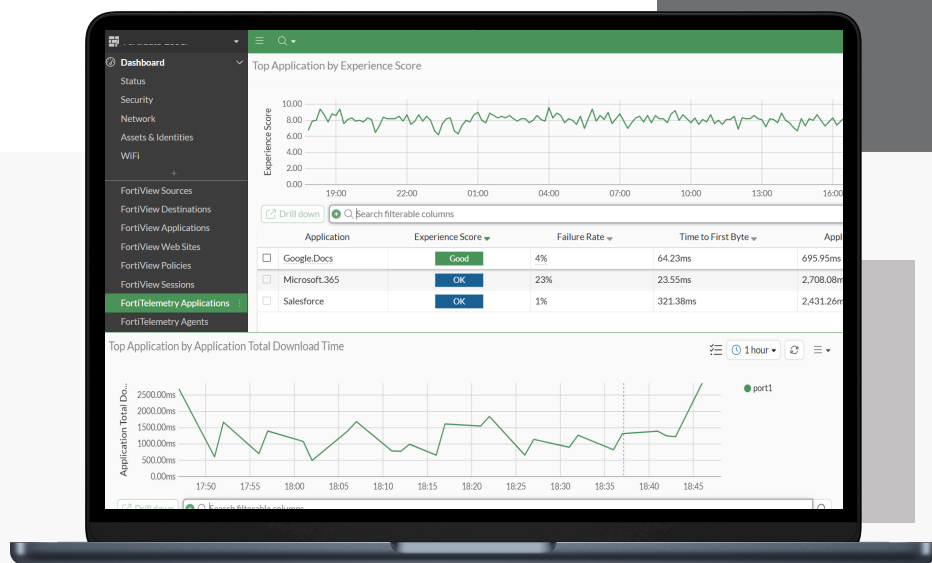


FortiTelemetry

Deep insights into application performance behaviors



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 and Application Failure Rate calculations
- Suitable for SD-WAN/SD-Branch sites, data centers, head offices, and any sites with a FortiGate
- Suitable for data centers, head offices, and SD-WAN/SD-Branch sites
- Measures underlay and overlay networks

Built-in telemetry profiles for business SaaS applications

With Software as a Service (SaaS) becoming as ubiquitous as essential utility and the recent transformative trends of AI as a Service (AlaaS), critical information about cloud-based application availability and performance is becoming more important in ensuring satisfactory user experiences.

FortiTelemetry, Fortinet's end-to-end user application telemetry monitoring, helps enterprises of any size improve SaaS application experience based on a comprehensive set of application-level and network-level performance metrics. FortiTelemetry includes on-premise FortiGate-integrated telemetry agents that continuously emulate, monitor, and detect performance metrics across SaaS applications.

FortiTelemetry collects real-time telemetry information from Top 10 Business SaaS applications using emulated user browsing activities to calculate different scores and network path information, so customers can understand each application and network behavior easily. With its built-in FortiGate Security Fabric integration, FortiTelemetry provides easy-to-implement powerful SaaS application visibility across your network and helps you identify bottlenecks for improved user productivity.

Key Benefits

- Site-specific, 24×7 user experience SaaS measurements
- Deep insights into application performance behaviors
- Quick root cause analysis of poor SaaS application performance
- Identify site network performance bottlenecks
- Improved SaaS user experience

