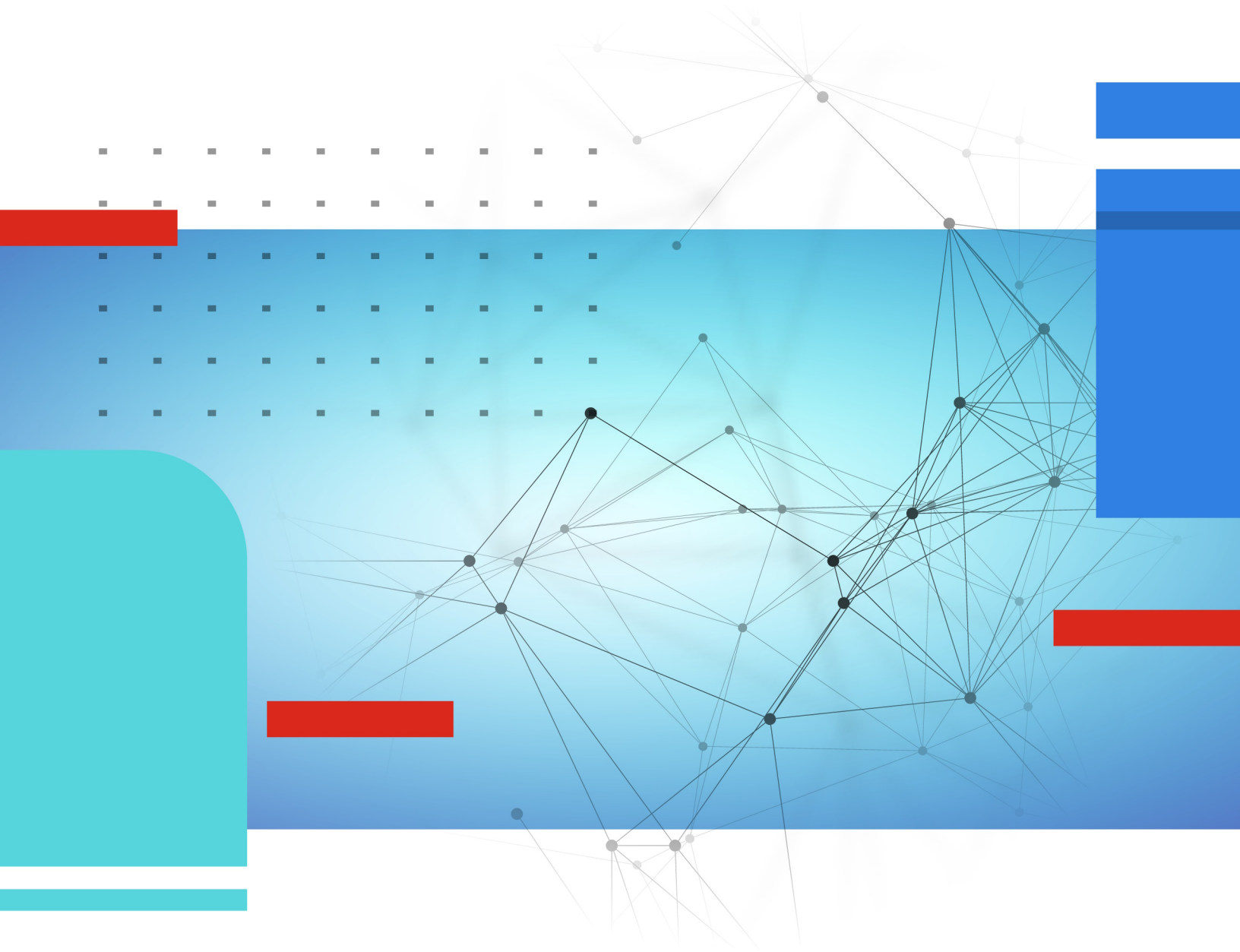
Administration Guide

FortiTelemetry 7.6.4



FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO LIBRARY
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

FORTINET TRAINING INSTITUTE
https://training.fortinet.com

FORTIGUARD LABS
https://www.fortiguard.com

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

FEEDBACK
Email: techdoc@fortinet.com

August 21, 2025
FortiTelemetry 7.6.4 Administration Guide
100-764-1116352-20250821

TABLE OF CONTENTS

Change Log

Date	Change Description
2025-08-21	Initial release.

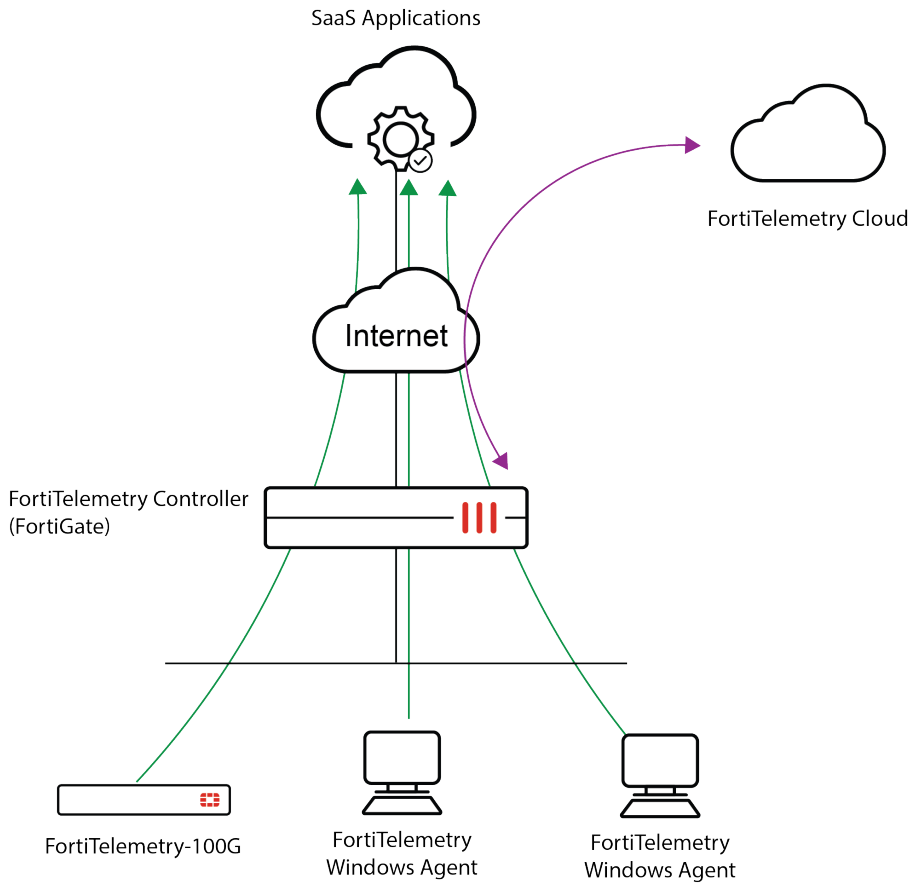
Introduction

FortiTelemetry provides end-to-end user application telemetry monitoring to help enterprises of all sizes improve SaaS application experience based on a comprehensive set of application-level and network-level performance metrics.

A FortiTelemetry deployment consists of one FortiGate acting as FortiTelemetry Controller and one or more FortiTelemetry agents.

- The FortiTelemetry Controller manages the agents by onboarding them to the Security Fabric, managing FortiTelemetry profiles and policies, and includes monitors to allow the administrator to view application metrics and statistics.
- FortiTelemetry agents are on-premise FortiGate-integrated telemetry agents that continuously emulate, monitor, and detect performance metrics across SaaS applications without any user intervention or involvement.

FortiTelemetry collects real-time telemetry information from top business SaaS applications using emulated user browsing activities to calculate different scores and network path information so customers can understand application and network behavior.



Requirements

The following is required in order to setup and use FortiTelemetry features:

- An on-premise hardware-based FortiGate acting as the FortiTelemetry Controller.
  - FortiOS 7.6.3 or later.
  - Hardware FortiGate must have at least 4GB of memory.
  - Network access to reach FortiTelemetry Cloud.
  - *Security Fabric Connection* access must be enabled on the interface used to connect to the agent(s).
  - FortiTelemetry Discovery feature must be enabled.
  - FortiTelemetry Controller must be located in the same layer 2 network segment as the FortiTelemetry agents.
- One or more FortiTelemetry agents must be deployed. There are two types of FortiTelemetry agents available with this release: hardware-based FTL-100G and Windows-based agents.
  - FortiTelemetry Windows agents must be run on a Windows machine with at least 4 CPUs and 8 GB RAM. See the FortiTelemetry Release Notes for more information.
  - FortiTelemetry agents must be deployed in the same layer 2 network segment as the FortiTelemetry Controller's internal interface.

Key features

FortiTelemetry provides the following key features:

- End-to-end user experience monitoring.
- FortiGate-integrated, agent-based synthetic telemetry.
- Built-in telemetry profiles for business SaaS applications.
- Automated measurements for application-level and network-level metrics.
- Application Experience Score (AES) and Application Failure Rate (AFR) calculations.
- Measurement of underlay and overlay networks.

Metrics collected by FortiTelemetry

Using its hardware or software-based agents, FortiTelemetry gathers and sends the following raw telemetry data to FortiTelemetry Cloud for data analysis:

Application-level metrics

- Experience score
- Failure rate
- Time to First Byte (TTFB)

- Application Total Downloading Time (ATDT)
- Application throughput

Network-level metrics

- Latency
- Jitter
- Packet Loss
- TCP Round Trip Time (RTT)
- 95% DNS Resolving Time
- 95% TLS Handshake Time

Setting up FortiTelemetry

This topic includes information about getting started with FortiTelemetry.

To set up FortiTelemetry:

1. Review the prerequisite information to ensure your environment meets the necessary requirements. See:
   - Requirements on page 6.
2. Configure FortiGate as the FortiTelemetry controller. See:
   - Configure FortiGate as FortiTelemetry controller on page 8.
3. Configure your FortiTelemetry agent(s). See:
   - FortiTelemetry-100G hardware agent on page 17
   - FortiTelemetry Windows software agent on page 20
4. Configure and authorize the FortiTelemetry agent(s) on the FortiTelemetry Controller. See:
   - Deploy and authorize the FortiTelemetry agent on page 9.
5. Register your FortiTelemetry Controller to a FortiTelemetry Cloud region. See:
   - Register to a FortiTelemetry Cloud region on page 14.
6. Manage your telemetry profiles to define monitored applications. See:
   - Predefined applications on page 28
   - Telemetry profiles on page 29
7. Configure a telemetry policy to allow the FortiTelemetry Controller to send monitoring tasks to the agents. See:
   - FortiTelemetry policies on page 38.
8. Monitor data from the FortiTelemetry monitor on the FortiTelemetry Controller (FortiGate).
   - Telemetry monitor on page 40

Configure FortiGate as FortiTelemetry controller

Use the CLI to configure a FortiGate as a FortiTelemetry controller. Enable FortiTelemetry on the GUI.

To configure FortiGate as FortiTelemetry controller:

1. In the CLI of the FortiGate that will act as the FortiTelemetry Controller, enter the following CLI to enable the FortiTelemetry Controller:

```
config system global
  set telemetry-controller enable <-- Enable/disable FortiTelemetry controller to manage
FortiTelemetry agents.
end
```

2. Configure the internal interface that the FortiGate will use to connect with the FortiTelemetry agent using the following commands:

```
config system interface
  edit port2
    set allowaccess ping fabric ... <-- Security Fabric Connection access is required for
incoming FortiTelemetry agent traffic.
    set telemetry-discover enable <-- Enables/disables the discovery response.
    set auto-auth-extension-device disable <-- Enables/disables auto-authorization after
agents are discovered.
  end
```

For security reasons, it is recommended that users set `telemetry-discover` to `disable` after agent deployment to avoid the possibility of DOS attacks by sending CAPWAP discover packets.

To enable FortiTelemetry in the GUI:

1. On the FortiGate acting as a FortiTelemetry Controller, go to *System > Feature Visibility*.
2. Under *Security Features*, enable *FortiTelemetry*, and click *Apply*.

Deploy and authorize the FortiTelemetry agent

You can configure and authorize FortiTelemetry agents on the FortiTelemetry Controller (FortiGate) using the GUI or CLI. On FortiGate acting as a FortiTelemetry controller, FortiTelemetry must be enabled on the *System > Feature Visibility* page to display telemetry features in the GUI.

The FortiTelemetry Controller connects to FortiTelemetry agents through the *Telemetry* fabric connector. The following methods are supported for adding FortiTelemetry agents to FortiTelemetry Controller.

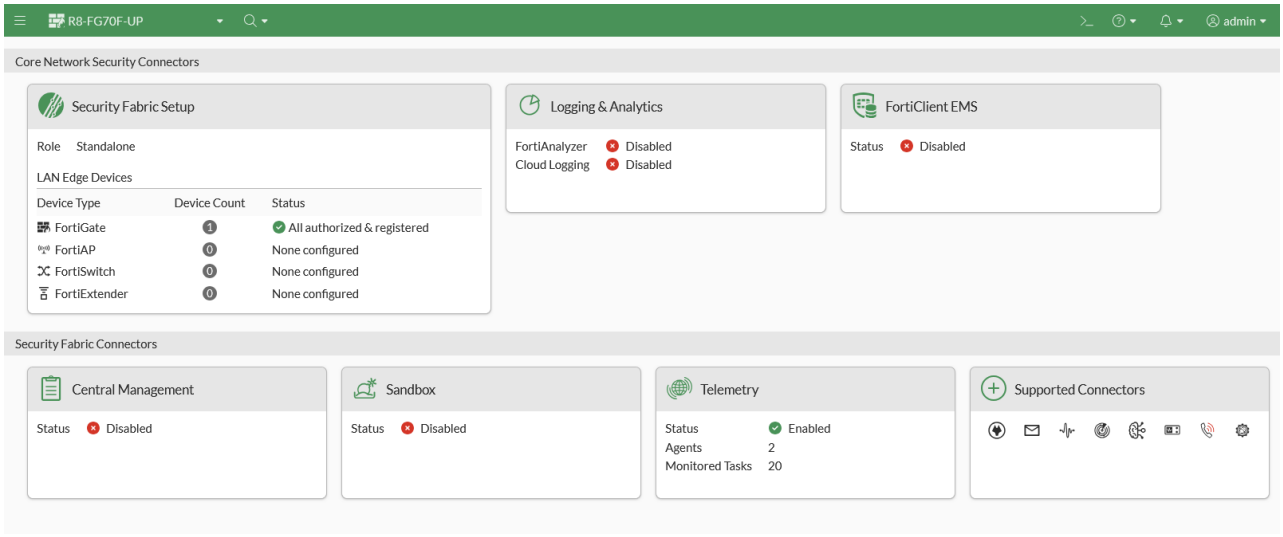
Discovery method	FortiTelemetry Controller discovers telemetry agents using CAPWAP. These agents are automatically displayed in the *Telemetry* fabric connector. The administrator must manually authorize each agent before it can be used by the FortiTelemetry Controller. See Authorizing FortiTelemetry agents on page 11.
Pre-configuration method	In the FortiTelemetry fabric connector settings, you can create FortiTelemetry agent using the FortiTelemetry agent's serial number as the name, and set the *Authorization* status to *Authorized*. When the FortiTelemetry Controller detects the real agent online, it will be automatically authorized. See Creating a FortiTelemetry agent in the Telemetry fabric connector on page 12.

