Browser Isolation

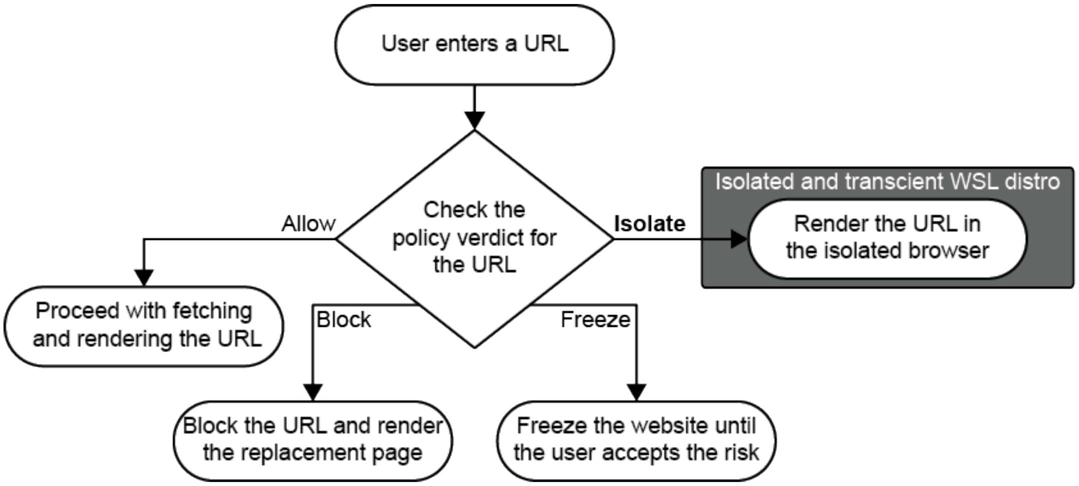
FortiProxy Client-based *Native Browser Isolation* (NBI) uses a Windows Subsystem for Linux (WSL) distribution (distro) to isolate the browser from the rest of the computer. As browsers are one of the biggest windows to external networks, they are one of the biggest attack vectors. Isolating or sandboxing the browser in a container helps decrease the attack surface.

The FortiNBI does not support isolation with IPv6 due to WSL limitation.

The endpoint must use FortiProxy as an HTTP proxy. The FortiNBI installer installs the Chrome browser extension, a WSL distro with a preloaded Chrome browser, a Windows Service to communicate with the FortiProxy that is providing the ratings, and a per-user application to launch the isolated browser and manage the system.

While FortiNBI allows multiple users on a machine, concurrent users are not supported. All users on a machine must have the same proxy settings for the FortiNBI to work properly. Make sure that the organizational security rule does not require distinct proxies for different users on the same machine.

The browser extension monitors each browser tab, and reports every new tab invocation to FortiProxy over the communication channel that it maintains, with FortiProxy acting as a secure web gateway.


User enters a URL
Check the policy verdict for the URL
Allow
Isolate
Block
Freeze
Isolated and transcient WSL distro
Render the URL in the isolated browser
Proceed with fetching and rendering the URL
Block the URL and render the replacement page
Freeze the website until the user accepts the risk

FortiProxy receives the web browsing information, applies the relevant explicit or transparent policy to it, generates a verdict, and then sends that verdict to the extension on the endpoint.

The browser extension acts based on the verdict: *Allow*, *Block*, *Freeze*, or *Isolate*. If the verdict is to isolate, the containerized browser opens in a new window and loads the URL. The user can then access the web through the isolated browser. When the user closes the browser, the WSL distro instance is closed, removing all of the web artifacts that were generated while browsing.

This guide covers the following topics about Browser Isolation:

- Licensing on page 3
- Deploying the Browser Isolation on page 4
- Using the FortiNBI application on page 12

Licensing

The FortiNBI license controls how many services are allowed to connect to the FortiProxy. Each seat allows one service to connect. When the license is full, no more services can connect to FortiProxy and traffic from unconnected services is bypass ed with no FortiNBI security checks. If the FortiProxy cannot connect to FortiGuard (such as when it is not licensed) then the default FortiNBI seat count is 10 for VM devices and 100 for hardware devices.

