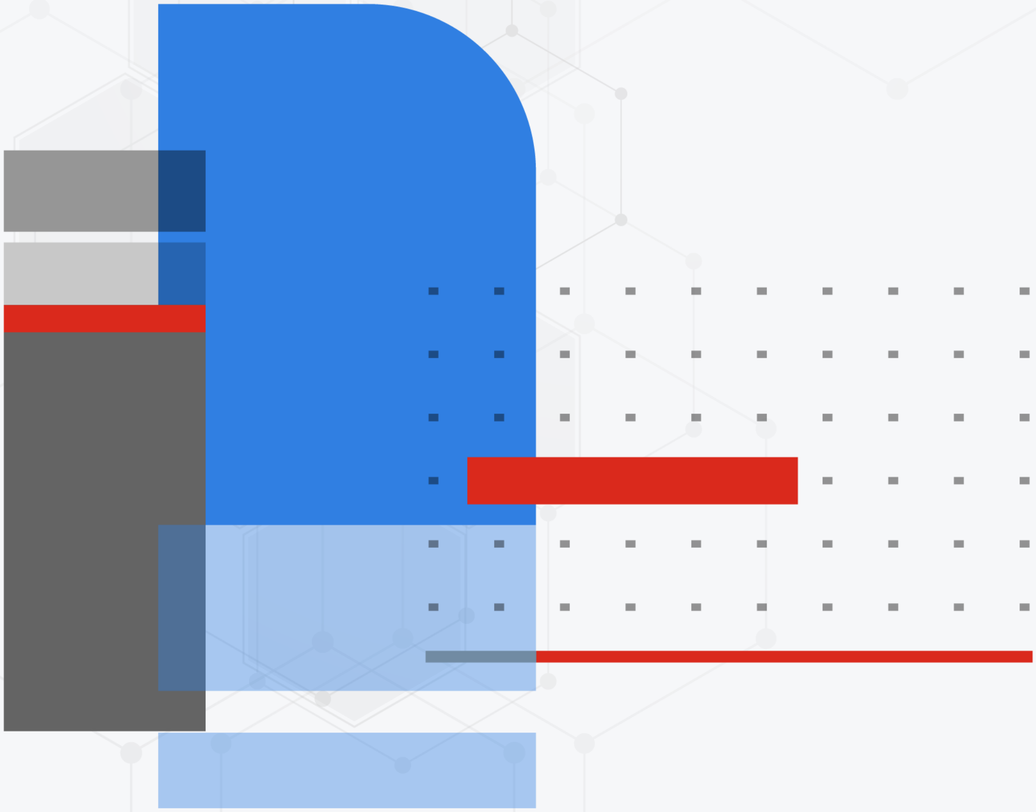
Administration Guide

Advanced Services 24.1



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

February 03, 2024
Advanced Services 24.1 Administration Guide
57-241-986048-20240203

TABLE OF CONTENTS

Change Log

Date	Change Description
2024-02-03	Initial release.

Introduction

The *Advanced Services* portal allows Fortinet customers with an active Advanced Support service or FortiGuard Incident Response service contract to request different service activities in exchange for Service Points.

Eligible contracts

The Advanced Services portal is available to customers with the following contracts:

- **For access to Advanced Services Requests (AS Requests)**: 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 and AS Pro Plus Global.
- **For access to Incident Response Requests (IR Requests)**: FortiGuard Incident Readiness Subscription Service.

Service requests

Two types Services Requests are available:

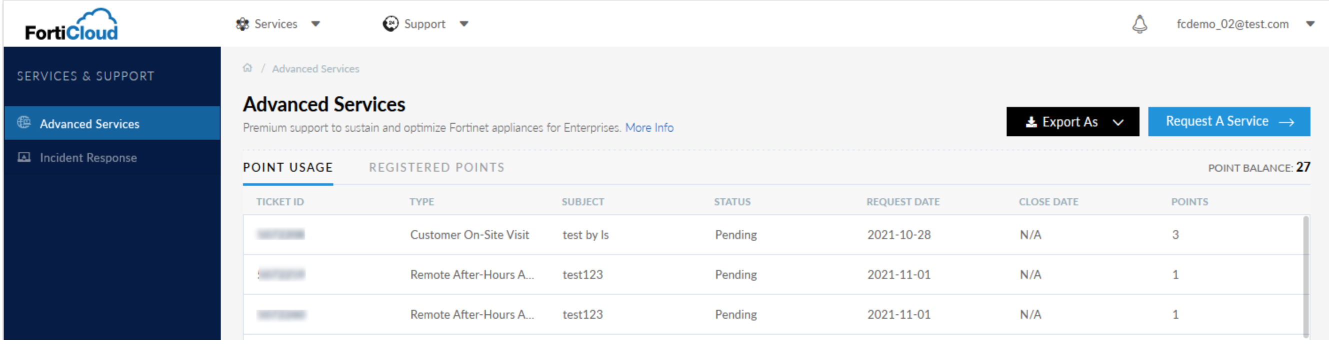
- **Advanced Services Requests**: Provides professional assistance to get the most out of your Fortinet products. Services include, Customer On-Site Visit, Remote After-Hours Assistance, and more.
- **Incident Response Requests**: Provides support for planning your security posture, identifying gaps 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.

