FortiConverter Service - Admin Guide

Version 23.1.0

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

December 18th, 2023
FortiConverter Service 23.1.0 Admin Guide
00-400-000000-20181031

TABLE OF CONTENTS

About FortiConverter Service

FortiConverter Service helps you migrate configurations to the latest version of FortiOS. This service is useful for migrating a pre-existing third-party firewall policy to a new FortiGate appliance, or even an older FortiGate policy to a new one.

Access to FortiConverter Service Portal and create service tickets:

https://service.forticonverter.com/

Click here for tutorial video on creating FortiConverter Service Ticket.

(The video will either play automatically or download to your local machine depending on the browser.)

Common questions on FortiConverter Service can be found in General FAQs on page 16.

Business Hours

FortiConverter service team processes all FortiConverter service tickets for configuration conversions. The following are the business hours for the FortiConverter service team:

Monday - Friday 9:00am - 6:00pm U.S. West/Pacific Standard Time

(Except U.S. holidays and weekends.)

Please note that FortiConverter service is a ticket based service, please post updates on the FortiConverter service portal and our Engineers will provide an email update as soon as possible.

FortiGate Configuration Migration

All FortiGate to FortiGate configurations are fully supported with the exceptions of the following:

- The upgrades for managed software or external devices (such as FortiAP, FortiToken, FortiClient EMS, FortiManager, FortiSwitch) are not supported.
- Merging new configurations to existing configurations as long as there is no network overlap. If there is a network overlap, converted files will be provided and customer needs to manually tune the configs.

- Device Conversions from non-vdom mode to vdom mode or vice versa is supported.
- Hardware switches will be converted to software switches where the new target device does not support the hardware switch.
- Limited addition of new features like SDWAN, LAG are supported. Other configuration of new feature sets (which are currently not in the existing configuration), please reach out to TAC support for assistance.
- For security purposes, the default admin account password will be reset. In general, encrypted secret data, credentials, e.g., VPN pre-shared keys, certificates, local users, and admin passwords, will remain valid after cross model migration as long as the FOS version is above 5.6.
- Legacy device migrations from 4.0 are fully supported. For 3.x there could be instances where specific sections of the configuration may not be able to be migrated.

3rd Party Security Vendors Conversion

Supported 3rd party vendors

Vendor	Models	Versions	Convertible Objects
Barracuda	Web Application Firewall	8.x 9.x	• Addresses & Address Groups • Interfaces • Policies • NAT • Service & Service Groups • Static Routes
Bluecoat	SGOS	6.5.10 6.7.4 6.7.5	• Addresses & Address Groups • Interface • Proxy Address & Address Groups • Proxy Policy • Service • Service group • Static route • Zones

Vendor	Models	Versions	Convertible Objects
CheckPoint	SmartCenter	NGFP1 (4.0) to NGX R82	• Addresses & Address Groups • Application List • Firewall-schedule • Interfaces • IPSEC VPN • Local Users & Groups • Multicast-address & policy • NAT (Central NAT) • OSPF • Policies • RPC Service • Schedules • Servers • Services & Service Groups • Session helper • Static Routes • Static URL
	Provider-1	NGX R65 to R82	
	VSX	R65 onward	
Ciena (Vyatta)	VyOS	5.2 to 6.7	• Addresses & Address Groups • DHCP server • Interface • IPSEC VPN • Policy • NAT (Central NAT) • Route • Services & Service Groups • Users & Groups • VLAN • Zone
CIPA	Cipafilter	11.x onward	• Addresses & Address Groups • Interfaces • NAT • Policies • Services & Service Groups • Static Routes

Vendor	Models	Versions	Convertible Objects
Cisco	ASA	7.x onward	• ACLs • Addresses & Address Groups • DHCP Servers • DNS • Dynamic Routing Protocols: RIP, BGP, OSPF • Enable default IPS profile on all NGFW policy (FTD) • FQDN (FTD) • Interfaces • Local Users & Groups • NAT (Central NAT) • NTP • Policies • Route, Filtering (Route Map, ACLS) • Schedule & Schedule Group • Services & Service Groups • SSLVPN • Static Routes • URL filter (FTD) • VIP & VIP Group • VPN IPSEC Phase1 & Phase2 • Zones
	FWSM	3.x onward	
	PIX	5.x onward	
	FTD	6.x onward	
Cisco	Meraki	MX64 10.107.2	• Address • Address Groups • DHCP server • Interfaces • IPSec VPN • L3 Firewall Rules • One To Many NAT • One To One NAT • Static Routes • VLANs
Huawei	USG Series	V500	• Addresses & Address Groups • DHCP Server • DNS Server

Vendor	Models	Versions	Convertible Objects
			• HA • Interface • IPSEC Policy (VPN) • NAT Policy (Converted to FortiGate SNAT) • NAT Server (Converted to FortiGate VIP) • Policy • Route • Routing Protocol: BGP, OSPF • Security Context • Services & Service Groups • Zone
Juniper	SSG/ISG	ScreenOS 4.x, 5.x, 6.x	• Addresses & Address Groups • BGP • Interfaces • Policies • DHCP Servers & Clients & Relays Interfaces • DNS • IPSEC VPN • Local Users & Groups • NAT (Policy NAT) • NTP • OSPF • RADIUS & LDAP • Schedule • Services & Service Groups • Static Routes • VRF • Zones
	SRX	JunosOS 10.x onward	• Addresses & Address Groups • BGP • DHCP Servers & Client & Relay • Interfaces • IPSEC VPN • Local Users & Groups • NAT (Central NAT) • OSPF

Vendor	Models	Versions	Convertible Objects
			• Policies • RADIUS & LDAP • Routing-instances (virtual-router) • Services & Service Groups • Static Routes • VRF • Zones
	MX - JunOS		• Addresses & Address Groups & FQDNs • BGP • FQDNs • Interfaces • Policies • Services & Service Groups • Static Routes • VIPs/MIPs
Forcepoint	Sidewinder	7.x onward	• Addresses & Address Groups & FQDNs • Interfaces • Local Users & Groups • Policies • Services & Service Groups • Static Routes • NAT (Policy NAT only) • VPN-IPSEC • Zones
	Stonesoft	5.7 onward	• Addresses & Address Groups • Alias • Interfaces • Local Users & Groups • Policies/ Sub-policy • Radius • Services & Service Groups • Static Routes • NAT • VPN-IPSEC • Zones
Mikrotik	RouterOS	6.49.10 onward	• Aggregate Interface • Addresses & Address Groups

Vendor	Models	Versions	Convertible Objects
			• DHCP • DNS • Interfaces • IPsec • IPV6 Policy • IPV6 Address & Address Groups • VLAN • NAT • NTP • Policies • Services & Service Groups • Static Routes • Zone

Vendor	Models	Versions	Convertible Objects
Palo Alto Networks	PAN OS	PAN-OS 1.x onward	• Addresses & Address Groups • Application ID • Config firewall schedule • Custom URL Filter • DHCP Server & Relay • DLP Profile • Dynamic Address Groups • File Filter Profile • High availability • Interfaces • IPSEC VPN • LDAP • Local Users & Groups • NAT (Central NAT) • NTP • Policies • Routing: BGP, OSPF • Schedules • Security Profile Group • Services & Service Groups • Static Routes • TACACS+ • Use Groups for Active directory • Virtual-wire pair • Web Filter Profile • Zones
PFSense		15.8 onward	• Address & Address Groups • DHCP Server • FQDN Remote Gateway • Interfaces • IP Pools • IPsec • NAT • Policies • Services & Service Groups • SSLVPN • Static Routes • System settings like (hostname, timezone,

Vendor	Models	Versions	Convertible Objects
			language) • User & User Group
Shorewall	Shorewall	1.4.21	• Addresses • Firewall Policies • Interfaces • Services • Zones
Smoothwall	Smoothwall	3.0	• Address & Address Groups • Firewall rules • Interfaces • IP filter • Local DNS hosts • NAT • Service & Service Groups
SonicWall	TZ Series NSA Series SuperMassive Series	SonicOS 4.x onward	• Addresses & Address Groups & FQDNs • Application Mapping • DHCP Servers & Clients & Relays • Interfaces • Local Users & Groups • NAT • NG-FW mode • OSPF • Policies • Schedules • Services & Service Groups • SSLVPN • Static Routes • VPN (IPSEC site to site) • Web Filter Profile • Zones
Sophos	XG Series	SFOS 17.0 - 17.5 MR3	• BGP • HA • Interface • LDAP • NAT • Policy Service & Service Groups • SNMP • SSL and IPsec

