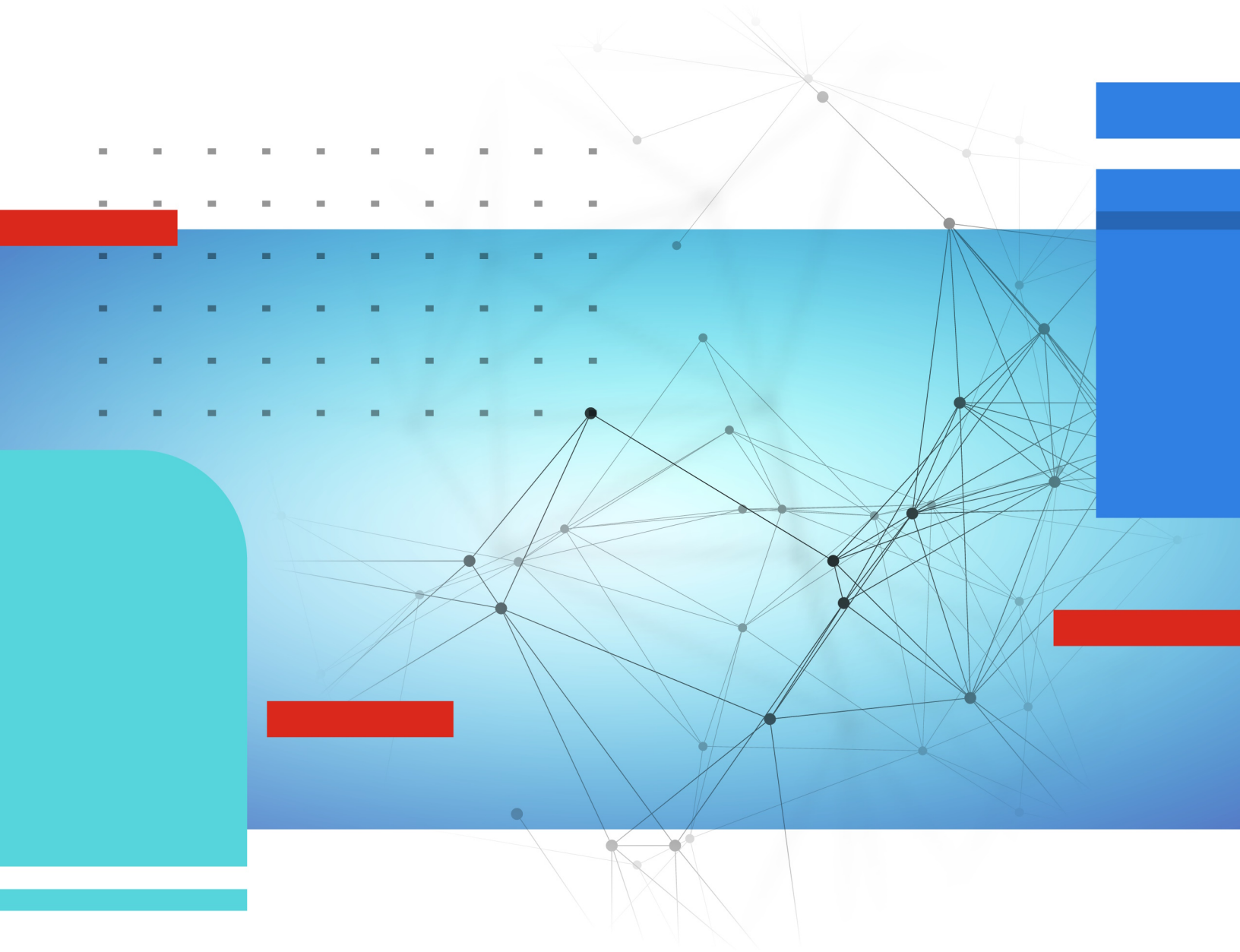
Managed Services Guide

FortiEndpoint 25.2



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 7, 2025
FortiEndpoint 25.2 Managed Services Guide
94-252-1186816-20250807