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 (AS) portal

The *Advanced Services* (AS) portal displays the current Point Usage and Registered Points for Advanced Service and Incident Response Services. Use the portal 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

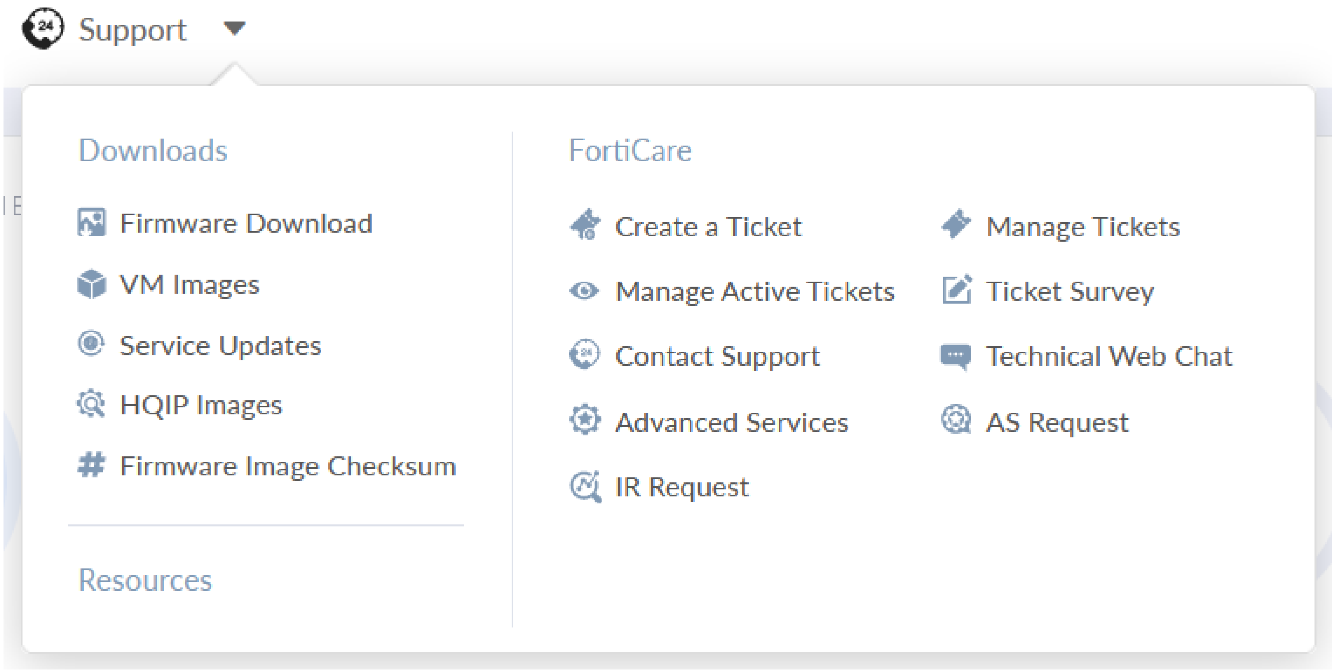
Premium support to sustain and optimize Fortinet appliances for Enterprises. More Info

TICKET ID	TYPE	SUBJECT	STATUS	REQUEST DATE	CLOSE DATE	POINTS
[redacted]	Customer On-Site Visit	test by ls	Pending	2021-10-28	N/A	3
[redacted]	Remote After-Hours A...	test123	Pending	2021-11-01	N/A	1
[redacted]	Remote After-Hours A...	test123	Pending	2021-11-01	N/A	1

Advanced Services	Displays the *Point Usage* and *Registered Points* for Advanced Services requests. Click *Request a Service* to create a new Advanced Service request. See, Creating an Advanced Service ticket on page 9.
Incident Response	Displays the *Point Usage* and *Registered Points* for Incident Response requests. Click *Request a Service* to create a new Incident Response request. See, Creating an Incident Response ticket on page 19.
Point Usage	Displays the current Advanced Services and Incident Response 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 a service	Click to create a new *Advanced Services* or *Incident Response* 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.

Accessing the Advanced Services portal

You can access the Advanced Services portal from the *Support* menu in the FortiCloud banner. Click *IR Request* or *AS Request* to open the portal. These menus are only visible when an eligible service contract is registered and active (see, Introduction on page 5).



Supported user types

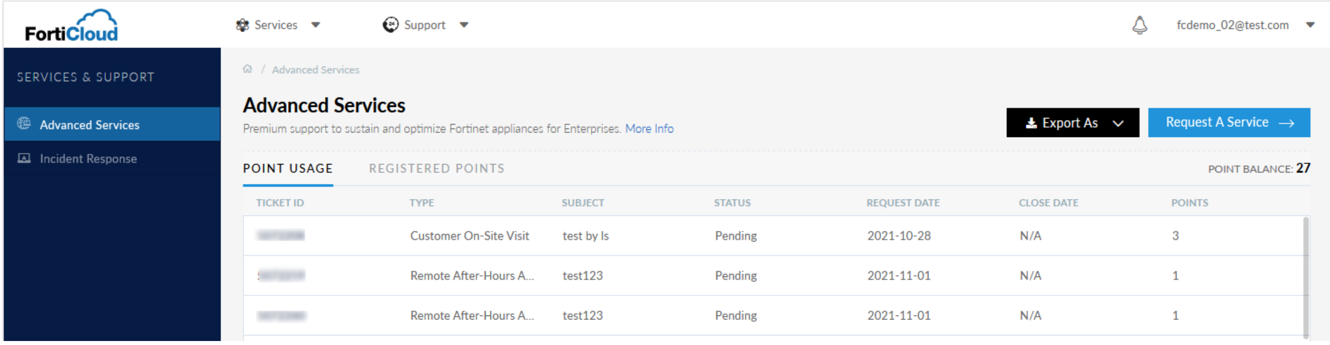
Advanced Services and Incident Response entitlements are required to access the portal. The Advanced Services portal supports both IAM and legacy Sub User models. For more information about FortiCloud's user management models, see *Identity & Access Management (IAM)* > *User management models*.

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 portal. Sub Users can view the *Advanced Services* and *Incident Response* tabs depending on the account and its entitlements.
Partner User	Partner users can access the portal after they select an account in the Asset Management portal. For information, see *Asset Management for Partners* > *Selecting accounts*. When a partner has Sub User (Full Access) permissions for the selected account, the permissions above apply.

Advanced Services view

Advanced Services provides professional assistance to get the most out of your Fortinet products.

The *Advanced Services* view displays the service tickets created in your account. Use this view to monitor your service points usage and registered points. You can also create a new service request or view the ticket and comment on it in FortiCloud.



