 MD5|SHA> <auth password>
     set snmpd-auth-method-pwd 1 password
set snmpd-trap-enable <disabled | enabled>
     set snmpd-trap-enable 1
set snmpd-trap-event <event num> <0|1 disabled | enabled>
     0: CHECK_SESSION_THRESHOLD
     1: MGMT_IP_OFF_DAYS
          set snmpd-trap-event 1 1
```

### To configure SNMP server, include these settings in SNMP `.conf` files:

- For SNMP v1 and v2:

```
> cat /etc/snmp/snmp.conf
mibs +ALL

> cat /etc/snmp/snmpd.conf
rocommunity fis_public default -V systemonly

> cat /var/log/syslog/snmptrapd.conf
authCommunity log,execute,net public
```

```
[SNMP Configurations]
Agent Listening Interface      : mgmt
Agent Community                : fis_public
Trap Host-IP                   : 192.168.1.100
Trap Host Community            : public
Session Threashold(%)          : 5
```

- For SNMP v3:

```
> cat /etc/snmp/snmp.conf
mibs +ALL

> cat /etc/snmp/snmpd.conf
rocommunity fis_public default -V systemonly

> cat /var/log/syslog/snmptrapd.conf
authCommunity log,execute,net fis_public
authUser log,execute,net fis_user auth
```

```
[SNMP Configurations]
Agent Listening Interface     : mgmt
Agent Community               : fis_public
Trap Host-IP                  :
Trap Host Community           :
Session Threashold(%)         : 5
SNMP V3 User Status           : Enabled
SNMP V3 Username              : fis_user
V3 Query Port Status          : Disabled
V3 Query Port Num             : 0
V3 Trap Port Status           : Enabled
V3 Trap Local Port Num        : 162
V3 Trap Remote Port Num       : 162
SNMP V3 Hosts:
    [1]: 172.30.157.208
Security Level                : auth
Authentication Status         : Enabled
Authentication Method         : MD5
Authentication Password       : password
Private Status                : Disabled
Encrypt Method                :
Encrypt Password              :
SNMP V3 Trap Events:
       check_session_threshold:  Enabled
       send_mgmt_ip_off_days:  Enabled
```

**Example results from SNMP traps:**

- For SNMP v1 and v2:

```
> tail -f /var/log/syslog | grep snmp

Apr 14 15:07:00 bigdata snmptrapd[32688]: 2021-04-14 15:07:00 <UNKNOWN> [UDP: [FIS_
     IP]:56623->[SNMP_Server_IP]:162]:#012DISMAN-EVENT-MIB::sysUpTimeInstance =
     Timeticks: (1460730) 4:03:27.30#011SNMPv2-MIB::snmpTrapOID.0 = OID: FORTINET-
     FORTIISOLATOR-MIB::fisTrapSessOverThreshold#011FORTINET-FORTIISOLATOR-
     MIB::fisSessUsage = INTEGER: 5
Apr 14 15:07:00 bigdata snmptrapd[32688]: 2021-04-14 15:07:00 <UNKNOWN> [UDP: [FIS_
     IP]:56623->[SNMP_Server_IP]:162]:#012DISMAN-EVENT-MIB::sysUpTimeInstance =
     Timeticks: (1460730) 4:03:27.30#011SNMPv2-MIB::snmpTrapOID.0 = OID: FORTINET-
     FORTIISOLATOR-MIB::fisTrapSessOverThreshold#011FORTINET-FORTIISOLATOR-
     MIB::fisSessUsage = INTEGER: 5
```

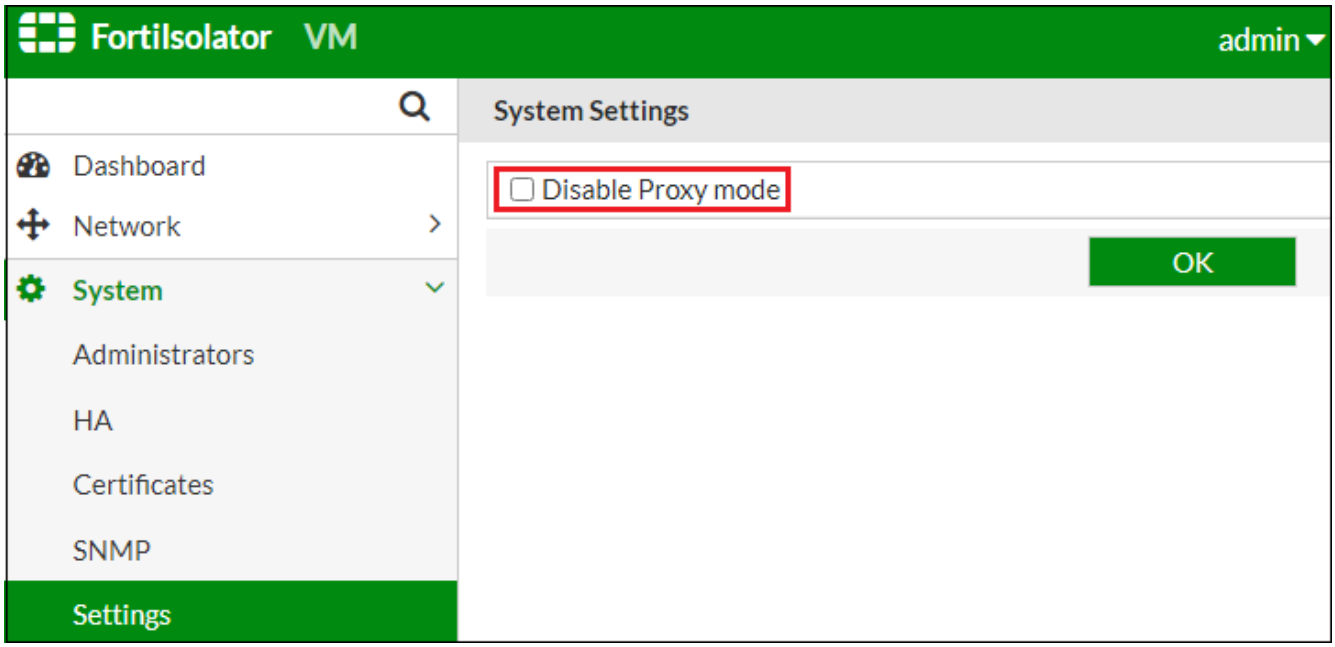
- For SNMP v3:

```
> sudo snmptrapd -C -c /etc/snmp/snmptrapd.conf -f -Dusm -Lo

registered debug token usm, 1
Log handling defined - disabling stderr
usmUser: created a new user fis_user at 80 00 1F 88 80 92 69 F2 3A F8 B8 E9 62 00 00 00
     00
NET-SNMP version 5.7.3 AgentX subagent connected
NET-SNMP version 5.7.3
usm: USM processing begun...
usm: match on user fis_user
usm: Verification succeeded.
usm: USM processing completed.
```

```
2022-08-04 16:28:10 <UNKNOWN> [UDP: [172.30.157.35]:34557->[172.30.157.208]:162]:
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (17079281) 1 day, 23:26:32.81 SNMPv2-
     MIB::snmpTrapOID.0 = OID: SNMPv2-SMI::enterprises.12356.199.2.0.101 SNMPv2-
     SMI::enterprises.12356.199.6.2.2 = INTEGER: 9
usm: USM processing begun...
usm: match on user fis_user
usm: Verification succeeded.
usm: USM processing completed.
2022-08-04 16:29:10 <UNKNOWN> [UDP: [172.30.157.35]:41908->[172.30.157.208]:162]:
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (17085283) 1 day, 23:27:32.83 SNMPv2-
     MIB::snmpTrapOID.0 = OID: SNMPv2-SMI::enterprises.12356.199.2.0.101 SNMPv2-
     SMI::enterprises.12356.199.6.2.2 = INTEGER: 9
```

## Settings - NEW

Use the *Settings* tab to disable proxy mode at a global level on the FortiIsolator:

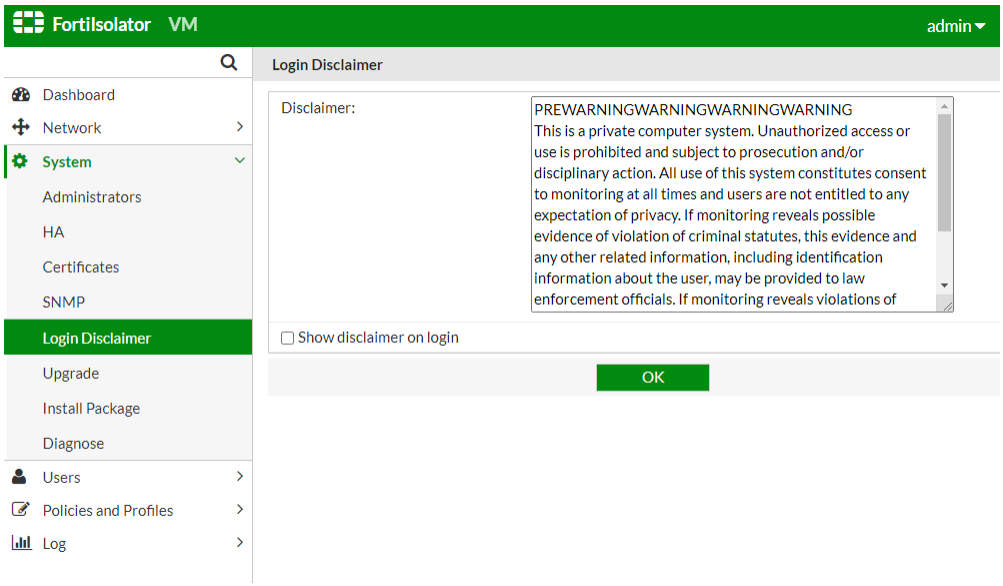



Alternatively, use the `disable proxy` command under system settings in the CLI.

# 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.




# Upgrade

This section the following ways to upgrade FortiIsolator firmware:

- Upgrade the firmware by GUI (Web and USB)
- Upgrade the firmware by CLI

In High Availability on page 46 mode, upgrading one FortiIsolator appliance or VM automatically batch upgrades all FortiIsolator appliances or VMs in the cluster. Each appliance or VM automatically reboots after it gets upgraded. The appliance or VM that triggers the batch upgrade is upgraded last. The reboot might take a few minutes.

## To upgrade the firmware by web

This feature applies to both FortiIsolator hardware appliances and FortiIsolator VMs.

1. Log into the FortiIsolator GUI as the admin administrative user.
2. Go to *System* > *Upgrade*.
3. Under *Upgrade by Web*, click *Choose File* and locate the previously downloaded firmware image file. See Upgrade information for instructions about downloading the upgrade firmware.
4. Under *Start Hour*, select the hour when FortiIsolator starts the upgrade process. Selecting *immediate* triggers the upgrade immediately.
5. Click *Submit* to upgrade the firmware.

The FortiIsolator unit backs up the current configuration, upgrades to the new firmware version, restarts it, and restores the backed up configuration. This process takes a few minutes.

### To upgrade the firmware by USB device

This feature only applies to FortiIsolator hardware appliances, such as FortiIsolator 1000F.

1. Log into the FortiIsolator GUI as the admin administrative user.
2. Go to *System* > *Upgrade*.
3. Under *Upgrade by USB*, click *Click here* and locate the previously downloaded firmware image file that stored in USB device.
4. Click *Submit* to upgrade the firmware.

## To upgrade the firmware in CLI

This feature applies to both FortiIsolator hardware appliances and FortiIsolator VMs.

1. Log into the FortiIsolator CLI as the admin administrative user.
2. Run the following command to install the firmware image from a server:
   `system-upgrade {tftp|ftp} <path> <server> [:<port>] [<user>:<password>]`

For FortiIsolator hardware appliances, you can also install the firmware image from a USB device that contains the previously downloaded firmware image by inserting the USB and running the `system-upgrade` command.

The FortiIsolator unit copies the new firmware image from the server or USB device to local hard disk, backs up the current configuration, and performs upgrade to the new firmware version. This process takes a few minutes. After the upgrade, the system reboots and deletes the firmware image from local disk.

# Install package

While you can view PDF (`.pdf`), TXT (`.txt`), and PNG (`.png`) files without downloading the actual file, you must manually install an additional package to view the following Microsoft Office document types without downloading the actual file:

- Word (`.doc`, `.docx`)
- Excel (`.xls`, `.xlsx`)
- PowerPoint (`.ppt`)

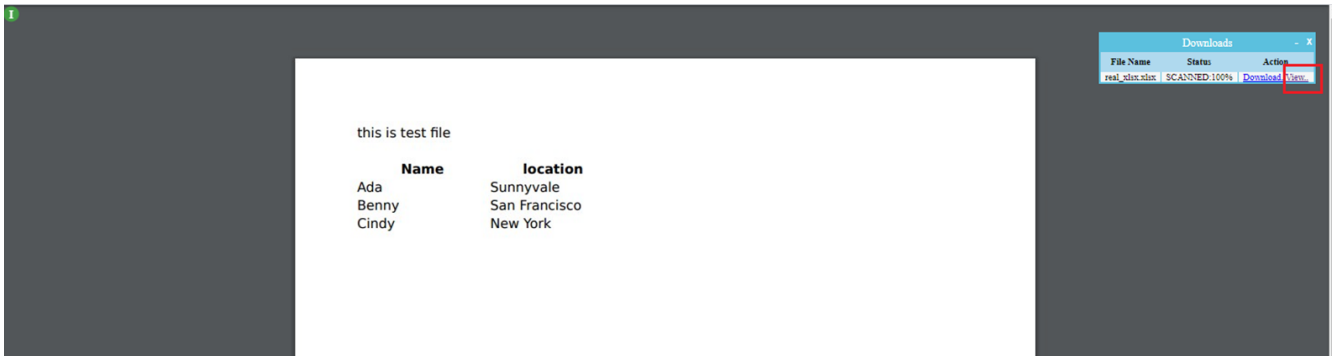
By default, the package is not installed, which is indicated in the *Applications Information* section in the dashboard.

### To install the package for viewing Microsoft Office document types without downloading the actual file:

1. Download the `office-1.5.zip` package by following the instructions here.
2. Install the package:
   a. Go to *FortiIsolator GUI* > *System* > *Install Package*.
   b. Click *Choose File*.
   c. Select the package file you downloaded in step 1.
   d. Click *Submit*.
3. After the installation is complete, verify the *Applications Information* section shows *office installed, version:latest* in the dashboard.


In HA mode, by default, you must install the package on each node where you want to view Microsoft Office document types without downloading the actual file. To avoid installing the package on multiple nodes, you can set an appliance or VM to be the dedicated file server for opening those document types by running the `set office-server-ip <internal IP>` command, which allows you to open those document types without downloading the actual file on all nodes as long as the package is installed on the server node. Setting a dedicated file server also improves system performance.

### Sample view of a Microsoft Office document in FortiIsolator:



# 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 LDAP servers to allow user accounts on the remote authentication servers to browse websites through the FortiIsolator unit.

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 LDAP servers, you can do the following:

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

## LDAP servers

LDAP is an Internet protocol used to maintain authentication data that can include departments, people, groups of people, passwords, email addresses, and printers. LDAP consists of a data-representation scheme, a set of defined operations, and a request/response network.

FortiIsolator uses Windows AD server with LDAP enabled and applies Fortinet Single Sign On Agent to authenticate users on remote servers when accessing websites through FortiIsolator.

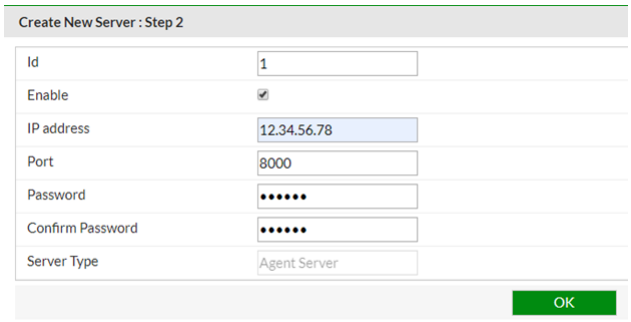
To manage LDAP servers on FortiIsolator, go to *Users* > *LDAP Server*.

### Create or edit a LDAP server

#### To add a new LDAP server:

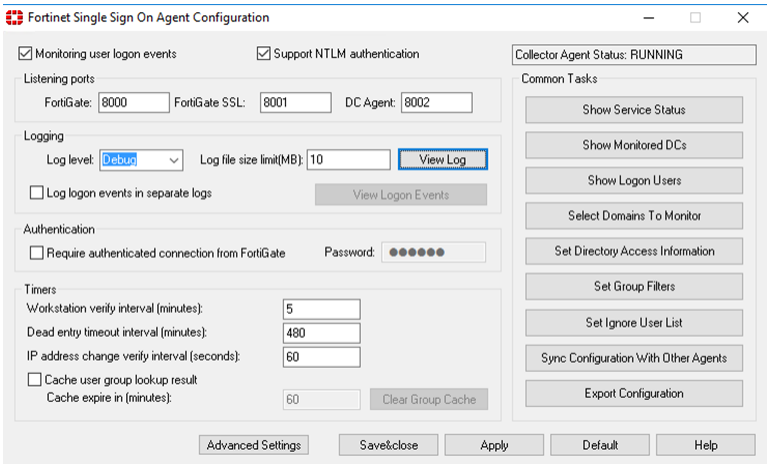
1. Go to *Users* > *LDAP Server*.
2. Select *Create New* from the toolbar. The *Create New Server* page opens.
3. Select *Agent Server* from the dropdown list. Configure the following accordingly:

| Agent Server | |
|---|---|
| Id | 1 – 4 (a unique ID for each server) |
| Enable | Check the box to enable the server |
| IP Address | IP Address of LDAP server |
| Port | Port number of FSSO Agent on LDAP server |
| Password | Password of FSSO Agent on LDAP server |




4. Click *OK*.
5. The FortiIsolator checks the connection. The connection must be successful for the FSSO Agent server to work.

### Fortinet Single Sign On (FSSO) agent server configuration




# 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:

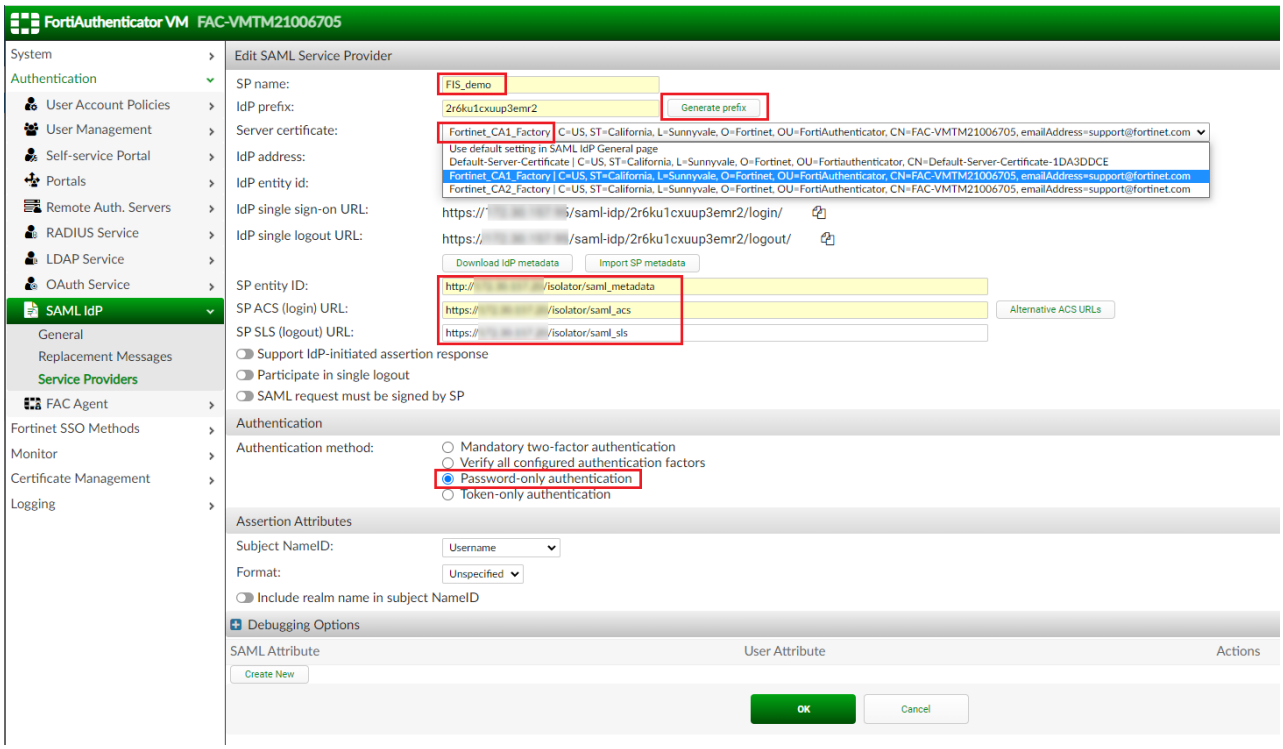
1. Setup in FortiAuthenticator on page 62
2. Setup in FortiIsolator on page 64

## Setup in FortiAuthenticator

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

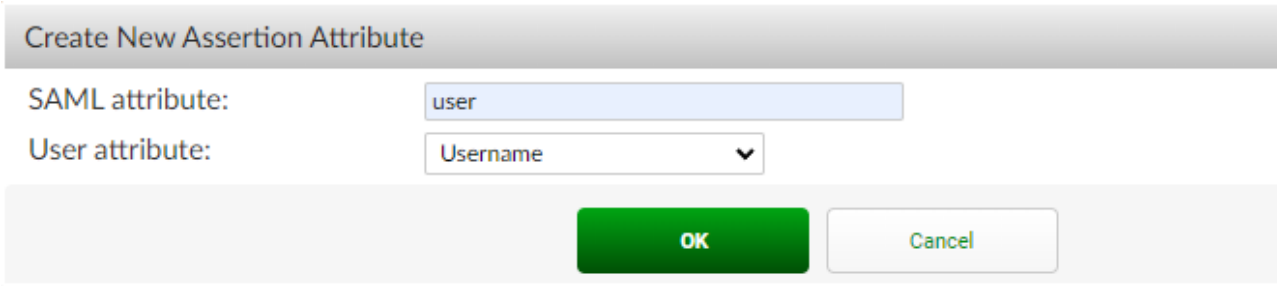
| | |
|---|---|
| SP Name | Name of the Service Provider |
| IdP prefix | Generate Prefix |
| Server Certificate | Fortinet_CA1_Factory |
| SP Entity ID | http://<*FortiIsolator ip or FQDN*>/isolator/saml_metadata |
| SP ACS (login) URL | https://<*FortiIsolator ip or FQDN*>/isolator/saml_acs |
| SP SLS (logout) URL | https://<*FortiIsolator ip or FQDN*>/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.
- The FortiIsolator FQDN is a combination of the host name and domain name. For example, if the host name is `fisisolator` and the domain name is `ddns.com`, the FQDN will be `fisisolator.ddns.com`.

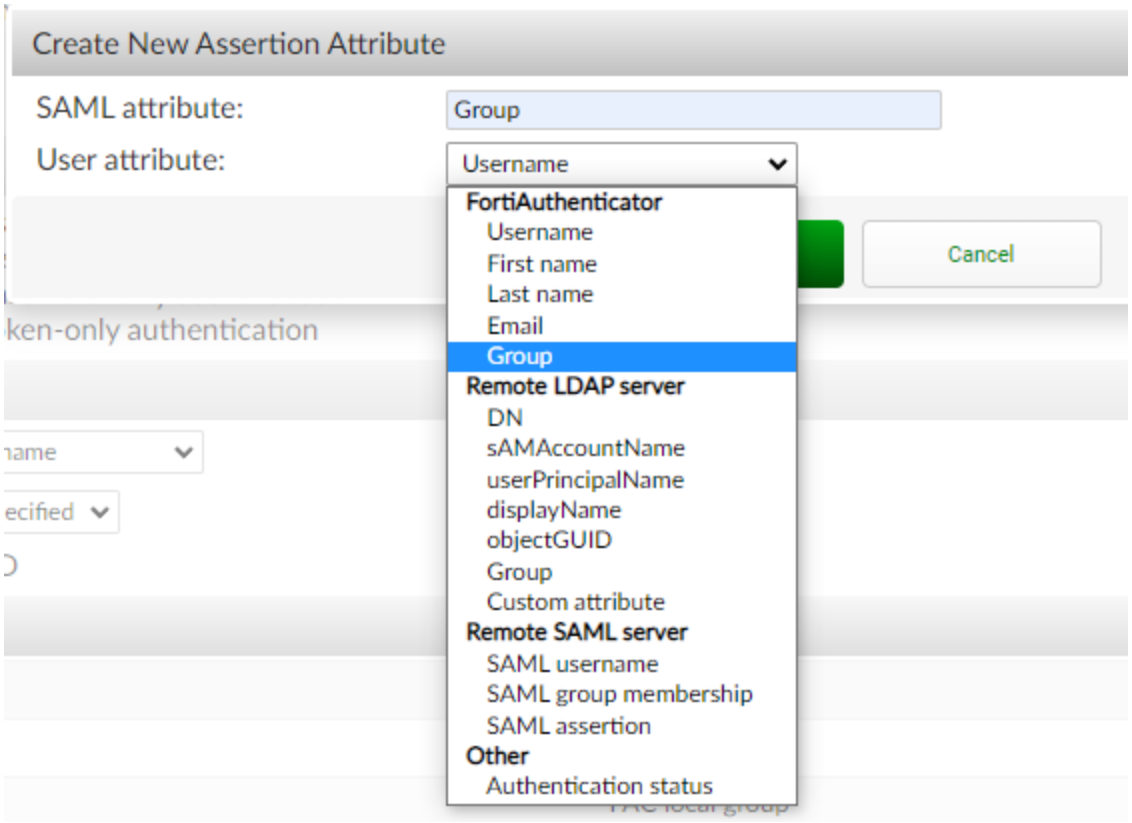



3. Click *OK*.
4. Click on *SP Name* then *Edit*.

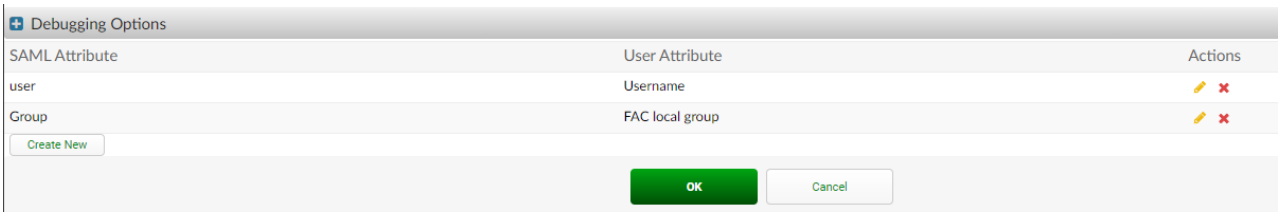
5. Add an SAML Attribute for user.




6. Add SAML Attribute for Group



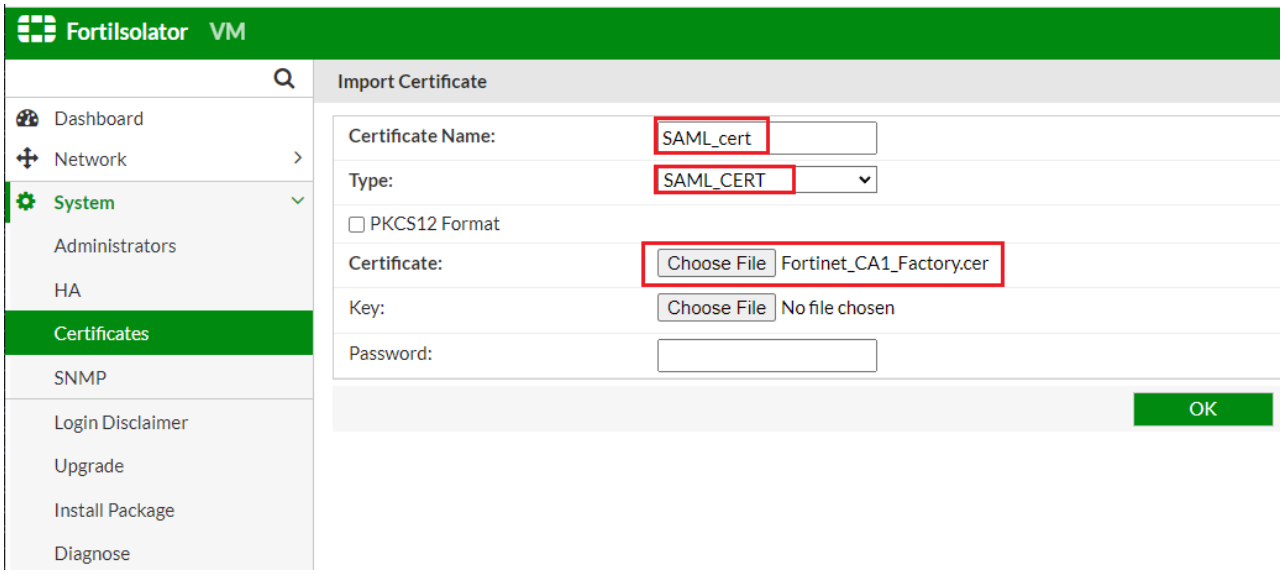

Debugging Options should look like this:




7. Go to *Certificate Management* > *End Entities* > *Local Services* and export the *Fortinet_CA1_Factory* certificate to later import to 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.



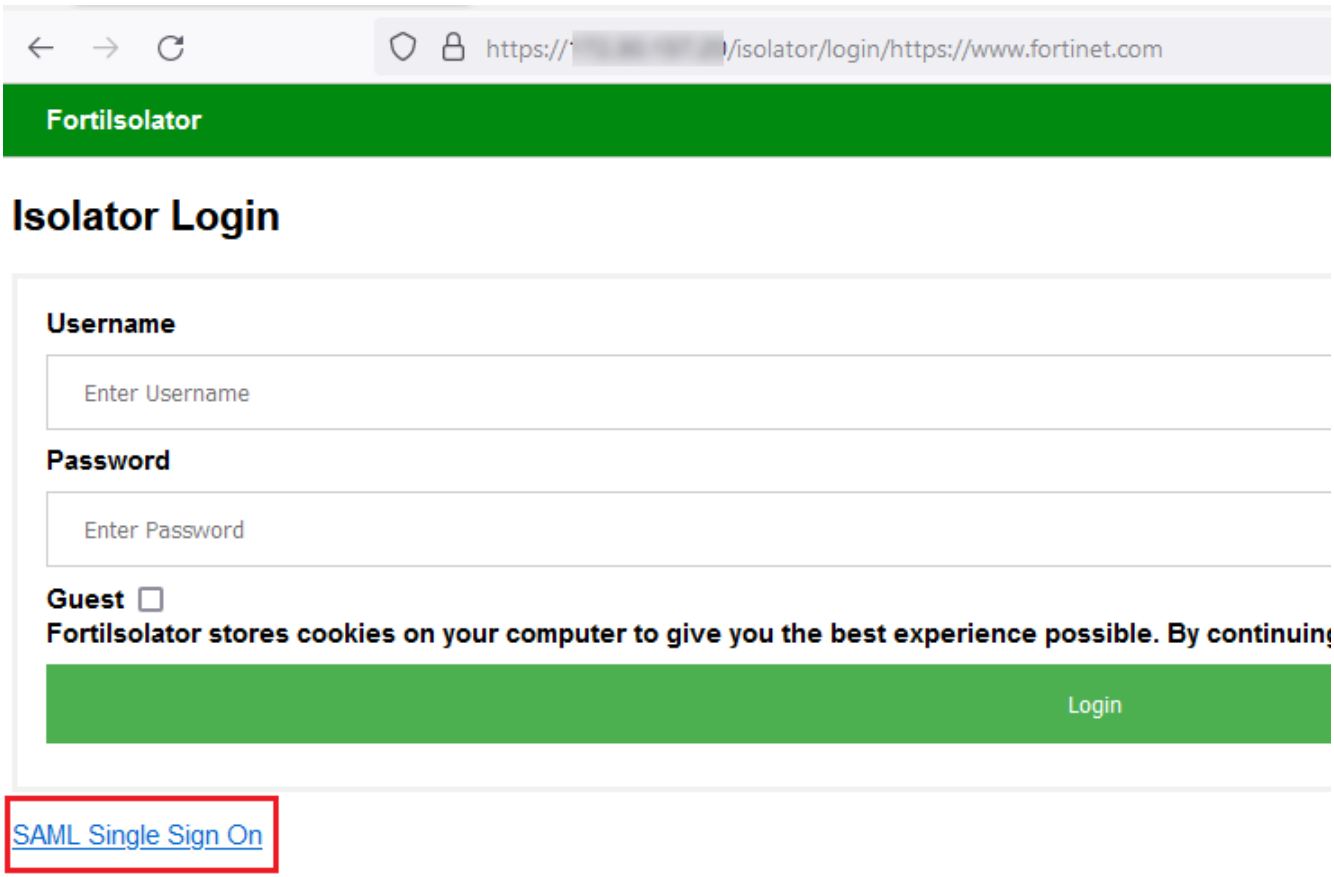

3. Navigate to *Users* > *LDAP Server* > *Create New*.
4. Select *SAML Server* and click *OK*.
5. Configure the following:

| | |
|---|---|
| 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 FQDN>/isolator/login/https://www.fortinet.com`




# 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:

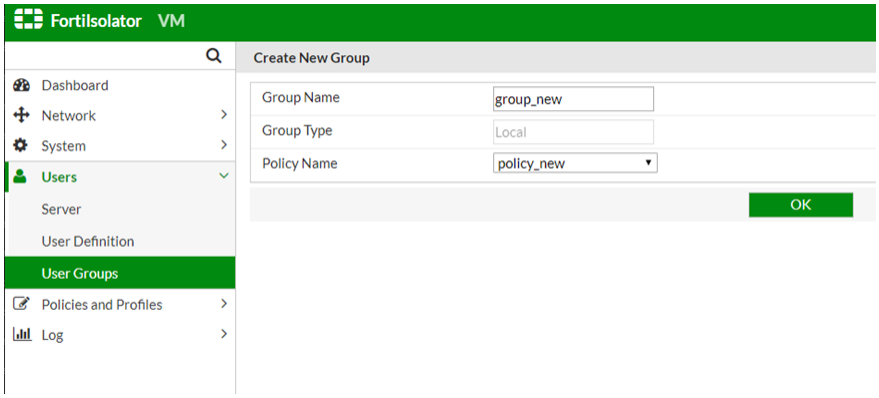
1. From the administration portal, go to *Users* > *User Groups* and click *Create New*.
2. Type in a name for the group and click *OK*.

## 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
>
```