FortiTelemetry agent(s) must be deployed in the same subnet as the internal interface of the FortiTelemetry Controller.

Viewing the FortiTelemetry fabric connector

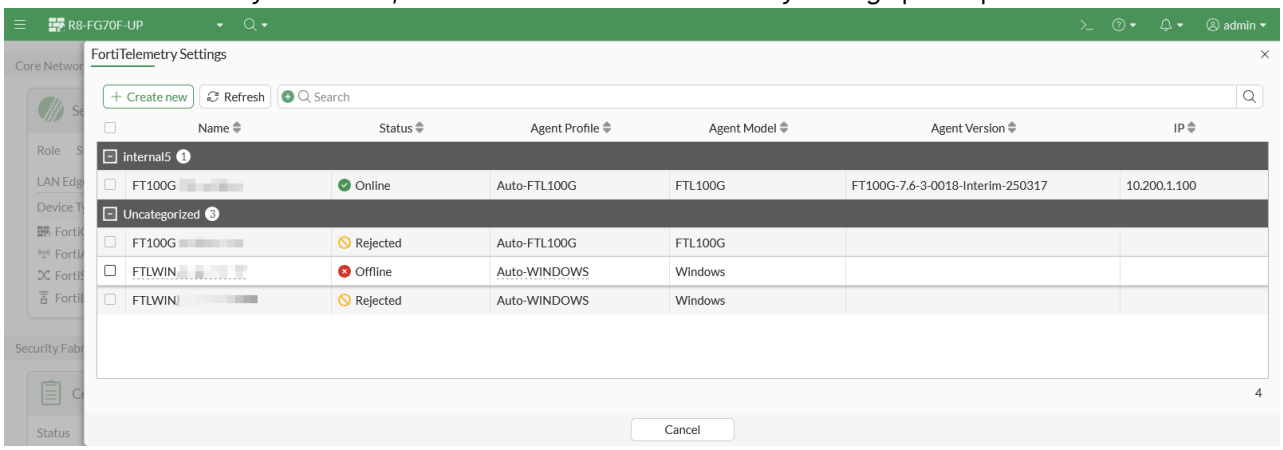
To view the FortiTelemetry fabric connector:

1. Go to *Security Fabric* > *Fabric Connectors*. The *Telemetry* connector is displayed with the following information:



Status	Status of FortiTelemetry: *Enabled* or *Disabled*.
Agents	The number of online, authorized FortiTelemetry agents discovered by the FortiTelemetry Controller.
Monitored Tasks	Number of tasks being monitored by the FortiTelemetry agents based on the configured telemetry profile(s) selected in the firewall policy used by the FortiTelemetry Controller.

2. Click on the *Telemetry* connector, and click *Edit*. The *FortiTelemetrySettings* pane opens.



FortiTelemetry agents are displayed and are grouped by interface. The following information is displayed:

Create new	Click to create pre-authorized Telemetry connectors to automatically authorize FortiTelemetry agents.

	See Creating a FortiTelemetry agent in the Telemetry fabric connector on page 12.
Name	Name of the FortiTelemetry agent.
Status	Status of the FortiTelemetry agent: *Authorized*, *Unauthorized*, or *Reject*.
Agent Profile	Profile assigned to the agent when FortiTelemetry Controller discovers the agent. FortiTelemetry Controller automatically creates and assigns the following profiles when no pre-configured profiles exist: • The *Auto-WINDOWS* agent profile is assigned to software agents. • The *Auto-FTL100G* agent profile is assigned to hardware agents. Agent profile details can be viewed in the CLI using the config telemetry-controller agent-profile command.
Agent Model	Model of the agent: Windows for software agents and FTL100G for hardware agents.
Agent Version	Agent version.
IP	IP address of the FortiTelemetry agent

3. Select an agent to access additional buttons, such as *Edit*, *Delete*, and *More*.
4. Select an agent, and click *Edit*. The *Telemetry Agent* pane opens.
5. Click *OK* to close the Telemetry Agent pane.
6. Click *Cancel* to close the FortiTelemetry Settings pane

Authorizing FortiTelemetry agents

When the FortiTelemetry Controller automatically discovers FortiTelemetry agents, it displays them in the Telemetry fabric connector and assigns a profile to each agent.

You must manually authorize each discovered FortiTelemetry agent before the FortiTelemetry Controller can use it.

After a FortiTelemetry agent is authorized, a firewall address with the agent's serial number is automatically created.

To authorize FortiTelemetry agents in the GUI:

1. Go to *Security Fabric* > *Fabric Connectors*.
2. Click the *Telemetry* connector, and click *Edit*. The *FortiTelemetry Settings* pane opens.
3. Select an agent, and click *More* > *Set Status* > *Authorize*.

To authorize FortiTelemetry agents in the CLI:

1. By default, automatically discovered telemetry agents are unauthorized, but you can authorize each agent after it connects to FortiGate:

```
config telemetry-controller agent
  edit "FT100GTK24000002"
    set authz authorize

  next
end
```

Creating a FortiTelemetry agent in the Telemetry fabric connector

You can configure Telemetry fabric connectors to automatically authorize agents after they connect to the FortiTelemetry Controller. You must know the agent name to configure pre-authorized telemetry connectors. The agent name is used to match the discovered agent to the corresponding telemetry connector. The agent name is the serial number of the FortiTelemetry agent.

You can create and use a custom agent profile, or you can use a default agent profile (Auto-WINDOWS for software agents or Auto-FTL100G for hardware agents) if the FortiTelemetry Controller has created a default agent profile. If you create an agent profile, ensure that the model in the agent profile matches the type of agent used.

To create agent profiles in the CLI:

1. Create an agent profile for the type of agent you are using.

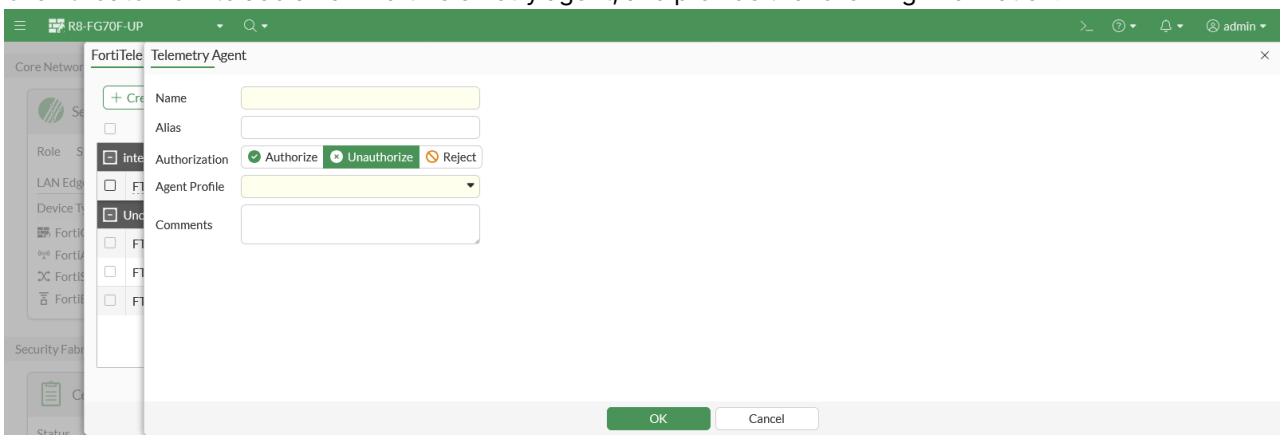
   A profile for hardware agents should use the FTL100G model, and a profile for software agents should use the WINDOWS model.

   ```
   config telemetry-controller agent-profile
     edit "WINDOWS-pre-auth"
       set comment windows devices
       set model WINDOWS
     next
     edit "FTL100G-pre-auth"
       set comment hardware
       set model FTL100G
     next
   end
   ```

To configure FortiTelemetry agents in the FortiOS GUI:

1. Go to *Security Fabric* > *Fabric Connectors*.
2. Click on the *Telemetry* connector, and click *Edit*. The *FortiTelemetry Settings* pane opens.

3. Click *Create New* to add a new FortiTelemetry agent, and provide the following information:



Name	Enter a name for the FortiTelemetry agent. The agent name is the serial number of the FortiTelemetry agent. The name starts with `FTLWIN` for Windows agents or `FT100G` for hardware agents.
Alias	(Optional) Provide an alias for the FortiTelemetry agent.
Authorization	Select *Authorize*.
Agent Profile	Select an agent profile. Ensure the model configured in the profile matches the type of agent.
Comments	(Optional) Add comments to help identify the agent.

4. Click *OK*. The telemetry connector is displayed in the uncategorized list until the FortiTelemetry Controller discovers the corresponding telemetry agent and uses the connector to automatically authorize the agent and assign a status of *Online*.

To create pre-authorized telemetry connectors in the CLI:

1. Create a pre-authorized telemetry connector for each agent to specify the agent name, authorization, and agent profile.
   The agent name starts with FTLWIN for Windows agents or FT100G for hardware agents.

```
config telemetry-controller agent
  edit "FT100GTK24000007"
    set alias "FTL100G"
    set authz authorized
    set agent-profile "FTL100G-pre-auth"
  next
  edit "FTLWIN8660000001"
    set alias "WINDOWS-108"
    set authz authorized
    set agent-profile "WINDOWS-pre-auth"
  next
end
```

Register to a FortiTelemetry Cloud region

Using the FortiTelemetry Controller (FortiGate) CLI, you can configure the FortiTelemetry Cloud region that your FortiTelemetry Controller connect to.

Currently, only the *Global* region is supported which is located in the Vancouver FortiStack data center.

To register to FortiTelemetry Cloud using the CLI:

1. On the FortiGate that is acting as FortiTelemetry Controller, enter the following commands in the CLI:

```
config telemetry-controller global
  set region global
  set retry-interval 120
end
```

For more information, see Config CLI commands on page 43.

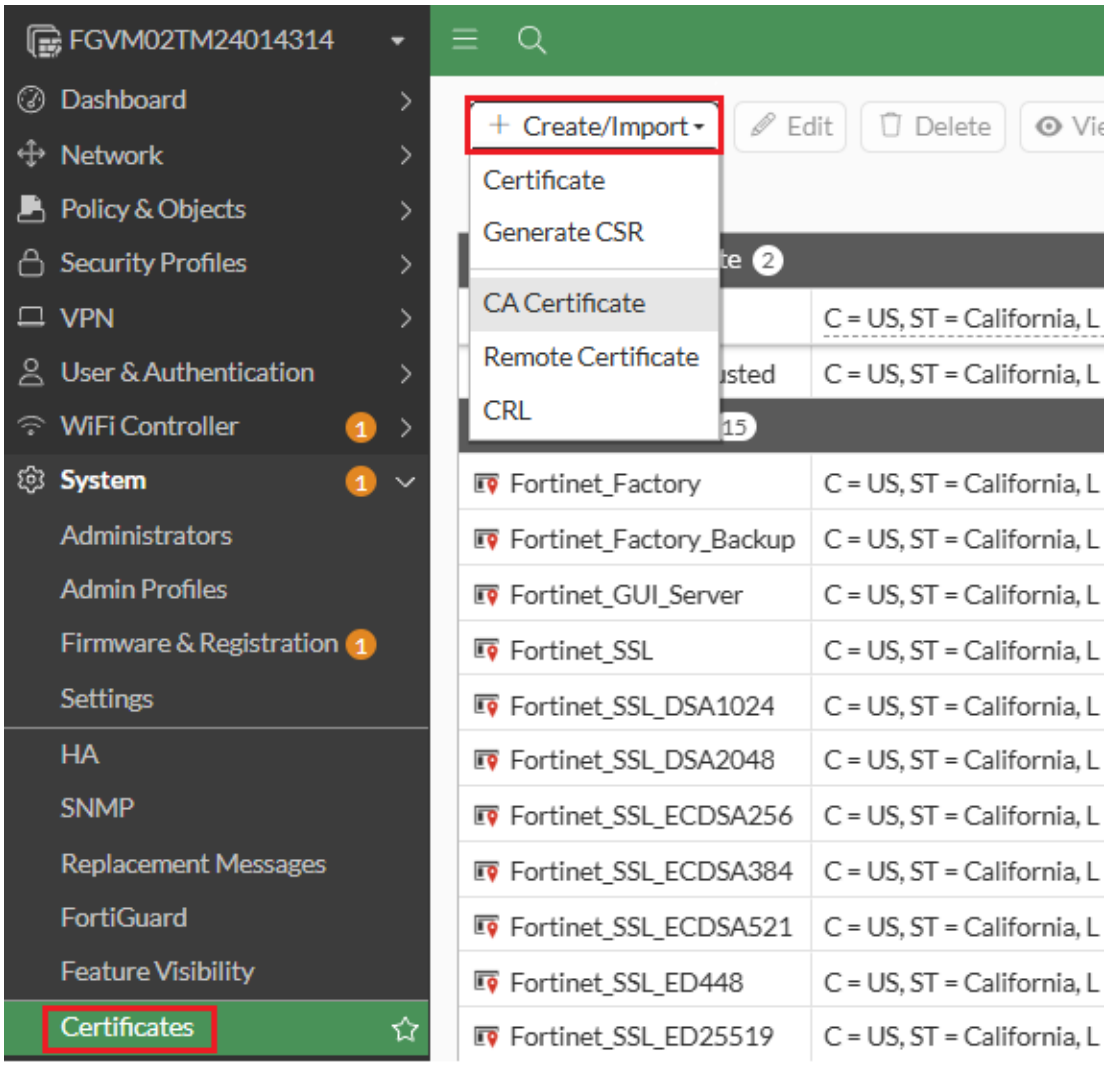
Configure the certificate (for FortiTelemetry Windows agent only)

A certificate authority must be configured on the FortiTelemetry Controller and the certificate must be uploaded to the FortiTelemetry Windows agent. The user is responsible for the creation and maintenance of this certificate. For the FortiTelemetry-100G agent, this step is not required because the hardware device includes a Fortinet certificate.

