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

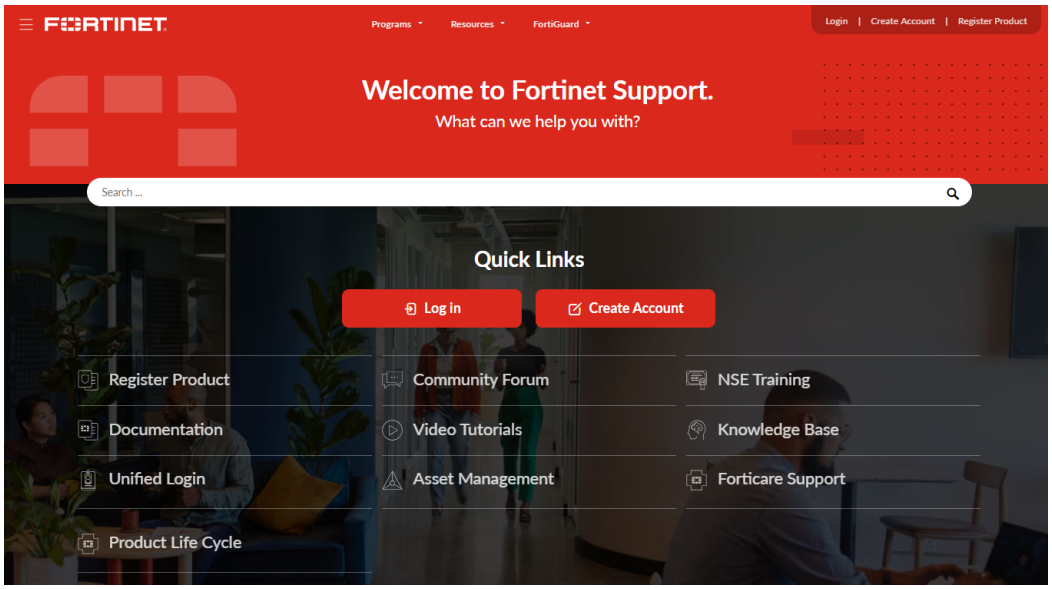
There are no new features included in FortiCare version 26.2.a. See the FortiCloud Services Release Notes for more information.

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.



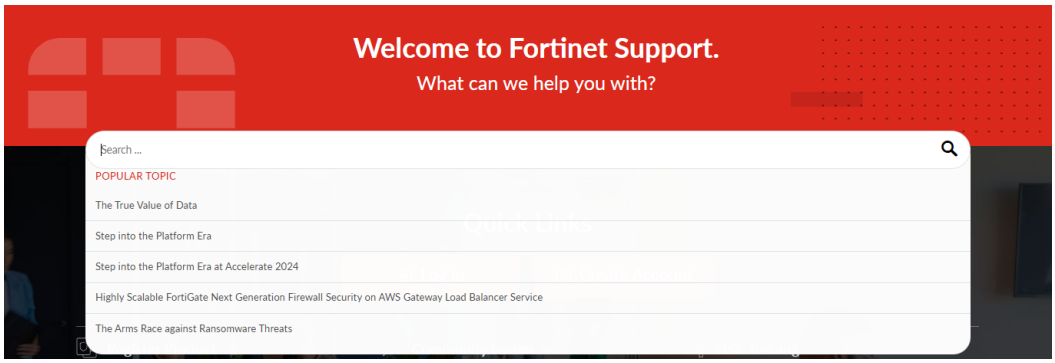
Users can also access FortiCloud Services and portals, including the FortiCare portal, through forticloud.com. If you log in through forticloud.com, you will be directed to the Asset Management dashboard instead of the FortiCare dashboard. See FortiCloud Services landing page in the Asset Management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

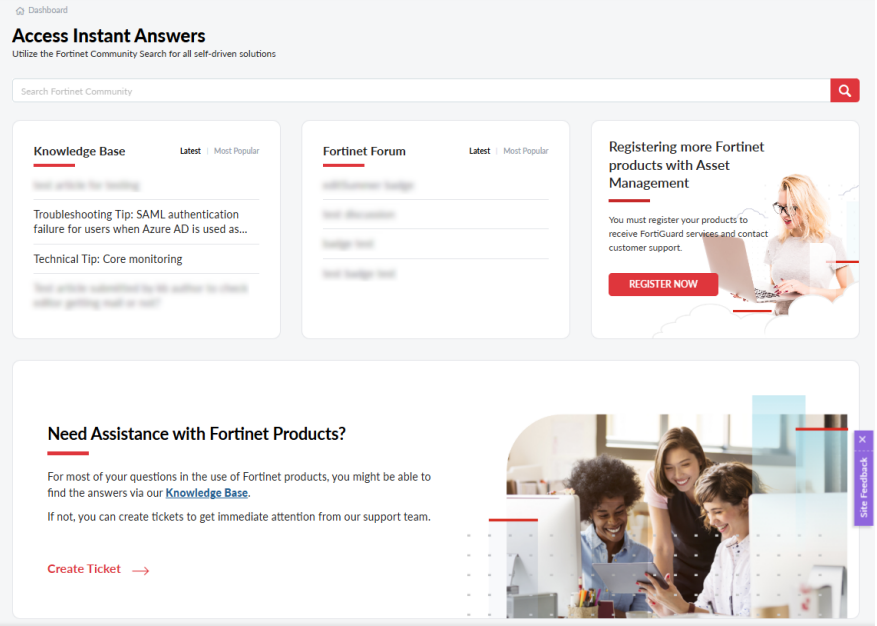
b. Enter information in the search field and press `Enter`. A new page is opened displaying information on the topic.

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.

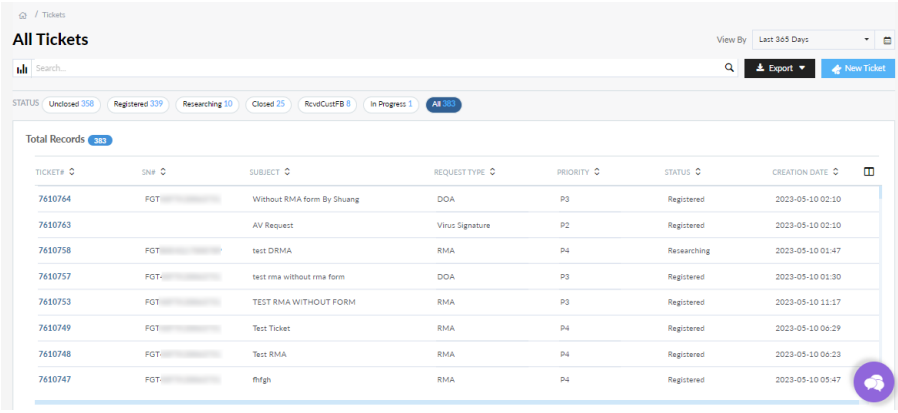


You can view the following information on the *Dashboard*:

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 *Register Now* 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.



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:

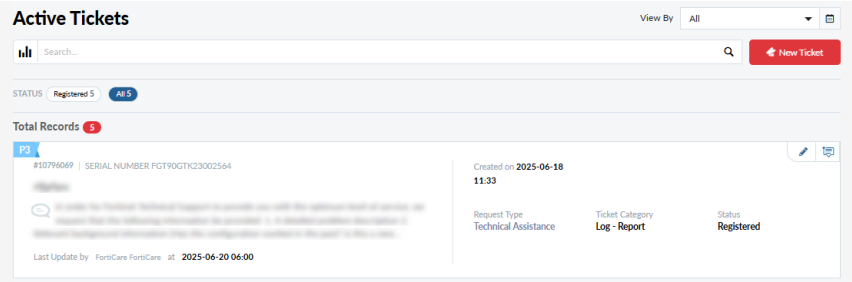
- Filter the ticket list. See Filtering tickets on page 12.
- Search for specific tickets. See Searching for tickets on page 13.
- View ticket information. See Ticket details on page 13.
- Create new tickets. See Creating tickets on page 15.
- Add comments and files to tickets. See Adding comments on 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*.

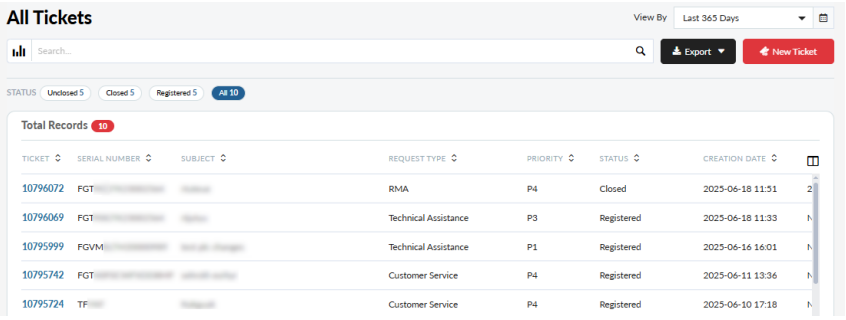


Closed tickets cannot be viewed in the *Active Tickets* page. To view closed tickets, go to *Tickets* > *All Tickets*. See All tickets on page 11 for more information.

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.



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.

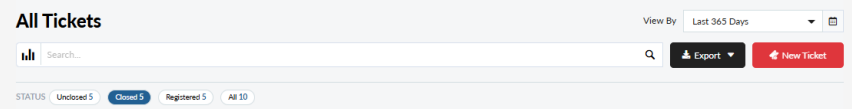
Filtering tickets

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

- Status
- Date
- Category

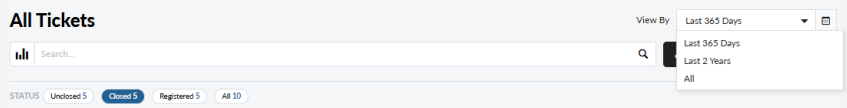
Filtering tickets by status

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



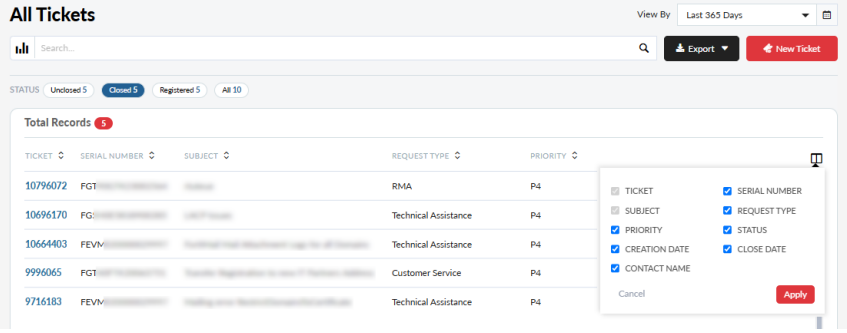
Filtering tickets by date

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.

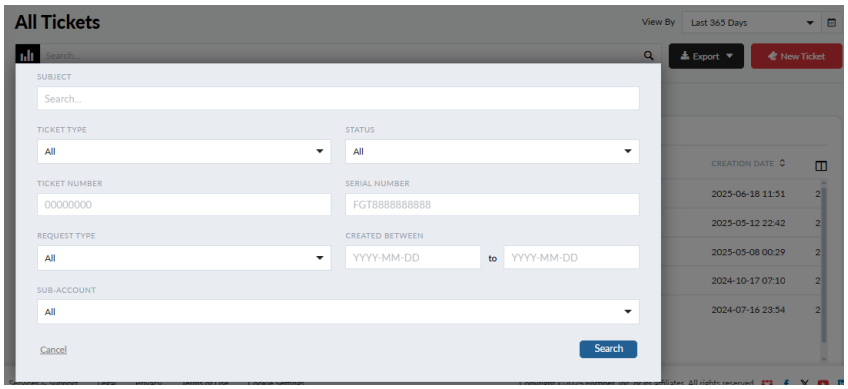
Searching for tickets

You can search for specific tickets using the *Search* field or the *Advanced Search* button. You can used *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 *Confirm* in the pop up dialog. You cannot delete attachments from someone else's comment.
Basic Info	Provides information on ticket *Status*, *Request Type*, *Category*, *Priority*, and so on.
Contact Info	Displays your contact information, including email and phone number.
SFTP Info	Displays *Upload* and *Download* information, such as *FTP Address* and *User ID*. Use the *Hide* and *Show* buttons to control *SFTP Information* visibility.
Ticket Visibility	Lists who can view the ticket.
RMA Info	Displays RMA information, such as: • *Return Material Authorization Info*: Contains ticket information, including *RMA Type* and *RMA Ticket ID*. • *Summary*: Contains information on product model status. • *Shipping & Billing Info*: Displays shipping and billing addresses and contacts. When editing, once you click *Confirm RMA Information*, the information can no longer be edited. The shipping address must be confirmed to submit a PRMA ticket. • *Transit To*: Provide transit information following shipping and click *Confirm Transit Address Information* to complete editing. Transit To information becomes read only after confirmation. • *Defective Product Info*: Displays information on the product, including serial number and model. • *RMA Contract and Service Transfer*: 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. • *Return Instructions*: Provides additional information on the *RMA Center* and return instructions. • *Replacement Product Info*: Provides shipping and tracking information. This section can only be edited by Partner users. Once the information has been confirmed, it becomes read only. • *Receiving Info*: 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 dietails.

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:

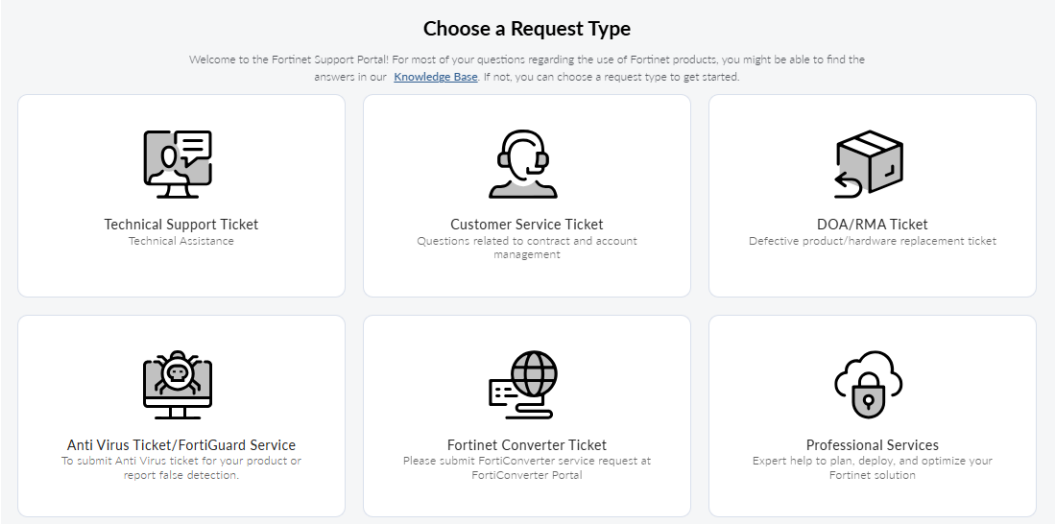
- Technical support ticket on page 15
- Customer service ticket on page 18
- DOA/RMA ticket on page 21
- Anti Virus ticket and FortiGuard Service on page 24
- Fortinet Converter ticket on page 25
- Professional Services ticket on page 26
- FortiClient Services on page 29

Technical support ticket

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

To create a new Technical Support ticket:

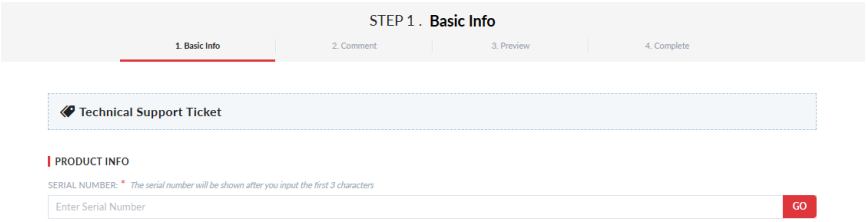
1. Go to *All Tickets*.
2. Click *New Ticket*. The *Choose a Request Type* dialog opens.