# 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

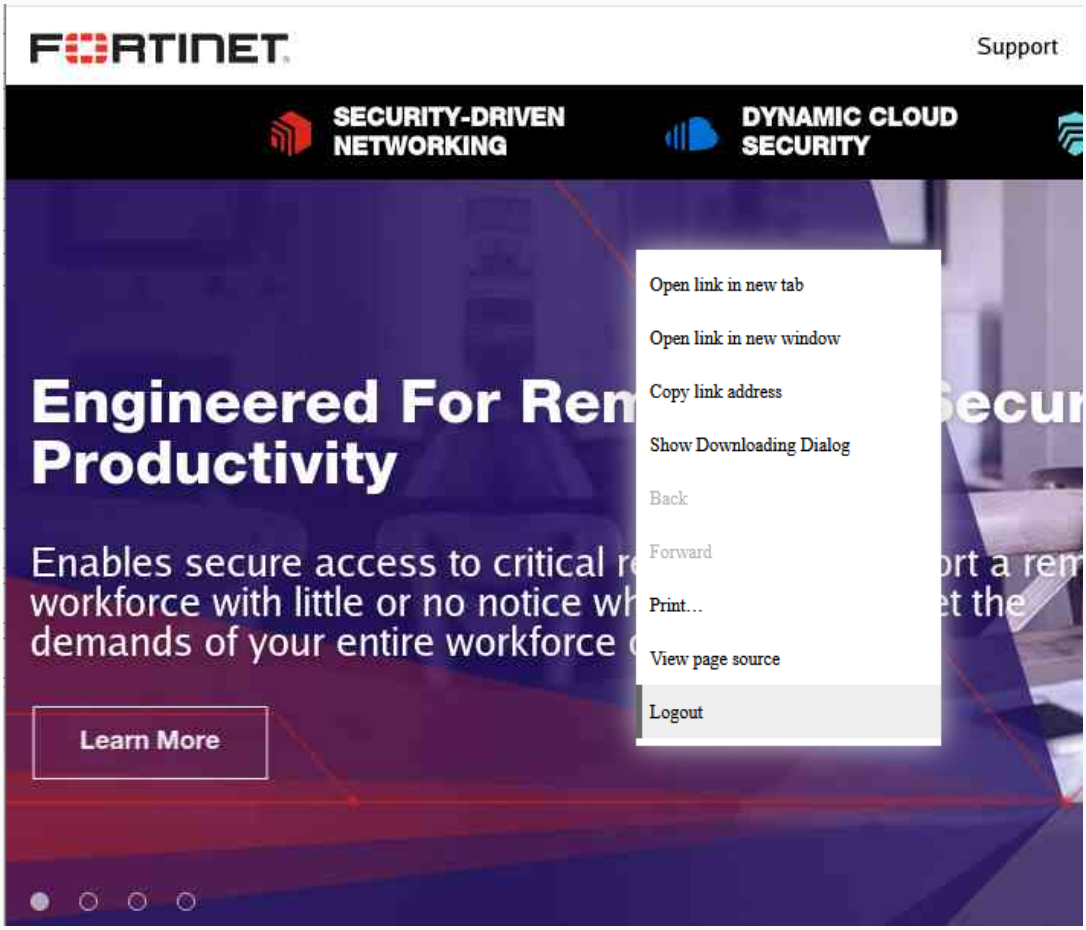
### Creating a Isolator browsing profile

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.<br>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.<br>  This option works only if *View-only Mode* is disabled. |




| | |
|---|---|
| Print | Users can print the current page as a PDF file. |
| Logout | Log out from the current session. |

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

| | |
|---|---|
| *Show Isolation Icon* | Specifies whether to show the FortiIsolator icon on the pages when users browse using FortiIsolator. |
| *Certificates* | Specifies which uploaded certificate(s) to enable for the profile.<br>FortiIsolator automatically lists all uploaded Certificates on page 51 of the following types. If no such certificate is uploaded, the list is empty.<br>• Self Signed Server Certificate<br>• Self Signed CA Root Certificate<br>• Intermediate CA Certificate<br>  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.<br>• *exe*<br>• *doc*<br>• *ppt*<br>• *pdf*<br>• *txt*<br>• *xls*<br>• *png*<br>• *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.<br>• *exe*<br>• *doc*<br>• *ppt*<br>• *pdf*<br>• *txt*<br>• *xls*<br>• *png*<br>• *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.<br>• *exe*<br>• *doc*<br>• *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.

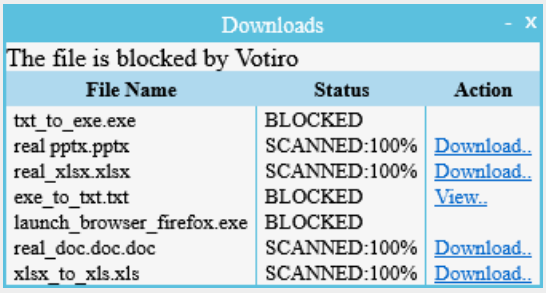
To verify connection with FortiSandbox, upload a file using FortiIsolator. When the following image appears, which means the upload is complete, verify that the file is being scanned in FortiSandbox and view the result of the scan.

