



Fortisolator - Administration Guide

Version 2.0.0

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



January 15, 2020

Fortisolator 2.0.0 Administration Guide

51-121-540944-20200115

TABLE OF CONTENTS

Change log	4
About this release	5
New in this release	5
Overview	6
Fortisolator models	6
Installation	7
Downloading Fortisolator firmware	7
Fortisolator appliance installation	7
Installing Fortisolator 1000F	7
Fortisolator VM installation	14
Installing Fortisolator VM for Linux KVM	14
Installing Fortisolator VM for VMware vSphere	22
Installing Fortisolator VM for VMware ESXi	31
Upgrade	37
Fortisolator appliance upgrade	37
Upgrading Fortisolator firmware using a web browser	37
Upgrading Fortisolator firmware using a USB flash drive	37
Setup	38
Configuring the console	38
Port forwarding	41
Configuration	53
Accessing the Fortisolator administration portal	53
Configuring time settings	54
Configuring network interface settings	55
Configuring DNS settings	55
Configuring routing settings	55
Configuring end user accounts	56
Configuring policies and profiles	59
Configuring log settings	64
Configuring high availability	65
Configuring the login disclaimer	68
End user operation	69
Run web browsers through Fortisolator	69
IP forwarding mode	69
Proxy mode	76
PAC file mode	88
Logging in as end user	98
Copying and pasting text	99
Downloading files	99
Diagnostics	101
Diagnostic tools	101

Change log

Date	Change description
2019-12-19	Fortinet Fortisolator 2.0.0 document release. See New in this release on page 5 .

About this release

This section provides information about new features in Fortisolator version 2.0.0.

New in this release

Fortisolator version 2.0.0 includes the following new features:

- Read-only guest administrator account, see [Accessing the Fortisolator administration portal on page 53](#)
- Single Sign-On with NTLM authentication, see [Setting up single sign-on for local users on page 59](#) and [Logging in as end user on page 98](#)
- Guest end user and local end user accounts, see [Configuring end user accounts on page 56](#) and [Logging in as end user on page 98](#)
- RADIUS database for secure user info storage
- Logs of end user activity that can be downloaded and/or sent to remote servers, see [Configuring log settings on page 64](#)
- Bandwidth usage control through image quality and video frame rate in Isolator browsing profile configuration, see [Creating Isolator browsing profile on page 59](#)
- Ability to upload and download files by end user, see [Creating Isolator browsing profile on page 59](#) and [Downloading files on page 99](#)
- Security feature that makes embedded links in downloaded files inactive, see [Creating Isolator browsing profile on page 59](#)
- Anti-virus scanner of files to be downloaded, see [Creating Isolator browsing profile on page 59](#) and [Downloading files on page 99](#)

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 7](#)
- [Fortisolator VM installation on page 14](#)

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 7](#).
- 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: :
IPv4 MGMT Gateway: :
hostname : FIS1KFT618000001
dns server :
dns server :
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: :
IPv4 MGMT Gateway: :
hostname : FIS1KFT618000001
dns server :
dns server :
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 Fortisolator
  system-upgrade     Upgrade Fortisolator System Image
  factory-reset      Reset configuration to defaults and delete all data
  shutdown           Shutdown the Fortisolator
  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 14](#)
- [Installing Fortisolator VM for VMware vSphere on page 22](#)
- [Installing Fortisolator VM for VMware ESXi on page 31](#)

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.

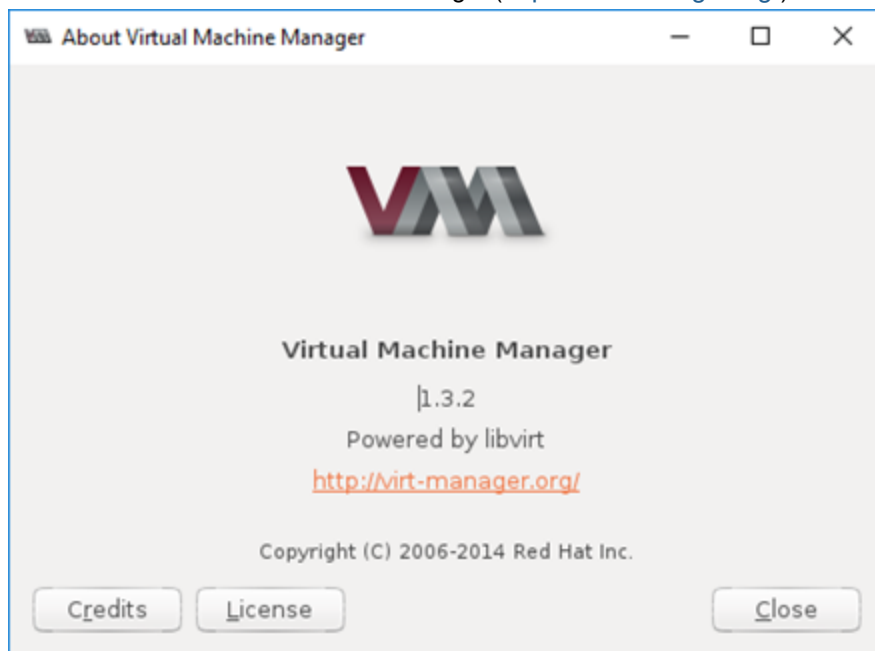
Prerequisites

- 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

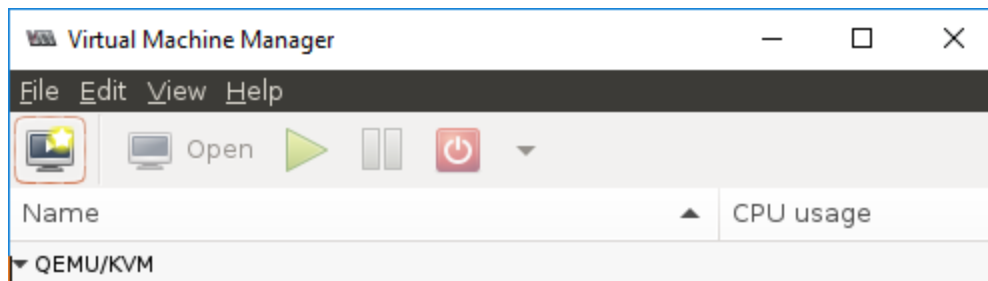
Steps

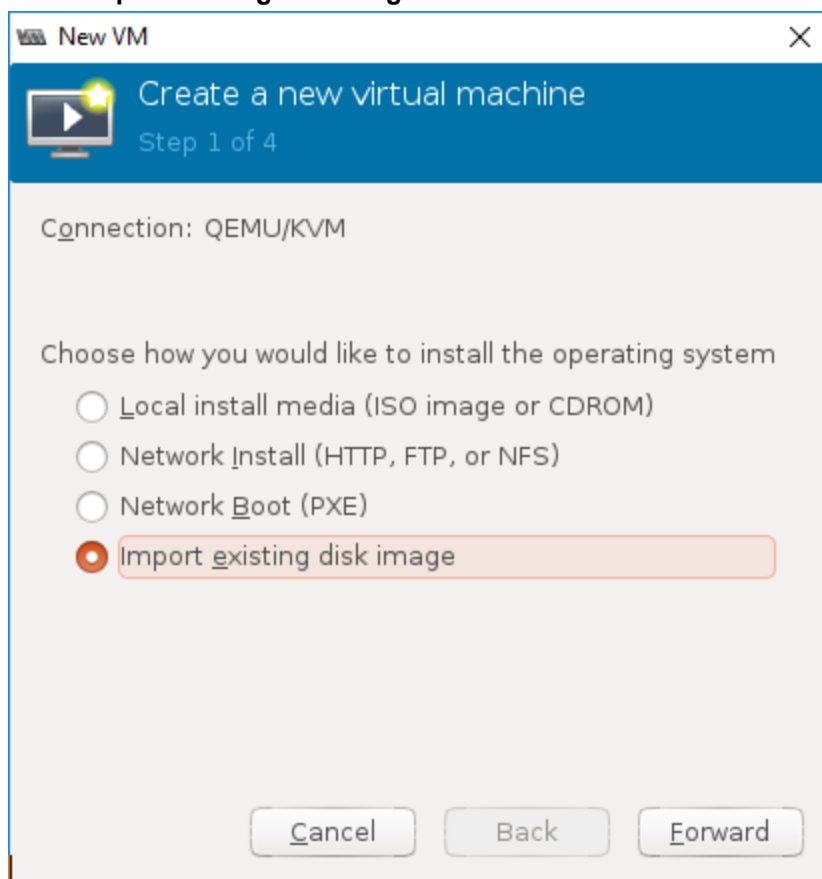
1. Download the Fortisolator firmware for KVM by following the instructions in [Downloading Fortisolator firmware on page 7](#).

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

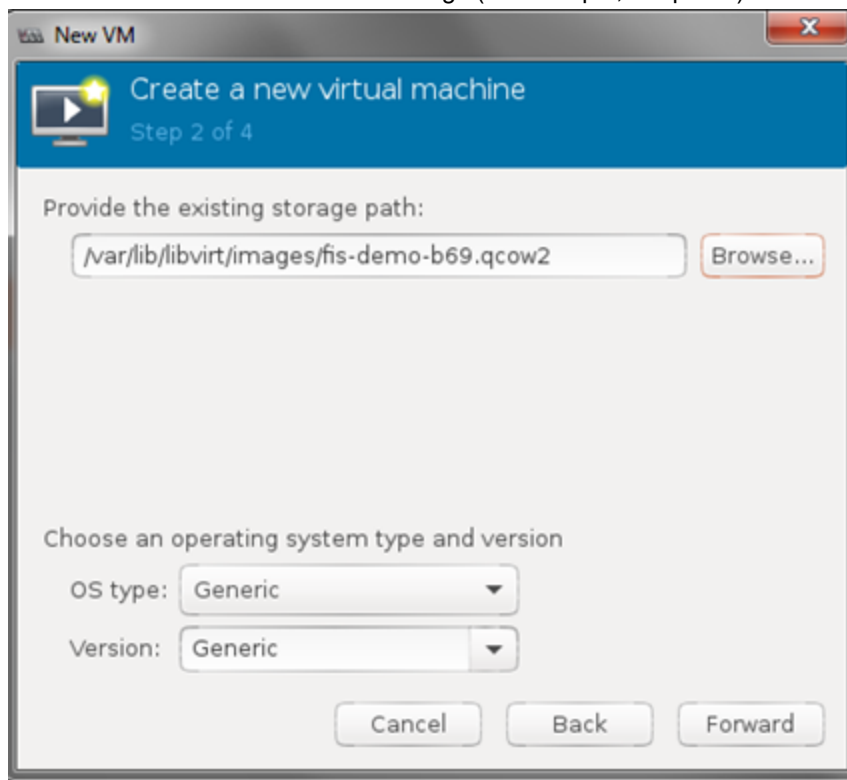


3. Create a new virtual machine.

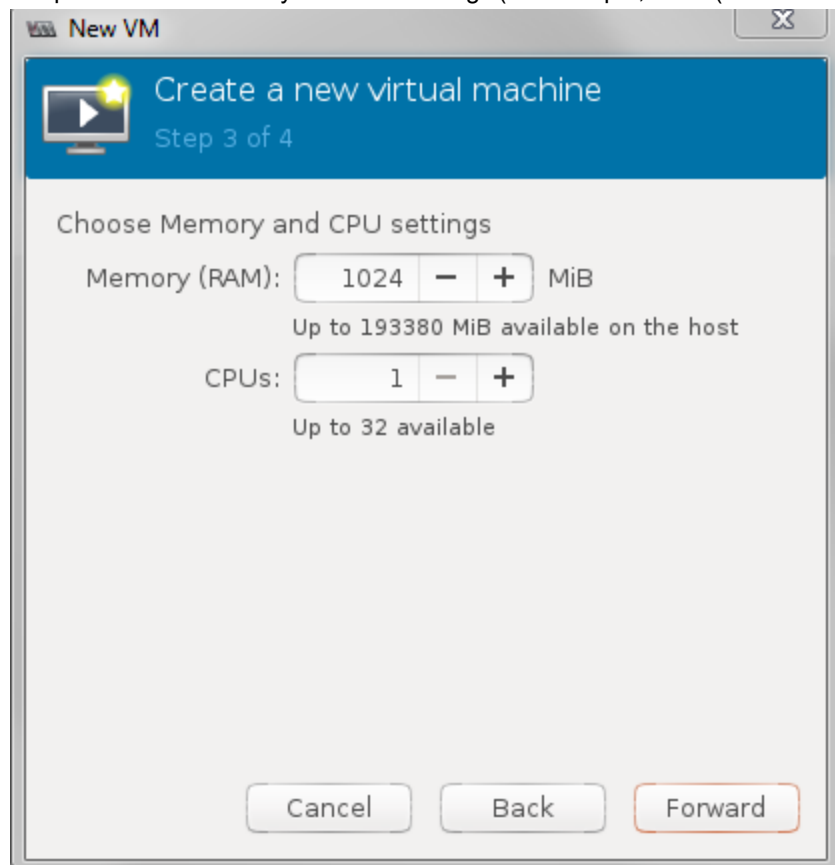


4. Select Import existing disk image.

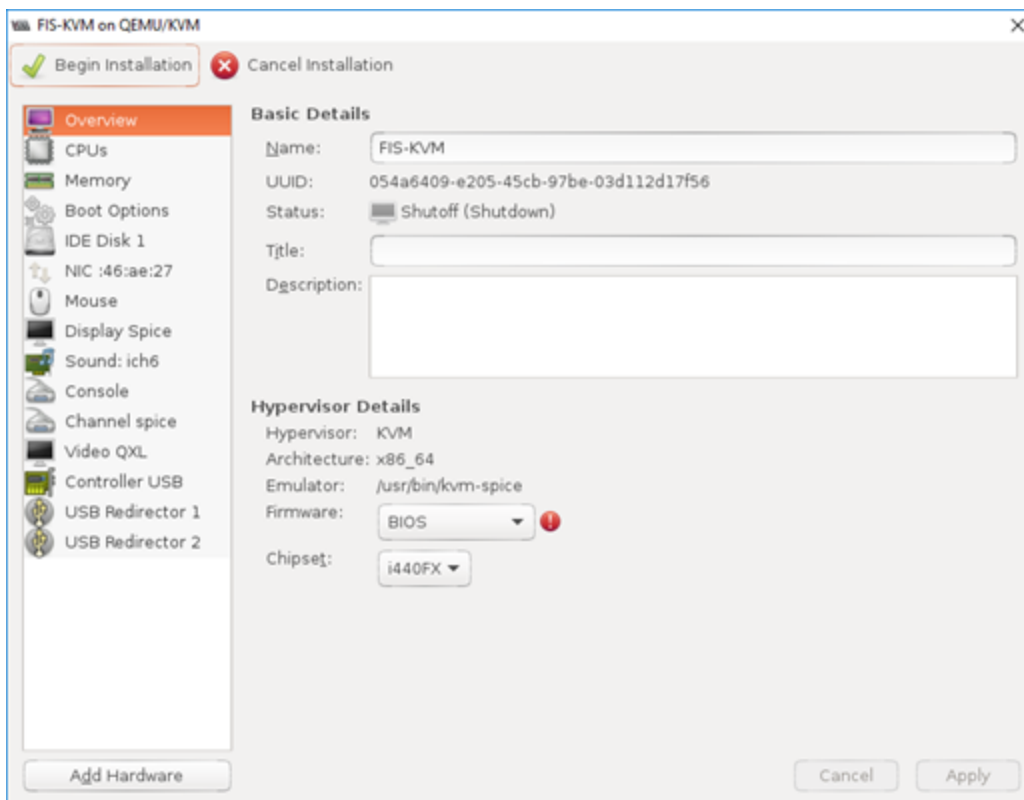
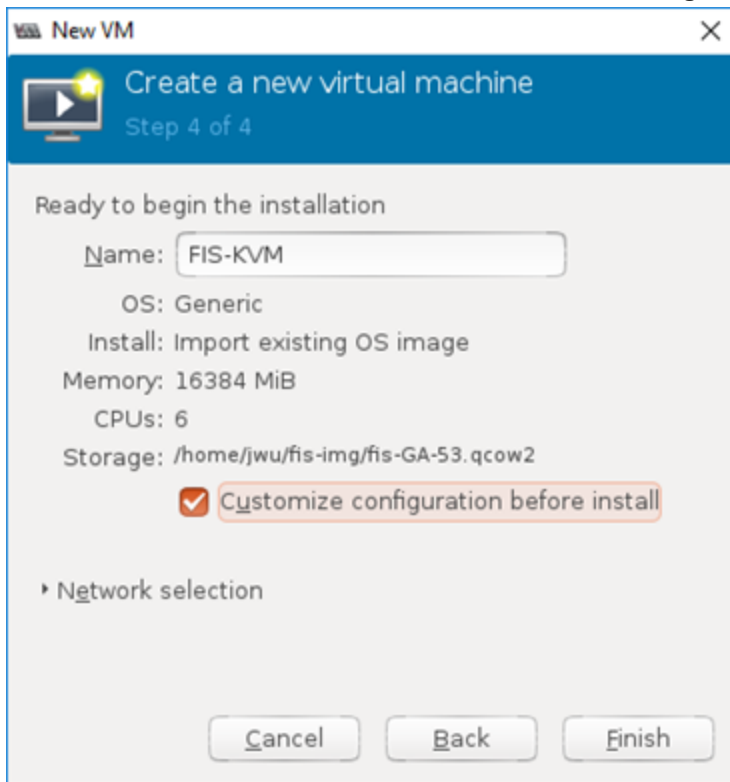
5. Browse and select the Fortisolator image (for example, fis.qcow2).



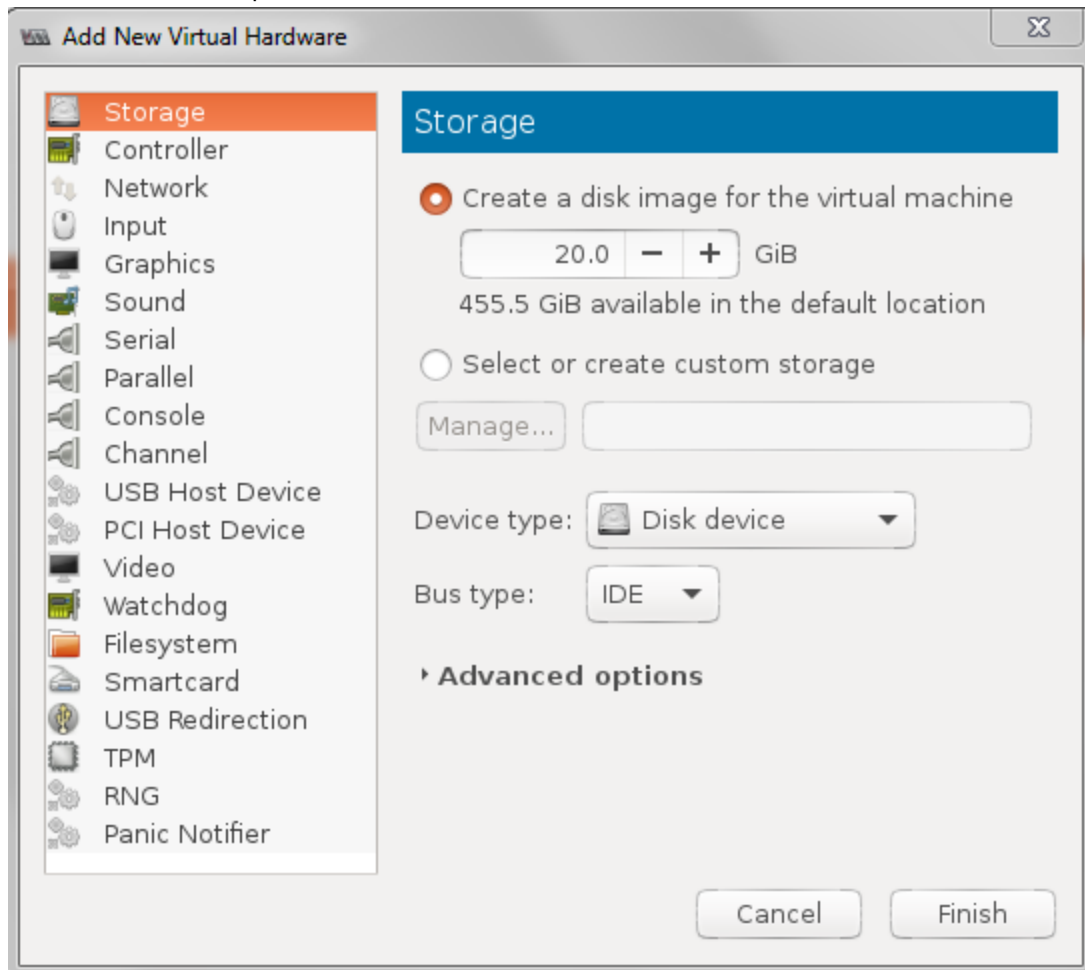
6. Keep the default memory and CPU settings (for example, 1024 (193380 MiB) of memory and 1 CPU).



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

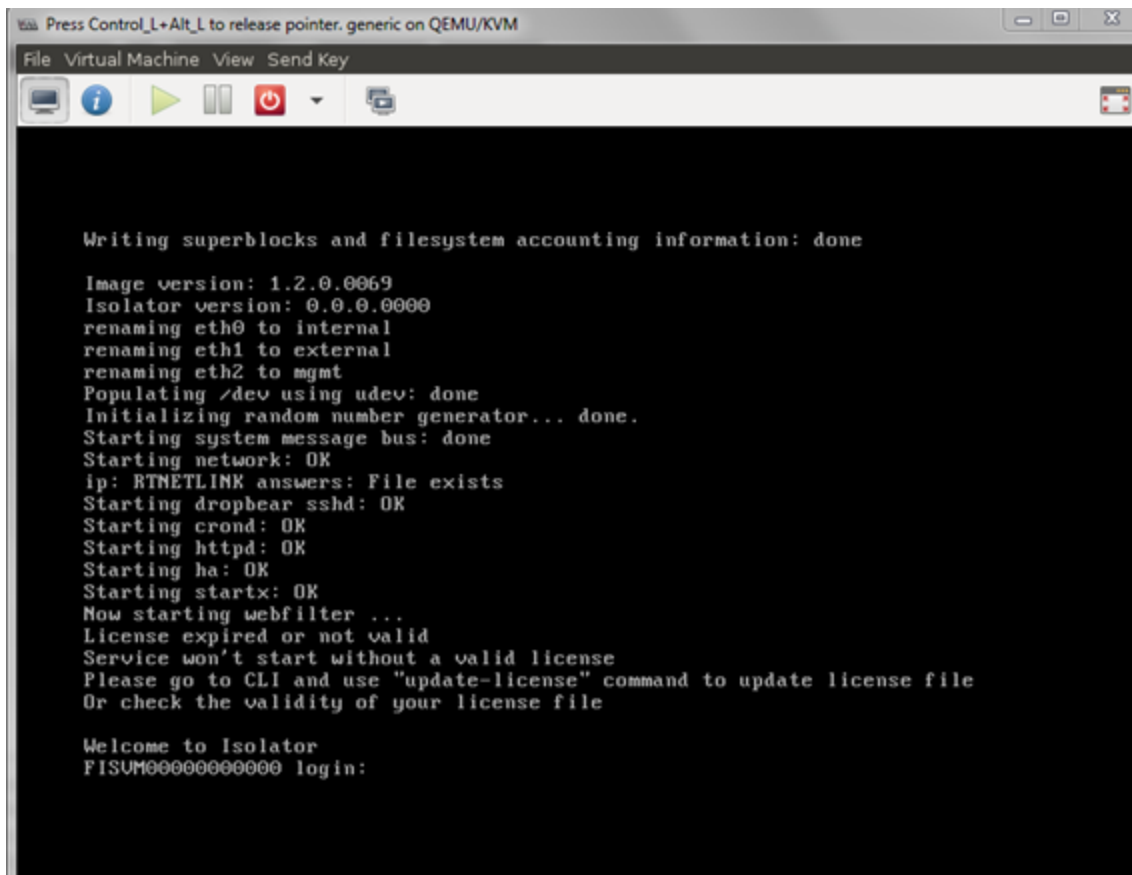
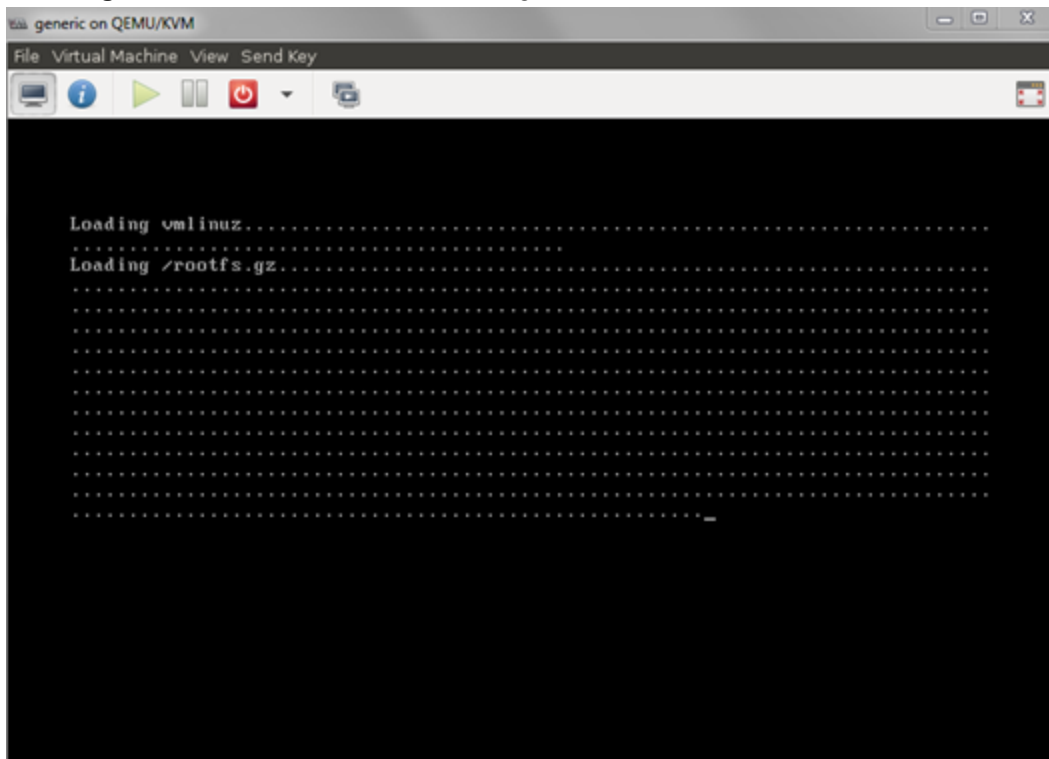


8. Add an IDE disk. Accept the default values.



9. Add three network interfaces: one for Network 2, one for Network 3, and one for Network 4. Leave the settings for **Network source** (Virtual network 'default':NAT) and **Device model** (Hypervisor default) at their default values.