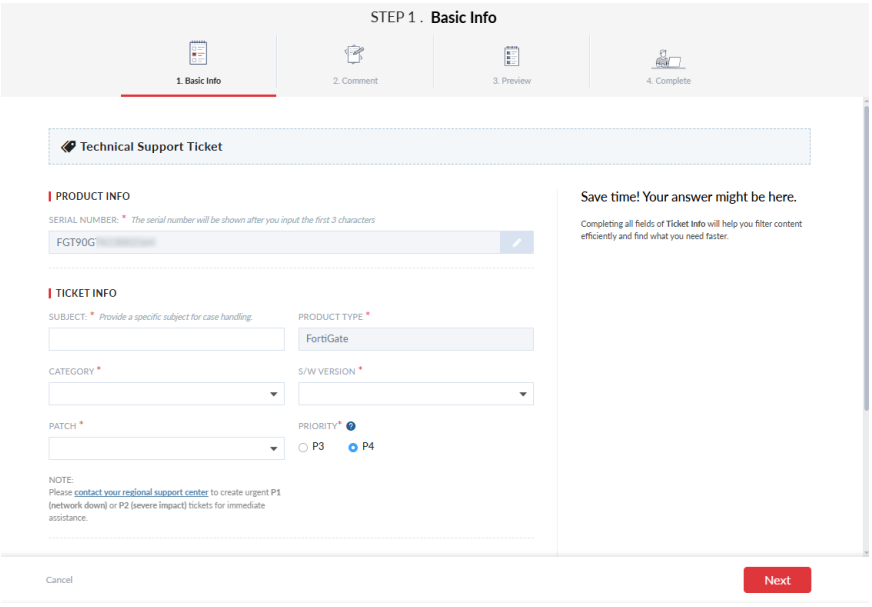
3. Hover over *Technical Support Ticket* and select *Submit Ticket*.

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

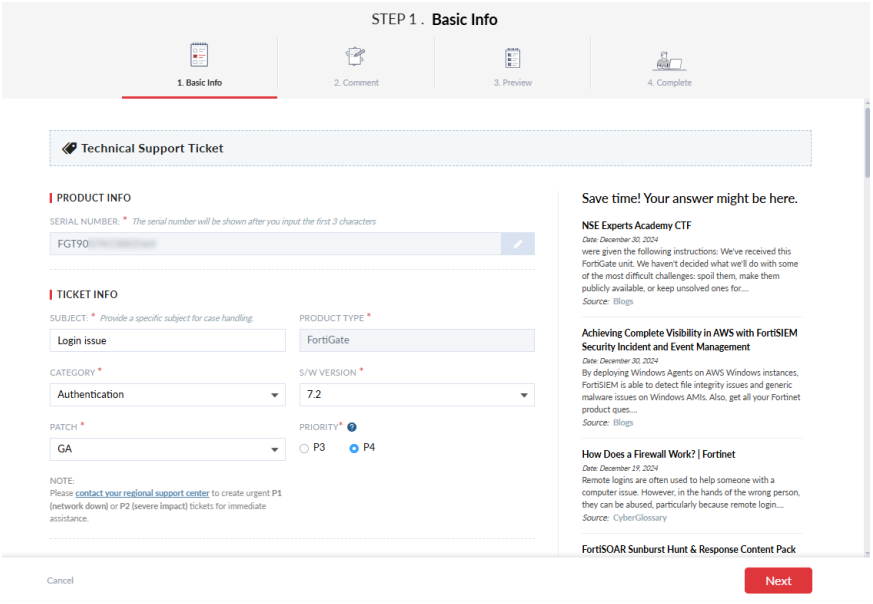
The *Basic Info* page opens.



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

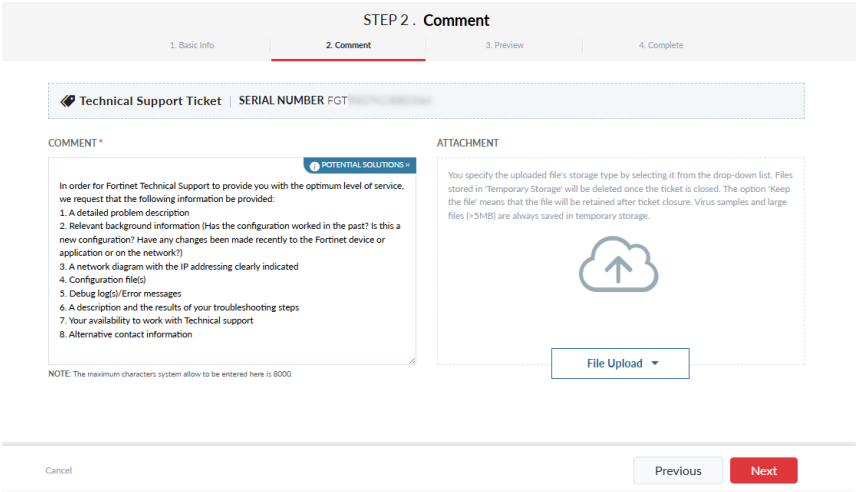


5. Enter the necessary information in the *Contact Info* and *Ticket Info* sections.



> 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.

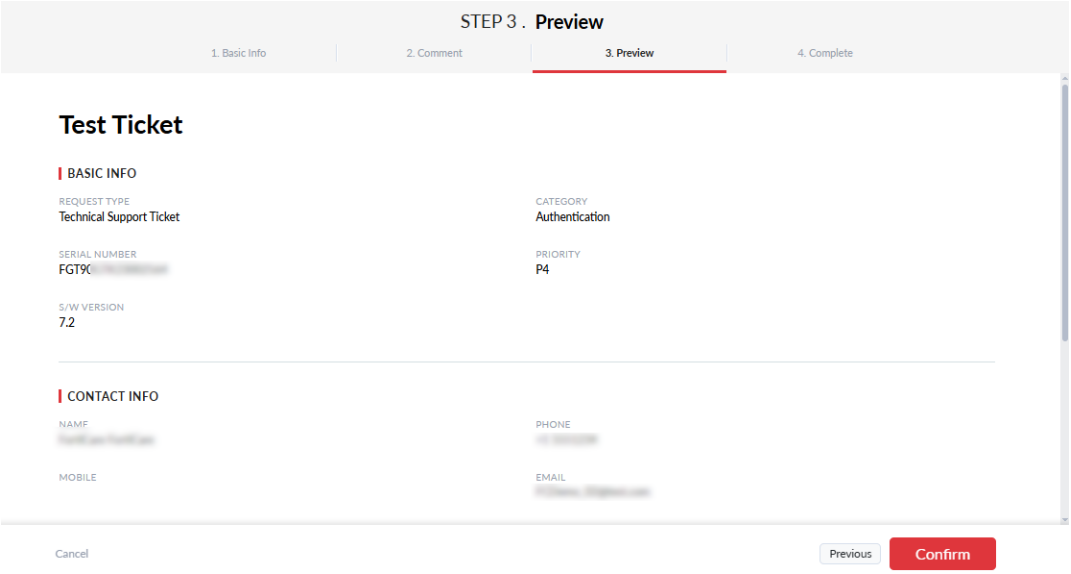


> Select *Potential Solutions* to view suggested community Knowledge Base articles, Fortinet documents, and FortiGuard resources that may help you solve the issue. Select an article to review the information or provide more detail in the Subject field for more filtered articles.

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.



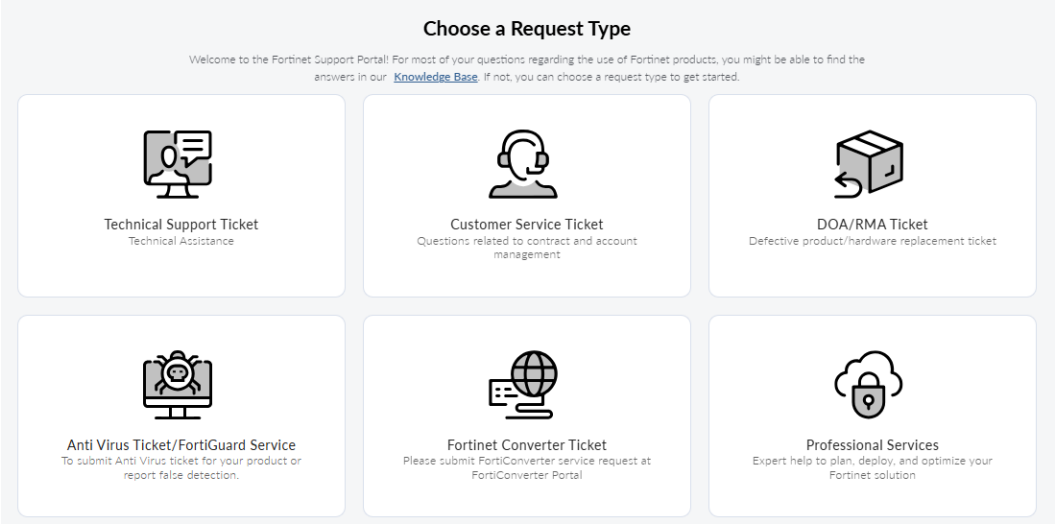
11. Click *Next*. The *Complete* page opens.
12. Review the ticket number and information and click *Done*.

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:

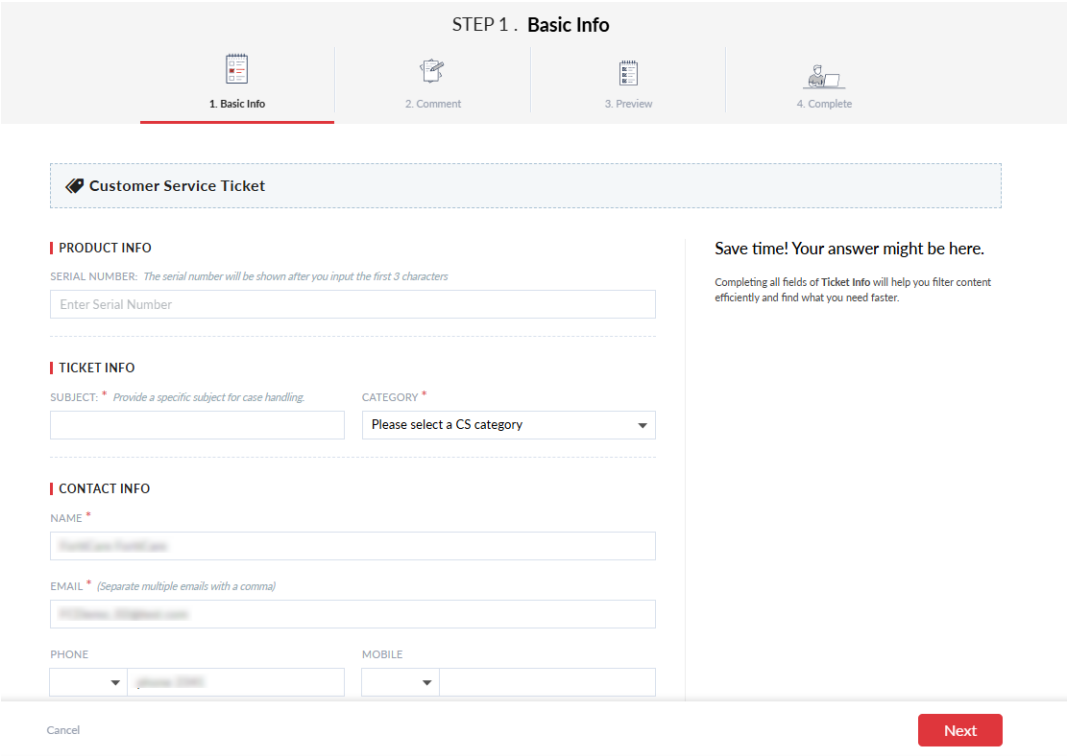
1. Go to *All Tickets*.
2. Click *New Ticket*. The *Choose a Request Type* page opens.



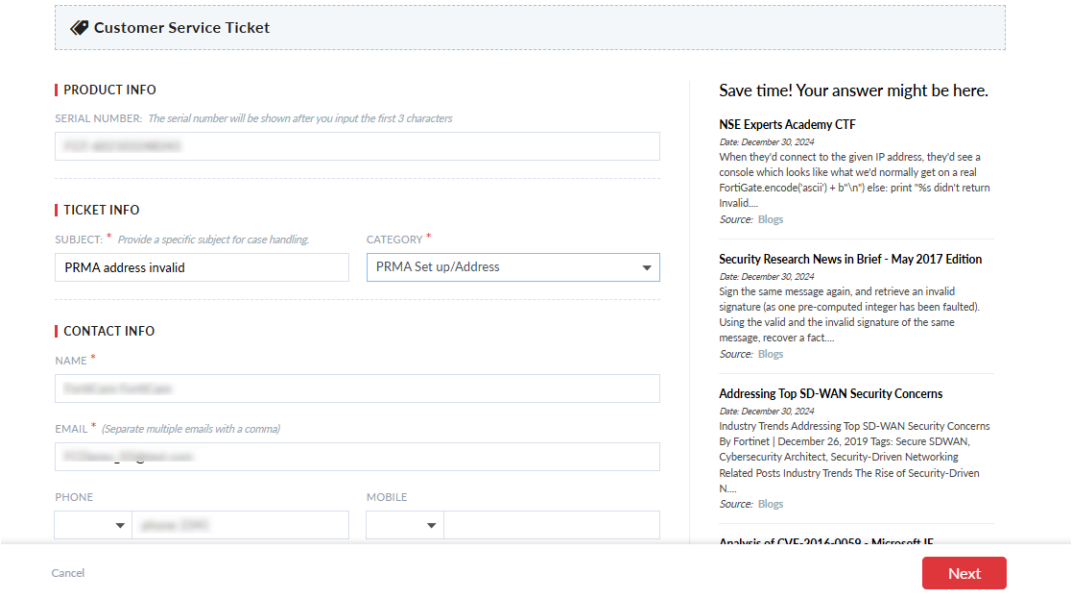
3. Hover over *Customer Service Ticket* and select *Submit ticket*.

> 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.

