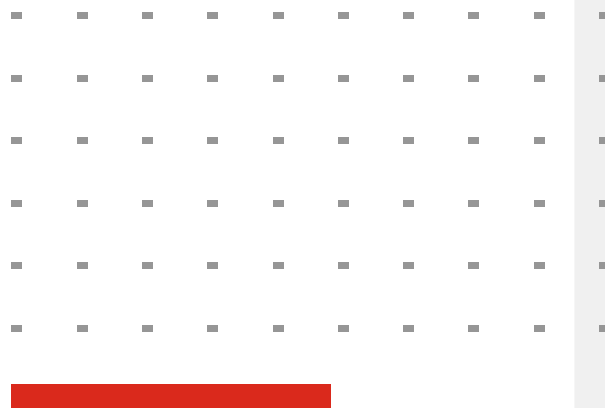




Administration Guide

FortiCare 26.2.a



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



June 05, 2026

FortiCare 26.2.a Administration Guide

57-262-1278524-20260605

TABLE OF CONTENTS

Change Log	5
Introduction to FortiCare	6
What's new with 26.2.a	6
Fortinet Support landing page	6
No access	8
Dashboard	9
Tickets	10
Active tickets	11
All tickets	11
Filtering tickets	12
Filtering tickets by status	12
Filtering tickets by date	12
Ordering tickets by category	12
Searching for tickets	13
Ticket details	13
Creating tickets	15
Technical support ticket	15
Customer service ticket	18
DOA/RMA ticket	21
Anti Virus ticket and FortiGuard Service	24
Fortinet Converter ticket	25
Professional Services ticket	26
FortiClient Services	29
Adding comments	29
Closing tickets	30
Exporting tickets	31
Advanced Services	32
Advanced services view	33
Supported user types	33
Point Usage	34
Registered points	35
Creating an Advanced Service ticket	35
Advanced Services types	37
Incident Response	42
Point Usage	42
Registered points	43
Creating an Incident Response ticket	44
Incident Response types	46
Downloads	54
Firmware Images	54
VM Images	55
Service Updates	56

HQIP Images	57
Get Checksum Code	58
Product Life Cycle	59
Hardware	59
Software	60
Services	61
Resources	62
Bug Tracker	63
Customer Support Bulletin	64
Technical Web Chat	65
Customer Service Web Chat	66
Ticket survey	67
Multilingual survey support	67
Guidelines and Policies	70
Preferences	71
User permissions	72
User access	72
IAM users and external IdP roles	72
Partners	72
Sub users	73
Organization view	74
Organizational Unit (OU) view	74
Member account view	75

Change Log

Date	Change Description
2026-06-05	Initial release.

Introduction to FortiCare

The FortiCare portal is a user-friendly ticketing system, designed to streamline your ticket management process. The new comprehensive ticketing web interface supports various workflows based on the ticket types to efficiently submit, track, prioritize, and resolve tickets with ease.

Key features include:

- Creating new tickets of various types:
 - Technical support
 - Customer service
 - DOA/RMA
 - Anti Virus and FortiGuard Service
 - FortiConverter
- Searching, viewing status, and commenting
- Exporting ticket information

FortiCare can be accessed from the FortiCloud *Support* dropdown by selecting *Support > FortiCare New*. Sign in with your unified FortiCloud Account to access the portal.

What's new with 26.2.a

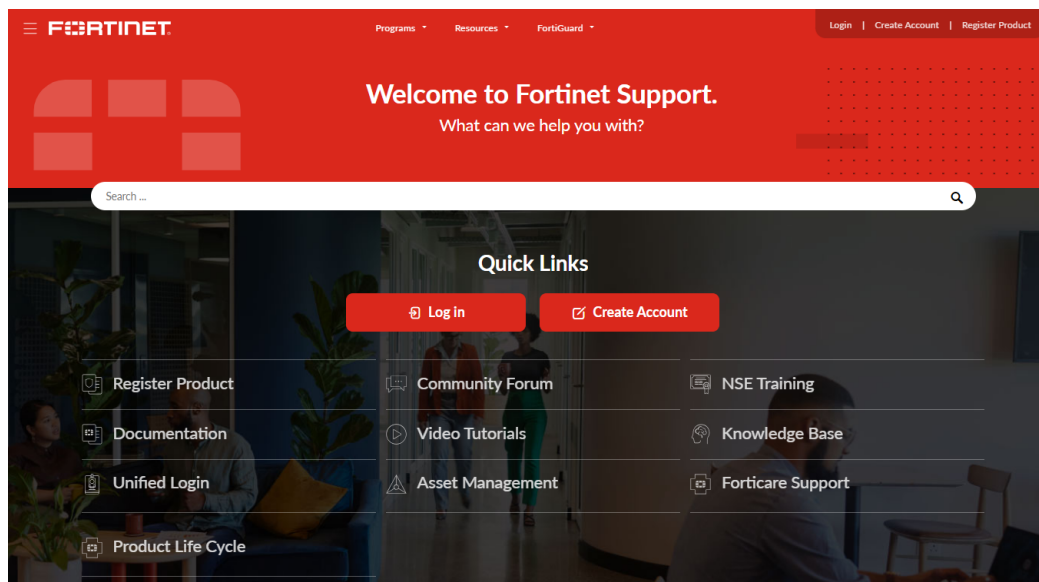
There are no new features included in FortiCare version 26.2.a. See the [FortiCloud Services Release Notes](#) for more information.

Additional Advanced Services type

The *Additional Tickets Package* has been added to Advanced Services. This type extends the initial ticket threshold by purchasing additional tickets. See [Advanced Services types on page 37](#).

Fortinet Support landing page

The Fortinet Support landing page can be found at support.fortinet.com. Logging into the Support landing page directs the user to the FortiCare portal dashboard. See [Dashboard on page 9](#).



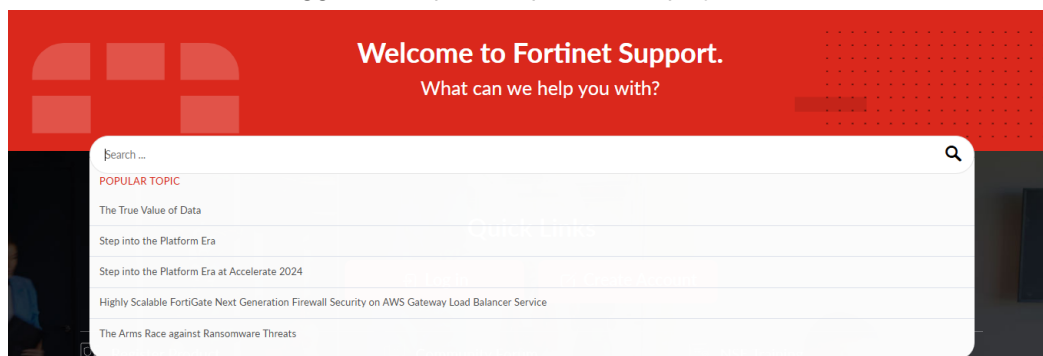
Users can also access FortiCloud Services and portals, including the FortiCare portal, through forticloud.com. If you log in through forticloud.com, you will be directed to the Asset Management dashboard instead of the FortiCare dashboard. See [FortiCloud Services landing page](#) in the Asset Management guide.

From the support landing page, users can:

- Search for information, including quick links, documents, and support.
- Access additional resources from the *Resources* dropdown menu.
- Log in to FortiCloud using existing credentials. See [Logging into an account](#) in the Asset Management guide.
- Access the *Product Life Cycle* without logging into the FortiCare portal. See [Product Life Cycle on page 59](#) for more information on the Product Life Cycle.

To use the Community Search function:

1. Go to support.fortinet.com.
2. Click the search field. Suggested *Popular Topics* are displayed.

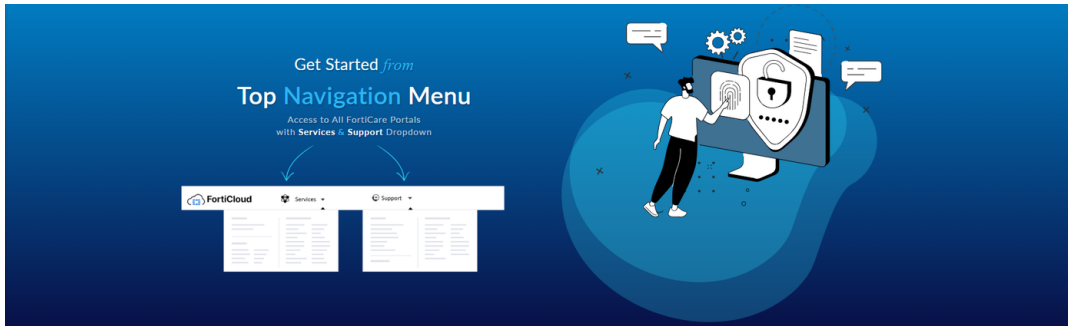


3. Define the search parameters:

- a. Select a *Popular Topic*. A new page is opened displaying information on the topic.
- b. Enter information in the search field and press Enter. A new page is opened displaying information on the topic.

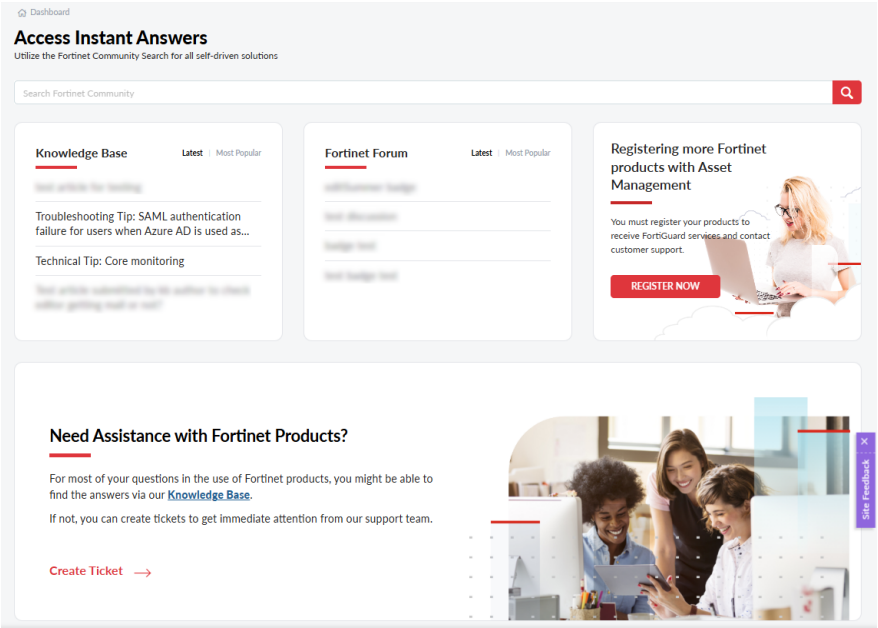
No access

If the user does not have access to the FortiCare portal, the following page will direct the user to select a service from the *Services* or *Support* menu after logging in through support.fortinet.com.



Dashboard

The *Dashboard* displays information about your tickets and updates from the FortiCare community.

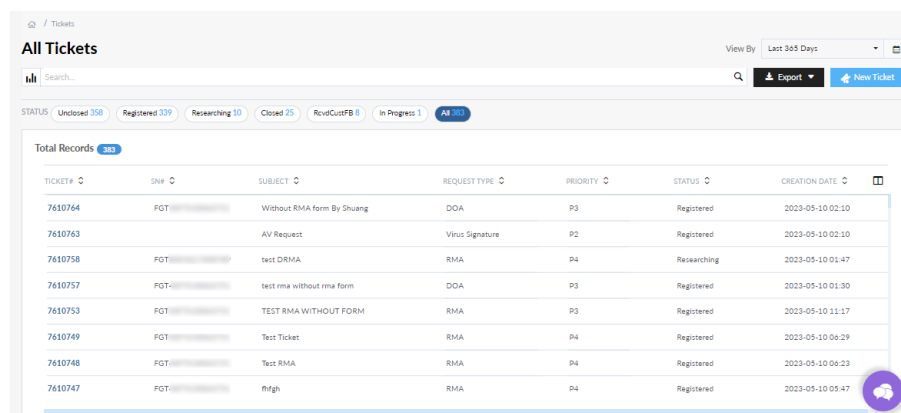


You can view the following information on the *Dashboard*:

Customer Support Bulletin	Displays helpful and important updates, tips, and notes from FortiCare customer service. For more detailed content, see the Customer Support Bulletin on page 64 .
Knowledge Base	Displays informative articles, podcasts, videos, and so on from the Knowledge Base.
Fortinet Forum	Displays articles and posts by FortiCare users on the community forum.
Tickets Pending Your Feedback	Displays tickets that you need to review and provide feedback based on the latest comments.
Latest from Fortinet Support	Displays high-level information on actions performed on your tickets by FortiCare support employees.
Registering more Fortinet products with Asset Management	Select <i>Register Now</i> to register assets in the Asset Management portal. See Registering assets in the Asset Management guide.

Tickets

You can create, review, and monitor active and closed tickets in the *Tickets* pages.



The screenshot shows the 'All Tickets' page in the FortiCare interface. It includes a search bar, status filters (Unclosed 358, Registered 139, Researching 10, Closed 25, Revoked 8, In Progress 1, All 363), and a table of tickets. A feedback icon is visible in the bottom right corner of the table.

Ticket#	SN#	Subject	Request Type	Priority	Status	Creation Date
7610764	FGT-XXXXXX	Without RMA form By Shuang	DOA	P3	Registered	2023-05-10 02:10
7610763		AV Request	Virus Signature	P2	Registered	2023-05-10 02:10
7610758	FGT-XXXXXX	test DRMA	RMA	P4	Researching	2023-05-10 01:47
7610757	FGT-XXXXXX	test rma without rma form	DOA	P3	Registered	2023-05-10 01:30
7610753	FGT-XXXXXX	TEST RMA WITHOUT FORM	RMA	P3	Registered	2023-05-10 11:17
7610749	FGT-XXXXXX	Test Ticket	RMA	P4	Registered	2023-05-10 00:29
7610748	FGT-XXXXXX	Test RMA	RMA	P4	Registered	2023-05-10 00:23
7610747	FGT-XXXXXX	thgh	RMA	P4	Registered	2023-05-10 05:47



Use the feedback icon to submit feedback on the new FortiCare interface.

Tickets is organized into the following pages:

- [Active tickets on page 11](#)
- [All tickets on page 11](#)

From the *Tickets* pages, you can:

- Filter the ticket list. See [Filtering tickets on page 12](#).
- Search for specific tickets. See [Searching for tickets on page 13](#).
- View ticket information. See [Ticket details on page 13](#).
- Create new tickets. See [Creating tickets on page 15](#).
- Add comments and files to tickets. See [Adding comments on page 29](#).
- Close tickets. See [Closing tickets on page 30](#).
- Export ticket information. See [Exporting tickets on page 31](#).



If the user has *Read Only* access assigned, they will be unable to create, edit, comment on, or close a ticket. See [User access on page 72](#).



Organization users must select a member account before accessing FortiCare portal features. See [Organization view on page 74](#), the [Identity & Access Management guide](#), and the [Organization Portal guide](#) for more information.

Active tickets

Active tickets can be found in the *Tickets > Active Tickets* page in a card view. The card view includes the *Request Type*, *Ticket Category*, and *Status*.

The screenshot shows the 'Active Tickets' interface. At the top, there's a 'View By' dropdown set to 'All' and a 'New Ticket' button. Below is a search bar and a status filter for 'Registered' (5 records). The main area displays a ticket card for ID #10796069, created on 2025-06-18 at 11:33. The card shows details like 'Request Type: Technical Assistance', 'Ticket Category: Log - Report', and 'Status: Registered'. It also includes a 'Last Update by' field showing 'FortiCare FortiCare' at 2025-06-20 06:00.

Closed tickets cannot be viewed in the *Active Tickets* page. To view closed tickets, go to *Tickets > All Tickets*. See [All tickets on page 11](#) for more information.



