



Fortisolator - Administration Guide

Version 2.1.0

FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO GUIDE

<https://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTINET TRAINING & CERTIFICATION PROGRAM

<https://www.fortinet.com/support-and-training/training.html>

NSE INSTITUTE

<https://training.fortinet.com>

FORTIGUARD CENTER

<https://fortiguard.com/>

END USER LICENSE AGREEMENT

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

FEEDBACK

Email: techdoc@fortinet.com



June 18, 2020

Fortisolator 2.1.0 Administration Guide

51-121-540944-20200618

TABLE OF CONTENTS

Change log	5
About this release	6
New in this release	6
Overview	7
Fortisolator models	7
Installation	8
Downloading Fortisolator firmware	8
Fortisolator appliance installation	8
Installing Fortisolator 1000F	8
Fortisolator VM installation	15
Installing Fortisolator VM for Linux KVM	15
Installing Fortisolator VM for VMware vSphere	23
Installing Fortisolator VM for VMware ESXi	32
Setup	38
Port forwarding	38
Dashboard	50
Changing host name	50
Configuring system time	50
VM license	51
Configuration and Certificate backups	51
Network	54
Interfaces	54
System DNS	55
System routing	56
Configuring routing settings	56
Configuring forwarding server	58
System	59
Administrators	59
Accessing the Fortisolator administration portal	59
High Availability	61
Login disclaimer	64
Configuring the login disclaimer	64
Upgrade	66
Upgrading the firmware by GUI	66
To upgrade the firmware in CLI	66
Users	68
Server	68
LDAP servers	68
User definition	69
User groups	70

Policies and profiles	72
Profile	72
Creating Isolator browsing profile	72
Creating Web Filter profile	75
Creating ICAP profile	77
Policy	78
Default policy	79
Applying default policy and profile settings	79
Log	82
Viewing logs	82
Antivirus	83
Web filter	84
Log settings	84
Run web browsers through Fortisolator	86
IP forwarding mode	86
Using IP forwarding mode with Mozilla Firefox	86
Using IP forwarding mode with Google Chrome	87
Using IP forwarding mode with Internet Explorer	92
Using IP forwarding mode with Edge	96
Proxy mode	99
Using proxy mode with Mozilla Firefox	99
Using proxy mode with Google Chrome	102
Using proxy mode with Internet Explorer	110
Using proxy mode with Edge	113
PAC file mode	115
PAC file mode with Mozilla Firefox	115
PAC file mode with Google Chrome	119
Logging in as end user	125
Copying and pasting text	126
Downloading files	126
Utilities and diagnostics	128
Utilities	128
Diagnostic tools	128

Change log

Date	Change description
2020-05-14	Fortinet Fortisolator 2.1.0 document release. See New in this release on page 6 .

About this release

This section provides information about new features in Fortisolator version 2.1.0.

New in this release

Fortisolator version 2.1.0 includes the following new features:

- Full support for Japanese language in Administrator portal and client browsing sites.
- Support for Antivirus scans when uploading/downloading files and keeping logs for related activities.
- Supports integration with FortiSandbox to scan files that have been uploaded/downloaded from FIS.
- Supports Internet Content Adaptation Protocol (ICAP) for Web Filtering
- Supports X-Forwarded-For (XFF) HTTP header field for identifying the originating IP address of a client connecting to FIS.
- Supports different guest login types.
- Print page into a PDF file
- Users can logout from current session.

Overview

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

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

Fortisolator models

Fortisolator is available in the following appliance and virtual machine models. These models allow you to select the most appropriate solution for your requirements.

- Fortisolator 1000F
- Fortisolator VM for Linux KVM
- Fortisolator VM for VMware vSphere
- Fortisolator VM for VMware ESXi

Fortisolator is available in the following appliance and virtual machine models:

Model	Description
Fortisolator appliance	<ul style="list-style-type: none">• Fortisolator 1000F• Supports 500 concurrent sessions, under normal traffic profiles
Fortisolator VM	<ul style="list-style-type: none">• VMware vSphere Hypervisor ESX/ESXi versions 6.0 and 6.5• KVM QEMU version 0.12.1 and higher, includes a hypervisor

Installation

The following sections provide installation instructions for each model:

- [Fortisolator appliance installation on page 8](#)
- [Fortisolator VM installation on page 15](#)

Downloading Fortisolator firmware

Use this procedure to download Fortisolator firmware for your Fortisolator model.

Steps

1. Go to <https://support.fortinet.com>.
2. Click **Login** and log in to the Fortinet Support website.
3. From the **Download** menu, select **Firmware Images**.
4. In the **Select Product** drop-down menu, select **Fortisolator**.
5. Select the **Download** tab.
6. In the **Image Folders/Files** section, navigate to the Fortisolator firmware file for your Fortisolator model.
7. To download the firmware, click **HTTPS**.
8. Unzip the firmware file.

For more information about downloading specific firmware versions for your Fortisolator model, see the [Fortisolator Release Notes](#).

Fortisolator appliance installation

Installing Fortisolator 1000F

Use this procedure to install Fortisolator 1000F.

Prerequisites

- Install Fortisolator 1000F hardware by following the instructions in the [Fortisolator 1000F QuickStart Guide](#).
- Download the Fortisolator firmware by following the instructions in [Downloading Fortisolator firmware on page 8](#).
- Connect to a console (for example, Tera Term).

Steps

1. Using the console, load the Fortisolator firmware file (for example, FIS_1000F-v1-build0084.out).

```
FortiBootLoader
>FortiIsolator-1000F (10:46-03.28.2018)
>Ver:TST20010
FortiIsolator-1000F (16:27-07.06.2018)
Ver:00020010
Serial number:FISlKFT618000001
Total RAM: 131072MB
Boot up, boot device capacity: 1960MB.
Press any key to display configuration menu...
....
[C]: Configure TFTP parameters.
[R]: Review TFTP parameters.
[T]: Initiate TFTP firmware transfer.
[F]: Format boot device.
[B]: Boot with backup firmware and set as default.
[Q]: Quit menu and continue to boot.
[H]: Display this list of options.

Enter C,R,T,F,B,Q,or H:

Image download port:      1
DHCP status:              enabled
Local VLAN ID:            none
Local IP address:         N/A
Local subnet mask:        N/A
Local gateway:            N/A
TFTP server IP address:   172.20.100.1
Firmware file name:      isolator.out

Enter C,R,T,F,B,Q,or H:

Please connect TFTP server to Ethernet port "1".
MAC:                      00:90:0B:50:1D:98

Image download port:      1
DHCP status:              enabled
Local VLAN ID:            none
IP:                      172.20.100.1
Subnet:                   255.255.255.0
Gateway:                  172.20.100.1
TFTP server IP address:   172.20.100.1
Firmware file name:      isolator.out
#####
```

```
#####
Total 131696234 bytes data downloaded.
Verifying the integrity of the firmware image..

Total 270336kB unzipped.

Save as Default firmware/Backup firmware/Run image without saving:[D/B/R]?d
Programming the boot device now.
.....
Reading boot image 7084460 bytes.
INIT: version 2.88 booting...
INIT: Entering runlevel: 3
Starting logging: OK
ext2fs_check_if_mount: Can't check if filesystem is mounted due to missing mtab
/dev/sda: recovering journal
/dev/sda: clean, 1364/61054976 files, 4348813/244190646 blocks
Image version: 1.2.0.0065
Isolator version: 1.2.0.0061
renaming eth0 to internal
renaming eth1 to external
renaming eth4 to mgmt
Populating /dev using udev: done
Initializing random number generator... done.
Starting system message bus: done
Starting network: OK
ip: RTNETLINK answers: File exists
ip: RTNETLINK answers: File exists
ip: RTNETLINK answers: File exists
Starting dropbear sshd: OK
Starting crond: OK
Starting httpd: OK
Starting ha: OK
Now starting webfilter ...
Starting startx: OK

Welcome to Isolator
FISlKFT6l8000001 login: █
```

2. Boot in to the Fortisolator login. The default username is **admin** and there is no default password.

```

Welcome to Isolator
FIS1KFT618000001 login: admin
Password:
> show
Configured parameters:
      Interface    internal    IPv4 IP:    192.168.1.100/24    MAC: 00:90:0B:50:1D:98
      Interface    external    IPv4 IP:    [REDACTED]        MAC: 00:90:0B:50:1D:99
      Interface      mgmt      IPv4 IP:    [REDACTED]        MAC: 00:90:0B:6D:A3:3B
IPv4 Internal Gateway: :                192.168.1.254
IPv4 External Gateway: :                [REDACTED]
IPv4 MGMT Gateway: :                [REDACTED]
hostname :                FIS1KFT618000001
dns server :                [REDACTED]
dns server :                [REDACTED]
build number :                0065(interim)
date time :                2019-05-02 13:05:25 PDT
> status
System Status:
Version :                vl.2.0-build0065 (Interim)
Serial number :                FIS1KFT618000001
System time :                Thu May 02 13:05:27 2019 PDT
Disk Usage :                1014360 bytes
Disk Size :                960381672 bytes
Max Sessions :                2048
Active Sessions :                0
>

```

3. Configure the network parameters (first time only). For example:

Configured parameters:

```

Interface    internal    IPv4 IP:    192.168.1.100/24
Interface    external    IPv4 IP:    [REDACTED]
Interface      mgmt      IPv4 IP:    [REDACTED]
IPv4 Internal Gateway:    192.168.1.254
IPv4 External Gateway:    [REDACTED]

hostname :                FIS1KFT618000001
dns server :                [REDACTED]
dns server :                [REDACTED]
build number:                0065(interim)
date time :                2019-05-02 13:05:25 PDT

```

4. Set the time zone.

```
> show
Configured parameters:
  Interface  internal  IPv4 IP:  192.168.1.100/24  MAC: 00:90:0B:50:1D:98
  Interface  external IPv4 IP:  [REDACTED]      MAC: 00:90:0B:50:1D:99
  Interface  mgmt    IPv4 IP:  [REDACTED]      MAC: 00:90:0B:6D:A3:3B
IPv4 Internal Gateway: : 192.168.1.254
IPv4 External Gateway: : [REDACTED]
IPv4 MGMT Gateway: : [REDACTED]
hostname : FIS1KFT618000001
dns server : [REDACTED]
dns server : [REDACTED]
build number : 0065(interim)
date time : 2019-05-02 13:05:25 PDT
```

5. You can use the `show` command to see the settings (for example, IP addresses, gateway address, DNS server information, and build number).

```
> show
Configured parameters:
  Interface  internal  IPv4 IP:  192.168.1.100/24  MAC: 00:90:0B:50:1D:98
  Interface  external IPv4 IP:  [REDACTED]      MAC: 00:90:0B:50:1D:99
  Interface  mgmt    IPv4 IP:  [REDACTED]      MAC: 00:90:0B:6D:A3:3B
IPv4 Internal Gateway: : 192.168.1.254
IPv4 External Gateway: : [REDACTED]
IPv4 MGMT Gateway: : [REDACTED]
hostname : FIS1KFT618000001
dns server : [REDACTED]
dns server : [REDACTED]
build number : 0065(interim)
date time : 2019-05-02 13:05:25 PDT
```

6. You can use the `status` command to see system information (for example, build version, serial number, system time, disk usage, disk size, and sessions information).

```
> status
System Status:
Version : v1.2.0-build0065 (Interim)
Serial number : FIS1KFT618000001
System time : Thu May 02 13:05:27 2019 PDT
Disk Usage : 1014360 bytes
Disk Size : 960381672 bytes
Max Sessions : 2048
Active Sessions : 0
>
```


7. You can use the `help` command to see the Fortisolator console comments.

```
COM1 - Tera Term VT
File Edit Setup Control Window Help
>
> help
Fortisolator Console
General:
  help      Display this text
  ?         Synonym for 'help'
  exit      Exit from the CLI
Configuration:
  show      Show bootstrap configuration
           Available attributes/values for show:
           ha-all          <null>
           ha-enabled      0/1
           ha-group-id     [1-255]
           ha-lost-threshold [1-60]
           ha-interval     [1-20]
                           in unit of 100ms
           ha-hello-holddown [5-300]
                           in unit of seconds
           ha-priority     [0-255]
                           255 means not used
           ha-allow-override 0/1
           ha-schedule     <schedule type>
           ha-virtual-ip   <IP/netmask>
                           e.g. 192.168.100.2/24
           ha-password     <PASSWORD>
           ha-password-enc <Encoded PASSWORD>
           ha-interface    <Interface Name>
                           e.g. internal/external/mgmt

  show-ipmap-ha Show HA ipmapping configuration
  set           Set configuration parameter
           Available attributes/values for set:
           internal-ip     <IP/netmask>
                           e.g. 192.168.100.2/24
           external-ip     <IP/netmask>
                           e.g. 192.168.100.2/24
           mgmt-ip         <IP/netmask>
                           e.g. 192.168.100.2/24
           date            <YYYY-MM-DD>
           time            <HH:MM:SS>
           dns             <pdns-ip sdns-ip>
                           e.g. 192.168.100.1 192.168.10.1
           ntp             <ntp-ip>
                           e.g. 192.168.100.1
           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
           hostname        <hostname>
           timezone        <timezone>
                           e.g. America/Los_Angeles
           ha-enabled      0/1
           ha-group-id     [1-255]
           ha-lost-threshold [1-60]
           ha-interval     [1-20]
                           in unit of 100ms
           ha-hello-holddown [5-300]
                           in unit of seconds
           ha-priority     [0-255]
                           255 means not used
           ha-allow-override 0/1
           ha-schedule     <schedule type>
           ha-virtual-ip   <IP/netmask>
                           e.g. 192.168.100.2/24
           ha-password     <PASSWORD>
           ha-password-enc <Encoded PASSWORD>
           ha-interface    <Interface Name>
                           e.g. internal/external/mgmt
           fis-ipmap-ha    <priority external_isolator_ip internal_isolator_ip external_po
rt internal_port>
                           e.g. 0 192.168.100.1 10.1.0.1 12443 12887
           fis-ipmap       <external_port internal_port [external_isolator_ip]>
                           e.g. 12443 12887 192.168.100.1
           fis-ipmap-vip   <external_port internal_port external_isolator_ip>
                           e.g. 14443 14887 192.168.122.1

  unset      Unset configuration parameter
           Available attributes for unset:
           dns
           ntp
           internal-gw
           external-gw
           mgmt-gw
           fis-ipmap-ha
           fis-ipmap
```

```

COM1 - Tera Term VT
File Edit Setup Control Window Help

ha-priority          [0-255]
                    255 means not used
ha-allow-override    0/1
ha-schedule           <schedule type>
ha-virtual-ip         <IP/netmask>
                    e.g. 192.168.100.2/24
ha-password          <PASSWORD>
ha-password-enc       <Encoded PASSWORD>
ha-interface          <Interface Name >
                    e.g. internal/external/mgmt

show-ipmap-ha        Show HA ipmapping configuration
set                  Set configuration parameter
                    Available attributes/values for set:

                    internal-ip      <IP/netmask>
                                    e.g. 192.168.100.2/24
                    external-ip      <IP/netmask>
                                    e.g. 192.168.100.2/24
                    mgmt-ip          <IP/netmask>
                                    e.g. 192.168.100.2/24
                    date             <YYYY-MM-DD>
                    time             <HH:MM:SS>
                    dns              <pdns-ip sdns-ip>
                                    e.g. 192.168.100.1 192.168.10.1
                    ntp              <ntp-ip>
                                    e.g. 192.168.100.1
                    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
                    hostname          <hostname>
                    timezone         <timezone>
                                    e.g. America/Los_Angeles
                    ha-enabled        0/1
                    ha-group-id       [1-255]
                    ha-lost-threshold [1-60]
                    ha-interval       [1-20]
                                    in unit of 100ms
                    ha-hello-holddown [5-300]
                                    in unit of seconds
                    ha-priority        [0-255]
                                    255 means not used
                    ha-allow-override 0/1
                    ha-schedule        <schedule type>
                    ha-virtual-ip      <IP/netmask>
                                    e.g. 192.168.100.2/24
                    ha-password        <PASSWORD>
                    ha-password-enc    <Encoded PASSWORD>
                    ha-interface       <Interface Name >
                                    e.g. internal/external/mgmt
                    fis-ipmap-ha       <priority external_isolator_ip internal_isolator_ip external_po
rt internal_port>
                                    e.g. 0 192.168.100.1 10.1.0.1 12443 12887
                    fis-ipmap          <external_port internal_port [external_isolator_ip]>
                                    e.g. 12443 12887 192.168.100.1
                    fis-ipmap-vip      <external_port internal_port external_isolator_ip>
                                    e.g. 14443 14887 192.168.122.1

unset                Unset configuration parameter
                    Available attributes for unset:

                    dns
                    ntp
                    internal-gw
                    external-gw
                    mgmt-gw
                    fis-ipmap-ha
                    fis-ipmap
                    fis-ipmap-vip

System:
reboot               Reboot the Fortiisolator
system-upgrade       Upgrade Fortiisolator System Image
factory-reset        Reset configuration to defaults and delete all data
shutdown             Shutdown the Fortiisolator
status               Display some status information
admin-pwd-reset      Reset Admin Password

Utilities:
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

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

```

Fortisolator VM installation

To install Fortisolator VM, follow the procedure for one of the following VM systems:

- [Installing Fortisolator VM for Linux KVM on page 15](#)
- [Installing Fortisolator VM for VMware vSphere on page 23](#)
- [Installing Fortisolator VM for VMware ESXi on page 32](#)

Installing Fortisolator VM for Linux KVM

Use this procedure to install Fortisolator VM for Linux KVM.

Fortisolator VM for Linux KVM supports both Video Graphics Array (VGA) and virtual serial console connections.

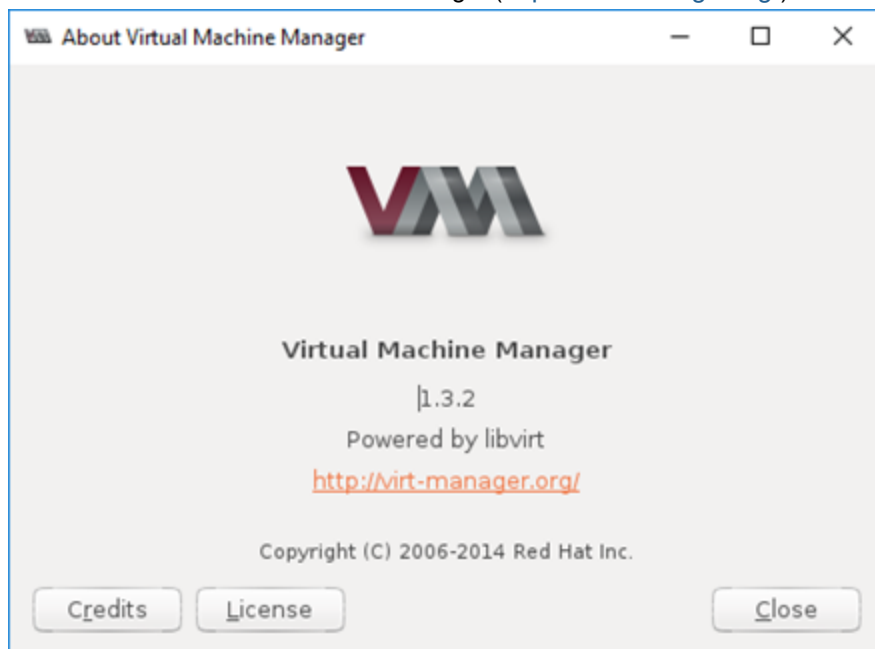
Prerequisites

- Ensure that your system has at least two hard disks of the following types:
 - IDE
 - SATA
 - SCSI
 - Virtio
- Ensure that your system has at least three network interfaces of the following types:
 - Hypervisor default (Rt18139)
 - E1000

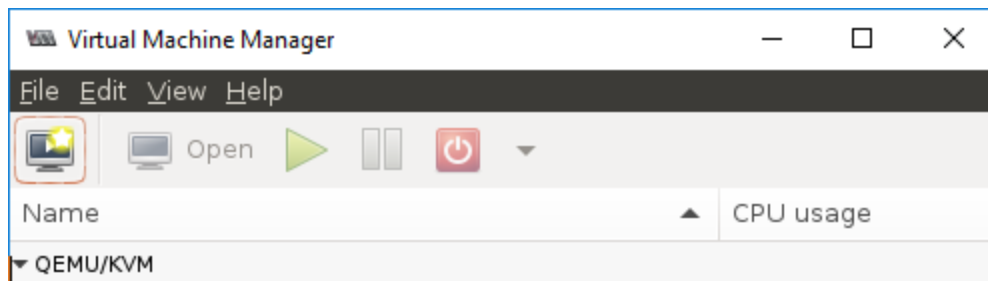
Steps

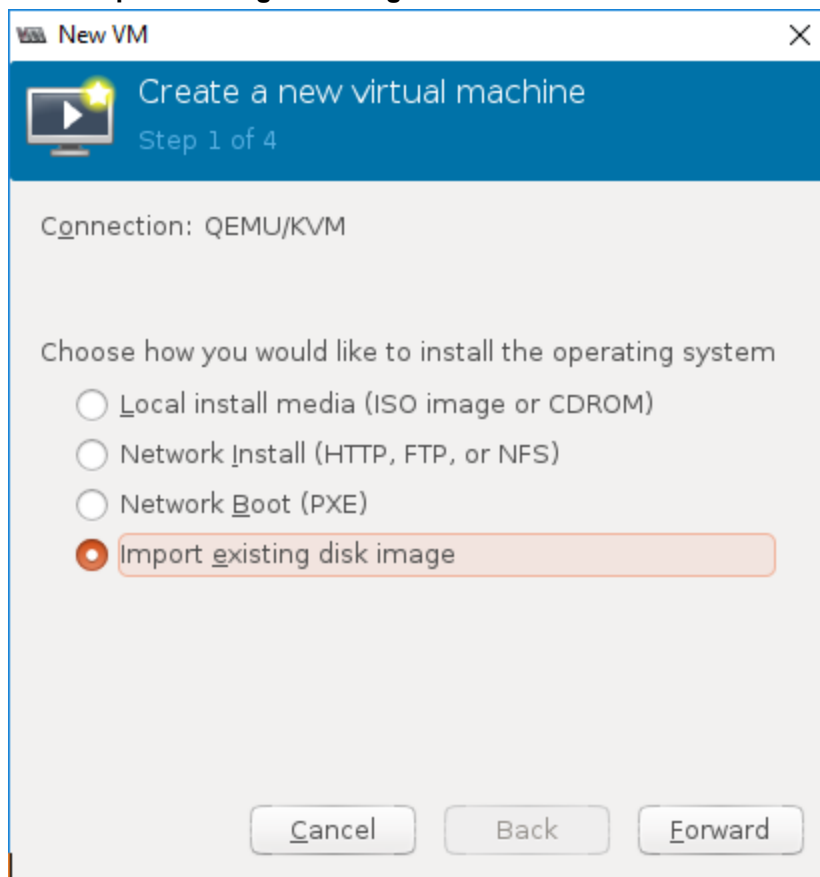
1. Download the Fortisolator firmware for KVM by following the instructions in [Downloading Fortisolator firmware on page 8](#).

2. Launch KVM with Virtual Machine Manager (<https://virt-manager.org/>).

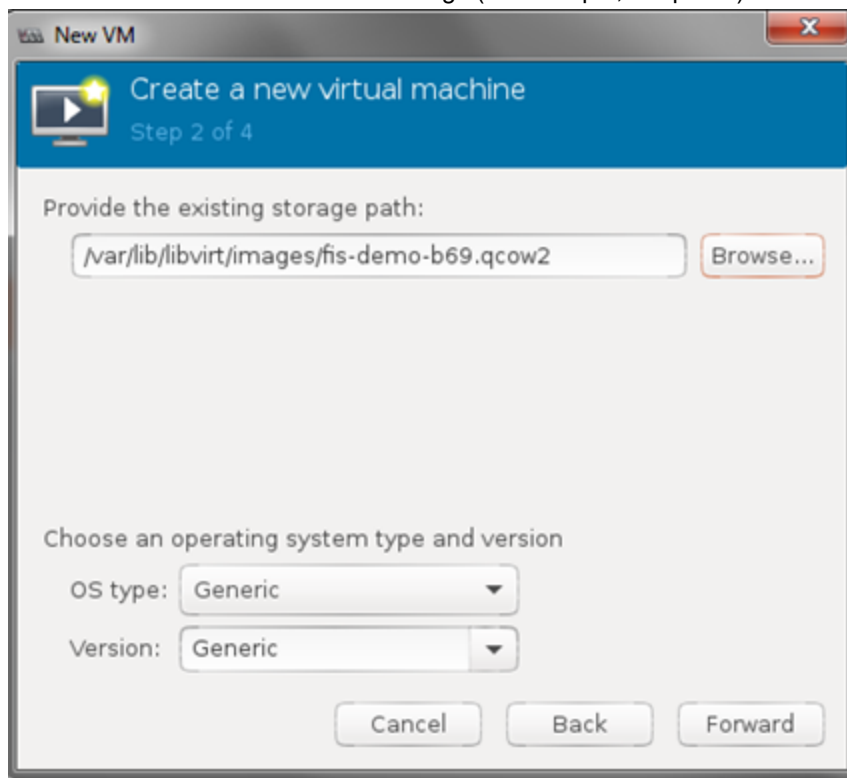


3. Create a new virtual machine.

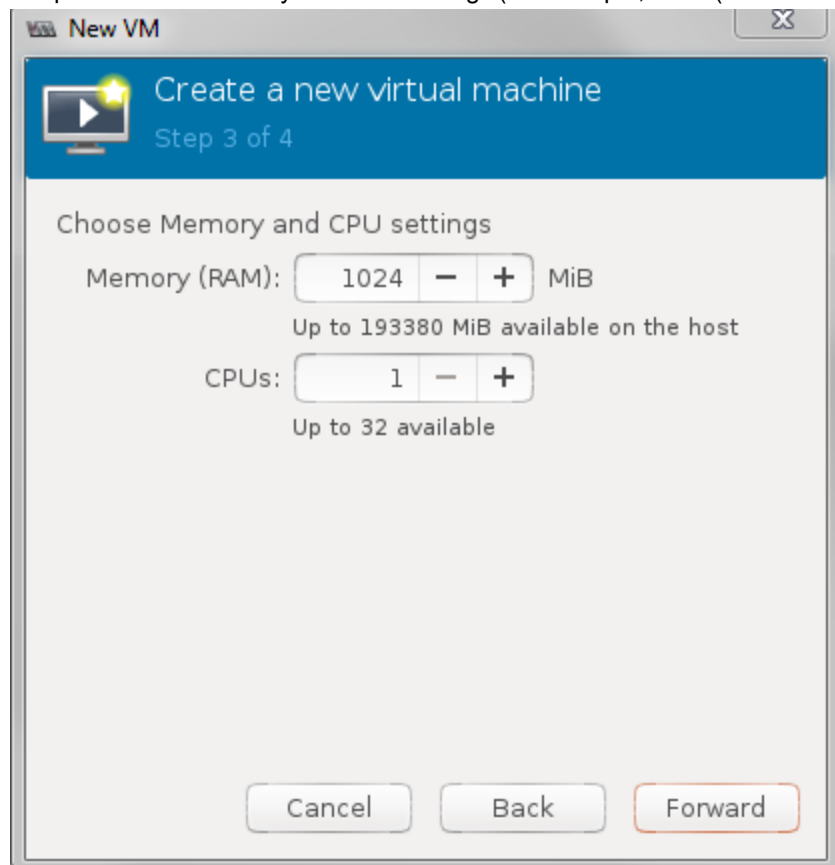


4. Select Import existing disk image.

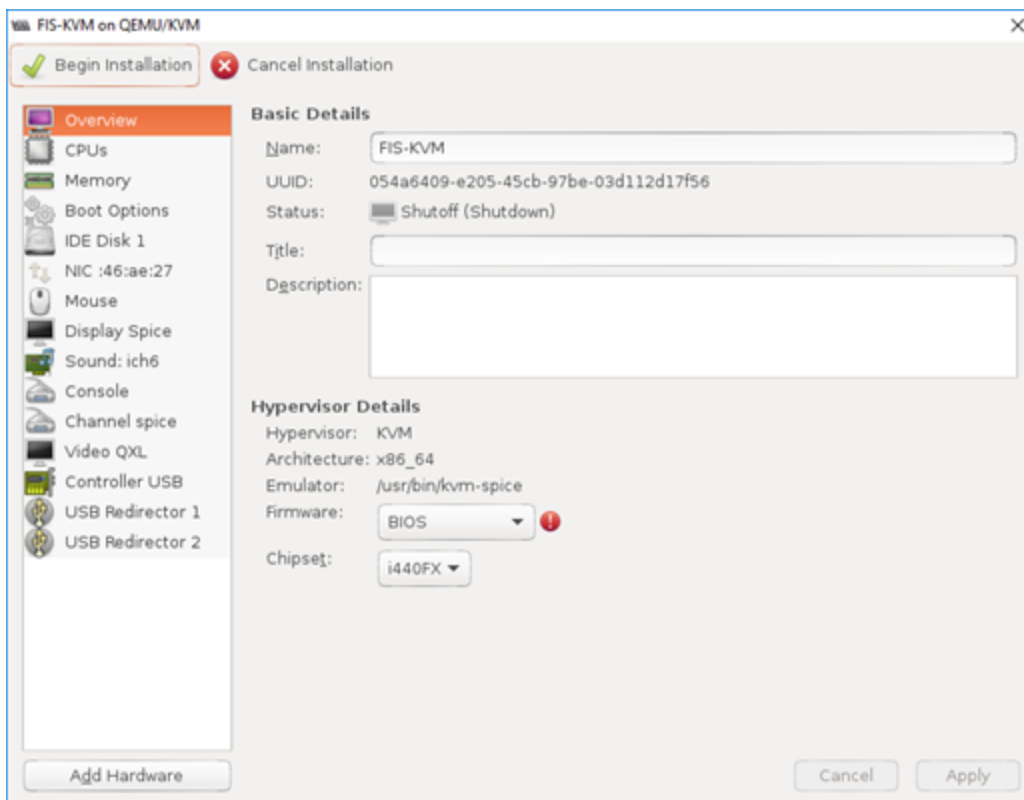
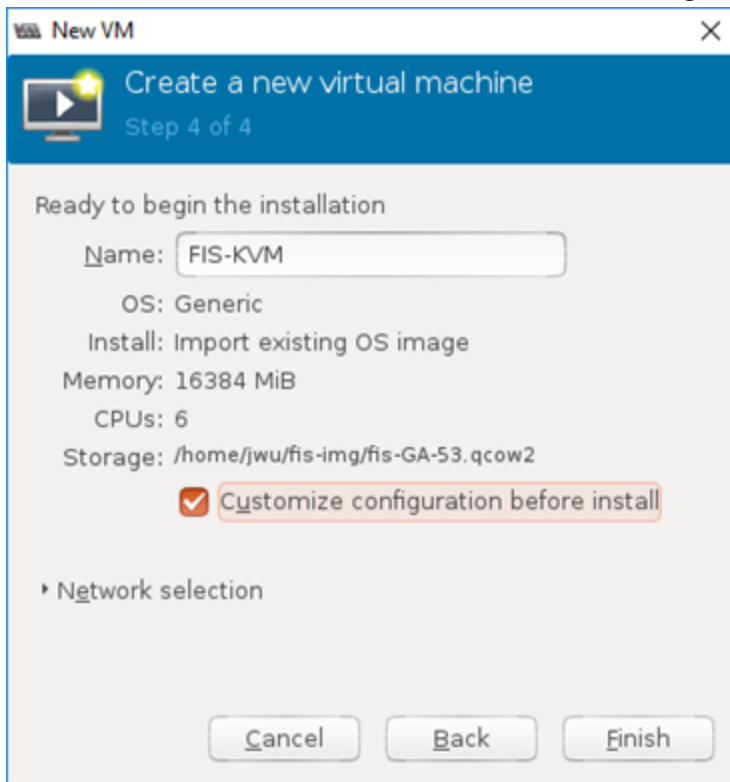
5. Browse and select the Fortisolator image (for example, fis.qcow2).



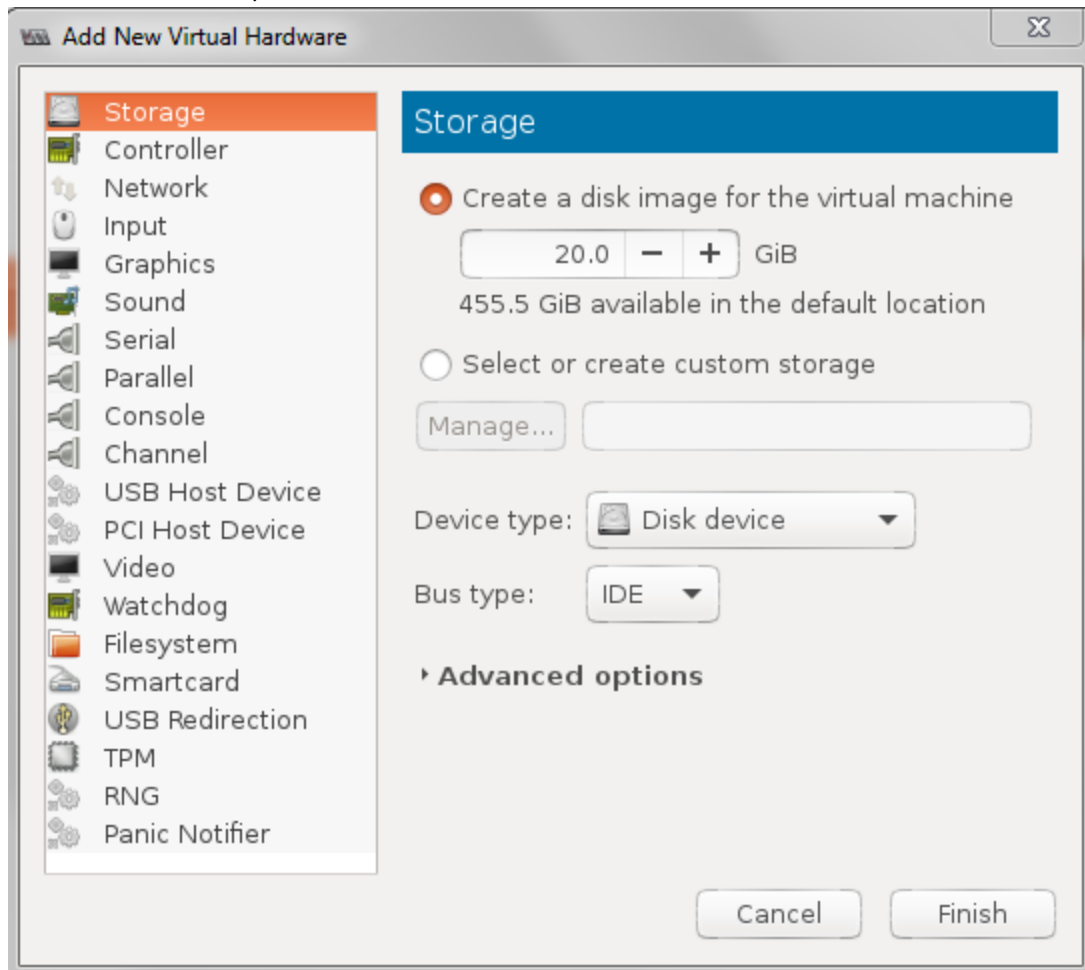
6. Keep the default memory and CPU settings (for example, 1024 (193380 MiB) of memory and 1 CPU).



