Administration Guide

FortiIsolator 2.4.0

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/training-certification

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

January 30, 2023
FortiIsolator 2.4.0 Administration Guide
51-240-809800-20230130

TABLE OF CONTENTS

Change log

Date	Change Description
2022-05-18	Initial release.
2022-08-10	• Added more details about new features. See New in this release on page 7. • Updated the following topics: • Certificates on page 85 • SNMP on page 87 • Upgrade on page 91 • Profile on page 103 • Policy on page 110 • Default policy on page 111
2022-09-16	Updated the following topics: • High Availability on page 80 • Install package on page 92
2022-12-02	Updated the following topics: • High Availability on page 80 • Upgrade on page 91
2023-01-06	Updated the FortiIsolator CA certificate on page 71 topic.
2023-01-30	Added the Port information on page 9 topic.

About this release

This section provides information about new features in FortiIsolator version 2.4.0.

New in this release

FortiIsolator version 2.4.0 includes the following new features:

High Availability (HA) support for AWS VMs

You can now configure AWS VMs that are built on the Nitro system to work in High Availability on page 80 (HA) mode. For more information about configuration in HA mode, see Configuring IP mapping in HA mode on page 57.

Support for SNMP v3

FortiIsolator 2.4.0 adds support for SNMP v3 which provides authentication and encryption capabilities. For more information about how to authenticate and encrypt SNMP v3 connection with FortiIsolator, see SNMP on page 87.

Enhancements to certificate support

FortiIsolator 2.4.0 has the following enhancements to certificate support:

- You can now import a self-signed CA root certificate (`root_ca.crt`) to the FortiIsolator, which is the origin of a certificate chain that all subordinate certificates stem from. When a self-signed CA root certificate (`root_ca.crt`) and the whole chain of subordinate certificates are uploaded on FortiIsolator, you need to install only the lowest level subordinate certificate in your browser.
- You can now import certificates with password, certificates in PKCS12 format, and/or certificates that bundle with a key file.
- The *Isolator CA Certificate* row is no longer available under *System* > *Certificate*, which reduces confusion as the Isolator CA Certificate is exclusive to Local Certificate, which means only one can be in effect.

For more information about certificates, see Certificates on page 85.

System upgrade using CLI

You can now use the following CLI command to upgrade the system:

```
system-upgrade {tftp|ftp} <path> <server> [:<port>] [<user>:<password>]
```

For more information about the different ways to upgrade the system, see Upgrade on page 91.

Authorization cookie lifetime configuration

When creating a new or default policy under *Policies and Profiles*, use the *Auth Cookie Lifetime* field to define how long the authorization cookie is active before it expires and the user needs to re-login. This setting does not take effect when the user is in guest mode. For more information, see Policy on page 110 and Default policy on page 111.

Port information

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

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

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

Overview

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

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

FortiIsolator models

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

- FortiIsolator 1000F
- FortiIsolator VM for Linux KVM
- FortiIsolator VM for VMware vSphere
- FortiIsolator VM for VMware ESXi
- FortiIsolator VM for Hyper-V
- Amazon Web Services (AWS)

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

Model	Description
FortiIsolator appliance	• FortiIsolator 1000F • Supports 250 concurrent sessions, under normal traffic profiles
FortiIsolator VM	• VMware vSphere Hypervisor ESX/ESXi versions 6.0 and 6.5 • KVM QEMU version 0.12.1 and higher, includes a hypervisor • Hyper-V Manager version 10.0.18362.1 and higher • Amazon Web Services (AWS)

Installation

The following sections provide installation instructions for each model:

- FortiIsolator appliance installation on page 11
- FortiIsolator VM installation on page 17

Downloading FortiIsolator firmware

To download FortiIsolator firmware for your FortiIsolator model:

1. Go to https://support.fortinet.com.
2. Click *Login* and log in to the Fortinet Support website.
3. From the *Support>>Downloads* menu, select *Firmware Download*.
4. In the *Select Product* dropdown menu, select *FortiIsolator*.
5. On the *Download* tab, navigate to the FortiIsolator firmware file for your FortiIsolator model in the *Image Folders/Files* section.

For more information about the specific firmware version to download for your FortiIsolator model, see the FortiIsolator Release Notes.

6. Click *HTTPS* to download the firmware.
7. Unzip the firmware file.

FortiIsolator appliance installation

Installing FortiIsolator 1000F

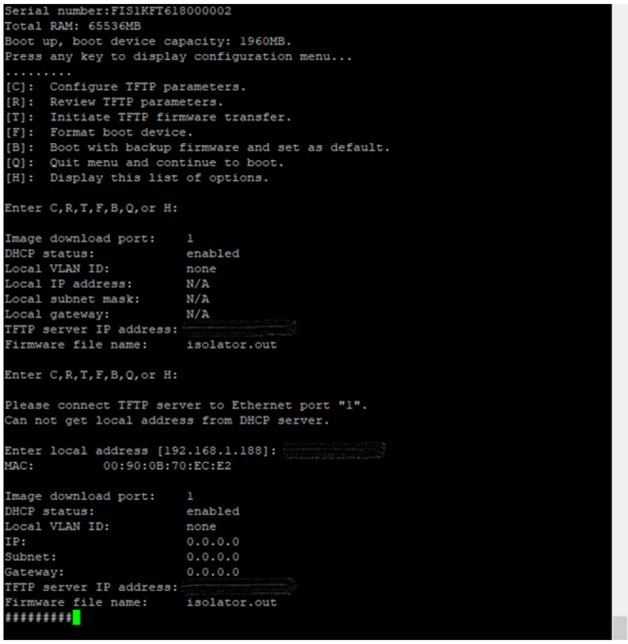
Use this procedure to install FortiIsolator 1000F.

Prerequisites

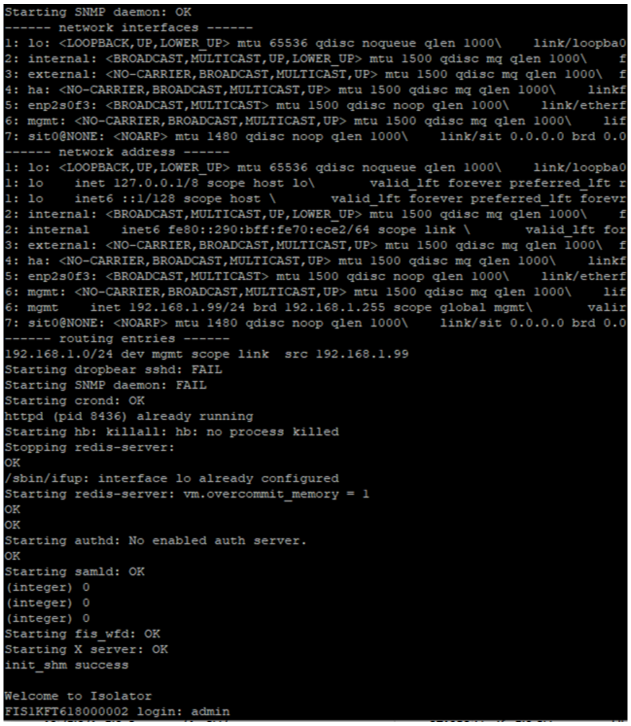
- Install FortiIsolator 1000F hardware by following the instructions in the FortiIsolator 1000F QuickStart Guide.
- Download the FortiIsolator firmware by following the instructions in Downloading FortiIsolator firmware on page 11.
- Connect to a console (for example, Tera Term).

Steps

1. Using the console, load the FortiIsolator firmware file (for example, `FIS_1000F-v1-build0308.out`).

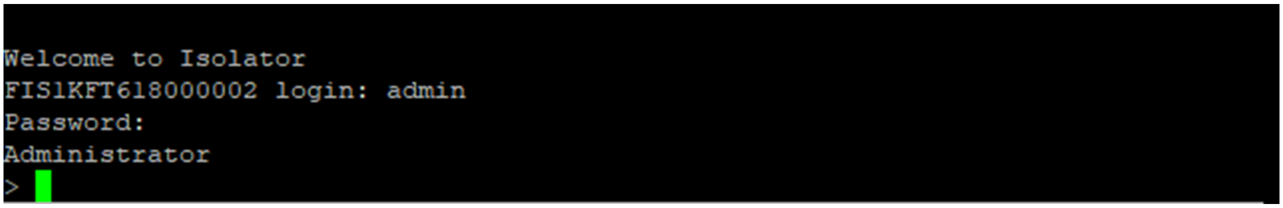


```
Serial number:FIS1KFT618000002
Total RAM: 65536MB
Boot up, boot device capacity: 1960MB.
Press any key to display configuration menu...
.........
[C]:  Configure TFTP parameters.
[R]:  Review TFTP parameters.
[T]:  Initiate TFTP firmware transfer.
[F]:  Format boot device.
[B]:  Boot with backup 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: [redacted]
Firmware file name:     isolator.out

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

Please connect TFTP server to Ethernet port "1".
Can not get local address from DHCP server.

Enter local address [192.168.1.188]: [redacted]
MAC:          00:90:0B:70:EC:E2

Image download port:    1
DHCP status:            enabled
Local VLAN ID:          none
IP:                     0.0.0.0
Subnet:                 0.0.0.0
Gateway:                0.0.0.0
TFTP server IP address: [redacted]
Firmware file name:     isolator.out
#########
```



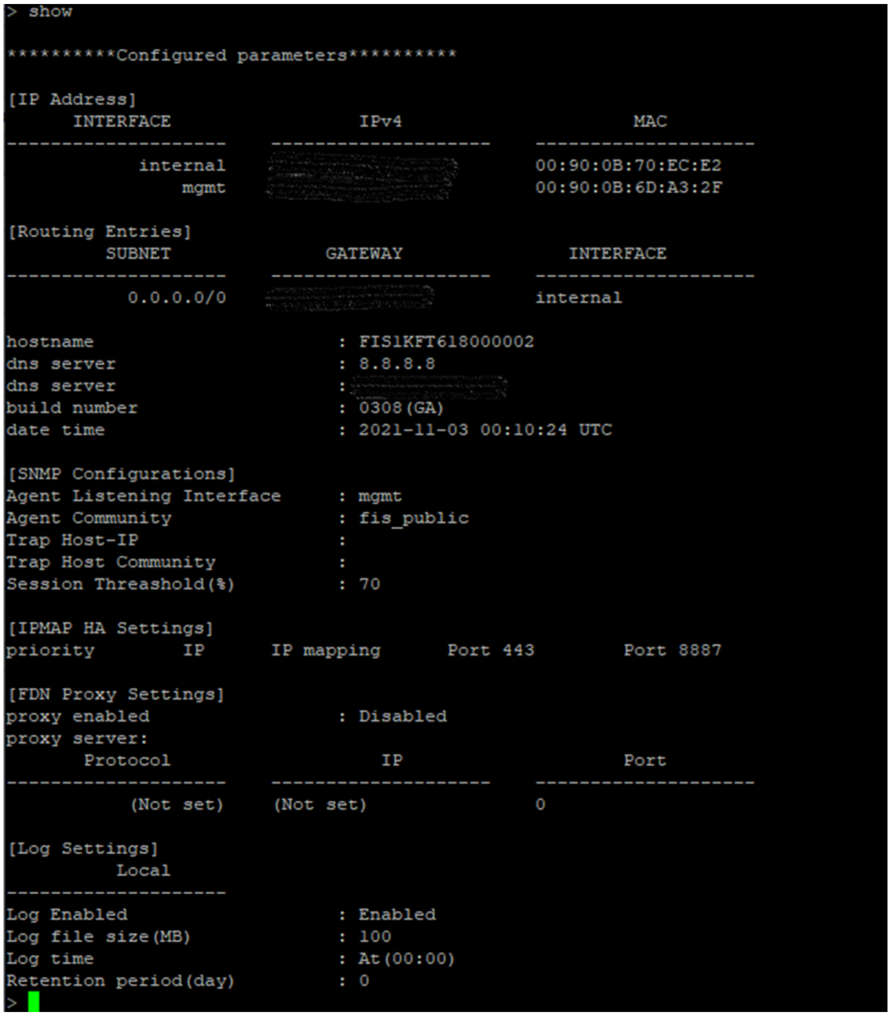
```
Starting SNMP daemon: OK
------ network interfaces ------
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue qlen 1000\    link/loopba0
2: internal: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq qlen 1000\    f
3: external: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc mq qlen 1000\  f
4: ha: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc mq qlen 1000\    linkf
5: enp2s0f3: <BROADCAST,MULTICAST> mtu 1500 qdisc noop qlen 1000\    link/etherf
6: mgmt: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc mq qlen 1000\    lif
7: sit0@NONE: <NOARP> mtu 1480 qdisc noop qlen 1000\    link/sit 0.0.0.0 brd 0.0
------ network address ------
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue qlen 1000\    link/loopba0
1: lo    inet 127.0.0.1/8 scope host lo\       valid_lft forever preferred_lft r
1: lo    inet6 ::1/128 scope host \       valid_lft forever preferred_lft forevr
2: internal: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq qlen 1000\    f
2: internal    inet6 fe80::290:bff:fe70:ece2/64 scope link \       valid_lft for
3: external: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc mq qlen 1000\  f
4: ha: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc mq qlen 1000\    linkf
5: enp2s0f3: <BROADCAST,MULTICAST> mtu 1500 qdisc noop qlen 1000\    link/etherf
6: mgmt: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc mq qlen 1000\    lif
6: mgmt    inet 192.168.1.99/24 brd 192.168.1.255 scope global mgmt\       valir
7: sit0@NONE: <NOARP> mtu 1480 qdisc noop qlen 1000\    link/sit 0.0.0.0 brd 0.0
------ routing entries ------
192.168.1.0/24 dev mgmt scope link  src 192.168.1.99
Starting dropbear sshd: FAIL
Starting SNMP daemon: FAIL
Starting crond: OK
httpd (pid 8436) already running
Starting hb: killall: hb: no process killed
Stopping redis-server:
OK
/sbin/ifup: interface lo already configured
Starting redis-server: vm.overcommit_memory = 1
OK
OK
Starting authd: No enabled auth server.
OK
Starting samld: OK
(integer) 0
(integer) 0
(integer) 0
Starting fis_wfd: OK
Starting X server: OK
init_shm success

Welcome to Isolator
FIS1KFT618000002 login: admin
```

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



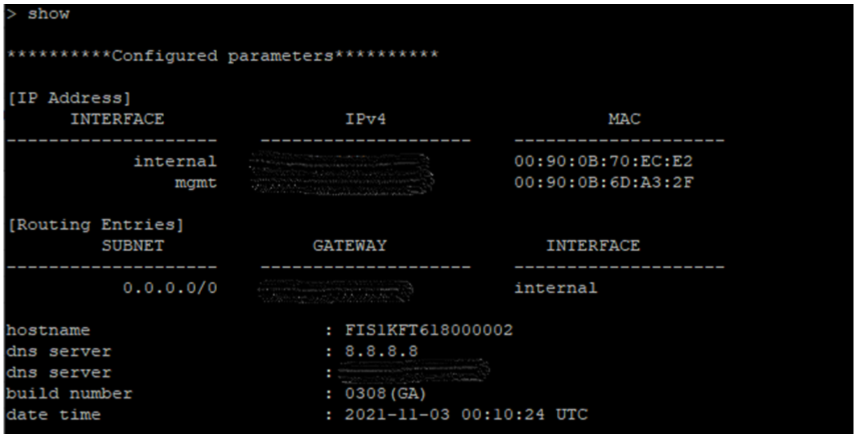
```
Welcome to Isolator
FIS1KFT618000002 login: admin
Password:
Administrator
>
```

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



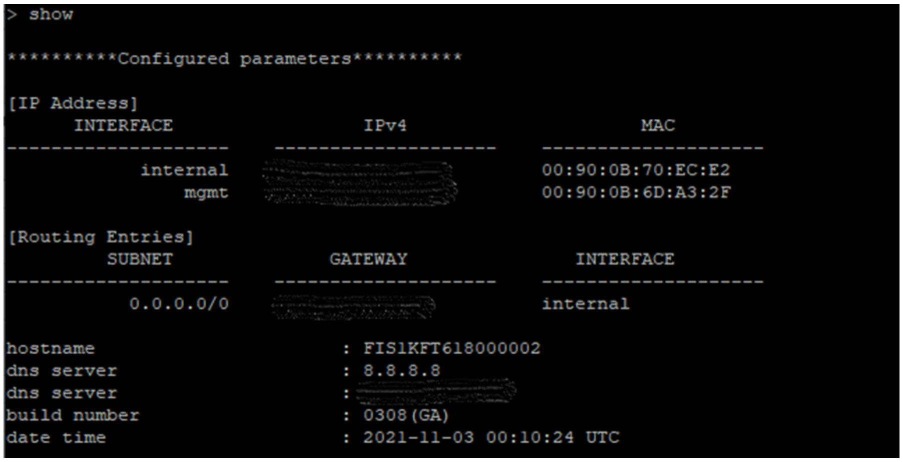
```
> show

**********Configured parameters**********

[IP Address]
      INTERFACE                 IPv4                     MAC
--------------------    --------------------    --------------------
            internal    [redacted]              00:90:0B:70:EC:E2
                mgmt                            00:90:0B:6D:A3:2F

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

hostname                      : FIS1KFT618000002
dns server                    : 8.8.8.8
dns server                    : [redacted]
build number                  : 0308(GA)
date time                     : 2021-11-03 00:10:24 UTC

[SNMP Configurations]
Agent Listening Interface     : mgmt
Agent Community               : fis_public
Trap Host-IP                  :
Trap Host Community           :
Session Threashold(%)         : 70

[IPMAP HA Settings]
priority        IP      IP mapping      Port 443        Port 8887

[FDN Proxy Settings]
proxy enabled                 : Disabled
proxy server:
       Protocol                   IP                    Port
--------------------    --------------------    --------------------
           (Not set)    (Not set)               0

[Log Settings]
          Local
--------------------
Log Enabled                   : Enabled
Log file size(MB)             : 100
Log time                      : At(00:00)
Retention period(day)         : 0
>
```

4. Set the time zone (for example, use `set timezone` command to set time zone as `PST8PDT`).



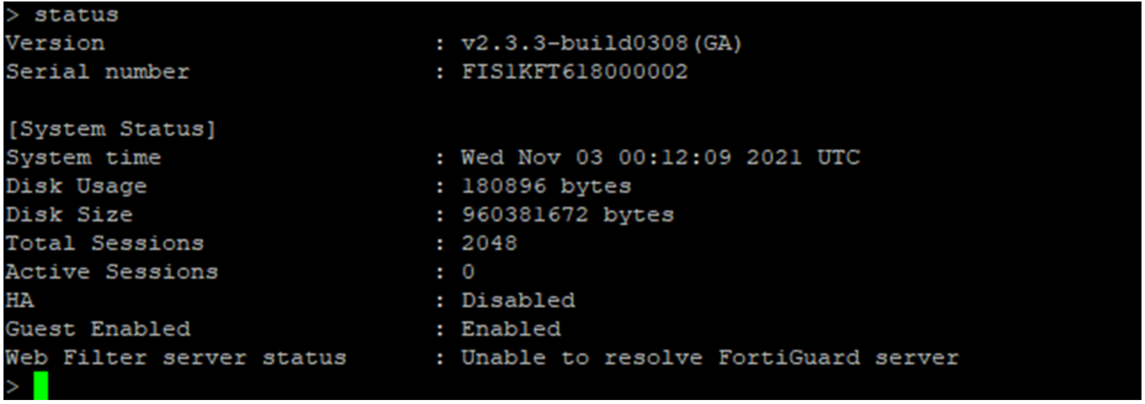
```
> show

**********Configured parameters**********

[IP Address]
      INTERFACE               IPv4                   MAC
--------------------   --------------------   --------------------
            internal   [redacted]             00:90:0B:70:EC:E2
                mgmt                          00:90:0B:6D:A3:2F

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

hostname                     : FIS1KFT618000002
dns server                   : 8.8.8.8
dns server                   : [redacted]
build number                 : 0308(GA)
date time                    : 2021-11-03 00:10:24 UTC
```

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



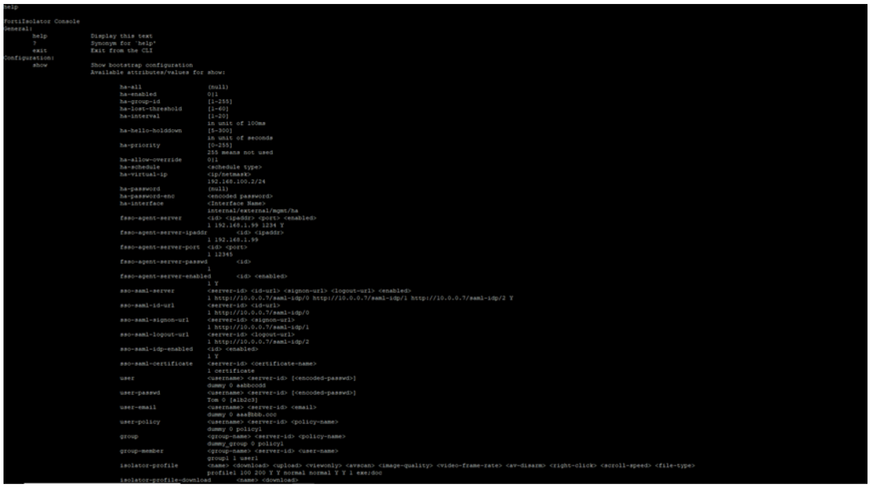
```
> show

**********Configured parameters**********

[IP Address]
      INTERFACE               IPv4                   MAC
--------------------   --------------------   --------------------
            internal   [redacted]             00:90:0B:70:EC:E2
                mgmt                          00:90:0B:6D:A3:2F

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

hostname                     : FIS1KFT618000002
dns server                   : 8.8.8.8
dns server                   : [redacted]
build number                 : 0308(GA)
date time                    : 2021-11-03 00:10:24 UTC
```

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).

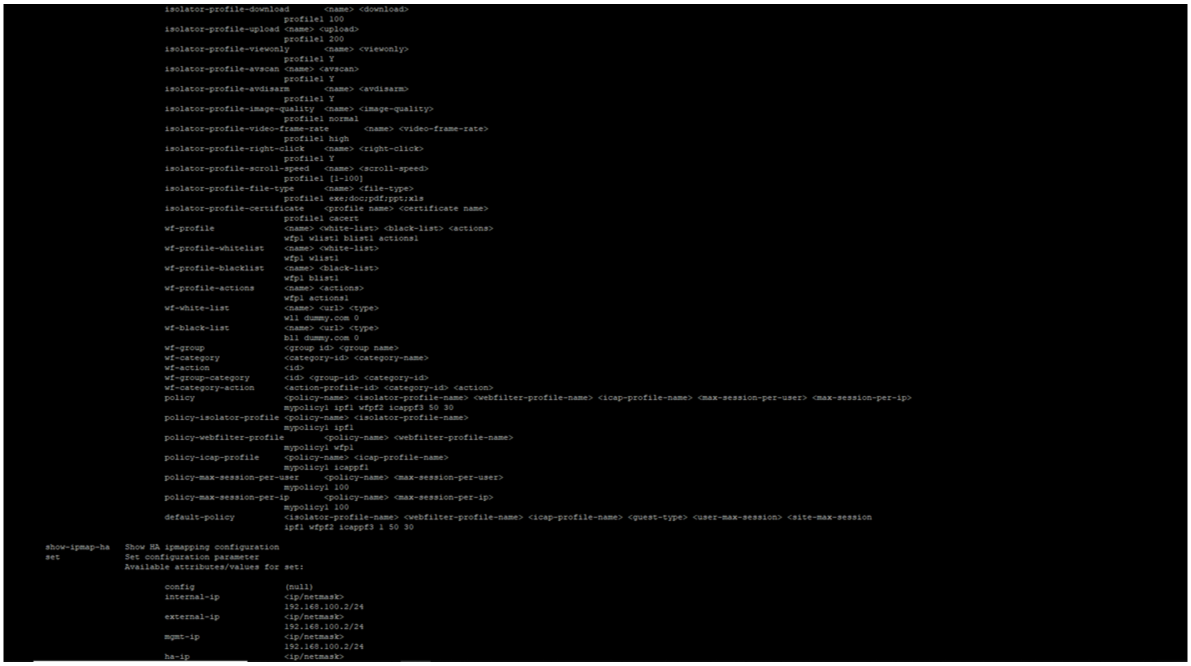


```
> status
Version                        : v2.3.3-build0308(GA)
Serial number                  : FIS1KFT618000002

[System Status]
System time                    : Wed Nov 03 00:12:09 2021 UTC
Disk Usage                     : 180896 bytes
Disk Size                      : 960381672 bytes
Total Sessions                 : 2048
Active Sessions                : 0
HA                             : Disabled
Guest Enabled                  : Enabled
Web Filter server status       : Unable to resolve FortiGuard server
>
```

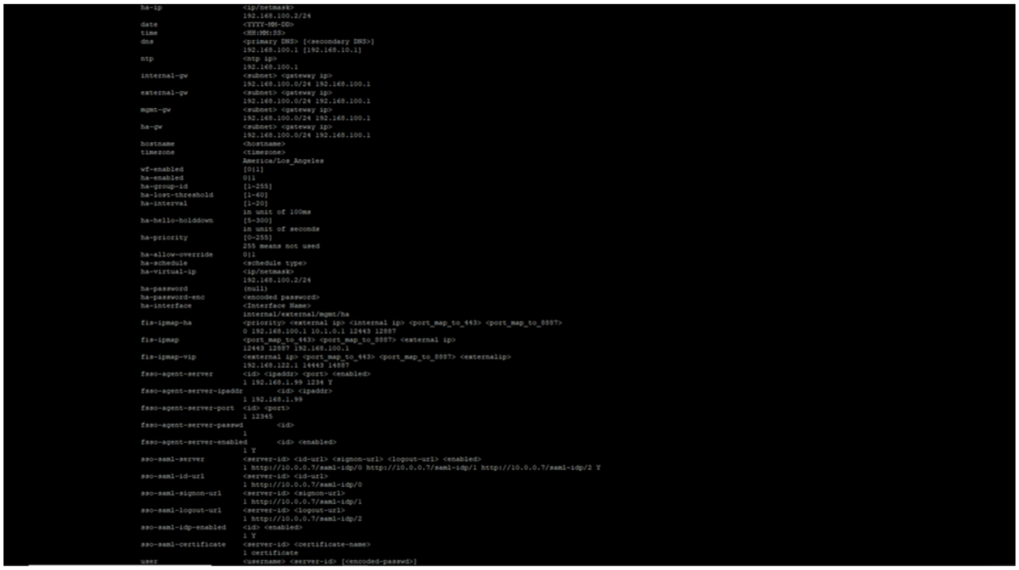
7. You can use the `help` command to see the FortiIsolator console comments.



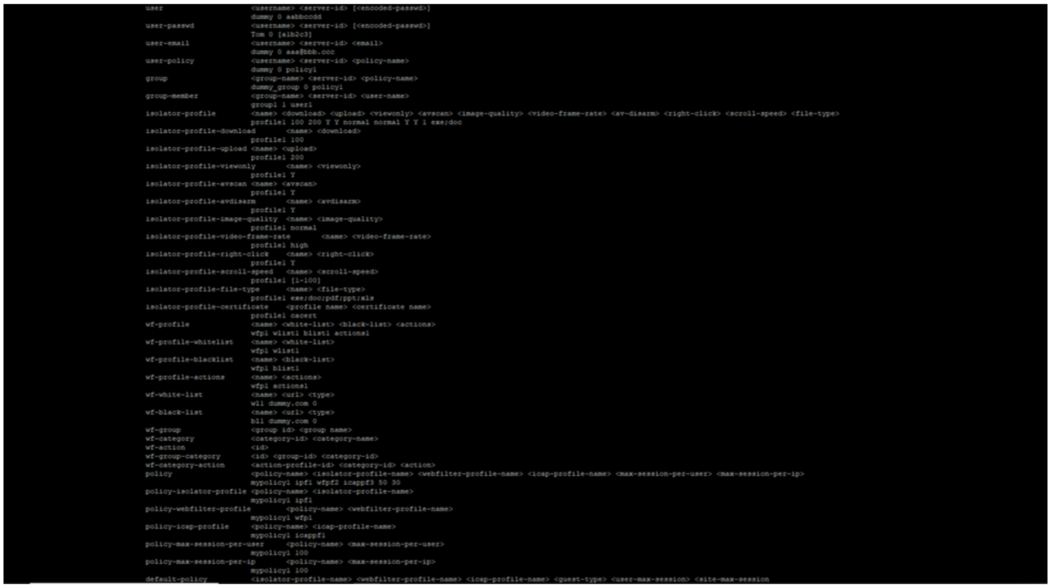
```
help

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>
                                                        192.168.100.2/24
                                ha-password             (null)
                                ha-password-enc         <encoded password>
                                ha-interface            <Interface Name>
                                                        internal/external/mgmt/ha
                                fsso-agent-server       <id> <ipaddr> <port> <enabled>
                                                        1 192.168.1.99 1234 Y
                                fsso-agent-server-ipaddr        <id> <ipaddr>
                                                        1 192.168.1.99
                                fsso-agent-server-port  <id> <port>
                                                        1 12345
                                fsso-agent-server-passwd        <id>
                                                        1
                                fsso-agent-server-enabled       <id> <enabled>
                                                        1 Y
                                sso-saml-server         <server-id> <id-url> <signon-url> <logout-url> <enabled>
                                                        1 http://10.0.0.7/saml-idp/0 http://10.0.0.7/saml-idp/1 http://10.0.0.7/saml-idp/2 Y
                                sso-saml-id-url         <server-id> <id-url>
                                                        1 http://10.0.0.7/saml-idp/0
                                sso-saml-signon-url     <server-id> <signon-url>
                                                        1 http://10.0.0.7/saml-idp/1
                                sso-saml-logout-url     <server-id> <logout-url>
                                                        1 http://10.0.0.7/saml-idp/2
                                sso-saml-idp-enabled    <id> <enabled>
                                                        1 Y
                                sso-saml-certificate    <server-id> <certificate-name>
                                                        1 certificate
                                user                    <username> <server-id> [<encoded-passwd>]
                                                        dummy 0 aabbccdd
                                user-passwd             <username> <server-id> [<encoded-passwd>]
                                                        Tom 0 [a1b2c3]
                                user-email              <username> <server-id> <email>
                                                        dummy 0 aaa@bbb.ccc
                                user-policy             <username> <server-id> <policy-name>
                                                        dummy 0 policy1
                                group                   <group-name> <server-id> <policy-name>
                                                        dummy_group 0 policy1
                                group-member            <group-name> <server-id> <user-name>
                                                        group1 1 user1
                                isolator-profile        <name> <download> <upload> <viewonly> <avscan> <image-quality> <video-frame-rate> <av-disarm> <right-click> <scroll-speed> <file-type>
                                                        profile1 100 200 Y Y normal normal Y Y 1 exe;doc
                                isolator-profile-download       <name> <download>
```



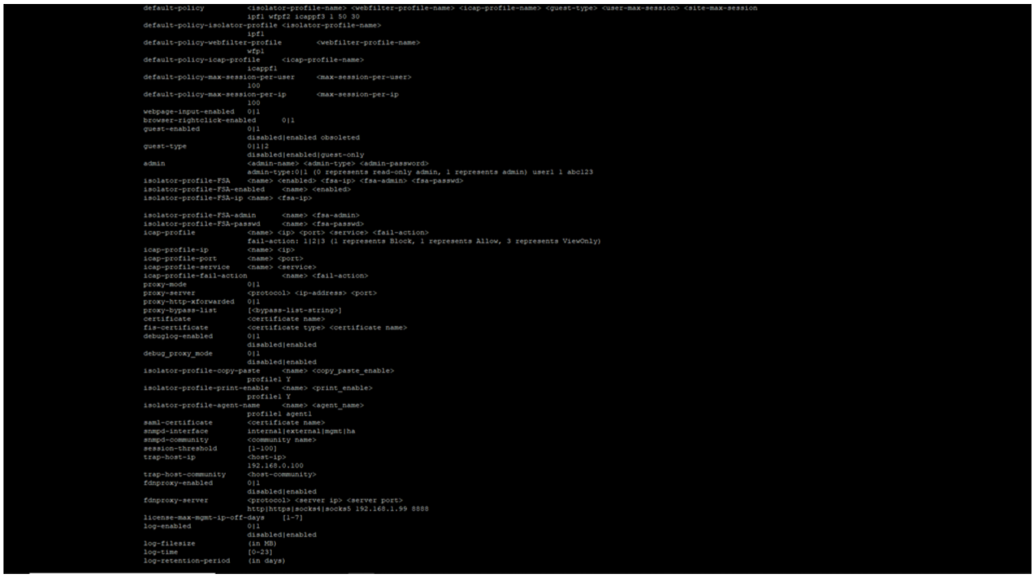
```
                                isolator-profile-download       <name> <download>
                                                        profile1 100
                                isolator-profile-upload <name> <upload>
                                                        profile1 200
                                isolator-profile-viewonly       <name> <viewonly>
                                                        profile1 Y
                                isolator-profile-avscan <name> <avscan>
                                                        profile1 Y
                                isolator-profile-avdisarm       <name> <avdisarm>
                                                        profile1 Y
                                isolator-profile-image-quality  <name> <image-quality>
                                                        profile1 normal
                                isolator-profile-video-frame-rate       <name> <video-frame-rate>
                                                        profile1 high
                                isolator-profile-right-click    <name> <right-click>
                                                        profile1 Y
                                isolator-profile-scroll-speed   <name> <scroll-speed>
                                                        profile1 [1-100]
                                isolator-profile-file-type      <name> <file-type>
                                                        profile1 exe;doc;pdf;ppt;xls
                                isolator-profile-certificate    <profile name> <certificate name>
                                                        profile1 cacert
                                wf-profile              <name> <white-list> <black-list> <actions>
                                                        wfp1 wlist1 blist1 actions1
                                wf-profile-whitelist    <name> <white-list>
                                                        wfp1 wlist1
                                wf-profile-blacklist    <name> <black-list>
                                                        wfp1 blist1
                                wf-profile-actions      <name> <actions>
                                                        wfp1 actions1
                                wf-white-list           <name> <url> <type>
                                                        wl1 dummy.com 0
                                wf-black-list           <name> <url> <type>
                                                        bl1 dummy.com 0
                                wf-group                <group id> <group name>
                                wf-category             <category-id> <category-name>
                                wf-action               <id>
                                wf-group-category       <id> <group-id> <category-id>
                                wf-category-action      <action-profile-id> <category-id> <action>
                                policy                  <policy-name> <isolator-profile-name> <webfilter-profile-name> <icap-profile-name> <max-session-per-user> <max-session-per-ip>
                                                        mypolicy1 ipf1 wfpf2 icappf3 50 30
                                policy-isolator-profile <policy-name> <isolator-profile-name>
                                                        mypolicy1 ipf1
                                policy-webfilter-profile        <policy-name> <webfilter-profile-name>
                                                        mypolicy1 wfp1
                                policy-icap-profile     <policy-name> <icap-profile-name>
                                                        mypolicy1 icappf1
                                policy-max-session-per-user     <policy-name> <max-session-per-user>
                                                        mypolicy1 100
                                policy-max-session-per-ip       <policy-name> <max-session-per-ip>
                                                        mypolicy1 100
                                default-policy          <isolator-profile-name> <webfilter-profile-name> <icap-profile-name> <guest-type> <user-max-session> <site-max-session
                                                        ipf1 wfpf2 icappf3 1 50 30

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

                                config                  (null)
                                internal-ip             <ip/netmask>
                                                        192.168.100.2/24
                                external-ip             <ip/netmask>
                                                        192.168.100.2/24
                                mgmt-ip                 <ip/netmask>
                                                        192.168.100.2/24
                                ha-ip                   <ip/netmask>
```



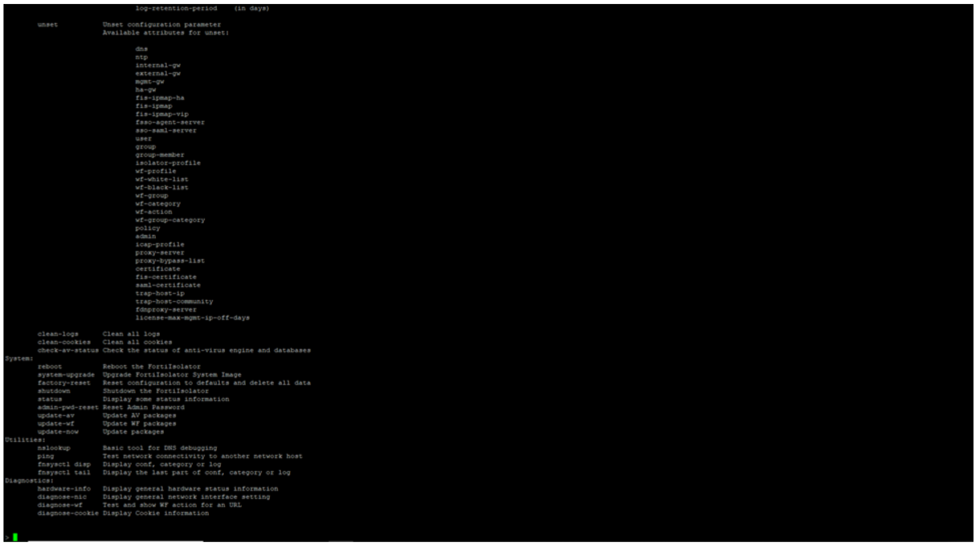
```
ha-ip                   <ip/netmask>
                        192.168.100.2/24
date                    <YYYY-MM-DD>
time                    <HH:MM:SS>
dns                     <primary DNS> [<secondary DNS>]
                        192.168.100.1 [192.168.10.1]
ntp                     <ntp ip>
                        192.168.100.1
internal-gw             <subnet> <gateway ip>
                        192.168.100.0/24 192.168.100.1
external-gw             <subnet> <gateway ip>
                        192.168.100.0/24 192.168.100.1
mgmt-gw                 <subnet> <gateway ip>
                        192.168.100.0/24 192.168.100.1
ha-gw                   <subnet> <gateway ip>
                        192.168.100.0/24 192.168.100.1
hostname                <hostname>
timezone                <timezone>
                        America/Los_Angeles
wf-enabled              [0|1]
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>
                        192.168.100.2/24
ha-password             (null)
ha-password-enc         <encoded password>
ha-interface            <Interface Name>
                        internal/external/mgmt/ha
fis-ipmap-ha            <priority> <external ip> <internal ip> <port_map_to_443> <port_map_to_8887>
                        0 192.168.100.1 10.1.0.1 12443 12887
fis-ipmap               <port_map_to_443> <port_map_to_8887> <external ip>
                        12443 12887 192.168.100.1
fis-ipmap-vip           <external ip> <port_map_to_443> <port_map_to_8887> <externalip>
                        192.168.122.1 14443 14887
fsso-agent-server       <id> <ipaddr> <port> <enabled>
                        1 192.168.1.99 1234 Y
fsso-agent-server-ipaddr        <id> <ipaddr>
                        1 192.168.1.99
fsso-agent-server-port  <id> <port>
                        1 12345
fsso-agent-server-passwd        <id>
                        1
fsso-agent-server-enabled       <id> <enabled>
                        1 Y
sso-saml-server         <server-id> <id-url> <signon-url> <logout-url> <enabled>
                        1 http://10.0.0.7/saml-idp/0 http://10.0.0.7/saml-idp/1 http://10.0.0.7/saml-idp/2 Y
sso-saml-id-url         <server-id> <id-url>
                        1 http://10.0.0.7/saml-idp/0
sso-saml-signon-url     <server-id> <signon-url>
                        1 http://10.0.0.7/saml-idp/1
sso-saml-logout-url     <server-id> <logout-url>
                        1 http://10.0.0.7/saml-idp/2
sso-saml-idp-enabled    <id> <enabled>
                        1 Y
sso-saml-certificate    <server-id> <certificate-name>
                        1 certificate
user                    <username> <server-id> [<encoded-passwd>]
```



```
user                    <username> <server-id> [<encoded-passwd>]
                        dummy 0 aabbccdd
user-passwd             <username> <server-id> [<encoded-passwd>]
                        Tom 0 [a1b2c3]
user-email              <username> <server-id> <email>
                        dummy 0 aaa@bbb.ccc
user-policy             <username> <server-id> <policy-name>
                        dummy 0 policy1
group                   <group-name> <server-id> <policy-name>
                        dummy_group 0 policy1
group-member            <group-name> <server-id> <user-name>
                        group1 1 user1
isolator-profile        <name> <download> <upload> <viewonly> <avscan> <image-quality> <video-frame-rate> <av-disarm> <right-click> <scroll-speed> <file-type>
                        profile1 100 200 Y Y normal normal Y Y 1 exe;doc
isolator-profile-download       <name> <download>
                        profile1 100
isolator-profile-upload <name> <upload>
                        profile1 200
isolator-profile-viewonly       <name> <viewonly>
                        profile1 Y
isolator-profile-avscan <name> <avscan>
                        profile1 Y
isolator-profile-avdisarm       <name> <avdisarm>
                        profile1 Y
isolator-profile-image-quality  <name> <image-quality>
                        profile1 normal
isolator-profile-video-frame-rate       <name> <video-frame-rate>
                        profile1 high
isolator-profile-right-click    <name> <right-click>
                        profile1 Y
isolator-profile-scroll-speed   <name> <scroll-speed>
                        profile1 [1-100]
isolator-profile-file-type      <name> <file-type>
                        profile1 exe;doc;pdf;ppt;xls
isolator-profile-certificate    <profile name> <certificate name>
                        profile1 cacert
wf-profile              <name> <white-list> <black-list> <actions>
                        wfp1 wlist1 blist1 actions1
wf-profile-whitelist    <name> <white-list>
                        wfp1 wlist1
wf-profile-blacklist    <name> <black-list>
                        wfp1 blist1
wf-profile-actions      <name> <actions>
                        wfp1 actions1
wf-white-list           <name> <url> <type>
                        wl1 dummy.com 0
wf-black-list           <name> <url> <type>
                        bl1 dummy.com 0
wf-group                <group id> <group name>
wf-category             <category-id> <category-name>
wf-action               <id>
wf-group-category       <id> <group-id> <category-id>
wf-category-action      <action-profile-id> <category-id> <action>
policy                  <policy-name> <isolator-profile-name> <webfilter-profile-name> <icap-profile-name> <max-session-per-user> <max-session-per-ip>
                        mypolicy1 ipf1 wfpf2 icappf3 50 30
policy-isolator-profile <policy-name> <isolator-profile-name>
                        mypolicy1 ipf1
policy-webfilter-profile        <policy-name> <webfilter-profile-name>
                        mypolicy1 wfp1
policy-icap-profile     <policy-name> <icap-profile-name>
                        mypolicy1 icappf1
policy-max-session-per-user     <policy-name> <max-session-per-user>
                        mypolicy1 100
policy-max-session-per-ip       <policy-name> <max-session-per-ip>
                        mypolicy1 100
default-policy          <isolator-profile-name> <webfilter-profile-name> <icap-profile-name> <guest-type> <user-max-session> <site-max-session
```



```
default-policy          <isolator-profile-name> <webfilter-profile-name> <icap-profile-name> <guest-type> <user-max-session> <site-max-session
                        ipf1 wfpf2 icappf3 1 50 30
default-policy-isolator-profile <isolator-profile-name>
                        ipf1
default-policy-webfilter-profile        <webfilter-profile-name>
                        wfp1
default-policy-icap-profile     <icap-profile-name>
                        icappf1
default-policy-max-session-per-user     <max-session-per-user>
                        100
default-policy-max-session-per-ip       <max-session-per-ip
                        100
webpage-input-enabled   0|1
browser-rightclick-enabled      0|1
guest-enabled           0|1
                        disabled|enabled obsoleted
guest-type              0|1|2
                        disabled|enabled|guest-only
admin                   <admin-name> <admin-type> <admin-password>
                        admin-type:0|1 (0 represents read-only admin, 1 represents admin) user1 1 abc123
isolator-profile-FSA    <name> <enabled> <fsa-ip> <fsa-admin> <fsa-passwd>
isolator-profile-FSA-enabled    <name> <enabled>
isolator-profile-FSA-ip <name> <fsa-ip>

isolator-profile-FSA-admin      <name> <fsa-admin>
isolator-profile-FSA-passwd     <name> <fsa-passwd>
icap-profile            <name> <ip> <port> <service> <fail-action>
                        fail-action: 1|2|3 (1 represents Block, 1 represents Allow, 3 represents ViewOnly)
icap-profile-ip         <name> <ip>
icap-profile-port       <name> <port>
icap-profile-service    <name> <service>
icap-profile-fail-action        <name> <fail-action>
proxy-mode              0|1
proxy-server            <protocol> <ip-address> <port>
proxy-http-xforwarded   0|1
proxy-bypass-list       [<bypass-list-string>]
certificate             <certificate name>
fis-certificate         <certificate type> <certificate name>
debuglog-enabled        0|1
                        disabled|enabled
debug_proxy_mode        0|1
                        disabled|enabled
isolator-profile-copy-paste     <name> <copy_paste_enable>
                        profile1 Y
isolator-profile-print-enable   <name> <print_enable>
                        profile1 Y
isolator-profile-agent-name     <name> <agent_name>
                        profile1 agent1
saml-certificate        <certificate name>
snmpd-interface         internal|external|mgmt|ha
snmpd-community         <community name>
session-threshold       [1-100]
trap-host-ip            <host-ip>
                        192.168.0.100
trap-host-community     <host-community>
fdnproxy-enabled        0|1
                        disabled|enabled
fdnproxy-server         <protocol> <server ip> <server port>
                        http|https|socks4|socks5 192.168.1.99 8888
license-max-mgmt-ip-off-days    [1-7]
log-enabled             0|1
                        disabled|enabled
log-filesize            (in MB)
log-time                [0-23]
log-retention-period    (in days)
```



```
                log-retention-period    (in days)

        unset           Unset configuration parameter
                        Available attributes for unset:

                                dns
                                ntp
                                internal-gw
                                external-gw
                                mgmt-gw
                                ha-gw
                                fis-ipmap-ha
                                fis-ipmap
                                fis-ipmap-vip
                                fsso-agent-server
                                sso-saml-server
                                user
                                group
                                group-member
                                isolator-profile
                                wf-profile
                                wf-white-list
                                wf-black-list
                                wf-group
                                wf-category
                                wf-action
                                wf-group-category
                                policy
                                admin
                                icap-profile
                                proxy-server
                                proxy-bypass-list
                                certificate
                                fis-certificate
                                saml-certificate
                                trap-host-ip
                                trap-host-community
                                fdnproxy-server
                                license-max-mgmt-ip-off-days

        clean-logs      Clean all logs
        clean-cookies   Clean all cookies
        check-av-status Check the status of anti-virus engine and databases
System:
        reboot          Reboot the FortiIsolator
        system-upgrade  Upgrade FortiIsolator System Image
        factory-reset   Reset configuration to defaults and delete all data
        shutdown        Shutdown the FortiIsolator
        status          Display some status information
        admin-pwd-reset Reset Admin Password
        update-av       Update AV packages
        update-wf       Update WF packages
        update-now      Update packages
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
        diagnose-cookie Display Cookie information


>
```

FortiIsolator VM installation

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

- Installing FortiIsolator VM for Linux KVM on page 18
- Installing FortiIsolator VM for VMware vSphere on page 24
- Installing FortiIsolator VM for VMware ESXi on page 33
- Installing FortiIsolator VM for Microsoft Hyper-V on page 38
- Installing FortiIsolator VM for AWS on page 46

Installing FortiIsolator VM for Linux KVM

Use this procedure to install FortiIsolator VM for Linux KVM.

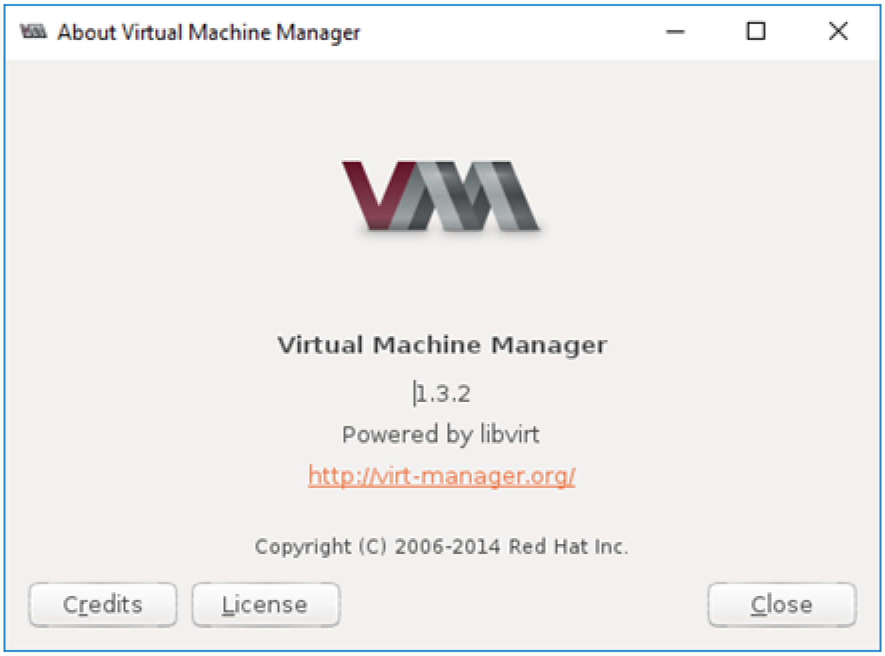
FortiIsolator VM for Linux KVM supports both Video Graphics Array (VGA) and virtual serial console connections.

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 FortiIsolator firmware for KVM by following the instructions in Downloading FortiIsolator firmware on page 11.
2. Launch KVM with Virtual Machine Manager (https://virt-manager.org/).



About Virtual Machine Manager

Virtual Machine Manager

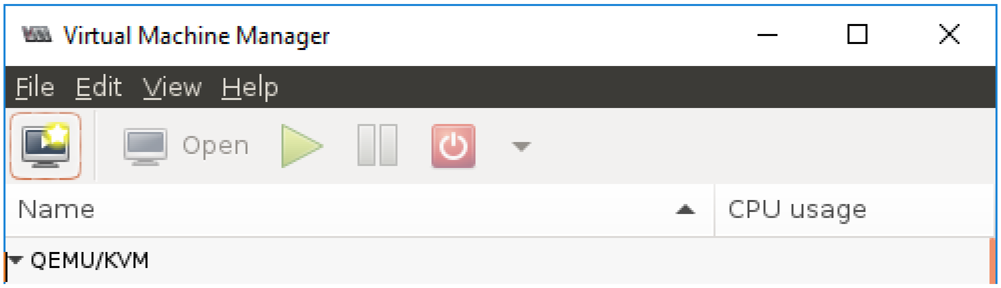
1.3.2

Powered by libvirt

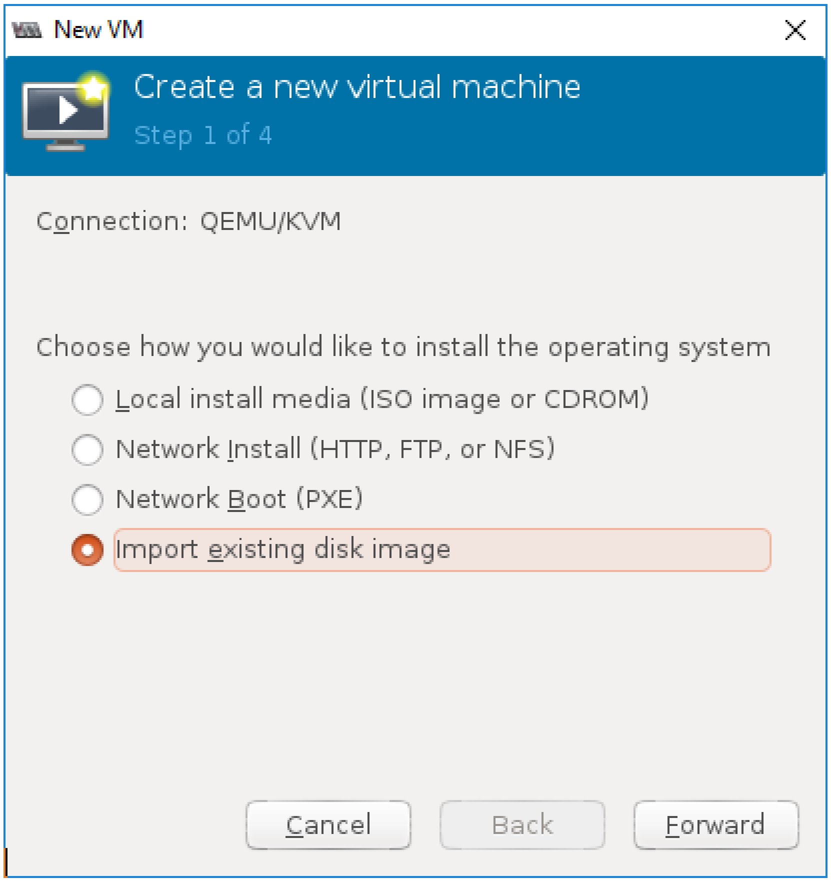
http://virt-manager.org/

Copyright (C) 2006-2014 Red Hat Inc.

3. Create a new virtual machine.



4. Select *Import existing disk image*.

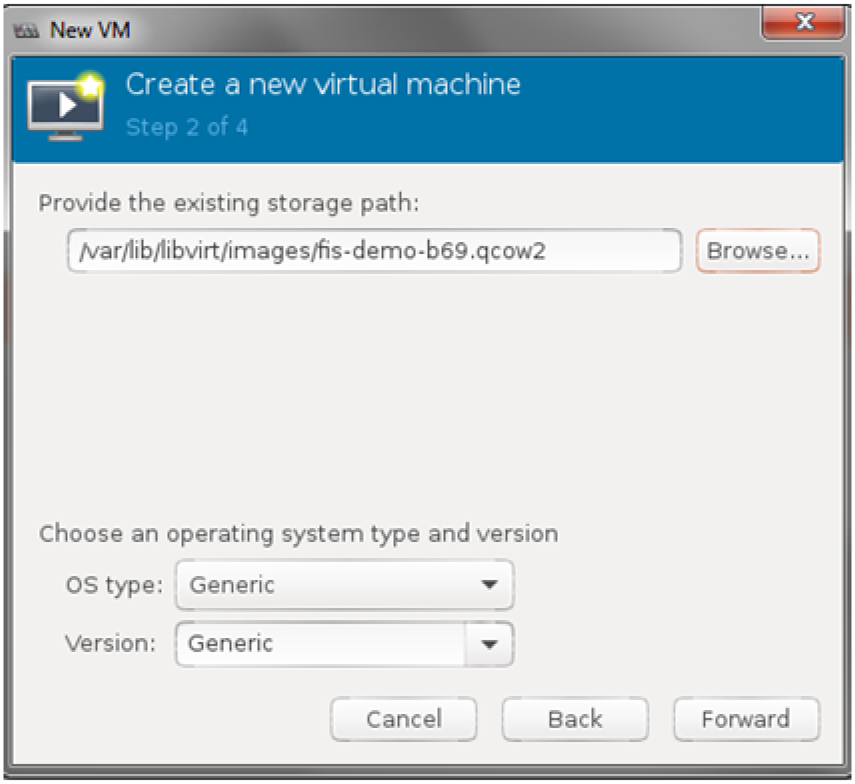


Connection: QEMU/KVM

Choose how you would like to install the operating system

○ Local install media (ISO image or CDROM)
○ Network Install (HTTP, FTP, or NFS)
○ Network Boot (PXE)
● Import existing disk image

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



New VM

Create a new virtual machine

Step 2 of 4

Provide the existing storage path:

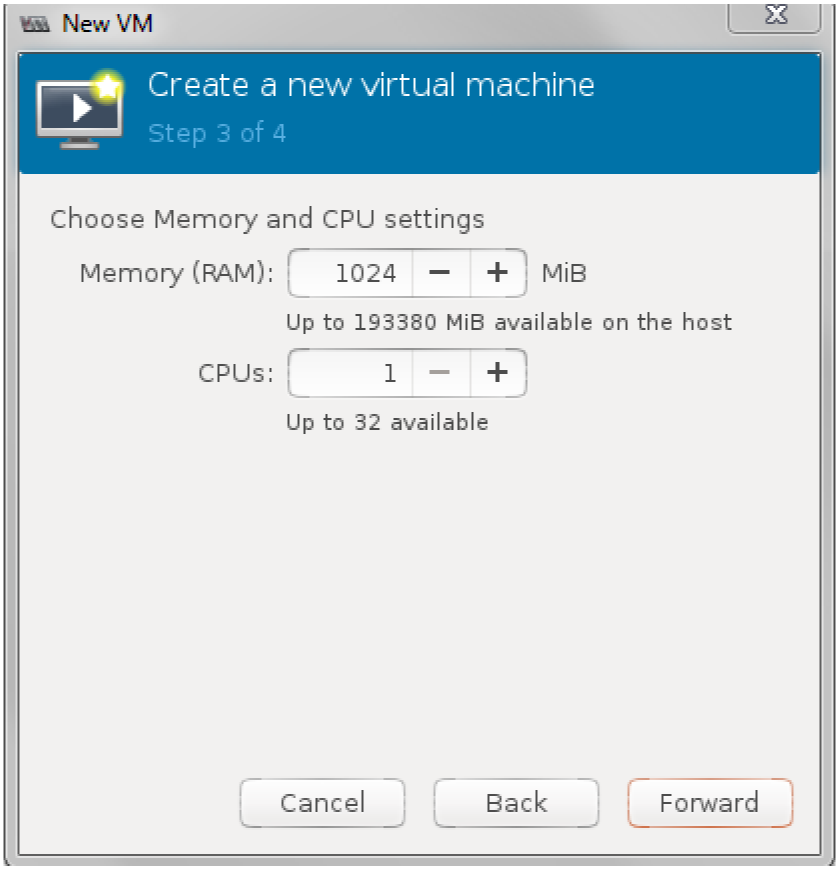
/var/lib/libvirt/images/fis-demo-b69.qcow2

Choose an operating system type and version

OS type: Generic

Version: Generic

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



Create a new virtual machine

Step 3 of 4

Choose Memory and CPU settings

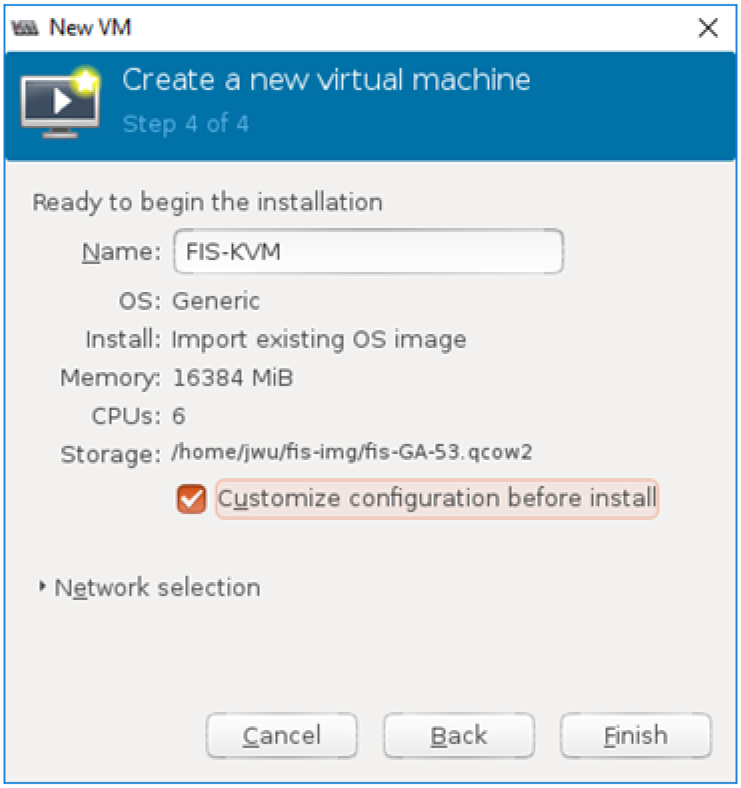
Memory (RAM): 1024 MiB

Up to 193380 MiB available on the host

CPUs: 1

Up to 32 available

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



Ready to begin the installation

Name: FIS-KVM

OS: Generic

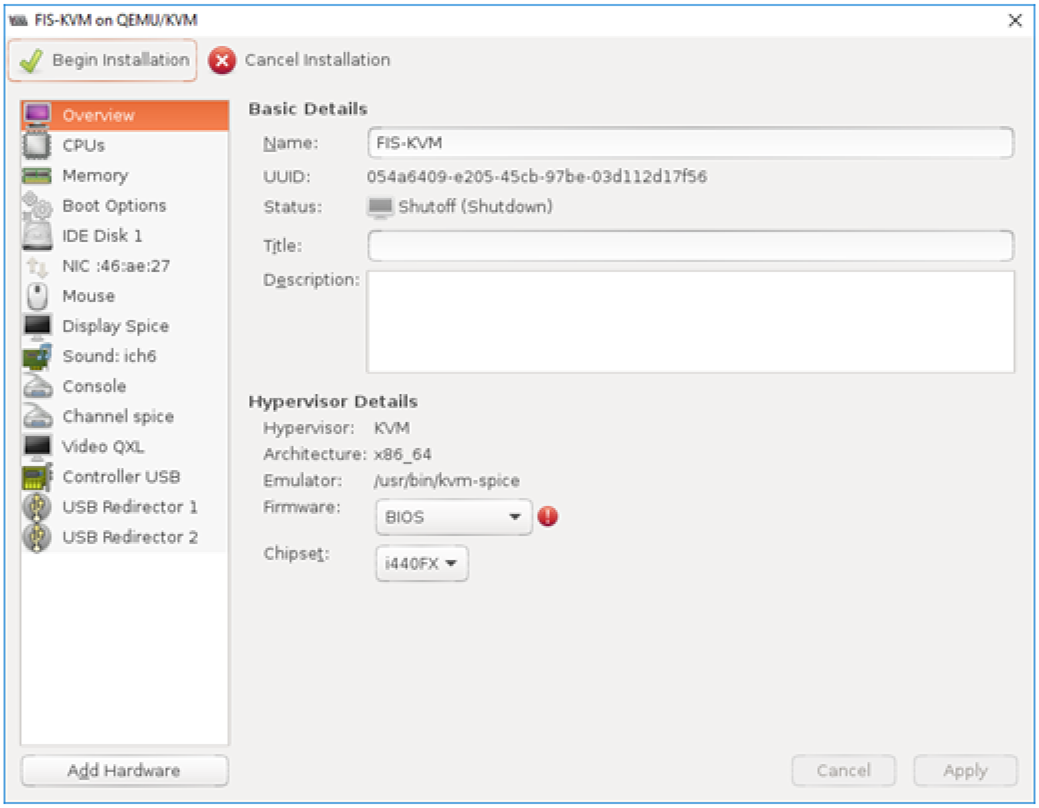
Install: Import existing OS image

Memory: 16384 MiB

CPUs: 6

Storage: /home/jwu/fis-img/fis-GA-53.qcow2

☑ Customize configuration before install



Basic Details

Name: FIS-KVM

UUID: 054a6409-e205-45cb-97be-03d112d17f56

Status: Shutoff (Shutdown)

Title:

Description:

Hypervisor Details

Hypervisor: KVM

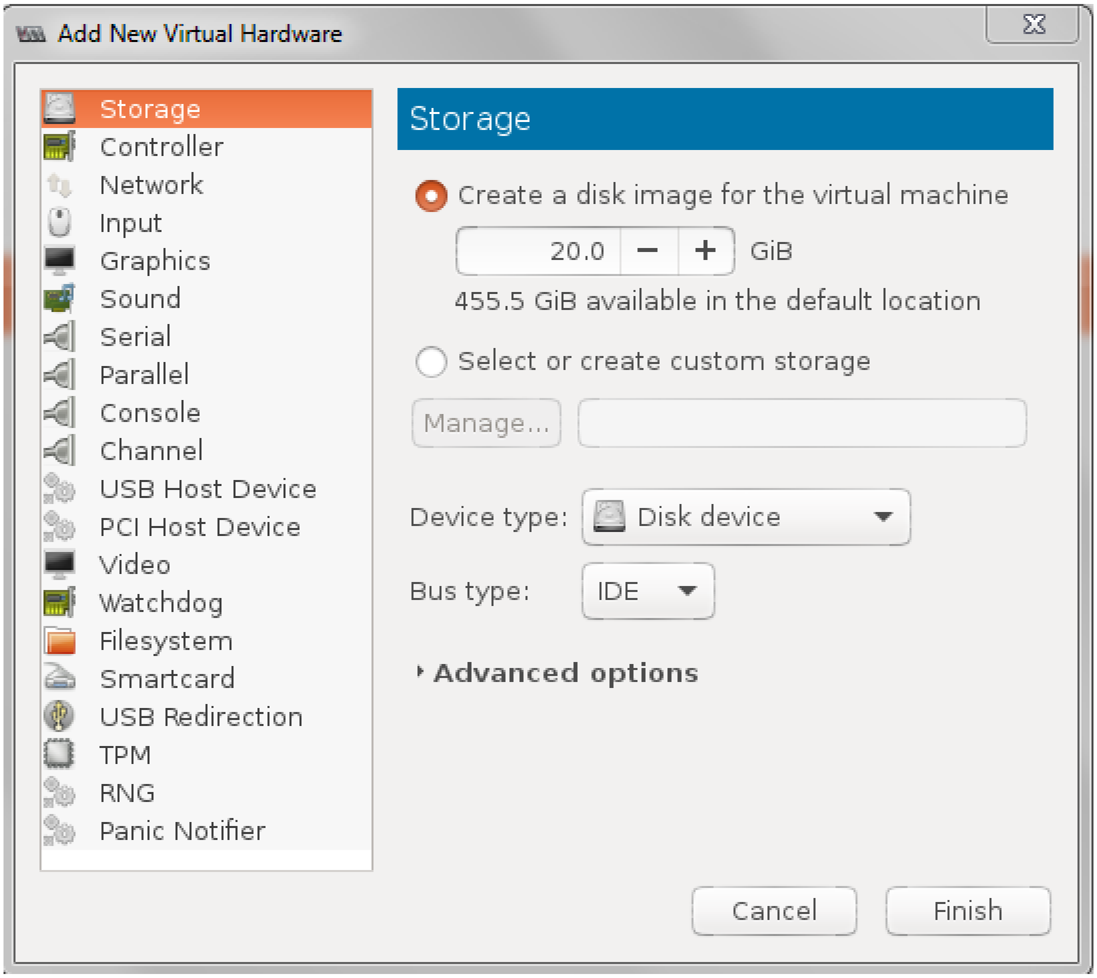
Architecture: x86_64

Emulator: /usr/bin/kvm-spice

Firmware: BIOS

Chipset: i440FX

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



Storage

● Create a disk image for the virtual machine

20.0 GiB

455.5 GiB available in the default location

○ Select or create custom storage

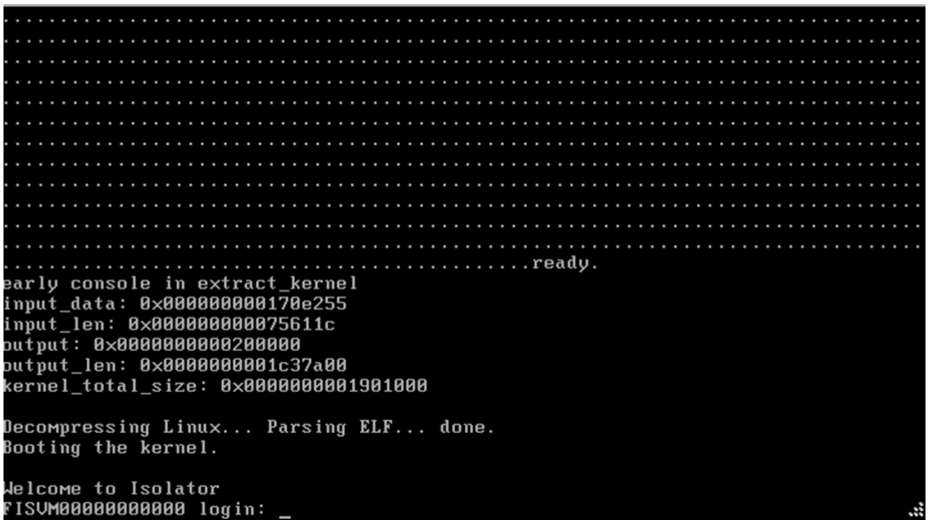
Device type: Disk device

Bus type: IDE

It is recommended to allocate enough system resources to the FortiIsolator VM. The suggested baseline is to have 8 virtual CPUs, 4 virtual NICs, 20 GB virtual machine storage, and 24 GB virtual machine memory.