Vendor	Models	Versions	Convertible Objects
			• Static route • Users & User Groups • VPN • VPN Users • Zone
	SG Series	6.6 onward	• Addresses & Address Groups • DHCP server • DLP Profile (Block File Extension) • DNS • DNS Conditional Forwarding • HA • Interface • NAT (Central NAT mode only) • NTP • Policy • PPPoE Interface • SD-WAN (Weight-based Load Balance) • Service & Service Groups • Users & User Groups • Web Filter Profile (Exempt Security Profile) • Zone
Ubiquiti	Unifi EdgeOS	7.5.174	• Addresses & Address Groups • DNS • Interfaces • IPsec • NAT • Policies • SDWAN • Services & Service Groups • Static Routes • VPN SSL
WatchGuard	Firebox Series XTM Series	Fireware 11.3 onward	• Addresses & Address Groups • BGP • Central NAT (Global NAT is not supported)

Vendor	Models	Versions	Convertible Objects
			• DHCP server • Interfaces • IPSEC VPN • LDAP and RADIUS servers • Local Users & Groups • NTP • Policies • Services & Service Groups • Static Routes • Zones
Zyxell	USG	4.7.3 onward	• Addresses & Address Groups • Firewall Policies (IPV4 & IPV6) • Interfaces • IP Pools • NAT (Central NAT) • Services & Service Groups • Static Routes • VPN IPSEC Phase1 & Phase2 • VPN SSL • User & User Groups • Zones

General FAQs

Portal Access and FortiGate Device Entitlement

FortiConverter Service Tickets

Configuration Migration

Portal Access and FortiGate Device Entitlement

License Purchase Options

FortiConverter Service is available from either the **Enterprise bundle** or **360 protection bundle**. If you have purchased any of the bundle package, please check your FGT/FWF entitlements to decide if you can skip this step.

For example, from FortiGate 100D to FortiGate 100F configuration migration, you need to purchase a FortiConverter Service contract for FortiGate 100F. Backup a source configuration file from FortiGate 100D and submit a service ticket against FortiGate 100F.

Purchase Option 1 - Through Local Sales Representative on page 17

Purchase Option 2 - Through FortiConverter Service Portal on page 18

Purchase Option 3 - Through Fortinet Support Portal on page 21

Purchase Option 1 - Through Local Sales Representative

Contact your local sales representative and ask for a quote for the FortiConverter Service.

If you don't have a sales contact, please kindly visit the link below to find your nearest sales contact.

https://www.fortinet.com/partners/partner-program/find-a-partner

After making your purchase through a local sales representative, please go to the next section – FortiConverter Service Contract Registration on page 23.

Purchase Option 2 - Through FortiConverter Service Portal

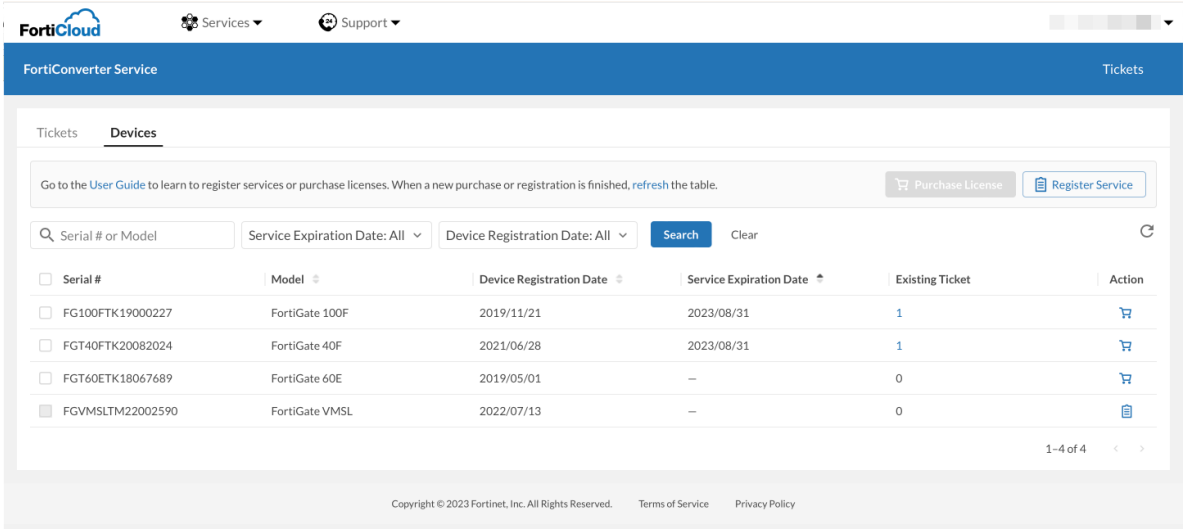
Order online through FortiConverter Service Portal is only available for **North America** users.

Prerequisite

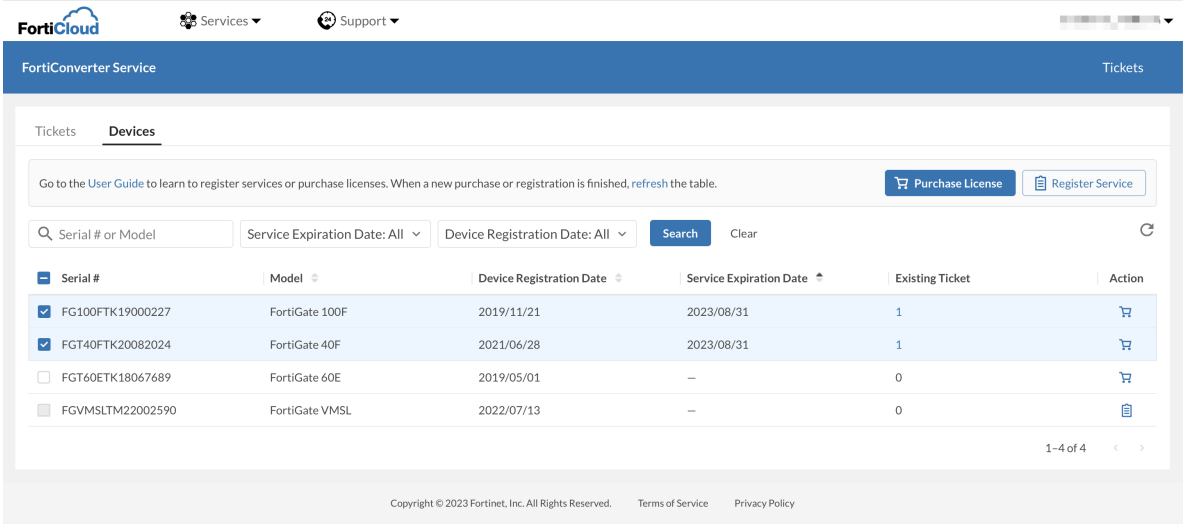
FGT/FWF device(s) are already registered with your FortiCare account. Fortinet only supports account that has less than **50** assets.

Steps to order online through the FortiConverter Service Portal

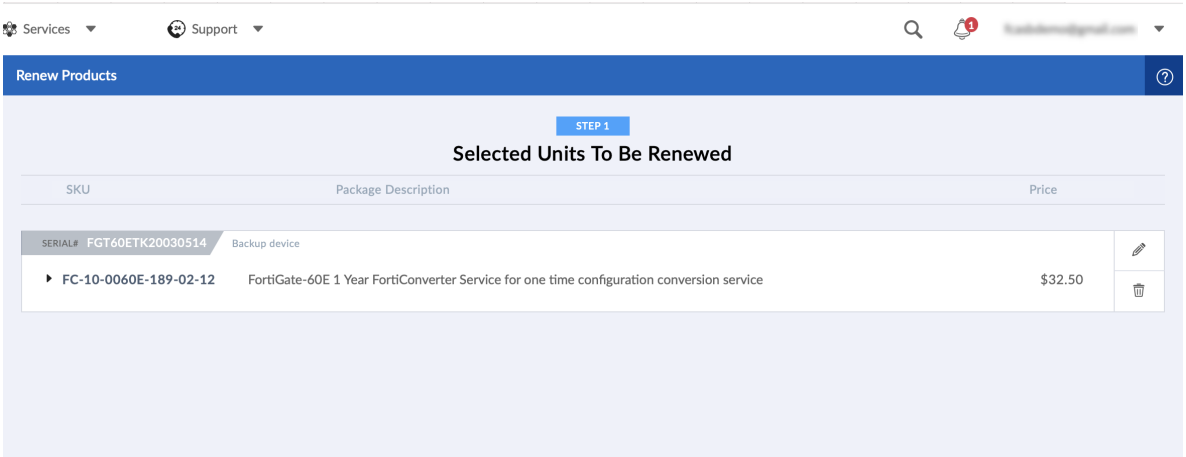
1. Go to **FortiConverter Service Portal** – https://service.forticonverter.com/
2. Click the **Login** button to input your FortiCloud account name and password.
3. **After login, click "Devices" tab and select the FGT/FWF device(s) which you want to purchase.** (The FGT/FWF device(s) shall be the target device, **which the configuration will be migrated to**.) Search your target device from the table by entering the **model** or **serial number**.