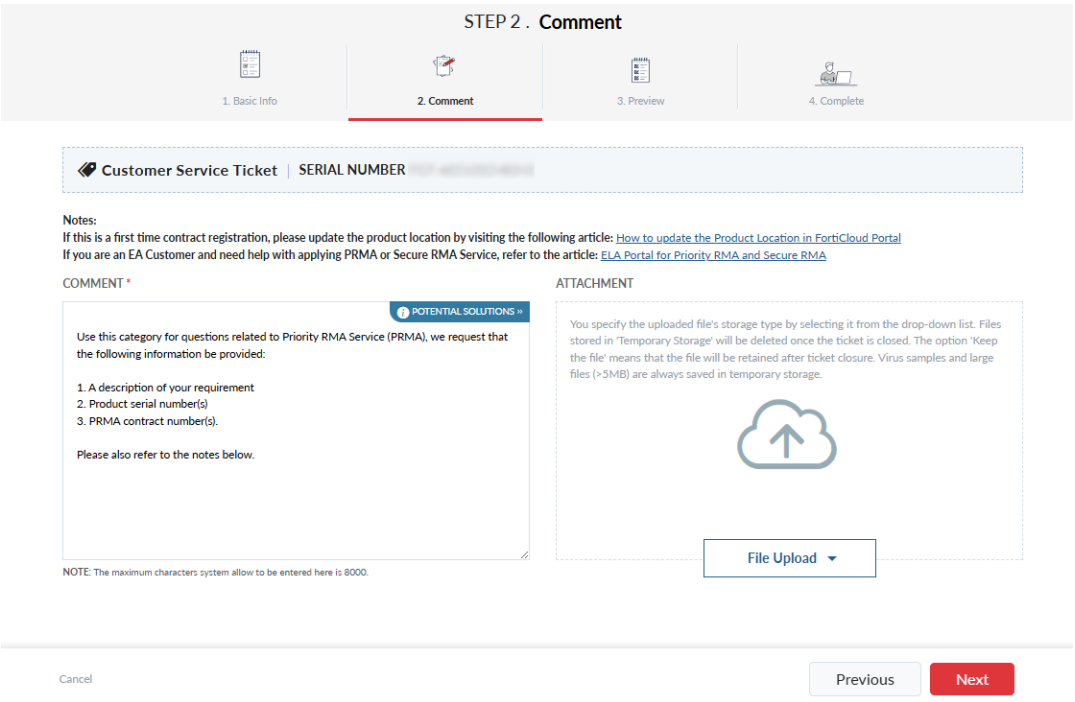


4. Enter the required information in the *Product Information*, *Contact Info*, and *Ticket Information* sections.



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.

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



> 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*.

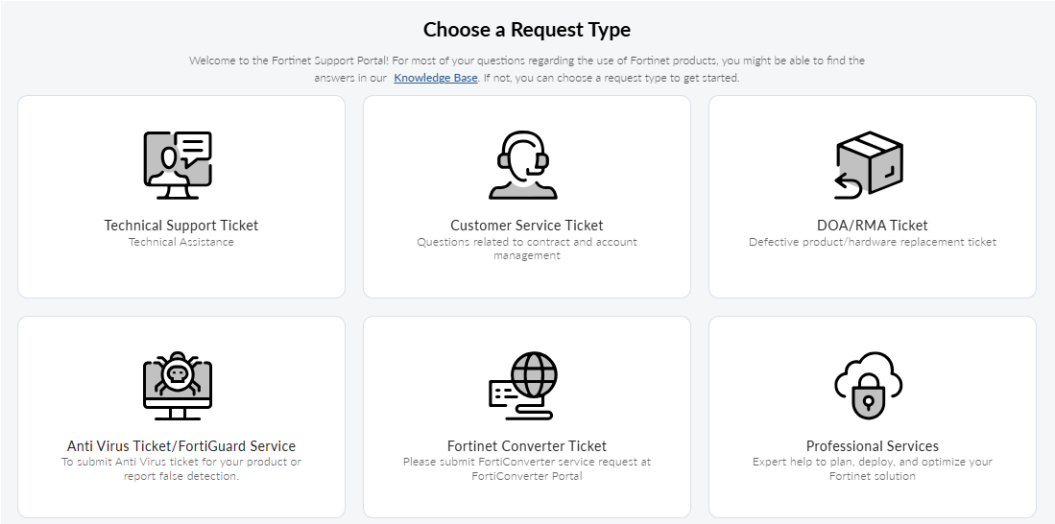
DOA/RMA ticket

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.

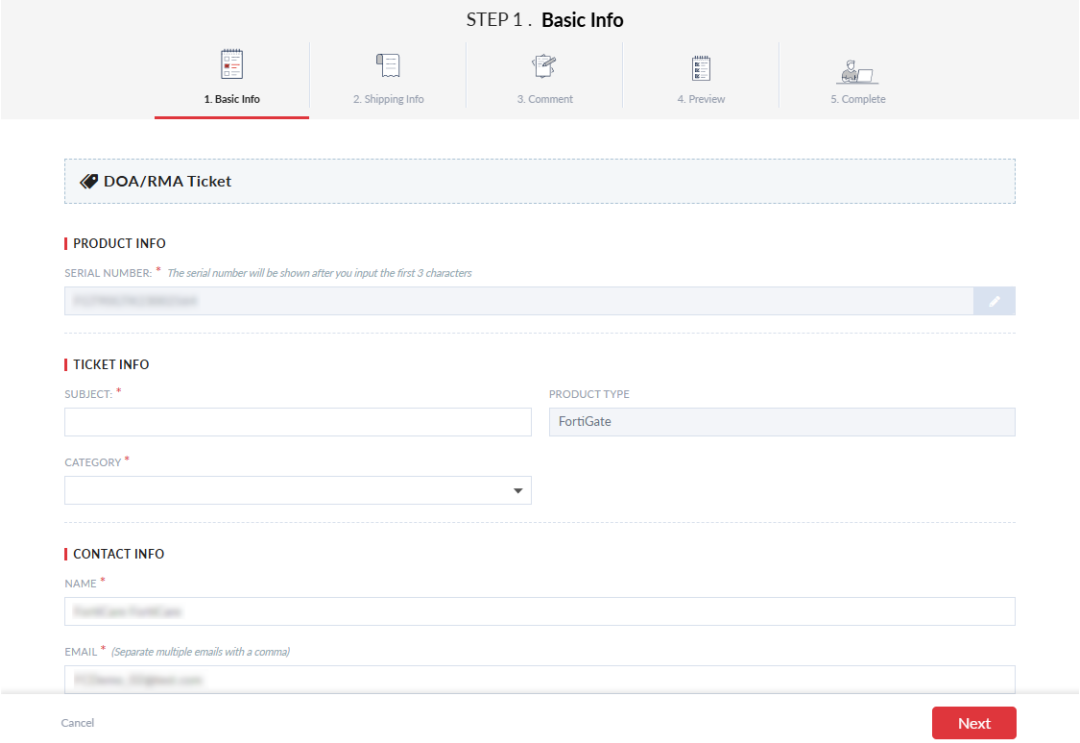
To create a new DOA/RMA ticket:

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

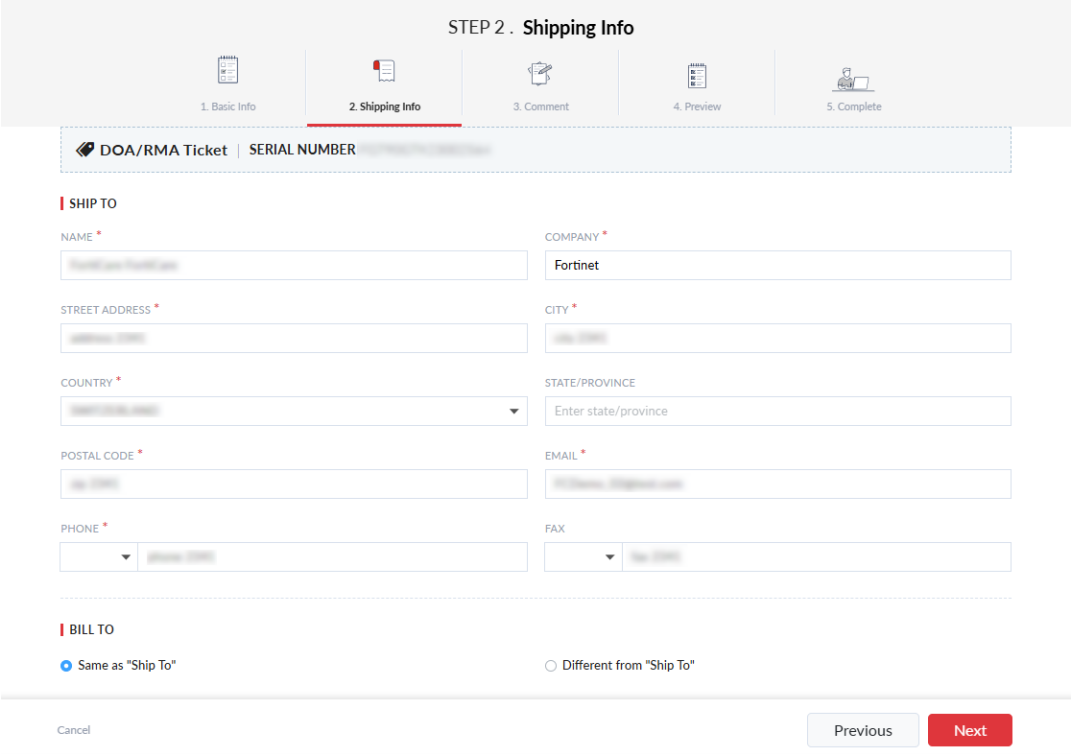


3. Select *DOA/RMA Ticket* and click *Next*. The *Basic Info* page opens.

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



5. Enter the required information in the *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 from the *Ticket Visibility* list and click *Next*. The *Shipping Info* page opens.



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.

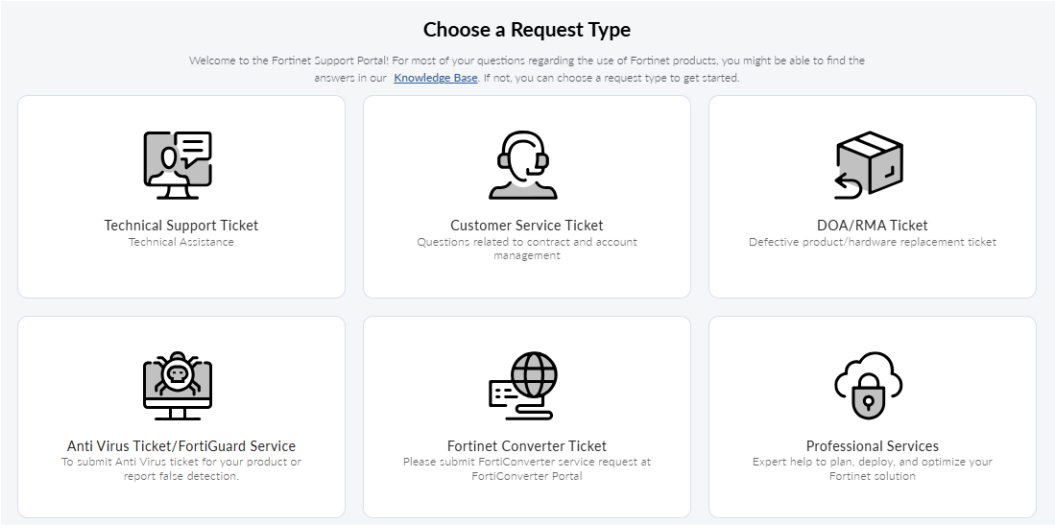
See DOA/RMA ticket on page 21 for information on how to create a DOA/RMA ticket.

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:

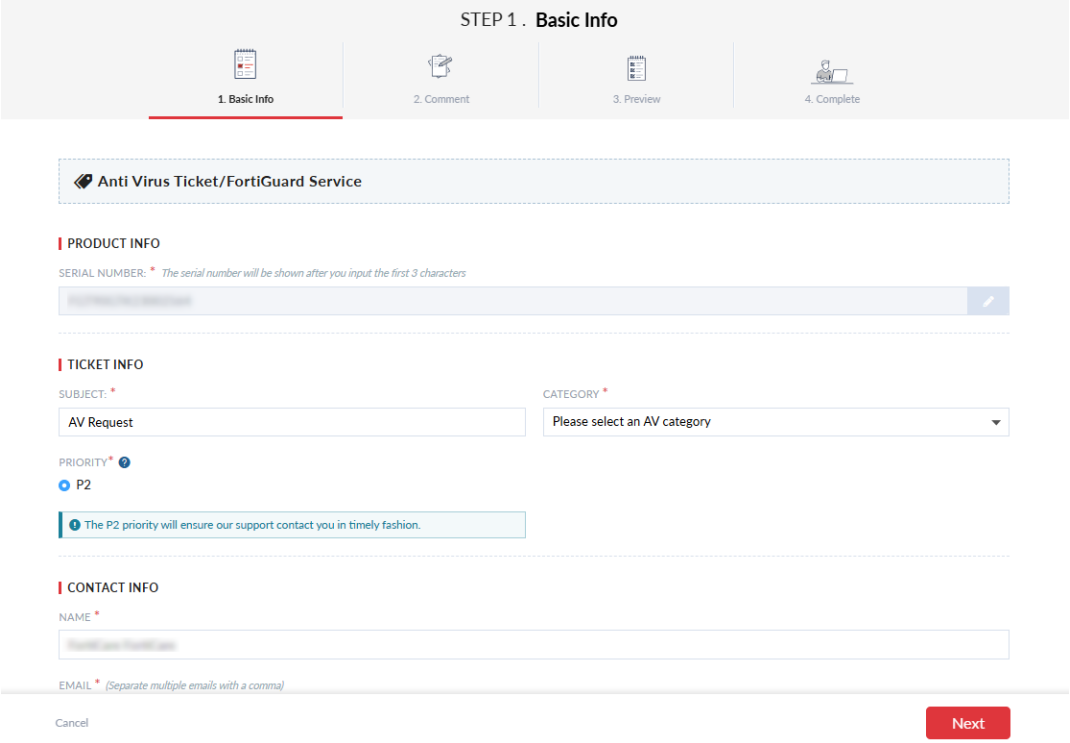
1. Go to *All Tickets*.
2. Click *New Ticket*. The *Choose a Request Type* page opens.



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.



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.

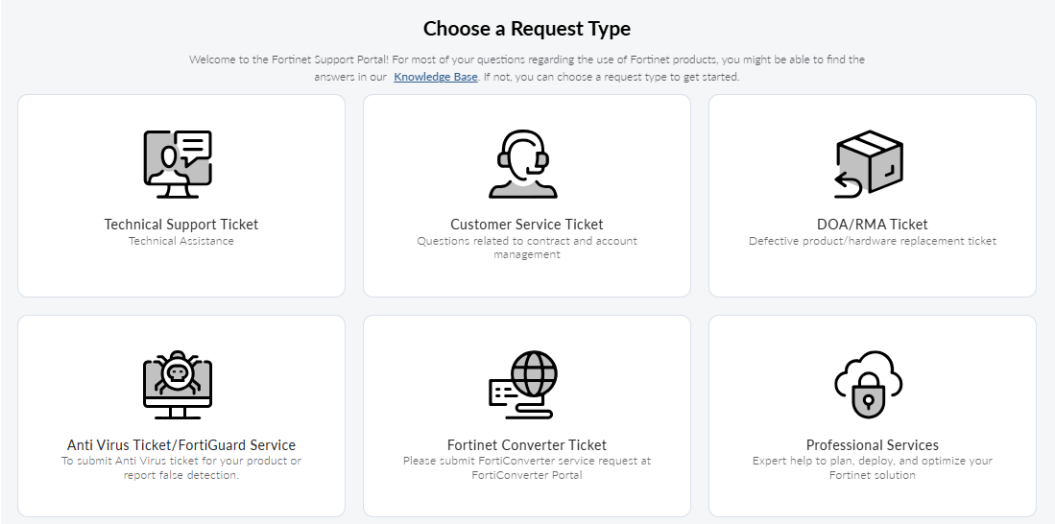
10. After your files have finished uploading, click *Next*. The *Preview* page opens.
11. Click *Next*. The *Complete* page opens.
12. Review the ticket number and information and click *Done*.