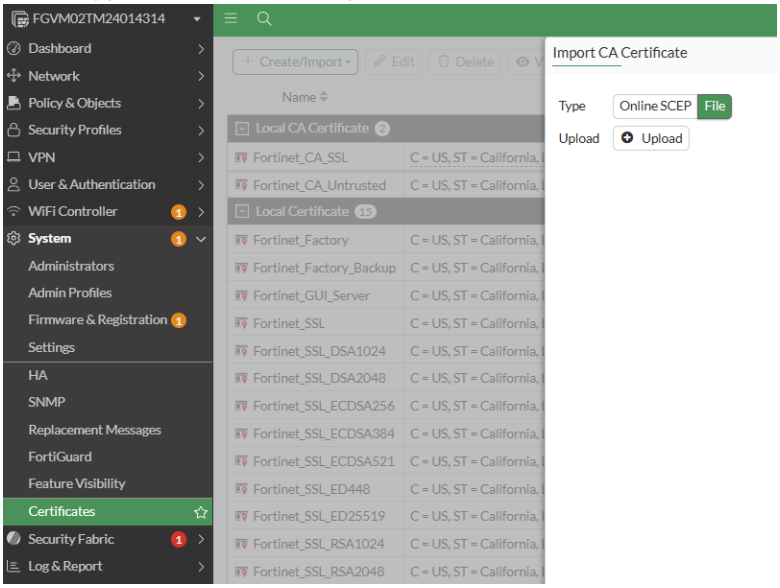
The certificate authority installed on the FortiGate is used to verify the telemetry agent's certificate, which allows authentication between the FortiGate and FortiTelemetry Windows agent.

To configure the certificate for FortiTelemetry Windows agent:

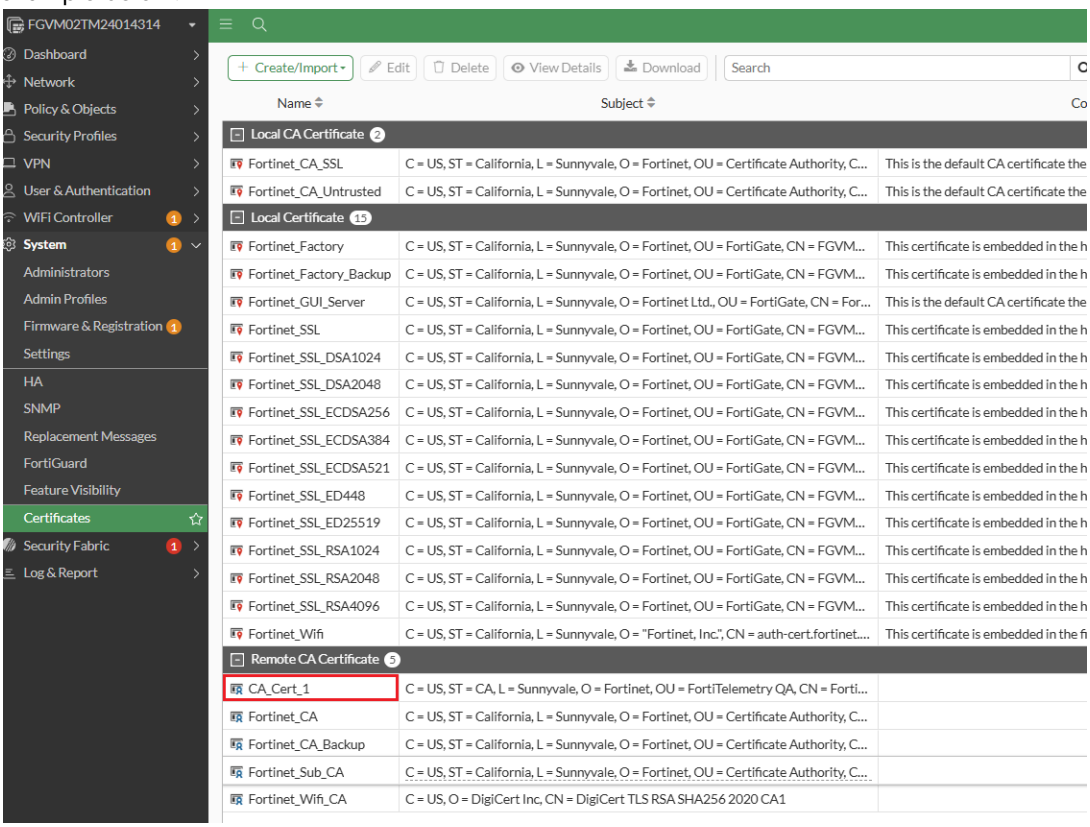
1. Create a certificate authority (CA) certificate. The certificates used by FortiTelemetry Windows agent are not included by default and must be supplied and maintained by the user.
2. Upload the CA certificate on the FortiGate acting as FortiTelemetry Controller:
   a. Go to *System* > *Certificates*.
   b. Click *Create/Import* > *CA Certificate*.



c. Select *Type* as *File* and then upload the CA certificate.



d. Click *OK*. Once uploaded, you will see the certificate under *Remote CA Certificate* as shown in the example below.



3. Configure the FortiGate global settings to use the CA for FortiTelemetry agents using the following commands in the CLI:

```
config telemetry-controller global
  set telemetry-ca-certificate "CA_Cert_1"
end
```

4. Using your chosen certificate authority, create a user certificate and download the certificate file on the Windows OS local machine that is hosting the FortiTelemetry Windows agent. The private key information is required and the certificate should be of the PFX or p12 file type.

5. In the FortiTelemetry Windows Agent GUI, navigate to *Settings* > *Agent Management Certificate* and import the certificate.

FortiTelemetry agents

FortiTelemetry uses on-premise telemetry agents which can be either hardware-based or software-based.

The telemetry agents collect data by simulating real users running the monitored SaaS applications on a web browser. The agents collect raw application-level and network-level statistics, turn them into meaningful telemetry metrics, and send the metrics to FortiTelemetry Cloud for further analysis and retention.

FortiTelemetry agents are controlled by an on-premise FortiGate, acting as the FortiTelemetry Controller.

The following FortiTelemetry agents are available at the time of the FortiTelemetry 7.6.4 release:

FortiTelemetry agent	Description
FortiTelemetry-100G Agent	A desktop size hardware appliance agent capable of actively emulating users browsing SaaS applications.
FortiTelemetry Windows Agent	A software agent running on a Windows machine (minimum of 4 CPU and 8 GB RAM) capable of actively emulating users browsing SaaS applications.

For information on set up and management of FortiTelemetry agents, see the following topics:

- FortiTelemetry-100G hardware agent on page 17
- FortiTelemetry Windows software agent on page 20

FortiTelemetry-100G hardware agent

FortiTelemetry-100G agent performs monitoring tasks and sends logs to the cloud, managed by the FortiTelemetry Controller through the control and provisioning of wireless access points (CAPWAP) protocol.

This topic includes the following sections:

- Initial configuration of the agent on page 17
- Starting the agent on page 20
- Troubleshooting on page 20

Initial configuration of the agent

The FortiTelemetry-100G agent automatically starts upon device boot-up.

The FortiTelemetry-100G defaults to using *port1* for connection with the FortiTelemetry Controller and requires an additional port for internet connectivity to execute monitoring tasks. By default, *port1* is in DHCP mode. Only *port1* can be used for CAPWAP connecting to the FortiTelemetry Controller (FortiGate).

You can use the FortiTelemetry console to configure network and system settings.

Display options in the FortiTelemetry console

You can use the `help` command in the FortiTelemetry console to view available commands.

```
>
> help

FortiTelemetry Console
General:
        help            Display this text.
        exit            Exit from the CLI.
        passwd          Change the password of the current user.
Configuration:
        show            Show bootstrap configuration.
        set             Set configuration parameter.
                        Available attributes/values for set:

                                port1-ip        <IP/netmask>|<dhcp>
                                                 e.g. port1-ip 1.2.3.4/24 or port1-ip dhcp
                                port2-ip        <IP/netmask>|<dhcp>
                                                 e.g. port2-ip 1.2.3.4/24 or port2-ip dhcp
                                port3-ip        <IP/netmask>|<dhcp>
                                                 e.g. port3-ip 1.2.3.4/24 or port3-ip dhcp
                                port4-ip        <IP/netmask>|<dhcp>
                                                 e.g. port4-ip 1.2.3.4/24 or port4-ip dhcp
                                port5-ip        <IP/netmask>|<dhcp>
                                                 e.g. port5-ip 1.2.3.4/24 or port5-ip dhcp
                                port6-ip        <IP/netmask>|<dhcp>
                                                 e.g. port6-ip 1.2.3.4/24 or port6-ip dhcp
                                port7-ip        <IP/netmask>|<dhcp>
                                                 e.g. port7-ip 1.2.3.4/24 or port7-ip dhcp
                                port8-ip        <IP/netmask>|<dhcp>
                                                 e.g. port8-ip 1.2.3.4/24 or port8-ip dhcp
                                port9-ip        <IP/netmask>|<dhcp>
                                                 e.g. port9-ip 1.2.3.4/24 or port9-ip dhcp
                                port10-ip       <IP/netmask>|<dhcp>
                                                 e.g. port10-ip 1.2.3.4/24 or port10-ip dhcp
                                default-gw      <IP>
                                date            <YYYY-MM-DD>
                                time            <HH:MM:SS>
                                timezone        <timezone id (0-73)>

        unset           Unset configuration parameter.
                        Available attributes for unset:

                                default-gw

System:
        reboot          Reboot the FortiTelemetry.
        shutdown        Shutdown the FortiTelemetry.
        factory-reset   Reset configuration to defaults and delete all data.
        status          Display some status information.
        fw-upgrade      Upgrade firmware or install VM via FTP or SCP.
        usg-license     Convert the unit to be USG licensed.
        set-maintainer  Disable or enable maintainer account.
Utilities:
        exec            Collect system status for troubleshooting.
        traceroute      Examine route taken to another network host.
Diagnostics:
        hardware-info   Display general hardware status information.
        disk-attributes Display system disk attributes.
        disk-errors     Display any system disk errors.
        disk-health     Display disk health information.
        disk-info       Display disk hardware status information.
```

Configure network settings

The following CLI commands can be used to configure network settings:

`set portN-ip <IP/netmask>`	Configure the IP address with the subnet mask information for the port. By default, port1 is used for connection with FortiTelemetry Controller.
`set portN-ip <dhcp>`	Set the port to receive its IP configuration via DHCP.
`set default-gw <IP>`	Configure the gateway IP address.

```
> set port1-ip 10.65.172.245/22
>
> set port1-ip 10.65.172.247/22
>
> set port2-ip dhcp
set interface port2 dhcp mode successfully.
>
> set default-gw 10.65.175.254
IPv4 default gateway was set successfully in CLI.
>
> show
Configured parameters:
        Port1   IPv4 IP: 10.65.172.247/22        MAC: 48:3A:02:5F:CE:E8
        Port2   IPv4 IP: 10.200.1.120/24        MAC: 48:3A:02:5F:CE:E9
        Port3   IPv4 IP: 192.168.2.99/24        MAC: 48:3A:02:5F:CE:EA
        Port4   IPv4 IP: 192.168.3.99/24        MAC: 48:3A:02:5F:CE:EB
        Port5   IPv4 IP: 192.168.4.99/24        MAC: 48:3A:02:5F:CE:EC
        Port6   IPv4 IP: 192.168.5.99/24        MAC: 48:3A:02:5F:CE:ED
        Port7   IPv4 IP: 192.168.6.99/24        MAC: 48:3A:02:5F:CE:EE
        Port8   IPv4 IP: 192.168.7.99/24        MAC: 48:3A:02:5F:CE:EF
        Port9   IPv4 IP: 192.168.8.99/24        MAC: 48:3A:02:5F:CE:F0
        Port10  IPv4 IP: 192.168.9.99/24        MAC: 48:3A:02:5F:CE:F1
        IPv4 Default Gateway: 10.65.175.254
```

Configure the date, time and timezone

The following CLI commands can be used to configure the system time and timezone:

`set date`	Configure the system date.
`set time`	Configure the system time.
`set timezone`	Configure the timezone.

```
> set date 2025-01-22
>
> set time 08:10:00
>
> set timezone 4
set timezone to 4       (GMT-8:00) Pacific Time (US & Canada)
>
```

Starting the agent

To start the FortiTelemetry-100G agent:

1. Access the FortiTelemetry console.
2. Use the `status` command to view the current status of the FortiTelemetry-100G agent, including the serial number and system time.

Troubleshooting

You can use the `exec ping` and `traceroute` commands to troubleshoot network issues on the FortiTelemetry-100G.