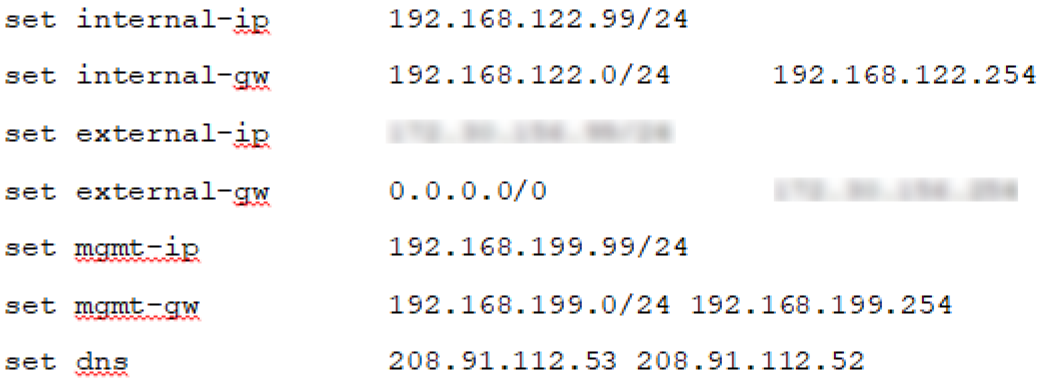
9. Add three network interfaces and configure them accordingly.
   - Network 1: Internal Interface
   - Network 2: External Interface
   - Network 3: Management Interface
   - Network 4: HA Interface

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



```
...............................................................................
...............................................................................
...............................................................................
...............................................................................
...............................................................................
...............................................................................
...............................................................................
...............................................................................
...............................................................................
...............................................................................
...............................................................................
...............................................................................
.............................................ready.
early console in extract_kernel
input_data: 0x000000000170e255
input_len: 0x000000000075611c
output: 0x0000000000200000
output_len: 0x0000000001c37a00
kernel_total_size: 0x0000000001901000

Decompressing Linux... Parsing ELF... done.
Booting the kernel.

Welcome to Isolator
FISVM000000000000 login: _
```

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        [redacted]
set external-gw        0.0.0.0/0             [redacted]
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 FortiIsolator VM for VMware vSphere

Use this procedure to install FortiIsolator VM for VMware vSphere.

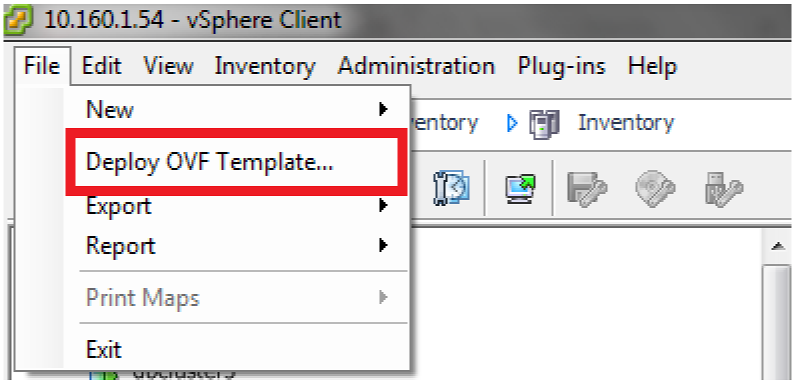
Prerequisites

- 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

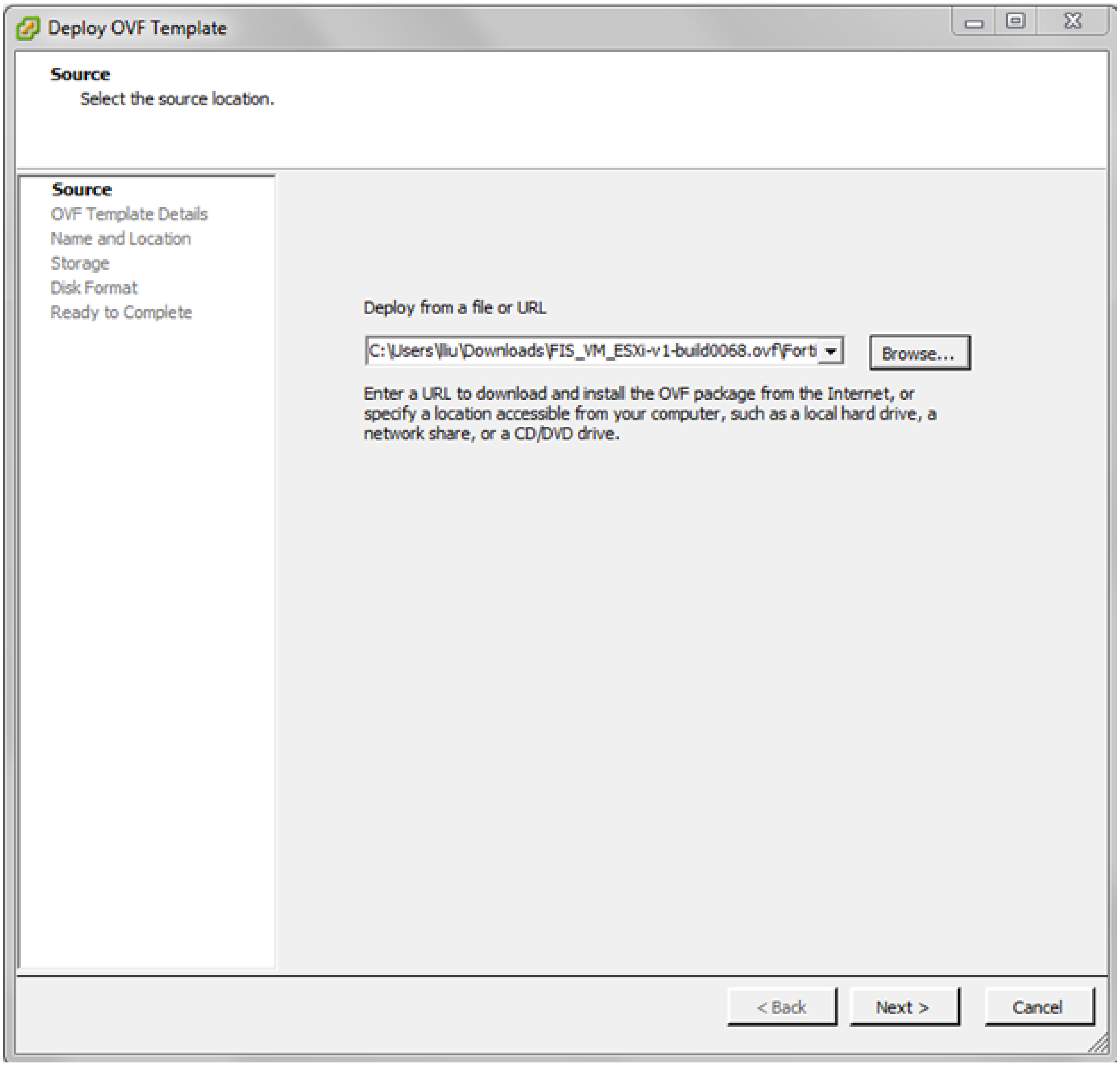
Steps

1. Download the FortiIsolator firmware for VMware by following the instructions in Downloading FortiIsolator firmware on page 11.

2. To create a new virtual machine, in vSphere Client, select *File* > *Deploy OVF Template*.



3. Browse to the folder that contains the FortiIsolator files and select `FortiIsolator.ovf`.



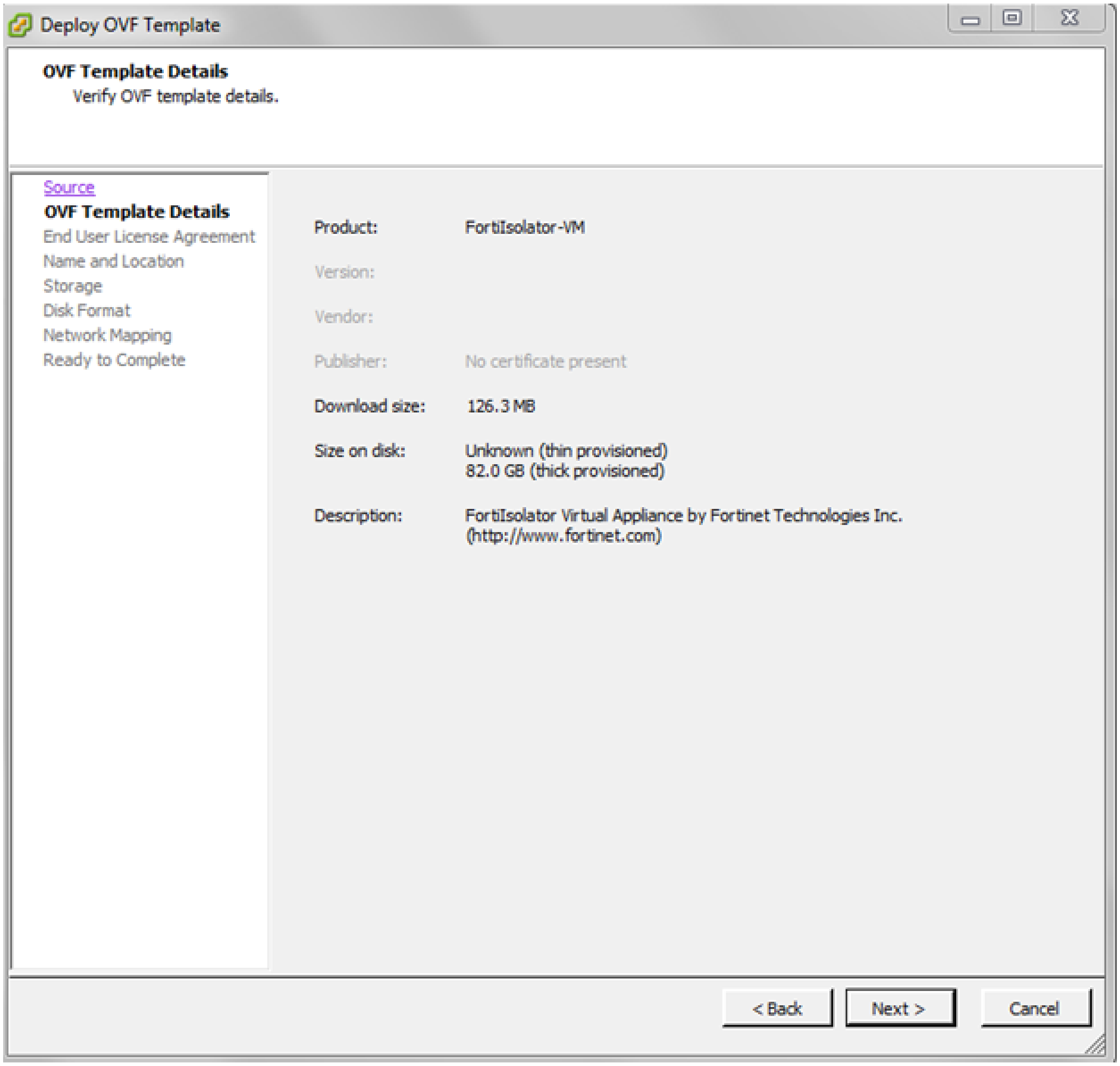
Select the source location.

Deploy from a file or URL

C:\Users\lliu\Downloads\FIS_VM_ESXi-v1-build0068.ovf\Forti

Enter a URL to download and install the OVF package from the Internet, or specify a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

4. Verify the OVF template details.



Deploy OVF Template

OVF Template Details

Verify OVF template details.

Product: FortiIsolator-VM

Version:

Vendor:

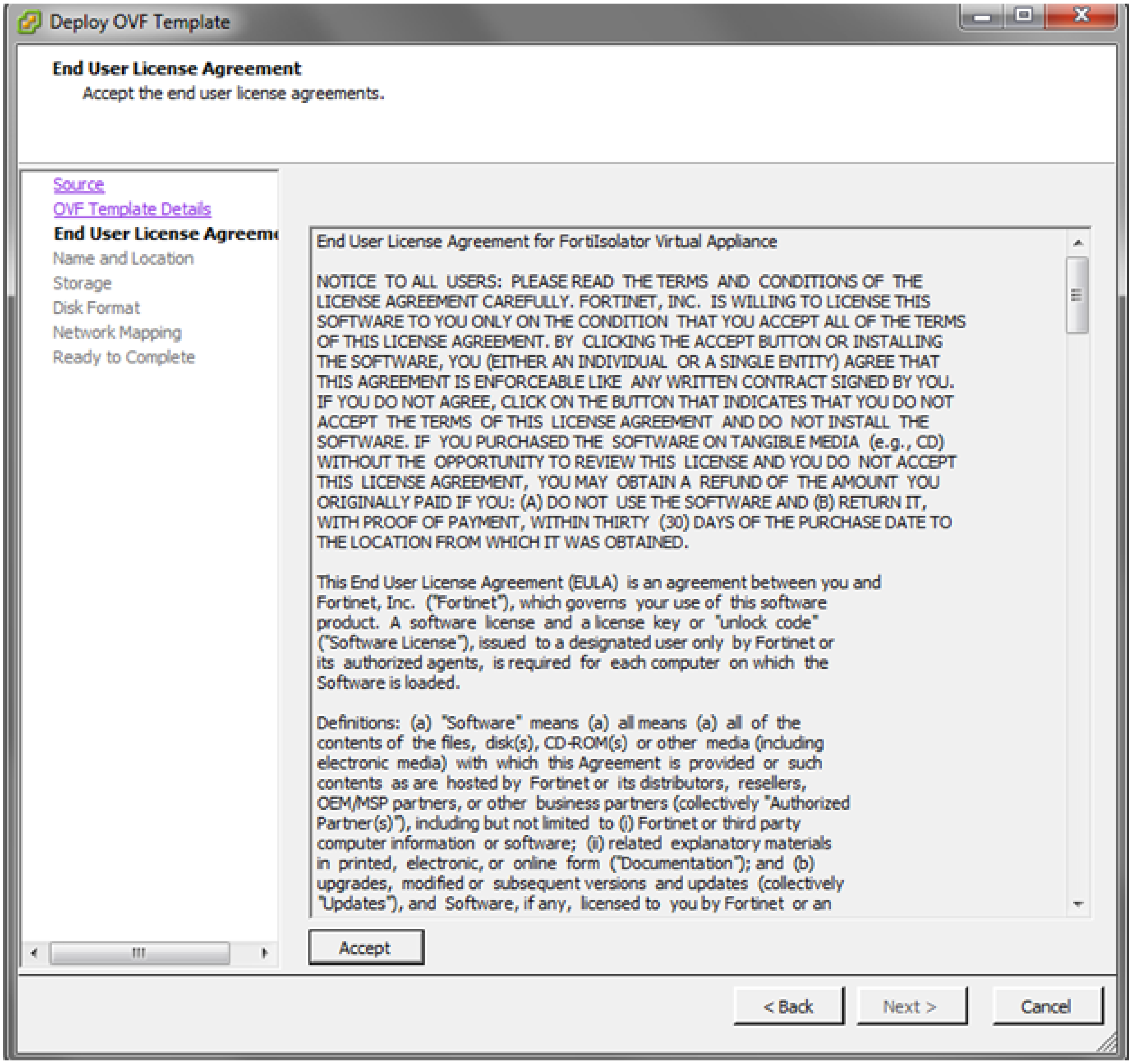
Publisher: No certificate present

Download size: 126.3 MB

Size on disk: Unknown (thin provisioned)
82.0 GB (thick provisioned)

Description: FortiIsolator Virtual Appliance by Fortinet Technologies Inc. (http://www.fortinet.com)

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



End User License Agreement

Accept the end user license agreements.

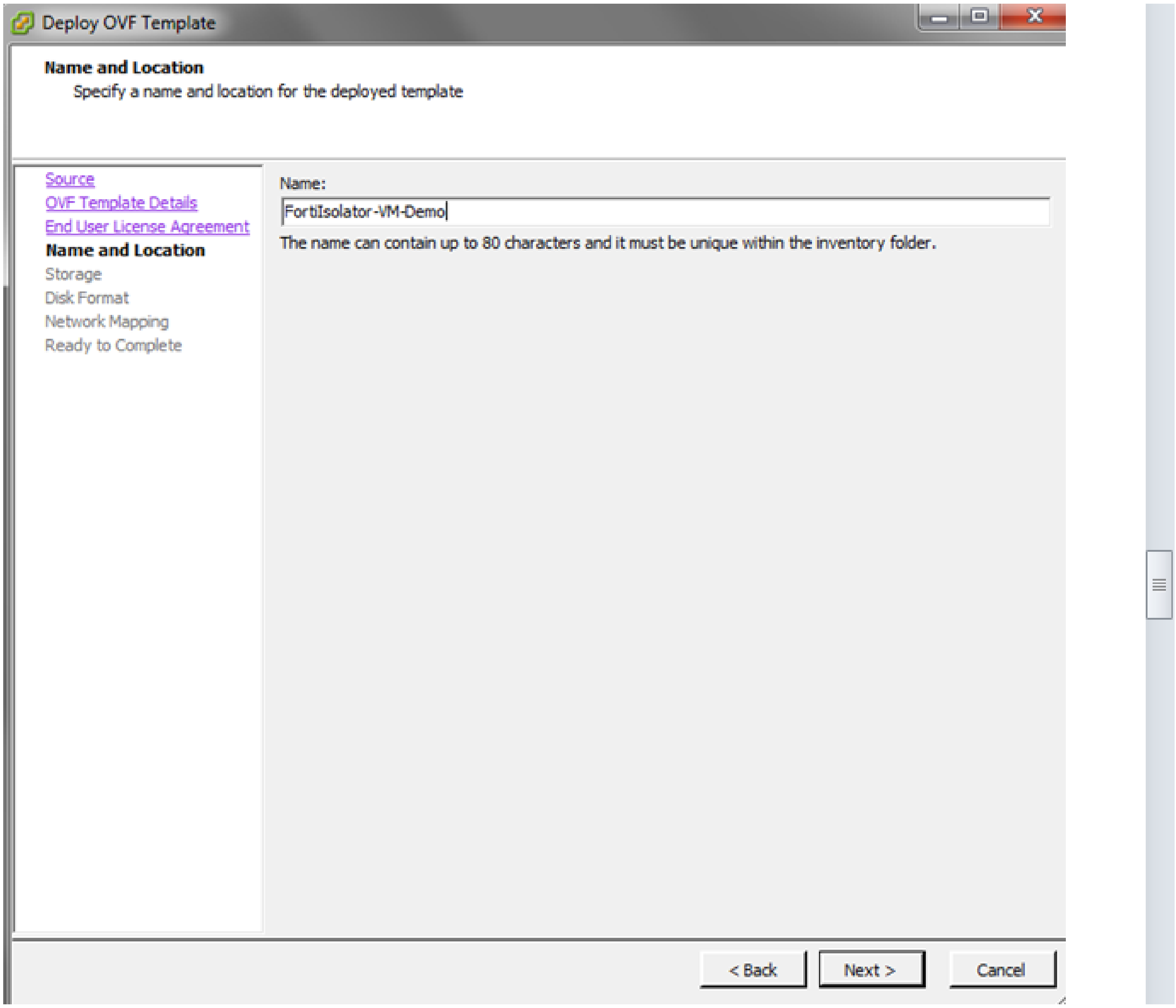
End User License Agreement for FortiIsolator Virtual Appliance

NOTICE TO ALL USERS: PLEASE READ THE TERMS AND CONDITIONS OF THE LICENSE AGREEMENT CAREFULLY. FORTINET, INC. IS WILLING TO LICENSE THIS SOFTWARE TO YOU ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS OF THIS LICENSE AGREEMENT. BY CLICKING THE ACCEPT BUTTON OR INSTALLING THE SOFTWARE, YOU (EITHER AN INDIVIDUAL OR A SINGLE ENTITY) AGREE THAT THIS AGREEMENT IS ENFORCEABLE LIKE ANY WRITTEN CONTRACT SIGNED BY YOU. IF YOU DO NOT AGREE, CLICK ON THE BUTTON THAT INDICATES THAT YOU DO NOT ACCEPT THE TERMS OF THIS LICENSE AGREEMENT AND DO NOT INSTALL THE SOFTWARE. IF YOU PURCHASED THE SOFTWARE ON TANGIBLE MEDIA (e.g., CD) WITHOUT THE OPPORTUNITY TO REVIEW THIS LICENSE AND YOU DO NOT ACCEPT THIS LICENSE AGREEMENT, YOU MAY OBTAIN A REFUND OF THE AMOUNT YOU ORIGINALLY PAID IF YOU: (A) DO NOT USE THE SOFTWARE AND (B) RETURN IT, WITH PROOF OF PAYMENT, WITHIN THIRTY (30) DAYS OF THE PURCHASE DATE TO THE LOCATION FROM WHICH IT WAS OBTAINED.

This End User License Agreement (EULA) is an agreement between you and Fortinet, Inc. ("Fortinet"), which governs your use of this software product. A software license and a license key or "unlock code" ("Software License"), issued to a designated user only by Fortinet or its authorized agents, is required for each computer on which the Software is loaded.

Definitions: (a) "Software" means (a) all means (a) all of the contents of the files, disk(s), CD-ROM(s) or other media (including electronic media) with which this Agreement is provided or such contents as are hosted by Fortinet or its distributors, resellers, OEM/MSP partners, or other business partners (collectively "Authorized Partner(s)"), including but not limited to (i) Fortinet or third party computer information or software; (ii) related explanatory materials in printed, electronic, or online form ("Documentation"); and (b) upgrades, modified or subsequent versions and updates (collectively "Updates"), and Software, if any, licensed to you by Fortinet or an

6. Name the new FortiIsolator virtual machine.



Deploy OVF Template

Name and Location

Specify a name and location for the deployed template

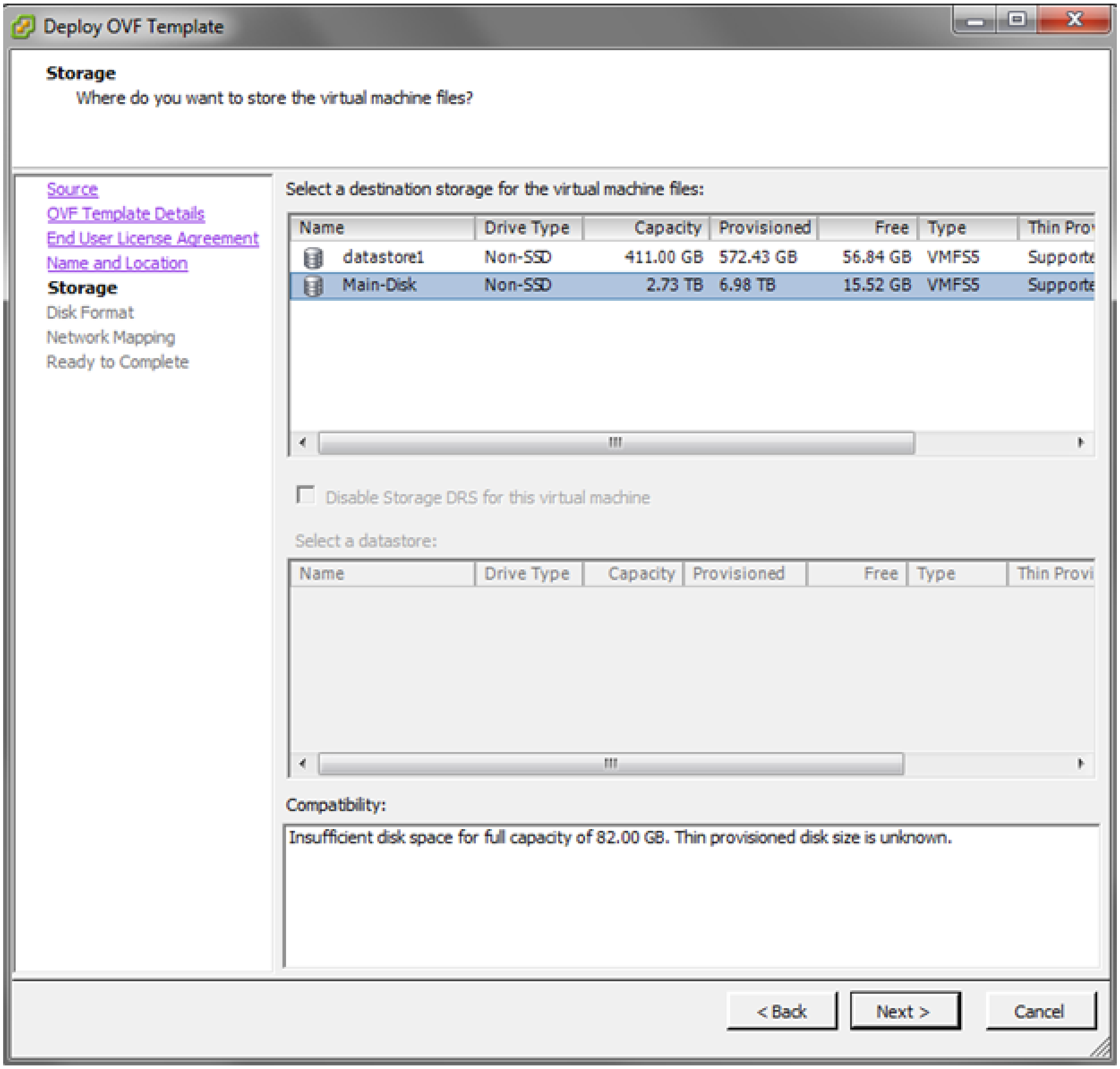
Source
OVF Template Details
End User License Agreement
Name and Location
Storage
Disk Format
Network Mapping
Ready to Complete

Name:

FortiIsolator-VM-Demo

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

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



Storage

Where do you want to store the virtual machine files?

Select a destination storage for the virtual machine files:

Name	Drive Type	Capacity	Provisioned	Free	Type	Thin Pro
datastore1	Non-SSD	411.00 GB	572.43 GB	56.84 GB	VMFS5	Supporte
Main-Disk	Non-SSD	2.73 TB	6.98 TB	15.52 GB	VMFS5	Supporte

□ Disable Storage DRS for this virtual machine

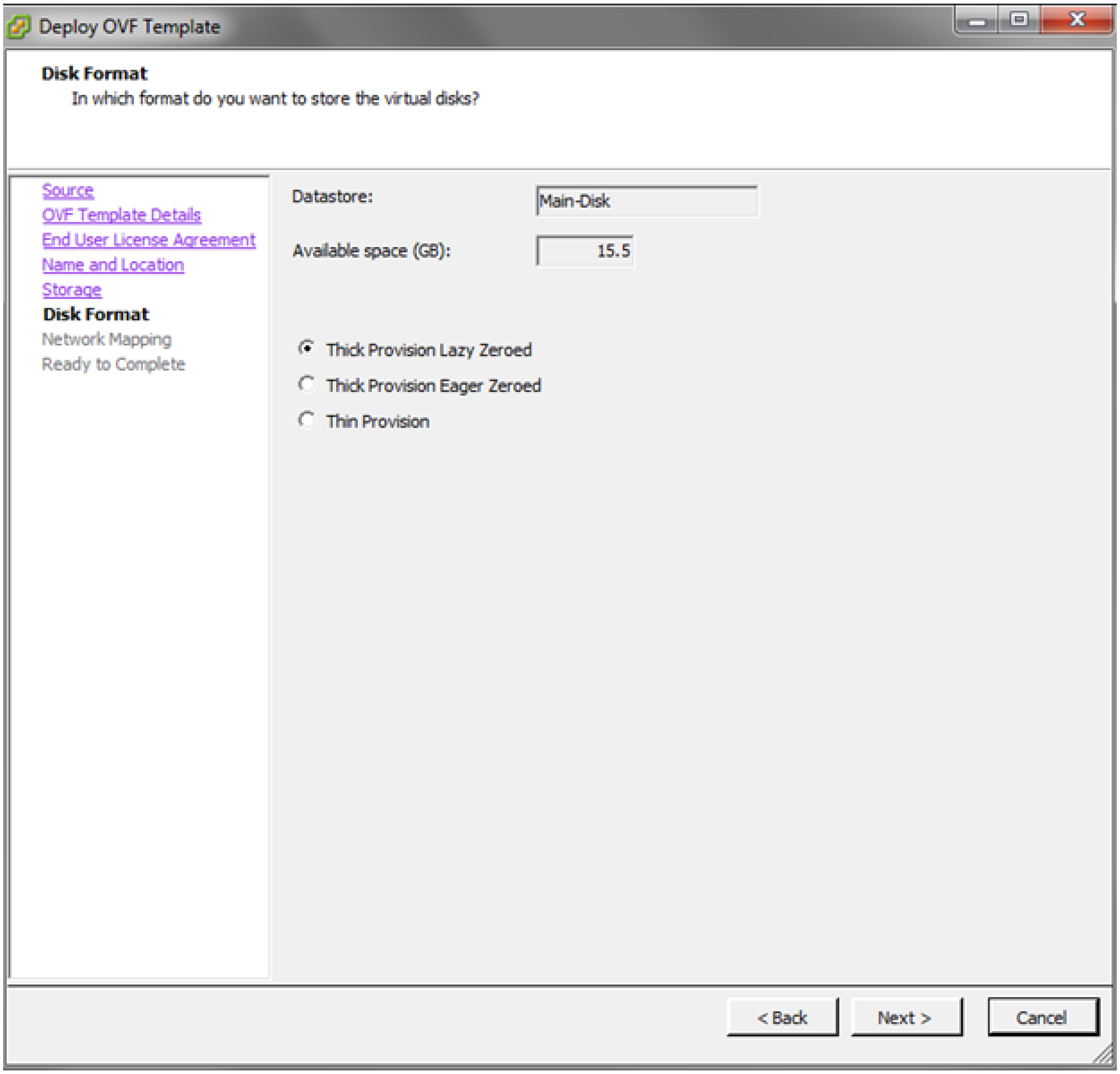
Select a datastore:

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.

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



Deploy OVF Template

Disk Format

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

Datastore: Main-Disk

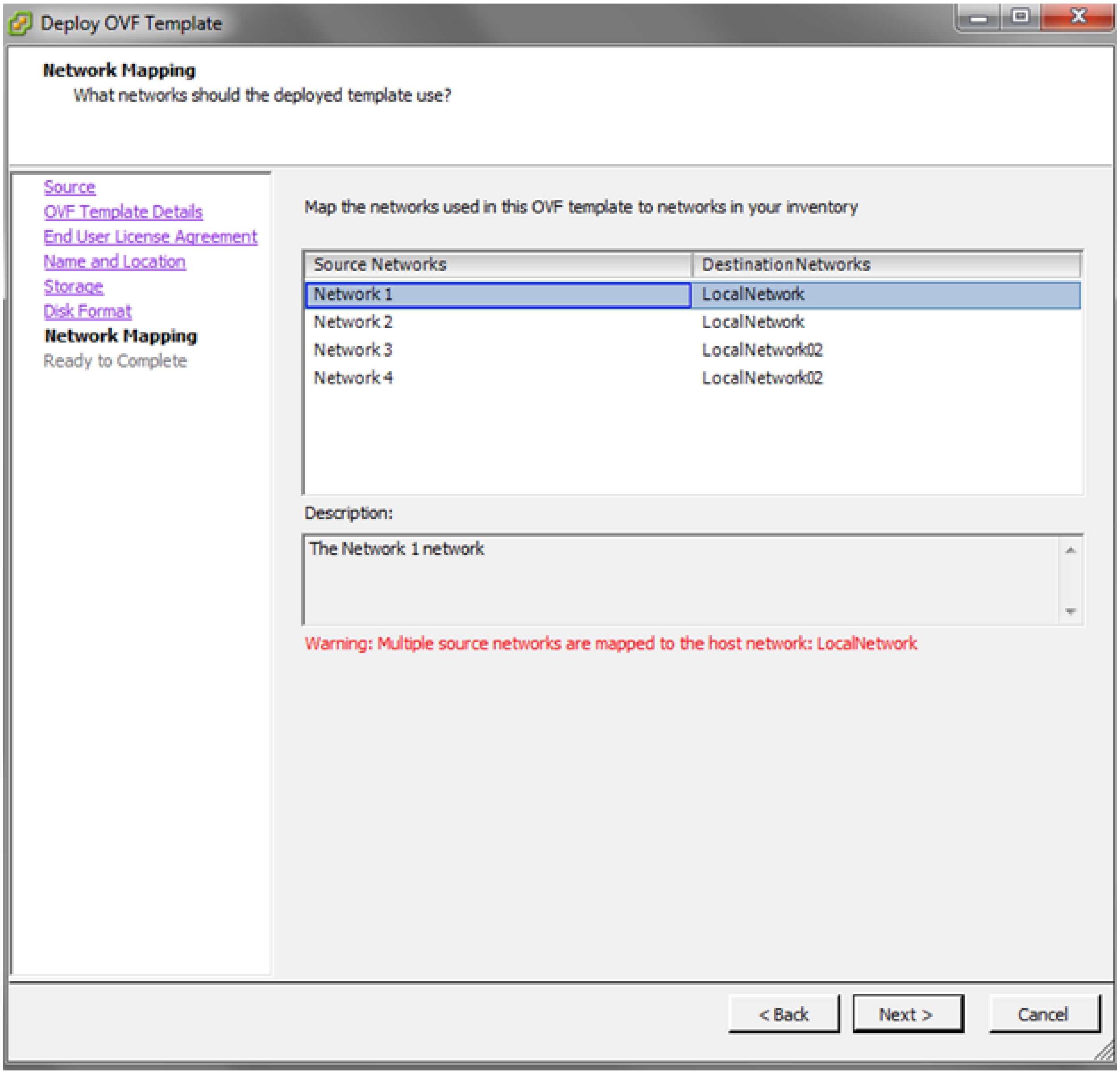
Available space (GB): 15.5

● Thick Provision Lazy Zeroed

○ Thick Provision Eager Zeroed

○ Thin Provision

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



Deploy OVF Template

Network Mapping

What networks should the deployed template use?

Map the networks used in this OVF template to networks in your inventory

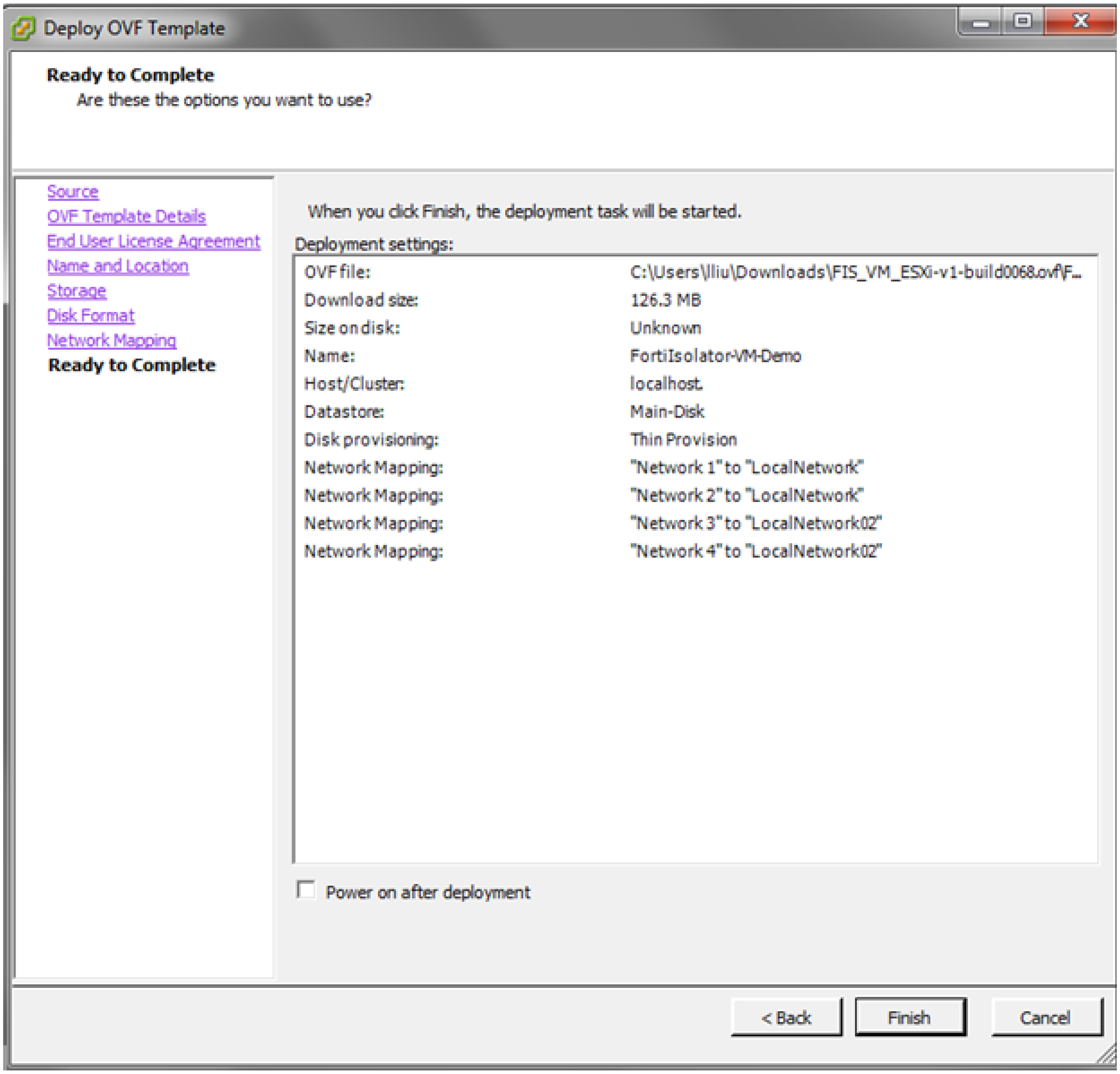
Source Networks	DestinationNetworks
Network 1	LocalNetwork
Network 2	LocalNetwork
Network 3	LocalNetwork02
Network 4	LocalNetwork02

Description:

The Network 1 network

Warning: Multiple source networks are mapped to the host network: LocalNetwork

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



Ready to Complete

Are these the options you want to use?

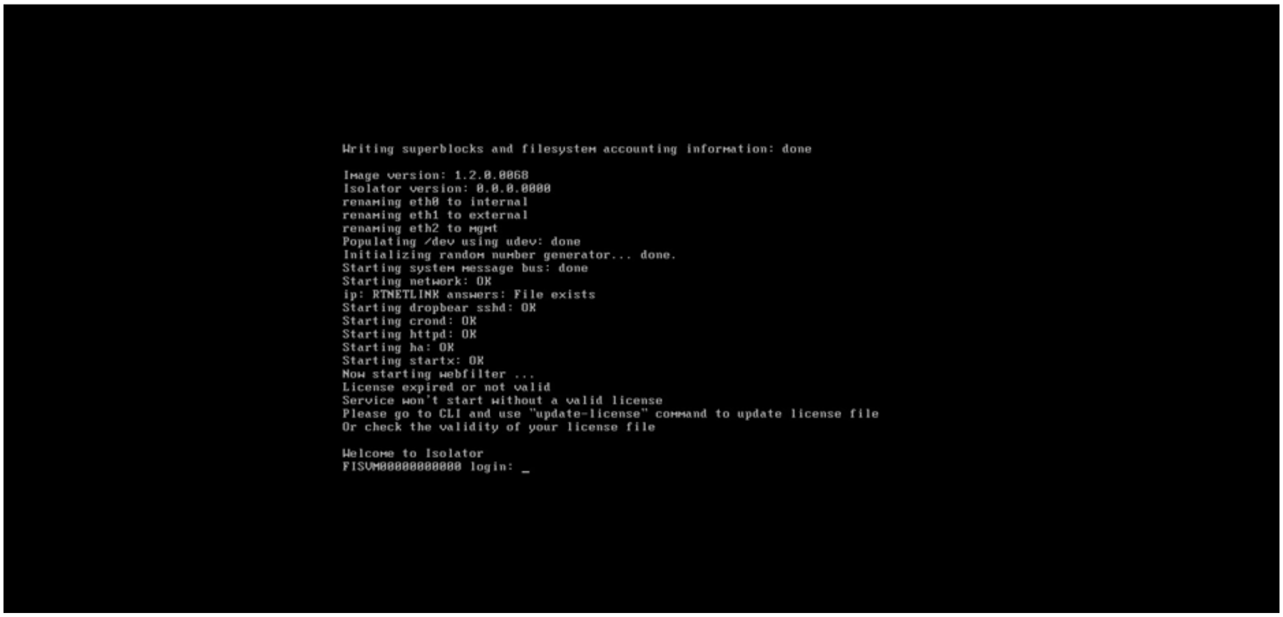
When you click Finish, the deployment task will be started.

Deployment settings:

OVF file:	C:\Users\lliu\Downloads\FIS_VM_ESXi-v1-build0068.ovf\F...
Download size:	126.3 MB
Size on disk:	Unknown
Name:	FortiIsolator-VM-Demo
Host/Cluster:	localhost.
Datastore:	Main-Disk
Disk provisioning:	Thin Provision
Network Mapping:	"Network 1" to "LocalNetwork"
Network Mapping:	"Network 2" to "LocalNetwork"
Network Mapping:	"Network 3" to "LocalNetwork02"
Network Mapping:	"Network 4" to "LocalNetwork02"

☐ Power on after deployment

11. Start the FortiIsolator VM.



```
Writing superblocks and filesystem accounting information: done

Image version: 1.2.0.0068
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
FISVM000000000000 login: _
```

12. Log in to FortiIsolator. The default username is `admin` and there is no default password.

Installing FortiIsolator VM for VMware ESXi

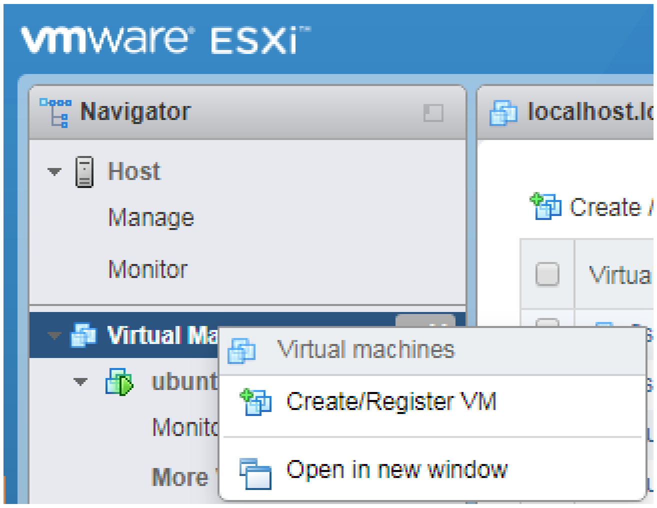
Use this procedure to install FortiIsolator VM for VMware ESXi.

Prerequisites

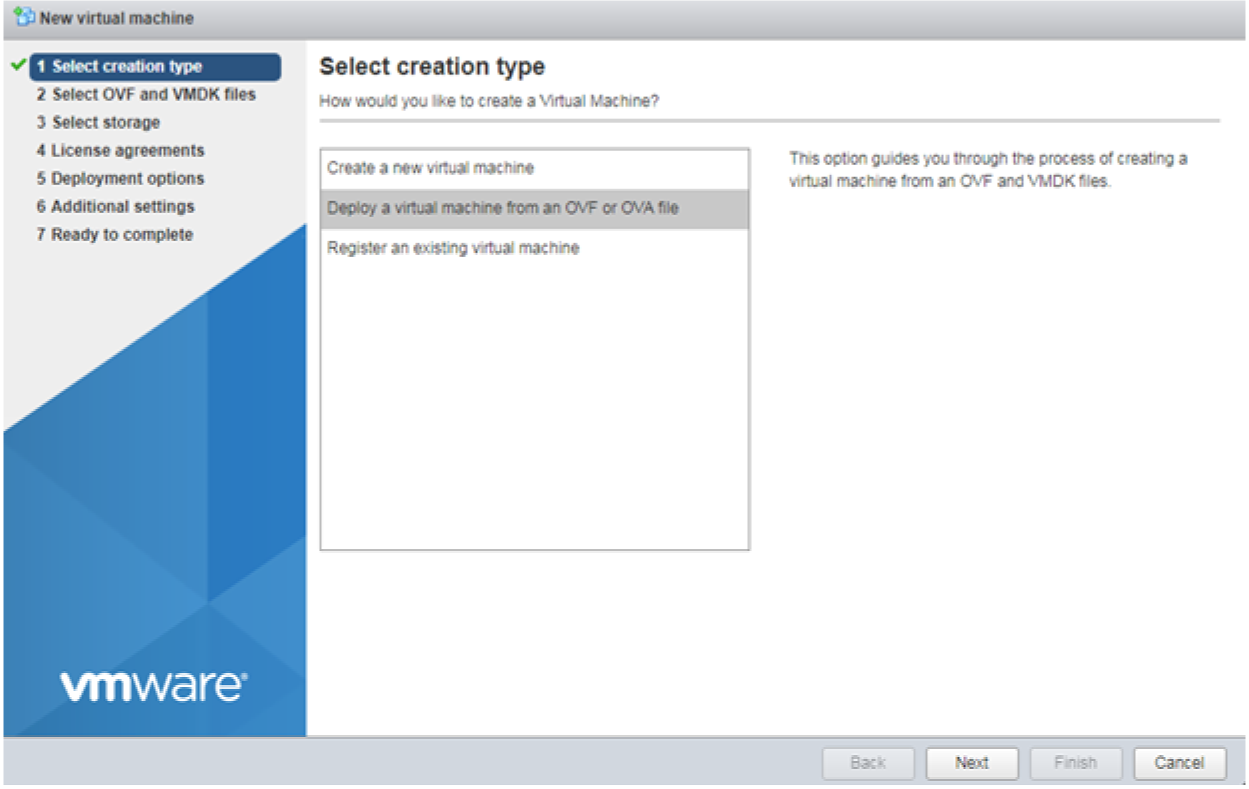
- Install VMware ESXi.
- Ensure that your system has one of the following combinations of hard disks and network adapters to support ESXI 6.5:
  - Two SCSI hard disks and three VMXNET 3 network adapters (this is the default)
  - Two SCSI hard disks and three E1000 network adapters

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*.



1 Select creation type
2 Select OVF and VMDK files
3 Select storage
4 License agreements
5 Deployment options
6 Additional settings
7 Ready to complete

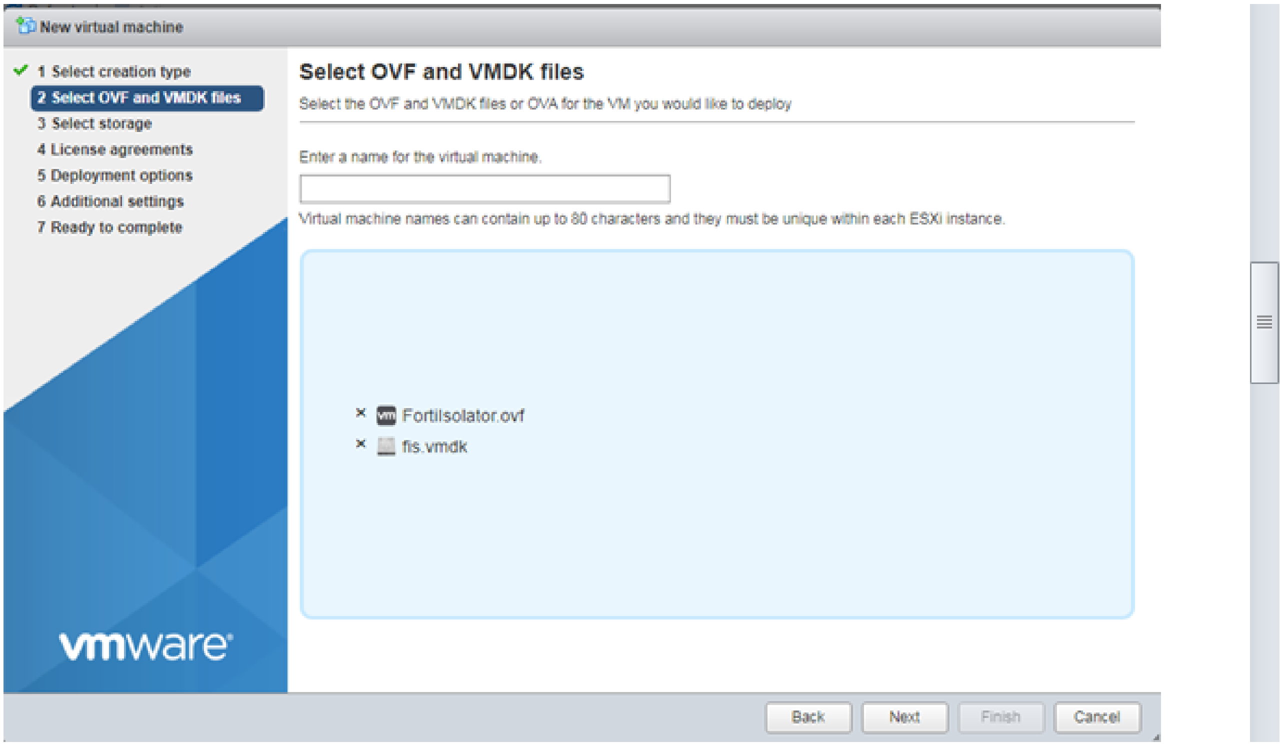
Select creation type

How would you like to create a Virtual Machine?

Create a new virtual machine
Deploy a virtual machine from an OVF or OVA file
Register an existing virtual machine

This option guides you through the process of creating a virtual machine from an OVF and VMDK files.

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



Select OVF and VMDK files

Select the OVF and VMDK files or OVA for the VM you would like to deploy

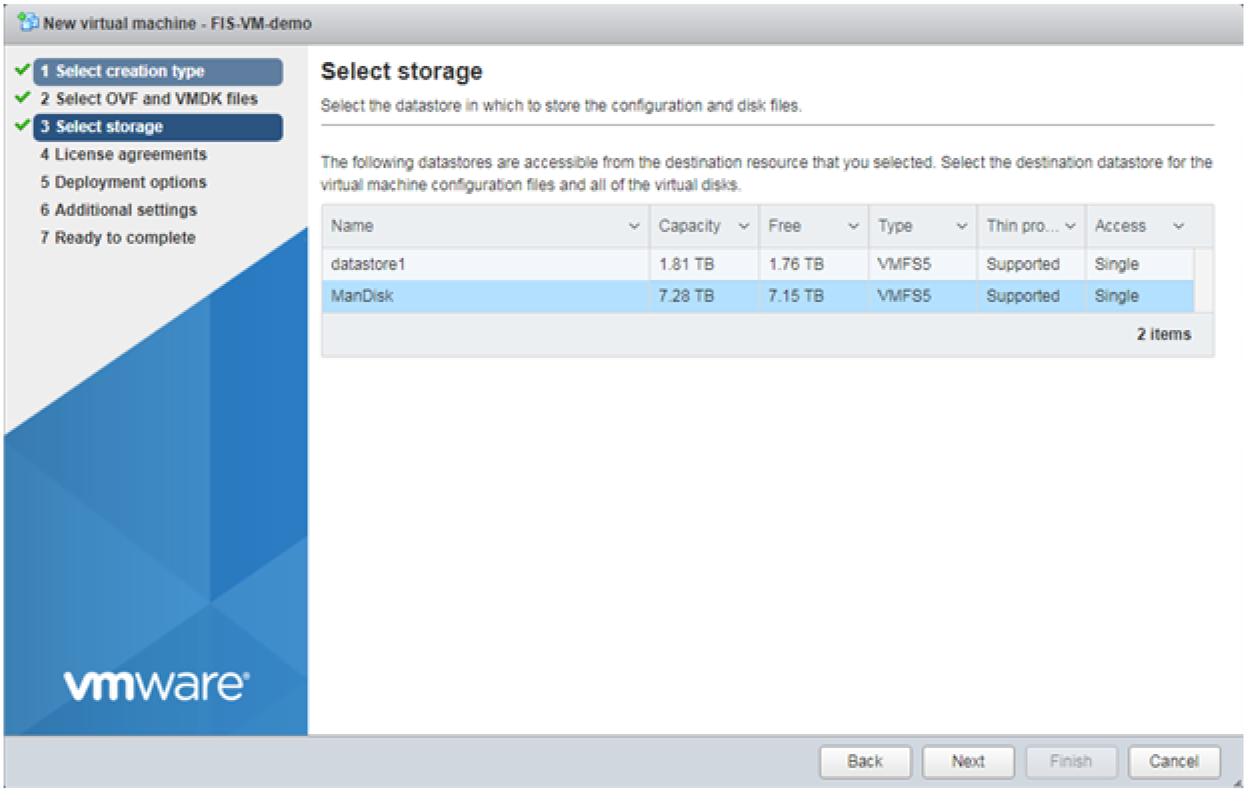
Enter a name for the virtual machine.

Virtual machine names can contain up to 80 characters and they must be unique within each ESXi instance.

× FortiIsolator.ovf

× fis.vmdk

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



Select storage

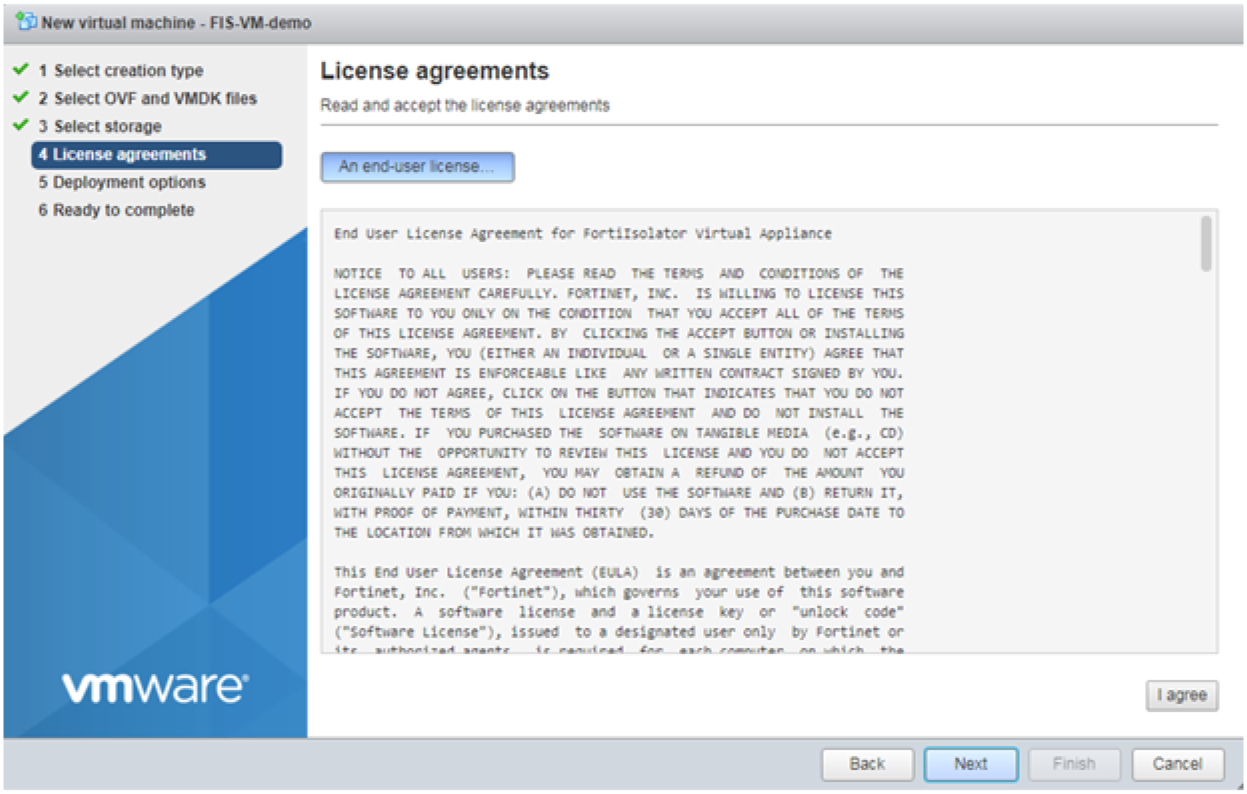
Select the datastore in which to store the configuration and disk files.

The following datastores are accessible from the destination resource that you selected. Select the destination datastore for the virtual machine configuration files and all of the virtual disks.