Fortinet Converter ticket

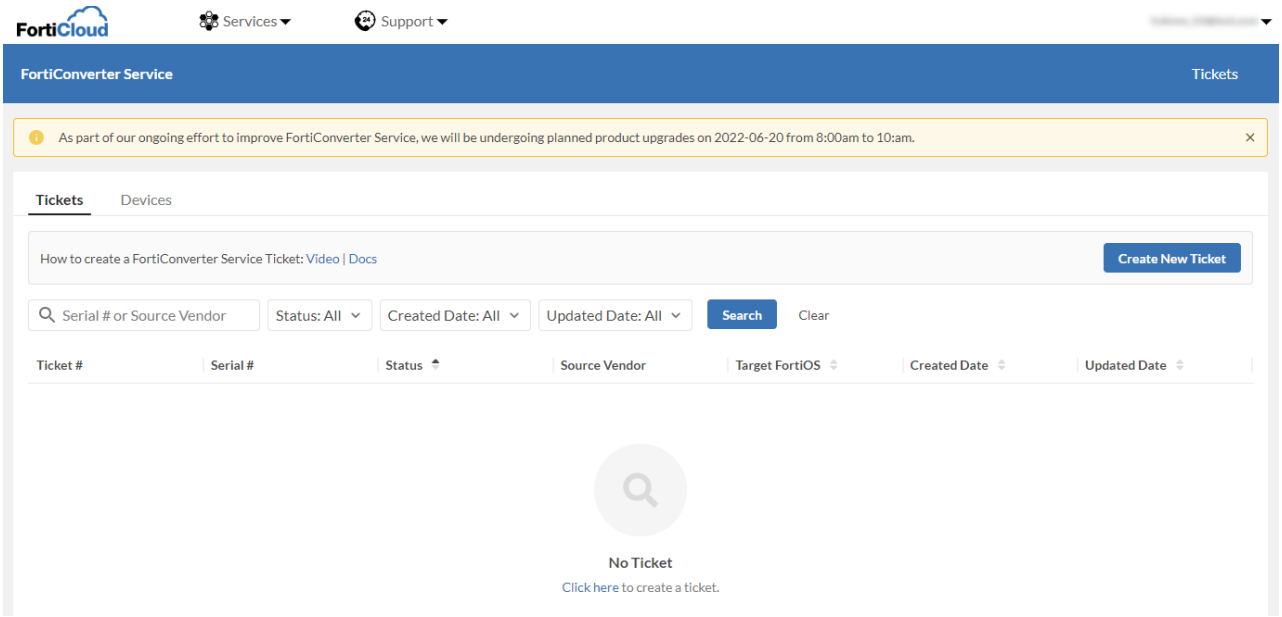
Fortinet Converter tickets should be submitted in the FortiConverter Services portal, which can be accessed from FortiCare.

To create a new Fortinet Converter ticket:

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



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



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

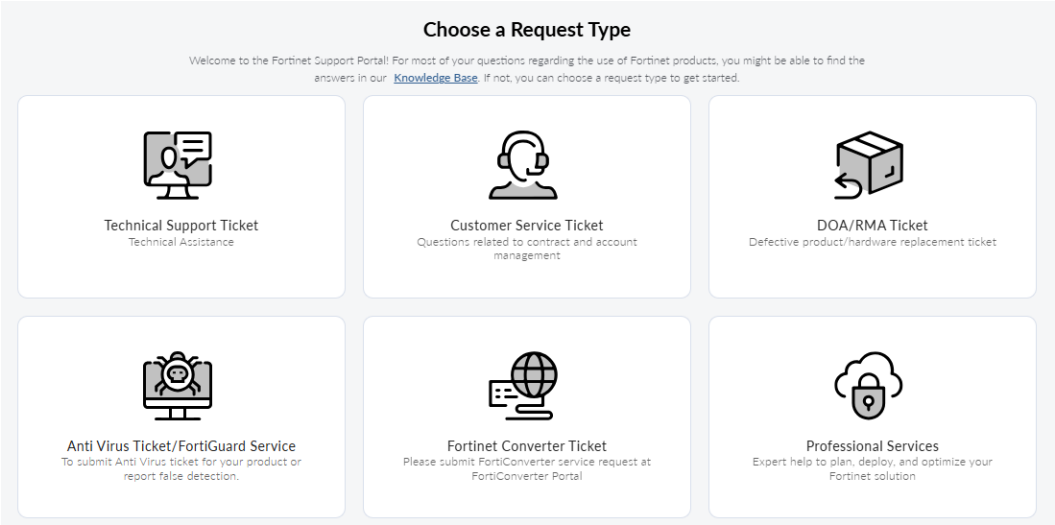
Professional Services ticket

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

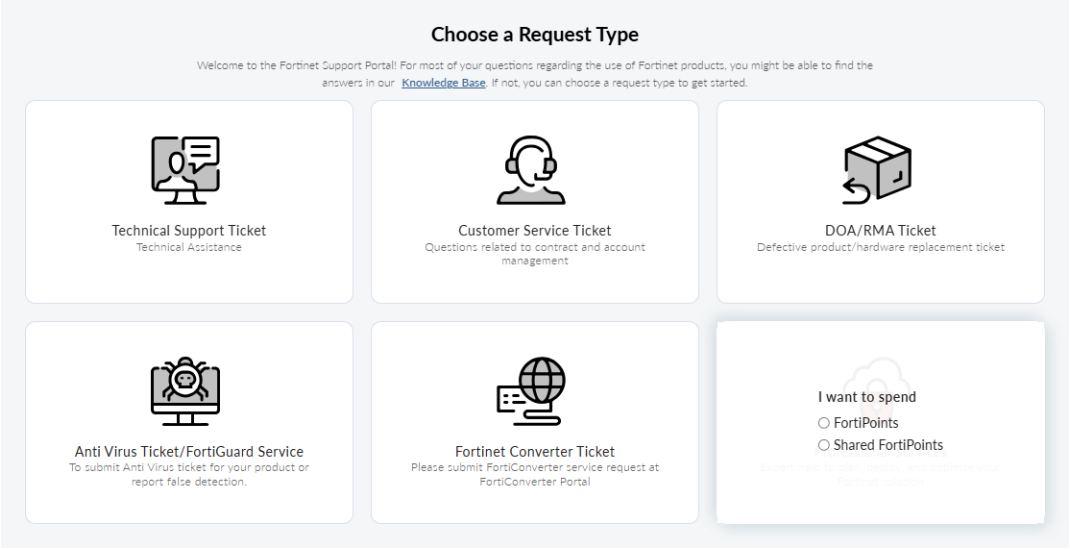
> You can also access the *Professional Services* ticket creation process by selecting the Professional Services Marketplace offering in the Asset Management guide. See Professional Services.

To create a new Professional Services ticket:

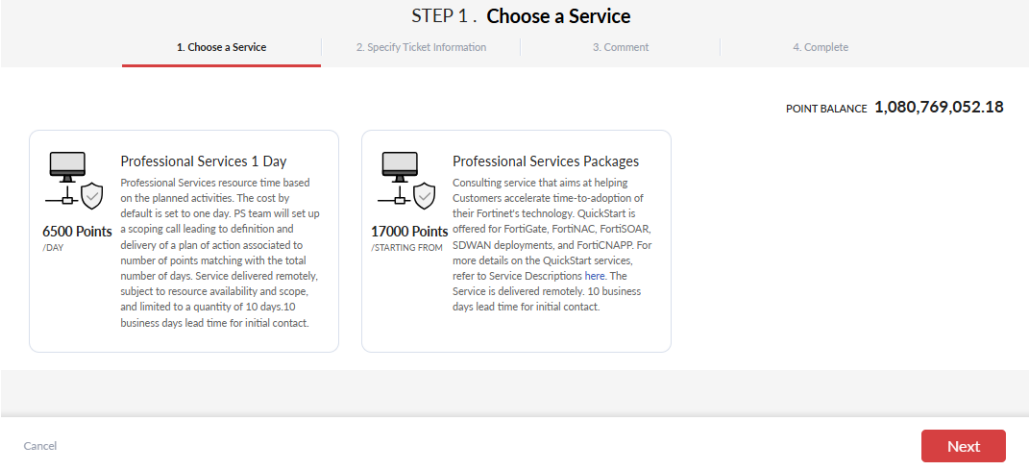
1. Go to *Tickets*.
2. Click *New Ticket*. The *Choose a Request Type* page opens.



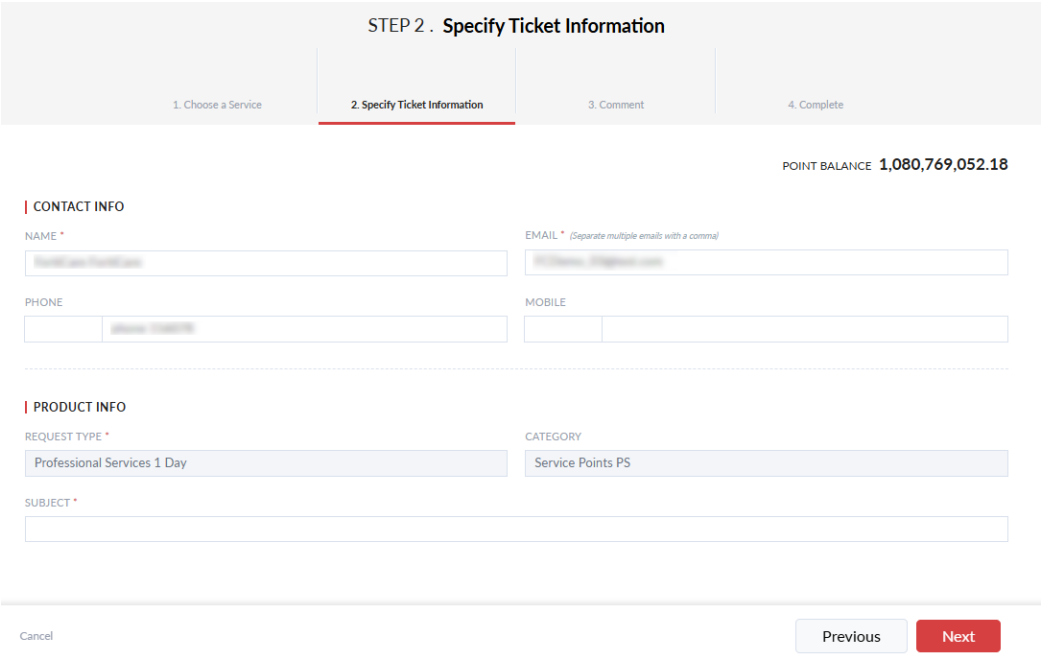
3. Select *Professional Services*.
4. If you have access to *Shared FortiPoints*, select the method of purchase. See Shared FortiPoints for more information.



5. Select the service.



6. Click *Next*.
7. Enter the contact and product information.



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.

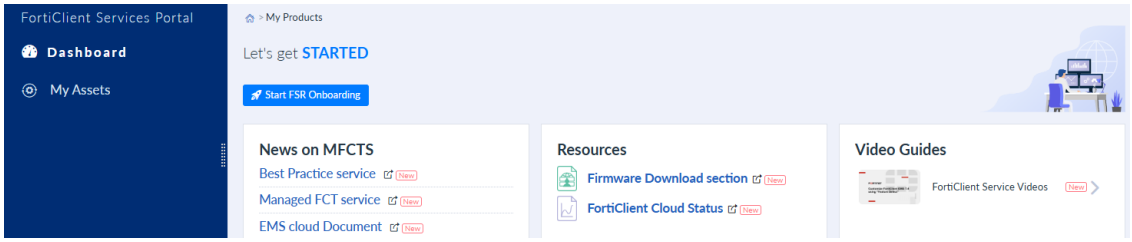
12. After your files have finished uploading, click *Next*.
    The ticket will be created and the professional services request submitted.

FortiClient Services

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



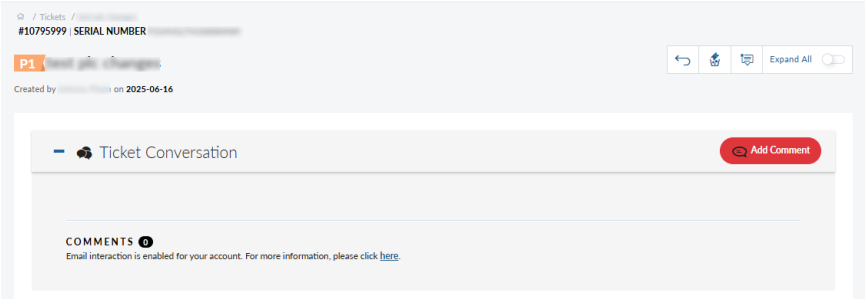
4. Create a support request in the FortiClient Services portal.

Adding comments

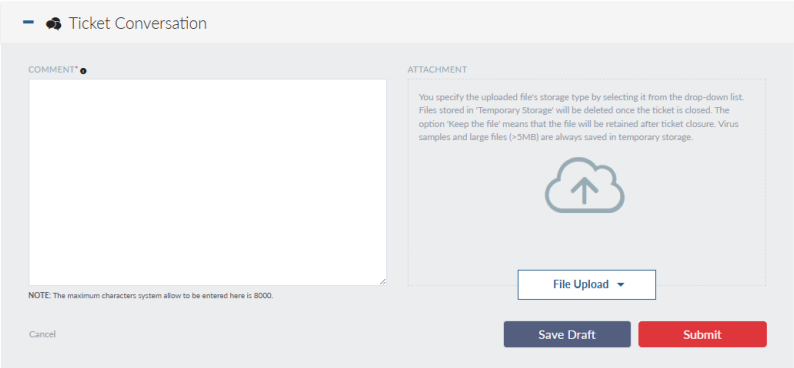
You can add a comment and attach files to the *Ticket Conversation*.

To add a comment:

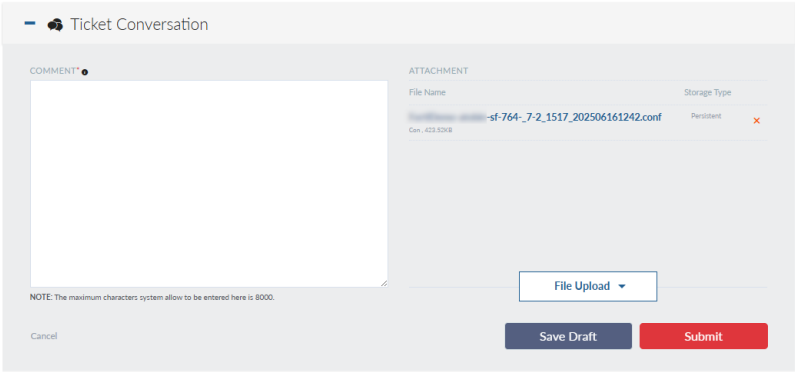
1. Go to *Tickets*.
2. Select the *Ticket#*. The ticket details are displayed.
3. Expand *Ticket Conversation*.



4. Select *Add Comment*.



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*.



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.

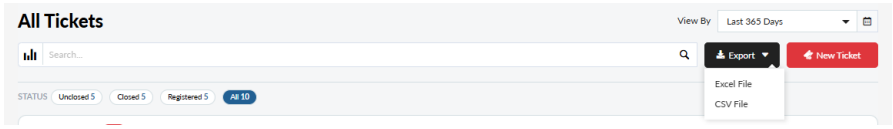
4. Select the *Reason* from the dropdown menu and add a *Comment*.
5. Click *Confirm*. The *Status* is changed to *Closed*.

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*.