7. Name the new virtual machine, and select **Customize configuration before install**.

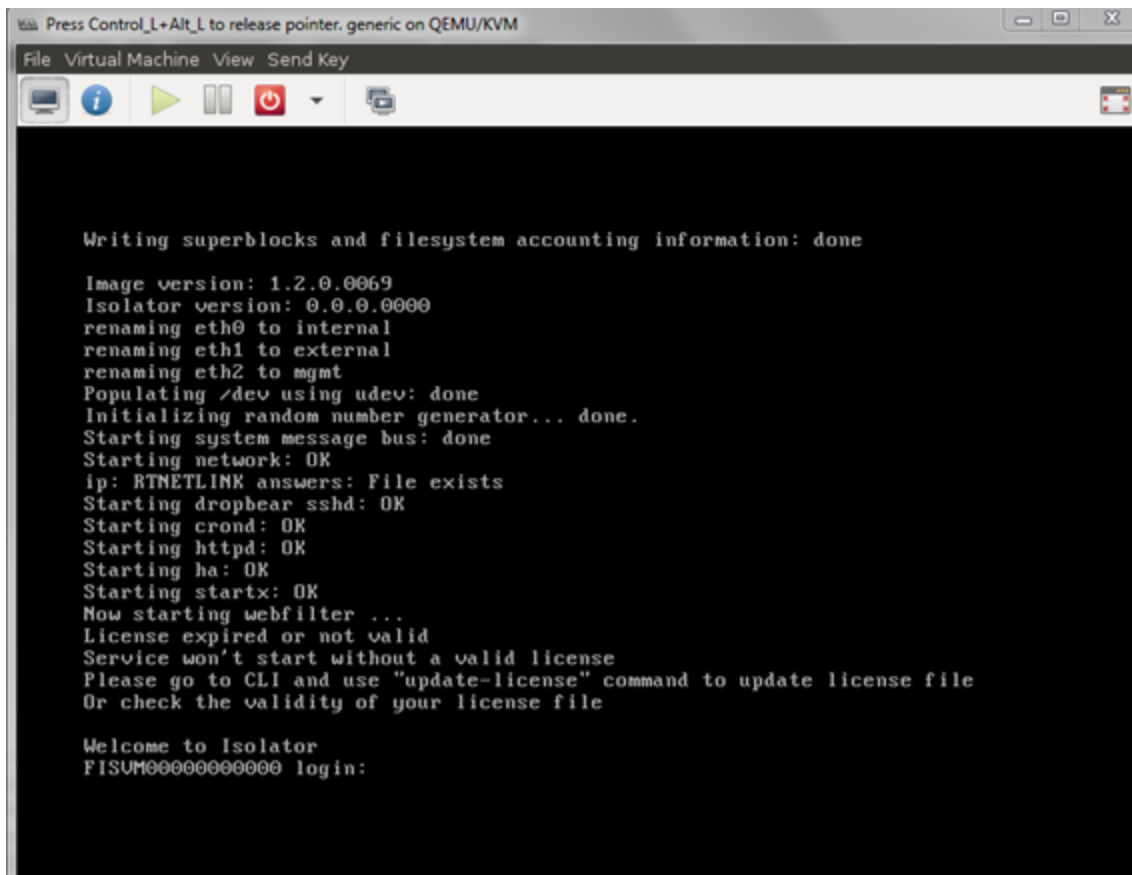
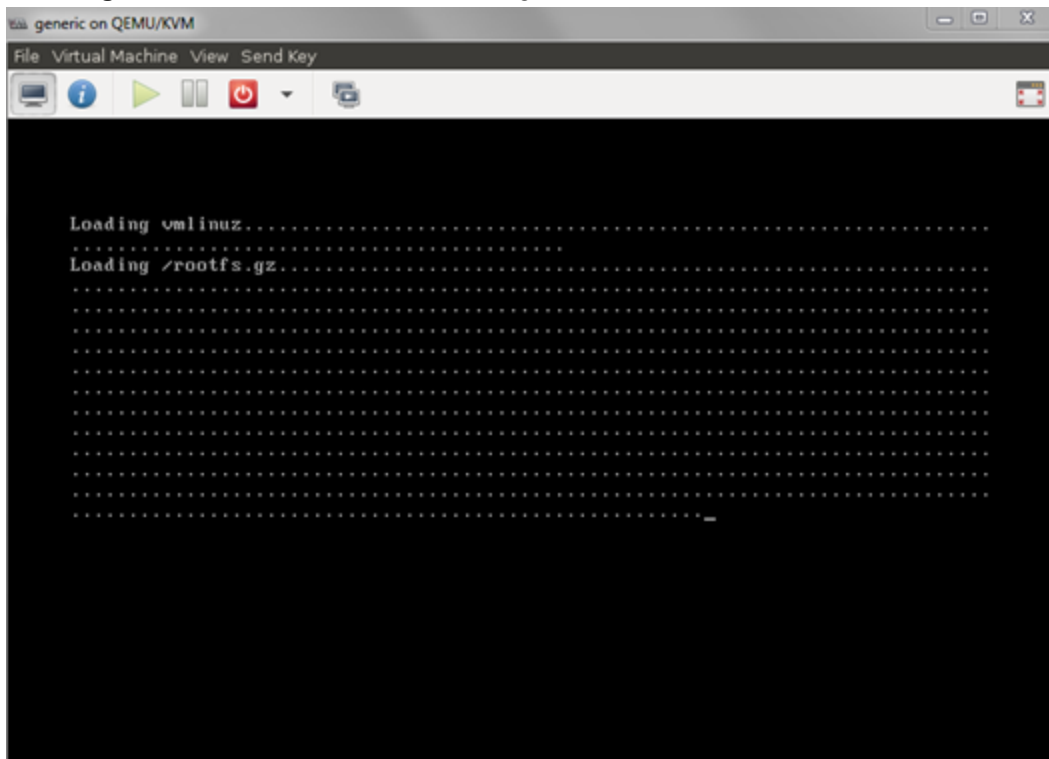


8. Add an IDE disk. Accept the default values.



9. Add three network interfaces and configure them accordingly.
- Network 1: Internal Interface
 - Network 2: External Interface
 - Network 3: Management Interface
 - Network 4: HA Interface

- 10.** Click **Begin Installation** to load the KVM image.



11. In the **Set default parameters** step, configure the network interfaces.

```
set internal-ip      192.168.122.99/24
set internal-gw      192.168.122.0/24      192.168.122.254
set external-ip      172.16.1.100/24
set external-gw      0.0.0.0/0            172.16.1.100
set mgmt-ip          192.168.199.99/24
set mgmt-gw          192.168.199.0/24      192.168.199.254
set dns              208.91.112.53 208.91.112.52
```

Installing Fortisolator VM for VMware vSphere

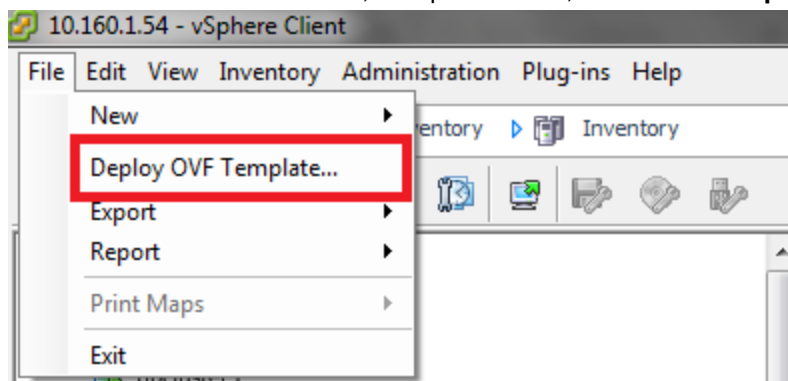
Use this procedure to install Fortisolator VM for VMware vSphere.

Prerequisites

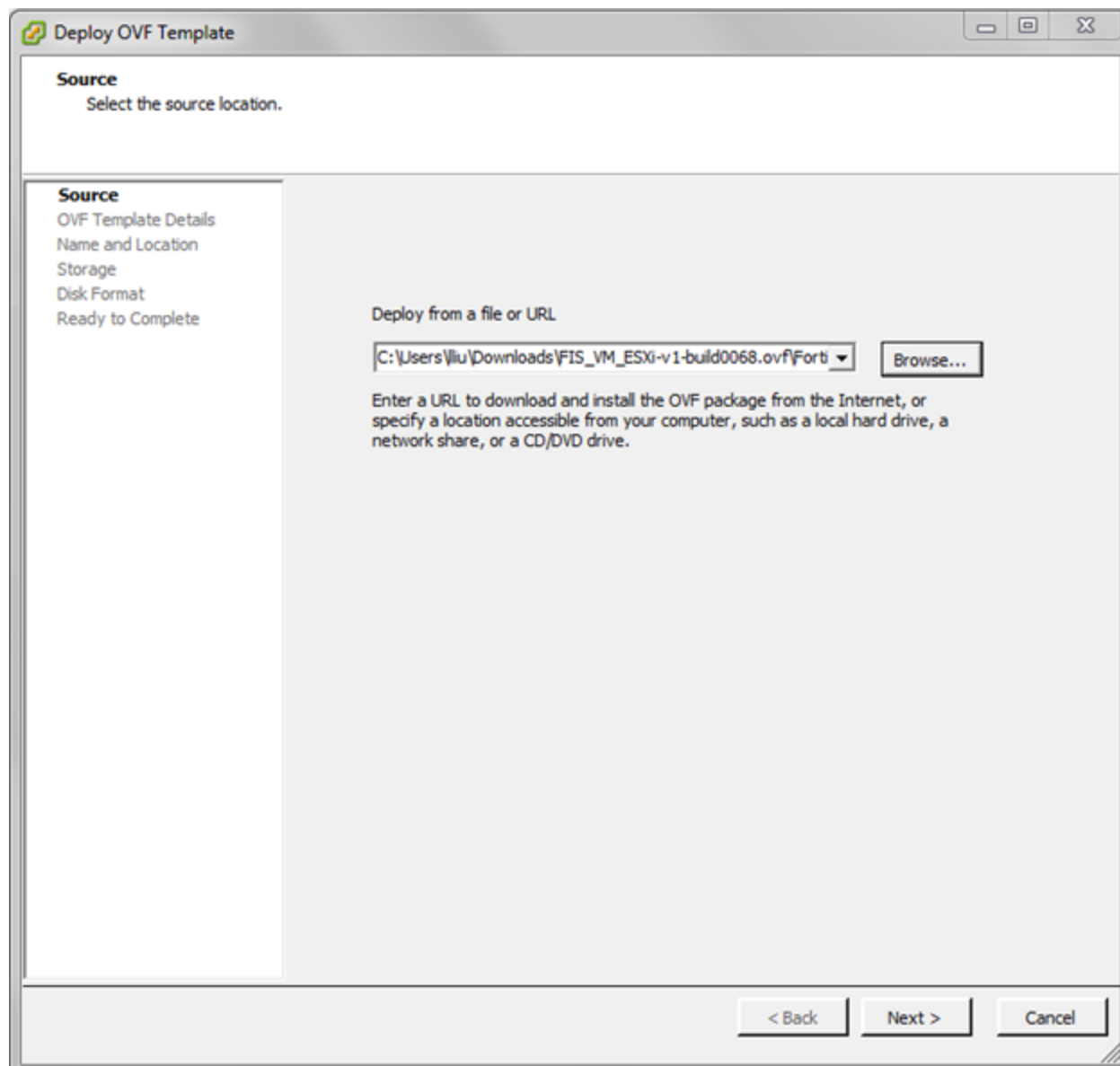
- Install VMware vSphere Client.
- Ensure that your system has one of the following combinations of hard disks and network adapters to support ESXi 6.0:
 - Two SCSI hard disks and three VMXNET 3 network adapters (this is the default)
 - One IDE hard disk and one SCSI hard disk and three E1000 network adapters

Steps

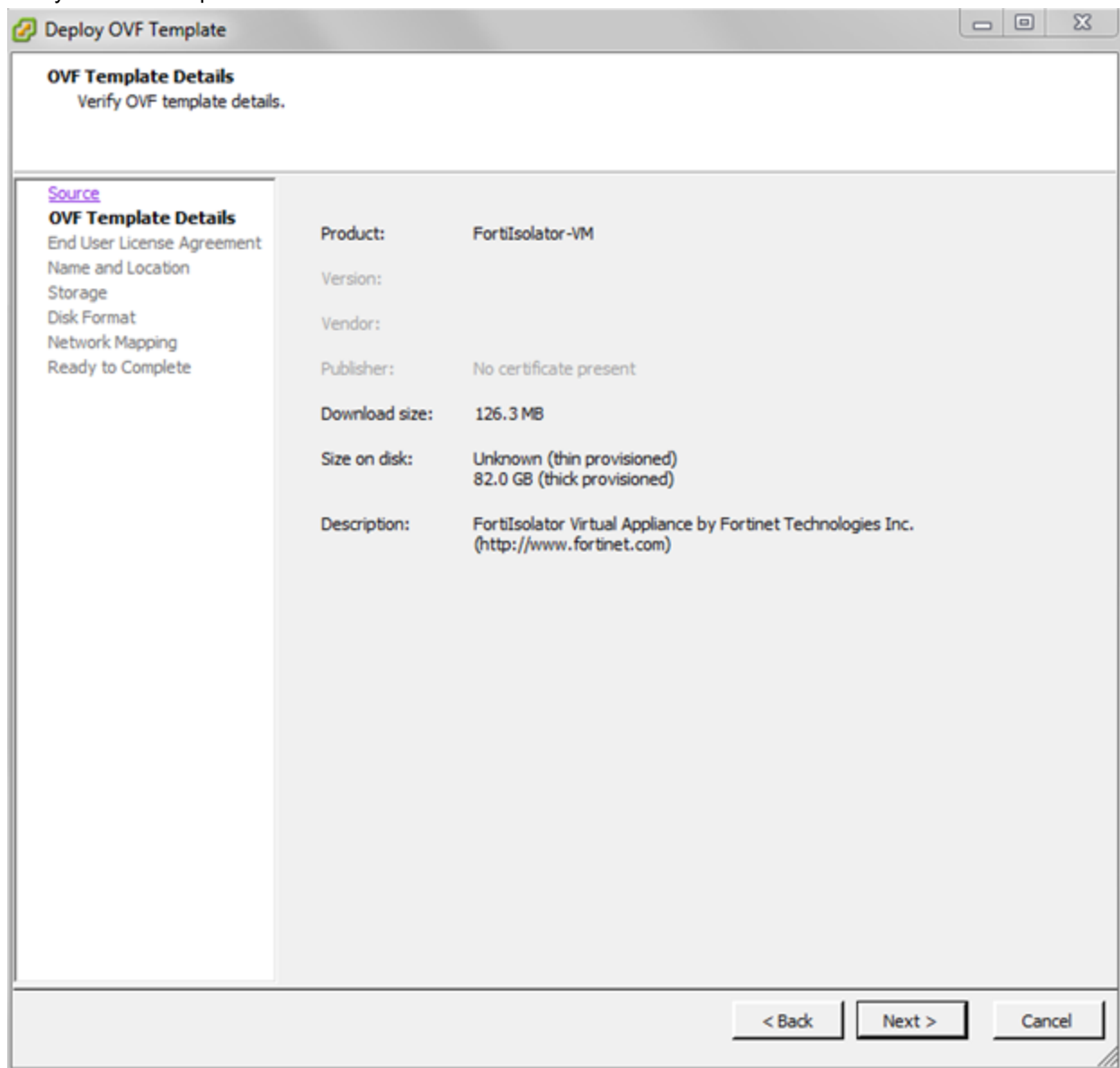
1. Download the Fortisolator firmware for VMware by following the instructions in [Downloading Fortisolator firmware on page 8](#).
2. To create a new virtual machine, in vSphere Client, select **File > Deploy OVF Template**.



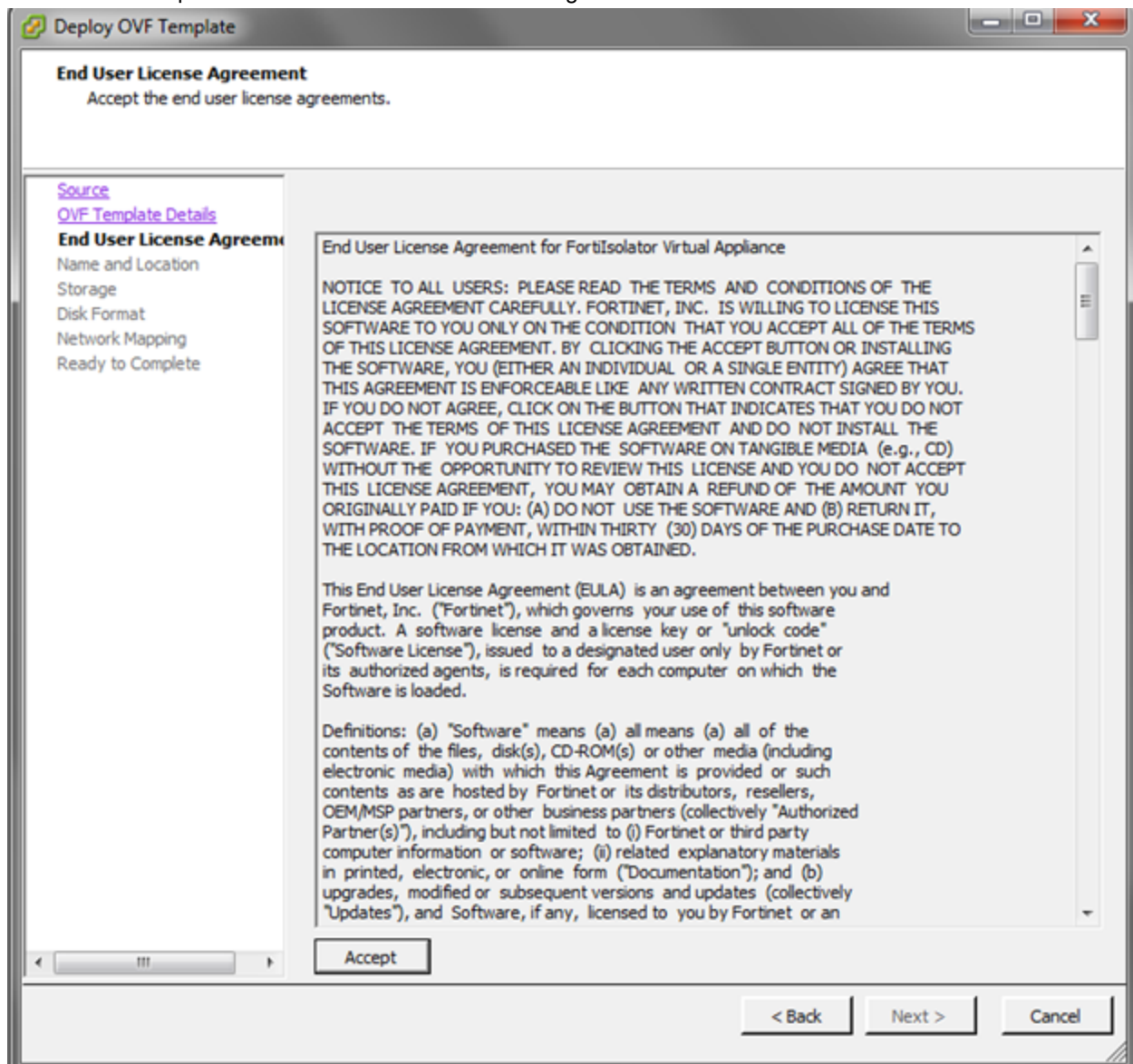
3. Browse to the folder that contains the Fortisolator files and select **Fortisolator.ovf**.

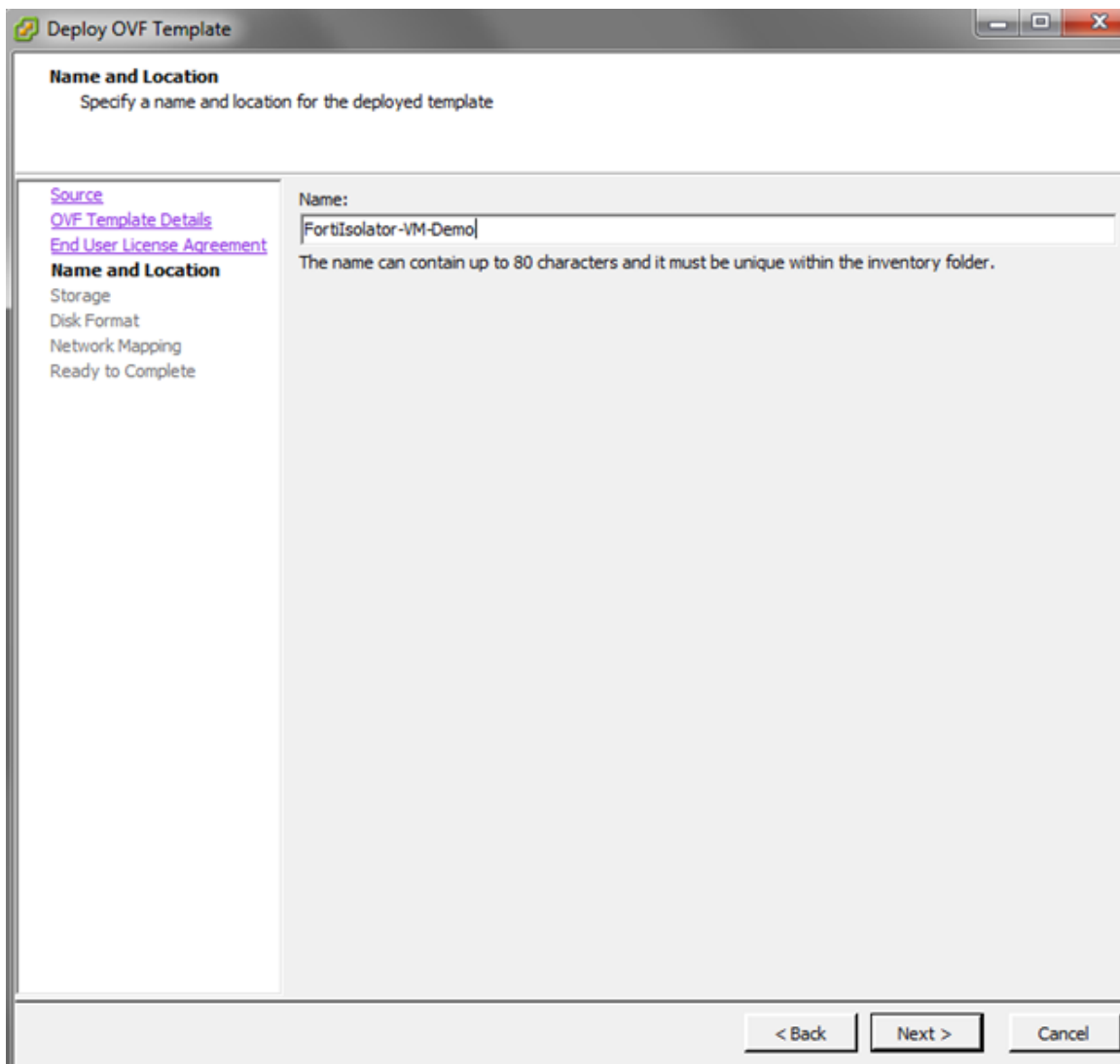


4. Verify the OVF template details.



5. Review and accept the Fortisolator End User License Agreement.



6. Name the new Fortisolator virtual machine.

The screenshot shows the 'Deploy OVF Template' wizard window. The title bar reads 'Deploy OVF Template'. The main heading is 'Name and Location' with the instruction 'Specify a name and location for the deployed template'. On the left, a sidebar lists the steps: 'Source', 'OVF Template Details', 'End User License Agreement', 'Name and Location' (which is highlighted), 'Storage', 'Disk Format', 'Network Mapping', and 'Ready to Complete'. The main area has a 'Name:' label above a text input field containing 'Fortisolator-VM-Demo'. Below the input field, a note states: 'The name can contain up to 80 characters and it must be unique within the inventory folder.' At the bottom right, there are three buttons: '< Back', 'Next >', and 'Cancel'.

7. Select the datastore where you want to install the Fortisolator VM.

Deploy OVF Template

Storage
Where do you want to store the virtual machine files?

[Source](#)
[OVF Template Details](#)
[End User License Agreement](#)
[Name and Location](#)

Storage
Disk Format
Network Mapping
Ready to Complete

Select a destination storage for the virtual machine files:

Name	Drive Type	Capacity	Provisioned	Free	Type	Thin Pro
datastore1	Non-SSD	411.00 GB	572.43 GB	56.84 GB	VMFSS	Supporte
Main-Disk	Non-SSD	2.73 TB	6.98 TB	15.52 GB	VMFSS	Supporte

☐ Disable Storage DRS for this virtual machine

Select a datastore:

Name	Drive Type	Capacity	Provisioned	Free	Type	Thin Provi
------	------------	----------	-------------	------	------	------------

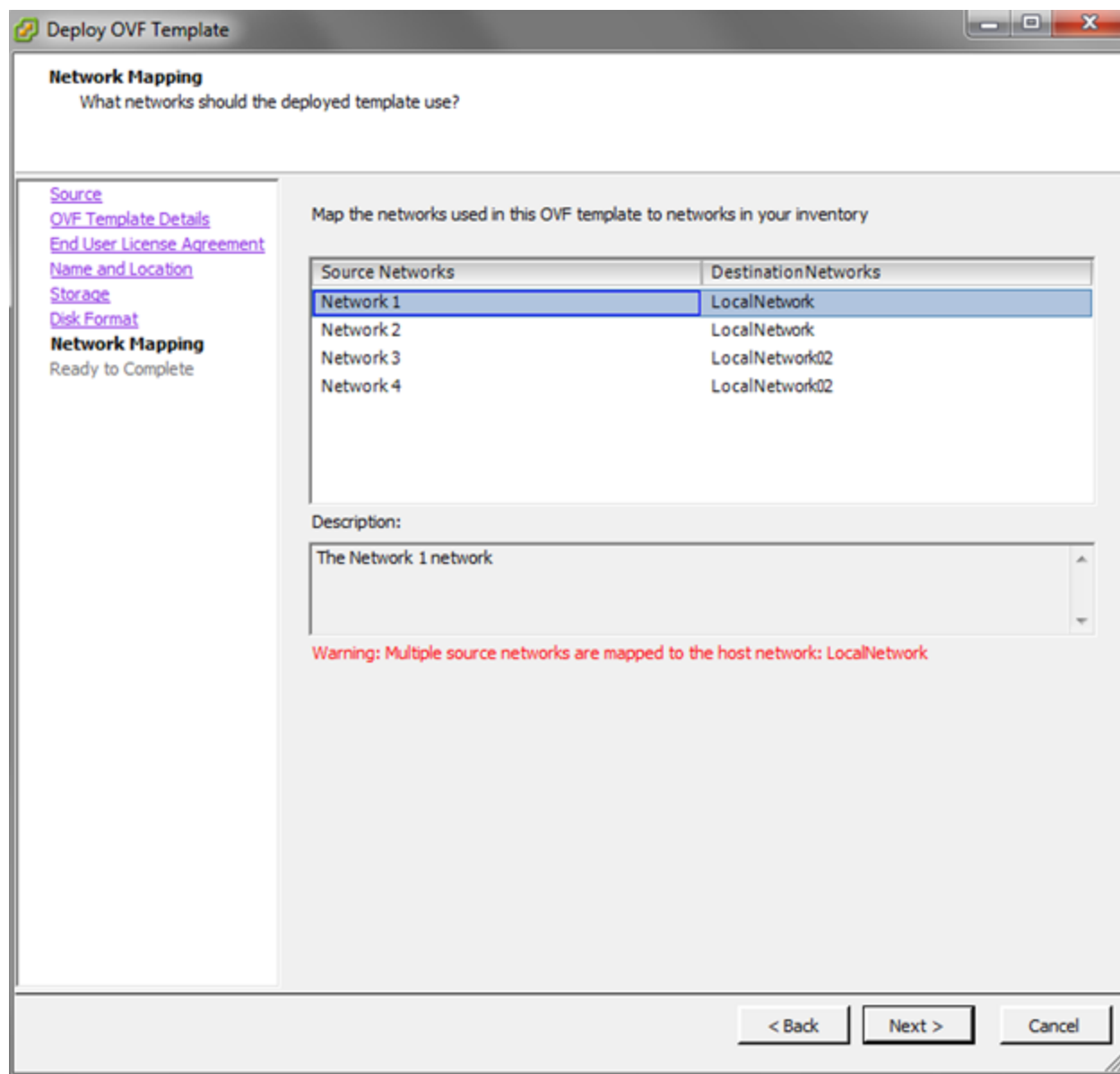
Compatibility:
Insufficient disk space for full capacity of 82.00 GB. Thin provisioned disk size is unknown.

< Back Next > Cancel

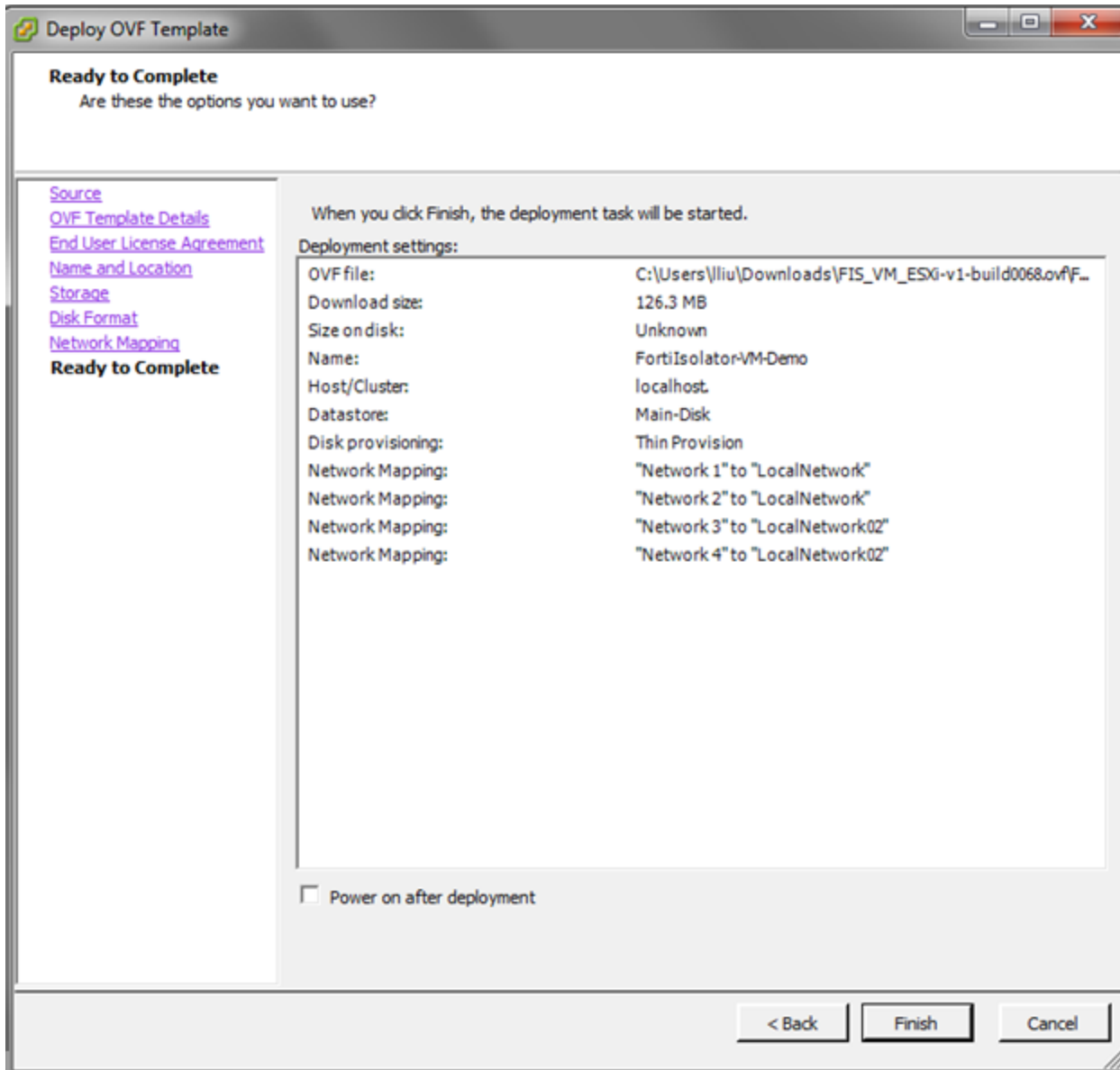
8. Select the disk provisioning format. For optimal performance, select a **Thick Provision** option.

The screenshot shows the 'Deploy OVF Template' window with the 'Disk Format' step selected. The window title is 'Deploy OVF Template'. The main heading is 'Disk Format' with the subtext 'In which format do you want to store the virtual disks?'. On the left, there is a navigation pane with links: 'Source', 'OVF Template Details', 'End User License Agreement', 'Name and Location', 'Storage', 'Disk Format' (highlighted), 'Network Mapping', and 'Ready to Complete'. The main area shows 'Datastore:' with a dropdown menu set to 'Main-Disk' and 'Available space (GB):' with a text box containing '15.5'. Below this, there are three radio button options: 'Thick Provision Lazy Zeroed' (selected), 'Thick Provision Eager Zeroed', and 'Thin Provision'. At the bottom right, there are three buttons: '< Back', 'Next >', and 'Cancel'.

9. Configure the required network interfaces. Add four network interfaces for Network Mapping and configure them accordingly:
- Network 1: Internal Interface
 - Network 2: External Interface
 - Network 3: Management Interface
 - Network 4: HA Interface



10. Verify the template deployment options, and click **Finish**.



11. Start the Fortisolator VM.

```
Writing superblocks and filesystem accounting information: done

Image version: 1.2.0.0050
Isolator version: 0.0.0.0000
renaming eth0 to internal
renaming eth1 to external
renaming eth2 to mgmt
Populating /dev using udev: done
Initializing random number generator... done.
Starting system message bus: done
Starting network: OK
ip: RTNETLINK answers: File exists
Starting dropbear sshd: OK
Starting crond: OK
Starting httpd: OK
Starting ha: OK
Starting startx: OK
Now starting webfilter ...
License expired or not valid
Service won't start without a valid license
Please go to CLI and use "update-license" command to update license file
Or check the validity of your license file

Welcome to Isolator
FISUM0000000000 login: _
```

12. Log in to Fortisolator. The default username is **admin** and there is no default password.

Installing Fortisolator VM for VMware ESXi

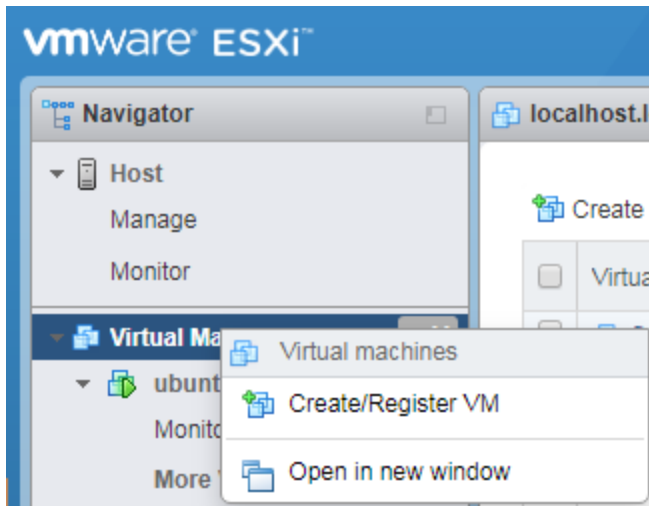
Use this procedure to install Fortisolator VM for VMware ESXi.