Name	Capacity	Free	Type	Thin pro...	Access
datastore1	1.81 TB	1.76 TB	VMFS5	Supported	Single
ManDisk	7.28 TB	7.15 TB	VMFS5	Supported	Single

2 items

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

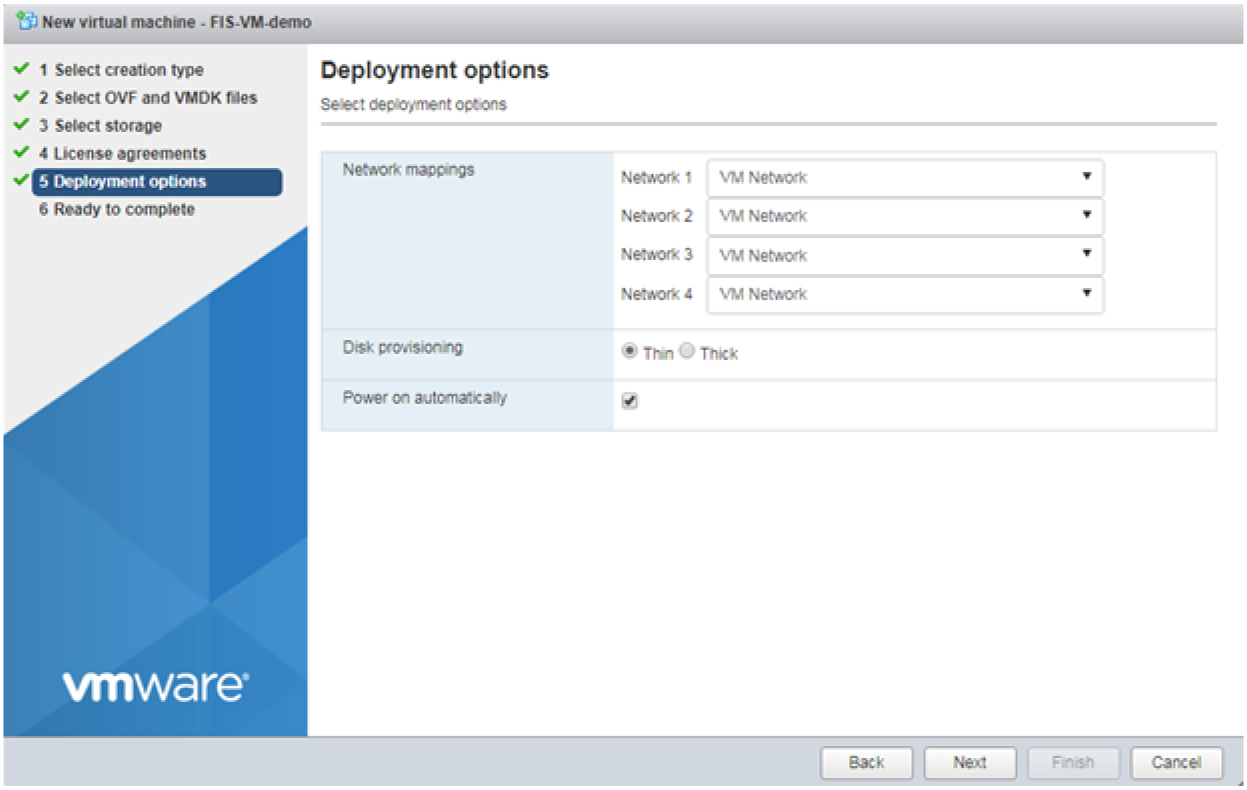


License agreements

Read and accept the license agreements

```
End User License Agreement for FortiIsolator Virtual Appliance

NOTICE  TO ALL  USERS:  PLEASE READ  THE TERMS  AND  CONDITIONS OF  THE
LICENSE AGREEMENT CAREFULLY. FORTINET, INC.  IS WILLING TO LICENSE THIS
SOFTWARE TO YOU ONLY ON THE CONDITION  THAT YOU ACCEPT ALL OF THE TERMS
OF THIS LICENSE AGREEMENT. BY  CLICKING THE ACCEPT BUTTON OR INSTALLING
THE SOFTWARE, YOU (EITHER AN INDIVIDUAL  OR A SINGLE ENTITY) AGREE THAT
THIS AGREEMENT IS ENFORCEABLE LIKE  ANY WRITTEN CONTRACT SIGNED BY YOU.
IF YOU DO NOT AGREE, CLICK ON THE BUTTON THAT INDICATES THAT YOU DO NOT
ACCEPT  THE TERMS  OF THIS  LICENSE AGREEMENT  AND DO  NOT INSTALL  THE
SOFTWARE. IF  YOU PURCHASED THE  SOFTWARE ON TANGIBLE MEDIA  (e.g., CD)
WITHOUT THE  OPPORTUNITY TO REVIEW THIS  LICENSE AND YOU DO  NOT ACCEPT
THIS  LICENSE AGREEMENT,  YOU MAY  OBTAIN A  REFUND OF  THE AMOUNT  YOU
ORIGINALLY PAID IF YOU: (A) DO NOT  USE THE SOFTWARE AND (B) RETURN IT,
WITH PROOF OF PAYMENT, WITHIN THIRTY  (30) DAYS OF THE PURCHASE DATE TO
THE LOCATION FROM WHICH IT WAS OBTAINED.

This End User License Agreement (EULA)  is an agreement between you and
Fortinet, Inc.  ("Fortinet"), which governs  your use of  this software
product.  A  software  license  and  a license  key  or  "unlock  code"
("Software License"), issued  to a designated user only  by Fortinet or
its  authorized agents,  is required  for  each computer  on which  the
```

6. In the *Deployment options* step, configure *Network mappings* with four network interfaces accordingly:
   - Network 1: Internal Interface
   - Network 2: External Interface
   - Network 3: Management Interface
   - Network 4: HA Interface



New virtual machine - FIS-VM-demo

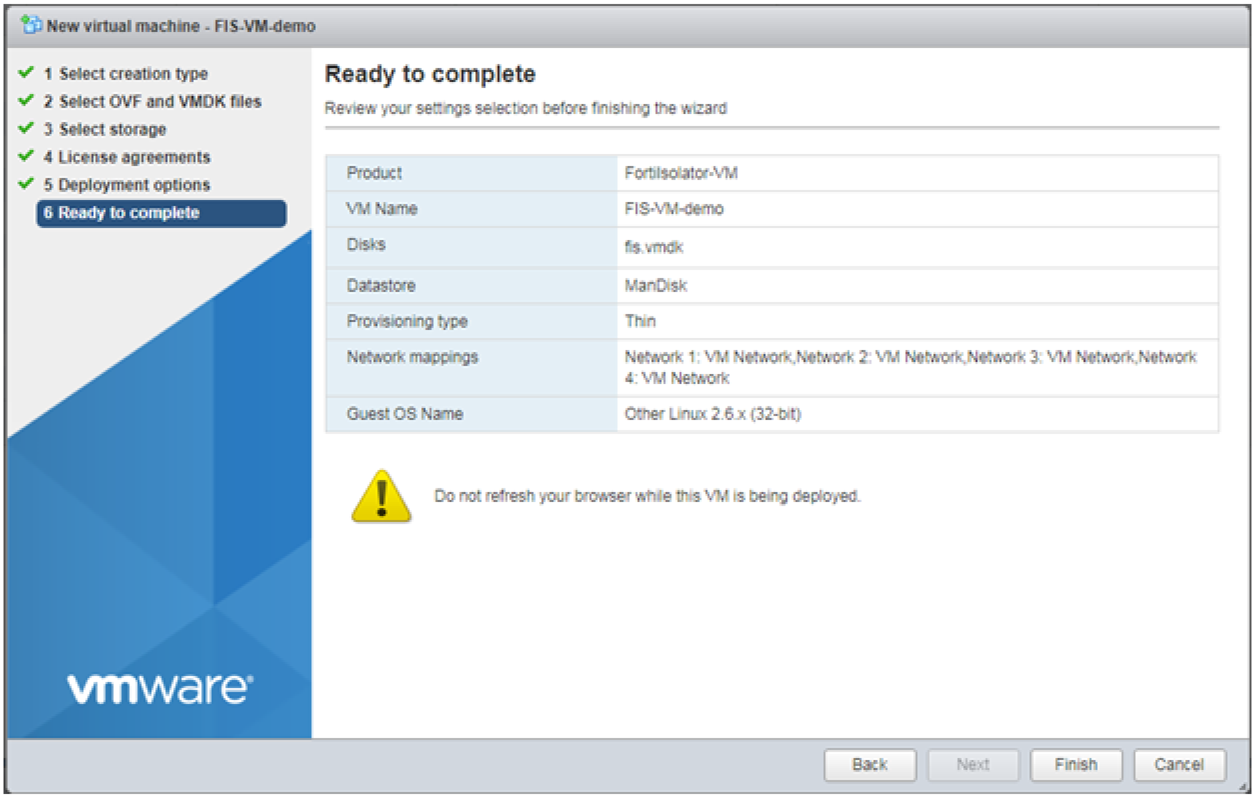
- ✓ 1 Select creation type
- ✓ 2 Select OVF and VMDK files
- ✓ 3 Select storage
- ✓ 4 License agreements
- ✓ 5 Deployment options
- 6 Ready to complete

Deployment options

Select deployment options

Network mappings	Network 1 VM Network Network 2 VM Network Network 3 VM Network Network 4 VM Network
Disk provisioning	● Thin ○ Thick
Power on automatically	☑

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



New virtual machine - FIS-VM-demo

- ✓ 1 Select creation type
- ✓ 2 Select OVF and VMDK files
- ✓ 3 Select storage
- ✓ 4 License agreements
- ✓ 5 Deployment options
- 6 Ready to complete

Ready to complete

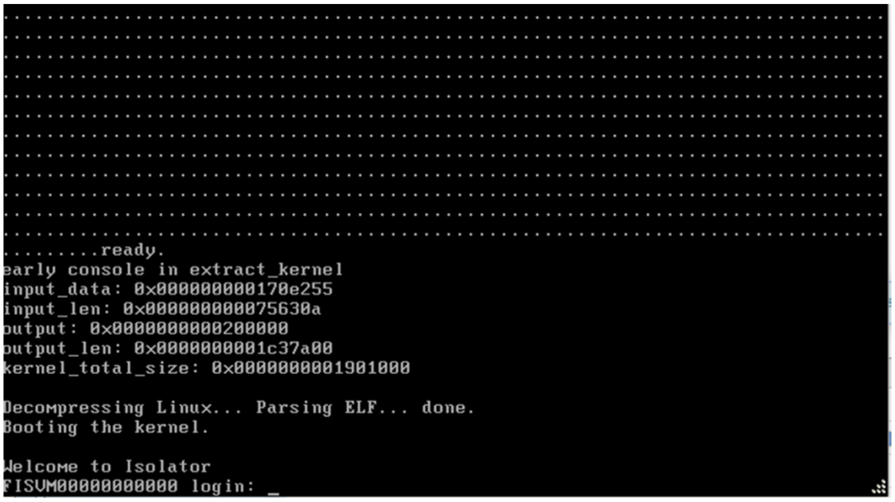
Review your settings selection before finishing the wizard

Product	FortiIsolator-VM
VM Name	FIS-VM-demo
Disks	fis.vmdk
Datastore	ManDisk
Provisioning type	Thin
Network mappings	Network 1: VM Network,Network 2: VM Network,Network 3: VM Network,Network 4: VM Network
Guest OS Name	Other Linux 2.6.x (32-bit)

Do not refresh your browser while this VM is being deployed.

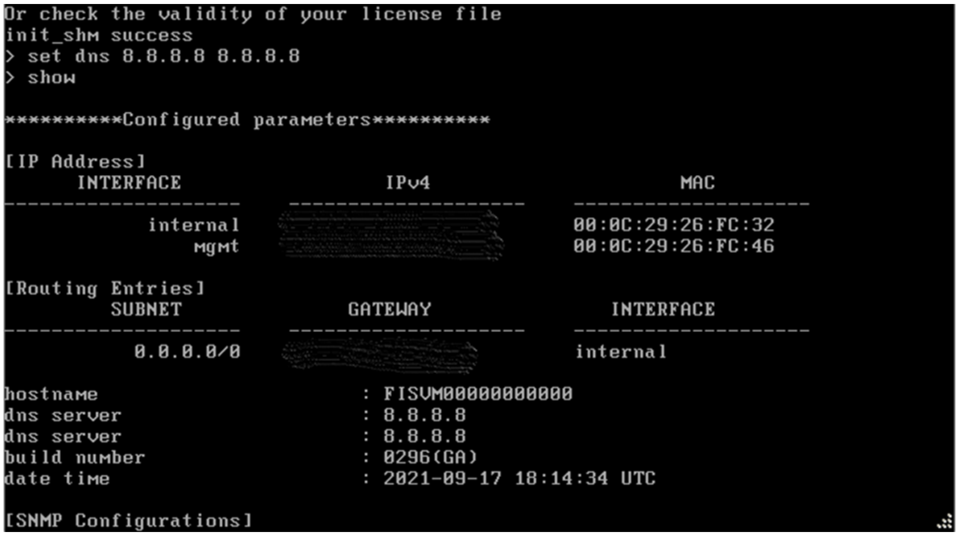
9. To start the VM, right-click the FortiIsolator VM name, and select *Power* > *Power on*.

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



```
................................................................................
................................................................................
................................................................................
................................................................................
................................................................................
................................................................................
................................................................................
................................................................................
................................................................................
................................................................................
................................................................................
................................................................................
.........ready.
early console in extract_kernel
input_data: 0x000000000170e255
input_len: 0x000000000075630a
output: 0x0000000000200000
output_len: 0x0000000001c37a00
kernel_total_size: 0x0000000001901000

Decompressing Linux... Parsing ELF... done.
Booting the kernel.

Welcome to Isolator
FISVM000000000000 login: _
```

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



```
Or check the validity of your license file
init_shm success
> set dns 8.8.8.8 8.8.8.8
> show

**********Configured parameters**********

[IP Address]
      INTERFACE                  IPv4                    MAC
--------------------    --------------------    --------------------
            internal    [redacted]              00:0C:29:26:FC:32
                mgmt                            00:0C:29:26:FC:46

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

hostname                             : FISVM000000000000
dns server                           : 8.8.8.8
dns server                           : 8.8.8.8
build number                         : 0296(GA)
date time                            : 2021-09-17 18:14:34 UTC

[SNMP Configurations]
```

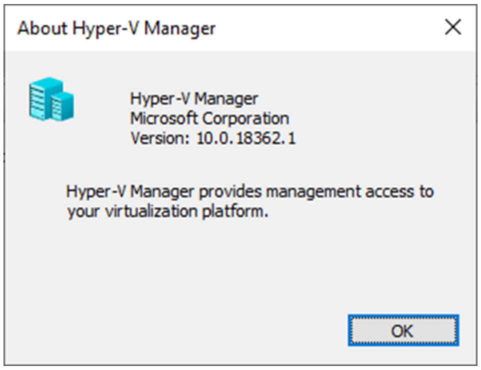
13. To verify that the internet connection works, ping `8.8.8.8`.
14. To access the FortiIsolator web portal, use the management IP address (for example, `http://10.160.17.63`).

Installing FortiIsolator VM for Microsoft Hyper-V

Use this procedure to install FortiIsolator VM for Microsoft Hyper-V.

Prerequisites

Install Microsoft Hyper-V Manager.



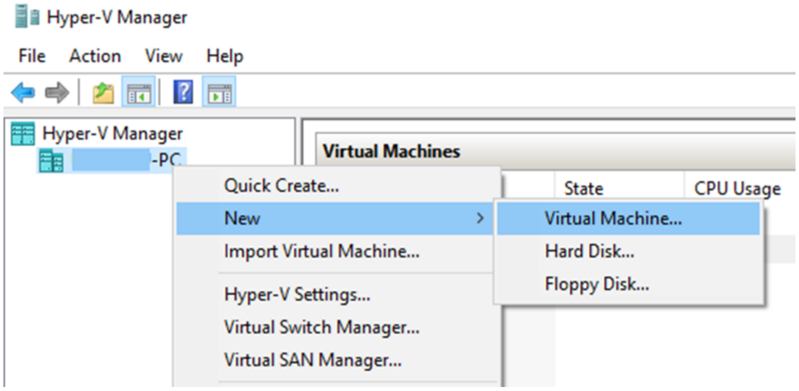
About Hyper-V Manager

Hyper-V Manager
Microsoft Corporation
Version: 10.0.18362.1

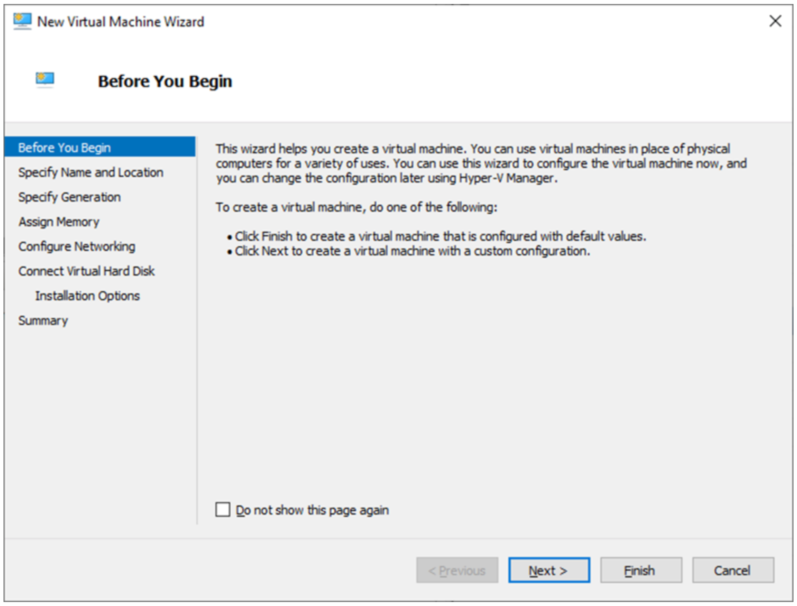
Hyper-V Manager provides management access to your virtualization platform.

Steps

1. Download the FortiIsolator firmware for Hyper-V by following the instructions in Downloading FortiIsolator firmware on page 11.
2. Unzip the downloaded .zip file to get "isolator.vhd" image.
3. To create a new virtual machine, launch Hyper-V Manager, connect to Server from Hyper-V Manager, then right clicking on *Server* to create *New Virtual Machine*.



4. In New Virtual Machine Wizard: *Next*.



New Virtual Machine Wizard

Before You Begin

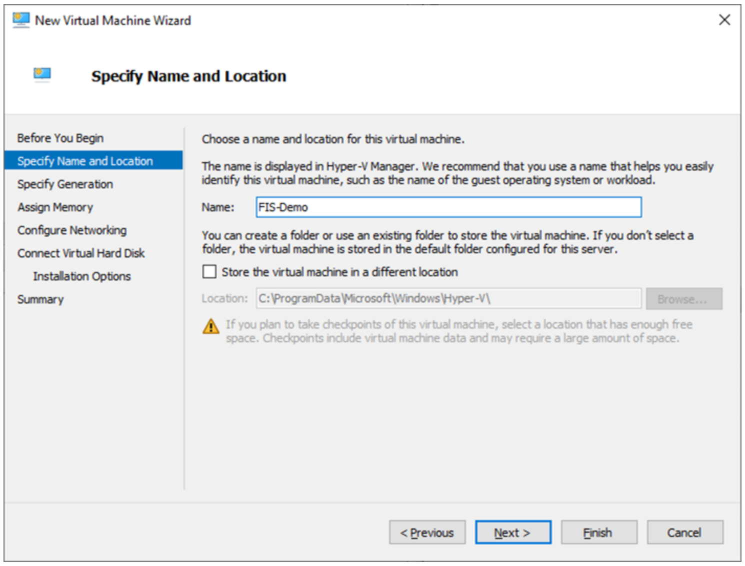
This wizard helps you create a virtual machine. You can use virtual machines in place of physical computers for a variety of uses. You can use this wizard to configure the virtual machine now, and you can change the configuration later using Hyper-V Manager.

To create a virtual machine, do one of the following:

- Click Finish to create a virtual machine that is configured with default values.
- Click Next to create a virtual machine with a custom configuration.

□ Do not show this page again

5. Specify Name and Location: provide a name for the new FortiIsolator VM, then *Next*.



Choose a name and location for this virtual machine.

The name is displayed in Hyper-V Manager. We recommend that you use a name that helps you easily identify this virtual machine, such as the name of the guest operating system or workload.

Name: FIS-Demo

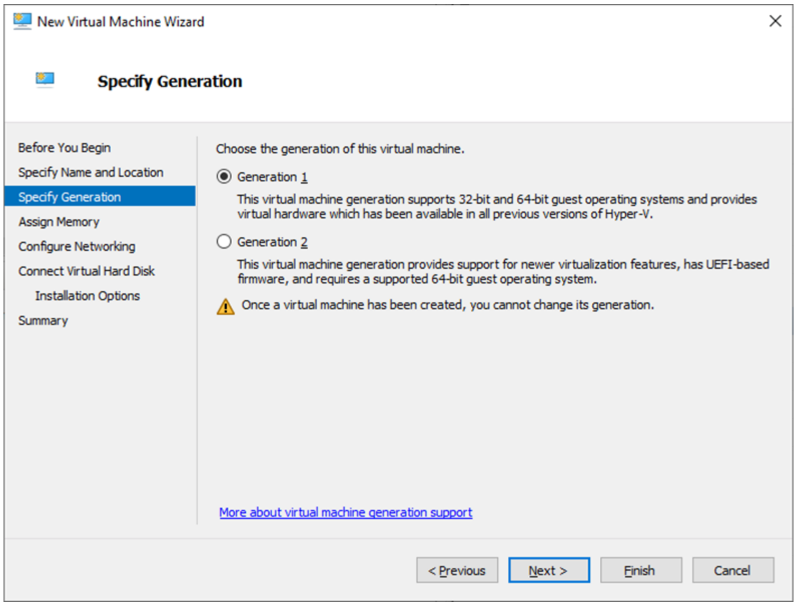
You can create a folder or use an existing folder to store the virtual machine. If you don't select a folder, the virtual machine is stored in the default folder configured for this server.

□ Store the virtual machine in a different location

Location: C:\ProgramData\Microsoft\Windows\Hyper-V\

If you plan to take checkpoints of this virtual machine, select a location that has enough free space. Checkpoints include virtual machine data and may require a large amount of space.

6. Specify Generation: select *Generation 1*, then *Next*.



Choose the generation of this virtual machine.

● Generation 1

This virtual machine generation supports 32-bit and 64-bit guest operating systems and provides virtual hardware which has been available in all previous versions of Hyper-V.

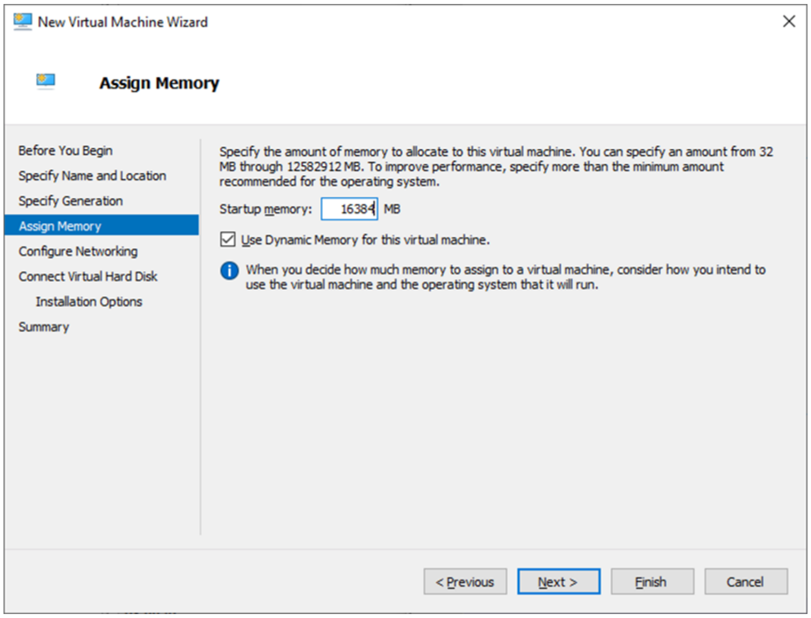
○ Generation 2

This virtual machine generation provides support for newer virtualization features, has UEFI-based firmware, and requires a supported 64-bit guest operating system.

Once a virtual machine has been created, you cannot change its generation.

7. Assign Memory: allocate sufficient RAM on to FortiIsolator.

- Make sure there is sufficient RAM allocated to the VM. This can be checked in Windows 10 through *Task Manager* > *Performance* > *Memory* > *Available*.
- It's recommended to allocate a minimum of 16GB (16384 MB) of RAM to FIS VM for supporting 50 sessions or more.



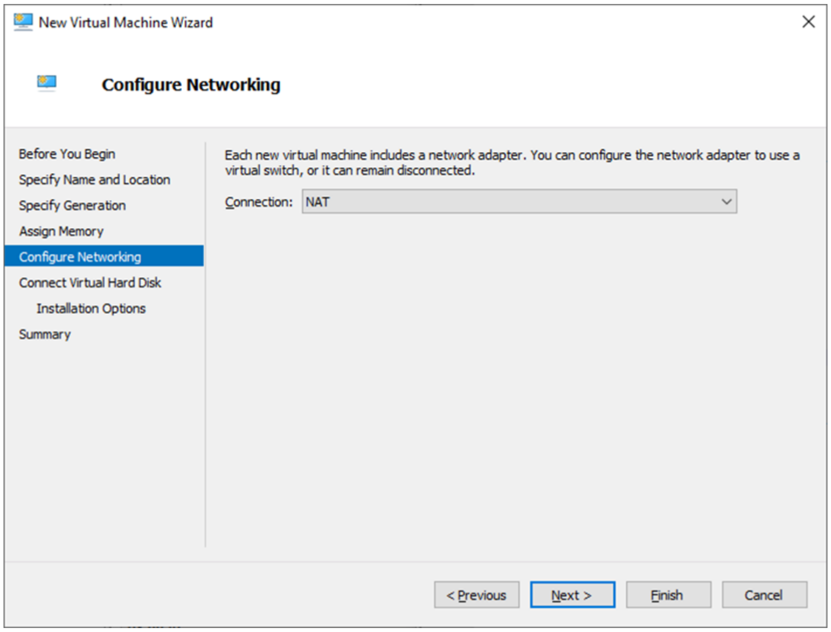
Specify the amount of memory to allocate to this virtual machine. You can specify an amount from 32 MB through 12582912 MB. To improve performance, specify more than the minimum amount recommended for the operating system.

Startup memory: 16384 MB

☑ Use Dynamic Memory for this virtual machine.

When you decide how much memory to assign to a virtual machine, consider how you intend to use the virtual machine and the operating system that it will run.

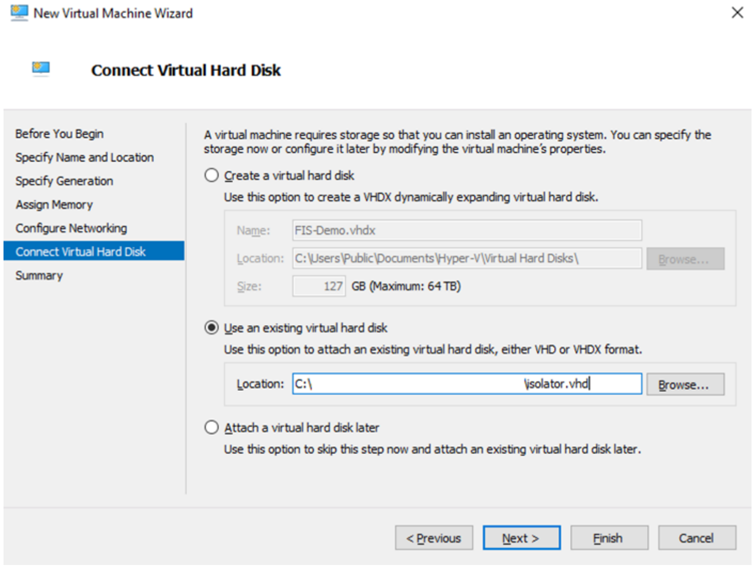
8. Configure Networking:
   Connection: NAT



Each new virtual machine includes a network adapter. You can configure the network adapter to use a virtual switch, or it can remain disconnected.

Connection: NAT

9. Connect Virtual Hard Disk:
   - Use an existing virtual hard disk: `isolator.vhd`.



New Virtual Machine Wizard

Connect Virtual Hard Disk

A virtual machine requires storage so that you can install an operating system. You can specify the storage now or configure it later by modifying the virtual machine's properties.

○ Create a virtual hard disk

Use this option to create a VHDX dynamically expanding virtual hard disk.

Name: FIS-Demo.vhdx

Location: C:\Users\Public\Documents\Hyper-V\Virtual Hard Disks\ Browse...

Size: 127 GB (Maximum: 64 TB)

● Use an existing virtual hard disk

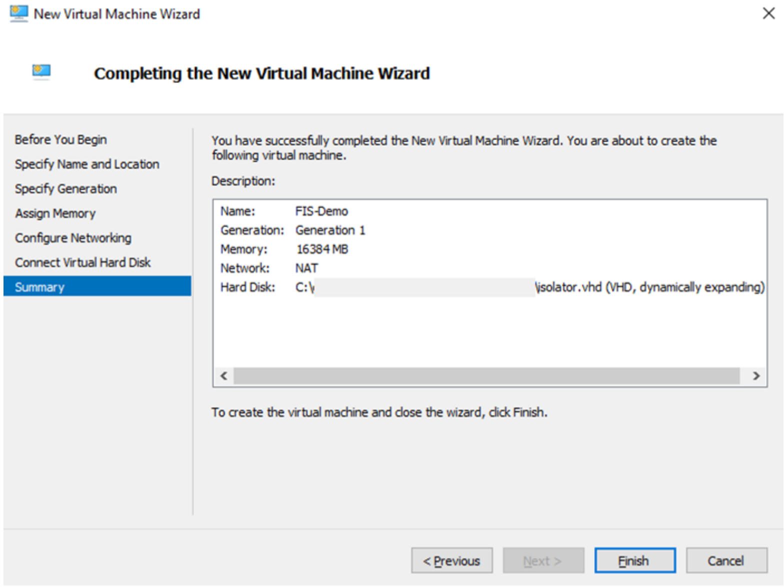
Use this option to attach an existing virtual hard disk, either VHD or VHDX format.

Location: C:\ \isolator.vhd Browse...

○ Attach a virtual hard disk later

Use this option to skip this step now and attach an existing virtual hard disk later.

10. Completing the New Virtual Machine Wizard: *Finish*.



New Virtual Machine Wizard

Completing the New Virtual Machine Wizard

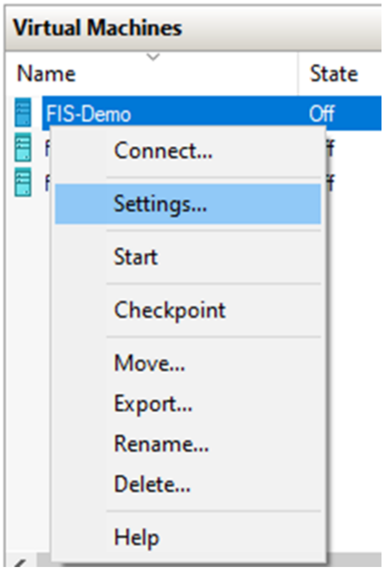
You have successfully completed the New Virtual Machine Wizard. You are about to create the following virtual machine.

Description:

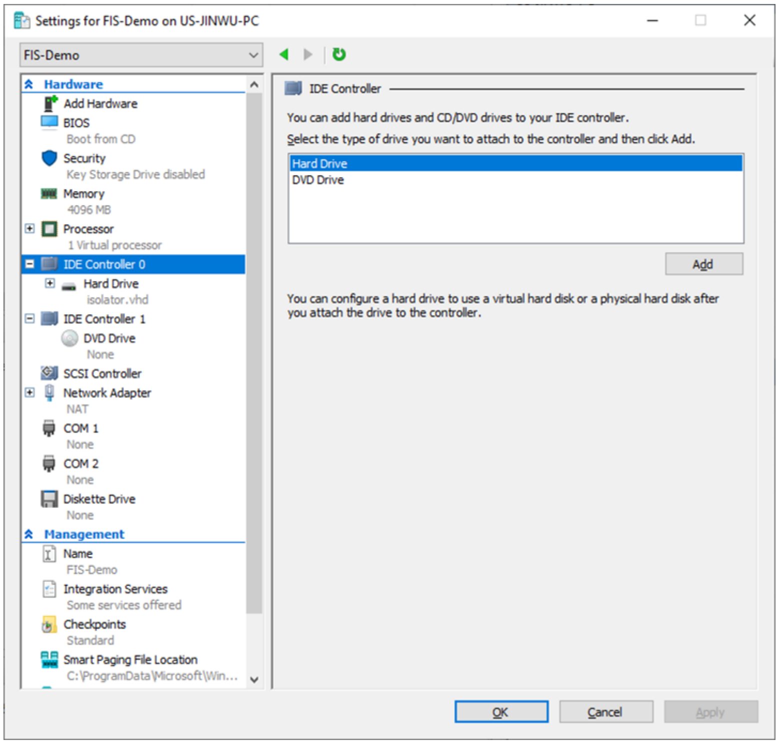
Name: FIS-Demo
Generation: Generation 1
Memory: 16384 MB
Network: NAT
Hard Disk: C:\ \isolator.vhd (VHD, dynamically expanding)

To create the virtual machine and close the wizard, click Finish.

11. After the new Virtual Machines is created and displays under Virtual Machines panel, right click on it and go to *Settings*.



12. To add new hard drive for FortiIsolator, from Settings wizard, select *IDE Controller 0*, select *Hard Drive*, then *Add*.

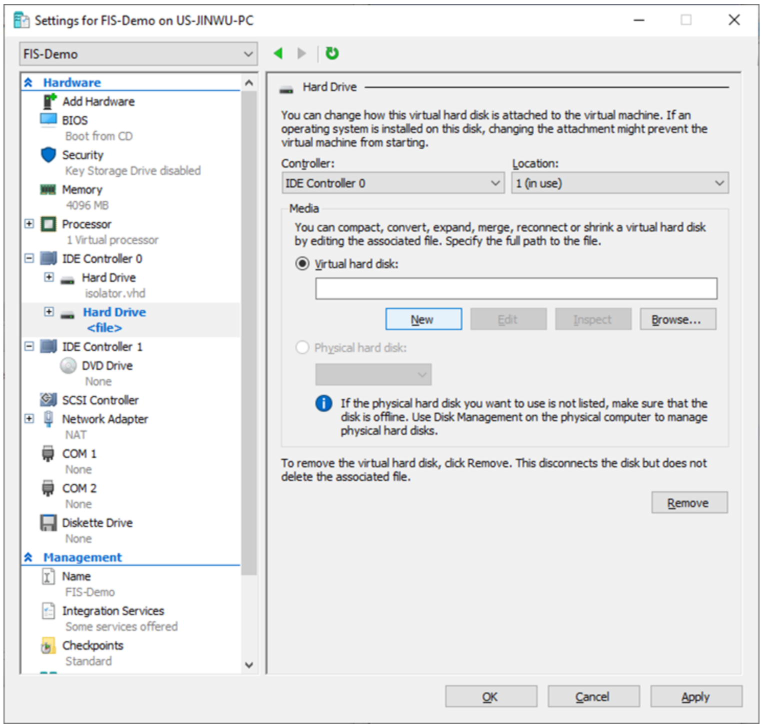


You can add hard drives and CD/DVD drives to your IDE controller.

Select the type of drive you want to attach to the controller and then click Add.

You can configure a hard drive to use a virtual hard disk or a physical hard disk after you attach the drive to the controller.

13. Under Media, select *Virtual hard disk* > *New*.



You can change how this virtual hard disk is attached to the virtual machine. If an operating system is installed on this disk, changing the attachment might prevent the virtual machine from starting.

Controller: IDE Controller 0

Location: 1 (in use)

Media

You can compact, convert, expand, merge, reconnect or shrink a virtual hard disk by editing the associated file. Specify the full path to the file.

● Virtual hard disk:

○ Physical hard disk:

If the physical hard disk you want to use is not listed, make sure that the disk is offline. Use Disk Management on the physical computer to manage physical hard disks.

To remove the virtual hard disk, click Remove. This disconnects the disk but does not delete the associated file.

14. Go to *Before You Begin* > *Next*.

Choose Disk Format: VHD

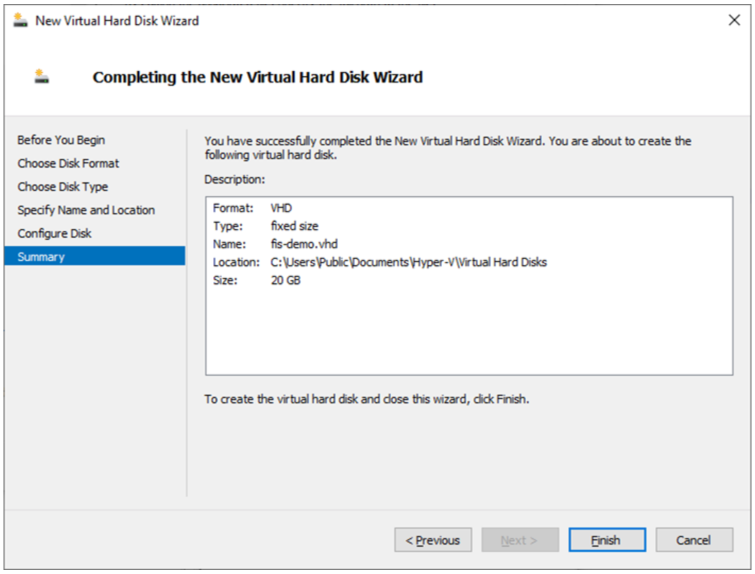
Choose Disk Type: Fixed size

Specify Name and Location

15. Configure Disk:

- Create a new blank virtual disk (e.g. Size: 20 GB)

16. Summary of New Virtual Hard Disk:



Completing the New Virtual Hard Disk Wizard

You have successfully completed the New Virtual Hard Disk Wizard. You are about to create the following virtual hard disk.

Description:

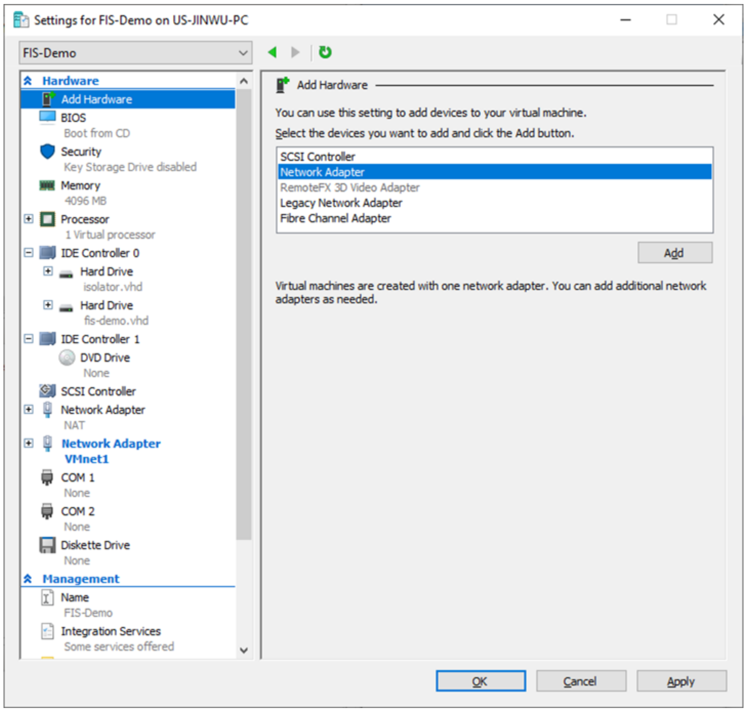
Format: VHD
Type: fixed size
Name: fis-demo.vhd
Location: C:\Users\Public\Documents\Hyper-V\Virtual Hard Disks
Size: 20 GB

To create the virtual hard disk and close this wizard, click Finish.

17. In Settings wizard, *Apply* to save the settings.

18. Follow these steps to add three new Network Adapters for FortiIsolator.

19. Select *Add Hardware* > *Network Adapter* > *Add*.

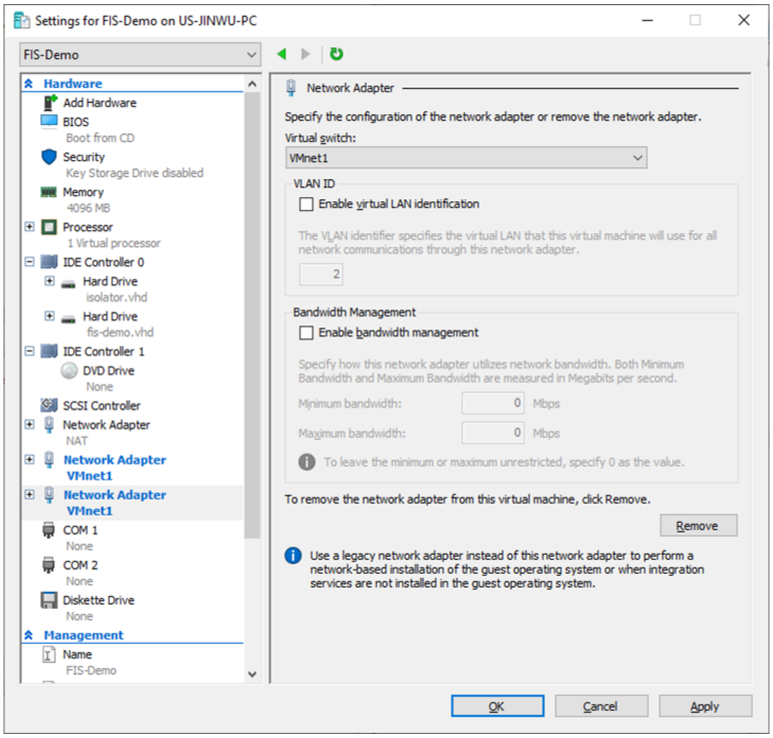


You can use this setting to add devices to your virtual machine.

Select the devices you want to add and click the Add button.

Virtual machines are created with one network adapter. You can add additional network adapters as needed.

20. *Virtual switch* > *VMnet1* > *Apply*.



Specify the configuration of the network adapter or remove the network adapter.

Virtual switch: VMnet1

VLAN ID

☐ Enable virtual LAN identification

The VLAN identifier specifies the virtual LAN that this virtual machine will use for all network communications through this network adapter.

2

Bandwidth Management

☐ Enable bandwidth management

Specify how this network adapter utilizes network bandwidth. Both Minimum Bandwidth and Maximum Bandwidth are measured in Megabits per second.

Minimum bandwidth: 0 Mbps

Maximum bandwidth: 0 Mbps

To leave the minimum or maximum unrestricted, specify 0 as the value.

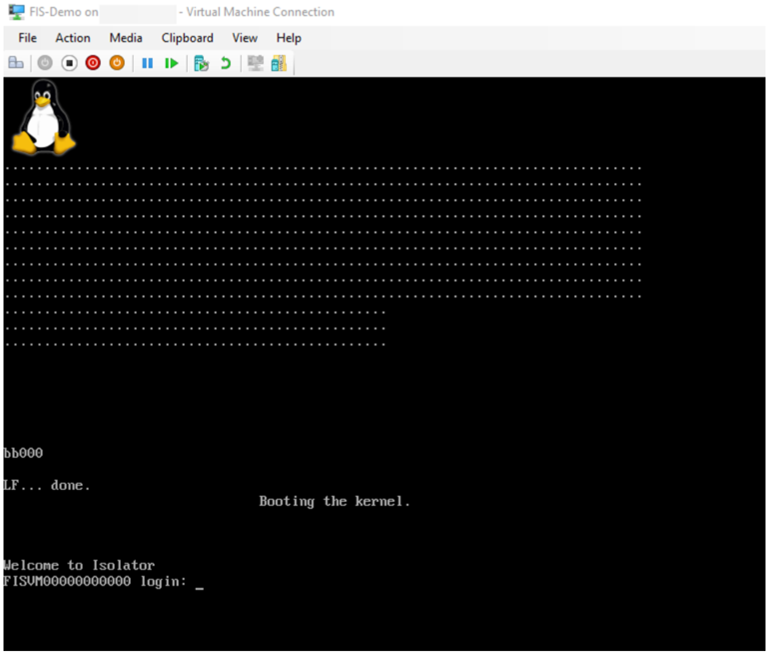
To remove the network adapter from this virtual machine, click Remove.

Use a legacy network adapter instead of this network adapter to perform a network-based installation of the guest operating system or when integration services are not installed in the guest operating system.

21. Repeat the last two steps to add two more Network Adapter:

- Network Adapter: VMnet 2
- Network Adapter: VMnet 3

22. Summary of Network Adapter:
    - Network Adapter: NAT (for FIS Internal port)
    - Network Adapter: VMnet 1 (for FIS External port)
    - Network Adapter: VMnet 2 (for FIS Management port)
    - Network Adapter: VMnet 3 (for FIS HA port)
23. Click *Apply* to save the setting and exit back to Virtual Machines Wizard.
24. Right-click *FIS VM* and connect to *start*.



```
..............................................................................
..............................................................................
..............................................................................
..............................................................................
..............................................................................
..............................................................................
..............................................................................
..............................................................................
..............................................................................
...............................................
...............................................
...............................................




bb000

LF... done.
                               Booting the kernel.



Welcome to Isolator
FISVM000000000000 login: _
```

25. Log in to FortiIsolator. The default username is `admin` and there is no default password.

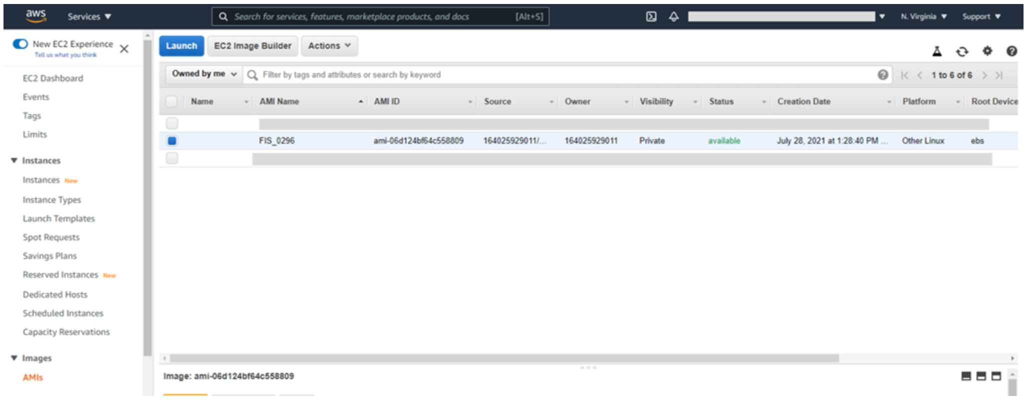
Installing FortiIsolator VM for AWS

The following section covers three steps:

- Step 1: Install FortiIsolator on AWS
- Step 2: Accessing to FortiIsolator CLI via Ubuntu
- Step 3: Browsing sites through FortiIsolator

Step 1: Install FortiIsolator on AWS

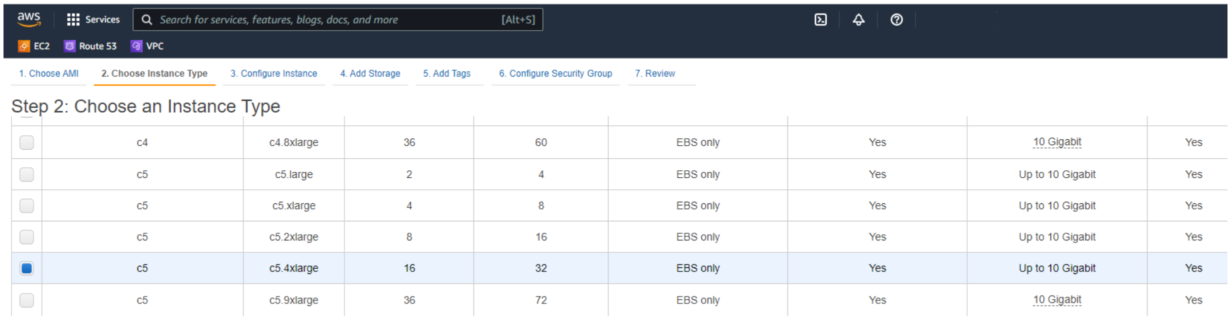
1. Verify the file has been uploaded in *AWS: EC2 > Images > AMIs*.



	Name	AMI Name	AMI ID	Source	Owner	Visibility	Status	Creation Date	Platform	Root Device
□		[redacted]								
☑		FIS_0296	ami-06d124bf64c558809	164025929011/...	164025929011	Private	available	July 28, 2021 at 1:28:40 PM ...	Other Linux	ebs
□		[redacted]								

Image: ami-06d124bf64c558809

2. Create instance from the file.
   - Select an instance type:

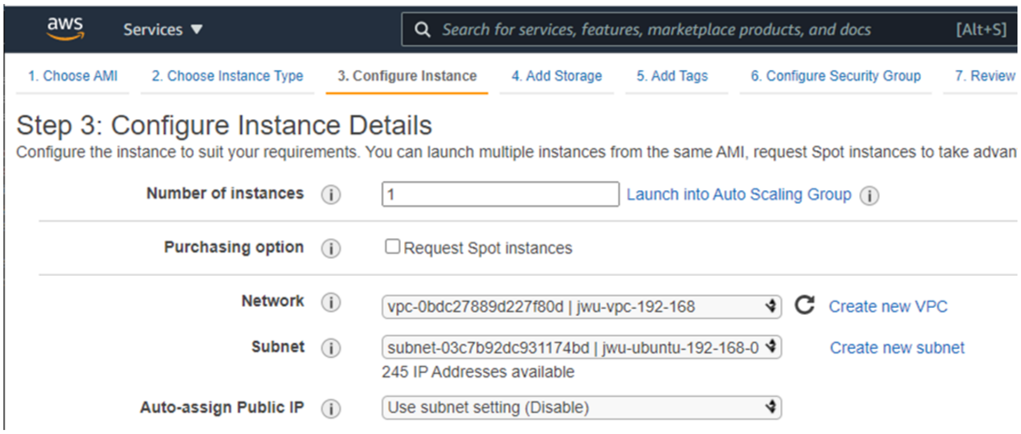


Step 2: Choose an Instance Type

□	c4	c4.8xlarge	36	60	EBS only	Yes	10 Gigabit	Yes
□	c5	c5.large	2	4	EBS only	Yes	Up to 10 Gigabit	Yes
□	c5	c5.xlarge	4	8	EBS only	Yes	Up to 10 Gigabit	Yes
□	c5	c5.2xlarge	8	16	EBS only	Yes	Up to 10 Gigabit	Yes
☑	c5	c5.4xlarge	16	32	EBS only	Yes	Up to 10 Gigabit	Yes
□	c5	c5.9xlarge	36	72	EBS only	Yes	10 Gigabit	Yes

FortiIsolator High Availabilities (HA) have to run on AWS Instances that are built on the Nitro System.

   - Select VPC and Subnets:



Step 3: Configure Instance Details

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advan

Number of instances: 1

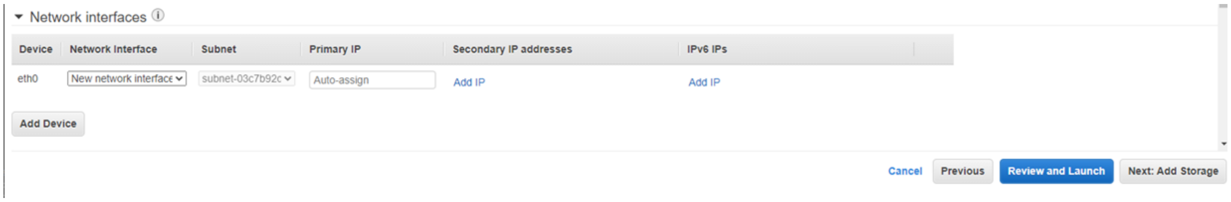
Purchasing option: □ Request Spot instances

Network: vpc-0bdc27889d227f80d | jwu-vpc-192-168

Subnet: subnet-03c7b92dc931174bd | jwu-ubuntu-192-168-0
245 IP Addresses available

Auto-assign Public IP: Use subnet setting (Disable)

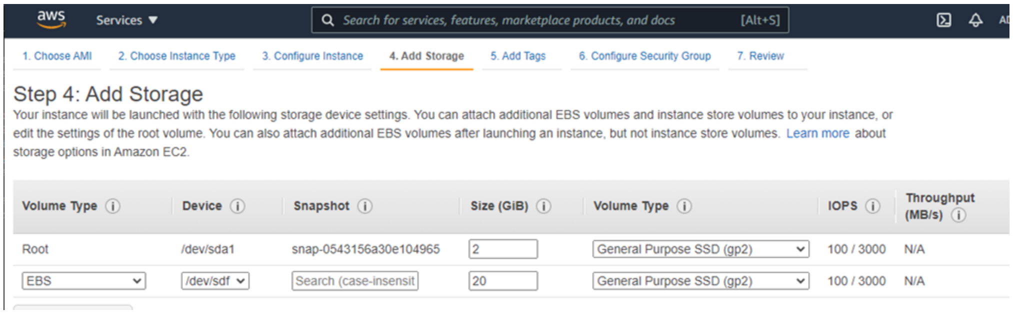
- Verify network interface, and click *Next: Add Storage*:



Network interfaces

Device	Network Interface	Subnet	Primary IP	Secondary IP addresses	IPv6 IPs
eth0	New network interface	subnet-03c7b92c	Auto-assign	Add IP	Add IP

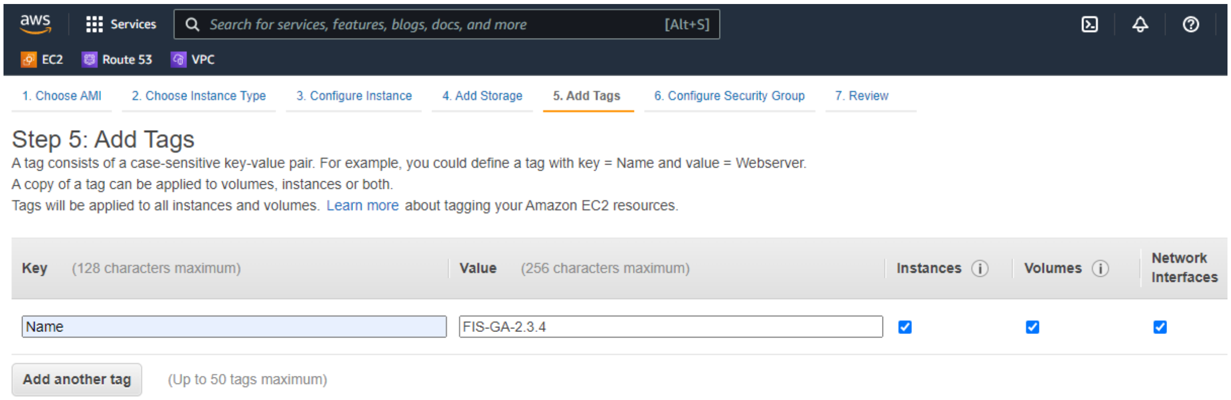
- Select */dev/sdf*, and assign size (GiB):



Step 4: Add Storage

Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. Learn more about storage options in Amazon EC2.

Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Throughput (MB/s)
Root	/dev/sda1	snap-0543156a30e104965	2	General Purpose SSD (gp2)	100 / 3000	N/A
EBS	/dev/sdf	Search (case-insensit	20	General Purpose SSD (gp2)	100 / 3000	N/A

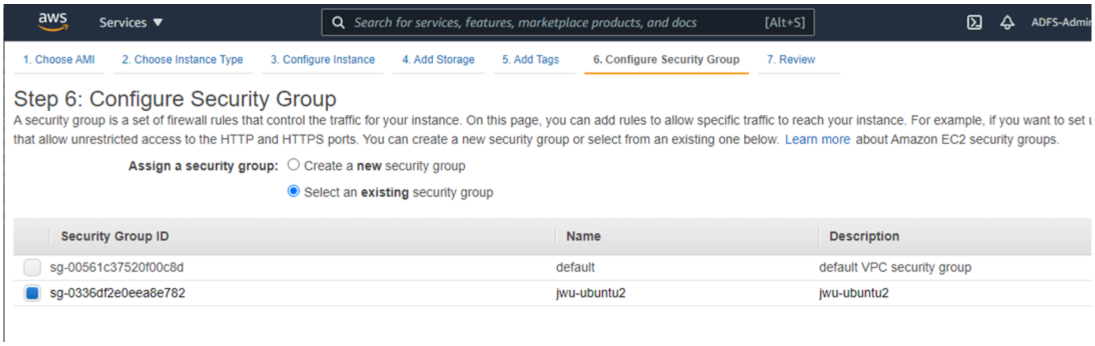


Step 5: Add Tags

A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver.
A copy of a tag can be applied to volumes, instances or both.
Tags will be applied to all instances and volumes. Learn more about tagging your Amazon EC2 resources.

Key (128 characters maximum)	Value (256 characters maximum)	Instances	Volumes	Network Interfaces
Name	FIS-GA-2.3.4	☑	☑	☑

- Select the security group that was created in the previous steps.

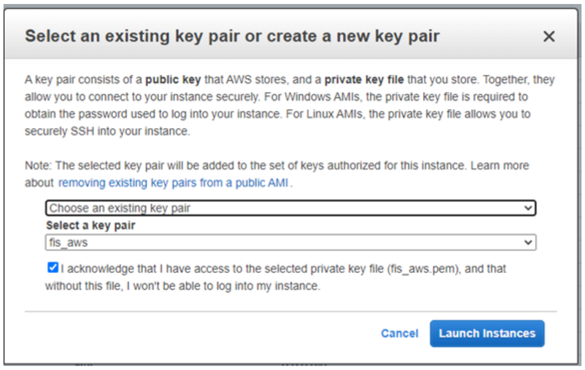


Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set u that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. Learn more about Amazon EC2 security groups.

Assign a security group: ○ Create a **new** security group
● Select an **existing** security group

	Security Group ID	Name	Description
□	sg-00561c37520f00c8d	default	default VPC security group
■	sg-0336df2e0eea8e782	jwu-ubuntu2	jwu-ubuntu2



Select an existing key pair or create a new key pair ✕

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about removing existing key pairs from a public AMI.

Choose an existing key pair

Select a key pair

fis_aws

☑ I acknowledge that I have access to the selected private key file (fis_aws.pem), and that without this file, I won't be able to log into my instance.

After clicking *Launch Instance*, stop the process, and go add another three interfaces. Make sure FortiIsolator has four interfaces:

- Internal Interface: 192.168.0.0/24
- External Interface: 192.168.2.0/24
- Management Interface: 192.168.1.0/24
- HA Interface: 192.168.3.0/24

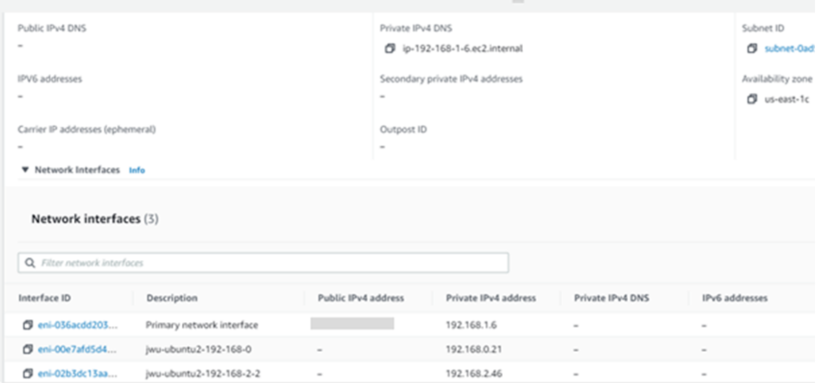
- Verify the interfaces are in this order.

Settings the third interface as `192.168.1.0/24` subnet allows you to access default management IP `192.168.1.99`.

Step 2: Accessing to FortiIsolator CLI via Ubuntu

Pre-requisites

- You need an Ubuntu in AWS that has same subnets as FortiIsolator
- You need an associated EIP as the public IP to the Ubuntu on `192.168.1.0/24` subnet.