If a ticket is part of an Organizational Unit, the *OU Path* and *Account* will be displayed in the ticket. Likewise, if a Partner user is viewing the ticket card view, the *Ticket Type* displays the ticket audience, such as Partner, customer, or internal.

All tickets

You can view all existing tickets, including closed tickets, on the *Tickets > All Tickets* page.

The screenshot shows the 'All Tickets' interface. It includes a 'View By' dropdown set to 'Last 365 Days' and an 'Export' button. Below is a search bar and status filters for 'Unclosed' (5), 'Closed' (5), and 'Registered' (5), totaling 10 records. The main area displays a table of tickets with columns for Ticket ID, Serial Number, Subject, Request Type, Priority, Status, and Creation Date. The table lists five tickets, including one with ID 10796072 in 'Closed' status and others in 'Registered' status.



Partner accounts can also select *Account* and *Ticket Quality* from the column selector.

You can create a new ticket in the *All Tickets* page with the same process as through the *Active Tickets* page. See [Creating tickets on page 15](#).

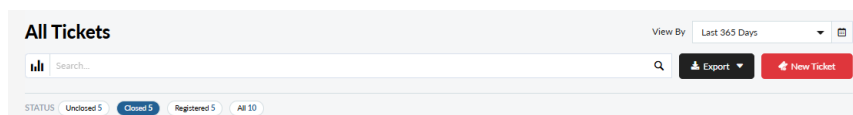
Filtering tickets

Tickets can be filters in the *Tickets* pages by:

- [Status](#)
- [Date](#)
- [Category](#)

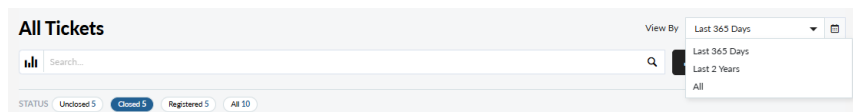
Filtering tickets by status

The tickets available for review can vary depending on the select *Status*. For example, you can choose to *All*, *Unclosed*, *Registered*, or *Closed* tickets.



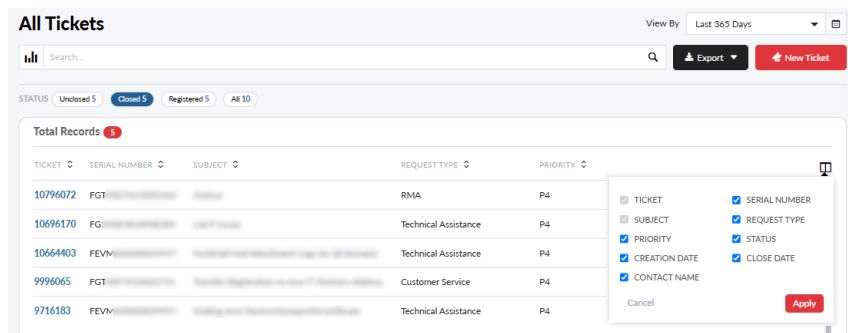
Filtering tickets by date

You can also restrict the number of tickets shown by selecting a date range from the *View By* dropdown list or calendar.



Ordering tickets by category

Tickets can be ordered by category, such as *Ticket #* or *Request Type*, by selecting the category arrow. More columns can be added to the table from the *Column Selector*. The columns available depend on the user type accessing FortiCare.





Partners can select two additional columns: *Account* and *Ticket Quality*. See *Switching accounts* in the *Asset Management Administration Guide* for information on switching partner accounts.



For advanced ticket filtering, use the *Advanced Search* feature. See *Searching for tickets* on page 13.

Searching for tickets

You can search for specific tickets using the *Search* field or the *Advanced Search* button. You can use *Advanced Search* to filter tickets by *Subject*, *Ticket Type*, and so on.



Not all of the *Advanced Search* fields must be filled when performing a search.

To perform an advanced ticket search:

1. Go to *Tickets*.
2. Select *Advanced Search*. The advanced search dialog opens.

3. Select the filters from the dropdown menus.
4. Enter the ticket subject in the *Subject* field.
5. Enter the ticket number in the *Ticket Number* field.
6. Enter the serial number in the *Serial Number* field.
7. Enter the date range of ticket creation in the *Created Between* fields.
8. Click *Search*. Tickets with parameters matching the set filters are displayed.

Ticket details

Ticket information can vary depending on the ticket type. Select a ticket to view detailed information, such as:

Ticket Conversation	Tracks comments between individuals related to the ticket, such as members of your organization and FortiCare support, and any attached files.  You can delete attachments you included with a comment by selecting the x next to the attachment and clicking <i>Confirm</i> in the pop up dialog. You cannot delete attachments from someone else's comment.
Basic Info	Provides information on ticket <i>Status</i> , <i>Request Type</i> , <i>Category</i> , <i>Priority</i> , and so on.
Contact Info	Displays your contact information, including email and phone number.
SFTP Info	Displays <i>Upload</i> and <i>Download</i> information, such as <i>FTP Address</i> and <i>User ID</i> . Use the <i>Hide</i> and <i>Show</i> buttons to control <i>SFTP Information</i> visibility.
Ticket Visibility	Lists who can view the ticket.
RMA Info	Displays RMA information, such as: • <i>Return Material Authorization Info</i>: Contains ticket information, including <i>RMA Type</i> and <i>RMA Ticket ID</i>. • <i>Summary</i>: Contains information on product model status. • <i>Shipping & Billing Info</i>: Displays shipping and billing addresses and contacts. When editing, once you click <i>Confirm RMA Information</i>, the information can no longer be edited. The shipping address must be confirmed to submit a PRMA ticket. • <i>Transit To</i>: Provide transit information following shipping and click <i>Confirm Transit Address Information</i> to complete editing. Transit To information becomes read only after confirmation. • <i>Defective Product Info</i>: Displays information on the product, including serial number and model. • <i>RMA Contract and Service Transfer</i>: States if all active services and support contracts will automatically be transferred to the new unit. This section can only be edited by Partner users. • <i>Return Instructions</i>: Provides additional information on the <i>RMA Center</i> and return instructions. • <i>Replacement Product Info</i>: Provides shipping and tracking information. This section can only be edited by Partner users. Once the information has been confirmed, it becomes read only. • <i>Receiving Info</i>: Displays information on the product model receipt.  Additional information is required in the ticket comments if you are requesting a PRMA ticket. See Requesting PRMA tickets on page 23.



If you have the necessary account permission, such as *Read/Write*, you can edit *Contact Information*, *RMA Info*, and *Ticket Visibility*. If you have *Read Only* access, you cannot edit any fields in the ticket details.

To view detailed ticket information:

1. Go to *All Tickets*.
2. Select the *Ticket*. The ticket details are displayed.



3. (Optional) Toggle *Expand All Info* to open all ticket details.

Creating tickets

You can create new tickets using the *New Ticket* button. You can create a ticket request for:

- [Technical support ticket on page 15](#)
- [Customer service ticket on page 18](#)
- [DOA/RMA ticket on page 21](#)
- [Anti Virus ticket and FortiGuard Service on page 24](#)
- [Fortinet Converter ticket on page 25](#)
- [Professional Services ticket on page 26](#)
- [FortiClient Services on page 29](#)

Technical support ticket

You can submit a technical support tickets for help with technical issues.

To create a new Technical Support ticket:

1. Go to *All Tickets*.
2. Click *New Ticket*. The *Choose a Request Type* dialog opens.

Choose a Request Type

Welcome to the Fortinet Support Portal! For most of your questions regarding the use of Fortinet products, you might be able to find the answers in our [Knowledge Base](#). If not, you can choose a request type to get started.



Technical Support Ticket
Technical Assistance



Customer Service Ticket
Questions related to contract and account management



DOA/RMA Ticket
Defective product/hardware replacement ticket



Anti Virus Ticket/FortiGuard Service
To submit Anti Virus ticket for your product or report false detection.



Fortinet Converter Ticket
Please submit FortiConverter service request at FortiConverter Portal



Professional Services
Expert help to plan, deploy, and optimize your Fortinet solution

3. Hover over *Technical Support Ticket* and select *Submit Ticket*.



If you select *Start web chat*, you will be redirected to the *Technical Web Chat* page. See *Technical Web Chat* on page 65.

The *Basic Info* page opens.

STEP 1 . Basic Info

1. Basic Info
2. Comment
3. Preview
4. Complete

 **Technical Support Ticket**

PRODUCT INFO

SERIAL NUMBER: * The serial number will be shown after you input the first 3 characters

Enter Serial Number

GO

4. Enter the *Product Info* and click *Go*. If the serial number is accepted, *Contact Info* and *Ticket Info* fields are displayed.

STEP 1 . Basic Info

1. Basic Info
2. Comment
3. Preview
4. Complete

 **Technical Support Ticket**

PRODUCT INFO

SERIAL NUMBER: * The serial number will be shown after you input the first 3 characters

FGT90G

TICKET INFO

SUBJECT: * Provide a specific subject for case handling.

CATEGORY: *

PATCH: *

PRODUCT TYPE: *

FortiGate

S/W VERSION: *

PRIORITY: *

☐ P3
 ☒ P4

NOTE:
Please [contact your regional support center](#) to create urgent P1 (network down) or P2 (severe impact) tickets for immediate assistance.

Cancel
Next

Save time! Your answer might be here.
Completing all fields of Ticket Info will help you filter content efficiently and find what you need faster.

5. Enter the necessary information in the *Contact Info* and *Ticket Info* sections.

STEP 1 . Basic Info

1. Basic Info 2. Comment 3. Preview 4. Complete

Technical Support Ticket

PRODUCT INFO

SERIAL NUMBER: * The serial number will be shown after you input the first 3 characters
FGT90

TICKET INFO

SUBJECT: * Provide a specific subject for case handling
Login issue

PRODUCT TYPE *
FortiGate

CATEGORY *
Authentication

S/W VERSION *
7.2

PATCH *
GA

PRIORITY *
☐ P3 ☒ P4

NOTE:
Please contact your regional support center to create urgent P1 (network down) or P2 (severe impact) tickets for immediate assistance.

Save time! Your answer might be here.

NSE Experts Academy CTF
Date: December 30, 2024
We've given the following instructions: We've received this FortiGate unit. We haven't decided what we'll do with some of the most difficult challenges: spoil them, make them publicly available, or keep unsolved ones for...
Source: Blogs

Achieving Complete Visibility in AWS with FortiSIEM Security Incident and Event Management
Date: December 30, 2024
By deploying Windows Agents on AWS Windows instances, FortiSIEM is able to detect file integrity issues and generic malware issues on Windows AMIs. Also, get all your Fortinet product ques...
Source: Blogs

How Does a Firewall Work? | Fortinet
Date: December 19, 2024
Remote logins are often used to help someone with a computer issue. However, in the hands of the wrong person, they can be abused, particularly because remote login...
Source: CyberGlossary

FortiSOAR Sunburst Hunt & Response Content Pack

Cancel Next



Once the appropriate fields have been entered, FortiCare will display suggested community Knowledge Base articles, Fortinet documents, and FortiGuard resources that may help you solve the issue. Select an article to review the information or provide more detail in the Subject field for more filtered articles.

6. Click *Next*. The *Ticket Visibility* pane opens if using a Partner user account.
7. Select who you would like to have permission to view the ticket and click *Next*. The *Comment* page opens.

STEP 2 . Comment

1. Basic Info 2. Comment 3. Preview 4. Complete

Technical Support Ticket | SERIAL NUMBER: FGT

COMMENT *

POTENTIAL SOLUTIONS *

In order for Fortinet Technical Support to provide you with the optimum level of service, we request that the following information be provided:

1. A detailed problem description
2. Relevant background information (Has the configuration worked in the past? Is this a new configuration? Have any changes been made recently to the Fortinet device or application or on the network?)
3. A network diagram with the IP addressing clearly indicated
4. Configuration file(s)
5. Debug log(s)/Error messages
6. A description and the results of your troubleshooting steps
7. Your availability to work with Technical support
8. Alternative contact information

NOTE: The maximum characters system allow to be entered here is 8000.

ATTACHMENT

You specify the uploaded file's storage type by selecting it from the drop-down list. Files stored in "Temporary Storage" will be deleted once the ticket is closed. The option "Keep the file" means that the file will be retained after ticket closure. Virus samples and large files (>5MB) are always saved in temporary storage.

File Upload

Cancel Previous Next



Select *Potential Solutions* to view suggested community Knowledge Base articles, Fortinet documents, and FortiGuard resources that may help you solve the issue. Select an article to review the information or provide more detail in the Subject field for more filtered articles.

8. Enter the suggested information in the *Comment* field.
9. Click *File Upload* and select the file format.



All files will be deleted 30 days after the ticket is closed.

10. After your files have finished uploading, click *Next*. The *Preview* page opens.

STEP 3 . Preview

1. Basic Info | 2. Comment | **3. Preview** | 4. Complete

Test Ticket

BASIC INFO

REQUEST TYPE
Technical Support Ticket

CATEGORY
Authentication

SERIAL NUMBER
FGT9C

PRIORITY
P4

S/W VERSION
7.2

CONTACT INFO

NAME
[Redacted]

PHONE
[Redacted]

MOBILE
[Redacted]

EMAIL
[Redacted]

Cancel Previous **Confirm**

11. Click *Next*. The *Complete* page opens.
12. Review the ticket number and information and click *Done*.

Customer service ticket

You can submit a customer service ticket for help with contract and account management questions. You can also start a live web chat session for small questions.

To create a new Customer Service ticket:

1. Go to *All Tickets*.
2. Click *New Ticket*. The *Choose a Request Type* page opens.

Choose a Request Type

Welcome to the Fortinet Support Portal! For most of your questions regarding the use of Fortinet products, you might be able to find the answers in our [Knowledge Base](#). If not, you can choose a request type to get started.

 Technical Support Ticket Technical Assistance	 Customer Service Ticket Questions related to contract and account management	 DOA/RMA Ticket Defective product/hardware replacement ticket
 Anti Virus Ticket/FortiGuard Service To submit Anti Virus ticket for your product or report false detection.	 Fortinet Converter Ticket Please submit FortiConverter service request at FortiConverter Portal	 Professional Services Expert help to plan, deploy, and optimize your Fortinet solution

3. Hover over *Customer Service Ticket* and select *Submit ticket*.



If you select *Start web chat*, you will be redirected to the *Customer Service Web Chat* page. See *Customer Service Web Chat* on page 66.

The *Basic Info* page opens.

STEP 1 . Basic Info

1. Basic Info
2. Comment
3. Preview
4. Complete

Customer Service Ticket

PRODUCT INFO

SERIAL NUMBER: The serial number will be shown after you input the first 3 characters

Save time! Your answer might be here.

Completing all fields of Ticket Info will help you filter content efficiently and find what you need faster.

TICKET INFO

SUBJECT: * Provide a specific subject for case handling.

CATEGORY *

Please select a CS category ▼

CONTACT INFO

NAME *

EMAIL * (Separate multiple emails with a comma)

PHONE

▼

MOBILE

▼

Cancel
Next

4. Enter the required information in the *Product Information*, *Contact Info*, and *Ticket Information* sections.

Customer Service Ticket

PRODUCT INFO

SERIAL NUMBER: *The serial number will be shown after you input the first 3 characters*

TICKET INFO

SUBJECT: * *Provide a specific subject for case handling.* CATEGORY *

CONTACT INFO

NAME *

EMAIL * *(Separate multiple emails with a comma)*

PHONE MOBILE

Save time! Your answer might be here.

NSE Experts Academy CTF
Date: December 30, 2024
When they'd connect to the given IP address, they'd see a console which looks like what we'd normally get on a real FortiGate.
Invalid....
Source: Blogs

Security Research News in Brief - May 2017 Edition
Date: December 30, 2024
Sign the same message again, and retrieve an invalid signature (as one pre-computed integer has been faulted). Using the valid and the invalid signature of the same message, recover a fact....
Source: Blogs

Addressing Top SD-WAN Security Concerns
Date: December 30, 2024
Industry Trends Addressing Top SD-WAN Security Concerns By Fortinet | December 26, 2019 Tags: Secure SDWAN, Cybersecurity Architect, Security-Driven Networking Related Posts Industry Trends The Rise of Security-Driven N...
Source: Blogs

Analysis of CVE-2014-0050 - Microsoft IE

Cancel

Next



Once the appropriate fields have been entered, FortiCare will display suggested community Knowledge Base articles, Fortinet documents, and FortiGuard resources that may help you solve the issue. Select an article to review the information or provide more detail in the Subject field for more filtered articles.