Prerequisites

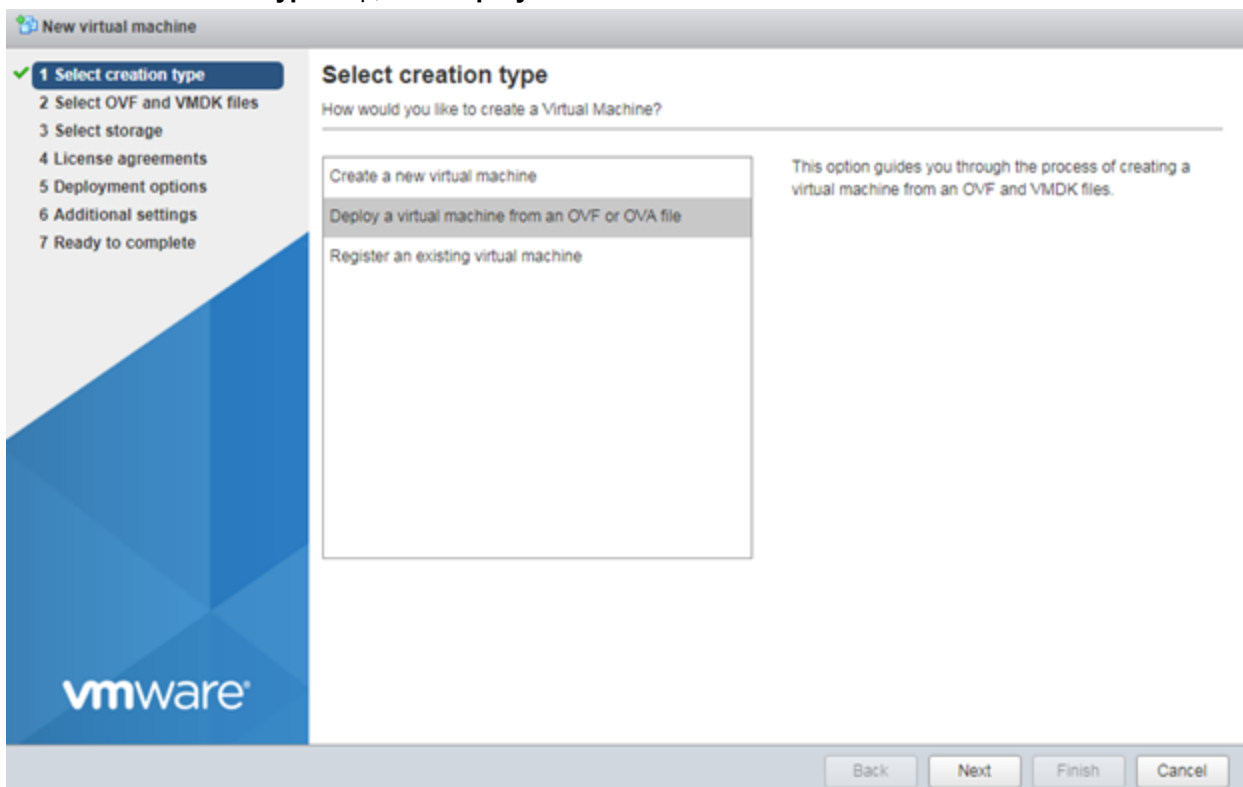
- Install VMware vSphere Client.
- Ensure that your system has one of the following combinations of hard disks and network adapters to support ESXi 6.5:
 - Two SCSI hard disks and three VMXNET 3 network adapters (this is the default)
 - Two SCSI hard disks and three E1000 network adapters

Steps

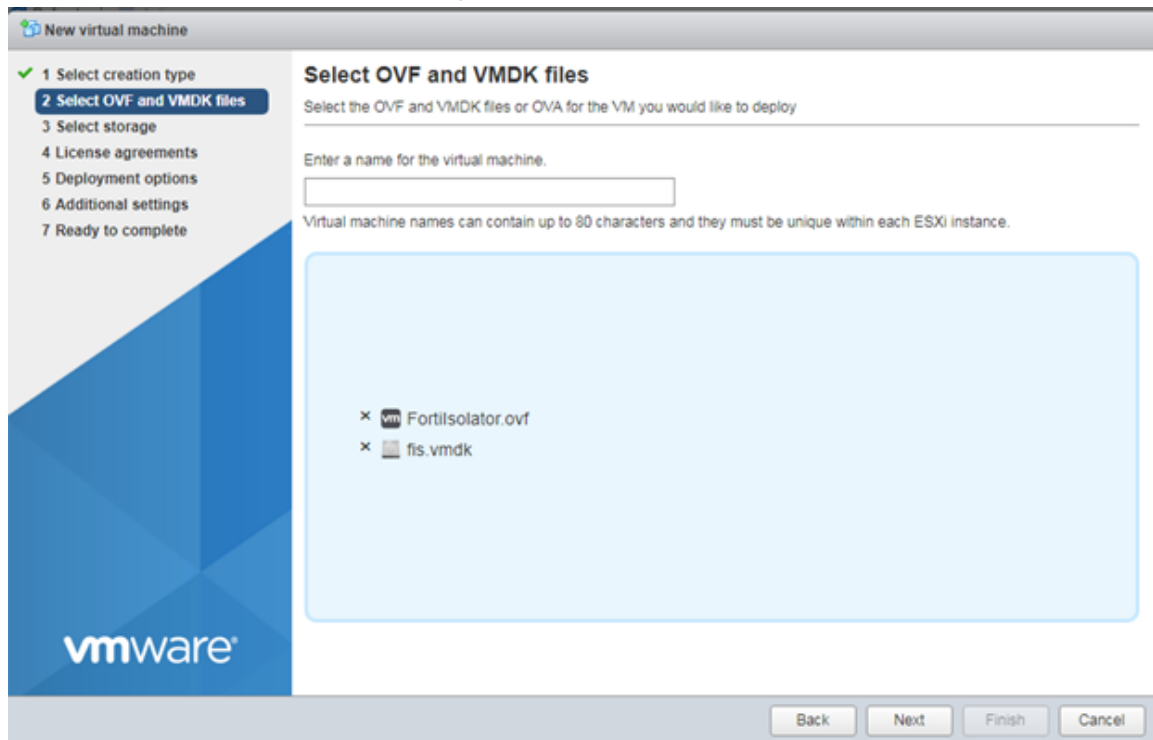
1. In the ESXi home page, click **Virtual Machine**, and then right-click and select **Create/Register VM**.



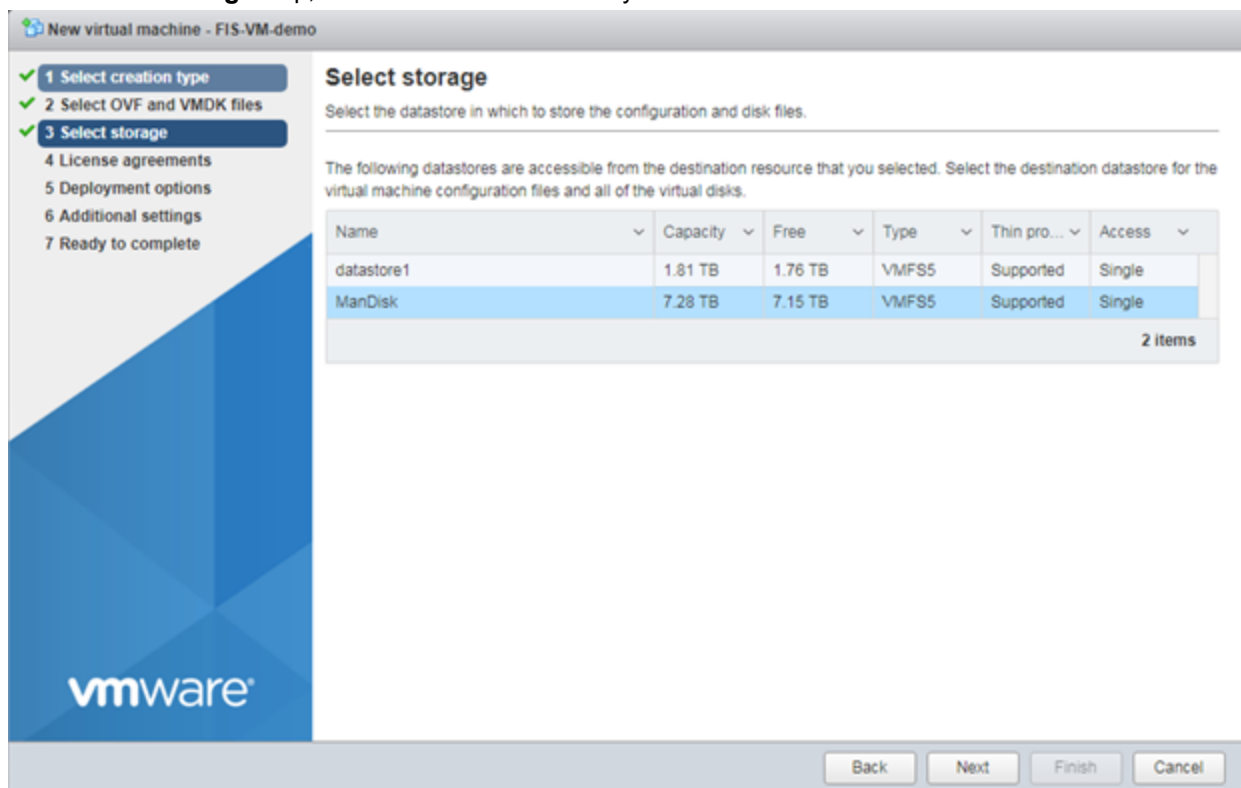
2. In the **Select creation type** step, click **Deploy a virtual machine from an OVF or OVA file**.



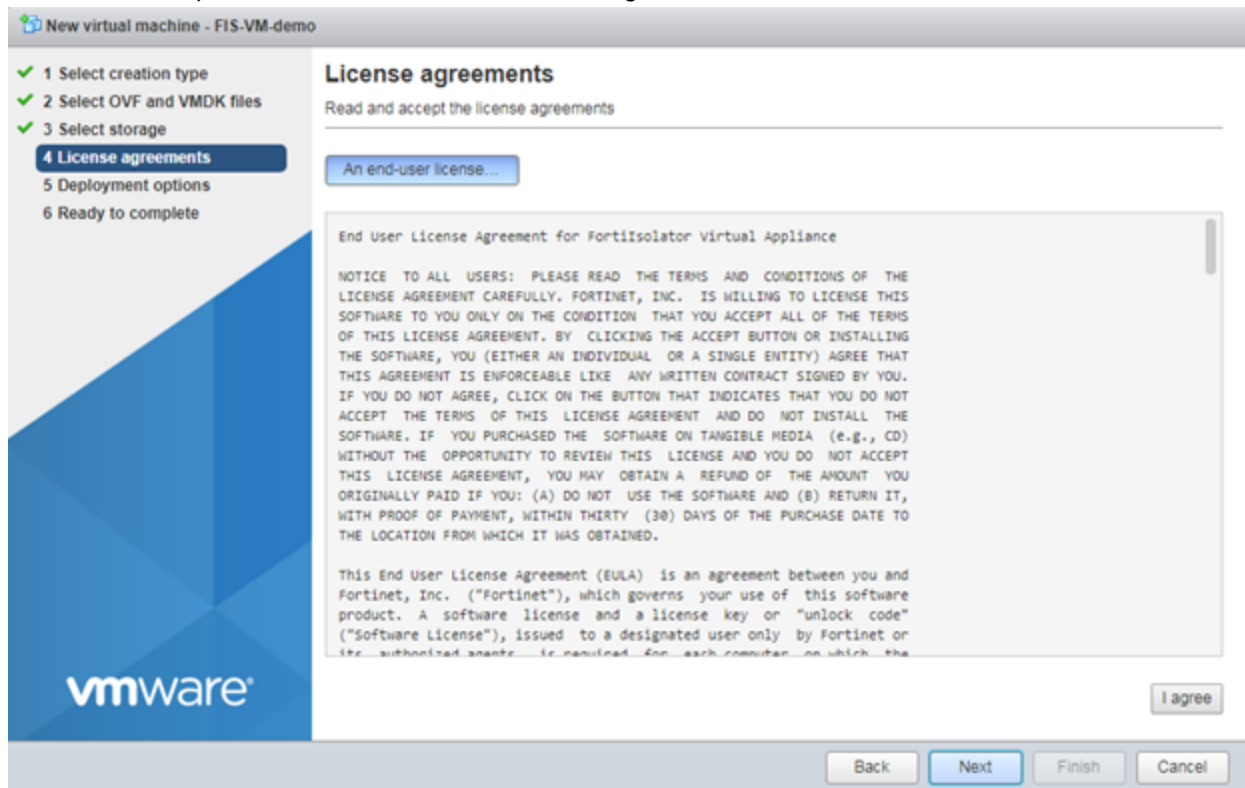
3. In the **Select OVF and VMDK files** step, select both the **Fortisolator.ovf** and **fis.vmdk** files.



4. In the **Select storage** step, select the datastore where you want to install the Fortisolator VM.

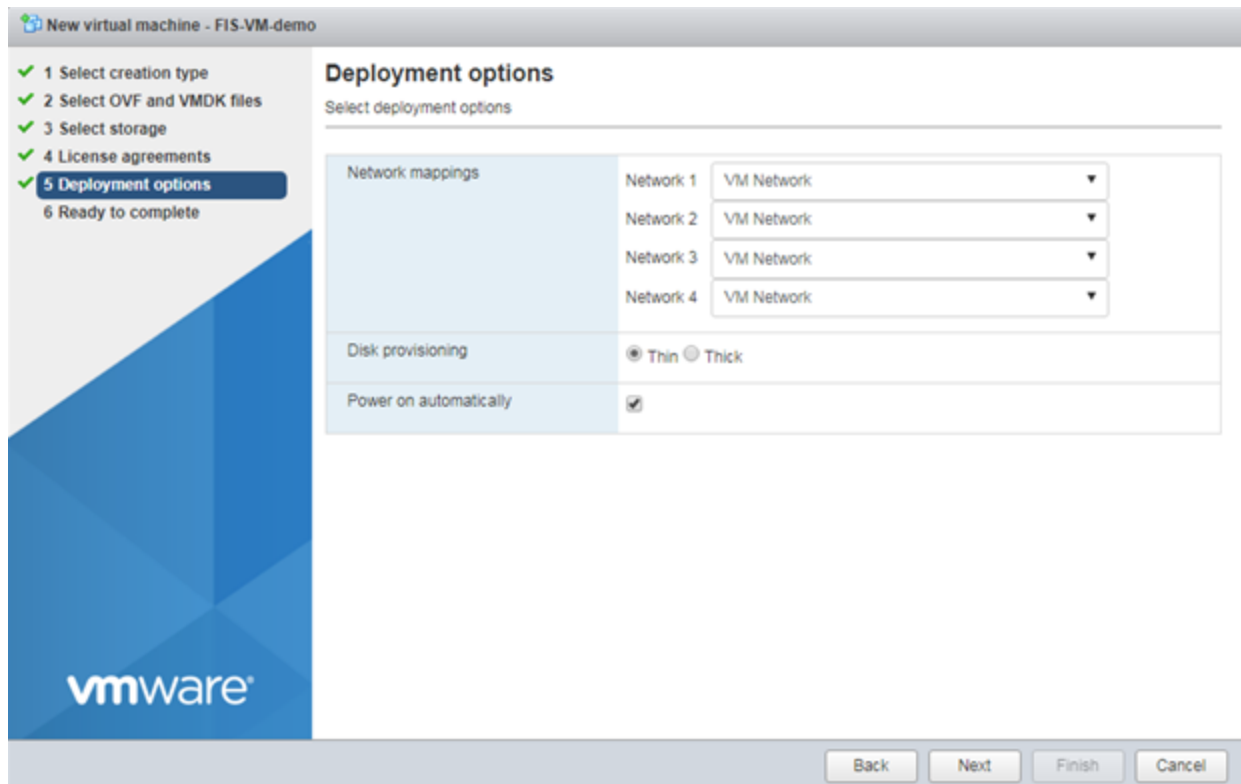


5. Review and accept the Fortisolator End User License Agreement.

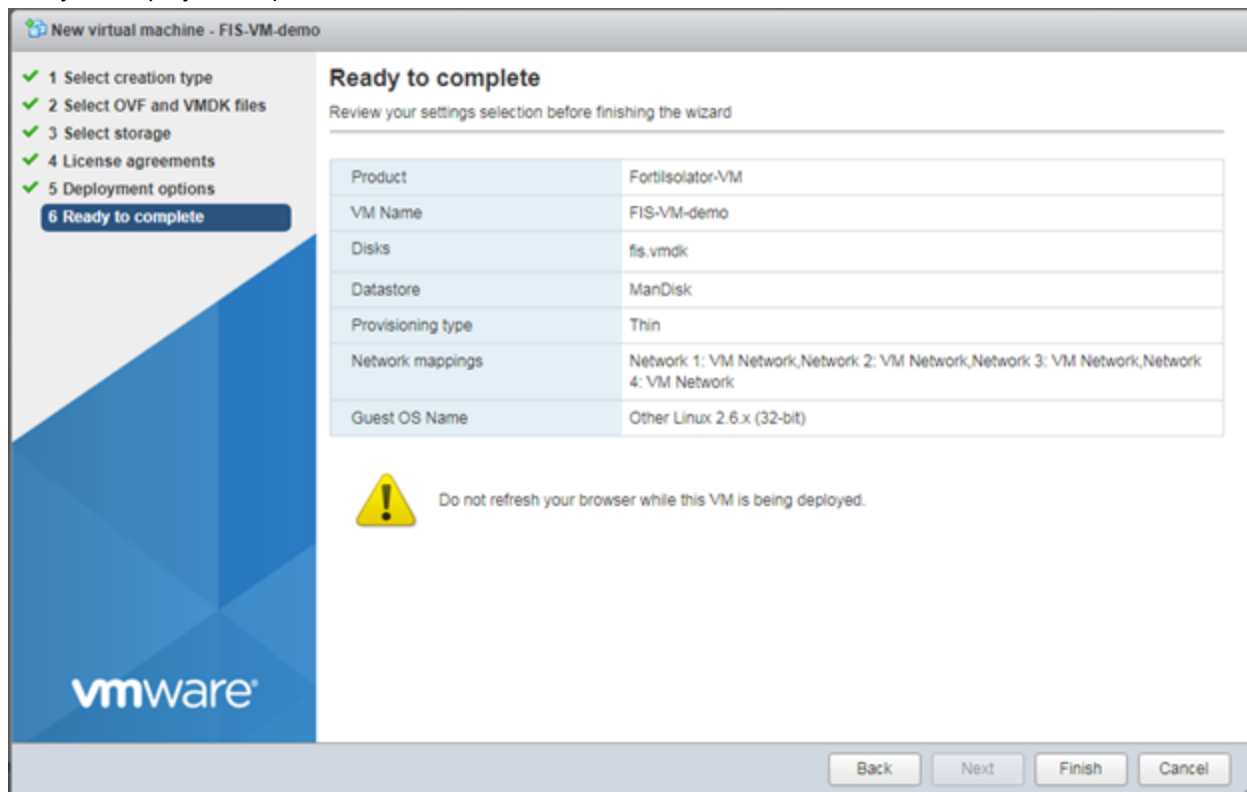


6. In the **Deployment options** step, configure **Network mappings** with four network interfaces accordingly:

- Network 1: Internal Interface
- Network 2: External Interface
- Network 3: Management Interface
- Network 4: HA Interface

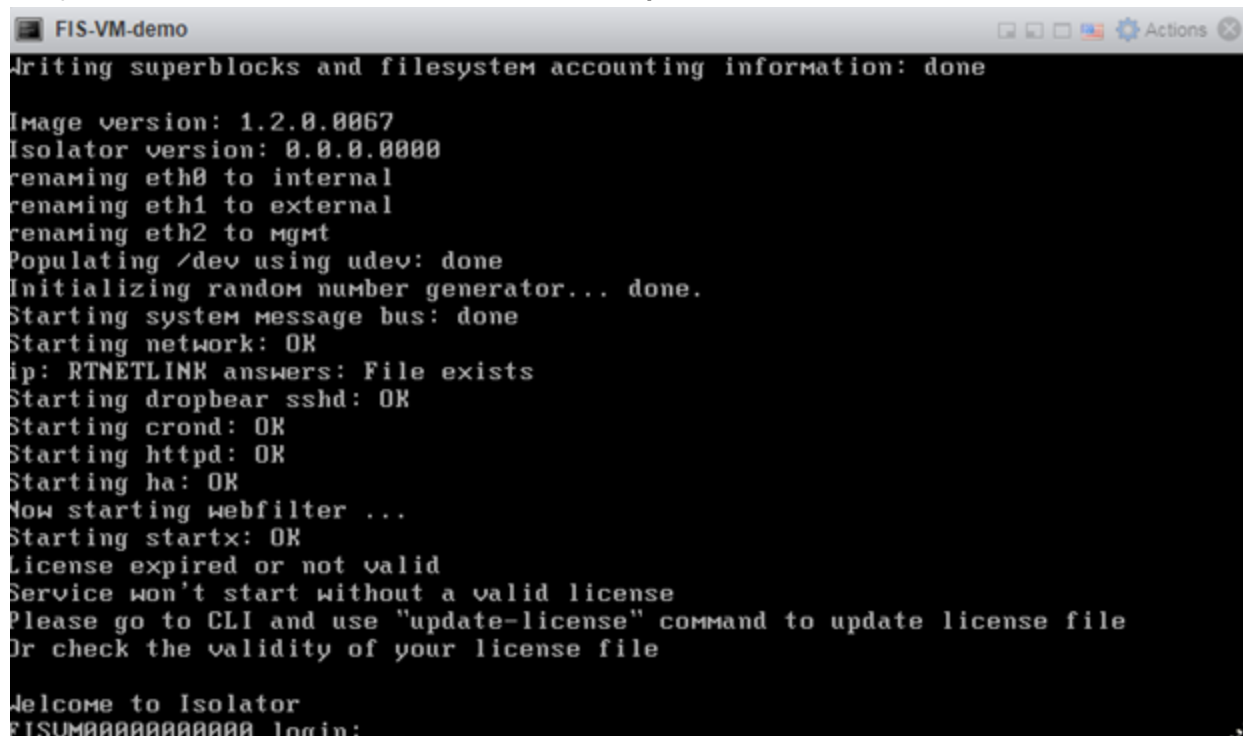


7. Configure **Disk provisioning**, and select the **Power on automatically** checkbox.
8. Verify the deployment options, and click **Finish**.



9. To start the VM, right-click the Fortisolator VM name, and select **Power > Power on**.

10. To open the Fortisolator VM console, click **Console > Open browser console**.



```

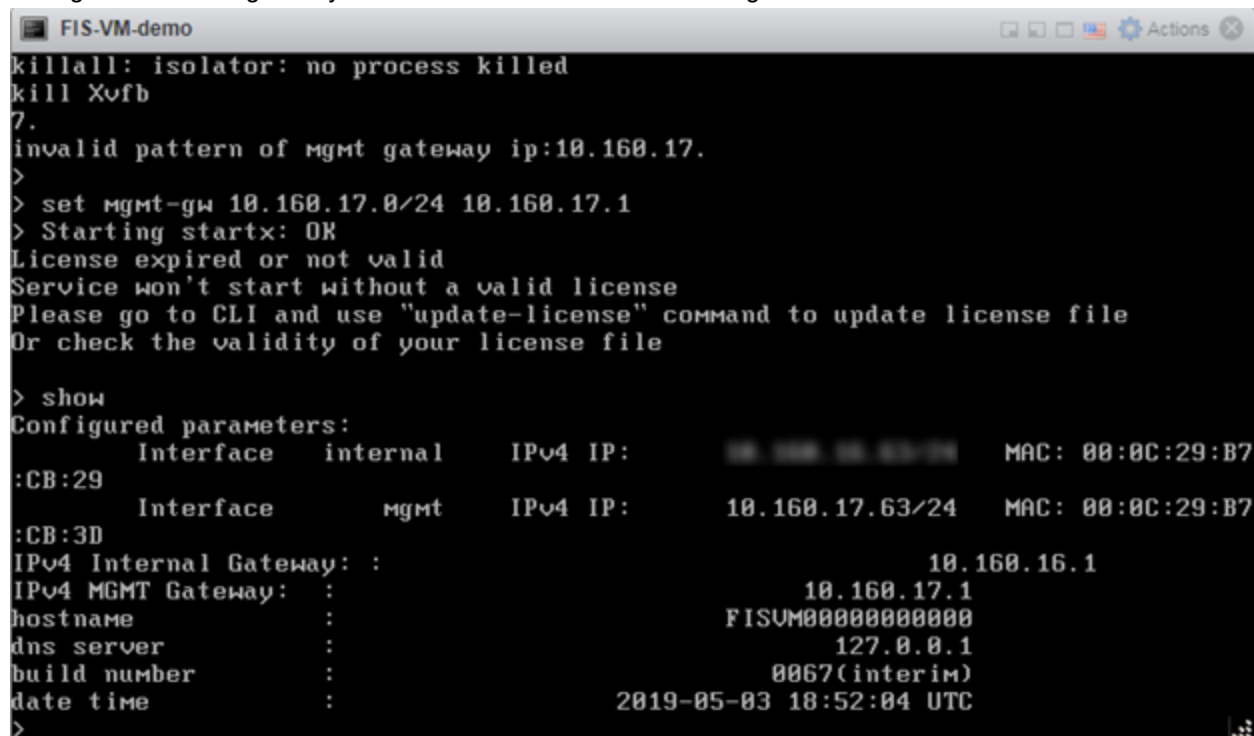
FIS-VM-demo
Writing superblocks and filesystem accounting information: done

Image version: 1.2.0.0067
Isolator version: 0.0.0.0000
renaming eth0 to internal
renaming eth1 to external
renaming eth2 to mgmt
Populating /dev using udev: done
Initializing random number generator... done.
Starting system message bus: done
Starting network: OK
ip: RTNETLINK answers: File exists
Starting dropbear sshd: OK
Starting crond: OK
Starting httpd: OK
Starting ha: OK
Now starting webfilter ...
Starting startx: OK
License expired or not valid
Service won't start without a valid license
Please go to CLI and use "update-license" command to update license file
Or check the validity of your license file

Welcome to Isolator
FISUM000000000000 login:

```

11. Log in to Fortisolator. The default username is **admin** and there is no default password.
12. Configure the IP and gateway addresses for the internal and management interfaces.



```

FIS-VM-demo
killall: isolator: no process killed
kill Xvfb
7.
invalid pattern of mgmt gateway ip:10.160.17.
>
> set mgmt-gw 10.160.17.0/24 10.160.17.1
> Starting startx: OK
License expired or not valid
Service won't start without a valid license
Please go to CLI and use "update-license" command to update license file
Or check the validity of your license file

> show
Configured parameters:
      Interface    internal    IPv4 IP:      10.160.17.0/24    MAC: 00:0C:29:B7
:CB:29
      Interface      mgmt      IPv4 IP:      10.160.17.63/24    MAC: 00:0C:29:B7
:CB:3D
IPv4 Internal Gateway: :                10.160.16.1
IPv4 MGMT Gateway:    :                10.160.17.1
hostname              :                FISUM000000000000
dns server             :                127.0.0.1
build number          :                0067(interim)
date time              :                2019-05-03 18:52:04 UTC
>

```

13. To verify that the internet connection works, ping 8.8.8.8.
14. To access the Fortisolator web portal, use the management IP address (for example, <http://10.160.17.63>).

Setup

The default IP address of the Fortisolator management interface is 192.168.1.99. To perform the initial configuration, connect a device to the management interface and configure the device with an IP address to 192.168.1.1/24. You can access Fortisolator using SSH or the Fortisolator GUI. The default username is **admin** and there is no default password.

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

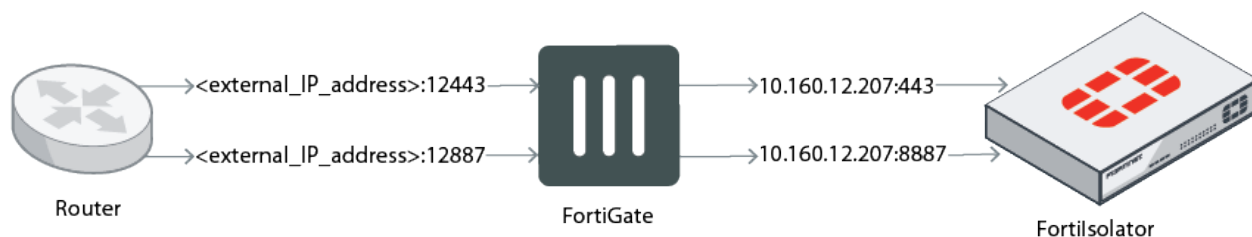
You can perform the initial configuration using the serial console. For more information, see the [Fortisolator 1000F QuickStart Guide](#).

Port forwarding

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

For example, if two networks, one external and one internal, connect to a FortiGate device, when IP addresses on the external network are accessed, traffic is redirected to the internal IP addresses on Fortisolator. 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 Fortisolator	10.160.12.207
Router redirections	<ul style="list-style-type: none"> <external_IP_address>:12443 > 10.160.12.207:443 <external_IP_address>:12887 > 10.160.12.207:8887

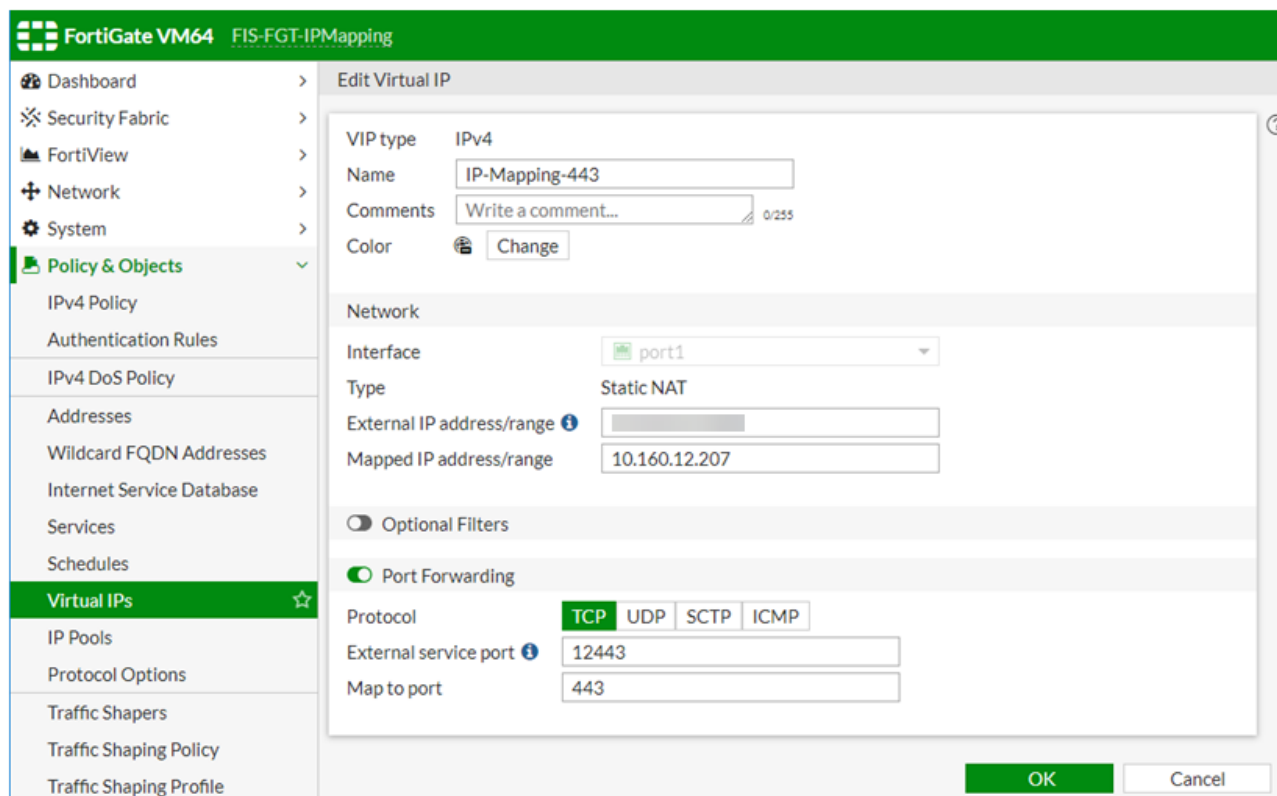
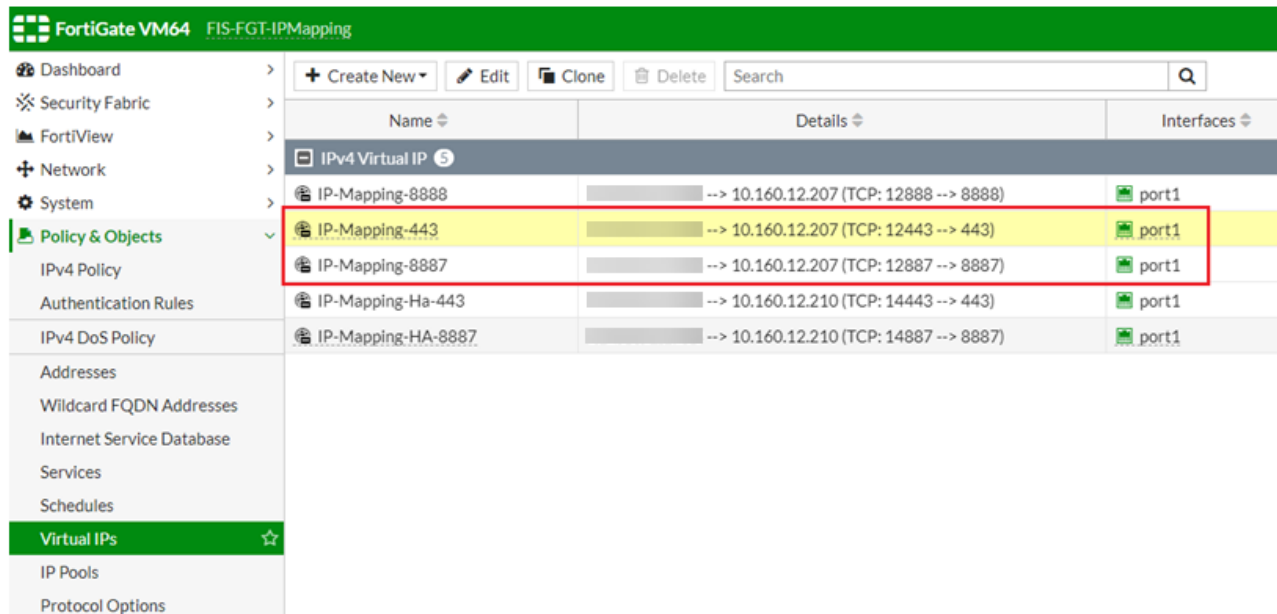


Configuring port forwarding in non-HA mode

FortiGate configuration

Complete the following steps in the FortiGate UI.

1. Go to **Policy & Objects > Virtual IPs**.
2. Create two IPv4 virtual IPs with the following information:
 - **IP-Mapping-443**: <external_IP_address> > 10.160.12.207 (TCP: 12443 > 443)
 - **IP-Mapping-8887**: <external_IP_address> > 10.160.12.207 (TCP: 12887 > 8887)



FortiGate VM64 FIS-FGT-IPMapping

Edit Virtual IP

VIP type: IPv4

Name: IP-Mapping-8887

Comments: Write a comment... 0/255

Color: Change

Network

Interface: port1

Type: Static NAT

External IP address/range:

Mapped IP address/range: 10.160.12.207

☐ Optional Filters

☒ Port Forwarding

Protocol: **TCP** UDP SCTP ICMP

External service port : 12887

Map to port: 8887

OK **Cancel**

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

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

The screenshot shows the FortiGate VM64 configuration interface. The left sidebar contains the navigation menu with 'Policy & Objects' selected. The main area displays the 'Edit Policy' configuration for a policy named 'p1->to->p2'. The configuration includes:

- Name:** p1->to->p2
- Incoming Interface:** port1
- Outgoing Interface:** port2
- Source:** all
- Destination:** IP-Mapping-443, IP-Mapping-8887
- Schedule:** always
- Service:** ALL
- Action:** ACCEPT (checked), DENY
- Inspection Mode:** Flow-based (selected), Proxy-based
- Firewall / Network Options:**
 - NAT: ☒
 - IP Pool Configuration: Use Outgoing Interface Address
 - Preserve Source Port: ☐
 - Protocol Options: PROX, default
- Security Profiles:**
 - AntiVirus: ☐
 - Web Filter: ☐
 - DNS Filter: ☐
 - Application Control: ☐
 - IPS: ☐

A 'Select Entries' dialog is open on the right, showing a list of addresses. The 'Address' tab is selected, and the list includes 'IP-Mapping-443' and 'IP-Mapping-8887', which are highlighted. The dialog also shows a search bar and a '+ Create' button.