Public IPv4 DNS	Private IPv4 DNS	Subnet ID
-	ip-192-168-1-6.ec2.internal	subnet-0ad
IPV6 addresses	Secondary private IPv4 addresses	Availability zone
-	-	us-east-1c
Carrier IP addresses (ephemeral)	Outpost ID	
-	-	

▼ Network Interfaces Info

Network interfaces (3)

Interface ID	Description	Public IPv4 address	Private IPv4 address	Private IPv4 DNS	IPv6 addresses
eni-036acdd203...	Primary network interface	[redacted]	192.168.1.6	-	-
eni-00e7afd5d4...	jwu-ubuntu2-192-168-0	-	192.168.0.21	-	-
eni-02b3dc13aa...	jwu-ubuntu2-192-168-2-2	-	192.168.2.46	-	-

1. Connect to Ubuntu:
   ```
   > ssh -i "fis_aws.pem" ubuntu@public_ip(EIP)
   ```
2. From Ubuntu SSH to FIS via Mgmt Interface pre-defined IP (`192.168.1.99`).
   ```
   > ssh admin@192.168.1.99
   ```
3. Set Internal IP:
   ```
   > set internal-ip 192.168.0.99/24
   ```

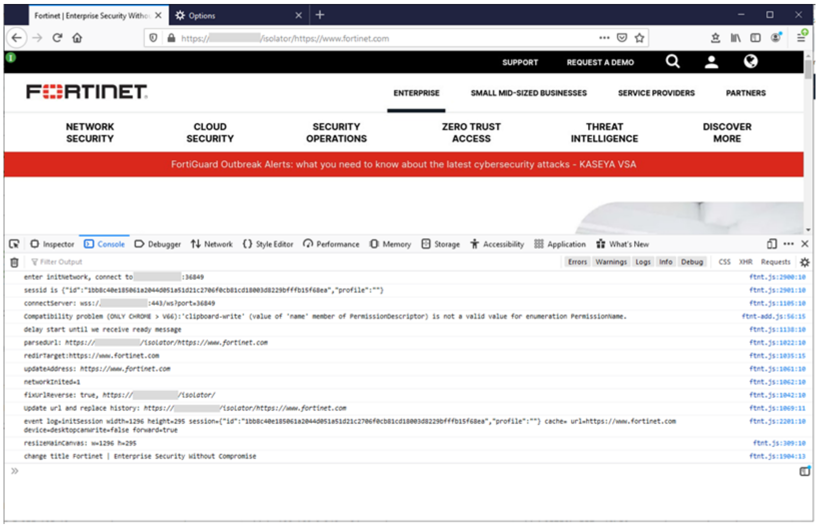
4. Set DNS:
   ```
   > set dns 192.168.0.2 192.168.0.2
   ```
5. Set IP Mapping on FIS to public IP:
   ```
   > set fis-ipmap 443 443 public_ip
   ```
6. Overview:

   e.g.
   ```
   > set internal-ip 192.168.0.99/24
   > set internal-gw 0.0.0.0/0 192.168.0.2
   > set dns 192.168.0.2
   > set fis-ipmap 443 443 public_ip
   ```

Step 3: Browsing sites through FortiIsolator

IP Forwarding:

https://<*public_ip*>/isolator/https://www.fortinet.com/



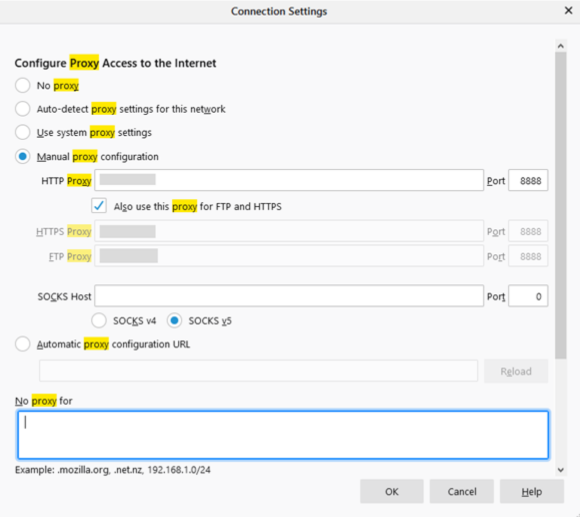
FortiGuard Outbreak Alerts: what you need to know about the latest cybersecurity attacks - KASEYA VSA

```
enter initNetwork, connect to[redacted]:36849                                                                ftnt.js:2900:10
sessid is {"id":"1bb8c40e185061a2044d051a51d21c2706f0cb81cd18003d8229bfffb15f68ea","profile":""}             ftnt.js:2901:10
connectServer: wss:/[redacted]:443/ws?port=36849                                                             ftnt.js:1105:10
Compatibility problem (ONLY CHROME > V66):'clipboard-write' (value of 'name' member of PermissionDescriptor) is not a valid value for enumeration PermissionName.   ftnt-add.js:56:15
delay start until we receive ready message                                                                   ftnt.js:1138:10
parsedUrl: https://[redacted]/isolator/https://www.fortinet.com                                              ftnt.js:1022:10
redirTarget:https://www.fortinet.com                                                                         ftnt.js:1035:15
updateAddress: https://www.fortinet.com                                                                      ftnt.js:1061:10
networkInited=1                                                                                              ftnt.js:1062:10
fixUrlReverse: true, https://[redacted]/isolator/                                                            ftnt.js:1042:10
Update url and replace history: https://[redacted]/isolator/https://www.fortinet.com                         ftnt.js:1069:11
event log=initSession width=1296 height=295 session={"id":"1bb8c40e185061a2044d051a51d21c2706f0cb81cd18003d8229bfffb15f68ea","profile":""} cache= url=https://www.fortinet.com   ftnt.js:2201:10
device=desktopcanWrite=false forward=true
resizeMainCanvas: w=1296 h=295                                                                               ftnt.js:309:10
change title Fortinet | Enterprise Security Without Compromise                                              ftnt.js:1904:13
```

Proxy:

Browser Setting:

```
> HTTP Proxy: public_ip port 8888
```



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 [redacted] Port 8888

☑ Also use this proxy for FTP and HTTPS

HTTPS Proxy [redacted] Port 8888

FTP Proxy [redacted] Port 8888

SOCKS Host Port 0

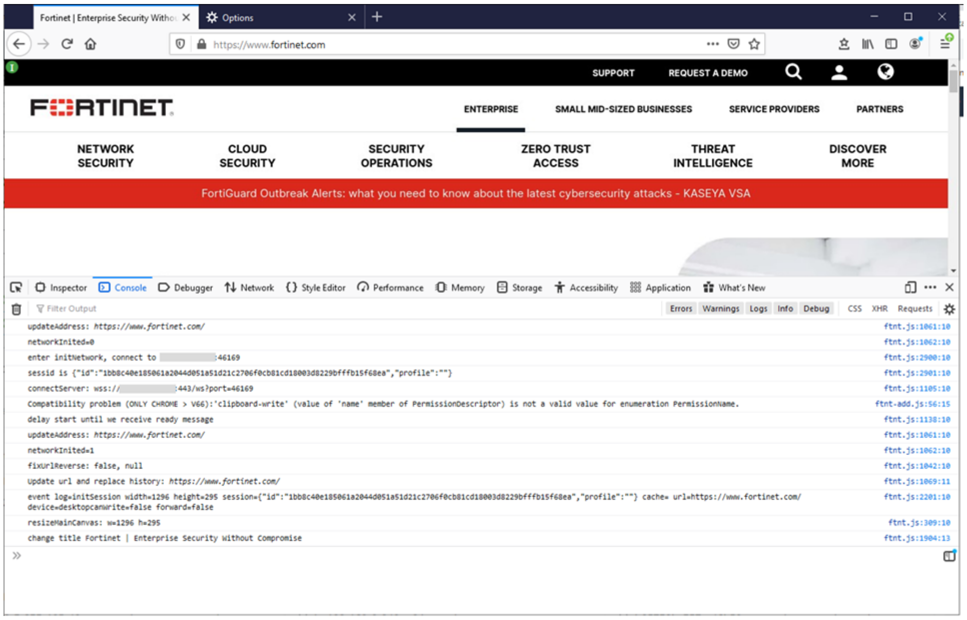
○ SOCKS v4 ● SOCKS v5

○ Automatic proxy configuration URL

Reload

No proxy for

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



```
updateAddress: https://www.fortinet.com/                                                          ftnt.js:1061:10
networkInited=0                                                                                   ftnt.js:1062:10
enter initNetwork, connect to [redacted]:46169                                                    ftnt.js:2900:10
sessid is {"id":"1bb8c40e185061a2044d051a51d21c2706f0cb81cd18003d8229bfffb15f68ea","profile":""}  ftnt.js:2901:10
connectServer: wss://[redacted]:443/ws?port=46169                                                 ftnt.js:1105:10
Compatibility problem (ONLY CHROME > V66):'clipboard-write' (value of 'name' member of PermissionDescriptor) is not a valid value for enumeration PermissionName.  ftnt-add.js:56:15
delay start until we receive ready message                                                        ftnt.js:1138:10
updateAddress: https://www.fortinet.com/                                                          ftnt.js:1061:10
networkInited=1                                                                                   ftnt.js:1062:10
fixUrlReverse: false, null                                                                        ftnt.js:1042:10
Update url and replace history: https://www.fortinet.com/                                         ftnt.js:1069:11
event log=initSession width=1296 height=295 session={"id":"1bb8c40e185061a2044d051a51d21c2706f0cb81cd18003d8229bfffb15f68ea","profile":""} cache= url=https://www.fortinet.com/  ftnt.js:2201:10
device=desktopcanWrite=false forward=false
resizeMainCanvas: w=1296 h=295                                                                    ftnt.js:309:10
change title Fortinet | Enterprise Security Without Compromise                                    ftnt.js:1904:13
```

Setting up IP mapping

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

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

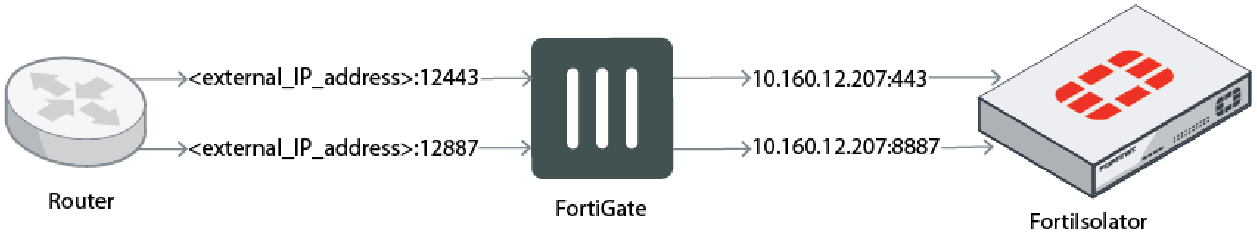
You can perform the initial configuration using the serial console. For more information, see the FortiIsolator 1000F QuickStart Guide.

Topology

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

For example, 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 FortiIsolator. The configuration information in this section follows an example setup with the following values:

External IP address of router	<external_IP_address>
Internal IP address of FortiIsolator	10.160.12.207
Router redirections	• <external_IP_address>:12443 > 10.160.12.207:443 • <external_IP_address>:12887 > 10.160.12.207:8887



Important note

Prior to GA release 2.3.1, FortiIsolator (FIS) used two ports to redirect HTTPS traffics in between web servers and FIS: port 443 and 8887.

Both ports handle network traffics for different purposes, for sending/receiving traffics from/to web servers and FortiIsolator.

In order to setup IP Mapping, FortiIsolator needs to map to both ports need from the external IP address to internal IP address of FortiIsolator's. This can be done over CLI commands only; it's currently not available on GUI.

The CLI command for mapping ports:

```
set fis-ipmap <port_map_to_443> <port_map_to_8887> <external_IP_address>
```

Example:

```
set fis-ipmap 12443 12887 172.30.147.207
```

Since GA release 2.3.1, FortiIsolator enhanced the IP Mapping with only one port: port 443. However, using the same CLI in order to compatible with previous versions, the CLI needs to map the same port, as follows:

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

Example:

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

Configuring IP mapping in regular mode

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

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

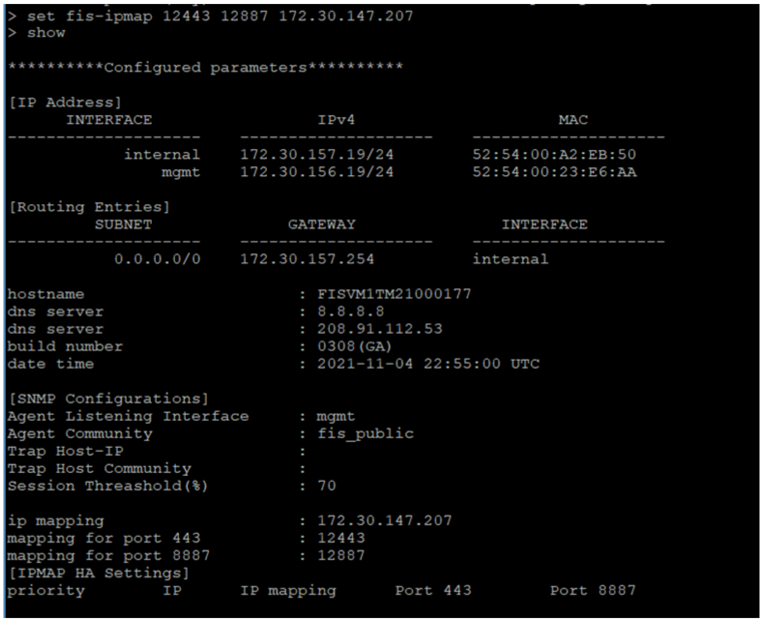
FortiIsolator configuration

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

```
set fis-ipmap <port_map_to_443> <port_map_to_8887> <external_IP_address>
```

For example,

```
set fis-ipmap 12443 12887 172.30.147.207
```



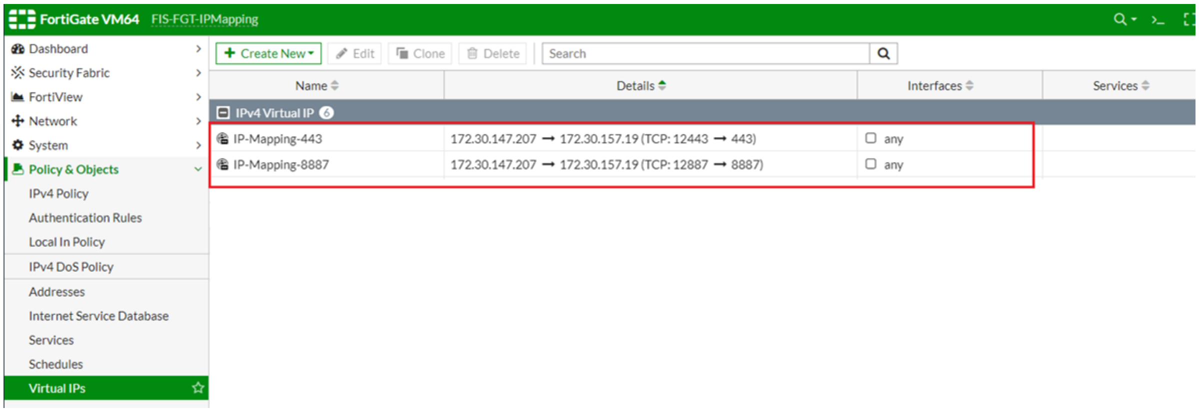
```
> set fis-ipmap 12443 12887 172.30.147.207
> show

**********Configured parameters**********

[IP Address]
      INTERFACE                  IPv4                    MAC
--------------------    --------------------    --------------------
            internal    172.30.157.19/24        52:54:00:A2:EB:50
                mgmt    172.30.156.19/24        52:54:00:23:E6:AA

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

hostname                      : FISVM1TM21000177
dns server                    : 8.8.8.8
dns server                    : 208.91.112.53
build number                  : 0308(GA)
date time                     : 2021-11-04 22:55:00 UTC

[SNMP Configurations]
Agent Listening Interface     : mgmt
Agent Community               : fis_public
Trap Host-IP                  :
Trap Host Community           :
Session Threashold(%)         : 70

ip mapping                    : 172.30.147.207
mapping for port 443          : 12443
mapping for port 8887         : 12887
[IPMAP HA Settings]
priority        IP      IP mapping      Port 443        Port 8887
```

FortiGate configuration

Complete the following steps in the FortiGate UI.

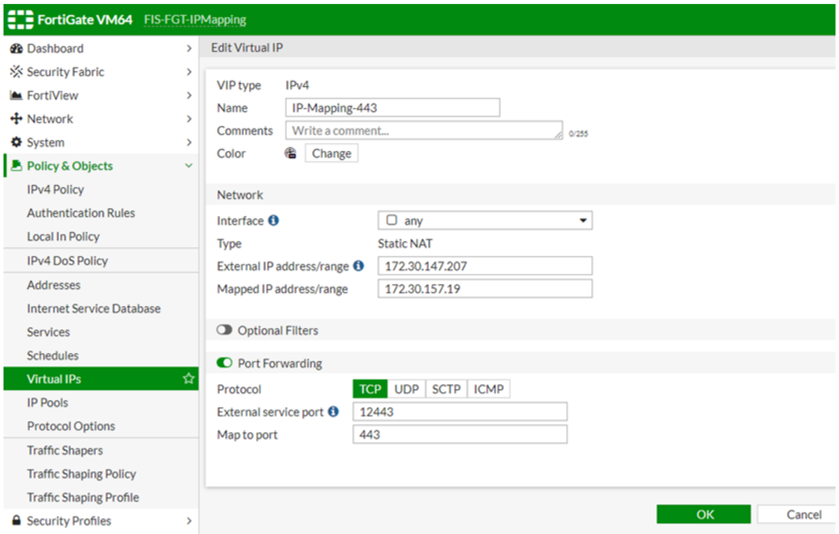
1. Go to *Policy & Objects* > *Virtual IPs*.
2. Create two IPv4 virtual IPs with the following information:
   - **IP-Mapping-443**: <external_IP_address> -> FIS_IP (TCP: 12443 > 443)
     e.g. 172.30.147.207 -> 172.30.157.19 (TCP: 12443 > 443)
   - **IP-Mapping-8887**: <external_IP_address -> FIS_IP (TCP: 12887 > 8887)
     e.g. 172.30.147.207 -> 172.30.157.19 (TCP: 12887 > 8887)

This example uses the following:
- External_IP_address: 172.30.147.207
- FIS_IP: 172.30.157.19



Name	Details	Interfaces	Services
IPv4 Virtual IP 6			
IP-Mapping-443	172.30.147.207 → 172.30.157.19 (TCP: 12443 → 443)	□ any	
IP-Mapping-8887	172.30.147.207 → 172.30.157.19 (TCP: 12887 → 8887)	□ any	

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



Edit Virtual IP

VIP type	IPv4
Name	IP-Mapping-443
Comments	Write a comment... 0/255
Color	Change

Network

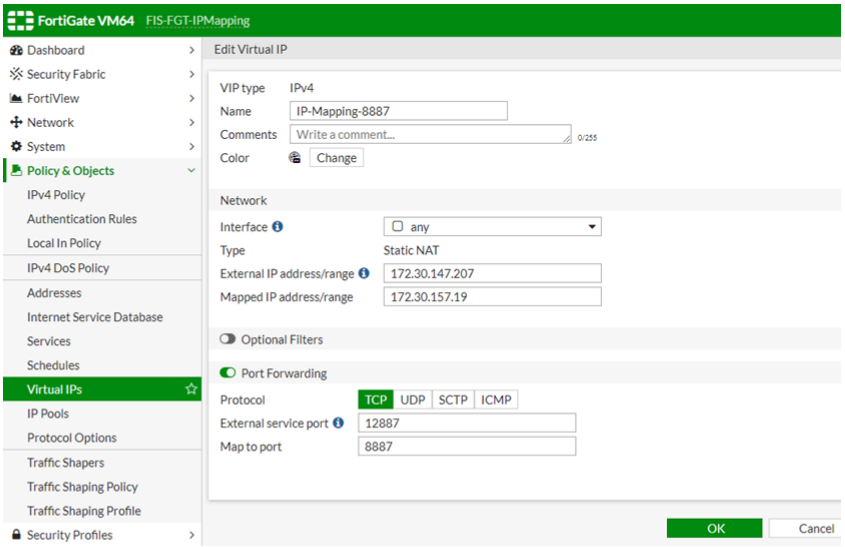
Interface	□ any
Type	Static NAT
External IP address/range	172.30.147.207
Mapped IP address/range	172.30.157.19

Optional Filters

Port Forwarding

Protocol	TCP UDP SCTP ICMP
External service port	12443
Map to port	443

Settings of **ip-mapping-8887**:



Edit Virtual IP

VIP type IPv4
Name IP-Mapping-8887
Comments Write a comment... 0/255
Color Change

Network

Interface ☐ any
Type Static NAT
External IP address/range 172.30.147.207
Mapped IP address/range 172.30.157.19

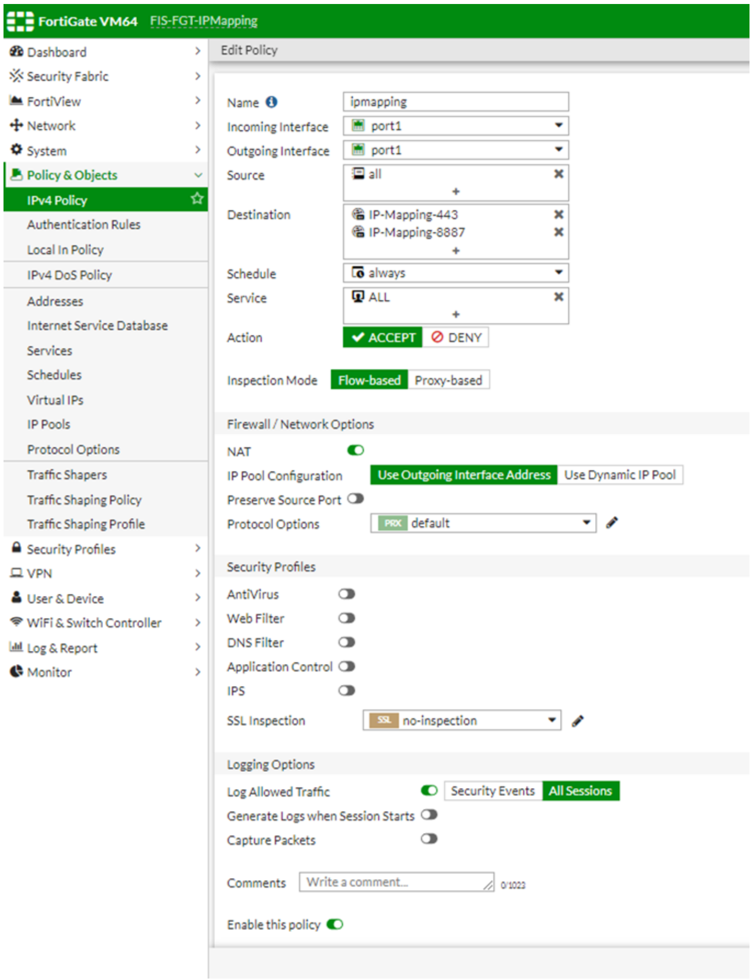
Optional Filters

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.



Edit Policy

Name ipmapping
Incoming Interface port1
Outgoing Interface port1
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] Use Dynamic IP Pool
Preserve Source Port ○
Protocol Options PRX default

Security Profiles

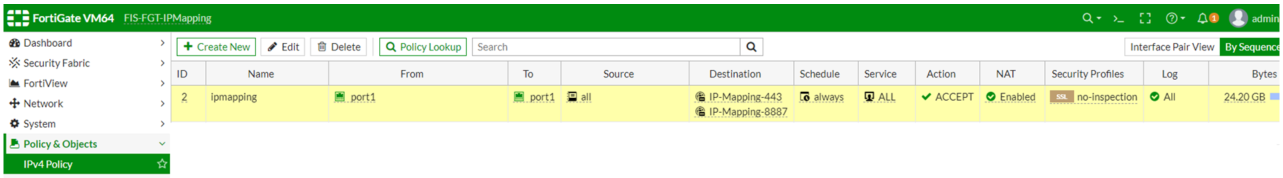
AntiVirus ○
Web Filter ○
DNS Filter ○
Application Control ○
IPS ○
SSL Inspection SSL no-inspection

Logging Options

Log Allowed Traffic ● Security Events [✓ All Sessions]
Generate Logs when Session Starts ○
Capture Packets ○

Comments Write a comment... 0/1023

Enable this policy ●

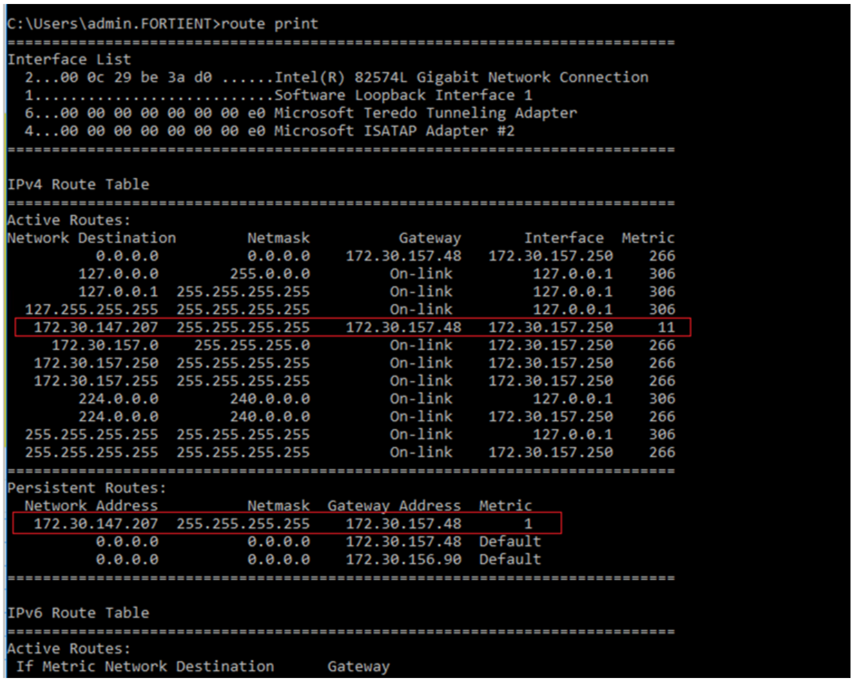


ID	Name	From	To	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
2	ipmapping	port1	port1	all	IP-Mapping-443 IP-Mapping-8887	always	ALL	✓ ACCEPT	✓ Enabled	SSL no-inspection	✓ All	24.20 GB

Client system configuration

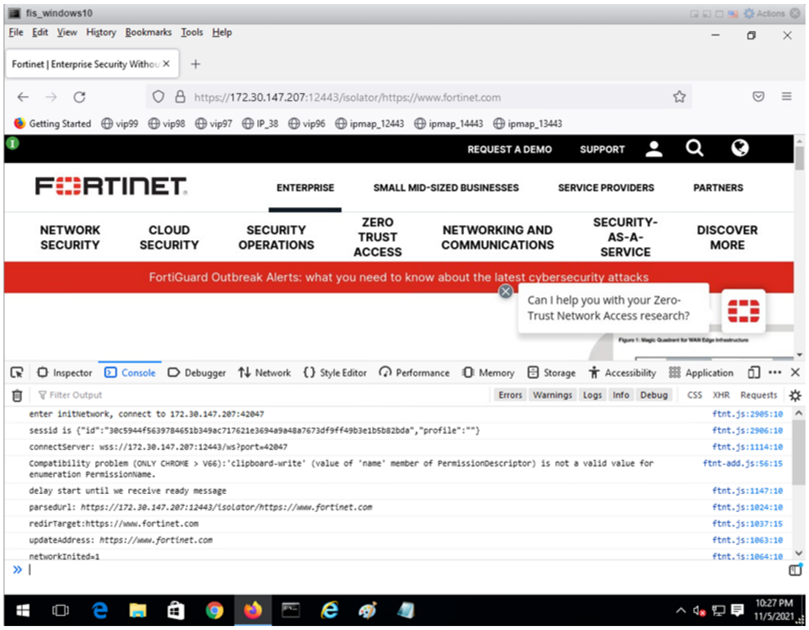
Complete the following steps on the client system (for example, Windows 10).

1. In Windows 10, launch CMD as administrator.
2. Use the following commands to add the FortiGate IP address to the routing table on the client system:
   a. At the command prompt, type
   ```
   route -p ADD <external_IP_address> Mask 255.255.255.255 <FGT_IP_address>
   ```
   For example,
   ```
   route -p ADD 172.30.147.207 MASK 255.255.255.255 172.30.157.48
   ```
   b. To confirm the setup, type `route print`.



```
C:\Users\admin.FORTIENT>route print
===========================================================================
Interface List
  2...00 0c 29 be 3a d0 ......Intel(R) 82574L Gigabit Network Connection
  1...........................Software Loopback Interface 1
  6...00 00 00 00 00 00 00 e0 Microsoft Teredo Tunneling Adapter
  4...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #2
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0    172.30.157.48  172.30.157.250    266
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    306
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    306
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    306
   172.30.147.207  255.255.255.255    172.30.157.48  172.30.157.250     11
     172.30.157.0    255.255.255.0         On-link    172.30.157.250    266
   172.30.157.250  255.255.255.255         On-link    172.30.157.250    266
   172.30.157.255  255.255.255.255         On-link    172.30.157.250    266
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    306
        224.0.0.0        240.0.0.0         On-link    172.30.157.250    266
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    306
  255.255.255.255  255.255.255.255         On-link    172.30.157.250    266
===========================================================================
Persistent Routes:
  Network Address          Netmask  Gateway Address  Metric
   172.30.147.207  255.255.255.255    172.30.157.48       1
          0.0.0.0          0.0.0.0    172.30.157.48  Default
          0.0.0.0          0.0.0.0     172.30.156.90  Default
===========================================================================

IPv6 Route Table
===========================================================================
Active Routes:
 If Metric Network Destination      Gateway
```

3. To verify that it works in a browser, browse to:
   ```
   https://<external_IP_address>:<port_map_to_443>/isolator/https://www.fortinet.com
   ```
   e.g.:
   ```
   https://172.30.147.207:12443/isolator/https://www.fortinet.com
   ```


fis_windows10
File Edit View History Bookmarks Tools Help
Fortinet | Enterprise Security Withou
https://172.30.147.207:12443/isolator/https://www.fortinet.com
Getting Started vip99 vip98 vip97 IP_38 vip96 ipmap_12443 ipmap_14443 ipmap_13443
REQUEST A DEMO
SUPPORT
FORTINET
ENTERPRISE
SMALL MID-SIZED BUSINESSES
SERVICE PROVIDERS
PARTNERS
NETWORK SECURITY
CLOUD SECURITY
SECURITY OPERATIONS
ZERO TRUST ACCESS
NETWORKING AND COMMUNICATIONS
SECURITY-AS-A-SERVICE
DISCOVER MORE
FortiGuard Outbreak Alerts: what you need to know about the latest cybersecurity attacks
Can I help you with your Zero-Trust Network Access research?
Inspector Console Debugger Network Style Editor Performance Memory Storage Accessibility Application
Filter Output
Errors Warnings Logs Info Debug CSS XHR Requests
10:27 PM
11/5/2021

```
enter initNetwork, connect to 172.30.147.207:42047                                      ftnt.js:2905:10
sessid is {"id":"30c5944f5639784651b349ac717621e3694a9a48a7673df9ff49b3e1b5b82bda","profile":""}   ftnt.js:2906:10
connectServer: wss://172.30.147.207:12443/ws?port=42047                                 ftnt.js:1114:10
Compatibility problem (ONLY CHROME > V66):'clipboard-write' (value of 'name' member of PermissionDescriptor) is not a valid value for
enumeration PermissionName.                                                             ftnt-add.js:56:15
delay start until we receive ready message                                              ftnt.js:1147:10
parsedUrl: https://172.30.147.207:12443/isolator/https://www.fortinet.com               ftnt.js:1024:10
redirTarget:https://www.fortinet.com                                                    ftnt.js:1037:15
updateAddress: https://www.fortinet.com                                                 ftnt.js:1063:10
networkInited=1                                                                         ftnt.js:1064:10
```

Configuring IP mapping in HA mode

Prerequisites:

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

Configuring IP Mapping in HA mode needs to set up in these systems:

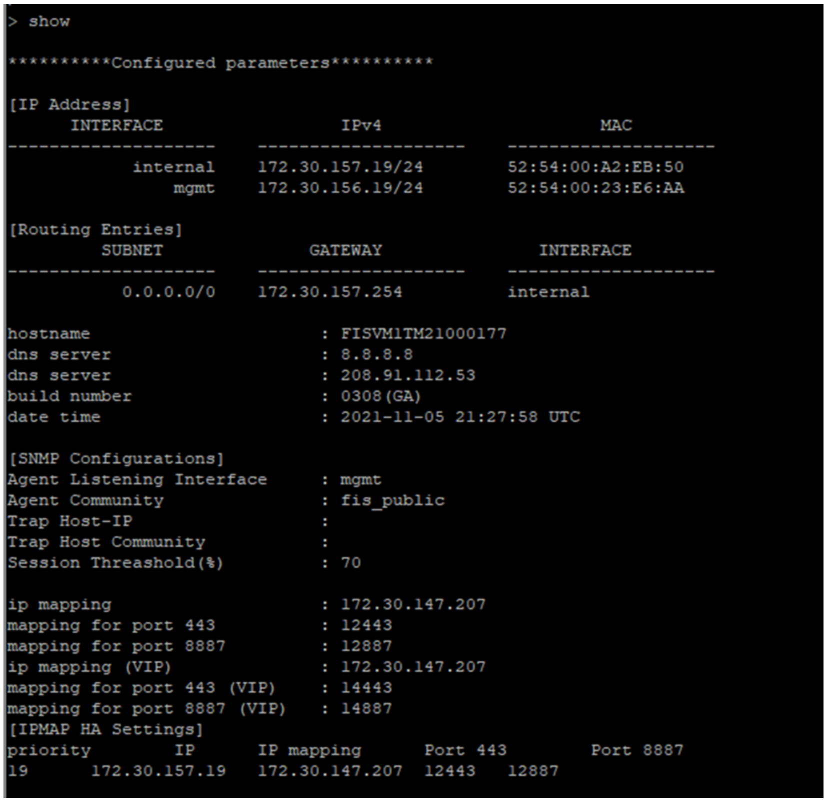
1. FortiIsolator configuration
2. FortiGate configuration
3. Client system configuration

Single-node setting (one-master only)

FortiIsolator configuration

Use FortiIsolator 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>`
   ```
   set fis-ipmap 12443 12887 172.30.147.207
   ```
2. `set fis-ipmap-vip <external IP> <vip_port_map_to_443> <vip_port_map_to_8887>`
   ```
   set fis-ipmap-vip 172.30.147.207 14443 14887
   ```
3. `set fis-ipmap-ha <priority> <external_IP_address> <internal_IP_address:master> <port_map_to_443> <port_map_to_8887>`
   ```
   set fis-ipmap-ha 19 172.30.147.207 172.30.157.19 12443 12887
   ```



```
> show

**********Configured parameters**********

[IP Address]
      INTERFACE                  IPv4                      MAC
--------------------    --------------------    --------------------
            internal    172.30.157.19/24        52:54:00:A2:EB:50
                mgmt    172.30.156.19/24        52:54:00:23:E6:AA

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

hostname                      : FISVM1TM21000177
dns server                    : 8.8.8.8
dns server                    : 208.91.112.53
build number                  : 0308(GA)
date time                     : 2021-11-05 21:27:58 UTC

[SNMP Configurations]
Agent Listening Interface     : mgmt
Agent Community               : fis_public
Trap Host-IP                  :
Trap Host Community           :
Session Threashold(%)         : 70

ip mapping                    : 172.30.147.207
mapping for port 443          : 12443
mapping for port 8887         : 12887
ip mapping (VIP)              : 172.30.147.207
mapping for port 443 (VIP)    : 14443
mapping for port 8887 (VIP)   : 14887
[IPMAP HA Settings]
priority        IP      IP mapping      Port 443        Port 8887
19      172.30.157.19   172.30.147.207  12443   12887
```

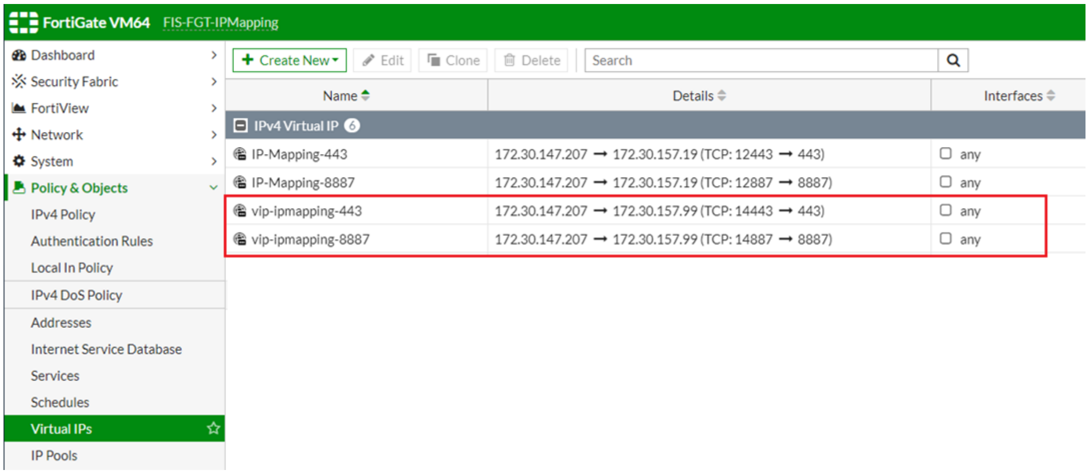
FortiGate configuration

Complete the following steps in the FortiGate UI.

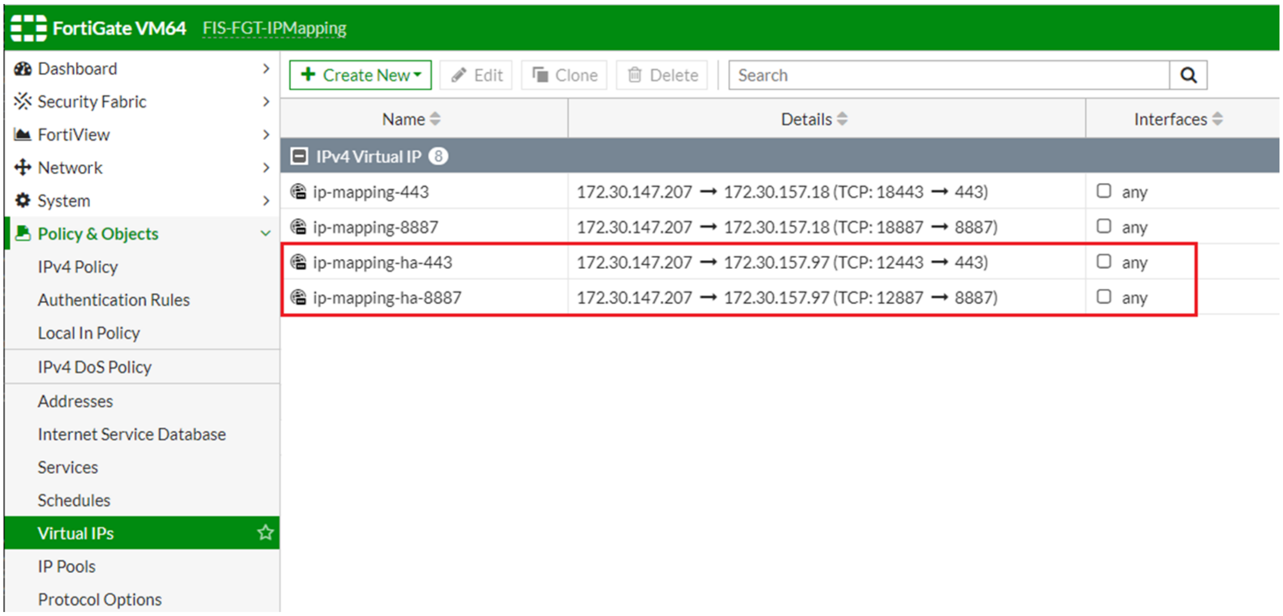
1. Go to *Policy & Objects* > *Virtual IPs*.
2. Create two IPv4 virtual IPs with the following information:
   - **IP-Mapping-443**: external_IP_address **->** FIS_IP (TCP: 12443 > 443)
     e.g. 172.30.147.207 **->** 172.30.157.97 (TCP: 12443 > 443)
   - **IP-Mapping-8887**: external_IP_address **->** FIS_IP (TCP: 12887 > 8887)
     e.g. 172.30.147.207 **->** 172.30.157.97 (TCP: 128887 > 8887)

In this example, we are using:

- External_IP_address: 172.30.147.207
- FIS HA Virtual IP: 172.30.157.99
- FIS_IP: 172.30.157.19

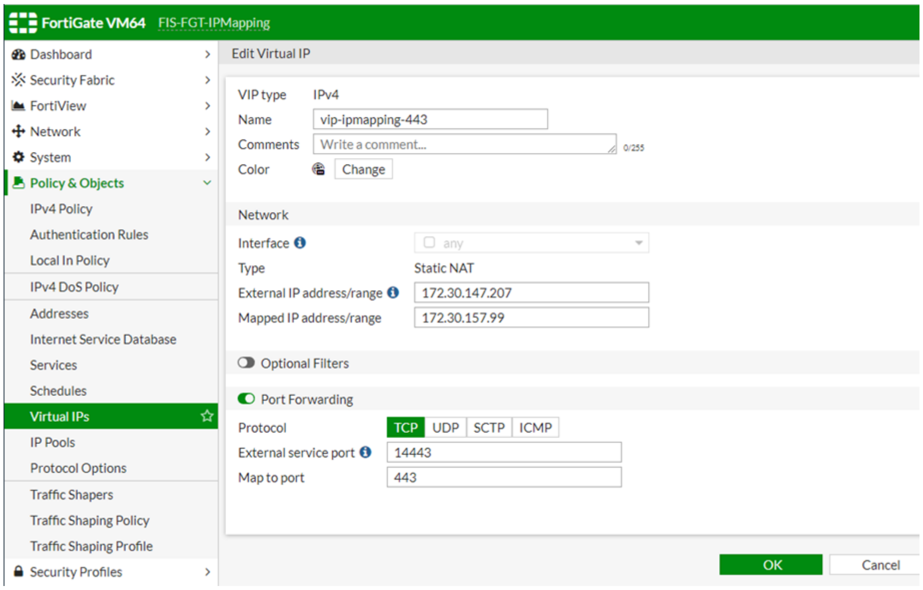


Name	Details	Interfaces
IPv4 Virtual IP 6		
IP-Mapping-443	172.30.147.207 → 172.30.157.19 (TCP: 12443 → 443)	□ any
IP-Mapping-8887	172.30.147.207 → 172.30.157.19 (TCP: 12887 → 8887)	□ any
vip-ipmapping-443	172.30.147.207 → 172.30.157.99 (TCP: 14443 → 443)	□ any
vip-ipmapping-8887	172.30.147.207 → 172.30.157.99 (TCP: 14887 → 8887)	□ any



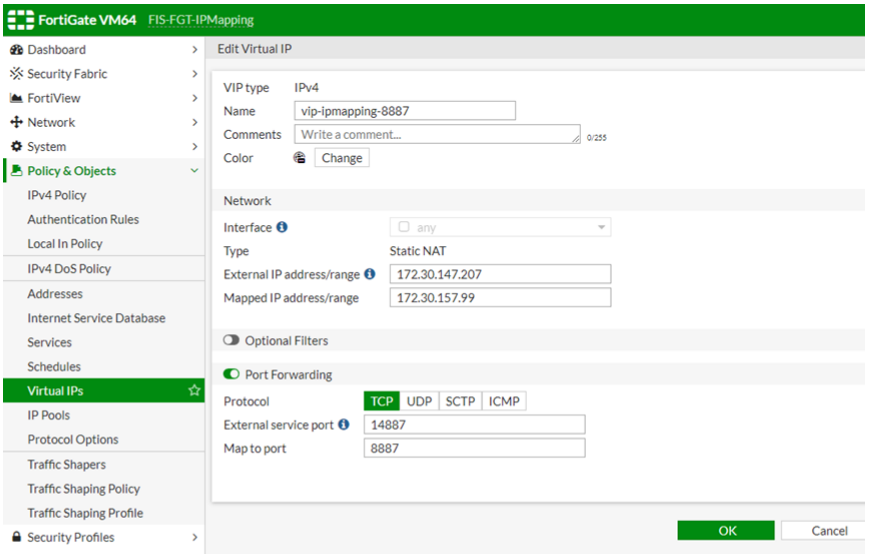
Name	Details	Interfaces
IPv4 Virtual IP 8		
ip-mapping-443	172.30.147.207 → 172.30.157.18 (TCP: 18443 → 443)	□ any
ip-mapping-8887	172.30.147.207 → 172.30.157.18 (TCP: 18887 → 8887)	□ any
ip-mapping-ha-443	172.30.147.207 → 172.30.157.97 (TCP: 12443 → 443)	□ any
ip-mapping-ha-8887	172.30.147.207 → 172.30.157.97 (TCP: 12887 → 8887)	□ any

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



VIP type	IPv4
Name	vip-ipmapping-443
Comments	Write a comment...
Network	
Interface	□ any
Type	Static NAT
External IP address/range	172.30.147.207
Mapped IP address/range	172.30.157.99
Optional Filters	○
Port Forwarding	●
Protocol	[✓ TCP] UDP SCTP ICMP
External service port	14443
Map to port	443

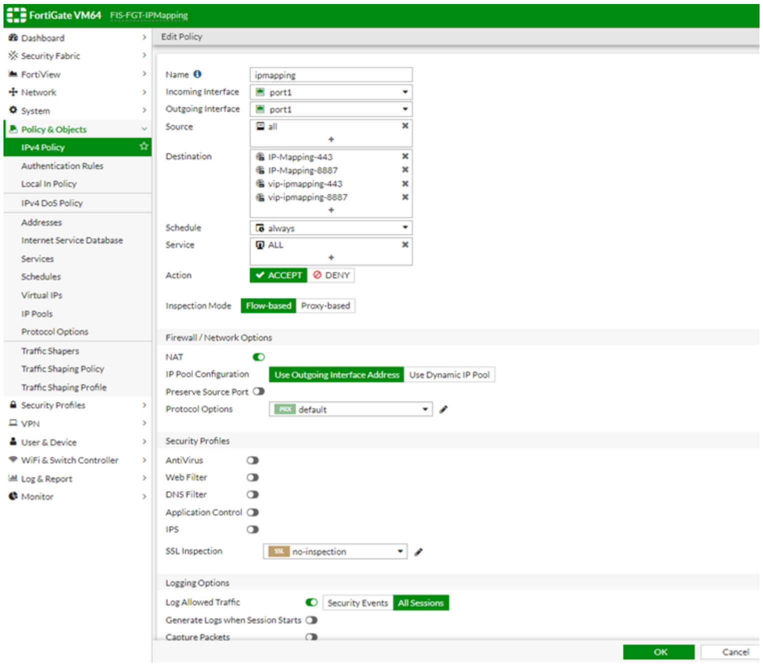
Settings of **IP-Mapping-HA-8887**:



VIP type	IPv4
Name	vip-ipmapping-8887
Comments	Write a comment...
Network	
Interface	□ any
Type	Static NAT
External IP address/range	172.30.147.207
Mapped IP address/range	172.30.157.99
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

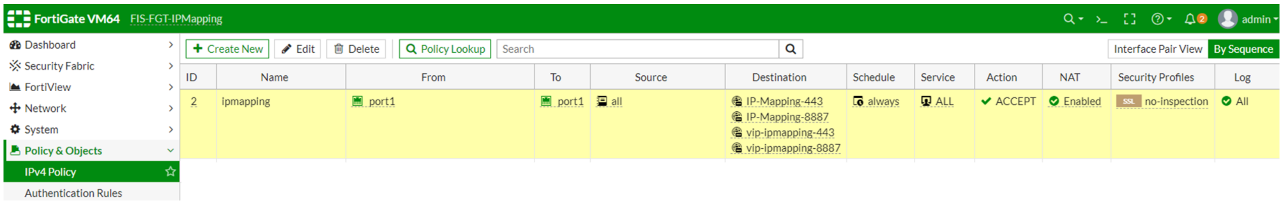
Edit Policy

Name: ipmapping
Incoming Interface: port1
Outgoing Interface: port1
Source: all
Destination: IP-Mapping-443, IP-Mapping-8887, vip-ipmapping-443, vip-ipmapping-8887
Schedule: always
Service: ALL
Action: ACCEPT
Inspection Mode: Flow-based

Firewall / Network Options
NAT: enabled
IP Pool Configuration: Use Outgoing Interface Address
Preserve Source Port: disabled
Protocol Options: default

Security Profiles
AntiVirus: disabled
Web Filter: disabled
DNS Filter: disabled
Application Control: disabled
IPS: disabled
SSL Inspection: no-inspection

Logging Options
Log Allowed Traffic: enabled, All Sessions
Generate Logs when Session Starts: disabled
Capture Packets: disabled



FortiGate VM64 FIS-FGT-IPMapping

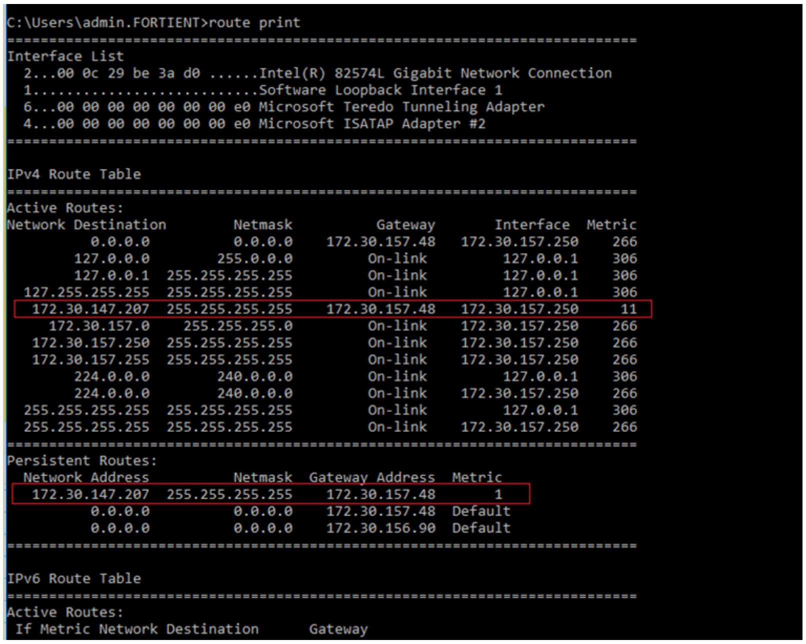
ID	Name	From	To	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log
2	ipmapping	port1	port1	all	IP-Mapping-443 IP-Mapping-8887 vip-ipmapping-443 vip-ipmapping-8887	always	ALL	✓ ACCEPT	Enabled	SSL no-inspection	All

Client system configuration

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

1. In Windows 10, launch CMD as administrator.
2. Use the following commands to add the FortiGate IP address to the routing table on the client system:
   a. At the command prompt, type `route -p ADD <external_IP_address> Mask 255.255.255.255 <FGT_IP_address>`.
      For example, `route -p ADD <external_IP_address> MASK 255.255.255.255 172.30.157.48`

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



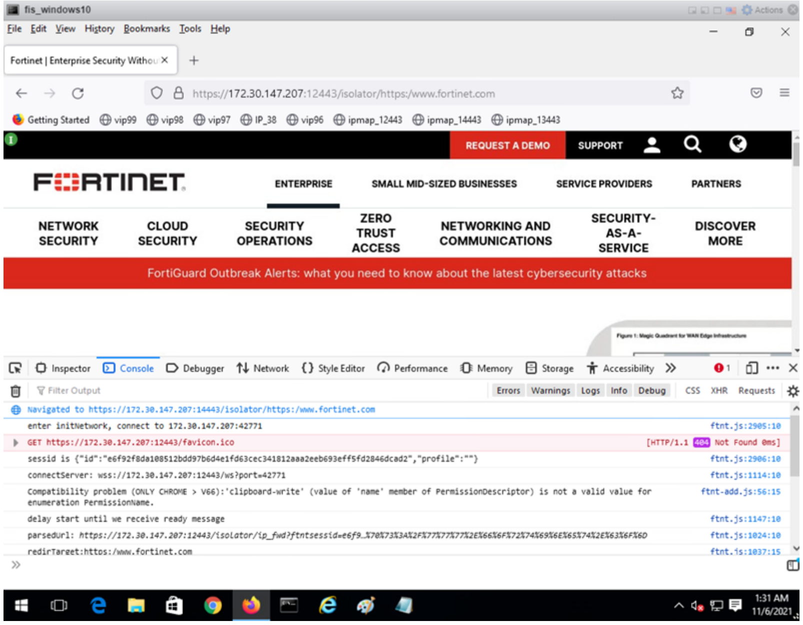
```
C:\Users\admin.FORTIENT>route print
===========================================================================
Interface List
  2...00 0c 29 be 3a d0 ......Intel(R) 82574L Gigabit Network Connection
  1...........................Software Loopback Interface 1
  6...00 00 00 00 00 00 00 e0 Microsoft Teredo Tunneling Adapter
  4...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #2
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0    172.30.157.48   172.30.157.250    266
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    306
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    306
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    306
   172.30.147.207  255.255.255.255    172.30.157.48   172.30.157.250     11
     172.30.157.0    255.255.255.0         On-link    172.30.157.250    266
   172.30.157.250  255.255.255.255         On-link    172.30.157.250    266
   172.30.157.255  255.255.255.255         On-link    172.30.157.250    266
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    306
        224.0.0.0        240.0.0.0         On-link    172.30.157.250    266
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    306
  255.255.255.255  255.255.255.255         On-link    172.30.157.250    266
===========================================================================
Persistent Routes:
  Network Address          Netmask  Gateway Address  Metric
   172.30.147.207  255.255.255.255    172.30.157.48       1
          0.0.0.0          0.0.0.0    172.30.157.48  Default
          0.0.0.0          0.0.0.0    172.30.156.90  Default
===========================================================================

IPv6 Route Table
===========================================================================
Active Routes:
 If Metric Network Destination      Gateway
```

3. To verify that it works in a browser, browse to:
`https://<external_IP_address>:<port_map_to_HA_443>/isolator/https://www.fortinet.com`

e.g.:

`https://172.30.147.207:14443/isolator/https://www.fortinet.com`

(It will now redirect to: `https://172.30.147.207:12443/isolator/https://www.fortinet.com`)



fis_windows10
File Edit View History Bookmarks Tools Help
Fortinet | Enterprise Security Withou
https://172.30.147.207:12443/isolator/https:/www.fortinet.com
Getting Started vip99 vip98 vip97 IP_38 vip96 ipmap_12443 ipmap_14443 ipmap_13443
REQUEST A DEMO
SUPPORT
FERTINET
ENTERPRISE
SMALL MID-SIZED BUSINESSES
SERVICE PROVIDERS
PARTNERS
NETWORK SECURITY
CLOUD SECURITY
SECURITY OPERATIONS
ZERO TRUST ACCESS
NETWORKING AND COMMUNICATIONS
SECURITY-AS-A-SERVICE
DISCOVER MORE
FortiGuard Outbreak Alerts: what you need to know about the latest cybersecurity attacks
Figure 1: Magic Quadrant for WAN Edge Infrastructure
Inspector Console Debugger Network Style Editor Performance Memory Storage Accessibility
Filter Output
Errors Warnings Logs Info Debug CSS XHR Requests
1:31 AM
11/6/2021

```
Navigated to https://172.30.147.207:14443/isolator/https:/www.fortinet.com
enter initNetwork, connect to 172.30.147.207:42771                                    ftnt.js:2905:10
GET https://172.30.147.207:12443/favicon.ico                            [HTTP/1.1 404 Not Found 0ms]
sessid is {"id":"e6f92f8da108512bdd97b6d4e1fd63cec341812aaa2eeb693eff5fd2846dcad2","profile":""}   ftnt.js:2906:10
connectServer: wss://172.30.147.207:12443/ws?port=42771                               ftnt.js:1114:10
Compatibility problem (ONLY CHROME > V66):'clipboard-write' (value of 'name' member of PermissionDescriptor) is not a valid value for
enumeration PermissionName.                                                          ftnt-add.js:56:15
delay start until we receive ready message                                            ftnt.js:1147:10
parsedUrl: https://172.30.147.207:12443/isolator/ip_fwd?ftntsessid=e6f9…%70%73%3A%2F%77%77%77%2E%66%6F%72%74%69%6E%65%74%2E%63%6F%6D   ftnt.js:1024:10
redirTarget:https:/www.fortinet.com                                                   ftnt.js:1037:15
```

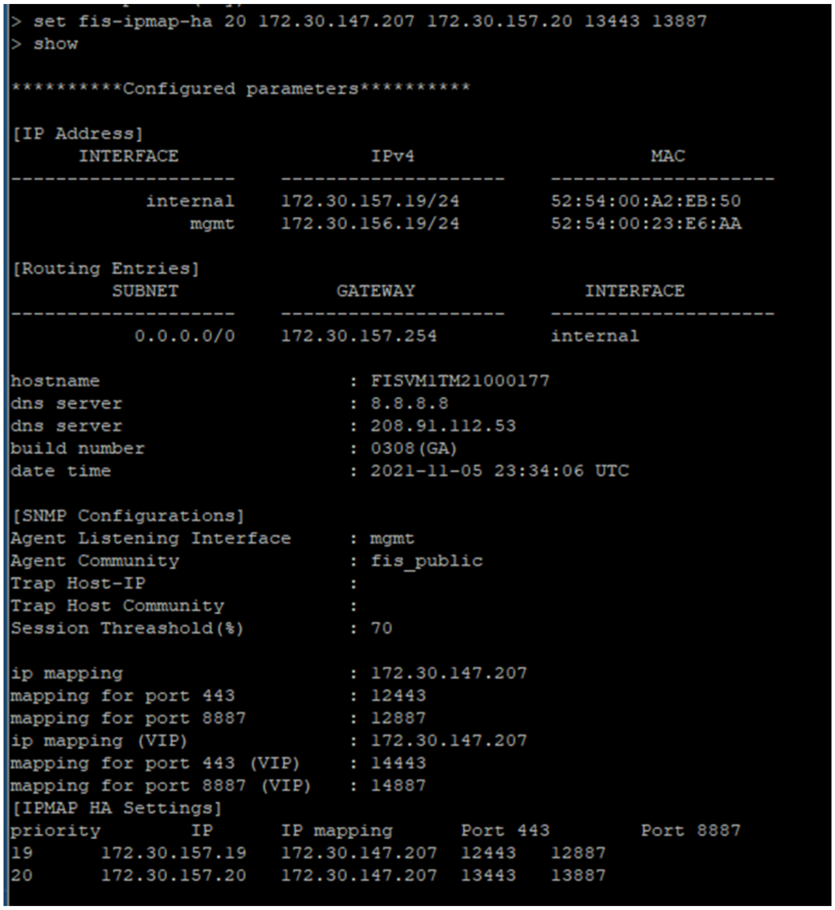
Multiple-nodes setting (one-master-one-slave)

FortiIsolator configuration

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

Under FIS Master:

1. `set fis-ipmap <port_map_to_443> <port_map_to_8887> <external_IP_address>`
   - `set fis-ipmap 12443 12887 172.30.147.207`
2. `set fis-ipmap-vip <external IP> <vip_port_map_to_443> <vip_port_map_to_8887>`
   - `set fis-ipmap-vip 172.30.147.207 14443 14887`
3. `set fis-ipmap-ha <priority> <external_IP_address> <internal_IP_address:master> <port_map_to_443> <port_map_to_8887>`
   - `set fis-ipmap-ha 19 172.30.147.207 172.30.157.19 12443 12887`
4. `set fis-ipmap-ha <priority> <external_IP_address> <internal_IP_address:slave1> <port_map_to_443> <port_map_to_8887>`
   - `set fis-ipmap-ha 20 172.30.147.207 172.30.157.20 13443 13887`

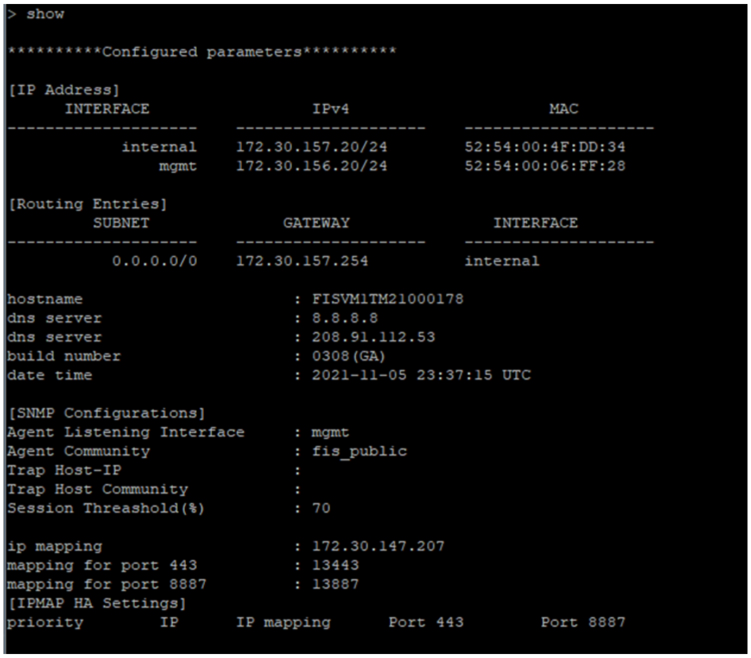


```
> set fis-ipmap-ha 20 172.30.147.207 172.30.157.20 13443 13887
> show

**********Configured parameters**********

[IP Address]
      INTERFACE                IPv4                      MAC
--------------------    --------------------    --------------------
            internal    172.30.157.19/24        52:54:00:A2:EB:50
                mgmt    172.30.156.19/24        52:54:00:23:E6:AA

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

hostname                      : FISVM1TM21000177
dns server                    : 8.8.8.8
dns server                    : 208.91.112.53
build number                  : 0308(GA)
date time                     : 2021-11-05 23:34:06 UTC

[SNMP Configurations]
Agent Listening Interface     : mgmt
Agent Community               : fis_public
Trap Host-IP                  :
Trap Host Community           :
Session Threashold(%)         : 70

ip mapping                    : 172.30.147.207
mapping for port 443          : 12443
mapping for port 8887         : 12887
ip mapping (VIP)              : 172.30.147.207
mapping for port 443 (VIP)    : 14443
mapping for port 8887 (VIP)   : 14887
[IPMAP HA Settings]
priority        IP      IP mapping      Port 443        Port 8887
19      172.30.157.19   172.30.147.207  12443   12887
20      172.30.157.20   172.30.147.207  13443   13887
```

5. **Under FIS slave**

   `set fis-ipmap <port_map_to_443> <port_map_to_8887> <external_IP_address>`

- `set fis-ipmap 13443 13887 172.30.147.207`



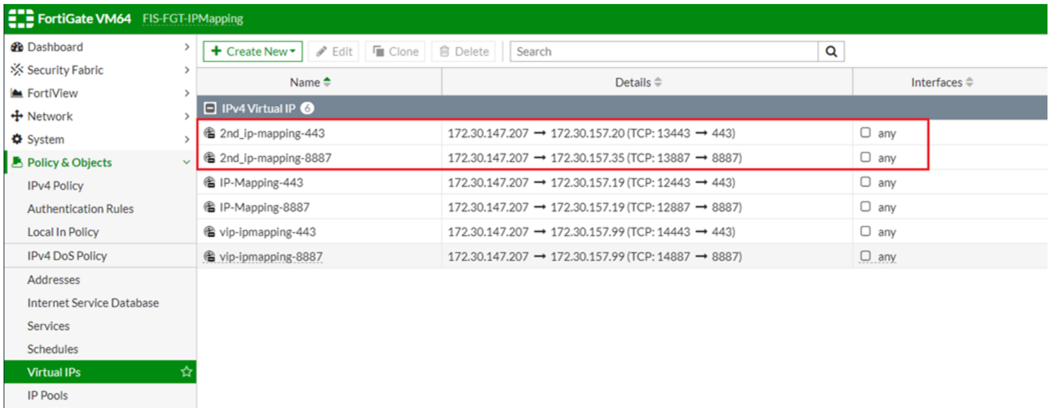
```
> show

**********Configured parameters**********

[IP Address]
      INTERFACE              IPv4                     MAC
--------------------    --------------------    --------------------
            internal    172.30.157.20/24        52:54:00:4F:DD:34
                mgmt    172.30.156.20/24        52:54:00:06:FF:28

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

hostname                       : FISVM1TM21000178
dns server                     : 8.8.8.8
dns server                     : 208.91.112.53
build number                   : 0308(GA)
date time                      : 2021-11-05 23:37:15 UTC

[SNMP Configurations]
Agent Listening Interface      : mgmt
Agent Community                : fis_public
Trap Host-IP                   :
Trap Host Community            :
Session Threashold(%)          : 70

ip mapping                     : 172.30.147.207
mapping for port 443           : 13443
mapping for port 8887          : 13887
[IPMAP HA Settings]
priority        IP      IP mapping      Port 443        Port 8887
```

Summary of examples

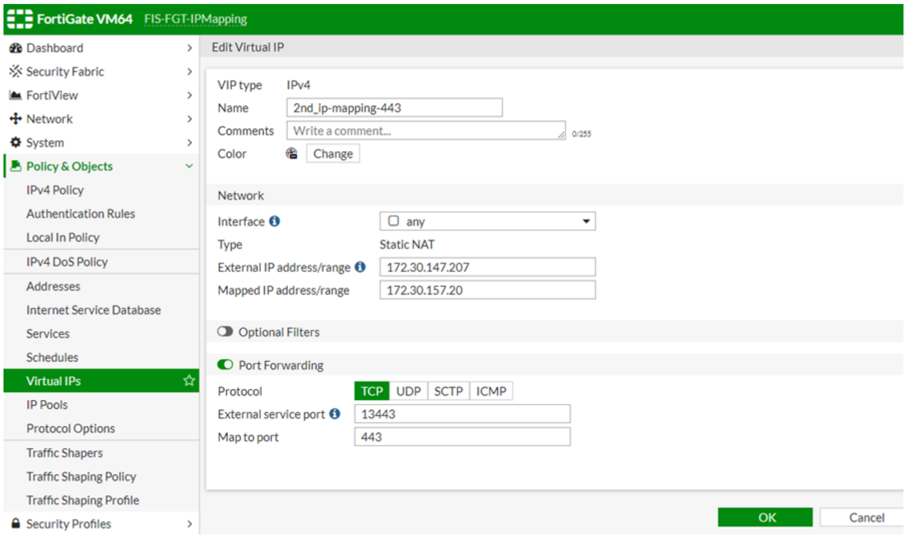
```
Master: 172.30.156.19
> set fis-ipmap 12443 12887 172.30.147.207
> set fis-ipmap-vip 172.30.147.207 14443 14887

> set fis-ipmap-ha 19 172.30.147.207 172.30.157.19 12443 12887
> set fis-ipmap-ha 20 172.30.147.207 172.30.157.20 13443 13887
Slave: 172.30.156.20
> set fis-ipmap 13443 13887 172.30.147.207
```

FortiGate configuration

Follow the FortiGate configuration in Configuring IP mapping in regular mode on page 53 to create IPv4 Virtual IP mapping for Slave node under Virtual IPs.