- Click **Next**. The *Ticket Visibility* pane opens if using a Partner user account.
- Select who you would like to have permission to view the ticket and click **Next**. The *Comment* page opens.

STEP 2 . Comment

1. Basic Info

2. Comment

3. Preview

4. Complete

Customer Service Ticket

SERIAL NUMBER

Notes:
If this is a first time contract registration, please update the product location by visiting the following article: [How to update the Product Location in FortiCloud Portal](#)
If you are an EA Customer and need help with applying PRMA or Secure RMA Service, refer to the article: [ELA Portal for Priority RMA and Secure RMA](#)

COMMENT *

POTENTIAL SOLUTIONS

Use this category for questions related to Priority RMA Service (PRMA), we request that the following information be provided:

1. A description of your requirement
2. Product serial number(s)
3. PRMA contract number(s).

Please also refer to the notes below.

ATTACHMENT

You specify the uploaded file's storage type by selecting it from the drop-down list. Files stored in 'Temporary Storage' will be deleted once the ticket is closed. The option 'Keep the file' means that the file will be retained after ticket closure. Virus samples and large files (>5MB) are always saved in temporary storage.

File Upload

NOTE: The maximum characters system allow to be entered here is 8000.

Cancel

Previous

Next



Select *Potential Solutions* to view suggested community Knowledge Base articles, Fortinet documents, and FortiGuard resources that may help you solve the issue. Select an article to review the information or provide more detail in the Subject field for more filtered articles.

7. Enter the suggested information in the *Comment* field.
8. Click *File Upload* and select the type of file to upload.



All files will be deleted 30 days after the ticket is closed.

9. After your files have finished uploading, click *Next*. The *Preview* page opens.
10. Click *Next*. The *Complete* page opens.
11. Review the ticket number and information and click *Done*.

DOA/RMA ticket

Submit a DOA/RMA ticket to report defective products or to receive a hardware replacement.



All DOA/RMA tickets will appear in the *Tickets* page list as an RMA ticket at first. After being review by Fortinet Inc. Customer Service, if it determined to be a DOA ticket, the *Request Type* will change to *DOA* after processing.

To create a new DOA/RMA ticket:

1. Go to *All Tickets*.
2. Click *New Ticket*. The *Choose a Request Type* page opens.

Choose a Request Type

Welcome to the Fortinet Support Portal! For most of your questions regarding the use of Fortinet products, you might be able to find the answers in our [Knowledge Base](#). If not, you can choose a request type to get started.

 Technical Support Ticket Technical Assistance	 Customer Service Ticket Questions related to contract and account management	 DOA/RMA Ticket Defective product/hardware replacement ticket
 Anti Virus Ticket/FortiGuard Service To submit Anti Virus ticket for your product or report false detection.	 Fortinet Converter Ticket Please submit FortiConverter service request at FortiConverter Portal	 Professional Services Expert help to plan, deploy, and optimize your Fortinet solution

3. Select *DOA/RMA Ticket* and click *Next*. The *Basic Info* page opens.

STEP 1 . Basic Info

1. Basic Info

2. Shipping Info

3. Comment

4. Preview

5. Complete

DOA/RMA Ticket

PRODUCT INFO

SERIAL NUMBER: * The serial number will be shown after you input the first 3 characters

Enter Serial Number

GO

- Enter the *Product Info* and click *Go*. If the serial number is accepted, *Contact Info* and *Ticket Info* fields are displayed.

STEP 1 . Basic Info

1. Basic Info

2. Shipping Info

3. Comment

4. Preview

5. Complete

DOA/RMA Ticket

PRODUCT INFO

SERIAL NUMBER: * The serial number will be shown after you input the first 3 characters

TICKET INFO

SUBJECT: *

PRODUCT TYPE

FortiGate

CATEGORY *

CONTACT INFO

NAME *

EMAIL * (Separate multiple emails with a comma)

Cancel

Next

- Enter the required information in the *Contact Info*, and *Ticket Info* sections.
- Click *Next*. The *Ticket Visibility* pane opens if using a Partner user account.
- Select who you would like to have permission to view the ticket from the *Ticket Visibility* list and click *Next*. The *Shipping Info* page opens.

STEP 2 . Shipping Info

1. Basic Info
2. Shipping Info
3. Comment
4. Preview
5. Complete

DOA/RMA Ticket | SERIAL NUMBER: XXXXXXXXXXXX

SHIP TO

NAME * Fortinet Product Dept	COMPANY * Fortinet
STREET ADDRESS * Address Street	CITY * City, State
COUNTRY * United States	STATE/PROVINCE Enter state/province
POSTAL CODE * Zip Code	EMAIL * Email Address
PHONE * Phone Phone Number	FAX Fax Fax Number

BILL TO

☒ Same as "Ship To"
 ☐ Different from "Ship To"

Cancel

Previous
Next

8. Enter the shipping information in the *Ship To* section.
9. If the billing address is different from the shipping address, select *Different from "Ship To"* and enter the billing information.
10. Select the appropriate information from *Defective Product Info* and *RMA Contract and Service Transfer*.
11. Click *Next*. The *Comment* page opens.
12. Enter the suggested information in the *Comment* field.



Additional information is required in the *Comment* field if you are intending to create a PRMA ticket. See [Requesting PRMA tickets on page 23](#) for more information.

13. Click *File Upload* and select the type of file to upload.



All files will be deleted 30 days after the ticket is closed.

14. After your files have finished uploading, click *Next*. The *Preview* page opens.
15. Click *Next*. The *Complete* page opens.
16. Review the ticket number and information and click *Done*.

Requesting PRMA tickets

To initiate a Premium RMA (PRMA) request with Fortinet Inc. Customer Service, you must:

- Confirm the shipping address. See [Ticket details on page 13](#).
- Provide the following mandatory information in the *Comments* field when creating a DOA/RMA ticket:

Primary contact	Provide the name, phone number, and email of the primary contact. The primary contact must be Onsite.
Secondary contact	Provide the name, phone number, and email of a secondary contact.
Site restrictions	Provide any site restrictions, such as business hours and days of availability.
Special requirements	Provide any special details required to complete the delivery or to allow the engineer to enter the site, such as an inbound ticket number or access pass.

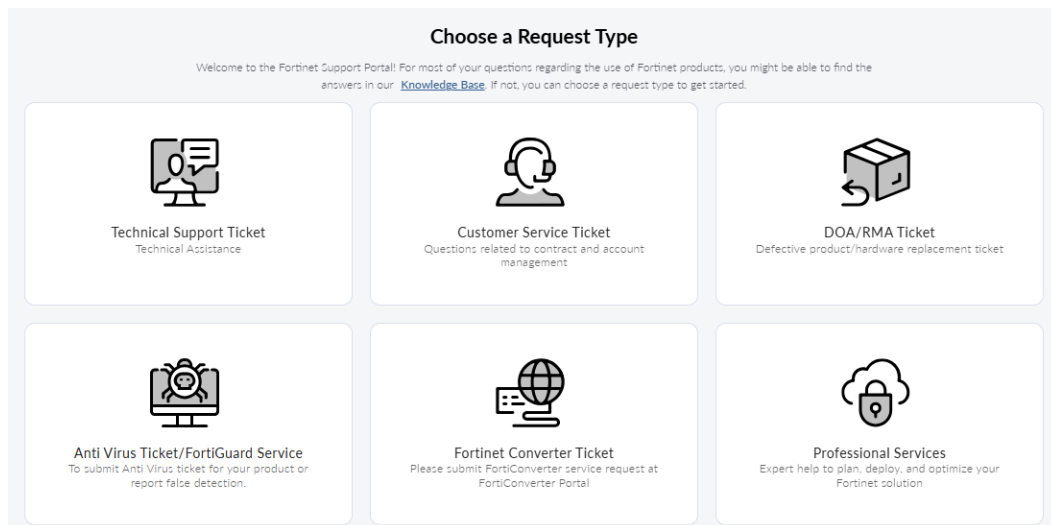
See [DOA/RMA ticket on page 21](#) for information on how to create a DOA/RMA ticket.

Anti Virus ticket and FortiGuard Service

Submit an antivirus or FortiGuard service tickets for your product or to report a false detection.

To create a new Anti Virus ticket:

1. Go to *All Tickets*.
2. Click *New Ticket*. The *Choose a Request Type* page opens.



3. Hover over *Anti Virus Ticket/FortiGuard Service* and select *Submit Anti Virus Ticket*.



Select *FortiGuard Service Ticket* to be redirected to the FortiGuard contact page.

4. Click *Next*. The *Basic Info* page opens.

STEP 1 . Basic Info

1. Basic Info

2. Comment

3. Preview

4. Complete

Anti Virus Ticket/FortiGuard Service

PRODUCT INFO

SERIAL NUMBER: * The serial number will be shown after you input the first 3 characters

TICKET INFO

SUBJECT: * CATEGORY: *

AV Request

Please select an AV category ▼

PRIORITY: * P2

i The P2 priority will ensure our support contact you in timely fashion.

CONTACT INFO

NAME *

EMAIL * (Separate multiple emails with a comma)

Cancel
Next

5. Enter the required information in the *Product Info*, *Contact Info*, and *Ticket Info* sections.
6. Click *Next*. The *Ticket Visibility* pane opens if using a Partner user account.
7. Select who you would like to have permission to view the ticket and click *Next*. The *Comment* page opens.
8. Enter the suggested information in the *Comment* field.
9. Click *File Upload* and select the type of file to upload.



All files will be deleted 30 days after the ticket is closed.

10. After your files have finished uploading, click *Next*. The *Preview* page opens.
11. Click *Next*. The *Complete* page opens.
12. Review the ticket number and information and click *Done*.

Fortinet Converter ticket

Fortinet Converter tickets should be submitted in the FortiConverter Services portal, which can be accessed from FortiCare.

To create a new Fortinet Converter ticket:

1. Go to *Tickets*.
2. Click *New Ticket*. The *Choose a Request Type* page opens.

Choose a Request Type

Welcome to the Fortinet Support Portal! For most of your questions regarding the use of Fortinet products, you might be able to find the answers in our [Knowledge Base](#). If not, you can choose a request type to get started.



Technical Support Ticket
Technical Assistance



Customer Service Ticket
Questions related to contract and account management



DOA/RMA Ticket
Defective product/hardware replacement ticket



Anti Virus Ticket/FortiGuard Service
To submit Anti Virus ticket for your product or report false detection.

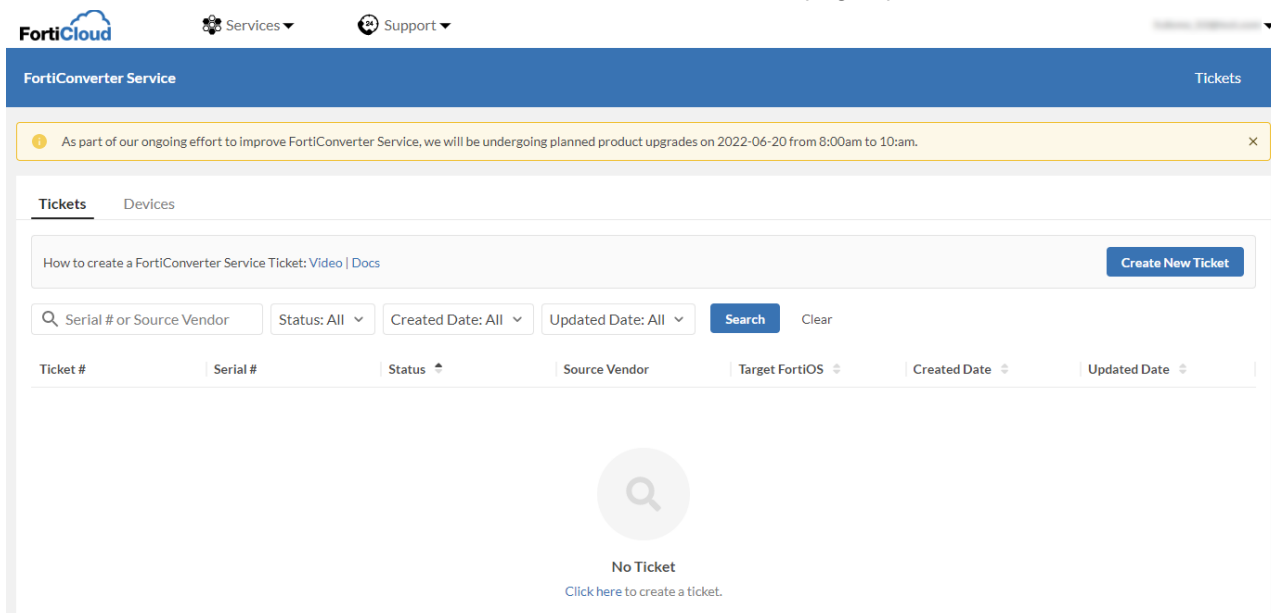


Fortinet Converter Ticket
Please submit FortiConverter service request at FortiConverter Portal



Professional Services
Expert help to plan, deploy, and optimize your Fortinet solution

3. Select *Fortinet Converter Ticket*. The *FortiConverter Service Portal* page opens.



4. Create a ticket on the *FortiConverter Service Portal*.

Professional Services ticket

The *Professional Services* ticket can be created to request the use of FortiPoints to purchase professional services offerings. After the ticket is created, the request will be reviewed and processed.



You can also access the *Professional Services* ticket creation process by selecting the Professional Services Marketplace offering in the Asset Management guide. See [Professional Services](#).

To create a new Professional Services ticket:

1. Go to *Tickets*.
2. Click *New Ticket*. The *Choose a Request Type* page opens.

Choose a Request Type

Welcome to the Fortinet Support Portal! For most of your questions regarding the use of Fortinet products, you might be able to find the answers in our [Knowledge Base](#). If not, you can choose a request type to get started.

 Technical Support Ticket Technical Assistance	 Customer Service Ticket Questions related to contract and account management	 DOA/RMA Ticket Defective product/hardware replacement ticket
 Anti Virus Ticket/FortiGuard Service To submit Anti Virus ticket for your product or report false detection.	 Fortinet Converter Ticket Please submit FortiConverter service request at FortiConverter Portal	 Professional Services Expert help to plan, deploy, and optimize your Fortinet solution

3. Select *Professional Services*.
4. If you have access to *Shared FortiPoints*, select the method of purchase. See [Shared FortiPoints](#) for more information.

Choose a Request Type

Welcome to the Fortinet Support Portal! For most of your questions regarding the use of Fortinet products, you might be able to find the answers in our [Knowledge Base](#). If not, you can choose a request type to get started.

 Technical Support Ticket Technical Assistance	 Customer Service Ticket Questions related to contract and account management	 DOA/RMA Ticket Defective product/hardware replacement ticket
 Anti Virus Ticket/FortiGuard Service To submit Anti Virus ticket for your product or report false detection.	 Fortinet Converter Ticket Please submit FortiConverter service request at FortiConverter Portal	 I want to spend ☐ FortiPoints ☐ Shared FortiPoints Expert help to plan, deploy, and optimize your Fortinet solution

5. Select the service.

STEP 1 . Choose a Service

1. Choose a Service 2. Specify Ticket Information 3. Comment 4. Complete

POINT BALANCE **1,080,769,052.18**



Professional Services 1 Day
Professional Services resource time based on the planned activities. The cost by default is set to one day. PS team will set up a scoping call leading to definition and delivery of a plan of action associated to number of points matching with the total number of days. Service delivered remotely, subject to resource availability and scope, and limited to a quantity of 10 days. 10 business days lead time for initial contact.

6500 Points
/DAY



Professional Services Packages
Consulting service that aims at helping Customers accelerate time-to-adoption of their Fortinet's technology. QuickStart is offered for FortiGate, FortiNAC, FortiSOAR, SDWAN deployments, and FortiCNAPP. For more details on the QuickStart services, refer to Service Descriptions [here](#). The Service is delivered remotely. 10 business days lead time for initial contact.