The screenshot shows the FortiGate VM64 configuration interface, specifically the 'Policy & Objects' section. The table below lists the configured policies:

ID	Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
2	p1->to->p2	all	IP-Mapping-443 IP-Mapping-8887	always	ALL	ACCEPT	Enabled	UTM	5.26 GB	
3	p2->to->p1	all	all	always	ALL	ACCEPT	Enabled	UTM	0 B	
0	Implicit Deny	all	all	always	ALL	DENY	Disabled	566.60 MB		

Fortisolator configuration

Use the Fortisolator CLI to configure port forwarding mappings. Use the `fis-ipmap` command in the following format:

```
set fis-ipmap <external_port> <internal_port> <external_IP_address>
```

For example, set `fis-ipmap 12443 12887 <external_IP_address>`

```
> set fis-ipmap 12443 12887 [REDACTED]
The apache will restart
httpd not running, trying to start
> show
Configured parameters:
  Interface    internal    IPv4 IP:      10.160.12.207/24    MAC: 00:0C:29:5F
:50:F1
  Interface    mgmt       IPv4 IP:      10.160.17.202/24    MAC: 00:0C:29:5F
:50:05
IPv4 Internal Gateway:      10.160.12.1
IPv4 MGMT Gateway :        10.160.17.1
hostname :                  N/A
dns server :                208.91.112.52
dns server :                172.30.1.105
build number :              0082(interim)
date time :                 2019-07-15 22:09:48 UTC
ip mapping :
mapping for port 443:        12443
mapping for port 8887:       12887
```

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 ADD <external_IP_address> Mask 255.255.255.255 <FortiGate_IP_address>`.
 For example, `route -p ADD <external_IP_address> MASK 255.255.255.255 10.160.17.89`.

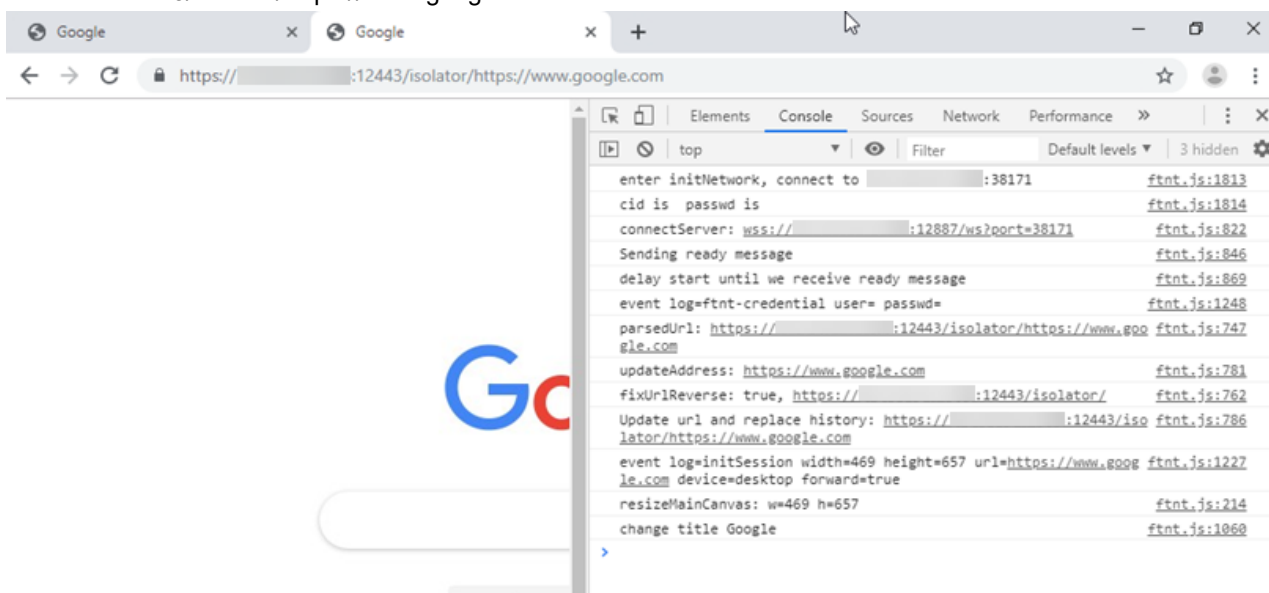
- b. To confirm the setup, type `route print`.

```
C:\WINDOWS\system32>route print

=====
Interface List
  5...00 0c 29 a2 fd 87 .....Intel(R) 82574L Gigabit Network Connection
  1.....Software Loopback Interface 1
=====

IPv4 Route Table
=====
Active Routes:
Network Destination        Netmask          Gateway          Interface        Metric
0.0.0.0                    0.0.0.0          10.160.17.1      10.160.17.205    25
10.160.17.0                255.255.255.0    On-link          10.160.17.205    281
127.255.255.255            255.255.255.255  On-link          127.0.0.1        331
[red box] 255.255.255.255      255.255.255.255  10.160.17.89     10.160.17.205    26
224.0.0.0                  240.0.0.0        On-link          127.0.0.1        331
224.0.0.0                  240.0.0.0        On-link          10.160.17.205    281
255.255.255.255            255.255.255.255  On-link          127.0.0.1        331
255.255.255.255            255.255.255.255  On-link          10.160.17.205    281
=====
Persistent Routes:
Network Address            Netmask          Gateway Address  Metric
[red box] 255.255.255.255      255.255.255.255  10.160.17.89     1
=====
```

3. To verify that it works in a browser, browse to `https://<external_IP_address>:12443/isolator/https://www.google.com`.



Configuring port forwarding in HA mode

FortiGate configuration

Complete the following steps in the FortiGate UI.

1. Go to **Policy & Objects > Virtual IPs**.
2. Create two IPv4 virtual IPs with the following information:
 - **IP-Mapping-443**: <external_IP_address> > 10.160.12.207 (TCP: 14443 > 443)
 - **IP-Mapping-8887**: <external_IP_address> > 10.160.12.207 (TCP: 14887 > 8887)

FortiGate VM64 FIS-FGT-IPMapping

Dashboard > Security Fabric > FortiView > Network > System > **Policy & Objects**

IPv4 Policy > Authentication Rules > IPv4 DoS Policy > Addresses > Wildcard FQDN Addresses > Internet Service Database > Services > Schedules > **Virtual IPs** > IP Pools > Protocol Options > Traffic Shapers > Traffic Shaping Policy

+ Create New Edit Clone Delete Search

Name	Details	Interfaces
IPv4 Virtual IP 5		
IP-Mapping-8888	--> 10.160.12.207 (TCP: 12888 --> 8888)	port1
IP-Mapping-443	--> 10.160.12.207 (TCP: 12443 --> 443)	port1
IP-Mapping-8887	--> 10.160.12.207 (TCP: 12887 --> 8887)	port1
IP-Mapping-Ha-443	--> 10.160.12.210 (TCP: 14443 --> 443)	port1
IP-Mapping-HA-8887	--> 10.160.12.210 (TCP: 14887 --> 8887)	port1

FortiGate VM64 FIS-FGT-IPMapping

Dashboard > Security Fabric > FortiView > Network > System > **Policy & Objects**

IPv4 Policy > Authentication Rules > IPv4 DoS Policy > Addresses > Wildcard FQDN Addresses > Internet Service Database > Services > Schedules > **Virtual IPs** > IP Pools > Protocol Options > Traffic Shapers

Edit Virtual IP

VIP type IPv4

Name IP-Mapping-Ha-443

Comments Write a comment... 0/255

Color Change

Network

Interface port1

Type Static NAT

External IP address/range

Mapped IP address/range 10.160.12.210

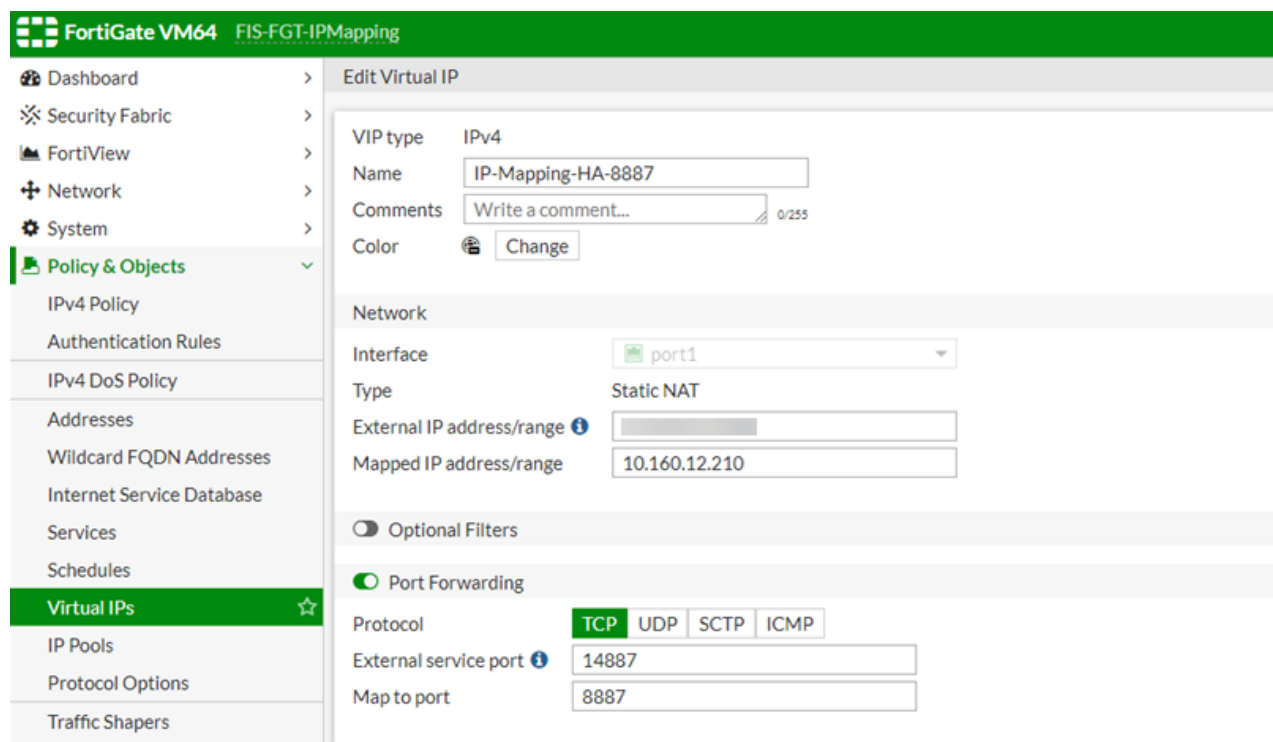
Optional Filters

Port Forwarding

Protocol TCP UDP SCTP ICMP

External service port 14443

Map to port 443




FortiGate VM64 FIS-FGT-IPMapping

Edit Virtual IP


VIP type: IPv4

Name: IP-Mapping-HA-8887


Comments: Write a comment... 0/255

Color:  [Change](#)

Network

Interface:  port1

Type: Static NAT


External IP address/range: 

Mapped IP address/range: 10.160.12.210

☐ Optional Filters

☒ Port Forwarding

Protocol: **TCP** UDP SCTP ICMP

External service port : 14887

Map to port: 8887

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

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

The screenshot shows the FortiGate VM64 configuration interface. The left sidebar lists various configuration sections, with 'Policy & Objects' expanded and 'IPv4 Policy' selected. The main area displays the 'Edit Policy' window for a policy named 'p1->to->p2'. The policy is configured with the following settings:

- Name:** p1->to->p2
- Incoming Interface:** port1
- Outgoing Interface:** port2
- Source:** all
- Destination:** IP-Mapping-Ha-443, IP-Mapping-HA-8887
- Schedule:** always
- Service:** ALL
- Action:** ACCEPT (checked), DENY (unchecked)
- Inspection Mode:** Flow-based (checked), Proxy-based (unchecked)
- Firewall / Network Options:**
 - NAT:** enabled
 - IP Pool Configuration:** Use Outgoing Interface Address
 - Preserve Source Port:** disabled
 - Protocol Options:** PRX (checked), default (unchecked)
- Security Profiles:**
 - AntiVirus: disabled
 - Web Filter: disabled
 - DNS Filter: disabled
 - Application Control: disabled
 - IPS: disabled

The 'Select Entries' dialog is open, showing a list of addresses. The 'Address' tab is selected, and the list includes:

- ADDRESS (7)
- all
- FABRIC_DEVICE
- gmail.com
- login.microsoft.com
- login.microsoftonline.com
- login.windows.net
- none
- ADDRESS GROUP (1)
- Microsoft Office 365
- VIRTUAL IP/SERVER (5)
- IP-Mapping-443
- IP-Mapping-8887
- IP-Mapping-Ha-443
- IP-Mapping-HA-8887

The 'Close' button is visible at the bottom of the dialog.

The screenshot shows the FortiGate VM64 configuration interface. The left sidebar lists various configuration sections, with 'Policy & Objects' expanded and 'IPv4 Policy' selected. The main area displays the 'Policy Lookup' table, which lists several policies. The 'p1->to->p2' policy is highlighted with a red box, showing its configuration details.

ID	Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles
2	p1->to->p2	all	IP-Mapping-Ha-443 IP-Mapping-HA-8887	always	ALL	✓ ACCEPT	✓ Enabled	
3	p2->to->p1	all	all	always	ALL	✓ ACCEPT	✓ Enabled	
0	Implicit Deny	all	all	always	ALL	✗ DENY		

Fortisolator configuration

Use the Fortisolator CLI to configure port forwarding mappings. Use the following commands:

1. `set fis-ipmap <port_map_to_443> <port_map_to_8887> <external_IP_address>`
For example, set `fis-ipmap 12443 12887 <external_IP_address>`.

```
> set fis-ipmap 12443 12887
The apache will restart
httpd not running, trying to start
> show
Configured parameters:
      Interface      internal      IPv4 IP:      10.160.12.207/24      MAC: 00:0C:29:5F
:50:F1
      Interface      mgmt      IPv4 IP:      10.160.17.202/24      MAC: 00:0C:29:5F
:50:05
IPv4 Internal Gateway:      10.160.12.1
IPv4 MGMT Gateway :      10.160.17.1
hostname :      N/A
dns server :      208.91.112.52
dns server :      172.30.1.105
build number :      0082(interim)
date time :      2019-07-15 22:09:48 UTC
ip mapping :
mapping for port 443:      12443
mapping for port 8887:      12887
```

2. `set fis-ipmap-vip <external IP> <port_map_to_443> <port_map_to_8887>`
For example, set `fis-ipmap-vip <external_IP_address> 14443 14887`.

```
> set fis-ipmap-vip 172.30.147.207 14443 14887
> show
Configured parameters:
      internal      IPv4 IP:      172.30.157.63/24      MAC: 00:0C:29:C8:7C:8F
      mgmt      IPv4 IP:      172.30.156.63/24      MAC: 00:0C:29:C8:7C:A3
IPv4 Internal Gateway:      172.30.157.254
hostname :      FISUM1TM20000048
dns server :      208.91.112.52
dns server :      208.91.112.53
build number :      0054(interim)
date time :      2020-05-20 20:37:59 UTC
ip mapping :
mapping for port 443:      12443
mapping for port 8887:      12887
ip mapping (VIP) :
mapping for port 443 (VIP):      14443
mapping for port 8887 (VIP):      14887
```

3. `set fis-ipmap-ha <priority> <external_IP_address> <internal_IP_address:slave_1> <port_map_to_443> <port_map_to_8887>`
For example, set `fis-ipmap-ha 10 <external_IP_address> <internal_IP_address:slave_1> 12443 12887`

```
> set fis-ipmap-ha 10 172.30.147.207 172.30.157.63 12443 12887
> show
Configured parameters:
      internal      IPv4 IP:      172.30.157.63/24      MAC: 00:0C:29:C8:7C:8F
      mgmt      IPv4 IP:      172.30.156.63/24      MAC: 00:0C:29:C8:7C:A3
IPv4 Internal Gateway:      172.30.157.254
hostname :      FISUM1TM20000048
dns server :      208.91.112.52
dns server :      208.91.112.53
build number :      0054(interim)
date time :      2020-05-20 20:48:40 UTC
ip mapping :
mapping for port 443:      12443
mapping for port 8887:      12887
ip mapping (VIP) :
mapping for port 443 (VIP):      14443
mapping for port 8887 (VIP):      14887
>
```

Client system configuration

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

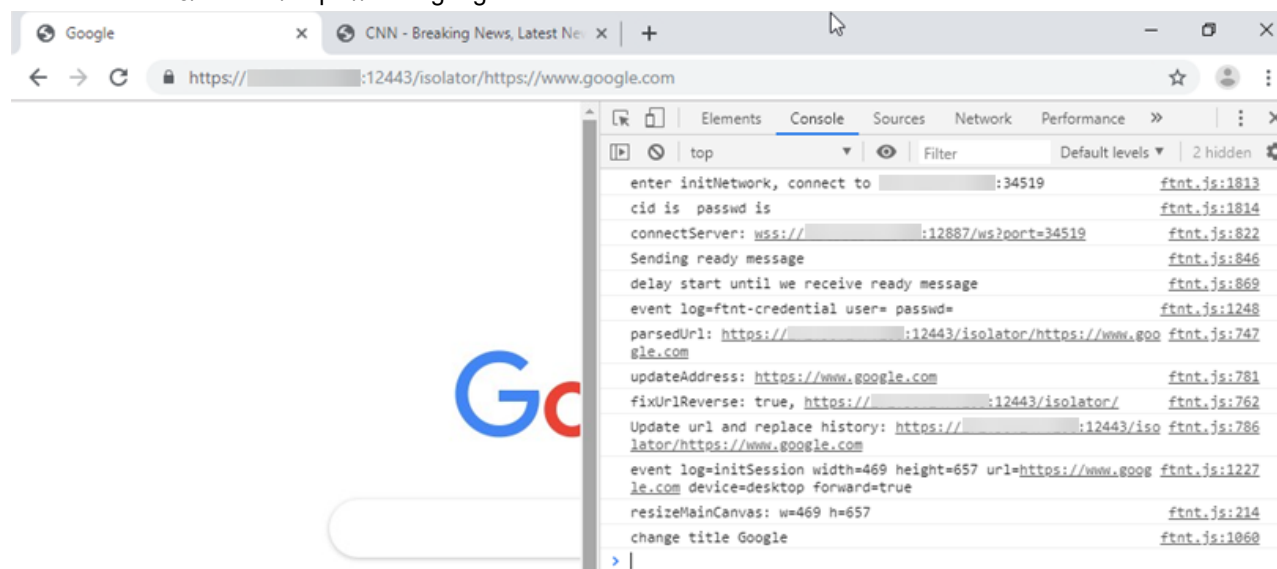
1. In Windows 10, launch CMD as administrator.
2. Use the following commands to add the FortiGate IP address to the routing table on the client system:
 - a. At the command prompt, type `route ADD <external_IP_address> Mask 255.255.255.255 <FortiGate_IP_address>`.
For example, `route -p ADD <external_IP_address> MASK 255.255.255.255 10.160.17.89`.
 - b. To confirm the setup, type `route print`.

```
C:\WINDOWS\system32>route print
=====
Interface List
  5...00 0c 29 a2 fd 87 .....Intel(R) 82574L Gigabit Network Connection
  1.....Software Loopback Interface 1
=====

IPv4 Route Table
=====
Active Routes:
Network Destination        Netmask          Gateway          Interface        Metric
    0.0.0.0                0.0.0.0         10.160.17.1      10.160.17.205     25
   10.160.17.0            255.255.255.0       On-link         10.160.17.205     281
  127.255.255.255        255.255.255.255       On-link         127.0.0.1        331
  [redacted] 255.255.255.255    10.160.17.89    10.160.17.205     26
   224.0.0.0             240.0.0.0       On-link         127.0.0.1        331
   224.0.0.0             240.0.0.0       On-link         10.160.17.205     281
  255.255.255.255        255.255.255.255       On-link         127.0.0.1        331
  255.255.255.255        255.255.255.255       On-link         10.160.17.205     281
=====
Persistent Routes:
Network Address          Netmask  Gateway Address  Metric
  [redacted] 255.255.255.255    10.160.17.89      1
=====
```

3. To verify that it works in a browser, browse to `https://<external_IP_`

address>:14443/isolator/https://www.google.com.



Dashboard

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

Changing host name

To change the **Host Name** from **GUI**:

Steps

1. From the administration portal, click **Dashboard**, and find 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 hostname can start with English characters/digits, but must not end with a hyphen. It may contain only the ASCII letters 'a' through 'z' (in a case-insensitive manner), the digits '0' through '9', and the hyphen ('-'). No other symbols, punctuation characters, or white space are permitted.

Configuring system time

Use this procedure to configure time settings for Fortisolator from GUI.

Steps

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

Fortisolator VM requires a valid license in order to allow all features fully functioning. To obtain a license, please obtain a registration code, go to **Fortinet Service & Support** (<https://support.fortinet.com/>) to register the code for Fortisolator VM product, and download the license file.

To upload a license from **GUI**:

Steps

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 on **Choose File** to upload the license file.
4. Click **Submit** to finish. This will take several minutes and system will reboot upon finish.



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

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

Configuration and Certificate backups

Once you successfully configure the Fortisolator, it is important to backup the configuration. In some cases, you may need to reset the Fortisolator 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 backup 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, backup the configuration before any upgrades of the Fortisolator's firmware. Should anything happen to the configuration during the upgrade, you can easily restore the saved configuration.

Always backup 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 Fortisolator 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 “**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 Fortisolator 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 Fortisolator. It takes few minutes.

Backing up Fortisolator CA Certification

To backup the Fortisolator CA Certificate:

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

Restoring a Fortisolator CA Certificate

To restore a Fortisolator CA Certificate:

1. From the administration portal, click **Dashboard**, and find the **Isolator CA Certificate** widget.
2. In the **Isolator CA Certificate** field, click **Backup/Restore**, it navigates to **Isolator CA Certificate** page.
3. In **Isolator CA Certificate** page, under **Restore** section, **Choose File** to locate your CA Certificate.
 - The source of the CA Certificate 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 CA Certificate and reboot the Fortisolator. It takes few minutes.

Re-Generating a Fortisolator CA Certificate

To re-generate a Fortisolator CA Certificate:

1. From the administration portal, click **Dashboard**, and find the **Isolator CA Certificate** widget.
2. In the **Isolator CA Certificate** field, click **Backup/Restore**; it navigates to the **Isolator CA Certificate** page.
3. In **Isolator CA Certificate** page, under **Re-Generate Isolator certificate** section, **Click here** to generate CA

Certificate.

- This will re-generate CA Certificate and reboot the Fortisolator. It takes few minutes.

Network

The default IP address of the Fortisolator management interface is 192.168.1.99. To perform the initial configuration, connect a device to the management interface and configure the device with an IP address to 192.168.1.0/24 subnet. You can access Fortisolator using SSH or the Fortisolator GUI. The default username is **admin** and there is no default password.

Use the Fortisolator 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 Fortisolator 1000F QuickStart Guide.

Interfaces

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

Setting the Management IP address

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

1. Go to Portal > Network > Interface
2. Edit the existing Gateway or Create New
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**, follow this format:

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

Setting the Internal IP address and Gateway

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

1. Go to 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**, follow format:

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

Setting the External IP address and Gateway

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

1. Go to 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**, follow format:

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

Setting the HA IP address and Gateway

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

1. Go to 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**, follow format:

```
> 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**:

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

To setup **system** DNS from **CLI**:

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

System routing

Configuring routing settings

Use this procedure to configure routing settings for FortiSolator.

Adding a static route

Use this procedure to add a static route.

Steps

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

Use this procedure to edit a static route.

Steps

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

Use this procedure to delete a static route.

Steps

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 Device dropdown.
3. Click **OK** to save it.

New Static Route	
Destination IP/Mask:	<input type="text" value="0.0.0.0/0"/>
Gateway:	<input type="text" value="192.168.1.254"/>
Device:	<input type="text" value="mgmt"/>

To set up system routing for **Management** IP from **CLI**:

```
> set mgmt-gw/<subnet> <gateway>
e.g.
> set mgmt-gw 0.0.0.0/0 192.168.1.254
```

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 Device dropdown.
3. Click **OK** to save it.

New Static Route	
Destination IP/Mask:	<input type="text" value="0.0.0.0/0"/>
Gateway:	<input type="text" value="192.168.2.254"/>
Device:	<input type="text" value="internal"/>

To set up system routing for **Internal** IP from **CLI**:

```
> set internal-gw/<subnet> <gateway>
e.g.
> set internal-gw 0.0.0.0/0 192.168.2.254
```

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 Device dropdown.
3. Click **OK** to save it.

New Static Route	
Destination IP/Mask:	<input type="text" value="0.0.0.0/0"/>
Gateway:	<input type="text" value="192.168.3.254"/>
Device:	<input type="text" value="external"/>

To set up system routing for **External** IP from **CLI**:

```
> set external-gw/<subnet> <gateway>
```

e.g.

```
> set external-gw 0.0.0.0/0 192.168.3.254
```

To set up system routing for **HA** IP from **GUI**:

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

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

To set up system routing for **HA** IP from **CLI**:

```
> set ha-gw/<subnet> <gateway>
```

e.g.

```
> set ha-gw 0.0.0.0/0 192.168.4.254
```

Configuring forwarding server

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

Configure forwarding server from GUI

Steps

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**.

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 Fortisolator covers the following:

- Administrators
- HA
- Login disclaimer
- Upgrade

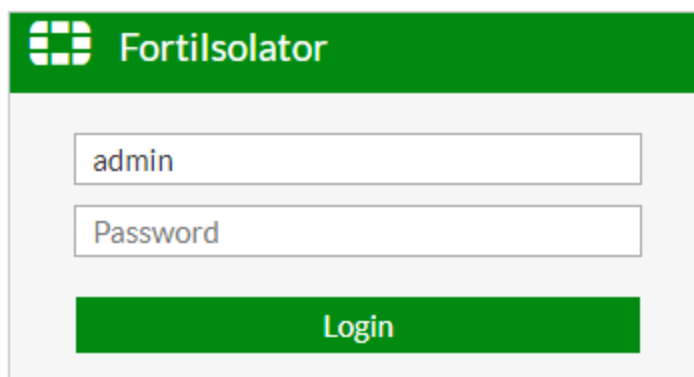
Administrators

Accessing the Fortisolator administration portal

Logging in as administrator

Steps

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



The screenshot shows the Fortisolator login interface. It features a green header bar with the Fortisolator logo and name. Below this is a light gray rectangular box. Inside this box, there are two input fields: the first is labeled 'admin' and the second is labeled 'Password'. Below these fields is a green button with the text 'Login' in white.

2. Type in your username and password to access the administration portal. The default username is **admin** with no password.
3. Click **Login**. You will be brought to the dashboard of the administration portal.

Changing the administrator password

Steps

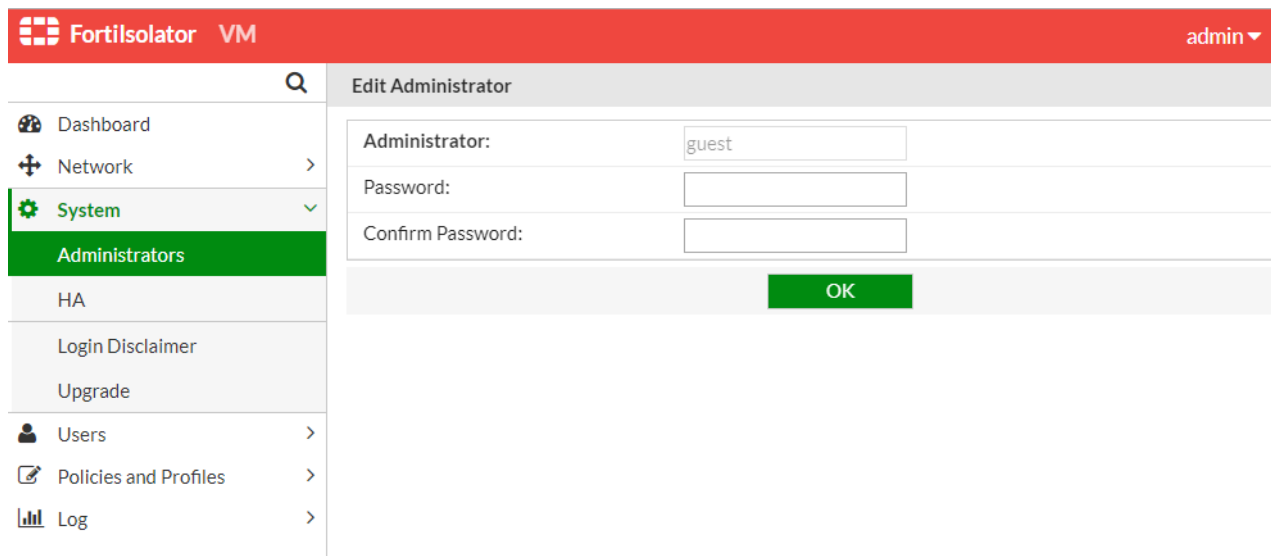
1. In the top-right corner of the administration portal, click the admin username.
2. Click **Change Password**.
3. In the **Password** field, type the new password.
4. In the **Confirm Password** field, type the new password again.
5. Click **OK**.

Setting up guest administer account

A guest administer 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.

Steps

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**, and defaults to no password. Add a password if desired.



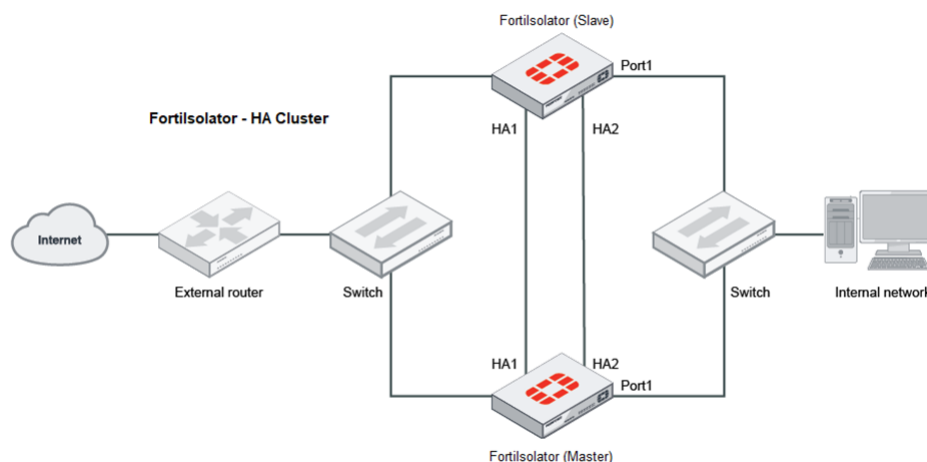
The screenshot shows the Fortisolator VM administration portal. The top header is red with the Fortisolator logo and 'VM' text on the left, and the username 'admin' with a dropdown arrow on the right. A left sidebar contains a search icon and a list of menu items: Dashboard, Network, System (highlighted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

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.

Fortisolator provides an HA solution whereby Fortisolator can find other member Fortisolators to negotiate and create a cluster. A Fortisolator HA cluster consists of at least two Fortisolator (members) configured for HA operation. All Fortisolators in the cluster do not need to be the same model (e.g. FIS 1000F, KVM, or ESXi), but they have to have the same firmware installed. Cluster members must have the same configuration, except for their IP address and priority in the HA settings. The cluster works like a device but always has a hot backup device.



How it works

Fortisolator allows each HA cluster to have up to 255 HA nodes. Each node must have the same settings for:

- Virtual IP
- Group ID
- Password
- Schedule Type
- Interface Name
- Lost Threshold
- Hello Holddown
- Interval

Each node must be assigned a unique priority ID, from 0 to 255, where 0 is the highest priority. The node with the highest priority ID in the cluster will be the master device for that HA cluster.

Fortisolator currently saves HA-related information and configuration into an internal database. The database will be synchronized from master to slaves every time the master has changes.

The HA-related information that is saved into the database includes:

- User Groups (Group Name, Group Policy Name)

- Isolator profile (Isolator Profile Name, Max Download Size, Max Upload Size, Limit of view only, Image Quality, Video Frame Rate, Use doc-rewrite when scanning file, Scan files for malware, Permit for Right-Click, Send file to FortiSandbox, FortiSandbox IP, FortiSandbox Administrator Name, and FortiSandbox Password)
- Web Filter profile (Web Filter profile name, actions of Web Filter category, white list, black list)
- ICAP Profile (ICAP Profile Name, IP address, Port number, Service, Action when server fails)
- Default policy (Default Isolator Profile Name, Default Web Filter Profile Name, Default ICAP Profile Name)
- Agent server (Agent Server ID, Enable/Disable, IP address, Port number, Password for Agent server)
- Polling server (Polling Server ID, Enable/Disable, IP address, Domain name, Port number, Username, Password, Max History, Frequency)

In an HA cluster, when making changes to any of these settings, all information will be saved into the master device, then synchronized to all slave devices. After this, only the master device's database is able to write. All slave devices will read from the master database and update to their own databases. Thus, all devices can read from their own database locally.

Fortisolator uses HA interface/port for database synchronization and heartbeat. HA interface/port is designed for better performance purpose, but it can choose other interface/port as well.

The VIP address will be put on interface, so it has to be the same subnet as internal interface. This is the IP for the web browsers access. Only the master device has VIP.

In HA mode, all web browsers will access VIP address, through IP Forwarding mode or Proxy mode:

1. IP Forwarding mode:

Web browser connects to VIP of master device first. Master receives request, forwards it to a node in the cluster immediately. The node can be itself (master) or any other nodes (slave). So after the first request to VIP, all the following requests are sent to an internal IP of a node in the cluster, which includes the master and all slaves.

2. Proxy mode:

Web browser connects to VIP of master device, and it will keep communicating (talking) to master. The master device web socket connection will connect to each cluster, including itself (master) or any of other nodes (slaves), on their internal IP. Then the corresponding web browser will run in that node.

Example

The following is an example of an HA Cluster setup.

HA Settings

Note: HA will restart after the HA settings are changed

Enable: ☒

Virtual IP:

Priority:

Cluster Settings

Group Id:

Password: Change

Allow Override: ☐

Schedule Type:

Interface Name	Lost Threshold	Hello Holddown	Interval
<input type="text" value="mgmt"/>	<input type="text" value="10"/>	<input type="text" value="5"/>	<input type="text" value="10"/>

Apply

To configure HA (Slave) 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
```

Verify HA Cluster Information in Master node from GUI - Dashboard:

HA Cluster Information	
Number of Slaves	1
Is Master	Yes
Other Machines:	
priority	IP
2	172.30.157.32

Verify HA Cluster Information in Master node from CLI:

```
show ha-all
  enabled : Enabled
  gid : 31
  lost threshold : 10
  interval : 10
  holddown : 5
  priority : 1
  allow override : 0
  schedule : Round Robin
  vip : 172.30.157.99
  password : ffff18ff28ff38ffff60ff3678ff2e03
  interface : mgmt
```

```
Cluster Information
Number of Slave : 1
Is Master : Yes
(Slaves)IP Priority
172.30.157.32 : 2
```

Verify HA Cluster Information in Slave node from GUI - Dashboard:

HA Cluster Information	
Is Master	False
Master IP	172.30.157.31
Other Machines:	
priority	IP
1	172.30.157.31

Verify HA Cluster Information in Slave node from CLI:

```
show ha-all
  enabled : Enabled
  gid : 31
  lost threshold : 10
  interval : 10
  holddown : 5
  priority : 2
  allow override : 0
  schedule : Round Robin
  vip : 172.30.157.99
  password : ffff18ff28ff38ffff60ff3678ff2e03
  interface : mgmt
```

```
Cluster Information
Number of Slave : 1
Is Master : No
(Master)IP Priority
172.30.157.31 : 1
(Slaves)IP Priority
```

Login disclaimer

Configuring the login disclaimer

Steps

1. To configure the login disclaimer, go to **System > Login Disclaimer**.

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

The screenshot shows the Fortisolator VM web interface. The top header is red with the Fortisolator logo and 'VM' text on the left, and 'admin' with a dropdown arrow on the right. A left sidebar contains a search icon and a list of menu items: Dashboard, Network, System (highlighted with a green bar and a checkmark), Administrators, HA, Login Disclaimer (highlighted with a green bar), Upgrade, Users, Policies and Profiles, and Log. The main content area is titled 'Login Disclaimer'. It features a 'Disclaimer:' label followed by a text area containing the text: 'PREWARNINGWARNINGWARNINGWARNING This is a private computer system. Unauthorized access or use is prohibited and subject to prosecution and/or disciplinary action. All use of this system constitutes consent to monitoring at all times and users are not entitled to any expectation of privacy. If monitoring reveals possible evidence of violation of criminal statutes, this evidence and any other related information, including identification information about the user, may be provided to law enforcement officials. If monitoring reveals violations of'. Below the text area is a checkbox labeled 'Show disclaimer on login'. At the bottom right of the main content area is a green 'OK' button.