Advanced Services

Premium support to sustain and optimize Fortinet appliances for Enterprises. More Info

POINT BALANCE: 27

TICKET ID	TYPE	SUBJECT	STATUS	REQUEST DATE	CLOSE DATE	POINTS
[redacted]	Customer On-Site Visit	test by ls	Pending	2021-10-28	N/A	3
[redacted]	Remote After-Hours A...	test123	Pending	2021-11-01	N/A	1
[redacted]	Remote After-Hours A...	test123	Pending	2021-11-01	N/A	1

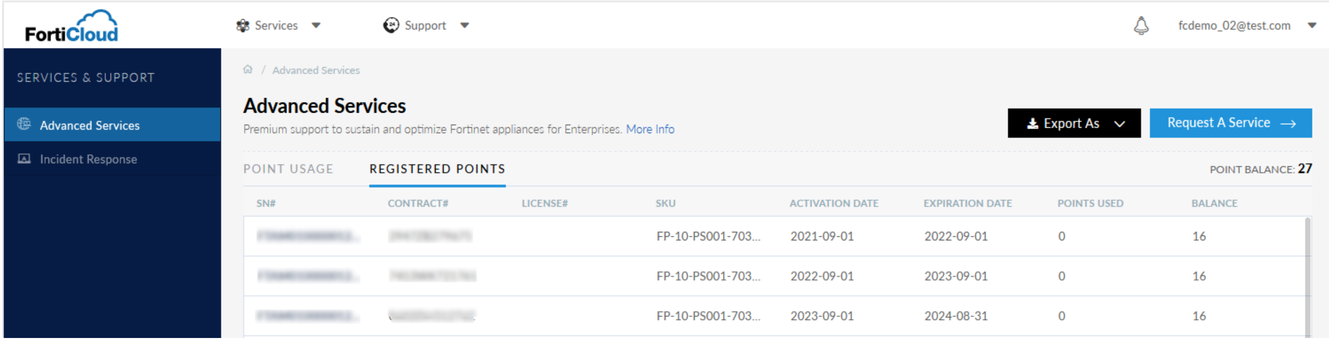
Point Usage

The *Points 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 Advanced Services types on page 13.
Subject	The *Subject* text that was entered at the time the ticket was created. See Creating an Advanced Service ticket on page 9.
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.



Advanced Services / Advanced Services

Advanced Services

Premium support to sustain and optimize Fortinet appliances for Enterprises. More Info

POINT BALANCE: 27

SN#	CONTRACT#	LICENSE#	SKU	ACTIVATION DATE	EXPIRATION DATE	POINTS USED	BALANCE
[redacted]	[redacted]		FP-10-PS001-703...	2021-09-01	2022-09-01	0	16
[redacted]	[redacted]		FP-10-PS001-703...	2022-09-01	2023-09-01	0	16
[redacted]	[redacted]		FP-10-PS001-703...	2023-09-01	2024-08-31	0	16

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. Click *Export As* and select either *Excel File* or *CSV File*.
2. In the dialog that opens, choose to open the file or save it to your device, and click *OK*.

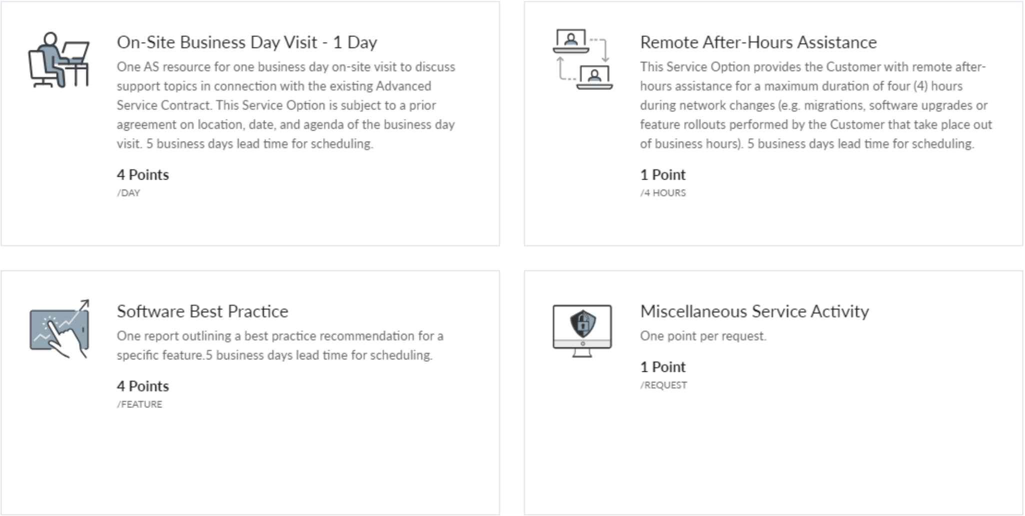
Creating an Advanced Service ticket

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 cancelled the points are released.

To create a service request:

1. Click *Request a Service*. The *Choose a Service* page opens.
2. Select a service and click *Next*.

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



On-Site Business Day Visit - 1 Day

One AS resource for one business day on-site visit to discuss support topics in connection with the existing Advanced Service Contract. This Service Option is subject to a prior agreement on location, date, and agenda of the business day visit. 5 business days lead time for scheduling.

4 Points
/DAY

Remote After-Hours Assistance

This Service Option provides the Customer with remote after-hours assistance for a maximum duration of four (4) hours during network changes (e.g. migrations, software upgrades or feature rollouts performed by the Customer that take place out of business hours). 5 business days lead time for scheduling.

1 Point
/4 HOURS

Software Best Practice

One report outlining a best practice recommendation for a specific feature.5 business days lead time for scheduling.