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            172.16.1.1
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

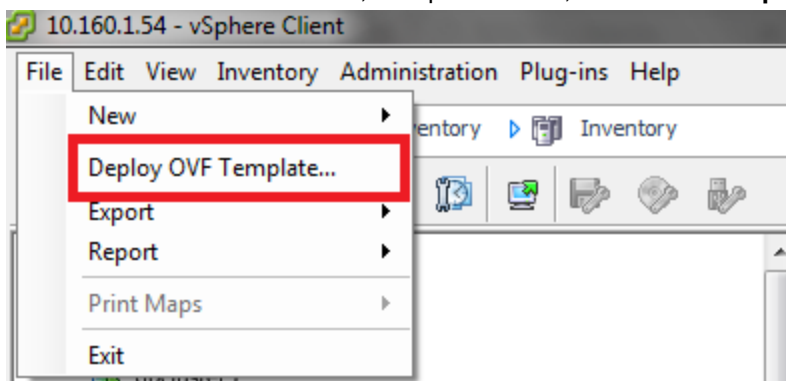
Use this procedure to install Fortisolator VM for VMware vSphere.

Prerequisites

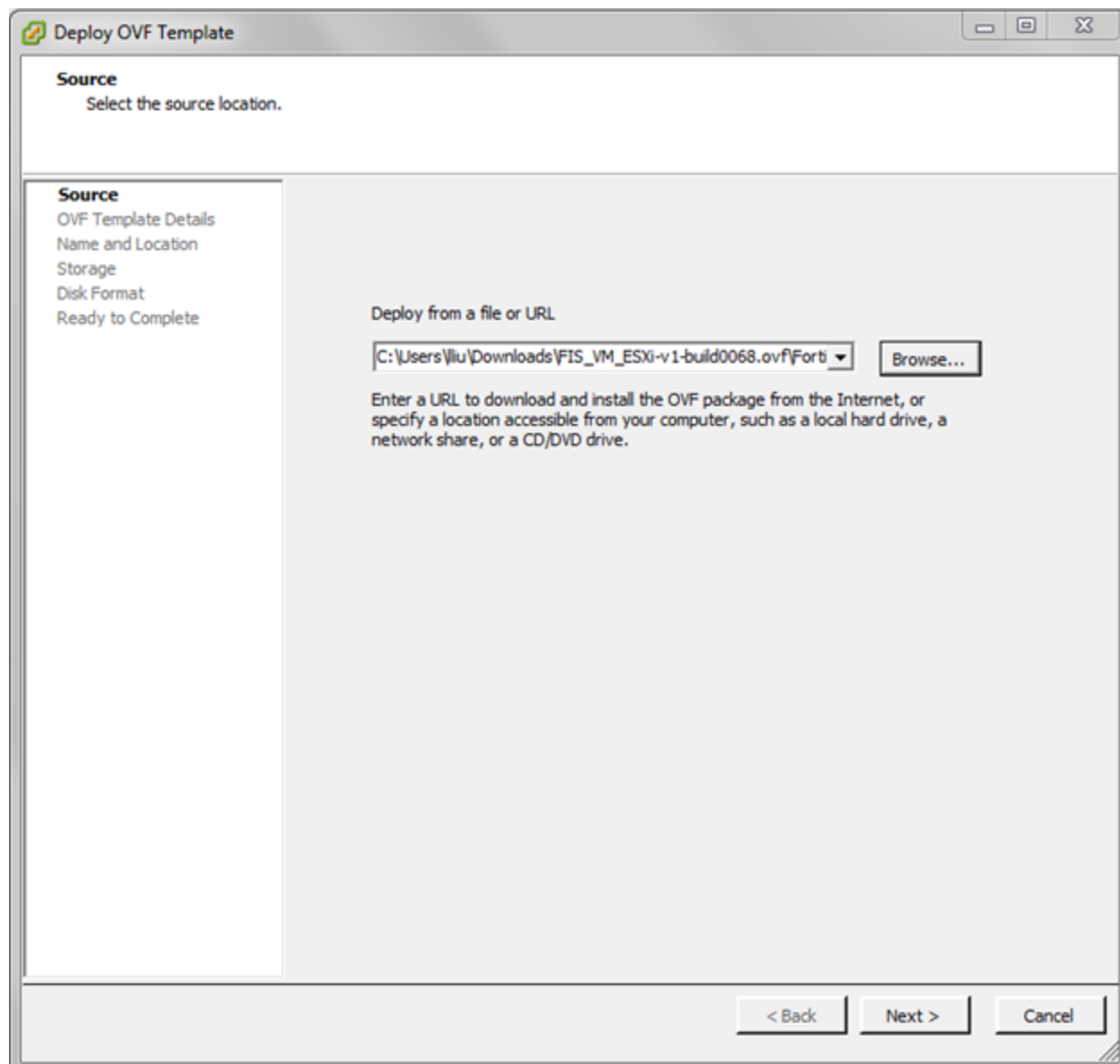
- Install VMware vSphere Client.
- Ensure that your system has one of the following combinations of hard disks and network adapters to support ESXi 6.0:
 - Two SCSI hard disks and three VMXNET 3 network adapters (this is the default)
 - One IDE hard disk and one SCSI hard disk and three E1000 network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

Steps

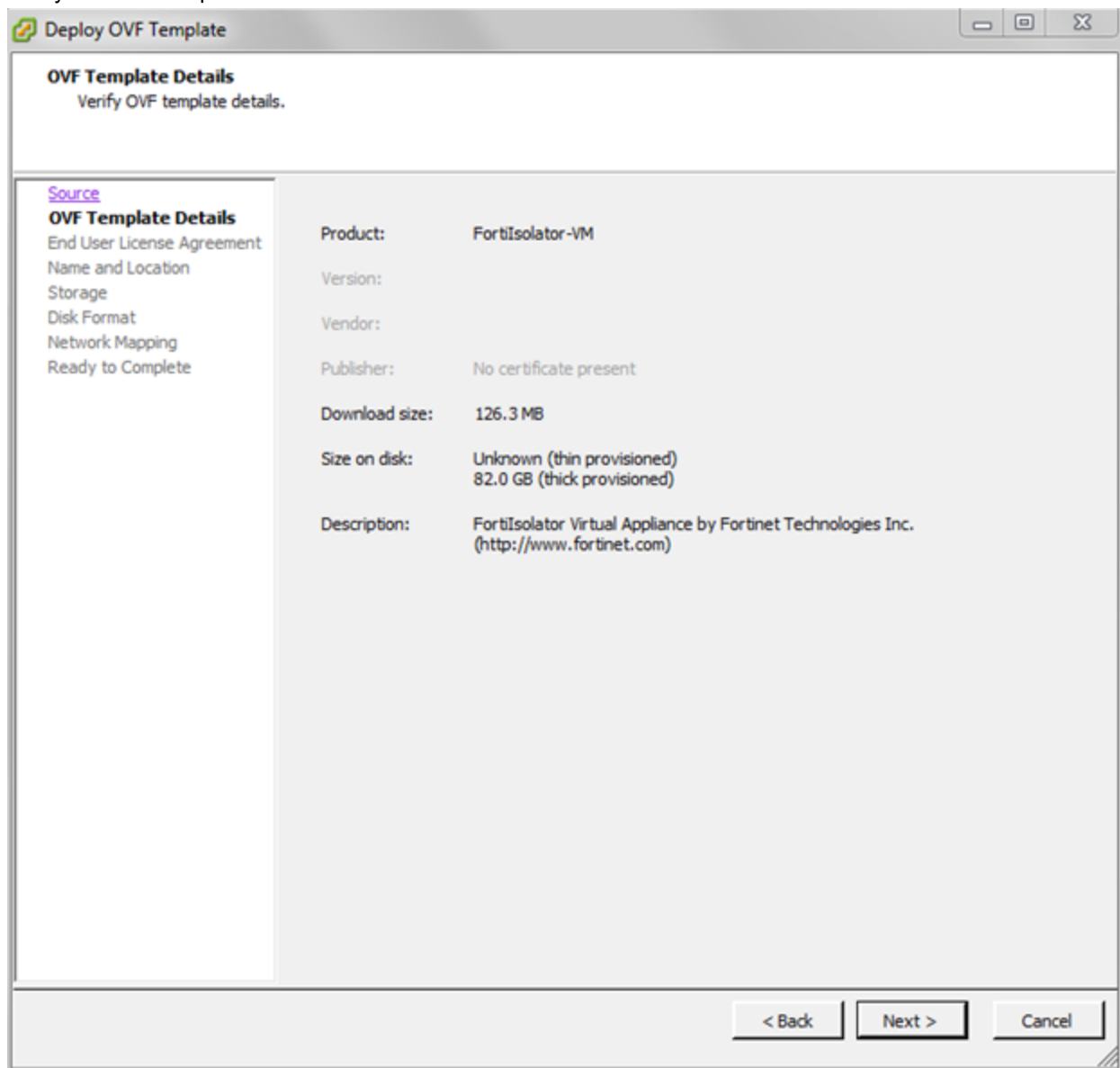
1. Download the Fortisolator firmware for VMware by following the instructions in [Downloading Fortisolator firmware on page 7](#).
2. To create a new virtual machine, in vSphere Client, select **File > Deploy OVF Template**.



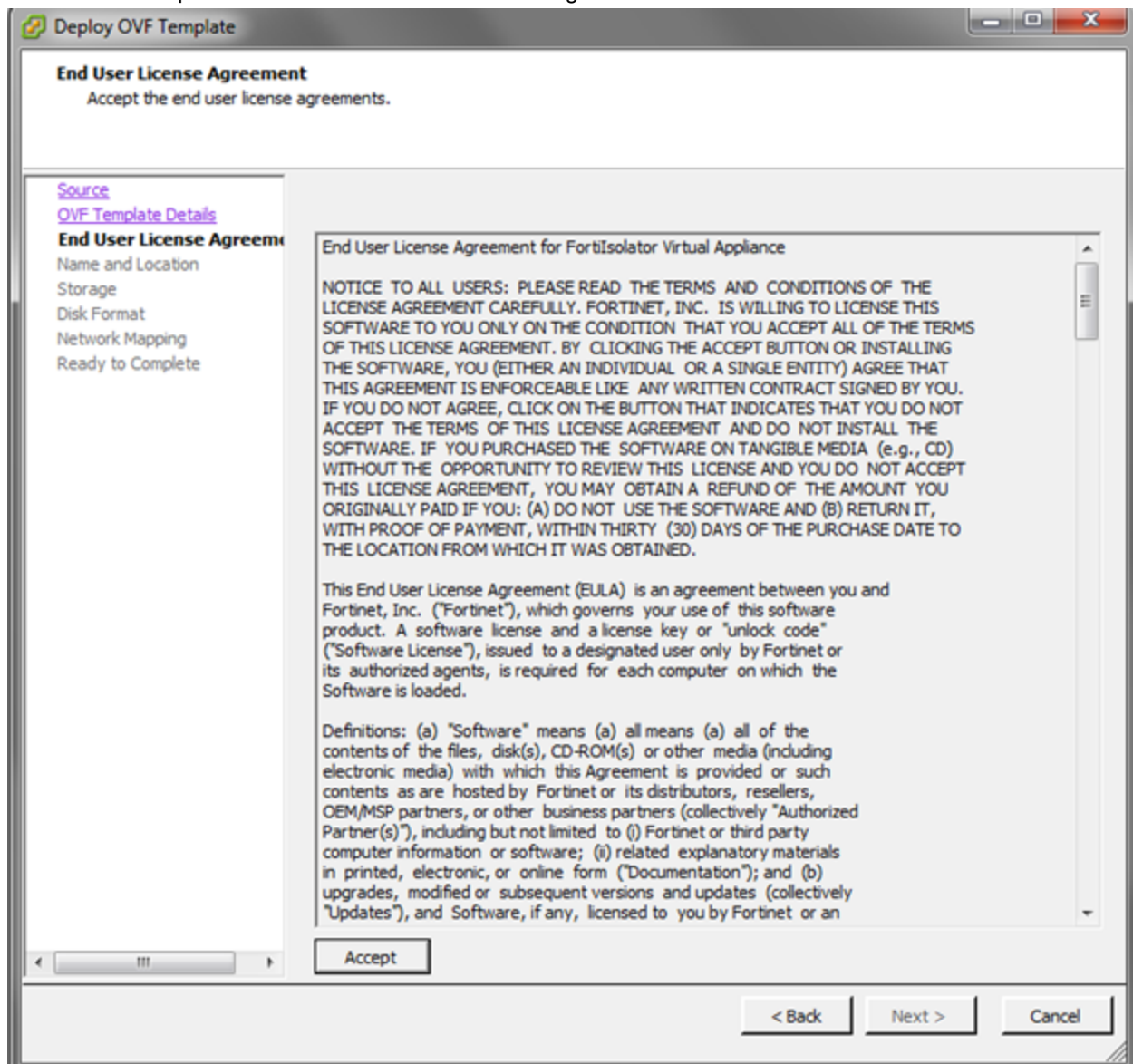
3. Browse to the folder that contains the Fortisolator files and select **Fortisolator.ovf**.

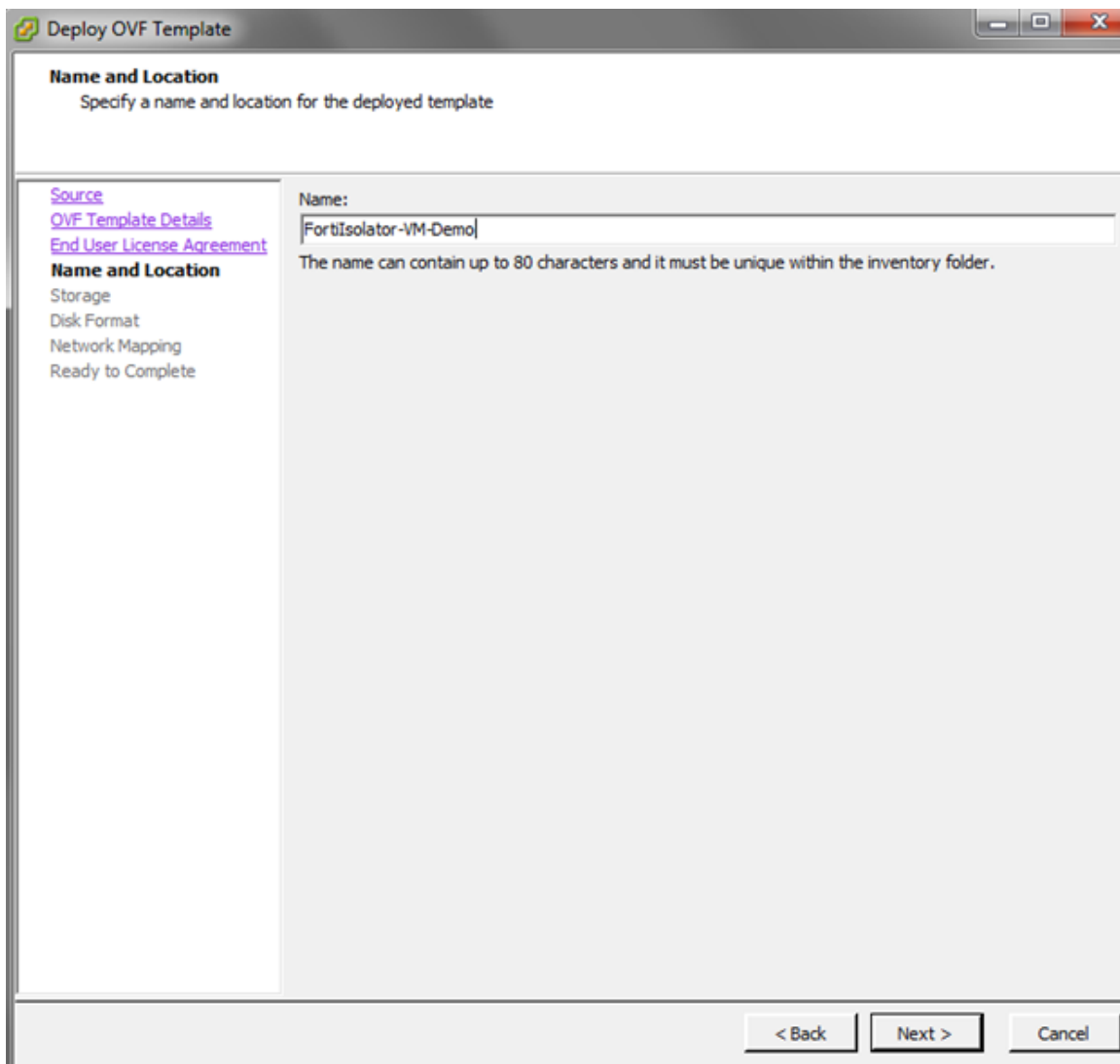


4. Verify the OVF template details.



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 followed by 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'.

Deploy OVF Template

Name and Location
Specify a name and location for the deployed template

[Source](#)
[OVF Template Details](#)
[End User License Agreement](#)
Name and Location
Storage
Disk Format
Network Mapping
Ready to Complete

Name:
Fortisolator-VM-Demo

The name can contain up to 80 characters and it must be unique within the inventory folder.

< Back Next > 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 Provi
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, a sidebar lists navigation options: 'Source', 'OVF Template Details', 'End User License Agreement', 'Name and Location', 'Storage', 'Disk Format' (highlighted), 'Network Mapping', and 'Ready to Complete'. The main area displays 'Datastore:' with a text box containing 'Main-Disk' and 'Available space (GB):' with a text box containing '15.5'. Below these, three radio buttons are listed: 'Thick Provision Lazy Zeroed' (selected), 'Thick Provision Eager Zeroed', and 'Thin Provision'. At the bottom right, there are three buttons: '< Back', 'Next >', and 'Cancel'.

Deploy OVF Template

Disk Format
In which format do you want to store the virtual disks?

[Source](#)
[OVF Template Details](#)
[End User License Agreement](#)
[Name and Location](#)
[Storage](#)
Disk Format
Network Mapping
Ready to Complete

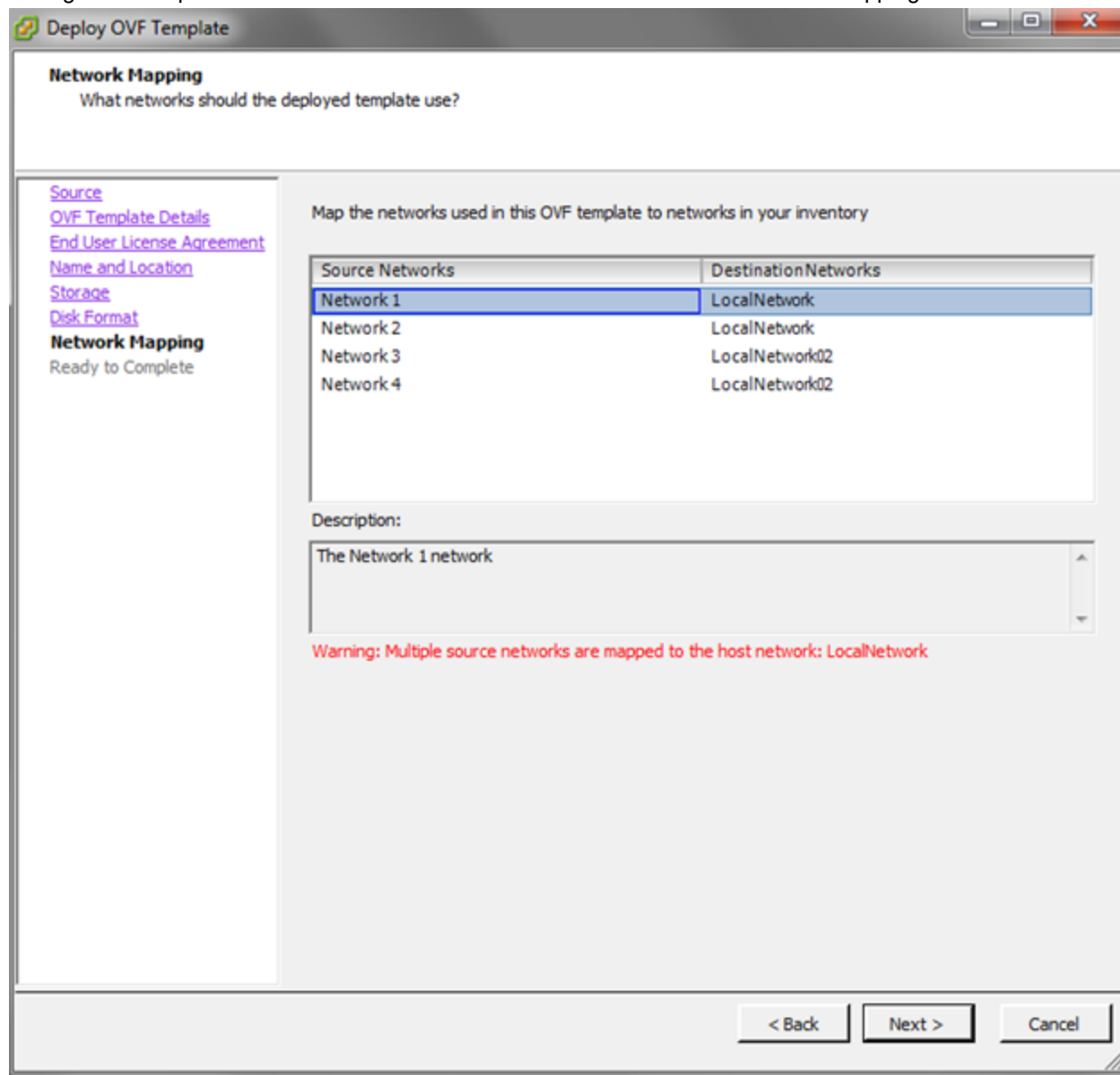
Datastore:

Available space (GB):

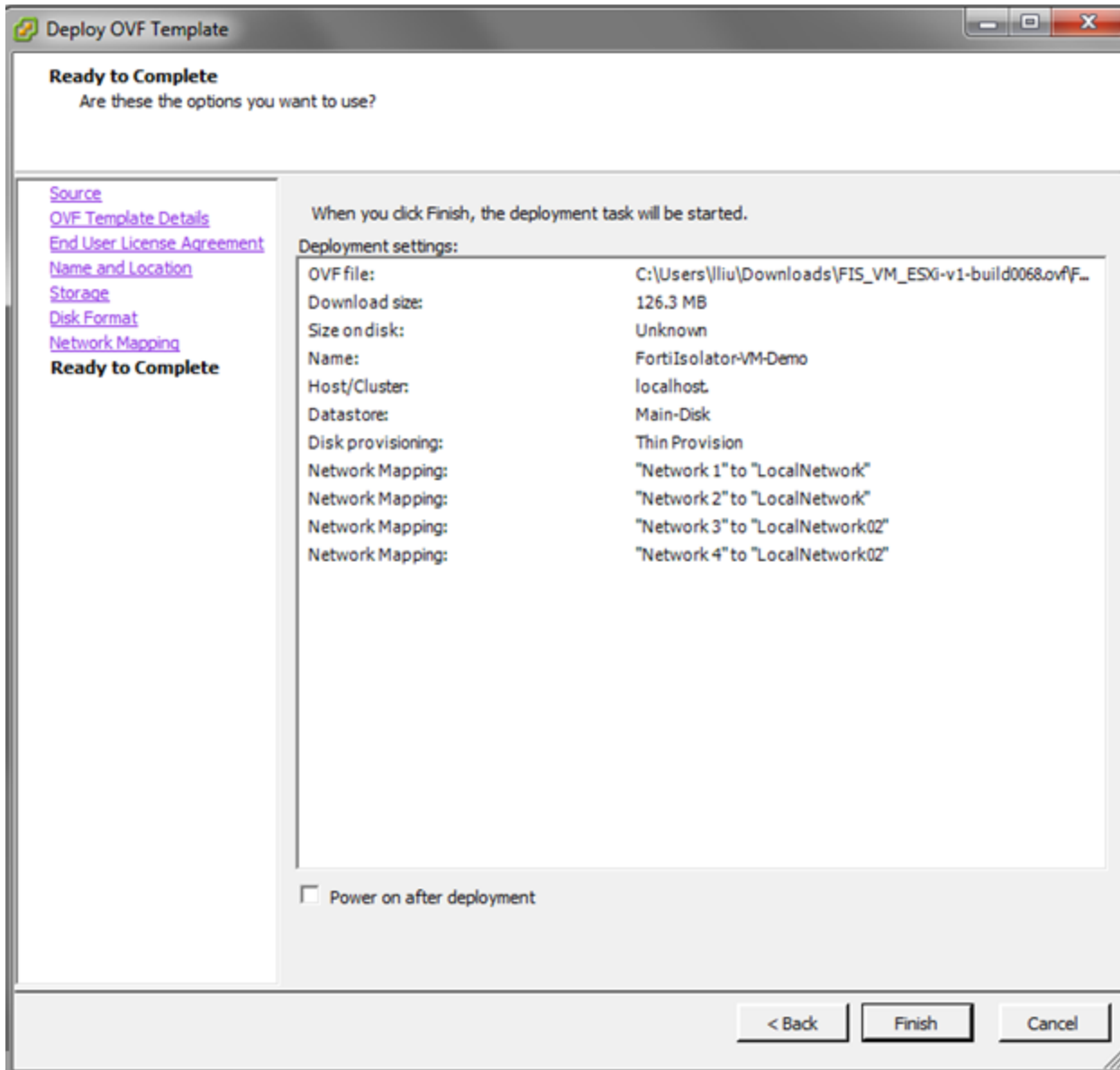
☒ Thick Provision Lazy Zeroed
☐ Thick Provision Eager Zeroed
☐ Thin Provision

< Back Next > Cancel

9. Configure the required network interfaces. Add four network interfaces for Network Mapping.



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

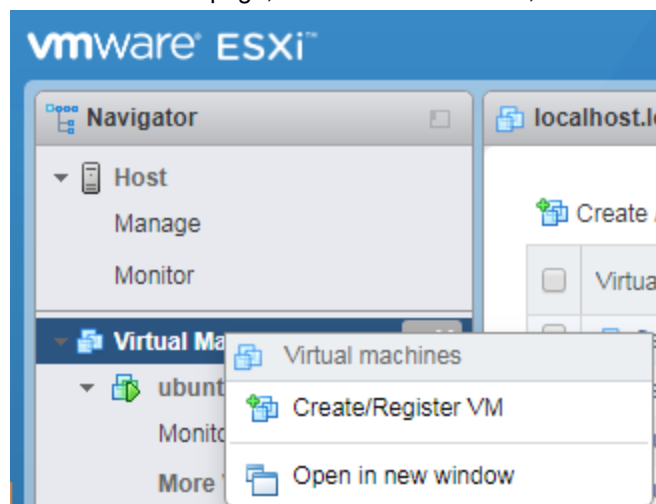
Use this procedure to install Fortisolator VM for VMware ESXi.