Name	Details	Interfaces
IPv4 Virtual IP 6		
2nd_ip-mapping-443	172.30.147.207 → 172.30.157.20 (TCP: 13443 → 443)	□ any
2nd_ip-mapping-8887	172.30.147.207 → 172.30.157.35 (TCP: 13887 → 8887)	□ any
IP-Mapping-443	172.30.147.207 → 172.30.157.19 (TCP: 12443 → 443)	□ any
IP-Mapping-8887	172.30.147.207 → 172.30.157.19 (TCP: 12887 → 8887)	□ any
vip-ipmapping-443	172.30.147.207 → 172.30.157.99 (TCP: 14443 → 443)	□ any
vip-ipmapping-8887	172.30.147.207 → 172.30.157.99 (TCP: 14887 → 8887)	□ any



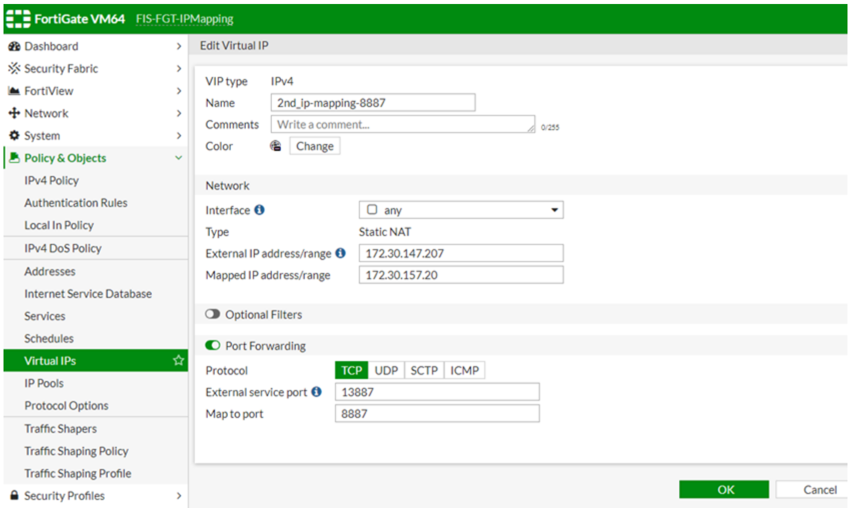
Edit Virtual IP

VIP type IPv4
Name 2nd_ip-mapping-443
Comments Write a comment... 0/255
Color Change

Network
Interface □ any
Type Static NAT
External IP address/range 172.30.147.207
Mapped IP address/range 172.30.157.20

Optional Filters

Port Forwarding
Protocol TCP UDP SCTP ICMP
External service port 13443
Map to port 443



Edit Virtual IP

VIP type IPv4
Name 2nd_ip-mapping-8887
Comments Write a comment... 0/255
Color Change

Network
Interface □ any
Type Static NAT
External IP address/range 172.30.147.207
Mapped IP address/range 172.30.157.20

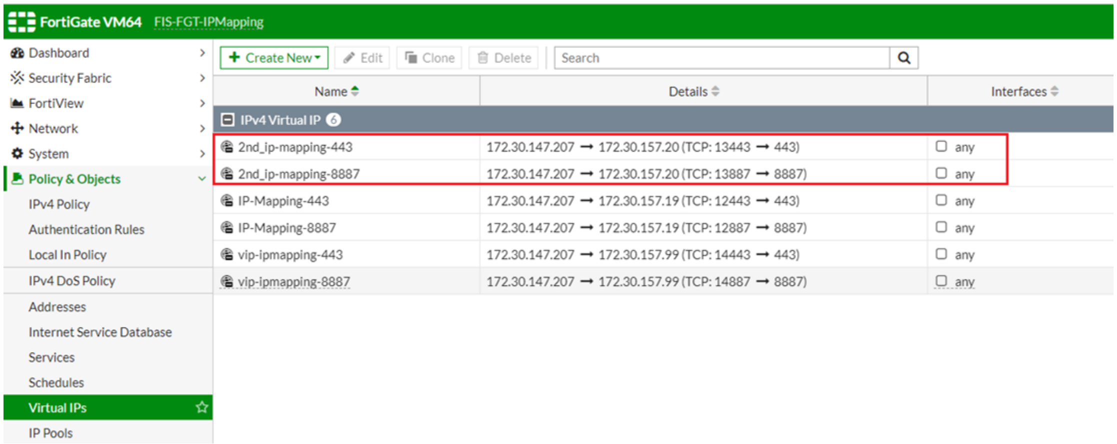
Optional Filters

Port Forwarding
Protocol TCP UDP SCTP ICMP
External service port 13887
Map to port 8887

Complete the following steps in the FortiGate UI.

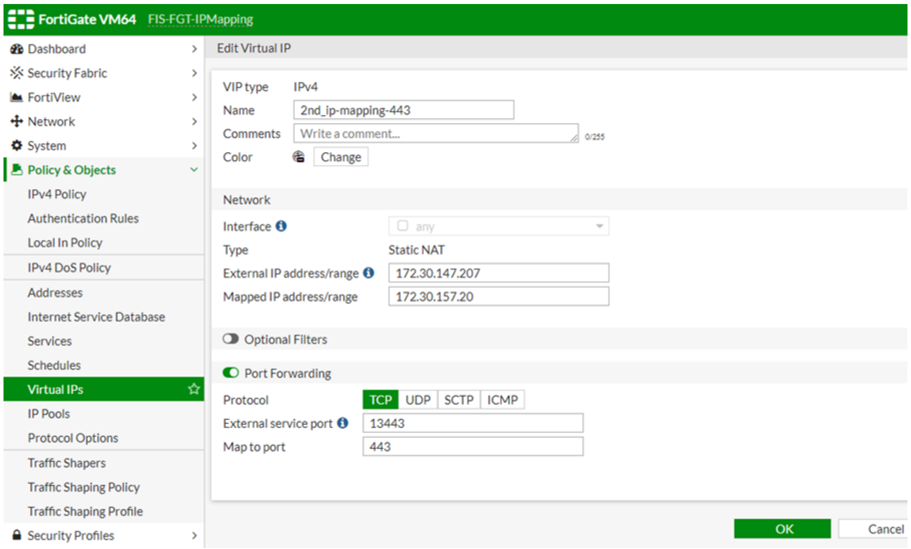
1. Go to **Policy & Objects > Virtual IPs.**
2. Create two IPv4 virtual IPs with the following information:
   - **IP-Mapping-HA-443**: external_IP_address -> FIS_IP (TCP: 14443 > 443)
     e.g. 172.30.147.207 -> 172.30.157.99 (TCP: 14443 > 443)
   - **IP-Mapping-HA-8887**: external_IP_address -> FIS_IP (TCP: 14887 > 8887)
     e.g. 172.30.147.207 -> 172.30.157.99 (TCP: 14887 > 8887)

The example uses the following:
External_IP_address: 172.30.147.207
FIS HA Virtual IP: 172.30.157.99
FIS_IP_Master: 172.30.157.19
FIS_IP_Slave: 172.30.157.20



Name	Details	Interfaces
IPv4 Virtual IP 6		
2nd_ip-mapping-443	172.30.147.207 → 172.30.157.20 (TCP: 13443 → 443)	any
2nd_ip-mapping-8887	172.30.147.207 → 172.30.157.20 (TCP: 13887 → 8887)	any
IP-Mapping-443	172.30.147.207 → 172.30.157.19 (TCP: 12443 → 443)	any
IP-Mapping-8887	172.30.147.207 → 172.30.157.19 (TCP: 12887 → 8887)	any
vip-ipmapping-443	172.30.147.207 → 172.30.157.99 (TCP: 14443 → 443)	any
vip-ipmapping-8887	172.30.147.207 → 172.30.157.99 (TCP: 14887 → 8887)	any

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



Edit Virtual IP

VIP type IPv4
Name 2nd_ip-mapping-443
Comments Write a comment... 0/255
Color

Network

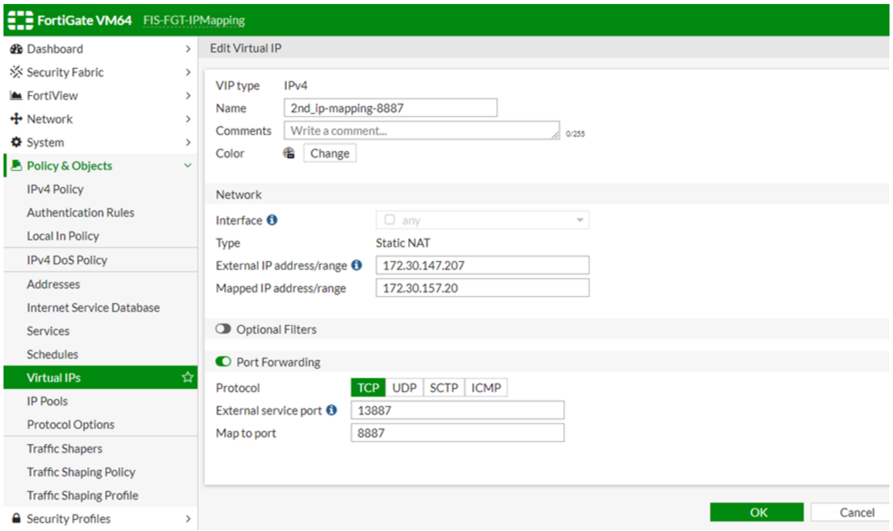
Interface any
Type Static NAT
External IP address/range 172.30.147.207
Mapped IP address/range 172.30.157.20

Optional Filters

Port Forwarding

Protocol TCP UDP SCTP ICMP
External service port 13443
Map to port 443

Settings of **IP-Mapping-HA-8887:**



Edit Virtual IP

VIP type IPv4
Name 2nd_ip-mapping-8887
Comments Write a comment... 0/255
Color

Network

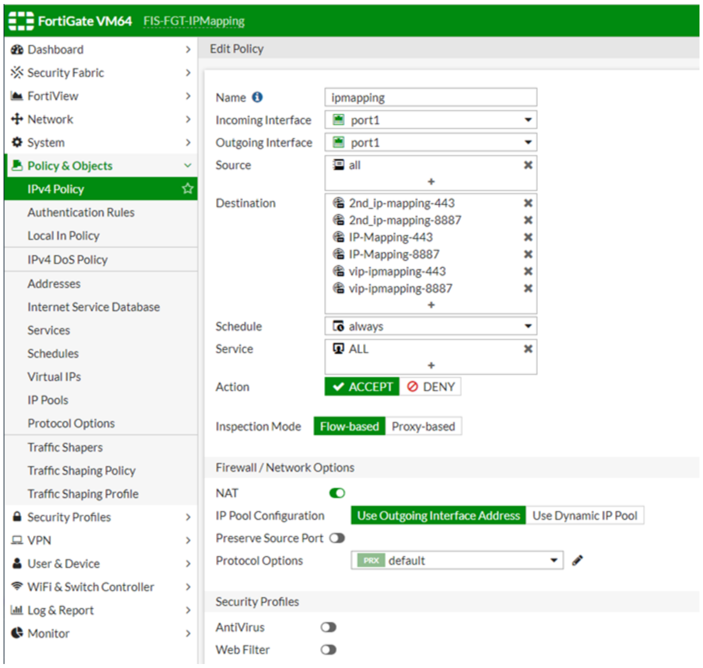
Interface any
Type Static NAT
External IP address/range 172.30.147.207
Mapped IP address/range 172.30.157.20

Optional Filters

Port Forwarding

Protocol TCP UDP SCTP ICMP
External service port 13887
Map to port 8887

3. Go to *Policy & Objects* > *IPv4 Policy* > *Create New*.
4. Create an IPv4 policy that includes the two more virtual IPs that you created.



Edit Policy

Name: ipmapping
Incoming Interface: port1
Outgoing Interface: port1
Source: all
Destination: 2nd_ip-mapping-443
2nd_ip-mapping-8887
IP-Mapping-443
IP-Mapping-8887
vip-ipmapping-443
vip-ipmapping-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] Use Dynamic IP Pool
Preserve Source Port: ○
Protocol Options: PROX default

Security Profiles

AntiVirus: ○
Web Filter: ○

Client system configuration

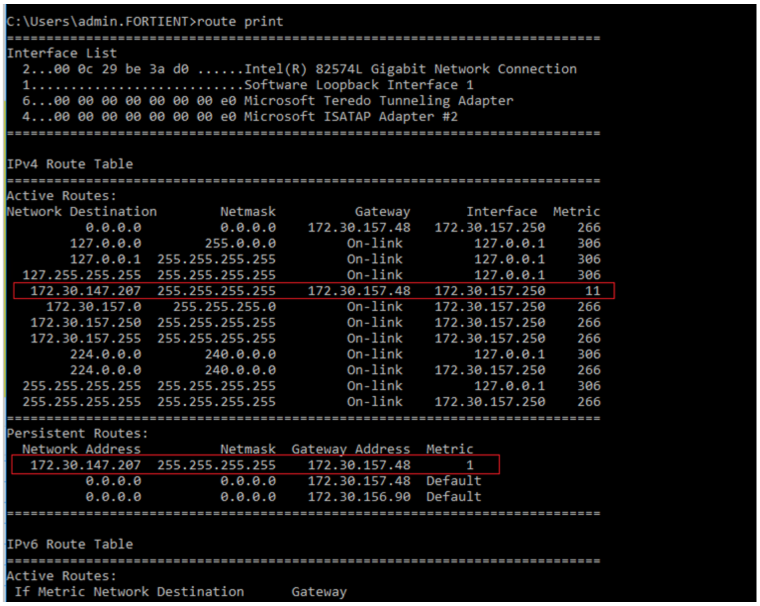
Complete the following steps on the client system (for example, Windows 10).

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

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

     For example,

     `route -p ADD 172.30.147.207 MASK 255.255.255.255 172.30.157.48`
   - To confirm the setup, type `route print`.



```
C:\Users\admin.FORTIENT>route print
===========================================================================
Interface List
  2...00 0c 29 be 3a d0 ......Intel(R) 82574L Gigabit Network Connection
  1...........................Software Loopback Interface 1
  6...00 00 00 00 00 00 00 e0 Microsoft Teredo Tunneling Adapter
  4...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #2
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0    172.30.157.48   172.30.157.250    266
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    306
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    306
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    306
   172.30.147.207  255.255.255.255    172.30.157.48   172.30.157.250     11
     172.30.157.0    255.255.255.0         On-link    172.30.157.250    266
   172.30.157.250  255.255.255.255         On-link    172.30.157.250    266
   172.30.157.255  255.255.255.255         On-link    172.30.157.250    266
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    306
        224.0.0.0        240.0.0.0         On-link    172.30.157.250    266
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    306
  255.255.255.255  255.255.255.255         On-link    172.30.157.250    266
===========================================================================
Persistent Routes:
  Network Address          Netmask  Gateway Address  Metric
   172.30.147.207  255.255.255.255    172.30.157.48       1
          0.0.0.0          0.0.0.0    172.30.157.48  Default
          0.0.0.0          0.0.0.0    172.30.156.90  Default
===========================================================================

IPv6 Route Table
===========================================================================
Active Routes:
 If Metric Network Destination      Gateway
```

3. To verify that it works in a browser, browse to:
   https://<external_IP_address>:<port_map_to_HA_443>/isolator/https://www.fortinet.com
   e.g.:
   https://172.30.147.207:14443/isolator/https://www.fortinet.com
   (It will now redirect to Master node: https://172.30.147.207:12443/isolator/https://www.fortinet.com
   Or, it will redirect to Slave node:
   https://172.30.147.207:13443/isolator/https://www.fortinet.com
)

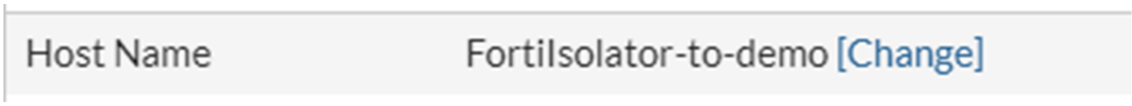
Dashboard

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

Changing host name

To change the *Host Name* from GUI:

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



Host Name FortiIsolator-to-demo [Change]

To change *Host Name* from CLI:

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

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

Configuring system time

To configure time settings for FortiIsolator from GUI:

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

To setup system time from CLI:

```
> set timezone
```

VM license

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

To upload a license from GUI:

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

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

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

System configuration

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

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

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

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

Backing up the configuration

To backup the configuration:

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

Restoring a configuration

To restore the FortiIsolator configuration:

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

FortiIsolator CA certificate

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

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

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

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

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

To revert to the default CA certificate:

1. In the *Re-Generate Isolator CA certificate* section, click the link in *Click here to generate Default CA certificate*.
   The default CA Certificate will be restored and the FortiIsolator will reboot, which might take a few minutes.

To use a custom-generated CA certificate:

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

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

To back up the current CA certificate:

1. In the *Backup CA certificate* section, click the link in *Click here to save your backup file* to save your backup file.
   This will save `ca.tgz` file into your local system; you can store it in a secure place for when you need to restore the system.

To use a local CA certificate:

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

1. Depending on the file type of the local certificate, go to the *Restore CA certificates by tgz file* or *Restore CA certificates by files* section.
2. Click *Choose File* to upload the local CA certificate file(s).
3. Specify the password(s), if any.
4. Click *Restore*.
5. Click *OK*.
   The local CA certificate will be used and the FortiIsolator will be rebooted, which might take a few minutes. If the CA certificate is a global CA certificate that grants global access to websites at browser level, follow the next two sections to upload the corresponding server certificate and management certificate for the whole certificate chain to work.

To use a local server certificate:

1. In the *Restore Server certificates by files*, click *Choose File* to upload the certificate and key. Make sure the server certificate is a match of the current CA certificate.
2. Specify the password and domain name, if any.
3. Click *Restore*.
4. Click *OK*.
   The local server certificate will be used and the FortiIsolator will be rebooted, which might take a few minutes.

To use a local management certificate:

1. In the *Restore Management certificates by files*, click *Choose File* to upload the certificate and key. Make sure the management certificate is a match of the current CA certificate.
2. Click *Restore*.
3. Click *OK*.
   The local management certificate will be used and the FortiIsolator will be rebooted, which might take a few minutes.

Network

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

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

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

Interfaces

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

Setting the management IP address

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

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

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

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

Setting the internal IP address and gateway

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

1. Go to *Portal* > *Network* > *Interface*.
2. Select Internal interface and then Edit it.
3. Follow IPv4 address with subnet format: e.g. 192.168.2.99/255.255.255.0.

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

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

Setting the external IP address and gateway

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

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

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

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

Setting the HA IP address and gateway

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

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

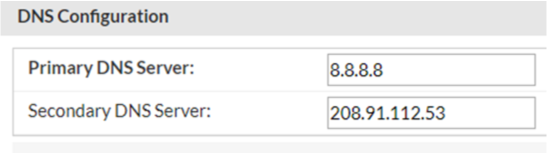
To change the HA IP address from CLI, use the following command:

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

System DNS

To setup system DNS from GUI:

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



DNS Configuration

Primary DNS Server:	8.8.8.8
Secondary DNS Server:	208.91.112.53

To setup system DNS from CLI:

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

System routing

Configuring routing settings

Use this procedure to configure routing settings for FortiIsolator.

Adding a static route

To add a static route:

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

Editing a static route

To edit a static route:

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

Deleting a static route

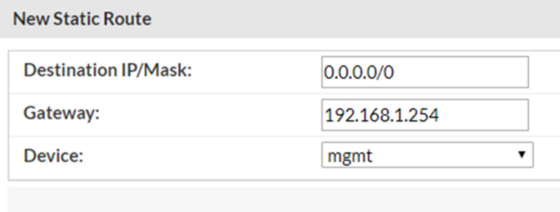
To delete a static route:

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

Setting up system routing for management IP

To set up system routing for management IP from GUI:

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



New Static Route

Destination IP/Mask:	0.0.0.0/0
Gateway:	192.168.1.254
Device:	mgmt

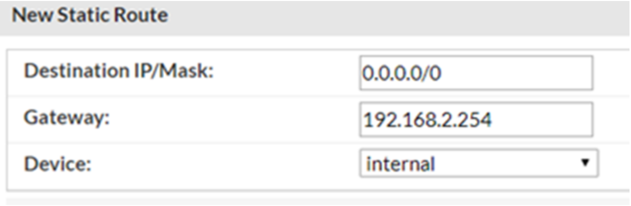
To set up system routing for management IP from CLI:

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

Setting up system routing for internal IP

To set up system routing for internal IP from GUI:

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



New Static Route

Destination IP/Mask: 0.0.0.0/0

Gateway: 192.168.2.254

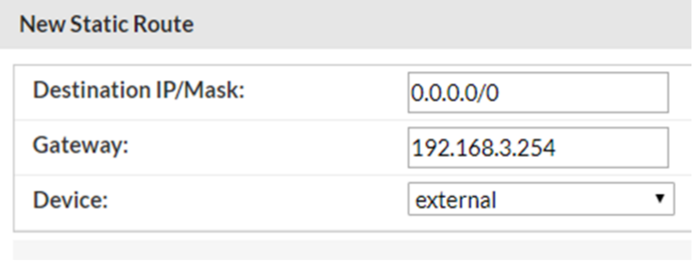
Device: internal

To set up system routing for internal IP from CLI:

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

To setup system routing for external IP from GUI:

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



New Static Route

Destination IP/Mask: 0.0.0.0/0

Gateway: 192.168.3.254

Device: external

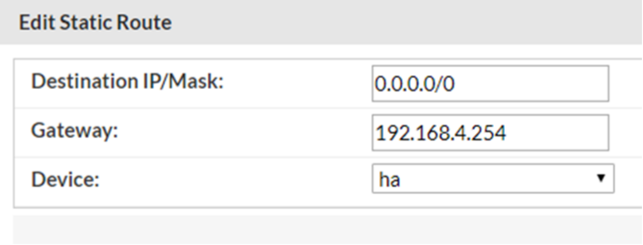
To set up system routing for external IP from CLI:

```
> set external-gw/<subnet> <gateway>
e.g.
> set external-gw 0.0.0.0/0 192.168.3.254
```

To set up system routing for HA IP from GUI:

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

3. Click *OK* to save it.



Edit Static Route

Destination IP/Mask:	0.0.0.0/0
Gateway:	192.168.4.254
Device:	ha

To set up system routing for HA IP from CLI:

```
> set ha-gw/<subnet> <gateway>
e.g.
> set ha-gw 0.0.0.0/0 192.168.4.254
```

Configuring multiple routing on one interface

FortiIsolator supports multiple routes per interface.

Setting up multiple routes on one interface from CLI

Creating FortiIsolator profile from CLI needs to follow this format:

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

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

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

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

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

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

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

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

To set multiple routes on one interface from GUI:

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

Forwarding server

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

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

Configuring forwarding server from GUI

To configure forwarding server from GUI:

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

Configuring forwarding server from CLI

To configure forwarding server from CLI:

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

System

The *System* section of FortiIsolator covers the following:

- Administrators
- High Availability (HA)
- Certificates
- SNMP
- Login disclaimer
- Upgrade
- Install Package

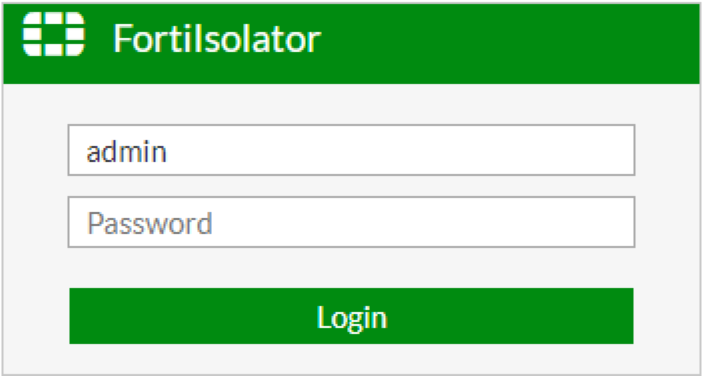
Administrators

Accessing the FortiIsolator administration portal

Logging in as administrator

To log in as an administrator:

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



2. Type in your username and password to access the administration portal. 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

To change the administrator password:

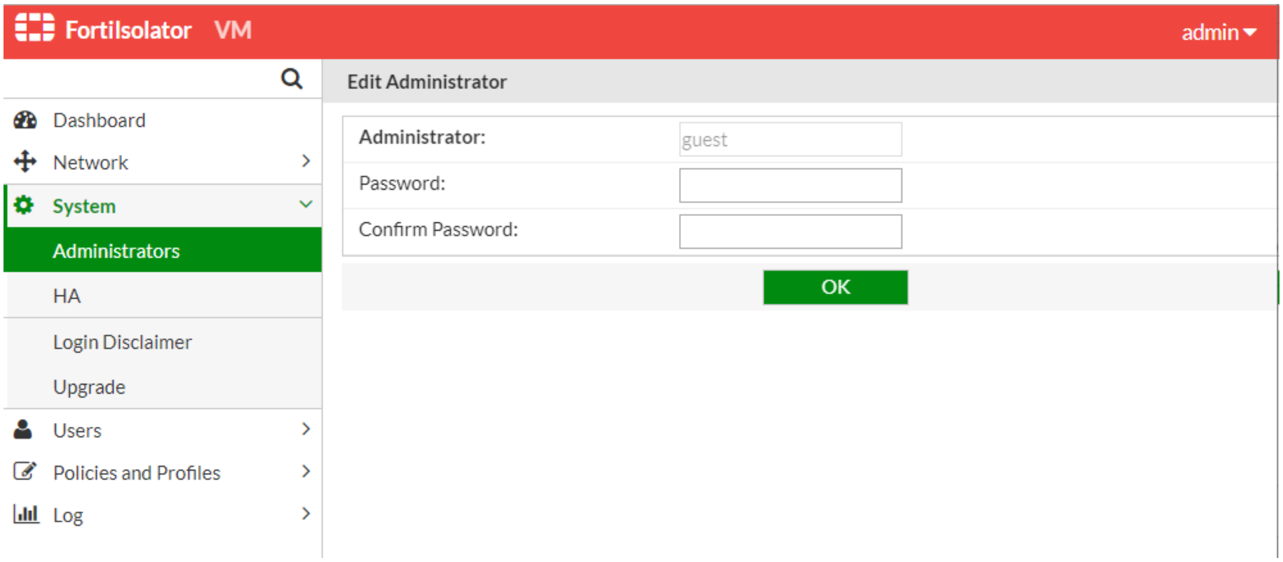
1. In the top-right corner of the administration portal, click the admin username.
2. Click *Change Password*.
3. In the *Password* field, type the new password.
4. In the *Confirm Password* field, type the new password again.
5. Click *OK*.

Setting up guest administer account

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

To set up a guest administer account:

1. Within the administration portal, go to *System* > *Administrators* and double-click the *guest* Administrator row, or select the *guest* Administrator row and click *Edit*.
2. The guest administrator account has a preset username of *guest*, and defaults to no password. Add a password if desired.



Administrator: guest
Password:
Confirm Password:

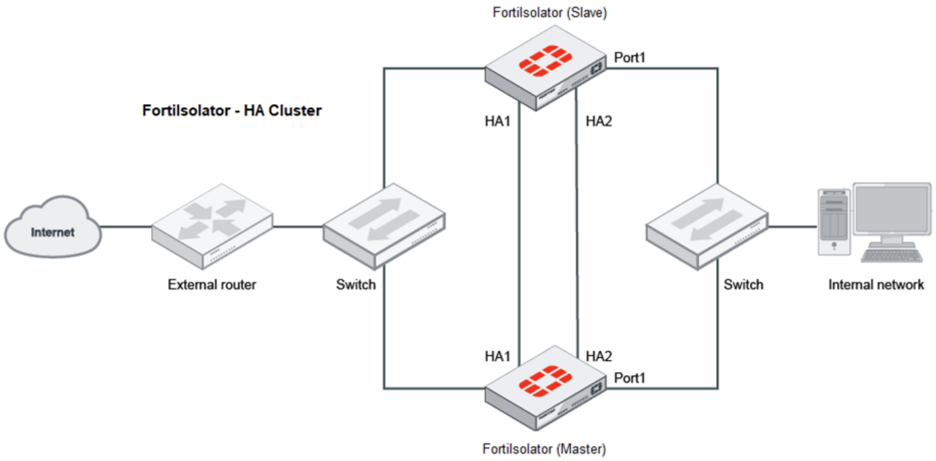
3. Click *OK* to save and apply the settings.

High Availability

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

Architecture

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



Configuration

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

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

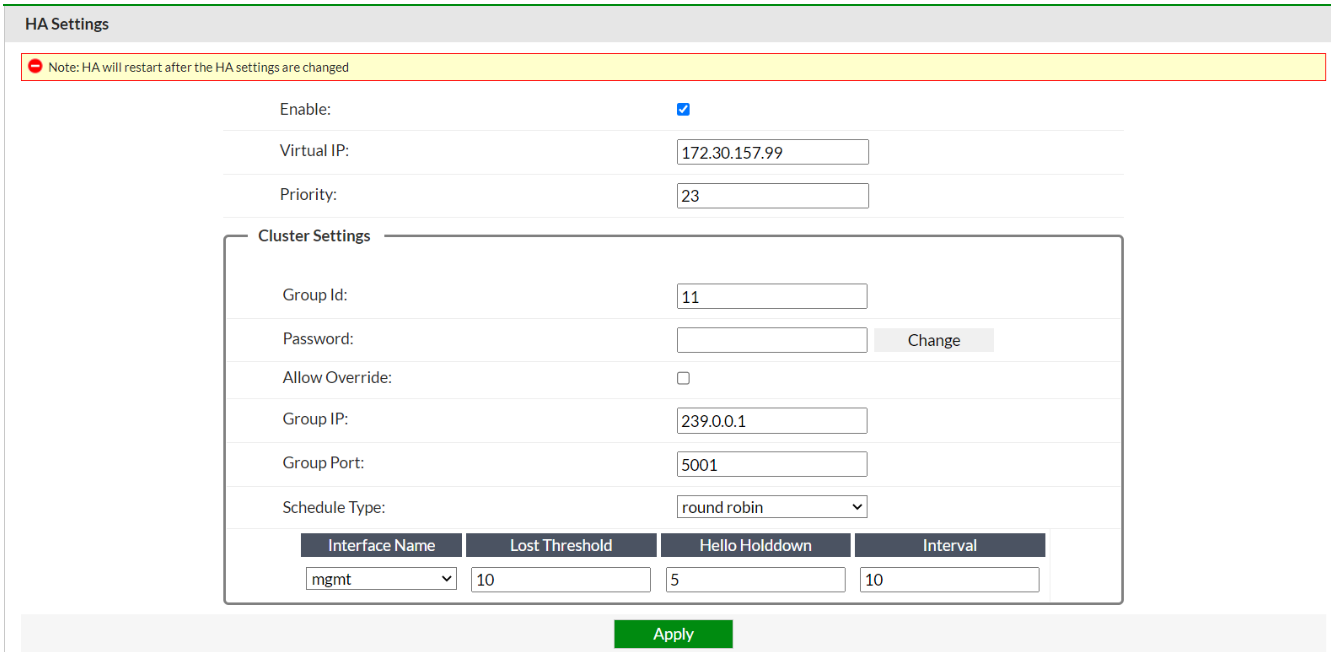
GUI

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

Parameter	Description
Enable	Specifies whether to enable HA mode for this node.
Virtual IP	IP for web browsers access from all nodes in the cluster. Only the primary device has virtual IP address, which is shared among all nodes within the cluster so all nodes can use this same virtual IP address to access sites. The virtual IP address must be the same subnet as the internal interface. In HA mode, web browsers access the virtual IP address in the following modes: • *IP Forwarding*—The web browser first connects to the virtual IP address of the primary node which then forwards the request to itself or another node in the cluster through the internal IP of the recipient node in the cluster, which

Parameter	Description
	can be the primary node itself or a secondary node. • *Proxy*—The web browser connects to the virtual IP address of the primary node and keeps communicating with the primary node, which then connects to a node (can be the primary node itself) on its internal IP through web socket connection. The web browser then runs the session on that node.
Priority	Priority of the node indicated with an integer between 0 to 254, where 0 means the highest priority. You must assign a unique priority ID to each node. The node with the highest priority ID automatically becomes the primary device of the HA cluster.
Group Id	A unique number to identify the cluster. One Group ID number represents one cluster, while different Group ID numbers represent different clusters. Group ID must be an integer between 1 – 255.
Password	Password for the group, which protects the cluster from unauthorized access.
Allow Override	Specifies whether to allow other nodes to override as a primary node when this node is primary. This option does not take effect when the node is secondary.
Group IP	IP multicast in the range of 224.0.0.0 and 239.255.255.255.
Group Port	Port of the group IP address.
Schedule Type	• *round robin*—Send URL requests can to all member nodes in circular order one by one. All handlings have equal priority. • *weighted round robin*: Round robin scheduling with a fixed number as configured weight which allows member nodes to deal with more than one URL requests in one circular order.
Interface Name	Name of the network interface for network traffic, such as the heartbeats to detect whether the member nodes are alive, and communication among all member nodes within the cluster.
Lost Threshold	Maximum number of successive heartbeat packets that can be missed from other nodes within the cluster. The HA cluster fails as soon as the number of successive missing packets exceeds *Lost Threshold*.
Hello Holddown	Duration (in seconds) of the transition from HA in Hello state to HA in work state. This parameter accepts integers between 5 - 300.
Interval	Duration (in seconds) between two successive packets.

The following is an example of an HA cluster setup.



HA Settings

Note: HA will restart after the HA settings are changed

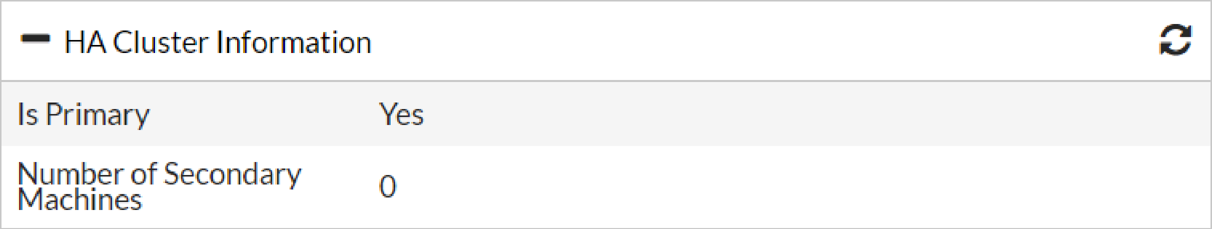
Enable:	☑
Virtual IP:	172.30.157.99
Priority:	23

Cluster Settings

Group Id:	11
Password:	Change
Allow Override:	☐
Group IP:	239.0.0.1
Group Port:	5001
Schedule Type:	round robin

Interface Name	Lost Threshold	Hello Holddown	Interval
mgmt	10	5	10

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



HA Cluster Information

Is Primary	Yes
Number of Secondary Machines	0

CLI

To configure HA from CLI:

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

To verify HA cluster Information from CLI:

```
show ha-all
      enabled : Enabled
      gid : 11
      lost-threshold : 10
      interval : 10
      holddown : 5
      priority : 68
      allow-override : 0
```

```
        schedule : Round Robin
        vip : 172.30.157.99
        password : ffff18ff28ff38ffff60ff3678ff2e03
        interface : mgmt
        ha-group-ip : 239.0.0.1
        ha-group-port : 5001

Cluster Information
   Number of Secondary : 1
   Is Primary : Yes
   (Secondary)IP Priority
   172.30.157.32 : 2
```

Database

FortiIsolator saves the following HA-related information and configuration in an internal database on the primary node, which gets synchronized to the database of all secondary nodes each time the primary node has changes. Each secondary node then reads from its own local database.

- User groups on page 101
- Profile on page 103
  - Web Filter profile
  - ICAP Profile
- Default policy on page 111
- Agent server
- Polling server

License management

FortiIsolator allows licenses to be shared among all clusters of the same HA setup. For example, an HA setup of 5 clusters will share 500 sessions; each cluster can have up to 500 sessions, or just one cluster can have up to 500 sessions. The split of the 500 sessions depends on when the session limit is reached, with the clusters dividing up the total of 500. A license file can be uploaded from any cluster, and will thus apply to the entire HA setup.

There are two configurations for managing license usage:

1. Max Session Per User: assigns session limit to each local user.
2. Max Session Per IP: assigns session limit to each unique IP address.

Configure license management through GUI

1. Go to *Policies and Profiles* > *Default Policy*.

To perform the configurations on license management from CLI:

For default policy:

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

For user-created policy:

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

Certificates

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

FortiIsolator only supports “Base-64 encoded X.509 (.CER)” format certificates.

To import a certificate:

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

Option	Certificate Type	Description
LOCAL_CERT	Local Certificate	This option allows users to import a customized local certificate to replace the built-in Isolator CA Certificate. If no local certificate is available, FortiIsolator uses the built-in Isolator CA Certificate.
SAML_CERT	SAML Certificate	Certificate for single-sign-on which is created in *LDAP Server* > *SAML Server*.
SELF SIGNED CA ROOT CERT	Self Signed CA root Certificate	This option allows the user to upload a self-signed CA root Certificate, which is the origin of a certificate chain that all subordinate certificates stem from. A *root_ca.crt* file should be uploaded here. The certificate chain must be complete for the certificate to work. You must also upload the relevant subordinate certificates under the *INTERMEDIATE CA CERT* option.

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

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

To view a certificate's details:

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

To delete a certificate:

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

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

To assign a certificate to user’s profile:

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

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

To regenerate a FortiIsolator CA Certificate:

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

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

SNMP

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

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

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

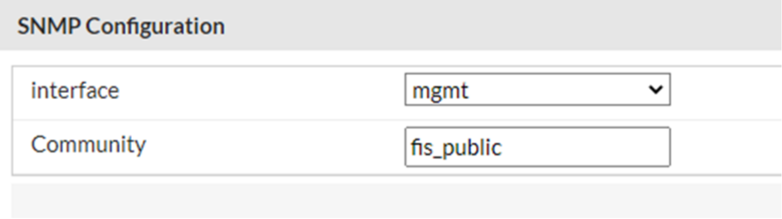
SNMP configuration

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

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

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

4. Click *OK*.



SNMP Configuration

interface	mgmt
Community	fis_public

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

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

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

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

To configure SNMP traps:

- For SNMP v1 and v2:

```
set session-threshold [1-100]
     set session-threshold 5
set trap-host-ip <host-ip>
     set trap-host-ip 192.168.1.100
set trap-host-community <host-community>
     set trap-host-community public
          File: /etc/snmp/ snmptrapd.conf
          authCommunity log,execute,net public
```

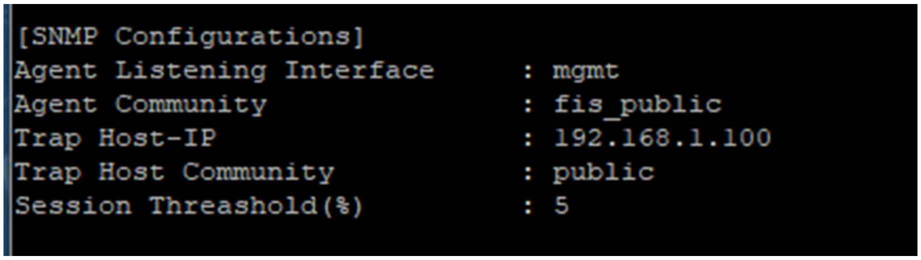
- For SNMP v3:

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

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

- For SNMP v1 and v2:

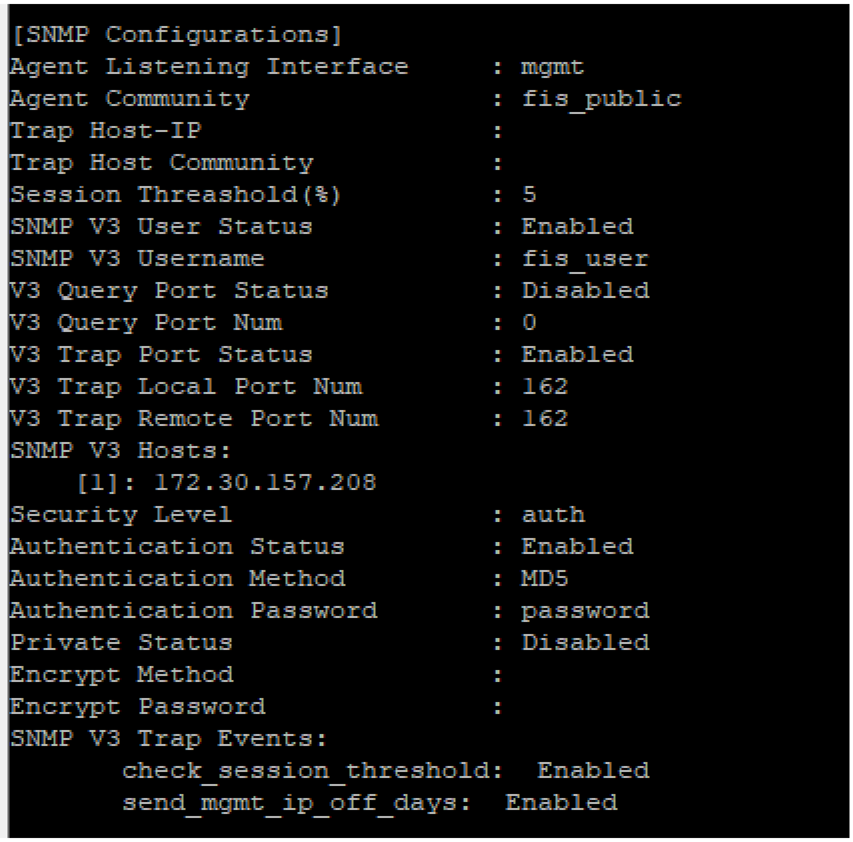
```
> cat /etc/snmp/snmp.conf
mibs +ALL

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

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



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

- For SNMP v3:

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

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

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



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

Example results from SNMP traps:

- For SNMP v1 and v2:

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

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

- For SNMP v3:

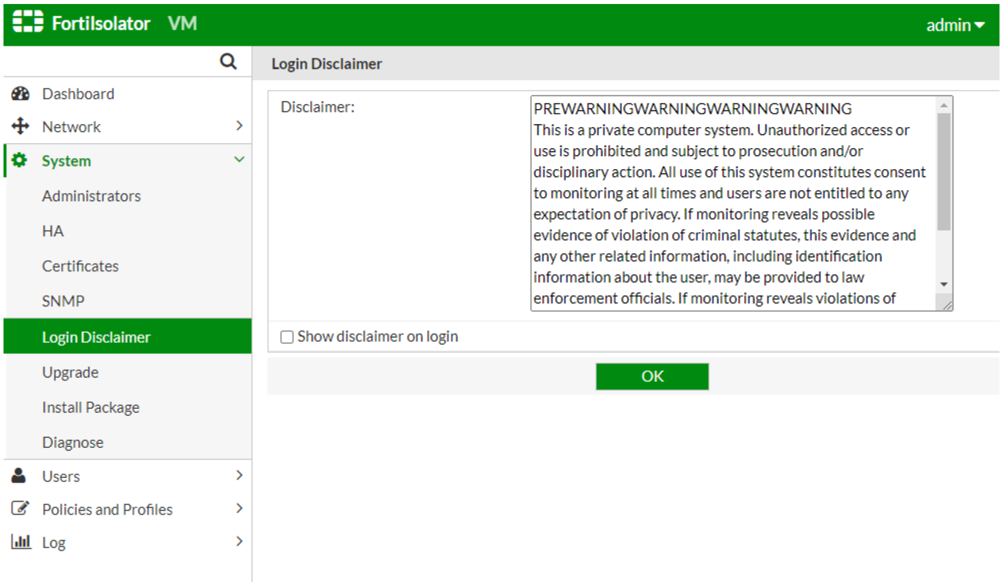
  ```
  > sudo snmptrapd -C -c /etc/snmp/snmptrapd.conf -f -Dusm -Lo

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

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

Login disclaimer

To configure the login disclaimer:

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



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

□ Show disclaimer on login

Upgrade

This section the following ways to upgrade FortiIsolator firmware:

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

To upgrade the firmware by web

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

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

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

To upgrade the firmware by USB device

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

1. Log into the FortiIsolator GUI as the admin administrative user.
2. Go to *System* > *Upgrade*.
3. Under *Upgrade by USB*, click *Click here* and locate the previously downloaded firmware image file that stored in USB device.
4. Under *Start Hour*, select the hour when FortiIsolator starts the upgrade process. Selecting *Now* triggers the upgrade immediately.
5. Click *Try* to upgrade the firmware.

To upgrade the firmware in CLI

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

1. Log into the FortiIsolator CLI as the admin administrative user.
2. Run the following command to install the firmware image from a server:

```
system-upgrade {tftp|ftp} <path> <server> [:<port>] [<user>:<password>]
```

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

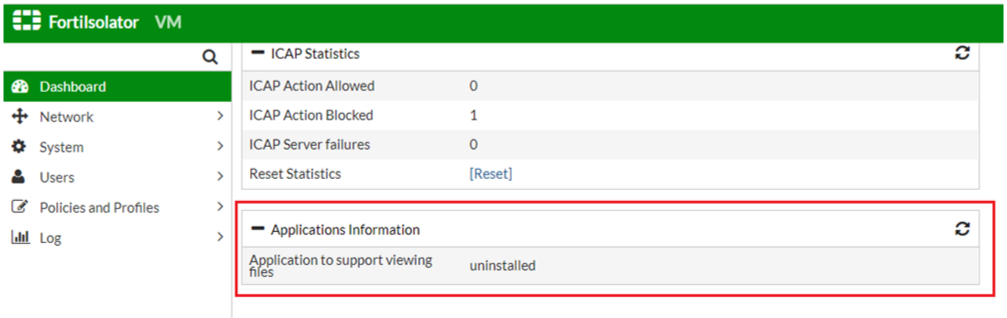
The FortiIsolator unit copies the new firmware image from the server or USB device to local hard disk, backs up the current configuration, and performs upgrade to the new firmware version. This process takes a few minutes. After the upgrade, the system reboots and deletes the firmware image from local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

Install package

While you can view PDF (`.pdf`) files without downloading the actual file in FortiIsolator, you must manually install an additional package to view the following file types without downloading the actual file:

- Word (`.doc`, `.docx`)
- Excel (`.xls`, `.xlsx`)
- PowerPoint (`.ppt`)
- TXT (`.txt`)
- PNG (`.png`)

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



ICAP Statistics

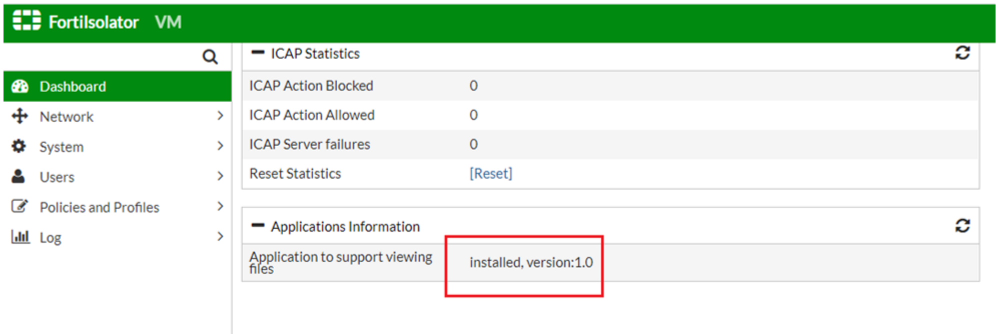
ICAP Action Allowed	0
ICAP Action Blocked	1
ICAP Server failures	0
Reset Statistics	[Reset]

Applications Information

Application to support viewing files	uninstalled

To install the package for viewing those document types without downloading the actual file:

1. Download the `Topdf-1.0.zip` package by following the instructions here.
2. Install the package:
   1. Go to *FortiIsolator GUI* > *System* > *Install Package*.
   2. Click *Choose File*.
   3. Select the package file you downloaded in step 1.
   4. Click *Submit*.
3. After the installation is complete, verify the *Applications Information* section shows *installed, version:1.0.* in the dashboard.



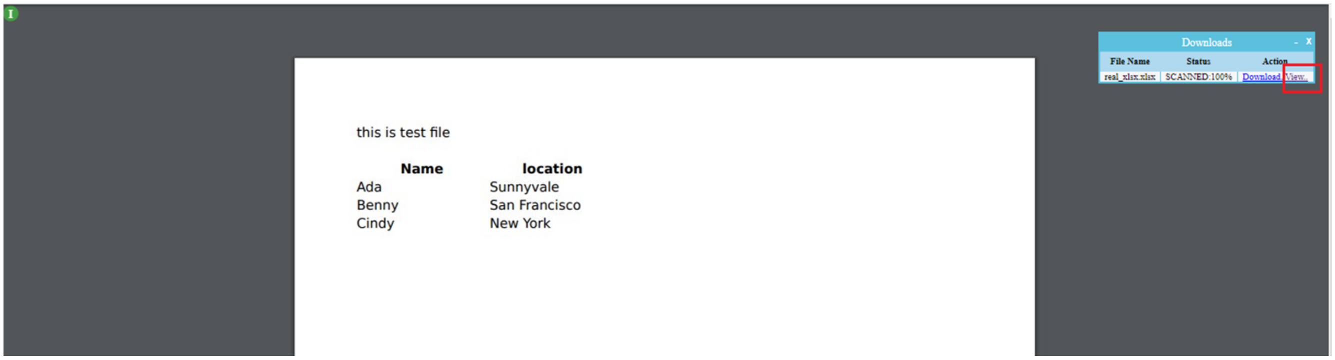
ICAP Statistics

ICAP Action Blocked	0
ICAP Action Allowed	0
ICAP Server failures	0
Reset Statistics	[Reset]

Applications Information

Application to support viewing files	installed, version:1.0

Sample view of a Microsoft Office document in FortiIsolator:



Downloads

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

this is test file

Name	location
Ada	Sunnyvale
Benny	San Francisco
Cindy	New York

Users

Covers the *Users* section of FortiIsolator.

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

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

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

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

LDAP servers

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

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

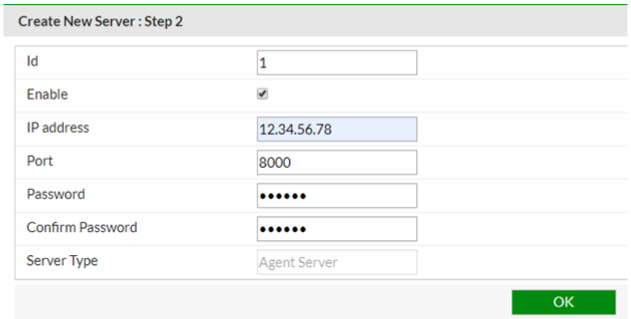
To manage LDAP servers on FortiIsolator, go to *Users* > *LDAP Server*.

Create or edit a LDAP server

To add a new LDAP server:

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

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

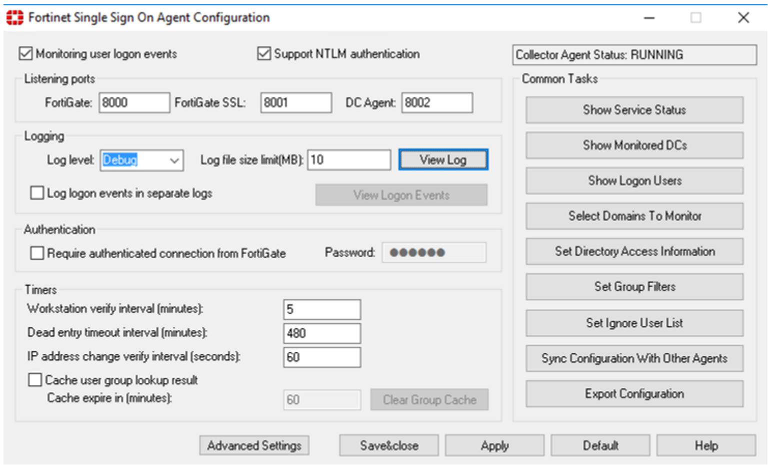


Create New Server : Step 2

Id	1
Enable	☑
IP address	12.34.56.78
Port	8000
Password	••••••
Confirm Password	••••••
Server Type	Agent Server

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

Fortinet Single Sign On (FSSO) agent server configuration



Fortinet Single Sign On Agent Configuration

☑ Monitoring user logon events ☑ Support NTLM authentication

Collector Agent Status: RUNNING

Listening ports

FortiGate: 8000 FortiGate SSL: 8001 DC Agent: 8002

Logging

Log level: Debug Log file size limit(MB): 10

☐ Log logon events in separate logs

Authentication

☐ Require authenticated connection from FortiGate Password: ●●●●●●

Timers

Workstation verify interval (minutes):	5
Dead entry timeout interval (minutes):	480
IP address change verify interval (seconds):	60

☐ Cache user group lookup result

Cache expire in (minutes): 60

SAML servers

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

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

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

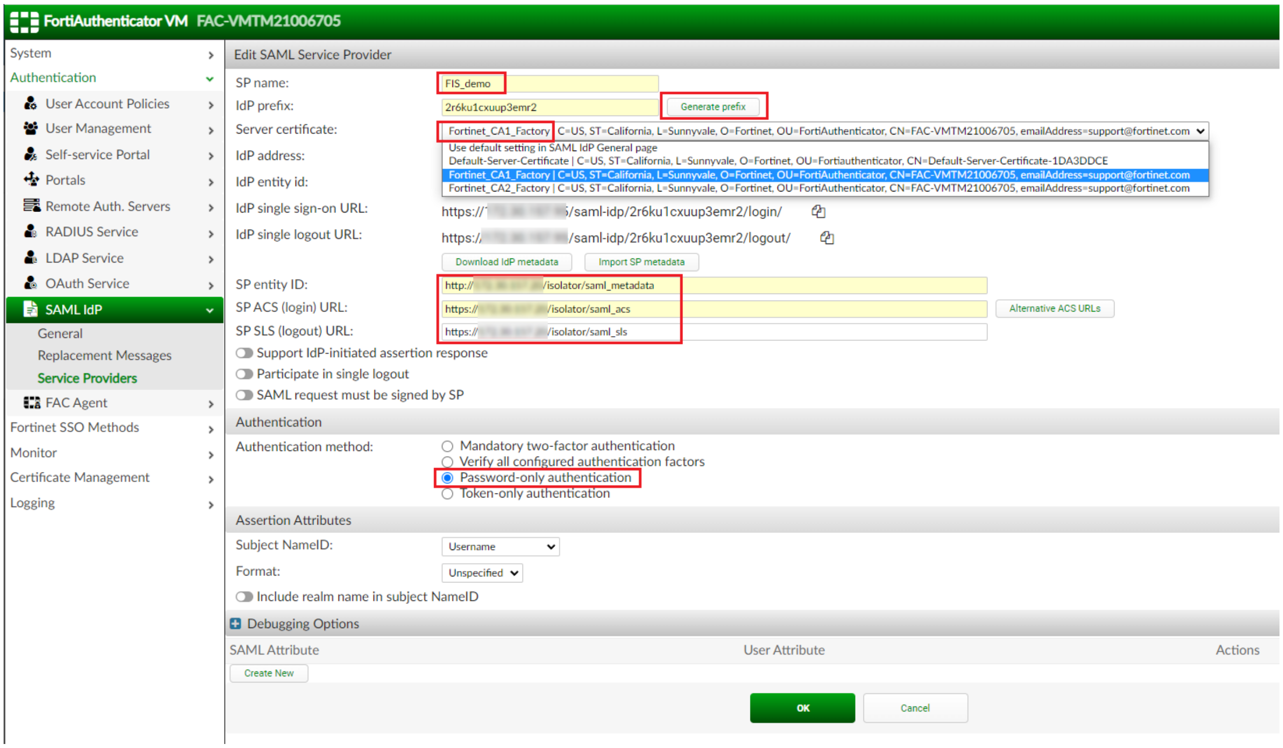
There are two parts of the setup:

1. Setup in FortiAuthenticator on page 97
2. Setup in FortiIsolator on page 99

Setup in FortiAuthenticator

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

SP Name	Name of the Service Provider
IdP prefix	Generate Prefix
Server Certificate	Fortinet_CA1_Factory
SP Entity ID	http://<*FortiIsolator_internal_ip*>/isolator/saml_metadata
SP ACS (login) URL	https://<*FortiIsolator_internal_ip*>/isolator/saml_acs
SP SLS (logout) URL	https://<*FortiIsolator_internal_ip*>/isolator/saml_sls
Authentication method	Password-only authentication



Edit SAML Service Provider

SP name: FIS_demo

IdP prefix: 2r6ku1cxuup3emr2

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

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

IdP address:

IdP entity id:

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

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

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

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

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

Support IdP-initiated assertion response

Participate in single logout

SAML request must be signed by SP

Authentication

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

Assertion Attributes

Subject NameID: Username

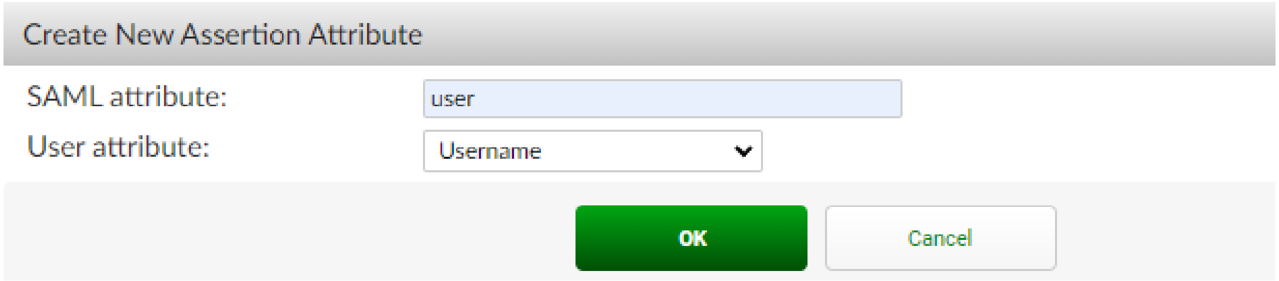
Format: Unspecified

Include realm name in subject NameID

If FortiIsolator is setup with only internal_IP, please use the internal_IP for FortiAuthenticator. If it is also set up with external_IP, please use the external_IP.

