Browser Isolation

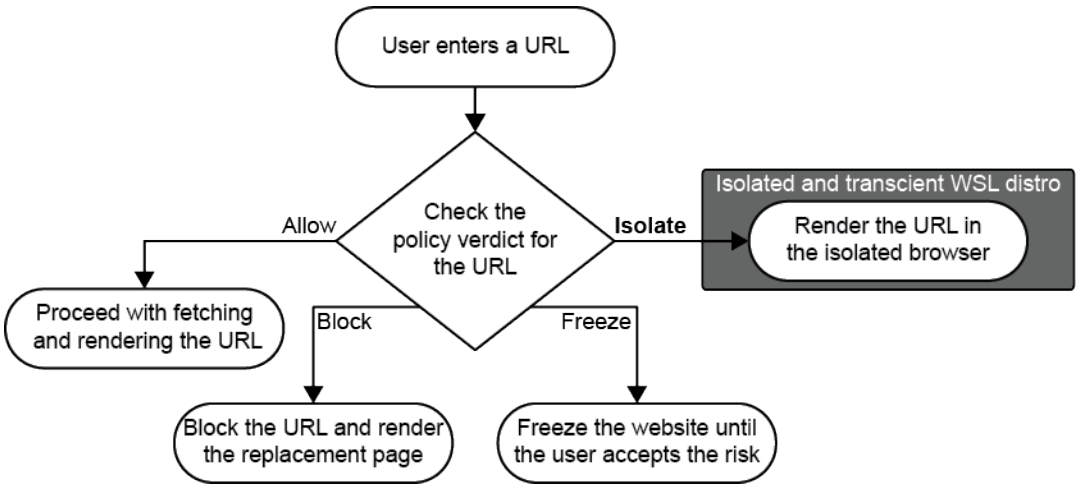
FortiProxy Client-based *Native Browser Isolation* (NBI) uses a Windows Subsystem for Linux (WSL) distribution (distro) to isolate the browser from the rest of the computer. As browsers are one of the biggest windows to external networks, they are one of the biggest attack vectors. Isolating or sandboxing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

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

The FortiNBI installer installs the 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.



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

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. Installing certificates on page 4
3. Configuring native browser isolation in FortiProxy on page 6
4. Uploading the FortiNBI installer and isolator image on page 11
5. Installing the FortiNBI application on page 12

Prerequisites

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

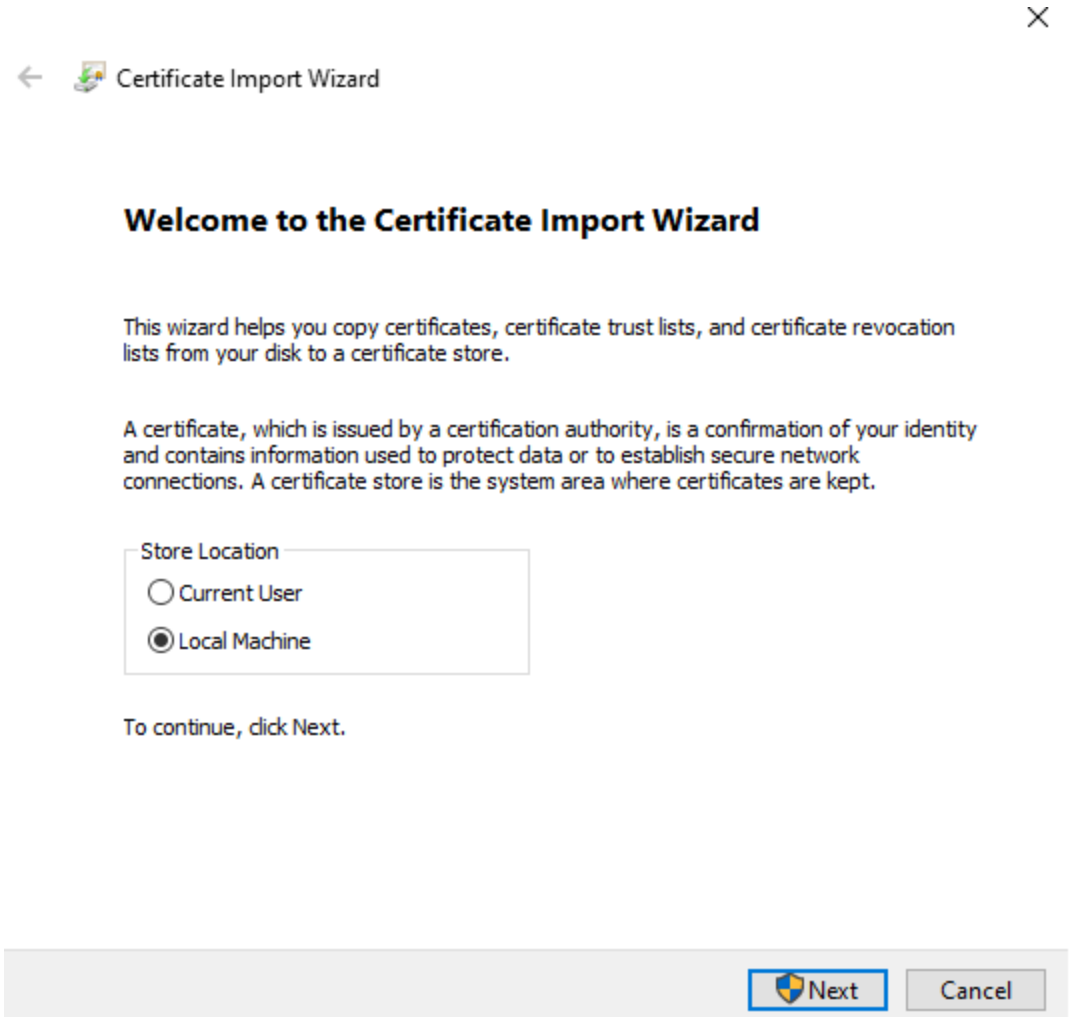
1. **System requirements**
   - Microsoft Windows 10 (build 20H1 19041 or later) or Windows 11 with one of the following browsers installed:
     - Google Chrome
     - Mozilla Firefox
     - Microsoft Edge
   - VMware with the following requirements:
     - 8 GB RAM
     - 2 CPUs (with *Hardware virtualization* enabled)