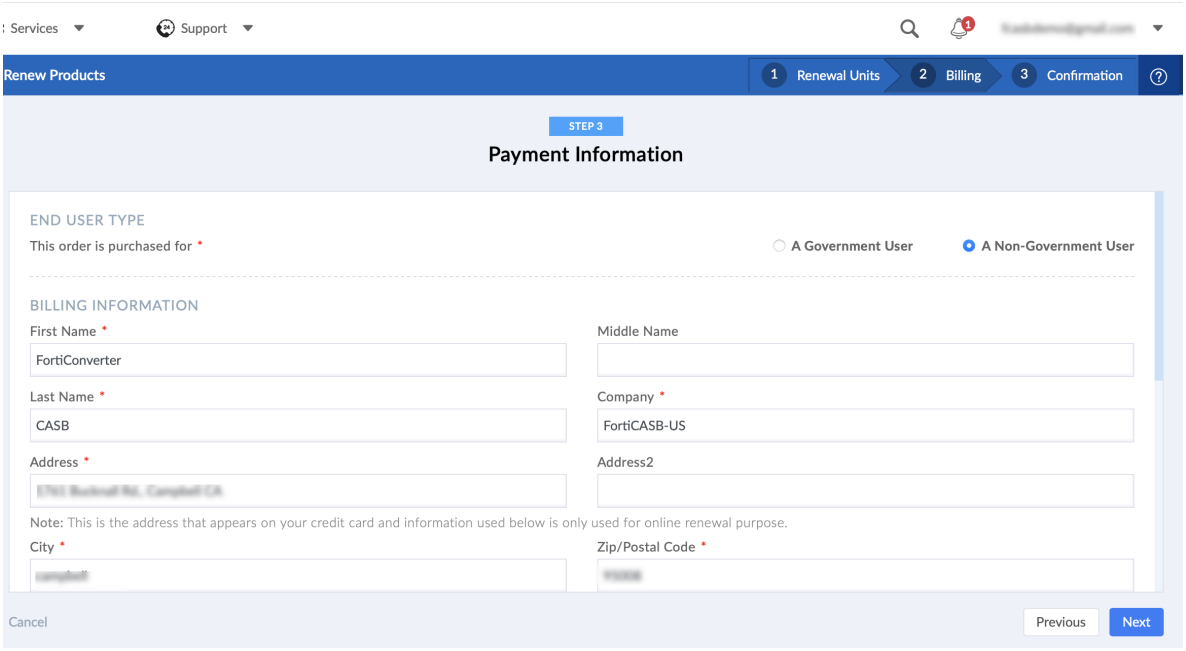
4. Locate the FGT/FWF device which you want to migrate configurations to and click the "**Shopping Cart**" icon.
   If you need to purchase this service for multiple FGT/FWF devices, please select the devices and click the "**Purchase License**" icon on top of the device table.
   You will be re-directed to Fortinet Support Portal - https://support.fortinet.com/.



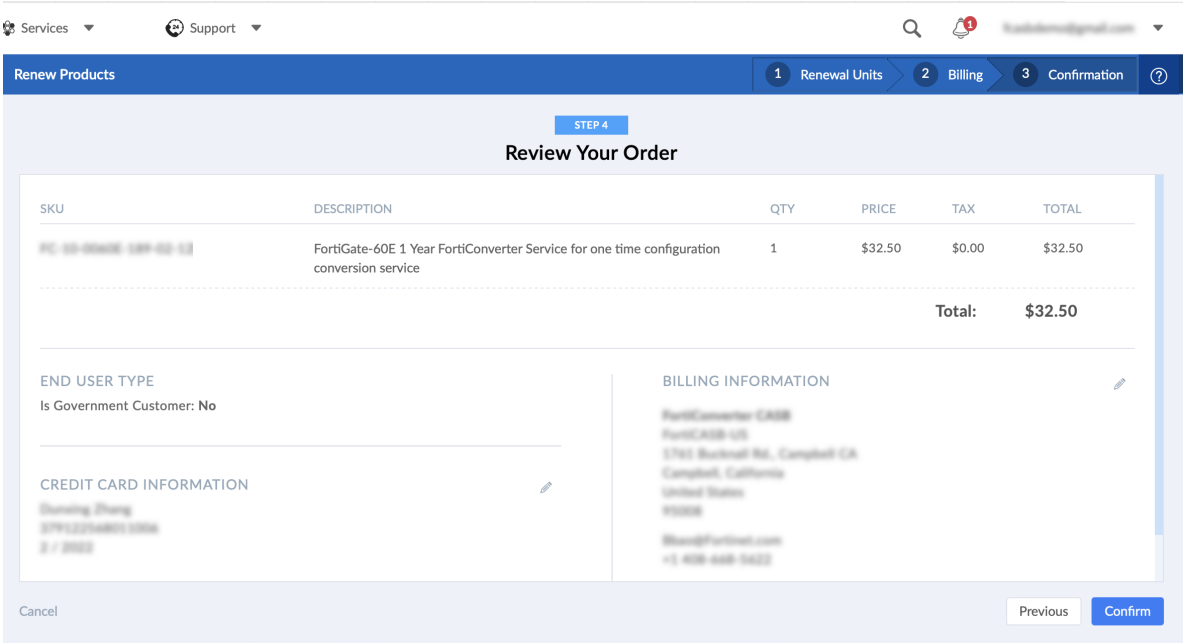
5. The FortiConverter Service SKU for the selected FGT device(s) will be automatically added to your shopping cart.



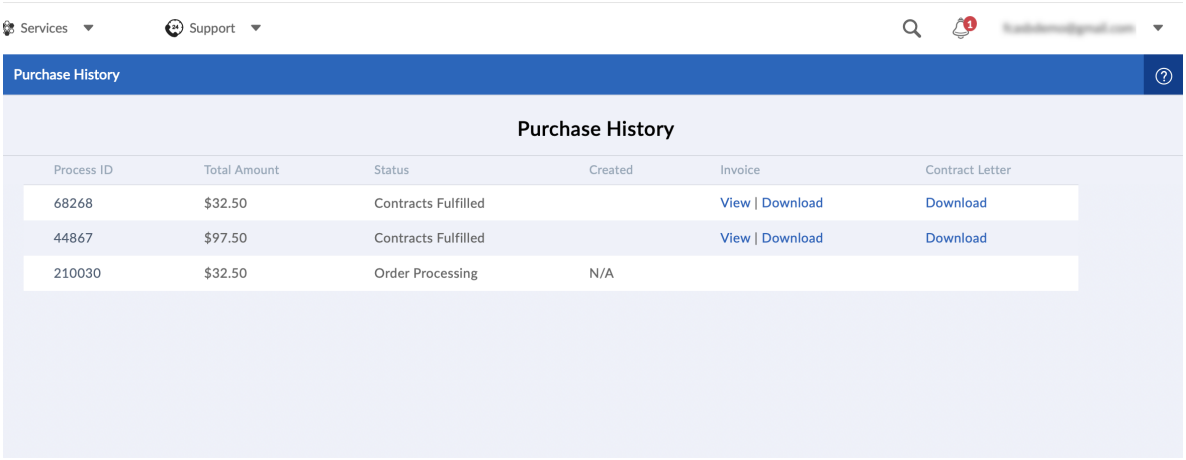
6. Follow the online purchase wizard to complete the purchase. Input billing information and click **Next** to proceed.



7. Review order details and click **Confirm** to place your order.



8. The status will be shown as "Order Processing" in Purchase History, it may take up to 48 hours to process. You will receive an email confirmation about your order. Once your order has been fulfilled, Fortinet will send you an email to update the latest order status.



Purchase Option 3 - Through Fortinet Support Portal

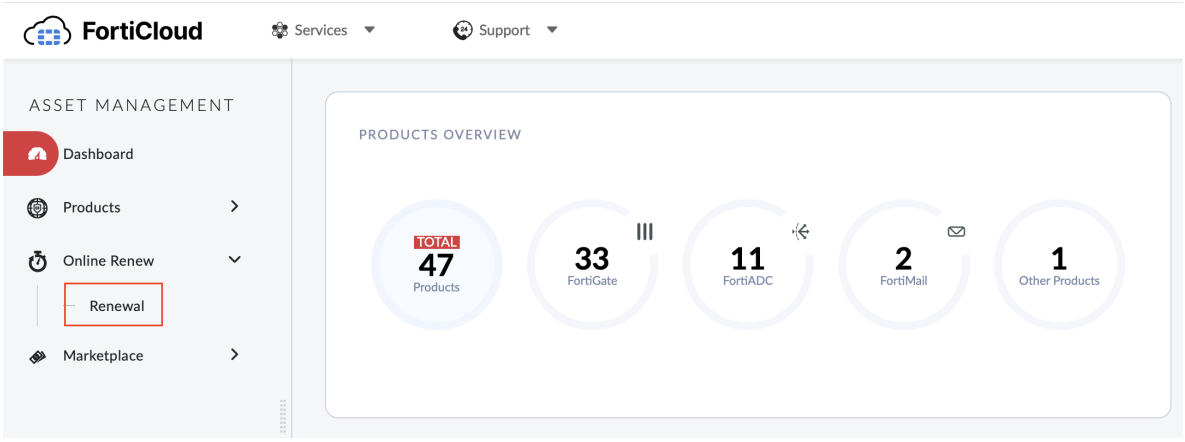
Order online through Fortinet Support Portal is only available for **North America** users.