17000 Points
/STARTING FROM

Cancel Next

6. Click **Next**.

7. Enter the contact and product information.

STEP 2 . Specify Ticket Information

1. Choose a Service 2. Specify Ticket Information 3. Comment 4. Complete

POINT BALANCE **1,080,769,052.18**

CONTACT INFO

NAME * EMAIL * (Separate multiple emails with a comma)

PHONE MOBILE

PRODUCT INFO

REQUEST TYPE * CATEGORY

SUBJECT *

Cancel Previous Next

8. If the selected offering has multiple options available, select the *Request Type* from the dropdown list.

9. Click **Next**.

10. Enter the suggested information in the *Comment* field.

11. Click *File Upload* and select the type of file to upload.



All files will be deleted 30 days after the ticket is closed.

12. After your files have finished uploading, click **Next**.

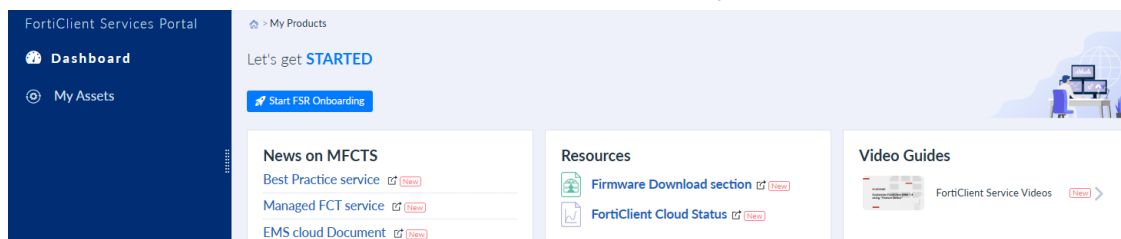
The ticket will be created and the professional services request submitted.

FortiClient Services

If a FortiClient Best Practice Services (BPS) license has been registered in the account, you can access the FortiClient Services portal from FortiCare.

To create a new FortiClient Services request:

1. Go to *Tickets*.
2. Click *New Ticket*. The *Choose a Request Type* page opens.
3. Select *FortiClient Services*. The *FortiClient Services Portal* opens.



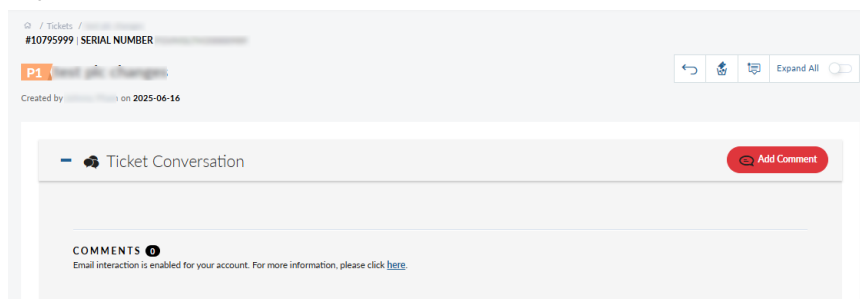
4. Create a support request in the FortiClient Services portal.

Adding comments

You can add a comment and attach files to the *Ticket Conversation*.

To add a comment:

1. Go to *Tickets*.
2. Select the *Ticket#*. The ticket details are displayed.
3. Expand *Ticket Conversation*.



4. Select *Add Comment*.

The screenshot shows the 'Ticket Conversation' interface. On the left is a large text area for 'COMMENT' with a character limit note: 'NOTE: The maximum characters system allow to be entered here is 8000.' Below it are 'Cancel', 'Save Draft', and 'Submit' buttons. On the right is the 'ATTACHMENT' section. It contains a text box with instructions: 'You specify the uploaded file's storage type by selecting it from the drop-down list. Files stored in "Temporary Storage" will be deleted once the ticket is closed. The option "Keep the file" means that the file will be retained after ticket closure. Virus samples and large files (>5MB) are always saved in temporary storage.' Below this is a cloud upload icon and a 'File Upload' dropdown button.

5. Enter a detailed comment in the *Comment* field.
6. Click *File Upload* and select the file type. The File Explorer opens.
7. Select the files you want to attach and click *Open*. The files are listed in *Attachment*.

This screenshot shows the 'Ticket Conversation' interface after a file has been uploaded. The 'COMMENT' field is empty. The 'ATTACHMENT' section now displays a table with one row:

File Name	Storage Type
sf-764-7-2_1517_202506161242.conf Gen: 423.5348	Persistent

 Below the table is a red 'x' icon for removal. At the bottom are 'Cancel', 'Save Draft', and 'Submit' buttons, along with the 'File Upload' dropdown.

8. Click *Submit*. The comment will appear in the *Ticket Conversation*.



If you do not want the comment to be public yet, select *Save Draft* instead of *Submit* and click elsewhere to exit the screen. This allows you to return to the comment later and publish it to the *Ticket Conversation* when you are ready. Select *Edit Draft* to make changes or publish it. Select *Discard Draft* to delete the draft.

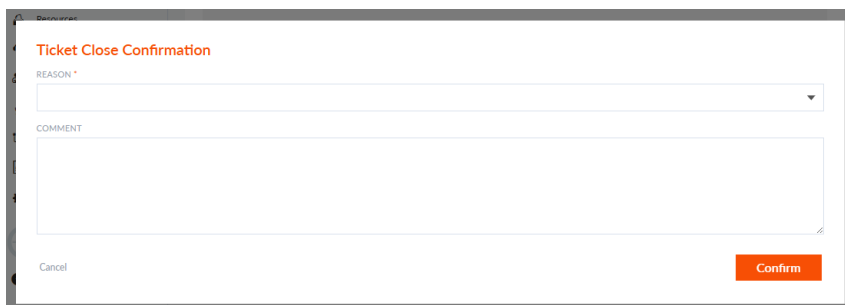
To delete a file from a comment, select the x and confirm the removal in the *Confirm File Removal* dialog.

Closing tickets

When a ticket has been resolved, you can close the ticket.

To close a ticket:

1. Go to *All Tickets*.
2. Select the *Ticket*. The ticket details are displayed.
3. Select *Close This Ticket*. A confirmation dialog is displayed.

A dialog box titled "Ticket Close Confirmation" with a red header. It contains a "REASON" dropdown menu and a "COMMENT" text area. At the bottom, there are "Cancel" and "Confirm" buttons. The "Confirm" button is orange.

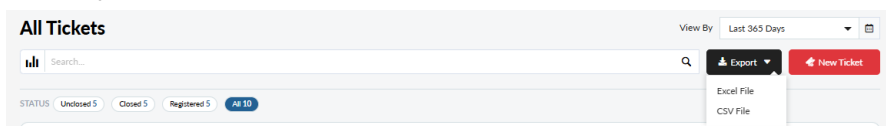
4. Select the *Reason* from the dropdown menu and add a *Comment*.
5. Click *Confirm*. The *Status* is changed to *Closed*.

Exporting tickets

You can export ticket information from the *Tickets* page to your device in Excel and CSV format.

To export ticket information:

1. Go to *All Tickets*.
2. Click *Export*.



3. Select the file format you want to export from the dropdown menu:
 - *Excel File*
 - *CSV File*

The file is saved to your device.

Advanced Services

Advanced Services (AS) allows Fortinet Inc. customers with an active Advanced Support service contract to request different service activities in exchange for Service Points.

Advanced Services
Premium support to sustain and optimize Fortinet appliances for Enterprises. [More info](#)

Search... [Export As](#) [Request Service](#)

POINT USAGE REGISTERED POINTS POINT BALANCE 11

Total Records 5

TICKET ID	TYPE	SUBJECT	STATUS	REQUEST DATE
	Remote After-Hours Assistance	Upgrade - Thursday August 15th 2024 @ 7pm CST.	Completed	2024-08-09
	Software Upgrade Testing	Need custom code	Cancelled	2022-08-05
	Software Upgrade Testing	Code Recommendation	Completed	2021-08-31
	Software Upgrade Assessment	Advanced Service Request for Software Recommendation regarding ticket	Completed	2021-08-25
	Software Upgrade Assessment	Advanced Service Request for Software Recommendation regarding ticket	Completed	2021-08-25



Users must have access to the root folder in their permission scope and have the correct entitlement registered to view the *Advanced Services* page. For information, see [Permission scope with Organizations](#) in the [Identity & Access Management](#) guide.

Eligible contracts

Advanced Services Requests (AS Requests) are available to customers with the following contracts:

- Enterprise Premium
- Enterprise Business
- Enterprise First or Global First
- Service Providers Select or Service Providers Elite or Global Elite
- AS Core
- AS Pro
- AS Pro Global
- AS Pro Plus
- AS Pro Plus Global

Service requests

Advanced Service Requests provide professional assistance to get the most out of your Fortinet Inc. products. Services include Customer On-Site Visit, Remote After-Hours Assistance, and more.

Service points

Service Points are exchanged to perform a service request. Each service request is assigned a set number of Service Points. After a request is created, a member of Fortinet's Support team will contact you to review the scope of the request and the number of points required to complete the request. The number of points required

may be adjusted depending on the scope of the request. After the scope and points required are agreed upon by you and the Support team, the points will be reserved in your account. Service points are deducted from your points balance at the time a service request is completed.

Advanced services view

Advanced Services displays the current *Point Usage* and *Registered Points*. Use the page to create a new service request and update open requests. You can export your point usage and registered points as an Excel or CSV file.

Advanced Services	Displays the <i>Point Usage</i> and <i>Registered Points</i> for Advanced Services requests. Click <i>Request Service</i> to create a new Advanced Service request. See Creating an Advanced Service ticket on page 35 .
Point Usage	Displays the current Advanced Services tickets and the number of Service Points used in ascending order by <i>Request Date</i> .
Registered Points	Displays the contracts registered to your account and your Service Points balance in ascending order by serial number.
Export As	Exports the <i>Point Usage</i> and <i>Registered Points</i> for the current view as an Excel or CSV file.
Request Service	Click to create a new <i>Advanced Services</i> request.
Point balance	Displays the total number of available Service Points. This number corresponds to the sum of the different Advanced Services contracts. If there is more than one active contract with different expiration dates, the balance will display the total available points at the current time. When a new Service Request is submitted, the points are instantly reserved and your points balance is adjusted. The reserved points will be deducted from the active contract at the time the Service Request is completed. If the service request is canceled, the points are instantly released.

Supported user types

The Advanced Services page supports both IAM and legacy Sub User models. For more information about FortiCloud's user management models, see [User management models](#) in the Identity & Access Management guide.

Users must have access to the root folder in their available scope and have the correct entitlement registered to view the *Advanced Services* page.

User type	Permissions
IAM User	IAM users with sufficient permissions can access the portal. For information, see IAM users and IAM user groups .
Sub User (Full Access)	Sub Users with Full Access can access the page.
Partner User	Partner users can access the page after they select an account in the Asset Management portal. For information, see Selecting accounts in the Asset Management for Partners guide. When a partner has Sub User (Full Access) permissions for the selected account, the permissions above apply.

Point Usage

The *Point Usage* tab shows the service requests for your account as well as the ticket type, status, and points consumed by each request.

POINT USAGE		REGISTERED POINTS		POINT BALANCE 11	
Total Records 5					
TICKET ID	TYPE	SUBJECT	STATUS	REQUEST DATE	
	Remote After-Hours Assistance	Upgrade - Thursday August 15th 2024 @ 7pm CST.	Completed	2024-08-09	
	Software Upgrade Testing	Need custom code	Cancelled	2022-08-05	
	Software Upgrade Testing	Code Recommendation	Completed	2021-08-31	
	Software Upgrade Assessment	Advanced Service Request for Software Recommendation regarding ticket	Completed	2021-08-25	
	Software Upgrade Assessment	Advanced Service Request for Software Recommendation regarding ticket	Completed	2021-08-25	

Point Usage	Description
Ticket ID	The FortiCare Ticket number associated with the service request. Click the <i>Ticket ID</i> to view the request details in FortiCloud and to comment on the ticket.
Type	The type of service requested. See Advanced Services types on page 37 .
Subject	The <i>Subject</i> text that was entered at the time the ticket was created. See Creating an Advanced Service ticket on page 35 .
Status	<i>Pending</i>: This is the default status after a service request is submitted. <i>Approved</i>: Indicates the scope of service to be delivered and the total number of service points has been agreed upon between you and Fortinet. <i>Canceled</i>: Indicates the service cannot be delivered. No points are applied. <i>Completed</i>: Indicates the agreed upon service has been delivered and you agree to close the Service Request.
Request Date	The date the service request was created.
Close Date	The date the service request was closed.
Points	The number of points used for this activity.

Registered points

The *Registered Points* tab shows the contracts registered to your account and the points balance for each contract. The entitlement period of the points corresponds to the contract period. This means any unused points will be forfeited on the contract expiry date. If there are multiple active contracts, the points are consumed based on a first-in-first-out rule to ensure the points that are expiring are used first.

POINT USAGE REGISTERED POINTS							POINT BALANCE 11
Total Records 5							
SERIAL NUMBER	CONTRACT#	LICENSE#	SKU	ACTIVATION DATE	EXPIRATION DATE	POINTS USED	BALANCE
XXXXXXXXXXXX	XXXXXXXXXX	XXXXXXXXXX	XXXXXXXXXXXX	2020-02-04	2021-02-03	0	16
XXXXXXXXXXXX	XXXXXXXXXX	XXXXXXXXXX	XXXXXXXXXXXX	2021-02-03	2022-02-03	6	10
XXXXXXXXXXXX	XXXXXXXXXX	XXXXXXXXXX	XXXXXXXXXXXX	2022-06-30	2023-06-30	0	12
XXXXXXXXXXXX	XXXXXXXXXX	XXXXXXXXXX	XXXXXXXXXXXX	2024-06-29	2025-06-29	1	11
XXXXXXXXXXXX	XXXXXXXXXX	XXXXXXXXXX	XXXXXXXXXXXX	2023-06-30	2024-06-29	0	12

Points	Description
SN#	The account level product serial number.
Contract#	The contract number.
License#	The contract license number.
SKU	The reference number for the service type.
Activation Date	The contract registration date.
Expiration Date	The contract end date.
Points Used	The number of service points used by this contract.
Balance	The number of service points remaining for this contract. This number is updated each time a Service Request is moved to <i>Completed</i> .

To export the Point Usage and Registered Points:

1. Go to *Advances Services*.
2. Click *Export As* and select either *Excel File* or *CSV File*.

Creating an Advanced Service ticket

When a new Service Request is created, the Service Points are reserved and your points balance is adjusted. After the request is submitted, a Fortinet Service representative will contact you to confirm the scope of the request and if necessary, adjust the number of points accordingly. The reserved points will be deducted from your balance when the Service Request is marked as *Completed*. If the service request is canceled the points are released.

To create a service request:

1. Go to *Advanced Services*.
2. Click *Request Service*. The *Choose a Service* page opens.

STEP 1. Choose a Service

1. Choose a Service 2. Specify Ticket Information 3. Comment 4. Complete

Service Points for Advanced Services: Customers with an active Advanced Service contract can exchange their Service Points by creating a Service Request. Please note that a Service Type CAN NOT be selected if there are not enough points in the balance. [More details about the Service points](#) POINT BALANCE 30

 Customer On-Site Visit One AS resource for one business day on-site visit to discuss support topics in connection with the existing Advanced Service Contract. This Service Option is subject to a prior agreement on location, date, and agenda of the business day visit. Lead time of 15 business days. 4 Points /day	 Remote After-Hours Assistance This Service Option provides the Customer with remote after-hours assistance for a maximum duration of four (4) hours during network changes (e.g. migrations, software upgrades or feature releases performed by the Customer that take place out of business hours). 5 business days lead time for scheduling. 1 Point /4 HOURS	 Software Upgrade Testing For one product software instance upgrade. Lab testing of a target Fortinet software release against the Customer's communicated configuration, and provision of a test report on the outcome. Lead time of 25 business days. 3 Points /APPLIANCE	 Software Best Practice One report outlining a best practice recommendation for a specific feature. Lead time of 15 business days. 4 Points /FEATURE
 Miscellaneous Service Activity One point per request. 1 Point /REQUEST	 Software Upgrade Assessment One product assessment of a target Fortinet software release against the Customer's communicated technical environment for the purpose of addressing known bug-related issues. Lead time of 15 business days. 6 Points /APPLIANCE	 FortiGuard Malware Analysis Service - Standard Report A report describing general behavior and functionalities of the malicious sample. 4 points /REPORT	 FortiGuard Malware Analysis Service - Expert Report An in-depth analysis report of the malicious sample offering a deeper visibility of the threat behavior. 8 points /REPORT

3. Select a service and click *Next*.



You cannot select a service if there are not enough points in your points balance.