FortiTelemetry Windows software agent

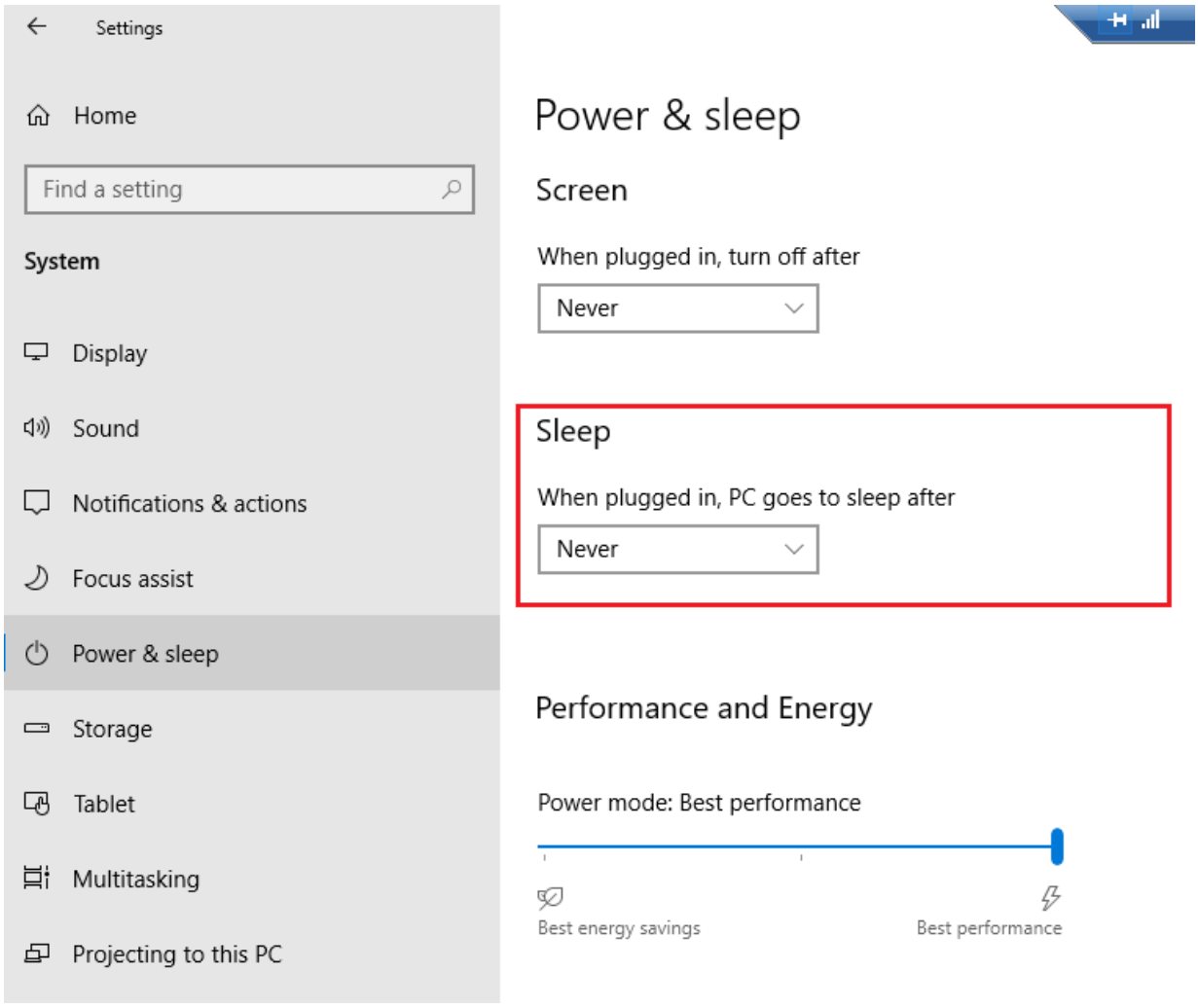
This topic covers administration of the Windows OS based FortiTelemetry endpoint agent, and includes the following sections:

Prerequisite configurations on the Windows host

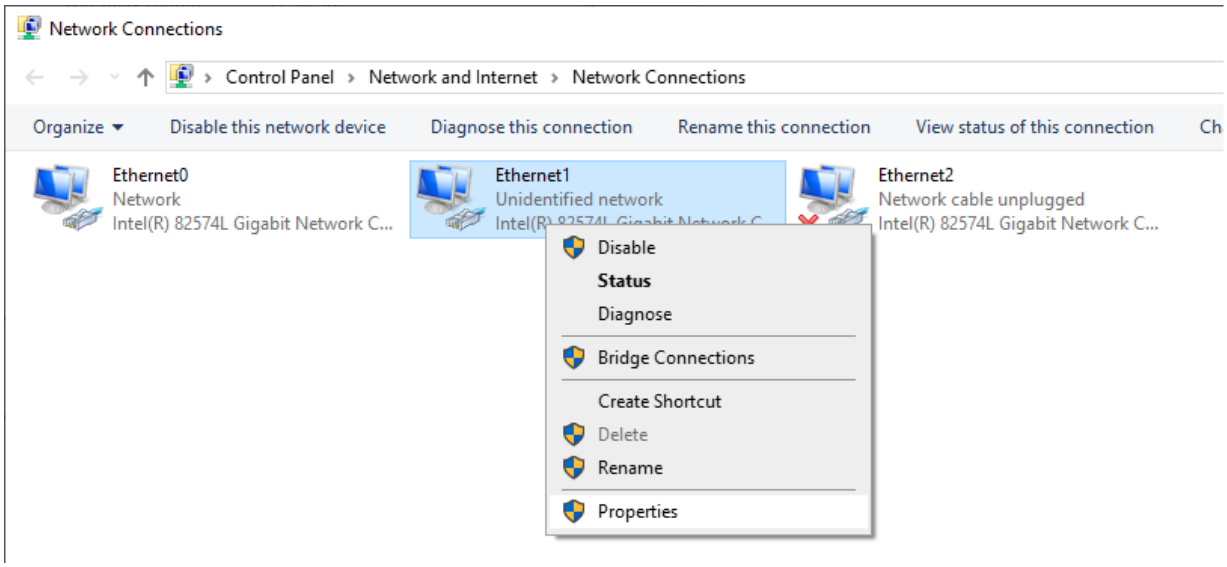
The following steps need to be taken on the Windows host for successful functioning of the FortiTelemetry agent. The example in this document uses Windows 10 (64-bit).

To configure the Windows host:

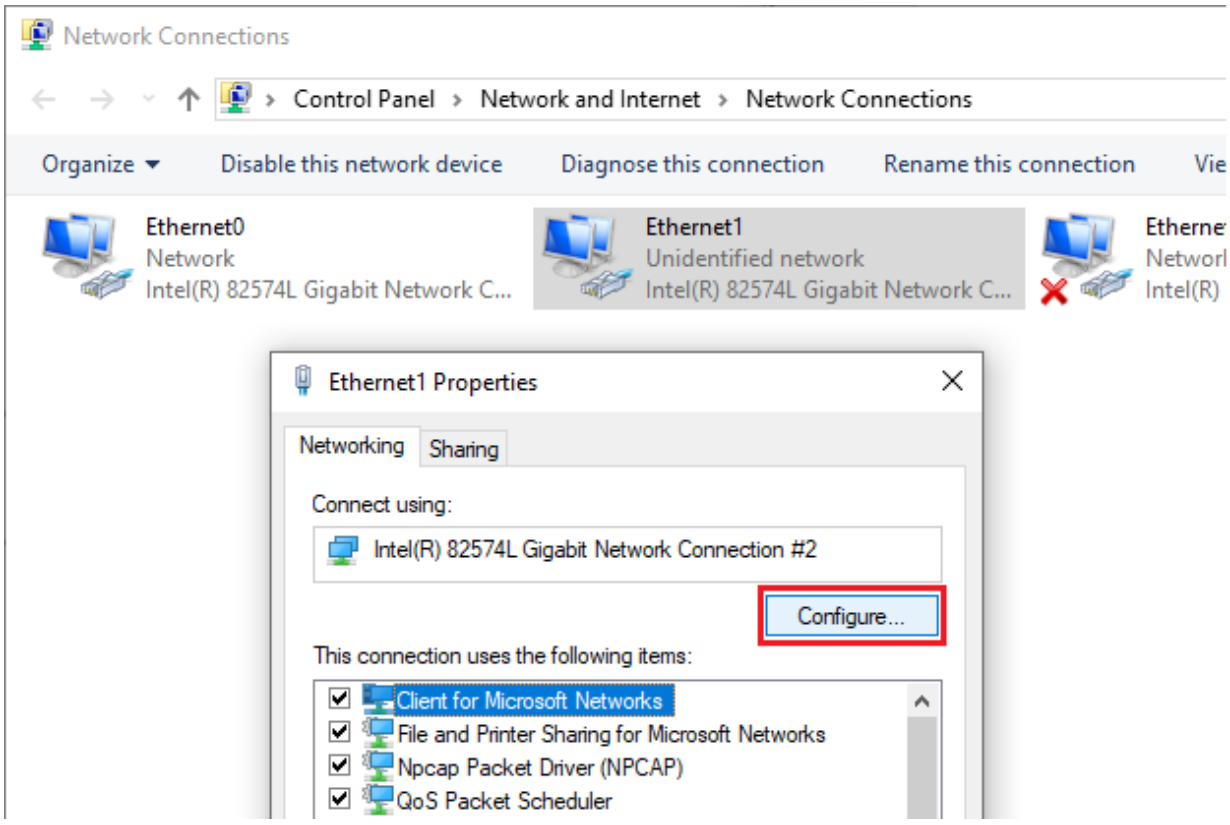
1. Configure *Power & Sleep* settings:
   a. On the Windows system, search and navigate to *System Settings* > *Power & Sleep* settings.
   b. Change the time for *Sleep* to *Never*.



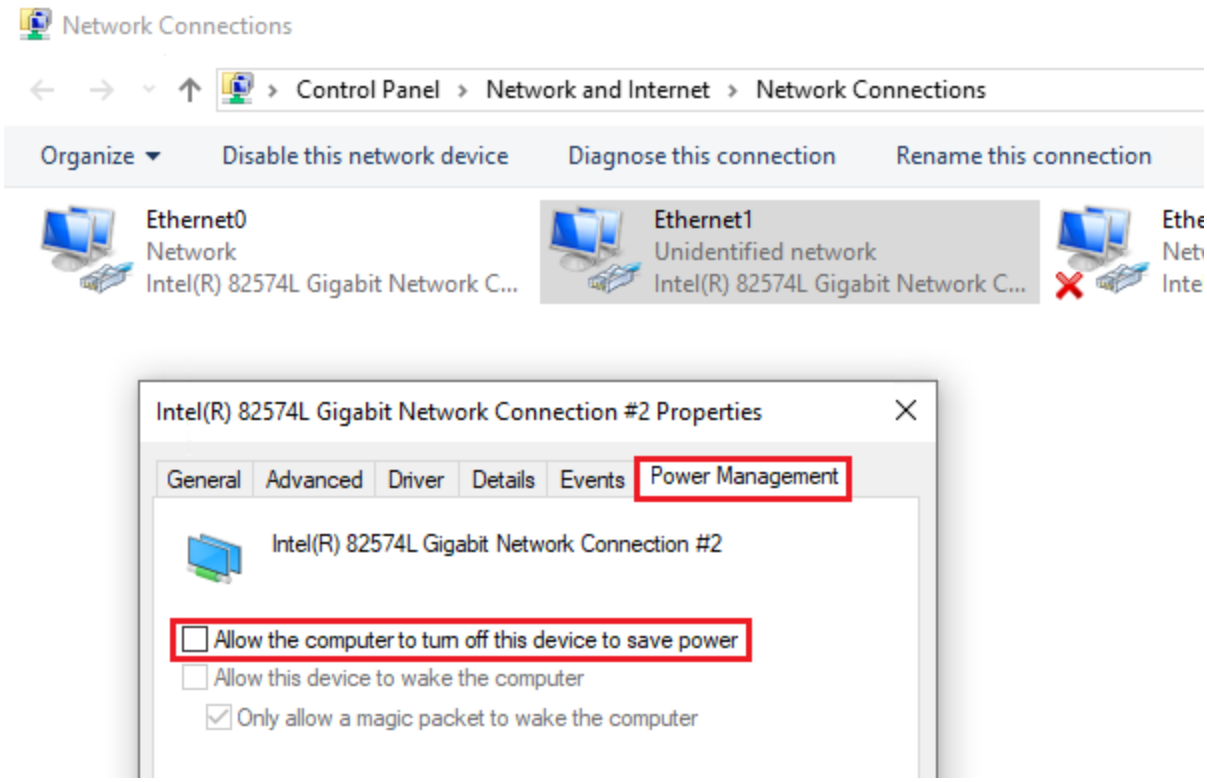
2. Configure network port management settings:
   a. Go to *Windows Settings > Network & Internet > Ethernet > Change adapter options*.
   The list of network adapters on the host is displayed.
   b. Right-click on the network adapter connecting to the FortiTelemetry Controller (FortiGate) and click on *Properties*.



c. Click on the *Configure* button under *Networking*.



d. Click on the *Power Management* tab, and uncheck the *Allow the computer to turn off this device to save power* setting.



3. Configure the FortiGate acting as FortiTelemetry Controller with a CA and install the certificate to the FortiTelemetry Windows agent. See Configure the certificate (for FortiTelemetry Windows agent only) on page 14.