Prerequisite

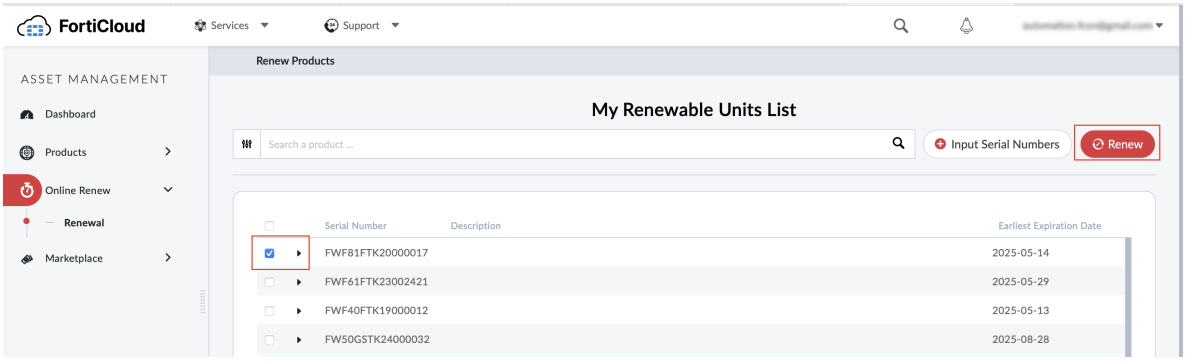
FGT/FWF device(s) are already registered with your FortiCare account. Fortinet only supports account that has less than **50** assets.

Steps to order online through Fortinet Support Portal

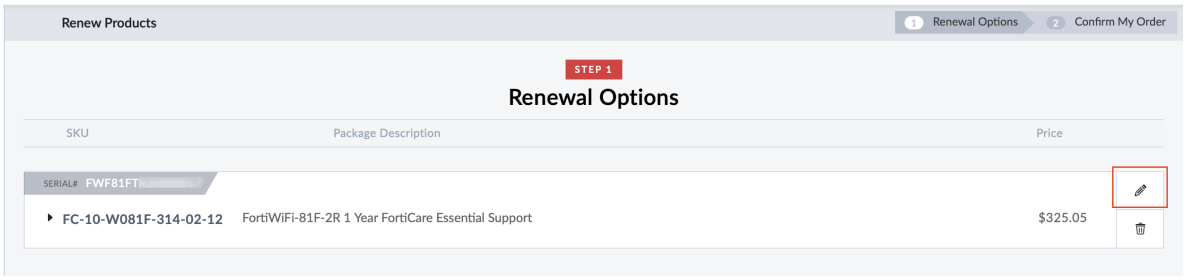
1. Go to **Fortinet Support Portal** - https://support.fortinet.com/.
2. Log in with your Fortinet account credentials.
3. In navigation menu, go to **Online Renew > Renewal**.



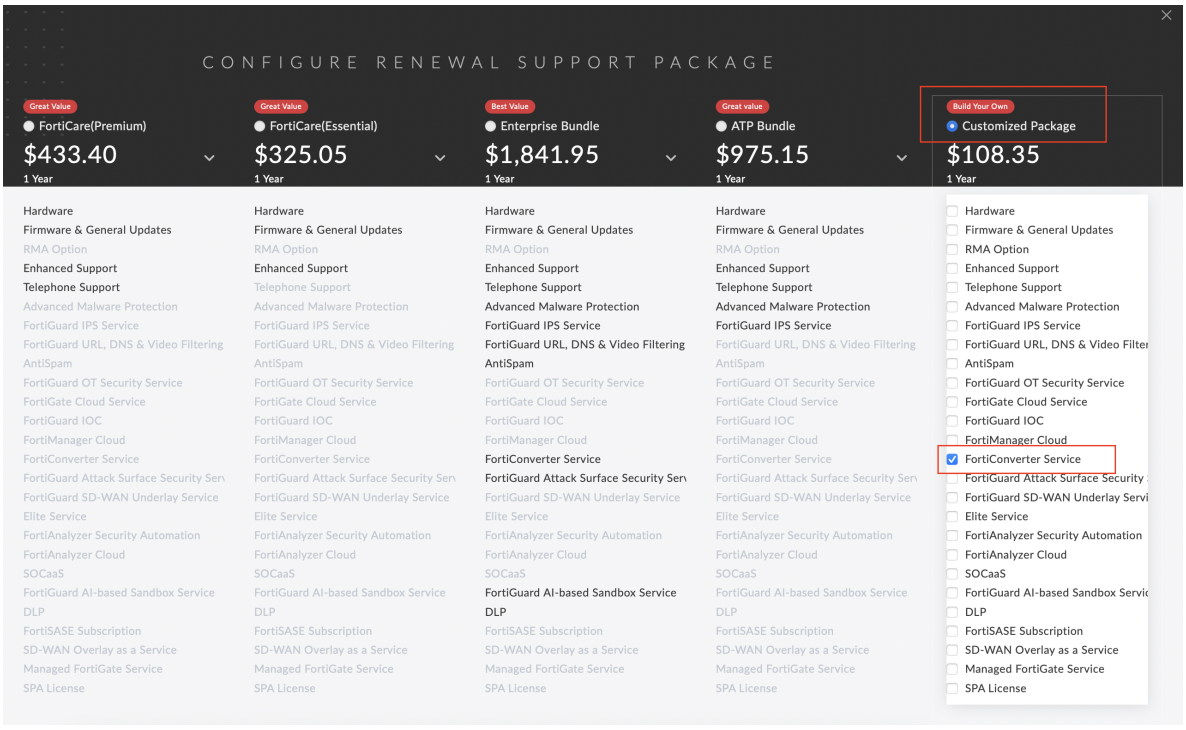
4. In **My Renewable Units List**, select the FGT/FWF device for which you want to migrate configurations to, then click **Renew**.



5. In **Renewal Options** page, click on the edit button.



6. In **Configure Renewal Support Package** page, select **Customized Package**, and check **FortiConverter Service**.



7. Click **Confirm** to continue.
8. Fill in your payment method and click **Submit Order**.

FortiConverter Service Contract Registration

Introduction

Notice: This section is only applicable for the purchase through a local sales representative, i.e. License Purchase Options on page 17

If you purchased through online order from Fortinet, i.e. License Purchase Options on page 17, please skip this section and go to Create FortiConverter Service Ticket on page 32. The FGT/FWF device(s) are already submitted through the purchase wizard when your order is processed, and the service contract would automatically register the designated FGT/FWF device(s).

You can always check your FortiConverter Service entitlement in FGT/FWF entitlement table, please refer to - Check FGT/FWF Device(s) Service Entitlement on page 30.

Prerequisite

Before starting contract registration, you should have received an email with PDF attachment(s) with your **Contract Registration Code** from your local sales representative. The file contents look like below.

PLEASE REMEMBER TO REGISTER YOUR CONTRACT REGISTRATION CODE

Service Entitlement Summary

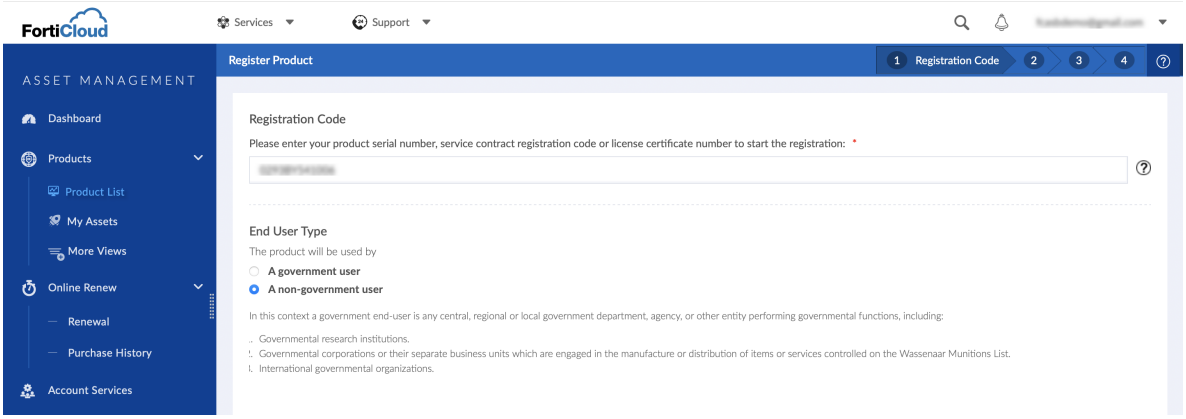
Date	:	August 31, 2021
Purchase Order Number	:	[illegible]
Contract Registration Code	:	[illegible]