Fortisolator VM admin

Search

Dashboard

Network

System

Administrators

HA

Login Disclaimer

Upgrade

Users

Policies and Profiles

Log

Login Disclaimer

Disclaimer:

PREWARNINGWARNINGWARNINGWARNING

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

☐ Show disclaimer on login

OK

Upgrade

This section the following ways to upgrade Fortisolator firmware:

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

Upgrading the firmware by GUI

Use this procedure to upgrade a Fortisolator hardware appliance or VM using a web browser. You can use the Fortisolator UI or Fortisolator CLI to perform the upgrade.

To upgrade the firmware by Web

This feature applies to both Fortisolator hardware appliances and Fortisolator VM.

1. Log into the Fortisolator 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.
4. Click **Submit** to upgrade the firmware.

The Fortisolator 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 Fortisolator hardware appliances, such as Fortisolator 1000F.

1. Log into the Fortisolator 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 only applies to Fortisolator hardware appliances, such as Fortisolator 1000F.

1. Log into the Fortisolator CLI as the admin administrative user.
2. Insert the USB that contains the previously downloaded firmware image.
3. Enter cli command "system-upgrade".

The Fortisolator unit starts to copy the new firmware image from the USB device and saves it into local hard disk, then backs up the current configuration, and performs upgrade to the new firmware version. This process takes a few minutes.

Users

Covers the Users section of Fortisolator.

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

Server

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.

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

To manage LDAP servers on Fortisolator, go to **User > Server**.

Create or edit a LDAP server

To add a new LDAP server:

1. In the Server page, select **Create New** from the toolbar. The Create New Server page opens.
2. Under Server Type dropdown list, select **Agent Server**.
3. Configure the following:

ID	0 – 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

Create New Server : Step 2

Id	1
Enable	<input checked="" type="checkbox"/>
IP Address	12.34.56.78
Port	8000
Password	*****
Confirm Password	*****
Server Type	Agent Server

OK

- Click OK.
- The Fortisolator checks the connection. The connection must be successful for the FSSO Agent server to work.

Fortinet Single Sign On (FSSO) Agent server configuration

Fortinet Single Sign On Agent Configuration

☒ Monitoring user login events ☒ Support NTLM authentication

Collector Agent Status: RUNNING

Listening ports
 FortiGate: 8000 FortiGate SSL: 8001 DC Agent: 8002

Logging
 Log level: Debug Log file size limit(MB): 10 View Log
☐ Log login events in separate logs View Logon Events

Authentication
☐ Require authenticated connection from FortiGate Password: *****

Timers
 Workstation verify interval (minutes): 5
 Dead entry timeout interval (minutes): 480
 IP address change verify interval (seconds): 60
☐ Cache user group lookup result
 Cache expire in (minutes): 60 Clear Group Cache

Common Tasks
 Show Service Status
 Show Monitored DCs
 Show Logon Users
 Select Domains To Monitor
 Set Directory Access Information
 Set Group Filters
 Set Ignore User List
 Sync Configuration With Other Agents
 Export Configuration

Advanced Settings Save&close Apply Default Help

User definition

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

Steps

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

Steps

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, please use CLI command

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

e.g.

```
> set group group_new 0 policy_new  
> show group  
    Group Name : group_new  
    Server ID  : 0  
    Policy     : policy_new  
>
```

The screenshot shows the FortiSolator VM administration portal. On the left is a sidebar with a search icon and a list of navigation items: Dashboard, Network, System, Users (highlighted with a green bar and a checkmark), Server, User Definition, User Groups (highlighted with a green bar), Policies and Profiles, and Log. The main content area is titled 'Create New Group' and contains three input fields: 'Group Name' (text box with 'group_new'), 'Group Type' (text box with 'Local'), and 'Policy Name' (dropdown menu with 'policy_new' selected). An 'OK' button is located at the bottom right of the form.

Policies and profiles

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

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

Profile

Creating Isolator browsing profile

Creating Isolator browsing profile from GUI

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

Steps

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.
Max download size / Max upload size	Type in the maximum file size in megabytes for uploading and downloading files.
Limit of view only	By selecting the Limit of view only box, you 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	Increase or decrease bandwidth usage.
Video frame rate	Increase or decrease bandwidth usage.
Use doc-rewrite when scanning file	Allow rewriting of documents during file scanning such that embedded links in the file are rendered inactive.
Scan files for malware	<p>Scans files when uploading or downloading through Fortisolator.</p> <p>Enable</p> <ul style="list-style-type: none"> • Fortisolator will scan the file for malware or viruses. If malware or viruses are detected, it will prompt a message to inform the user that "Virus is discovered in the file." • If the file does not contain a virus, Fortisolator then allows the user to upload or download the file normally. <p>Disable</p>

- Will not scan files. Files will be uploaded and downloaded normally.

Permit for Right-Click

Allows the client user to right click on mouse to display a menu.



Feature only works when you:

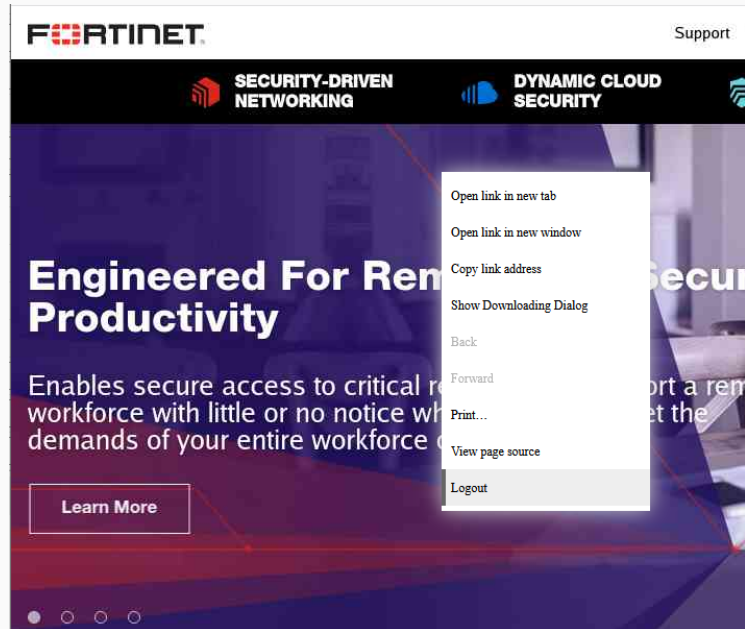
- Disable "Limit of view only."

Print

User can print the current page as a PDF file.

Logout

Log out from the current session.



Send file to FortiSandbox



To enable FortiSandbox scanning, you need to also enable:

- Scan file for malware

Fortisolator provides the option to send files to FortiSandbox to scan for virus or malware. When uploading or downloading a file through Fortisolator, the file will send to FortiSandbox.

If FortiSandbox detects the file as containing virus or malware, it blocks the file and sends back the result to Fortisolator.

Fortisolator then displays the result in the client browser, not allowing the user to proceed any further.

If it is a sanitized file, FortiSandbox allows the client user to upload or download the file through Fortisolator.

To send a file to FortiSandbox

1. Verify that the FortiSandbox setting is valid.
2. Upload a file through Fortisolator. Image will appear when

file upload is finished.

File Upload Finished

Information about the uploaded data

Filename	test_file.ddcbb6c1-ff7c-49e8-9547-a0f7f246bc2a.docx
Filesize	17920 bytes
Connect	POST
Protocol	HTTP

3. Verify that the file is being scanned in FortiSandbox, and view the results of the scan.

FortiSandbox IP	Set the IP of the connected FortiSandbox.
FortiSandbox administrator name	Set the FortiSandbox administrator name.
FortiSandbox password	Set the FortiSandbox password.

Creating Isolator browsing profile from CLI

To create a Fortisolator profile from CLI, follow this format:

```
> set isolator-profile <name> <download> <upload> <viewonly> <avscan> <image-quality> <video-frame-rate> <av-disarm> <right-click>
```

e.g.

```
> set isolator-profile profile_new 100 200 Y Y normal normal Y Y
```

<name>	Isolator Profile Name
<download>	Max Download Size (MB)
<upload>	Max Upload Size (MB)
<viewonly>	Limit of view only
<avscan>	Scan files for malware
<image-quality>	Image Quality
<video-frame-rate>	Video Frame Rate
<av-disarm>	Use doc-rewrite when scanning file
<right-click>	Permit for Right-Click

Displaying Isolator browsing profile from CLI

```
> show isolator-profile
Isolator Profile:profile_new
  Download Size(MB) : 100
  Upload Size(MB) : 200
  Viewonly Enabled : Y
  Antivirus Scan Enabled : Y
  Antivirus Disarm Enabled : Y
  Right Click Enabled : Y
  Image Quality : normal
  Video Frame Rate : normal
```

>

Creating Web Filter profile

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

Prerequisites

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

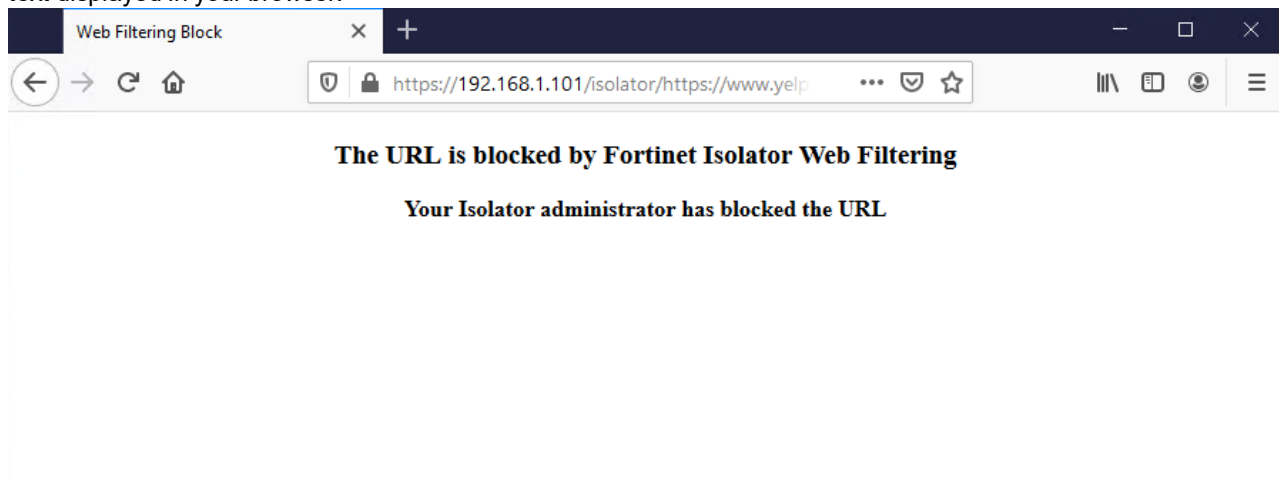
Creating Web Filter profile from GUI

Steps

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 white list or black list specific websites, click the corresponding **Create New** button in the **White List** or **Black List** section. Enter the URL details and click **OK**. The white list and black 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:



Creating Webfilter profile from CLI

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

TYPE

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

e.g.

```
> set wf-white-list white_list_new website.com 0
```

```
> show wf-white-list
```

```
white_list-white_list_new testsite.com 0
set wf-black-list <name> <url> <type>
```

e.g.

```
> set wf-black-list black_list_new blocksite.com 0
```

TYPE

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



```
> show wf-black-list
black_list-black_list_new blocksite.com 0

set wf-profile <name> <white-list> <black-list> <actions>

e.g.
> set wf-profile webprofile_new white_list_new black_list_new 0

> show wf-profile

Web Filter Profile:webprofile_new
    whitelist : white_list_new
    blacklist : black_list_new
    action profile : 0
```

Creating ICAP profile

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

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

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

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

Creating ICAP profile from GUI

Prerequisites

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

Steps

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

ICAP Profile Name	Name of the ICAP profile
IP Address	IP Address of the ICAP server
Port	Port number that the ICAP server running the service on
Service	Service name of the ICAP server

Action when server fails

Actions on Fortisolator if fails to connect to ICAP

- Allow
- Block
- View only

Creating 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

The screenshot shows the Fortisolator VM web interface. On the left is a navigation menu with options: Dashboard, Network, System, Users, Policies and Profiles (selected), Profile (sub-menu), Policy, Default Policy, and Log. The main area is titled 'Edit Profile' and contains a form with the following fields:

ICAP Profile Name	icap_new
IP address	172.30.157.208
Port	1344
Service	url_check
Action when server fails	Block

At the bottom right of the form is a green 'OK' button.

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.

Creating a policy from GUI

Steps

1. To create a new policy, 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. Click **OK** to finish.

Creating a policy from CLI

To create FortiIsolator profile from CLI, follow this format:

```
> set policy <policy-name> <isolator-profile-name> <wf profile-name> <icap-profile-name>
```

e.g.

```
> set policy policy_new system_default webfilter_profile ICAP_profile
> show policy
    Policy:policy_new
    Isolator Profile : system_default
    WebFilter Profile : webfilter_profile
    ICAP Profile : ICAP_profile
```

<policy-name >	Policy Name
<isolator-profile-name >	Isolator profile name
<wf profile-name >	Web Filter profile name
<icap-profile-name >	ICAP profile name

Default policy

Applying Isolator profile and Web Filter profile settings

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.

Applying profiles to default policy from GUI

Steps

1. To apply profiles to Default policy, go to **Policies and Profiles > Default Policy** and select the desired Guest Type. Guest Type:
 - Guest Disable: A user has to login with user account that was defined in **Users > User Definition**
 - Guest Enable: A user can login with either user account or as a guest
 - Guest Only: A user has to login as a guest



With Guest Only, the Login page will not show; users will browse sites directly without asking to go through the login page.

2. Select the Isolator profile, Web Filter profile, and/or ICAP Filter profile to be used in the 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.

3. Click **OK** to finish.

Applying profiles to default policy from CLI

To apply profiles to Default Policy from CLI follow this format:

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

For example:

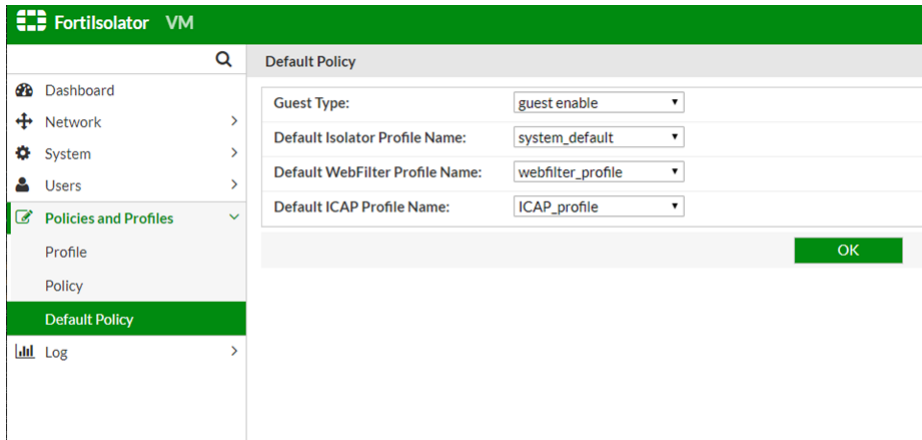
```
> set guest-type 0
> show guest-type
guest type : Disabled
> set guest-type 1
> show guest-type
guest type : Enabled
> set guest-type 2
> show guest-type
guest type : Guest Only
```

```
> set default-policy <isolator-profile-name> <wf-profile-name> <icap-profile-name>
e.g.
```

```
> set default-policy system_default webfilter_profile ICAP_profile
```

```
> show default-policy
Default Policy:
Isolator Profile : system_default
WebFilter Profile : webfilter_profile
ICAP Profile : ICAP_profile
```

<isolator-profile-name >	Isolator profile name
<wf profile-name >	Web Filter profile name
<icap-profile-name >	ICAP profile name



Applying profile settings to local user account

Steps

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

Steps

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 Fortisolator devices and on networks, and to inform you about certain activities, such as:

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

The following topics provide information about logging:

- Viewing logs
- Antivirus logs
- Web Filter logs
- Log Settings

Viewing logs

All event logs, except Antivirus logs and Web Filter logs, are available from the log page **Log > Log** by default.

Date	Time	Type	Content
2020-05-11	17:38:46	notice	canonical_hostname = FISVM1TM20000048
2020-05-11	17:38:46	notice	mem: per-conn: 552 bytes + protocol rx buf
2020-05-11	17:38:46	notice	Listening on port 43873
2020-05-11	17:38:46	notice	Creating Vhost 'default' port 0, 1 protocols, IPv6 off
2020-05-11	17:38:46	notice	mem: platform fd map: 8192 bytes
2020-05-11	17:38:46	notice	Threads: 1 each 1024 fds
2020-05-11	17:38:46	notice	libuv support not compiled in
2020-05-11	17:38:46	notice	libev support not compiled in
2020-05-11	17:38:46	notice	IPv6 not compiled in
2020-05-11	17:38:46	notice	Libwebsockets version: 2.3.0 root@dops-fso-93-fso_2_0107-10-g6e27282
2020-05-11	17:38:46	notice	Initial logging level 7
2020-05-11	17:38:46	notice	canonical_hostname = FISVM1TM20000048
2020-05-11	17:38:46	notice	mem: per-conn: 552 bytes + protocol rx buf
2020-05-11	17:38:46	notice	Listening on port 23773
2020-05-11	17:38:46	notice	Creating Vhost 'default' port 0, 1 protocols, IPv6 off

- The log messages are organized by tabs that can be accessed at the top of the window.

Fis_daemon.log	Logs for daemons running in Fortisolator devices
Messages.django	Logs for Fortisolator Web framework activities
Message.secure	Logs for connectivity from remote server to Fortisolator through SSH
Message.user	Logs for connectivity with FDN server, internal Redis database, Anti-Virus servers, HA heartbeats information, etc.
Message.cron	Logs for Fortisolator processes
Access_log	Logs for accessing Fortisolator local devices

- 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**.

Antivirus

This page displays Antivirus logs. Organize them by selecting the following options:

Filter	Detail
Date	The day the log was recorded.
Time	The minute the log was recorded.
Action	<ul style="list-style-type: none"> Upload file—The file was uploaded. Download file—The file was downloaded.
UserID	<p>"0" means the user is a guest, or another local_user, or an NTLM user.</p> <p>The number is auto-generated by the admin when a local user is created or an NTLM user is used.</p>
Path	The path of the file on Fortisolator device that stores the uploaded/downloaded files.
Target URL	The destination the user is trying to access through Fortisolator.
Result	<ul style="list-style-type: none"> Passthrough—Allows the file (assuming uncorrupted) to be downloaded/uploaded. Block—Blocks the file if a virus is detected.
File Size	The size of the file. No limit. However, it must comply to the file size defined under Profile.
Isolator Profile Name	Name of the profile as defined in Policies and Profile.

Web filter

This page displays the web filter logs. Organize them by selecting the following options:

Filter	Detail
Date	The day the log was recorded.
Time	The minute the log was recorded.
Action	<ul style="list-style-type: none">• Allow—Allows web browsing to continue.• Block—Blocks web browsing.• View Only—Only allows user to view when browsing.
UserID	"0" means the user is a guest, or another local_user, or an NTLM user. The number is auto-generated by the admin when a local user is created or an NTLM user is used.
URL	The destination the user is trying to access through Fortisolator.
Category	Block / Passthrough as determined under the specified Web Filter Profile.
WF Profile Name	Name of the Web Filter profile as defined in Profiles and Policies.

Log settings

Configuring the log server

Here you can back up log messages and/or send syslog messages to a remote server.

Steps

1. From the administration portal, go to **Log > Log Settings**.
2. To save your current log messages as a file, select the **Click here** link inside the **Backup Logs** section.
3. Fill in the settings.

Logging protocol	Syslog
Network protocol	<ul style="list-style-type: none">• udp• tcp
Log Server IP Address	Remote server IP that receives the logs.
Port	The port number of the remote server that receives the logs.

4. Choose logs to send to remote server.
5. Click **+ Create New**. Select the Application and Severity. See the descriptions in the [Viewing logs on page 82](#). Click **OK**.
6. Don't forget to **Submit**.

Run web browsers through Fortisolator

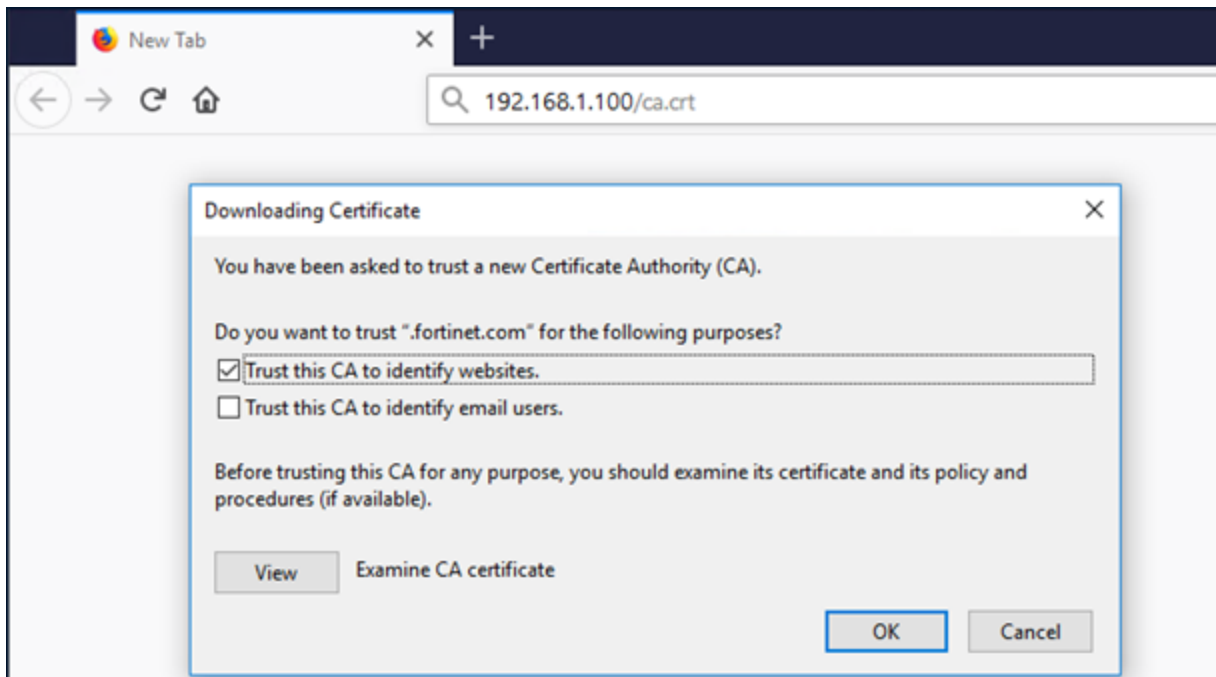
IP forwarding mode

Using IP forwarding mode with Mozilla Firefox

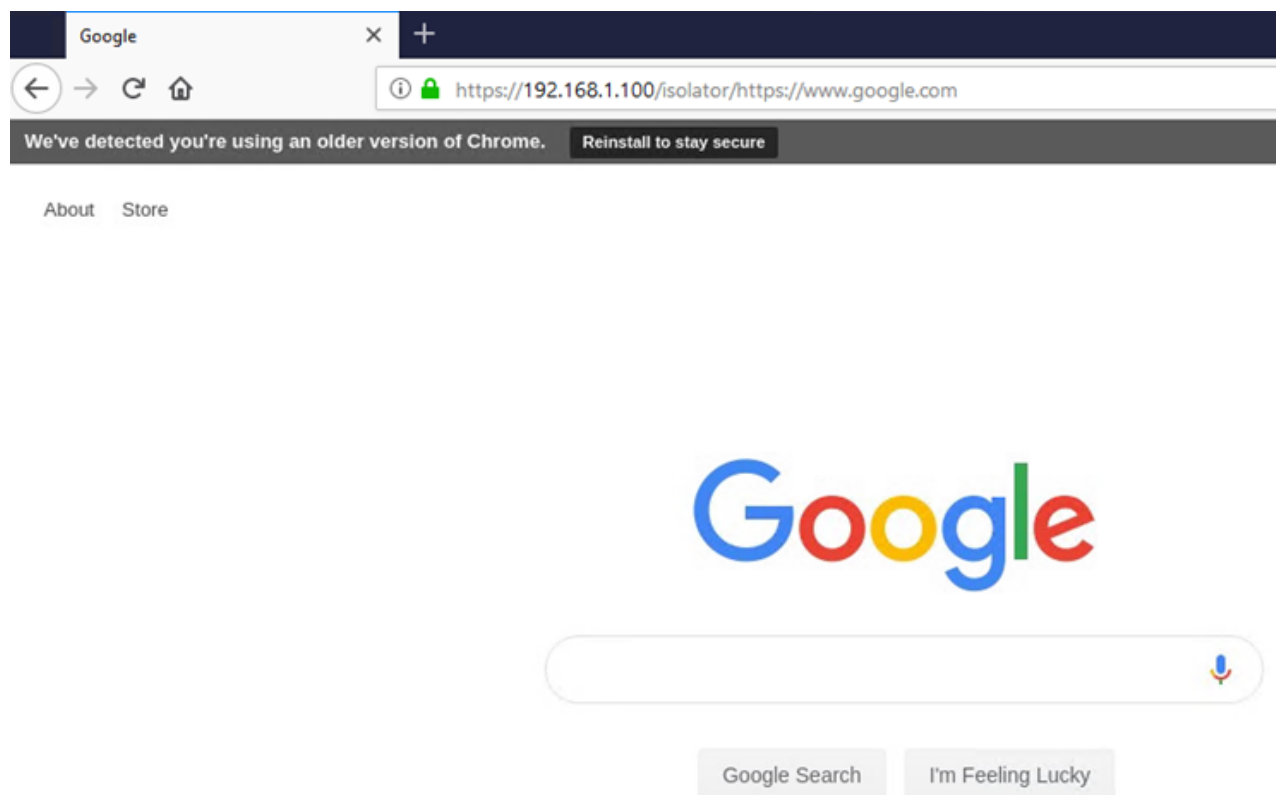
Use this procedure to configure IP forwarding mode with Mozilla Firefox.

Steps

1. To download the Fortisolator certificate (ca.crt) and import it into the Mozilla Firefox browser, follow these steps:
 - a. In the Mozilla Firefox browser address bar, type `http://<internal_IP_address>/ca.crt` (for example, `http://192.168.1.100/ca.crt`).
 - where `<internal_IP_address>` is the IP address of the Fortisolator internal interface. For example, the IP address of the internal interface that you configured in step 3 of [Installing Fortisolator 1000F on page 8](#).
 - 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.google.com` (for example, `https://192.168.1.100/isolator/https://www.google.com`).
 - where `<internal_IP_address>` value is the IP address of the Fortisolator internal interface



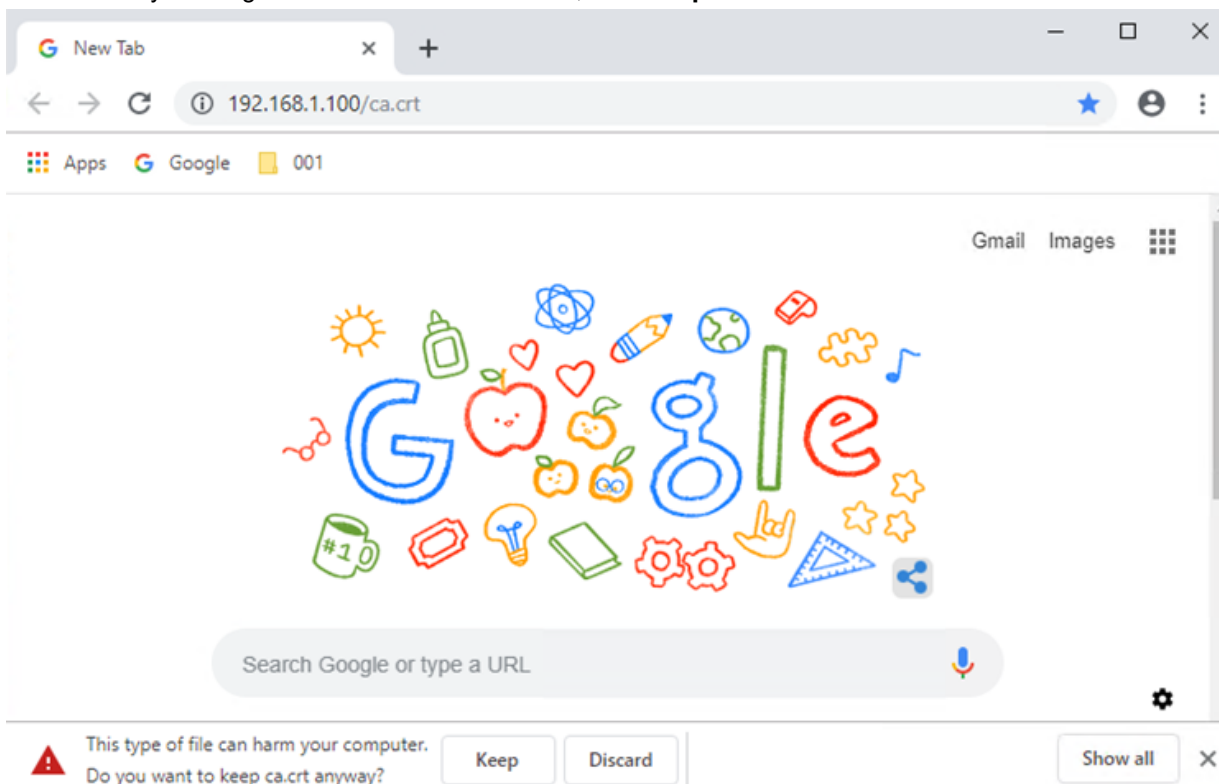
Using IP forwarding mode with Google Chrome

Use this procedure to configure IP forwarding mode with Google Chrome.

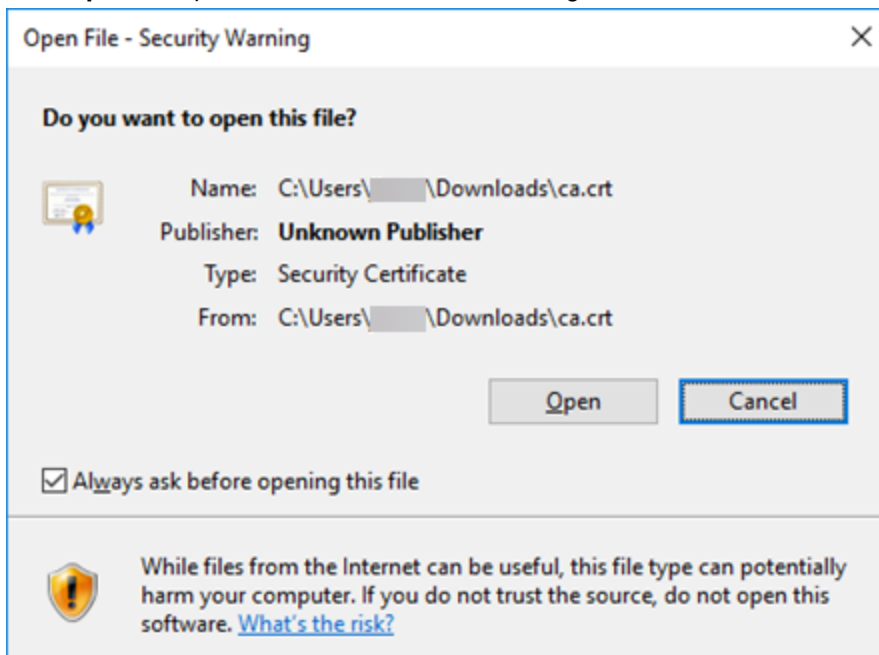
Steps

1. To download the Fortisolator certificate (ca.crt) and import it into your Google Chrome browser, follow these steps:
 - a. In the Google Chrome browser address bar, type `http://<internal_IP_address>/ca.crt` (for example, `http://192.168.1.100/ca.crt`).
 - where `<internal_IP_address>` value is the IP address of the Fortisolator internal interface. For example, the IP address of the internal interface that you configured in step 3 of [Installing Fortisolator 1000F on page 8](#).

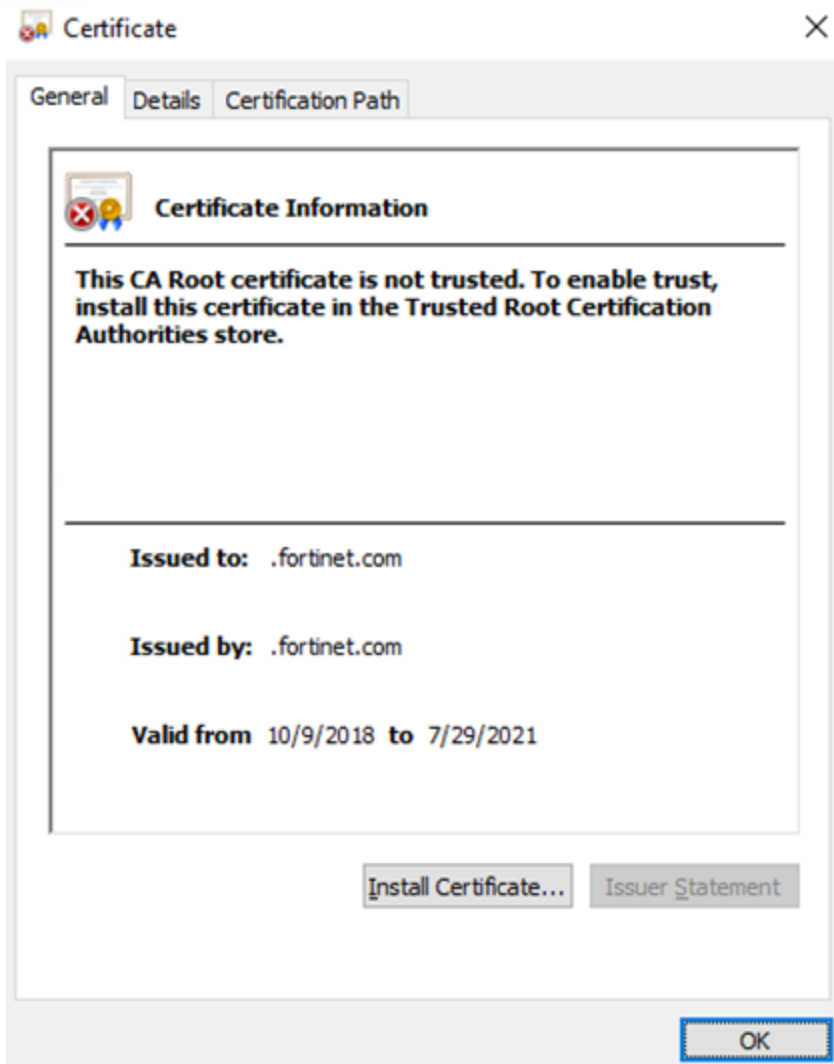
- b. In the security warning at the bottom of the browser, click **Keep** to download the certificate.



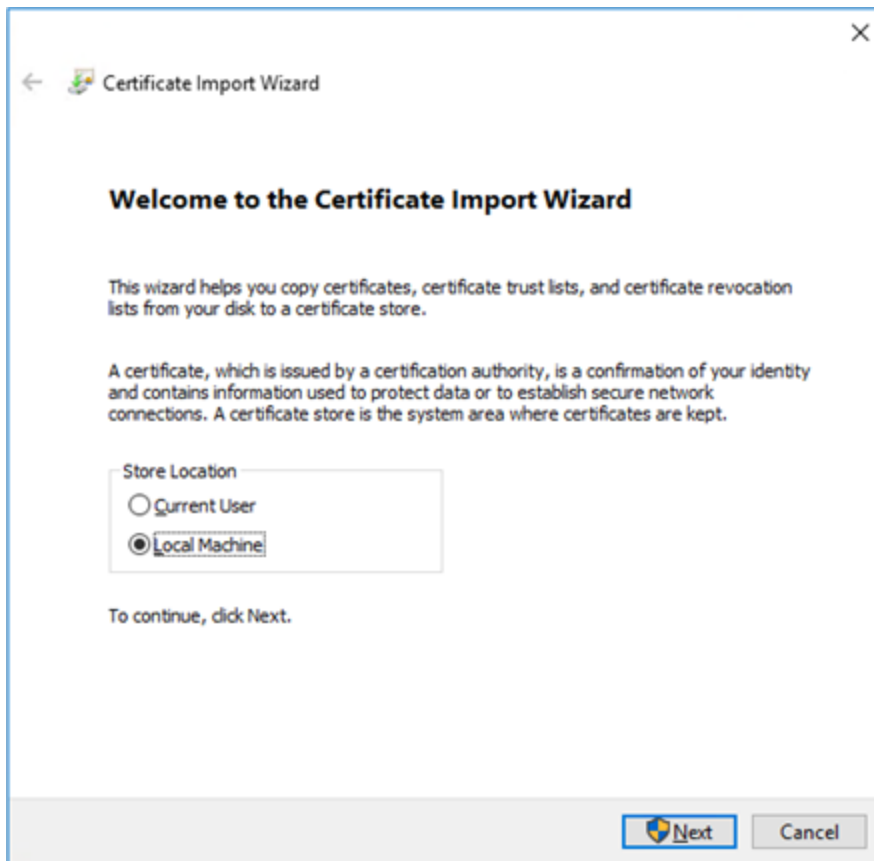
- c. Click **Open** to import the ca.crt certificate into Google Chrome.