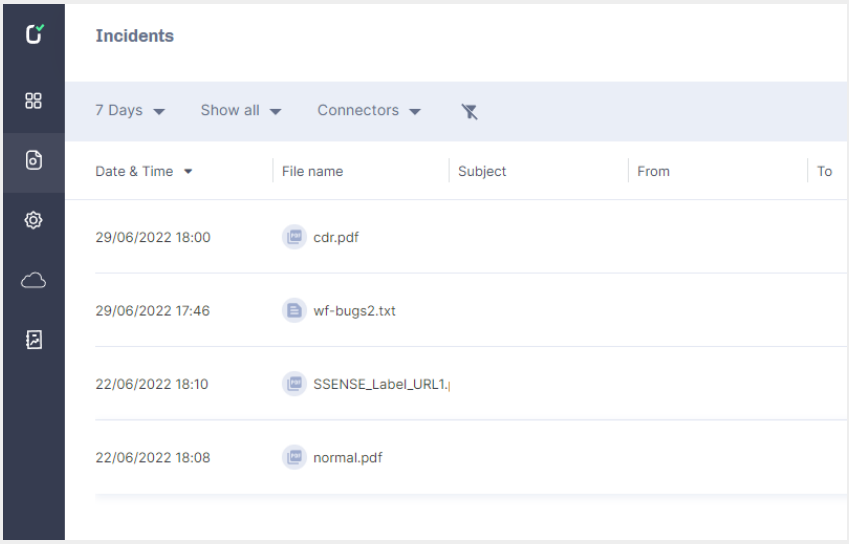

*Scan Files with FortiIsolator*

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:<br>• *Votiro URL*—URL of the Votiro application.<br>• *Votiro Token*—Service token that you created in Votiro which allows FortiIsolator to communicate with Votiro.<br>• *Votiro Channel ID*—ID of the Votiro service token.<br>• *Votiro Policy Name*—Name of the Votiro policy to use.<br>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. |




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)<br>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)<br>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

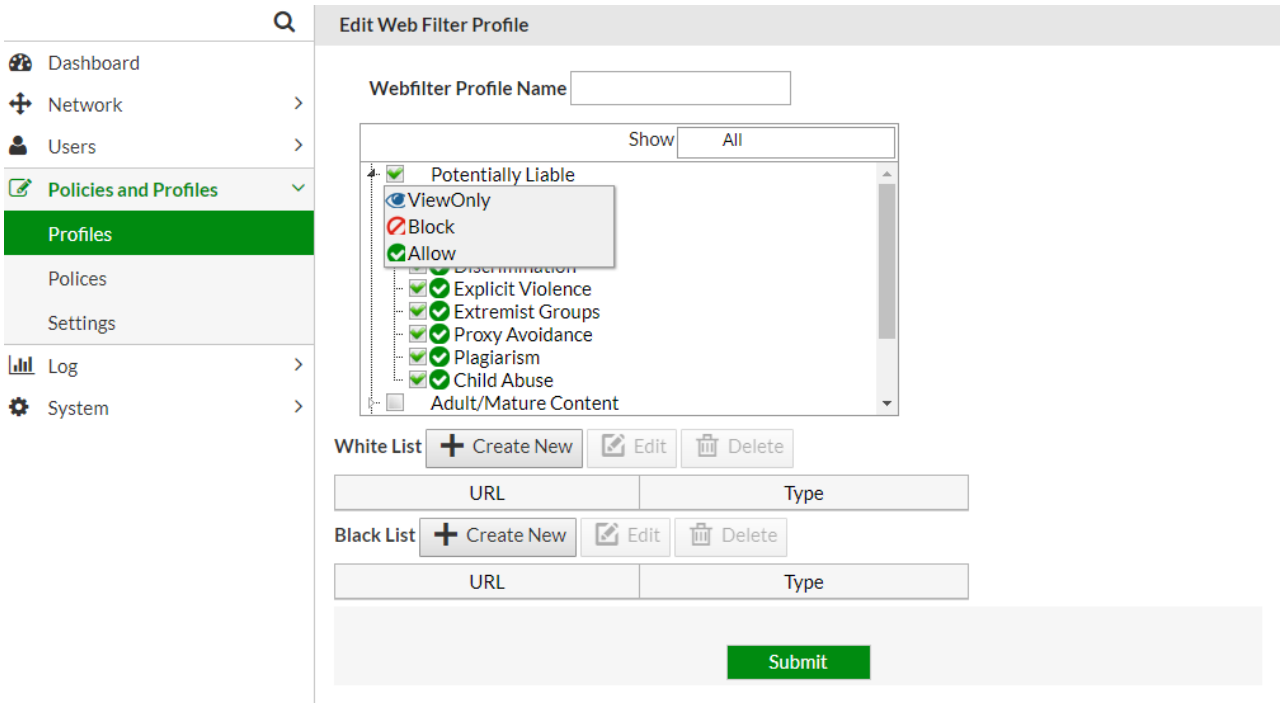
FortiIsolator supports web filtering, which enables the administrator to control which webpages that end users are allowed to view. You can block specific URLs or websites, which prevents the end user's browser from loading web pages from these websites.

### 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.



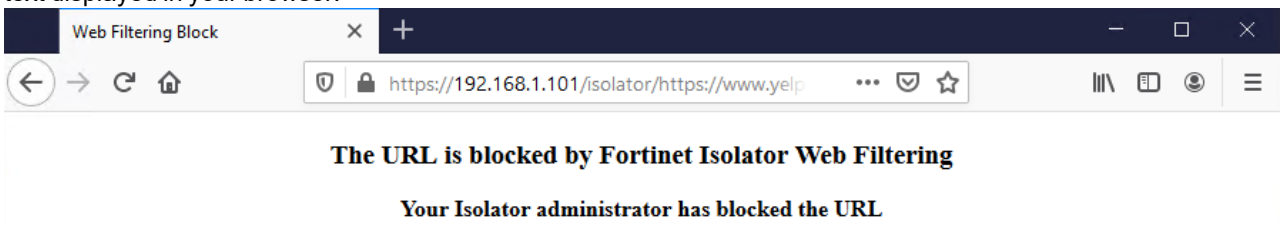

Right-click on any checked box to select the desired action:

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:



### 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.

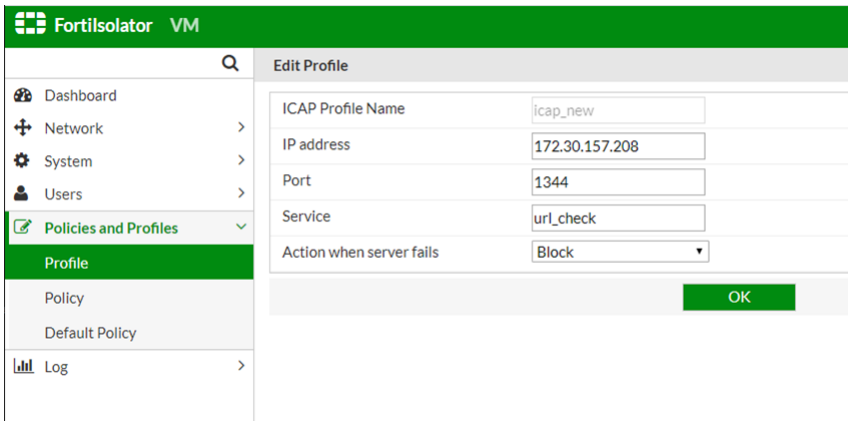
### To create an ICAP profile from GUI:

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<br>• Allow<br>• Block<br>• 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
```




# 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 and select the desired Isolator and/or Web Filter profiles, and/or ICAP Filter profile to be used in the policy.
3. Specify the value for *Max Session Per User*, which is the maximum number of sessions (tabs) allowed for requests from a same local user.
4. Specify the value for *Max Session Per IP*, which is the maximum number of sessions (tabs) allowed for requests from a unique IP address.
5. 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.

6. 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.<br>  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.

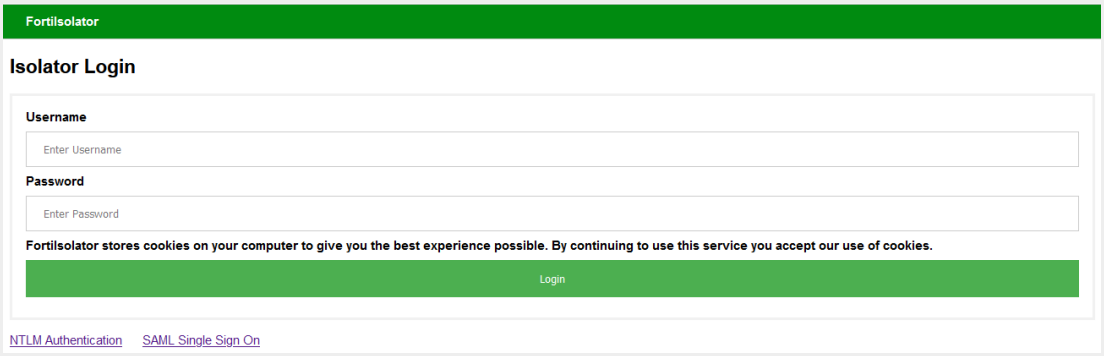
### To apply profiles to default policy from GUI:

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 121.

| | |
|---|---|
| *guest disable* | A user has to log in with a user account of one of the following types:<br>• **Local user** - The user can log in by entering the designated username and password |

configured in User definition on page 65 if *Login Option* is *Local User or SAML User Only*.

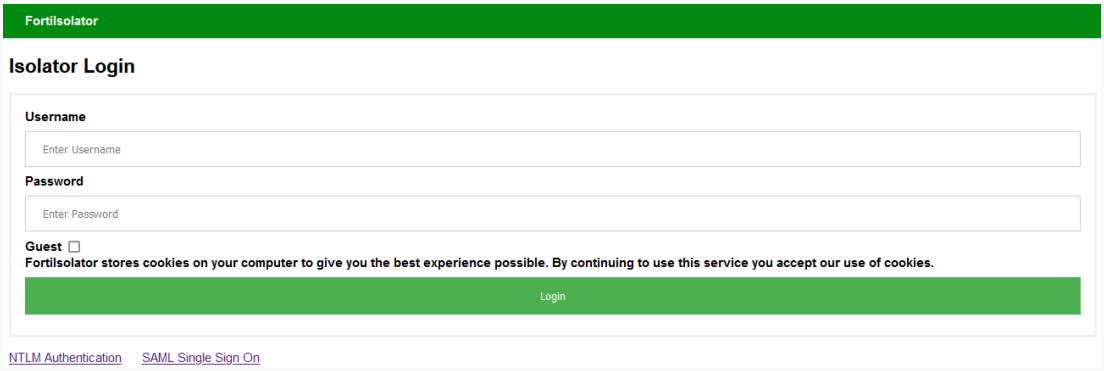
- **NTLM user** - If an FSSO agent server is configured in LDAP servers on page 60, the user can log in with single-sign-on by clicking the *NTLM Authentication* link and entering the credentials.
- **SAML user** - If a SAML server is configured through FortiAuthenticator in SAML servers on page 61, the user can log in with single-sign-on by clicking the *SAML Single Sign On* link and entering the credentials.




*guest enable*

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

- To log in with a user account, the user enters the credentials of one of the following account types:
  - **Local user** - The user enters the designated username and password configured in User definition on page 65.
  - **NTLM user** - If an FSSO agent server is configured in LDAP servers on page 60, the user can single-sign-on by clicking the *NTLM Authentication* link and entering the credentials.
  - **SAML user** - If a SAML server is configured through FortiAuthenticator in SAML servers on page 61, the user can single-sign-on by clicking the *SAML Single Sign On* link and entering the credentials.
- To log in as a guest, the user leaves the username and password empty and selects *Guest*.




*guest only*

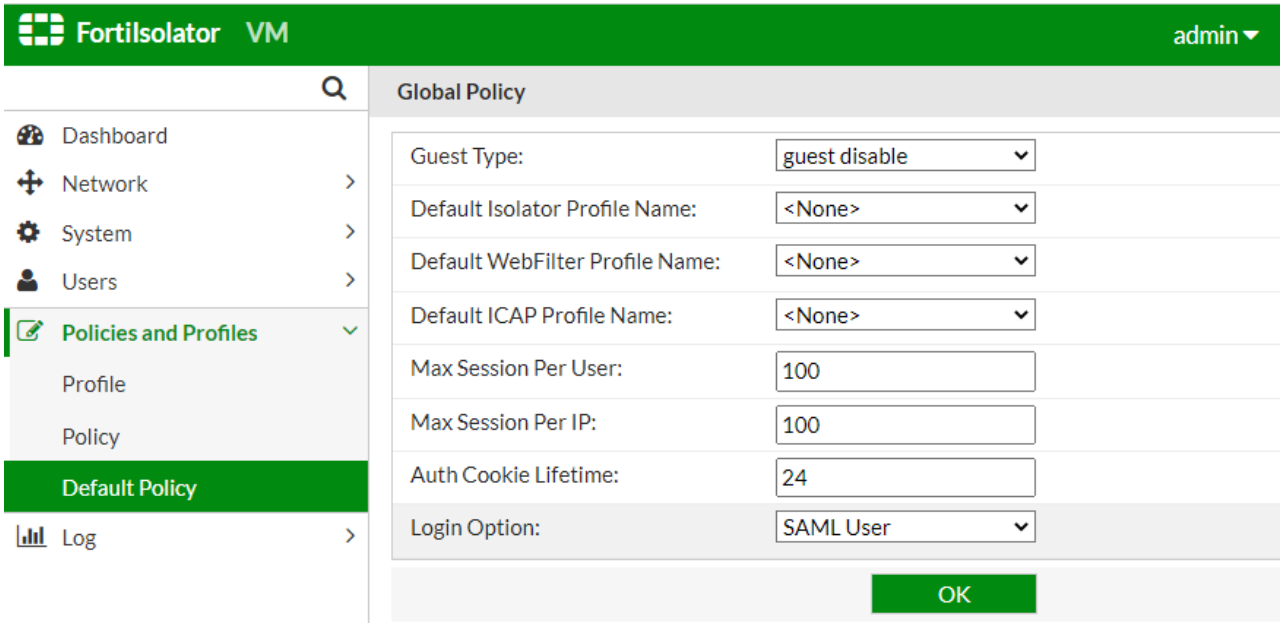
A user has to log in as a guest.

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

2. Select the Isolator profile, Web Filter profile, and/or ICAP Filter profile to be used in the policy. Also set *Max Session Per User*, *Max Session Per IP*, *Auth Cookie Lifetime*, and *Login Option* to be used in the 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.<br><br>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 61.<br>• *Local User or SAML User*—Allow the user to log in using a local user account or SAML credentials.<br>• *SAML User*—Allow the user to log in using the SAML credentials only. Local user accounts are not allowed. |

3. Click *OK* to finish.




## 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
```

| | |
|---|---|
| <isolator-profile-name > | Isolator profile name |
| <webfilter-profile-name > | Web Filter profile name |
| <icap-profile-name > | ICAP profile name |
| <guest-type> | Login mode of the user:<br>1 — *guest disable*: A user must log in with the following types of credentials:<br>• Local user account—Only if *Login Option* is *Local User or SAML User*.<br>• SAML credentials—Only if a SAML server is configured through FortiAuthenticator in SAML servers on page 61.<br>2 — *guest enable*: A user can log in with a user account, SAML/NTML authentication, or as a guest.<br>0 — *guest only*: A user has to log in as a guest. No credentials are required. |
| <max-session-per-user> | Maximum number of sessions (tabs) allowed for requests from a same local user |
| <max-session-per-ip> | Maximum number of sessions (tabs) allowed for requests from a unique IP address |
| <auth-cookie-lifetime> | Number of hours after which the authorization cookie expires and the user needs to re-login. This parameter accepts integers within the range of 1-240.<br>This parameter does not take effect when the user is in guest mode. |

| | |
|---|---|
| <global-policy-login-option> | Login option allowed for the user. This option is available only if *Guest Type* is *guest disable* and a SAML server is configured through FortiAuthenticator in SAML servers on page 61. |
| 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

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

- Daemons running on FortiIsolator devices
- 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 using filters:

- Traffic logs on page 84
  - Antivirus
  - Web Filter
- Event logs on page 85

You can also configure FortiIsolator to send the log to a third-party Remote Server on page 85, including FortiAnalyzer.

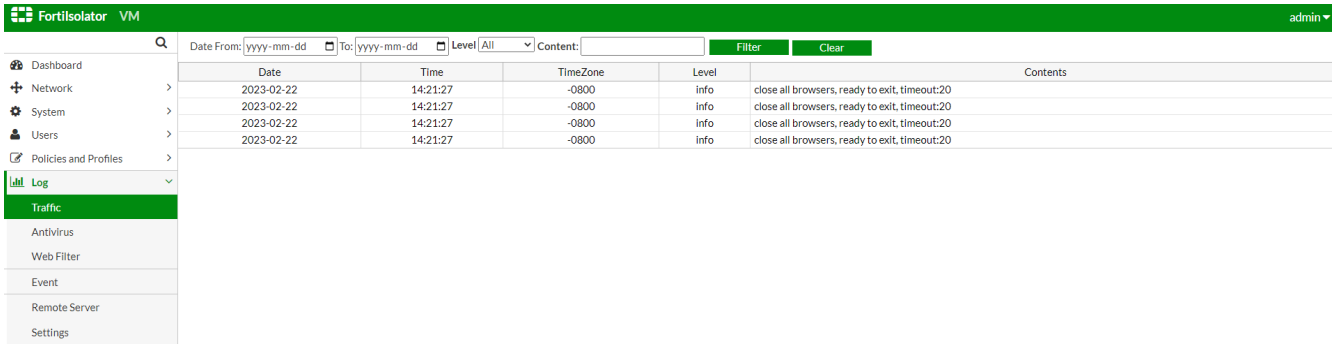
- FortiAnalyzer— FortiIsolator routes the log to FortiAnalyzer for display, processing, or reporting. FortiIsolator no longer displays the logs under the log categories. See the FortiAnalyzer Administration Guide for more information.
- Third-party remote server—FortiIsolator sends a copy of the raw 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 86 tab.

Refer to the FortiIsolator Log Message Reference Guide for more information about how to interpret the log messages.

## Traffic logs

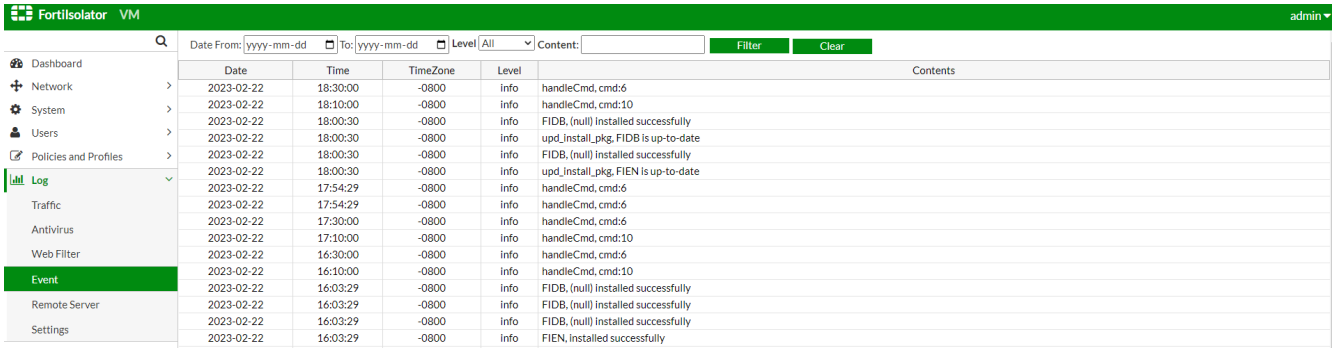
Traffic logs record the traffic flowing through your FortiIsolator unit. All traffic logs are available from the log page *Log* > *Traffic* by default, except Antivirus and Web Filter logs which are listed in the Antivirus and Web Filter sub-pages.



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

# Event logs

All event logs are available from the log page *Log* > *Event* by default.




- To filter the log messages, enter the desired filter criteria using the date, application name, type, 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<br>• 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 84.
   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 delete unused temporarily data files, click the *Click here* link inside the *Clean up System* 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. |

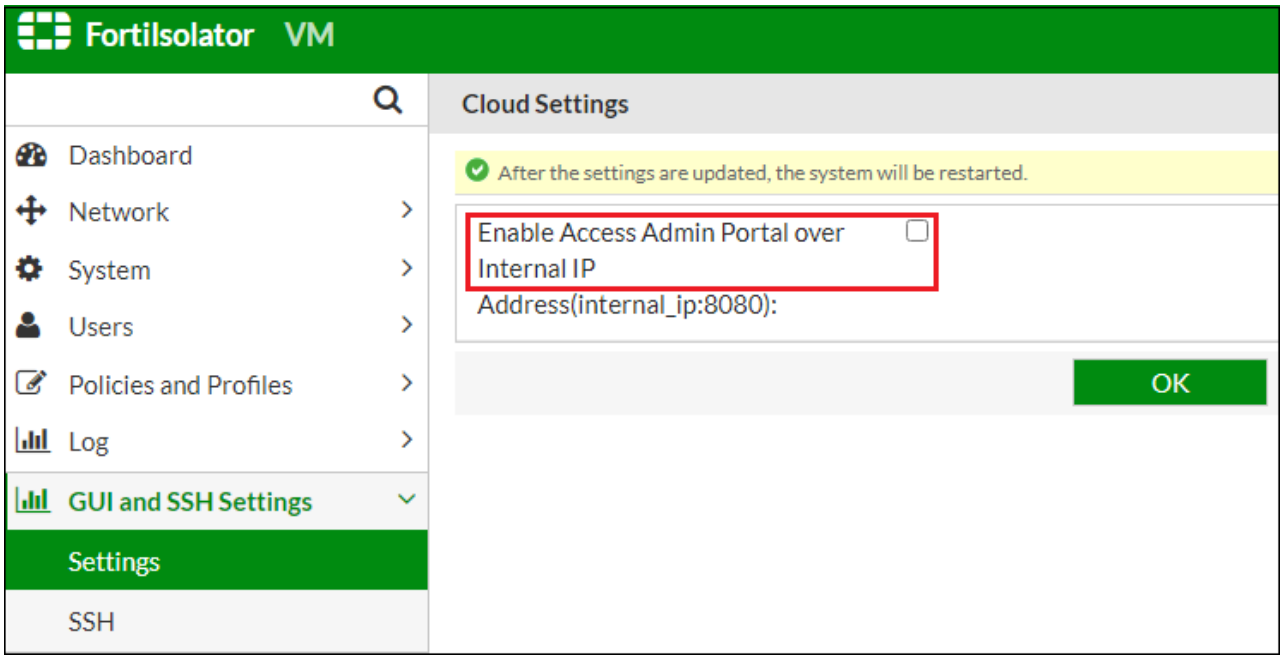
  **c.** Click *Submit*.

# GUI and SSH Settings - NEW

Use the *GUI and SSH Settings* menu to configure FortiIsolator to use internal IP (instead of the management IP) for admin portal and SSH access.