Support / Maintenance / Subscription Services Included

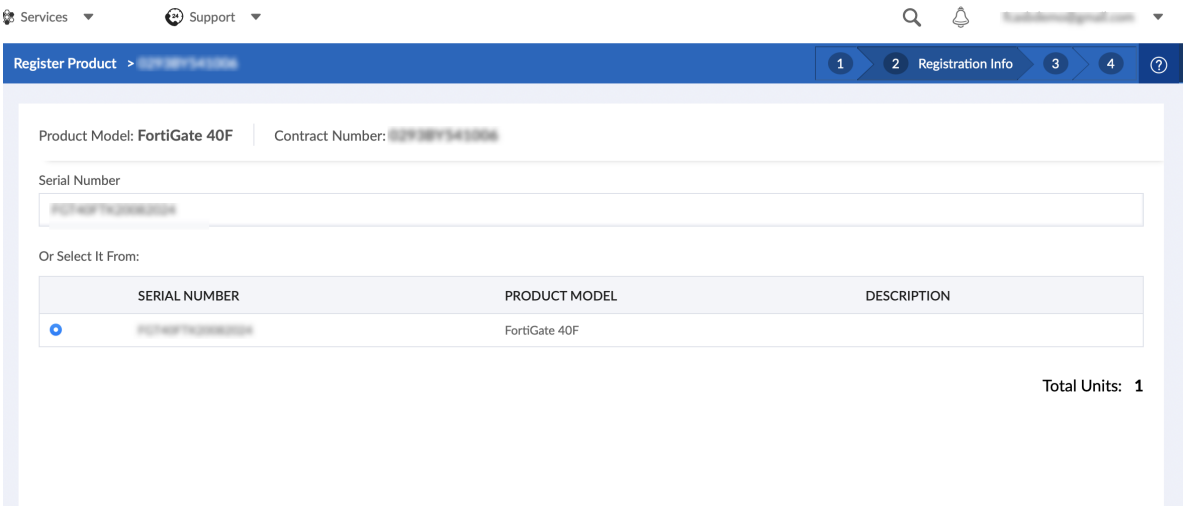
Qty	Part Number	Description
1	FC-10-0040F-189-02-12	366Days coverage for FortiGate 40F include: FortiConverter Service 8x5

Steps to register FortiConverter Service Contract:

1. Log in to Fortinet Support Portal to register your newly purchased service contract - https://support.fortinet.com/asset/#/regs/entry
   The registration page can also be accessed through **Products > Product List** page, locate "**Register More**" button from the top-right corner.
2. Copy and paste your Product Registration Code and click **Next**.



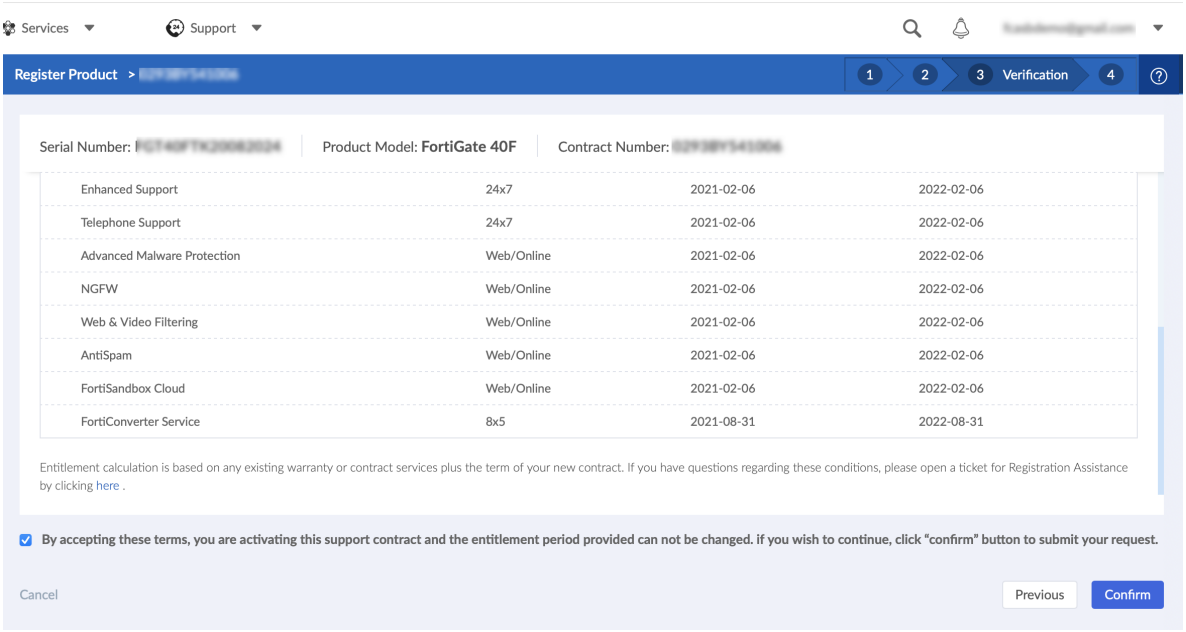
3. **Select** the appropriate FGT/FWF device to register with the FortiConverter Service contract, and click **Next**.



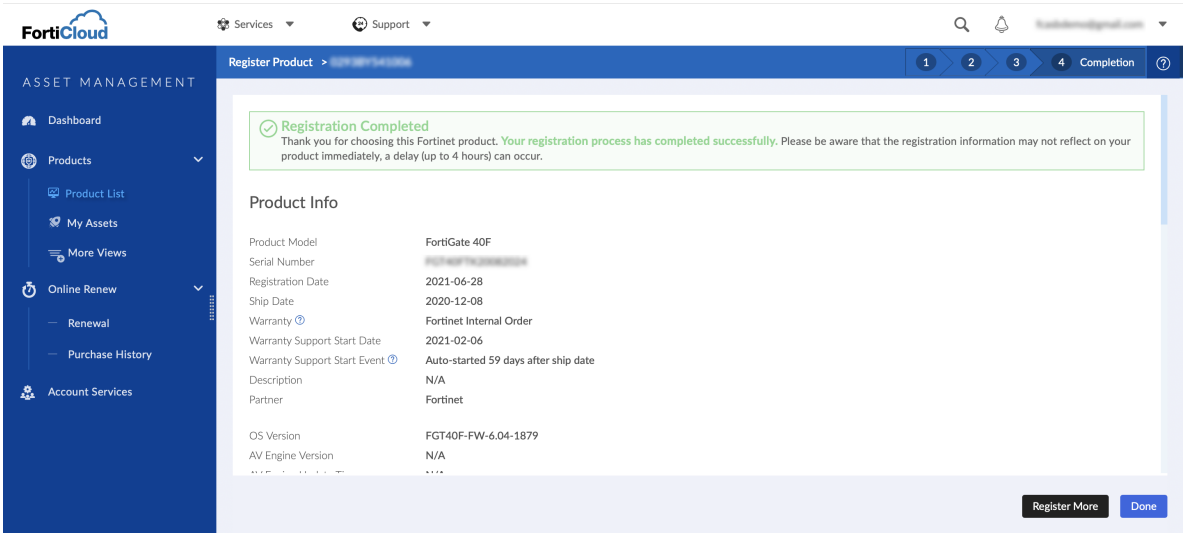
Note: that the service contract you purchased is based on a specific FGT/FWF model.

For example, you cannot register a 50E's service contract with a 60F device.

4. Verify the product entitlement summary and click **Confirm**.



5. In the last page, you shall see "**Registration Completed**" sign to mark the completion of registering your service contract with FortiConverter Service.



Congratulations! Now your FGT/FWF device has the FortiConverter service entitlement.

You can now check the current status of the product entitlement. Please refer to - Check FGT/FWF Device(s) Service Entitlement on page 30.

FortiConverter Service Portal Access

FortiConverter Service Portal can be accessed by two types of users:

1. Regular account user with email address as the username.
2. **IAM user** created by the account owner.

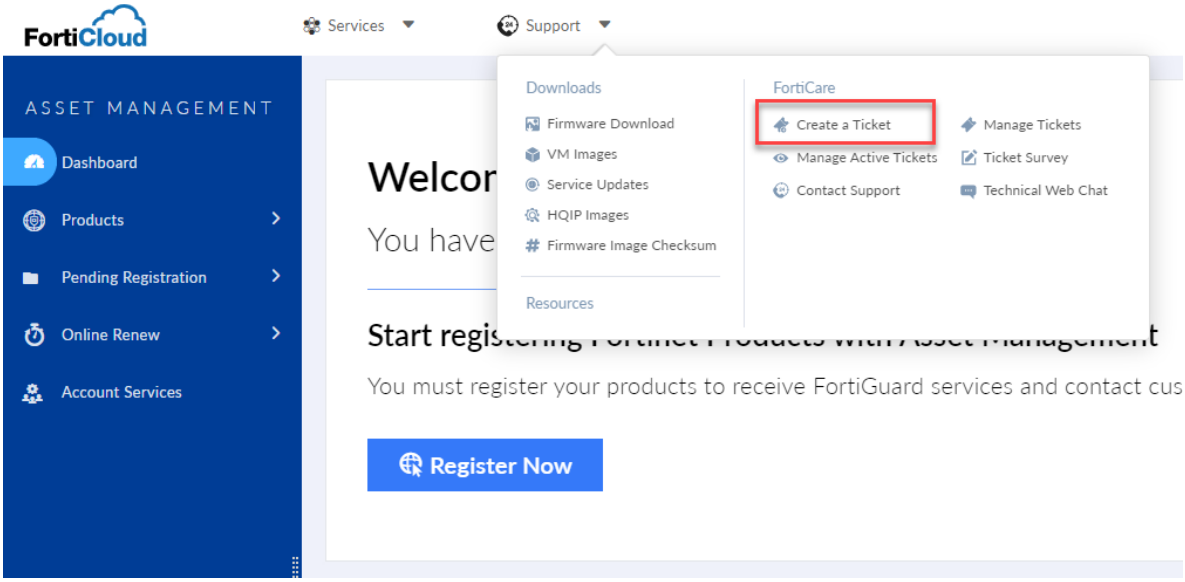
For IAM user creation and access, please see **Grant FortiConverter Service Access to IAM user on page 28**.