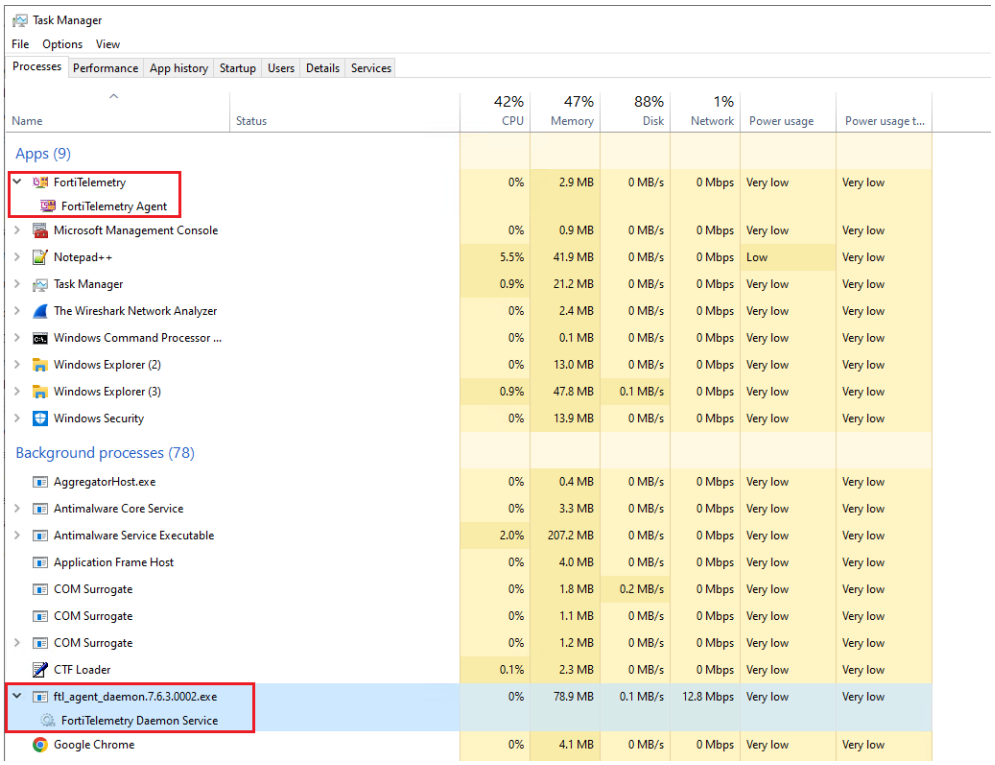
Installing the agent

To install the FortiTelemetry Windows agent:

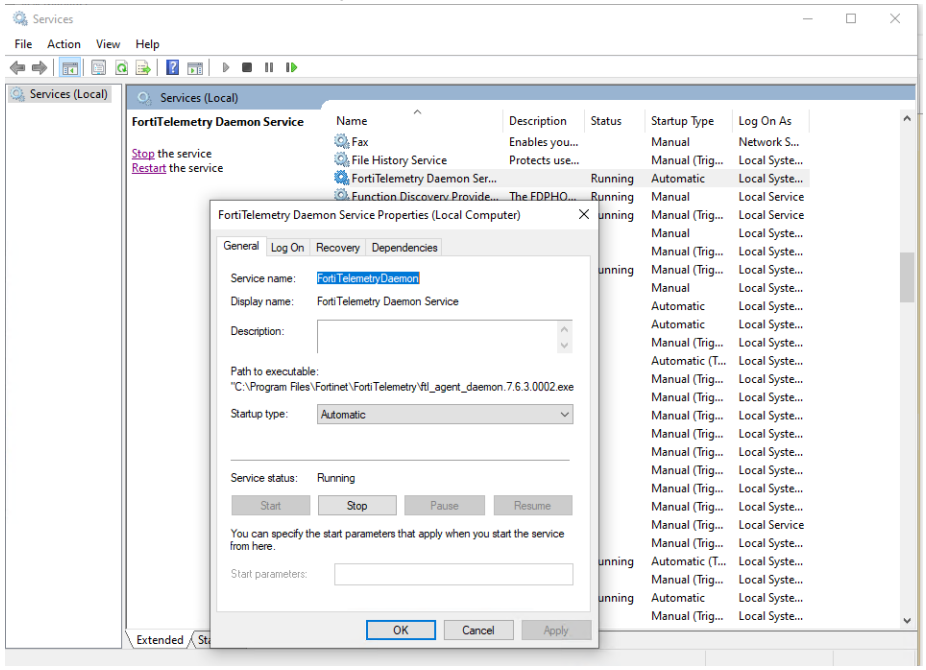
1. Copy the FortiTelemetry agent installer (.msi) file on the Windows host system.
2. Run the installer by double-clicking or *right-click* > *Install*. This will start the FortiTelemetry Agent Setup Wizard.
3. Click *Next*, review and accept the *License Agreement*, and click *Next* again.
4. Configure the installation path and click *Next*.
5. Click *Install*. This will install the FortiTelemetry agent.
6. Click *Finish* to complete the installation.

Managing the agent in Windows

You can use the Windows Task Manager to check the status of the FortiTelemetry agent processes, as in the example below.



The FortiTelemetry agent daemon will automatically run after installation or on restarting the Windows system. You can use the *Services* app on the Windows system to *Start*, *Stop*, *Pause* and *Resume* the *FortiTelemetry Daemon* service as shown in the example below.



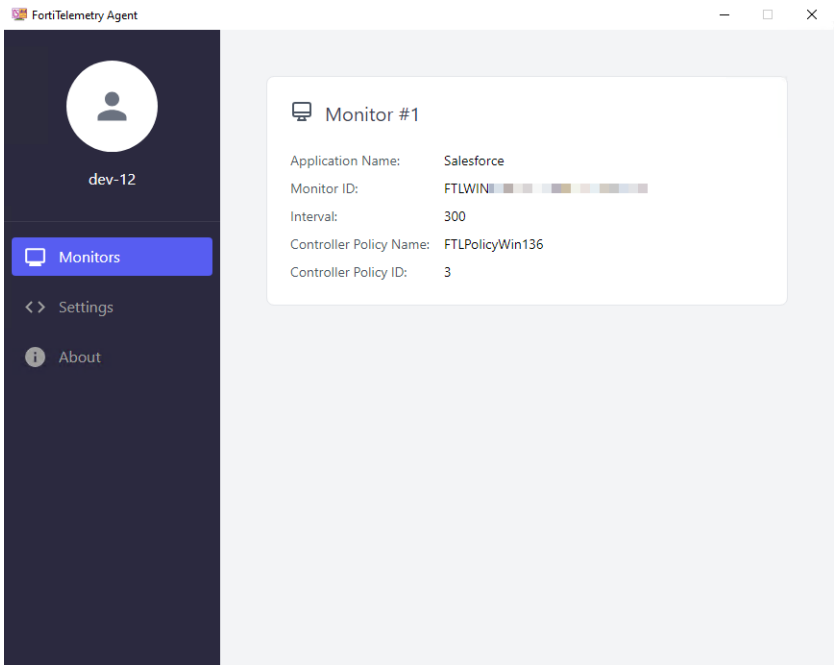
Using the FortiTelemetry Windows agent GUI

The FortiTelemetry Windows agent has two components: The graphical user interface (GUI) and the backend daemon.

The GUI includes 3 tabs which display different information about the FortiTelemetry Windows agent and allows you to make selections for configuration. These tabs include *Monitors*, *Settings*, and *About*.

Monitor

When the connection between the FortiTelemetry Windows agent and the FortiTelemetry Controller is successful, and the correct configuration for application monitoring is present on the FortiGate, the FortiGate will send monitoring tasks to the agent. The details of the current monitoring tasks on the agent can be seen from the *Monitor* tab.

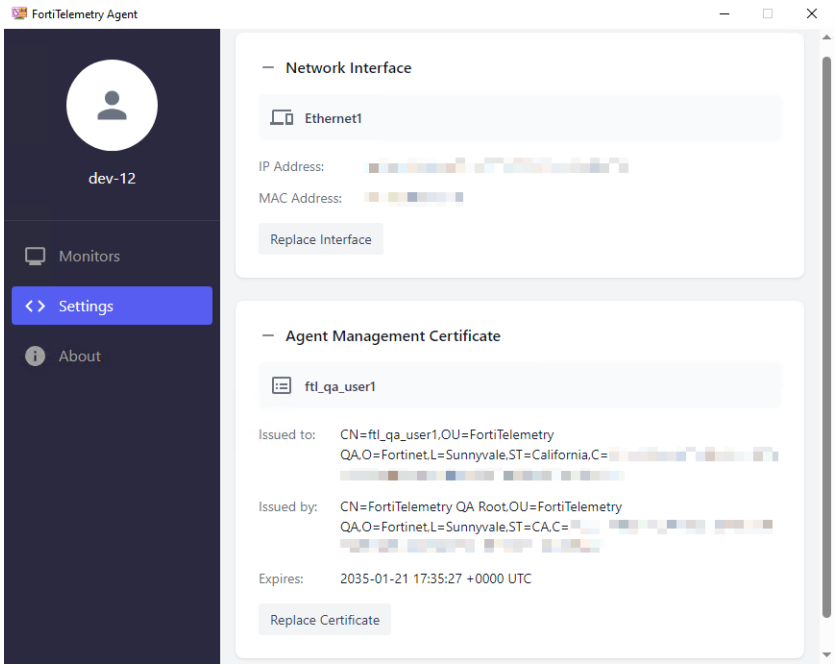


Settings

The *Settings* tab allows you to configure certain settings for the FortiTelemetry Windows Agent, including:

Network Interface	Configure the interface to use while connecting to the FortiTelemetry Controller (FortiGate). By default, the interface with the default gateway will be chosen, but you can select any other interface that you prefer.
Agent Management Certificate	Select the certificate for the agent to use while negotiating Client Authentication in DTLS for CAPWAP channel. This certificate needs to be installed before the agent installation as mentioned in the *Requirements* section. If you have more than one certificate, you may make a selection for the correct one here.

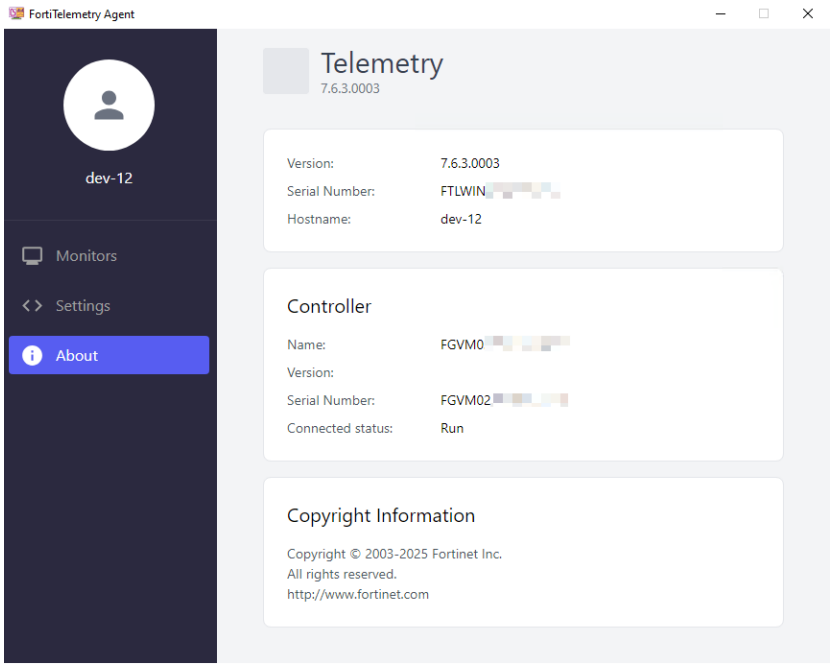
This tab can be used to later replace the interface or certificate used by the FortiTelemetry Windows agent.



About

The *About* tab displays information about the FortiTelemetry Windows agent and connected FortiTelemetry Controller, including:

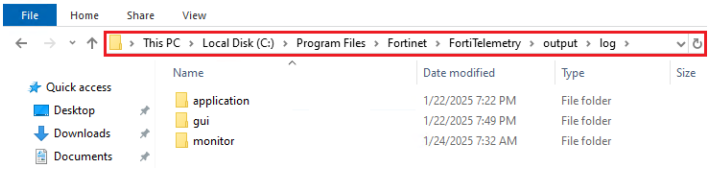
- FortiTelemetry agent version and serial number.
- FortiTelemetry Controller (FortiGate) information, including the name, version, serial number and connected status.



Viewing agent logs

By default, the install directory is `C:\Program Files\Fortinet\FortiTelemetry`.

Logs related to the operation of the FortiTelemetry agent and the monitoring tasks can be located in the `output\log` directory inside the install directory.



FortiTelemetry Controller

The FortiTelemetry Controller can be any on-premise hardware-based FortiGate running a compatible FortiOS version. The FortiTelemetry agents must be connected to the on-premise FortiGate using the same local area network (LAN).

The FortiGate acting as FortiTelemetry Controller discovers, authorizes, and manages all agents using the FortiOS *Security Profile* and *Firewall Policy* framework.

Using the FortiTelemetry Controller, you can view and configure FortiTelemetry information including the supported predefined applications, telemetry profiles, and policies that enable FortiTelemetry operation.

For more information, see:

Predefined applications

FortiTelemetry agents monitor the application experience for SaaS applications.

The following predefined SaaS applications are available on FortiOS 7.6.4:

- Adobe
- Atlassian Cloud
- Dropbox
- Elastic Search
- Google Docs
- Google Drive
- Google Maps
- Google Search
- Go To Meeting
- Microsoft 365
- Microsoft SharePoint
- Microsoft Teams
- Sales Force
- Slack
- Twilio
- Webex
- Yahoo
- Zendesk
- Zoom

On the FortiGate acting as FortiTelemetry Controller, you can use the `config telemetry-controller application predefine` CLI command to view and configure these applications and their properties.

For example:

```
config telemetry-controller application predefine
  show
    config telemetry-controller application predefine
      edit "Microsoft.Teams"
      next
      edit "Microsoft.365"
```

```
        next
        edit "Slack"
        next
        edit "Google.Maps"
        next
        edit "Webex"
        next
        edit "Google.Drive"
        next
        edit "Zoom"
        next
        edit "Microsoft.SharePoint"
        next
        edit "Google.Search"
        next
        edit "Google.Docs"
        next
        edit "GoToMeeting"
        next
        edit "Dropbox"
        next
        edit "Atlassian.Cloud"
        next
        edit "Zendesk"
        next
        edit "Salesforce"
        next
        edit "Adobe"
        next
        edit "Yahoo"
        next
        edit "Twilio"
        next
        edit "ElasticSearch"
        next
    end
```

Application upgrade

Predefined applications are packaged as part of the FortiOS image and are upgraded with new FortiOS releases. In the future, additional predefined applications will be made available through the FortiGuard service to allow for more frequent updates.

Telemetry profiles

On the FortiGate acting as FortiTelemetry Controller, you can create telemetry profiles.

Telemetry profiles are used to inform the FortiTelemetry agent(s) what predefined applications to monitor.

By default, there is one telemetry profile available on FortiOS. Additional profiles can be created by administrators.

Telemetry profiles must be added to a Firewall policy in order to create a telemetry policy. See FortiTelemetry policies on page 38.