FortiNBI licenses support license sharing for HA and security fabric. In HA mode, seats from different FortiProxy devices are added together to act as a single FortiProxy. In a security fabric, seats from the root FortiProxy and downstream FortiProxy devices are merged into a pool and dynamically allocated to the FortiProxy devices.

The FortiGuard license contract name for FortiNBI is *PXCB* (FortiProxy client browser isolation).

To view the license status on the FortiProxy:

```
# get system fortiguard
...
fnbi-license         : Contract, no sharing, seat: 100
fnbi-expiration      : Sun Sep 10 2023
...
```

Deploying the Browser Isolation

The deployment of the Browser Isolation includes the following steps:

1. Prerequisites on page 4
2. Configuring native browser isolation in FortiProxy on page 4
3. Uploading the FortiNBI isolator image on page 9
4. Installing the FortiNBI application on page 9

Prerequisites

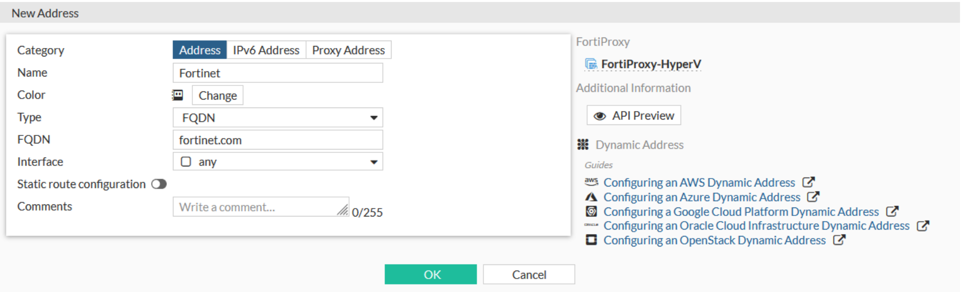
Before you deploy the Native Browser Isolation (NBI), perform the following preparation tasks:

1. Make sure the deployment machine runs Microsoft Windows 10 (build 20H1 19041 or later) with Google Chrome installed. You can also deploy the Native Browser Isolation on VMware with a minimum of 4 GB RAM and 2 CPUs (with *Hardware virtualization* enabled). Refer to the FortiProxy VMware vSphere Deployment Guide for more information.
2. Contact the customer support or sales team to request the FortiNBI isolator image by referencing ticket ID 876947. You will need to upload the image during the Browser Isolation deployment.
3. Install FortiProxy 7.2, which is required in order to install the FortiNBI application for browser isolation. For more information about installing FortiProxy, refer to the FortiProxy Release Notes.

Configuring native browser isolation in FortiProxy

To configure native browser isolation in the FortiProxy GUI:

1. Configure an HTTP portal for the client to download the isolator image:
   a. Go to *Policy & Objects* > *Addresses* and click *Create New* > *Address*.
   b. Enter a name for the address.
   c. Set *Type* to *FQDN*.
   d. Enter the *FQDN*.



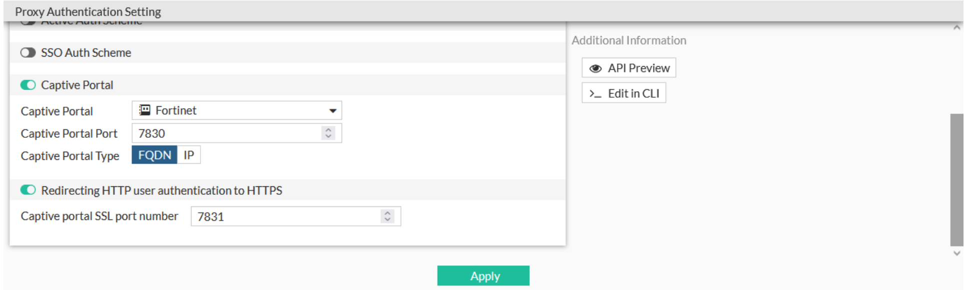
New Address

Category	Address
Name	Fortinet
Color	Change
Type	FQDN
FQDN	fortinet.com
Interface	☐ any
Static route configuration	○
Comments	Write a comment... 0/255