**To enable admin portal access using internal IP:**

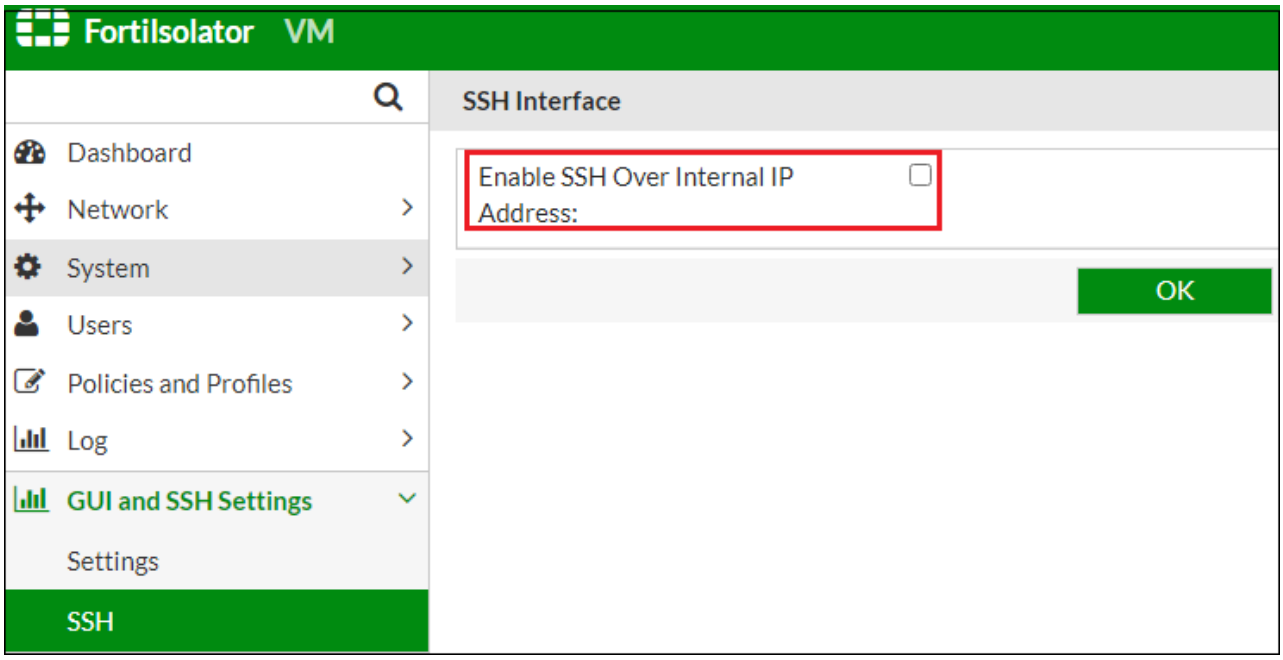
1. Go to the *Settings* tab.
2. Check the *Enable Access Admin Portal over Internal IP Address* option.




3. Click *OK*.

**To enable SSH access using internal IP:**

1. Go to the *SSH* tab.
2. Check the *Enable SSH Over Internal IP Address* option.


FortiIsolator VM
Dashboard
Network
System
Users
Policies and Profiles
Log
GUI and SSH Settings
Settings
SSH
SSH Interface
Enable SSH Over Internal IP Address:
OK

3. Click *OK*.

# Running web browsers through FortiIsolator

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

- IP Forwarding mode
- Proxy mode

## IP Forwarding mode

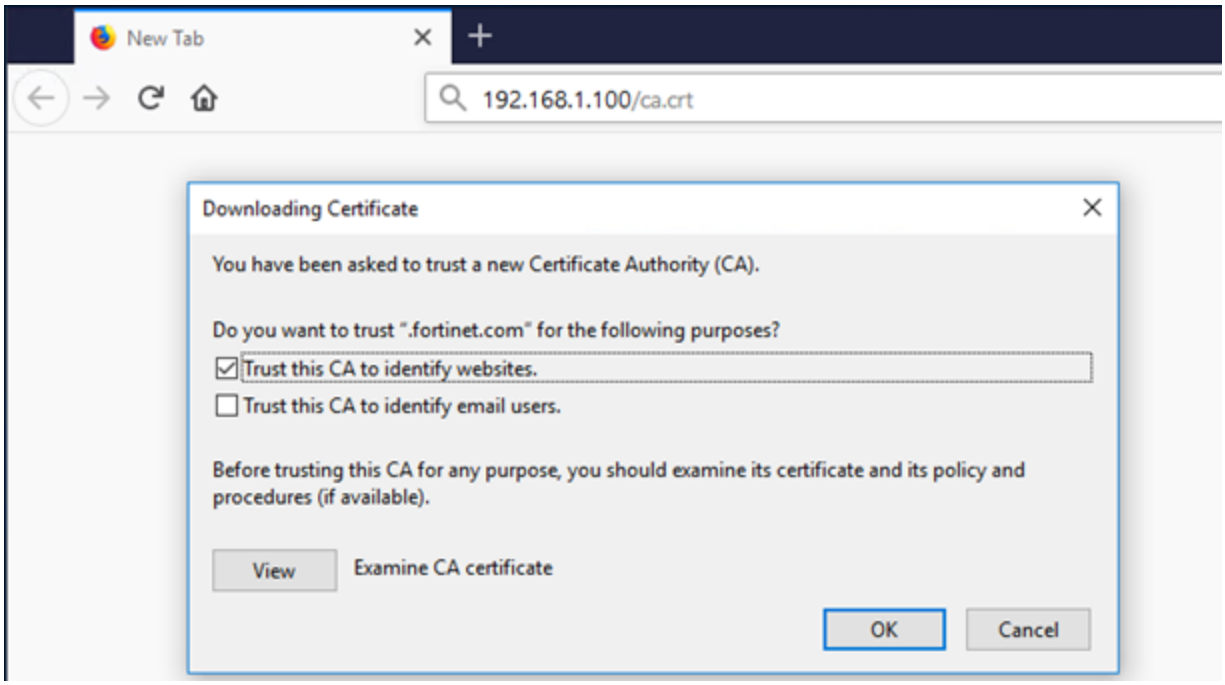
You can configure FortiIsolator to run in IP Forwarding mode using the following types of browsers:


- Using IP Forwarding mode with Mozilla Firefox on page 89
- Using IP Forwarding mode with Google Chrome on page 91
- Using IP Forwarding mode with Internet Explorer on page 96
- Using IP Forwarding mode with Edge on page 100

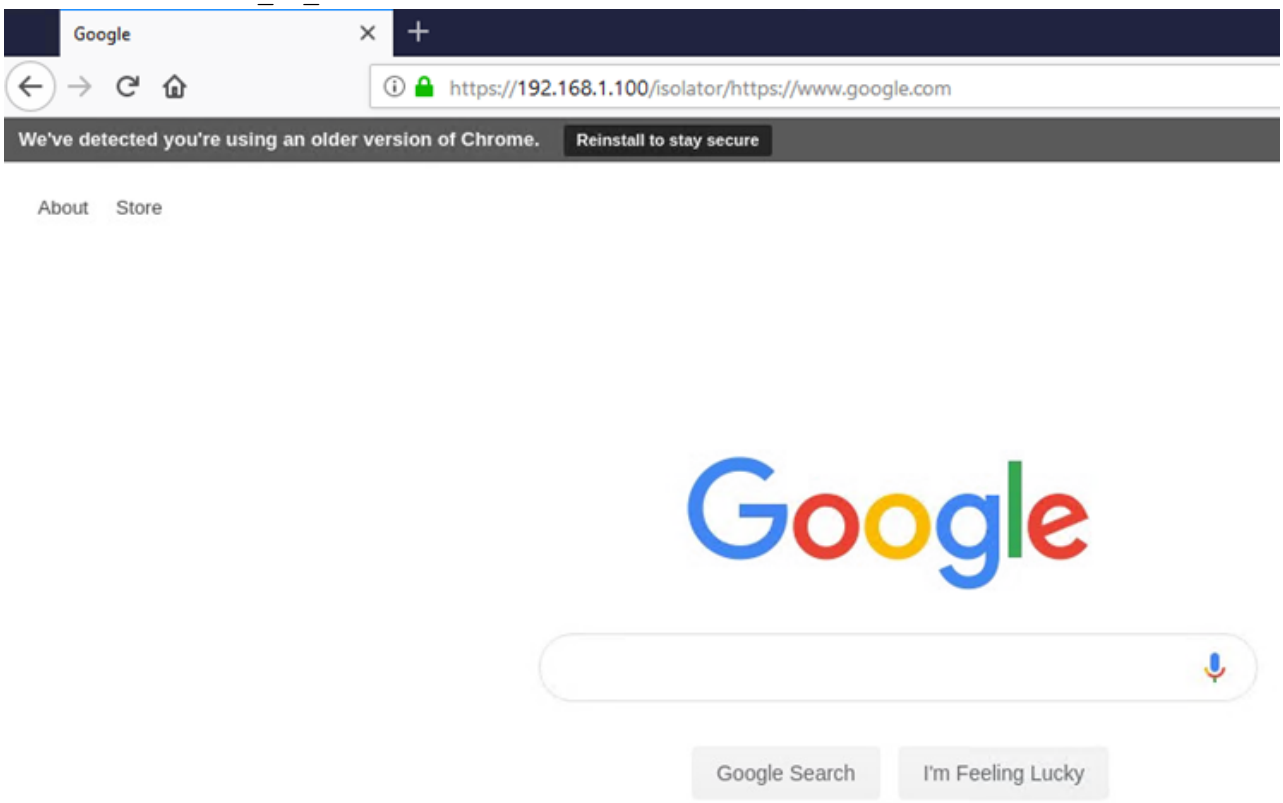

### Using IP Forwarding mode with Mozilla Firefox

#### To configure IP Forwarding mode with Mozilla Firefox:

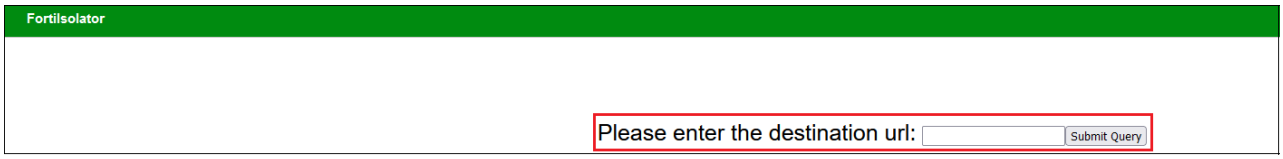
1. Download the FortiIsolator certificate (ca.crt) and import it into the Mozilla Firefox browser:
   a. In the Mozilla Firefox browser address bar, type http://<internal_IP_address>/ca.crt (for example, http://192.168.1.100/ca.crt).
      - where <internal_IP_address> is the IP address of the FortiIsolator internal interface. For example, the IP address of the internal interface that you configured in step 3 of Installing FortiIsolator 1000F.
   b. In the *Downloading Certificate* window, select the *Trust this CA to identify websites* checkbox.
   c. Click *OK*.




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



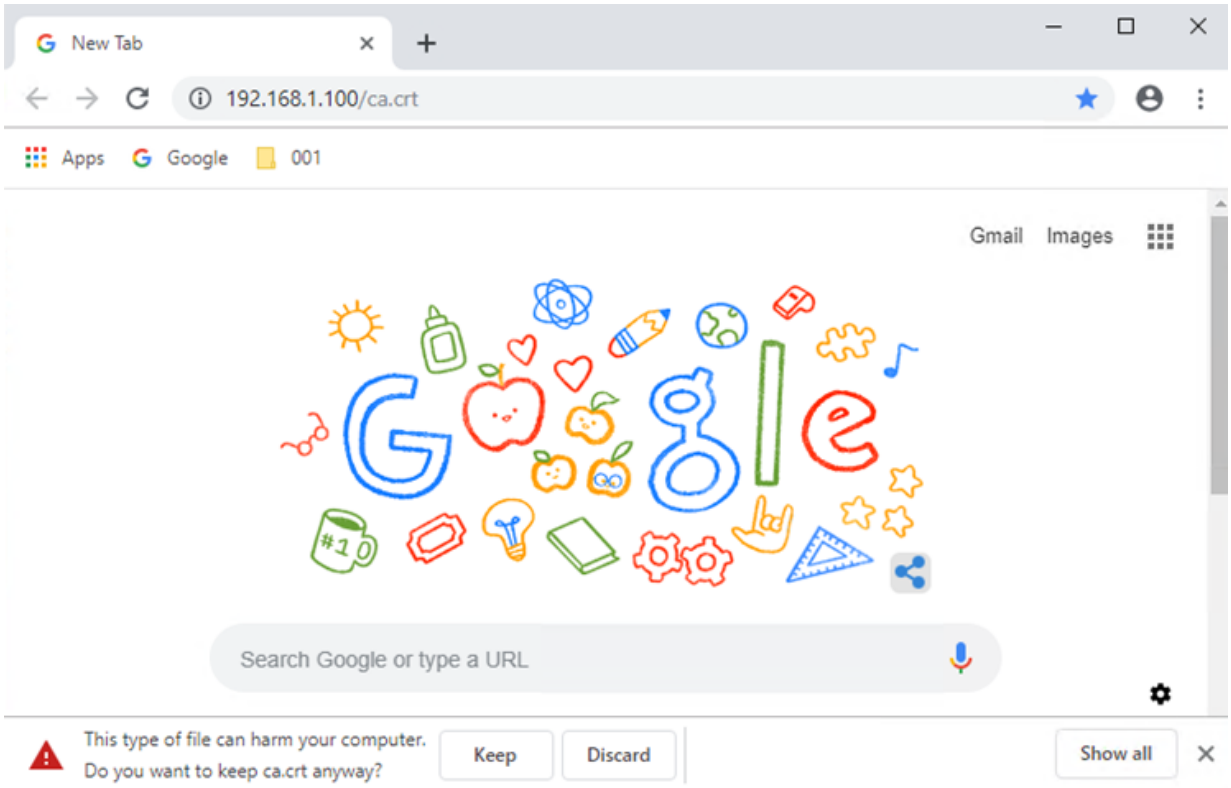
You can also omit the `/isolator/https://www.<website-url>.com` portion when typing the URL in the address bar, in which case you will then be prompted to specify the destination URL of the website to browse.



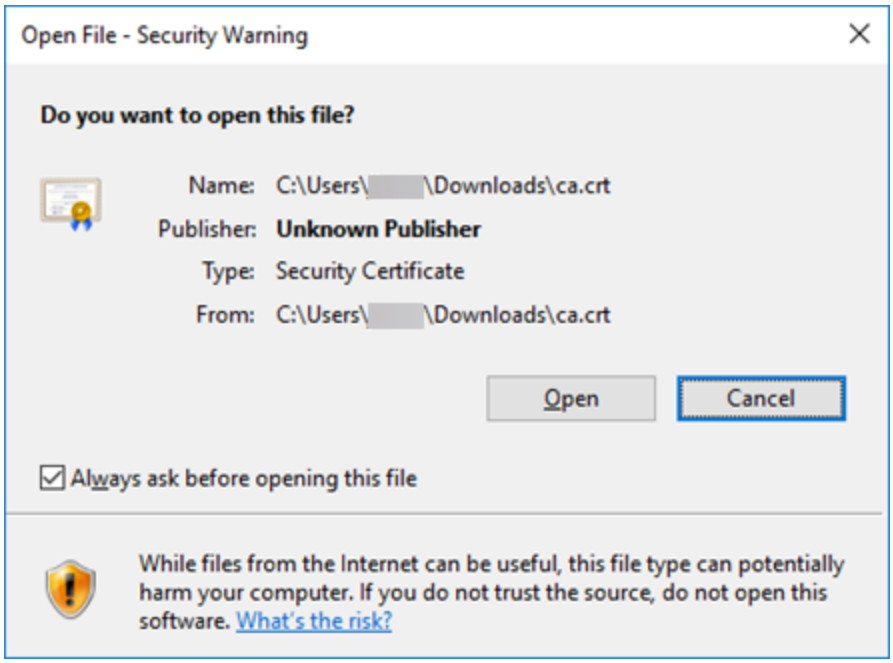

## Using IP Forwarding mode with Google Chrome

### To configure IP Forwarding mode with Google Chrome:

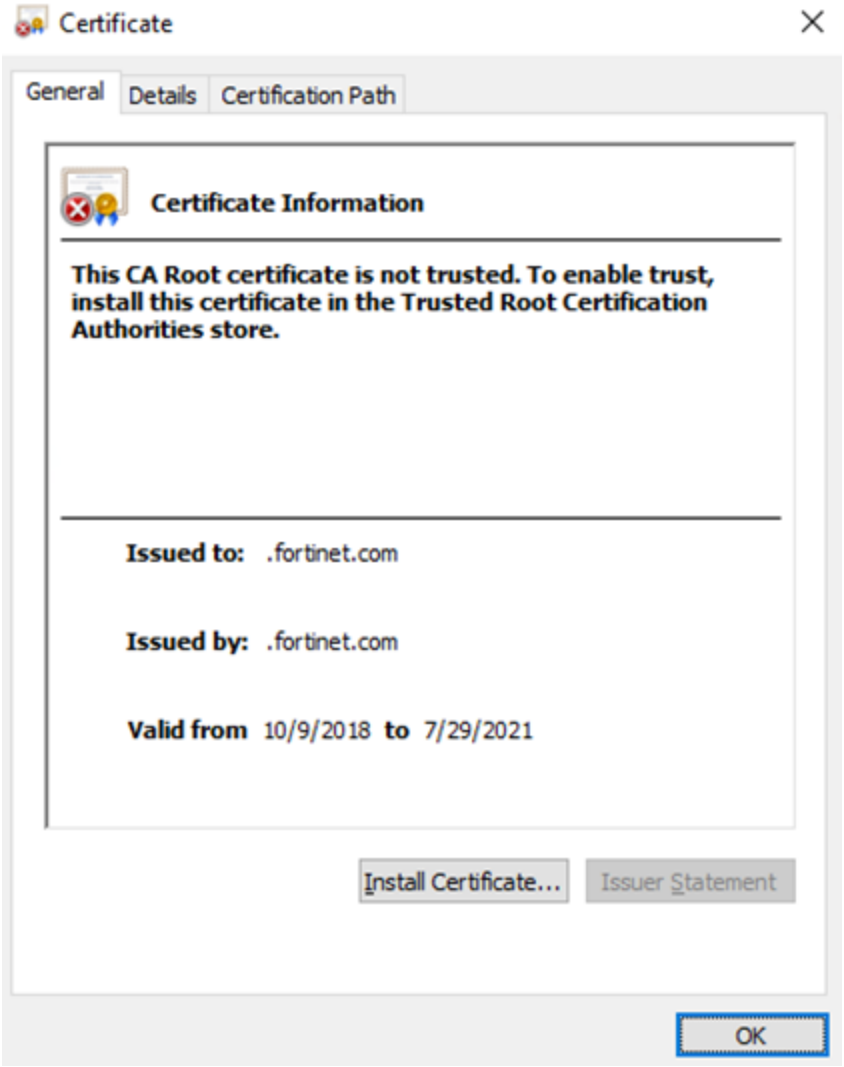
1. Download the FortiIsolator certificate (ca.crt) and import it into your Google Chrome browser:
   a. In the Google Chrome browser address bar, type `http://<internal_IP_address>/ca.crt` (for example, `http://192.168.1.100/ca.crt`).
      - where `<internal_IP_address>` value is the IP address of the FortiIsolator internal interface. For example , the IP address of the internal interface that you configured in step 3 of Installing FortiIsolator 1000F.
   b. In the security warning at the bottom of the browser, click *Keep* to download the certificate.



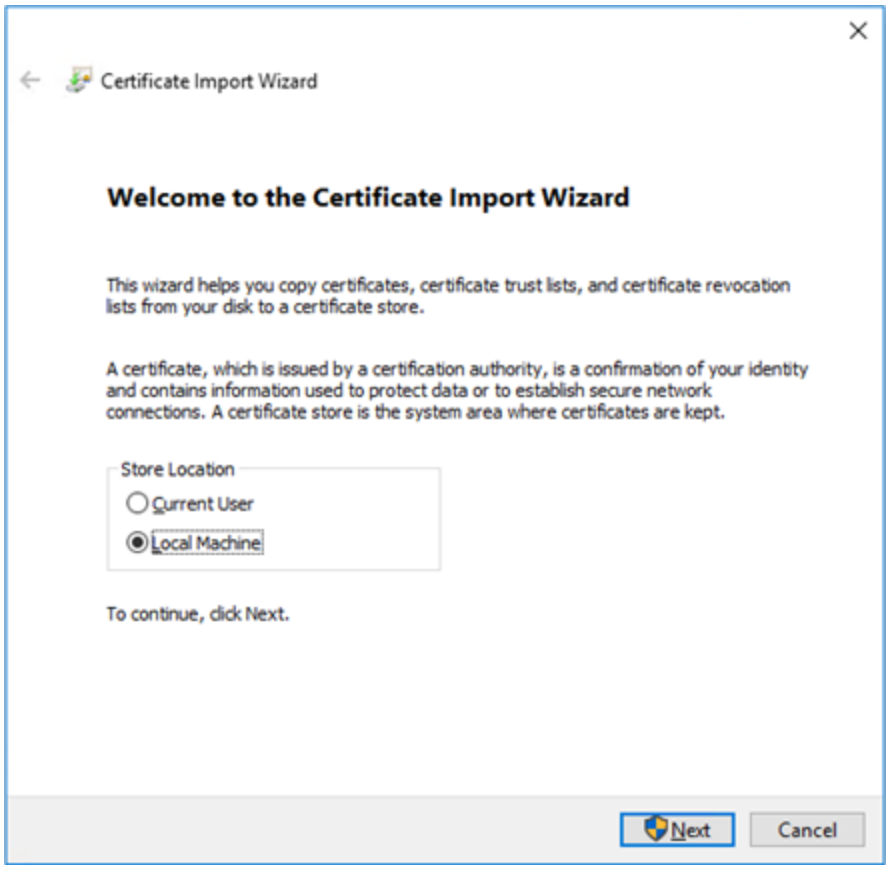
**c.** Click *Open* to import the `ca.crt` certificate into Google Chrome.