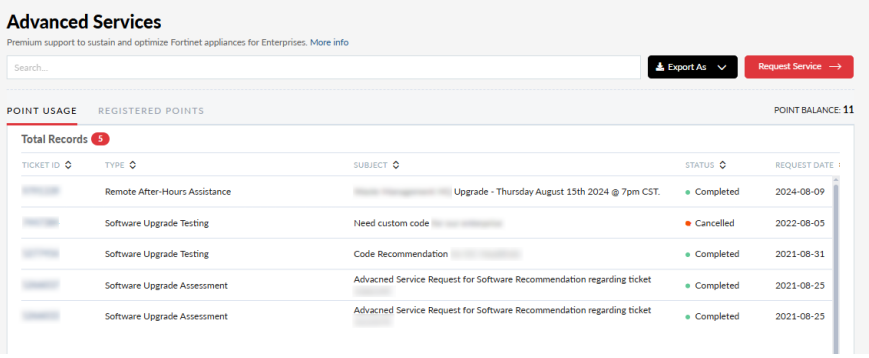


3. Select the file format you want to export from the dropdown menu:
   - *Excel File*
   - *CSV File*

   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.



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 *Point Usage* and *Registered Points* for Advanced Services requests. Click *Request Service* 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 *Request Date*.
Registered Points	Displays the contracts registered to your account and your Service Points balance in ascending order by serial number.
Export As	Exports the *Point Usage* and *Registered Points* for the current view as an Excel or CSV file.
Request Service	Click to create a new *Advanced Services* 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

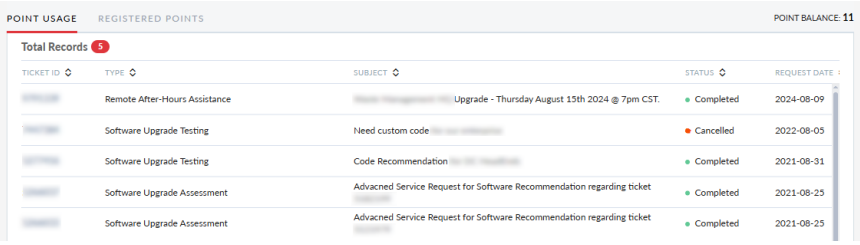
The Advanced Services page supports both IAM and legacy Sub User models. For more information about FortiCloud's user management models, see User management models in the Identity & Access Management guide.

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

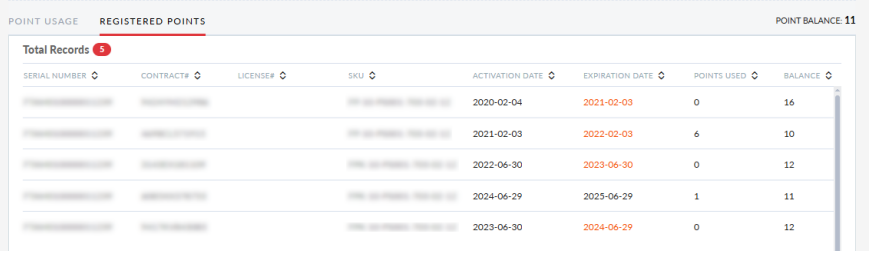
The *Point Usage* tab shows the service requests for your account as well as the ticket type, status, and points consumed by each request.



Point Usage	Description
Ticket ID	The FortiCare Ticket number associated with the service request. Click the *Ticket ID* 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 *Subject* text that was entered at the time the ticket was created. See Creating an Advanced Service ticket on page 35.
Status	• *Pending*: This is the default status after a service request is submitted. • *Approved* : Indicates the scope of service to be delivered and the total number of service points has been agreed upon between you and Fortinet. • *Canceled*: Indicates the service cannot be delivered. No points are applied. • *Completed*: 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.



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 *Completed*.

To export the Point Usage and Registered Points:

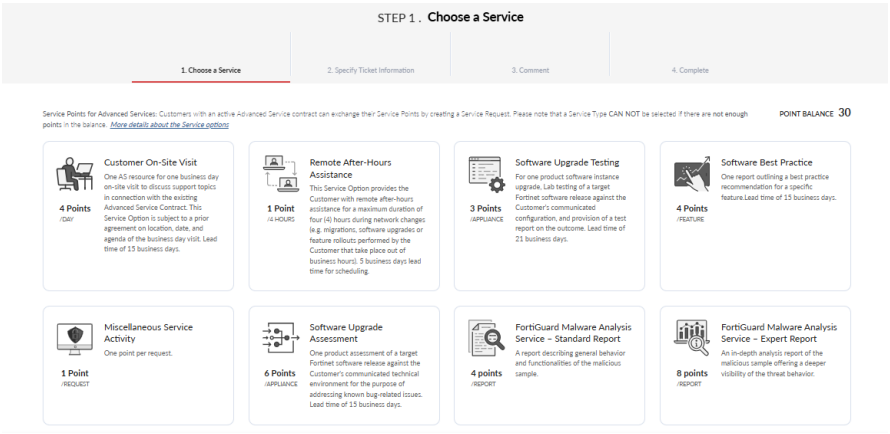
1. Go to *Advances Services*.
2. Click *Export As* and select either *Excel File* or *CSV File*.

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:

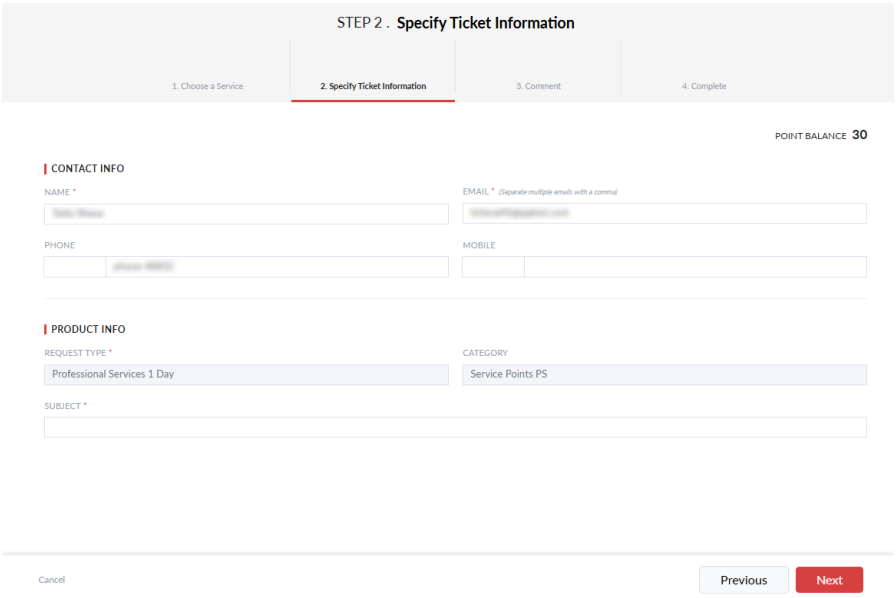
1. Go to *Advanced Services*.
2. Click *Request Service*. The *Choose a Service* page opens.



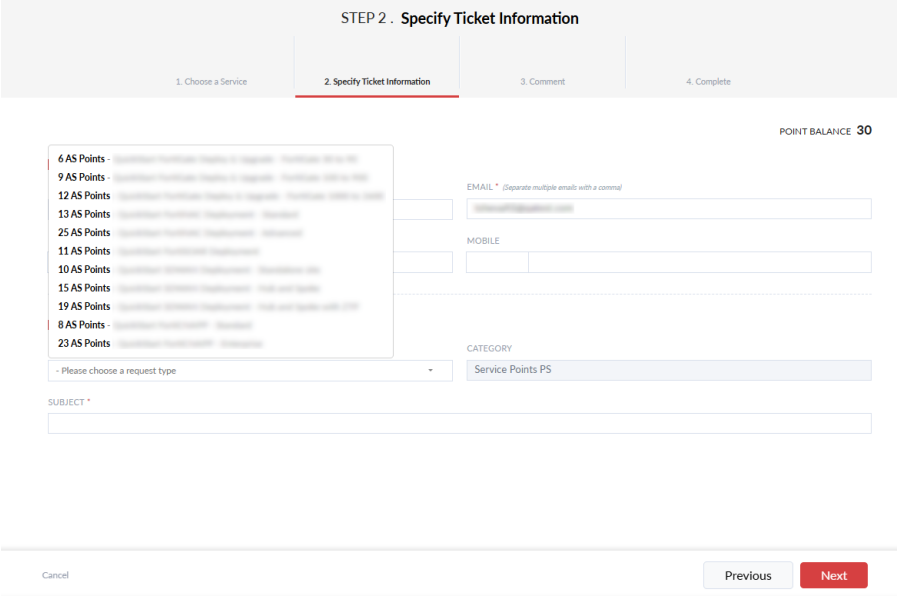
3. Select a service and click *Next*.

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

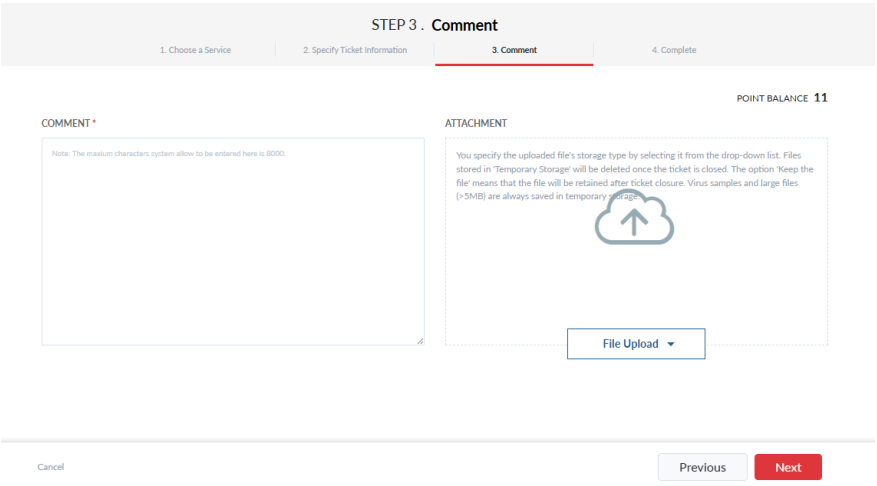
4. Complete the *Specify Ticket Information* form.
   a. In the *Contact Info* section enter your *Name*, *Email*, *Phone*, and *Mobile*.
   b. In the *Product Info* section, use the *Subject* field to describe the request, and click *Next*.



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



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*.



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

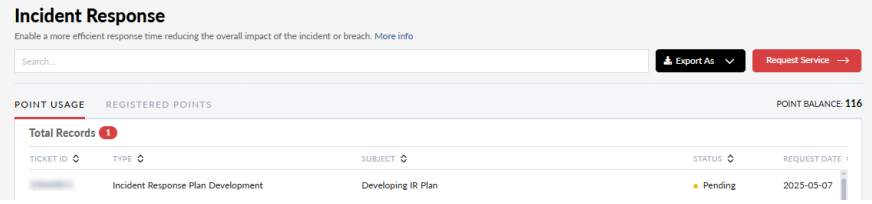
More information about each Advanced Services option is available in the Service Points description available in the Customer Service portal.

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

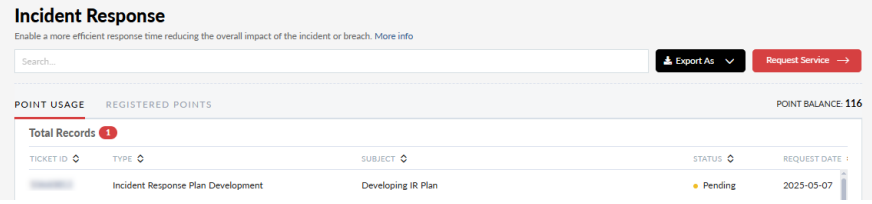
Service requests

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

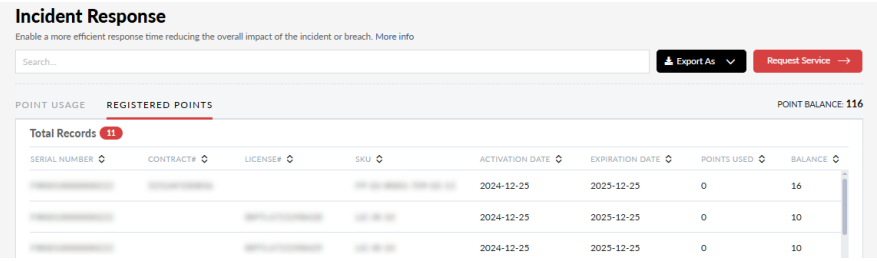
The *Point Usage* tab shows the Service Requests for your account as well the ticket type, status, and points consumed by each request.



Point Usage	Description
Ticket ID	The FortiCare Ticket number associated with the Service Request. Click the *Ticket ID* 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 *Subject* text that was entered at the time the ticket was created. See Creating an Incident Response ticket on page 44.
Status	• *Pending*: This is the default status after a service request has been submitted. • *Approved* : Indicates the scope of service to be delivered and the total number of service points has been agreed upon between you and Fortinet Inc.. • *Canceled*: Indicates the service cannot be delivered. No points are applied. • *Completed*: 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.



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 *Completed*.

To export the Point Usage and Registered Points:

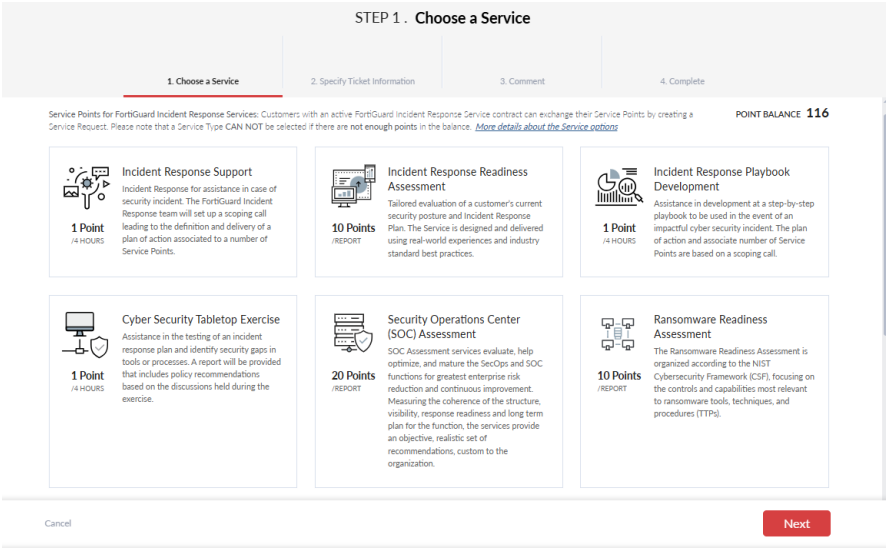
1. Go to *Incident Response*.
2. Click *Export As* and select either *Excel File* or *CSV File*.

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:

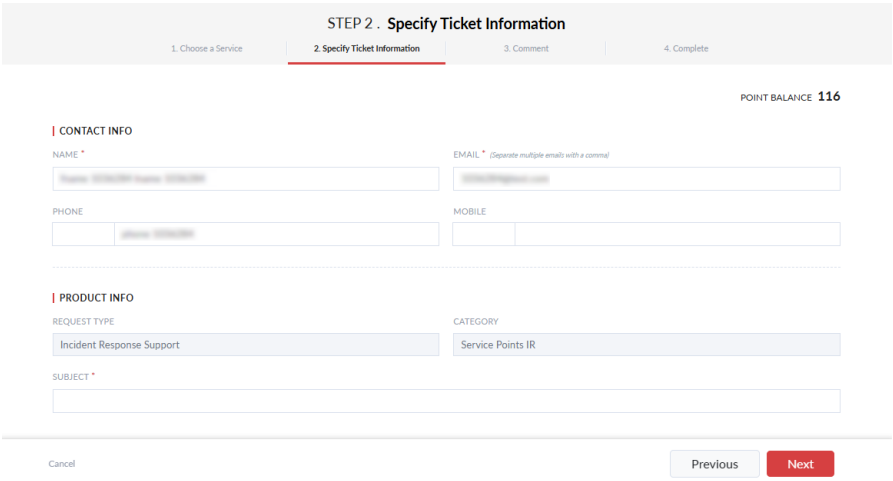
1. Go to *Incident Response*.
2. Click *Request Service*. The *Choose a Service* page opens.