IPv6 Address
Proxy Address
FortiProxy
FortiProxy-HyperV
Additional Information
API Preview
Dynamic Address
Guides
Configuring an AWS Dynamic Address
Configuring an Azure Dynamic Address
Configuring a Google Cloud Platform Dynamic Address
Configuring an Oracle Cloud Infrastructure Dynamic Address
Configuring an OpenStack Dynamic Address
OK
Cancel

   e. Click *OK*.

2. Enable Captive Portal:
   a. Go to *Policy & Objects > Proxy Auth Setting*.
   b. Enable *Captive Portal* and select the just create address.
   c. Set the *Captive Portal Port*.
   d. Set *Captive Portal Type* to *FQDN*.



Proxy Authentication Setting

SSO Auth Scheme

Captive Portal

Captive Portal: Fortinet

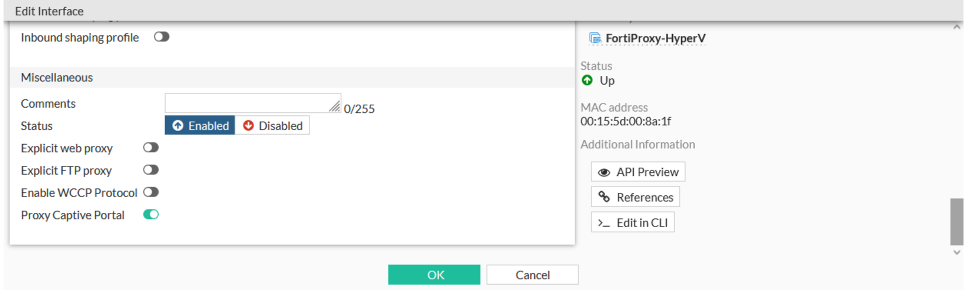
Captive Portal Port: 7830

Captive Portal Type: FQDN | IP

Redirecting HTTP user authentication to HTTPS

Captive portal SSL port number: 7831

   e. Click *Apply*.
3. Enable captive portal on the interface:
   a. Go to *Network > Interfaces* and edit the interface.
   b. Enable *Proxy Captive Portal*.



Edit Interface

Inbound shaping profile

Miscellaneous

Comments: 0/255

Status: Enabled | Disabled

Explicit web proxy

Explicit FTP proxy

Enable WCCP Protocol

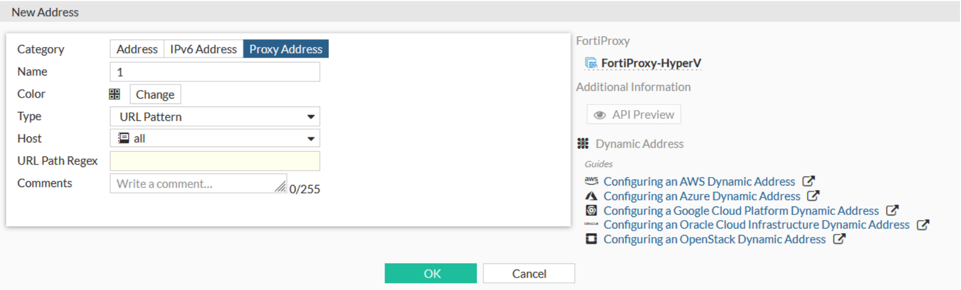
Proxy Captive Portal

FortiProxy-HyperV

Status: Up

MAC address: 00:15:5d:00:8a:1f

   c. Click *OK*.
4. Configure a firewall proxy address:
   a. Go to *Policy & Objects > Addresses* and click *Create New > Address*.
   b. Set *Category* to *Proxy Address*.
   c. Enter a name for the address, such as *1*.
   d. Set *Host* to *all* and enter the *URL Path Regex*.