More Information

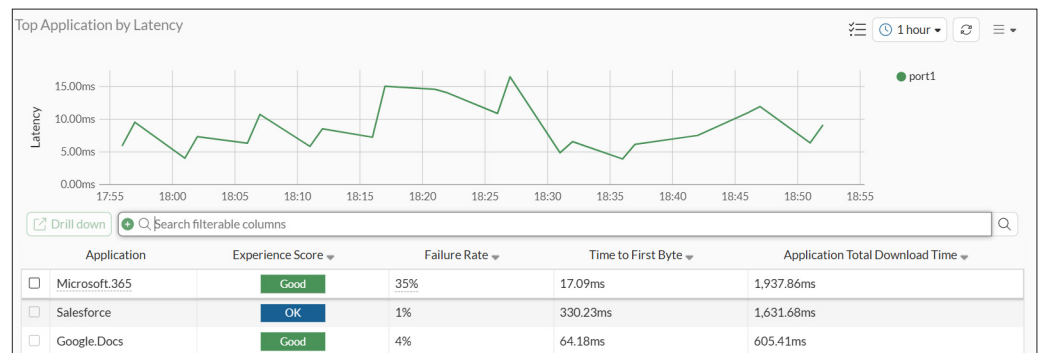
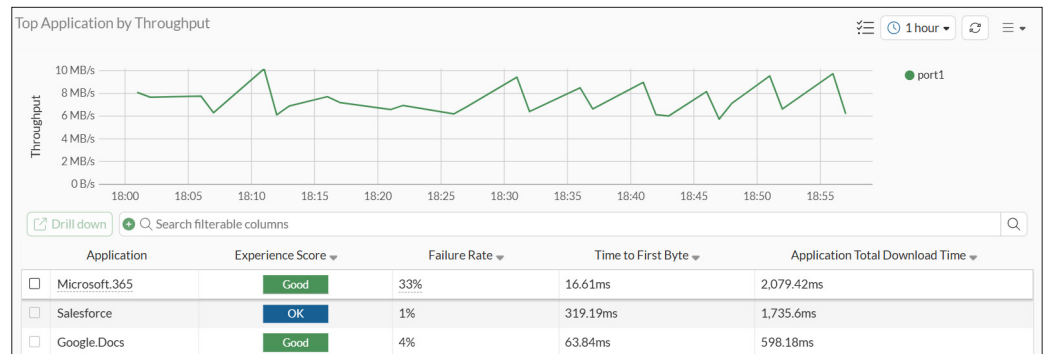
Additional information can be found at: [FortiTelemetry documentation site](#).

Metric Highlights

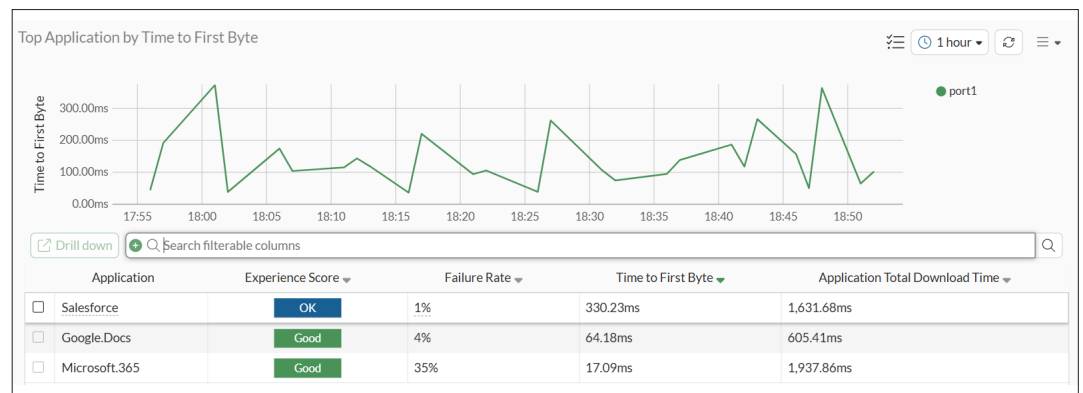
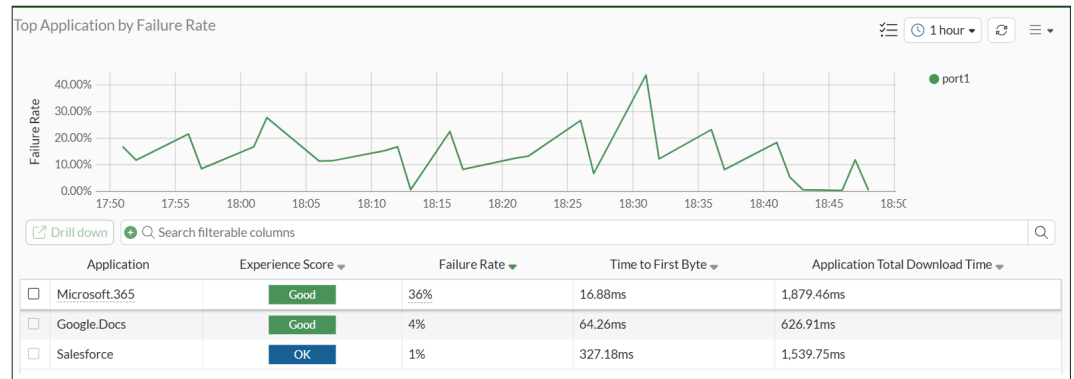
A key differentiator of FortiTelemetry lies in its ability to look inside each application session to collect real end user telemetry information 24×7 automatically without user interventions or involvements.