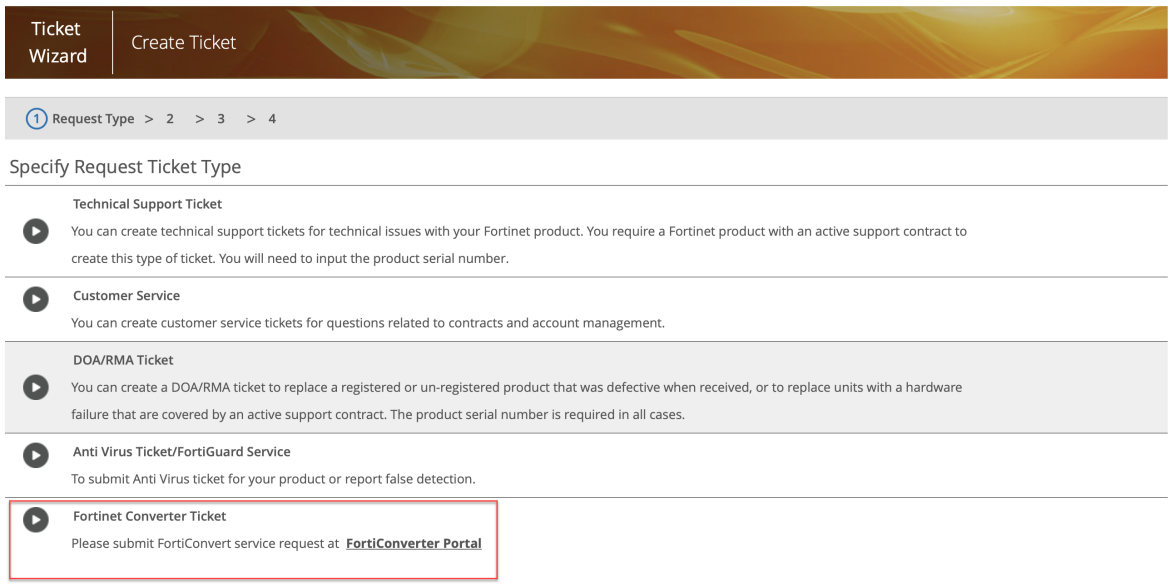
There are three ways to access FortiConverter Service Portal:

1. **Access through Fortinet Support Portal's ticket wizard. on page 26**
2. **Access through FortiConverter Service Portal - FortiCloud Application Menu on page 27**
3. **Access FortiConverter Service Portal through the site URL on page 28**

Access through Fortinet Support Portal's ticket wizard.

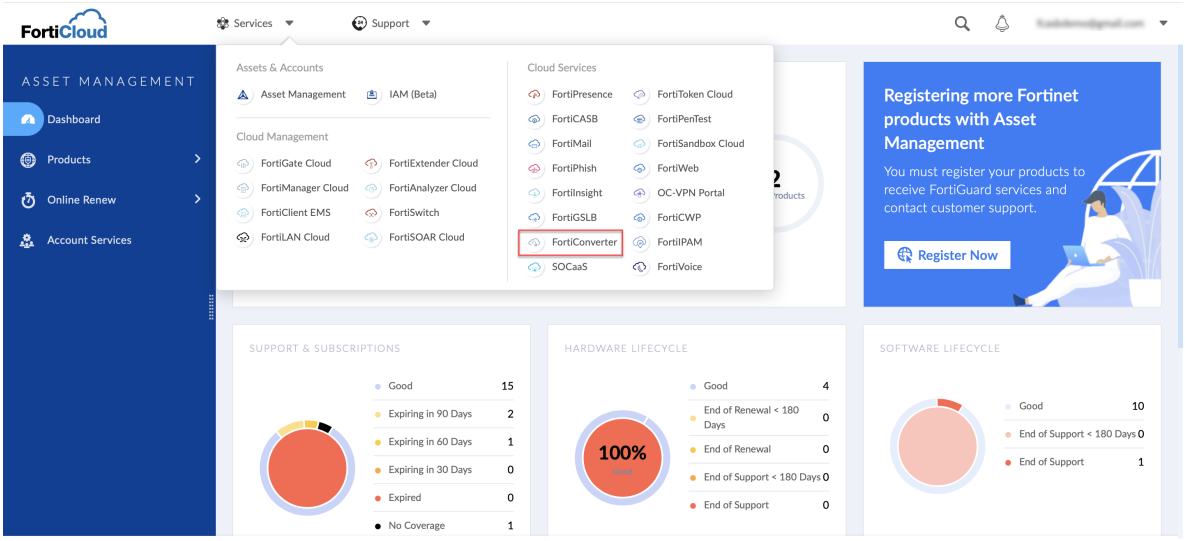
1. Log into Fortinet Support Portal - https://support.fortinet.com/
2. Click **Support > Create a Ticket** from the top menu, click the hyperlink **FortiConverter Portal** to access FortiConverter Service.





Access through FortiConverter Service Portal - FortiCloud Application Menu

1. Log into Fortinet Support Portal - https://support.fortinet.com/
2. Click on **Services** drop down menu from the top-left corner and select **FortiConverter** Cloud Service.



Access FortiConverter Service Portal through the site URL

FortiConverter Service Portal URL:

https://service.forticonverter.com/

Grant FortiConverter Service Access to IAM user

There are two steps to grant FortiConverter Service Access to IAM user:

1. Create an new IAM user.
2. Generate a password reset link and share with it with the selected IAM user.

For details and steps to create and configure IAM user, please see Add IAM User in FortiCloud Account Services documentation.

Locate FGT/FWF Device(s) on FortiConverter Service

The FGT/FWF device(s) can be found in **FortiConverter Service Portal** under **FortiGate Entitled Device List**.

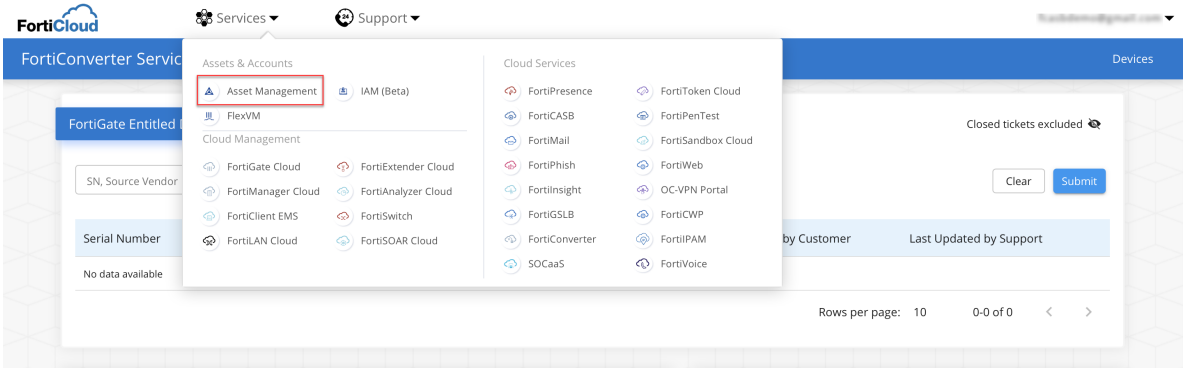
If you cannot find the FGT/FWF device(s) from the FortiConverter Service Portal, please visit the **Fortinet Support Portal** to check if the specific FGT/FWF device(s) are registered with Fortinet. See Steps to Check for your FGT/FWF device(s) in FortiCare on page 29

Note 1: Please allow 3-5 hours right after your initial device registration with Fortinet to allow information exchange and synchronization between our systems. You can contact **Fortinet TAC** if you encounter any difficulty registering your device(s) with Fortinet, or not being able to see the registered device(s) on your FortiCloud account after 24 hours.

Note 2: Fortinet partner(s) accounts do not have privileges to access their managing accounts' cloud portals. Please notify the customers whom the FGT/FWF device(s) are registered with to contact Fortinet customer support directly to raise service ticket(s) with their FortiCloud accounts.