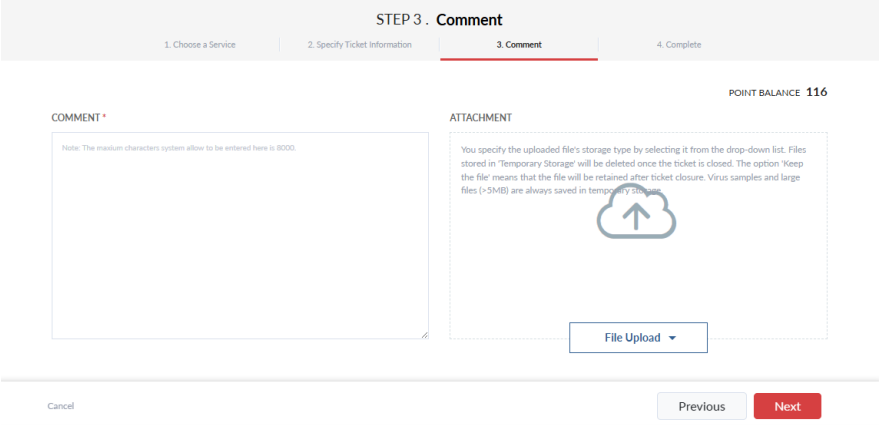
3. Select a service and click *Next*. See Incident Response types on page 46.

> 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*.



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*.



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. • *Event and Incident Response (IR)*: 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. • *Asset Management*: 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
	• *Identify and Access Management*: 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. • *Threat and Vulnerability Management*: 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. • *Continuity of Operations (COOP)/Disaster Recovery (DR)*: 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. • *Network Security*: 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: • *Organization*: 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). • *Visibility*: 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. • *Response*: 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. • *Evolution*: 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: • *Identity*: The mix of IT and business-critical assets, threat intelligence, and vulnerabilities that determine an organization's ransomware attack surface. • *Project*: The defenses in place prevent ransomware vectors or, if an initial compromise is successful, halt further action (lateral movement, credential misuse) by the attacker. • *Detect*: Visibility to ransomware attackers as they enter and scout an environment before they fully strike. • *Evolution*: Reactions to ransomware that require a solid game plan with an understanding of the technical options, communication needs, and business impacts. • *Recover*: 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: • *Policy and procedures*: 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. • *Account Management*: 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. • *Network and Host Configuration*: 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
	• *Audit Configuration*: 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. • *Monitoring*: 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. • *Internal Network*: 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. • *External Network*: 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. • *Web Application*: 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. • *Mobile Application*: 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. • *Internal Networks*: 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. • *External Networks*: 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. • *Web Applications*: 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. • *Mobile Applications*: 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

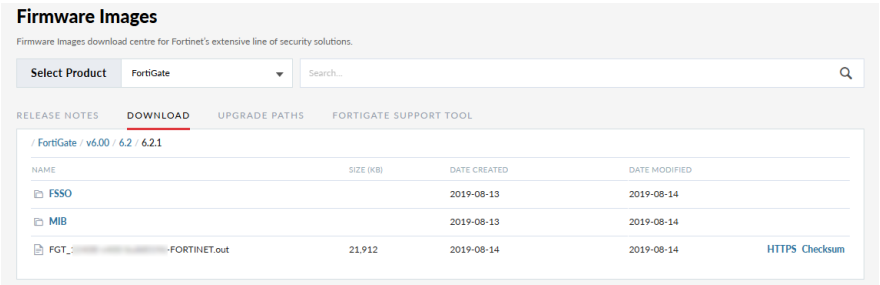
Firmware Images

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:

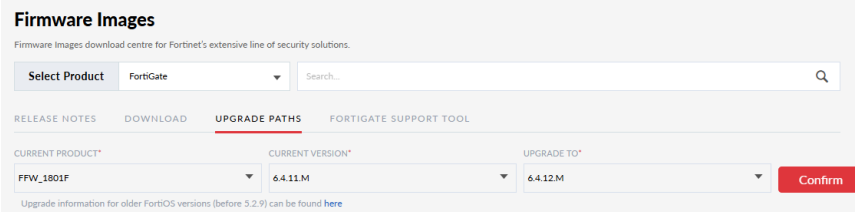
1. Go to *Downloads* > *Firmware Images*.
2. Select the *Download* tab.
3. Select the product you want from the *Select Product* dropdown list.
4. Select the major, minor, and patch version that you need from the provided folders.



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

To view the upgrade path:

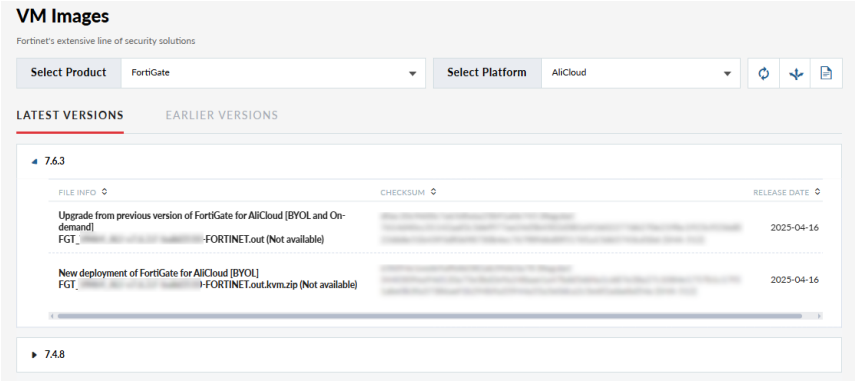
1. Go to *Downloads* > *Firmware Images*.
2. Select the *Upgrade Paths* tab.
3. Select the product you want from the *Current Product* dropdown list.
4. Select the current and desired versions from the dropdown lists.



5. Click *Confirm*.

VM Images

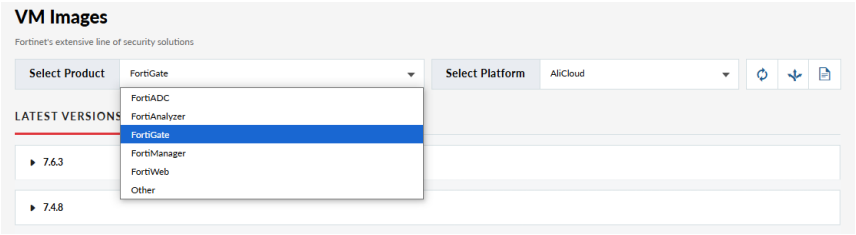
You can refresh, upgrade the path, and access release notes of product VM images from the *Downloads* > *VM Images* page. You can select the product, platform, and versions.



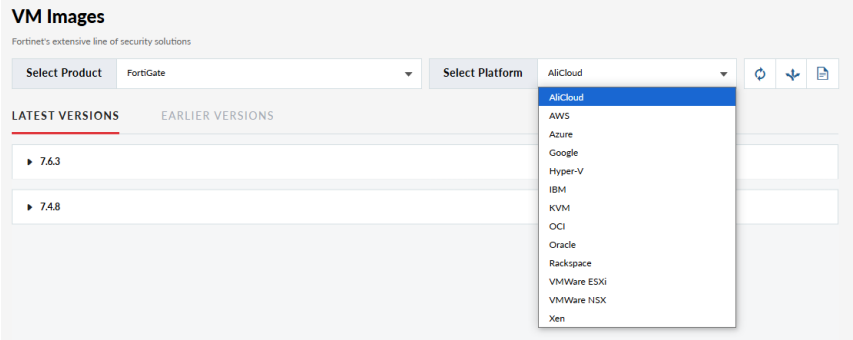
Select *Refresh* to update the information on the VM Images page. Select *Release Notes* to be directed to the product release notes on the Document Library.

To upgrade the path:

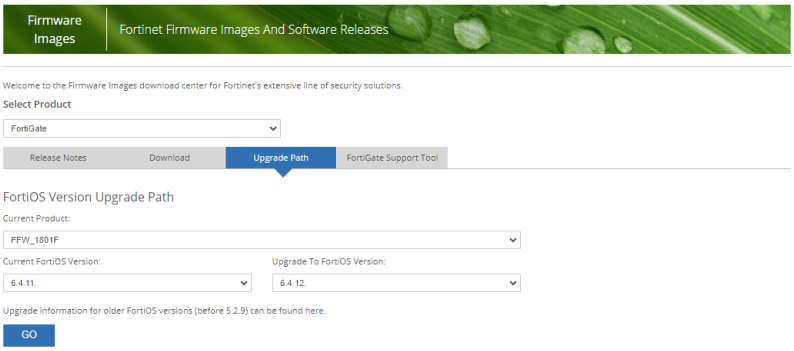
1. Go to *Downloads* > *VM Images*.
2. Select the product whose path you want to update from the *Select Product* dropdown list.



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



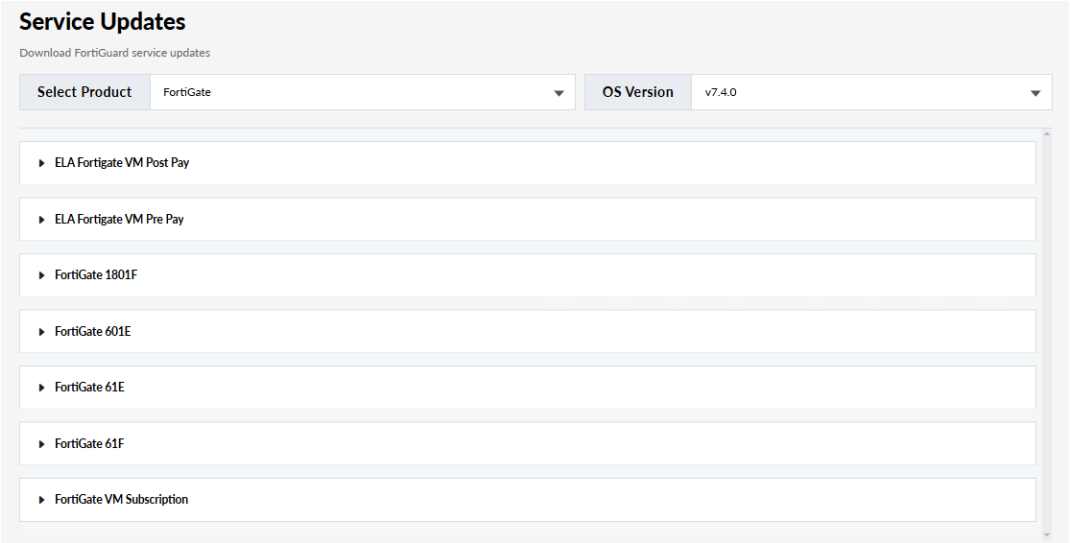
4. Click *Upgrade Path*. You will be directed to the *Firmware Images* page to proceed.



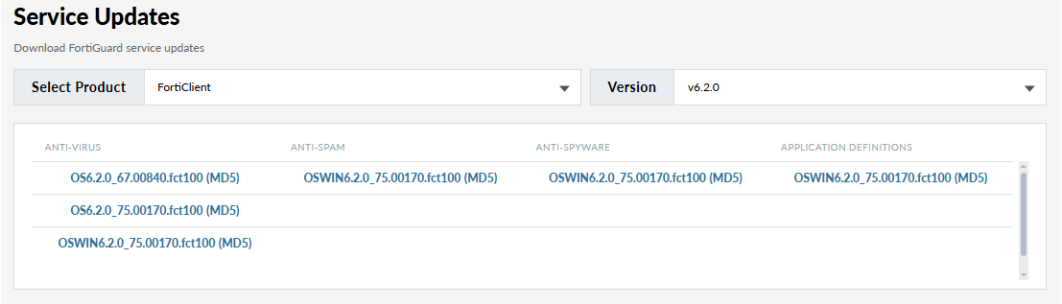
Service Updates

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



- FortiClient



To download a service update:

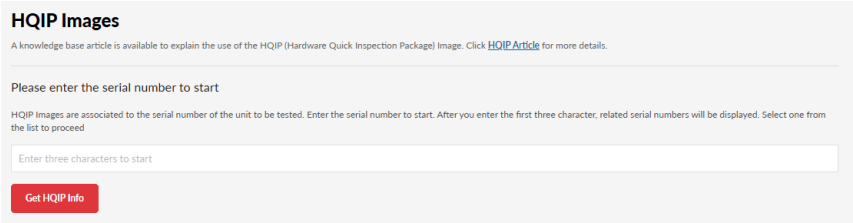
1. Go to *Downloads* > *Service Updates*.
2. Select the product from the *Select Product* dropdown list.

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

3. Select the appropriate version from the *Version* dropdown list.
4. Select the appropriate service update you need from the available options. A verification message is displayed.
5. 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.

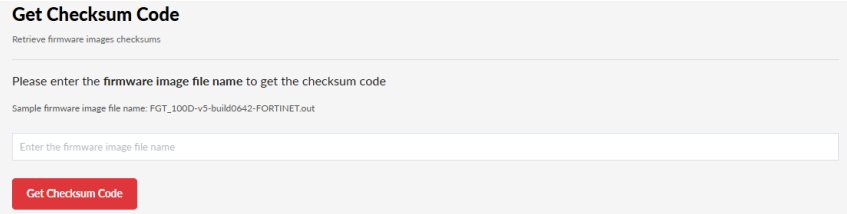


To get the HQIP image:

1. Go to *Downloads* > *HQIP Images*.
2. Enter the serial number in the provided field.
3. 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*.



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.

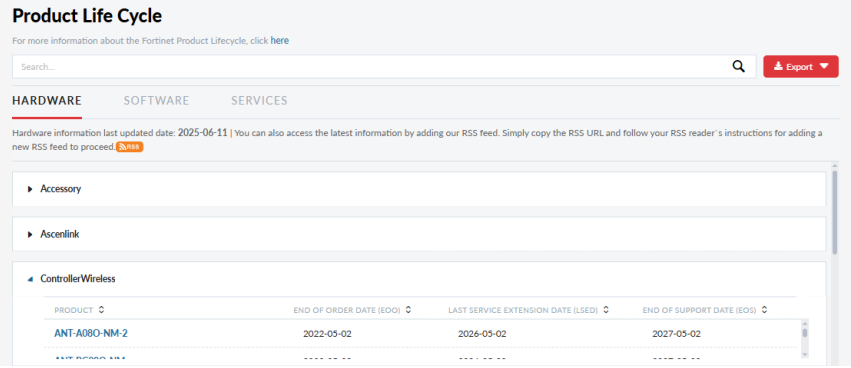
To export the product life cycle:

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.