Prerequisites

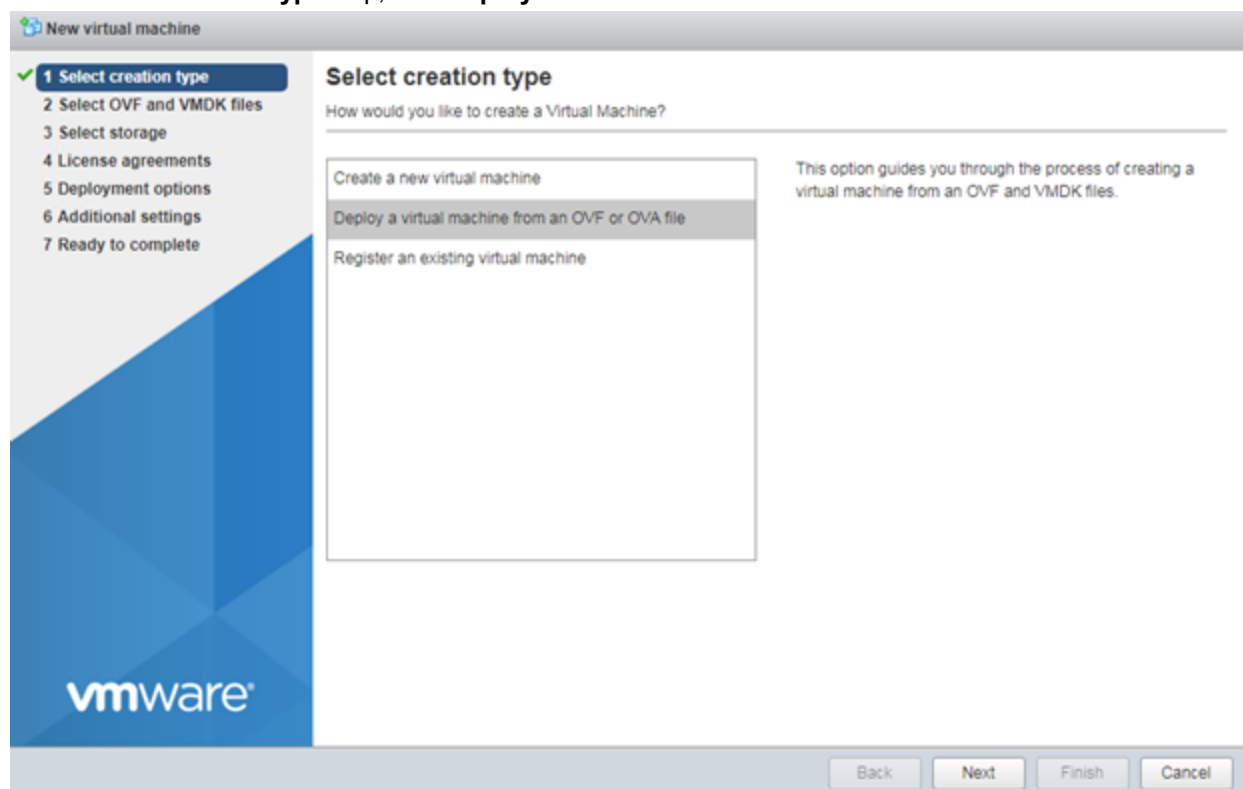
- Install VMware vSphere Client.
- Ensure that your system has one of the following combinations of hard disks and network adapters to support ESXi 6.5:
 - Two SCSI hard disks and three VMXNET 3 network adapters (this is the default)
 - Two SCSI hard disks and three E1000 network adapters

Steps

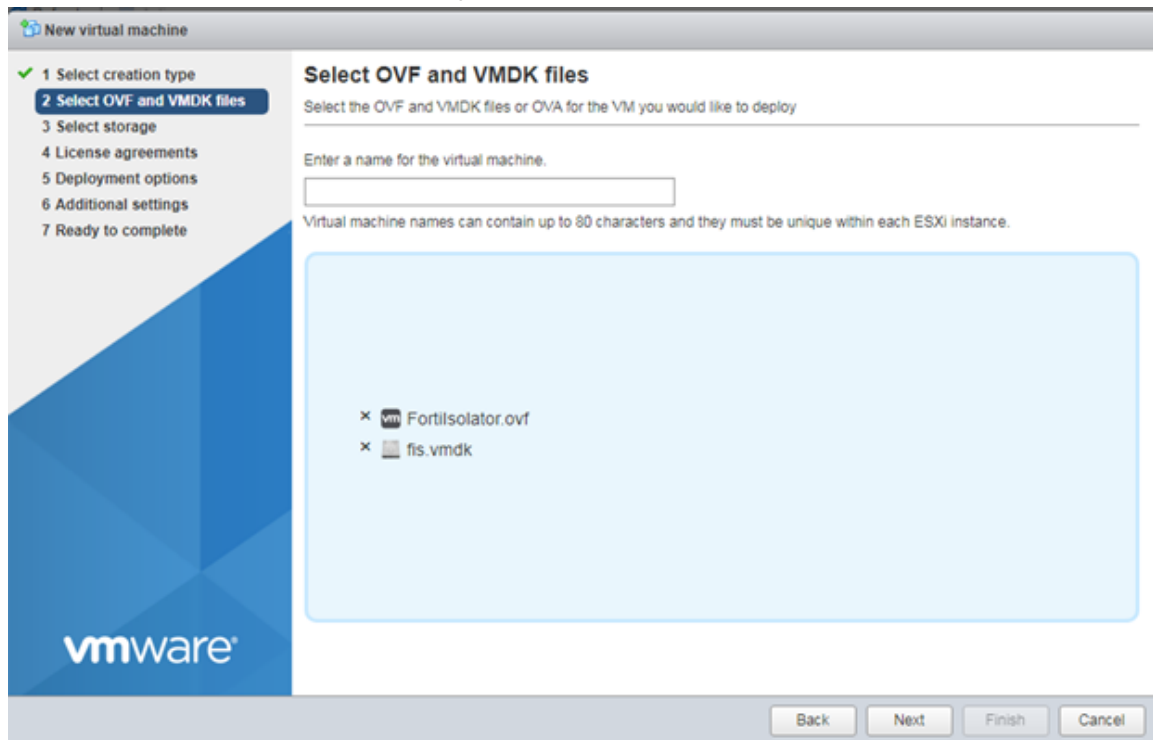
1. In the ESXi home page, click **Virtual Machine**, and then right-click and select **Create/Register VM**.



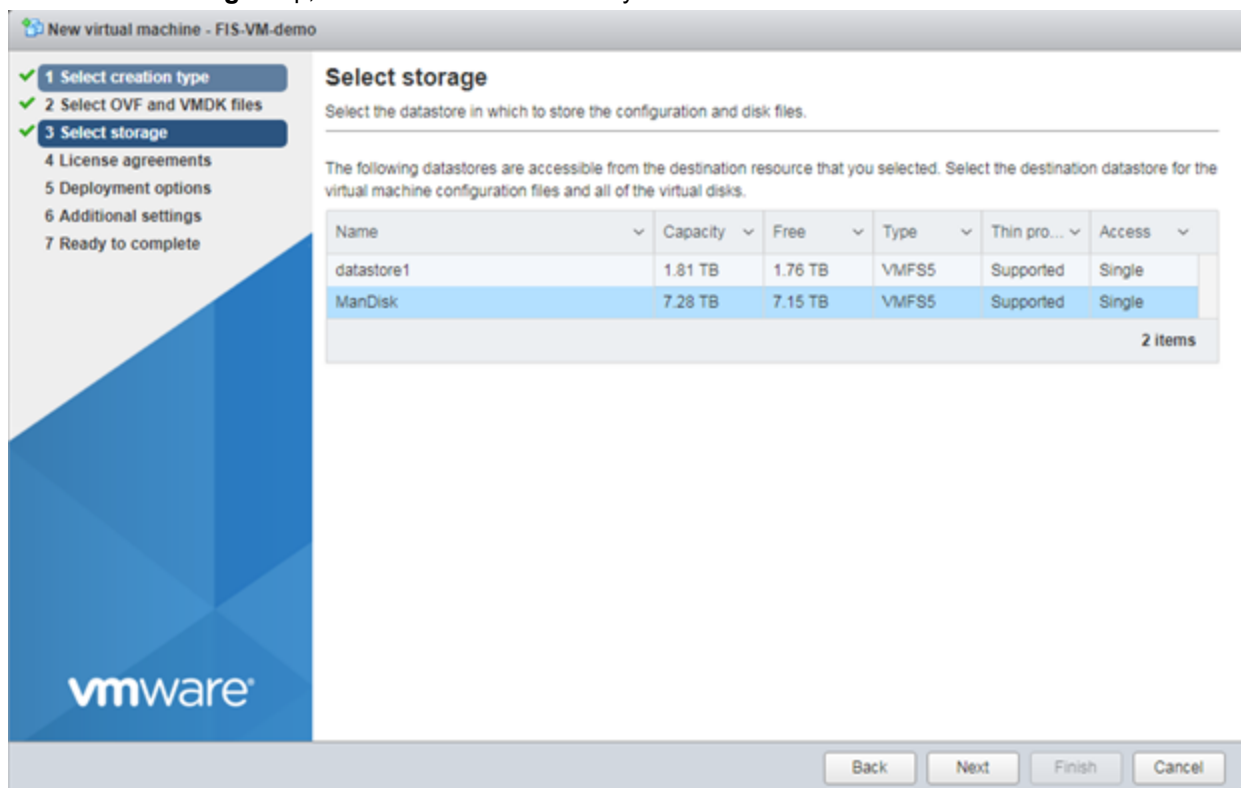
2. In the **Select creation type** step, click **Deploy a virtual machine from an OVF or OVA file**.



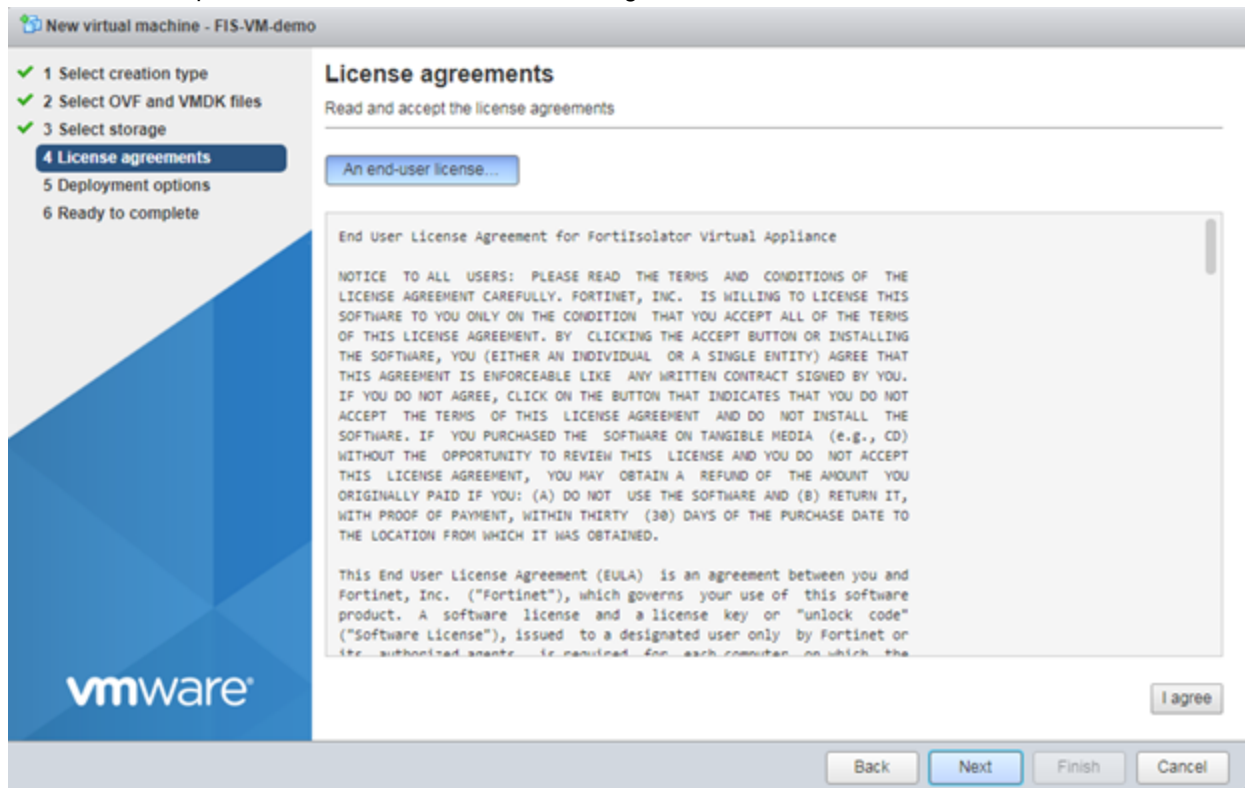
3. In the **Select OVF and VMDK files** step, select both the **Fortisolator.ovf** and **fis.vmdk** files.



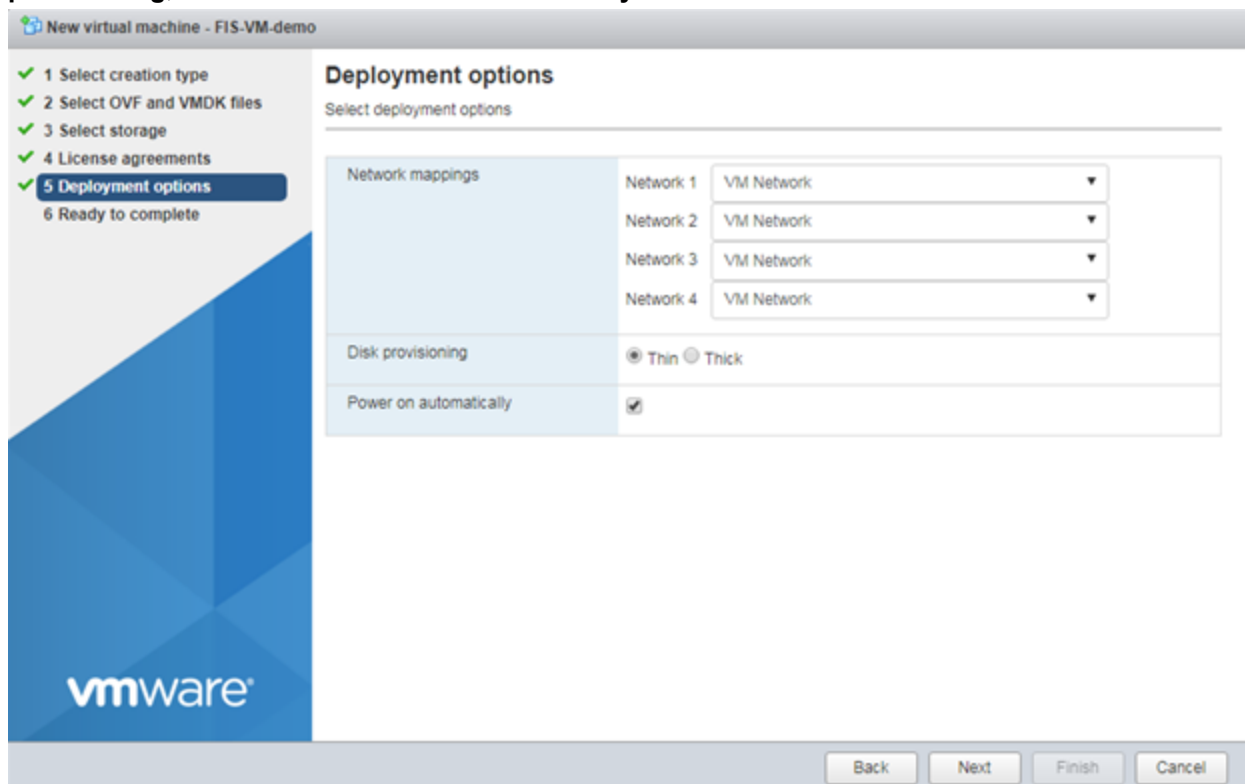
4. In the **Select storage** step, select the datastore where you want to install the Fortisolator VM.



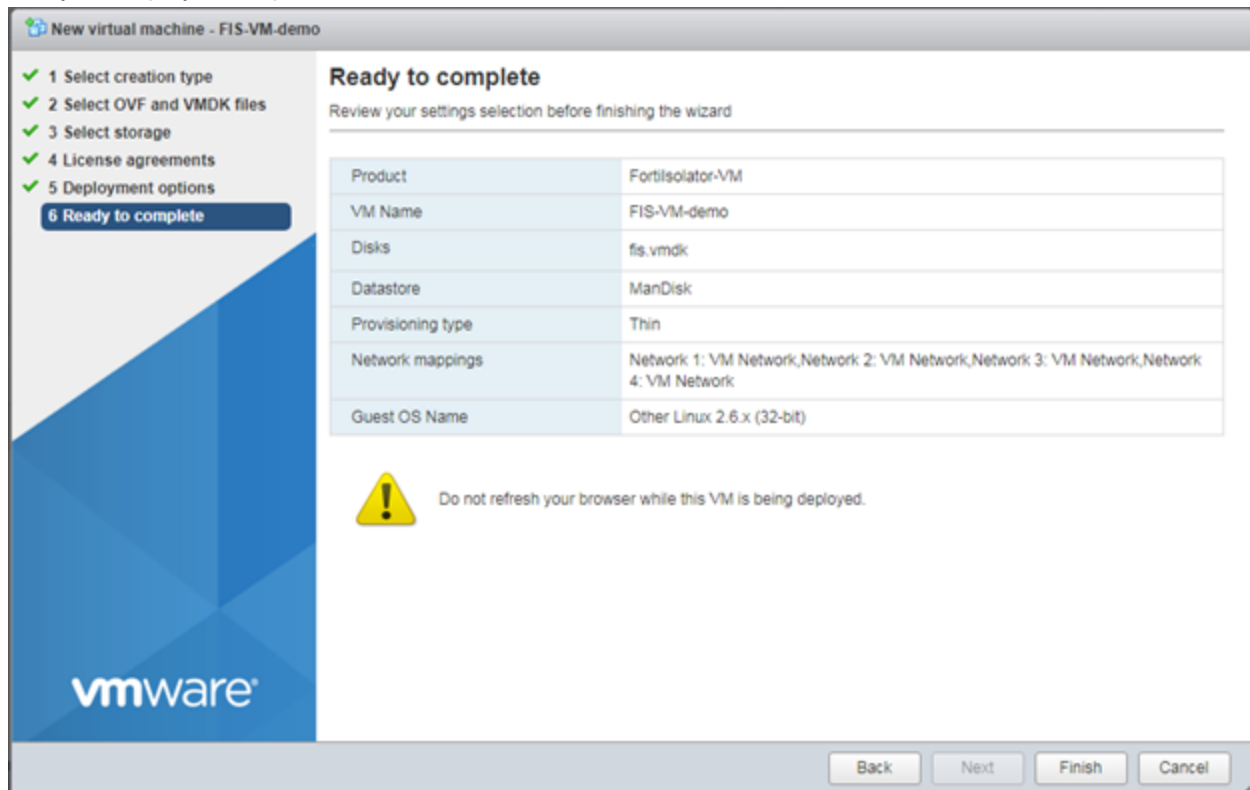
5. Review and accept the Fortisolator End User License Agreement.



6. In the **Deployment options** step, configure **Network mappings** with four network interfaces, configure **Disk provisioning**, and select the **Power on automatically** checkbox.



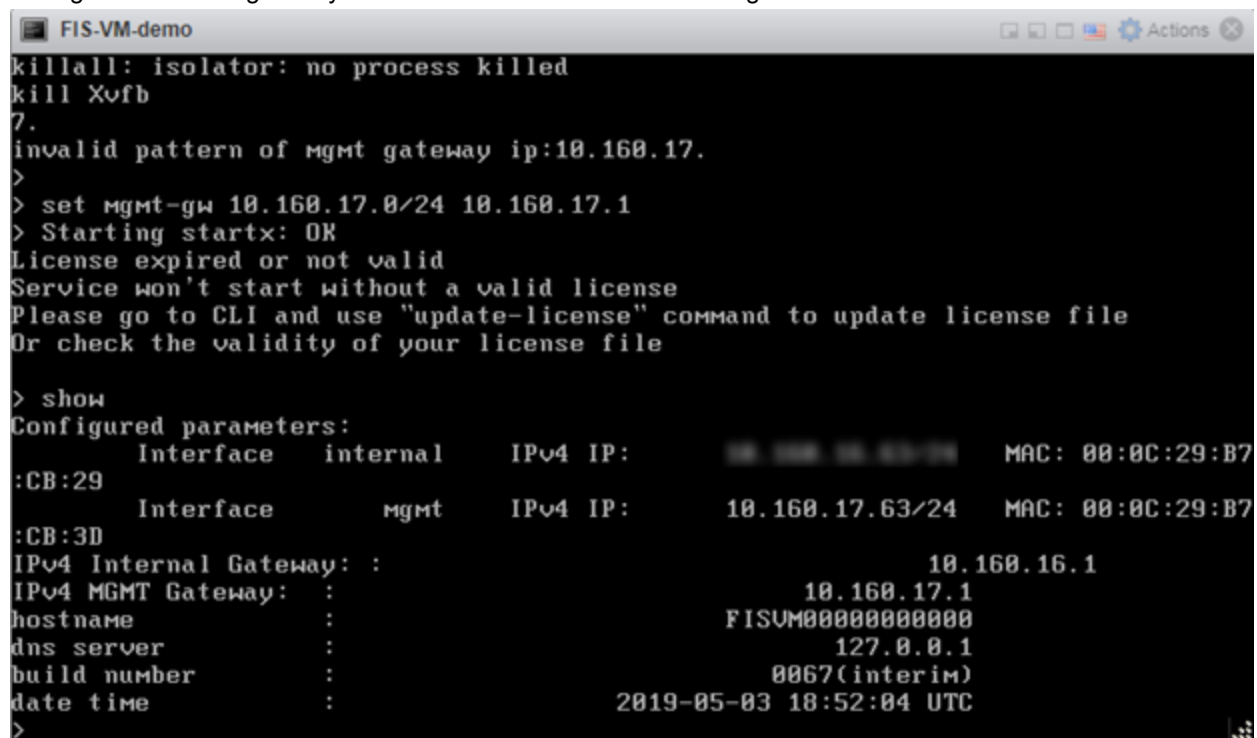
7. Verify the deployment options, and click **Finish**.