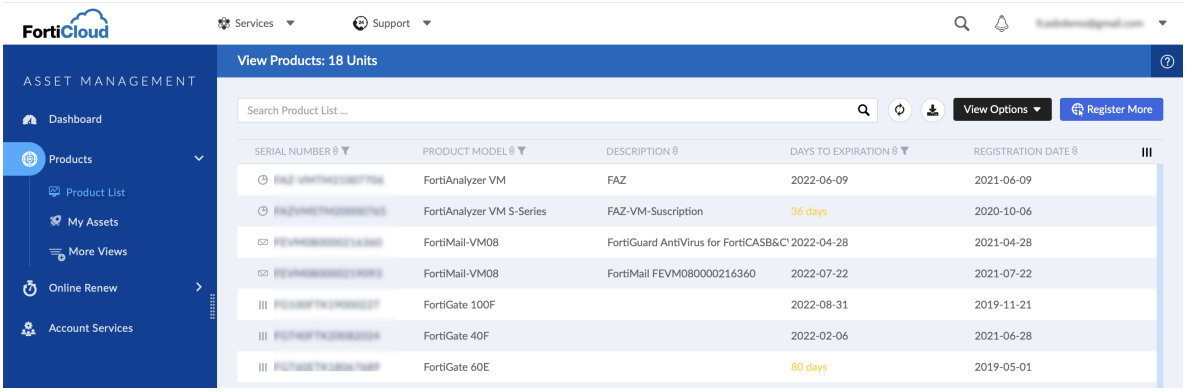
Steps to Check for your FGT/FWF device(s) in FortiCare

1. Click on the **Services** drop down menu and select the **Asset Management** icon.

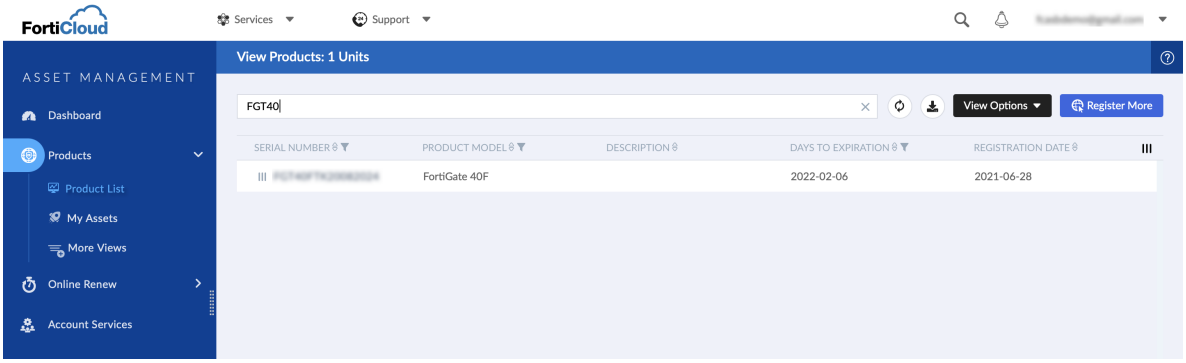


You will be re-directed to **Fortinet Support Portal** - https://support.fortinet.com/.

2. Click **Products > Product List** to see all your registered Fortinet products.



3. You can search your FGT/FWF device(s) from the registered products list by typing in the model number.

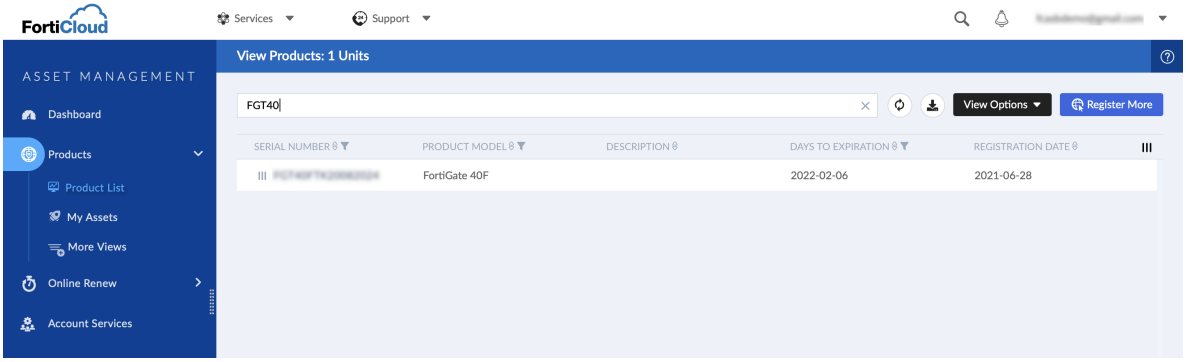


Check FGT/FWF Device(s) Service Entitlement

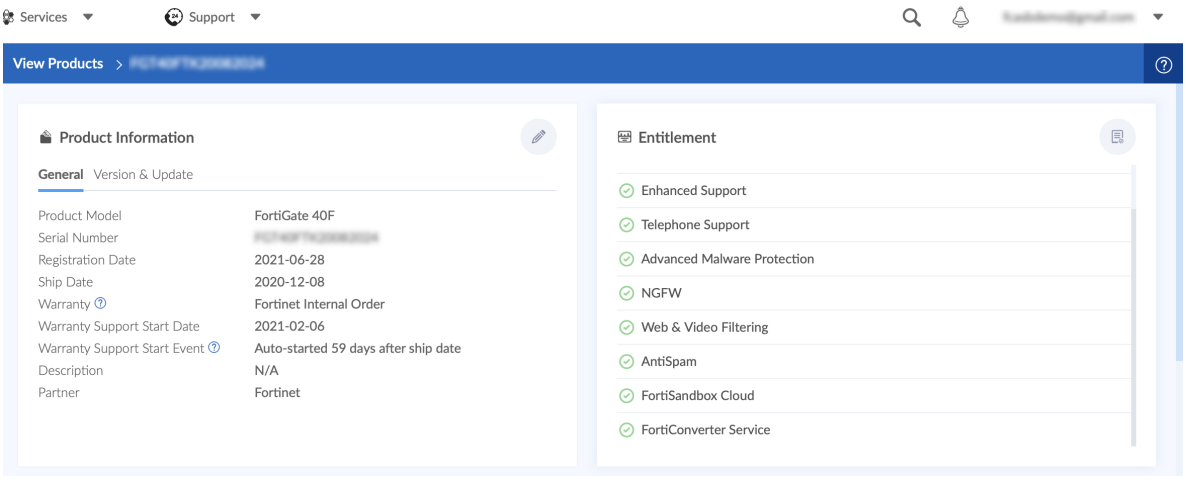
If you are not sure whether your FGT/FWF device(s) have FortiConverter Service entitlement, you can check through **Fortinet Support Portal**. Please note that FortiConverter Service is a one-time conversion service valid for 12 months period.

Steps to check service entitlement on FGT/FWF device(s)

1. Log into **Fortinet Support Portal** - https://support.fortinet.com.
2. Go to **Products > Product List** from the navigation menu to enter **Product List** page.
3. Enter the FGT/FWF product serial number or model number.



4. Click on the **Serial Number** to enter the **Product Information** page.
5. On the right, there is **Entitlement** information, look for the support coverage of the FortiConverter Service. Please note that FortiConverter Service is a one-time conversion service valid within the 12 months period from the time of purchase.



FortiConverter Service Tickets

Create FortiConverter Service Ticket

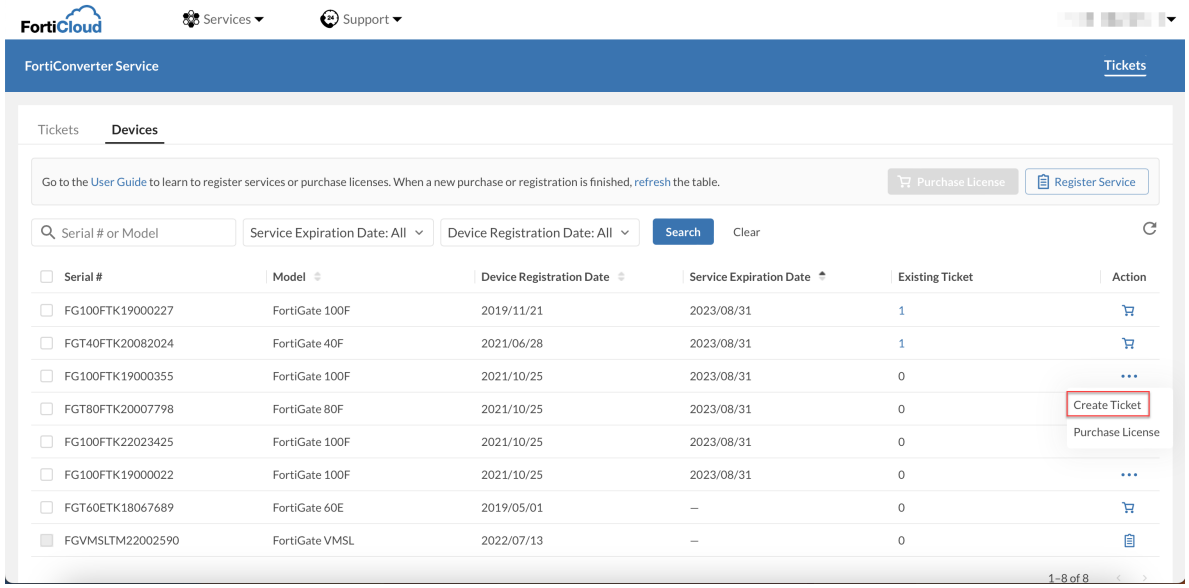
After your verify that your FGT/FWF device(s) have FortiConverter Service entitlement, you can create conversion service ticket to process configuration migration for your registered devices.