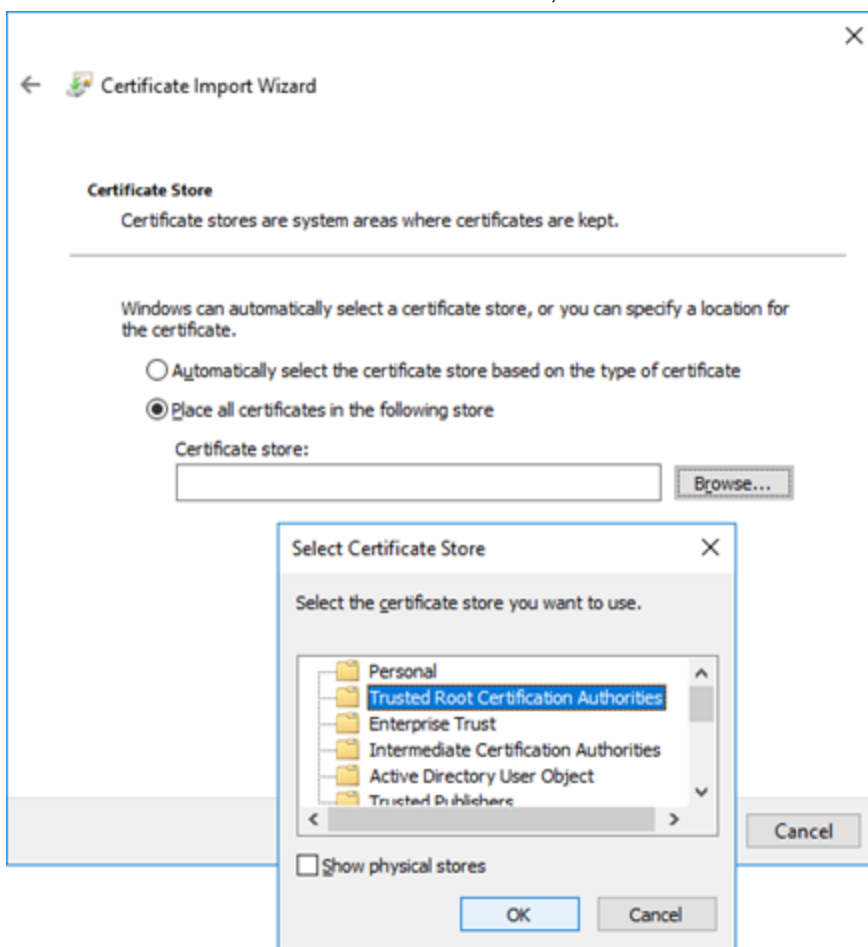
- d. Click **Install Certificate**.



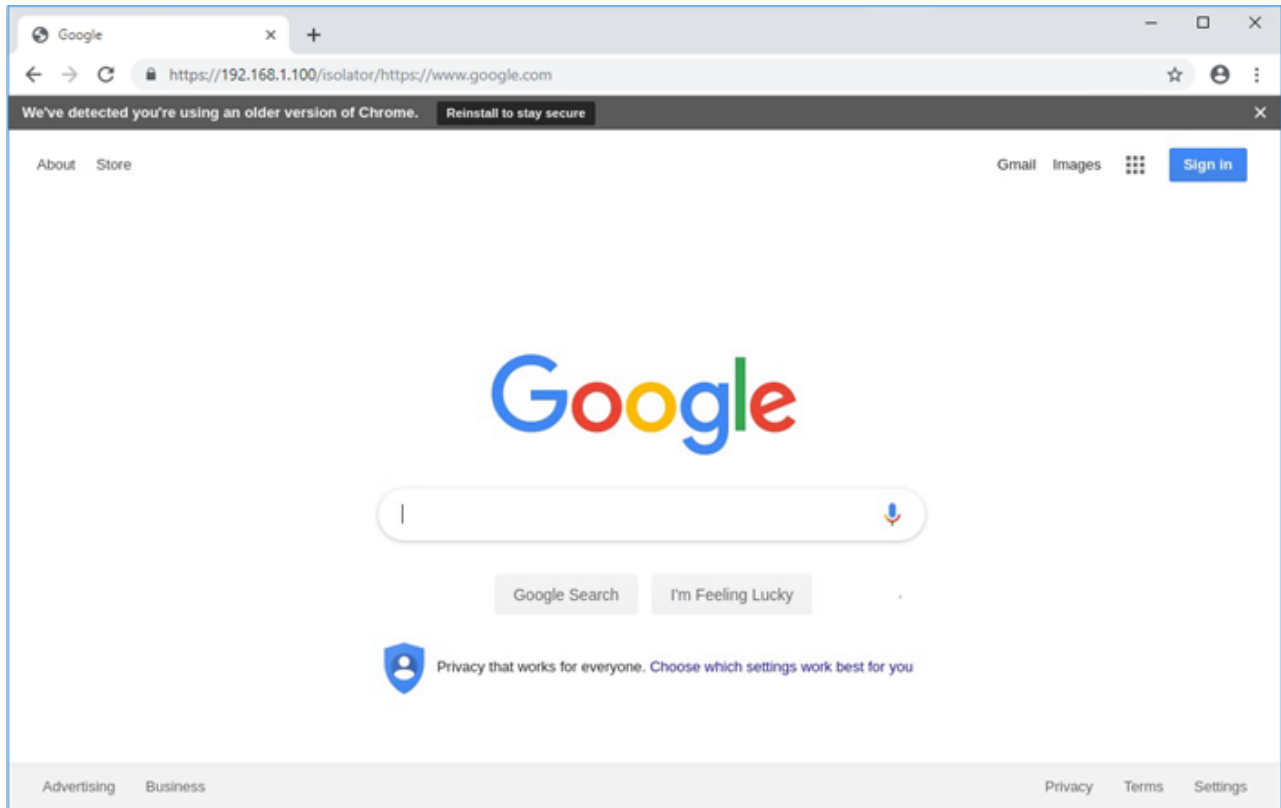
- e. Select **Local Machine**, and click **Next**.



- 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.google.com` (for example, `https://192.168.1.100/isolator/https://www.google.com`).
- where `<internal_IP_address>` value is the IP address of the Fortisolator internal interface



Using IP forwarding mode with Internet Explorer

Use this procedure to configure IP forwarding mode with Internet Explorer.

Steps

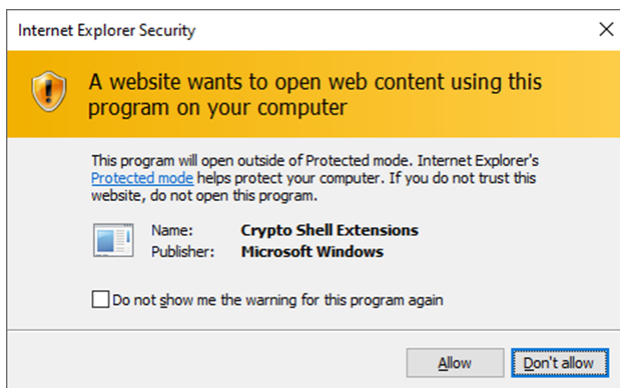
1. To download the Fortisolator certificate (ca.crt) and import it into your Internet Explorer browser, follow these steps:
 - a. In the Internet Explorer browser address bar, type `http://<internal_IP_address>/ca.crt` (for example, `http://192.168.1.100/ca.crt`).
 - where `<internal_IP_address>` value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



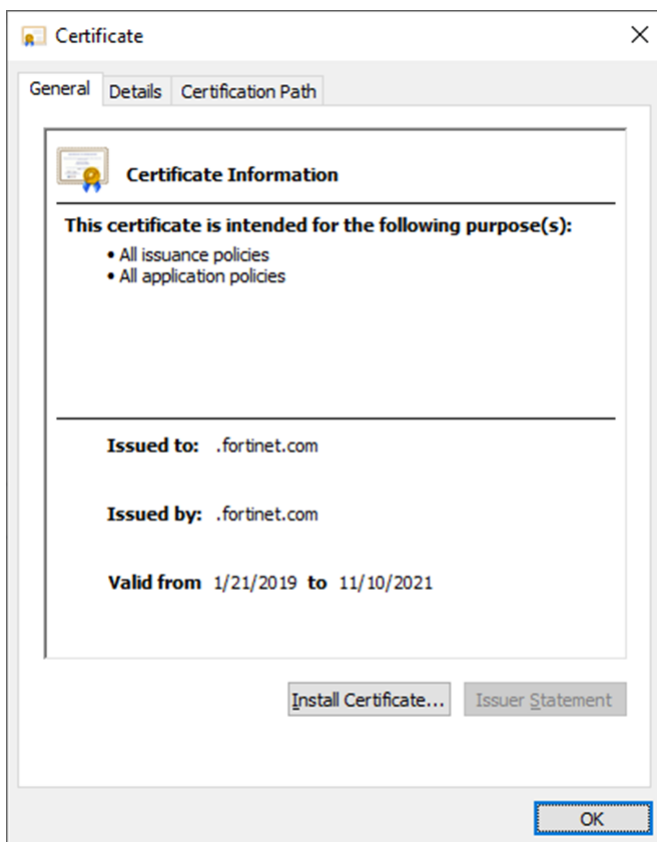
- c. Click Open to import the ca.crt certificate into Internet Explorer.



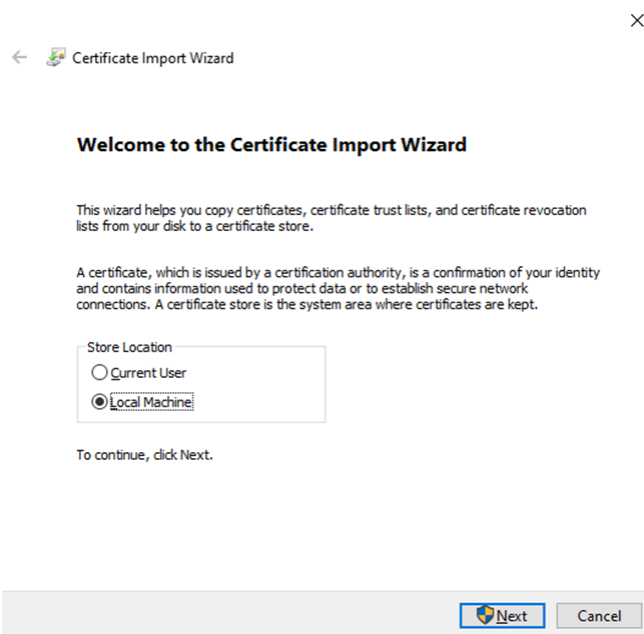
- d. Click Allow to install certificate.



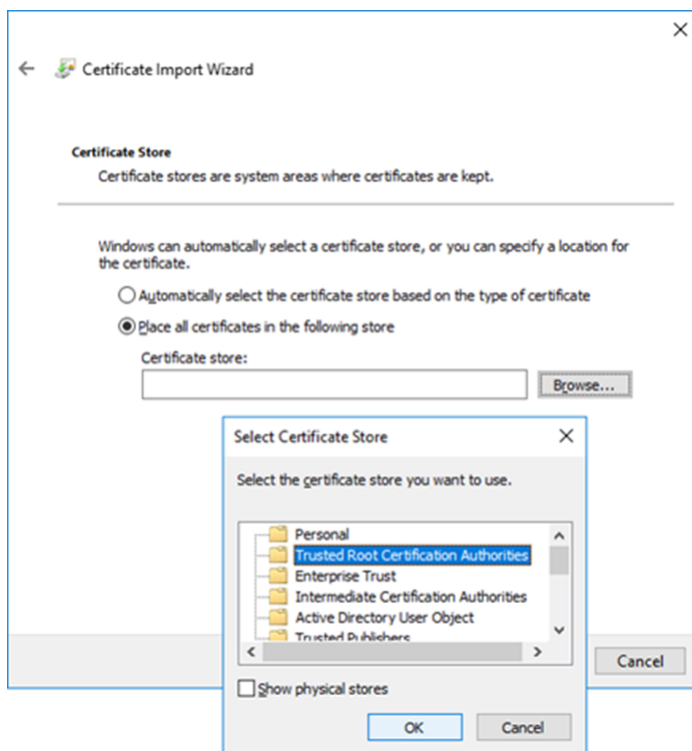
- e. Click Install Certificate



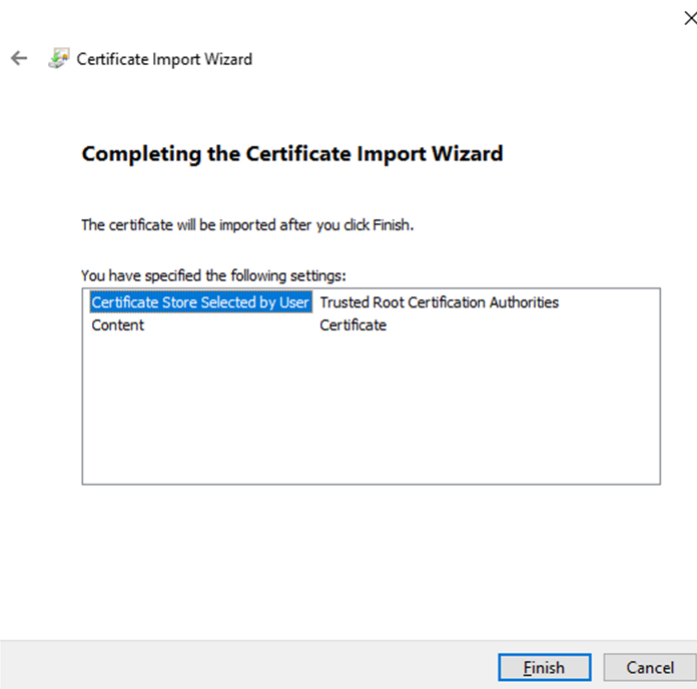
- f. Select Local Machine, and click Next.



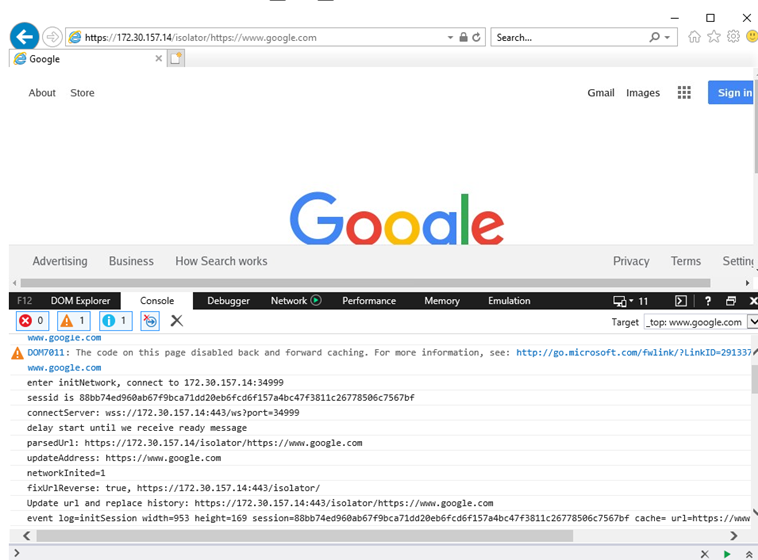
- g. Select Trusted Root Certification Authorities, and click OK.



- h. Completing the Certificate Import Wizard



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



Using proxy mode with Edge

Use this procedure to configure proxy mode with Edge.

Steps

- 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 on Advanced
4. Under Proxy setup, click on Open proxy settings
5. Enable Manual proxy setup, paste your proxy IP address into the Address field with port 8888 and exception list:
6. Click Save to exit from Settings, and restart Edge browser.

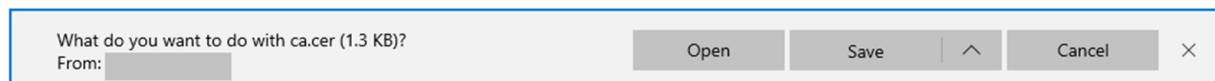
Verifying Fortisolator proxy mode with Edge

Using IP forwarding mode with Edge

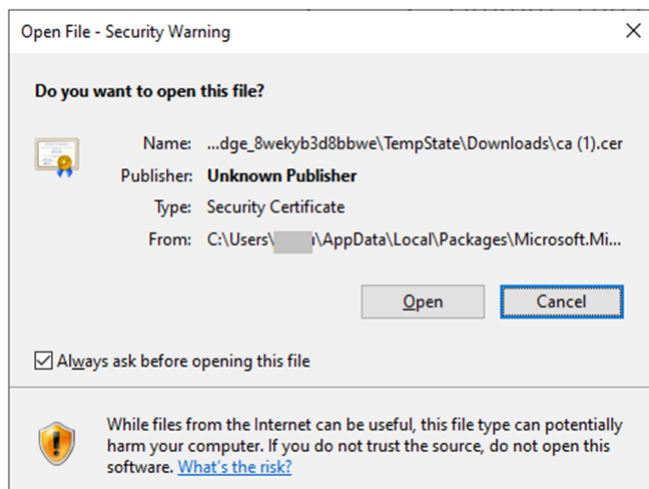
Use this procedure to configure IP forwarding mode with Edge browser.

Steps

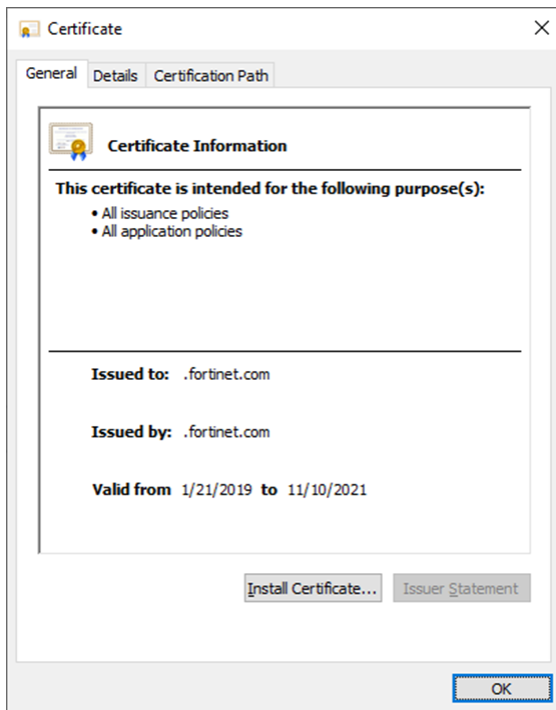
1. To download the Fortisolator certificate (ca.crt) and import it into your Edge browser, follow these steps:
 - a. In the Edge browser address bar, type `http://<internal_IP_address>/ca.crt` (for example, `http://192.168.1.100/ca.crt`).
 - where `<internal_IP_address>` value is the IP address of the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



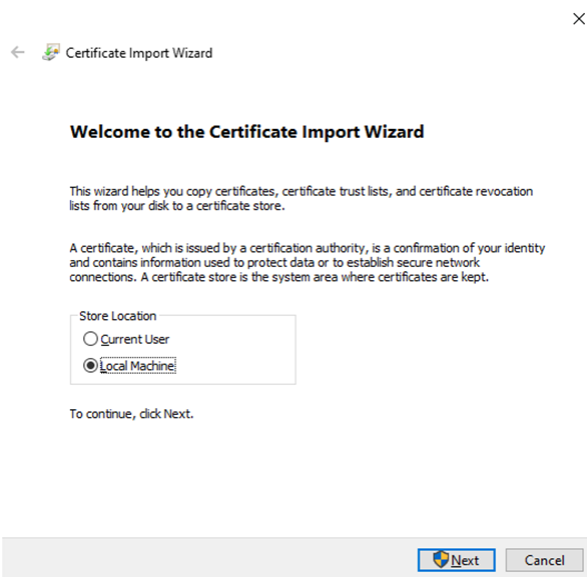
- c. Click Open to import the ca.crt certificate into Edge.



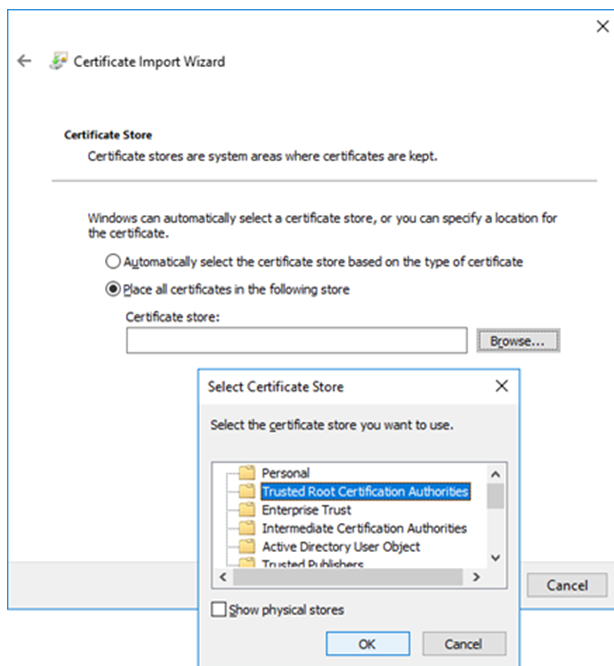
d. Click Install Certificate



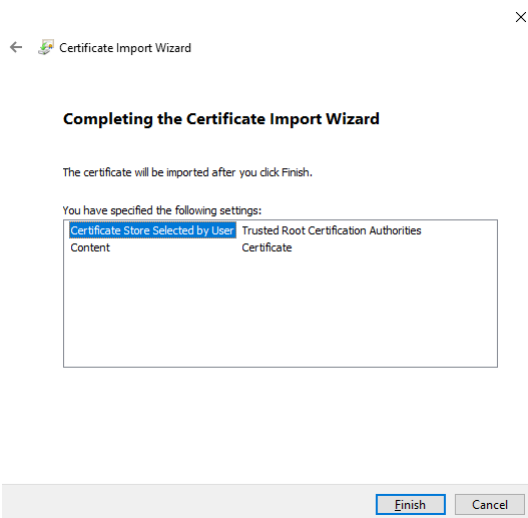
e. Select Local Machine, and click Next.



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

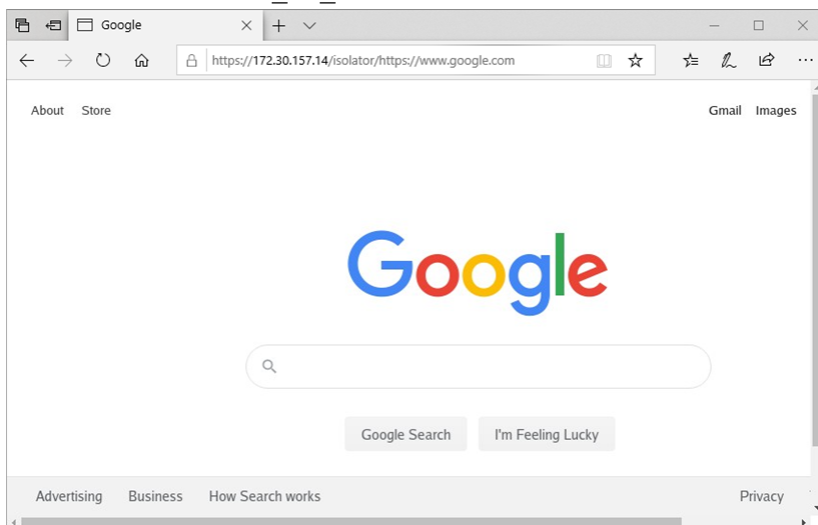


- g. Completing the Certificate Import Wizard.



In the Edge browser address bar, type `https://<internal_IP_address>/isolator/https://www.google.com` (for example, `https://172.30.157.14/isolator/https://www.google.com`)

- where `<internal_IP_address>` value is the IP address of the Fortisolator internal interface



Proxy mode

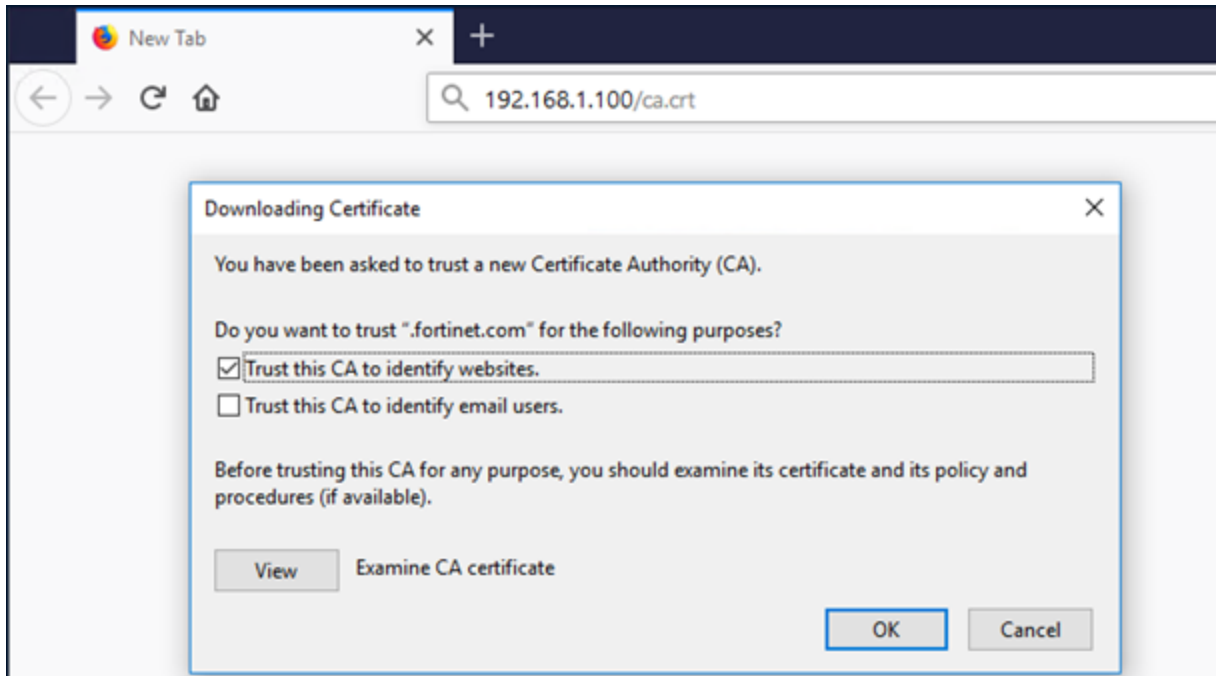
Using proxy mode with Mozilla Firefox

Use this procedure to configure proxy mode with Mozilla Firefox.

Steps

1. To download the Fortisolator certificate (ca.crt) and import it into the Mozilla Firefox browser, follow these steps:
 - a. In the Mozilla Firefox browser address bar, type `http://<internal_IP_address>/ca.crt` (for example, `http://192.168.1.100/ca.crt`).

- where `<internal_IP_address>` is the IP address of the Fortisolator internal interface. For example, the IP address of the internal interface that you configured in step 3 of [Installing Fortisolator 1000F on page 8](#).
- b. In the **Downloading Certificate** window, select the **Trust this CA to identify websites** checkbox.
- c. Click **OK**



2. Open the Mozilla Firefox browser.
3. In the menu, click **Options**.
4. Click **General**.
5. In the **Network Settings** section, click **Settings**.
6. In the **Connection Settings** window, select **Manual proxy configuration**, and enter the following settings (values shown here are examples):
 - **HTTP Proxy:** 192.168.1.100, **Port:** 8888
 - **SSL Proxy:** 192.168.1.100, **Port:** 8888
 - **No Proxy for:** "localhost, 127.0.0.1, `<internal_IP_address>/24`", where `<internal_IP_address>` is the IP address of the Fortisolator internal interface. For example, the IP address of the internal interface that you configured in step 3 of [Installing Fortisolator 1000F on page 8](#).
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

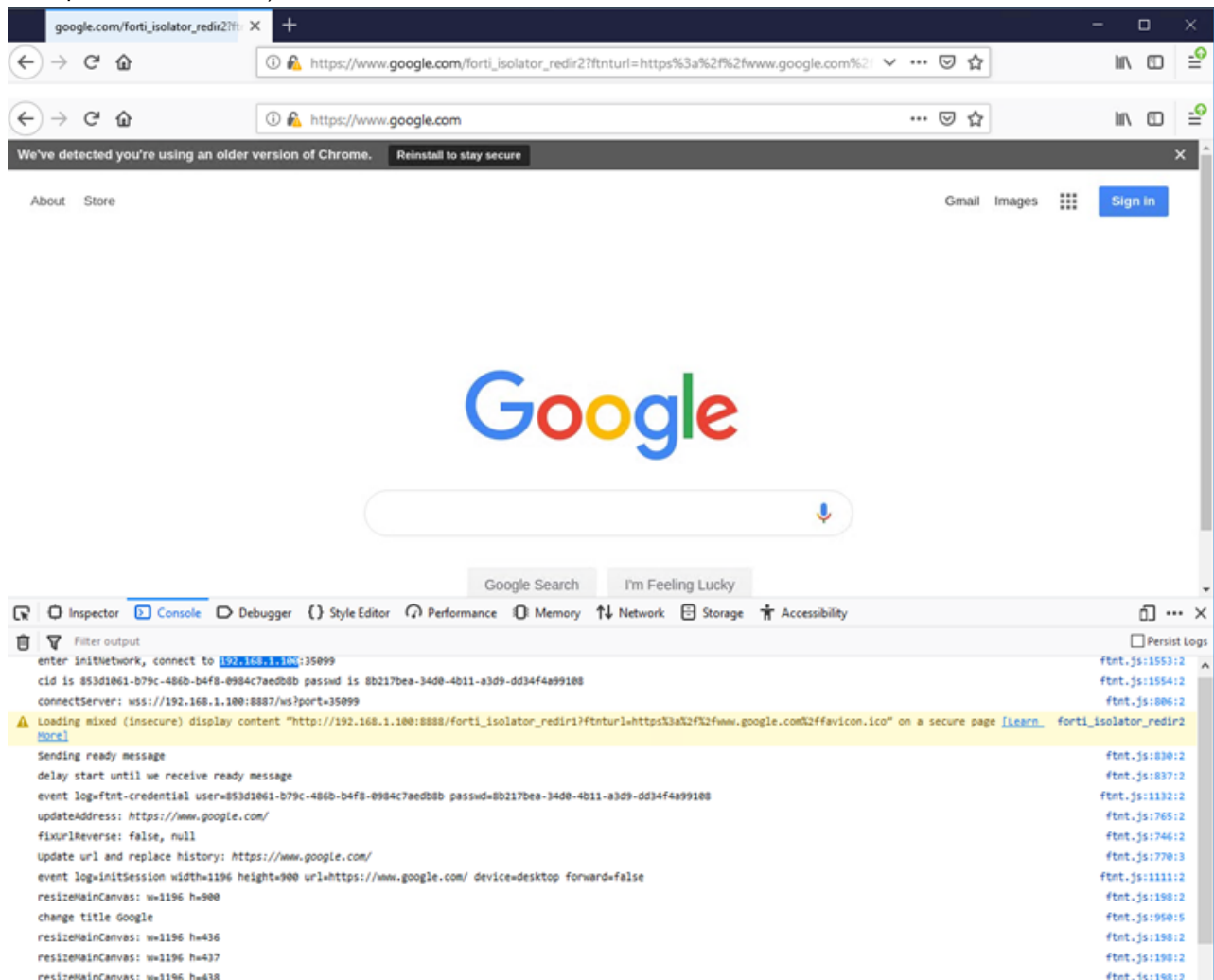
Help

Verifying Fortisolator proxy mode with Mozilla Firefox

Use this procedure to verify that Fortisolator proxy mode is working correctly with Mozilla Firefox.

Steps

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



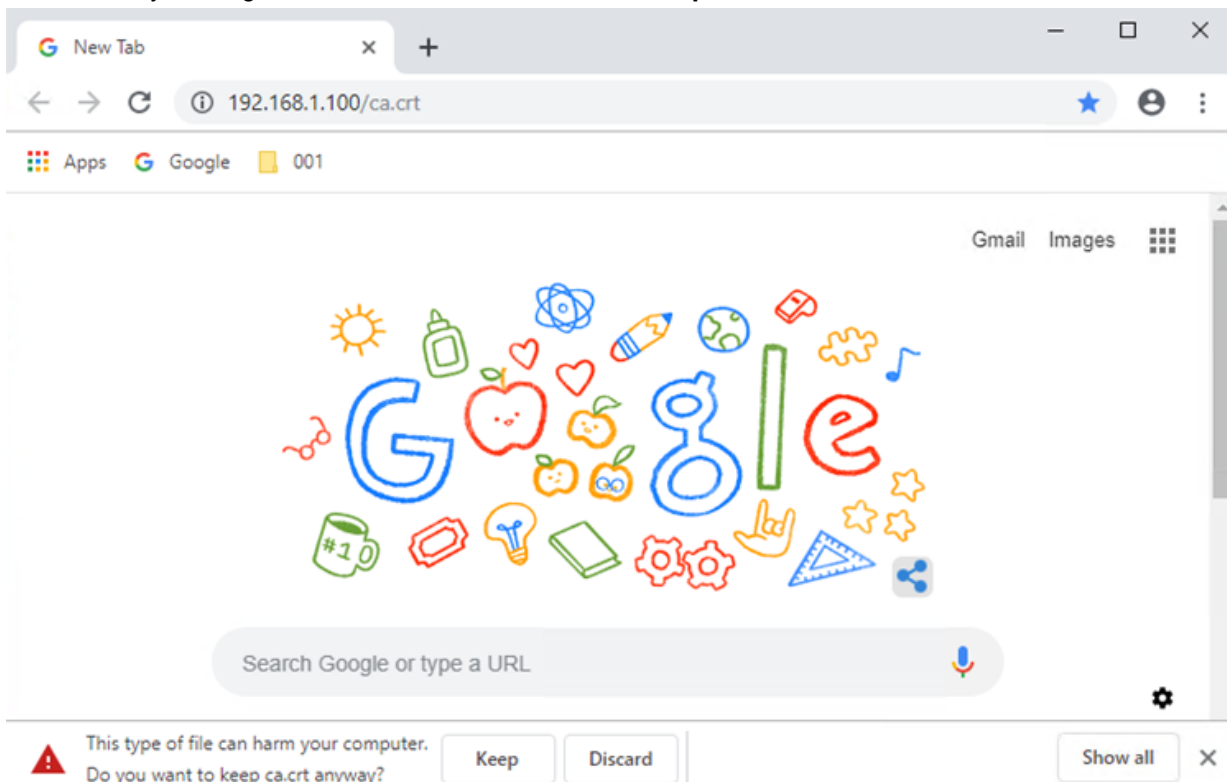
Using proxy mode with Google Chrome

Use this procedure to configure proxy mode with Google Chrome.