4. Complete the *Specify Ticket Information* form.
 - a. In the *Contact Info* section enter your *Name*, *Email*, *Phone*, and *Mobile*.
 - b. In the *Product Info* section, use the *Subject* field to describe the request, and click *Next*.

STEP 2. Specify Ticket Information

1. Choose a Service 2. Specify Ticket Information 3. Comment 4. Complete

POINT BALANCE 30

CONTACT INFO

NAME *

EMAIL * (Separate multiple emails with a comma)

PHONE

MOBILE

PRODUCT INFO

REQUEST TYPE *

CATEGORY

SUBJECT *

Cancel Previous Next

- c. If the service you selected was a package, you may need to select the *Request Type* from the dropdown menu.

STEP 2 . Specify Ticket Information

1. Choose a Service
2. Specify Ticket Information
3. Comment
4. Complete

POINT BALANCE **30**

6 AS Points - FortiCare FortiGate FortiSwitch FortiRouter FortiWeb FortiMail
 9 AS Points - FortiCare FortiGate FortiSwitch FortiRouter FortiWeb FortiMail
 12 AS Points - FortiCare FortiGate FortiSwitch FortiRouter FortiWeb FortiMail
 13 AS Points - FortiCare FortiGate FortiSwitch FortiRouter FortiWeb FortiMail
 25 AS Points - FortiCare FortiGate FortiSwitch FortiRouter FortiWeb FortiMail
 11 AS Points - FortiCare FortiGate FortiSwitch FortiRouter FortiWeb FortiMail
 10 AS Points - FortiCare FortiGate FortiSwitch FortiRouter FortiWeb FortiMail
 15 AS Points - FortiCare FortiGate FortiSwitch FortiRouter FortiWeb FortiMail
 19 AS Points - FortiCare FortiGate FortiSwitch FortiRouter FortiWeb FortiMail
 8 AS Points - FortiCare FortiGate FortiSwitch FortiRouter FortiWeb FortiMail
 23 AS Points - FortiCare FortiGate FortiSwitch FortiRouter FortiWeb FortiMail

- Please choose a request type -

EMAIL * (Separate multiple emails with a comma)

MOBILE

CATEGORY

Service Points PS

SUBJECT *

Cancel

Previous
Next

5. Click *Next*.
6. Add a comment and attachment.
 - a. In the *Comment* section, describe the attachment.
 - b. In the *Attachment* section, click *File Upload*.
 - c. From the menu, select *Log File*, *Configuration*, or *Other*.
 - d. Click *Next*.

STEP 3 . Comment

1. Choose a Service
2. Specify Ticket Information
3. Comment
4. Complete

POINT BALANCE **11**

COMMENT *

Note: The maximum characters system allow to be entered here is 8000.

ATTACHMENT

You specify the uploaded file's storage type by selecting it from the drop-down list. Files stored in 'Temporary Storage' will be deleted once the ticket is closed. The option 'Keep the file' means that the file will be retained after ticket closure. Virus samples and large files (>5MB) are always saved in temporary storage.

File Upload ▾

Cancel

Previous
Next

7. (Optional) Click *Create Another Ticket* to request another service.

Advanced Services types

The following types of Advanced Services options are available for request:

Service	Description	Points
Customer On-Site Visit	Attendance at the customer location by an Advanced Services engineer for meetings or operational activities during a business day. This option may include: - Quarterly or annual business reviews. - Support with simple troubleshooting. - Presentation of an existing best practice recommendation. - Open discussion on planned activities.	4
Remote After-Hours Assistance	This service option provides remote after-hours assistance for a maximum duration of four hours during network changes (such as migrations, software upgrades or feature roll outs that take place out of business hours). Network changes covered under this service option shall be agreed in advance. This service option consists of: - A meeting to discuss the proposed network change which will be documented in a technical ticket. - Assistance with respect to questions, concerns or issues during the agreed maintenance window. - Support over the phone for remote diagnostics of reasonably unforeseen issues that may occur. An activity exceeding the maximum four hours will result in a deduction of additional Service Points for the actual remote after-hours assistance duration.	1
Software Best Practices	This Service Option consists of the delivery of a report outlining a best practice recommendation for a specific feature, such as: - The creation of a report tailored to the customer's communicated environment, detailing best practices to ensure Fortinet appliances are correctly configured for the required feature. - Guidelines to optimize the usage of Fortinet appliances or to identify potential issues. - A focus on the operational effectiveness of a specific product feature. For clarity, it explicitly excludes any design or integration with specific third party products or services.	4
Miscellaneous Service Activity	A custom request to address a specific requirement for your account.	1
Software Upgrade Assessment	A product assessment of a target software release against the customer's communicated technical environment for the purpose of addressing known bug-related issues. For clarity, this assessment shall only: Focus on Fortinet's software elements, excluding	6

Service	Description	Points
	hardware components. • Issue a bug scrub report with respect to the target Fortinet software release, focusing on the known issues of the software release. The bug scrub report shall generally consist of: • An assessment of the customer's communicated environment. • Bug scrub assessment of known issues that may potentially impact the customer's communicated environment. • A list of vulnerabilities resolved between the customer's deployed software release and the target software release. • Indicative recommendation on the suitability of the target software release for the customer's communicated technical environment.	
Software Upgrade Testing	This service option applies to one product instance upgrade and it consists of: • The testing of a target software release against the customer's communicated configuration within laboratory conditions. • The provision of a test report on the outcome. In particular, Fortinet will: • Conduct a preliminary assessment of the communicated environment. • Build a laboratory environment in accordance with the communicated environment. • Test the target's software release in the laboratory environment. • Issue an indicative report detailing findings during laboratory testing: • Identification of a recommended software release based on known issues. • Identification of a recommended upgrade path. • List of potential error messages displayed during upgrade path, including workarounds or minor configuration requirements required for a successful upgrade.	3
FortiGuard Malware Analysis Service – Standard Report	A report describing general behavior and functionality of the malicious sample.	4
FortiGuard Malware Analysis Service – Expert Report	An in-depth analysis report of the malicious sample offering a deeper visibility of the threat behavior.	8

Service	Description	Points
Knowledge Transfer - Custom Webinar	Webinar type chalk talk session that is conducted remotely and up to two hours in duration. The webinar consists of Show and Tell sessions in English where one feature is explained and described based on customer's configuration. The webinar will be also supplemented with best practice troubleshooting steps for commonly seen issues. Lead time to deliver the webinar is 10 business days.	5
Knowledge Transfer - Custom Workshop	Custom troubleshooting training with remote hands-on troubleshooting exercise designed by a Fortinet Support engineer for a maximum of three users. The knowledge transfer custom workshop is based on three relevant product features, or use cases, provided by the customer. Upon receipt of this information from the customer, Fortinet Support will create a specific lab environment to run the workshop and meet customer expectations. The custom workshop will be focused on FortiGate, FortiAnalyzer, or FortiManager. Lead time to deliver the custom workshop is four weeks.	10
Configuration Hardening Check	A point-in-time snapshot of customer FortiGate configurations deployed on the customer network within the lead region. A detailed report is provided to the customer to harden and improve the security of their FortiGate devices.	5
Device Performance Health Check	One performance health check as a point-in-time snapshot of a standalone FortiGate, or a cluster of FortiGate devices. The process involves the running of a non-intrusive monitoring script, in the customer's environment, for a recommended five calendar days against the targeted FortiGates. The resulting report will not only include key statistics of the FortiGates, but also provide recommendations to optimize utilization. A support ticket will be required to investigate any identified issues.	10
Lifecycle Audit Report	One life cycle audit report detailing : • The products deployed (FortiGate, FortiManager, and FortiAnalyzer) within the customer environment and their hardware and software life cycle status. • A bug tracking summary. • FortiGate feature usage and gap analysis. • A summary of current and future state recommendations.	10

Service	Description	Points
Customer Readiness Testing	Lab testing of customer specific scenarios and deployments, utilizing Fortinet products under specific configuration and loading conditions. This includes extensive or complex lab testing, and rely on the use of modern testing tools and methodologies. The lab will replicate with a network topology as close as possible to the one used by the customer with traffic patterns analysis and simulation, together with operational behavior replication. Typical testing projects include: • Long term soak testing. • Performance validation. • Software upgrade verification. • Traffic load evolution.	20
Professional Services 1 Day	The Service provides professional service resource time based on the planned activities and technology selection. The cost by default is set to one day. Professional Service team will set up a scoping call leading to definition and delivery of a plan of action associated to number of service points matching with the total number of days. The Service is subject to resource availability and scope. 10 business days for initial contact.	2.5
Professional Services Packages	QuickStart is a suite of services intended to assist with the implementation of Fortinet's products and to maximize the value of the investment in Fortinet's technology. QuickStart Services provide a basic product configuration for a specific use case and are aimed at increasing Customer's knowledge in configuring the Products. It is provided through a remote technical session based on the service option selected. It is offered for FortiGate, FortiNAC, FortiSOAR, SDWAN deployments, and FortiCNAPP. For more details on the service provided, see the QuickStart Service Descriptions. 10 business days for initial contact.	Selection dependent
Additional Tickets Package	Customers who wish to extend the initial ticket threshold will have the option to purchase additional tickets using this option. AS services maintain a Fair Usage Policy ("FUP") set against a permitted count of technical assistance tickets raised during the service term and excluding tickets classified by Fortinet as bug, RMA and customer service tickets. The option provides 5 additional tickets, and the task will be considered completed once all 5 tickets have been opened or at AS service expiration, whichever occurs earlier.	2

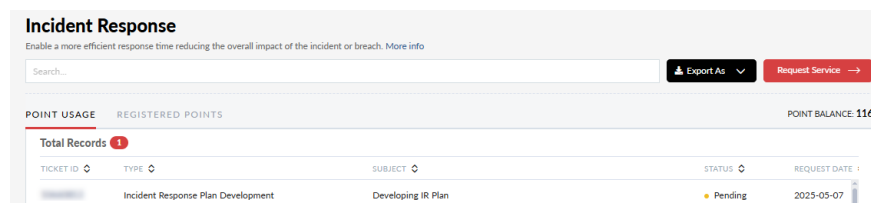
More information about each Advanced Services option is available in the Service Points description available in the [Customer Service portal](#).

Incident Response

Incident Response allows Fortinet Inc. customers with an active FortiGuard Incident Response service contract to request different service activities in exchange for Service Points. *Incident Response* provides support for planning your security posture, identifying gaps in your security processes, and develop a playbook in the event of a critical attack.

More information is available in the *FortiGuard Incident Response Service* description available in the [Customer Service portal](#).

The *Incident Response* view displays the support tickets for your account. Use this view to monitor the status of your support requests and the Service Points applied to each request. You can create a new service ticket or view the ticket and comment on it in FortiCloud.



Users must have access to the root folder in their permission scope and have the correct entitlement registered to view the *Incident Response* page. For information, see [Permission scope with Organizations](#) in the Identity & Access Management guide.

Eligible contracts

Incident Response Requests (IR Requests) are available to customers with the following contracts:

- FortiGuard Incident Readiness Subscription Service

Service requests

Incident Response Requests provide support for planning your security posture, identifying gaps in your security processes, and develop a playbook in the event of a critical attack. Services include Incident Response Support, Incident Response Playbook Development, and more.



For information on service points, see [Advanced Services](#) on page 32.

Point Usage

The *Point Usage* tab shows the Service Requests for your account as well the ticket type, status, and points consumed by each request.

Incident Response
Enable a more efficient response time reducing the overall impact of the incident or breach. [More info](#)

Search...

Export As Request Service

POINT USAGE REGISTERED POINTS POINT BALANCE: 116

Total Records 1

TICKET ID	TYPE	SUBJECT	STATUS	REQUEST DATE
	Incident Response Plan Development	Developing IR Plan	Pending	2025-05-07

Point Usage	Description
Ticket ID	The FortiCare Ticket number associated with the Service Request. Click the <i>Ticket ID</i> to view the request details in FortiCloud and to comment on the ticket.
Type	The type of service requested. See Incident Response types on page 46 .
Subject	The <i>Subject</i> text that was entered at the time the ticket was created. See Creating an Incident Response ticket on page 44 .
Status	<i>Pending</i>: This is the default status after a service request has been submitted. <i>Approved</i>: Indicates the scope of service to be delivered and the total number of service points has been agreed upon between you and Fortinet Inc.. <i>Canceled</i>: Indicates the service cannot be delivered. No points are applied. <i>Completed</i>: Indicates the agreed upon service has been delivered and you agree to close the Service Request.
Request Date	The date the service request was created.
Close Date	The date the service request was closed.
Points	The number of points used for this activity.

Registered points

The *Registered Points* tab shows the contracts registered to your account and the points balance for each contract. The entitlement period of the points corresponds to the contract period. This means any unused points will be forfeited on the contract expiry date. If there are multiple active contracts, the points are consumed based on a first-in-first-out rule to ensure the points that are expiring are used first.

Incident Response
Enable a more efficient response time reducing the overall impact of the incident or breach. [More info](#)

Search...

Export As Request Service

POINT USAGE REGISTERED POINTS POINT BALANCE: 116

Total Records 11

SERIAL NUMBER	CONTRACT#	LICENSE#	SKU	ACTIVATION DATE	EXPIRATION DATE	POINTS USED	BALANCE
				2024-12-25	2025-12-25	0	16
				2024-12-25	2025-12-25	0	10
				2024-12-25	2025-12-25	0	10

Points	Description
SN#	The account level product serial number.
Contract#	The contract number.
License#	The contract license number.
SKU	The reference number for the service type.
Activation Date	The contract registration date.
Expiration Date	The contract end date.
Points Used	The number of service points used by this contract.
Balance	The number of service points remaining for this contract. This number is updated each time a Service Request is moved to <i>Completed</i> .

To export the Point Usage and Registered Points:

1. Go to *Incident Response*.
2. Click *Export As* and select either *Excel File* or *CSV File*.

Creating an Incident Response ticket

When a new Incident Response request is created, the Service Points are reserved and your points balance is adjusted. After the request is submitted, a Fortinet Service representative will contact you to confirm the scope of the request and, if necessary, adjust the number of points accordingly. The reserved points will be deducted from your balance when the Incident Response is marked as *Completed*. If the ticket is canceled, the points are released.

To create an Incident Response request:

1. Go to *Incident Response*.
2. Click *Request Service*. The *Choose a Service* page opens.

STEP 1. Choose a Service

1. Choose a Service 2. Specify Ticket Information 3. Comment 4. Complete

Service Points for FortiGuard Incident Response Services: Customers with an active FortiGuard Incident Response Service contract can exchange their Service Points by creating a Service Request. Please note that a Service Type CAN NOT be selected if there are not enough points in the balance. [More details about the Service options](#)

POINT BALANCE **116**

Incident Response Support
Incident Response for assistance in case of security incident. The FortiGuard Incident Response team will set up a scoping call leading to the definition and delivery of a plan of action associated to a number of Service Points.

1 Point
/4 HOURS

Incident Response Readiness Assessment
Tailored evaluation of a customer's current security posture and Incident Response Plan. The Service is designed and delivered using real-world experiences and industry standard best practices.

10 Points
/REPORT

Incident Response Playbook Development
Assistance in development at a step-by-step playbook to be used in the event of an impactful cyber security incident. The plan of action and associate number of Service Points are based on a scoping call.