4 Points
/FEATURE

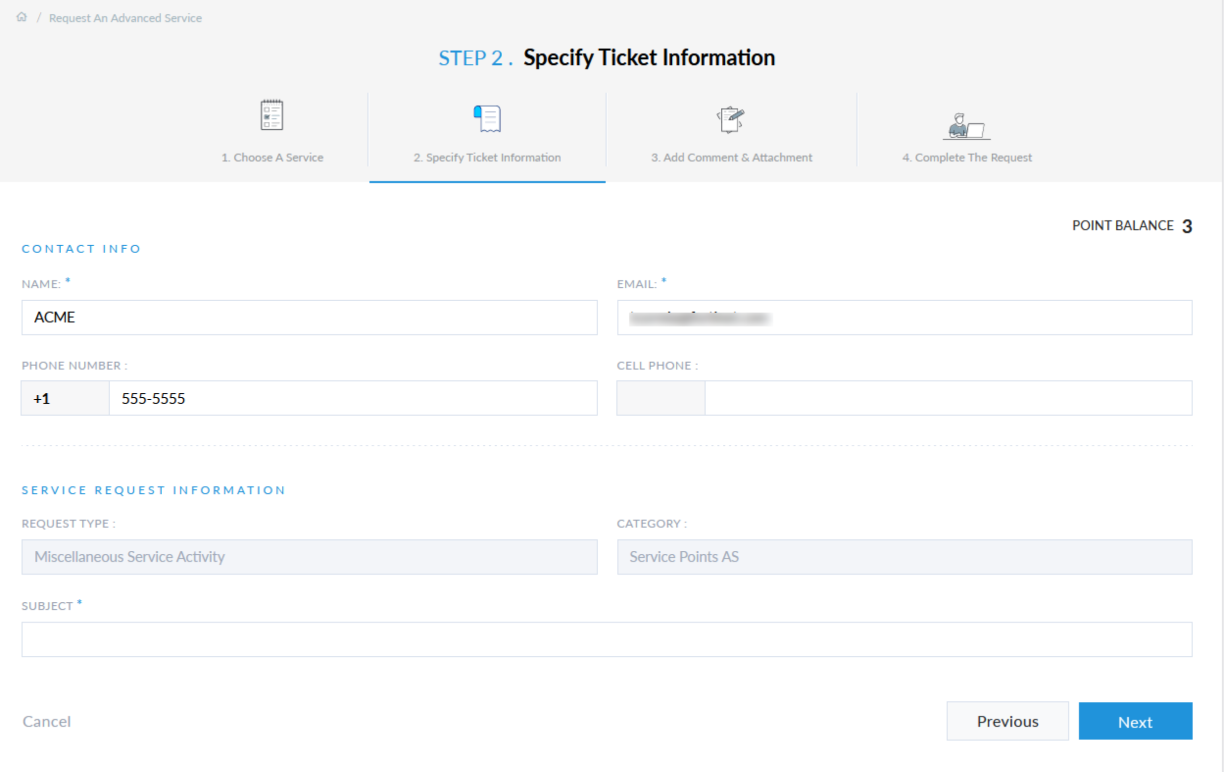
Miscellaneous Service Activity

One point per request.

1 Point
/REQUEST

3. Complete the *Specify Ticket Information* form.
   a. In the *Contact Info* section enter your *Name*, *Email*, *Phone Number*, and *Cell Phone*.
   b. In the *Service Request* Information section, use the *Subject* field to describe the request, and click Next. The

Add Comment & Attachment page opens.



Request An Advanced Service
STEP 2 . Specify Ticket Information
1. Choose A Service
2. Specify Ticket Information
3. Add Comment & Attachment
4. Complete The Request
Cancel
Previous
Next