8. To start the VM, right-click the Fortisolator VM name, and select **Power > Power on**.
9. To open the Fortisolator VM console, click **Console > Open browser console**.

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

11. 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:    10.160.16.1/24    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
>

```

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

Upgrade

Fortisolator appliance upgrade

Upgrading Fortisolator firmware using a web browser

Use this procedure to upgrade a Fortisolator hardware appliance, such as the Fortisolator 1000F, using a web browser. You can use the Fortisolator UI or Fortisolator CLI to perform the upgrade.

Fortisolator UI

To perform an upgrade, go to **System > Upgrade**. In the **Upgrade by Web** section, click **Choose File**, and follow the instructions.

Fortisolator CLI

To perform an upgrade, use the `system-upgrade` command.

Upgrading Fortisolator firmware using a USB flash drive

Use this procedure to upgrade a Fortisolator hardware appliance, such as the Fortisolator 1000F, using a USB flash drive. You can use the Fortisolator UI or Fortisolator CLI to perform the upgrade.

Fortisolator UI

To perform an upgrade, go to **System > Upgrade**. In the **Upgrade by USB** section, select **Click here**, and follow the instructions.

Fortisolator CLI

To perform an upgrade, use the `system-upgrade` command.

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](#).

Configuring the console

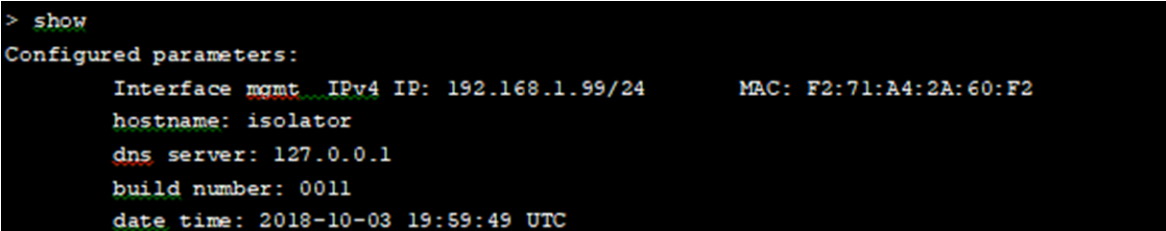
After the Fortisolator starts up, use the default console to complete initial interface configuration. By default, the management interface on Fortisolator (port3 on a VM installation) is set to 192.168.1.99.

The examples in this section are based on Fortisolator VM. The process is similar for other Fortisolator appliances, but interface settings can vary depending on the Fortisolator model.

Finding the current settings

To find the current settings on Fortisolator, type the `show` command in the Fortisolator CLI.

The following image shows an example of results from the `show` command:



```
> show
Configured parameters:
  Interface mgmt IPv4 IP: 192.168.1.99/24      MAC: F2:71:A4:2A:60:F2
  hostname: isolator
  dns server: 127.0.0.1
  build number: 0011
  date time: 2018-10-03 19:59:49 UTC
```

Setting the management IP address

To set the management IP address, type `set mgmt-ip <ip_address>/<subnet_mask>`. For example:

```
> set mgmt-ip 192.168.1.214/24
```

Setting the management gateway address

To set the management gateway, type `set mgmt-gw <subnet>/<gateway>`. For example:

```
> set mgmt-ip 0.0.0.0/0 192.168.1.254
```

All console commands

The following image shows the full list of console commands:

```

COM1 - Tera Term VT
File Edit Setup Control Window Help
>
> help
FortiIsolator 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 Fortisolator
system-upgrade       Upgrade Fortisolator System Image
factory-reset        Reset configuration to defaults and delete all data
shutdown             Shutdown the Fortisolator
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

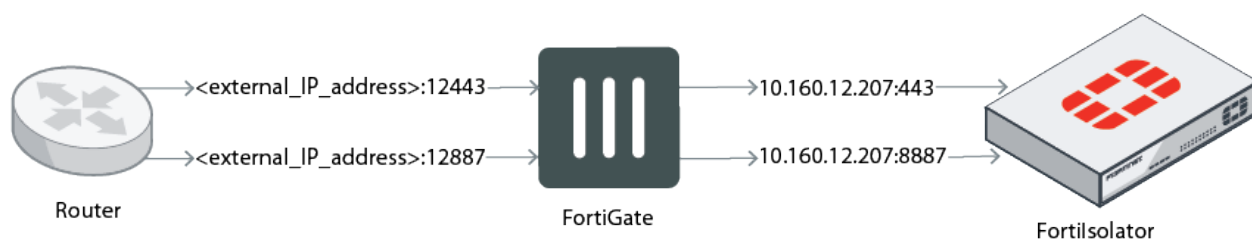
```


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

Dashboard > + Create New Edit Clone Delete Search

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

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 > Edit Virtual IP

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

Traffic Shaping Profile

VIP type IPv4

Name IP-Mapping-443

Comments Write a comment... 0/255

Color Change

Network

Interface port1

Type Static NAT

External IP address/range

Mapped IP address/range 10.160.12.207

Optional Filters

Port Forwarding

Protocol TCP UDP SCTP ICMP

External service port 12443

Map to port 443

OK Cancel

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.

FortiGate VM64 FIS-FGT-IPMapping

Edit Policy

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, DENY

Inspection Mode: Flow-based, Proxy-based

Firewall / Network Options

NAT: ☒

IP Pool Configuration: Use Outgoing Interface Address

Preserve Source Port: ☐

Protocol Options: PRX, default

Security Profiles

AntiVirus: ☐

Web Filter: ☐

DNS Filter: ☐

Application Control: ☐

IPS: ☐

Select Entries

Address: Internet Service

Search: + Create

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-8888
- IP-Mapping-Ha-443
- IP-Mapping-HA-8887

Close

OK Cancel

FortiGate VM64 FIS-FGT-IPMapping

admin

Interface Pair View By Sequence

ID	Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
1	port1->port2	all	all	always	ALL	ACCEPT	Enabled	UTM	5.26 GB	
2	p1->to->p2	all	IP-Mapping-443 IP-Mapping-8887	always	ALL	ACCEPT	Enabled	UTM	0 B	
3	port2->port1	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 : [REDACTED]
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`.

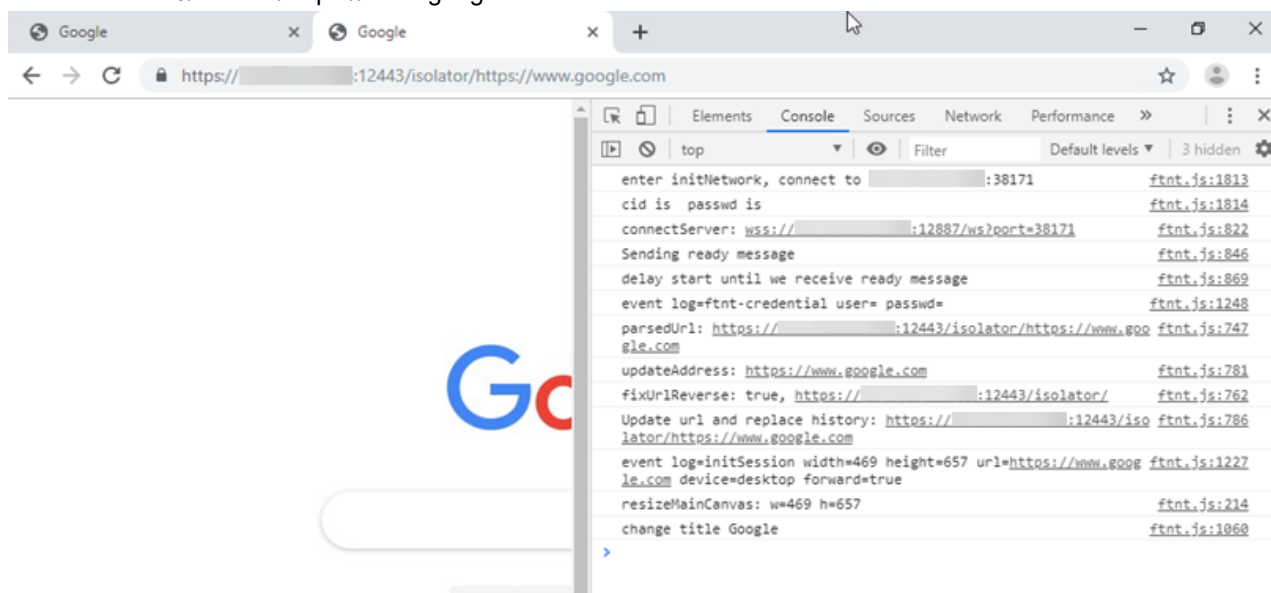
- b. To confirm the setup, type `route print`.

```
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
  [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>:12443/isolator/https://www.google.com`.

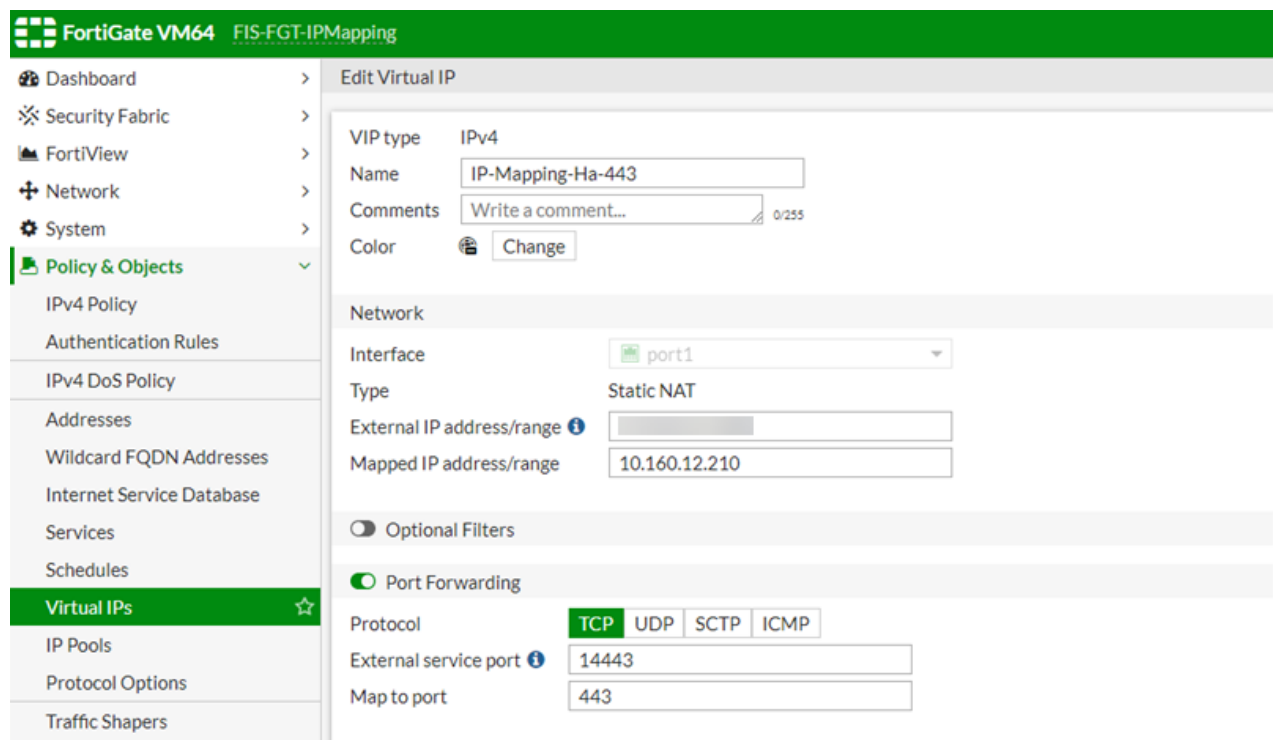
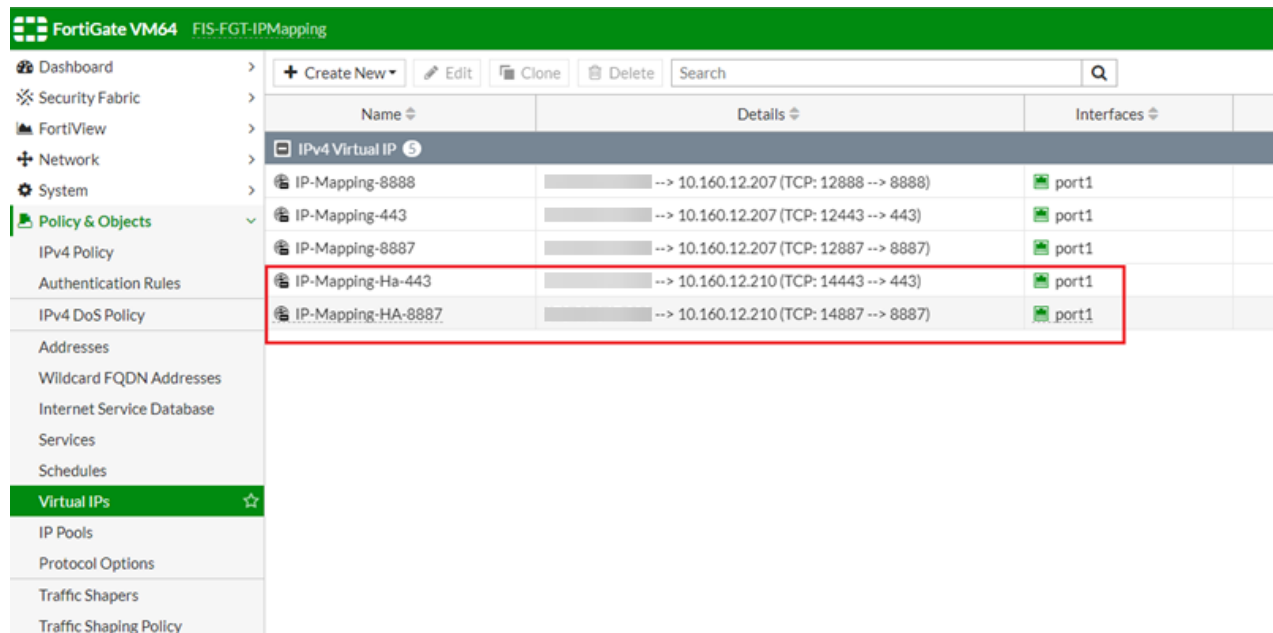


Configuring port forwarding in HA mode

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

Policy & Objects

- 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-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.

FortiGate VM64 FIS-FGT-IPMapping

Edit Policy

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

Inspection Mode: Flow-based

Firewall / Network Options

NAT: ☒ NAT

IP Pool Configuration: Use Outgoing Interface Address

Preserve Source Port: ☐

Protocol Options: PRX default

Security Profiles

AntiVirus: ☐

Web Filter: ☐

DNS Filter: ☐

Application Control: ☐

IPS: ☐

Select Entries

Address: Internet Service

Search: + Create

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

Close

OK Cancel

FortiGate VM64 FIS-FGT-IPMapping

+ Create New Edit Delete Policy Lookup Search

ID	Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles
1	port1 -> port2	all	IP-Mapping-Ha-443 IP-Mapping-HA-8887	always	ALL	ACCEPT	Enabled	
2	p1->to->p2	all	IP-Mapping-Ha-443 IP-Mapping-HA-8887	always	ALL	ACCEPT	Enabled	
3	port2 -> port1	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 [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
```

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

```
> set fis-ipmap-vip 14443 14887 [REDACTED]
> 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 23:05:47 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> 10.160.12.207 12443 12887`

```

> set fis-ipmap-ha 10 [REDACTED] 10.160.12.207 12443 12887
> 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 23:54:44 UTC
ip mapping         :      [REDACTED]
mapping for port 443:      12443
mapping for port 8887:      12887
ip mapping (VIP)    :      [REDACTED]
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`.

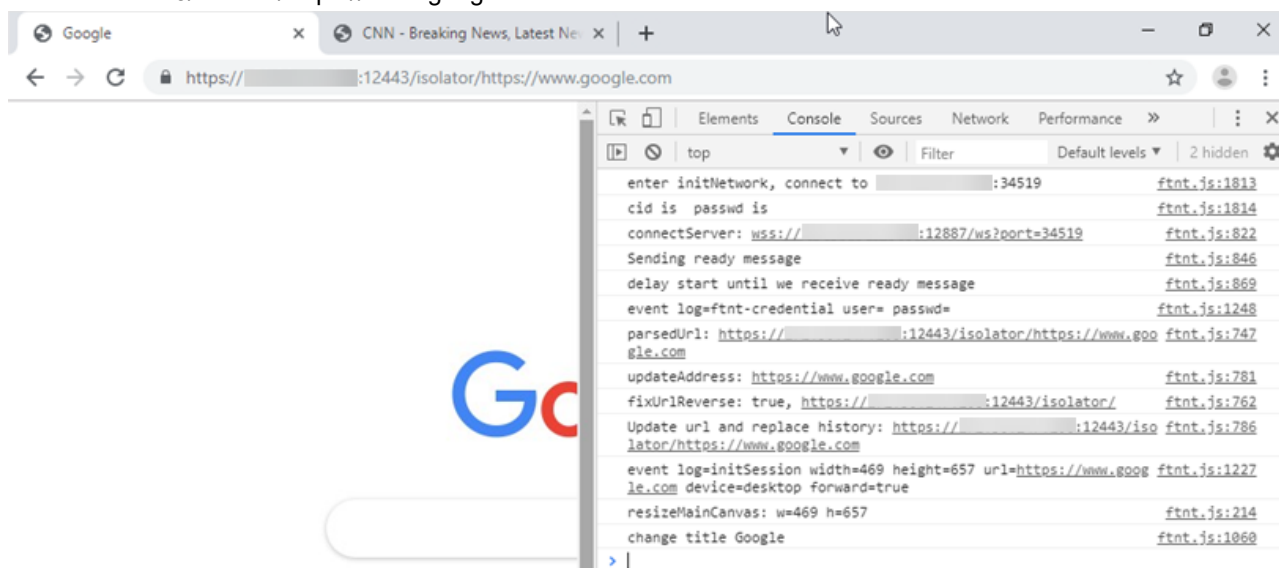
- b. To confirm the setup, type `route print`.

```
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
[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>:14443/isolator/https://www.google.com`.



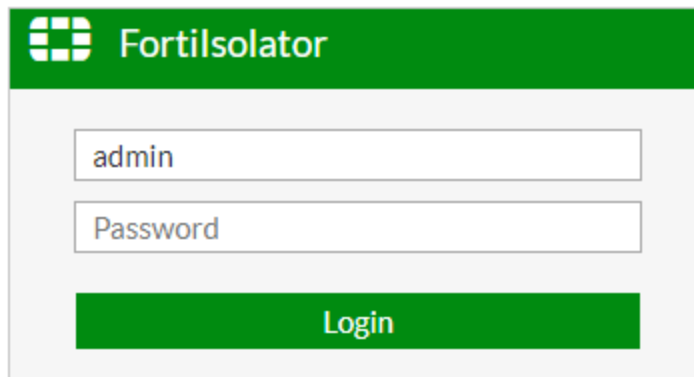
Configuration

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.



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 adminster account

A guest adminster 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 navigation bar is red with the Fortisolator logo and 'VM' text. A user dropdown menu shows 'admin'. The left sidebar contains a search bar and a list of navigation items: Dashboard, Network, System (highlighted with a green checkmark), Administrators (highlighted in green), HA, Login Disclaimer, Upgrade, Users, Policies and Profiles, and Log. The main content area is titled 'Edit Administrator'. It contains three input fields: 'Administrator:' with the value 'guest', 'Password:', and 'Confirm Password:'. At the bottom right of the form is a green 'OK' button.

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

Configuring time settings

Use this procedure to configure time settings for Fortisolator.

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**.

Configuring network interface settings

Steps

1. From the administration portal, go to **Network > Interfaces**.
2. From the table, select the desired interface to edit and click **Edit**.
3. To change the interface status, set the **Interface Status** field to one of the following options:
 - To turn on the interface, click **Link Up**.
 - To turn off the interface, click **Link Down**.
4. To change the IP address of the interface, enter an IP address and netmask in the **IPv4** field.
5. Click **OK**.

Configuring DNS settings

Steps

1. In the Fortisolator UI, go to **Network > System DNS**.
2. Type the IP address of the **Primary DNS Server**.
3. Type the IP address of the **Secondary DNS Server**.
4. Click **OK**.

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**.

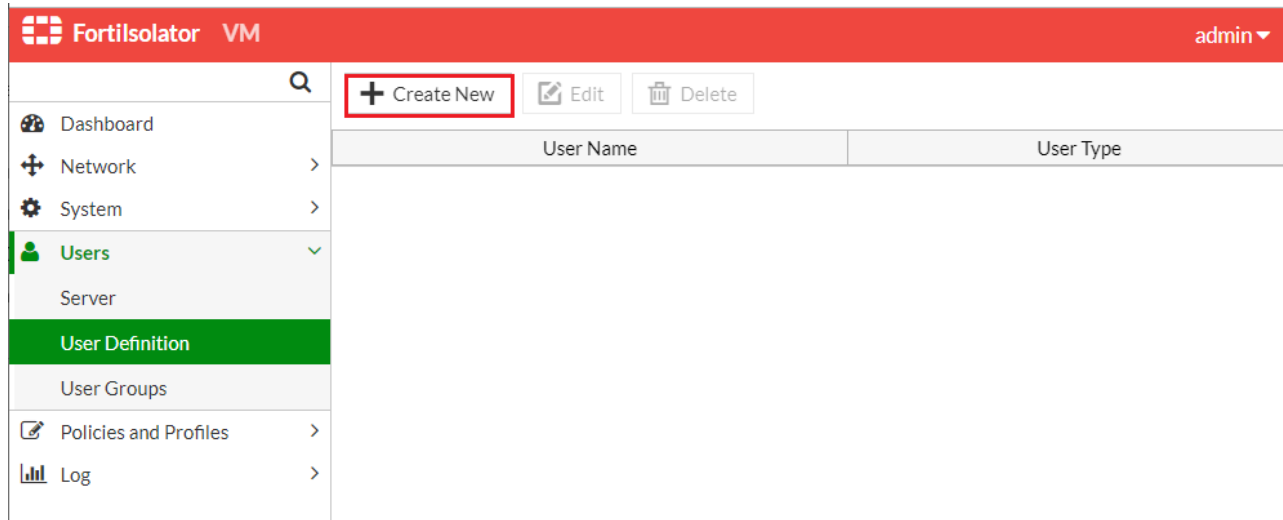
Configuring end user accounts

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.

Creating local user accounts

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.



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 user groups

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

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**.

The screenshot shows the FortiSOLATOR administration portal. On the left is a sidebar menu with icons and labels: Dashboard, Network, System, Users (highlighted with a green checkmark), Server, User Definition, User Groups (highlighted in green), Policies and Profiles, and Log. The main content area is titled 'Create New Group'. It contains three input fields: 'Group Name' with the value 'group1', 'Group Type' with the value 'Local', and 'Policy Name' with a dropdown menu showing 'Isolator_policy'. At the bottom right of the form is a green 'OK' button.

3. To add a user to a group, go to **Users > User Definition**. Select the user you want to add to a group and click **Edit**.

The screenshot shows the FortiSOLATOR administration portal. On the left is a sidebar menu with icons and labels: Dashboard, Network, System, Users (highlighted with a green checkmark), Server, User Definition (highlighted in green), User Groups, Policies and Profiles, and Log. The main content area is titled 'Create New Local User'. It contains several input fields: 'User Name' with the value 'user1', 'User Email' with the value 'user@fortinet.com', 'Password' and 'Confirm Password' both masked with dots, 'User Type' with the value 'Local', 'Groups' with a checked checkbox and the value 'group1', and 'Policy Name' with a dropdown menu showing 'Isolator_policy'. At the bottom right of the form is a green 'OK' button.

4. In the **Groups** section, select the box for the group you want to add the user to.

Setting up single sign-on for local users

Steps

1. Open a browser window and navigate to the Administration Portal page.
2. Go to **Users > Server > Create New**.
3. Select **Agent Server** from the **Server Type** dropdown menu and click **OK**.