New Address

Category: Address | IPv6 Address | Proxy Address

Name: 1

Color: Change

Type: URL Pattern

Host: all

URL Path Regex:

Comments: Write a comment... 0/255

FortiProxy

FortiProxy-HyperV

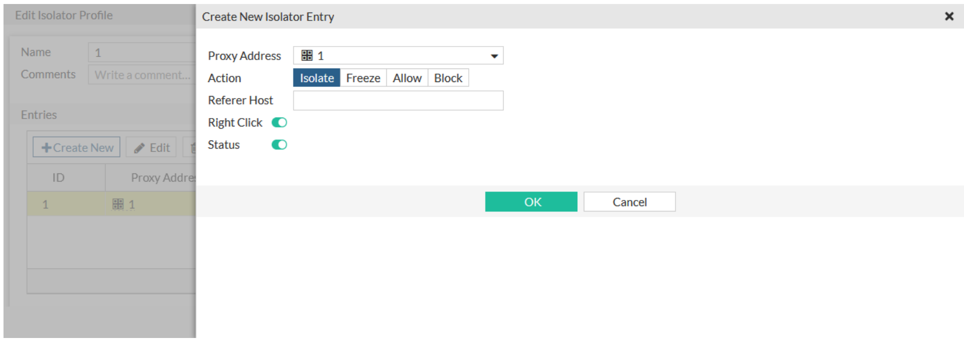
Additional Information
API Preview
Dynamic Address
Guides
Configuring an AWS Dynamic Address
Configuring an Azure Dynamic Address
Configuring a Google Cloud Platform Dynamic Address
Configuring an Oracle Cloud Infrastructure Dynamic Address
Configuring an OpenStack Dynamic Address
OK
Cancel

   e. Click *OK*.
5. Configure an isolator profile that uses the proxy address:
   a. Go to *Security Profiles > Isolator Profile* and click *Create New*.
   b. Enter a name for the profile.

c. In the *Entries* table, click *Create New*.

d. Select the *Proxy Address*.

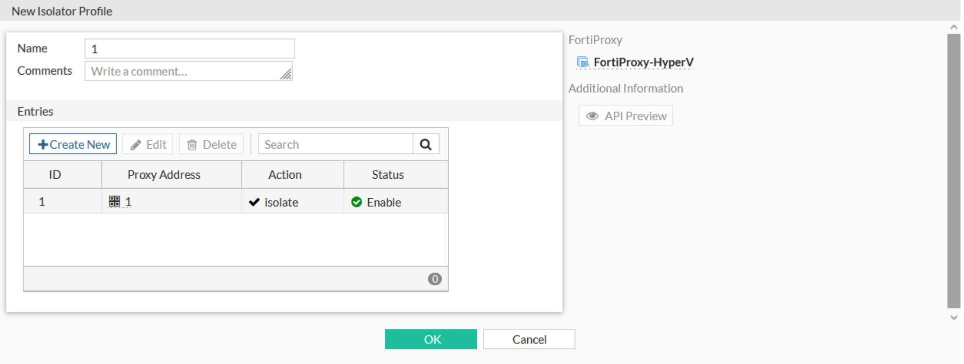
e. Set *Action* to *Isolate*.



Name: 1
Comments: Write a comment...
1 | 1

Proxy Address: 1
Action: Isolate
Referer Host:
Right Click: on
Status: on

f. Click *OK*.



Name: 1
Comments: Write a comment...

ID	Proxy Address	Action	Status
1	1	✓ isolate	✓ Enable

g. Click *OK*.

6. Configure an SSL/SSH profile with full ssl inspection:

a. Go to *SSL/SSH Inspection* and click *Create New*.

b. Enter a name for the profile, such as *test*.

c. In *Enable SSL inspection of*, select *Multiple Clients Connecting to Multiple Servers*.

d. In *Inspection method*, select *Full SSL Inspection*.

e. In *CA Certificate*, select a CA certificate from the drop-down menu.