POINT BALANCE 3

CONTACT INFO

NAME: *	EMAIL: *
ACME	[redacted]
PHONE NUMBER :	CELL PHONE :
+1 555-5555	

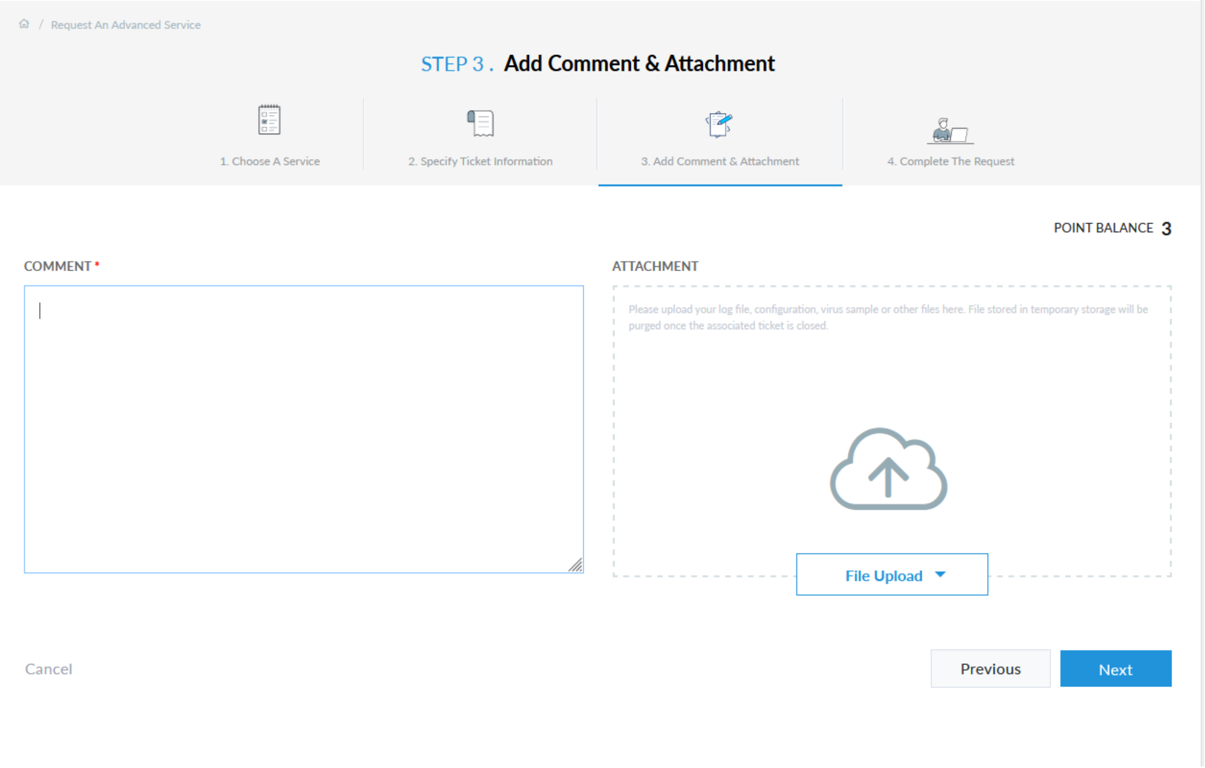
SERVICE REQUEST INFORMATION

REQUEST TYPE :	CATEGORY :
Miscellaneous Service Activity	Service Points AS

SUBJECT *

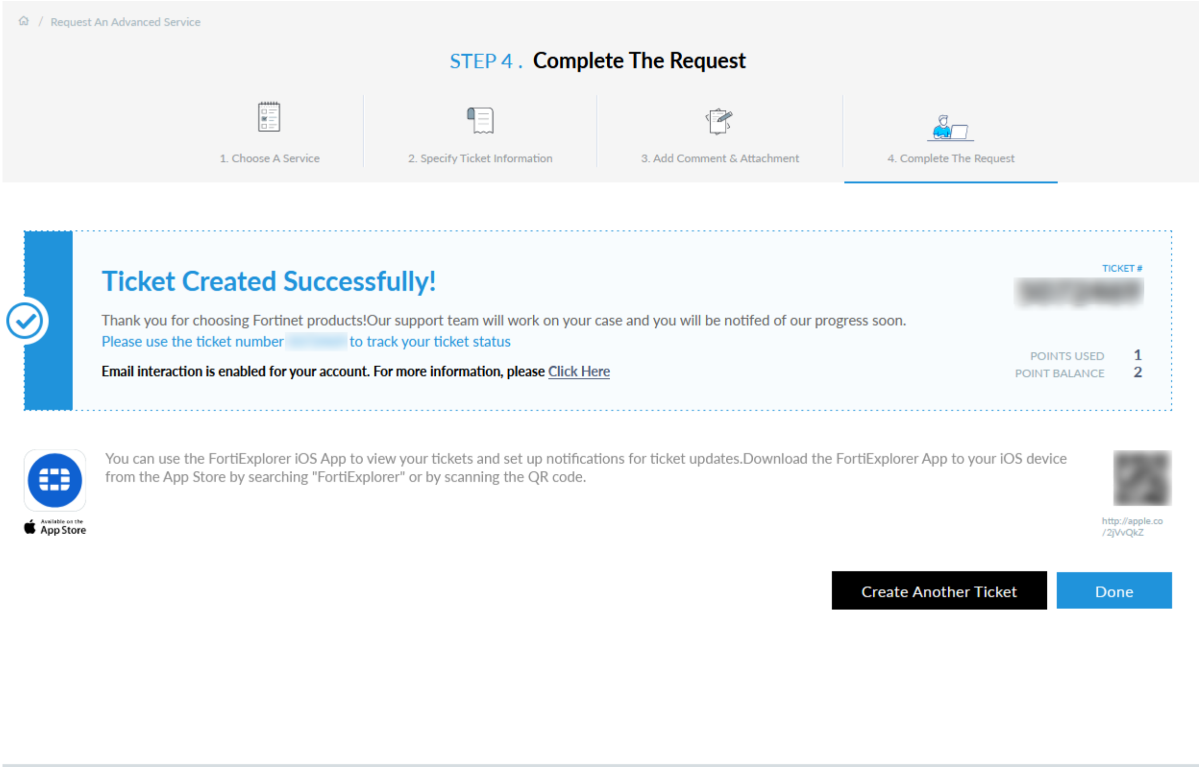
4. Add a comment and attachment.
   1. In the *Comment* section, describe the attachment.
   2. In the *Attachment* section, click *File* Upload.
   3. From the menu, select *Log File*, *Configuration*, *Virus Sample File (Temp)*, or *Other*.

d. Click *Next*. The *Complete The Request* page opens and your ticket reference number is displayed.


Request An Advanced Service
STEP 3 . Add Comment & Attachment
1. Choose A Service
2. Specify Ticket Information
3. Add Comment & Attachment
4. Complete The Request
POINT BALANCE 3
COMMENT *
ATTACHMENT
File Upload
Cancel
Previous
Next

Please upload your log file, configuration, virus sample or other files here. File stored in temporary storage will be purged once the associated ticket is closed.

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


Request An Advanced Service
STEP 4 . Complete The Request
1. Choose A Service
2. Specify Ticket Information
3. Add Comment & Attachment
4. Complete The Request
Available on the App Store
http://apple.co /2jVvQkZ
Create Another Ticket
Done

Ticket Created Successfully!

TICKET # [redacted]

Thank you for choosing Fortinet products!Our support team will work on your case and you will be notifed of our progress soon.

Please use the ticket number [redacted] to track your ticket status

Email interaction is enabled for your account. For more information, please Click Here

POINTS USED	1
POINT BALANCE	2

You can use the FortiExplorer iOS App to view your tickets and set up notifications for ticket updates.Download the FortiExplorer App to your iOS device from the App Store by searching "FortiExplorer" or by scanning the QR code.

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 hardware components.	6

Service	Description	Points
	• 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
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

Service	Description	Points
Knowledge Transfer - Customer 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	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
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

More information about each Advanced Services option is available in the *Service Points* description available in the Customer Service portal at https://support.fortinet.com/Information/DocumentList.aspx.

Incident Response view

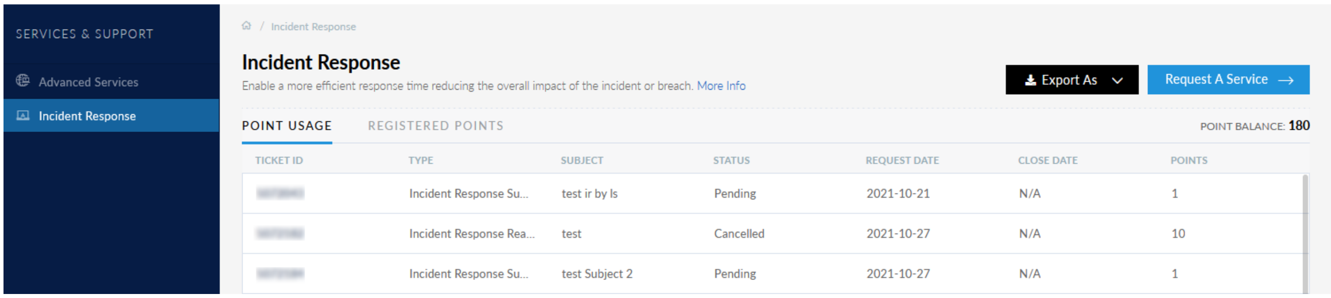
Incident Response provides support for planning your security posture, identifying gaps in your security processes, and develop a playbook in the event of a critical attack.