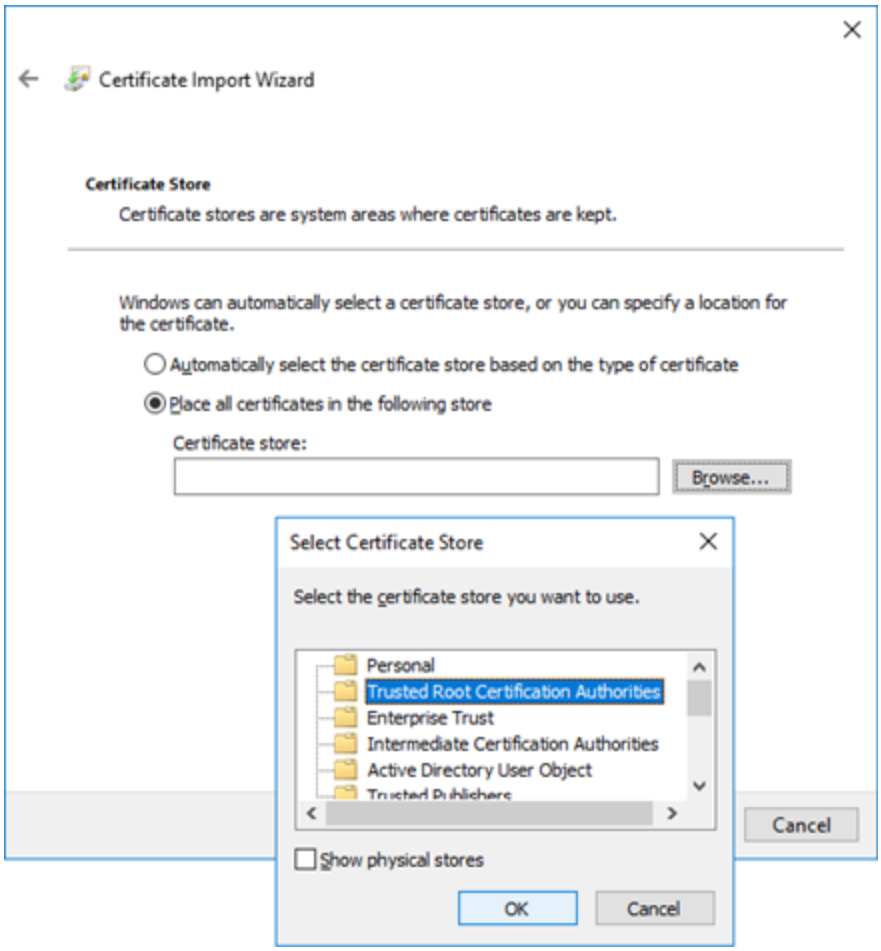
**d.** Click *Install Certificate*.



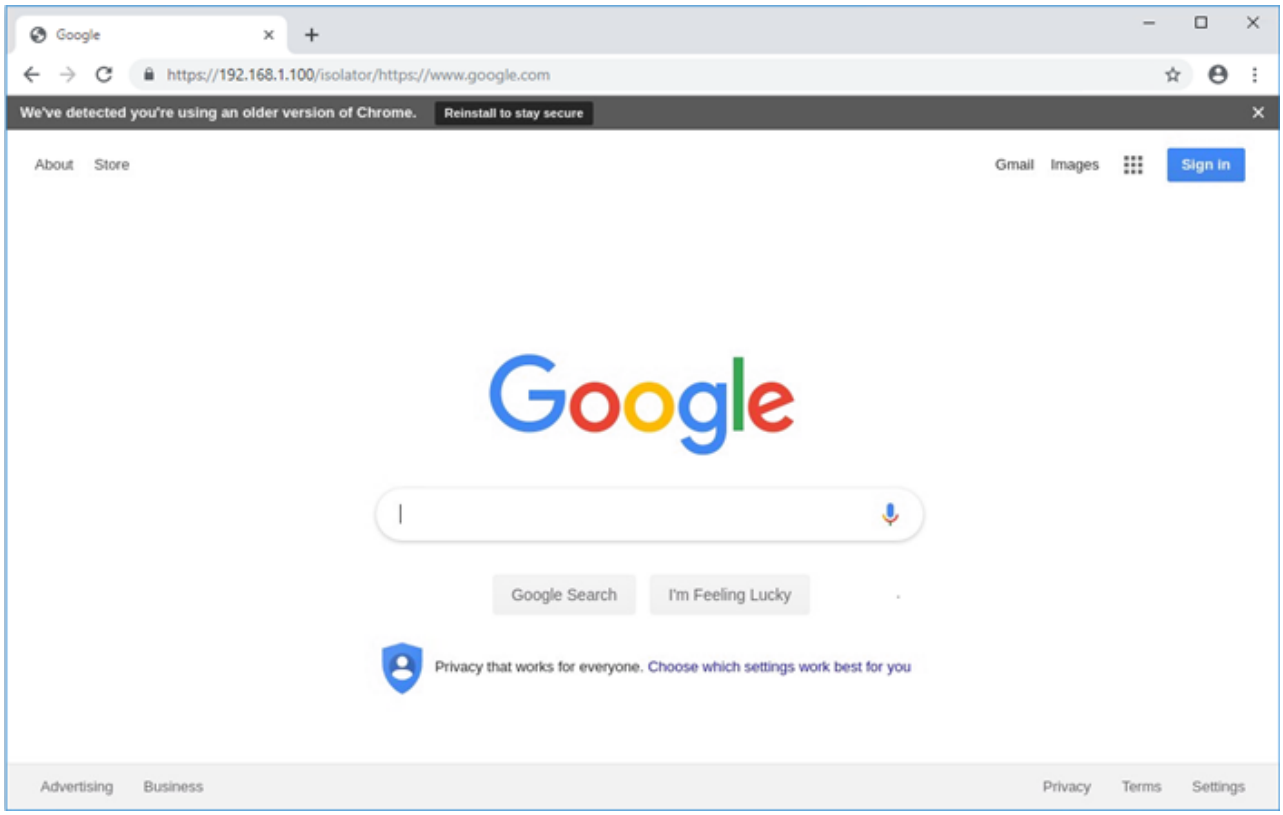
**e.** Select *Local Machine*, and click *Next*.



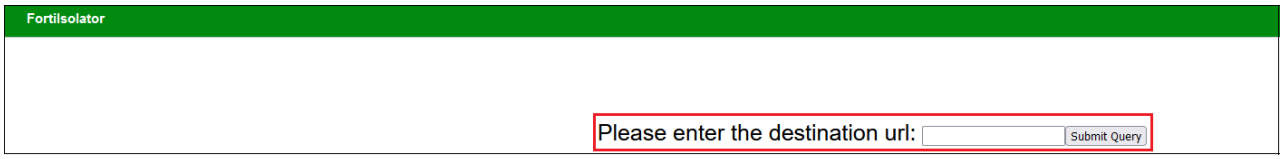
**f.** Select *Trusted Root Certification Authorities*, and click *OK*.




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




You can also omit the `/isolator/https://www.<website-url>.com` portion when typing the URL in the address bar, in which case you will then be prompted to specify the destination URL of the website to browse.

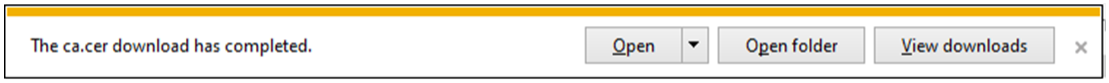



## Using IP Forwarding mode with Internet Explorer

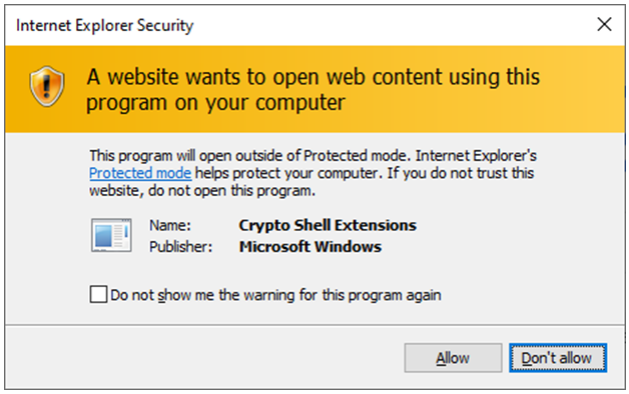
### To configure IP Forwarding mode with Internet Explorer:

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. For example , the IP address of the internal interface that you configured in step 3 of Installing FortiIsolator 1000F.
   b. In the security warning at the bottom of the browser, click *Save* to download the certificate.

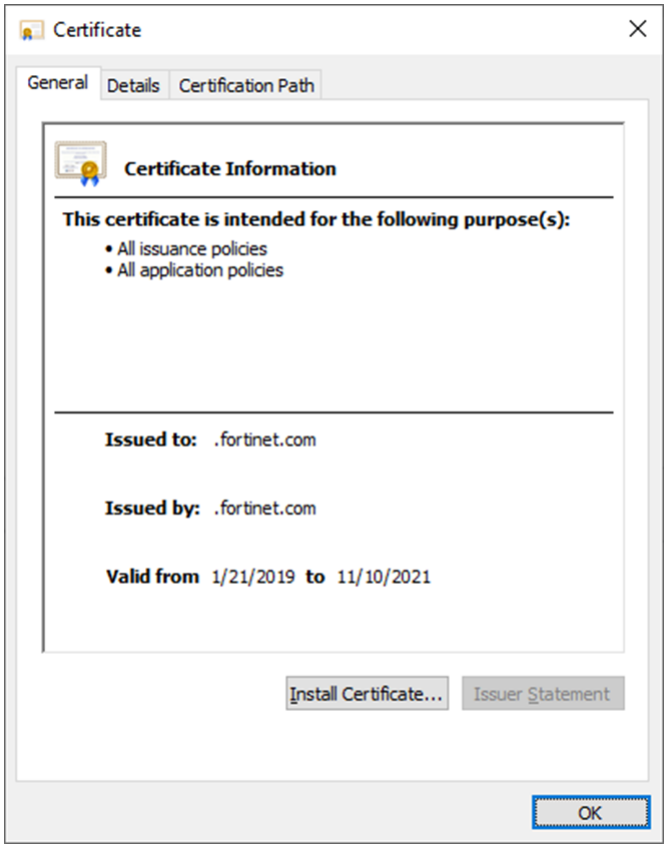
**c.** Click *Open* to import the ca.crt certificate into Internet Explorer.



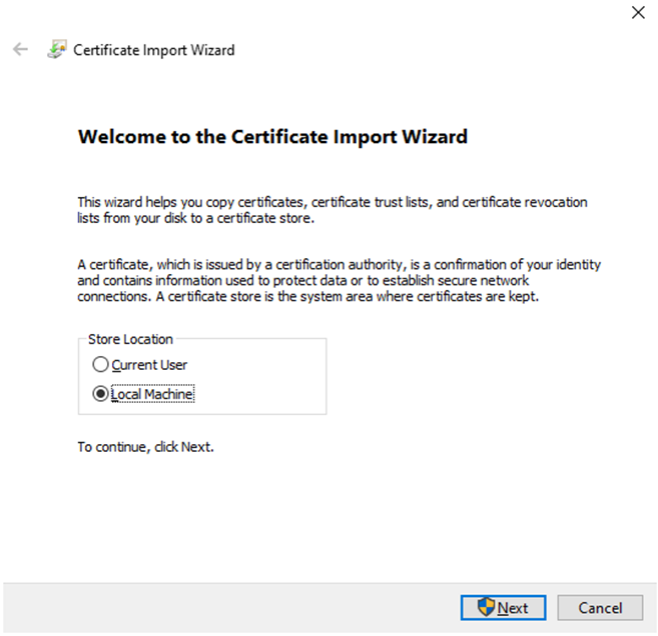

**d.** Click *Allow* to install certificate.



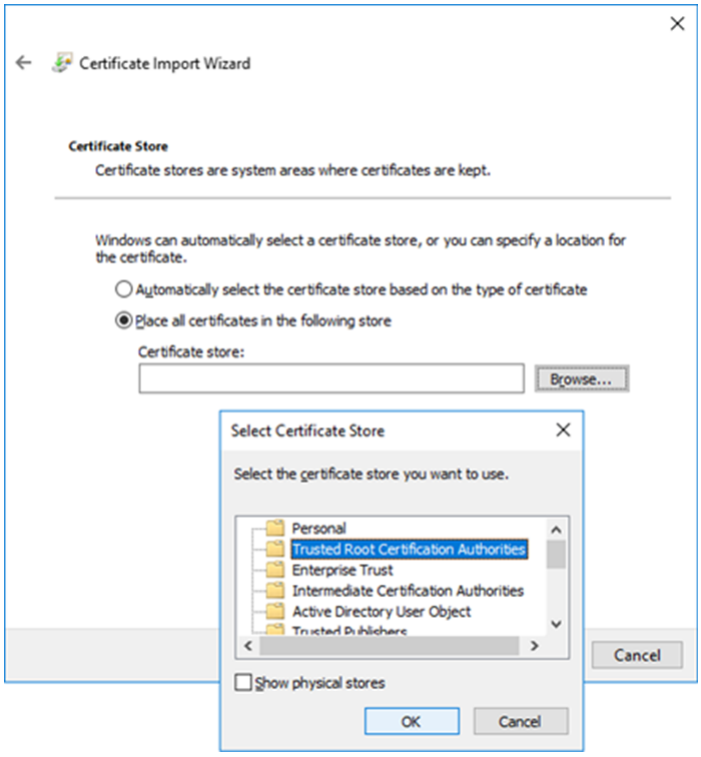

**e.** Click *Install Certificate*.



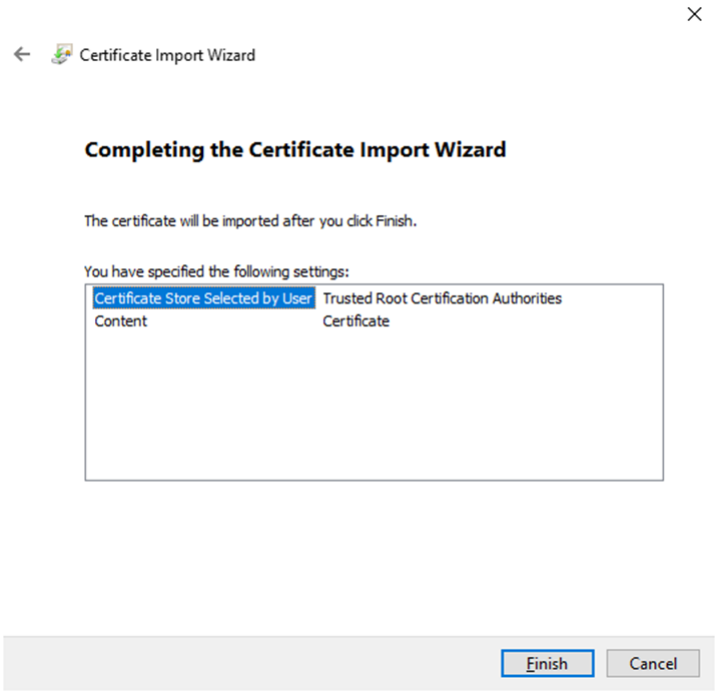
**f.** Select *Local Machine*, and click *Next*.



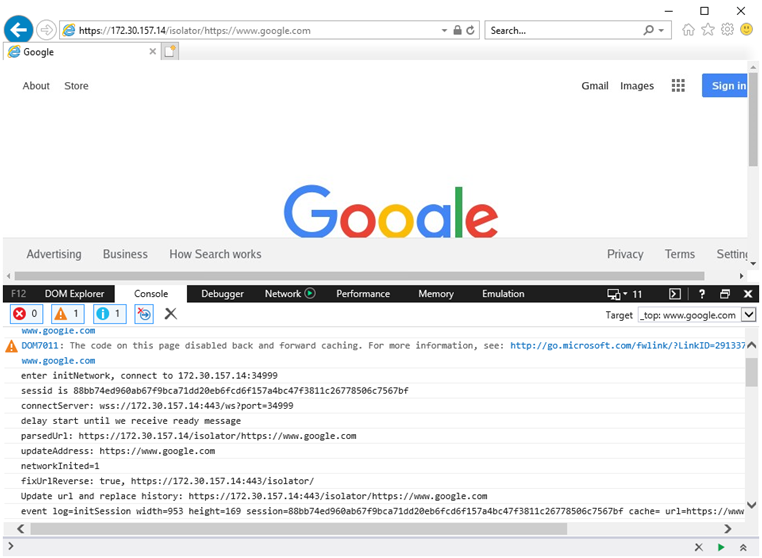

**g.** Select *Trusted Root Certification Authorities*, and click *OK*.



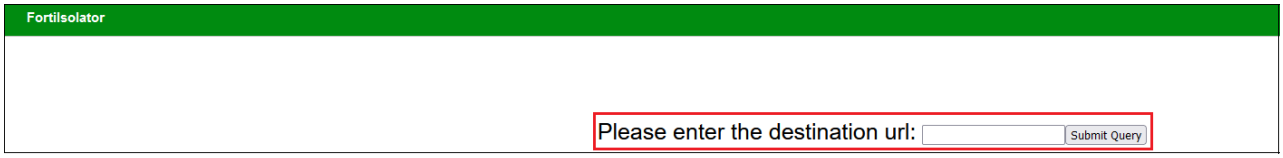
**h.** Completing the Certificate Import Wizard.




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.




You can also omit the `/isolator/https://www.<website-url>.com` portion when typing the URL in the address bar, in which case you will then be prompted to specify the destination URL of the website to browse.

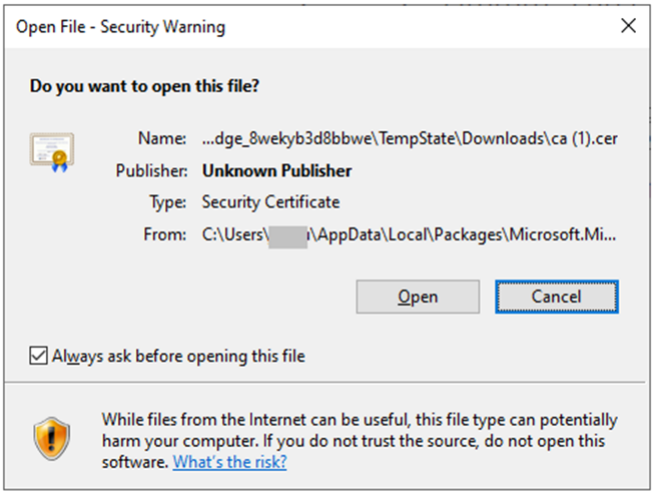


# Using IP Forwarding mode with Edge

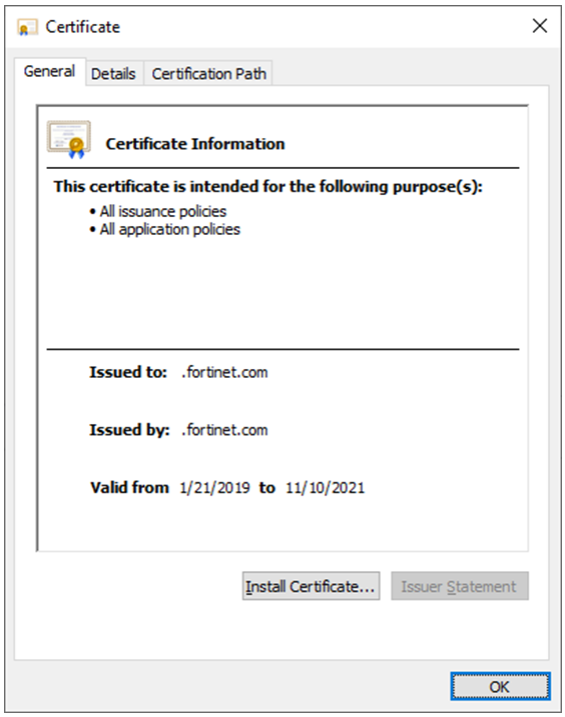
## To configure IP Forwarding mode with Edge browser:

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. For example , the IP address of the internal interface that you configured in step 3 of Installing FortiIsolator 1000F.
   b. In the security warning at the bottom of the browser, click *Save* to download the certificate.