1 Point
/4 HOURS

Cyber Security Tabletop Exercise
Assistance in the testing of an incident response plan and identify security gaps in tools or processes. A report will be provided that includes policy recommendations based on the discussions held during the exercise.

1 Point
/4 HOURS

Security Operations Center (SOC) Assessment
SOC Assessment services evaluate, help optimize, and mature the SecOps and SOC functions for greatest enterprise risk reduction and continuous improvement. Measuring the coherence of the structure, visibility, response readiness and long term plan for the function, the services provide an objective, realistic set of recommendations, custom to the organization.

20 Points
/REPORT

Ransomware Readiness Assessment
The Ransomware Readiness Assessment is organized according to the NIST Cybersecurity Framework (CSF), focusing on the controls and capabilities most relevant to ransomware tools, techniques, and procedures (TTPs).

10 Points
/REPORT

Cancel Next

3. Select a service and click *Next*. See [Incident Response types on page 46](#).



You cannot select a service if there are not enough points in your balance.

4. Complete the *Specify Ticket Information* form.
 - a. In the *Contact Info* section enter your *Name*, *Email*, *Phone*, and *Mobile*.
 - b. In the *Product Info* section, use the *Subject* field to describe the request, and click *Next*.

STEP 2. Specify Ticket Information

1. Choose a Service 2. Specify Ticket Information 3. Comment 4. Complete

POINT BALANCE **116**

CONTACT INFO

NAME * EMAIL * (Separate multiple emails with a comma)

PHONE MOBILE

PRODUCT INFO

REQUEST TYPE CATEGORY

SUBJECT *

Cancel Previous Next

5. Add a comment and attachment.
 - a. In the *Comment* section, describe the attachment.
 - b. In the *Attachment* section, click *File Upload*.
 - c. From the menu, select *Log File*, *Configuration*, or *Other*.
 - d. Click *Next*.

STEP 3 . **Comment**

1. Choose a Service 2. Specify Ticket Information **3. Comment** 4. Complete

POINT BALANCE 116

COMMENT *

Note: The maximum characters system allow to be entered here is 8000.

ATTACHMENT

You specify the uploaded file's storage type by selecting it from the drop-down list. Files stored in 'Temporary Storage' will be deleted once the ticket is closed. The option 'Keep the file' means that the file will be retained after ticket closure. Virus samples and large files (>5MB) are always saved in temporary storage.



File Upload ▾

Cancel Previous Next

6. (Optional) Click *Create Another Ticket* to request another service.

Incident Response types

The following types of Incident Response options are available for request:

Service	Description	Points
Incident Response Support	Incident Response for assistance in case of a security incident. The FortiGuard Incident Response team will set up a scoping call leading to definition and delivery of a plan of action associated to number of a service points.	1
Incident Response Readiness Assessment	This Incident Response Option is a custom-tailored evaluation of an organization's current security posture and incident response plan. The Fortinet Incident Response Readiness Assessment is designed and delivered by the Fortinet Incident Response Proactive Team built using real-world experiences and industry standard best practices. The assessment is organized into six domains that each incorporate people, processes, and technology. The assessment will incorporate a mixture of document review and stakeholder input through workshops that will help to identify additional areas of improvement. • <i>Event and Incident Response (IR)</i>: Establish and maintain plans, procedures, and technologies to detect, analyze, and respond to cybersecurity events and to sustain operations throughout a cybersecurity event, commensurate with the risk to critical infrastructure and organizational objectives. • <i>Asset Management</i>: Manage the organization's information technology (IT) and operations technology (OT) assets, including both hardware and software, commensurate with the risk to critical infrastructure and organizational objectives.	10

Service	Description	Points
	• <i>Identify and Access Management</i>: Create and manage identities for entities that may be granted logical or physical access to the organization's assets. Control access to the organization's assets, commensurate with the risk to critical infrastructure and organizational objectives. • <i>Threat and Vulnerability Management</i>: Establish and maintain plans, procedures, and technologies to detect, identify, analyze, manage, and respond to cybersecurity threats and vulnerabilities, commensurate with the risk to the organization's infrastructure (e.g., critical, IT, operational) and organizational objectives. • <i>Continuity of Operations (COOP)/Disaster Recovery (DR)</i>: Ability of an organization to establish and maintain plans, procedures, and technologies to sustain operations and quickly recover from a cybersecurity incident, commensurate to business risks and defined organizational objectives. • <i>Network Security</i>: Ability of an organization to diagnose, configure, and maintain Network Security technologies to sustain operations throughout a cybersecurity incident, commensurate to critical infrastructure risks and defined organizational objectives.	
Incident Response Playbook Development	This Incident Response Option provides assistance to the Customer in the development of a step-by-step playbook to be used in the event of an impactful cybersecurity incident on its network based on the most likely incidents. This playbook is meant to help Customer's security analysts to handle a security incident from detection through eradication and recovery and may be part of an organization's larger incident response plan. Some of the current probable events may include: • A ransomware attack. • Phishing email messages. • A compromised user's credentials. The plan of action and associate number of Service Points are based on a scoping call.	1
Cyber Security Tabletop Exercise	This Service Option assists the Customer in testing its incident response plan and identifying security gaps in tools or processes. The Cyber Security Tabletop Exercises are designed and delivered by the Fortinet Incident Response Team and leverages their experience and expertise handling Incident Response engagements such as: • A ransomware attack. • Phishing email messages. • A compromised user's credentials.	1

Service	Description	Points
	Cyber Security Tabletop Exercises are then separated into several incident scenarios and then verbally discussed during a roundtable discussion to enhance the Customer's understanding of actions to be taken, and by whom they are performed under its incident response plan. At the end of this exercise, a report will be provided that includes policy recommendations based on the discuss held during the exercise. The plan of action and associate number of Service Points are based on a scoping call.	
Security Operations Center (SOC) Assessment	This Service Option is a custom-tailored evaluation of an organization's current security operations center. The Fortinet Security Operations Center Assessment is designed and delivered by the Fortinet Incident Response Proactive Team built using real-world experiences and industry standard best practices. The SOC Assessment is organized in four areas of focus that each incorporate people, processes, and technology. The assessment will incorporate a mixture of document review and stakeholder input via workshops that will help to identify additional areas of improvement. Focus Areas: • <i>Organization:</i> This focus area addresses the coherence of structures outside and inside the SOC Topics covered include the alignment of SOC with the business, the organization of the SOC itself, and how it fits in the Incident Response Plan (IRP). • <i>Visibility:</i> This area baselines and uncovers gaps in the SOC's ability to detect malicious activity. To do so, practices assess the maturity of use cases, logging, SIEM, and the use of threat intelligence. • <i>Response:</i> All the visibility in the world doesn't matter if the SOC response is not timely and thorough. The topics in this area cover triage, playbooks, workflows and data sharing, digital forensics, and communications planning. • <i>Evolution:</i> A SOC that achieves a certain maturity and then freezes in time will quickly lose its value as attackers evolve every day. The Evolution focus area explores the activities that sustain the SOC's continued improvement and responsiveness to new threat landscapes over time. The subjects include the SOC Strategic Plan, metrics, staff training, exercises, and the processes of security tool assessment and acquisition.	20

Service	Description	Points
Ransomware Readiness Assessment	This Incident Response Option is designed to help organizations gain greater visibility and understanding of their current risks to a ransomware attack. The Fortinet Ransomware Readiness Assessment is designed and delivered by the Fortinet Incident Response Proactive Team built using real-world experiences and industry standard best practices. The assessment focuses on the implementation and management of incident response cybersecurity practices specific to known ransomware attacks. This includes the TTPs of known ransomware as well as common issues and forensic evidence from across ransomware incidents investigated by the FortiGuard Incident Response team. Each assessment provides guidance on the approach to cybersecurity incident response maturity. Focus Areas: • <i>Identity</i>: The mix of IT and business-critical assets, threat intelligence, and vulnerabilities that determine an organization's ransomware attack surface. • <i>Project</i>: The defenses in place prevent ransomware vectors or, if an initial compromise is successful, halt further action (lateral movement, credential misuse) by the attacker. • <i>Detect</i>: Visibility to ransomware attackers as they enter and scout an environment before they fully strike. • <i>Evolution</i>: Reactions to ransomware that require a solid game plan with an understanding of the technical options, communication needs, and business impacts. • <i>Recover</i>: Clean, protected backups to restore systems quickly and large-scale mitigation planning to minimize a ransomware incident.	10
Compromise Assessment	This Incident Response Option is designed to identify hidden but active cyber threats in our customers' enterprise environment. It provides detailed threat hunting in Client infrastructure to discover the anomalies that could be signs of a past or ongoing compromise. This allows to identify past breach attempts and incidents, ongoing and/or undetected attack activities, including threat removal and provides advice and prevention plans to avoid future incidents. The Compromise Assessment ('CA') is conducted by the Fortinet Incident Response Proactive Team and can be combined with automated detection tools and further threat intelligence to create a clear view of the actual threats in the network and what needs to be done to ensure attacks are not repeated. The CA provides organizations with a clear and decisive answer to the question, "are we breached?". It provides all the information needed in case there is a compromise.	1

Service	Description	Points
	What makes FortiGuard IR team powerful is the independent of other third-party tools, especially on the collection phase. 99% of the used software are developed by Fortinet. The below list mentions the products that may be used during a CA engagement: • FortiEDR/FortiXDR • FortiNDR • FortiSandbox • FortiRecon/FortiGuard • FortiDeceptor The plan of action and associate number of Service Points are based on a scoping call.	
Active Directory Security Assessment	This Incident Response Option provides a third-party, objective, review of the security posture of an Active Directory ('AD') installation. It helps to identify critical issues and areas of the highest concern. It also provides the organization a means for tracking the continuing improvement and maturity of the Active Directory security posture. The Service is organized in five areas of focus that each incorporate people, processes, and technology. Each of the areas consists of a number of maturity practices that are used to assess the AD installations security and fit for purpose within the larger business mission, current threats, and capacity to evolve efficiently over time. Focus Areas: • <i>Policy and procedures</i>: this area starts with governance and basic procedures that are derived from the goals and objectives of the governance policies. The focus will be ensuring that your AD installation has proper executive backing and resources, as well as basic procedures that ensure the environment is ready for adverse events and incident response. • <i>Account Management</i>: This area addresses account management policies, procedures, and security settings which are derived from various standards bodies and Microsoft publications. Many issues addressed in this section are considered to be critical to the security of AD and your IAM program. • <i>Network and Host Configuration</i>: AD hosts are high value targets for threat actors and need to be hardened. In addition, based on its utility and design, AD is frequently deployed redundantly and to multiple locations within the organization. This section addresses both network and host security configuration issues.	1

Service	Description	Points
	• <i>Audit Configuration:</i> In order to ensure visibility for auditing and investigation, default audit configurations need to be verified, and specific audit flags may need to be set. If proper auditing is not enabled then information will not be collected, and critical questions about access and activities may not be able to be answered. This section covers the most important audit settings based on both Microsoft and standards bodies recommendations. • <i>Monitoring:</i> Because AD and Administrator accounts are high value targets for threat actors, continuous monitoring of some critical AD events needs to be implemented. This section reviews the most critical events which should be monitored and reviewed for legitimacy and authorization. The plan of action and associate number of Service Points are based on a scoping call.	
Vulnerability Assessments	This Service is designed to identify known vulnerabilities within information systems or services. With this assessment, you'll understand the known vulnerabilities within your organization's internal and external networks and applications. Our experts use various automated tools and manual techniques to systematically examine your environment to determine the effectiveness of your current security measures, identify security gaps, and provide data to help you predict how impactful the safeguards you have in place today will be in the future. After the technical phases of the assessment are completed, our team prepares a report, sharing the potential issues found during the assessment along with recommended remediation procedures. As a result, it's easy for your team to prioritize remediation efforts according to identified severity levels of Critical, High, Medium, or Low—following the Common Vulnerability Scoring System (CVSS) standard—and the overall risk each vulnerability represents to the organization. • <i>Internal Network:</i> Our team is equipped to conduct internal network vulnerability assessments to evaluate your organization's internal network and devices. These assessments are scoped based on the number of IP addresses included. • <i>External Network:</i> The external network vulnerability assessment focuses on the external or internet-facing systems you make available, including web servers, database servers, network devices, and other network-based equipment. These assessments are scoped based on the number of IP addresses included. • <i>Web Application:</i> The FortiGuard Web Application Vulnerability Assessment focuses on one or more web	1

Service	Description	Points
	applications to identify known or unknown vulnerabilities within the application. The vulnerability assessment also identifies areas where confidentiality, availability, or systems data integrity compromises exist. These assessments are scoped based on the number of your organization's web applications. • <i>Mobile Application:</i> The FortiGuard Mobile Application Vulnerability Assessment focuses on one or more mobile applications to identify known or unknown vulnerabilities. The vulnerability assessment also identifies areas where confidentiality, availability, or systems data integrity compromises exist. These assessments are scoped based on your organization's number of mobile applications.	
Penetration Test	This Service is a specialized assessment our team conducts on networks, systems, and applications to identify unknown vulnerabilities that an adversary could exploit. Penetration testing mimics real-world attacks to pinpoint potential ways that threat actors might impact the confidentiality, integrity, or availability of your networks, systems, and applications. When conducting a penetration test, our team of experts uses various tools and techniques commonly utilized by attackers to detect vulnerabilities and test the resilience of your organization's network. • <i>Internal Networks:</i> Our team is equipped to conduct internal network penetration testing to evaluate threats to your organization's internal network and devices. These assessments are scoped based on the number of IP addresses included. • <i>External Networks:</i> External network penetration testing focuses on the external, or internet-facing, systems your organization makes available, including web servers, database servers, network devices, and other network-based equipment. These assessments are scoped based on the number of IP addresses included. • <i>Web Applications:</i> The FortiGuard Web Application Vulnerability Penetration Test focuses on one or more web applications with the goal of identifying known and previously unknown vulnerabilities within the application. The test also evaluates the ability to use discovered vulnerabilities to further penetrate the organization. It looks for areas where somebody could compromise the confidentiality, availability, or integrity of systems or data. These assessments are scoped based on the number of your organization's web applications. • <i>Mobile Applications:</i> The FortiGuard Mobile Application	1

Service	Description	Points
	Penetration Test focuses on one or more mobile applications with the goal of identifying either known or unknown vulnerabilities within the application. The test also evaluates the ability to use discovered vulnerabilities to further penetrate the organization. It looks for areas where somebody could compromise the confidentiality, availability, or integrity of systems or data. These assessments are scoped based on the number of your organization's mobile applications.	

More information about each Incident Response option is available in the *Service Points* description available in the [Customer Service portal](#).

Downloads

You can download Cloud and product resources, such as VM images and service updates, from the *Downloads* pages.

This section includes the following:

- [Firmware Images on page 54](#)
- [VM Images on page 55](#)
- [Service Updates on page 56](#)
- [HQIP Images on page 57](#)
- [Get Checksum Code on page 58](#)

Firmware Images

You can download product firmware images, review the suggested upgrade path, and access the FortiGate Support Tool from the *Downloads > Firmware Images* page.



Firmware image downloads are available only for registered products with an active support contract. Ensure your product is registered as well as has an active support entitlement to access firmware downloads.

To download firmware images or checksum code:

1. Go to *Downloads > Firmware Images*.
2. Select the *Download* tab.
3. Select the product you want from the *Select Product* dropdown list.
4. Select the major, minor, and patch version that you need from the provided folders.

Firmware Images
Firmware Images download centre for Fortinet's extensive line of security solutions.

Select Product: FortiGate Search...

RELEASE NOTES **DOWNLOAD** UPGRADE PATHS FORTIGATE SUPPORT TOOL

/ FortiGate / v6.00 / 6.2 / 6.2.1

NAME	SIZE (KB)	DATE CREATED	DATE MODIFIED
FSSO		2019-08-13	2019-08-14
MIB		2019-08-13	2019-08-14
FGT_...-FORTINET.out	21.912	2019-08-14	2019-08-14

HTTPS Checksum

5. Click *HTTPS* for the image you want to download.
6. Click *Checksum* to view the checksum code.

To view the upgrade path:

1. Go to *Downloads > Firmware Images*.
2. Select the *Upgrade Paths* tab.
3. Select the product you want from the *Current Product* dropdown list.
4. Select the current and desired versions from the dropdown lists.