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

5. Add an SAML Attribute for user.

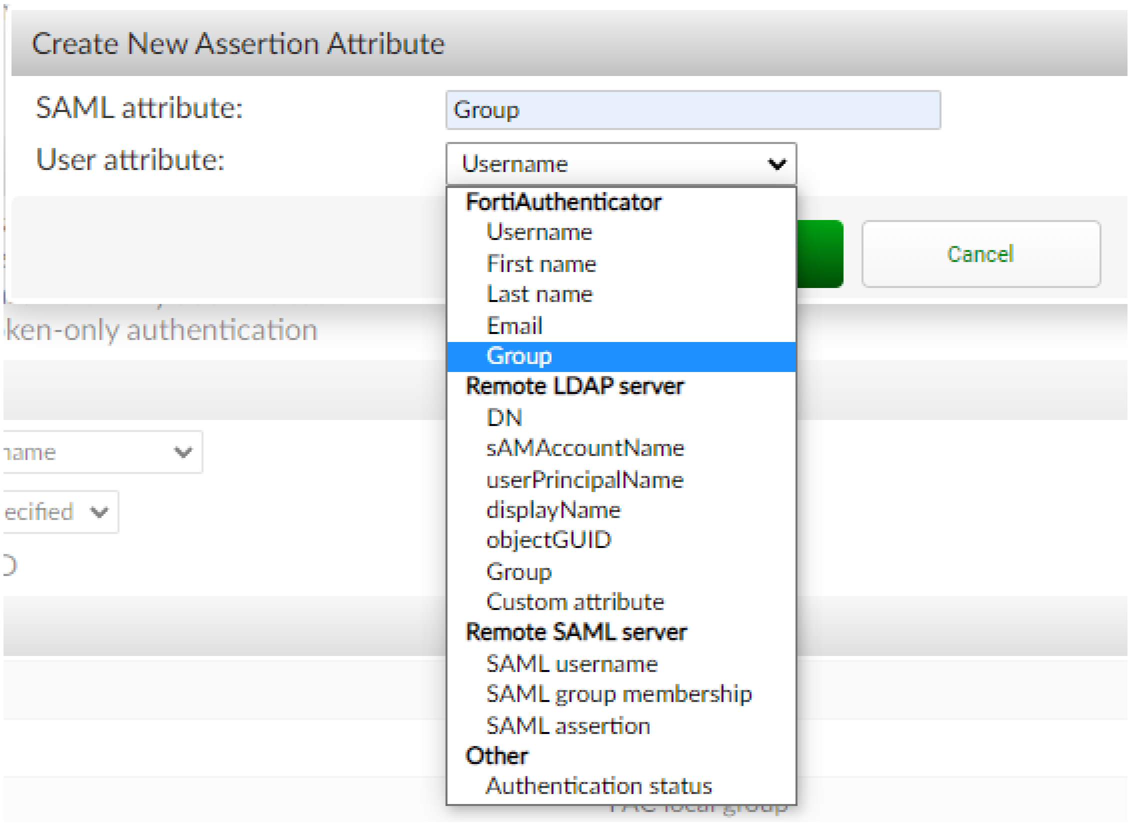


Create New Assertion Attribute

SAML attribute: user

User attribute: Username

6. Add SAML Attribute for Group

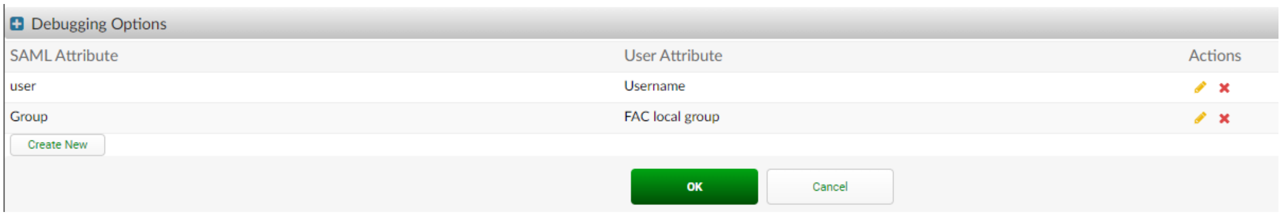


Create New Assertion Attribute

SAML attribute: Group

User attribute: Username

Debugging Options should look like this:



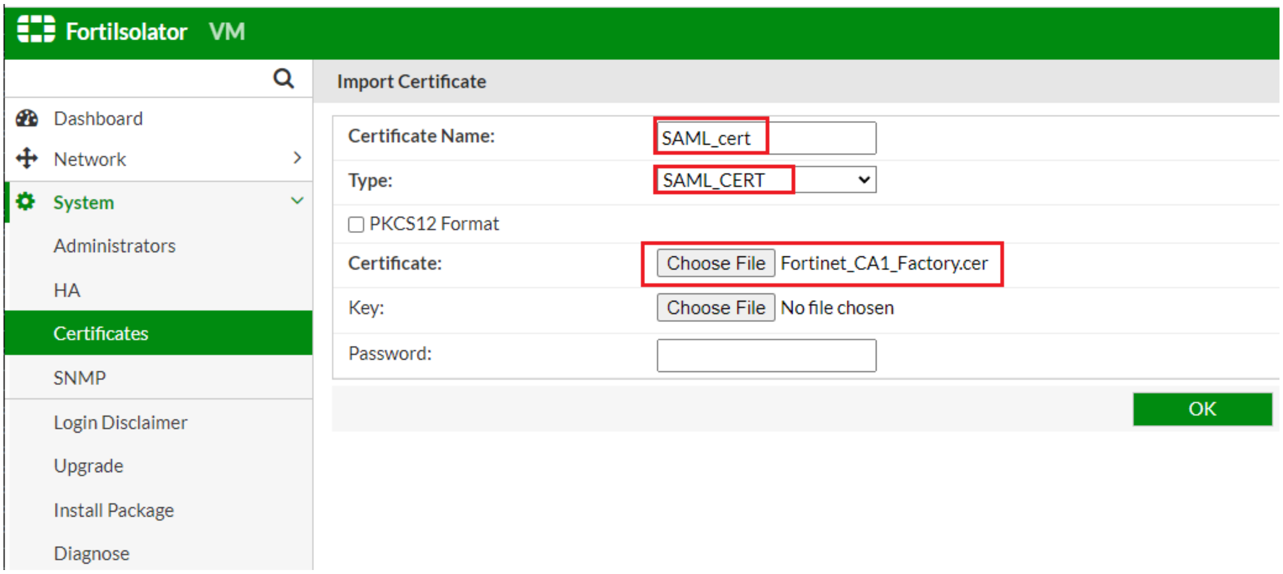
Debugging Options

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

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

Setup in FortiIsolator

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



Certificate Name: SAML_cert
Type: SAML_CERT
□ PKCS12 Format
Certificate: Choose File Fortinet_CA1_Factory.cer
Key: Choose File No file chosen
Password:
OK

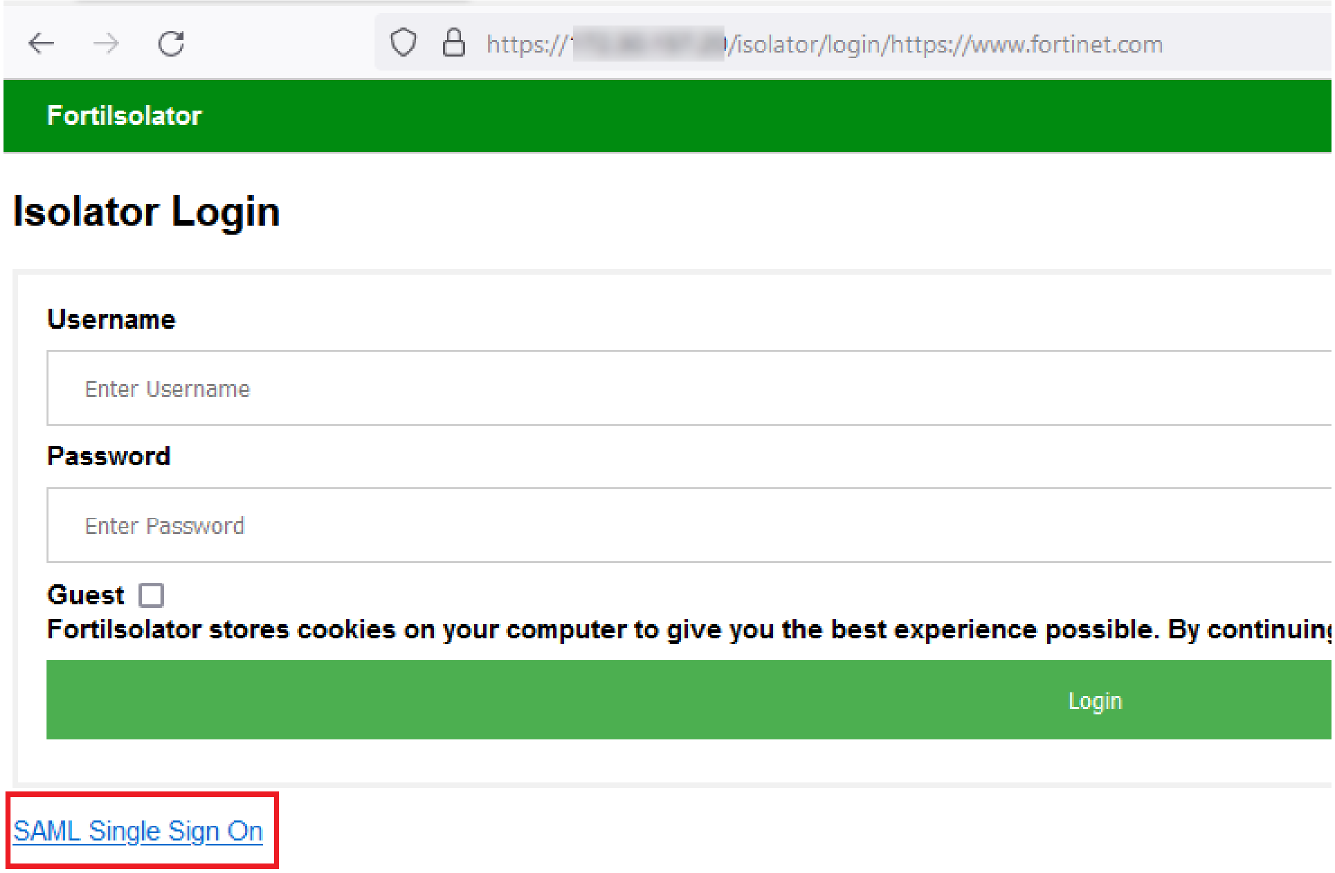
3. Navigate to *Users* > *LDAP Server* > *Create New*.
4. Select *SAML Server* and click *OK*.
5. Configure the following:

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

Run Traffic through FortiIsolator with FortiAuthenticator Users

Example:

```
https://<FortiIsolator_internal_ip>/isolator/login/https://www.fortinet.com
```



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

FortiIsolator

Isolator Login

Username

Enter Username

Password

Enter Password

Guest ☐

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

Login

SAML Single Sign On

User definition

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

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

Creating local user accounts from GUI

To create a local user account from GUI:

1. Open a browser window and navigate to the *Administration Portal* page.
2. Go to *Users* > *User Definition* > *Create New*
3. Under *Create New Local User*, fill in the username and password fields and any optional fields as desired, then click *OK*.
   a. To place the user in an existing group, select the boxes for the groups you would like to assign the user to.
   b. To apply an existing policy to the user, select the policy name from the drop-down menu Policy Name.

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

Creating local user accounts from CLI

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

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

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

e.g.
> set user fis_user 0
Enter the password:
Re-enter the password:
Please enter email:fis_user@fortinet.com
Please enter policy name:policy_new

> show user
Displaying only local users...
        name : fis_user
        server_id : 0
        email : fis_user@fortinet.com
        policy_name : policy_new
        encoded password : ffff18ff28ff38ffff60ff3678ff2e03
>
```

User groups

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

Creating user groups from GUI

To create a user group from GUI:

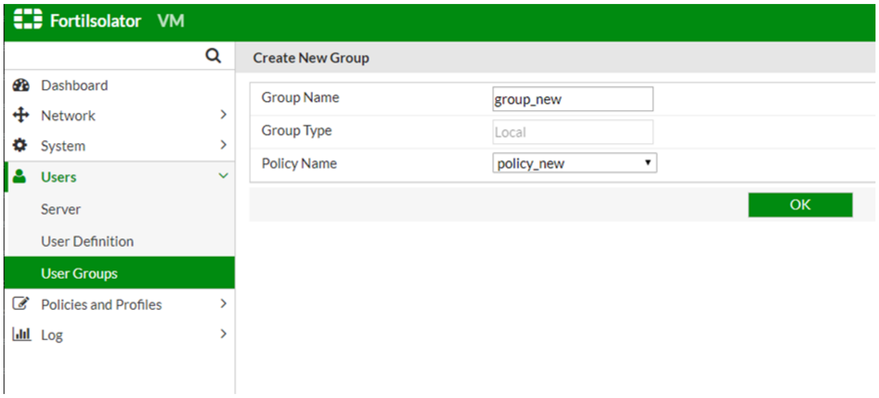
1. From the administration portal, go to *Users* > *User Groups* and click *Create New*.
2. Type in a name for the group and click *OK*.

Creating user groups from CLI

To create a user group from CLI:

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

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



Create New Group

Group Name	group_new
Group Type	Local
Policy Name	policy_new

Policies and profiles

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

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

Profile

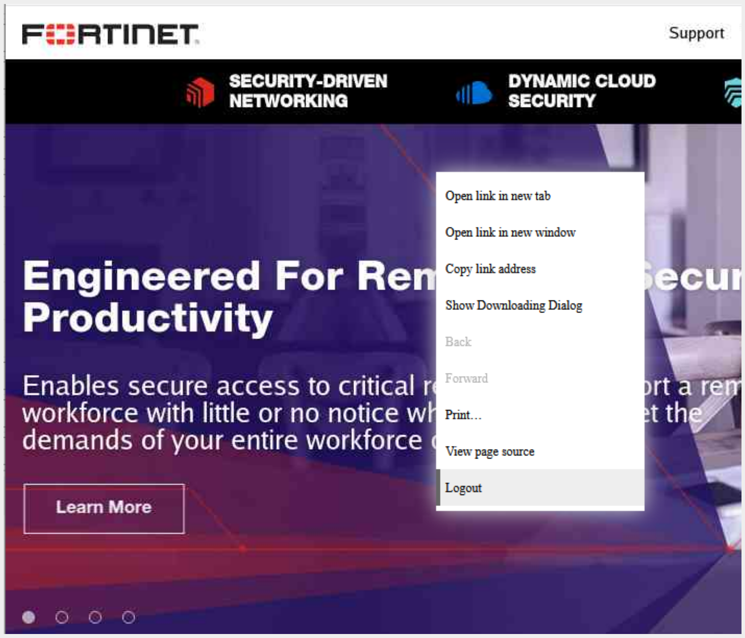
Creating a Isolator browsing profile

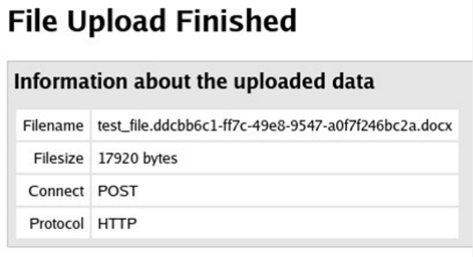
Configure the Isolator profile to dictate how the end user browses the web through FortiIsolator. There are various settings for you to configure, including the bandwidth use and end user privileges.

To create an Isolator browsing profile from GUI:

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

Isolator Profile Name	Name of the Isolator profile. No restrictions.
Max Download/Upload Size	Type in the maximum file size in megabytes for uploading and downloading files.
Limit of View-only	By selecting the *Limit of view only* box, you limit the user to view-only access of web pages. The user is restricted from interacting with the pages, such as right-clicking or typing in text.
Image Quality	Increase or decrease bandwidth usage.
Video Frame Rate	Increase or decrease bandwidth usage.
Scroll Speed	Allows end uses to control the scrolling speed on the mouse wheel while navigating pages. The range is from 1 - 100; 1 is the minimum speed, while 100 is the maximum speed. When the speed is set at 100, one scroll on the mouse wheel will scroll through one full page on the browser window.
Use Doc-rewrite when Scanning File	Allow rewriting of documents during file scanning such that embedded links in the file are rendered inactive.
Scan Files for Malware	Scans files when uploading or downloading through FortiIsolator. *Enable* • FortiIsolator will scan the file for malware or viruses. If malware or viruses are detected, it will prompt a message to

<table>
<tr><td></td><td>inform the user that "Virus is discovered in the file."
• If the file does not contain a virus, FortiIsolator then allows the user to upload or download the file normally.
<i>Disable</i>
• Will not scan files. Files will be uploaded and downloaded normally.</td></tr>
<tr><td>Permit for Right-Click</td><td>Allows the client user to right click on mouse to display a menu.
This option works only if <i>Limit of View-only</i> is disabled.

FORTINET
Support
SECURITY-DRIVEN NETWORKING
DYNAMIC CLOUD SECURITY
Engineered For Rem… Secur… Productivity
Enables secure access to critical r… workforce with little or no notice wh… demands of your entire workforce …ort a rem… …t the
Learn More
Open link in new tab
Open link in new window
Copy link address
Show Downloading Dialog
Back
Forward
Print…
View page source
Logout
<table>
<tr><td>Print</td><td>User can print the current page as a PDF file.</td></tr>
<tr><td>Logout</td><td>Log out from the current session.</td></tr>
</table></td></tr>
<tr><td>Permit of Copying and Pasting</td><td><i>Enable</i>
• User can copy and paste from keyboard.
<i>Disable</i>
• User cannot copy and paste from keyboard.</td></tr>
<tr><td>Permit of Printing</td><td>Allows client user to print current page into a PDF file.</td></tr>
<tr><td>User Agent</td><td>Customized user agent name.</td></tr>
</table>

Send File to FortiSandbox	To enable FortiSandbox scanning, you need to also enable: • Scan file for malware FortiIsolator provides the option to send files to FortiSandbox to scan for virus or malware. When uploading or downloading a file through FortiIsolator, the file will send to FortiSandbox. If FortiSandbox detects the file as containing virus or malware, it blocks the file and sends back the result to FortiIsolator. FortiIsolator then displays the result in the client browser, not allowing the user to proceed any further. If it is a sanitized file, FortiSandbox allows the client user to upload or download the file through FortiIsolator. **To send a file to FortiSandbox:** 1. Verify that the FortiSandbox setting is valid. 2. Upload a file through FortiIsolator. Image will appear when file upload is finished.  File Upload Finished Information about the uploaded data Filename test_file.ddcbb6c1-ff7c-49e8-9547-a0f7f246bc2a.docx Filesize 17920 bytes Connect POST Protocol HTTP 3. Verify that the file is being scanned in FortiSandbox, and view the results of the scan.
FortiSandbox IP	Set the IP of the connected FortiSandbox.
FortiSandbox Administrator Name	Set the FortiSandbox administrator name.
FortiSandbox Password	Set the FortiSandbox password.
To Block File Types from Download/Upload	Allow / disallow file types from download or upload. • Uncheck: allow all file types from download or upload. • Check: disallow the selected file type from download or upload.

4. Click *OK*.

To create a FortiIsolator profile from CLI:

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

For example,

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

Parameter	Description
`<name>`	Name of the Isolator profile.
`<download>`	Max download size in megabytes (MB).
`<upload>`	Max upload size in megabytes (MB).
`<viewonly>`	Limit of view-only (Y/N).
`<avscan>`	Scan files for malware (Y/N).
`<image-quality>`	Image quality. Specify a percentage within 1-100.
`<video-frame-rate>`	Video frame rate (high, normal, low).
`<av-disarm>`	Use doc-rewrite when scanning file (Y/N).
`<right-click>`	Permit to right-click (Y/N). This parameter is valid only when <viewonly> is N.
`<scroll-speed>`	Scrolling speed on the mouse wheel while navigating pages. The range is from 1 - 100 with1 as the minimum speed and 100 the maximum.
`<file-type>`	File types to block from downloading and uploading.
`<permit-of-copy>`	Permit to copy and paste from keyboard (Y/N).
`<permit-of-print>`	Permit to print current page into a PDF file (Y/N).
`<agent-name>`	Customized user agent name.

To display Isolator browsing profile from CLI:

```
> show isolator-profile system_default
        Remote Render : N
        Download Size(MB) : 100
        Upload Size(MB) : 100
        Viewonly Enabled : N
        Antivirus Scan Enabled : Y
        Antivirus Disarm Enabled : Y
        Right Click Enabled : Y
        Image Quality : 100
        Video Frame Rate : normal
        Scroll Speed : 10
        Blocking file type for downloading and uploading : exe;doc
        Agent Name : fortiisolator
        FortiSandbox Enabled : N
        FortiSandbox IP : ""
        FortiSandbox Admin : ""
>
```

Creating Web Filter profile

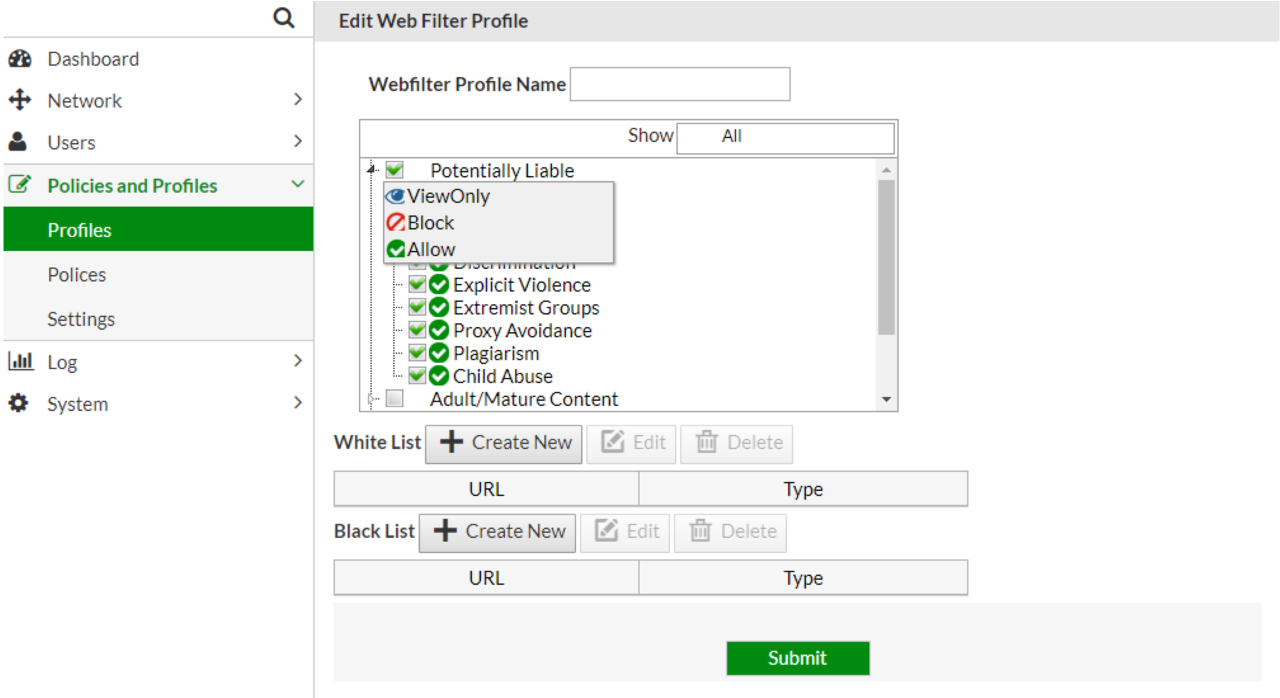
FortiIsolator supports web filtering, which enables the administrator to control which webpages that end users are allowed to view. You can block specific URLs or websites, which prevents the end user's browser from loading web pages from these websites.

Prerequisites

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

To create a Web Filter profile from GUI:

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

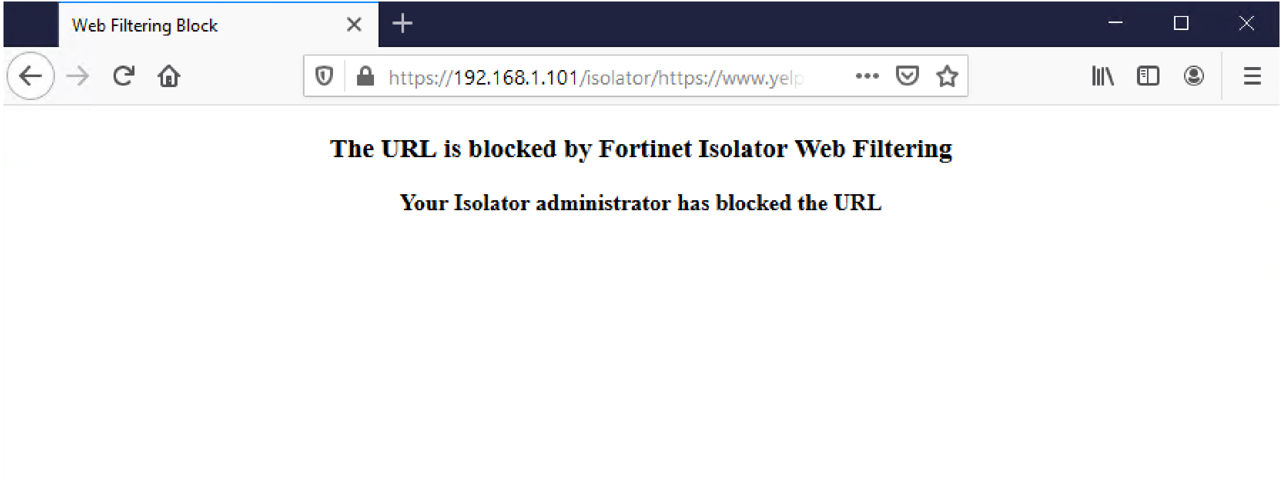


Right-click on any checked box to select the desired action:

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

5. To allow or block specific websites, click the corresponding *Create New* button in the *Allow List* or *Block List* section. Enter the URL details and click *OK*. The allow list and block list filters accept simple URLs, regular expressions, wildcards, and exemptions as URL filter criteria.
6. To finish creating the Web Filter Profile, click *Submit*.

7. To verify that the web filter is working, try browsing to one of the blocked web pages. You should see the following text displayed in your browser:



The URL is blocked by Fortinet Isolator Web Filtering

Your Isolator administrator has blocked the URL

To create a Webfilter profile from CLI:

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

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

e.g.
> set wf-allow-list allow_list_new website.com 0


> show wf-allow-list
allow_list-allow_list_new testsite.com 0
set wf-block-list <name> <url> <type>

e.g.
> set wf-block-list block_list_new blocksite.com 0

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

> show wf-block-list
block_list-block_list_new blocksite.com 0


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

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


> show wf-profile
```

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

Creating ICAP profile

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

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

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

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

Prerequisites

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

To create an ICAP profile from GUI:

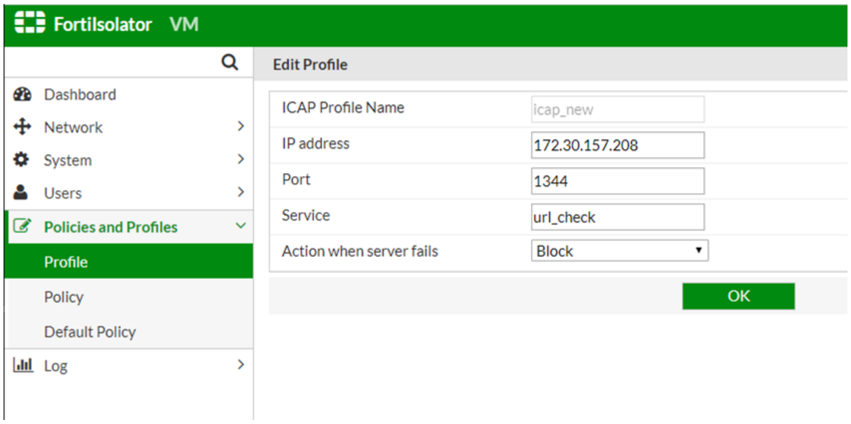
1. From the administration portal, go to *Policies and Profiles* > *Profiles* and click *Create New*.
2. From the *Profile Type* drop-down menu, select ICAP Profile and click *OK*.
3. Fill in the new ICAP profile information with desired settings:

ICAP Profile Name	Name of the ICAP profile
IP Address	IP Address of the ICAP server
Port	Port number that the ICAP server running the service on
Service	Service name of the ICAP server
Action when server fails	Actions on FortiIsolator if fails to connect to ICAP • Allow • Block • View only

To create an ICAP profile from CLI:

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

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

```
e.g.
> set icap-profile icap_new 172.30.157.208 1344 url_check 1

> show icap-profile
ICAP Profile:icap_new
        IP Address : 172.30.157.208
        Port : 1344
        Service Name : url_check
```



Edit Profile

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

Policy

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

To create a policy from GUI:

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

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

6. Click *OK* to finish.

To create a FortiIsolator policy from CLI:

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

e.g.

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

`<policy-name >`	Policy name
`<isolator-profile-name >`	Isolator profile name
`<webfilter-profile-name >`	Web Filter profile name
`<icap-profile-name >`	ICAP profile name
`<max-session-per-user>`	Maximum number of sessions (tabs) allowed for requests from a same local user
`<max-session-per-ip>`	Maximum number of sessions (tabs) allowed for requests from a unique IP address
`<auth-cookie-lifetime>`	Number of hours after which the authorization cookie expires and the user needs to re-login. This parameter accepts integers within the range of 1-240. This parameter does not take effect when the user is in guest mode.

To display a FortiIsolator policy from CLI:

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

Default policy

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

Applying default policy and profile settings

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

To apply profiles to default policy from GUI:

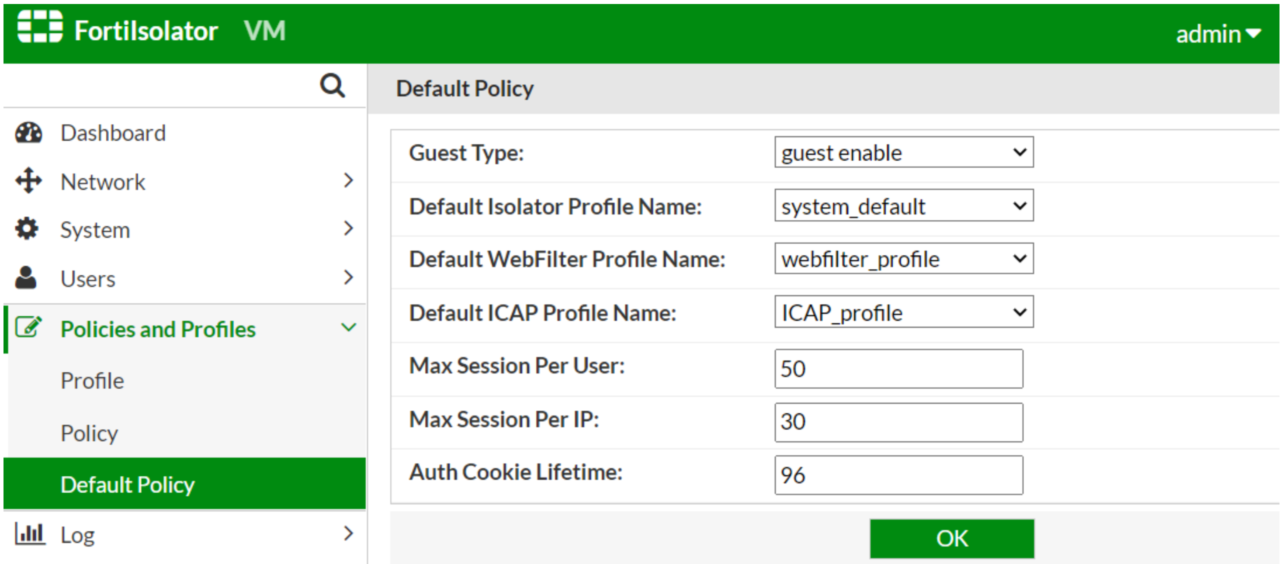
1. Go to *Policies and Profiles* > *Default Policy* and select the desired *Guest Type*:

guest disable	A user has to log in with user account.
guest enable	A user can log in with either user account or as a guest.
guest only	A user has to log in as a guest. With *guest only*, the login page will not show. Users can browse sites directly without being prompted to log in.

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

Default Isolator Profile Name	Select an Isolator profile for Default Policy.
Default WebFilter Profile Name	Select a Web Filter profile for Default Policy.
Default ICAP Profile Name	Select an ICAP profile for Default Policy.
Max Session Per User	Maximum number of sessions (tabs) allowed for requests from a same local user
Max Session Per IP	Maximum number of sessions (tabs) allowed for requests from a unique IP address
Auth Cookie Lifetime	Number of hours after which the authorization cookie expires and the user needs to re-login. Enter an integer within the range of 1-240. This setting does not take effect when the user is in guest mode.

3. Click *OK* to finish.



Default Policy

Guest Type: guest enable

Default Isolator Profile Name: system_default

Default WebFilter Profile Name: webfilter_profile

Default ICAP Profile Name: ICAP_profile

Max Session Per User: 50

Max Session Per IP: 30

Auth Cookie Lifetime: 96

To apply profiles to default policy from CLI:

```
> set guest-type 0|1|2
(disabled = 0, enabled = 1, guest-only = 2)
For example:
> set guest-type 0
> show guest-type
guest type : Disabled
> set guest-type 1
> show guest-type
guest type : Enabled
> set guest-type 2
> show guest-type
guest type : Guest Only


> set default-policy <isolator-profile-name> <webfilter-profile-name> <icap-profile-name>
     <guest-type> <max-session-per-user> <max-session-per-ip> <auth-cookie-lifetime>
e.g.

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

`<isolator-profile-name >`	Isolator profile name
`<webfilter-profile-name >`	Web Filter profile name
`<icap-profile-name >`	ICAP profile name
`<guest-type>`	Login mode of the user: `1` *guest disable*: A user has to log in with user account.

	2 *guest enable*: A user can log in with either user account or as a guest. 0 *guest only*: A user has to log in as a guest.
`<max-session-per-user>`	Maximum number of sessions (tabs) allowed for requests from a same local user
`<max-session-per-ip>`	Maximum number of sessions (tabs) allowed for requests from a unique IP address
`<auth-cookie-lifetime>`	Number of hours after which the authorization cookie expires and the user needs to re-login. This parameter accepts integers within the range of 1-240. This parameter does not take effect when the user is in guest mode.

To display the default policy profile from CLI:

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

Applying profile settings to local user account

To apply profile settings to local user account:

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

Applying profile settings to user groups

To apply profile settings to user groups:

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

Log

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

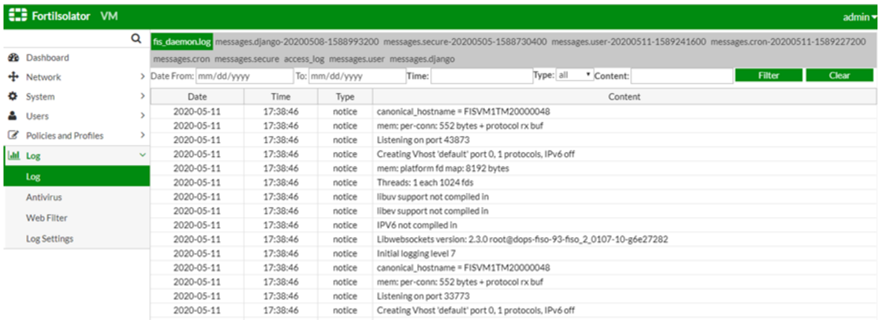
- Daemons running on FortiIsolator devices
- Connectivity with FDN server, internal database, Anti-Virus servers, etc.
- Heartbeat information among the nodes when have HA cluster setup
- Detections of virus when uploading or downloading files
- Web filtering activities on sites to passing through or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

The following topics provide information about logging:

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

Viewing logs

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



Date	Time	Type	Content
2020-05-11	17:38:46	notice	canonical_hostname = FISVM1TM20000048
2020-05-11	17:38:46	notice	mem: per-conn: 552 bytes + protocol rx buf
2020-05-11	17:38:46	notice	Listening on port 43873
2020-05-11	17:38:46	notice	Creating Vhost 'default' port 0, 1 protocols, IPv6 off
2020-05-11	17:38:46	notice	mem: platform fd map: 8192 bytes
2020-05-11	17:38:46	notice	Threads: 1 each 1024 fds
2020-05-11	17:38:46	notice	libuv support not compiled in
2020-05-11	17:38:46	notice	libev support not compiled in
2020-05-11	17:38:46	notice	IPV6 not compiled in
2020-05-11	17:38:46	notice	Libwebsockets version: 2.3.0 root@dops-fiso-93-fiso_2_0107-10-g6e27282
2020-05-11	17:38:46	notice	Initial logging level 7
2020-05-11	17:38:46	notice	canonical_hostname = FISVM1TM20000048
2020-05-11	17:38:46	notice	mem: per-conn: 552 bytes + protocol rx buf
2020-05-11	17:38:46	notice	Listening on port 33773
2020-05-11	17:38:46	notice	Creating Vhost 'default' port 0, 1 protocols, IPv6 off

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

FORTIGUARD AGENT	Log for daily process to get updates for Web Filter categories from FortiGuard
ISOLATOR	Logs for connectivity with FDN server, internal database, Anti-Virus servers, HA heartbeats information, etc.
CRON	Logs for FortiIsolator daemons for healthy checks
ACCESS LOG	Logs for accessing FortiIsolator local devices
DAEMON	Logs for daemons running in FortiIsolator devices
ADMIN GUI	Logs for FortiIsolator Web framework activities
SECURE	Logs for connectivity from remote server to FortiIsolator through SSH

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

Antivirus

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

Filter	Detail
Date	The day the log was recorded.
Time	The minute the log was recorded.
Action	• Upload file—The file was uploaded. • Download file—The file was downloaded.
UserID	"0" means the user is a guest, or another local_user, or an NTLM user. The number is auto-generated by the admin when a local user is created or an NTLM user is used.
Path	The path of the file on FortiIsolator device that stores the uploaded/downloaded files.
Target URL	The destination the user is trying to access through FortiIsolator.
Result	• Passthrough—Allows the file (assuming uncorrupted) to be downloaded/uploaded. • Block—Blocks the file if a virus is detected.
File Size	The size of the file. No limit. However, it must comply to the file size defined under Profile.
Isolator Profile Name	Name of the profile as defined in *Policies and Profile*.

Web Filter

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

Filter	Detail
Date	The day the log was recorded.
Time	The minute the log was recorded.
Action	• Allow—Allows web browsing to continue. • Block—Blocks web browsing. • View Only—Only allows user to view when browsing.
UserID	"0" means the user is a guest, or another local_user, or an NTLM user. The number is auto-generated by the admin when a local user is created or an NTLM user is used.
URL	The destination the user is trying to access through FortiIsolator.
Category	Block / Passthrough as determined under the specified Web Filter Profile.
WF Profile Name	Name of the Web Filter profile as defined in Profiles and Policies.

Log settings

Configuring the log server

To back up log messages and/or send syslog messages to a remote server:

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

Logging protocol	Syslog
Network protocol	• udp • tcp
Log Server IP Address	Remote server IP that receives the logs.
Port	The port number of the remote server that receives the logs.

4. Choose logs to send to remote server.
5. Click + *Create New*. Select the Application and Severity. See the descriptions in the Viewing logs on page 115. Click *OK*.
6. Click *Submit*.

Run web browsers through FortiIsolator

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

- IP Forwarding mode
- Proxy mode
- PAC file mode

IP Forwarding mode

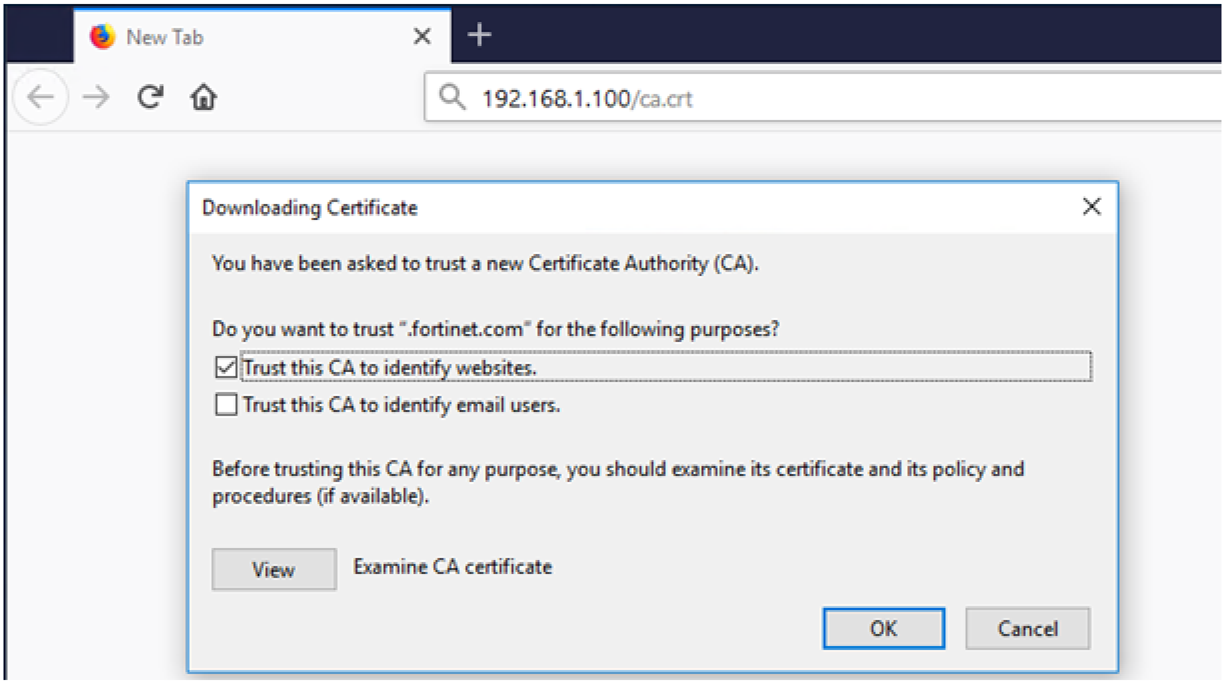
Using IP Forwarding mode with Mozilla Firefox

To configure IP Forwarding mode with Mozilla Firefox:

1. Download the FortiIsolator certificate (ca.crt) and import it into the Mozilla Firefox browser:
   a. In the Mozilla Firefox browser address bar, type http://`<internal_IP_address>`/ca.crt (for example, http://192.168.1.100/ca.crt).
      - where `<internal_IP_address>` is the IP address of the FortiIsolator internal interface. For example, the IP address of the internal interface that you configured in step 3 of Installing FortiIsolator 1000F on page 11.

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

   c. Click *OK*.



Downloading Certificate

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

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

☑ Trust this CA to identify websites.

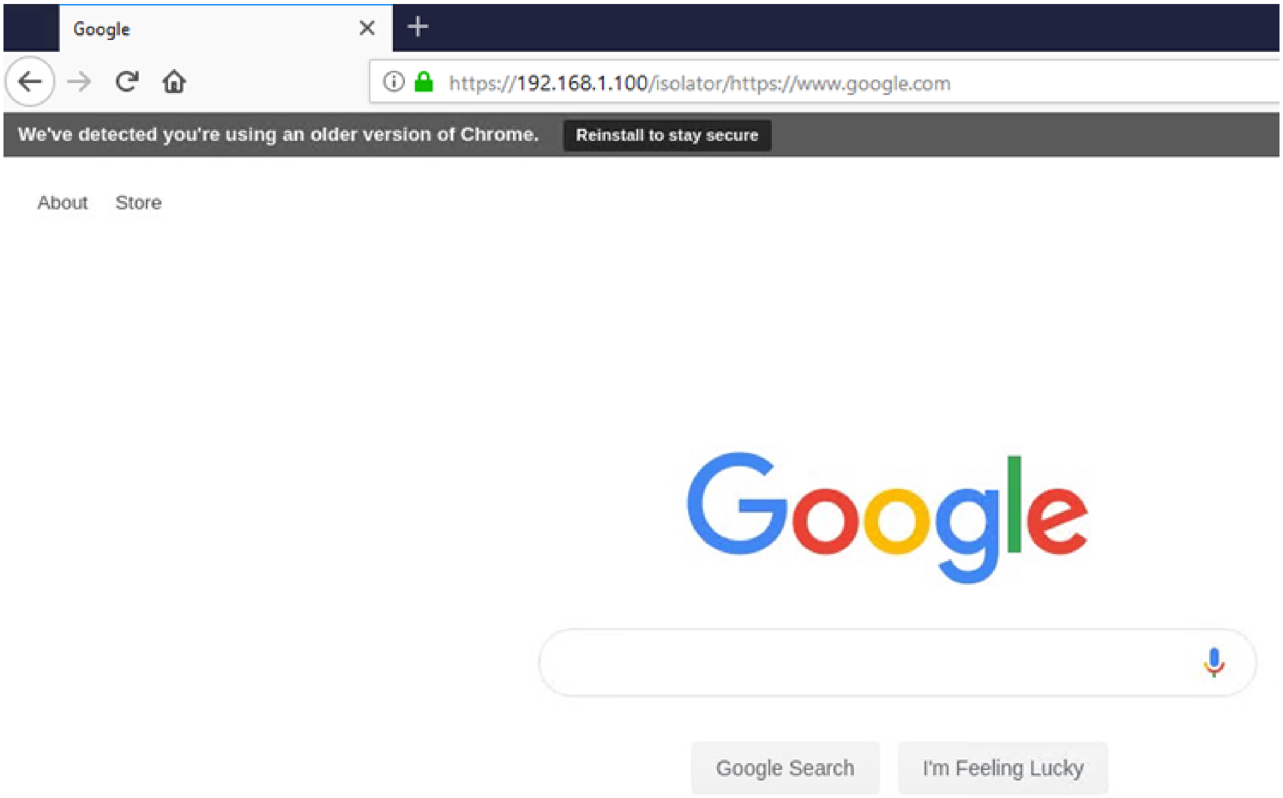
☐ Trust this CA to identify email users.

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

View | Examine CA certificate

OK | Cancel

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

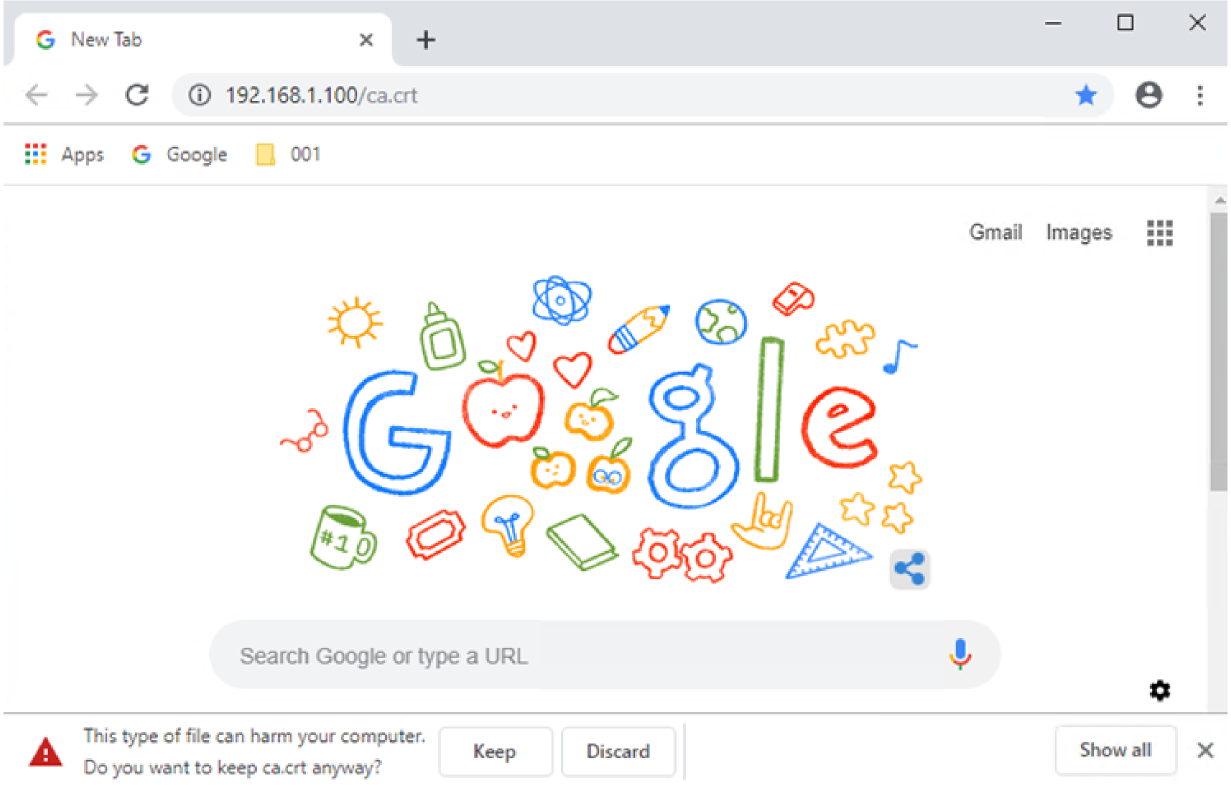

Google
https://192.168.1.100/isolator/https://www.google.com
We've detected you're using an older version of Chrome.
Reinstall to stay secure
About
Store
Google
Google Search
I'm Feeling Lucky

Using IP Forwarding mode with Google Chrome

To configure IP Forwarding mode with Google Chrome:

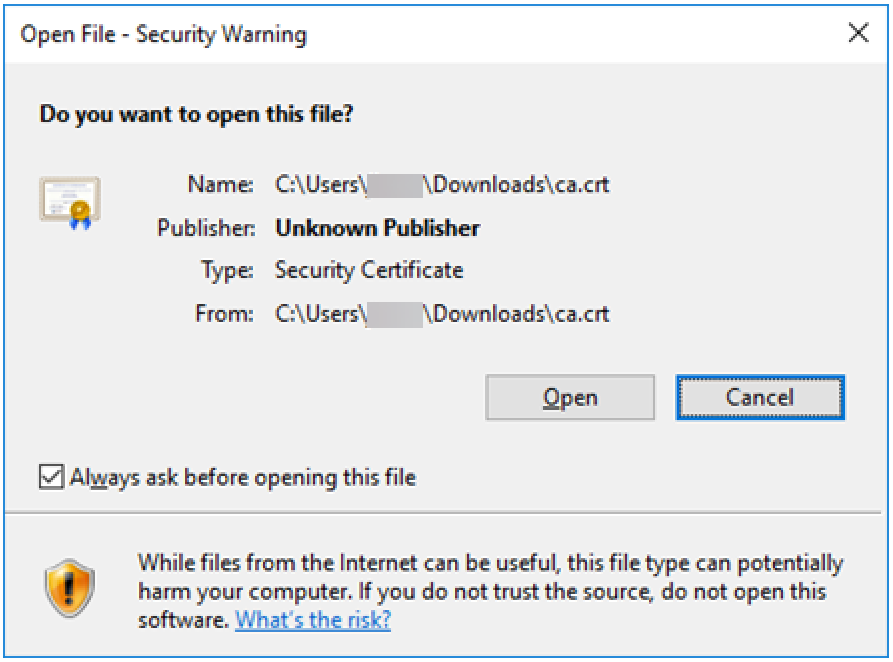
1. Download the FortiIsolator certificate (ca.crt) and import it into your Google Chrome browser:
   a. In the Google Chrome browser address bar, type `http://<internal_IP_address>/ca.crt` (for example, `http://192.168.1.100/ca.crt`).
      - where `<internal_IP_address>` value is the IP address of the FortiIsolator internal interface. For example , the IP address of the internal interface that you configured in step 3 of Installing FortiIsolator 1000F on page 11.

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



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

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



Open File - Security Warning

Do you want to open this file?

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

Publisher: **Unknown Publisher**

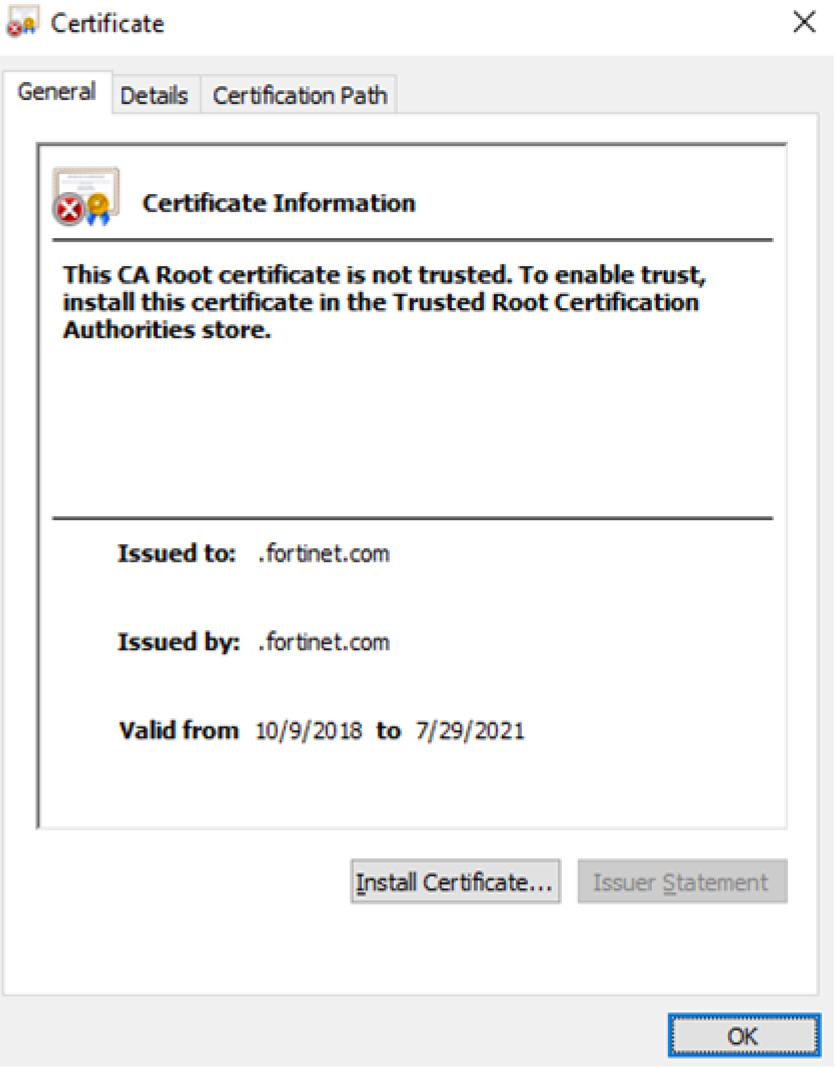
Type: Security Certificate

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

☑ Always ask before opening this file

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

d. Click *Install Certificate*.



Certificate Information

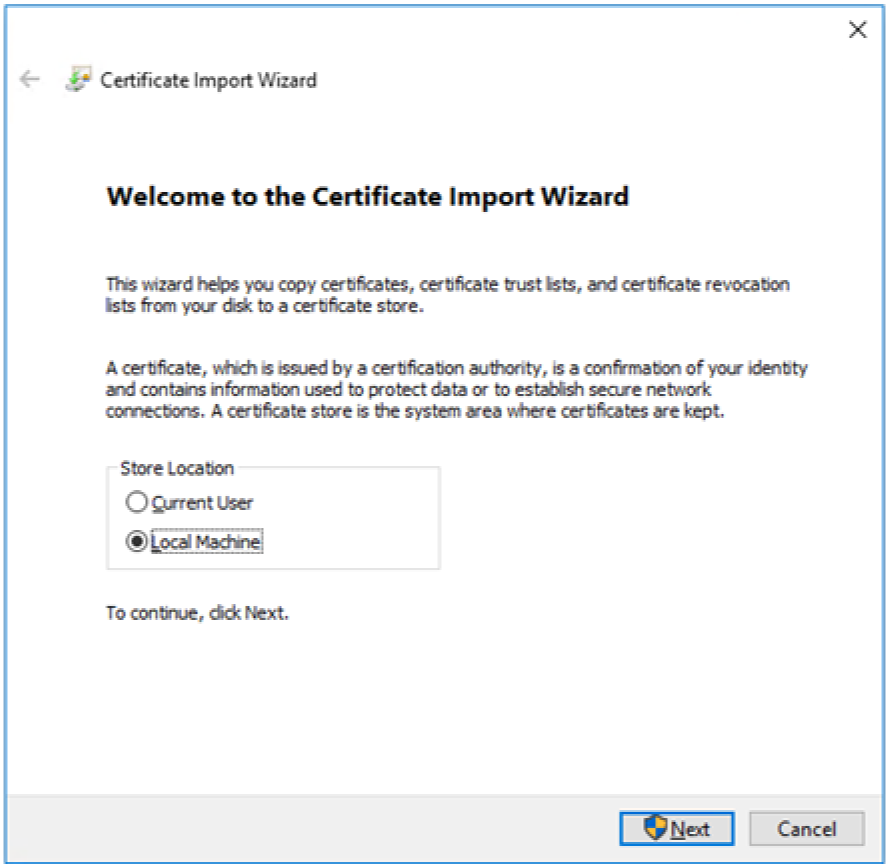
This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

Issued to: .fortinet.com

Issued by: .fortinet.com

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

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



Certificate Import Wizard

Welcome to the Certificate Import Wizard

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

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

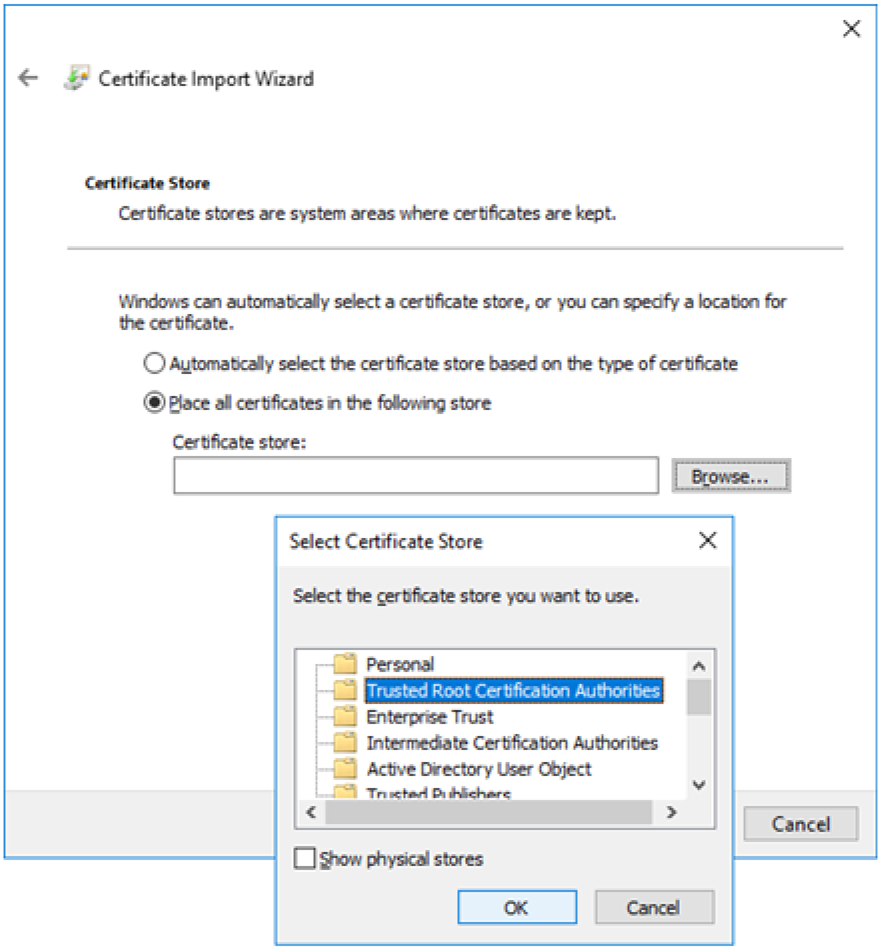
Store Location

○ Current User

● Local Machine

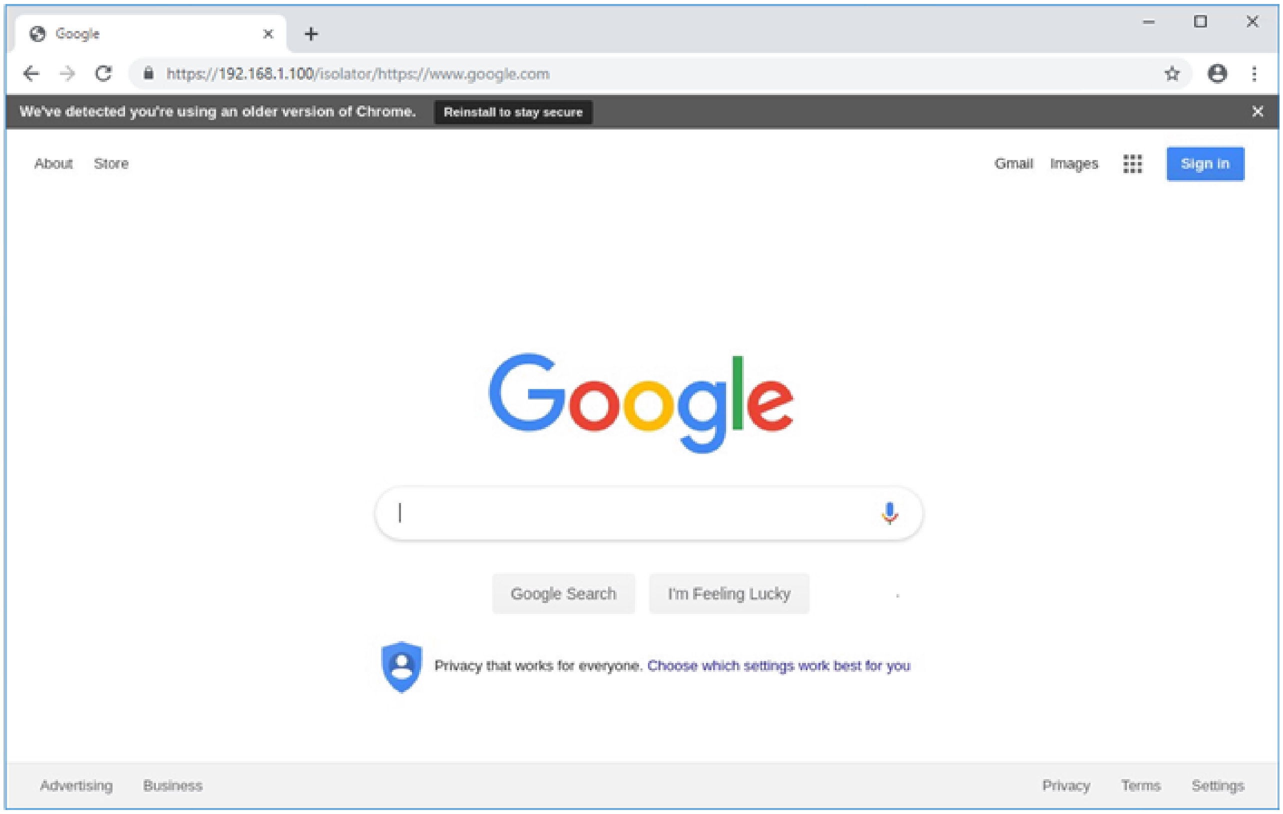
To continue, click Next.

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


Certificate Import Wizard
Certificate Store
Certificate stores are system areas where certificates are kept.
Windows can automatically select a certificate store, or you can specify a location for the certificate.
○ Automatically select the certificate store based on the type of certificate
● Place all certificates in the following store
Certificate store:
Browse...
Cancel
Select Certificate Store
Select the certificate store you want to use.
Personal
Trusted Root Certification Authorities
Enterprise Trust
Intermediate Certification Authorities
Active Directory User Object
Trusted Publishers
□ Show physical stores
OK
Cancel

2. In the Google Chrome browser address bar, type `https://<internal_IP_address>/isolator/https://www.<website-url>.com` (for example, `https://192.168.1.100/isolator/https://www.google.com`).

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



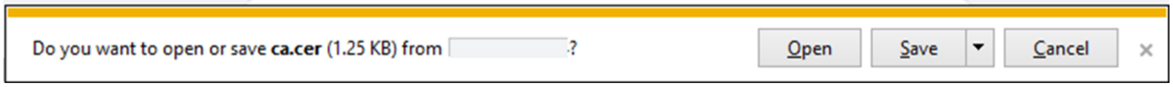
We've detected you're using an older version of Chrome.

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

Using IP Forwarding mode with Internet Explorer

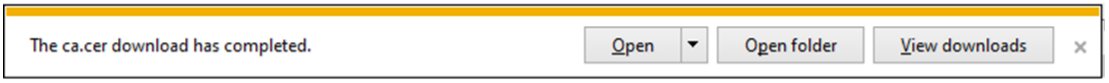
To configure IP Forwarding mode with Internet Explorer:

1. Download the FortiIsolator certificate (`ca.crt`) and import it into your Internet Explorer browser:
   - **a.** In the Internet Explorer browser address bar, type `http://<internal_IP_address>/ca.crt` (for example, `http://192.168.1.100/ca.crt`).
     - where `<internal_IP_address>` value is the IP address of the FortiIsolator internal interface. For example , the IP address of the internal interface that you configured in step 3 of FortiIsolator appliance installation on page 11.
   - **b.** In the security warning at the bottom of the browser, click *Save* to download the certificate.



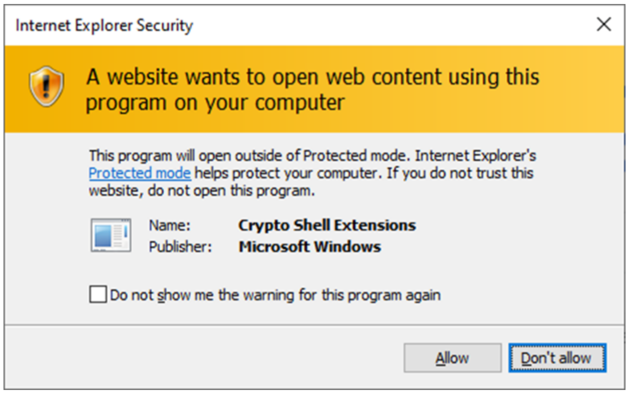
Do you want to open or save **ca.cer** (1.25 KB) from ?

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



The ca.cer download has completed.

d. Click *Allow* to install certificate.



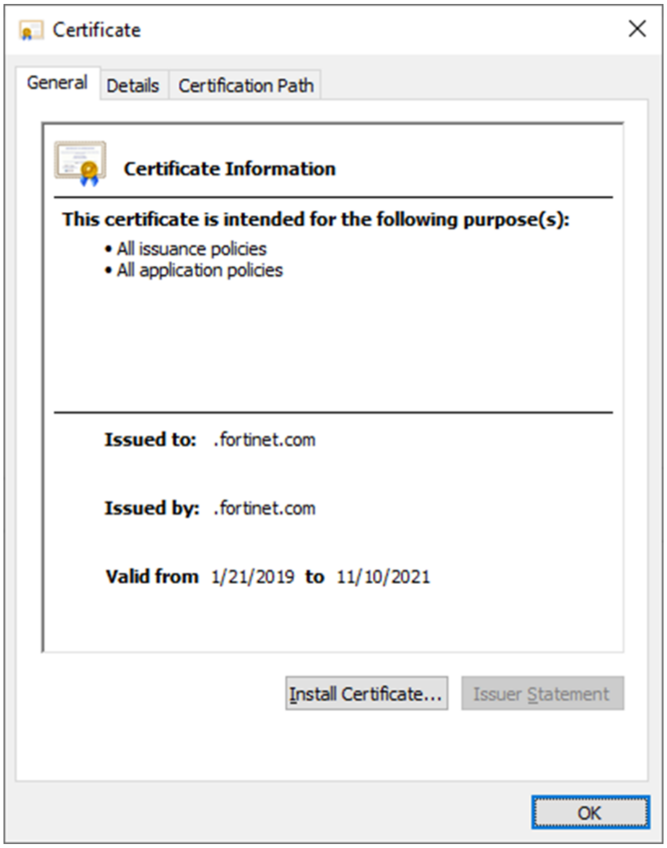
A website wants to open web content using this program on your computer

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

Name: Crypto Shell Extensions
Publisher: Microsoft Windows

☐ Do not show me the warning for this program again

e. Click *Install Certificate*.



Certificate Information

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

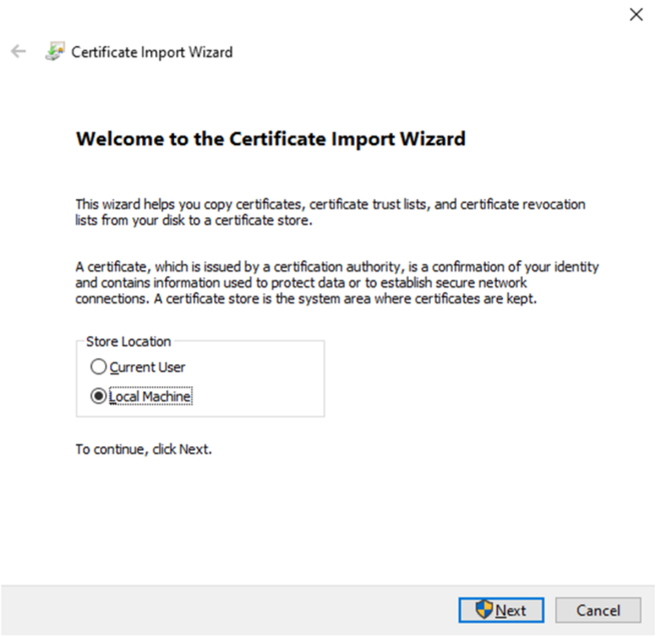
- All issuance policies
- All application policies

Issued to: .fortinet.com

Issued by: .fortinet.com

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

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



Certificate Import Wizard

Welcome to the Certificate Import Wizard

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

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

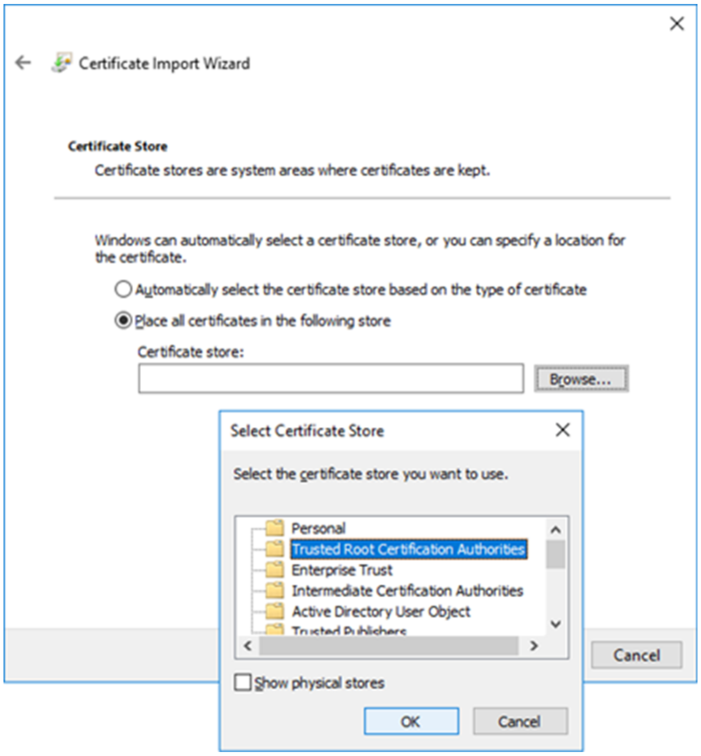
Store Location

○ Current User

● Local Machine

To continue, click Next.

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



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

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

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

● Place all certificates in the following store

Certificate store:

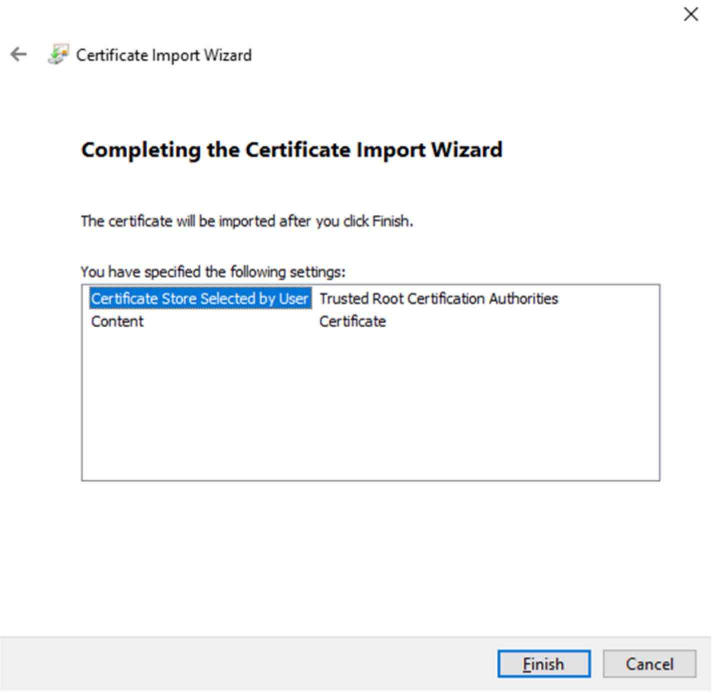
Select Certificate Store

Select the certificate store you want to use.

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

□ Show physical stores

h. Completing the Certificate Import Wizard.



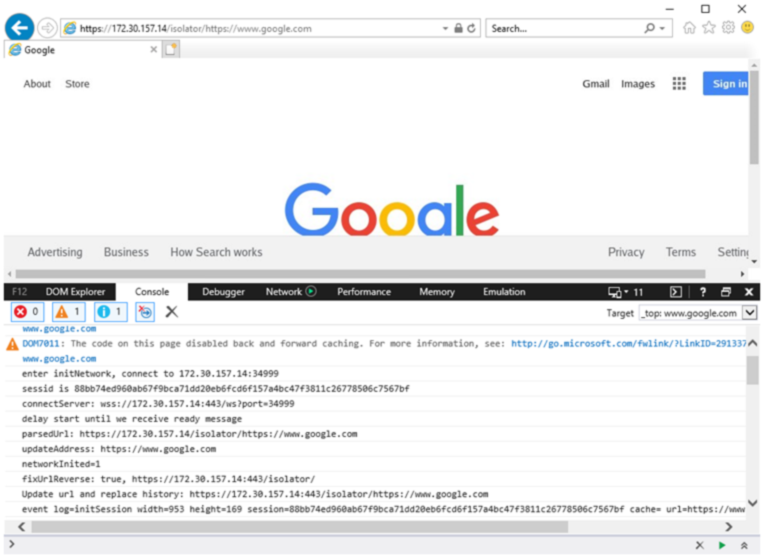
Completing the Certificate Import Wizard

The certificate will be imported after you click Finish.

You have specified the following settings:

Certificate Store Selected by User	Trusted Root Certification Authorities
Content	Certificate

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



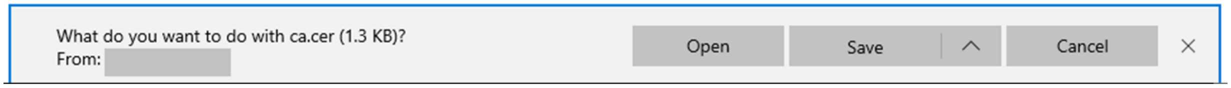
```
www.google.com
DOM7011: The code on this page disabled back and forward caching. For more information, see: http://go.microsoft.com/fwlink/?LinkID=291337
www.google.com
enter initNetwork, connect to 172.30.157.14:34999
sessid is 88bb74ed960ab67f9bca71dd20eb6fcd6f157a4bc47f3811c26778506c7567bf
connectServer: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