TABLE OF CONTENTS

Introduction **4**
Process overview **6**
How and when to initiate a Managed Service onboarding request **7**
When to engage Managed Service? 8
Change log **10**

Introduction

To assist and offload busy IT teams, Fortinet offers FortiEndpoint Managed Services to streamline the configuration, deployment, monitoring of FortiClient agents and Managed Detection & Response for security incidents. Services included with this offering include:

Service	Description
Initial FortiEndpoint Cloud	The managed services team works with customers to set up and configure their FortiEndpoint Cloud environment for the following capabilities (but not limited to): • Endpoint groups setup • Zero trust network access (ZTNA) • Security profiles and policies configuration • Vulnerability management • Threat Hunting & Communication Control • Endpoint posture check rules • Custom FortiClient installer creation and ongoing installer updates • Events Tuning & Analysis
Endpoint onboarding	The Managed Services team creates custom Unified installers for customer-specific use cases, sends invitation emails to users, and onboards them for FortiClient Cloud management and provisioning.
Fortinet Security Fabric setup and integration	The Managed Services team integrates FortiClient Cloud with the Security Fabric to support use cases such as ZTNA, incident response, and automation.
Endpoint security alerts	The Managed Services team monitors customer endpoints to identify high-risk endpoints and alert the customer of endpoints with critical and high vulnerabilities that would be easy targets for cyber-attacks. The Managed Services team detects, reports, and guides customers to remediate those vulnerable endpoints.
FortiGuard Managed Detection and Response (MDR) Service	The MDR Services team provides organizations with 24x7 monitoring of alerts and threats detected by FortiEDR. Fortinet experts review and analyze every alert, proactively hunt for threats, and take action to keep customers protected according to their risk profiles. The team also guides incident responders and IT administrators with recommended next steps as needed.

FortiClient Managed Services sends regular endpoint security overview and vulnerability summary reports.

The following lists all features that FortiClient Managed Services includes:

- Zero Trust Agent
  - ZTNA (also requires a FortiGate)
  - Central management
  - Central logging and reporting
  - IPsec VPN with multifactor authentication (MFA)
  - SSL VPN with MFA
  - Single sign on mobility agent
- IT hygiene
  - Vulnerability agent and remediation
  - FortiGuard Web Filter
  - Software Inventory
  - USB device control
- Endpoint security
  - FortiSandbox (on-premises or platform-as-a-service)
  - FortiClient Cloud Sandbox
  - Artificial intelligence-powered next-generation antivirus
  - Automated endpoint quarantine
  - Ransomware protection
  - Application Control
  - Communication Control
  - Automated Playbooks
- Managed FortiClient service
  - Endpoint onboarding
  - Initial provisioning
  - Security Fabric setup and integration
  - Vulnerability monitoring
  - Endpoint security monitoring
- 24x7 technical support available
- Onboarding and change requests are actioned (5) day per week basis, excluding weekends and public holidays, during the hours of 09:00 and 18:00 in the local time zone where the service is being delivered (“Business Hours”). For clarity, the time zone for North America is typically Pacific Standard Time (PST), Central European Time (CET) for EMEA, and Malaysia Time (MYT) for APAC.

The FortiEndpoint Managed Service team provides services only for FortiClient EMS, FortiClient, and FortiEDR. For other Fortinet products (FortiGate, FortiAnalyzer, etc.), please contact sales to inquire about available services like Professional Services or Jump Start.

Process overview

1. Register BPS and product contract in the Forticloud portal (https://support.fortinet.com).
2. Initiate Managed Service onboarding request (https://mfcts.mss.fortinet.com/mfcts/cli_out/#/welcome).