Later you will need to install the certificate in the browser of each machine that uses Native Browser Isolation to avoid certificate warnings.

f. Configure the other settings as required, then click *OK*.

See the FortiProxy Administration Guide for more information about the configuration options.

7. Configure a firewall policy that uses the isolator and SSL/SSH profiles:

a. Go to *Policy & Objects* > *Policy* and click *Create New*.

b. Configure the following:

Type	Explicit
Explicit Web Proxy	web-proxy
Outgoing Intergave	any
Source	all

Destination	all
Schedule	always
Service	webproxy
Action	Accept
SSL/SSH Inspection	test
Isolator	1
Comments	isolator traffic inspect

c. Click *OK*.

To configure native browser isolation in the CLI:

1. Configure an HTTP portal for the client to download the FortiNBI isolator image:

```
config firewall address
    edit "Fortinet"
        set type fqdn
        set fqdn "fortinet.com"
    next
end
```

2. In the authentication settings, set the captive portal name:

```
config authentication setting
    set captive-portal "Fortinet"
end
```

3. Enable captive portal on the interface:

```
config system interface
    edit <interface>
        set proxy-captive-portal enable
    next
end
```

4. Configure a firewall proxy address:

```
config firewall proxy-address
    edit "1"
        set host "all"
    next
end
```

5. Configure an isolator profile that uses the proxy address:

```
config isolator profile
    edit "1"
        config entries
            edit 1
                set proxy-address "1"
                set action isolate
                set status enable
            next
        end
    next
end
```

`proxy-address <proxy-address>`	Choose the proxy-address for this isolator profile entry.
`action {block | allow | freeze | isolate}`	Choose the action for this isolator entry: • `isolate`: Open the website in an isolated browser (default). • `freeze`: Freeze the website. The user is able to unfreeze and get access to the website when they accept the risk. • `block`: Block the traffic to the website. • `allow`: Bypass the traffic to the website.
`status {enable | disable}`	Enable/disable this isolator entry (default = enable).

6. Configure an SSL/SSH profile with full SSL inspection:

```
config firewall ssl-ssh-profile
    edit "test"
        config https
            set ports 443
            set status deep-inspection
        end
        config ftps
            set ports 990
            set status deep-inspection
        end
        config imaps
            set ports 993
            set status deep-inspection
        end
        config pop3s
            set ports 995
            set status deep-inspection
        end
        config smtps
            set ports 465
            set status deep-inspection
        end
        config ssh
            set ports 22
            set status disable
        end
        config dot
            set status disable
        end
    next
end
```

7. Configure a firewall policy that uses the isolator and SSL/SSH profiles:

```
config firewall policy
    edit 2
        set type explicit-web
        set dstintf "any"
        set srcaddr "all"
```

```
            set dstaddr "all"
            set action accept
            set schedule "always"
            set service "webproxy"
            set explicit-web-proxy "web-proxy"
            set utm-status enable
            set comments "isolator traffic inspect"
            set ssl-ssh-profile "test"
            set isolator-profile "1"
        next
    end
```

Uploading the FortiNBI isolator image

After Configuring native browser isolation in FortiProxy on page 4, you must manually upload the FortiNBI isolator image by running the following command in FortiProxy:

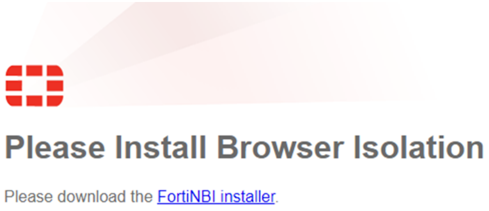
```
# execute upload isolator-image tftp <file_name> <tftp_server>
```

To request the FortiNBI isolator image, contact the customer support or sales team by referencing ticket ID 876947.

When the upload process is complete, restart FortiProxy to apply the changes. FortiProxy then automatically distributes the image to the endpoints via the FortiNBI system, which is a prerequisite for FortiProxy to prompt the user to download the FortiNBI installer when the user attempts to access a website that FortiProxy is configured to isolate. See Installing the FortiNBI application on page 9.