This chapter includes the following information:

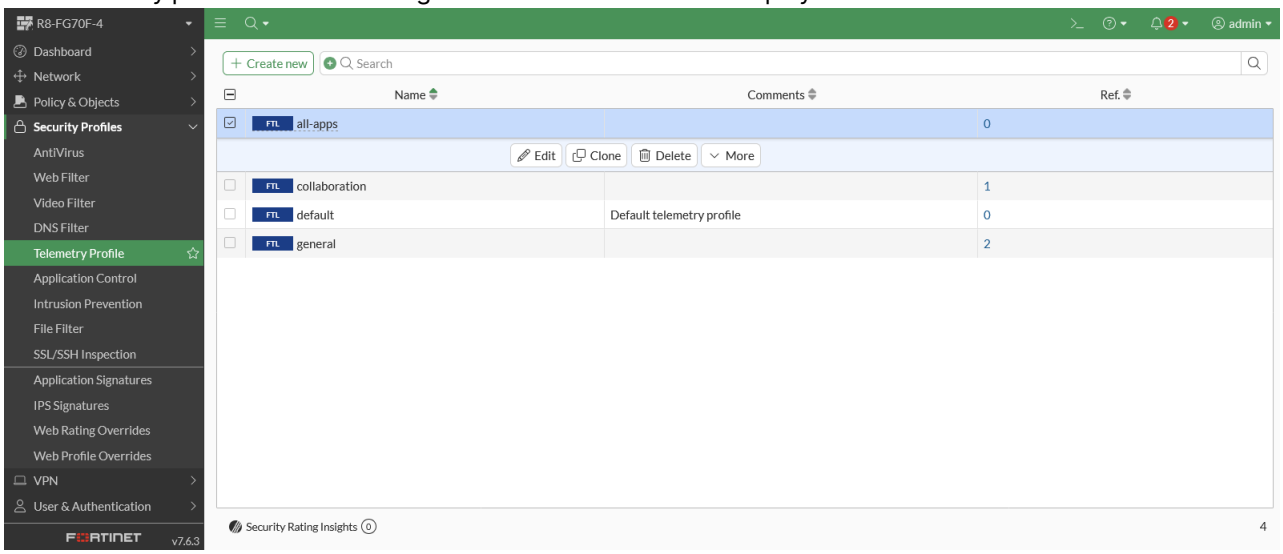
Viewing telemetry profiles

Telemetry profiles can be viewed on the FortiGate acting as FortiTelemetry Controller by navigating to *Security Profiles > Telemetry Profile*.

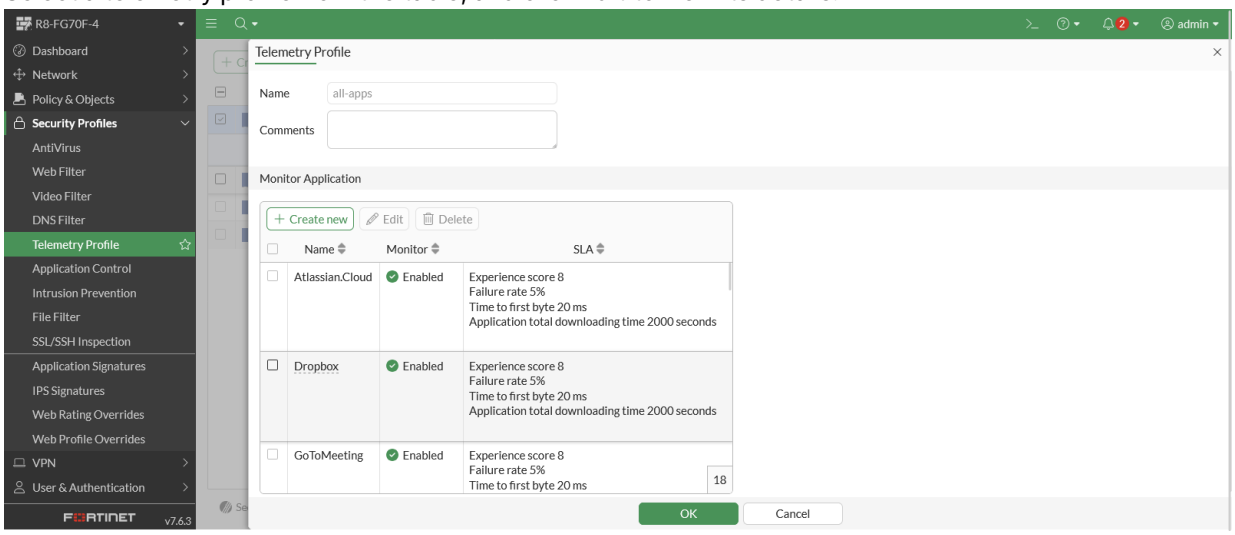
Example: Viewing telemetry profiles

To view the telemetry profile in the GUI:

1. Go to *Security Profiles > Telemetry Profile*.
   The telemetry profiles that are configured on this FortiGate are displayed.



2. Select a telemetry profile from the table, and click *Edit* to view its details.



To view the telemetry profile in the CLI:

1. In the FortiGate CLI, enter the following command :

```
config telemetry-controller profile
       show
```

Details of telemetry-controller profiles found on the FortiGate are displayed.
For example:

```
config telemetry-controller profile
  show
    config telemetry-controller profile
      edit "default"
        set comment "Default telemetry profile"
        config application
          edit 1
            set app-name "Google.Search"
            set latency-threshold 50
            set jitter-threshold 30
            set ttfb-threshold 50
            set atdt-threshold 3000
            set tcp-rtt-threshold 50
            set dns-time-threshold 2000
            set tls-time-threshold 2000
          next
          edit 2
            set app-name "Microsoft.365"
            set latency-threshold 50
            set jitter-threshold 30
            set ttfb-threshold 50
            set atdt-threshold 3000
            set tcp-rtt-threshold 50
            set dns-time-threshold 2000
```

```
            set tls-time-threshold 2000
        next
        edit 3
            set app-name "Salesforce"
            set interval 420000
            set latency-threshold 50
            set jitter-threshold 30
            set ttfb-threshold 50
            set atdt-threshold 3000
            set tcp-rtt-threshold 50
            set dns-time-threshold 2000
            set tls-time-threshold 2000
        next
        edit 4
            set app-name "Atlassian.Cloud"
        next
```

Creating and editing telemetry profiles

Telemetry profiles are created on the FortiGate acting as FortiTelemetry Controller. Telemetry profiles can be configured using the FortiOS GUI or CLI.

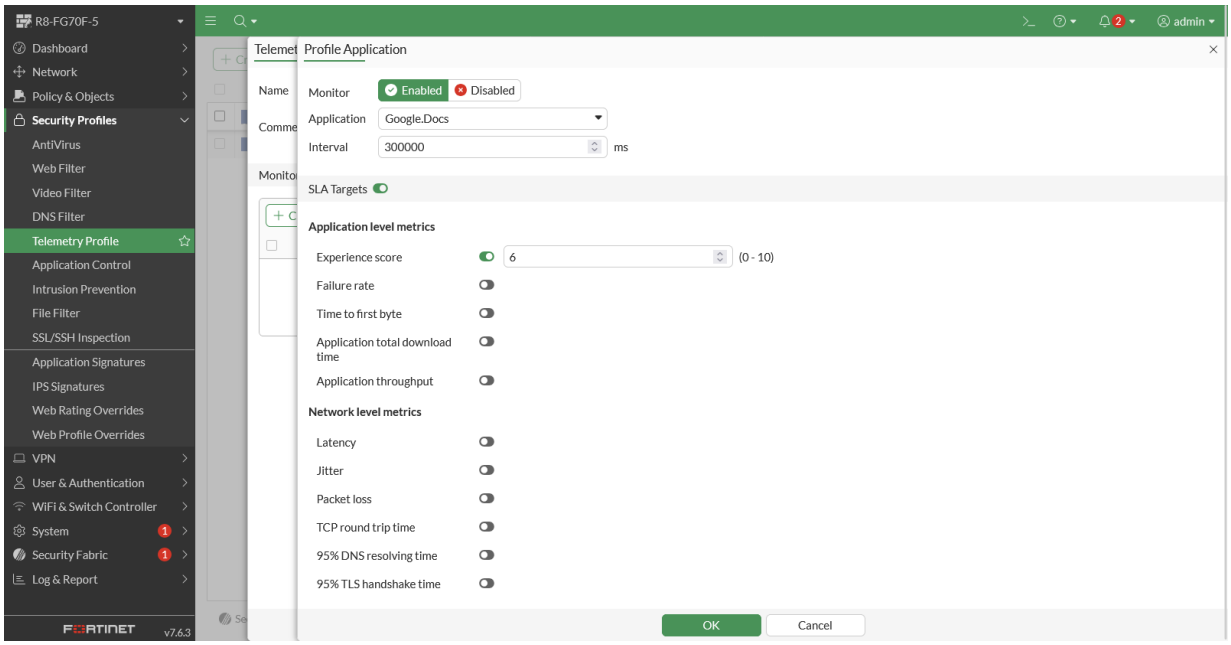
For full instructions on creating and editing telemetry profiles, see the FortiOS Administration Guide.

Example: Creating a telemetry profile

The following examples demonstrate how to configure a telemetry profile on a FortiGate (firmware version 7.6.3) acting as FortiTelemetry Controller.

To configure a telemetry profile to monitor Google Docs:

1. Go to *Security Profiles* > *Telemetry Profile*.
2. Click *Create New*.
3. Enter a name and optional comment for the profile.
4. In the *Monitored Applications* section, add applications to the profile:
   a. Click *Create New* to add a profile application.
   b. Choose the *Monitor* status for the application as *Enabled*.
   c. Select the *Google.Docs* predefined application from the *Applications* dropdown. See Predefined applications on page 28.
   d. Optionally, you can enable *SLA Targets* to configure the SLA threshold values for the selected application. SLA targets are optional and can be disabled. For more information on each threshold value, seeTelemetry profile SLA targets on page 33



5. Click *OK* to save the monitored application.
6. Click *OK* to save the telemetry profile.

To create a telemetry profile in the FortiGate CLI:

1. In the FortiGate CLI, enter the following command :

```
config telemetry-controller profile
       edit <profile name>
              config application
```

For example:

```
config telemetry-controller profile
  edit my-tlm-profile
    new entry 'my-tlm-profile' added
```

Telemetry profile SLA targets

Each telemetry profile includes one or more predefined applications, and can set SLA threshold values for the metrics that are monitored for each application. SLA threshold values are optionally and are not required when configuring the telemetry profile.

Below is information about the different SLA threshold values that are configurable in a telemetry profile.

Setting	Description
Application level metrics	

Setting		Description
	Time to first byte	Time to first byte threshold monitor requests in milliseconds (ms). CLI example: `set ttfb-threshold 50`
	Application total downloading time	Application total download time threshold for monitoring HTTP requests in milliseconds (ms). CLI example: `set atdt-threshold 3000`
Network level metrics		
	Latency	Average latency threshold for network probes in milliseconds (ms). CLI example: `set latency-threshold 50`
	Jitter	Jitter threshold for network probes in milliseconds (ms). CLI example: `set jitter-threshold 30`
	Packet loss	Packet-loss threshold for network probes as a percentage. CLI example: `set packet-loss threshold 5`
	TCP round trip time	TCP round trip time threshold for monitoring HTTP requests in milliseconds (ms). CLI example: `set tcp-rtt-threshold 50`
	DNS resolving time	DNS resolving time threshold for monitoring HTTP requests in milliseconds. CLI example: `set dns-time-threshold 2000`
	Application throughput	The throughput threshold for monitoring HTTP requests in megabytes (MBps). CLI example: `set app-throughput 2`
	TLS	TLS time threshold. CLI example: `set tls-time-threshold 2000`

FortiTelemetry addresses and address groups

Telemetry firewall addresses and address groups are used to define and manage telemetry agents, allowing both individual telemetry addresses and grouped telemetry address objects to be used in telemetry polices, improving clarity, policy targeting, and operational efficiency.

Telemetry firewall addresses use the *telemetry* sub-type as well as an `agent-id` attribute which specifies the serial number of the FortiTelemetry agent (for example: `FT100GTK240000001`).

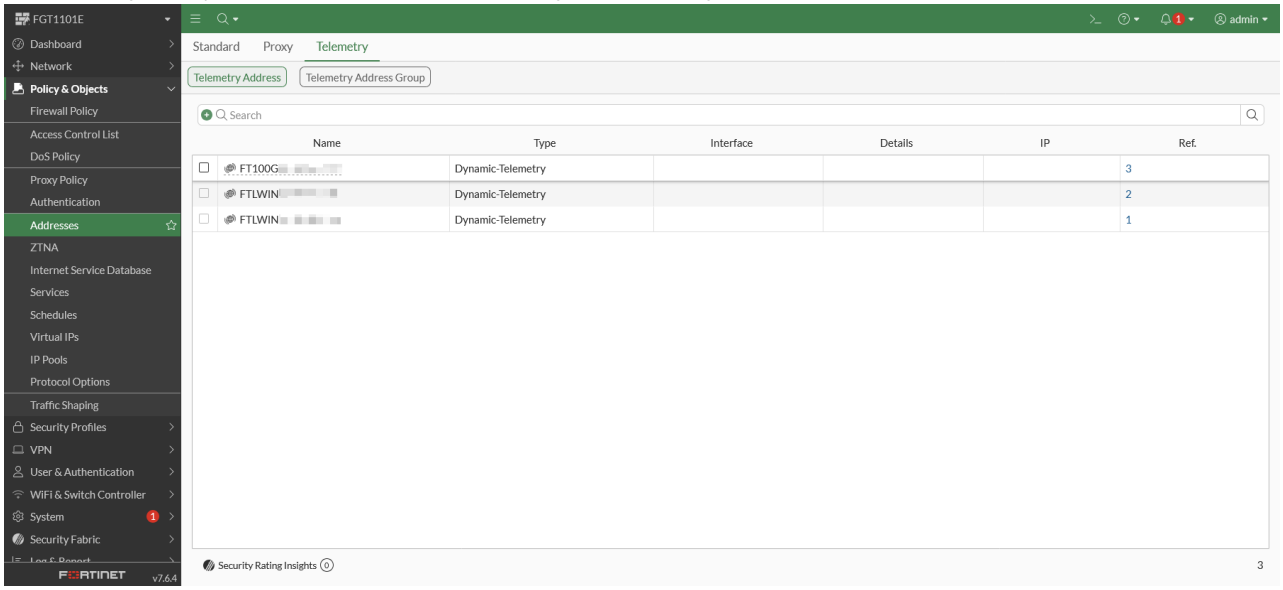
For more information on adding telemetry addresses and address groups to a policy, see FortiTelemetry policies on page 38.