Using IP Forwarding mode with Edge

To configure IP Forwarding mode with Edge browser:

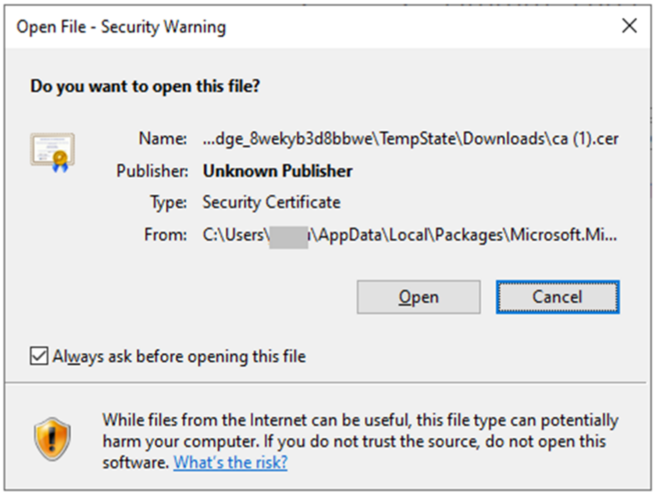
1. Download the FortiIsolator certificate (`ca.crt`) and import it into your Edge browser:
   a. In the Edge browser address bar, type `http://<internal_IP_address>/ca.crt` (for example, `http://192.168.1.100/ca.crt`).
      - where <`internal_IP_address`> value is the IP address of the FortiIsolator internal interface. For example , the IP address of the internal interface that you configured in step 3 of FortiIsolator appliance installation on page 11.

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



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

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



Open File - Security Warning

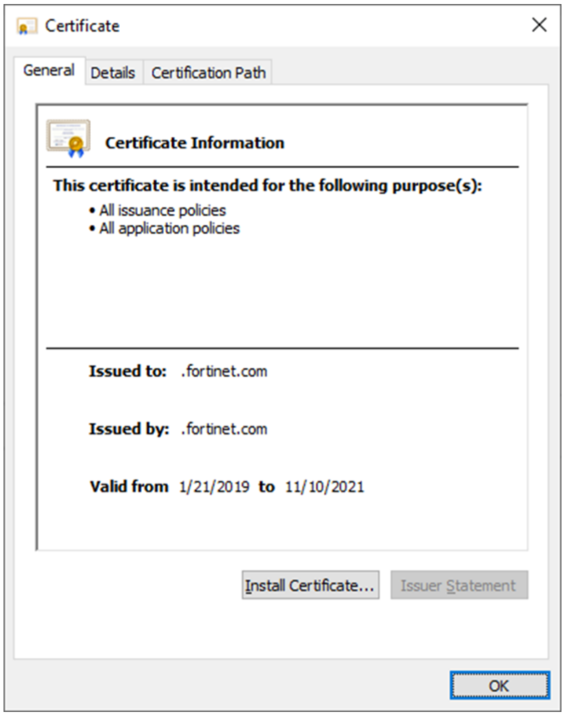
Do you want to open this file?

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

☑ Always ask before opening this file

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

d. Click *Install Certificate*.



Certificate

Certificate Information

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

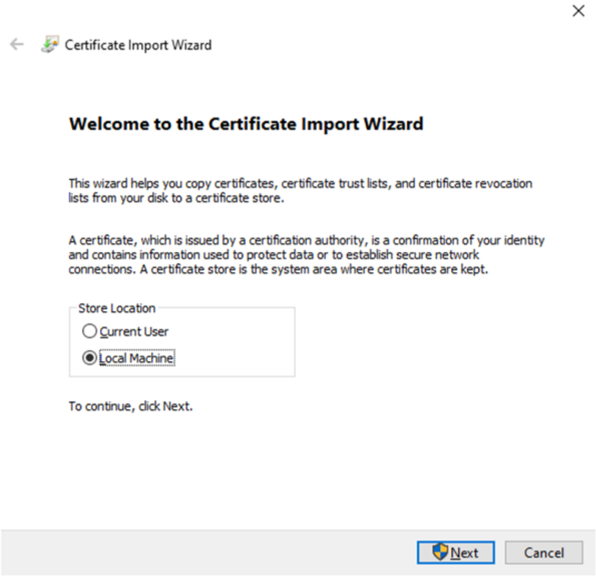
- All issuance policies
- All application policies

Issued to: .fortinet.com

Issued by: .fortinet.com

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

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



Certificate Import Wizard

Welcome to the Certificate Import Wizard

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

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

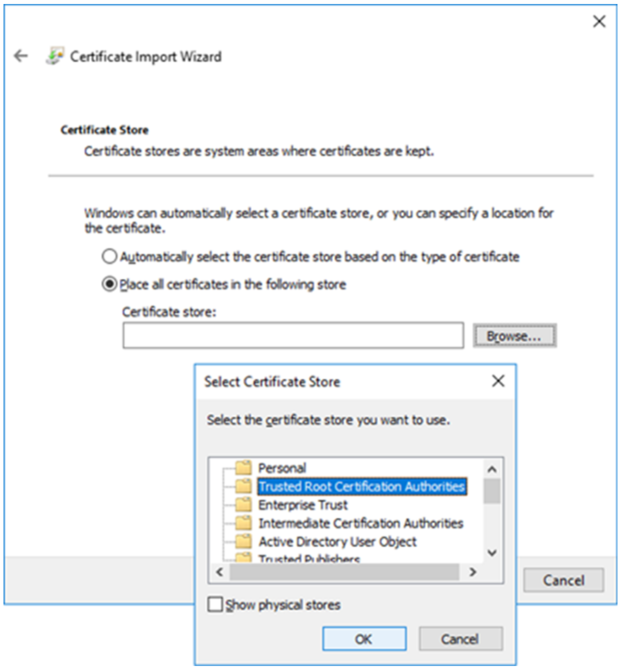
Store Location

○ Current User

● Local Machine

To continue, click Next.

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



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

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

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

● Place all certificates in the following store

Certificate store:

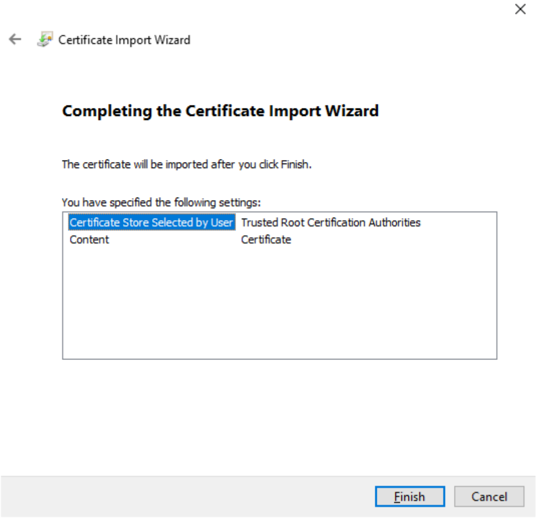
Select Certificate Store

Select the certificate store you want to use.

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

□ Show physical stores

g. Completing the Certificate Import Wizard.



Certificate Import Wizard

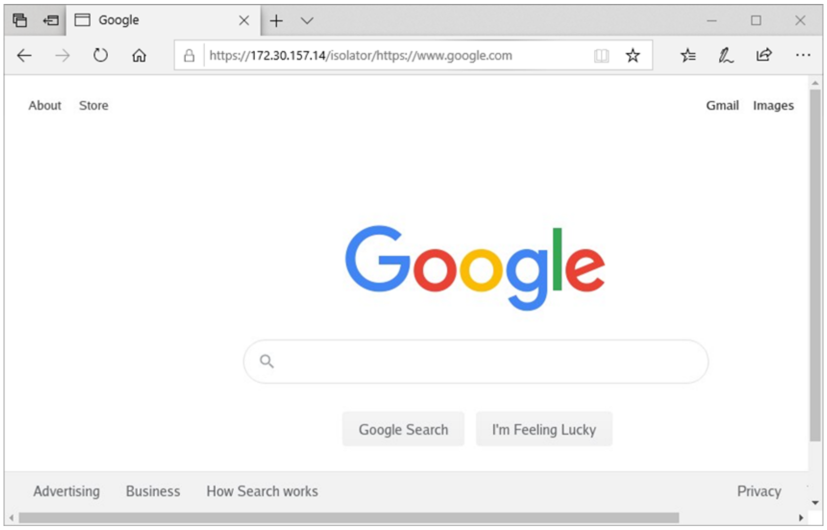
Completing the Certificate Import Wizard

The certificate will be imported after you click Finish.

You have specified the following settings:

Certificate Store Selected by User	Trusted Root Certification Authorities
Content	Certificate

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



https://172.30.157.14/isolator/https://www.google.com

Proxy mode

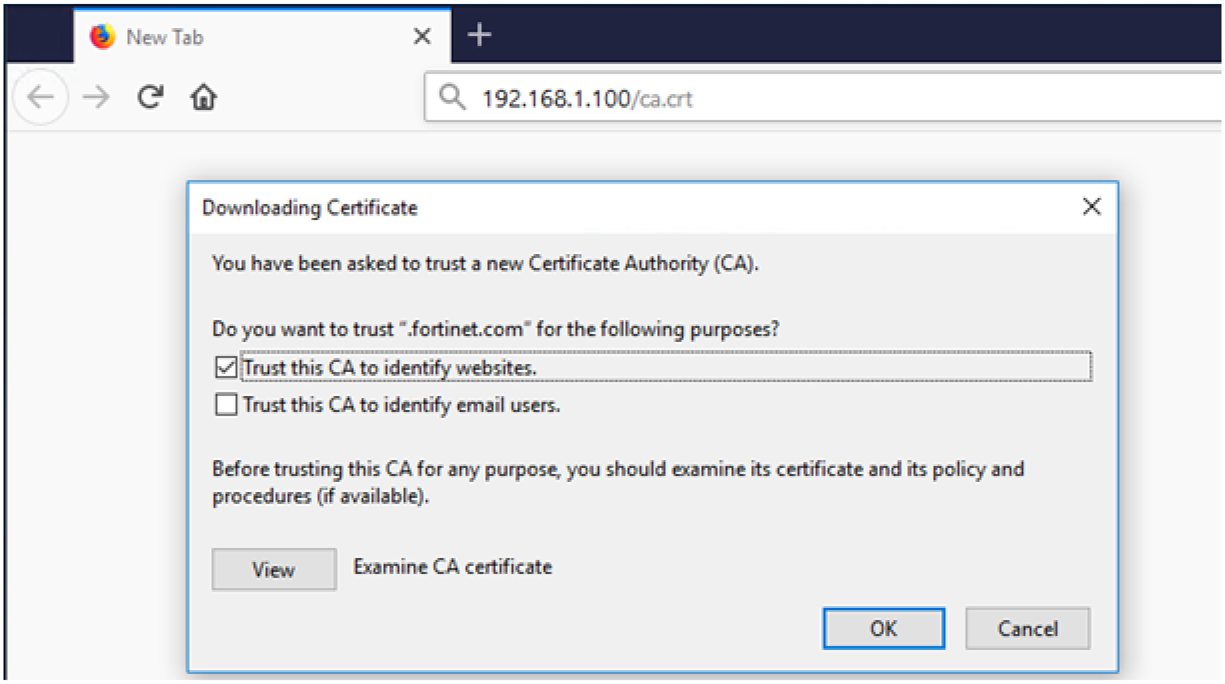
Using proxy mode with Mozilla Firefox

To configure proxy mode with Mozilla Firefox:

1. Download the FortiIsolator certificate (`ca.crt`) and import it into the Mozilla Firefox browser:
   a. In the Mozilla Firefox browser address bar, type `http://<internal_IP_address>/ca.crt` (for example, `http://192.168.1.100/ca.crt`).
      - where *<internal_IP_address>* is the IP address of the FortiIsolator internal interface. For example, the IP address of the internal interface that you configured in step 3 of Installing FortiIsolator 1000F on page 11.

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

   c. Click *OK*.



Downloading Certificate

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

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

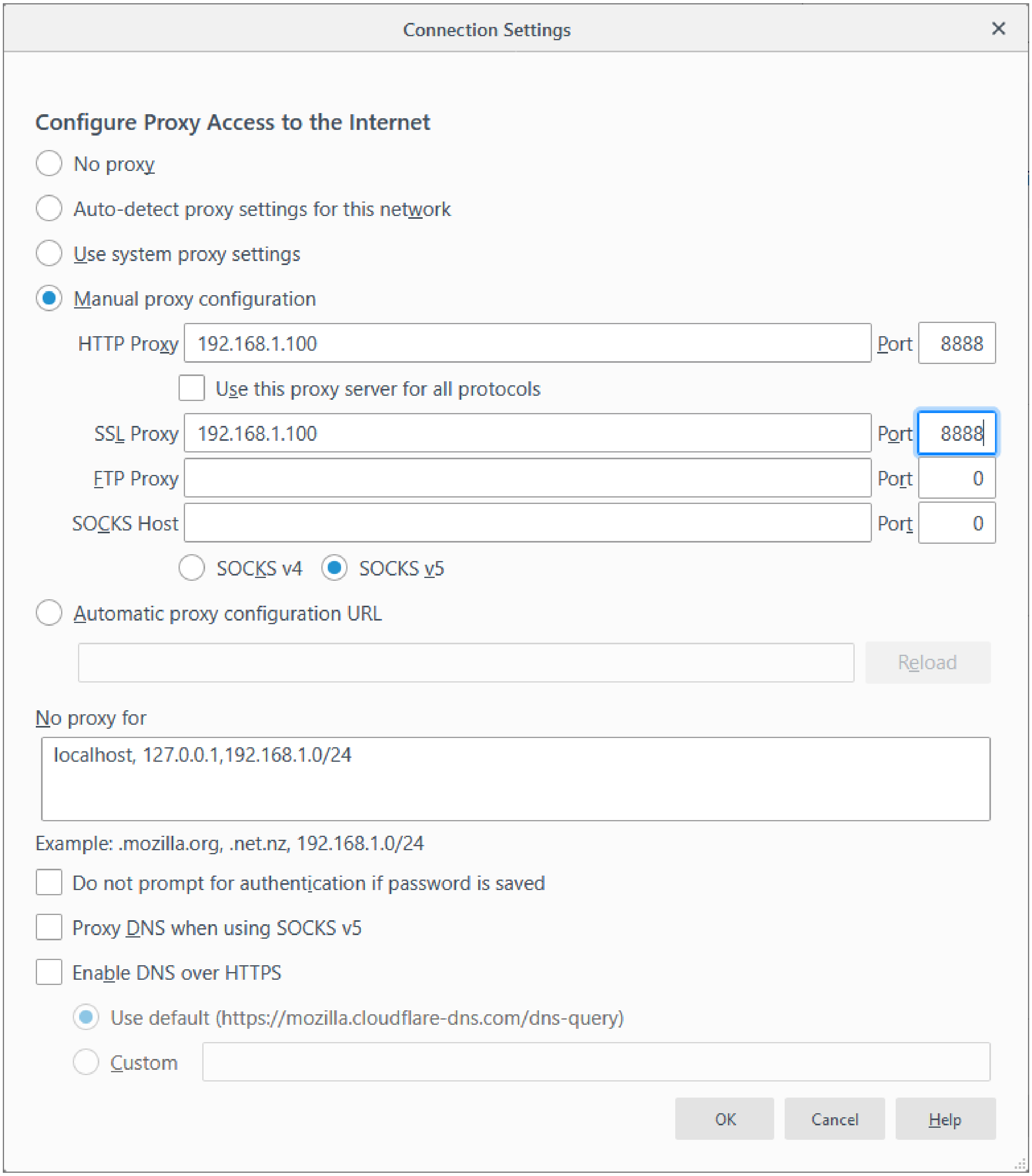
☑ Trust this CA to identify websites.

□ Trust this CA to identify email users.

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

Examine CA certificate

2. Open the Mozilla Firefox browser.
3. In the menu, click *Options*.
4. Click *General*.
5. In the *Network Settings* section, click *Settings*.
6. In the *Connection Settings* window, select *Manual proxy configuration*, and enter the following settings (values shown here are examples):
   - **HTTP Proxy**: 192.168.1.100, **Port**: 8888
   - **SSL Proxy**: 192.168.1.100, **Port**: 8888
   - **No Proxy for**: "localhost, 127.0.0.1,`<internal_IP_address>`/24", where `<internal_IP_address>` is the IP address of the FortiIsolator internal interface. For example , the IP address of the internal interface that you configured in step 3 of Installing FortiIsolator 1000F on page 11.
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

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

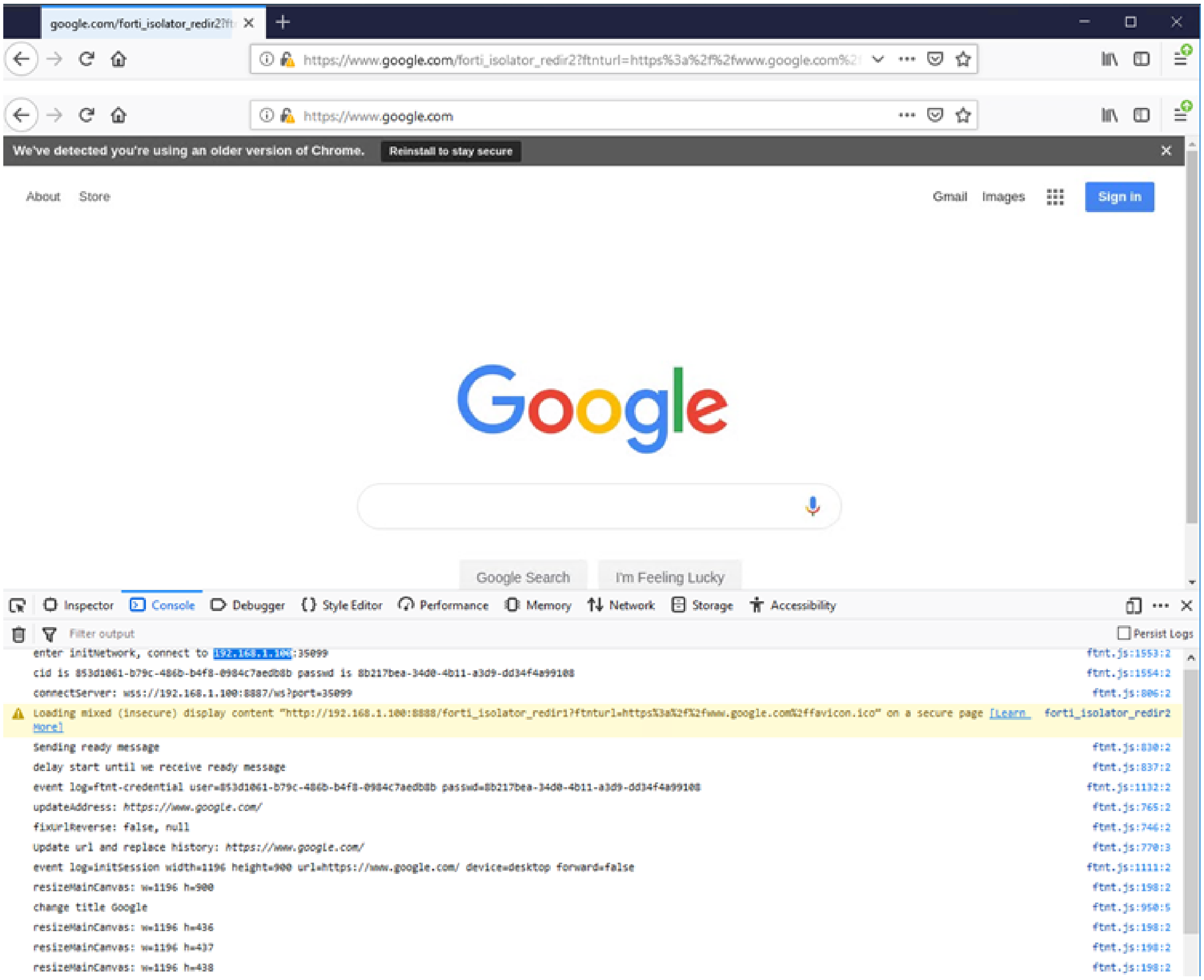
● Use default (https://mozilla.cloudflare-dns.com/dns-query)

○ Custom

Verifying FortiIsolator proxy mode with Mozilla Firefox

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

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



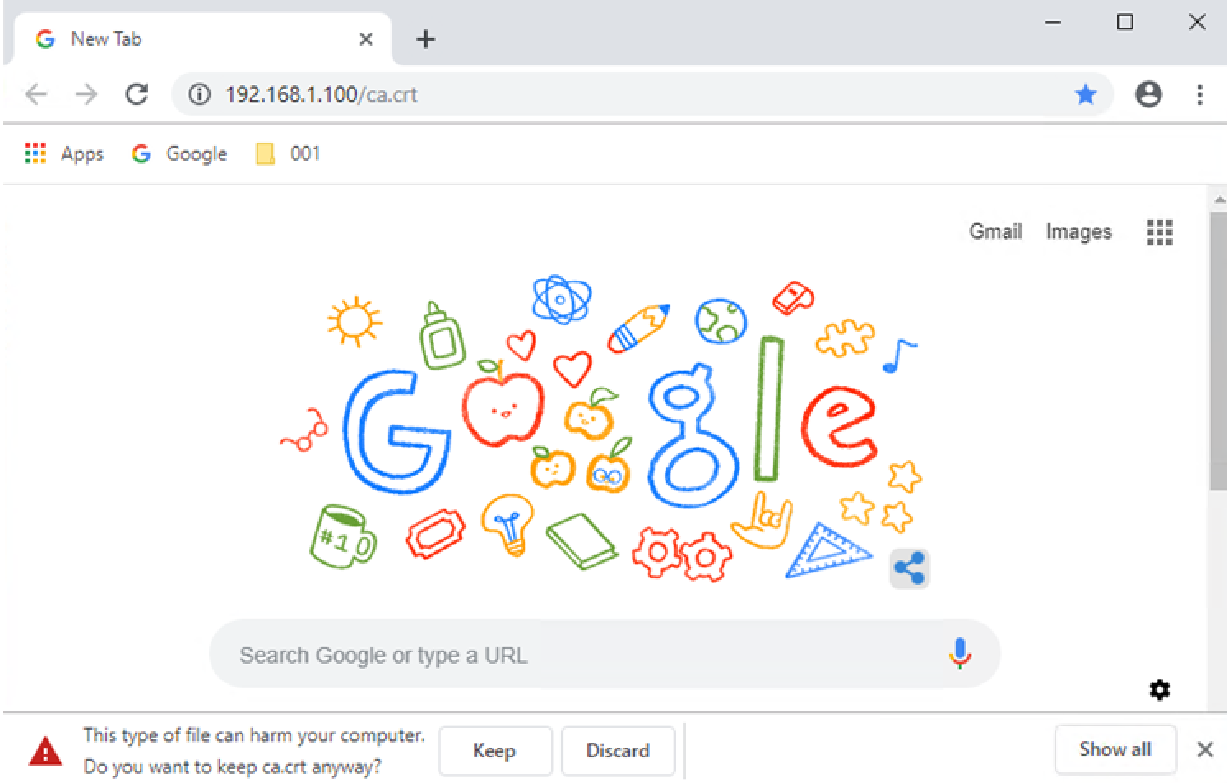
```
enter initNetwork, connect to 192.168.1.100:35099                                                    ftnt.js:1553:2
cid is 853d1061-b79c-486b-b4f8-0984c7aedb8b passwd is 8b217bea-34d0-4b11-a3d9-dd34f4a99108            ftnt.js:1554:2
connectServer: wss://192.168.1.100:8887/ws?port=35099          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

Using proxy mode with Google Chrome

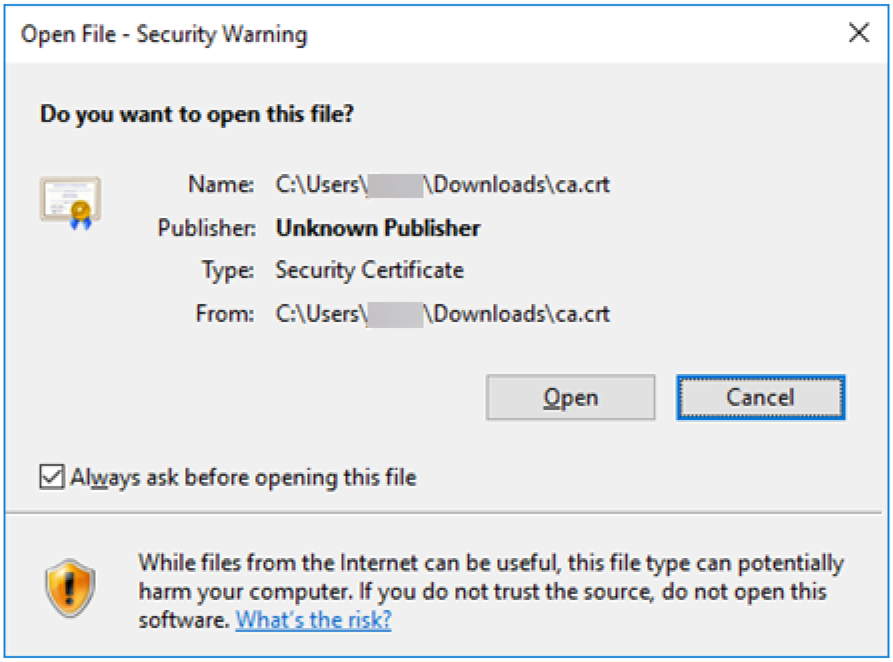
To configure proxy mode with Google Chrome:

1. Download the FortiIsolator certificate (`ca.crt`) and import it into your Google Chrome browser:
   a. In the Google Chrome browser address bar, type `http://<internal_IP_address>/ca.crt` (for example, `http://192.168.1.100/ca.crt`).
      - where *`<internal_IP_address>`* value is the IP address of the FortiIsolator internal interface. For example , the IP address of the internal interface that you configured in step 3 of Installing FortiIsolator 1000F on page 11.

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


New Tab
192.168.1.100/ca.crt
Apps
Google
001
Gmail
Images
Search Google or type a URL
This type of file can harm your computer.
Do you want to keep ca.crt anyway?
Keep
Discard
Show all

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



Open File - Security Warning

Do you want to open this file?

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

Publisher: **Unknown Publisher**

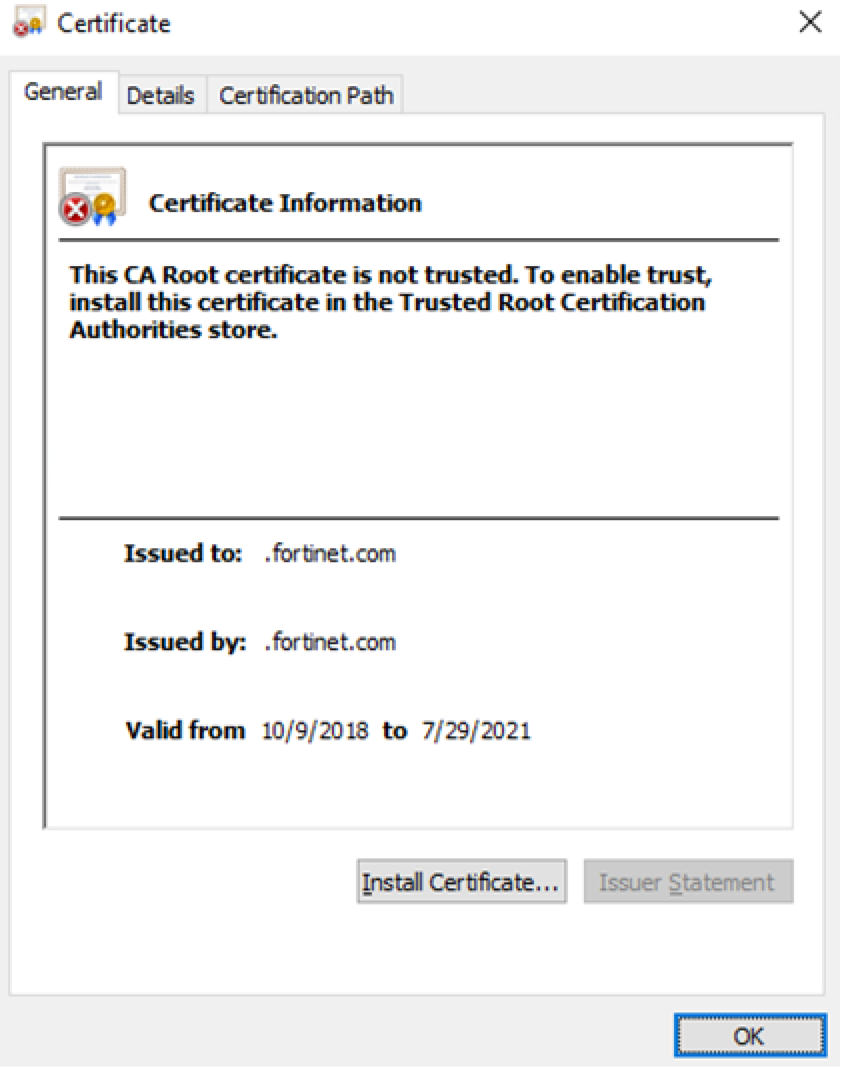
Type: Security Certificate

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

☑ Always ask before opening this file

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

d. Click *Install Certificate*.



Certificate Information

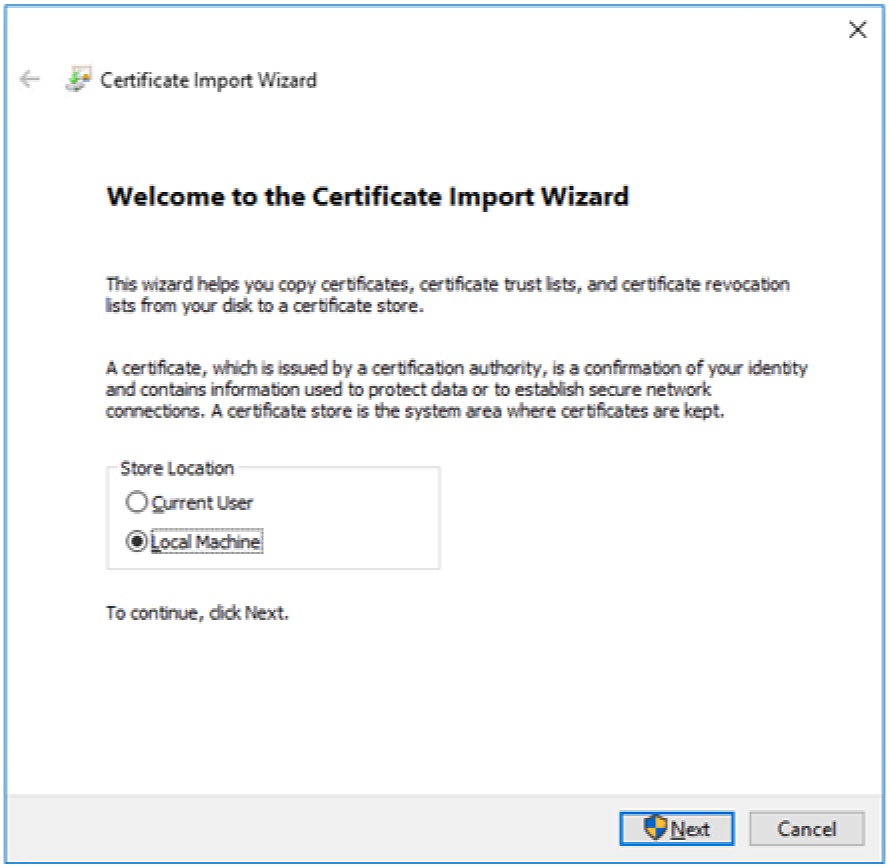
This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

Issued to: .fortinet.com

Issued by: .fortinet.com

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

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



Certificate Import Wizard

Welcome to the Certificate Import Wizard

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

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

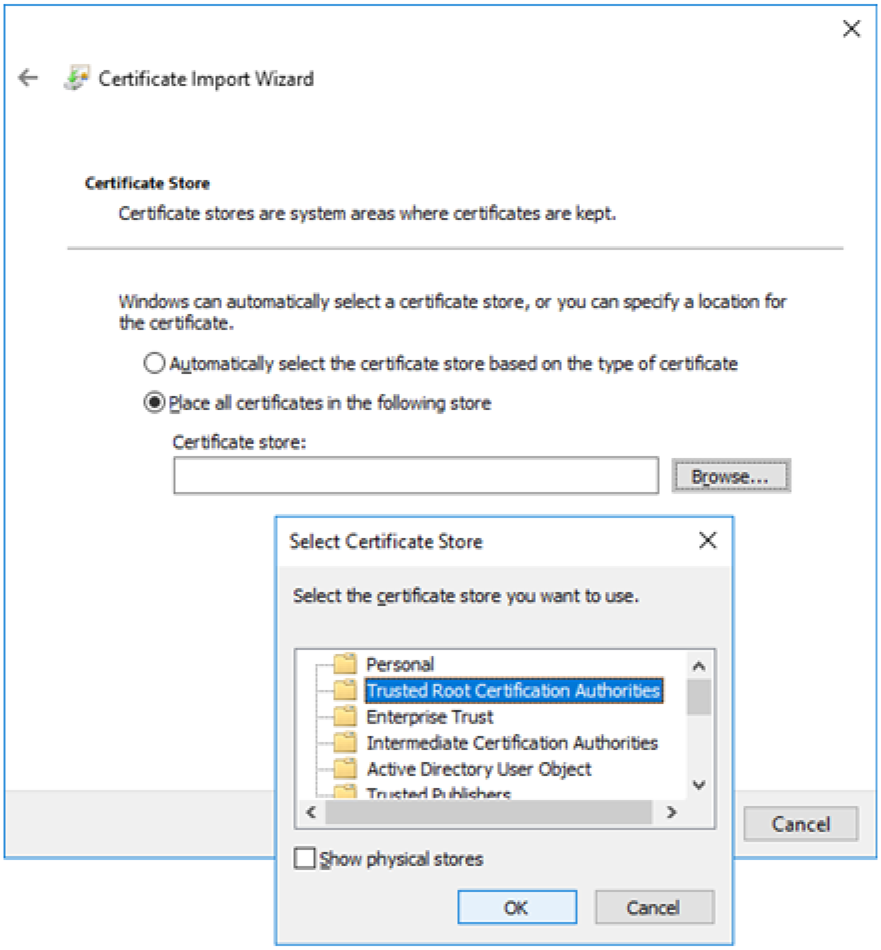
Store Location

○ Current User

● Local Machine

To continue, click Next.

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



Certificate Store

Certificate stores are system areas where certificates are kept.

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

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

● Place all certificates in the following store

Certificate store:

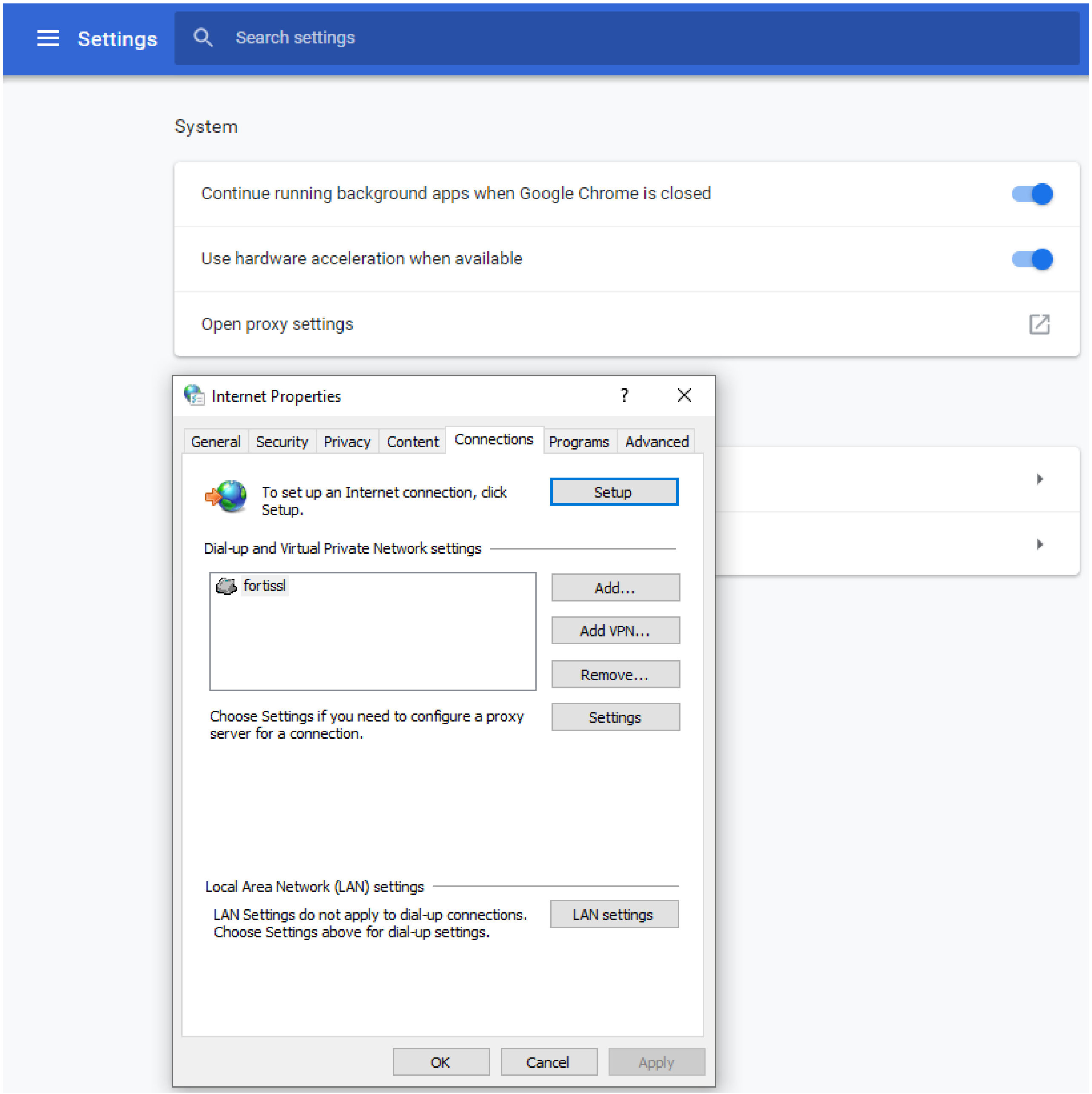
Select the certificate store you want to use.

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

□ Show physical stores

2. Open the Google Chrome browser.

3. In the menu, click *Settings*.



Continue running background apps when Google Chrome is closed

Use hardware acceleration when available

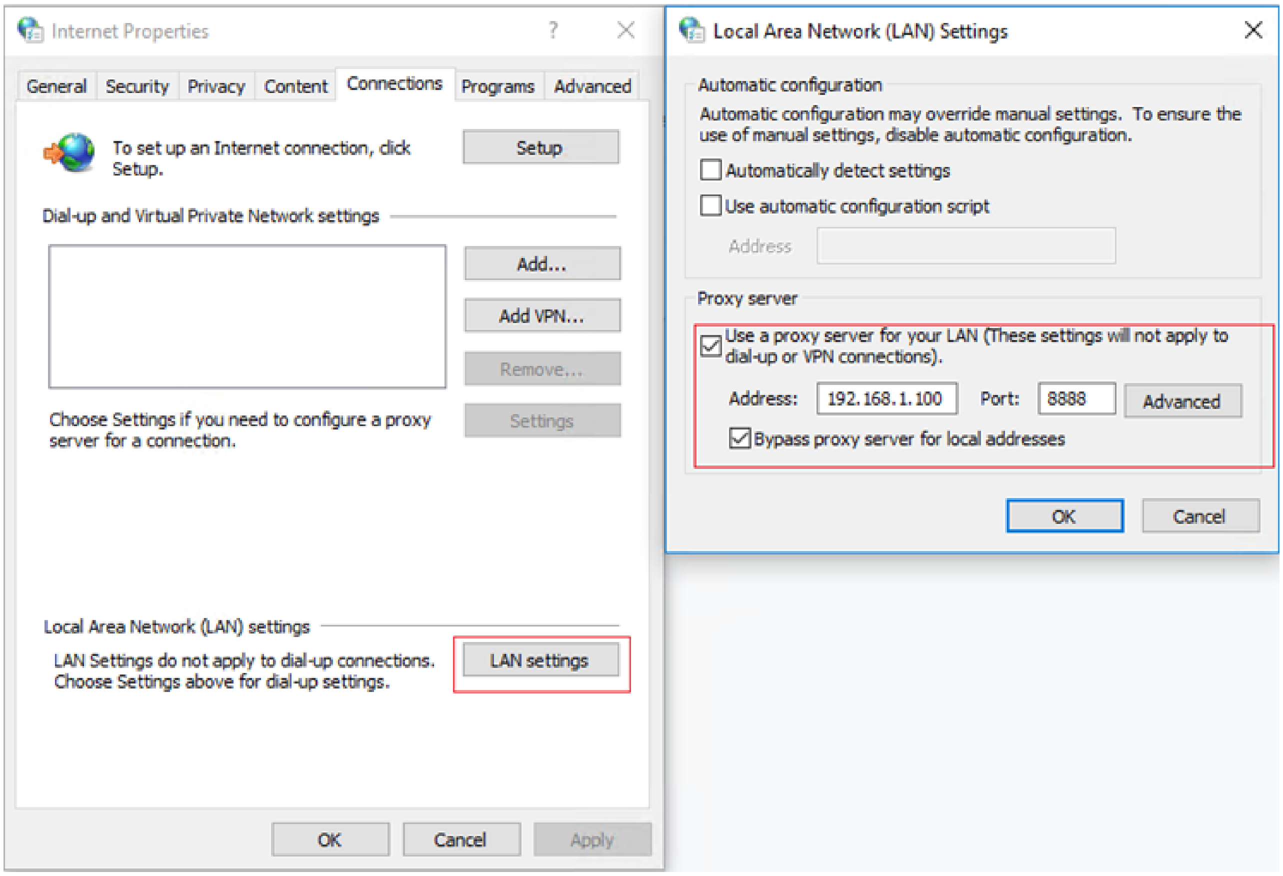
Open proxy settings

To set up an Internet connection, click Setup.

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

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

4. 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



Internet Properties

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

To set up an Internet connection, click Setup. [Setup]

Dial-up and Virtual Private Network settings

[Add...] [Add VPN...] [Remove...]

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

Local Area Network (LAN) settings

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

[OK] [Cancel] [Apply]

Local Area Network (LAN) Settings

Automatic configuration

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

☐ Automatically detect settings

☐ Use automatic configuration script

Address

Proxy server

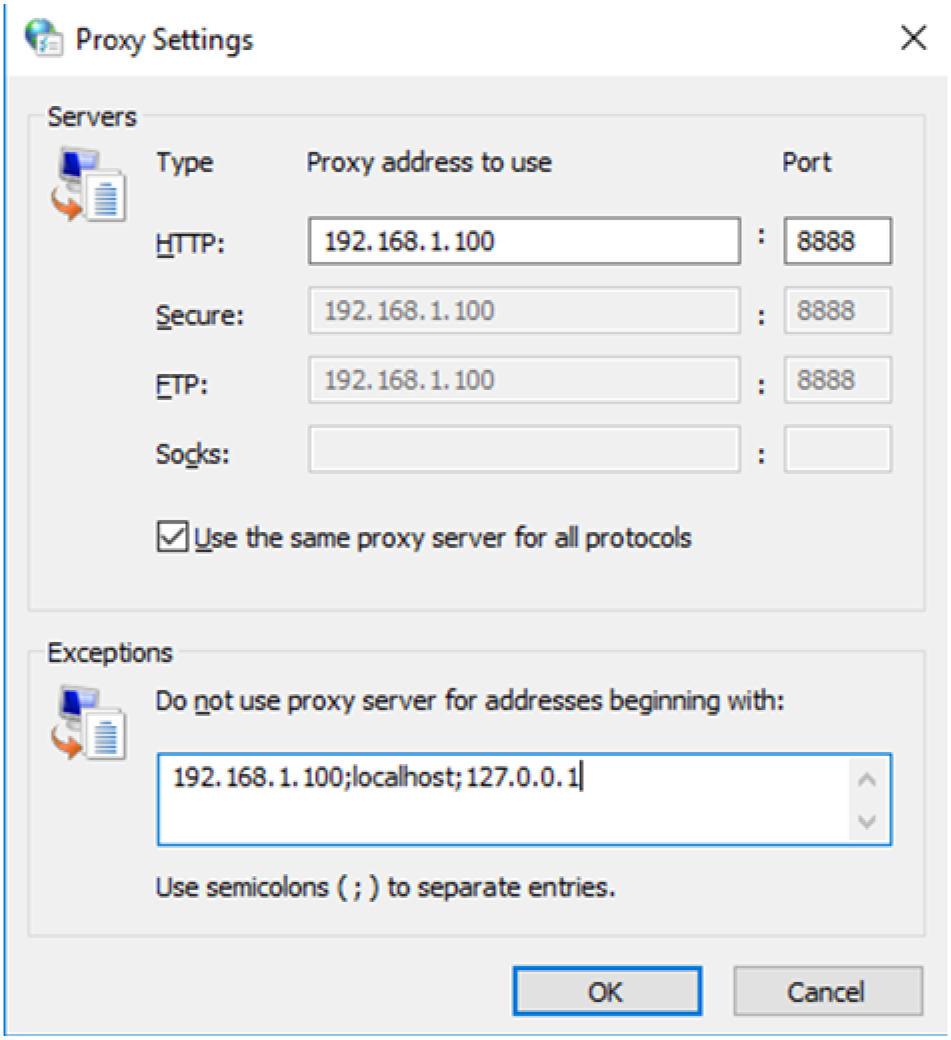
☑ Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).

Address: 192.168.1.100 Port: 8888 [Advanced]

☑ Bypass proxy server for local addresses

[OK] [Cancel]

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



Proxy Settings

Servers

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

☑ Use the same proxy server for all protocols

Exceptions

Do not use proxy server for addresses beginning with:

192.168.1.100;localhost;127.0.0.1

Use semicolons (;) to separate entries.

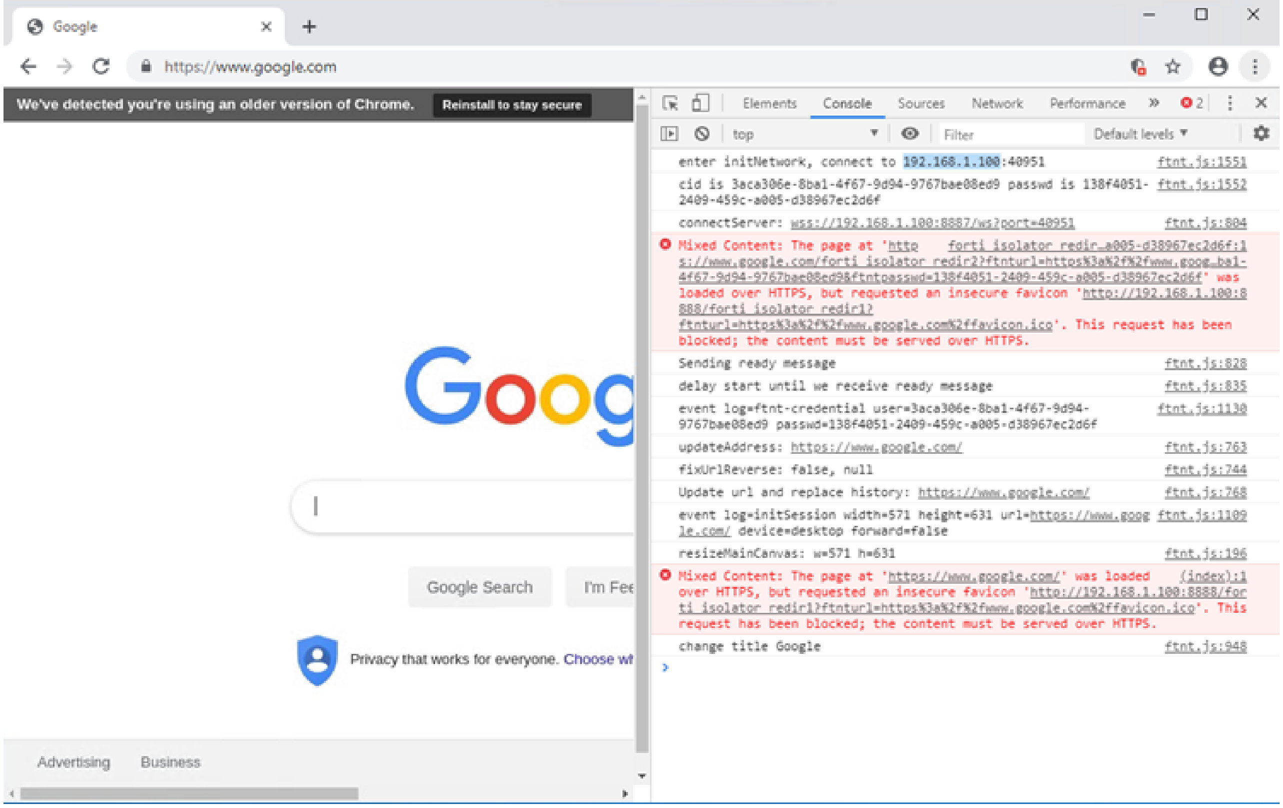
11. Click *OK* to accept the settings in all windows.

Verifying FortiIsolator proxy mode with Google Chrome

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

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

192.168.1.100).