5. Click *Confirm*.

VM Images

You can refresh, upgrade the path, and access release notes of product VM images from the *Downloads > VM Images* page. You can select the product, platform, and versions.

Select *Refresh* to update the information on the VM Images page. Select *Release Notes* to be directed to the product release notes on the Document Library.

To upgrade the path:

1. Go to *Downloads > VM Images*.
2. Select the product whose path you want to update from the *Select Product* dropdown list.

3. Select the platform hosting the VM from the *Select Platform* dropdown list.

The screenshot shows the 'VM Images' page with the 'Select Platform' dropdown menu open. The menu lists various platforms: AliCloud, AWS, Azure, Google, Hyper-V, IBM, KVM, OCI, Oracle, Rackspace, VMWare ESXi, VMWare NSX, and Xen. The 'LATEST VERSIONS' tab is selected, showing versions 7.6.3 and 7.4.8.

4. Click *Upgrade Path*. You will be directed to the *Firmware Images* page to proceed.

The screenshot shows the 'Firmware Images' page with the 'Upgrade Path' tab selected. The 'Current Product' is set to 'FW_1801F'. The 'Current FortiOS Version' is '6.4.11' and the 'Upgrade To FortiOS Version' is '6.4.12'. A 'GO' button is visible at the bottom.

Service Updates

You can access and download FortiGuard service updates from the *Downloads > Service Updates* page. Service updates are available for multiple products, including but not limited to:

- FortiGate

The screenshot shows the 'Service Updates' page with the 'Select Product' dropdown set to 'FortiGate' and the 'OS Version' dropdown set to 'v7.4.0'. A list of products is displayed, including ELA Fortigate VM Post Pay, ELA Fortigate VM Pre Pay, FortiGate 1801F, FortiGate 601E, FortiGate 61E, FortiGate 61F, and FortiGate VM Subscription.

- FortiClient

Service Updates
Download FortiGuard service updates

Select Product: FortiClient Version: v6.2.0

ANTI-VIRUS	ANTI-SPAM	ANTI-SPYWARE	APPLICATION DEFINITIONS
OS6.2.0_67.00840.fct100 (MD5)	OSWIN6.2.0_75.00170.fct100 (MD5)	OSWIN6.2.0_75.00170.fct100 (MD5)	OSWIN6.2.0_75.00170.fct100 (MD5)
OS6.2.0_75.00170.fct100 (MD5)			
OSWIN6.2.0_75.00170.fct100 (MD5)			

To download a service update:

- Go to *Downloads > Service Updates*.
- Select the product from the *Select Product* dropdown list.



The *Service Updates* page and options vary depending on the selected product.

- Select the appropriate version from the *Version* dropdown list.
- Select the appropriate service update you need from the available options. A verification message is displayed.
- Enter the provided Captcha Code and click *Confirm*.

HQIP Images

Hardware Quick Inspection Package (HQIP) is a hardware diagnostic firmware image that detects hardware problems on FortiGates. An HQIP image file is required to perform an HQIP test which can be acquired in the *Downloads > HQIP Images* page.

HQIP Images
A knowledge base article is available to explain the use of the HQIP (Hardware Quick Inspection Package) image. Click [HQIP Article](#) for more details.

Please enter the serial number to start

HQIP Images are associated to the serial number of the unit to be tested. Enter the serial number to start. After you enter the first three character, related serial numbers will be displayed. Select one from the list to proceed

Enter three characters to start

[Get HQIP Info](#)

To get the HQIP image:

- Go to *Downloads > HQIP Images*.
- Enter the serial number in the provided field.
- Click *Get HQIP Info*.

Get Checksum Code

You can retrieve the image checksum for firmware images in the *Downloads > Get Checksum Code* page by entering the firmware image file name and clicking *Get Checksum Code*.

Get Checksum Code
Retrieve firmware images checksums

Please enter the **firmware image file name** to get the checksum code

Sample firmware image file name: FGT_100D-v5-build0642-FORTINET.out

Get Checksum Code

Product Life Cycle

A product's hardware, software, and services life cycles can be viewed and exported in the *Product Life Cycle* page.

Select *RSS* to view the RSS feed for End of Order (EOO) announcements.

To export the product life cycle:

1. Go to *Product Life Cycle*.
2. Select the type of file you would like from the *Export* dropdown menu. The file is downloaded to your device.



Life cycle information for all of the products are included in the spreadsheet. You can filter by product to view the specific information you want.

Hardware

The *Hardware* tab displays information on product hardware End of Order (EOO) dates, End of Support (EOS) dates, and Last Service Extension Date (LSED). Select a dropdown menu to view the available hardware information. Select the *Product* to view more detailed information, if it is available.

Product Life Cycle

For more information about the Fortinet Product Lifecycle, click [here](#)

Search... Export

HARDWARE SOFTWARE SERVICES

Hardware information last updated date: 2025-06-11 | You can also access the latest information by adding our RSS feed. Simply copy the RSS URL and follow your RSS reader's instructions for adding a new RSS feed to proceed. [View](#)

► Accessory

► Ascenlink

◄ ControllerWireless

PRODUCT	END OF ORDER DATE (EOO)	LAST SERVICE EXTENSION DATE (LSED)	END OF SUPPORT DATE (EOS)
ANT-A080-NM-2	2022-05-02	2026-05-02	2027-05-02

The *Last Supported Software Version (LSSV)* has been added to the *Product Life Cycle > Hardware & VM* tables where applicable. For example, the LSSV is listed for certain FortiGate products.

HARDWARE & VM

SOFTWARE

SERVICES

Hardware information last updated date: 2026-03-13 | You can also access the latest information by adding our RSS feed. Simply copy the RSS URL and follow your RSS reader's instructions for adding a new RSS feed to proceed [Learn More](#)

FortiGate

PRODUCT	END OF ORDER DATE (EOD)	LAST SERVICE EXTENSION DATE (LSED)	END OF SUPPORT DATE (EOS)	LAST SUPPORTED SOFTWARE VERSION (LSSV)
FortiGate-1000C-USG	2017-01-17	2021-01-17	2022-01-17	
FortiGate-1000D	2023-04-16	2027-04-16	2028-04-16	6.4.0
FortiGate-1000D-LENC	2025-06-29	2029-06-29	2030-06-29	
FortiGate-1000D-USG	2023-07-15	2027-07-15	2028-07-15	7.0.0
FortiGate-100A	2009-04-15	2013-04-15	2014-04-15	
FortiGate-100D	2018-07-26	2022-07-26	2023-07-26	
FortiGate-100D-G	2017-08-29	2021-08-29	2022-08-29	
FortiGate-100D-LENC	2020-01-14	2024-01-14	2025-01-14	
FortiGate-100E	2021-08-17	2025-08-17	2026-08-17	
FortiGate-100E-LENC	2022-05-30	2026-05-30	2027-05-30	

Software

The *Software* tab displays information on product software version support and life cycle information. Select a dropdown menu to view the available software version information.

Product Life Cycle

For more information about the Fortinet Product Lifecycle, click [here](#)

Search...

Q

Export

HARDWARE

SOFTWARE

SERVICES

Software information last updated date: 2025-06-18 | You can also access the latest information by adding our RSS feed. Simply copy the RSS URL and follow your RSS reader's instructions for adding a new RSS feed to proceed [Learn More](#)

This Software Support Policy applies to any and all software produced and / or sold by Fortinet, covering firmware for appliances and applications ("Software") installed on customer owned systems.

Fortinet will provide Engineering Software support for thirty six (36) months from the GA release date of the major or minor release. Fortinet will also provide "Must Fix" support for an additional eighteen (18) months from the End of Engineering Support date for software which was supported on or released after August 1, 2015. "Software Releases" constitute either major or minor version increments and support is provided on the latest patch release of each version.

The following tables provide details on the current supported versions and End of Support dates for each of these:

FortiADC

FortiADC Manager

SOFTWARE VERSION	RELEASE DATE (GA)	END OF ENGINEERING SUPPORT DATE (EDES)	END OF SUPPORT DATE (EOS)
5.2	2019-01-01	2022-01-01	2023-07-01
...	...	...	...

Long term support information is included where applicable. For example, FortiOS version 7.0.0 is marked as *Long Term Support* and the Extended End of Support (EOS) is identified.

Product Life Cycle

For more information about the Fortinet Product Lifecycle, click [here](#)

Search...

Q

Export

HARDWARE

SOFTWARE

SERVICES

Software information last updated date: 2025-06-18 | You can also access the latest information by adding our RSS feed. Simply copy the RSS URL and follow your RSS reader's instructions for adding a new RSS feed to proceed [Learn More](#)

This Software Support Policy applies to any and all software produced and / or sold by Fortinet, covering firmware for appliances and applications ("Software") installed on customer owned systems.

Fortinet will provide Engineering Software support for thirty six (36) months from the GA release date of the major or minor release. Fortinet will also provide "Must Fix" support for an additional eighteen (18) months from the End of Engineering Support date for software which was supported on or released after August 1, 2015. "Software Releases" constitute either major or minor version increments and support is provided on the latest patch release of each version.

The following tables provide details on the current supported versions and End of Support dates for each of these:

FortiNAC-F

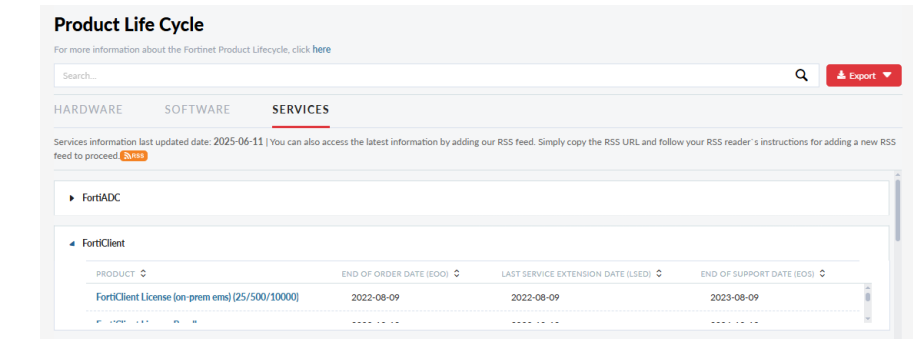
FortiNDR

FortiOS

SOFTWARE VERSION	RELEASE DATE (GA)	END OF ENGINEERING SUPPORT DATE (EDES)	END OF SUPPORT DATE (EOS)
7.0.0 (Long Term Support)	2025-06-30	2028-06-30	2029-12-30 (Extended EOS: 2031-06-30)

Services

The *Services* tab displays information on product services End of Order (EOO) dates, End of Support (EOS) dates, and Last Service Extension Date (LSED). Select a dropdown menu to view the available service information.



Select the *Product* to view more detailed information, if it is available.

Resources

The *Resource* page provides links to help and reference resources. Select a link for more information on the available resource.

Resources

QUICK LINKS

Community (Knowledge Base)

Customer Support Bulletin

Video Library

Product Life Cycle

Training & Certification

DOCUMENTS

Technical Documentation

Fortinet Service Terms & Conditions

Guidelines, Policies & Documents

Help Documents

FORTIGUARD

Advisories & Reports

FortiGuard Services

FortiGuard Outbreak Alerts

FortiGuard Blog

Global Threat Level

Resources Library

PROGRAMS

Support Offerings

Premium Support

Priority RMA

Professional Services

Resources available include:

Category	Resources
Quick Links	Provides links to support, reference, and training materials.
Documents	Provides links to help, administration, and reference documentation.
FortiGuard	Provides links to FortiGuard services and resources.
Programs	Provides links to FortiCloud program resources.

Bug Tracker

The bug tracker provides an overview of active bugs being tracked by the Global Technical Support organization.



The *Bug Tracker* page is only available to Partners. For more information, see the [Partner Administration Guide](#).

Customer Support Bulletin

The *Customer Support Bulletin* displays important new features, bug fixes, and Fortinet Inc. content at a high level.

Customer Support Bulletin

New features, bug fixes, and content highlights you don't want to miss

CSB-250527-1

FortiDLP Agent 12.0.5 Re-release

FortiDLP Agent releases 12.0.4 and 12.0.5 were temporarily removed from the FortiDLP Agent download options

2025-05-30
10:34

CSB-250501-1

FortiDDoS and FGT Migration to IPSEC

FortiDDoS tuning may be required for FortiGate migration to IPsec VPN

2025-05-05
05:33

CSB-250430-1

IPS engine 7.1040 released to FortiGuard™

New IPS engine released to FortiGuard

2025-04-30
07:22

CSB-250416-1

FortiOS 7.6.3 SSL-VPN to IPsec VPN Migration

SSL-VPN migration to IPsec VPN prior to upgrade to FortiOS 7.6.3

2025-04-17
11:10

CSB-250415-1

FortiDDoS F-Series Continuous Restarts

FortiDDoS restarting after FortiGuard update

2025-04-16
03:16

Select a bulletin card to expand it for more information.

Customer Support Bulletin

New features, bug fixes, and content highlights you don't want to miss

CSB-250527-1

FortiDLP Agent 12.0.5 Re-release

FortiDLP Agent releases 12.0.4 and 12.0.5 were temporarily removed from the FortiDLP Agent download options

2025-05-30
10:34

Description:

On May 13, 2025, FortiDLP Agent releases 12.0.4 and 12.0.5 were temporarily removed from the FortiDLP Agent download options within the FortiDLP UI, due to a reported issue with the upgrade that may affect device restart. The upgrade issue is limited to the 12.0.4 and 12.0.5 releases for Linux, and the current FortiDLP Agent release 12.1.0 for Linux is not affected

Affected Products:

FortiDLP Agent 12.0.4 and 12.0.5 for Linux.

Affected OS:

Linux

Resolution:

The FortiDLP Agent release 12.0.5 will soon be made available as a download option in the FortiDLP UI, for Windows and macOS platforms only. As 12.0.4 was replaced by 12.0.5 as the latest maintenance release for the 12.0.x agent, release 12.0.4 will not be reinstated. Customers should review the Automatic upgrades setting in FortiDLP agent configurations in the UI and Customers should ensure that any agent configurations targeted to Linux devices are set to 12.1.0 release, or Latest. If preferred, a separate agent configuration targeted (labelled) specifically for Linux devices can be used to upgrade only Linux devices.

FortiCare 26.2.a Administration Guide
Fortinet Inc.

64

Technical Web Chat

You can join a live chat with a FortiCare support employee using the *Technical Web Chat* page. Live chats can be useful for asking general questions about FortiCare products and services.

To join a web chat:

1. Go to *Technical Web Chat*.
2. Select a product model from the *Product Model* dropdown list.

SN#	DESCRIPTION	REGISTRATION DATE
ABMC		Sep 24 2023
ELAVM		
ELAVM		Aug 16 2023

3. Select a serial number from the *SN#* list. The *Technical Assistance Chat* opens.
4. Answer the questions posed in the chat.

How can we help?

Fortinet

Let us know what you're contacting us about.

Fortinet

Technical Assistance Chat

JULY 16, 2024 AT 2:46 PM

Are you a government user?

Yes

No

Please provide your First Name

Type a message... Send

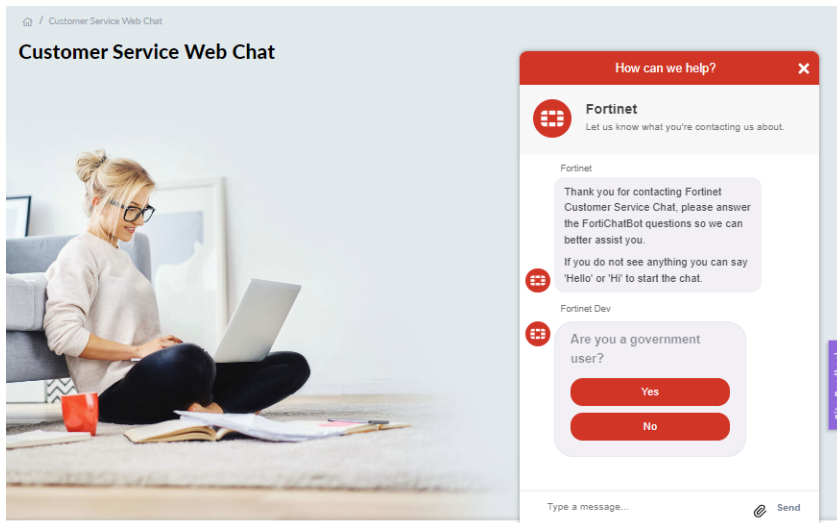
5. Once all of the information has been collected, you will be directed to a live chat.