   Assigned Managed Service engineer will schedule onboarding kickoff meeting, followed by consecutive configuration meetings.
3. Deployment of agent and events & settings tuning based on feedback.
4. Switch to prevention mode.
5. Project handover to MDR team for onboarding.
6. Project closure.

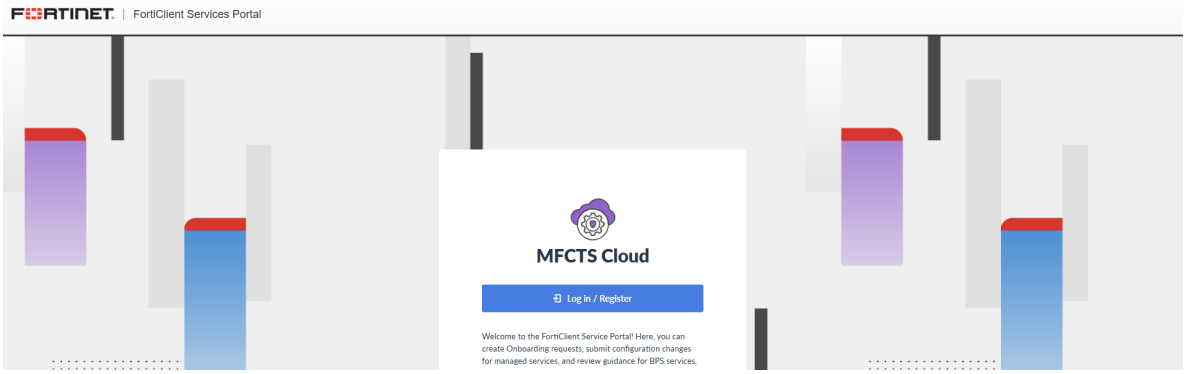
Post onboarding, customer needs to open change requests with all required details and implementation date for the Managed Service team to make the changes in the backend.

How and when to initiate a Managed Service onboarding request

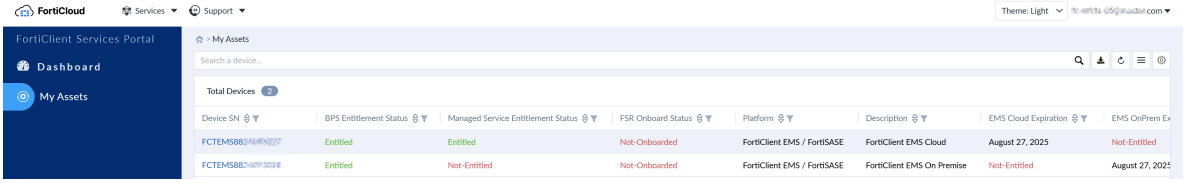
You can initiate a Managed Service onboarding request by following these steps.

To initiate a Managed Service onboarding request:

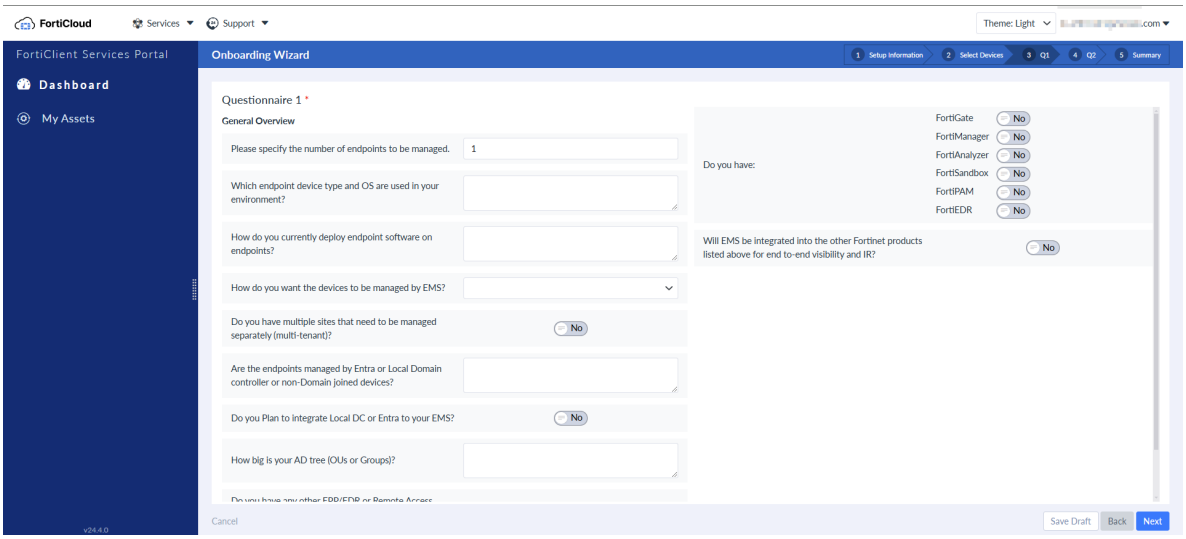
1. Log in to the FortiClient Services Portal.