   Refer to the FortiProxy VMware vSphere Deployment Guide for more information.
2. Install FortiProxy 7.2.11 or later, 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.

Installing certificates

To deploy the FortiNBI, you must first install the following certificates, which can be downloaded from Certificate list under *System* > *Certificates* in the FortiProxy GUI:

- **FortiProxy CA certificate** (`Fortinet_CA_SSL`)—This certificate is required for connection between the FNBI client system and the FortiProxy. Install the certificate in the browser on the local machine trusted root CA stores by selecting the *Local Machine* option.

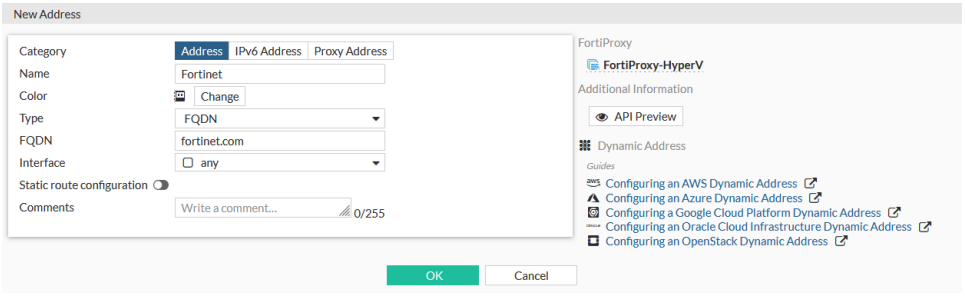


- **FortiProxy server certificate**—This certificate is defined in *Proxy Settings* > *Web Proxy Setting* > *Default Server Certificate* and is required for downloading the isolator image. You must configure the web proxy to use a custom certificate that you create which is signed by `Fortinet_CA_SSL`:
  a. Go to *System* > *Certificates* and click *Create/Import* > *Certificate*.
  b. Click *Generate Certificate*.
  c. Specify the certificate name.
  d. Specify the FQDN of the configured captive portal in the *Common name* field or specify the IP of the configured captive portal in the *Subject alternative name* field. Failing to do so will result in certificate errors on the client machine. You can access captive portal information in *Policy & Objects* > *Proxy Auth Setting*.
  e. Click *Create*.
  f. Go to *Proxy Settings* > *Web Proxy Setting* and select the certificate you just created under *Default Server Certificate*.
  g. After the certificate is installed, verify the trust on the client machine by downloading the isolator module manually using the following URL:
  `https://<captive_portal_domain>:<captive _portal_https_port>/XX/YY/ZZ/wsl_installer`