Using its hardware- or software-based agents, FortiTelemetry gathers and provides the following SaaS application telemetry metrics:

- Application-level:
 - Application Experience Score (AES)
 - Application Failure Rate (AFR)
 - Time to First Byte (TTFB)
 - Application Total Downloading Time (ATDT)
 - Throughput
- Network-level:
 - Latency
 - Jitter
 - Packet loss
 - TCP Round Trip Time (RTT)
 - 95th percentile DNS resolution time
 - 95th percentile TLS handshake time



With its own real-time streaming analytics engine running in the cloud, FortiTelemetry actively measures each SaaS application health, provides intelligent alerting when a threshold is breached, and predicts potential link quality deterioration using its AI algorithms. These application-focused telemetry metrics produce real actionable insights into SaaS applications, over and above traditional application performance monitoring (APM) solutions.



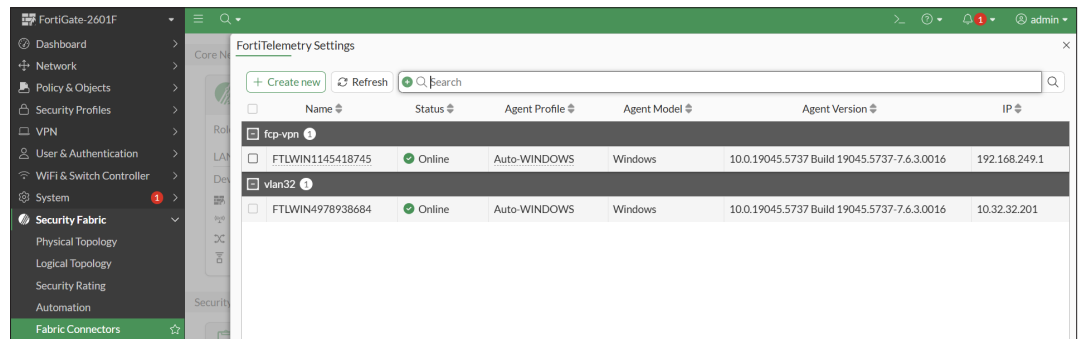
Agents

FortiTelemetry relies on on-premise telemetry agents, which can be hardware-based or software-based agents. There are two types of telemetry agents available:

- FortiTelemetry 100G Agent – A desktop size hardware appliance agent
- FortiTelemetry Windows Agent – A software agent running on Windows machine

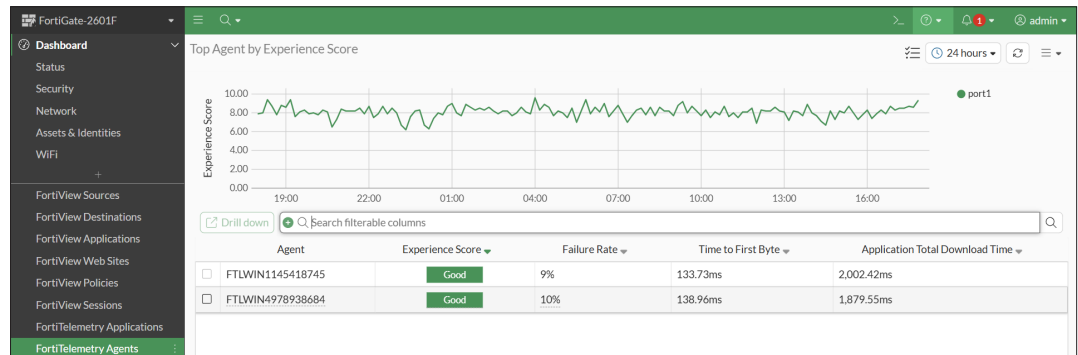
The telemetry agents simulate real users running the monitored SaaS applications on a web browser. The agents collect raw application-level and network-level statistics, turn them into meaningful telemetry metrics, and stream the metrics to FortiTelemetry Cloud for further analysis and retention.

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



The screenshot shows the FortiGate-2601F interface with the FortiTelemetry Settings page. The left sidebar shows the navigation menu with 'Fabric Connectors' selected. The main content area displays a table of agents with columns: Name, Status, Agent Profile, Agent Model, Agent Version, and IP. There are three agents listed: fcp-vpn, FTLWIN1145418745, and vlan32. All agents are 'Online' and use the 'Auto-WINDOWS' profile and 'Windows' model.