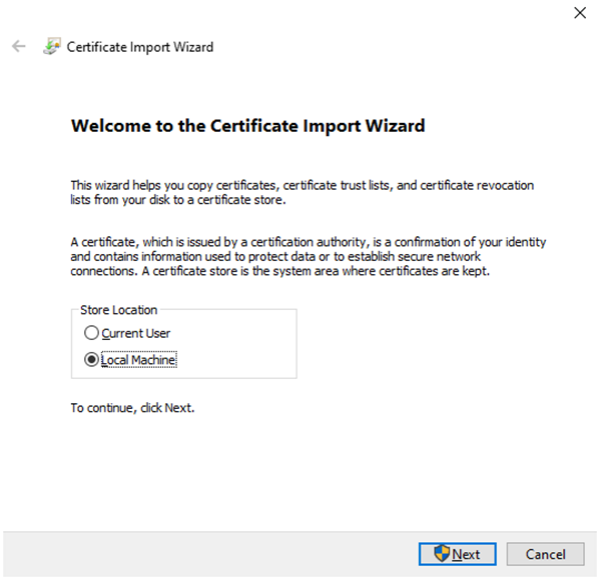

   c. Click *Open* to import the `ca.crt` certificate into Edge.



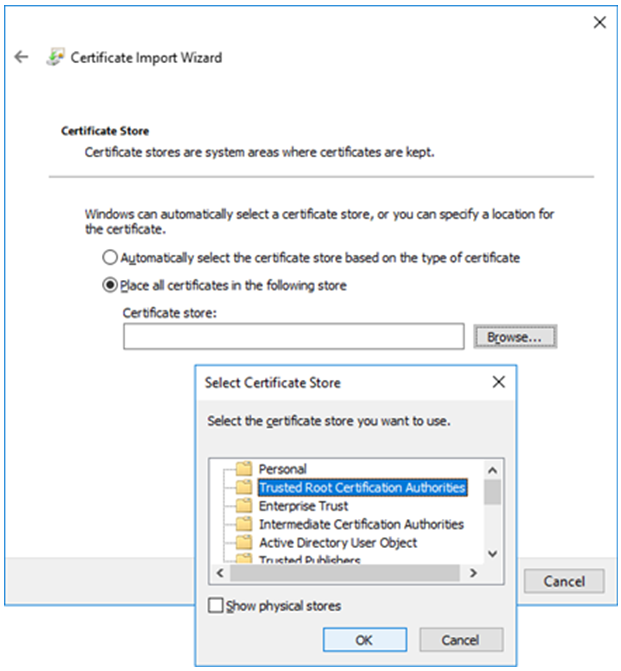
**d.** Click *Install Certificate*.



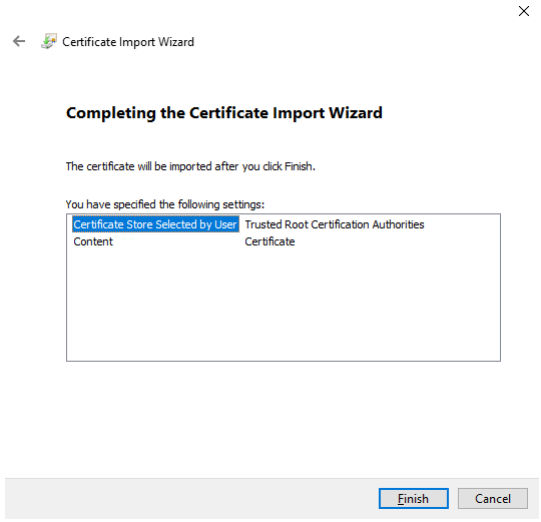

**e.** Select *Local Machine*, and click *Next*.



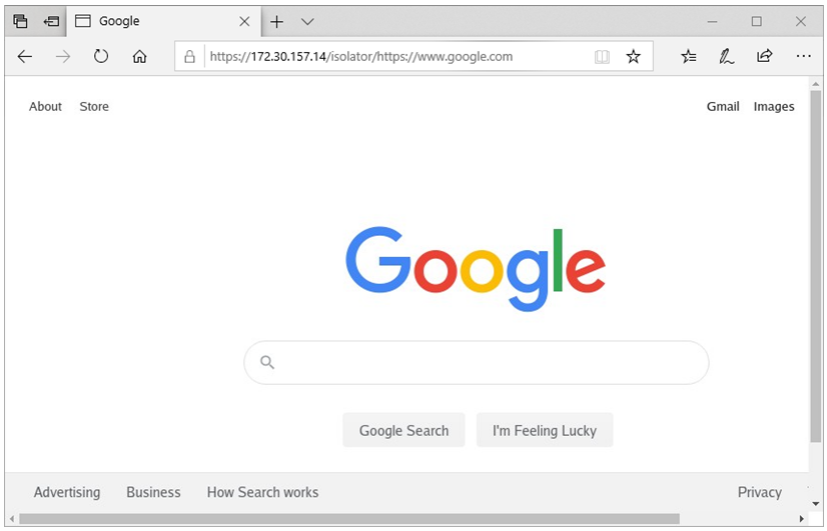
**f.** Select *Trusted Root Certification Authorities*, and click *OK*.



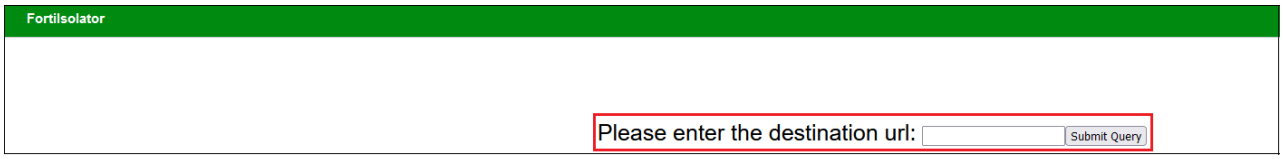

**g.** Completing the Certificate Import Wizard.




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




You can also omit the `/isolator/https://www.<website-url>.com` portion when typing the URL in the address bar, in which case you will then be prompted to specify the destination URL of the website to browse.




# Proxy mode

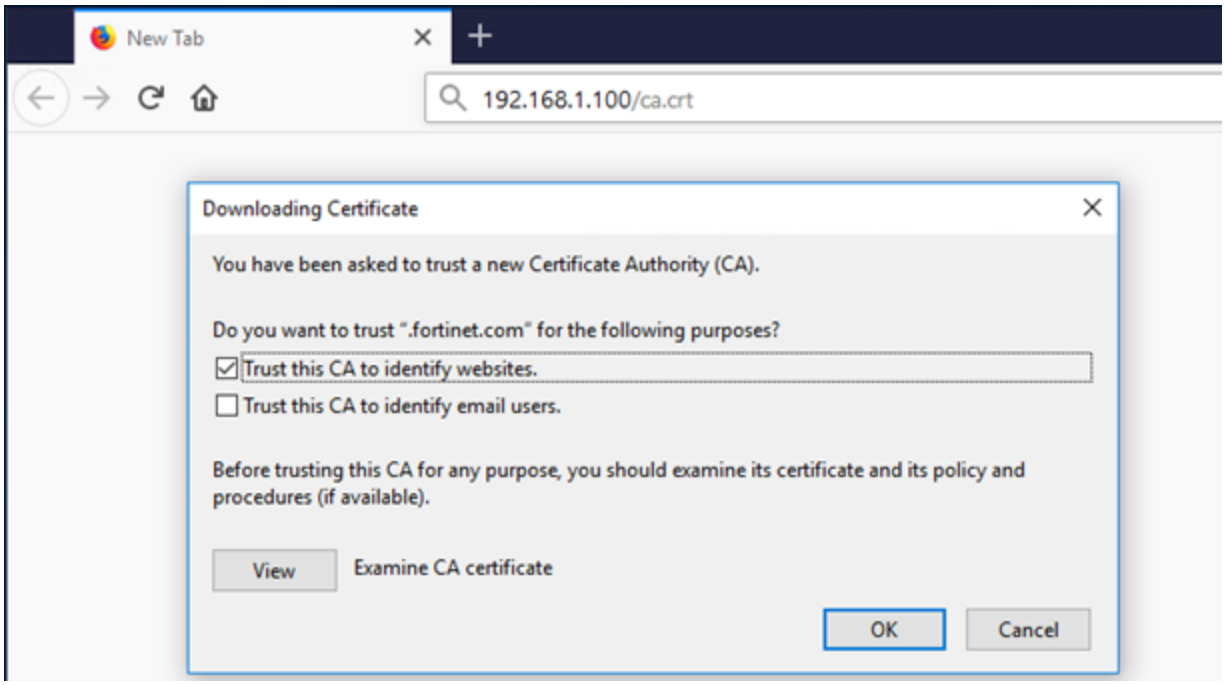
You can configure FortiIsolator to run in Proxy mode using the following types of browsers:

- Using proxy mode with Mozilla Firefox on page 103
- Using proxy mode with Google Chrome on page 107
- Using proxy mode with Internet Explorer on page 115
- Using proxy mode with Edge on page 119

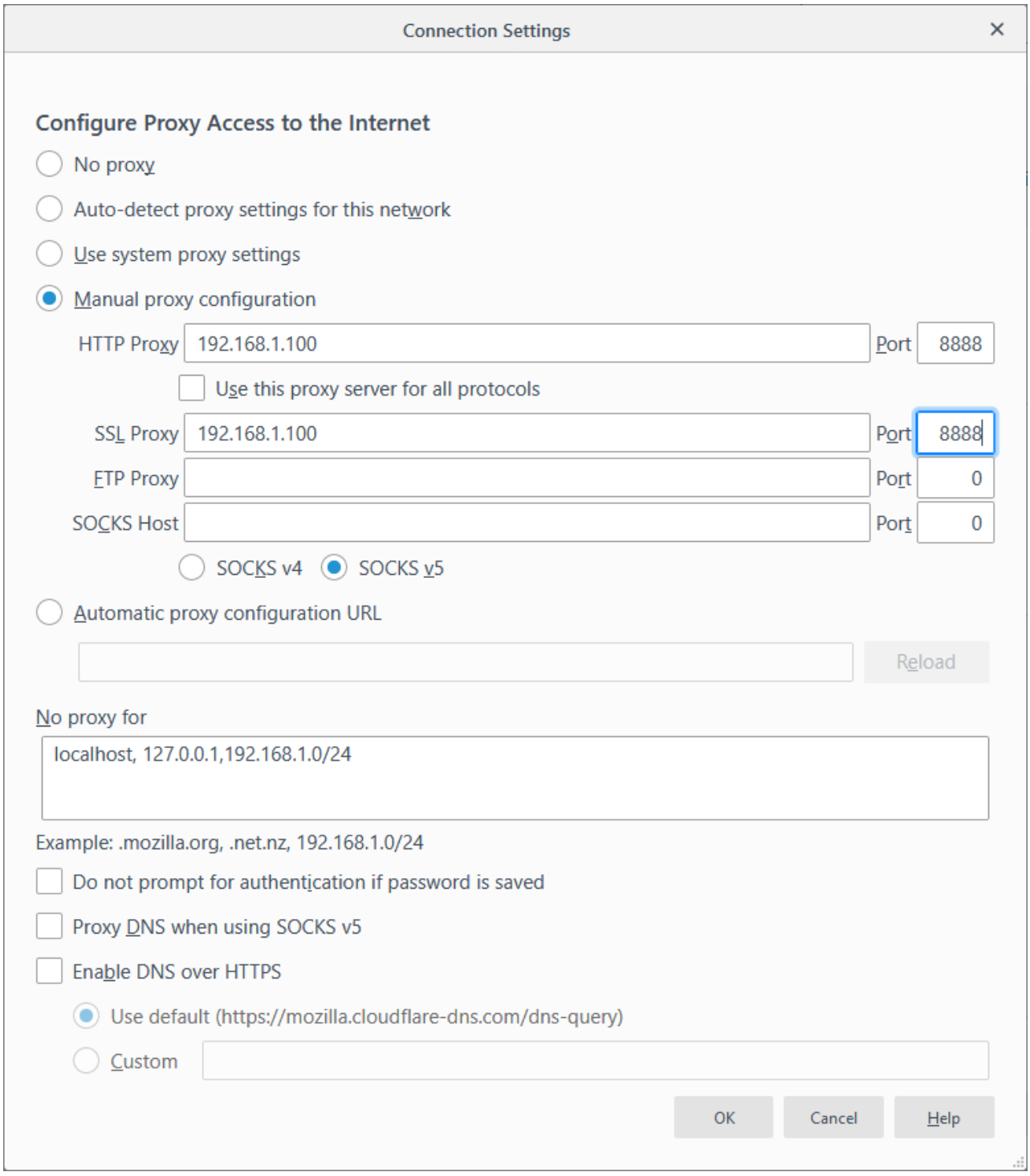
## Using proxy mode with Mozilla Firefox

### 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. For example, the IP address of the internal interface that you configured in step 3 of Installing FortiIsolator 1000F.
   b. In the *Downloading Certificate* window, select the *Trust this CA to identify websites* checkbox.
   c. Click *OK*.



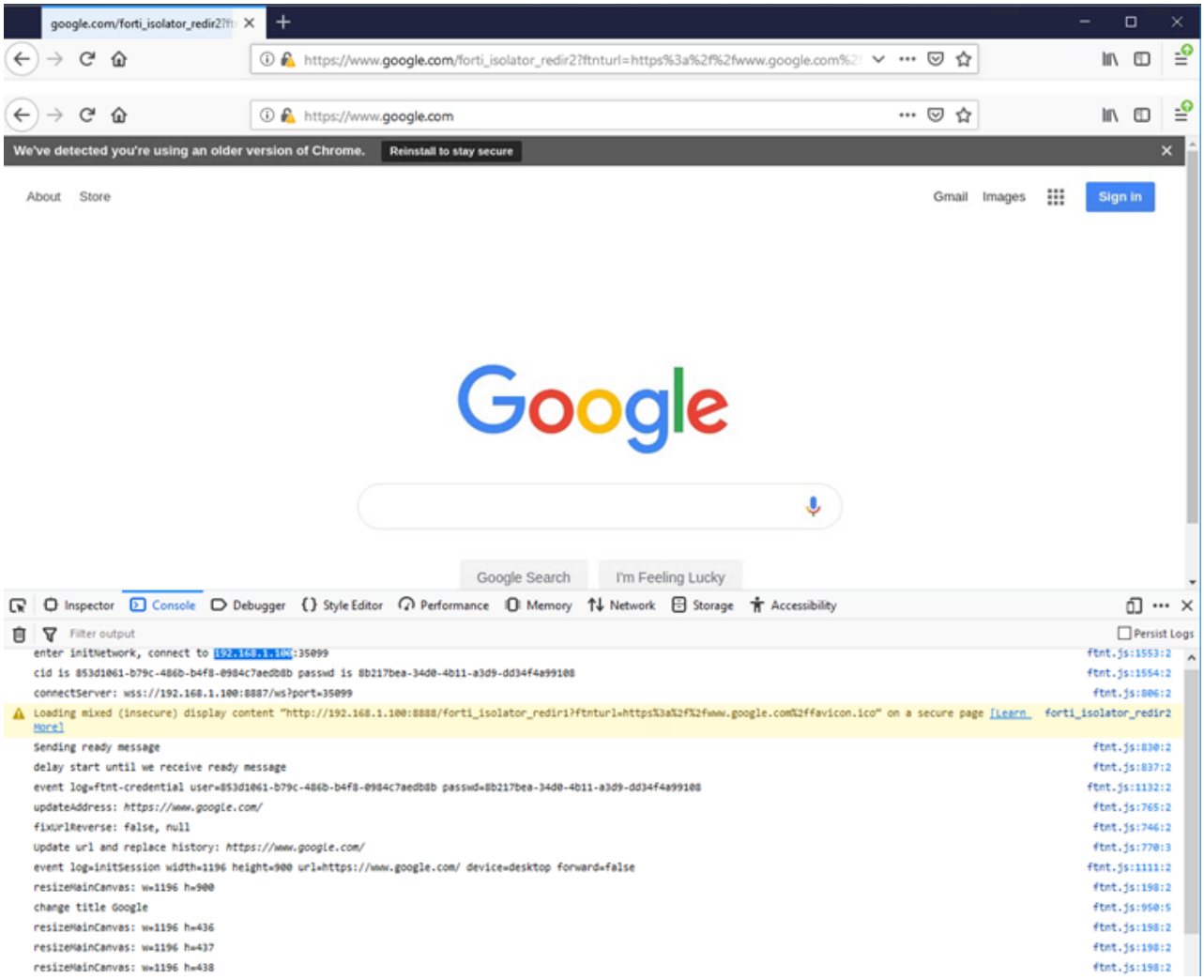

2. Open the Mozilla Firefox browser.
3. In the menu, click *Options*.
4. Click *General*.
5. In the *Network Settings* section, click *Settings*.
6. In the *Connection Settings* window, select *Manual proxy configuration*, and enter the following settings (values shown here are examples):
   - **HTTP Proxy**: 192.168.1.100, **Port**: 8888
   - **SSL Proxy**: 192.168.1.100, **Port**: 8888
   - **No Proxy for**: “localhost, 127.0.0.1,<*internal_IP_address*>/24”, where <*internal_IP_address*> is the IP address of the FortiIsolator internal interface. For example , the IP address of the internal interface that you configured in step 3 of Installing FortiIsolator 1000F.
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:

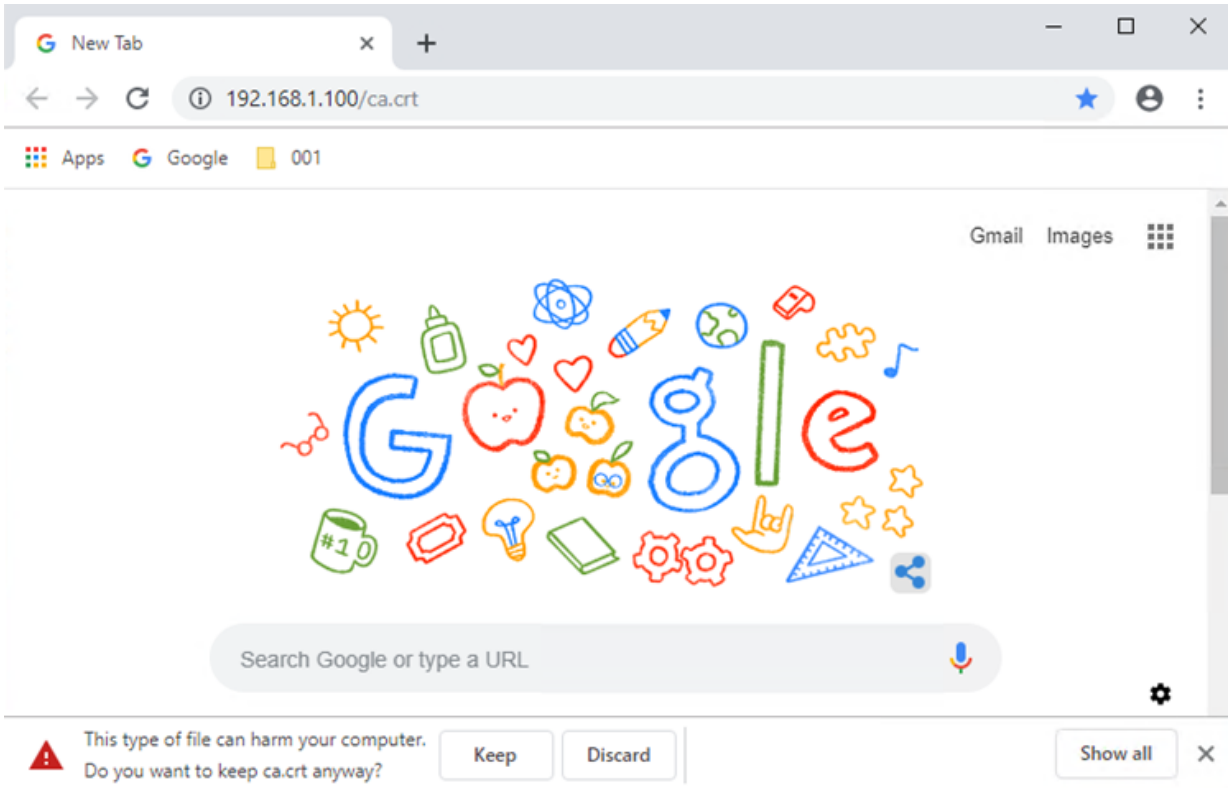
1. In the Mozilla Firefox browser, type `https://www.google.com`.
   The URL redirects the browser to forti_isolator for a short period of time. For example, `https://www.google.com/forti_isolator_redir2?ftnturl=https%3a%2f%2fwww.google.com%2f&ftntcid=5f4084e8-7978-4c89-97c5-31ef3640600c&ftntpasswd=35026d03-9a1c-42e9-959e-fca18d67e4c0`. 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).