The screenshot shows the Fortisolator VM Administration Portal. The top bar is red with the Fortisolator logo and 'VM' text, and a user dropdown 'admin'. The left sidebar has a search icon and a list of menu items: Dashboard, Network, System, Users (highlighted), Server (highlighted), User Definition, User Groups, Policies and Profiles, and Log. The main content area is titled 'Create New Server : Step 2' and contains a form with the following fields:

Id	<input type="text"/>
Enable	<input type="checkbox"/>
IP address	<input type="text"/>
Port	<input type="text"/>
Password	<input type="password"/>
Confirm Password	<input type="password"/>
Server Type	Agent Server

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

4. Enter a unique ID number between 0 and 4. (You can create a maximum of 5 servers.)
5. If you would like to enable single sign-on for this server now, check the **Enable** box. (You can always enable later by editing the server settings.)
6. Enter the server IP address and LDAP listening port.
7. Create a password and click **OK**.

Configuring policies and profiles

Creating Isolator browsing profile

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

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.

The screenshot shows the Fortisolator VM administration interface. The top bar is red with the Fortisolator logo and 'VM' text. The right side of the top bar shows 'admin' with a dropdown arrow. The left sidebar is white with a search icon and a list of navigation items: Dashboard, Network, System, Users, Policies and Profiles (highlighted in green), Profiles, Policies, Default Policy, and Log. The main content area is titled 'Create New Profile : Step 2' and contains a form with the following fields:

Isolator Profile Name	Isolator_profile
File Size for Downloading(MB)	100
File Size for Uploading(MB)	100
Limit of view only	<input checked="" type="checkbox"/>
Right for scanning files by vscanner	<input checked="" type="checkbox"/>
Image Quality	normal
Video Frame Rate	normal
Right for doc rewrite when scanning file	<input type="checkbox"/>

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

- Type in the maximum file size in megabytes for uploading and downloading files.
- 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.
- By selecting the **Right for scanning files by vscanner** box, you allow files to be scanned by Vscanner
- You can increase or decrease bandwidth usage by selecting the desired **Image Quality** and **Video Frame Rate** from the corresponding drop-down menus.
- By selecting the **Right for doc rewrite when scanning file** box, you allow rewriting of documents during file scanning such that embedded links in the file are rendered inactive.

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 webpages 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.

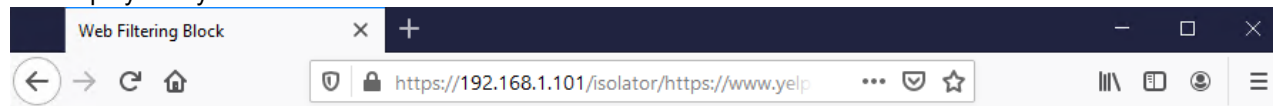
Steps

- From the administration portal, go to **Policies and Profiles > Profiles** and click **Create New**.
- 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.
- Enter a Web Filter Profile Name.

- 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:

- 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.
 - 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.
 - Allow:** End user has full access of the website. By default, all web categories are allowed.
- 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.
 - To finish creating the Web Filter Profile, click **Submit**.
 - To verify that the web filter is working, try browsing to one of the blocked web pages. You should see the following text displayed in your browser:



The URL is blocked by Fortinet Isolator Web Filtering

Your Isolator administrator has blocked the URL

Creating a 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. See the next section [Applying Isolator profile and Web Filter profile settings on page 62](#)

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 to be used in the policy.
3. Click **OK** to finish.

The screenshot shows the FortiSolator VM administration portal. The top navigation bar is red with the FortiSolator logo and 'VM' text on the left, and 'admin' with a dropdown arrow on the right. A search icon is in the center. Below the navigation bar is a sidebar menu with icons and labels: Dashboard, Network, System, Users, Policies and Profiles (highlighted with a green checkmark), Profiles, Policies (highlighted with a green bar), Default Policy, and Log. The main content area is titled 'Create New Policy' and contains three input fields: 'Policy Name' with the value 'Isolator_policy', 'Isolator Profile Name' with a dropdown menu showing 'Isolator_profile', and 'WebFilter Profile Name' with a dropdown menu showing 'Webfilter_profile'. At the bottom right of the form is a green 'OK' button.

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

Steps

1. From the administration portal, go to **Policies and Profiles > Default Policy**.
2. From the **Default Isolator Profile Name** drop-down menu, select the Isolator profile you wish to apply.
3. From the **Default WebFilter Profile Name** drop-down menu, select the Web Filter profile you wish to apply.

- Click **OK** to finish.

FortiSolator VM admin

Search

- Dashboard
- Network
- System
- Users
- Policies and Profiles**
 - Profiles
 - Policies
 - Default Policy**
- Log

Default Policy

Default Isolator Profile Name: <None>

Default WebFilter Profile Name: <None>

OK

Applying profile settings to local user account

Steps

- 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.
- Go to **Users > User Definition**. Select the user you wish to apply the profile settings to and click **Edit**.
- From the **Policy Name** drop-down menu, select the policy you wish to apply to the local user
- Click **OK** to finish.

FortiSolator VM admin

Search

- Dashboard
- Network
- System
- Users**
 - Server
 - User Definition**
 - User Groups
- Policies and Profiles
- Log

Create New Local User

User Name: user1

User Email:

Password:

Confirm Password:

User Type: Local

Groups: group1

Policy Name: Isolator_policy

OK

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.

The screenshot shows the Fortisolator VM administration interface. The top bar is red with the Fortisolator logo and 'VM' text, and a user dropdown 'admin'. The left sidebar contains a navigation menu with items: Dashboard, Network, System, Users (highlighted), Server, User Definition, User Groups (highlighted), Policies and Profiles, and Log. The main content area is titled 'Edit Group' and contains three input fields: 'Group Name' with the value 'group1', 'Group Type' with the value 'Local', and 'Policy Name' with a dropdown menu showing 'Isolator_policy'. At the bottom right of the form is a green 'OK' button.

Configuring log settings

The log is the place where the administrator can keep track of all end user activity in Fortisolator. The log messages show what is happening in the back end associated with all end user activity.

Navigating the log interface

The following image is an example of what the log interface looks like:

The screenshot shows the Fortisolator VM administration interface with the 'Log' section selected in the sidebar. The top bar is red with the Fortisolator logo and 'VM' text. The left sidebar contains a navigation menu with items: Dashboard, Network, System, Users, Policies and Profiles, Log (highlighted), and Log Settings. The main content area shows a log interface with a search bar at the top containing 'messages.cron', 'messages.django', 'messages.secure', and 'messages.user'. Below the search bar are filters for 'Date From: mm/dd/yyyy', 'To: mm/dd/yyyy', 'Application Name:', 'Type:', and 'Content:', followed by a green 'Filter' button. A green 'Clean' button is also present. Below the filters is a table with the following columns: Date, Application, Type, and Content.

Date	Application	Type	Content
2019-12-20T01:00:00	cron	Info	USER root pid 9863 cmd /sbin/logrotate -v /etc/logrotate.d/isolator_logrotate.conf
2019-12-20T00:21:33	cron	Info	crond (busybox 1.28.1) started, log level 8
2019-12-20T00:19:42	cron	Info	crond (busybox 1.28.1) started, log level 8
2019-12-20T00:14:29	cron	Info	crond (busybox 1.28.1) started, log level 8
2019-12-20T00:12:44	cron	Info	crond (busybox 1.28.1) started, log level 8
2019-12-20T00:08:39	cron	Info	crond (busybox 1.28.1) started, log level 8

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

Configuring the log server

Steps

1. From the administration portal, go to **Log > Log Settings**.
2. From the **Log Settings** window, you can back up log messages and/or send syslog messages to a remote server.

The screenshot shows the Fortisolator VM administration portal. The left sidebar contains a menu with the following items: Dashboard, Network, System, Users, Policies and Profiles, Log, and Log Settings (highlighted in green). The main content area is titled 'Log Server Configuration' and contains two sections: 'Backup Logs' and 'Log Server Settings'. The 'Backup Logs' section has a text box saying 'You can backup your current logs.' and a link 'Click here to save your log file.'. The 'Log Server Settings' section has three fields: 'Log protocol' (a dropdown menu set to 'Syslog'), 'Log Server IP Address' (a text input field), and 'Port' (a text input field). At the bottom right of the settings section is a green 'OK' button.

- a. To save your current log messages as a file, select the **Click here** link inside the **Backup Logs** section.
- b. To send syslog messages to a remote server, enter the server IP address and port number into the **Log Server Settings** section.

Configuring high availability

Fortisolator supports high availability and A-A clustering. You can deploy devices in a cluster and distribute traffic using Round Robin or Weighted Round Robin load balancing. You can use the Fortisolator UI or the Fortisolator CLI to configure high availability.

Configuring high availability in Fortisolator UI

Steps

1. From the administration portal, go to **System > HA**.
2. Fill in the desired settings and click **Apply** to finish.

Fortisolator VM admin ▾

HA Settings

⚠ Note: Apache and HA will restart after the HA settings are changed

Enable: ☒

Virtual IP:

Priority:

Cluster Settings

Group Id:

Password: Change

Allow Override: ☐

Schedule Type: round robin ▾

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

Apply

Configuring high availability in Fortisolator CLI

Steps

1. To configure high availability, use the following CLI commands:

Fortisolator High Availability CLI commands

```

ha-enabled 0/1
ha-group-id [1-255]
ha-lost-threshold [1-60]
ha-interval [1-20] in unit of seconds
ha-hello-holddown [5-300] in unit of seconds
ha-priority [0-255] where 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>

```

Fortisolator High Availability CLI commands

```
ha-password-enc <Encoded PASSWORD>
```

```
ha-interface <Interface Name> e.g. internal/external/mgmt
```

- After you enable or disable high availability, you must restart Fortisolator.

```
VT COM1 - Tera Term VT
File Edit Setup Control Window Help

Welcome to Isolator
Fortisolator login:
Welcome to Isolator
Fortisolator login: admin
Password:
> show
Configured parameters:
  Interface      internal  IPv4 IP: [REDACTED] /22  MAC: 00:90:0B:70:EC:E2
  Interface      mgmt     IPv4 IP: [REDACTED] /24  MAC: 00:90:0B:6D:A3:2F
IPv4 Internal Gateway:
hostname         : Fortisolator
dns server       :
dns server       :
build number     : 0082<interim>
date time        : 2019-07-15 12:01:16 PDT
ip mapping <VIP> :
mapping for port 443 <VIP>: 12443
mapping for port 8887 <VIP>: 12887
> show
Configured parameters:
  Interface      internal  IPv4 IP: [REDACTED] /22  MAC: 00:90:0B:70:EC:E2
  Interface      mgmt     IPv4 IP: [REDACTED] /24  MAC: 00:90:0B:6D:A3:2F
IPv4 Internal Gateway:
hostname         : Fortisolator
dns server       :
dns server       :
build number     : 0082<interim>
date time        : 2019-07-15 12:01:21 PDT
ip mapping <VIP> :
mapping for port 443 <VIP>: 12443
mapping for port 8887 <VIP>: 12887
> show ha-all
ha enabled       : Enabled
ha gid           : 30
ha lost threshold : 7
ha interval      : 7
ha holddown      : 5
ha priority      : 50
ha allow override : 0
ha schedule      : Round Robin
ha vip           : [REDACTED]
ha password      :
ha interface     : internal
> set ha-enabled
[0]Disabled
[1]Enabled
[2]Duplicated
Please choose the value<0 to 2>:0
The ha enabled is set as "Disabled"
Warning: Fortisolator will need reboot after the HA settings are changed
> █
```

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 configuration interface. The top bar is red with the Fortisolator logo and 'VM' on the left, and 'admin' with a dropdown arrow on the right. A search icon is in the top left of the main content area. The left sidebar contains a menu with the following items: Dashboard, Network, System (highlighted with a green bar and a green 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 contains a text area labeled 'Disclaimer:' with the following 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.

End user operation

Run web browsers through Fortisolator

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

- IP forwarding mode
- Proxy mode
- PAC file mode

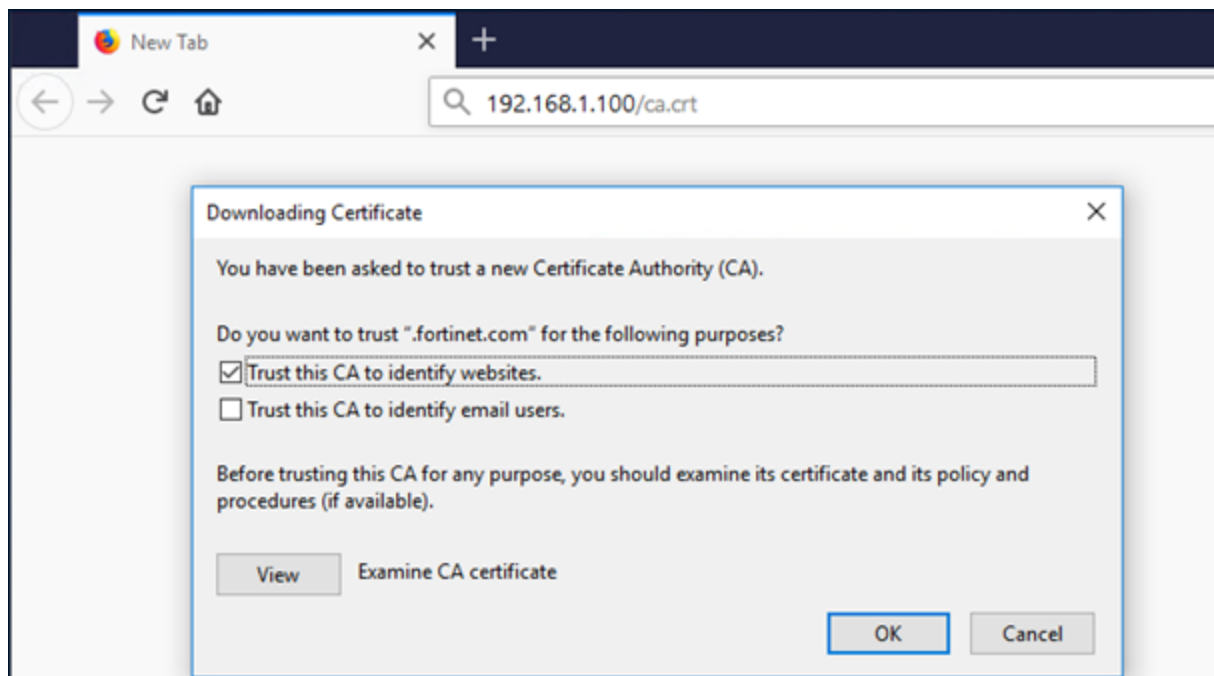
IP forwarding mode

Using IP forwarding mode with Mozilla Firefox

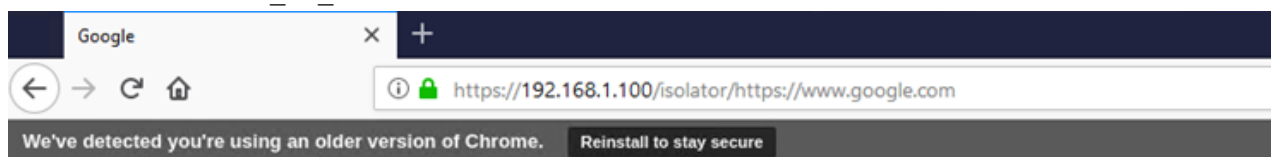
Use this procedure to configure IP forwarding mode with Mozilla Firefox.

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 7](#).
 - 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



About Store

Google

Google Search

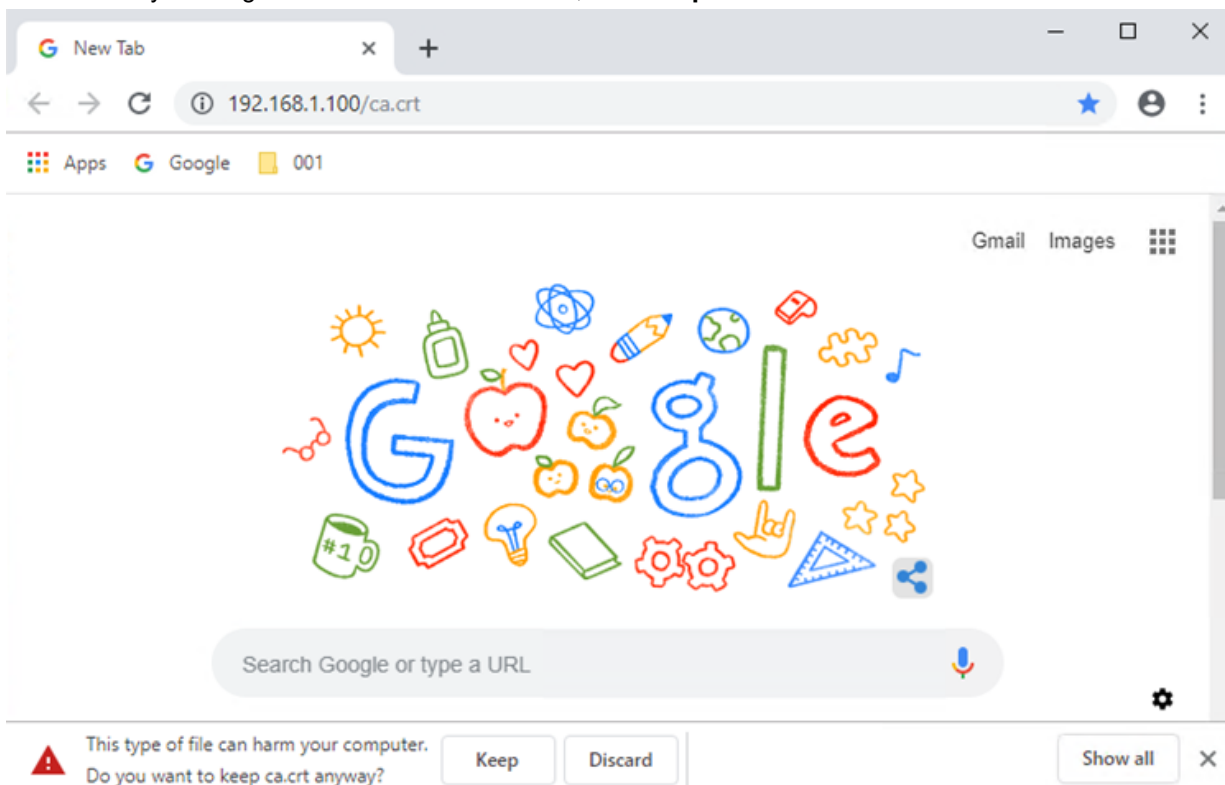
I'm Feeling Lucky

Using IP forwarding mode with Google Chrome

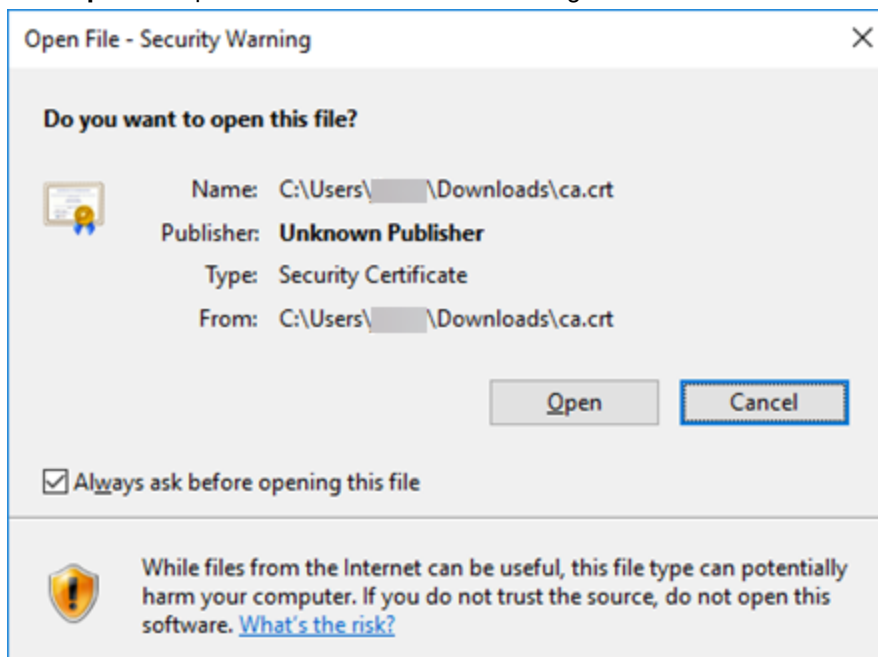
Use this procedure to configure IP forwarding mode with Google Chrome.

Steps

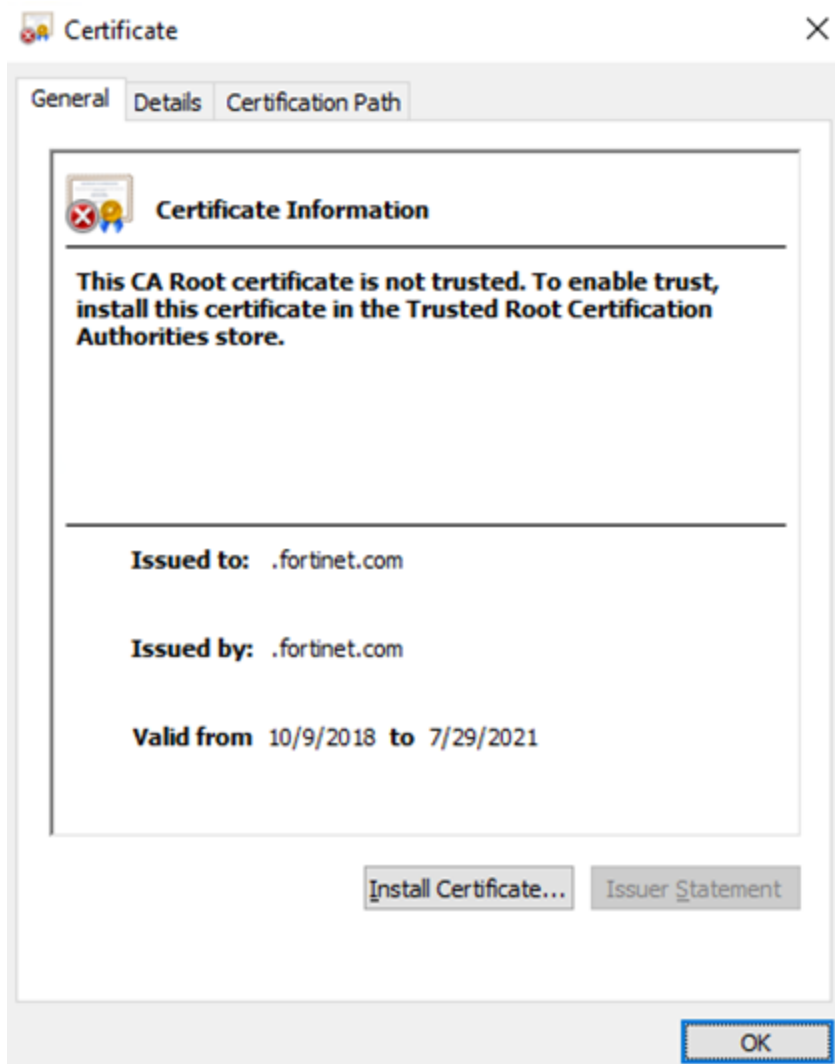
1. To download the Fortisolator certificate (ca.crt) and import it into your Google Chrome browser, follow these steps:
 - a. In the Google Chrome browser address bar, type `http://<internal_IP_address>/ca.crt` (for example, `http://192.168.1.100/ca.crt`).
 - where `<internal_IP_address>` value is the 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 7](#).
 - b. In the security warning at the bottom of the browser, click **Keep** to download the certificate.



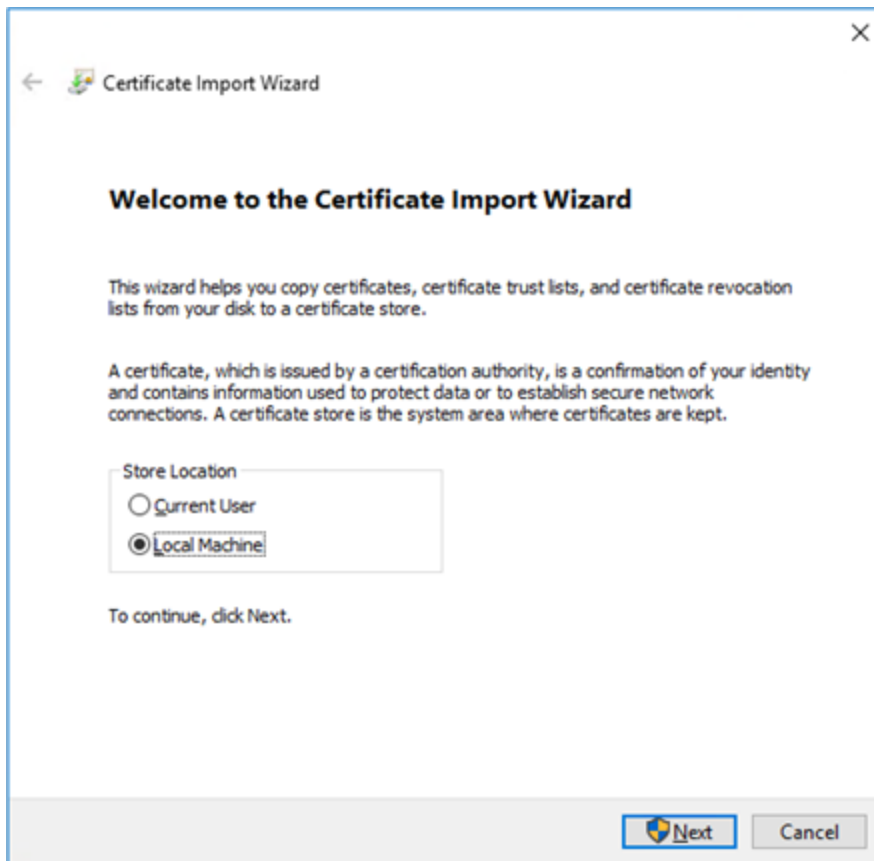
- c. Click **Open** to import the ca.crt certificate into Google Chrome.