Name	Status	Agent Profile	Agent Model	Agent Version	IP
fcp-vpn	Online	Auto-WINDOWS	Windows	10.0.19045.5737 Build 19045.5737-7.6.3.0016	192.168.249.1
FTLWIN1145418745	Online	Auto-WINDOWS	Windows	10.0.19045.5737 Build 19045.5737-7.6.3.0016	10.32.32.201
FTLWIN4978938684	Online	Auto-WINDOWS	Windows	10.0.19045.5737 Build 19045.5737-7.6.3.0016	10.32.32.201



Controller

Any on-premise FortiGate, except for models lower than 7xF/7xG and FG-VM/Cloud, running a compatible FortiOS (7.6.3+) can act as a FortiTelemetry Controller. The FortiGate must be connected to the agents via the same local area network (LAN).

The telemetry controller discovers, authorizes, and manages all agents using the well-known FortiOS Security Profile and Firewall Policy framework.

Profile Application

Monitor
☒ Enabled
☐ Disabled

Application
Google.Docs

Interval
300000
ms

SLA Targets
☒

Application level metrics

Experience score
☒ 6 (0 - 10)

Failure rate
☒ 5 %

Time to first byte
☒ 200 ms

Application total download time
☒ 3000 ms

Application throughput
☒ 2 MB/s

Network level metrics

Latency
☒ 100 ms

Jitter
☒ 50 ms

Packet loss
☒ 5 %

TCP round trip time
☒ 100 ms

95% DNS resolving time
☒ 100 ms

95% TLS handshake time
☒ 200 ms

Cloud

FortiTelemetry Cloud receives, processes, analyzes, and retains streaming telemetry data sent by the agents. It calculates the Application Experience Score and Application Failure Rate of each application metric set.

FortiTelemetry Cloud provides this additional telemetry analytics to the FortiTelemetry Controller, which consumes and displays them as FortiView Telemetry.



Technical Specifications

Components	Description	Integrations
FortiTelemetry Hardware Agent – FTL-100G	Available in a desktop form factor, FTL-100G is hardware agent, actively emulates SaaS application browsing, collects their relevant telemetry statistics, and pushes them to FortiTelemetry Cloud.	FortiTelemetry Controller, FortiTelemetry Cloud
FortiTelemetry Software Agent – Windows	FTL-Windows is software agent running on a Windows machine (min. four CPUs and 8 GB RAM), actively emulates SaaS application browsing, collects their relevant telemetry statistics, and pushes them to FortiTelemetry Cloud.	FortiTelemetry Controller, FortiTelemetry Cloud
FortiTelemetry Controller	A built-in software component of a FortiGate, FortiTelemetry Controller automatically discovers and authorizes FortiTelemetry Agents via Zero Touch Provisioning, including manages them over a common Layer 2 network.	FortiTelemetry Agent, FortiTelemetry Cloud, FortiGuard
FortiTelemetry Cloud	A collection of cloud-native, big-data streaming infrastructure running on dedicated Fortinet Data Centers globally, FortiTelemetry Cloud receives, analyzes, and stores real-time application telemetry information from FortiTelemetry Agents.	FortiTelemetry Agent, FortiTelemetry Controller, FortiCare

Order Information

FortiTelemetry license is available as part of the SDWAN Underlay Monitoring Services bundle that includes FortiTelemetry Windows Software Agent.

FortiTelemetry 100G Hardware Agent is an appliance that needs to be ordered separately using the following SKUs.

Product	SKU	Description
SDWAN-Underlay Monitoring Services (Base)	FC-10-FGXXX-288-02-DD	SDWAN Underlay and Application Monitoring plus FortiTelemetry user license
FortiTelemetry-100G	FTL-100G	10 x GE RJ45 ports (including 7 x Internal Ports, 2 x WAN Ports, 1 x DMZ Port), 128 GB SSD onboard storage
	FC-10-T100G-247-02-DD	FortiCare Premium Support
	FC-10-T100G-284-02-DD	FortiCare Elite Support
	FC-10-T100G-204-02-DD	Upgrade FortiCare Premium to Elite (Require FortiCare Premium)

Visit <https://www.fortinet.com/resources/ordering-guides> for related ordering guides.