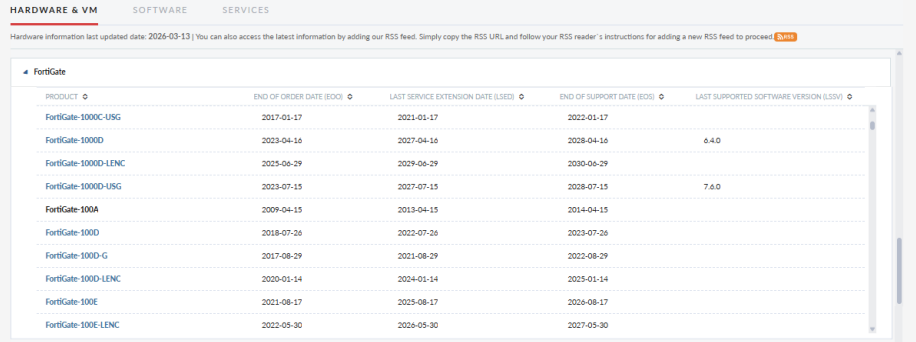
> Life cycle information for all of the products are included in the spreadsheet. You can filter by product to view the specific information you want.

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.

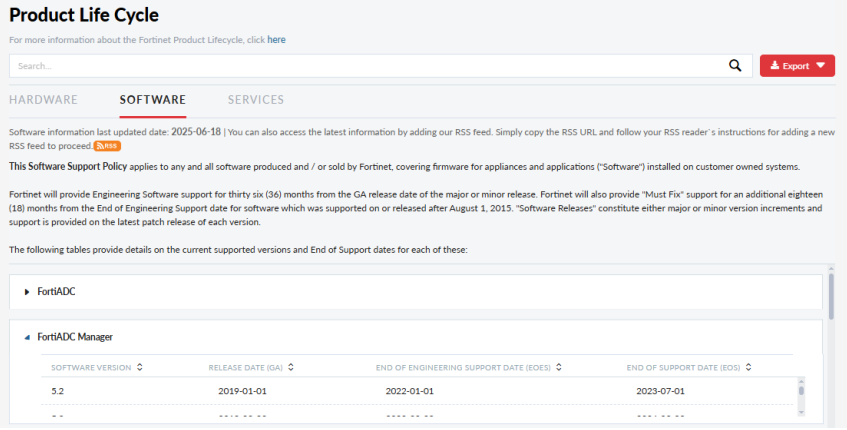


The *Last Supported Software Version (LSSV)* has been added to the *Product Life Cycle* > *Hardware & VM* tables where applicable. For example, the LSSV is listed for certain FortiGate products.

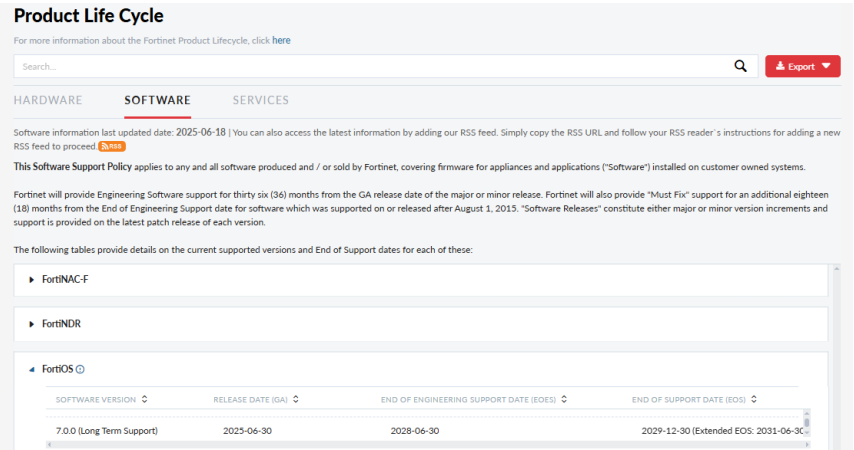


Software

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.

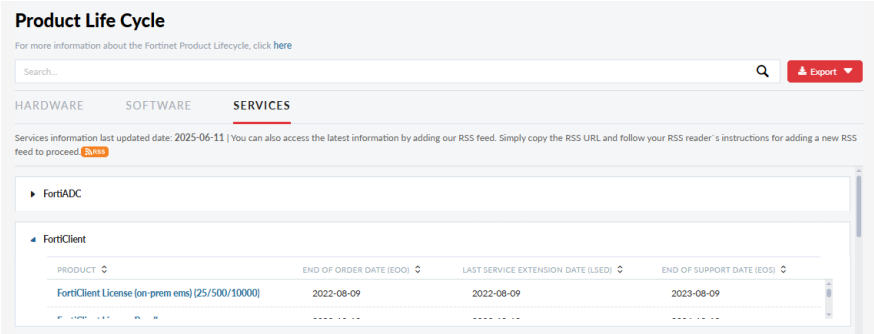


Long term support information is included where applicable. For example, FortiOS version 7.0.0 is marked as *Long Term Support* and the Extended End of Support (EOS) is identified.



Services

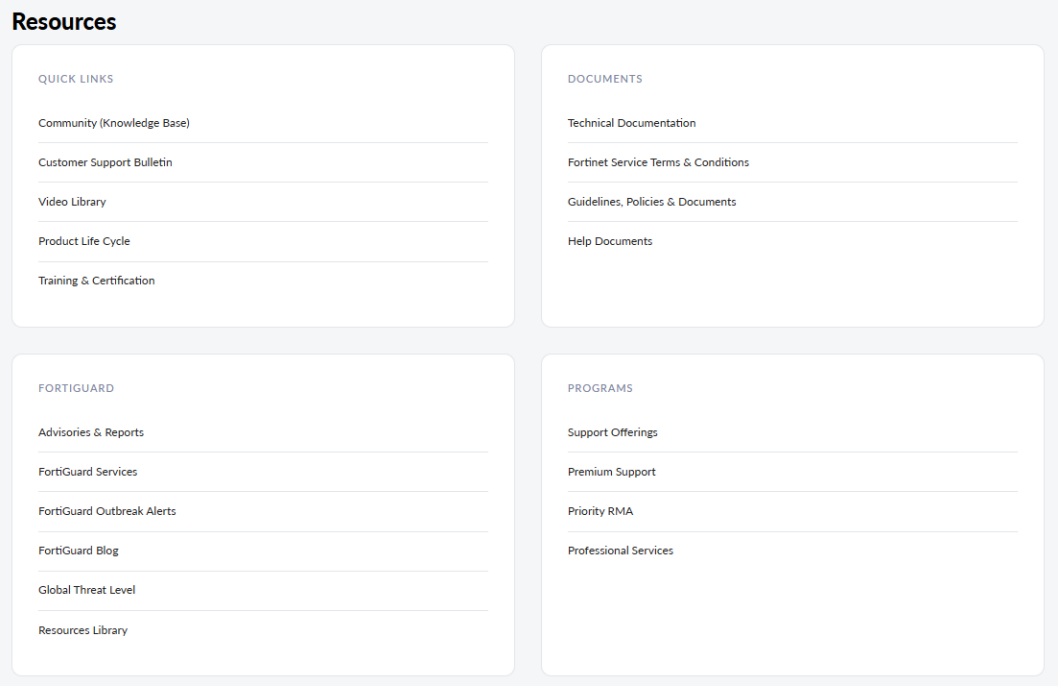
The *Services* tab displays information on product services End of Order (EOO) dates, End of Support (EOS) dates, and Last Service Extension Date (LSED). Select a dropdown menu to view the available service information.



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 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.

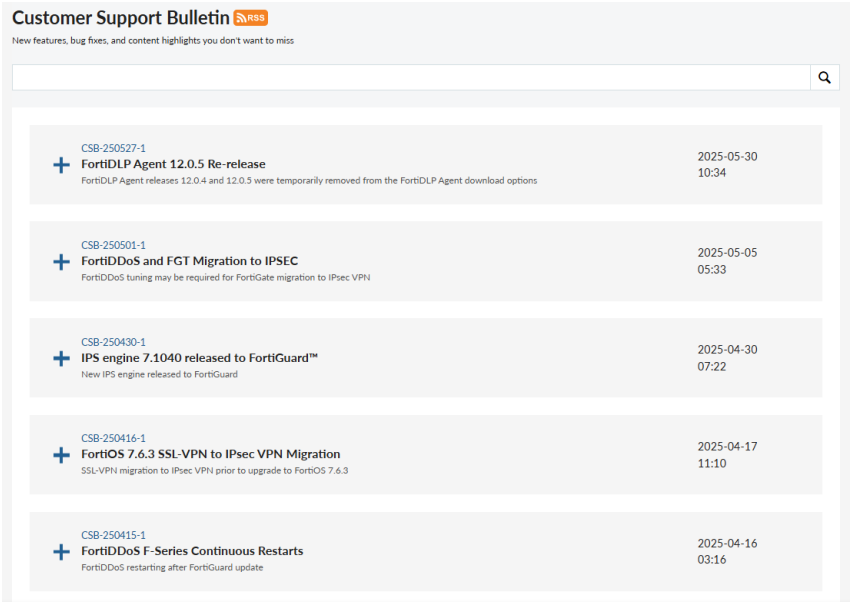
Bug Tracker

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

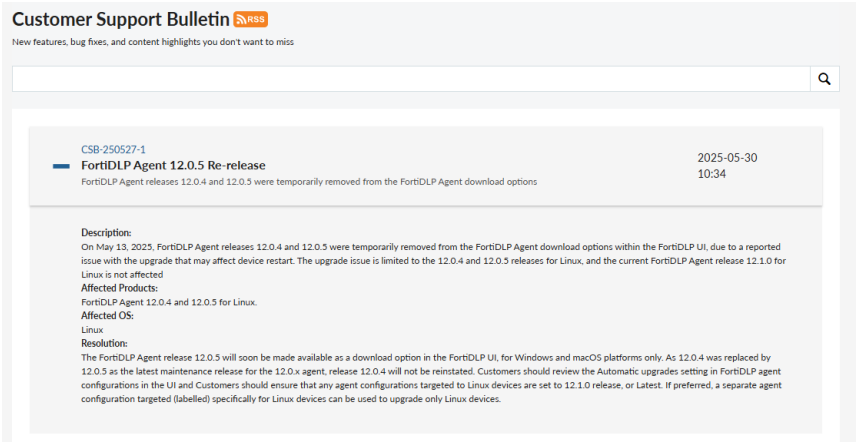
The *Bug Tracker* page is only available to Partners. For more information, see the Partner Administration Guide.

Customer Support Bulletin

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



Select a bulletin card to expand it for more information.

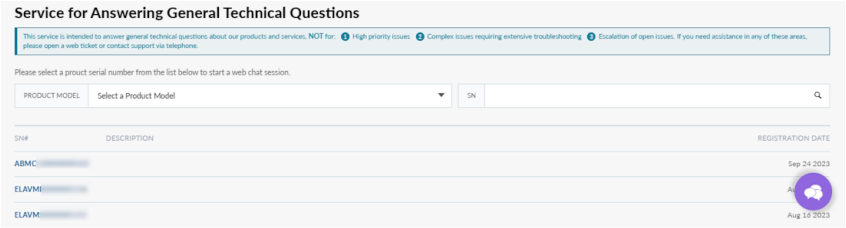


Technical Web Chat

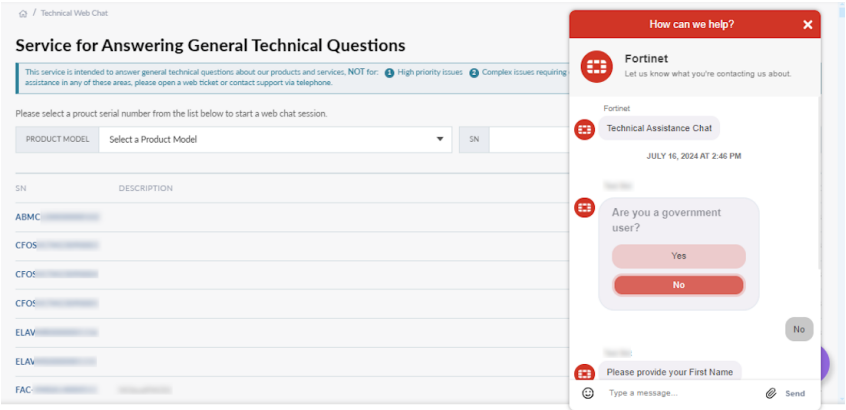
You can join a live chat with a FortiCare support employee using the *Technical Web Chat* page. Live chats can be useful for asking general questions about FortiCare products and services.

To join a web chat:

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



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



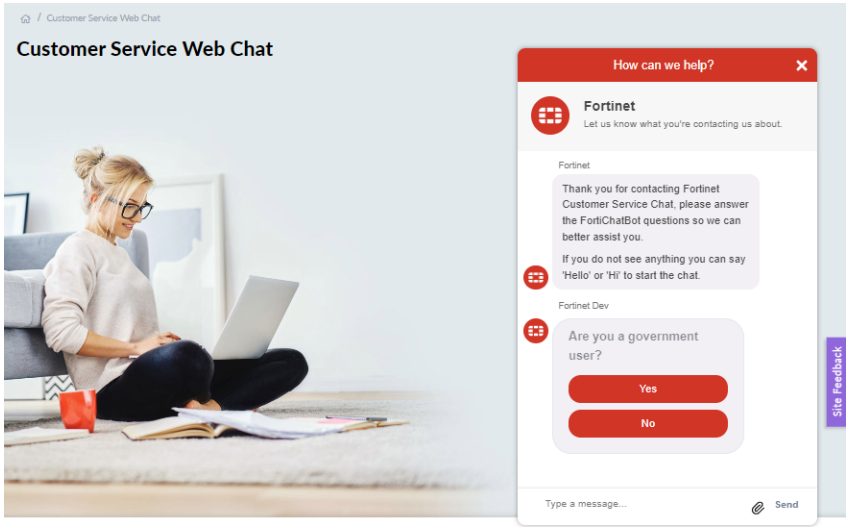
5. Once all of the information has been collected, you will be directed to a live chat.

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.

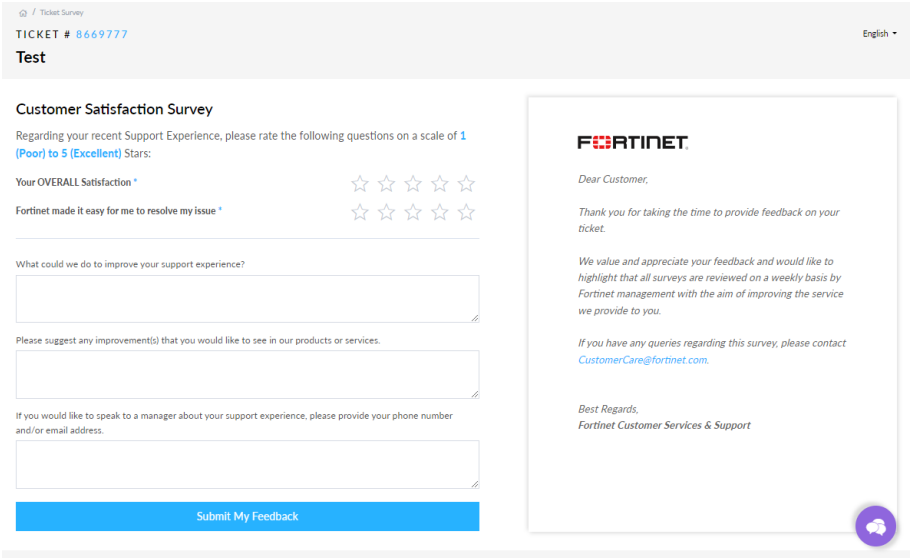
Ticket survey

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*. You experience survey is submitted.

