



# Release Notes

FortiTelemetry Controller 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](mailto:techdoc@fortinet.com)



August 26, 2025

FortiTelemetry Controller 7.6.4 Release Notes

100-764-1187940-20250826

# TABLE OF CONTENTS

<b>Change log</b> .....	<b>4</b>
<b>Introduction and supported models</b> .....	<b>5</b>
Supported models .....	5
What's new .....	5
Dynamic telemetry firewall address type and telemetry address group .....	6
FortiTelemetry monitor includes support for VDOMs .....	6
Add FortiTelemetry access profile .....	6
Add system event log for FortiTelemetry .....	7
<b>Product integration and support</b> .....	<b>8</b>
FortiTelemetry Controller .....	8
Minimum system requirements .....	8
FortiTelemetry agents .....	8
<b>Known Issues</b> .....	<b>9</b>
<b>Resolved issues</b> .....	<b>10</b>

# Change log

Date	Change Description
2025-08-21	Initial release.
2025-08-26	Updated <a href="#">Product integration and support on page 8</a> .

# Introduction and supported models

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.

The FortiTelemetry solution is made up of a FortiGate hardware device acting as FortiTelemetry Controller and one or more FortiTelemetry agents, which continuously emulate, monitor, and detect performance metrics across SaaS applications without user involvement.

This release notes document provides information about FortiTelemetry Controller version 7.6.4.

## Supported models

FortiTelemetry Controller version 7.6.4 supports the following FortiTelemetry agent models:

<b>FortiTelemetry hardware-based agent</b>	FortiTelemetry-100G Agent
<b>FortiTelemetry software-based agent</b>	FortiTelemetry Windows Agent

For information about the agents, see the following release notes:

- [FortiTelemetry-100G Agent Release Notes](#)
- [FortiTelemetry Windows Agent Release Notes](#)

## What's new

FortiTelemetry Controller version 7.6.4 includes the following new features and enhancements:

- [Dynamic telemetry firewall address type and telemetry address group on page 6](#)
- [FortiTelemetry monitor includes support for VDOMs on page 6](#)
- [Add FortiTelemetry access profile on page 6](#)
- [Add system event log for FortiTelemetry on page 7](#)

## Dynamic telemetry firewall address type and telemetry address group

A new `telemetry` sub-type has been added to the dynamic firewall address type, along with a new `agent-id` attribute that directly references a FortiTelemetry agent. A new `telemetry` category has been added for firewall address groups.

Previously, FortiTelemetry agents were represented as firewall addresses of type `ipmask`. The firewall address name started with the reserved prefixes "FT100G" or "FTLWIN" and included the agent's serial number. The telemetry address could not be renamed, and the firewall addresses were dynamically updated by telemetryd.

This enhancement introduces a more structured and scalable way to define and manage telemetry agents, allowing both individual telemetry addresses and grouped telemetry address objects to be used in telemetry policies, improving clarity, policy targeting, and operational efficiency.

In addition, a static telemetry address group named `TELEMETRY` and `set auto-group-telemetry-addr enable` under `config telemetry-controller global` are available. When enabled, the telemetry address from each approved FortiTelemetry agent is automatically added to the `TELEMETRY` group. When a new telemetry policy is created in the GUI, the source address is automatically set to the `TELEMETRY` address group.

When upgrading from FortiTelemetry Controller 7.6.3 to 7.6.4:

- The `ipmask` firewall address is automatically migrated to the new address type. With FortiTelemetry Controller 7.6.4, telemetry firewall objects no longer require the "FT100G" or "FTLWIN" prefixes. Although the telemetry firewall objects can be renamed in the CLI, it is not recommended to rename the objects.
- All existing telemetry addresses are added to the `TELEMETRY` address group.

## FortiTelemetry monitor includes support for VDOMs

The Telemetry monitor returns data for current VDOM instead of all VDOMs. Requires 7.6.4 or later version of FortiTelemetry-100G agent and FortiTelemetry Windows agent.

## Add FortiTelemetry access profile

Access profile settings for system administrators now include options for FortiTelemetry.

You can configure system access profiles using the FortiTelemetry Controller (FortiGate) CLI.

**To configure FortiTelemetry in system access profiles:**

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

```
    next
end
```

## Add system event log for FortiTelemetry

A new attribute to enable/disable telemetry event logging has been added to the log event filter.

**To enable/disable telemetry in the log event filter:**

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

# Product integration and support

This section lists the integration and support of the FortiTelemetry Controller 7.6.4 and agents:

- [FortiTelemetry Controller on page 8](#)
- [FortiTelemetry agents on page 8](#)

## FortiTelemetry Controller

The FortiOS version of the FortiGate hardware device acting as the FortiTelemetry Controller determines the FortiTelemetry Controller version. For FortiTelemetry Controller version 7.6.4, the FortiOS version must be 7.6.4.

For more information about FortiOS 7.6.4, including special notices, product integration, and known and resolved issues, see the [FortiOS Release Notes](#).

## Minimum system requirements

The FortiTelemetry Controller must be a FortiGate hardware device with at least 4GB of memory.

## FortiTelemetry agents

See the [FortiTelemetry Agent Compatibility chart](#) for information about FortiTelemetry Controller support for all FortiTelemetry agents.

# Known Issues

There are no known issues identified in FortiTelemetry Controller version 7.6.4.

To inquire about a particular bug, please contact Fortinet support.

# Resolved issues

There are no resolved issues for the release of FortiTelemetry Controller **7.6.4**.

To inquire about a particular bug, please contact Fortinet support.



[www.fortinet.com](http://www.fortinet.com)

Copyright© 2025 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's Chief Legal Officer, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.