More information is available in the *FortiGuard Incident Response Service* description available in the Customer Service portal at https://support.fortinet.com/Information/DocumentList.aspx.

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.

Point Usage

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



Incident Response

Enable a more efficient response time reducing the overall impact of the incident or breach. More Info

POINT BALANCE: 180

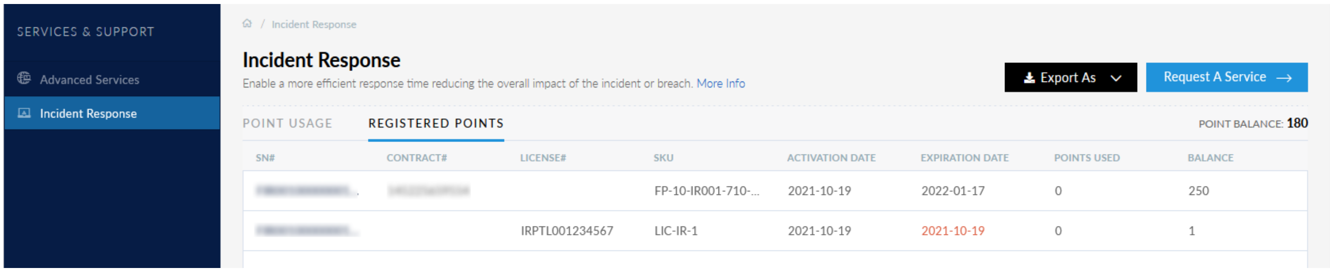
TICKET ID	TYPE	SUBJECT	STATUS	REQUEST DATE	CLOSE DATE	POINTS
[redacted]	Incident Response Su...	test ir by ls	Pending	2021-10-21	N/A	1
[redacted]	Incident Response Rea...	test	Cancelled	2021-10-27	N/A	10
[redacted]	Incident Response Su...	test Subject 2	Pending	2021-10-27	N/A	1

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 22.
Subject	The *Subject* text that was entered at the time the ticket was created. See Creating an Incident Response ticket on page 19.
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 servies points has been agreed upon between you and Fortinet. • *Cancelled*: 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.

Point Usage	Description
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 service points balance for each contract. The entitlement period of the points corresponds to the contract period. This means any unused points will be forfeited on the contract expiry date. If there are multiple active contracts, the points are consumed based on a first-in-first-out rule to ensure the points that are expiring are used first.



Incident Response

Enable a more efficient response time reducing the overall impact of the incident or breach. More Info

POINT BALANCE: 180

SN#	CONTRACT#	LICENSE#	SKU	ACTIVATION DATE	EXPIRATION DATE	POINTS USED	BALANCE
[redacted]	[redacted]		FP-10-IR001-710-...	2021-10-19	2022-01-17	0	250
[redacted]		IRPTL001234567	LIC-IR-1	2021-10-19	2021-10-19	0	1

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. Click *Export As* and select either *Excel File* or *CSV File*.
2. In the dialog that opens, choose to open the file or save it to your device, and click *OK*.

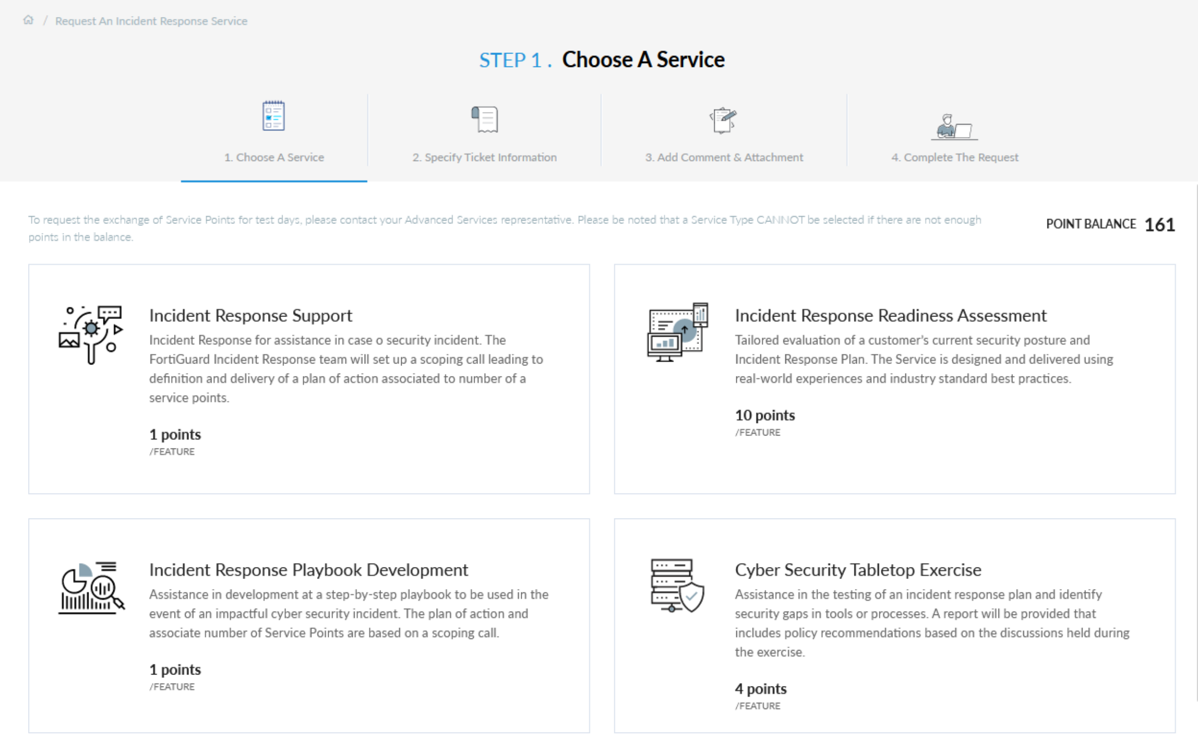
Creating an Incident Response ticket

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. Click *Request a Service*. The *Choose a Service* page opens.
2. Select a service and click *Next*. See, Incident Response types on page 22.