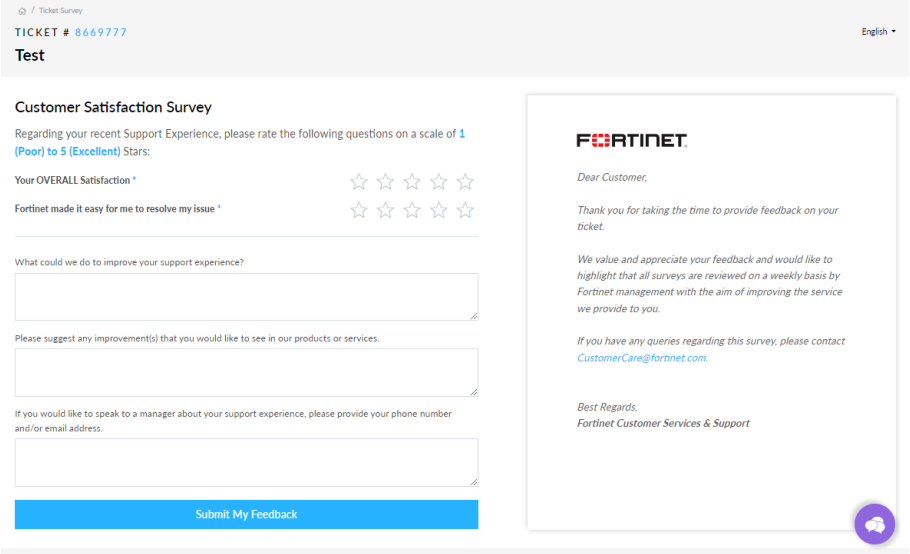
Multilingual survey support

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

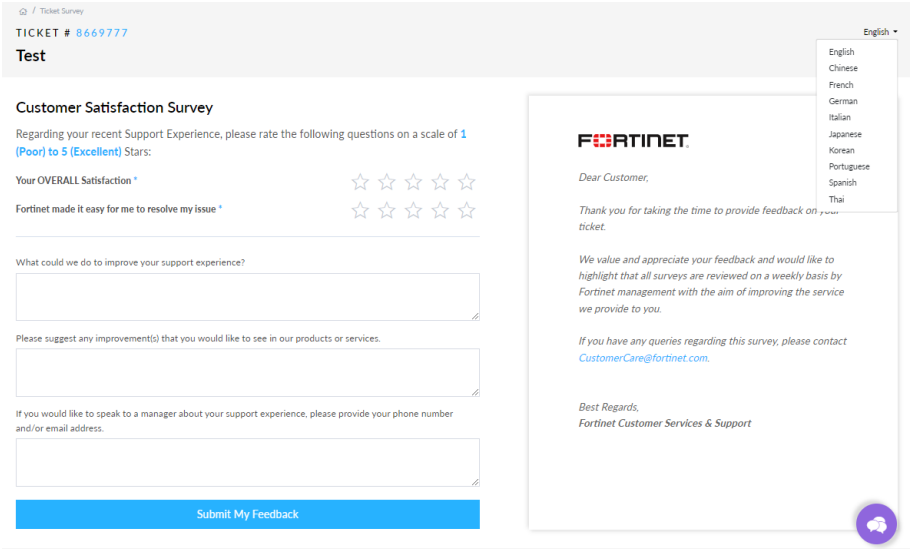
- English
- Chinese
- French
- German
- Italian
- Japanese
- Korean
- Portuguese
- Spanish
- Thai

To change the language:

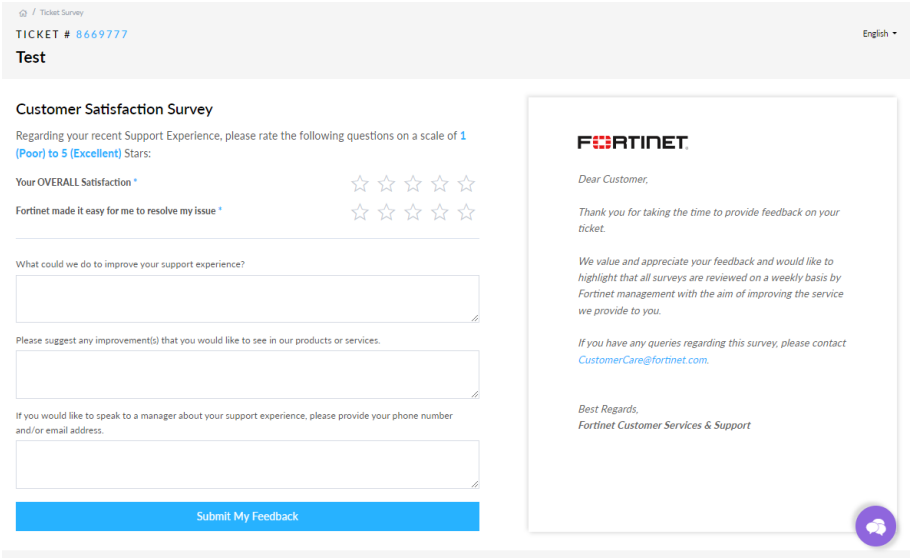
1. Go to *Ticket Survey*.
2. Select the *Ticket#*. The *Customer Satisfaction Survey* opens.



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

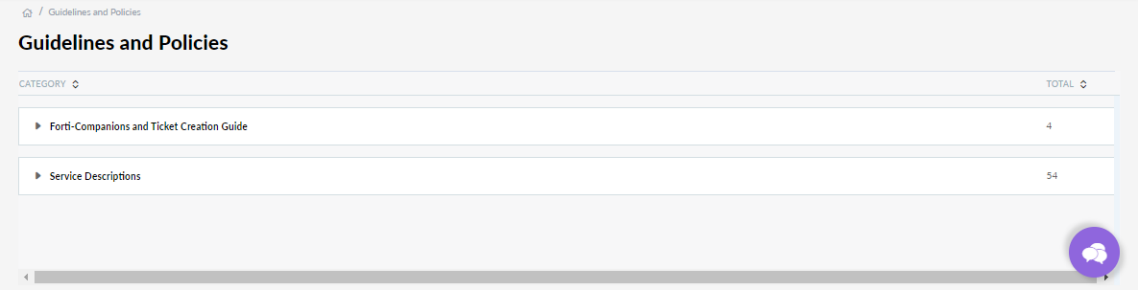


4. Select the language you want. The ticket survey will change to the selected language.

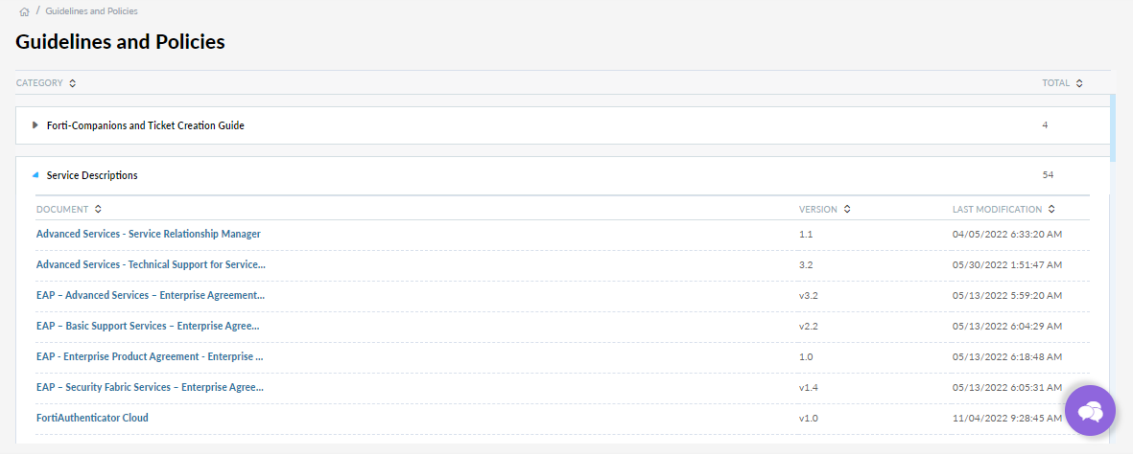


Guidelines and Policies

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



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



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 seethe three most recent comments for tickets.
Customize columns on ticket list	Select which columns to automatically display on the *Tickets* 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:

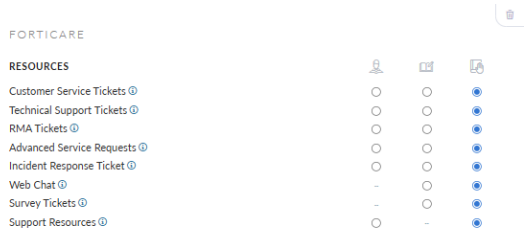
- IAM user, external IdP roles, and Partner accounts. See User access on page 72.
- Organization member account access. See Organization view on page 74.

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.



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.

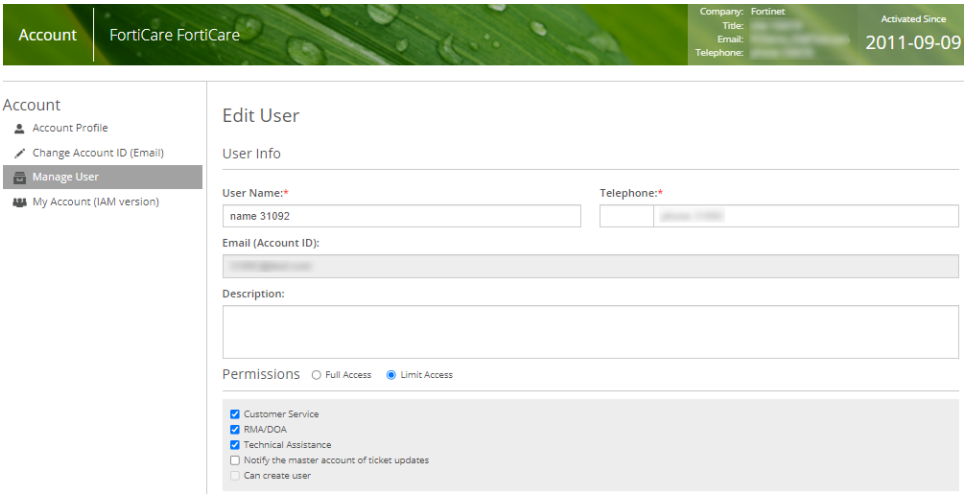
Partners without a FortiCloud account and connected accounts

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.

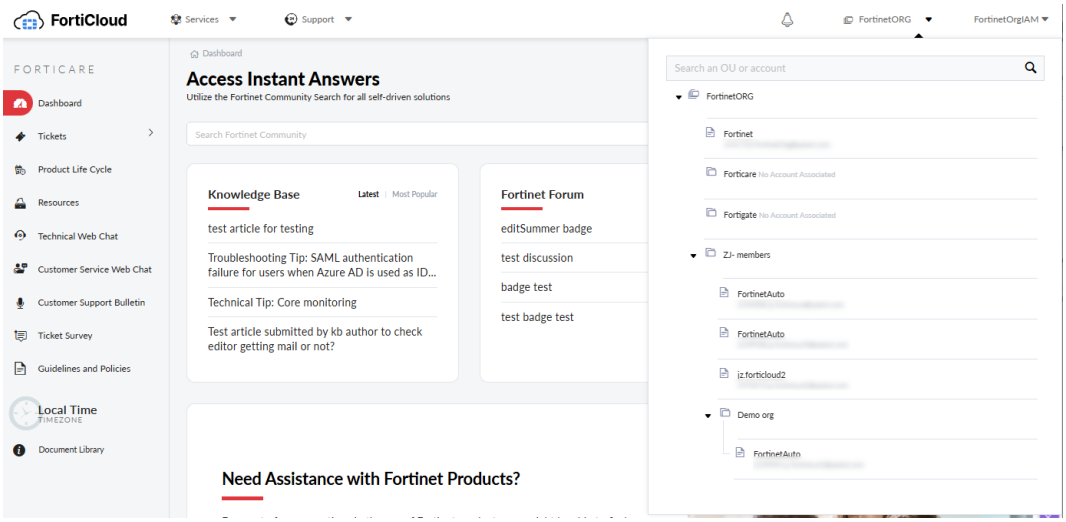


If *Limit Access* is selected, anything not selected from the additional permissions is not available to the sub user. FortiCare access depends on these permissions.

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.

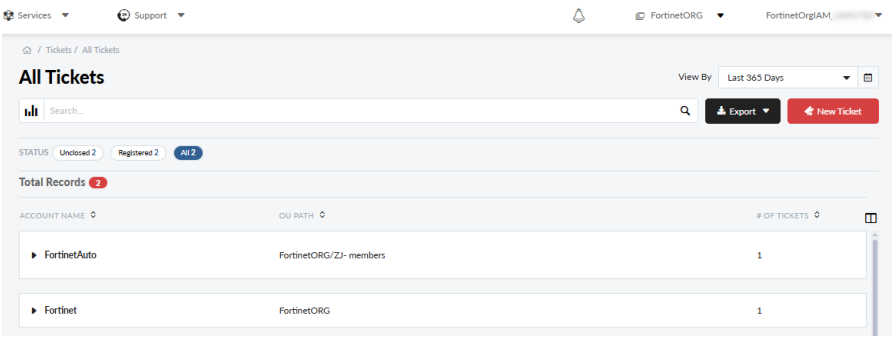
You can switch between Organization member accounts and OUs using the context switch menu. See OU context switch in the Identity & Access Management guide for more information.



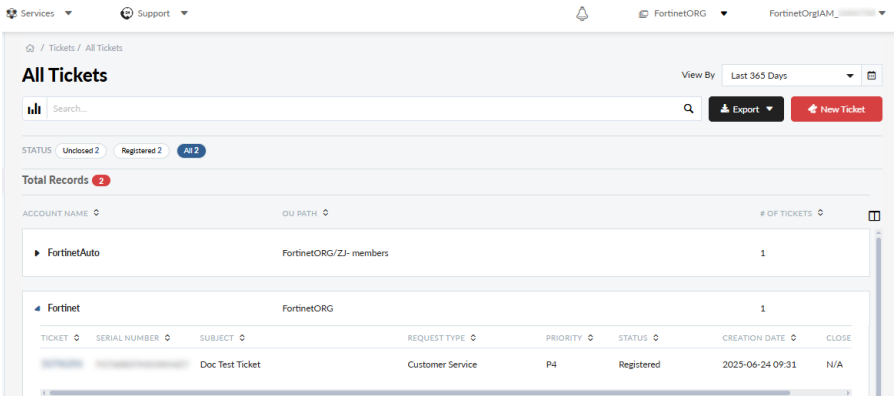
Organizational Unit (OU) view

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.

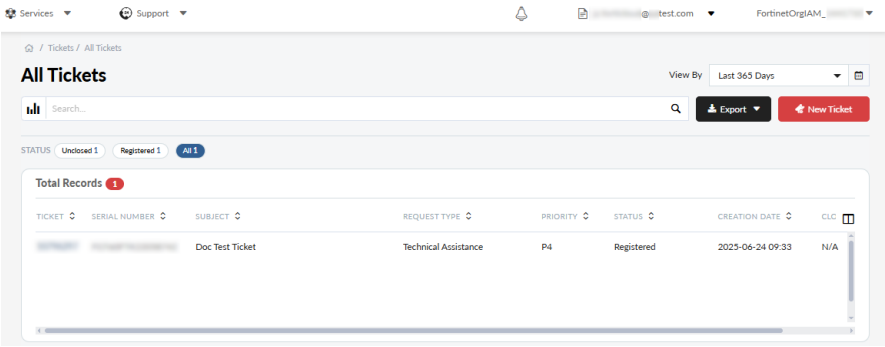
3. Hover over the account you want to assign the ticket to and click *Select*.

> 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.



To create a ticket within the member account view, follow the same procedure as creating a ticket outside of the Organization view. See Creating tickets on page 15.

www.fortinet.com