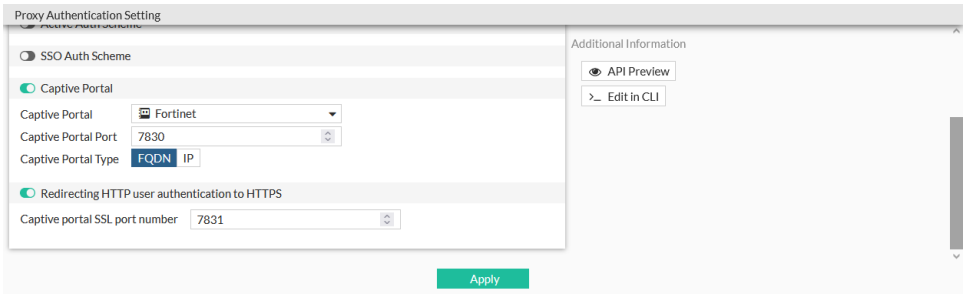
Configuring native browser isolation in FortiProxy

To configure native browser isolation in the FortiProxy GUI:

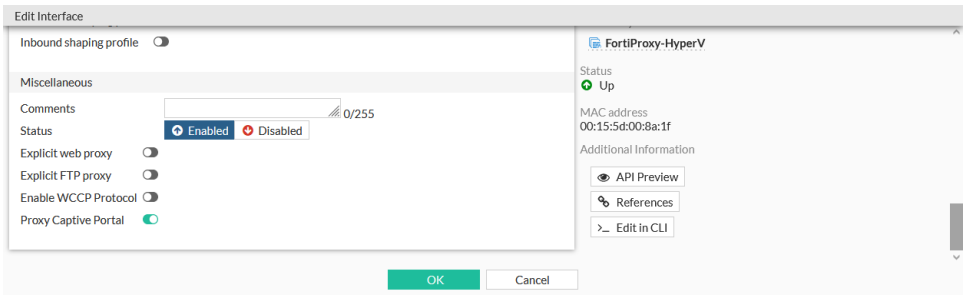
1. Configure an HTTP portal for the client to download the isolator image:
   a. Go to *Policy & Objects* > *Addresses* and click *Create New* > *Address*.
   b. Enter a name for the address.
   c. Set *Type* to *FQDN*.
   d. Enter the *FQDN*.



   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*.

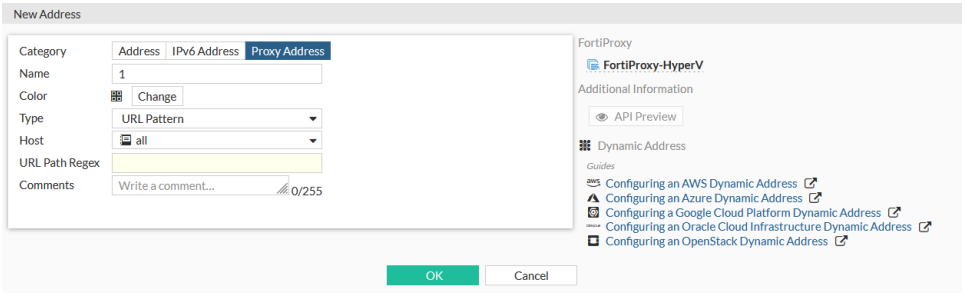


   e. Click *Apply*.
3. Enable captive portal on the interface:
   a. Go to *Network* > *Interfaces* and edit the interface.
   b. Enable *Proxy Captive Portal*.



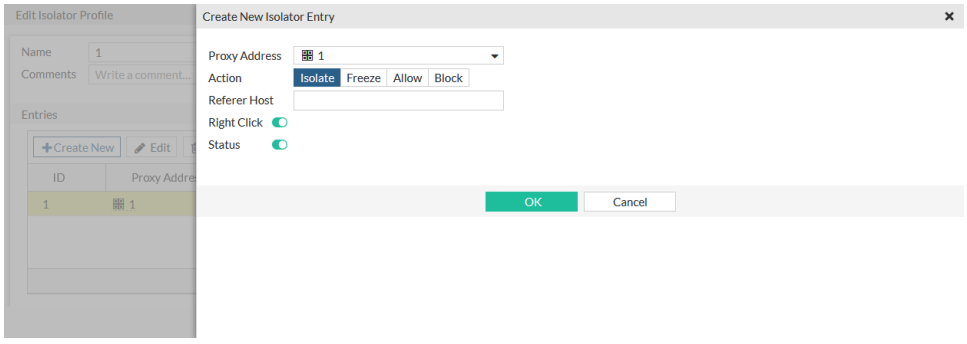
c. Click *OK*.