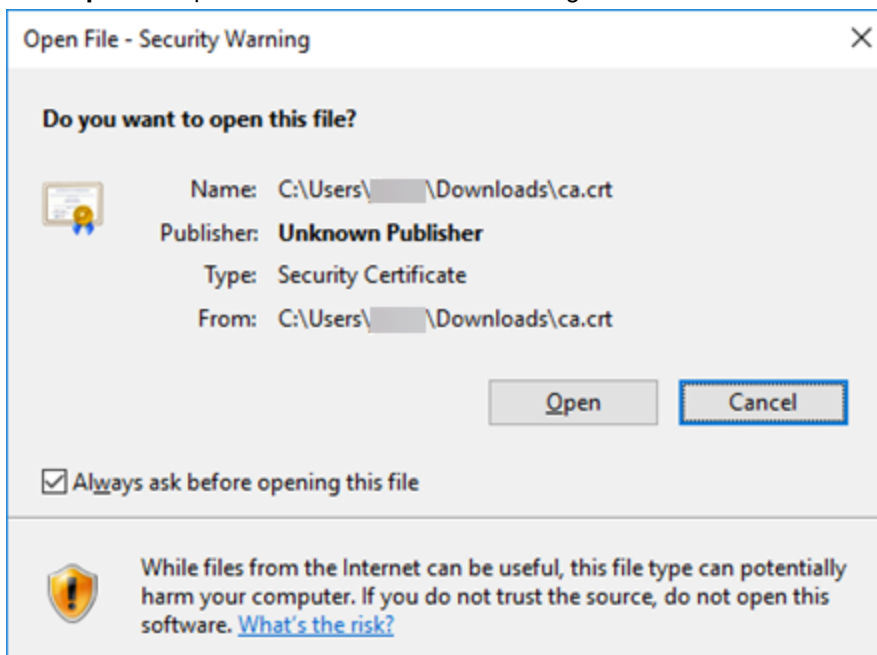
Steps

1. To download the Fortisolator certificate (`ca.crt`) and import it into your Google Chrome browser, follow these steps:

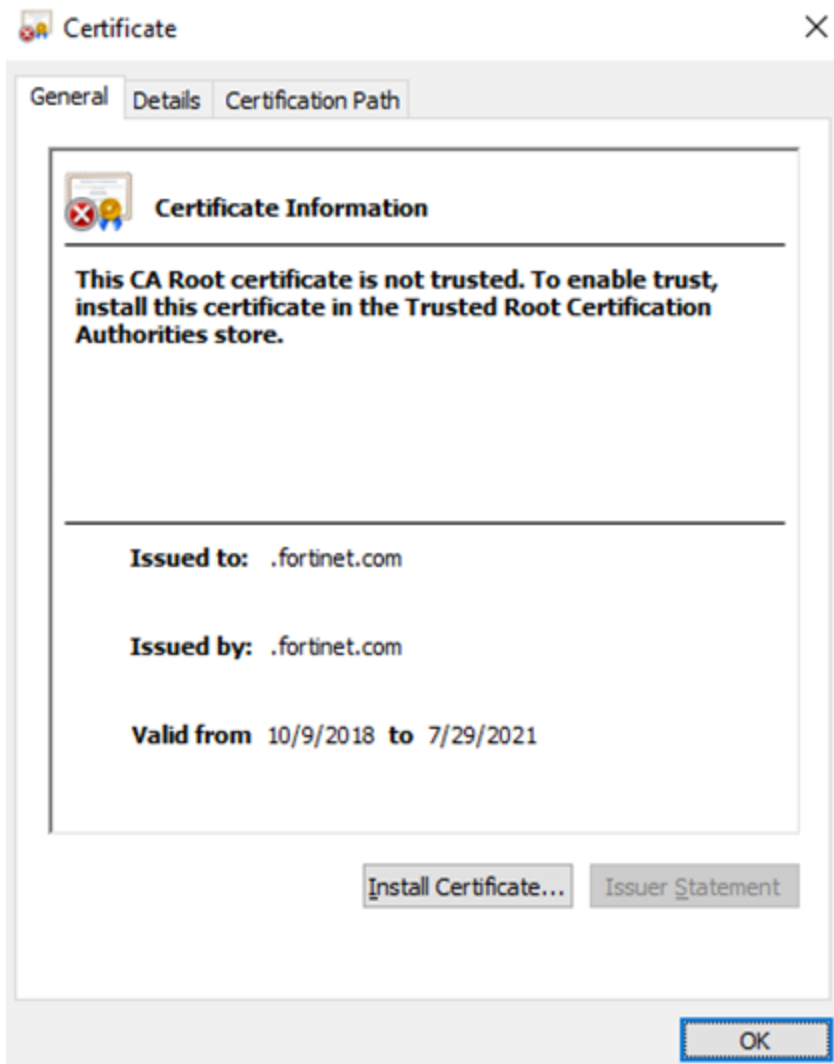
- a. In the Google Chrome browser address bar, type `http://<internal_IP_address>/ca.crt` (for example, `http://192.168.1.100/ca.crt`).
 - where `<internal_IP_address>` value is the IP address of the Fortisolator internal interface. For example, the IP address of the internal interface that you configured in step 3 of [Installing Fortisolator 1000F on page 8](#).
- b. In the security warning at the bottom of the browser, click **Keep** to download the certificate.



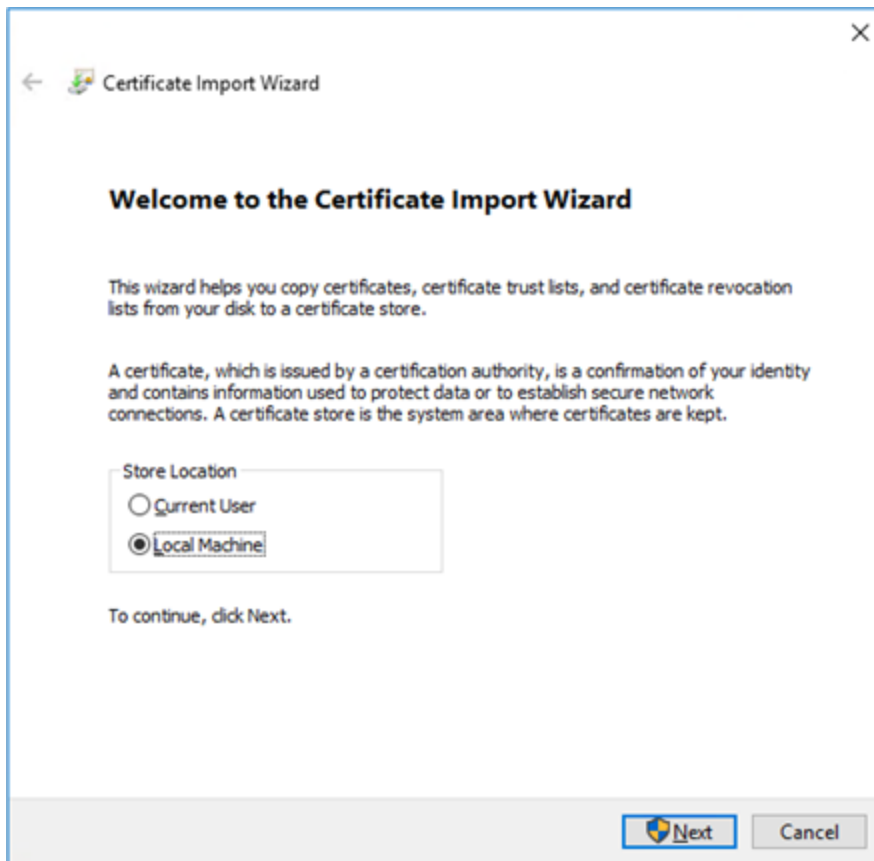
- c. Click **Open** to import the ca.crt certificate into Google Chrome.



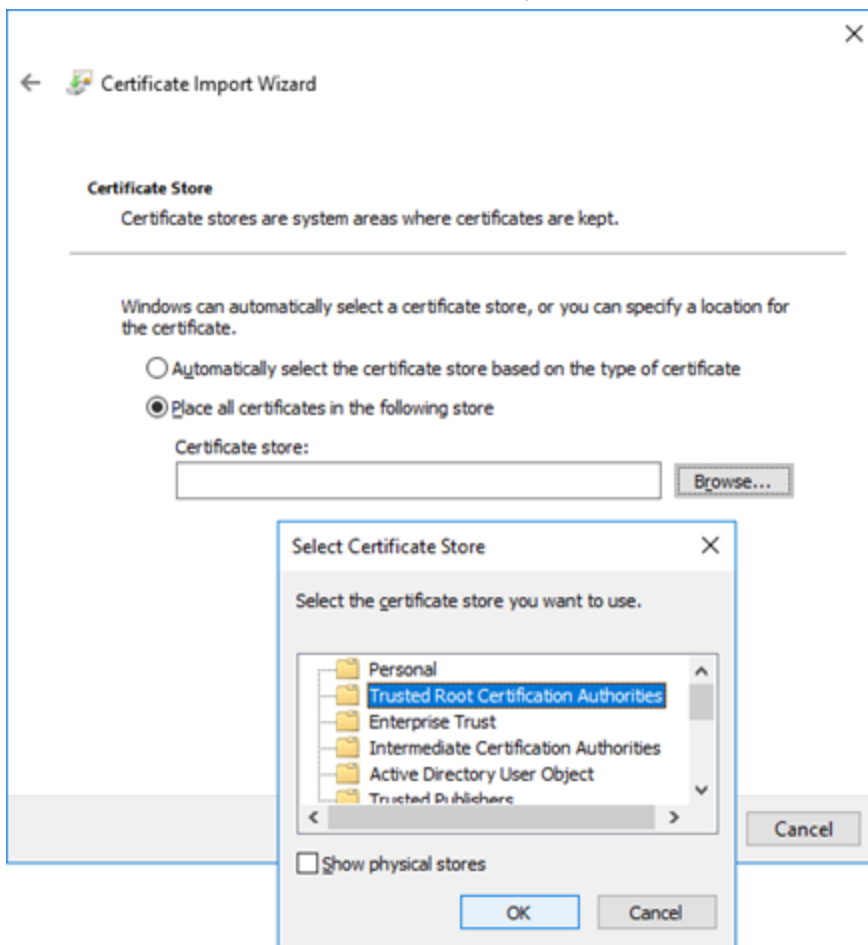
- d. Click **Install Certificate**.



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

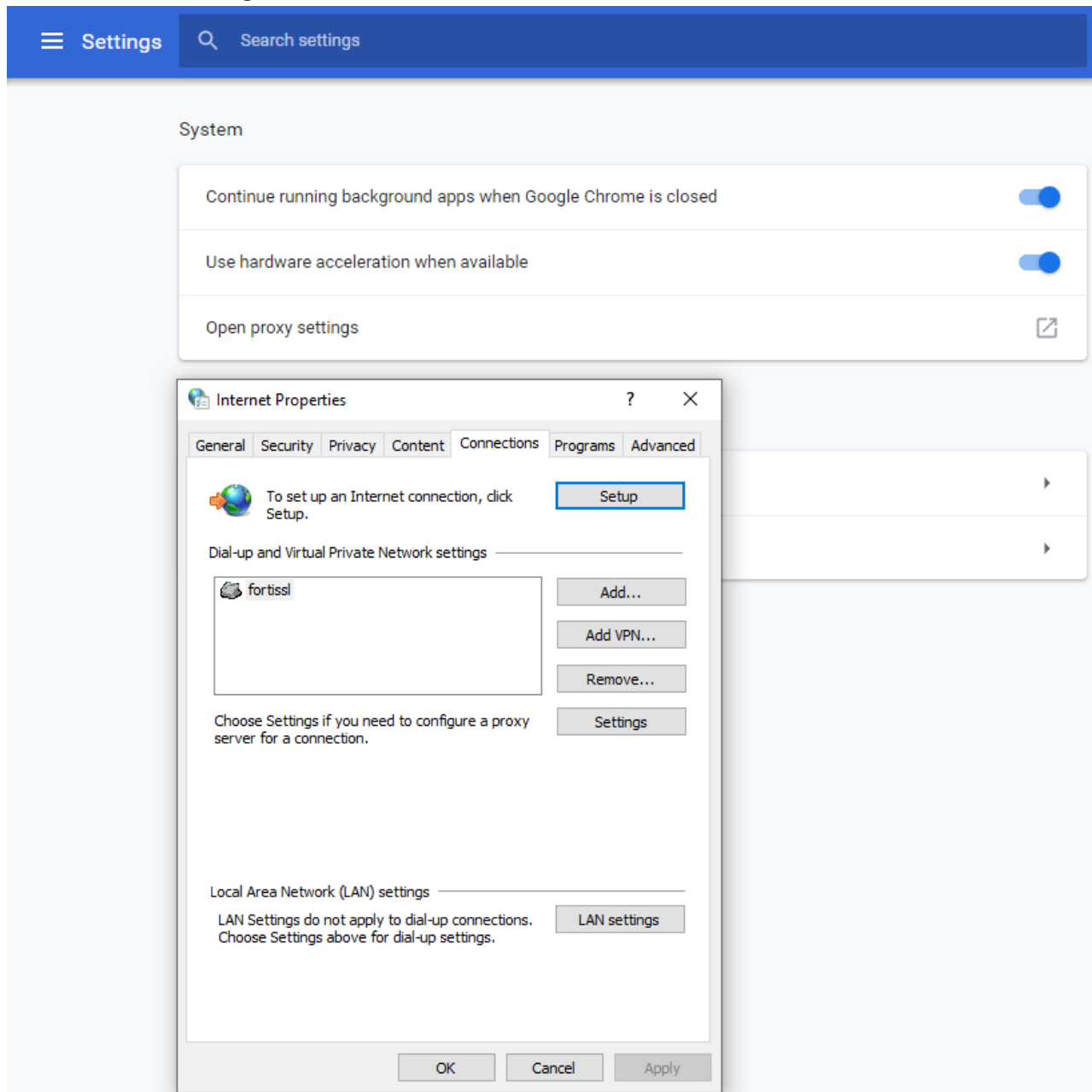


- f. Select **Trusted Root Certificate Authorities**, and click **OK**.

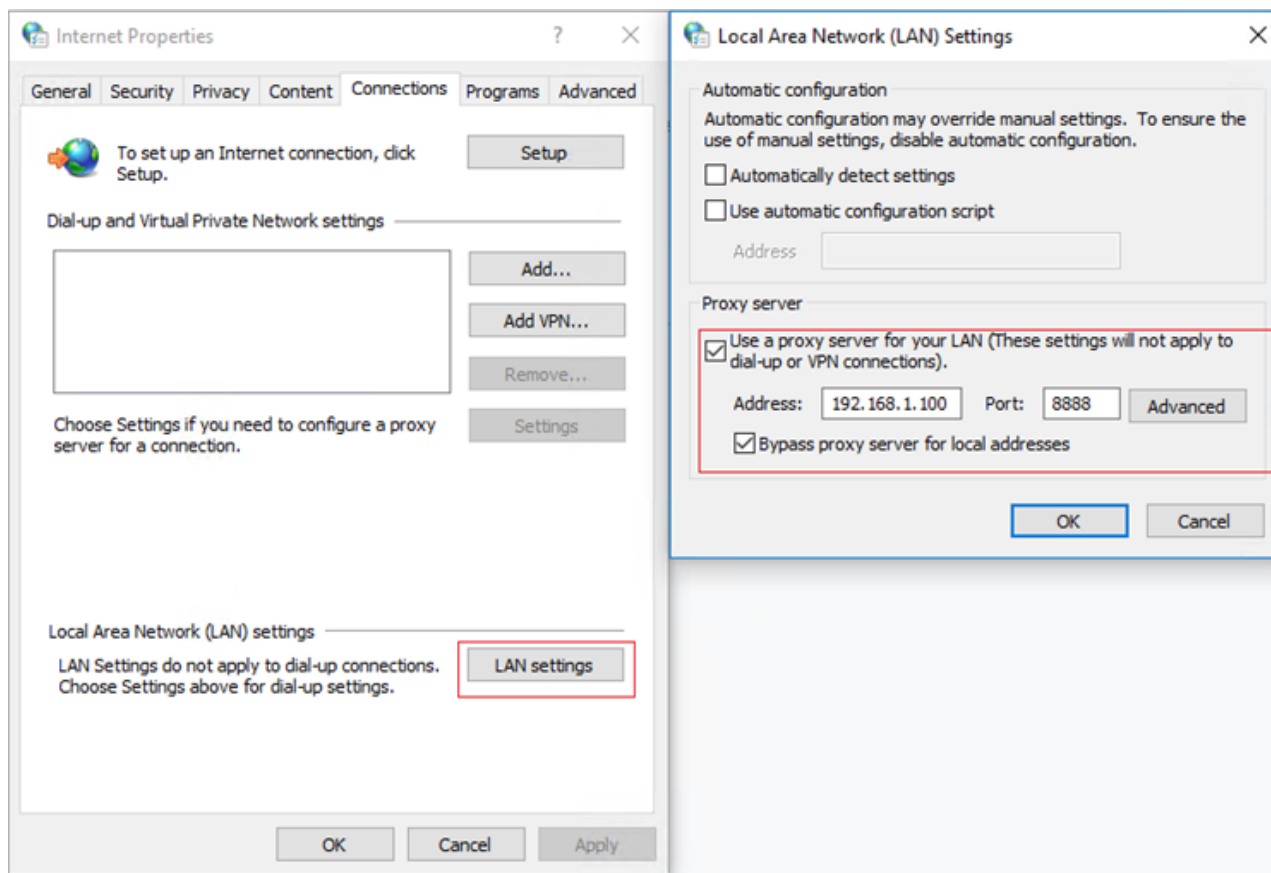


2. Open the Google Chrome browser.

3. In the menu, click **Settings**.

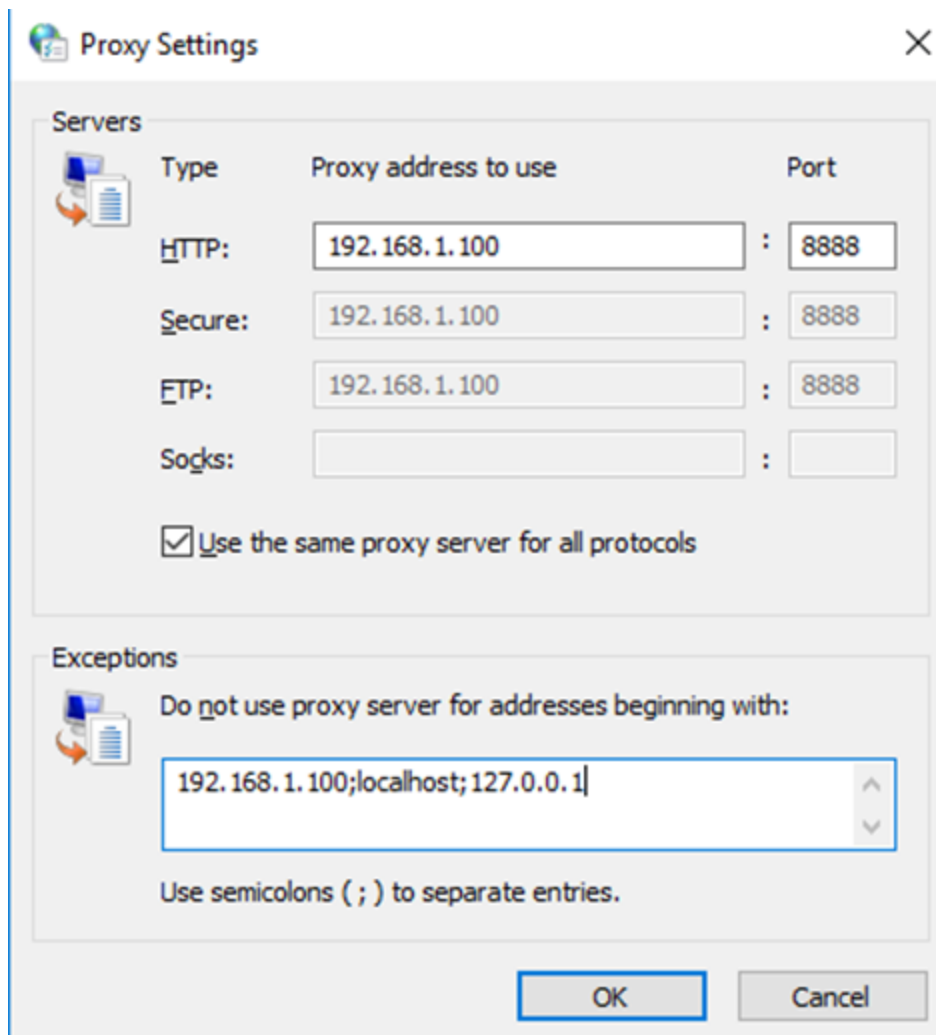


4. Expand **Advanced**.
5. In the **System** section, click **Open proxy settings**.
6. In the **Internet Properties** window, click the **Connections** tab.
7. Click **LAN settings**.
8. In the **Proxy server** section, select **Use a proxy server for your LAN**, and enter the following setting (values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



9. Click **Advanced**.

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



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

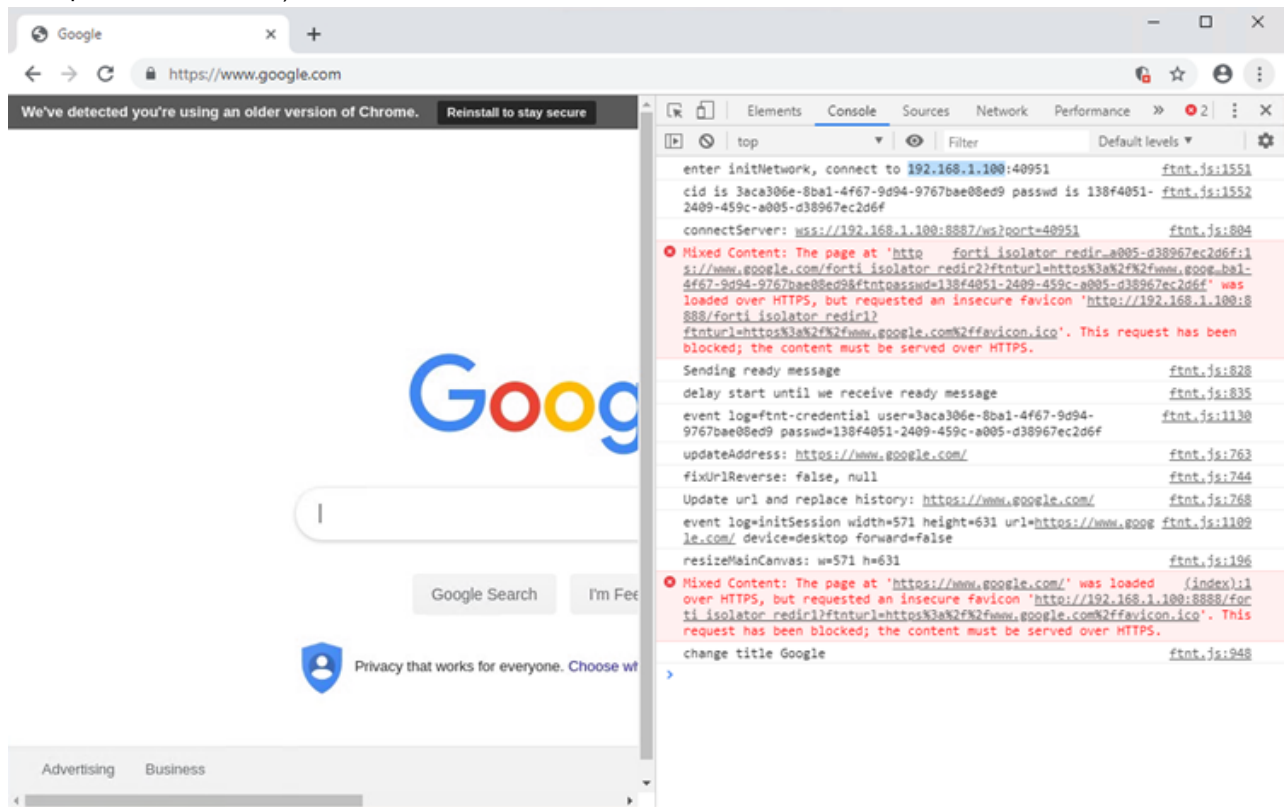
Verifying Fortisolator proxy mode with Google Chrome

Use this procedure to verify that Fortisolator proxy mode is working correctly with Google Chrome.

Steps

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

example, 192.168.1.100).



Using proxy mode with Internet Explorer

Use this procedure to configure proxy mode with Internet Explorer.

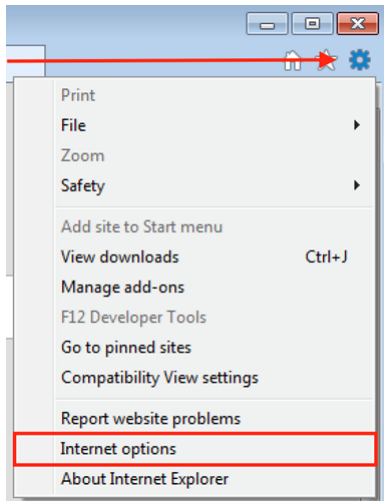


Pre-requisites:

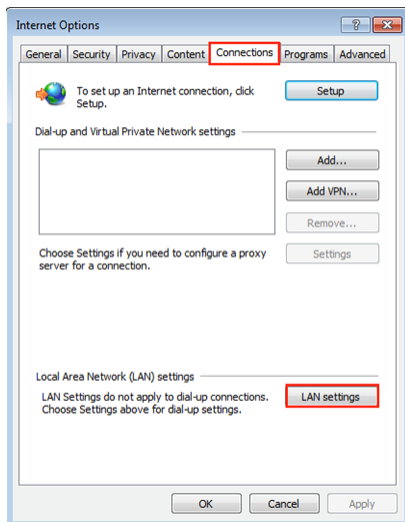
Please follow [Using IP forwarding mode with Internet Explorer on page 92](#) step 1 to install Fortisolator “ca.crt” certificate prior to using proxy mode.

Steps

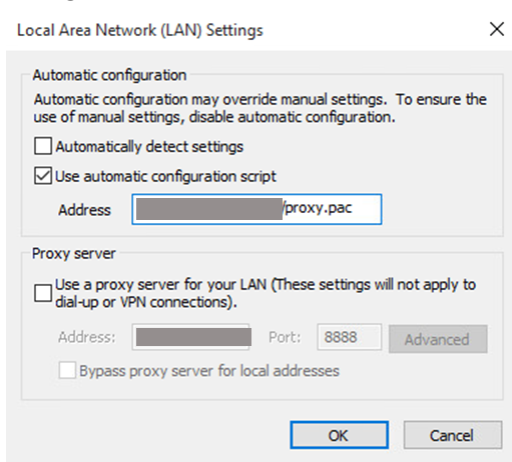
1. Open an Internet Explorer browser window and click the gear icon at the top right corner to open browser settings.
2. Select **Internet options** from the settings menu.



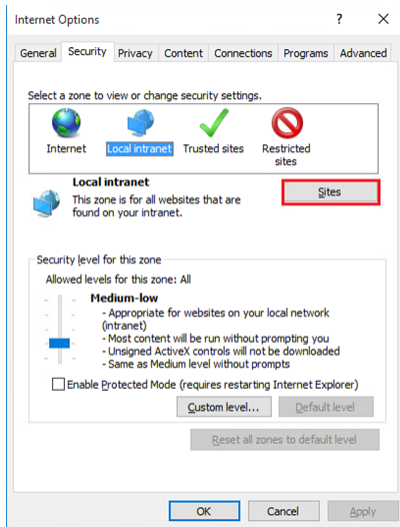
3. Navigate to the **Connections** tab and select the **LAN settings** button.



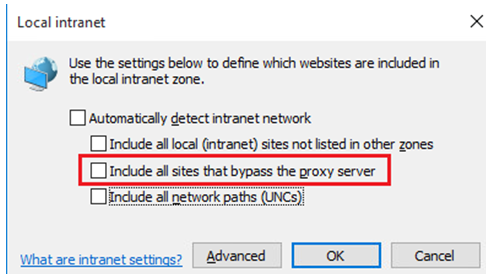
4. Make sure the **Automatically detect settings** box is not checked. (If it is checked, uncheck it).
5. Check the **Use automatic configuration script** box and paste your proxy IP address into the **Address** field and click **OK**.



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

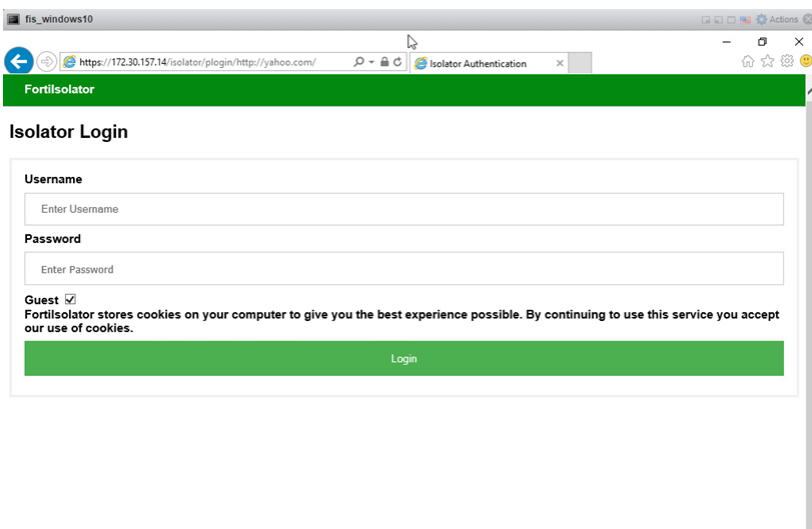


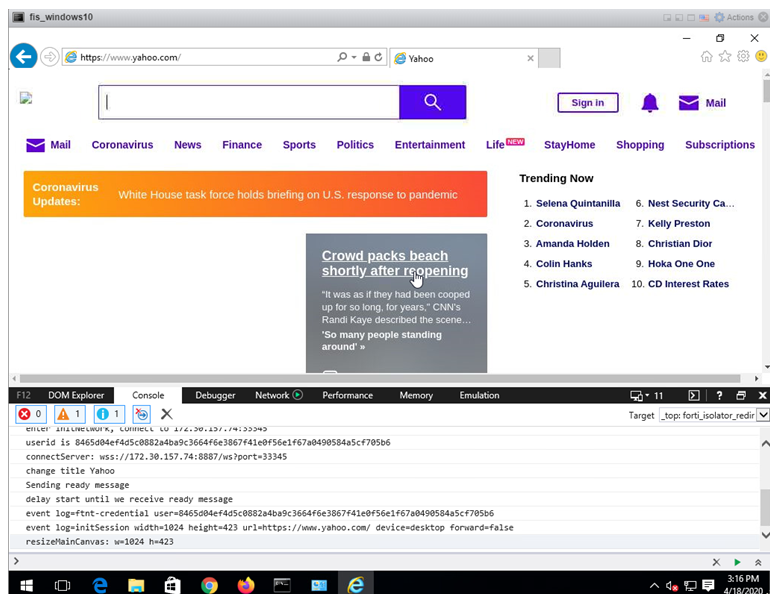
7. Click the **Sites** button to configure how Intranet sites are detected.
8. Make sure that at the very least the **Include all sites that bypass the proxy server** box is not checked. We recommend that all the options for these settings are not checked when possible. Click **OK**.



9. Close and restart Internet Explorer.

Verifying Fortisolator proxy mode with Internet Explorer



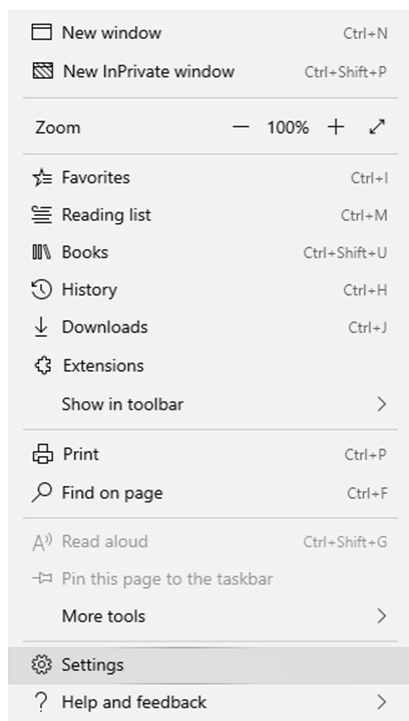


Using proxy mode with Edge

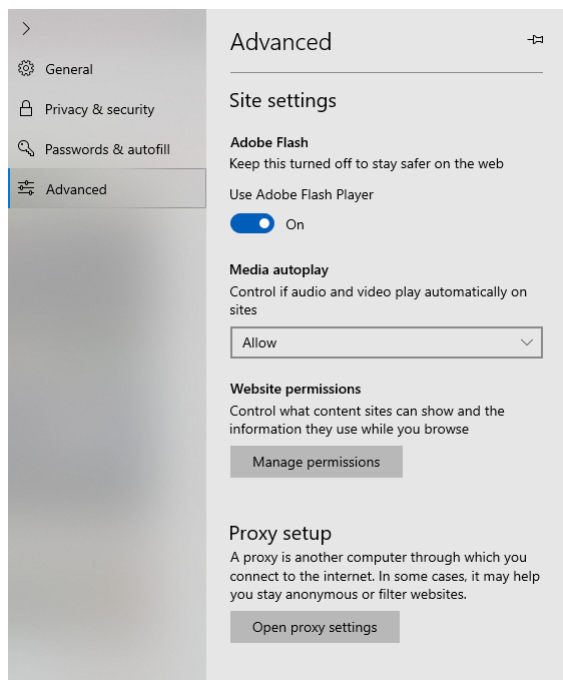
Use this procedure to configure proxy mode with Edge.

Steps

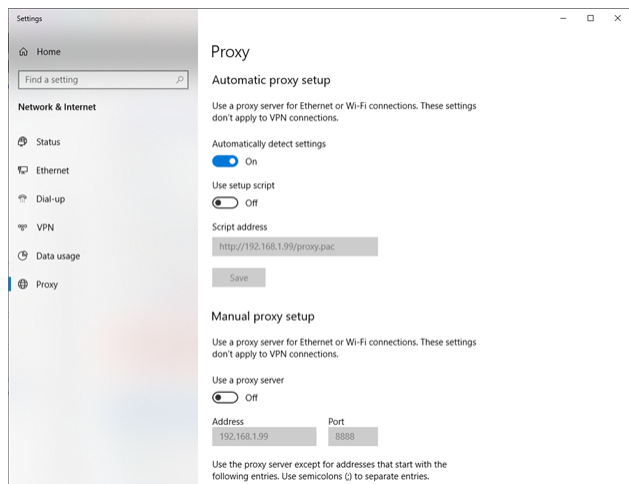
1. Open an Edge browser and click the gear icon at the top right corner to open browser settings.
2. Select **Settings** from the menu.



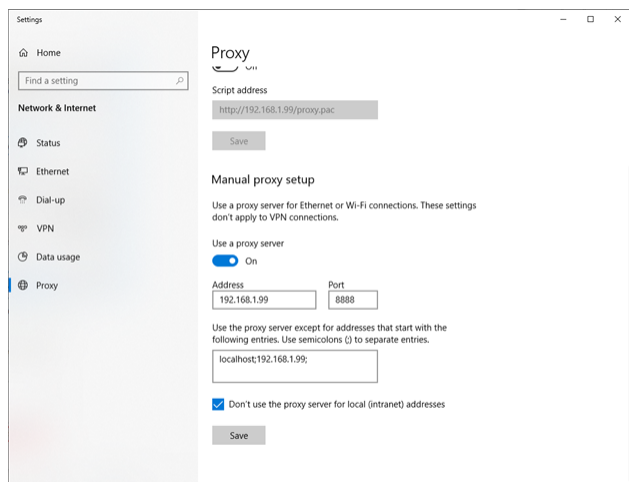
3. Click on **Advanced**.