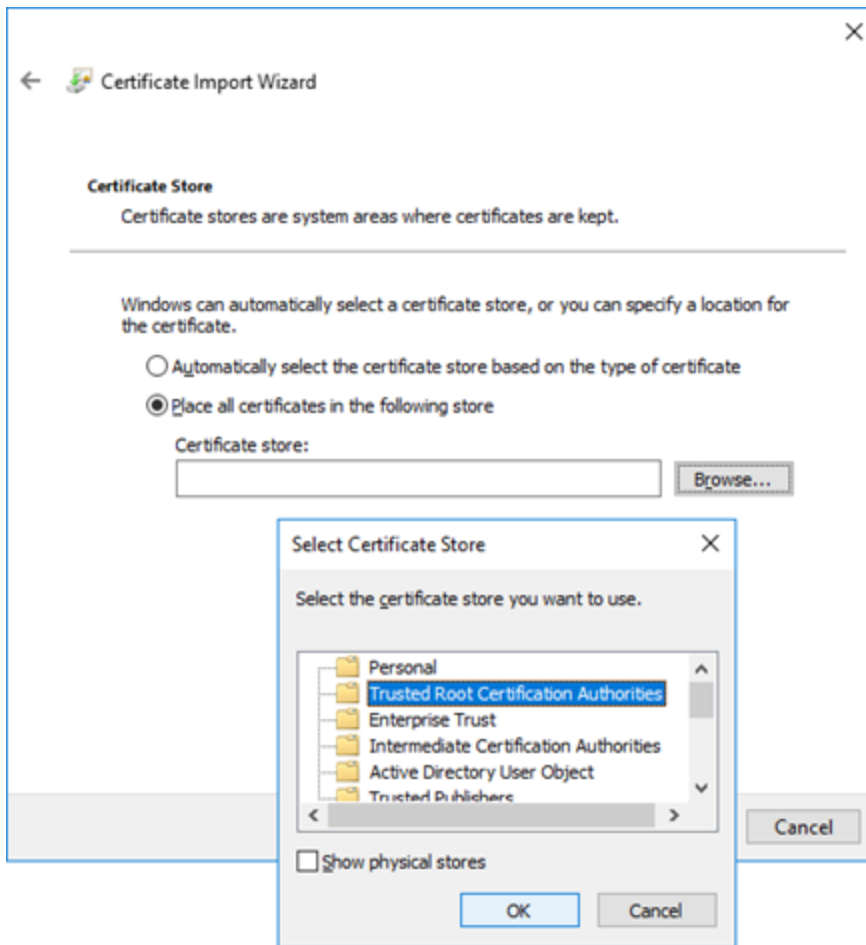
- d. Click **Install Certificate**.



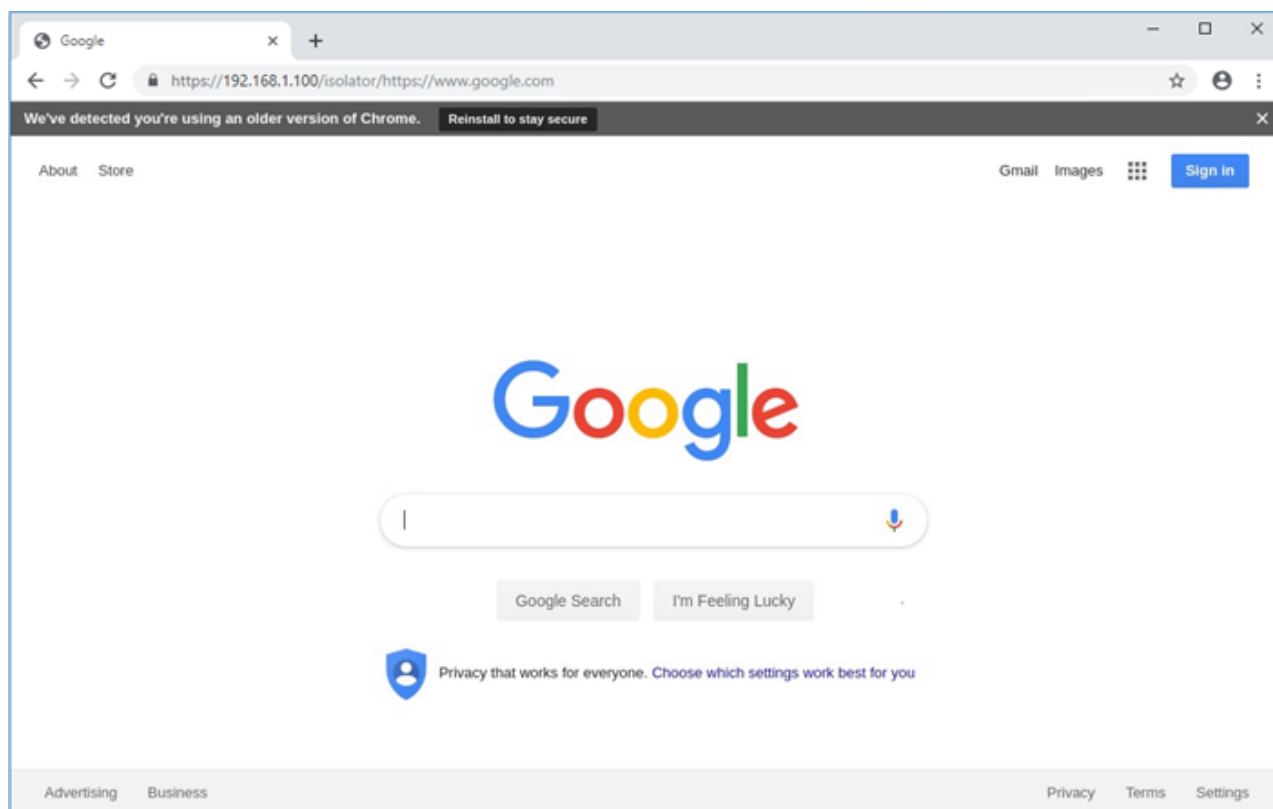
- e. Select **Local Machine**, and click **Next**.



- 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



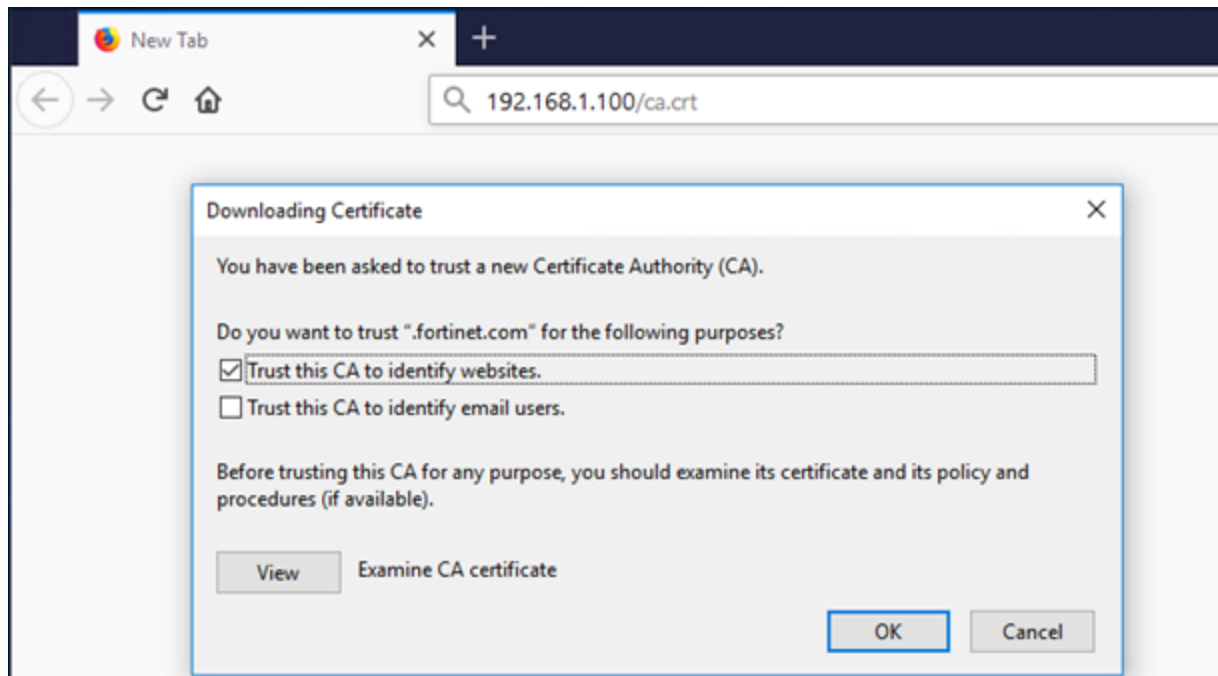
Proxy mode

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 7](#).
 - 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 7](#).
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

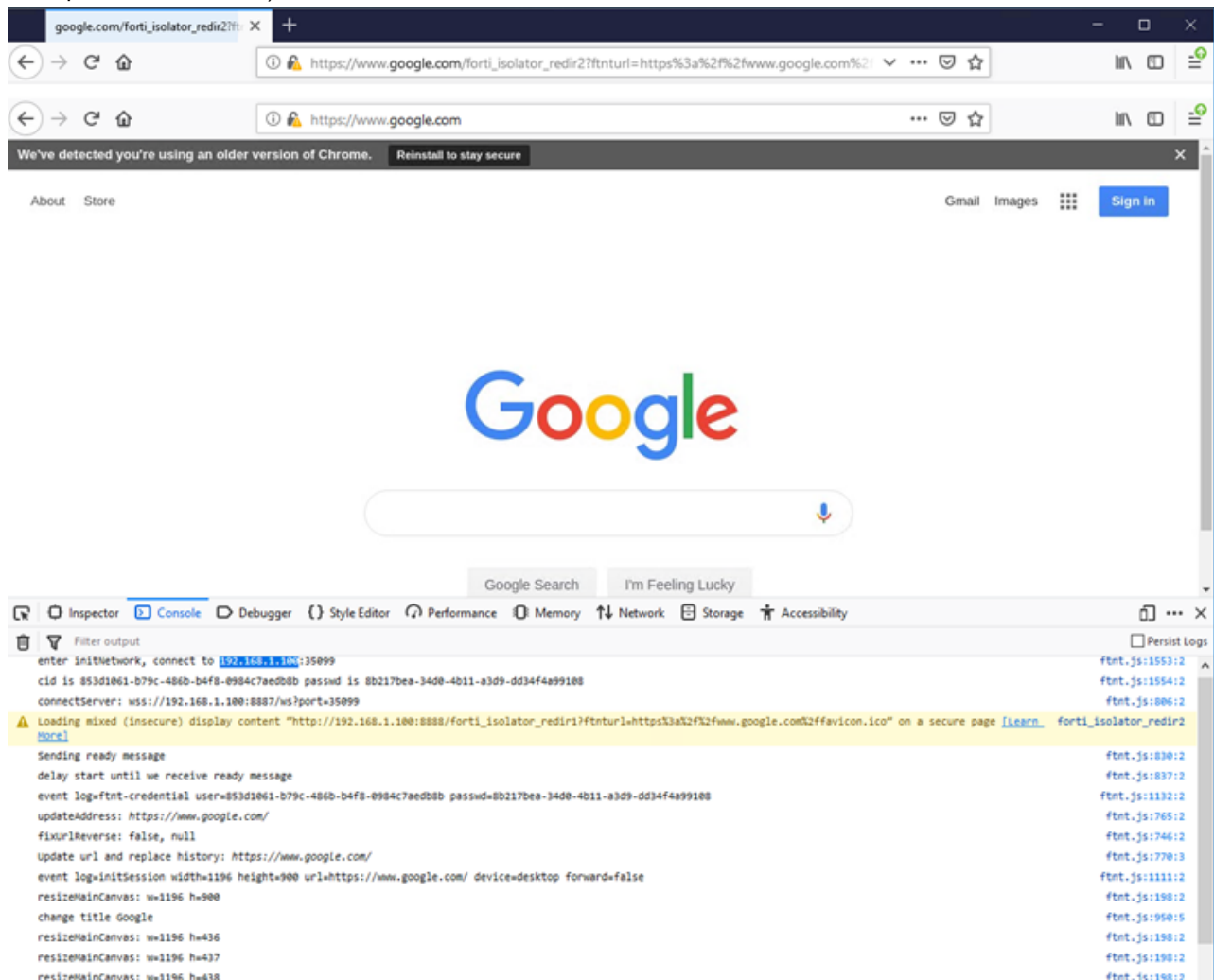
OK Cancel Help

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`).



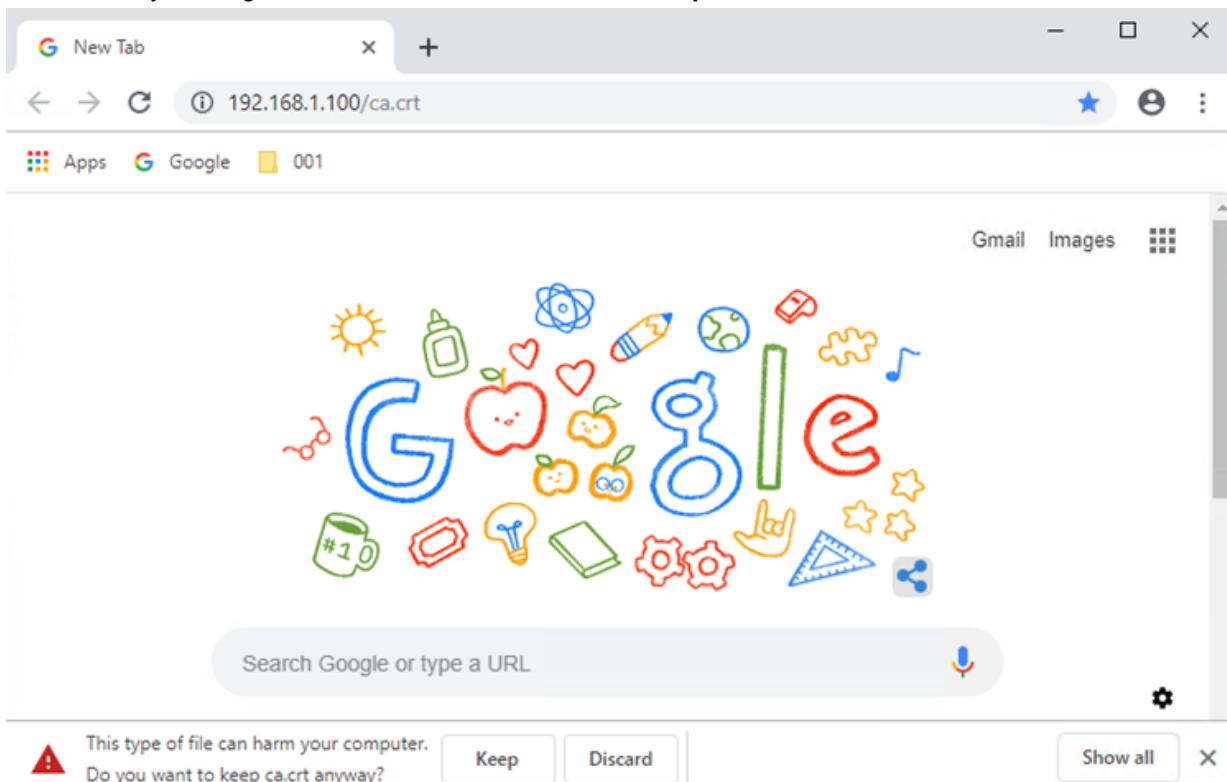
Using proxy mode with Google Chrome

Use this procedure to configure proxy mode with Google Chrome.

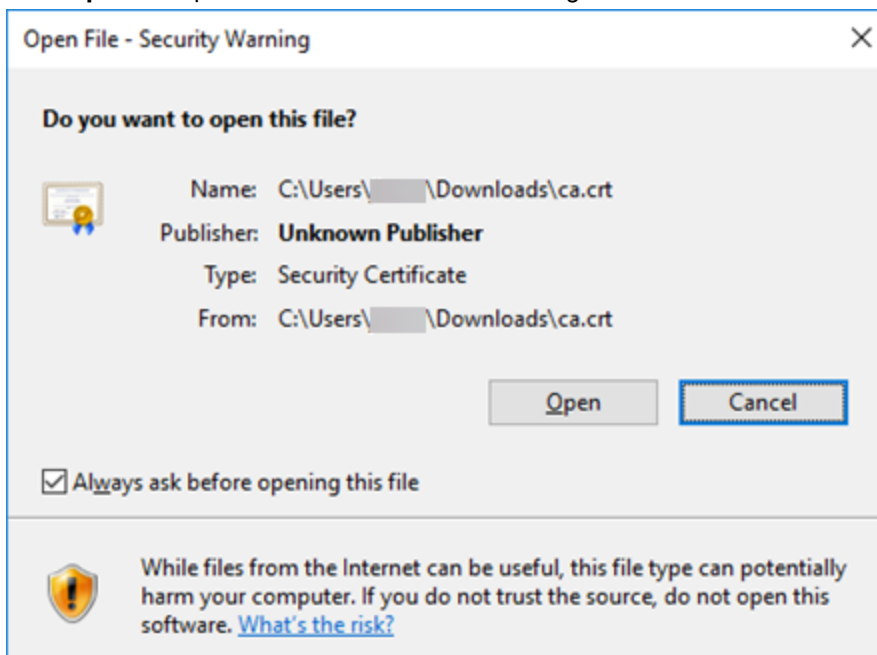
Steps

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

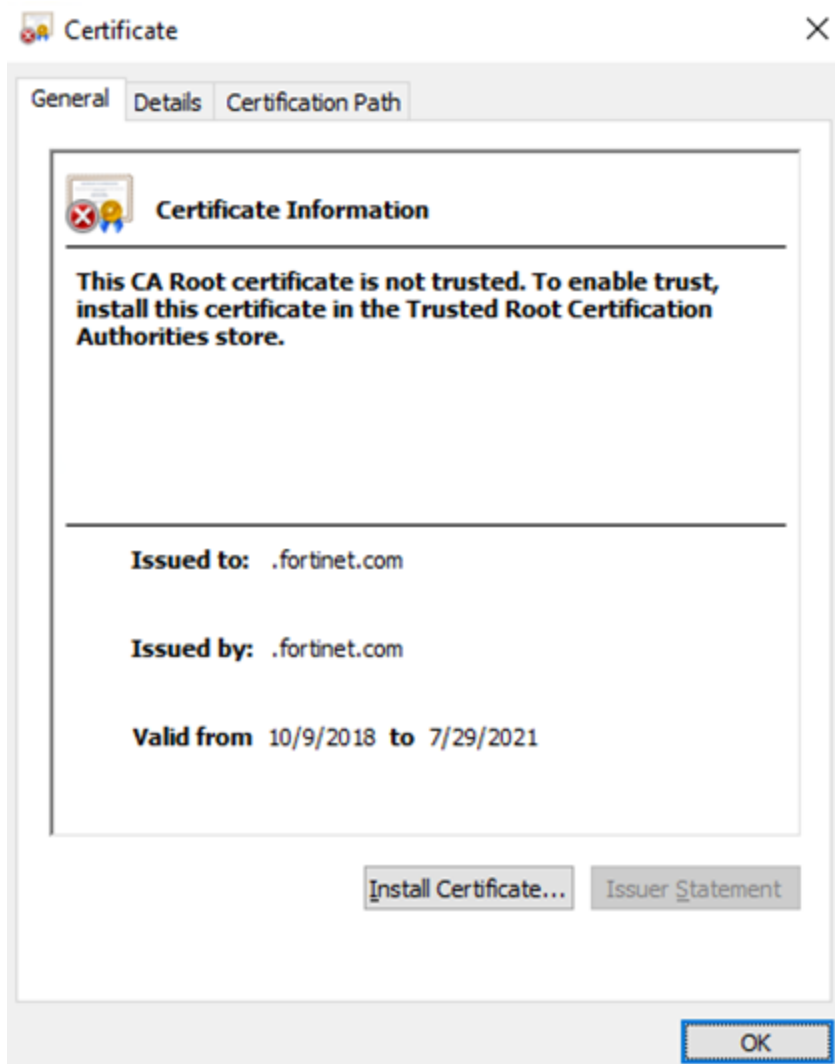
- a. In the Google Chrome browser address bar, type `http://<internal_IP_address>/ca.crt` (for example, `http://192.168.1.100/ca.crt`).
 - where `<internal_IP_address>` value is the IP address of the Fortisolator internal interface. For example, the IP address of the internal interface that you configured in step 3 of [Installing Fortisolator 1000F on page 7](#).
- b. In the security warning at the bottom of the browser, click **Keep** to download the certificate.



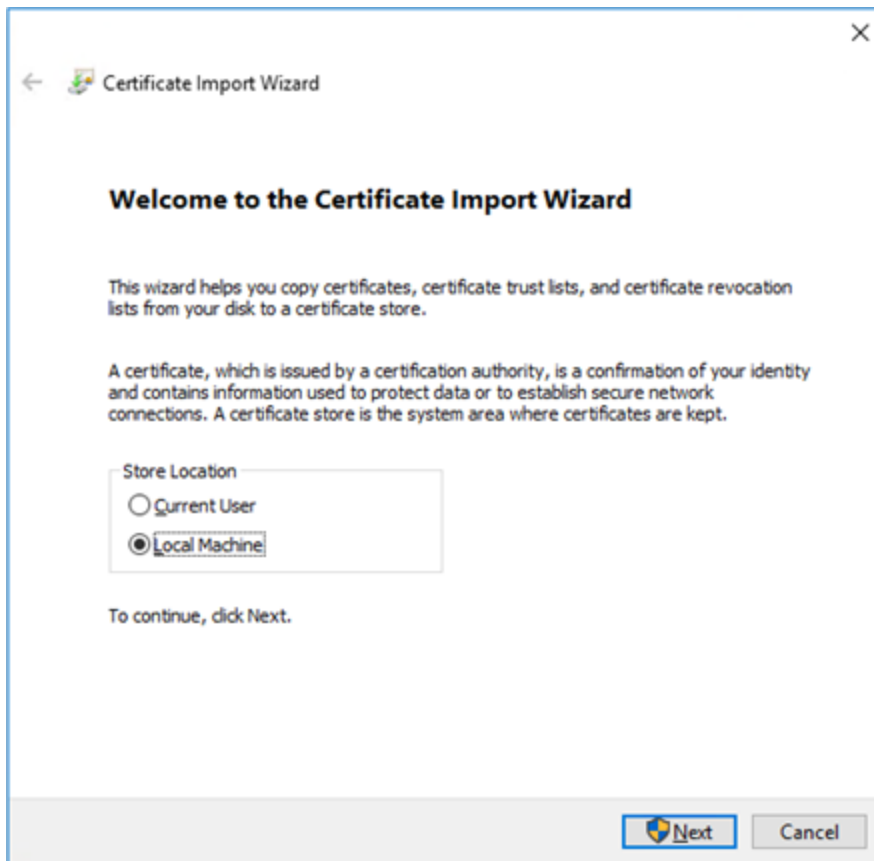
- c. Click **Open** to import the ca.crt certificate into Google Chrome.