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*.

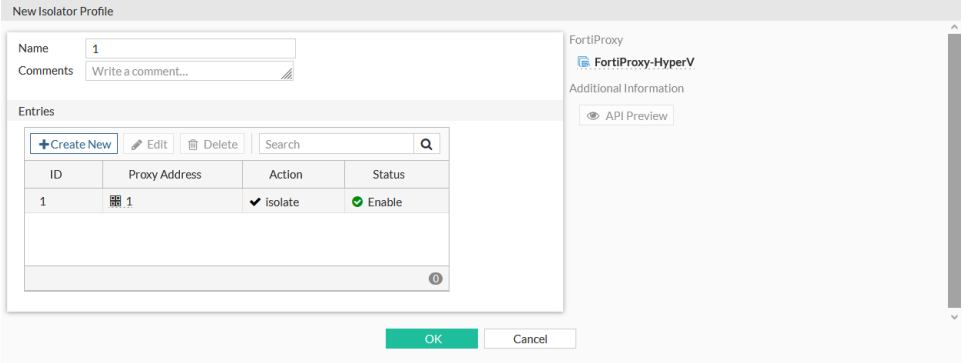


   e. Click *OK*.

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*.



   f. Click *OK*.



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 the default isolator profile to use and action to perform on sessions with missing information (defective session) or do not match any existing policies (unmatched session):

```
config isolator setting
   set default-isolator-profile {string}
   set defective-session [use-default-profile|pass|...]
   set unmatched-session [use-default-profile|pass|...]
end
```

`default-isolator-profile`	Choose the name of an isolator profile that will be used when no policy is matched.
`defective-session`	Choose the action to perform on rating requests for sessions with missing information: • `use-default-profile`: Use default isolator profile to handle the session. • `pass`: Return bypass response to the rating request of the session (default). • `block`: Return block response to the rating request of the session.
`unmatched-session`	Choose the action to perform on rating requests for sessions that do not match any policy: • `use-default-profile`: Use default isolator profile to handle the session. If the session does not match the default profile still, the session is passed. • `pass`: Return bypass response to the rating request of the session (default). • `block`: Return block response to the rating request of the session.