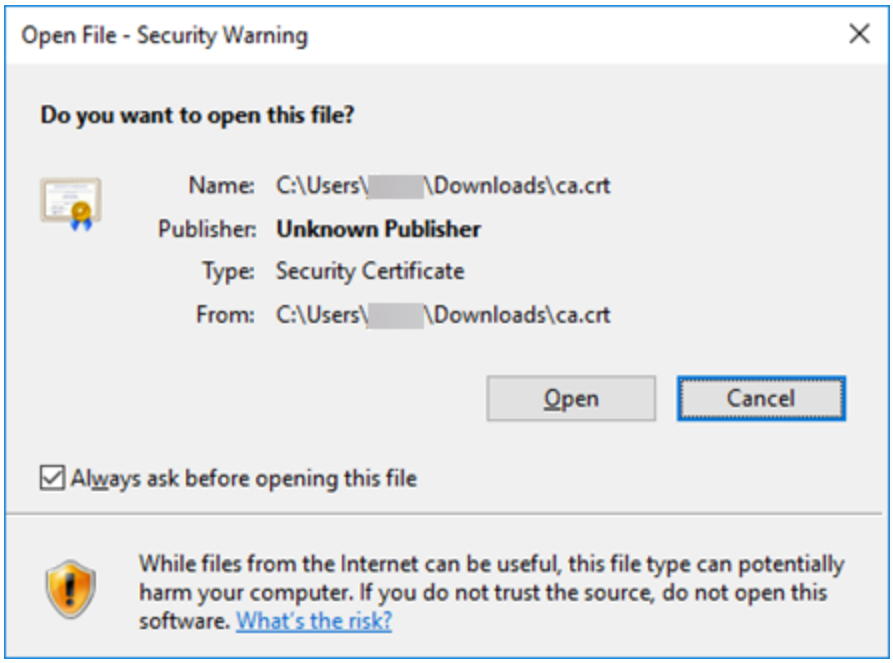
# Using proxy mode with Google Chrome

## To configure proxy mode with Google Chrome:

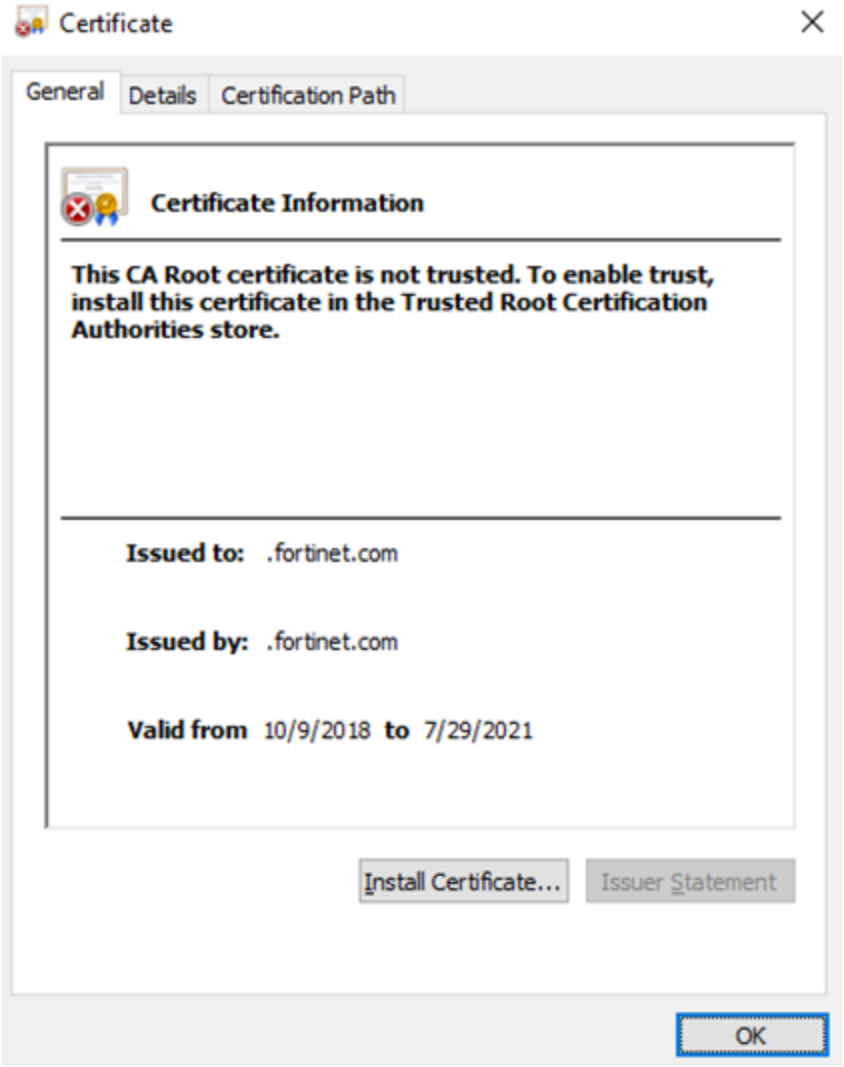
1. Download the FortiIsolator certificate (`ca.crt`) and import it into your Google Chrome browser:
   a. In the Google Chrome browser address bar, type `http://<internal_IP_address>/ca.crt` (for example, `http://192.168.1.100/ca.crt`).
      - where `<internal_IP_address>` value is the IP address of the FortiIsolator internal interface. For example , the IP address of the internal interface that you configured in step 3 of Installing FortiIsolator 1000F.
   b. In the security warning at the bottom of the browser, click *Keep* to download the certificate.



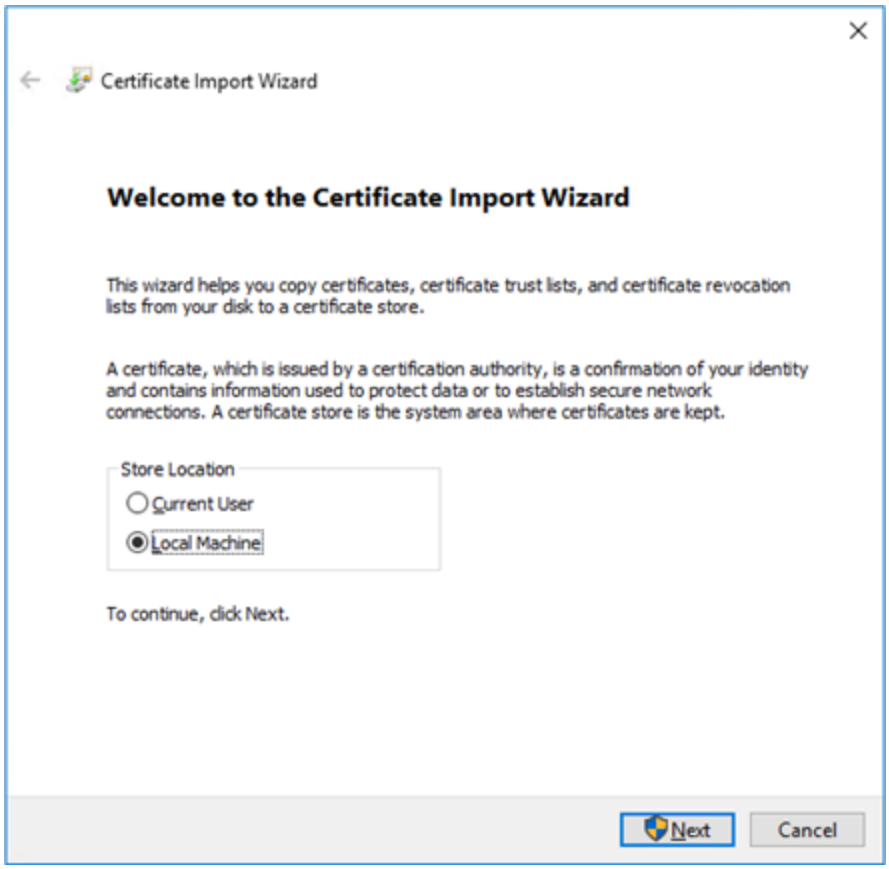
**c.** Click *Open* to import the `ca.crt` certificate into Google Chrome.



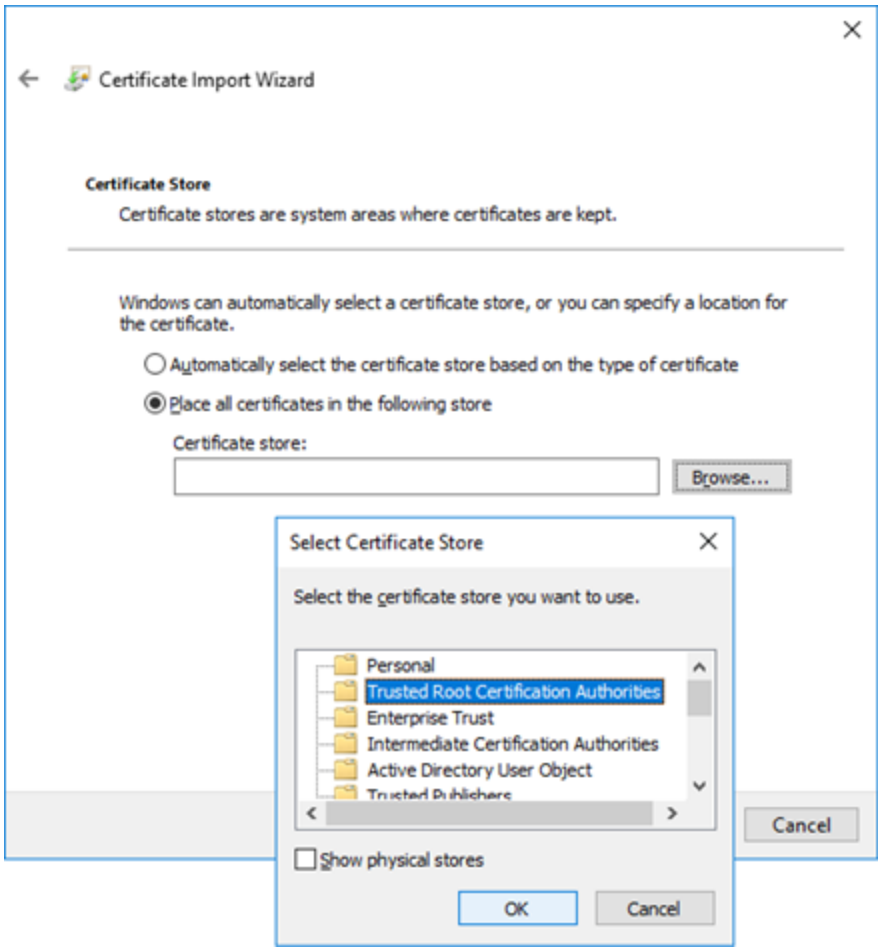
**d.** Click *Install Certificate*.



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

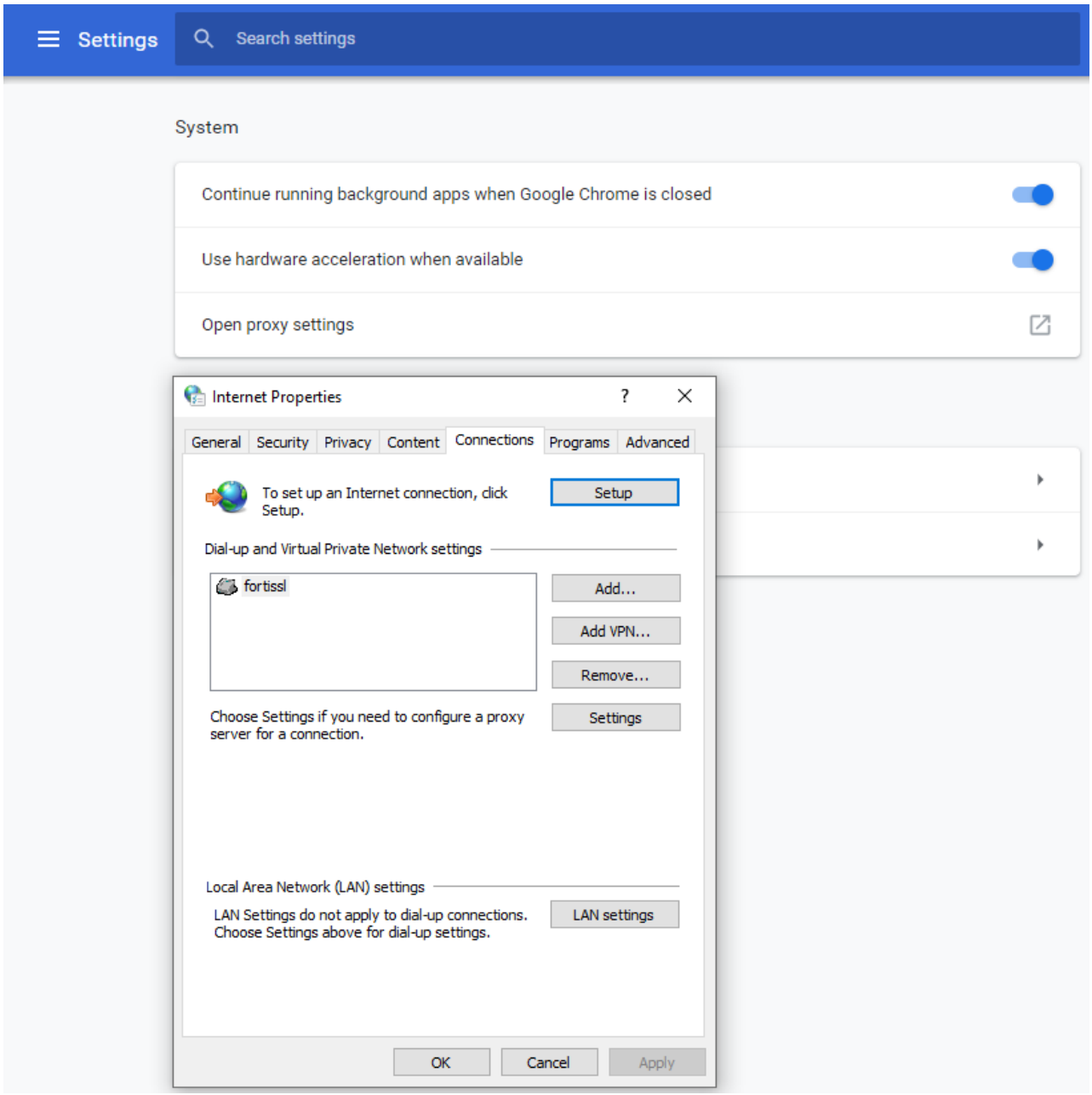


**f.** Select *Trusted Root Certificate Authorities*, and click *OK*.

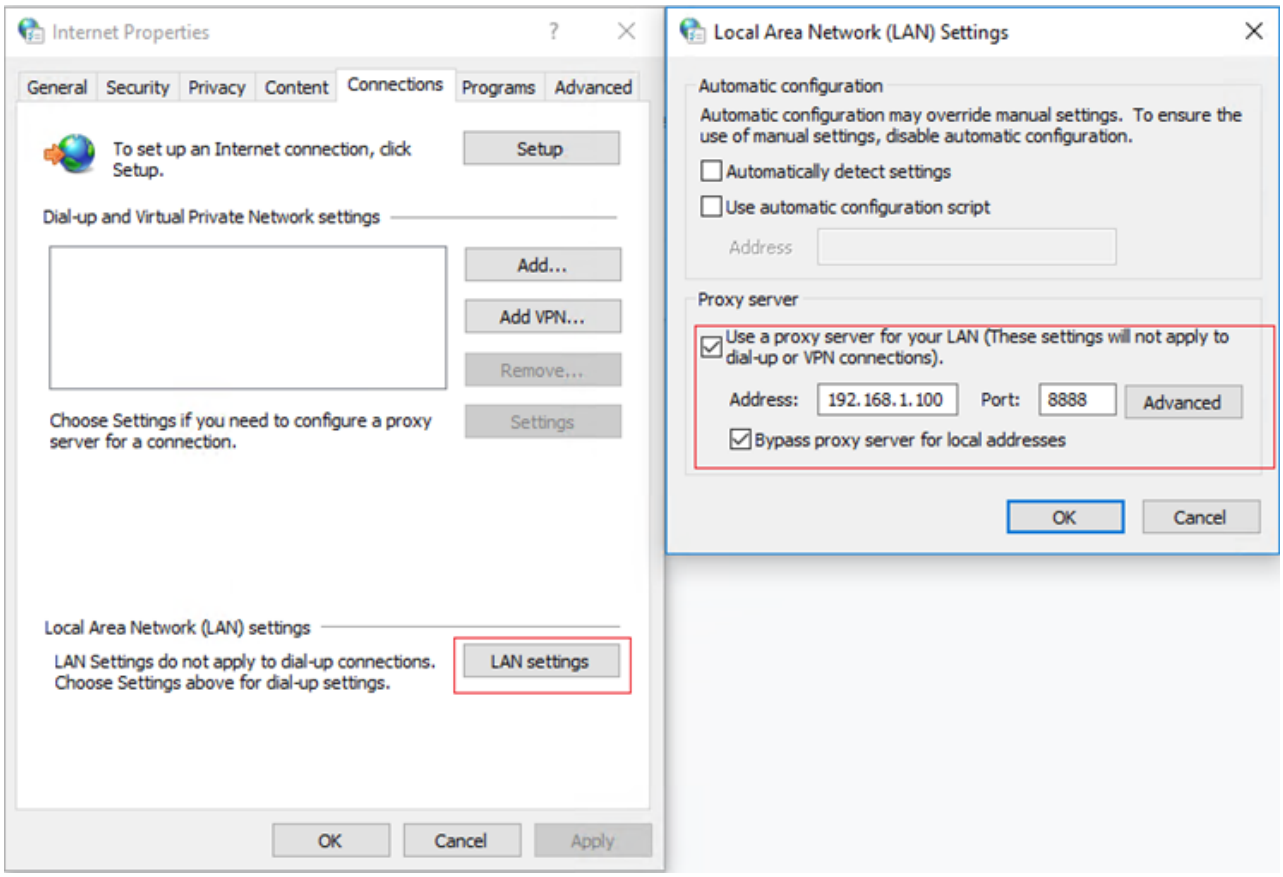



**2.** Open the Google Chrome browser.

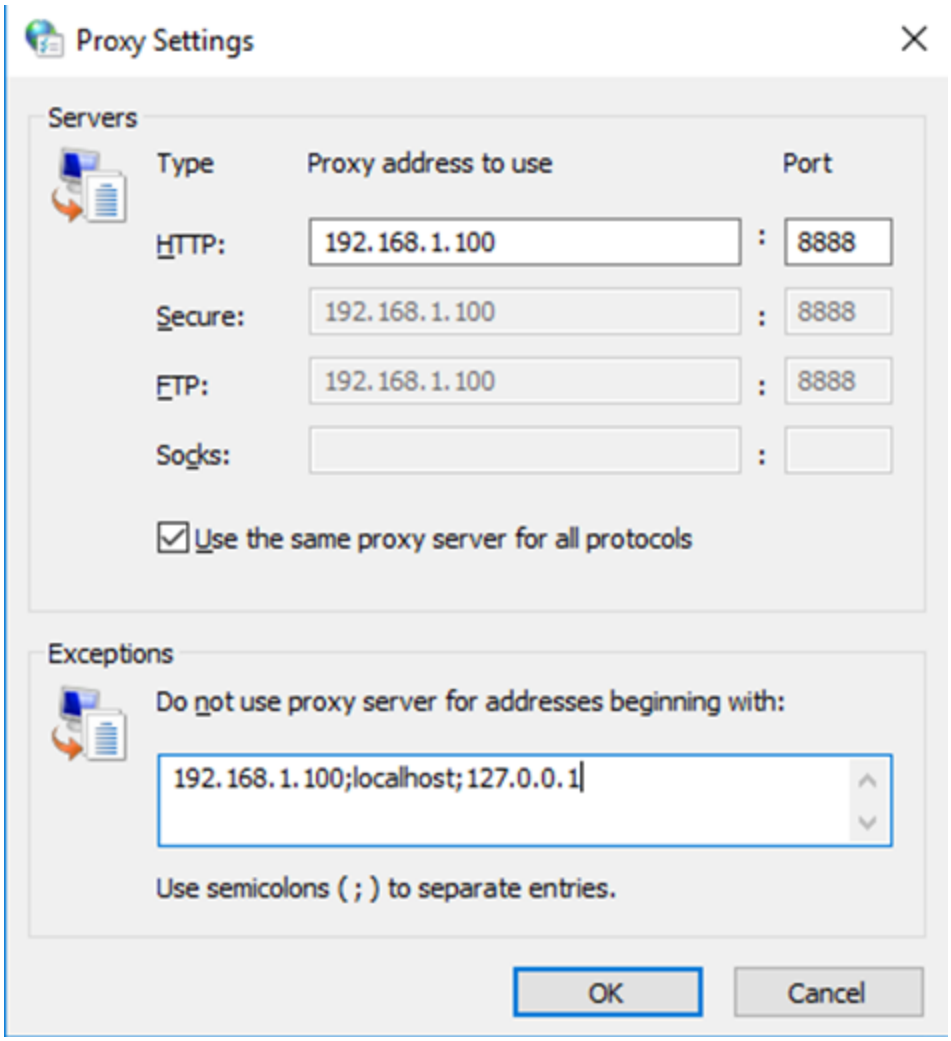
3. In the menu, click *Settings*.