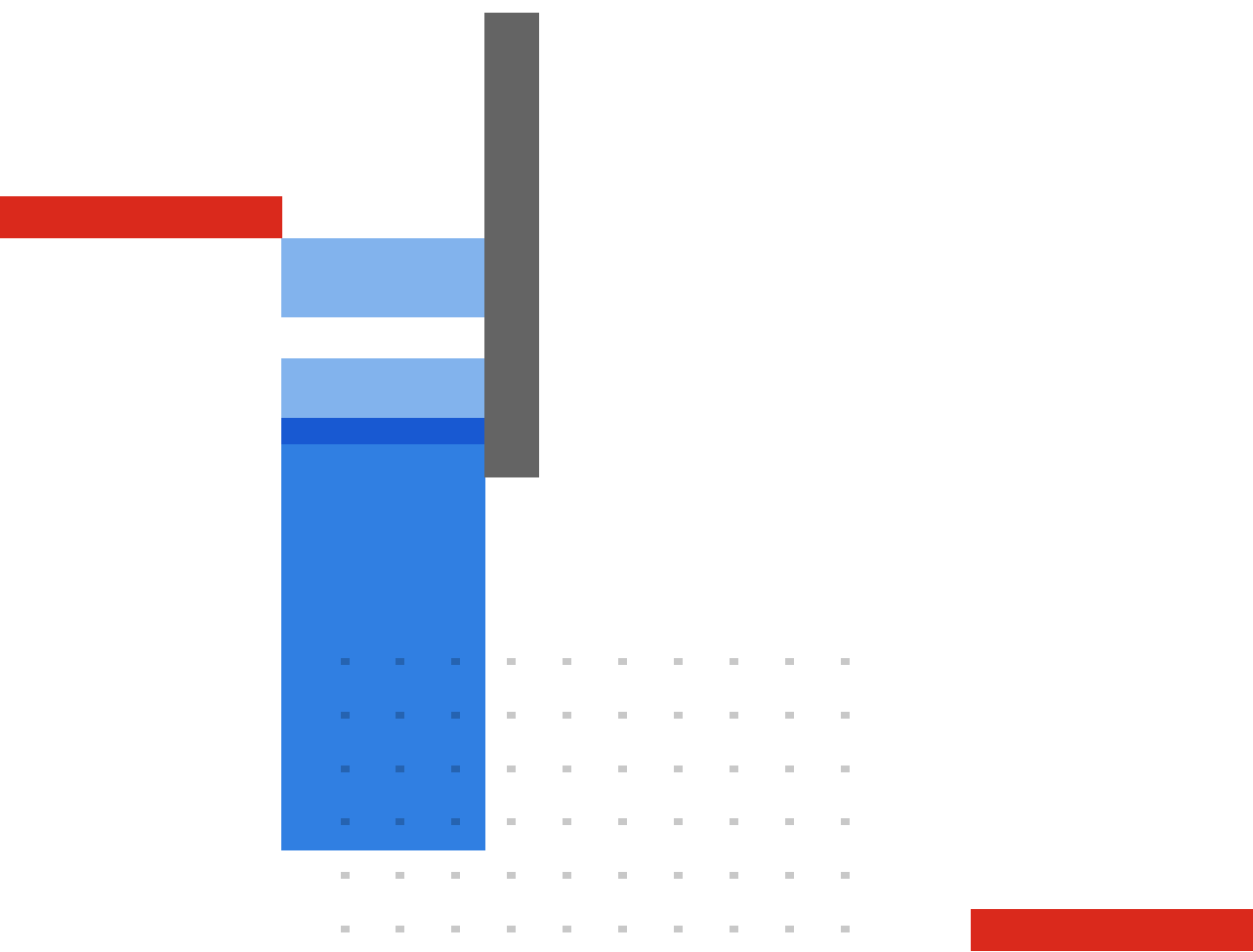
The number of agents that can be supported varies based on the FortiGate model acting as the FortiTelemetry Controller:

- FG-7xF/G to FG-10xF: up to 5 agents
- FG-12xG to 60xF: up to 10 agents
- FG-90xG to FG-100xF: up to 50 agents
- FG-180xF and beyond: up to 100 agents



Fortinet Corporate Social Responsibility Policy

Fortinet is committed to driving progress and sustainability for all through cybersecurity, with respect for human rights and ethical business practices, making possible a digital world you can always trust. You represent and warrant to Fortinet that you will not use Fortinet's products and services to engage in, or support in any way, violations or abuses of human rights, including those involving illegal censorship, surveillance, detention, or excessive use of force. Users of Fortinet products are required to comply with the [Fortinet EULA](#) and report any suspected violations of the EULA via the procedures outlined in the [Fortinet Whistleblower Policy](#).



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 SVP Legal and above, 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.