7. 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
```

8. 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 installer and isolator image

After Configuring native browser isolation in FortiProxy on page 6, you must manually upload the latest FortiNBI installer and isolator image:

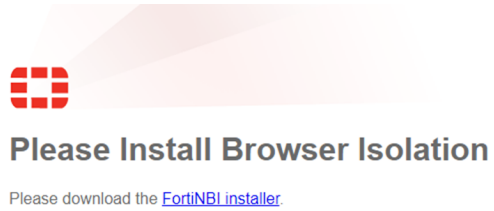
1. Run the following commands in FortiProxy:
   - `execute upload fortinbi-installer cloud`
   - `execute upload fortinbi-isolator-image cloud`
2. When the upload process is complete, verify the uploaded FortiNBI installer and isolator image version by running `diagnose wad nbi status`.
3. Restart FortiProxy to apply the changes.

   FortiProxy then automatically distributes the files 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 12.

Out-of-the-box support for some Asian languages is limited in the isolator. A special image can be requested from the support team when required, referencing bug number *1083310*.

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.



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. .NET Runtime 7.0 and Windows App SDK 1.4 are automatically installed. If the automatic installation fails, you must manually download and install these components from the Microsoft website:
      - .NET Runtime 7.0
      - Windows App SDK 1.4
   b. Files are unpacked to the installation folder, by default *C:\Program Files (x86)\Fortinet\FortiNBI*.
   c. 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 portal through HTTPS, 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.
   d. If using Firefox, the first time that you use FortiNBI you will see a prompt page with instructions to enable

browser permissions to access site data. Follow the instructions to enable the browser permissions.

4. When required, the client will receive an RDP pop-up window for isolation.