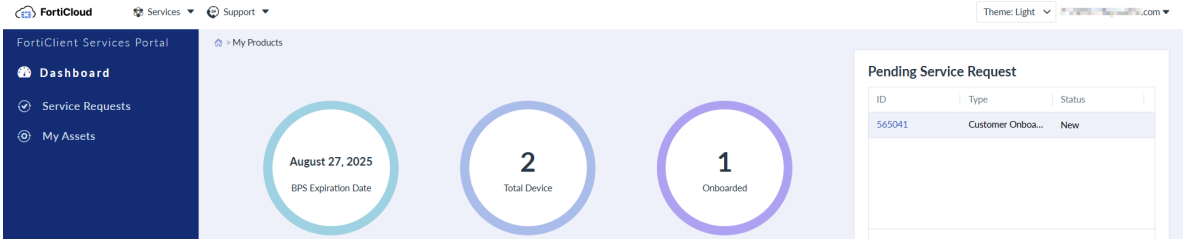
2. Go to *My Assets*. Confirm that it lists your EMS serial number and respective service entitlement. The *Managed Service Entitlement Status* column shows *Entitled*. If this is not the case, confirm that you have registered your EMS and Managed Service contracts.



3. Go to *Dashboard*.
4. Click *Start Onboarding*.
5. From the *Timezone* dropdown list, select your timezone. Click *Next*.
6. Select the desired EMS instance. Click *Next*.
7. The following page displays a questionnaire regarding your desired EMS configuration. Answer the questions, then click *Next*.



8. The following page displays a questionnaire regarding which features to enable on your EMS instance. Answer the questions, then click *Next*.
9. The following page displays a summary of the information that you have provided. Review the summary, and, once satisfied, click *Submit*. In the *Pending Service Request* widget on the *Dashboard*, you can view that you have a pending customer onboarding request.



When to engage Managed Service?

Customers are encouraged to engage Managed Service services in the following scenarios:

Scenario	Description
During initial FortiEndpoint Cloud configuration	Seek assistance from Managed Service experts during the initial setup and configuration of FortiClient Cloud.
Initial planning for FortiEndpoint Cloud	Engage Managed Service early in the planning phase for deploying FortiClient Cloud to leverage expert guidance and best practices.
On-premises EMS to FortiEndpoint Cloud migration	Managed Service can provide support and guidance during the migration process from on-premises EMS to FortiClient Cloud.

Scenario	Description
Post-deployment configuration review	Use Managed Service for reviewing and optimizing EMS configurations post-deployment to ensure optimal performance and security.
How-to questions	Reach out to Managed Service for clarifications, guidance, or assistance with any specific questions or challenges encountered during usage of FortiClient, FortiClient EMS, and FortiEDR.

Change log

Date	Change description
2025-08-07	Initial document release.

www.fortinet.com