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



Request An Incident Response Service

STEP 1 . Choose A Service

To request the exchange of Service Points for test days, please contact your Advanced Services representative. Please be noted that a Service Type CANNOT be selected if there are not enough points in the balance.

POINT BALANCE 161

Incident Response Support
Incident Response for assistance in case o 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 points
/FEATURE

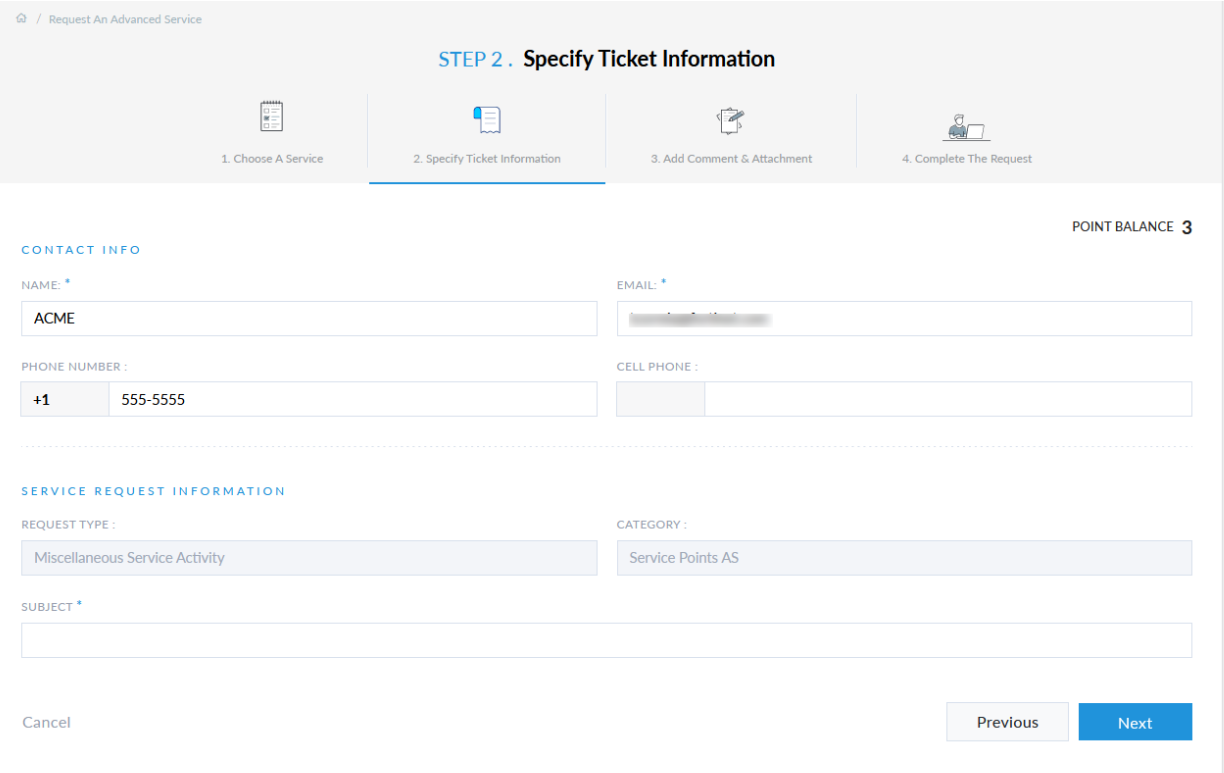
Incident Response Readiness Assessment
Tailored evaluation of a customer's current security posture and Incident Response Plan. The Service is designed and delivered using real-world experiences and industry standard best practices.
10 points
/FEATURE

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

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

3. Complete the *Specify Ticket Information* form.
   a. In the *Contact Info* section enter your *Name*, *Email*, *Phone Number*, and *Cell Phone*.
   b. In the *Service Request* Information section, use the *Subject* field to describe the request, and click Next. The

Add Comment & Attachment page opens.


Request An Advanced Service
1. Choose A Service
2. Specify Ticket Information
3. Add Comment & Attachment
4. Complete The Request
Cancel
Previous
Next

STEP 2 . Specify Ticket Information

POINT BALANCE 3

CONTACT INFO

NAME: * ACME	EMAIL: * [redacted]
PHONE NUMBER : +1 555-5555	CELL PHONE :