Viewing telemetry addresses

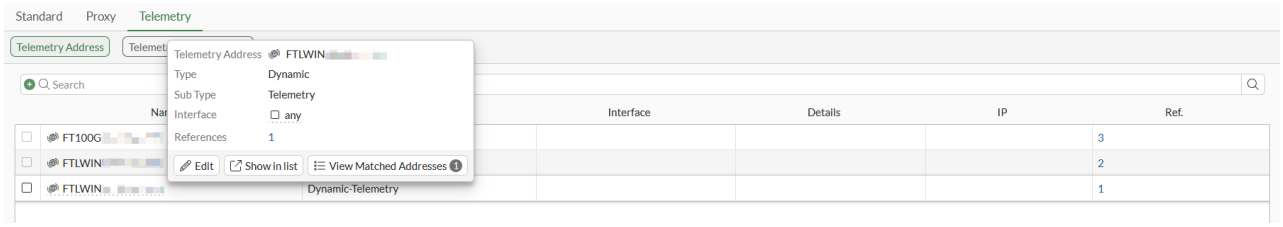
After a FortiTelemetry agent is authorized in FortiOS, a telemetry address is automatically created. The name of the telemetry address is the serial number of the FortiTelemetry agent. You can view the address in the GUI or CLI.

To view a telemetry address in the GUI:

1. Go to *Policy & Objects* > *Addresses* > *Telemetry* > *Telemetry Address*.



2. Hover over the address name, and click the *View Matched Addresses* button.



The *Resolved Addresses* pane is displayed and shows the IP address (`192.168.14.8`) of the FortiTelemetry agent.

To view a telemetry address in the CLI:

1. View the telemetry address.

   The type is dynamic, the `sub-type` is `telemetry`, and the `agent-id` is the serial number of the FortiTelemetry agent:

```
show full firewall address FTLWIN5798911362
config firewall address
    edit "FTLWIN5798911362"
        set uuid 8e6e691a-4ba6-51f0-5a93-9e03e58c5a19
        set type dynamic
        set sub-type telemetry
        set comment ''
        set associated-interface ''
        set color 0
        set fabric-object disable
        set agent-id "FTLWIN5798911362"
    next
end
```

2. View the IP address (`10.1.100.106`) of the FortiTelemetry agent.

```
# diagnose firewall dynamic address FTLWIN5798911362
CMDB name: FTLWIN5798911362
FTLWIN5798911362: ID(250)
        ADDR(10.1.100.106)
Total IP dynamic range blocks: 0.
Total IP dynamic addresses: 1.
```

Creating a telemetry address group

You can create a telemetry address group in the GUI or CLI.

A group named TELEMETRY is available by default. Telemetry addresses are automatically added to the TELEMETRY group when they are created.

To enable/disable use of the default TELEMETRY group:

```
config telemetry-controller global
    set auto-group-telemetry-addr {enable | disable}
end
```

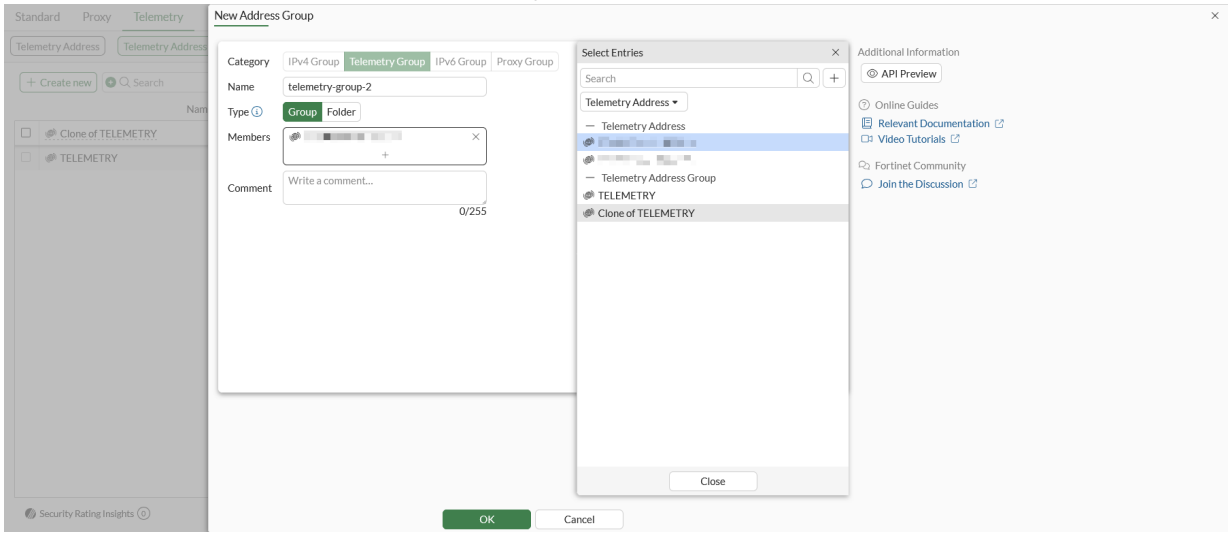
```
enable - Automatically add telemetry address to the default addrgrp TELEMETRY.
disable - Do not automatically add telemetry address to the default addrgrp TELEMETRY.
```

To create a telemetry address group in the GUI:

1. Go to *Policy & Objects* > *Addresses* > *Telemetry* > *Telemetry Address Group*.

2. Click the *Create New* button. The *New Address Group* pane is displayed.
3. Set the following options and click *OK*.

- Set *Name* to a unique name.
- Set *Type* to *Group*.
- Click *Members* to select one or more telemetry addresses.



The telemetry group contains the selected telemetry addresses.

To create a telemetry address group in the CLI:

1. View a telemetry address group, for example, `Telemetry-group-1`.
   The type can be default or folder, and the category is telemetry:

```
show full firewall addrgrp Telemetry-group-1
config firewall addrgrp
    edit "Telemetry-group-1"
        set type default
        set category telemetry
        set member "FT100GTK24000007"
        set comment ''
        set uuid 4f197cee-4d65-51f0-2942-8214af708a17
        set exclude disable
        set color 0
        set fabric-object disable
    next
end
```

2. Create a new telemetry address group:

```
config firewall addrgrp
    edit Telemetry-group-2
        set category telemetry
        set member FTLWIN5798911362
    next
end
```

FortiTelemetry policies

A firewall policy must be created on the FortiGate FortiTelemetry Controller to allow it to send monitoring tasks to the agents.

The telemetry firewall policy has type set to *Telemetry*, source set to telemetry agents, and a telemetry profile selected. FortiTelemetry Controller uses the following firewall policy configuration elements to automatically create a monitoring task for agents:

- FortiTelemetry agent from the policy source
- Applications to monitor from the telemetry profile

FortiOS automatically places telemetry policies at the top of the policy table. This position allows the policy to function correctly.

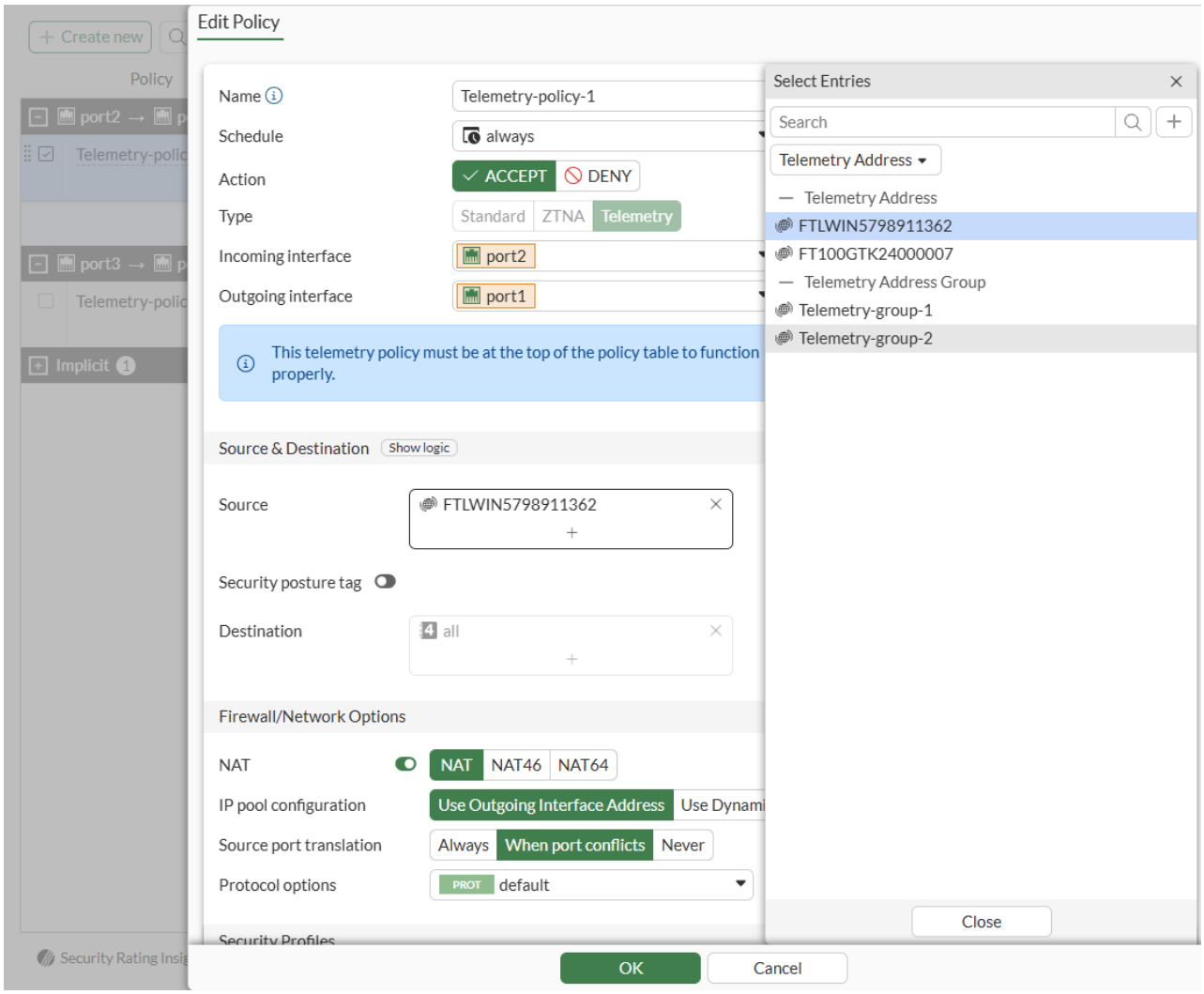
For full instructions on creating FortiTelemetry policies, see the FortiOS Administration Guide.

Example: Creating a telemetry policy

To create a FortiTelemetry policy:

1. Go to *Policy & Objects* > *Firewall Policy*.
2. Click *Create New* to create a new firewall policy.
3. Configure the policy with the following settings:

Name	Enter a name for the policy.
Action	Set the action to *Accept* to allow sending monitoring tasks to the agents
Type	Select *Telemetry* as the policy type.
Telemetry	Select a telemetry profile configured on the FortiGate.
Incoming Interface	Choose the FortiGate port that is used to connect to the FortiTelemetry agent.
Outgoing Interface	Select the outgoing interface.
Source	Select the FortiTelemetry firewall address or address that will be using this policy. Telemetry firewall addresses are automatically created when the agents connect to the FortiTelemetry Controller, and the name matches the serial numbers of the FortiTelemetry agents. See FortiTelemetry addresses and address groups on page 34.



4. Click *OK* to save the policy.

To configure a FortiTelemetry policy in the CLI:

1. Use the following commands to configure a telemetry policy in the CLI:

```
config firewall policy
  edit "3"
    show
      config firewall policy
        edit 3
          set name "FTLPolicyWin136"
          set uuid 2a86e78c-d9c9-51ef-33d5-6ddd81cfcc63
          set srcintf "port3"
          set dstintf "port1"
          set action accept
          set srcaddr "FTLWIN4665500001"
          set dstaddr "all"
          set schedule "always"
```

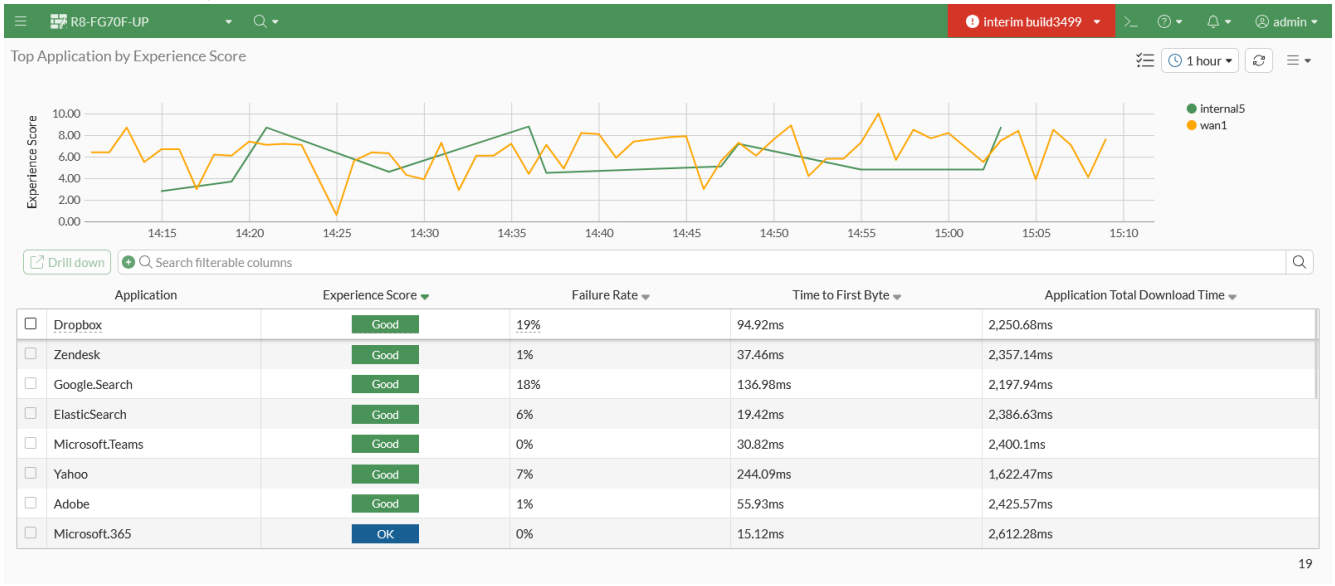
```
        set service "ALL"
        set telemetry-profile "default"
        set logtraffic all
        set nat enable
        set comments "FTLPolicyWin136"
      next
    end
```

Telemetry monitor

The FortiTelemetry monitor lets you view telemetry information from a FortiTelemetry Controller and its agents.