Installing the FortiNBI application

When a FortiProxy user with a matching policy that has the isolator profile attempts to access a website on a machine without the FortiNBI service running, the user will see the following prompt page with a download link to the FortiNBI installer.



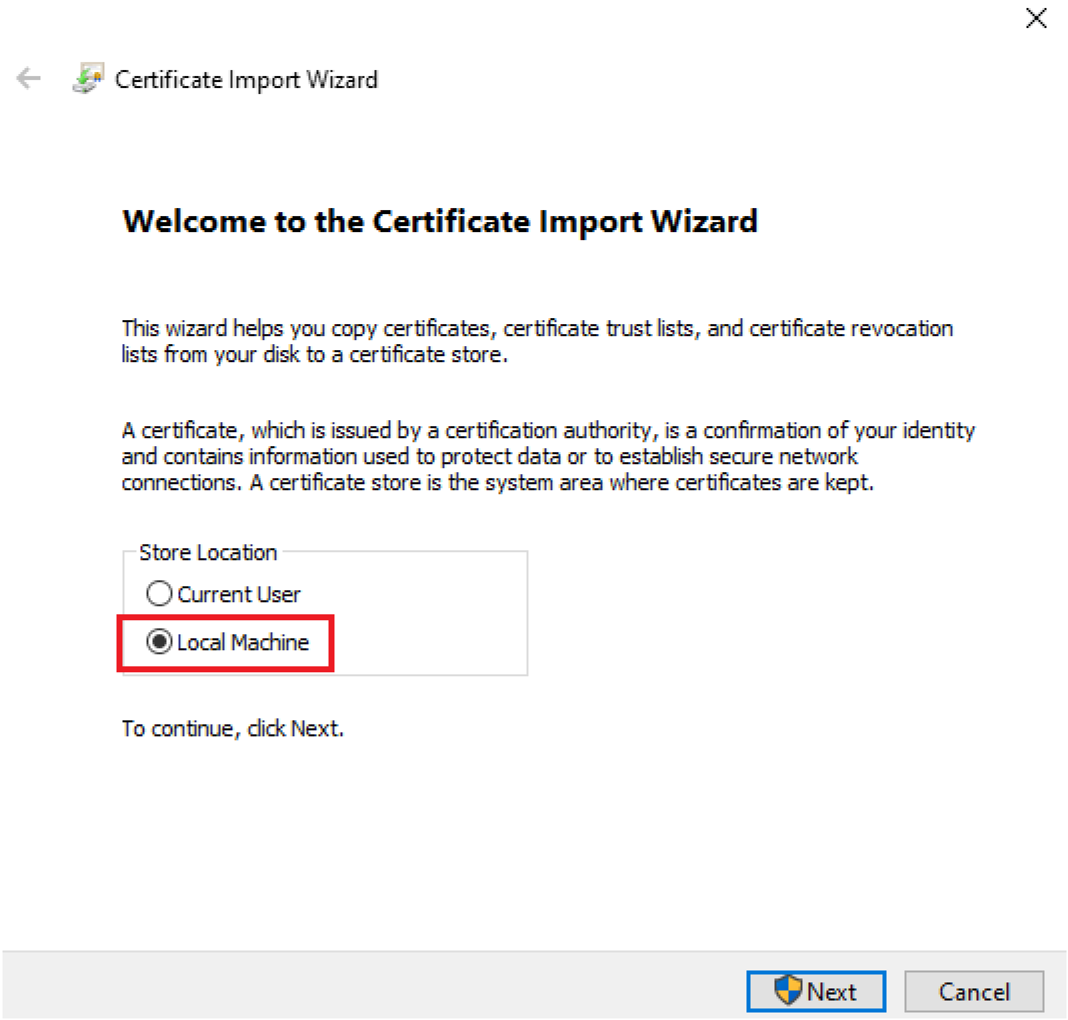
Please Install Browser Isolation

Please download the FortiNBI installer.