```
enter initNetwork, connect to 192.168.1.100:40951                      ftnt.js:1551
cid is 3aca306e-8ba1-4f67-9d94-9767bae08ed9 passwd is 138f4051-       ftnt.js:1552
2409-459c-a005-d38967ec2d6f
connectServer: wss://192.168.1.100:8887/ws?port=40951                   ftnt.js:804
Mixed Content: The page at 'http    forti_isolator_redir…a005-d38967ec2d6f:1
s://www.google.com/forti_isolator_redir2?ftnturl=https%3a%2f%2fwww.goog…ba1-
4f67-9d94-9767bae08ed9&ftntpasswd=138f4051-2409-459c-a005-d38967ec2d6f' was
loaded over HTTPS, but requested an insecure favicon 'http://192.168.1.100:8
888/forti_isolator_redir1?
ftnturl=https%3a%2f%2fwww.google.com%2ffavicon.ico'. This request has been
blocked; the content must be served over HTTPS.
Sending ready message                                                   ftnt.js:828
delay start until we receive ready message                              ftnt.js:835
event log=ftnt-credential user=3aca306e-8ba1-4f67-9d94-                ftnt.js:1130
9767bae08ed9 passwd=138f4051-2409-459c-a005-d38967ec2d6f
updateAddress: https://www.google.com/                                  ftnt.js:763
fixUrlReverse: false, null                                              ftnt.js:744
Update url and replace history: https://www.google.com/                 ftnt.js:768
event log=initSession width=571 height=631 url=https://www.goog ftnt.js:1109
le.com/ device=desktop forward=false
resizeMainCanvas: w=571 h=631                                           ftnt.js:196
Mixed Content: The page at 'https://www.google.com/' was loaded    (index):1
over HTTPS, but requested an insecure favicon 'http://192.168.1.100:8888/for
ti_isolator_redir1?ftnturl=https%3a%2f%2fwww.google.com%2ffavicon.ico'. This
request has been blocked; the content must be served over HTTPS.
change title Google                                                     ftnt.js:948
```

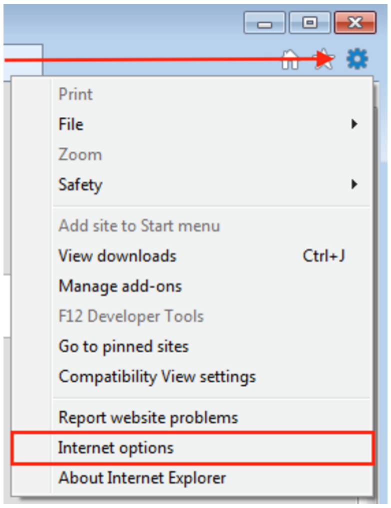
Using proxy mode with Internet Explorer

Pre-requisites:

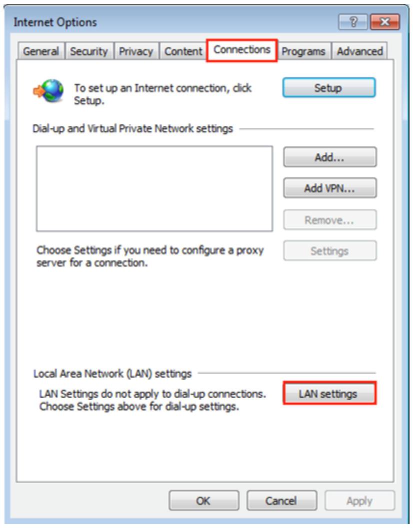
Please follow step 1 in Using IP Forwarding mode with Internet Explorer on page 124 to install FortiIsoaltor `ca.crt` certificate prior to using proxy mode.

To configure proxy mode with Internet Explorer:

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



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

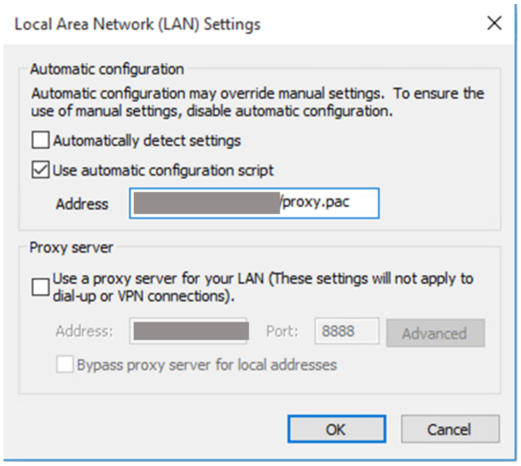


To set up an Internet connection, click Setup.

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

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

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



Local Area Network (LAN) Settings

Automatic configuration

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

□ Automatically detect settings

☑ Use automatic configuration script

Address [redacted]/proxy.pac

Proxy server

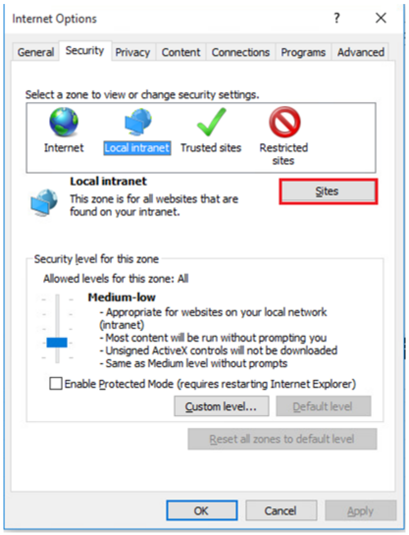
□ Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).

Address: [redacted] Port: 8888 Advanced

□ Bypass proxy server for local addresses

OK Cancel

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



Internet Options

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

Select a zone to view or change security settings.

Internet | Local intranet | Trusted sites | Restricted sites

Local intranet

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

Sites

Security level for this zone

Allowed levels for this zone: All

Medium-low

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

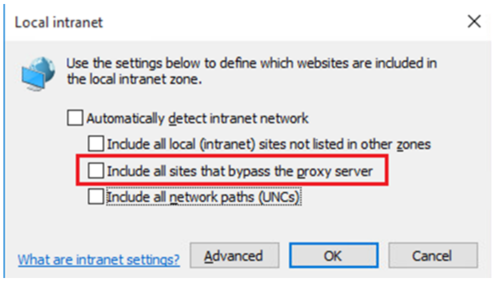
□ Enable Protected Mode (requires restarting Internet Explorer)

Custom level... Default level

Reset all zones to default level

OK Cancel Apply

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



Local intranet

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

□ Automatically detect intranet network

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

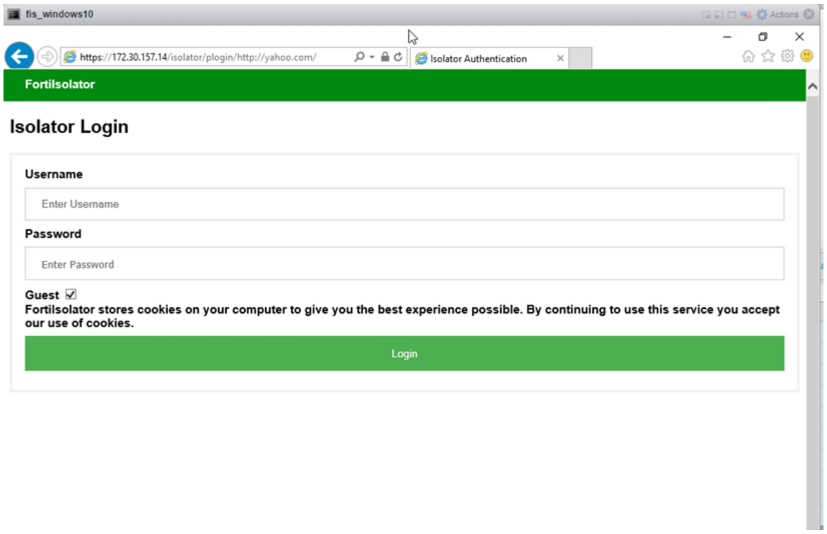
□ Include all sites that bypass the proxy server

□ Include all network paths (UNCs)

What are intranet settings? Advanced OK Cancel

9. Close and restart Internet Explorer.

Verifying FortiIsolator proxy mode with Internet Explorer



Isolator Login

Username

Enter Username

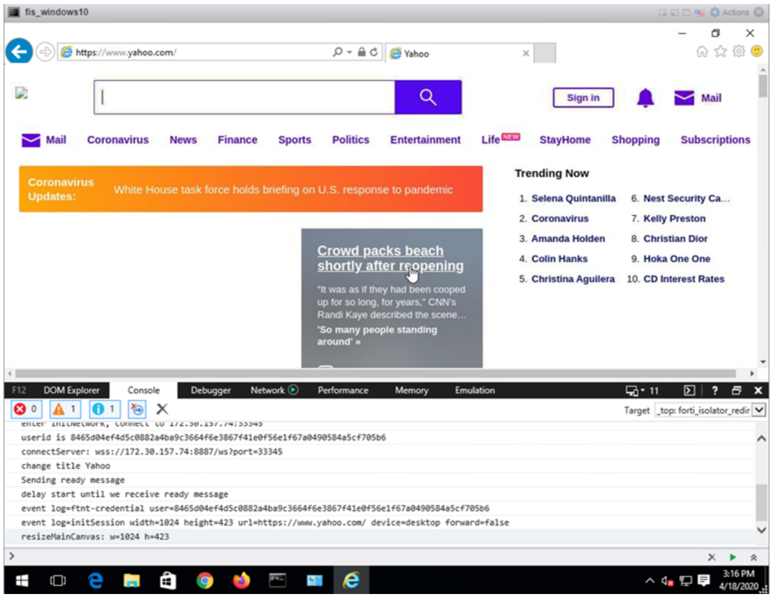
Password

Enter Password

Guest ☑

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

Login



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

Trending Now

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

Crowd packs beach shortly after reopening

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

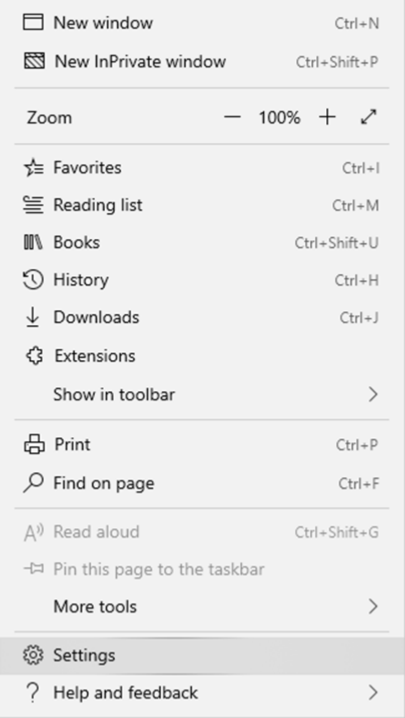
'So many people standing around' »

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

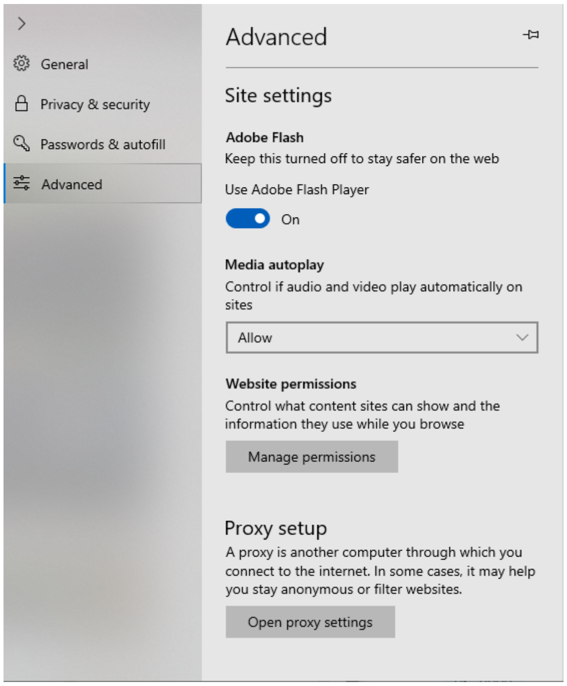
Using proxy mode with Edge

To configure proxy mode with Edge:

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



3. Click *Advanced*.



Advanced

Site settings

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

Use Adobe Flash Player
On

Media autoplay
Control if audio and video play automatically on sites

Allow

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

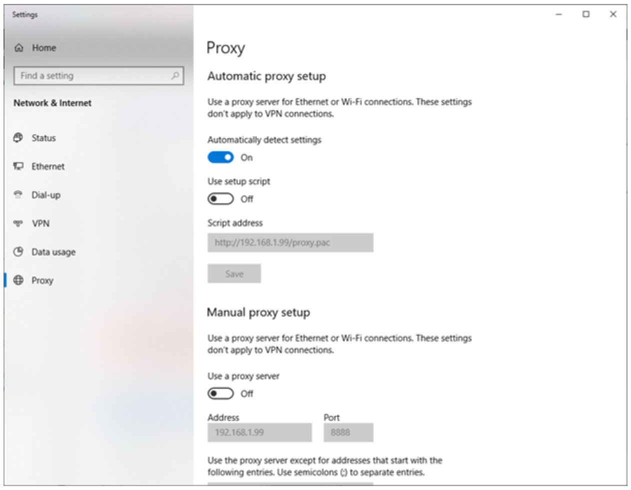
Manage permissions

Proxy setup

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

Open proxy settings

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



Proxy

Automatic proxy setup

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

Automatically detect settings
On

Use setup script
Off

Script address
http://192.168.1.99/proxy.pac

Save

Manual proxy setup

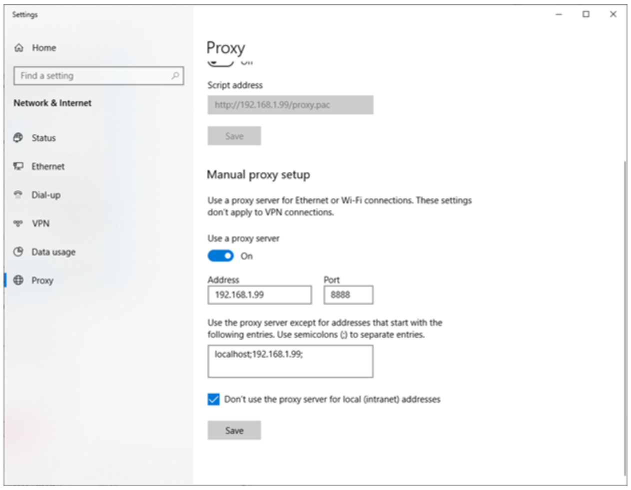
Use a proxy server for Ethernet or Wi-Fi connections. These settings don't apply to VPN connections.

Use a proxy server
Off

Address: 192.168.1.99
Port: 8888

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

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



Proxy

Script address
http://192.168.1.99/proxy.pac

Save

Manual proxy setup

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

Use a proxy server
On

Address: 192.168.1.99
Port: 8888

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

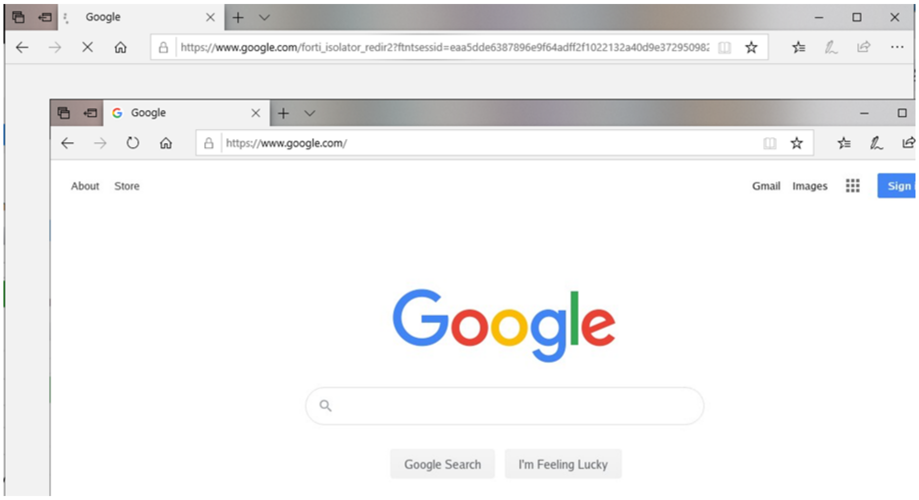
localhost;192.168.1.99;

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

Save

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

Verifying FortiIsolator proxy mode with Edge



https://www.google.com/forti_isolator_redir2?ftntsessid=eaa5dde6387896e9f64adff2f1022132a40d9e37295098:

https://www.google.com/

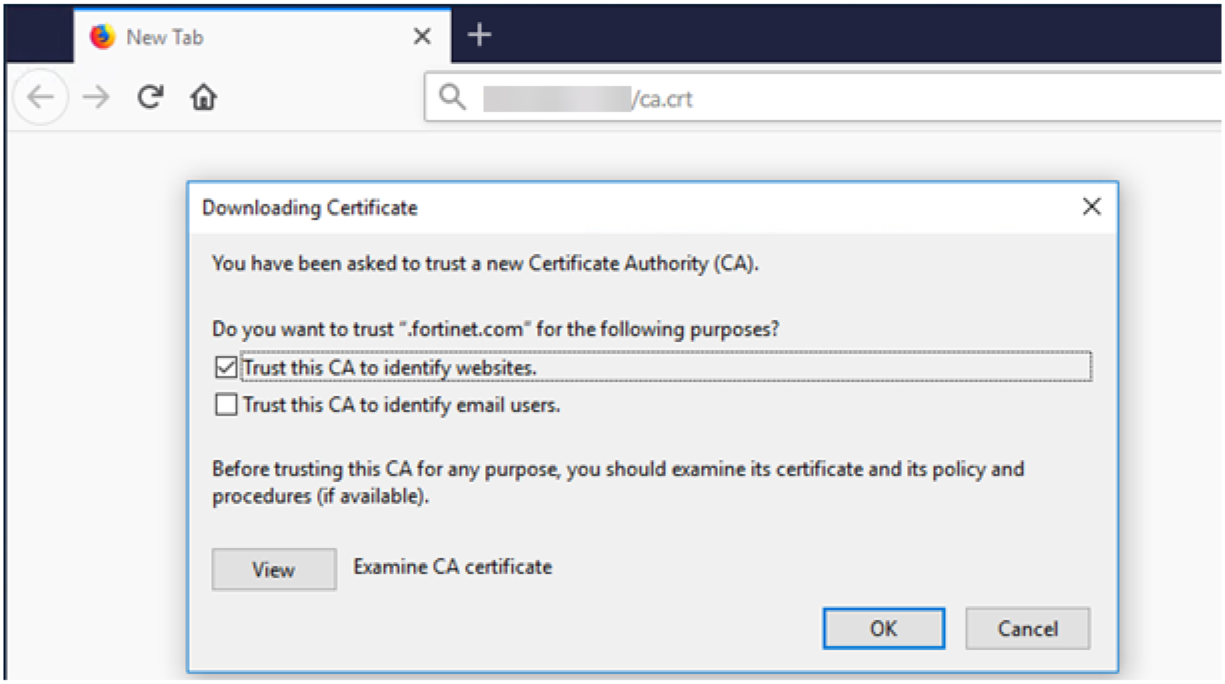
PAC file mode

PAC file mode with Mozilla Firefox

Importing the FortiIsolator certificate into the Mozilla Firefox browser

To import the FortiIsolator certificate into the Mozilla Firefox browser:

1. Download the FortiIsolator certificate (`ca.crt`) and import it into the Mozilla Firefox browser:
   a. In the Mozilla Firefox browser address bar, type `http://<internal_IP_address>/ca.crt`.
      - where `<internal_IP_address>` is the IP address of the FortiIsolator internal interface. For example, the IP address of the internal interface that you configured in step 3 of Installing FortiIsolator 1000F on page 11
   b. In the *Downloading Certificate* window, select the *Trust this CA to identify websites* checkbox.
   c. Click *OK*.



Downloading Certificate

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

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

☑ Trust this CA to identify websites.

☐ Trust this CA to identify email users.

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

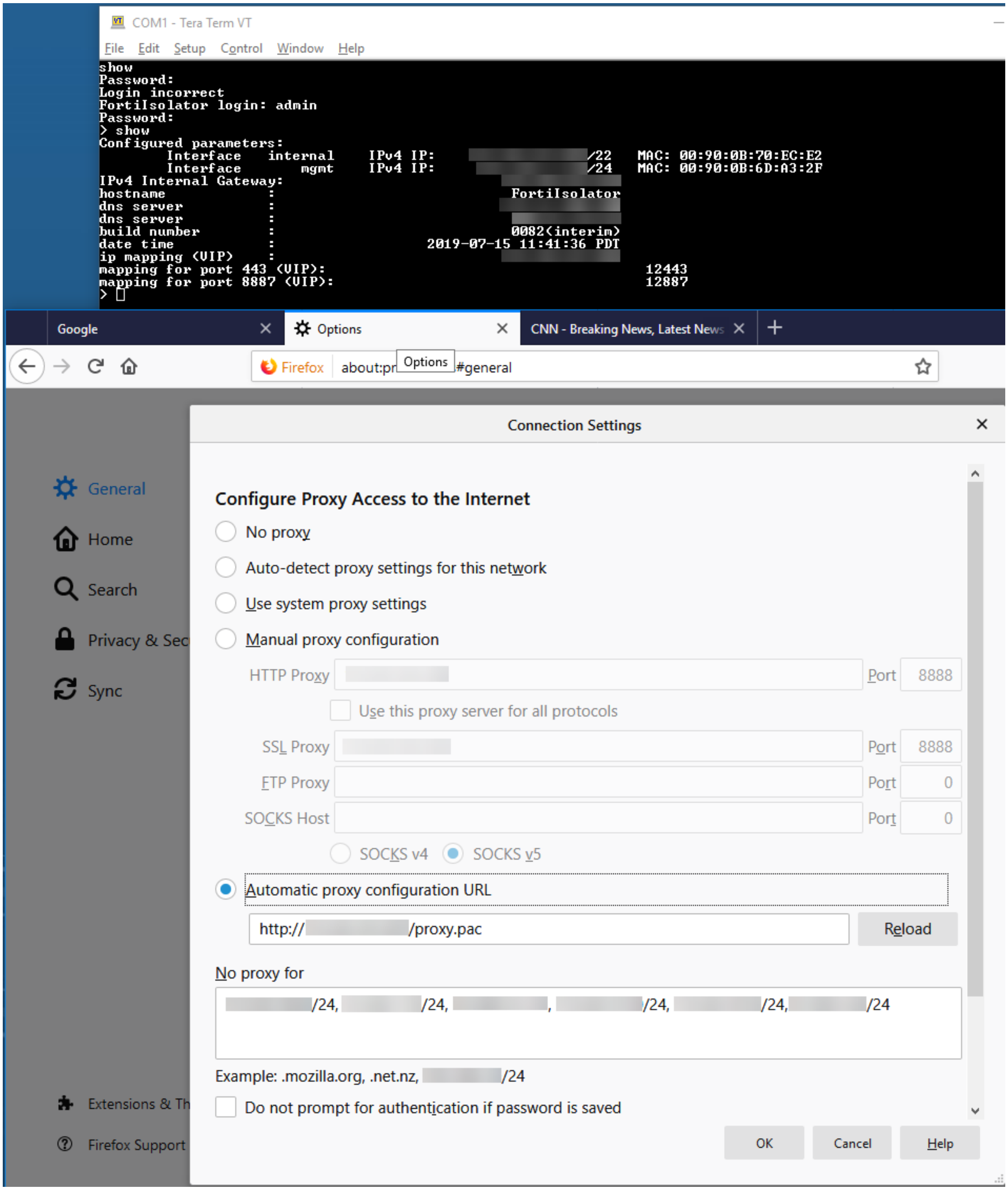
Examine CA certificate

Configuring PAC file mode in Mozilla Firefox

To configure PAC file mode in Mozilla Firefox:

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`.



```
show
Password:
Login incorrect
FortiIsolator 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:                       [redacted]
hostname               :                  FortiIsolator
dns server             :                     [redacted]
dns server             :                     [redacted]
build number           :                  0082(interim)
date time              :        2019-07-15 11:41:36 PDT
ip mapping (VIP)       :                     [redacted]
mapping for port 443 (VIP):                         12443
mapping for port 8887 (VIP):                        12887
> 
```

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 [redacted] Port 8888

□ Use this proxy server for all protocols

SSL Proxy [redacted] Port 8888

FTP Proxy Port 0

SOCKS Host Port 0

○ SOCKS v4 ● SOCKS v5

● Automatic proxy configuration URL

http://[redacted]/proxy.pac Reload

No proxy for

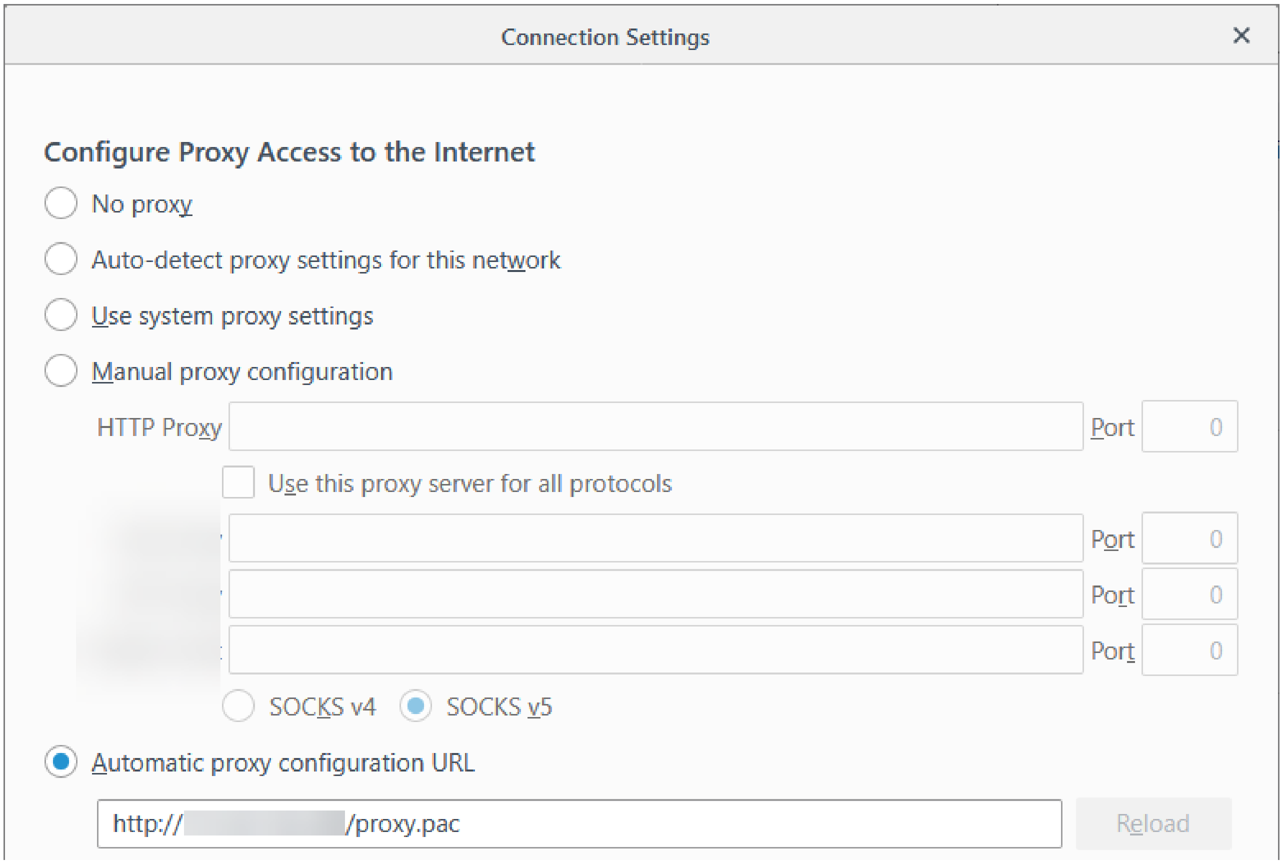
[redacted]/24, [redacted]/24, [redacted], [redacted]/24, [redacted]/24,[redacted]/24

Example: .mozilla.org, .net.nz, [redacted]/24

□ Do not prompt for authentication if password is saved

OK Cancel Help

6. 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 Port 0

□ Use this proxy server for all protocols

Port 0

Port 0

Port 0

○ SOCKS v4 ● SOCKS v5

● Automatic proxy configuration URL

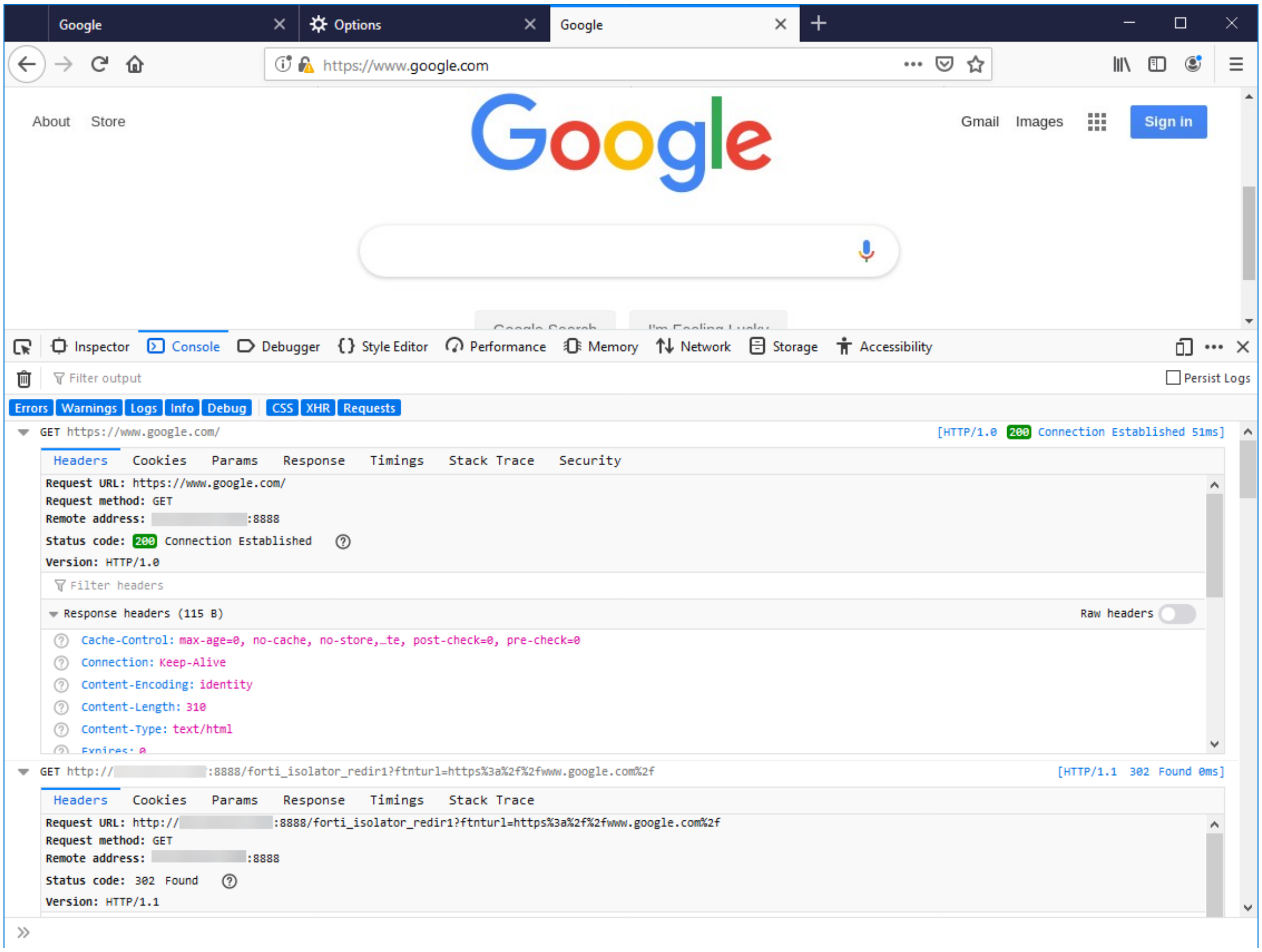
http://[redacted]/proxy.pac

Verifying FortiIsolator PAC file mode with Mozilla Firefox

To verify that FortiIsolator PAC file mode is working correctly with Mozilla Firefox:

1. In the Mozilla Firefox browser, type: `https://www.google.com`.
   The URL redirects the browser to forti_isolator for a short period of time. For example, `https://www.google.com/forti_isolator_redir2?ftnturl=https%3a%2f%2fwww.google.com%2f&ftntcid=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 FortiIsolator (for example,

192.168.1.100).



```
GET https://www.google.com/                                    [HTTP/1.0 200 Connection Established 51ms]
  Headers  Cookies  Params  Response  Timings  Stack Trace  Security
  Request URL: https://www.google.com/
  Request method: GET
  Remote address: [redacted]:8888
  Status code: 200 Connection Established
  Version: HTTP/1.0
  Filter headers
  Response headers (115 B)                                                                   Raw headers
    Cache-Control: max-age=0, no-cache, no-store,…te, post-check=0, pre-check=0
    Connection: Keep-Alive
    Content-Encoding: identity
    Content-Length: 310
    Content-Type: text/html
    Expires: 0
GET http://[redacted]:8888/forti_isolator_redir1?ftnturl=https%3a%2f%2fwww.google.com%2f    [HTTP/1.1 302 Found 0ms]
  Headers  Cookies  Params  Response  Timings  Stack Trace
  Request URL: http://[redacted]:8888/forti_isolator_redir1?ftnturl=https%3a%2f%2fwww.google.com%2f
  Request method: GET
  Remote address: [redacted]:8888
  Status code: 302 Found
  Version: HTTP/1.1
```

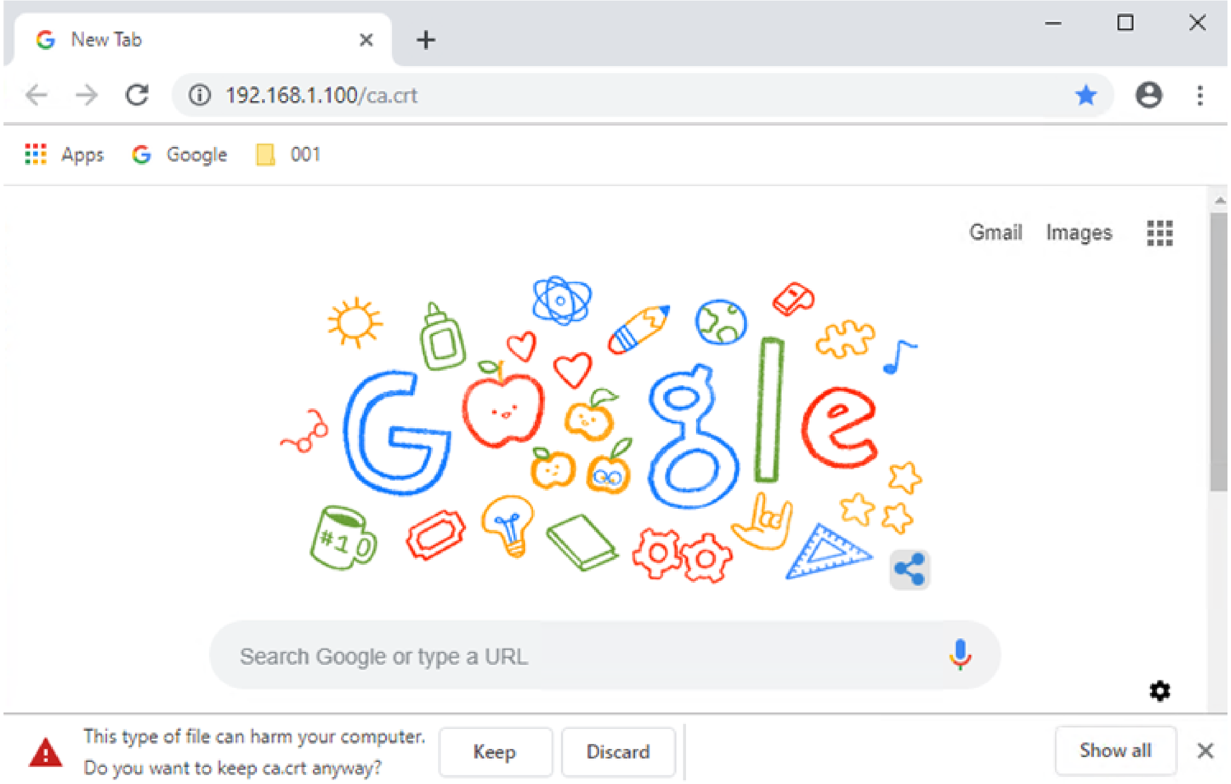
PAC file mode with Google Chrome

Importing the FortiIsolator certificate into the Google Chrome browser

To import the FortiIsolator certificate into the Google Chrome browser:

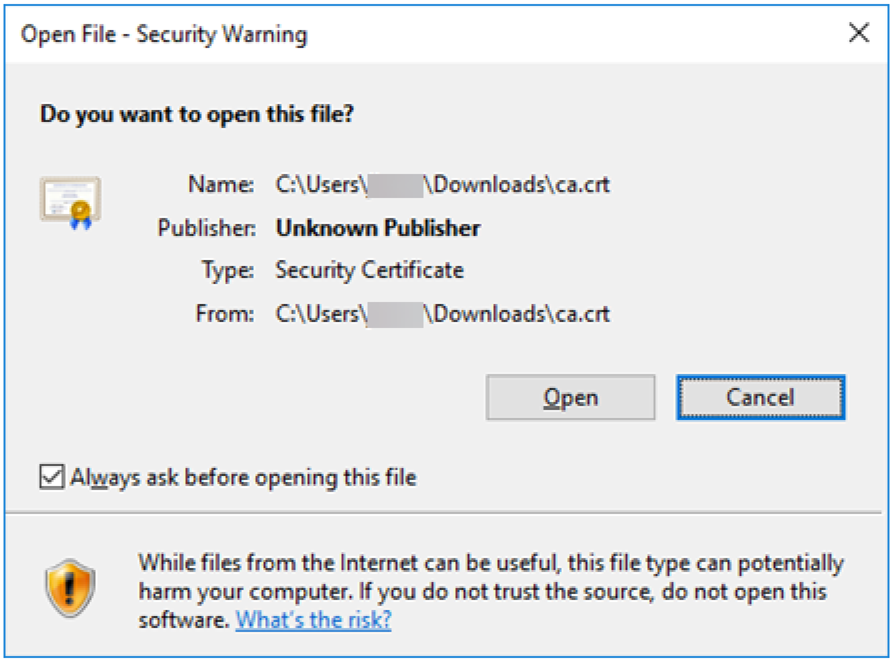
1. Download the FortiIsolator certificate (`ca.crt`) and import it into the Google Chrome browser:
   a. In the Google Chrome browser address bar, type `http://<internal_IP_address>/ca.crt` (for example, `http://192.168.1.100/ca.crt`).
      - where `<internal_IP_address>` value is the IP address of the FortiIsolator internal interface. For example , the IP address of the internal interface that you configured in step 3 of Installing FortiIsolator 1000F on page 11.

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



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

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



Open File - Security Warning

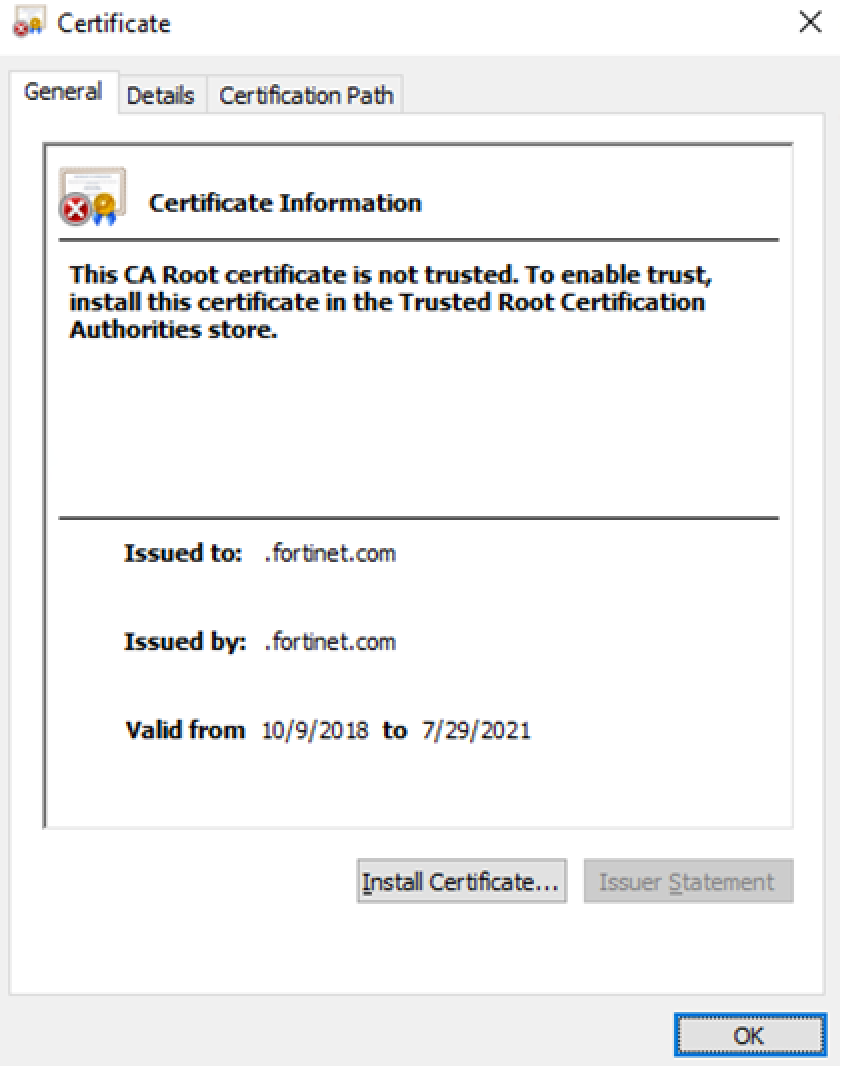
Do you want to open this file?

Name:	C:\Users\[redacted]\Downloads\ca.crt
Publisher:	**Unknown Publisher**
Type:	Security Certificate
From:	C:\Users\[redacted]\Downloads\ca.crt

☑ Always ask before opening this file

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

d. Click *Install Certificate*.



Certificate Information

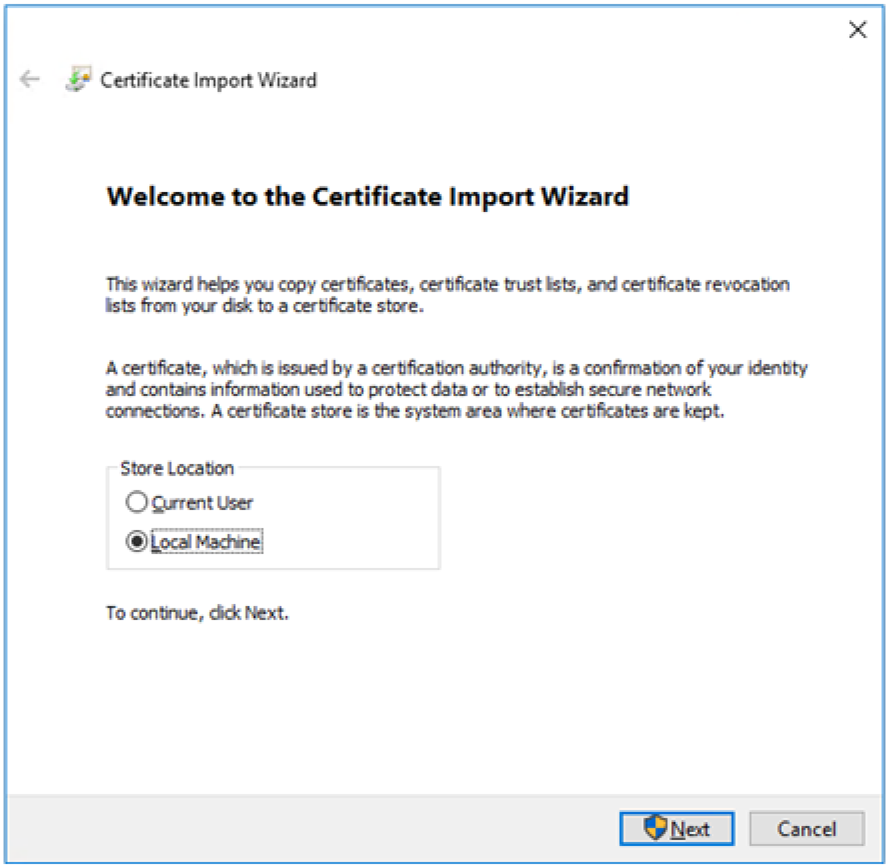
This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

Issued to: .fortinet.com

Issued by: .fortinet.com

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

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



Welcome to the Certificate Import Wizard

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

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

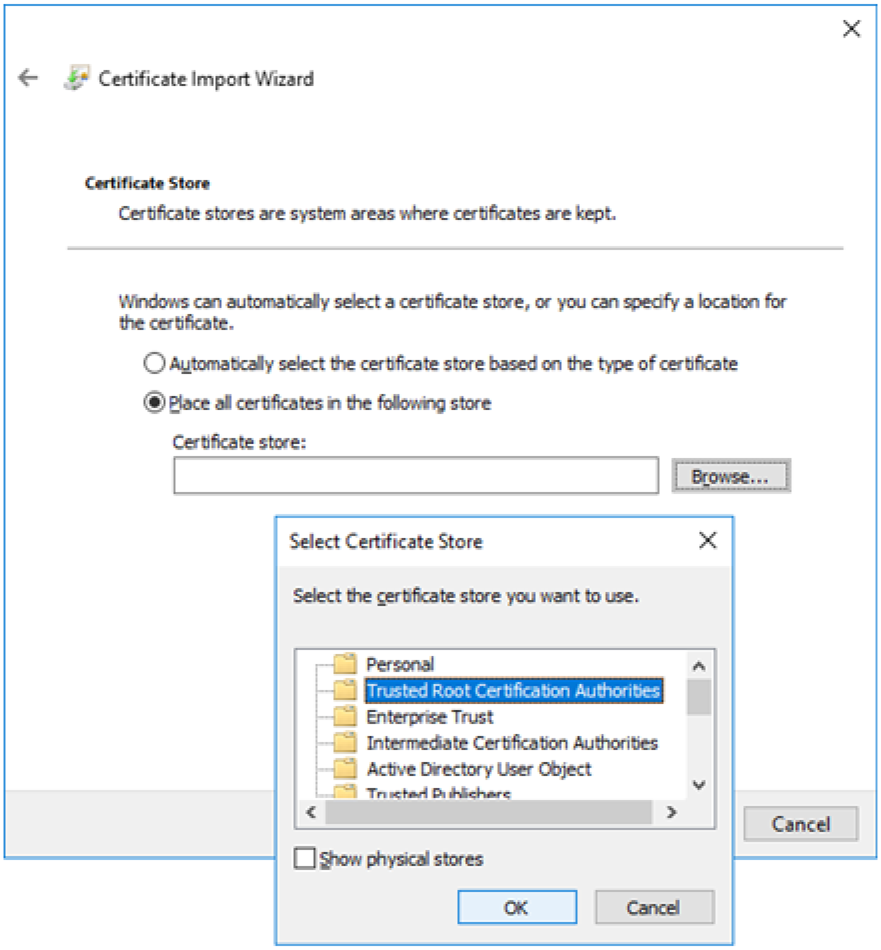
Store Location

○ Current User

● Local Machine

To continue, click Next.

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



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

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

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

● Place all certificates in the following store

Certificate store:

Select Certificate Store

Select the certificate store you want to use.

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

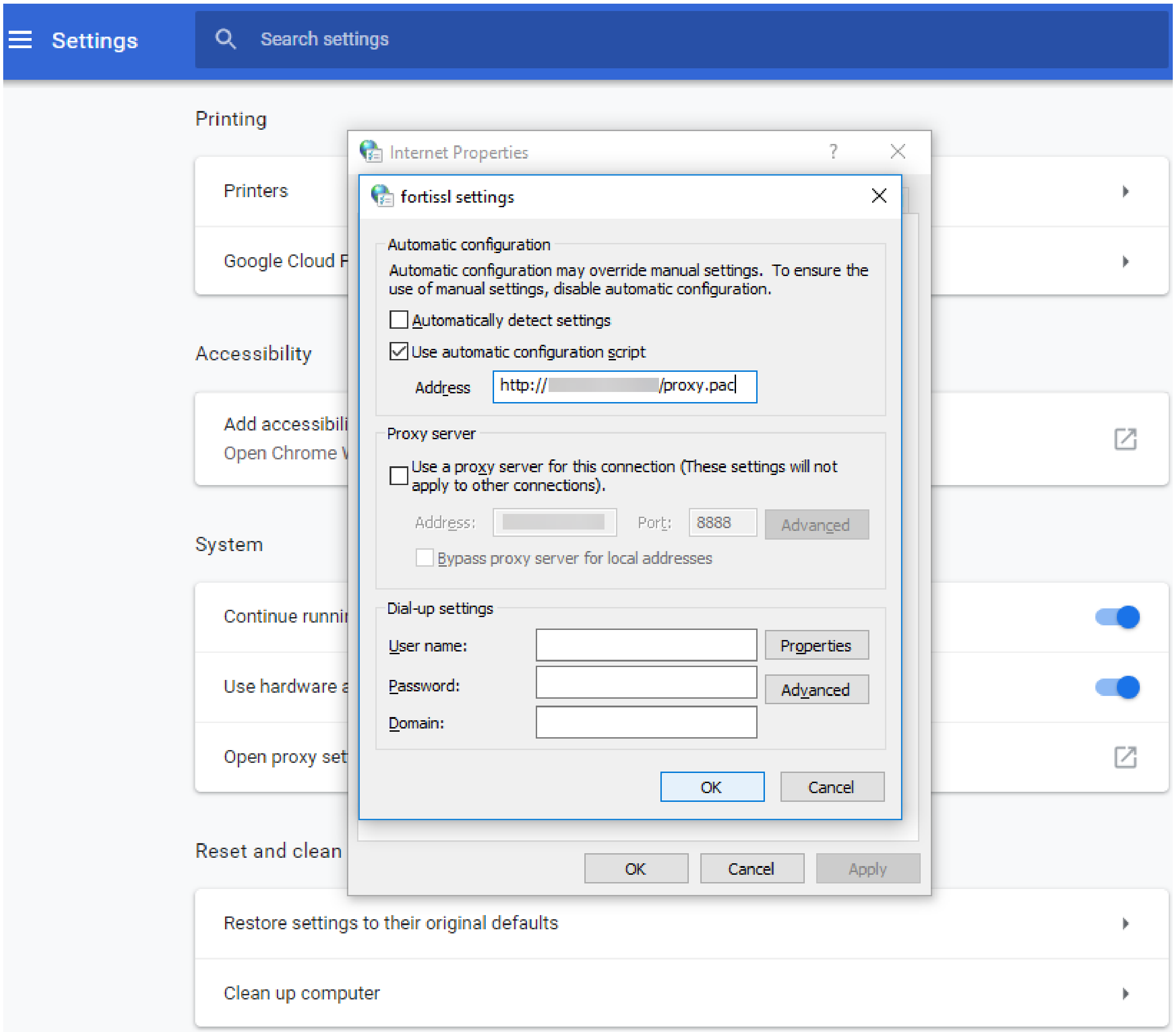
□ Show physical stores

Configuring PAC file mode in Google Chrome

To configure PAC file mode in Google Chrome:

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

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



fortissl settings

Automatic configuration

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

□ Automatically detect settings

☑ Use automatic configuration script

Address: http://[redacted]/proxy.pac

Proxy server

□ Use a proxy server for this connection (These settings will not apply to other connections).

Address: [redacted] Port: 8888 Advanced

□ Bypass proxy server for local addresses

Dial-up settings

User name: Properties

Password: Advanced

Domain:

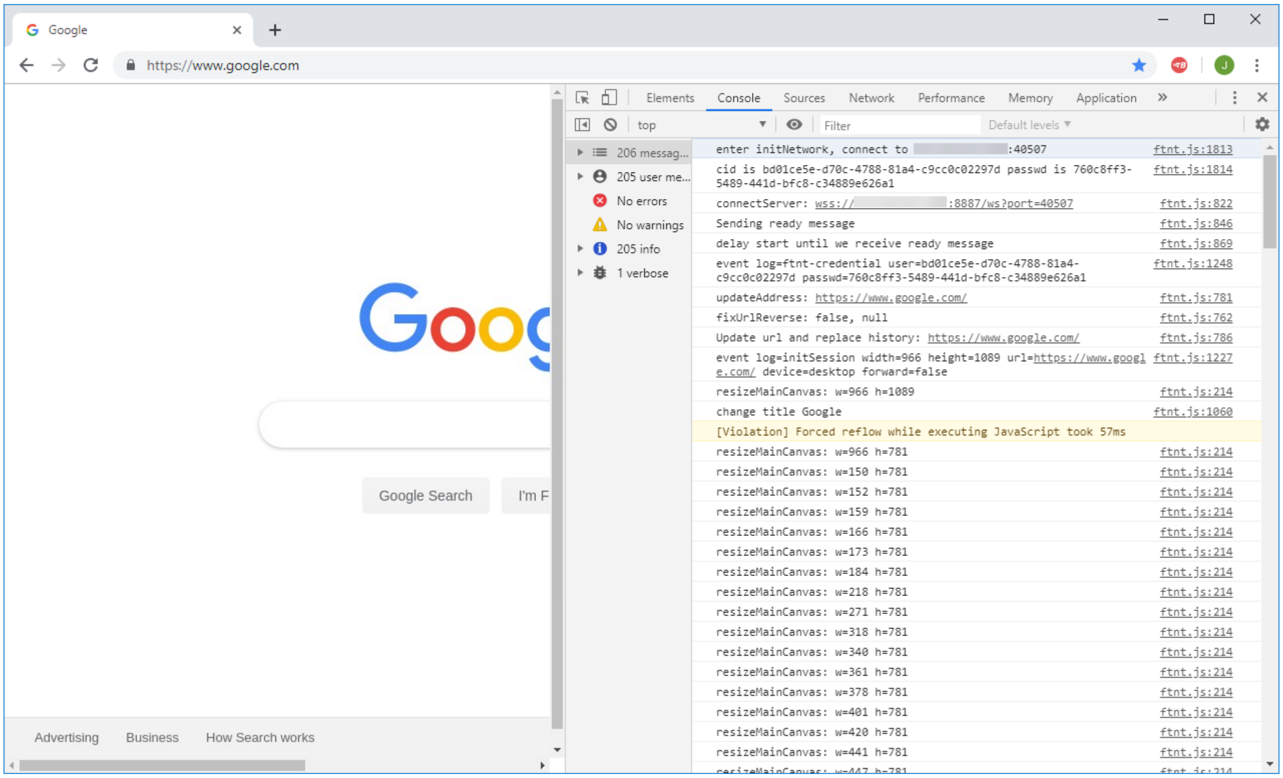
OK Cancel

Verifying FortiIsolator PAC file mode with Google Chrome

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

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

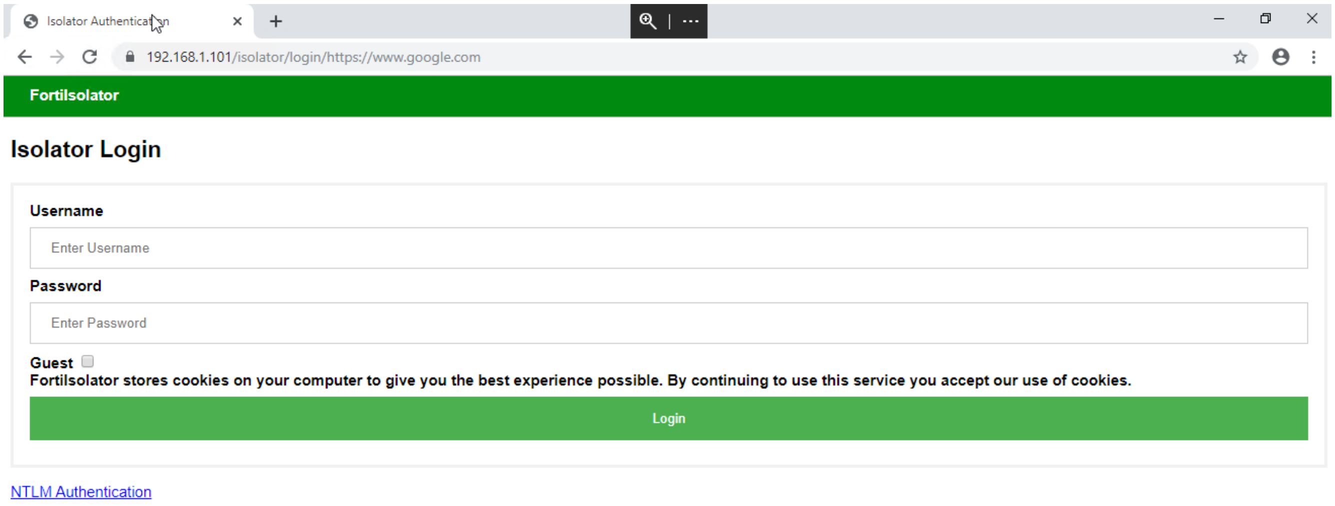
192.168.1.100).



```
enter initNetwork, connect to [redacted]:40507                                ftnt.js:1813
cid is bd01ce5e-d70c-4788-81a4-c9cc0c02297d passwd is 760c8ff3-               ftnt.js:1814
5489-441d-bfc8-c34889e626a1
connectServer: wss://[redacted]:8887/ws?port=40507                            ftnt.js:822
Sending ready message                                                         ftnt.js:846
delay start until we receive ready message                                    ftnt.js:869
event log=ftnt-credential user=bd01ce5e-d70c-4788-81a4-                       ftnt.js:1248
c9cc0c02297d passwd=760c8ff3-5489-441d-bfc8-c34889e626a1
updateAddress: https://www.google.com/                                        ftnt.js:781
fixUrlReverse: false, null                                                    ftnt.js:762
Update url and replace history: https://www.google.com/                       ftnt.js:786
event log=initSession width=966 height=1089 url=https://www.googl             ftnt.js:1227
e.com/ device=desktop forward=false
resizeMainCanvas: w=966 h=1089                                                ftnt.js:214
change title Google                                                           ftnt.js:1060
[Violation] Forced reflow while executing JavaScript took 57ms
resizeMainCanvas: w=966 h=781                                                 ftnt.js:214
resizeMainCanvas: w=150 h=781                                                 ftnt.js:214
resizeMainCanvas: w=152 h=781                                                 ftnt.js:214
resizeMainCanvas: w=159 h=781                                                 ftnt.js:214
resizeMainCanvas: w=166 h=781                                                 ftnt.js:214
resizeMainCanvas: w=173 h=781                                                 ftnt.js:214
resizeMainCanvas: w=184 h=781                                                 ftnt.js:214
resizeMainCanvas: w=218 h=781                                                 ftnt.js:214
resizeMainCanvas: w=271 h=781                                                 ftnt.js:214
resizeMainCanvas: w=318 h=781                                                 ftnt.js:214
resizeMainCanvas: w=340 h=781                                                 ftnt.js:214
resizeMainCanvas: w=361 h=781                                                 ftnt.js:214
resizeMainCanvas: w=378 h=781                                                 ftnt.js:214
resizeMainCanvas: w=401 h=781                                                 ftnt.js:214
resizeMainCanvas: w=420 h=781                                                 ftnt.js:214
resizeMainCanvas: w=441 h=781                                                 ftnt.js:214
resizeMainCanvas: w=447 h=781                                                 ftnt.js:214
```

Logging in as end user

If it is the end user's first time browsing the web through FortiIsolator 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:



Isolator Login

Username

Enter Username

Password

Enter Password

Guest □

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

Login

NTLM Authentication

Login options

End users can log into FortiIsolator 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.

Copying and pasting text

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

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

Copying and pasting images

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

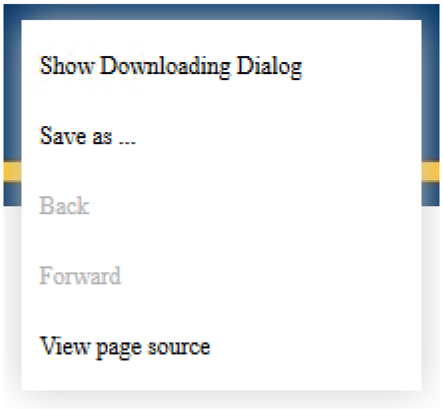
1. In a browser, right-click on the images that you want to save.
2. Click *Copy Image to clipboard*.
3. Open MS Word, MS Excel, or MS Powerpoint
4. Press `Ctrl+V` or right-click to paste the image.

Downloading files

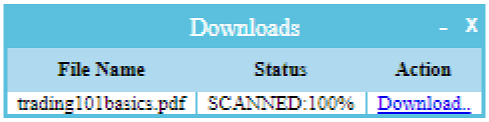
End users are able to download files up to a certain file size while browsing through FortiIsolator if the administrator has configured the Isolator Profile settings to allow it.

To download a file:

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



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



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

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

Adding Web Isolation Profile from FortiProxy to FortiIsolator

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

FortiIsolator setup

To download FortiIsolator CA certificate:

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

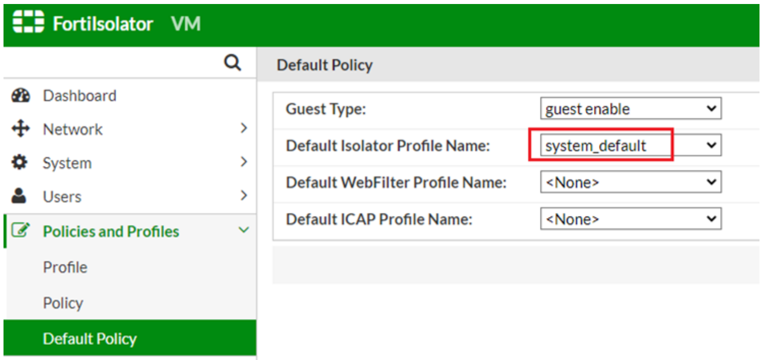
To configure default policy:

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

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

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

Example



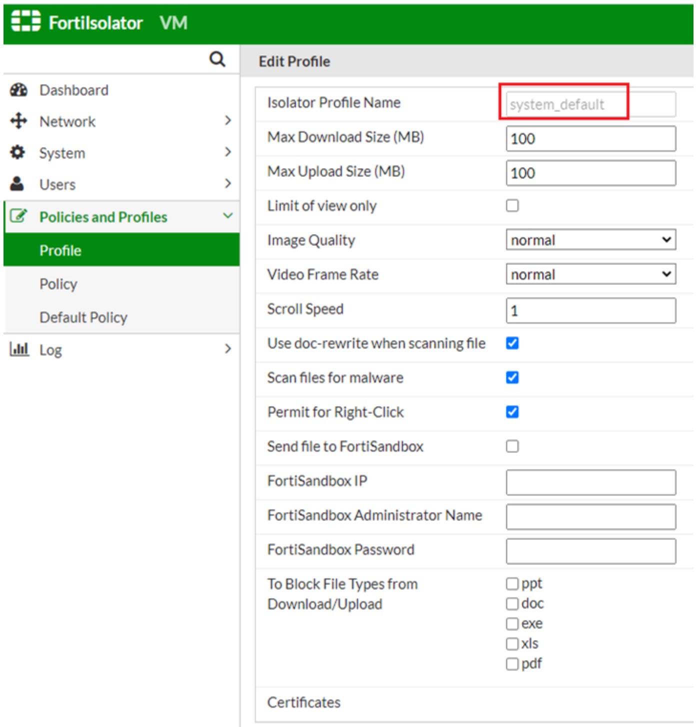
Default Policy

Guest Type: guest enable

Default Isolator Profile Name: system_default

Default WebFilter Profile Name: <None>

Default ICAP Profile Name: <None>



Edit Profile

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

FortiProxy setup

To enable explicit web proxy on FortiProxy:

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

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

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

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

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

j. Leave eveything else as it is.
k. Click *OK*

Doing so ensures that FortiProxy can use SSL Deep Inspection.

2. Create Web Proxy Profile:
   a. Go to *Policy & Objects* > *Web Proxy Profile* > *Create New*.
      Name: FIS-read-only
      Header Client IP: pass
      Header Via Request: pass
      Header Via Response: pass
      Header X Forwarded For: add
      Header Front End Https: pass
      Header X Authenticated User: pass
      Header X Authenticated Groups: pass
      Strip Encoding: Disable
      Log Header Change: Disable
   b. Go to *Header* > *Create New.*
      ID: 1
      Name: fis-isolator-profile
      Action: add-to-request
      Header Content: system_default
      Base64 Encoding: Disable
      Add Option: new
      Protocol: HTTP HTTPS
3. Create SSL/SSH Inspection Profile:
   a. Go to *Security Profiles* > *SSL/SSH Inspection* > *Create New*.
      Name: **deep_inspection2**
      CA Certificate: **FIS_CA_Cert**
      Leave everything else as is.
   b. Click *OK*.

Create Isolator Server

1. Go to *Policy & Objects* > *Isolator Server* > *Create New*.
   Name: FIS
   Comments: FortiIsolator
   Address Type: IP
   IP: 192.168.1.18
   Port: 8888
2. Click *OK*.

Create Explicit Web Proxy Policy

To create a policy to isolate Unrated/Malicious websites:

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

Utilities and diagnostics

Utilities

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

Diagnostic tools

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

www.fortinet.com