Upgrading FortiNBI

When a new FortiNBI version or isolator image is available, you can upgrade your FortiNBI or isolator image version without upgrading your FortiProxy:

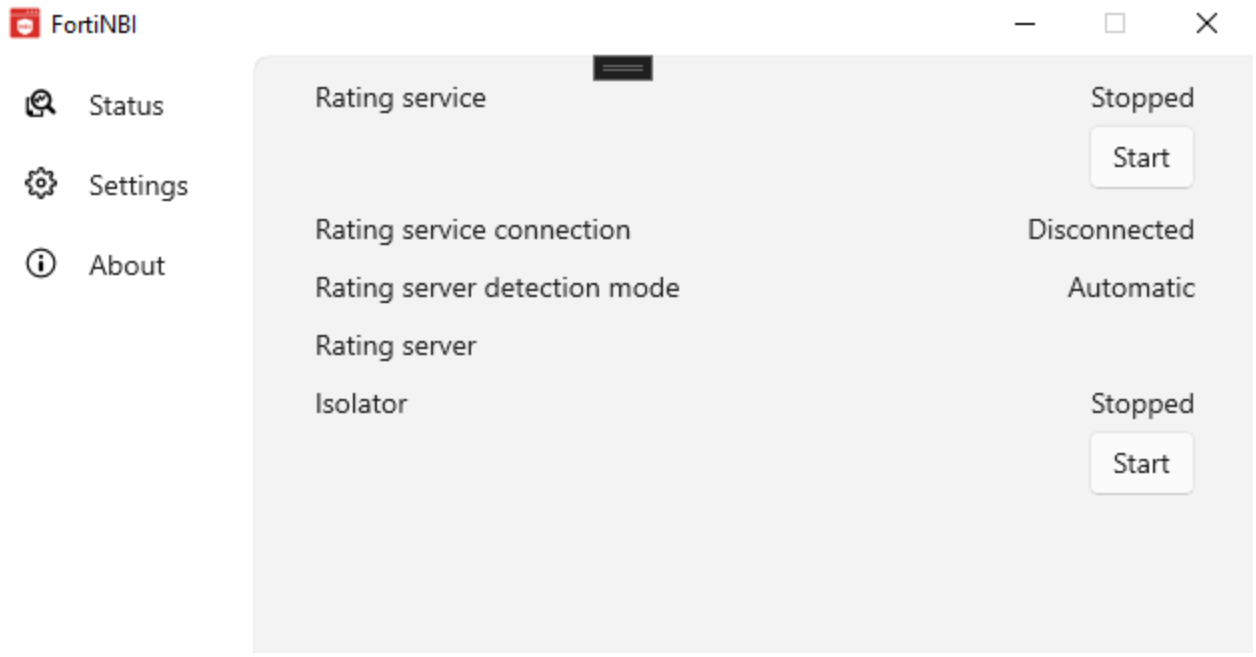
1. Upload the latest FortiNBI installer or isolator image to FortiProxy by running the following commands:
   - `execute upload fortinbi-installer cloud`
   - `execute upload fortinbi-isolator-image cloud`
2. When the upload process is complete, verify the uploaded installer or image version by running `diag wad nbi status`.
3. **(FortiNBI installer)** In Task Manager, restart `FortiNBI.tating_service` to trigger FortiProxy to automatically install the new version of FortiNBI application.
4. **(Isolator image)** In the *Status* tab of the FortiNBI application, click *Start* in the Isolator row to trigger the installation of the new isolator image.
5. Wait for the installation to complete and reboot the machine when requested.
6. **(FortiNBI installer)** Verify the current FortiNBI version in the *About* tab of the FortiNBI application.

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.

Status tab

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

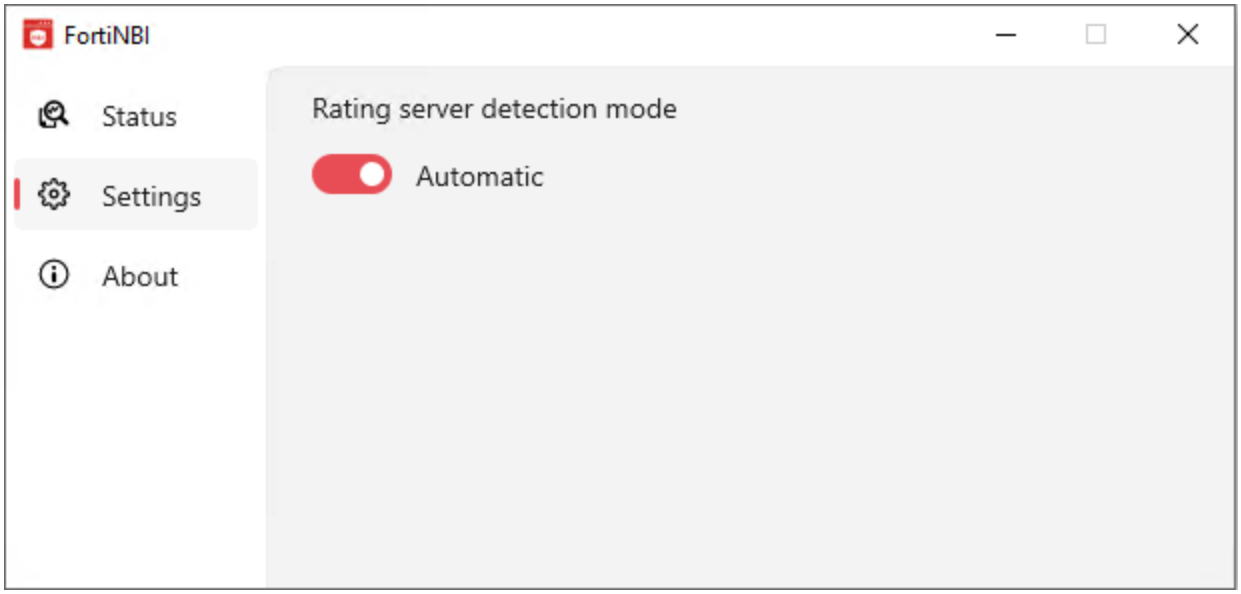


Rating service	Status of the FortiNBI rating service. Click the button to start or stop the service.
Rating service connection	Status of the connection between the GUI and the FortiNBI rating service.
Rating server detection mode	Mode in which the FortiProxy detects the rating server IP address: • *Automatic*: The rating server IP address is resolved using the user's proxy settings. • *Manual*: The rating server IP address is manually configured with a custom FortiProxy IP address. In this mode, the client machine does not need to have a proxy configured.
Rating server	IP address of the rating server.