To install the FortiNBI application:

1. Click the *FortiNBI installer* link on the browser isolation replacement page to download the installer.
2. Run the installer with an administrator account:

   a. Files are unpacked to the installation folder, by default *C:\Program Files (x86)\Fortinet\FortiNBI*.
   b. The FortiNBI GUI is registered as a task that runs automatically every time that a user logs on.
3. FortiNBI starts automatically, followed by isolator and extension installations:
   a. FortiNBI checks if the system has Windows Subsystem for Linux (WSL) and Virtual Machine Platform enabled. If not, the installer will automatically enable and configure it.
   b. The isolator image is downloaded from the FortiProxy's HTTP portal, extracted to a temporary folder, imported to the system, and then the temporary files are removed.
   c. After the installation procedure finishes, restart the browser (if the browser is already open) for the FNBI extension to be installed. Reboot Windows when requested.
4. When required, the client will receive an RDP pop-up window for isolation.
5. To avoid certificate warnings, install the FortiProxy CA certificate in the browser on the machine with the ***Local Machine*** option selected.



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.

You can download the CA certificate in the following ways:

- In the FortiProxy GUI, download the CA certificate from the Certificate list page under *System* > *Certificates*.
- In the FortiProxy CLI, run the following command to download the CA certificate:

```
exe vpn certificate <store> export tftp <CA name> <export format> <filename in
tftp server> <tftp server address>
```

where `store` is `local` for default CA certificate.

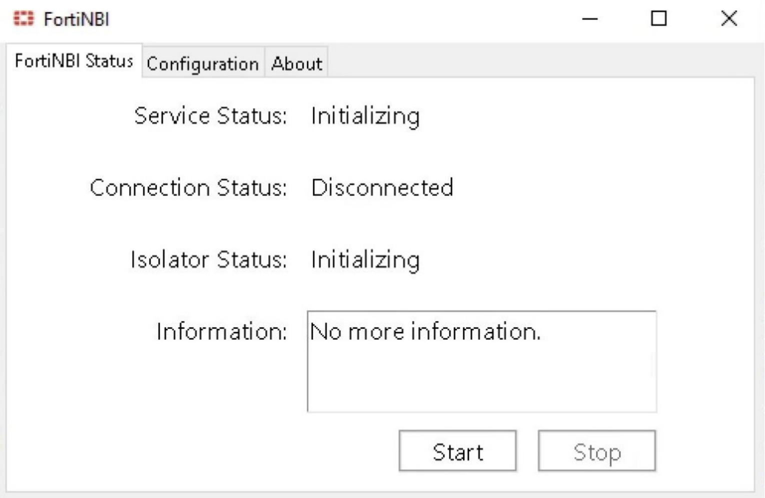
For example, `exe vpn certificate local export tftp FTNT_CA_SSL cer FTNT_CA 0.0.0.0`

Using the FortiNBI application

The FortiNBI application allows users to monitor isolation status and change the FortiProxy IP address that the application is connected to when needed.

FortiNBI Status tab

The *FortiNBI Status* tab shows the statuses of several components.



Service Status: Initializing

Connection Status: Disconnected

Isolator Status: Initializing

Information: No more information.

Service Status	Status of the FortiNBI service.
Connection Status	Status of the connection between the GUI and the FortiNBI service.
Isolator Status	Status of the isolator.
Information	The output of pressing the *Start* or *Stop* button, which starts or stops the FortiNBI service.
Start/Stop	Start or stop the background FortiNBI service.