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

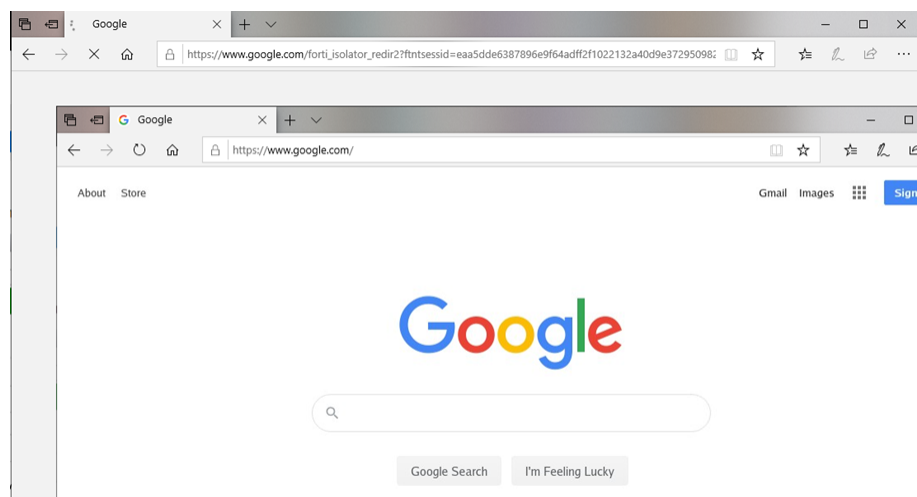


5. Enable **Manual proxy setup**, paste your proxy IP address into the **Address** field with **port 8888** and exception list:



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

Verifying Fortisolator proxy mode with Edge



PAC file mode

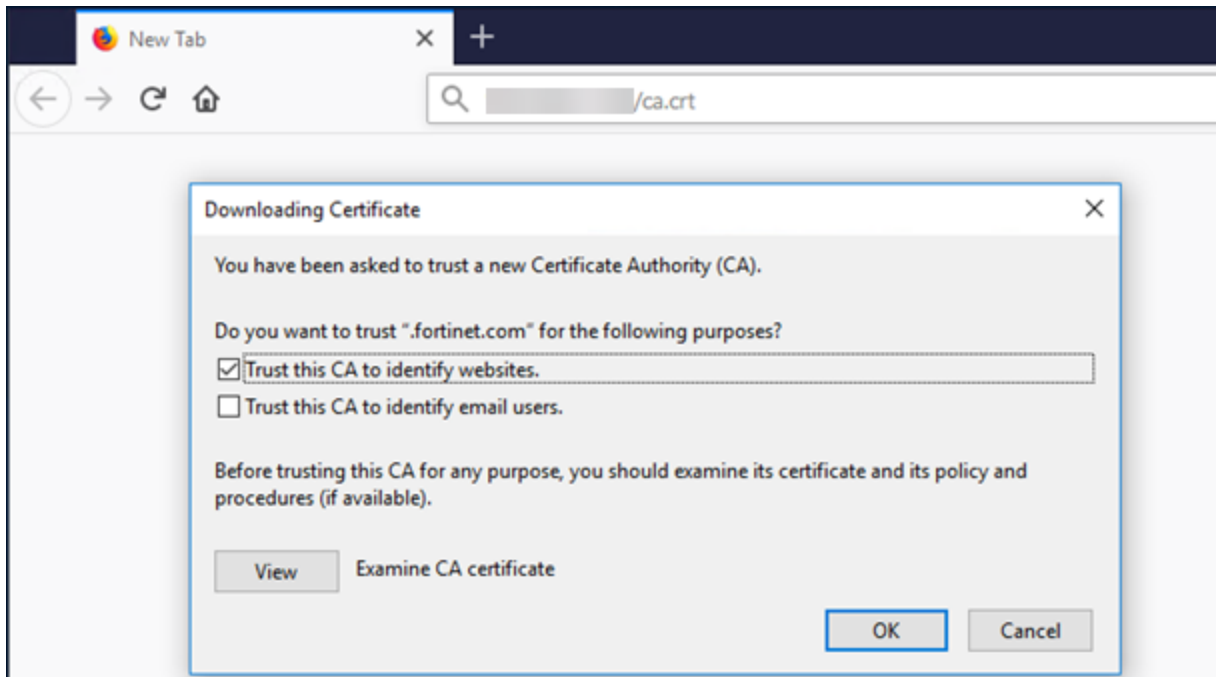
PAC file mode with Mozilla Firefox

Importing the Fortisolator certificate into the Mozilla Firefox browser

Use this procedure to import the Fortisolator certificate into the Mozilla Firefox browser.

Steps

1. To download the Fortisolator certificate (ca.crt) and import it into the Mozilla Firefox browser, follow these steps:
 - a. In the Mozilla Firefox browser address bar, type `http://<internal_IP_address>/ca.crt`.
 - where `<internal_IP_address>` is the IP address of the Fortisolator internal interface. For example, the IP address of the internal interface that you configured in step 3 of [Installing Fortisolator 1000F on page 8](#)
 - b. In the **Downloading Certificate** window, select the **Trust this CA to identify websites** checkbox.
 - c. Click **OK**

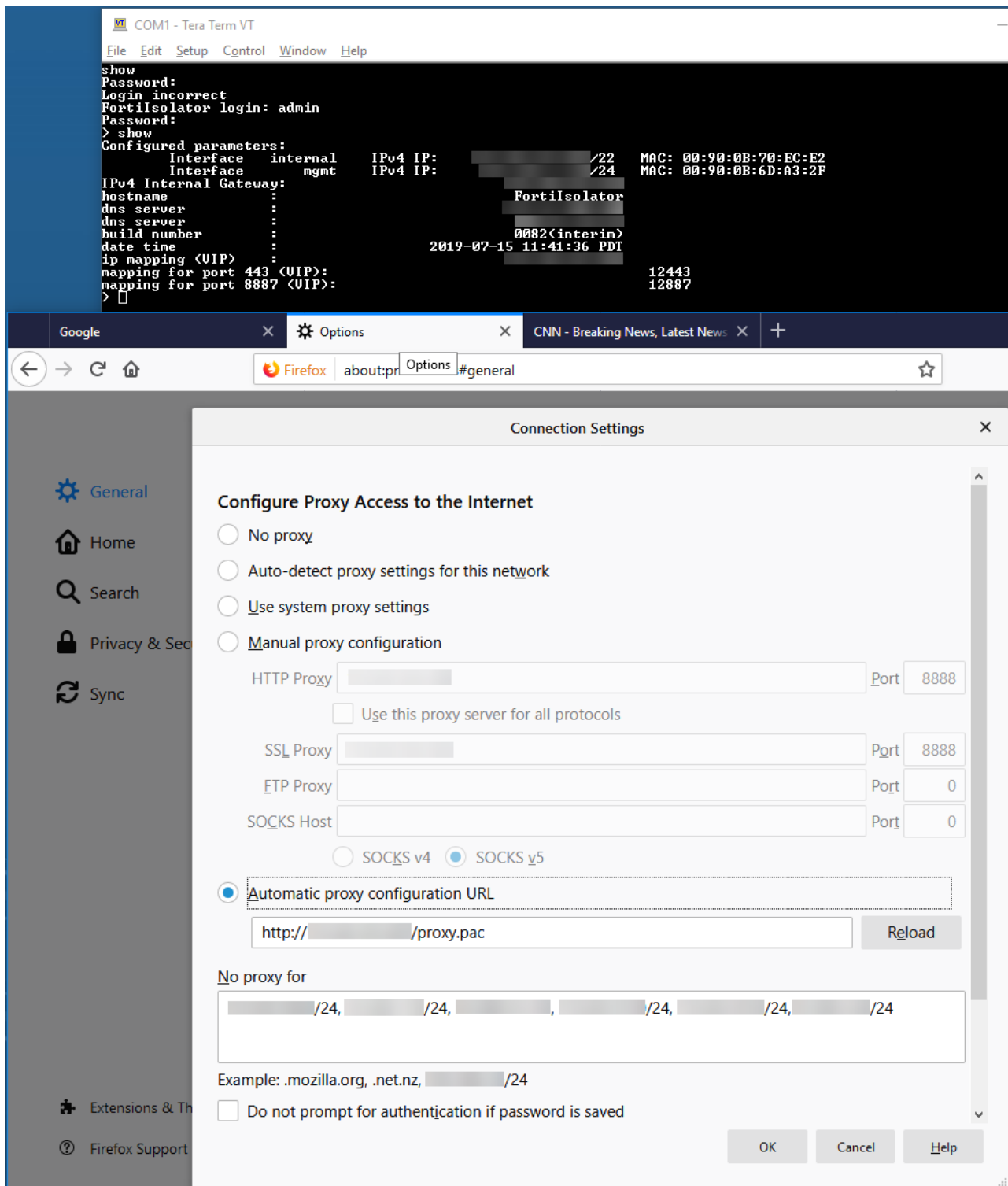


Configuring PAC file mode in Mozilla Firefox

Use this procedure to configure PAC file mode in Mozilla Firefox.

Steps

1. Open the Mozilla Firefox browser.
2. In the menu, click **Options**.
3. Click **General**.
4. In the **Network Settings** section, click **Settings**.
5. In the **Connection Settings** window, select **Automatic proxy configuration URL**, and enter `http://<internal_IP_address>/proxy.pac`.



6. Click **OK**.

Connection Settings [X]

Configure Proxy Access to the Internet

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

HTTP Proxy Port
☐ Use this proxy server for all protocols
 Port
 Port
 Port
☐ SOCKS v4 ☒ SOCKS v5

☒ Automatic proxy configuration URL

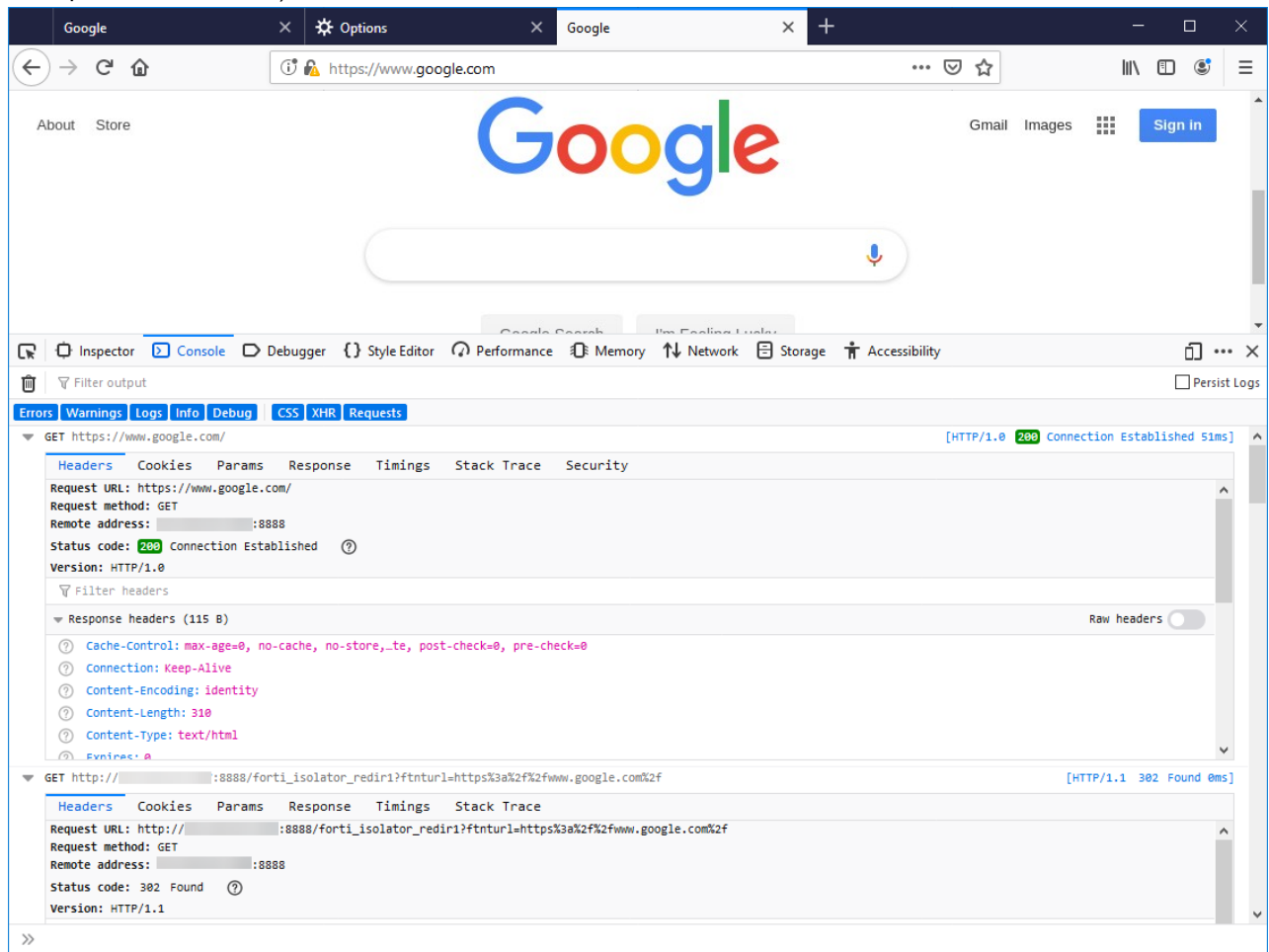
Verifying Fortisolator PAC file mode with Mozilla Firefox

Use this procedure to verify that Fortisolator PAC file mode is working correctly with Mozilla Firefox.

Steps

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=853d1061-b79c-486b-b4f8-0984c7aedb8b&ftntpasswd=8b217bea-34d0-4b11-a3d9-dd34f4a99108`.
The page should load successfully with the URL displayed as you typed it (`https://www.google.com`).
2. Check the browser console to make sure that it is connecting to the internal IP address of Fortisolator (for

example, 192.168.1.100).



PAC file mode with Google Chrome

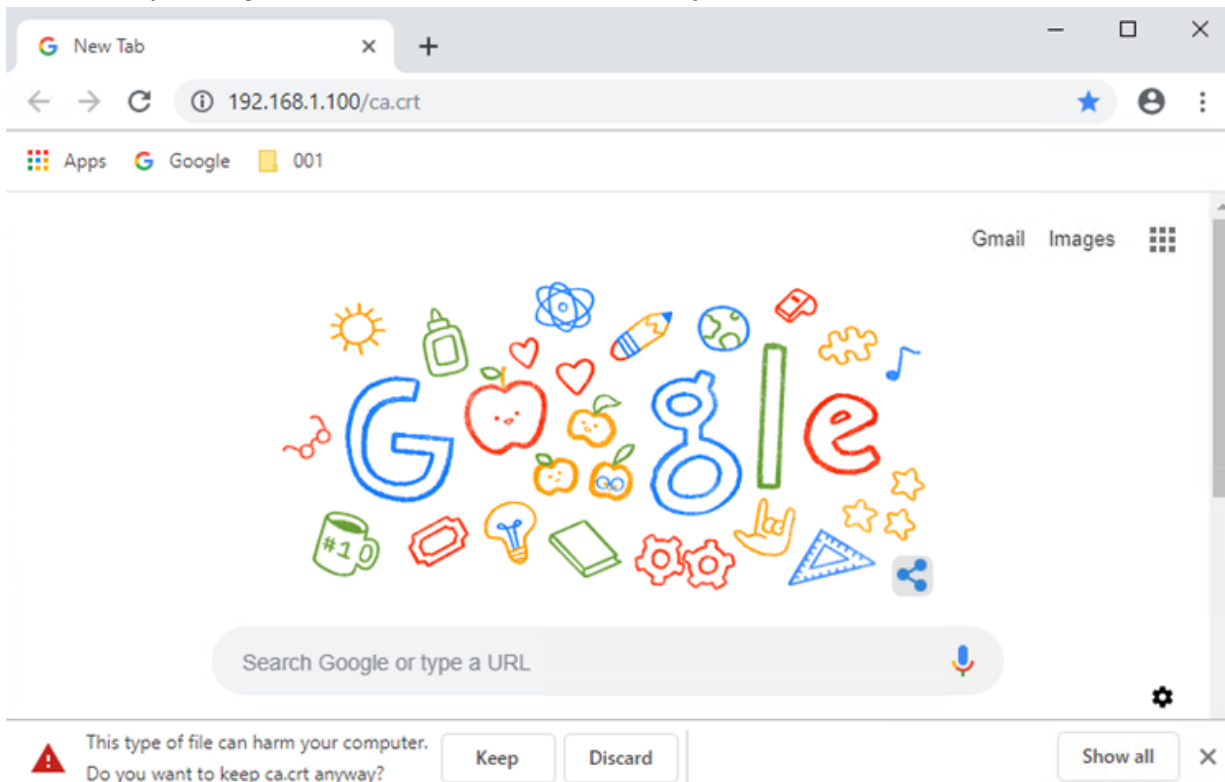
Importing the Fortisolator certificate into the Google Chrome browser

Use this procedure to import the Fortisolator certificate into the Google Chrome browser.

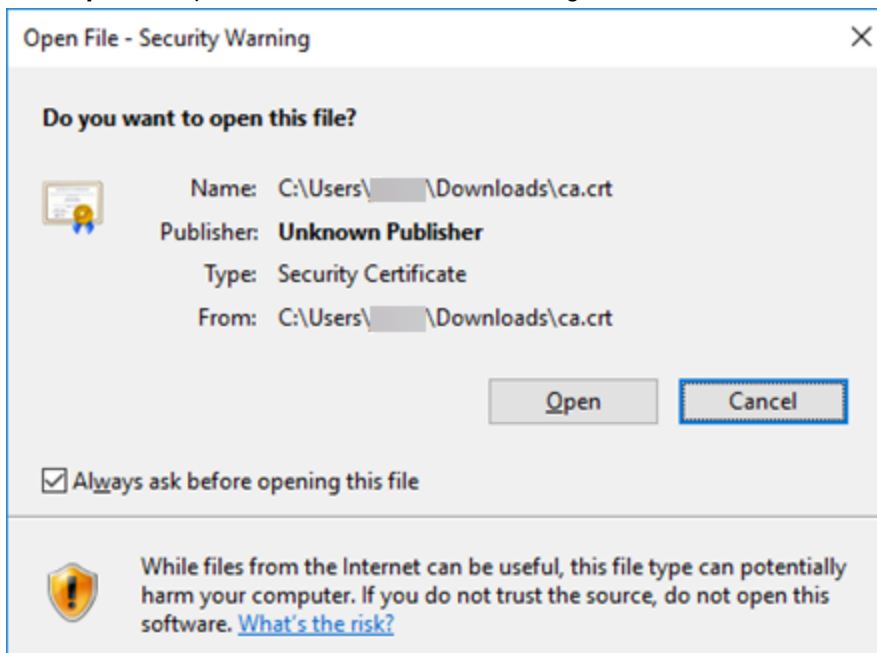
Steps

1. To download the Fortisolator certificate (ca.crt) and import it into the Google Chrome browser, follow these steps:
 - a. In the Google Chrome browser address bar, type `http://<internal_IP_address>/ca.crt` (for example, `http://192.168.1.100/ca.crt`).
 - where `<internal_IP_address>` value is the IP address of the Fortisolator internal interface. For example, the IP address of the internal interface that you configured in step 3 of [Installing Fortisolator 1000F](#) on page 8.

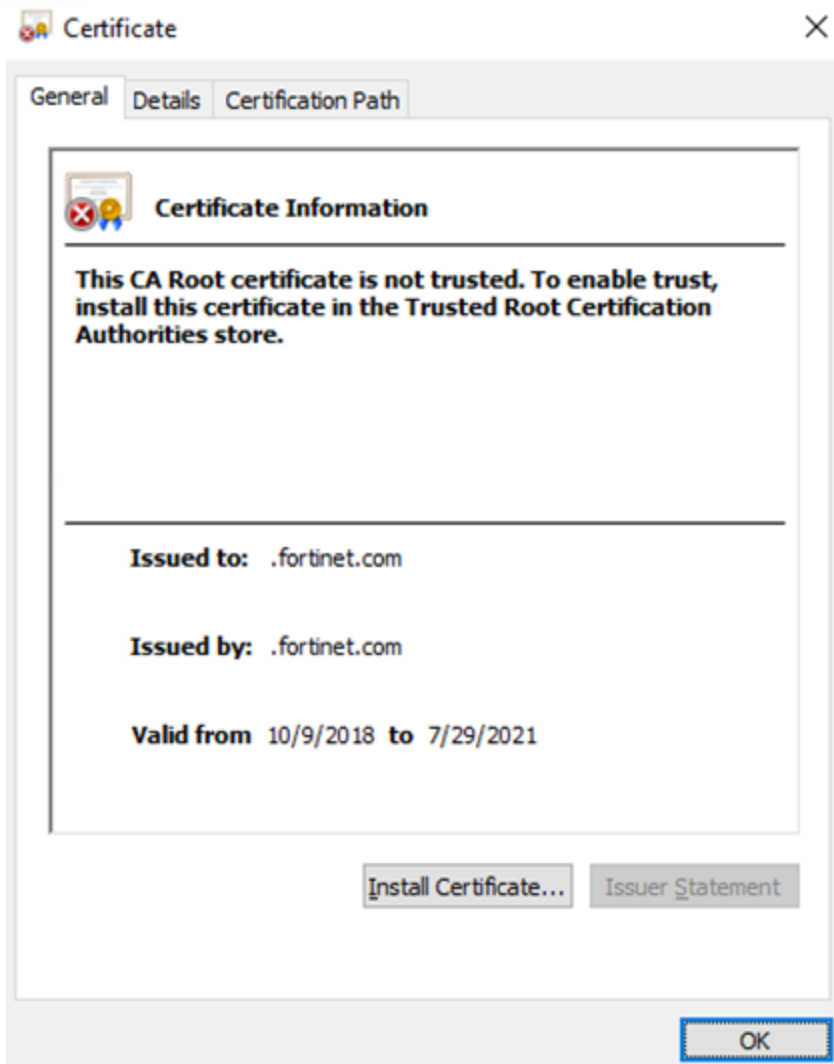
- b. In the security warning at the bottom of the browser, click **Keep** to download the certificate.



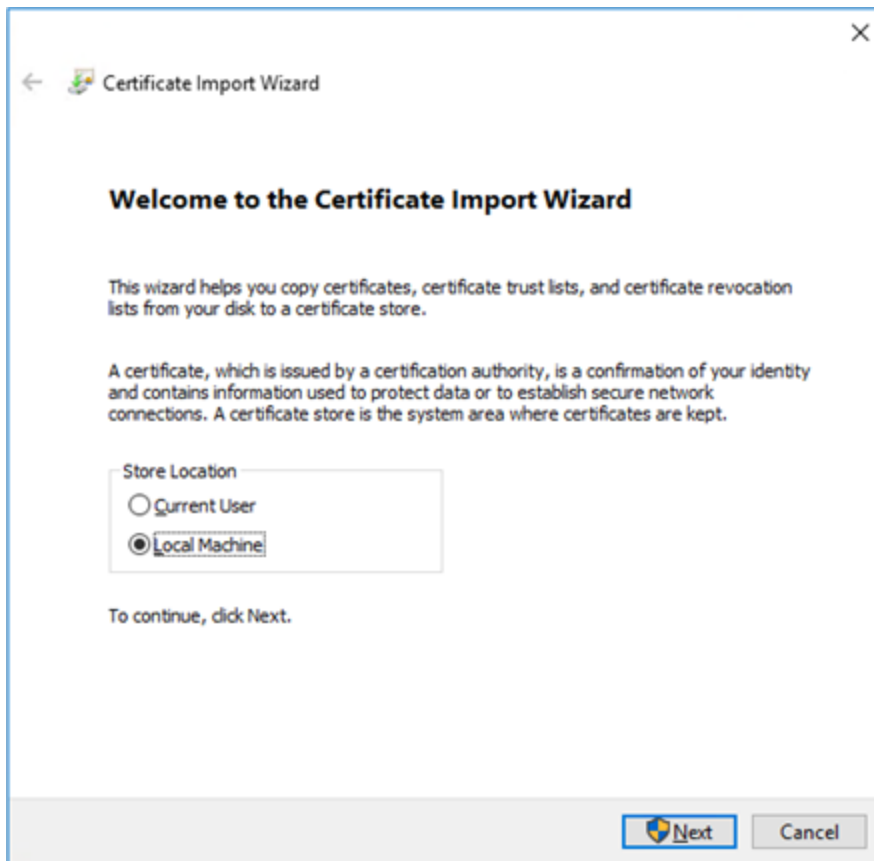
- c. Click **Open** to import the ca.crt certificate into Google Chrome.



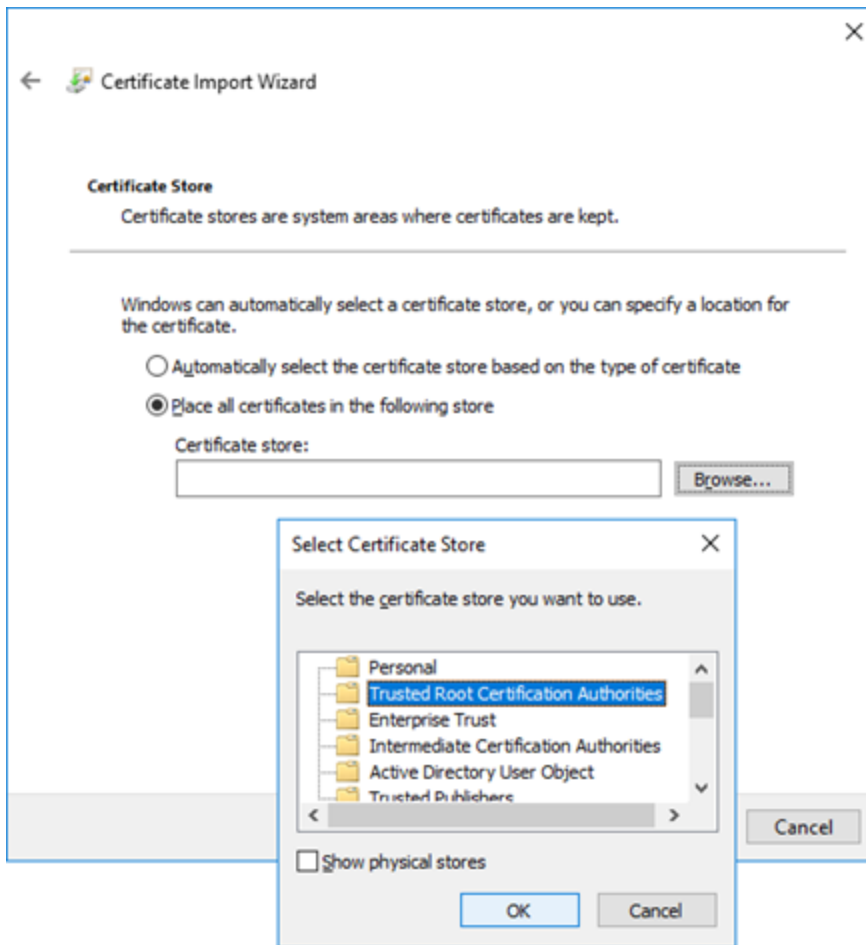
- d. Click **Install Certificate**.



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



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



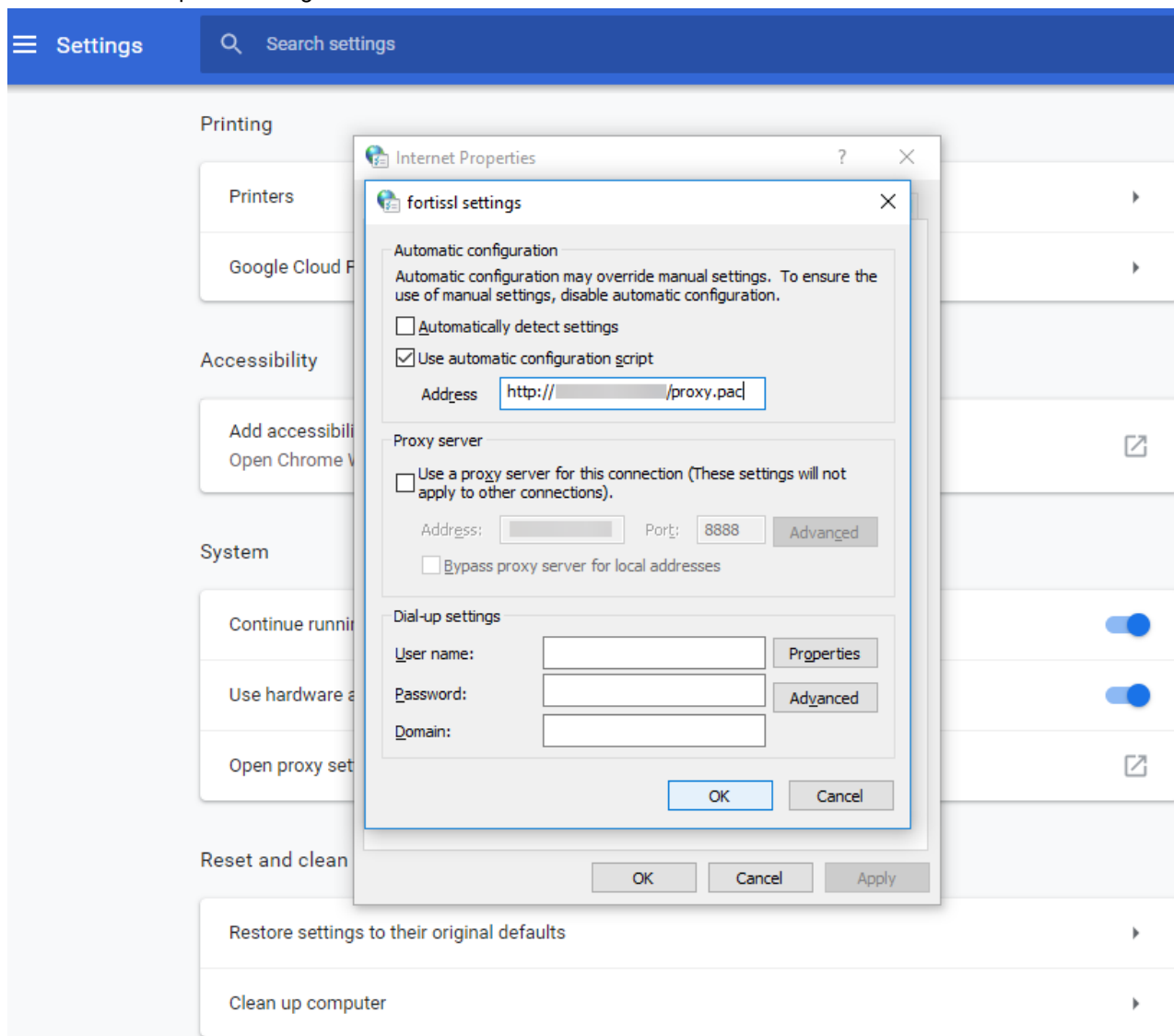
Configuring PAC file mode in Google Chrome

Use this procedure to configure PAC file mode in Google Chrome.

Steps

1. Open the Google Chrome browser.
2. In the menu, click **Settings**.
3. Expand **Advanced**.
4. In the **System** section, click **Open proxy settings**.
5. In the **Internet Properties** window, click the **Connections** tab.
6. Click **LAN settings**.
7. In the **Automatic configuration** section, select **Use automatic configuration script**, and enter `http://<internal_IP_address>/proxy.pac` in the **Address** field.

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



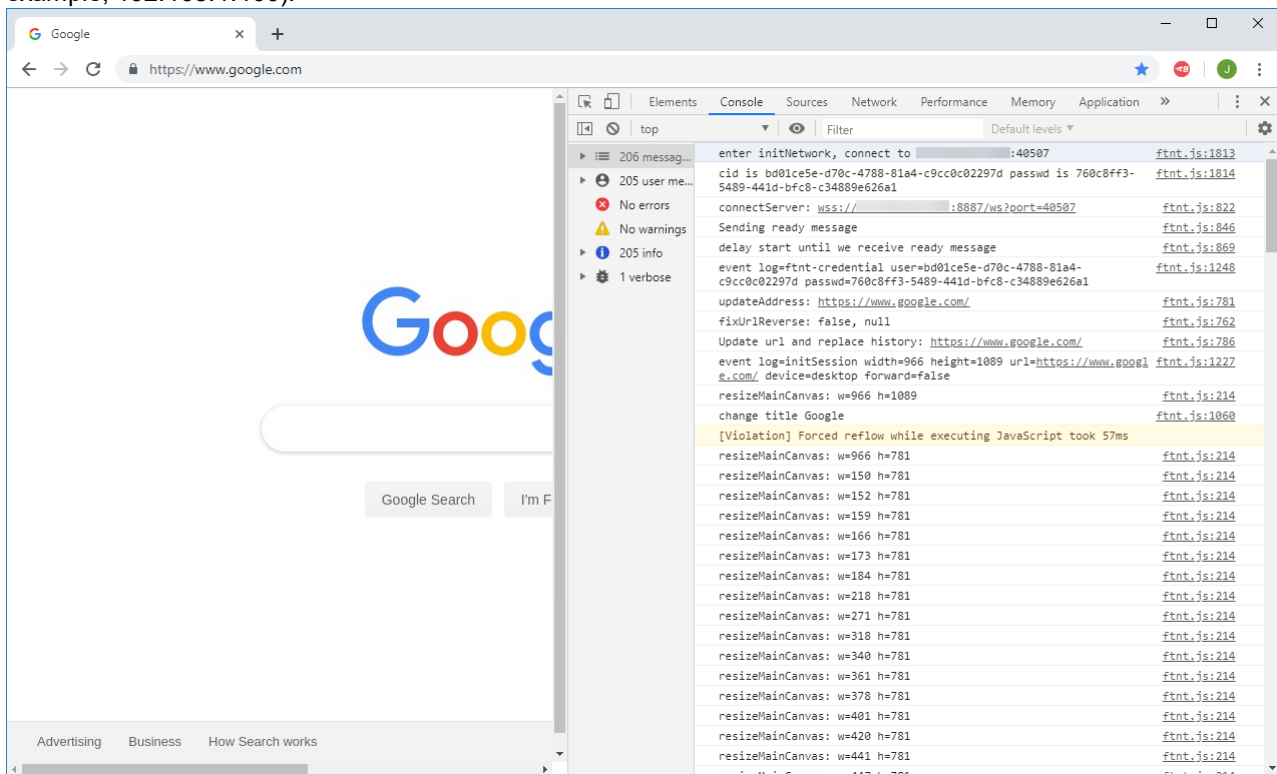
Verifying Fortisolator PAC file mode with Google Chrome

Use this procedure to verify that Fortisolator proxy mode is working correctly with Google Chrome.

Steps

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

2. Check the browser console to make sure that it is connecting to the internal IP address of Fortisolator (for example, 192.168.1.100).



Logging in as end user

If it is the end user's first time browsing the web through Fortisolator or if the browser cache has been cleared, the end user will be prompted to log into their user account through the following login page:

The screenshot shows the Fortisolator login page. The browser address bar shows the URL '192.168.1.101/isolator/login/https://www.google.com'. The page has a green header with the text 'Fortisolator'. Below the header, the title 'Isolator Login' is displayed. The login form includes a 'Username' field with the placeholder 'Enter Username', a 'Password' field with the placeholder 'Enter Password', and a 'Guest' checkbox. Below the checkbox, there is a message: 'Fortisolator stores cookies on your computer to give you the best experience possible. By continuing to use this service you accept our use of cookies.' At the bottom of the form is a green 'Login' button.

[NTLM Authentication](#)

Login options

End users can log into Fortisolator in one of three ways:

- **Local user** - User enters their designated username and password
- **Guest user** - User leaves **Username** and **Password** fields blank and checks the Guest box
- **Single sign-on** - User clicks on the **NTLM Authentication** link, which will prompt the end user to enter their organization's single sign-on credentials. See [User definition on page 69](#) for information on how to set up single sign-on.

Copying and pasting text

Use this procedure to copy and paste text in a browser that is running through Fortisolator.

Steps

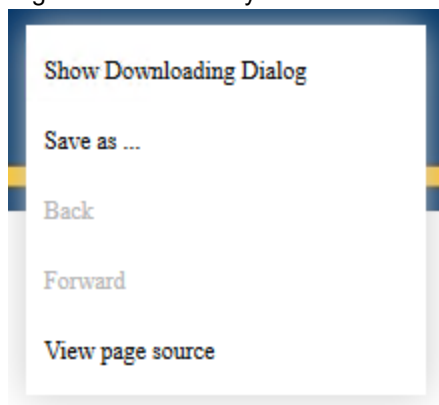
1. In a browser, select text that you want to copy, and then right-click.
2. Click **Copy**.
3. Navigate to the location where you want to paste the text, and then right-click.
4. Click **Paste**.

Downloading files

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

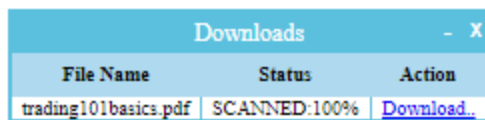
Steps

1. Right click on the file you wish to download and a menu will appear.



2. Click **Save as...** and the **Downloads** dialog box will pop 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.



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

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

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



FORTINET®



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