Isolator	Status of the isolator. Click the button to start or stop the isolator.

Settings tab

Use the *Settings* tab to configure *Rating server detection mode*, which can be one of the following:

- *Automatic*: The rating server IP address is resolved using the user's proxy settings.



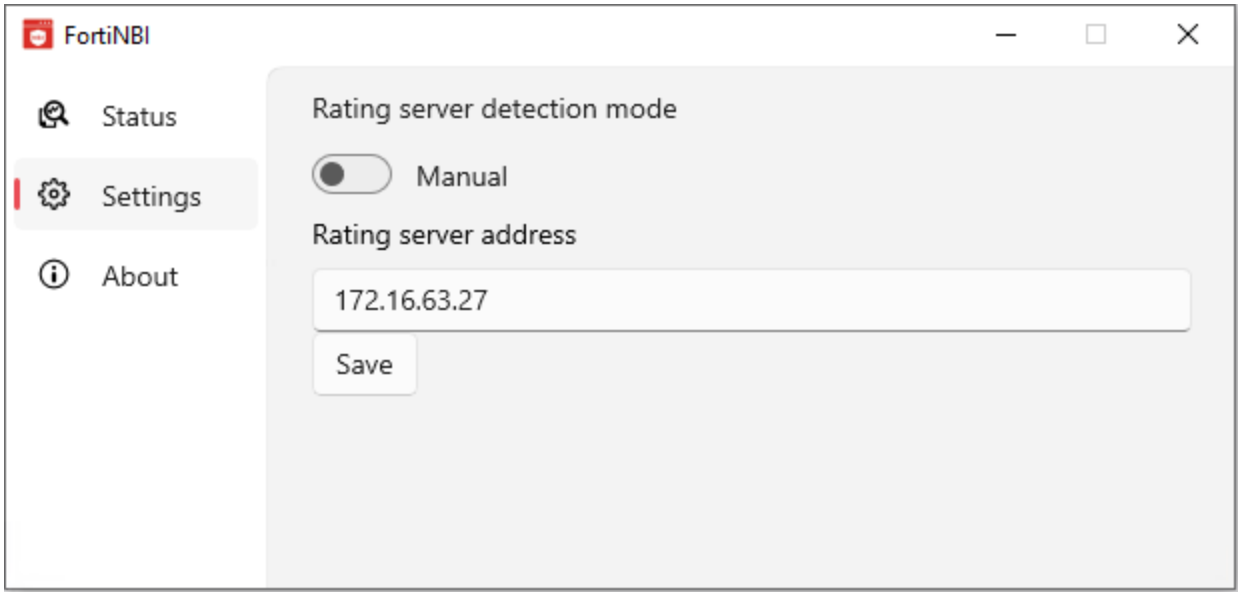
In *Automatic* mode, the FortiNBI detects the rating server IP address using the following:

- DNS WPAD
- PAC URL
- User's proxy configuration

For DNS WPAD and PAC URL, you must set direct access to `system.fortinbi.fortinet.com` and proxy `https://pacdetectproxy.fortinbi.fortinet.com` to the FortiProxy with the configured FortiNBI profile. The web server must be configured to allow `.pac` files to be downloaded and specified using the MIME type `application/x-ns-proxy-autoconfig` in the `Content-Type` header.

- *Manual*: Manually enter a custom FortiProxy IP address. In this mode, the client machine does not need to have a

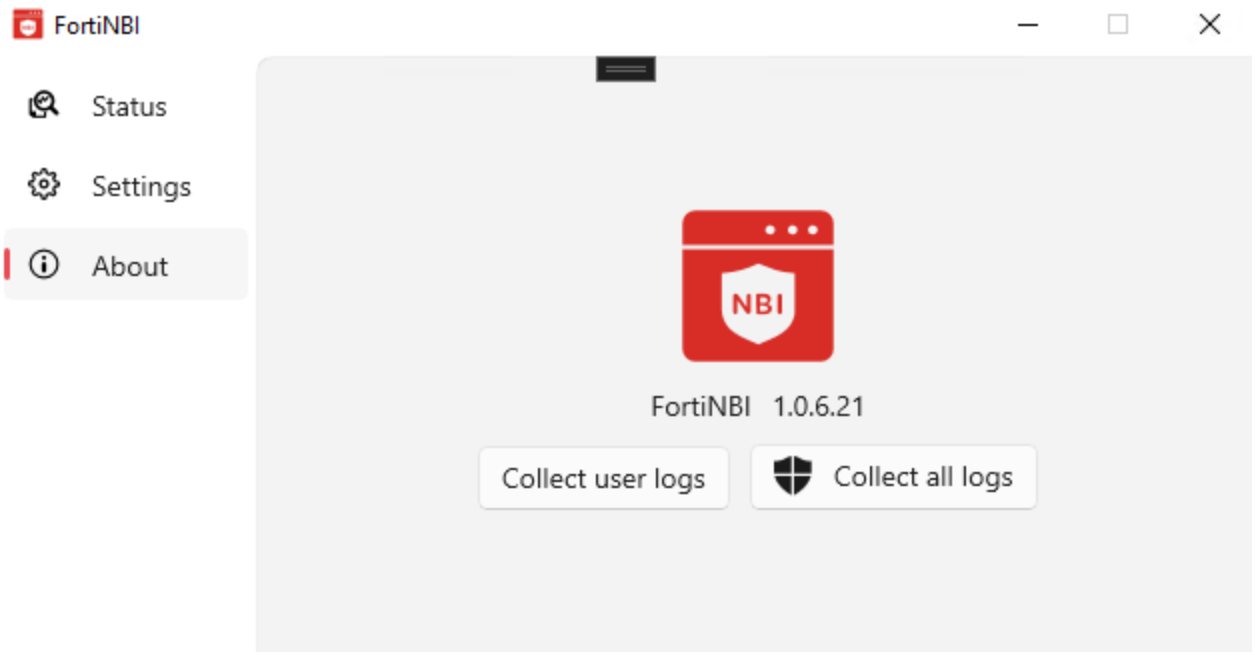
proxy configured.



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 rating server IP address.

About tab

The *About* tab shows the version of FortiNBI that is installed and provides quick access to debug logs. The *Collect user logs* button collects logs for the user while the *Collect all logs* button collects the user's logs AND service logs. Privilege is required to access service logs to protect other users' data on the machine.



To quit the FortiNBI application:

Clicking the *Close* button in the FNBI application window does not quit the application: it will still run in the background in the system tray. To stop the FortiNBI application and the isolator completely, right-click the Fortinet icon in the system tray and click *Quit*.

Change log

Date	Change Description
2024-07-30	Initial document release.