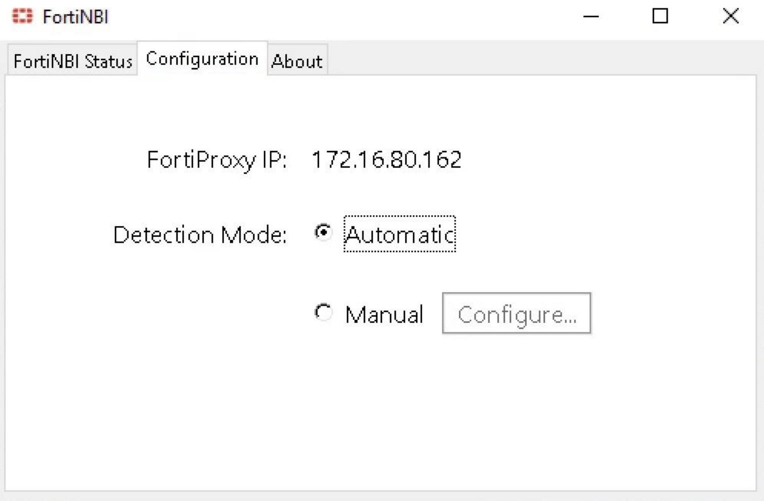
Configuration tab

The *Configuration* tab displays the FortiProxy IP address that FortiNBI is connected to. Configure *Detection Mode* with one of the following options:

- *Automatic*: The FortiProxy IP address is resolved using the user's proxy settings.
- *Manual*: Manually configure the FortiProxy IP address by clicking *Configure* and entering the FortiProxy IP address. The client machine must have a proxy configured, which must match the IP address you configured in the

FortiProxy.

Fortinet recommends that you use *Automatic* mode as much as you can. Use *Manual* mode only if an issue with automatic mode prevents the system from detecting the FortiProxy IP address.



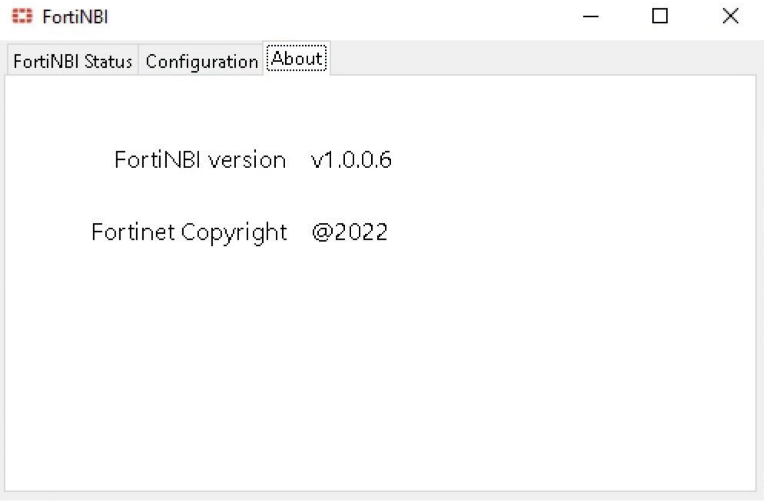
FortiProxy IP: 172.16.80.162

Detection Mode: ● Automatic

○ Manual

About tab

The *About* tab shows the version of FortiNBI that is installed.



FortiNBI version v1.0.0.6

Fortinet Copyright @2022

To quit the FortiNBI application:

In the system tray, right-click the Fortinet icon and click *Quit* to stop the FortiNBI application and the isolator. To stop the background FortiNBI service, click the *Stop* button in the *FortiNBI Status* tab.

To restart the FortiNBI application:

Run the executable file *FortiNBILauncher.exe* in the installation directory.

Change log

Date	Change Description
2022-09-16	Initial release.
2023-04-04	Updated Browser Isolation on page 1.
2023-06-06	- Added the following topics: - Deploying the Browser Isolation on page 4 - Prerequisites on page 4 - Uploading the FortiNBI isolator image on page 9 - Updated the following topics: - Browser Isolation on page 1 - Configuring native browser isolation in FortiProxy on page 4 - Installing the FortiNBI application on page 9 - Using the FortiNBI application on page 12
2023-06-07	Updated Installing the FortiNBI application on page 9.
2023-08-30	Updated Browser Isolation on page 1.
2023-10-06	Updated some links.
2024-01-03	Updated Prerequisites on page 4.
2023-02-09	Updated Licensing on page 3.