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




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



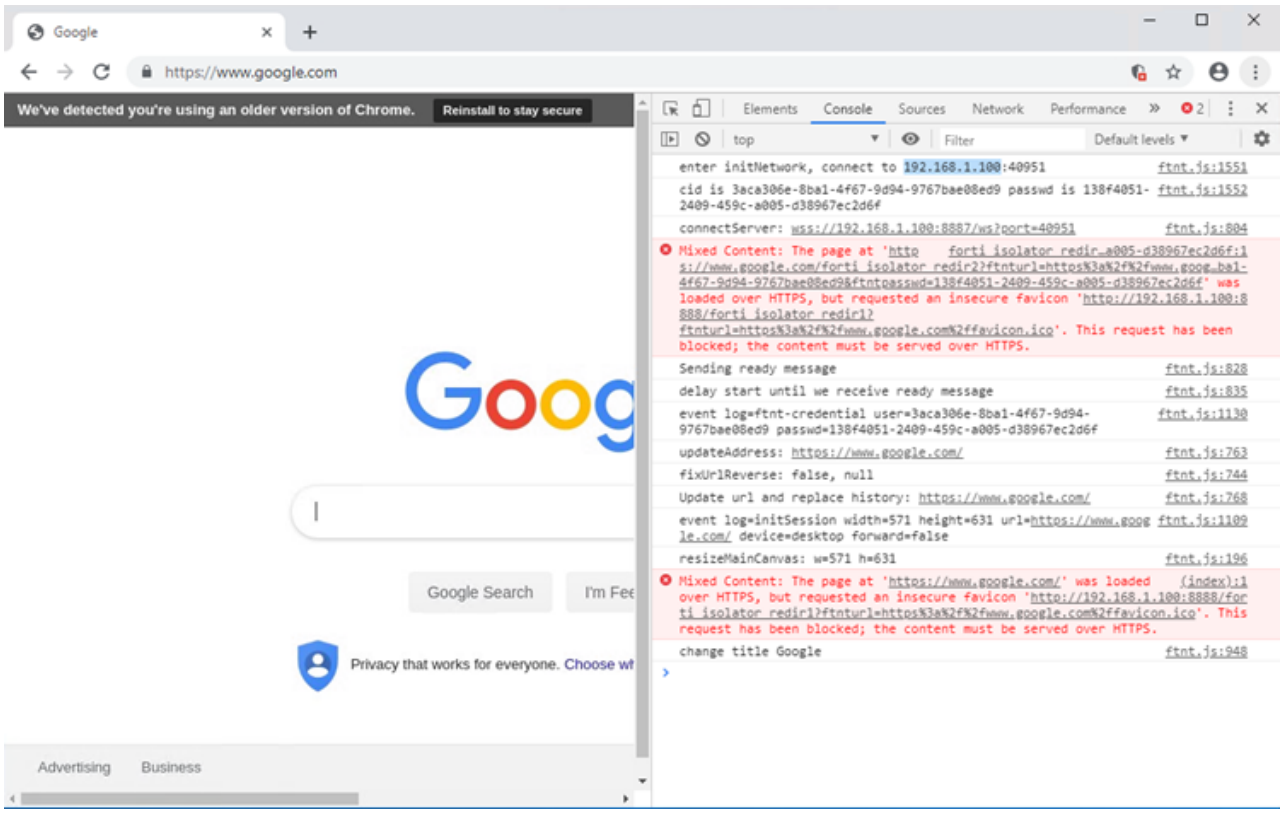

11. Click *OK* to accept the settings in all windows.

## Verifying 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).



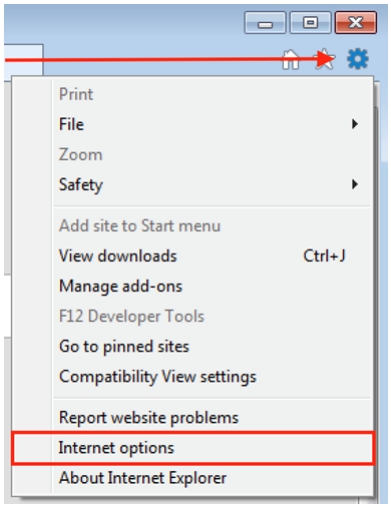

## Using proxy mode with Internet Explorer

### Pre-requisites:

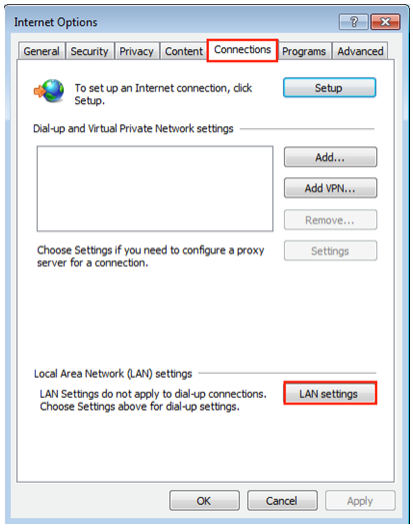
Please follow step 1 in Using IP Forwarding mode with Internet Explorer on page 96 to install FortiIsoaltor `ca.crt` certificate prior to using proxy mode.

### To configure proxy mode with Internet Explorer:

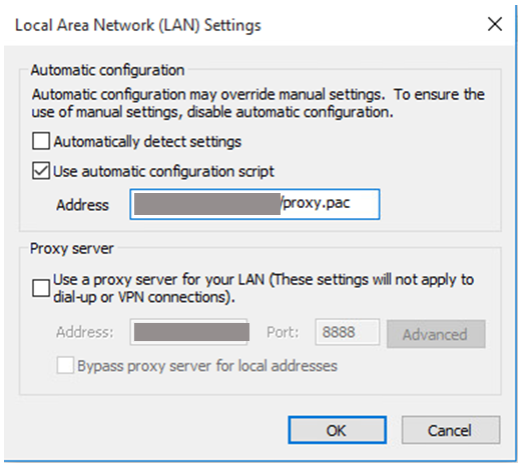
1. Open an Internet Explorer browser window and click the gear icon at the top right corner to open browser settings.
2. Select *Internet options* from the settings menu.



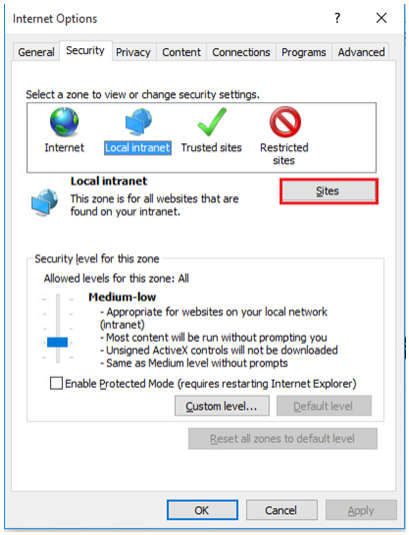

3. Navigate to the *Connections* tab and select the *LAN settings* button.



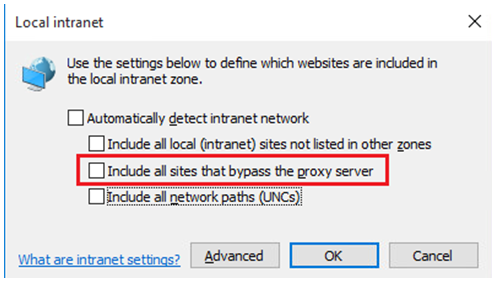

4. Make sure the *Automatically detect settings* box is not checked. (If it is checked, uncheck it).
5. Check the *Use automatic configuration script* box and paste your proxy IP address into the *Address* field and click *OK*.




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

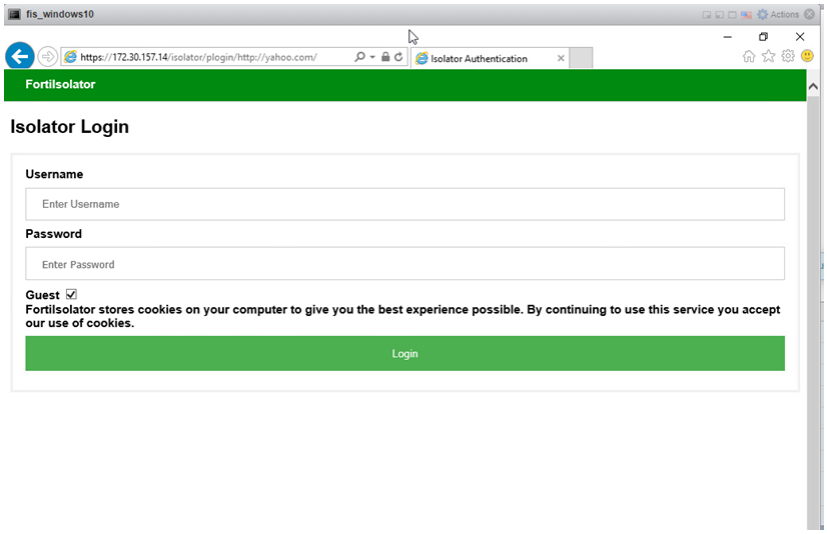


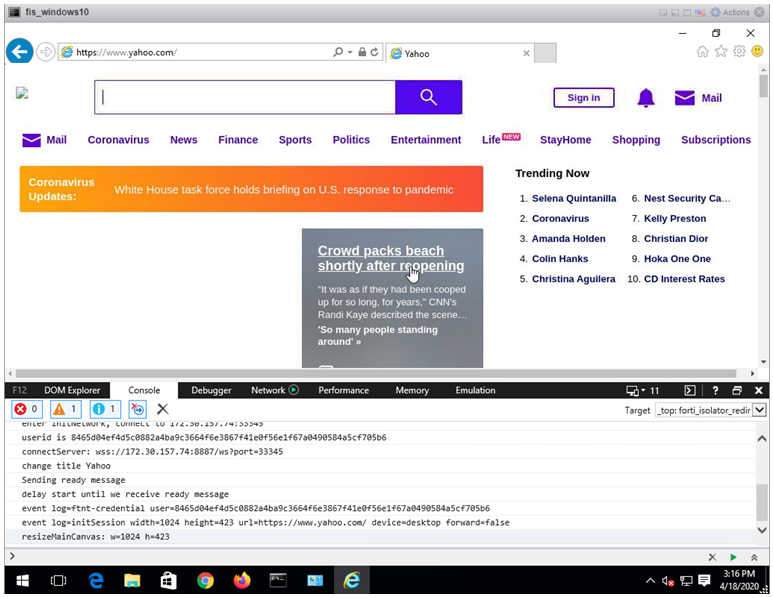

7. Click the *Sites* button to configure how Intranet sites are detected.
8. Make sure that at the very least the *Include all sites that bypass the proxy server* box is not checked. We recommend that all the options for these settings are not checked when possible. Click *OK*.




9. Close and restart Internet Explorer.

## Verifying FortiIsolator proxy mode with Internet Explorer

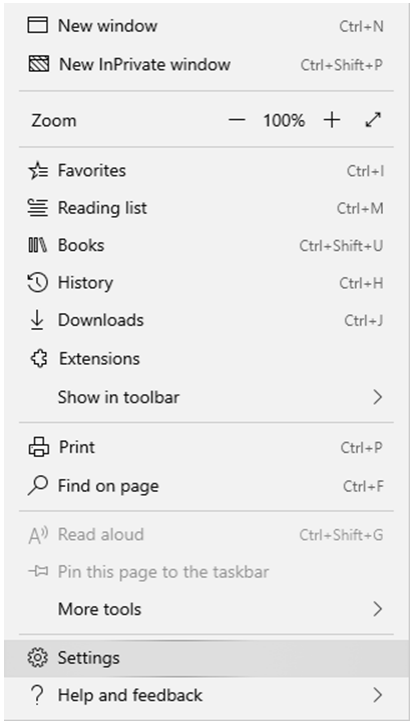


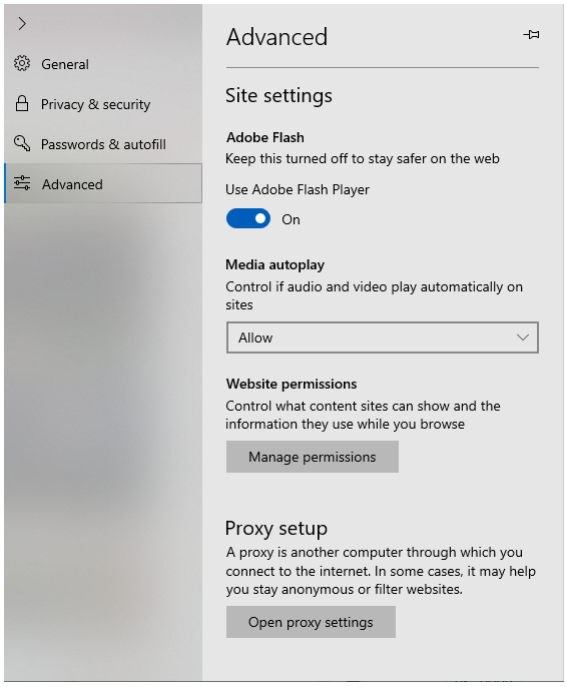
# Using proxy mode with Edge

## To configure proxy mode with Edge:

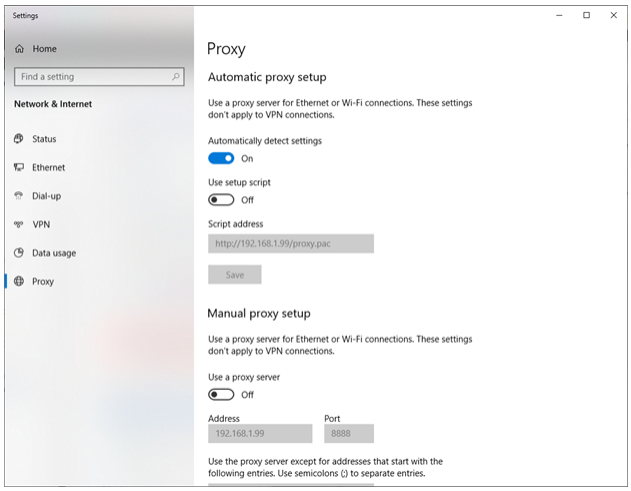
1. Open an Edge browser and click the gear icon at the top right corner to open browser settings.
2. Select *Settings* from the menu.



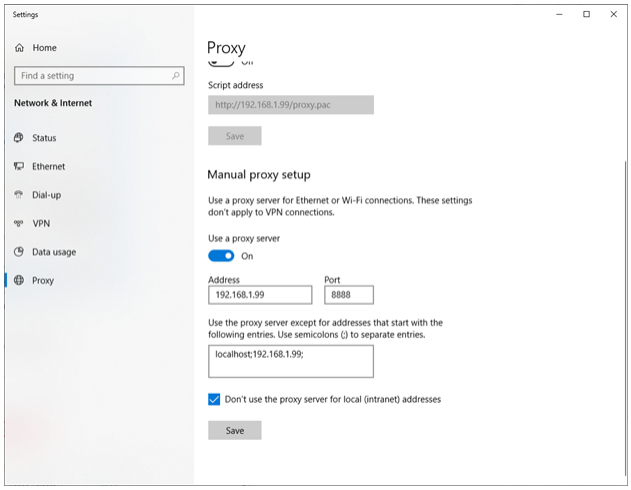

3. Click *Advanced*.



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

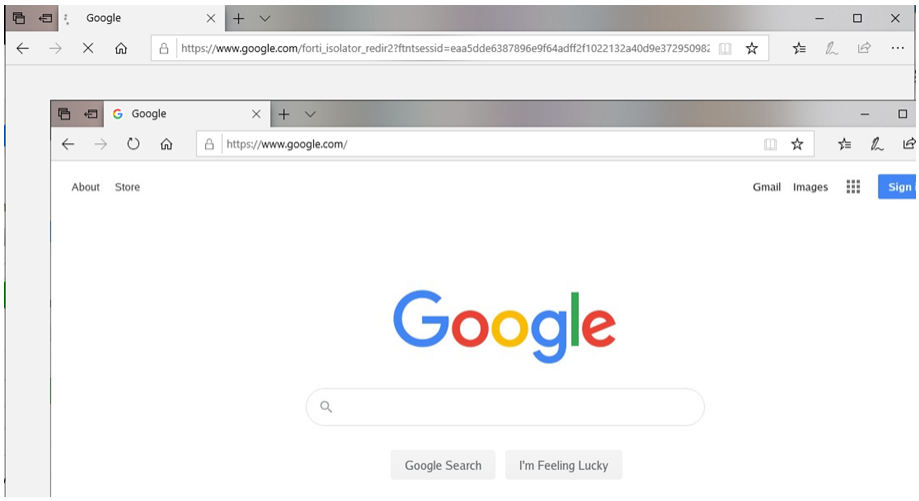



5. Enable *Manual proxy setup*, paste your proxy IP address into the *Address* field with *port 8888* and exception list:




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

### Verifying FortiIsolator proxy mode with Edge



# Logging in as an end user

Depending on the Default policy on page 79 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 65. 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.
- **NTLM Authentication** - If an FSSO agent server is configured in LDAP servers on page 60, the user can log in with single-sign-on by clicking the *NTLM Authentication* link and entering the credentials. This option is available only if *Guest Type* of the default policy is *guest enable* or *guest disable*.
- **SAML Single Sign On** - If a SAML server is configured through FortiAuthenticator in SAML servers on page 61, 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:

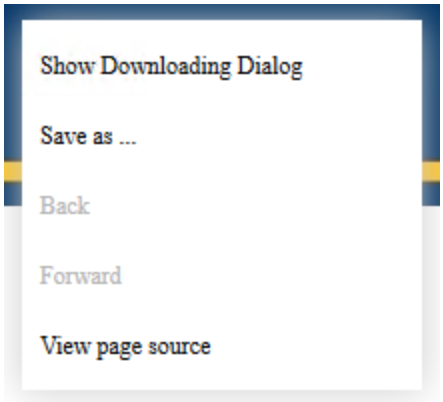
1. In a browser, right-click on the images that you want to save.
2. Click *Copy Image to clipboard*.
3. Open MS Word, MS Excel, or MS Powerpoint
4. Press `Ctrl+V` or right-click to paste the image.

# Downloading files

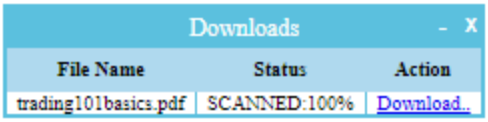
End users are able to download files up to a certain file size while browsing through FortiIsolator if the administrator has configured the Isolator Profile settings to allow it.

### 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.




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.

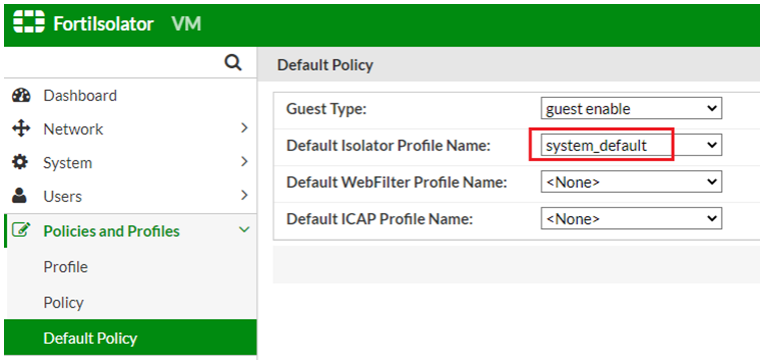
**To configure default policy:**

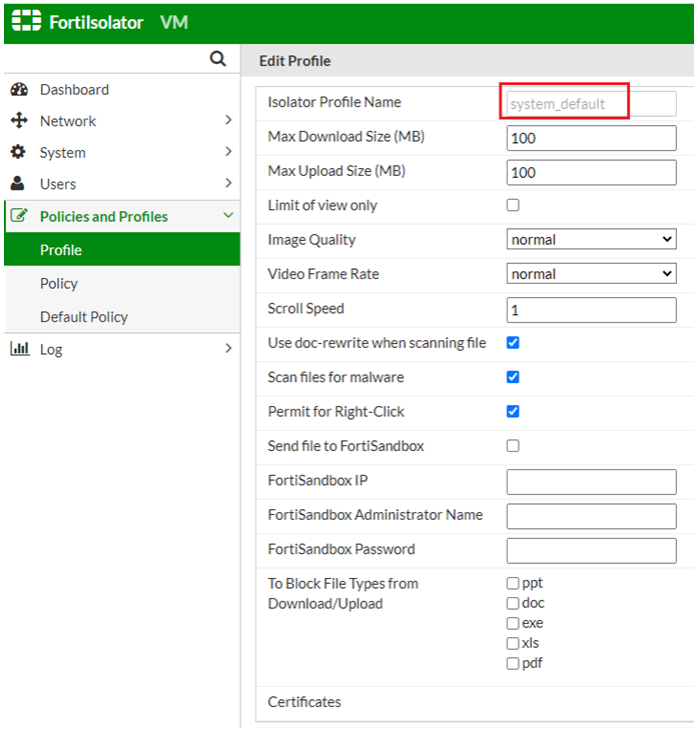
1. Set the Guest Type to *guest only*.
2. Set Default Isolator Profile Name to system_default.
3. Click *OK*.

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**






## 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 |
|---|---|
| hardware-info | Display general hardware status information |
| diagnose-nic | Display general network interface setting |
| diagnose-wf | Test and show WF action for an URL |

www.fortinet.com