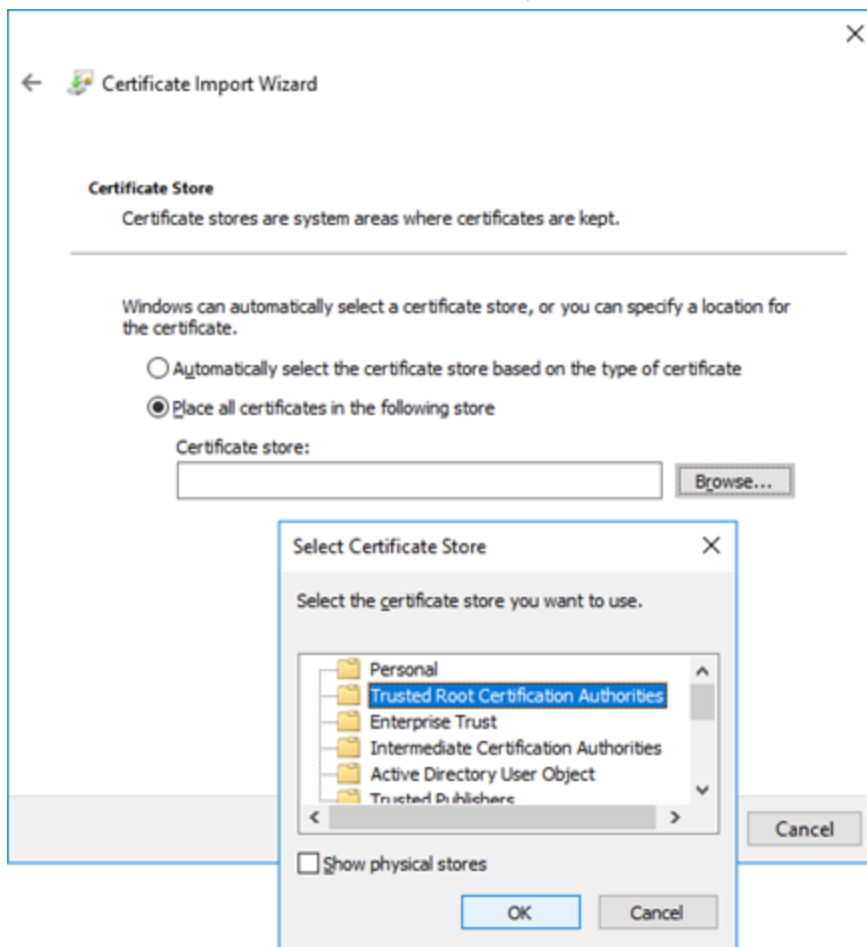
- d. Click **Install Certificate**.



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

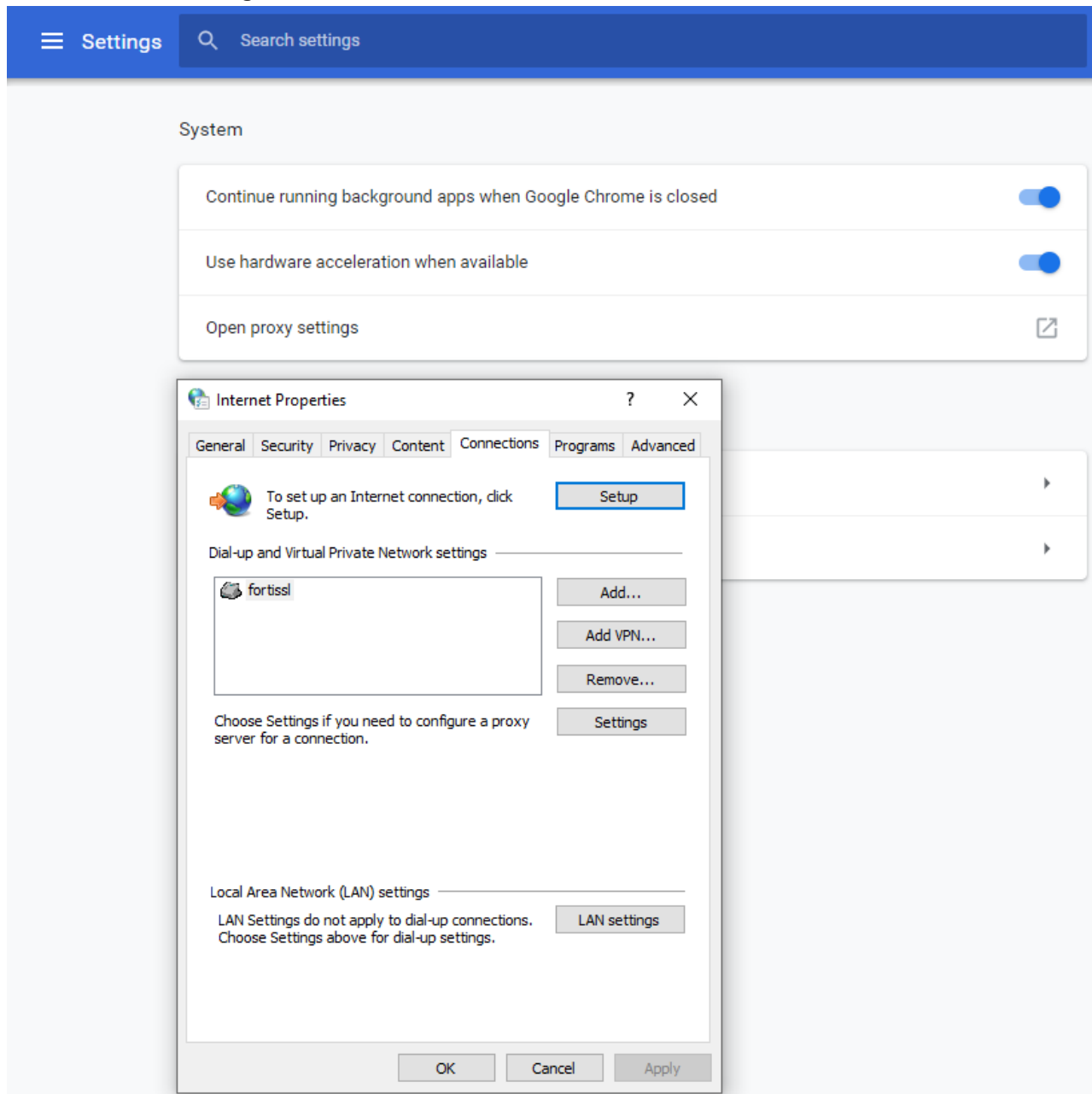


- f. Select **Trusted Root Certificate Authorities**, and click **OK**.

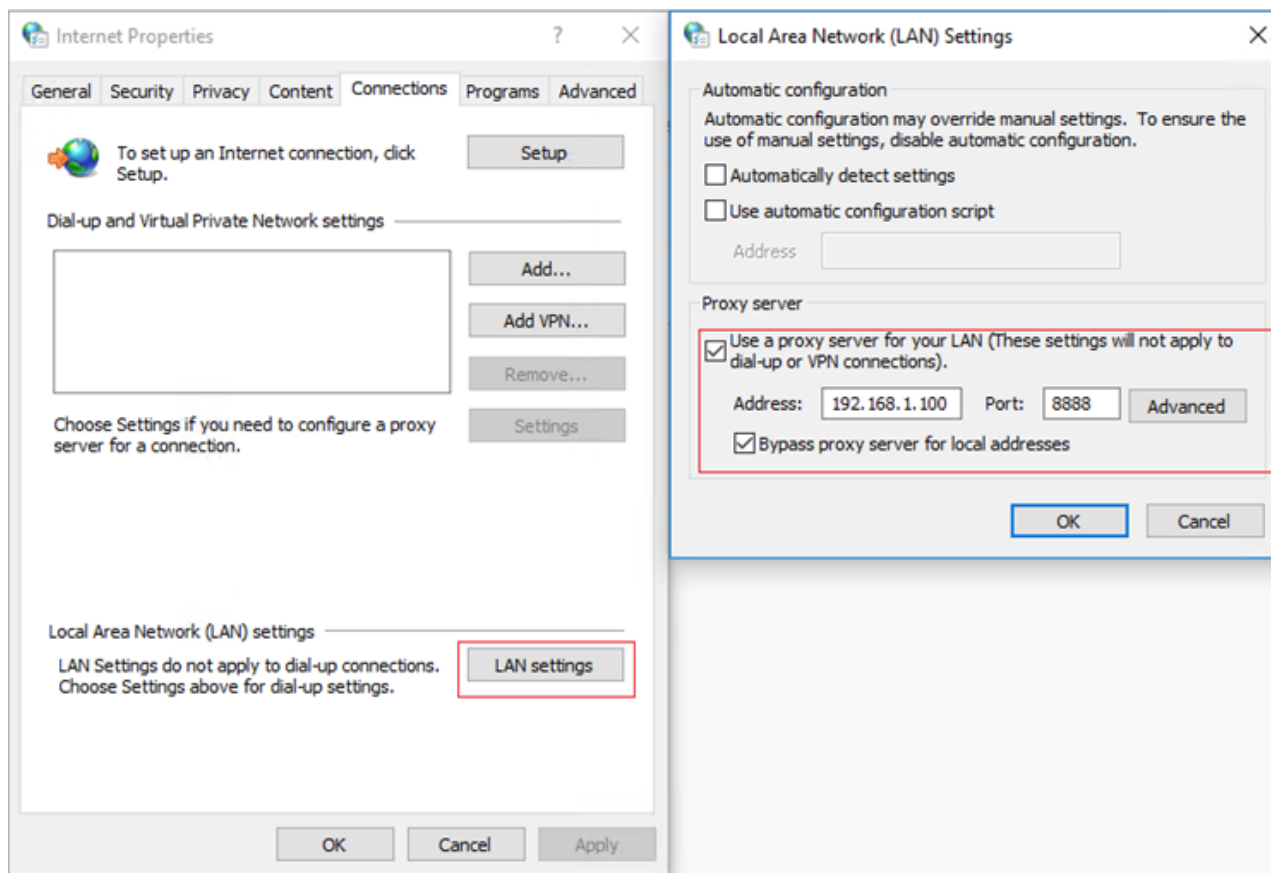


2. Open the Google Chrome browser.

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

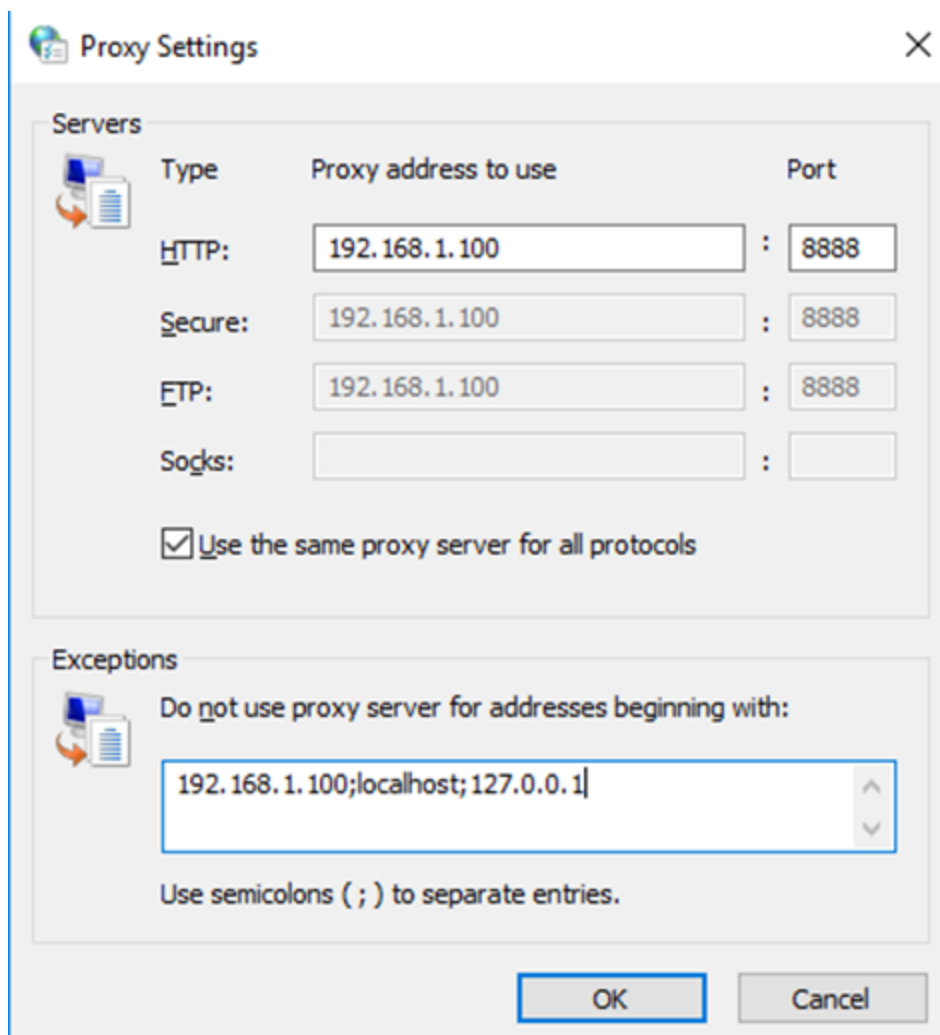


4. Expand **Advanced**.
5. In the **System** section, click **Open proxy settings**.
6. In the **Internet Properties** window, click the **Connections** tab.
7. Click **LAN settings**.
8. In the **Proxy server** section, select **Use a proxy server for your LAN**, and enter the following setting (values 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.

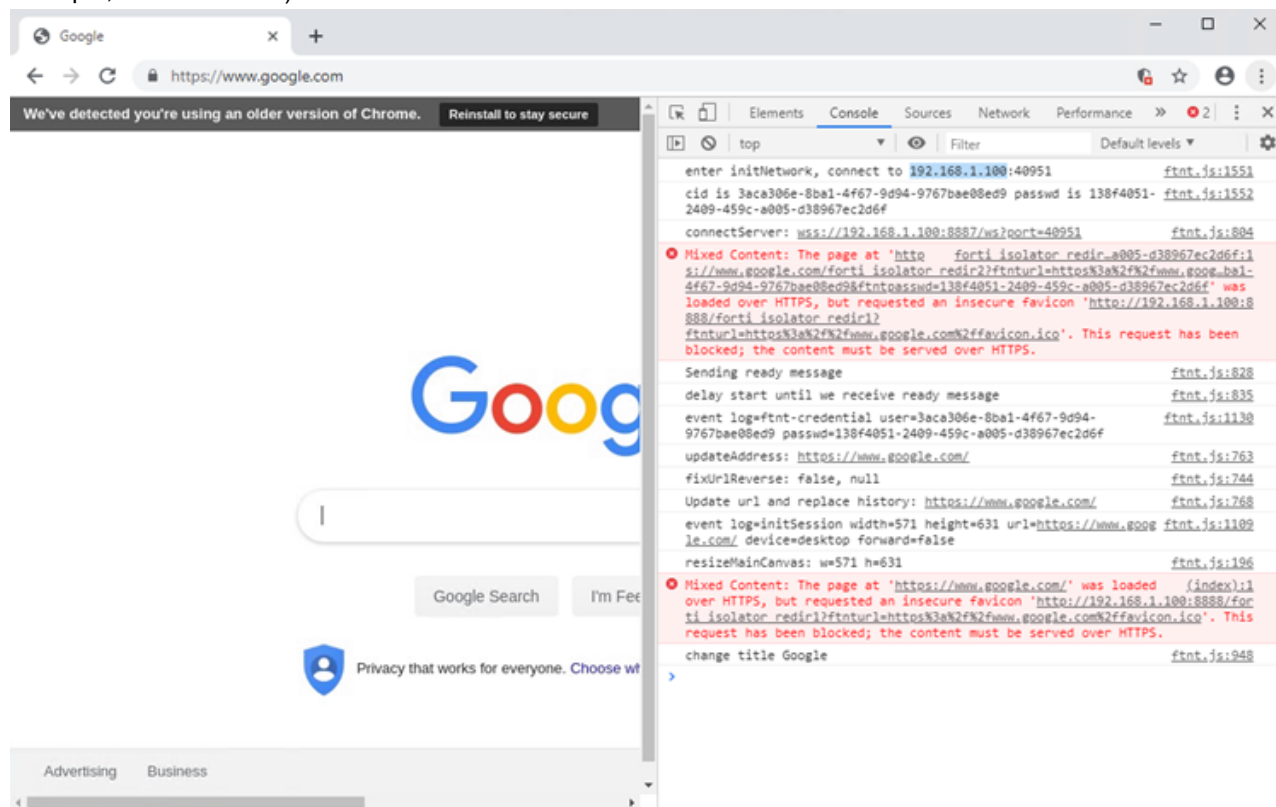
Verifying Fortisolator proxy mode with Google Chrome

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).



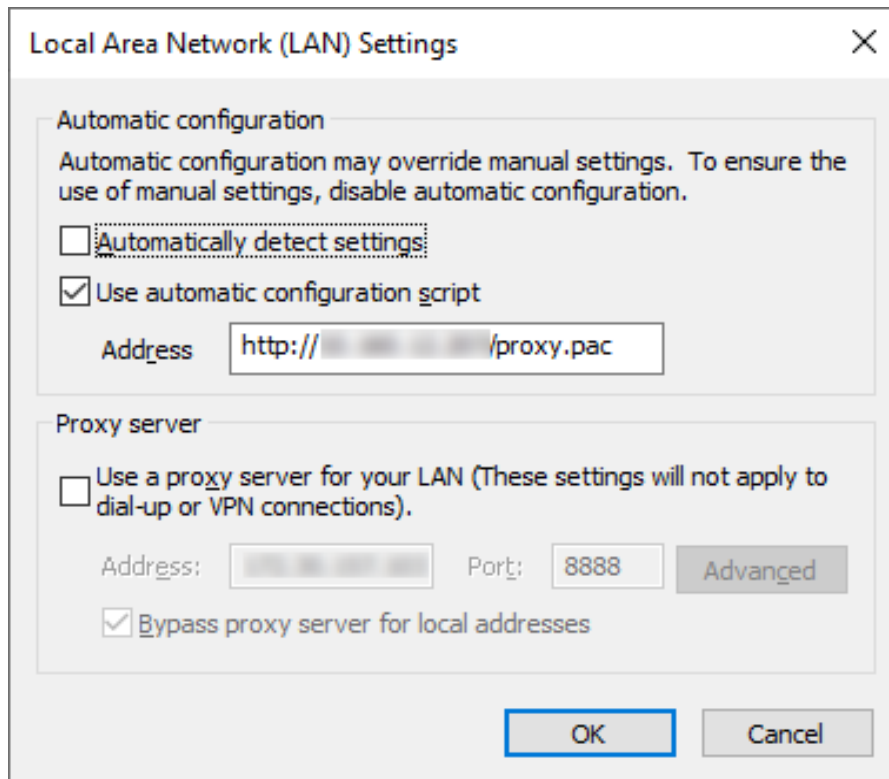
Using proxy mode with Internet Explorer

Use this procedure to configure proxy mode with Internet Explorer.

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.

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.

PAC file mode

PAC file mode with Mozilla Firefox

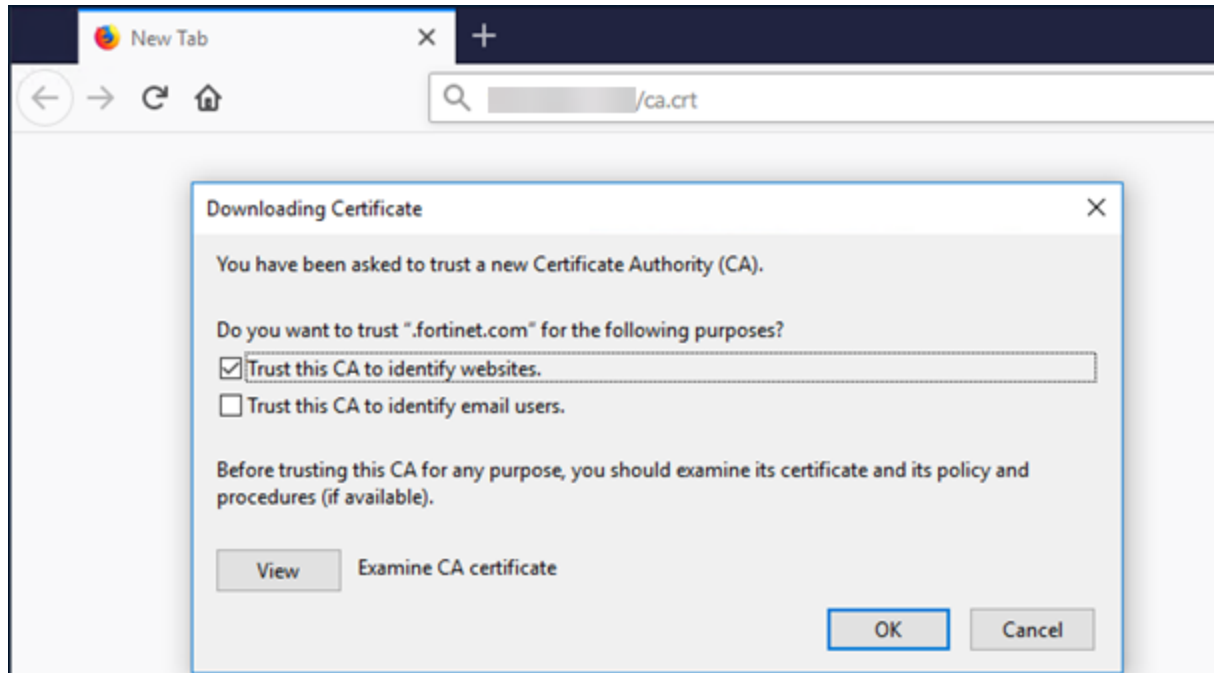
Importing the Fortisolator certificate into the Mozilla Firefox browser

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 7](#)

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

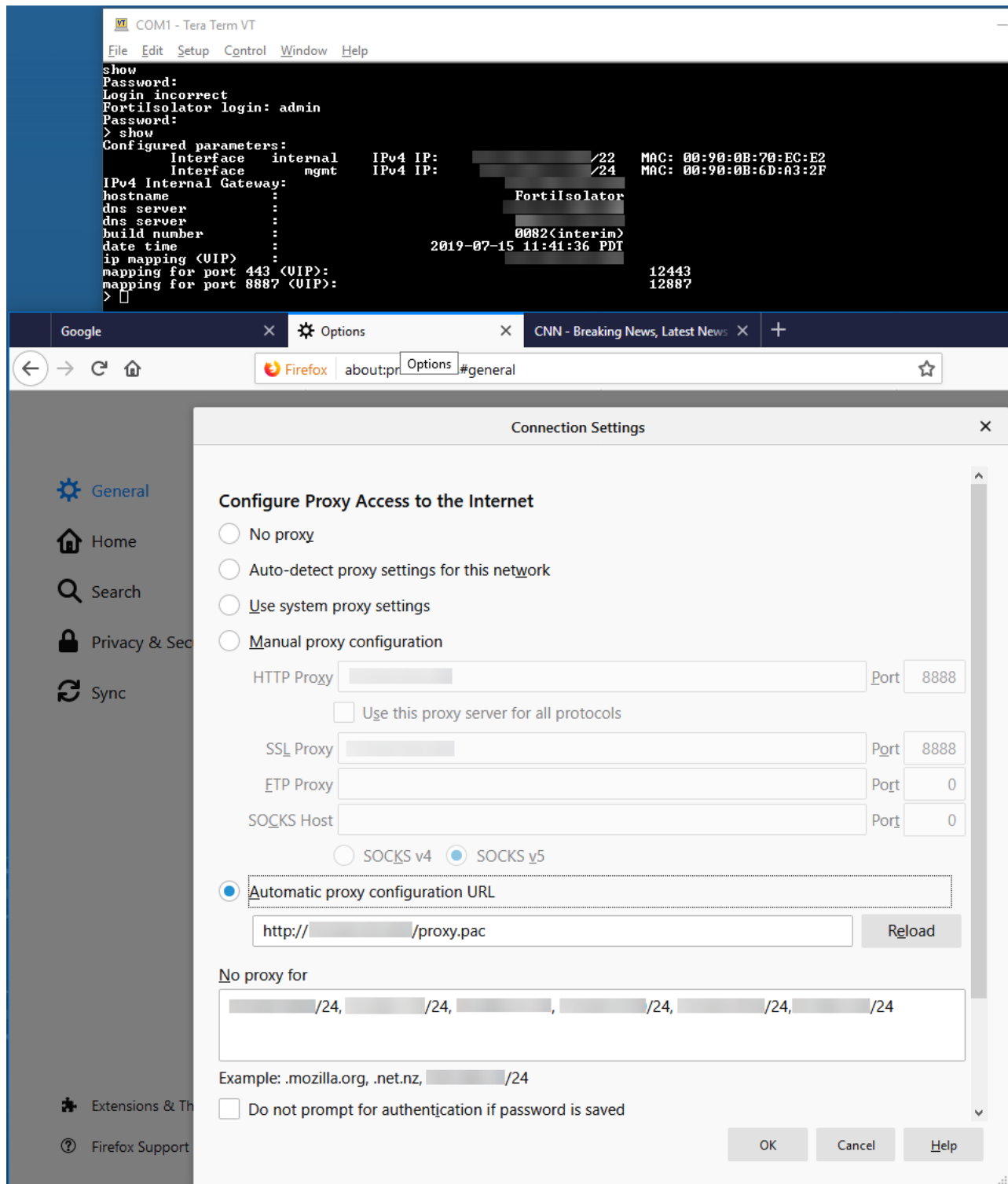


Configuring PAC file mode in Mozilla Firefox

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**.