When VDOMs are enabled on the FortiTelemetry Controller, the Telemetry monitor returns data for current VDOM when the FortiTelemetry-100G agent and FortiTelemetry Windows agent are version 6.4 or later.

Add FortiTelemetry monitors to view and monitor data collected by the agents and analyzed by FortiTelemetry Cloud. After FortiTelemetry Cloud analyzes the data, it returns to the FortiTelemetry Controller an application experience score and an application failure rate along with other network telemetry metrics, which you can view in the FortiTelemetry monitor.



To create a FortiTelemetry monitor:

1. On the FortiTelemetry Controller (FortiGate), go to *Dashboard* and click the *Add Monitor* button. The Add Monitor window appears.
2. Under the *Security Fabric* category, select *FortiTelemetry*. The *Add FortiTelemetry as Standalone Dashboard* window appears.
3. Configure the following:

Name	Enter a name for the dashboard.

FortiGate	By default, the FortiTelemetry Controller is selected.
Source	Choose a source for the dashboard. The *FortiView Telemetry* monitor includes views based on the following sources: • Application • Agent • Source Interface • Destination Interface • Profiles • Policy
Time Period	Choose a time period for metrics included in the dashboard from 1 hour to 7 days.
Sort by	Select one of the following metrics to use as the default sorting for the dashboard: • Experience score • Failure Rate • Time to First Byte • Application Total Download Time • Latency • Jitter • Packet Loss • TCP Round Trip Time • 95% DNS Resolving Time • 95% TLS Handshake Time • Throughput

4. Click *OK* to create the dashboard.

For more information on using FortiTelemetry monitors, see Adding FortiTelemetry Monitors in the FortiGate/FortiOS Administration Guide.

The *FortiView Telemetry* monitor is not available by default. You can add monitors to the tree menu by clicking the *Add Monitor (+)* button and selecting *FortiTelemetry*. For more information, see Adding FortiView Monitors.

FortiTelemetry event logs

When enabled on the FortiTelemetry Controller, the following events for FortiTelemetry are captured in the FortiOS system event log:

- FortiTelemetry agent discovered, online, or offline
- FortiTelemetry agent authorized, unauthorized, rejected, or deleted
- FortiGate connected to or disconnected from FortiTelemetry cloud server

- Telemetry tasks pushed to FortiTelemetry agents

To enable telemetry event logging:

```
config log eventfilter
    set telemetry enable
end
```

Appendix A - Config CLI commands

This topic includes information about the commands that can be used to configure FortiTelemetry in the FortiGate CLI, including `config system global`, `config system interface`, `config telemetry-controller agent`, `config telemetry-controller agent-profile`, `config telemetry controller global`, and `config firewall address`, `config firewall addrgrp`.

config system global

Parameter	Description	Type	Size	Default
`telemetry-controller`	Enable/disable FortiTelemetry Controller.	option	-	enable
`telemetry-data-port`	Data port for FortiTelemetry.	integer	Minimum value: 1024 Maximum value: 49150	35246

config system interface

Parameter	Option	Description
`allowaccess`	fabric	Permit FortiTelemetry Security Fabric connection access
`telemetry-discover`	enable	Enable automatic registration of unknown FortiTelemetry agents.
	disable	Disable automatic registration of unknown FortiTelemetry agents.
`auto-auth-extension-device`	enable	Enable automatic authorization of FortiTelemetry agent.
	disable	Disable automatic authorization of FortiTelemetry agent.

config telemetry-controller agent

Configure FortiTelemetry agents.

```
config telemetry-controller agent
Description: Configure FortiTelemetry agents.
  edit < agentid>
    set comment {string}
    set alias {string}
    set authz [rejected|authorized|unauthorized]
    set agent-profile {string}
  next
end
```

Parameter	Description	Type	Size	Default
agentid	FortiTelemetry agent ID that begins with the prefix FT100G or FTLWIN.	string	16	-
comment	Comment	string	Maximum value: 255	-
alias	Alias	string	Maximum value: 35	-
authz	Authorization status of FortiTelemetry agent.	option	-	unauthorized
agent-profile	Name of FortiTelemetry agent profile.	string	Maximum value: 35	-

config telemetry-controller agent-profile

Configure FortiTelemetry agent profiles.

```
config telemetry-controller agent
Description: Configure FortiTelemetry agent profiles.
  edit <name>
    set model [FTL100G|WINDOWS]
    set comment {string}
  next
end
```

Parameter	Description	Type	Size	Default
name	Name of the FortiTelemetry agent profile.	string	Maximum value: 35	-
comment	Comment	string	Maximum value: 255	-
model	Model of the FortiTelemetry agent.	option	-	FTL100G
	Option	**Description**		
	FTL100G	Model is FTL-100G.		
	WINDOWS	Model is Windows.		

config telemetry-controller global

Configure FortiTelemetry global settings.

```
config telemetry-controller global
Description: Configure FortiTelemetry global settings.
  set retry-interval {integer}
  set telemetry-certificate {string}
  set region [global|usa]
  set server {string}
  set auto-group-telemetry-addr {enable| disable}
end
```

Parameter	Description	Type	Size	Default
retry-interval	The interval time between failed setup attempts to establish connection with the cloud.	integer	Minimum value: 1 Maximum value: 999	300
telemetry-ca-certificate	Name of the CA certificate which is used to verify the telemetry agent certificate.	string	Maximum value: 79	-
set auto-group-telemetry-addr	Enable/disable automatically adding the telemetry address to the default addrgrp TELEMETRY.	option	-	enable
region	Region of FortiTelemetry Cloud.		-	-
	Option	**Description**		
	usa	Set USA as region.		
	global	Set global as region.		
server	FQDN of FortiTelemetry Cloud.	string	-	-

config log eventfilter

Configure FortiTelemetry log eventfilter settings.

```
config log eventfilter
    set telemetry enable/disable
end
```

Parameter	Option	Description
telemetry	enable	Enable FortiTelemetry in the logging event filter.
	disable	Disable FortiTelemetry in the logging event filter.

config utmgrp-permission

Configure access profile permissions.

```
config system accprofile
    edit <name>
        set utmgrp custom
        config utmgrp-permission
            set telemetry [none|read|read-write]
        end
    next
end
```

Parameter	Option	Description
telemetry	none	No access.
	read	Read access.
	read-write	Read/write access.

config firewall address

View telemetry address objects.

```
config firewall address
    edit <FortiTelemetry agent serial number>
        set type dynamic
        set sub-type {telemetry}
        set agent-id <FortiTelemetry agent serial number>
    next
end
```

Parameter	Description	Type	Size	Default
sub-type	Telemetry address.	option	-	
agent-id	FortiTelemetry agent serial number	string	-	

config firewall addrgrp

Configure telemetry address groups.

```
config firewall addrgrp
    edit "telemetry-group"
        set category telemetry
        set member FT100GTK24000001
    next
end
```

Parameter	Description	Type	Size	Default
category	Telemetry. Members must be telemetry groups or telemetry addresses. Can be used to determine telemetry policy.	option	-	

Appendix B - Get and Diagnose commands

FortiTelemetry is a solution for monitoring the health of applications and network path as experienced from a customer environment. This is done by executing monitor tasks and network probes using FortiTelemetry agents that are connected to a FortiGate.

There are several configurations on FortiGate for FortiTelemetry. This topic provides information about the available `Get` and `Diagnose` commands that can be used in FortiOS that relate to FortiTelemetry.

The following FortiGate CLI commands can be used to view different properties related to FortiTelemetry.

get telemetry-controller agent

Lists the FortiTelemetry agents that have been discovered.

For example:

```
get telemetry-controller agent
  == [ FTLWIN5631300001 ]
  agent-id: FTLWIN5631300001
  == [ FTLWIN5170500002 ]
  agent-id: FTLWIN5170500002
  == [ FT100GTK24000003 ]
  agent-id: FT100GTK24000003
```

get telemetry-controller agent-status

Shows the status for the discovered FortiTelemetry agents. You can narrow down further by providing a specific agent.

For example:

```
get telemetry-controller agent-status
  FT100GTK24000004:
    alias            :
    model            : FTL100G
    vdom             : root
    capwap state     : idle
  FTLWIN5170500002:
    alias            :
    model            : WINDOWS
    vdom             : root
    capwap state     : idle
  FTLWIN5631300001:
    alias            :
    model            : WINDOWS
    software version : 10.0.19045.5371 Build 19045.5371-7.6.3.0005
```

```
    vdom             : root
    capwap state     : run
    join time        : Thu Feb 06 15:57:59 PST 2025
    session id       : 0xbea93583486372f239fb6bb0000000
    interface        : port3
    ipv4 addr        : 10.200.11.100
    port             : 56908
    local ipv4 addr  : 10.200.11.1

get telemetry-controller agent-status FTLWIN5170500002
  FTLWIN5170500002:
    alias            :
    model            : WINDOWS
    vdom             : root
    capwap state     : idle
```

get telemetry-controller agent-profile

Lists the FortiTelemetry agent profiles (currently only 'Auto-FTL100G' and 'Auto-WINDOWS').

For example:

```
get telemetry-controller agent-profile
  == [ Auto-WINDOWS ]
  name: Auto-WINDOWS
  == [ Auto-FTL100G ]
  name: Auto-FTL100G
  auto-2-fg1 (Interim)#
```

get telemetry-controller agent-task

Shows the tasks for the discovered FortiTelemetry agent. You can narrow down further by providing a specific agent.

For example:

```
   get telemetry-controller agent-task
   ************************
   ID : "FT100GTK24000004@Google.Docs-333"
   Update Time : 2025-02-03 12:03:35
   Monitor ID Seed : 1738613015
   Monitor Info :
      Interval : 300000
   Agent Info :
      Agent ID : "FT100GTK24000004"
      Selector Type : dedicated
   Application Info :
      App Name : "Google.Docs"
      App Version : "1.0"
   Policy Info :
      Policy ID : 333
      Profile Name : "default"
      Source Interface : "port3"
```

```
   Destination Interface : "virtual-wan-link"
Status : Valid
Sync Info :
   Action : ADD
   Status : In Progress
   Last Sync Time : 2025-02-03 12:29:22
   Last Sync Result : Success
************************
ID : "FT100GTK24000004@Microsoft.365-333"
Update Time : 2025-02-03 12:03:36
Monitor ID Seed : 1738613016
Monitor Info :
   Interval : 300000
Agent Info :
   Agent ID : "FT100GTK24000004"
   Selector Type : dedicated
Application Info :
   App Name : "Microsoft.365"
   App Version : "1.0"
Policy Info :
   Policy ID : 333
   Profile Name : "default"
   Source Interface : "port3"
   Destination Interface : "virtual-wan-link"
Status : Valid
Sync Info :
   Action : ADD
   Status : In Progress
   Last Sync Time : 2025-02-03 12:29:22
   Last Sync Result : Success
************************
ID : "FT100GTK24000004@Salesforce-333"
Update Time : 2025-02-03 12:03:37
Monitor ID Seed : 1738613017
Monitor Info :
   Interval : 300000
Agent Info :
   Agent ID : "FT100GTK24000004"
   Selector Type : dedicated
Application Info :
   App Name : "Salesforce"
   App Version : "1.0"
Policy Info :
   Policy ID : 333
   Profile Name : "default"
   Source Interface : "port3"
   Destination Interface : "virtual-wan-link"
Status : Valid
Sync Info :
   Action : ADD
   Status : In Progress
   Last Sync Time : 2025-02-03 12:29:22
   Last Sync Result : Success

get telemetry-controller agent-task FTLWIN5631300001
```

```
***********************
ID : "FTLWIN5631300001@Google.Docs-333"
Update Time : 2025-02-03 12:03:38
Monitor ID Seed : 1738613018
Monitor Info :
   Interval : 300000
Agent Info :
   Agent ID : "FTLWIN5631300001"
   Selector Type : dedicated
Application Info :
   App Name : "Google.Docs"
   App Version : "1.0"
Policy Info :
   Policy ID : 333
   Profile Name : "default"
   Source Interface : "port3"
   Destination Interface : "virtual-wan-link"
Status : Valid
Sync Info :
   Action : ADD
   Status : Complete
   Last Sync Time : 2025-02-06 15:58:05
   Last Sync Result : Success
***********************
```

get telemetry-controller cloud-status

Shows the status for the FortiGate connection to the FortiTelemetry Cloud environment.

For example:

```
get telemetry-controller cloud-status
   Region : Default
   Domain : apigw.fortitelemetry.com
   IP Address : 154.52.20.52
   Gateway ID : 7f33b834-1e45-428c-9329-0000000000
   Log Settings :
      Output Address : ingest.fortitelemetry.com
      Output Type : kafka
      Kafka Topic : ftl_logs
      Service Output Address : ingest.fortitelemetry.com
      Service Output Type : kafka
      Service Kafka Topic : ftl_agents
      Certificate Subject : CN = 7f33b834-1e45-428c-9329-000000000
      Certificate Issuer : C = US, ST = CA, L = Sunnyvale, O = Fortinet, OU = Fortitelemetry,
            CN = Fortitelemetry_Intermediate_Prod, emailAddress = noreply@for
      tinet.com
      Certificate Valid From : 2025-02-01 00:04:10 GMT
      Certificate Valid To : 2035-01-30 00:04:20 GMT
      Certificate Fingerprint :
            57:AB:9E:2A:2D:6B:5A:C2:36:FF:A3:F5:B3:30:AB:01:9D:56:8F:C3:9D:C8:AE
      Sequence Number : d662c56ef8b6374a079ff6c1000000
   Report Settings :
      Query Address : apigw.fortitelemetry.com
```

```
        Sequence Number : 4a4bbb30c392c0002dc3b400000000
    Setup Status : Completed
    Cloud Connection : Not Connected
    Last Action : Setup
    Last Attempt : 2025-02-10 12:44:53
```

get telemetry-controller global

Shows the retry-interval for FortiGate connection attempt to FortiTelemetry Cloud and the ca-certificate used to validate agent certificates for client authentication during CAPWAP DTLS negotiation.

For example:

```
get telemetry-controller global
   region : global
   retry-interval : 1
   telemetry-ca-certificate: CA_Cert_1
```

diagnose debug application telemetryd 255

Shows the debug logs for the telemetry daemon on the FortiOS.

For example:

```
diagnose debug enable
diagnose debug application telemetryd 255
   Debug messages will be on for unlimited time
```

www.fortinet.com