Customer Service Web Chat

You can join a live chat with a FortiCare support employee using the *Customer Support Web Chat* page. Live chats can be useful for asking general questions about FortiCare products and services.

To start a customer service web chat session:

1. Go to *Customer Service Web Chat*.
2. Answer the preliminary information questions posed in the chat.



3. Once all of the information has been collected, you will be directed to a live chat.

Ticket survey

You can submit feedback and rate your experience with solving a ticket through a ticket survey.



Only one customer survey can be created per ticket. When multiple surveys are submitted, the rating is updated and comments from the new survey are appended to the original survey response.

Any user that can access the ticket can create a survey if there is no pre-existing survey. If there is a pre-existing survey, any user that can access the ticket can edit the survey until 15 days have passed following the closing of the ticket.

To rate your experience:

1. Go to *Ticket Survey*.
2. Select the *Ticket#*. The *Customer Satisfaction Survey* opens.

3. Select a rating out of five stars for *Your overall satisfaction* and *Fortinet made it easy for me to resolve my issue*.
4. Enter feedback in the comment fields.
5. Enter your phone number and email if you would like to speak further with a manager.
6. Click *Submit My Feedback*. Your experience survey is submitted.

Multilingual survey support

The *Ticket Survey* page is supported in multiple languages, including:

- English
- Chinese
- French
- German
- Italian
- Japanese
- Korean
- Portuguese
- Spanish
- Thai

To change the language:

1. Go to *Ticket Survey*.
2. Select the *Ticket#*. The *Customer Satisfaction Survey* opens.

The screenshot shows the Fortinet Customer Satisfaction Survey interface. At the top, there is a header bar with a search icon, the text "/ Ticket Survey", the ticket number "TICKET # 8669777", the word "Test", and a language dropdown menu set to "English". Below the header, the main content area is divided into two columns. The left column contains the survey questions: "Customer Satisfaction Survey", "Regarding your recent Support Experience, please rate the following questions on a scale of 1 (Poor) to 5 (Excellent) Stars:", "Your OVERALL Satisfaction *", "Fortinet made it easy for me to resolve my issue *", "What could we do to improve your support experience?", "Please suggest any improvement(s) that you would like to see in our products or services.", and "If you would like to speak to a manager about your support experience, please provide your phone number and/or email address.". Each question has a corresponding star rating or text input field. At the bottom of the left column is a blue "Submit My Feedback" button. The right column contains the Fortinet logo, a greeting "Dear Customer,", a thank you message, a statement about feedback review, contact information for CustomerCare@fortinet.com, and a sign-off "Best Regards, Fortinet Customer Services & Support". A purple speech bubble icon is located at the bottom right of the right column.

3. Select the language dropdown list. A list of supported languages is displayed.

Ticket survey

Ticket Survey

TICKET # 8669777

Test

English

English

Chinese

French

German

Italian

Japanese

Korean

Portuguese

Spanish

Thai

Customer Satisfaction Survey

Regarding your recent Support Experience, please rate the following questions on a scale of 1 (Poor) to 5 (Excellent) Stars:

Your OVERALL Satisfaction *

Fortinet made it easy for me to resolve my issue *

What could we do to improve your support experience?

Please suggest any improvement(s) that you would like to see in our products or services.

If you would like to speak to a manager about your support experience, please provide your phone number and/or email address.

Submit My Feedback

FORTINET.

Dear Customer,

Thank you for taking the time to provide feedback on your ticket.

We value and appreciate your feedback and would like to highlight that all surveys are reviewed on a weekly basis by Fortinet management with the aim of improving the service we provide to you.

If you have any queries regarding this survey, please contact CustomerCare@fortinet.com.

Best Regards,

Fortinet Customer Services & Support

4. Select the language you want. The ticket survey will change to the selected language.

Ticket Survey

TICKET # 8669777

Test

English

English

Chinese

French

German

Italian

Japanese

Korean

Portuguese

Spanish

Thai

Customer Satisfaction Survey

Regarding your recent Support Experience, please rate the following questions on a scale of 1 (Poor) to 5 (Excellent) Stars:

Your OVERALL Satisfaction *

Fortinet made it easy for me to resolve my issue *

What could we do to improve your support experience?

Please suggest any improvement(s) that you would like to see in our products or services.

If you would like to speak to a manager about your support experience, please provide your phone number and/or email address.

Submit My Feedback

FORTINET.

Dear Customer,

Thank you for taking the time to provide feedback on your ticket.

We value and appreciate your feedback and would like to highlight that all surveys are reviewed on a weekly basis by Fortinet management with the aim of improving the service we provide to you.

If you have any queries regarding this survey, please contact CustomerCare@fortinet.com.

Best Regards,

Fortinet Customer Services & Support

Guidelines and Policies

The *Guidelines and Policies* page provides links for reference documents on ticket guidelines, policies, and cloud service descriptions.

Guidelines and Policies

CATEGORY

TOTAL

Forti-Companions and Ticket Creation Guide

4

Service Descriptions

54

Select a *Category* dropdown to view the available documents.

Guidelines and Policies

CATEGORY

TOTAL

Forti-Companions and Ticket Creation Guide

4

Service Descriptions

54

DOCUMENT

VERSION

LAST MODIFICATION

Advanced Services - Service Relationship Manager

1.1

04/05/2022 6:33:20 AM

Advanced Services - Technical Support for Service...

3.2

05/30/2022 1:51:47 AM

EAP - Advanced Services - Enterprise Agreement...

v3.2

05/13/2022 5:59:20 AM

EAP - Basic Support Services - Enterprise Agree...

v2.2

05/13/2022 6:04:29 AM

EAP - Enterprise Product Agreement - Enterprise ...

1.0

05/13/2022 6:18:48 AM

EAP - Security Fabric Services - Enterprise Agree...

v1.4

05/13/2022 6:05:31 AM

FortiAuthenticator Cloud

v1.0

11/04/2022 9:28:45 AM

Preferences

You can set your personal preferences on the *Preferences* page. Available settings include:

Setting	Definition
Allow ticket processing by email	Email ticket processing can streamline your support experience. When enabled, you can submit and manage tickets by email. When disabled, all ticket-related interactions must be performed within the portal.
Use Pacific Standard Time	Allow the FortiCare portal to adjust settings to match the Pacific Standard Time timzone. If this feature is disabled, the default timezone is your local timezone. The current timezone being used by the portal can be identified in the bottom, left corner of the portal.
Expand last 3 comments	Enable this option to view in-depth comments and discussions related to the preferences and settings. When activated, you can see the three most recent comments for tickets.
Customize columns on ticket list	Select which columns to automatically display on the <i>Tickets</i> lists. Choose from a variety of information fields to create a personalized and efficient overview of your support tickets.



When changes are made in the *Preferences* page, confirmation dialogs may appear. Once confirmed, click *Update* to save the changes.

User permissions

The tickets and features available in the FortiCare portal are dependent on the user and permission type used to access the portal.

Different user and access types include:

- IAM user, external IdP roles, and Partner accounts. See [User access on page 72](#).
- Organization member account access. See [Organization view on page 74](#).

User access

FortiCare features and available tickets are dependent on the type of user logged in and their assigned permissions.

IAM users and external IdP roles

If you are logged in as an IAM user or external IdP role, FortiCare access and features depend on the user's assigned permission profile. When creating a permission profile with FortiCare portal access, you can assign access based on individual FortiCare resources using the *FortiCare* option. See [Portals with resource-based permissions](#) in the Identity & Access Management guide for more information.

FORTICARE			
RESOURCES			
Customer Service Tickets	☐	☐	☒
Technical Support Tickets	☐	☐	☒
RMA Tickets	☐	☐	☒
Advanced Service Requests	☐	☐	☒
Incident Response Ticket	☐	☐	☒
Web Chat	-	☐	☒
Survey Tickets	-	☐	☒
Support Resources	☐	-	☒



The FortiCare Legacy portal permissions can be assigned using the role-based *FortiCare Legacy* option.

Partners

When a Partner logs in, they must select a connected account to access the registered assets for that account. For more information, see the [Partner Administration Guide](#).

Partner aggregated view

When accessing the FortiCare portal as a Partner, the *Tickets > All Tickets* list is displayed in an aggregated view to include the connected Partner roles' assets. For more information, see the [Partner Administration Guide](#).

Partners without a FortiCloud account and connected accounts

If a Fortinet Partner account that does not have a FortiCloud account or any connected accounts, the Partner will be directed to the FortiCare portal upon logging in. The *Services* dropdown menu will be unavailable for switching to other portals. For more information, see the [Partner Administration Guide](#).

Sub users



The Sub User model will be deprecated in the near future. It is strongly recommended that you use the IAM User Model to take full advantage of the new features.

The abilities of sub users in the FortiCare portal depends on the access permission defined by the Master account user. The sub user permissions can be defined in the *My Account > Manage User > User Details* page. The Master account user can assign the *Permission* as either *Full Access* or *Limit Access*, with various features selected.

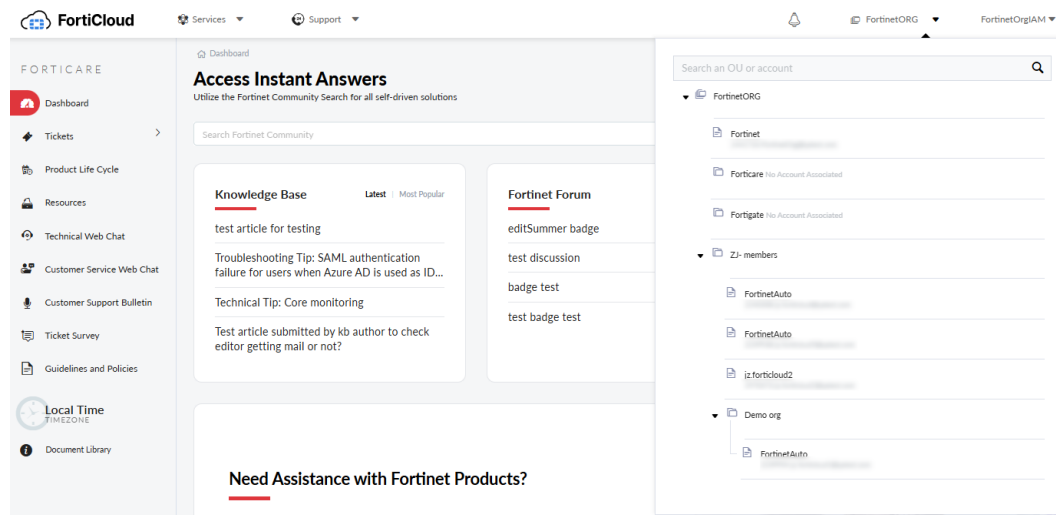
The screenshot displays the 'Edit User' interface in the FortiCare portal. At the top, there's a header bar with 'Account' and 'FortiCare FortiCare'. To the right, it shows 'Company: Fortinet', 'Activated Since: 2011-09-09', and fields for 'Title', 'Email', and 'Telephone'. On the left, a sidebar lists 'Account' with options: 'Account Profile', 'Change Account ID (Email)', 'Manage User' (highlighted), and 'My Account (IAM version)'. The main content area is titled 'Edit User' and contains a 'User Info' section with fields for 'User Name' (containing 'name 31092'), 'Telephone', 'Email (Account ID)', and a 'Description' text area. Below this is the 'Permissions' section with two radio buttons: 'Full Access' and 'Limit Access' (which is selected). Under 'Limit Access', there are several checkboxes: 'Customer Service' (checked), 'RMA/DQA' (checked), 'Technical Assistance' (checked), 'Notify the master account of ticket updates' (unchecked), and 'Can create user' (unchecked).

If *Limit Access* is selected, anything not selected from the additional permissions is not available to the sub user. FortiCare access depends on these permissions.

Organization view

Users logged into FortiCloud with Organization access can view tickets based on Organization, Organizational Units (OUs), or member accounts. Tickets displayed on the *Tickets* page will only include tickets pertaining to the selected scope, see [Permission scope](#) in the Identity & Access Management administration guide.

You can switch between Organization member accounts and OUs using the context switch menu. See [OU context switch](#) in the Identity & Access Management guide for more information.

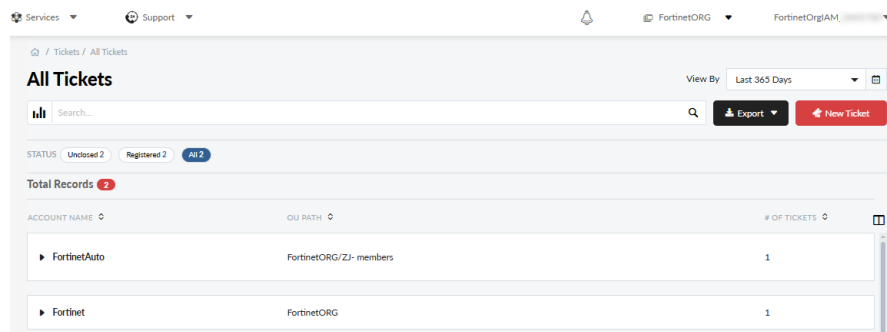


Organizational Unit (OU) view

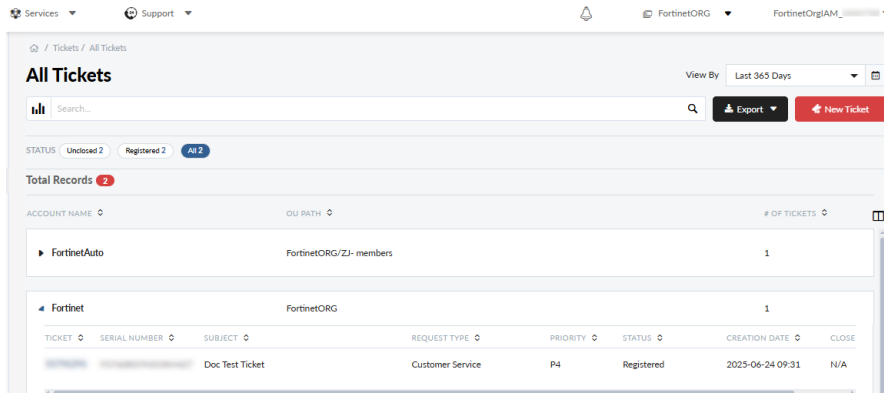
When an OU is chosen for the selected scope, the tickets displayed include tickets that relate to any of the member accounts within that OU. The *Tickets* page will be organized by the member accounts within the OU.



Any assigned filters will affect all the member account tickets within the OU. See [Filtering tickets on page 12](#) and [Searching for tickets on page 13](#) for more information on filtering tickets.



To view ticket details, expand the member account to review all of the tickets included for that member account.



To create a ticket in Organizational Unit view:

1. Go to *Tickets*.
2. Select *New Ticket*. The *Select An Account* dialog is displayed.

Select An Account

I Want to Create a Ticket for

Search an OU or account

FortinetORG

Fortinet

Forticare No Account Associated

Fortigate No Account Associated

ZJ- members

FortinetAuto

FortinetAuto

iz.forticloud2

Demo org

FortinetAuto

3. Hover over the account you want to assign the ticket to and click *Select*.



If you are a Partner, another *Select An Account* dialog is displayed prompting you to choose a connected account or proceed as a Partner. See [Partners on page 72](#).

4. Select the ticket type and proceed with the ticket creation process. See [Creating tickets on page 15](#).

Member account view

When a member account is chosen as the selected scope, the tickets displayed relate only to the selected member account. New tickets can only be created for the selected member account.



www.fortinet.com

Copyright© 2026 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.