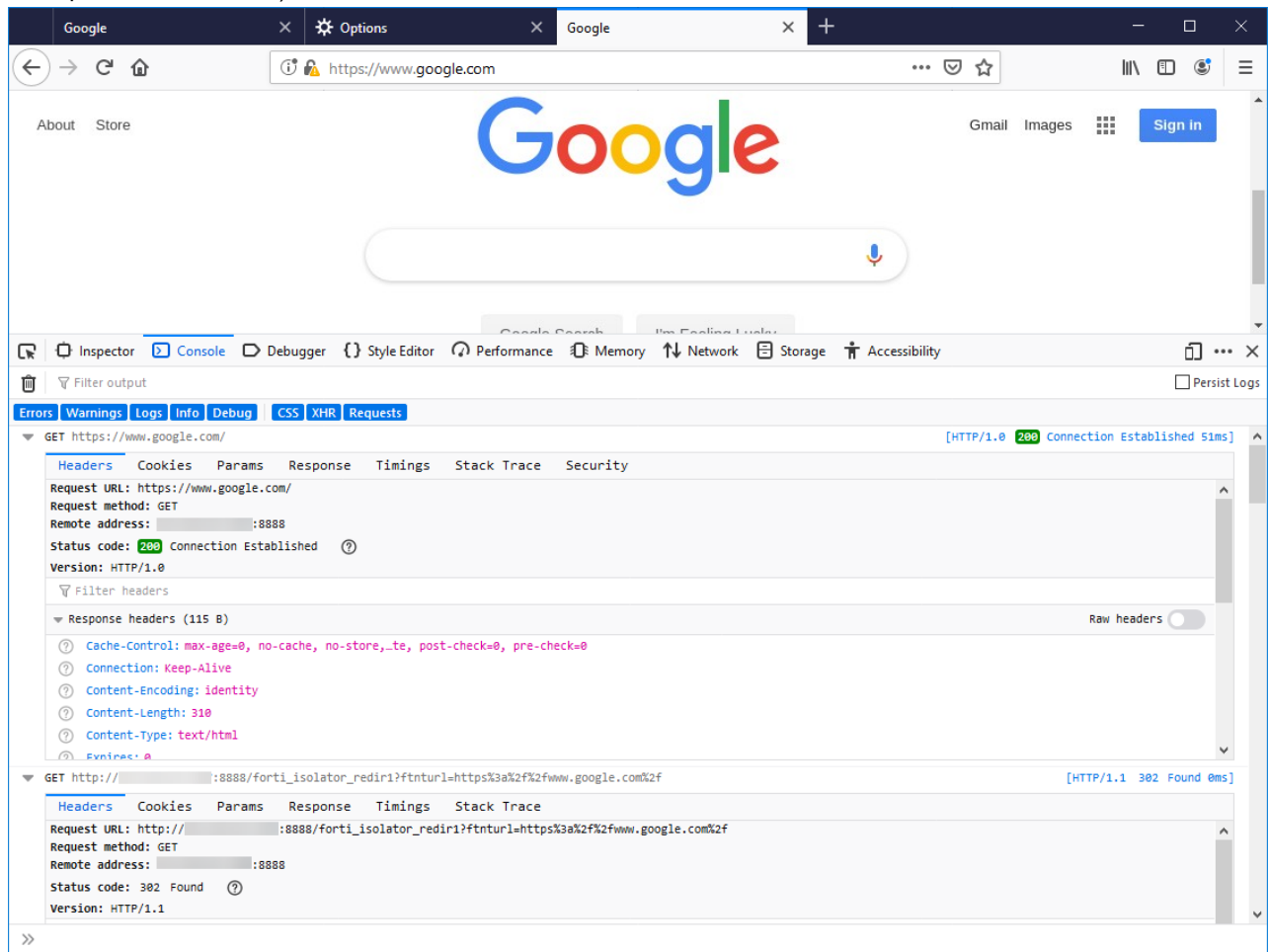
Verifying Fortisolator PAC file mode with Mozilla Firefox

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

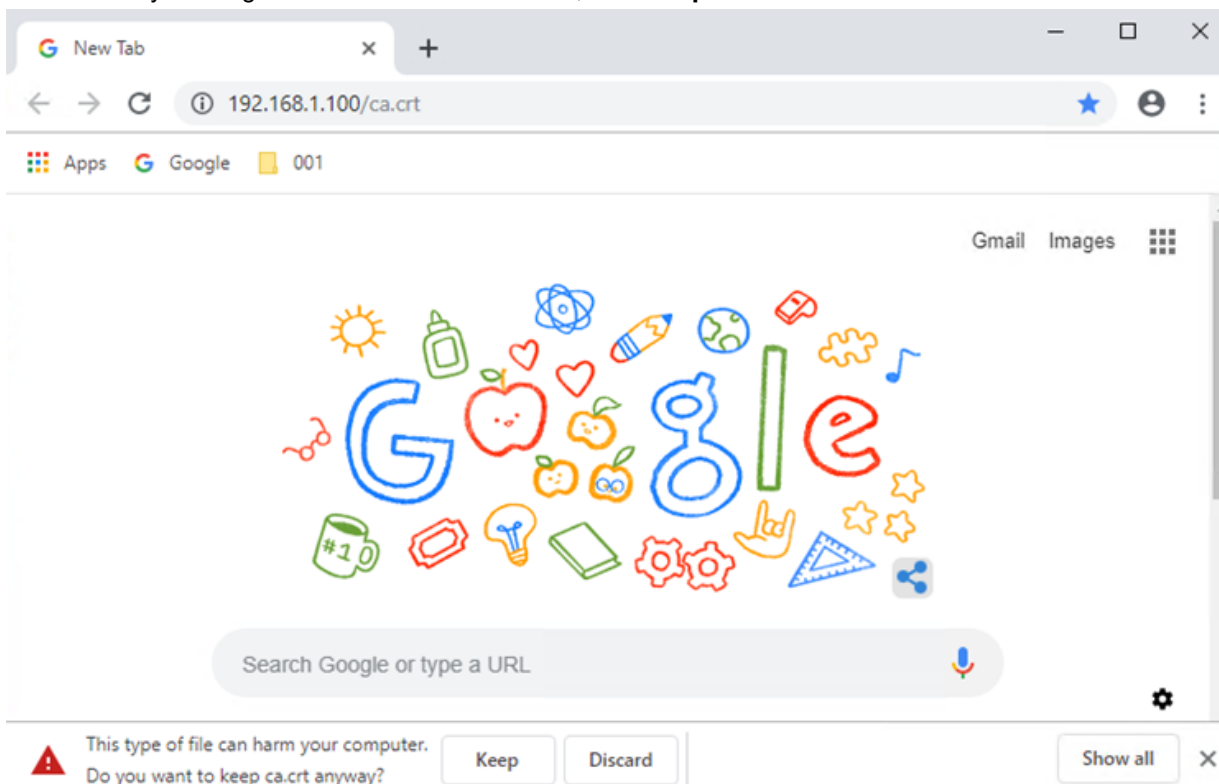
Importing the Fortisolator certificate into the Google Chrome browser

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

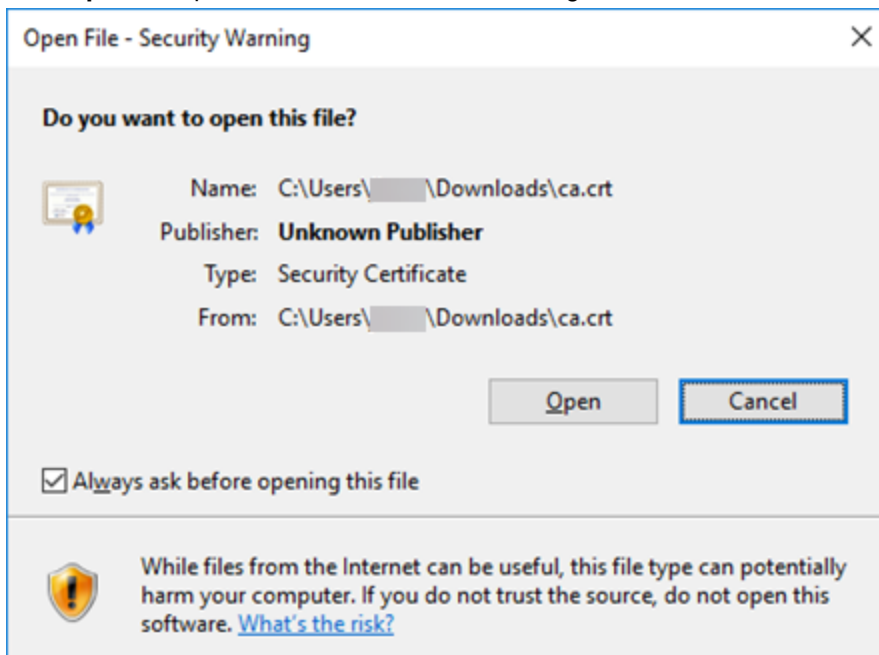
Steps

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 7](#).

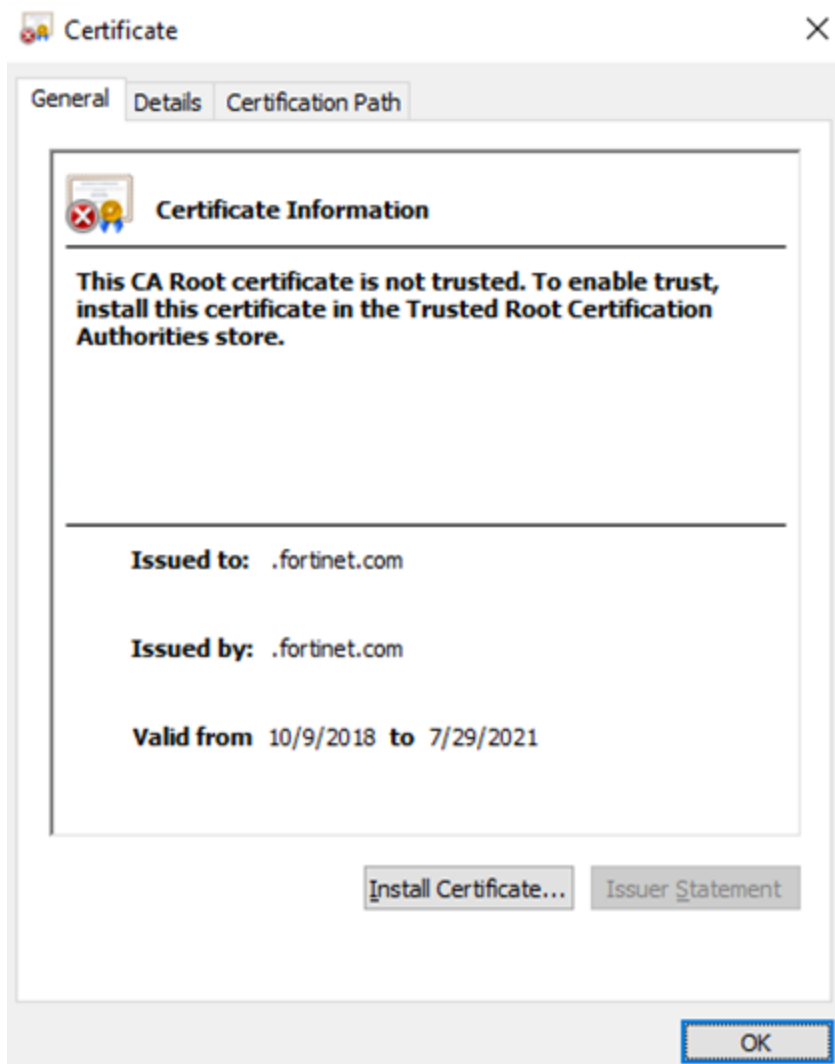
- b. In the security warning at the bottom of the browser, click **Keep** to download the certificate.



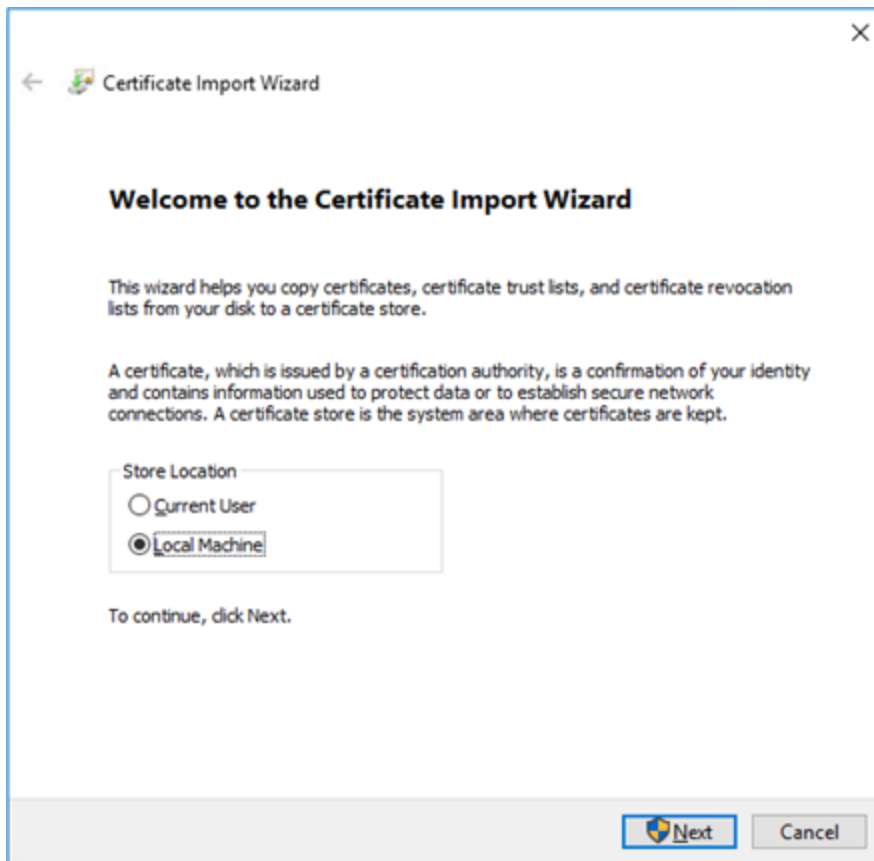
- c. Click **Open** to import the ca.crt certificate into Google Chrome.



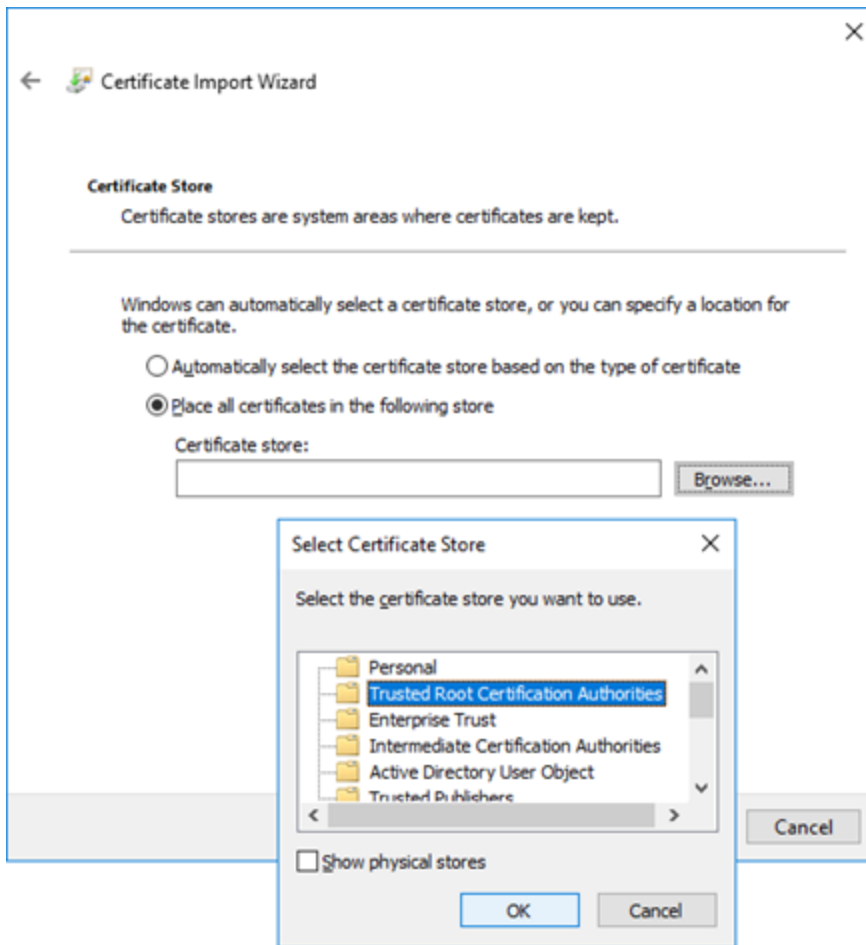
- d. Click **Install Certificate**.



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



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



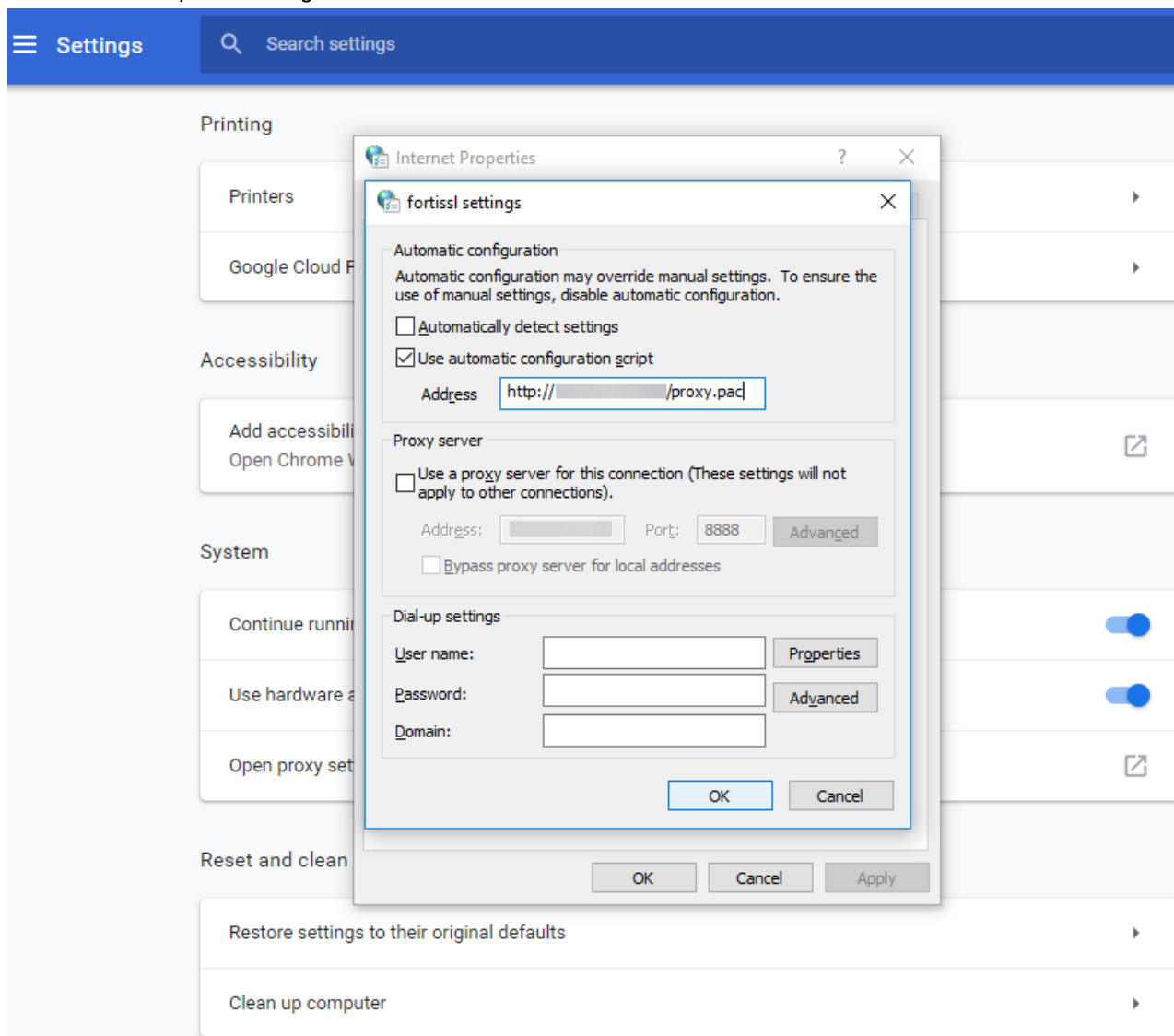
Configuring PAC file mode in Google Chrome

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.

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



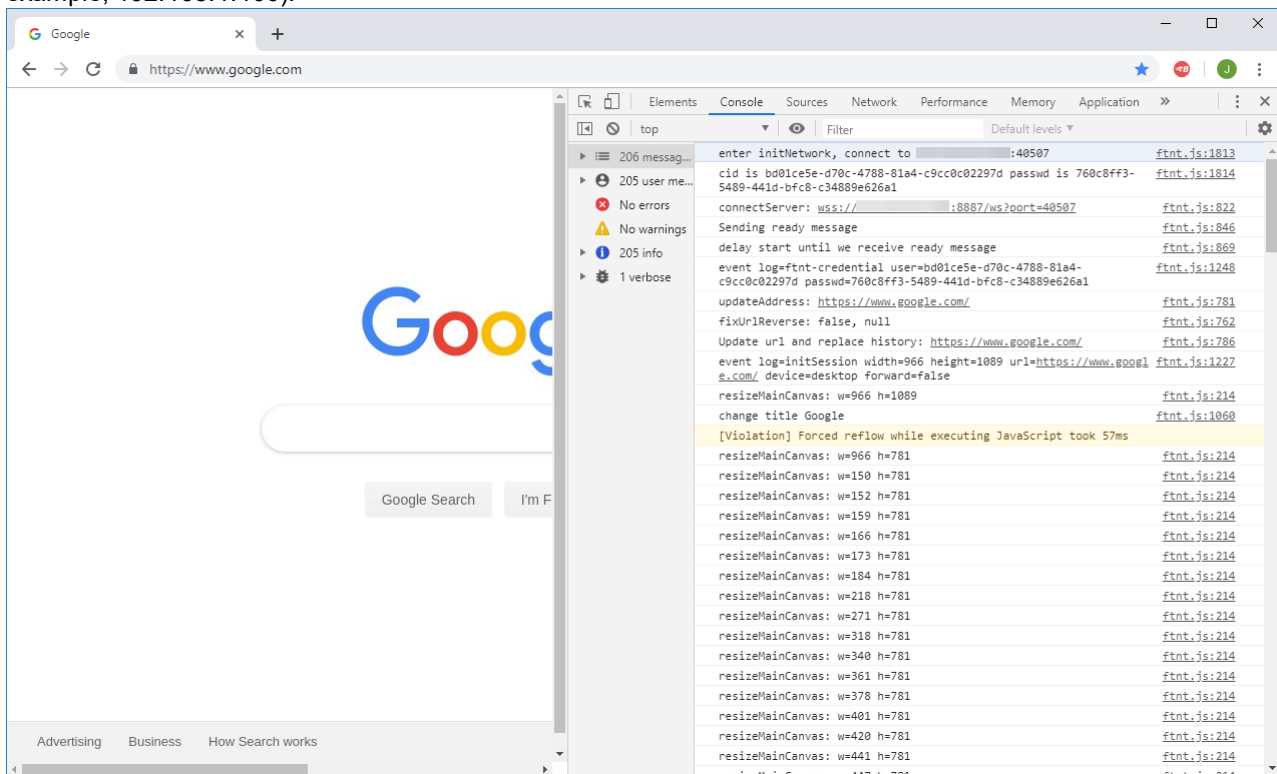
Verifying Fortisolator PAC file mode with Google Chrome

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

Steps

- 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:

A screenshot of the Fortisolator login page. The page has a green header with the text 'Fortisolator'. Below the header, there is a login form with the following elements: a 'Username' label and an input field with the placeholder text 'Enter Username'; a 'Password' label and an input field with the placeholder text 'Enter Password'; a 'Guest' checkbox; and a message stating '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 button labeled 'Login'. The browser's address bar shows the URL '192.168.1.101/isolator/login/https://www.google.com'.

[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 [Setting up single sign-on for local users on page 59](#) 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

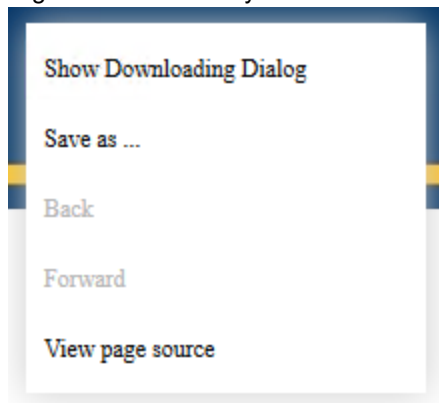
1. In a browser, select text that you want to copy, and then right-click.
2. Click **Copy**.
3. Navigate to the location where you want to paste the text, and then right-click.
4. Click **Paste**.

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.

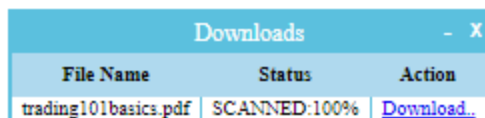
Steps

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.



The screenshot shows a window titled 'Downloads' with a standard Windows-style title bar (minimize, maximize, close buttons). Inside the window is a table with three columns: 'File Name', 'Status', and 'Action'. There is one row of data in the table.

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.

Diagnostics

Diagnostic tools

Tool	Definition
ping	Test network connectivity to another network host.
hardware-info	Display general hardware status information.
diagnose-nic	Display general network interface setting.



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.