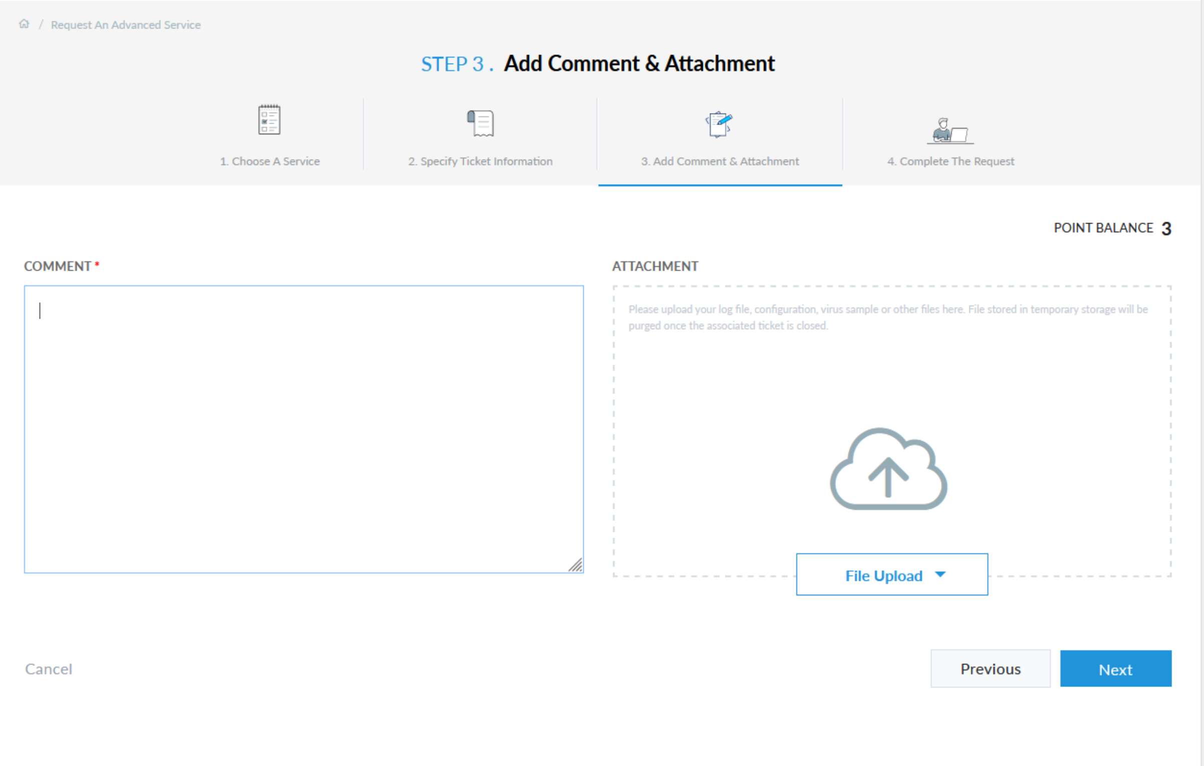
SERVICE REQUEST INFORMATION

REQUEST TYPE : Miscellaneous Service Activity	CATEGORY : Service Points AS

SUBJECT *

4. 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*, *Virus Sample File (Temp)*, or *Other*.

d. Click *Next*. The *Complete The Request* page opens and your ticket reference number is displayed.



Request An Advanced Service

STEP 3 . Add Comment & Attachment

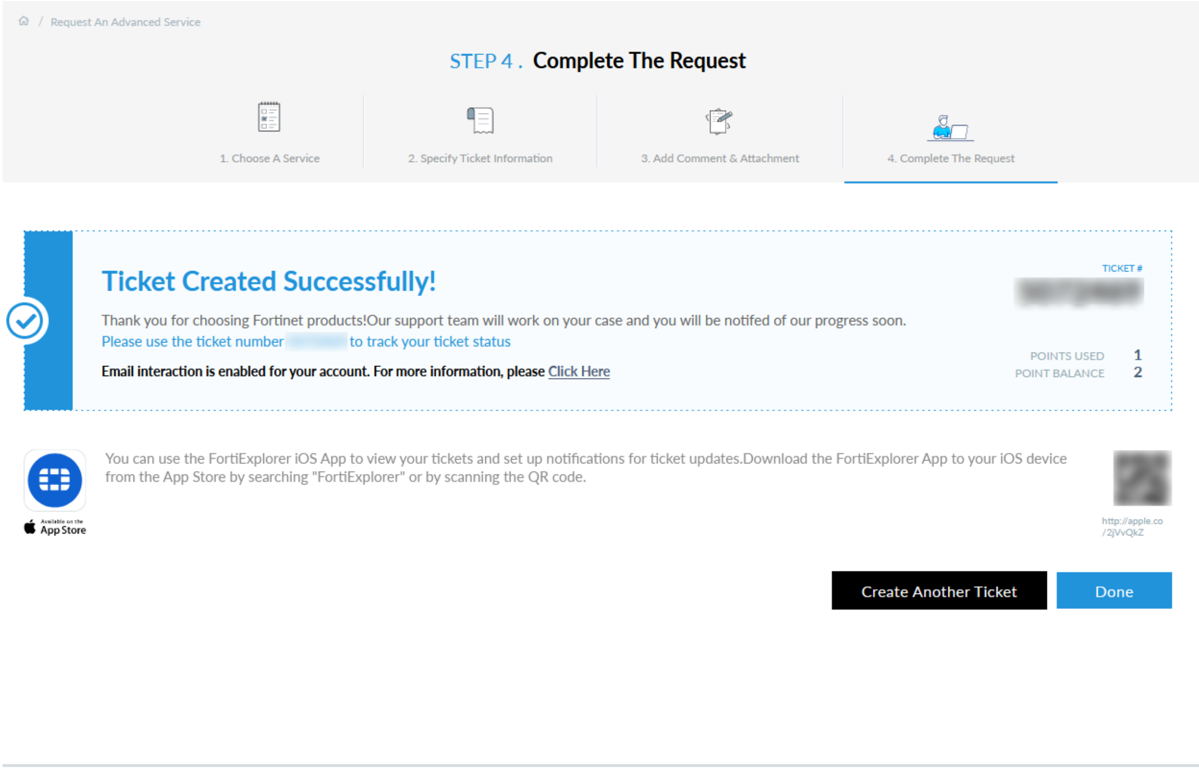
POINT BALANCE 3

COMMENT *

ATTACHMENT

Please upload your log file, configuration, virus sample or other files here. File stored in temporary storage will be purged once the associated ticket is closed.

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



Request An Advanced Service

STEP 4 . Complete The Request

Ticket Created Successfully!

Thank you for choosing Fortinet products!Our support team will work on your case and you will be notifed of our progress soon.
Please use the ticket number [redacted] to track your ticket status

Email interaction is enabled for your account. For more information, please Click Here

TICKET # [redacted]

POINTS USED	1
POINT BALANCE	2

You can use the FortiExplorer iOS App to view your tickets and set up notifications for ticket updates.Download the FortiExplorer App to your iOS device from the App Store by searching "FortiExplorer" or by scanning the QR code.

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. • *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,	10

Service	Description	Points
	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. 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.	1
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	20

Service	Description	Points
	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.	
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	10

Service	Description	Points
	incident.	
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. 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.	1
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.	1

Service	Description	Points
	- *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. - *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	1

Service	Description	Points
	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 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	1

Service	Description	Points
	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 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 at https://support.fortinet.com/Information/DocumentList.aspx.

www.fortinet.com