If this is your first time accessing FortiConverter Service Portal, please see FortiConverter Service Portal Access on page 26.

If you can access the FortiConverter Service Portal, please continue below to submit a conversion ticket.

Conversion Service Ticket Wizard

1. Log in to **FortiConverter Service Portal** with your **FortiCloud account** user name and password - https://service.forticonverter.com/
2. In **Devices** tab, look for your "FGT/FWF" devices.
   If the device has FortiConverter Service Entitlement, **Create Ticket** button will be available for the device on the page.

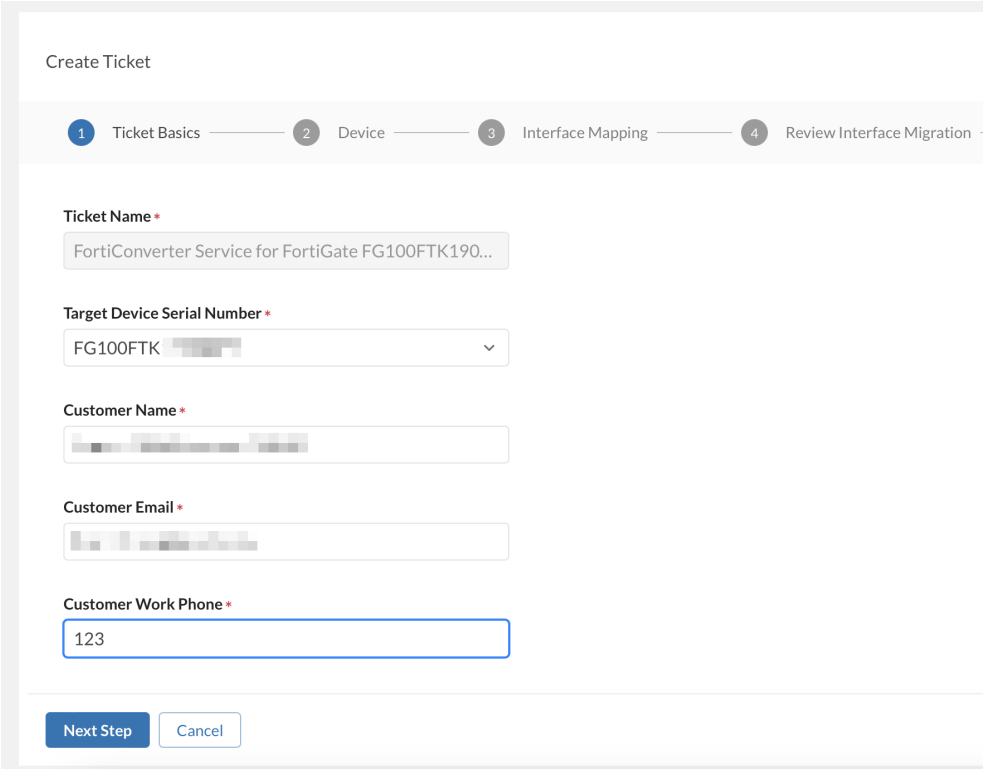


Click **Create Ticket** to enter ticket creation wizard.

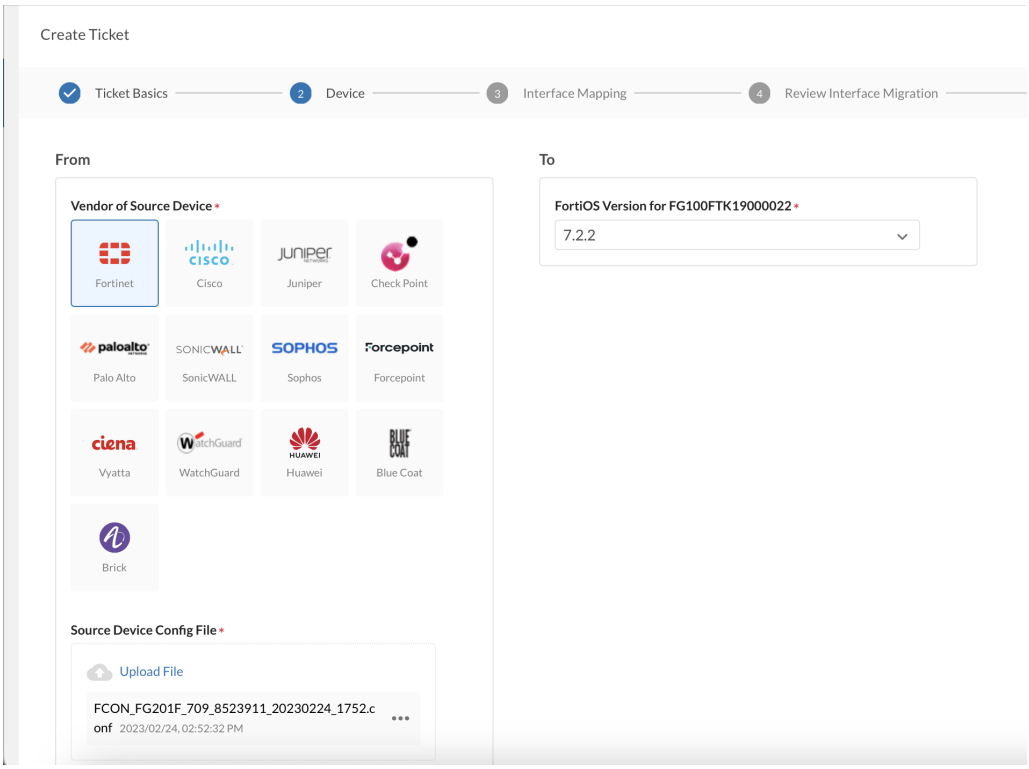
This is a one-time only conversion service, you can only create one service ticket within 12 months of your service contract registration date.

3. Please review and update the pre-filled customer email address and name fields. Fill the **Customer Work Phone** field, and click **Next Step**.

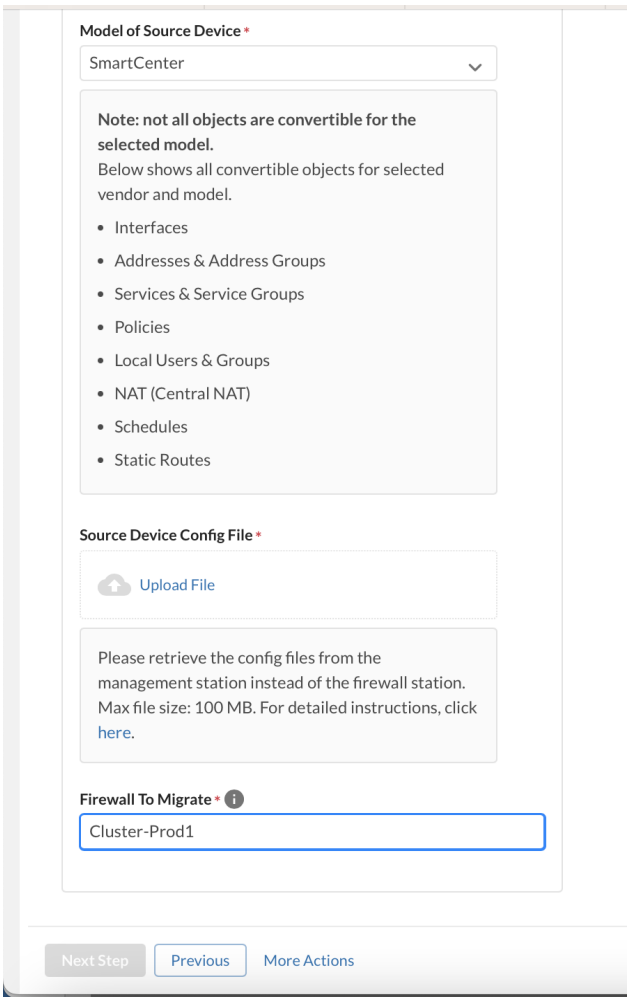
   Note: You can also add more email recipients and phone numbers, please input each one after another separated by space. Email notification covers all ticket change status and new posts/comments updated by Fortinet service team staff.



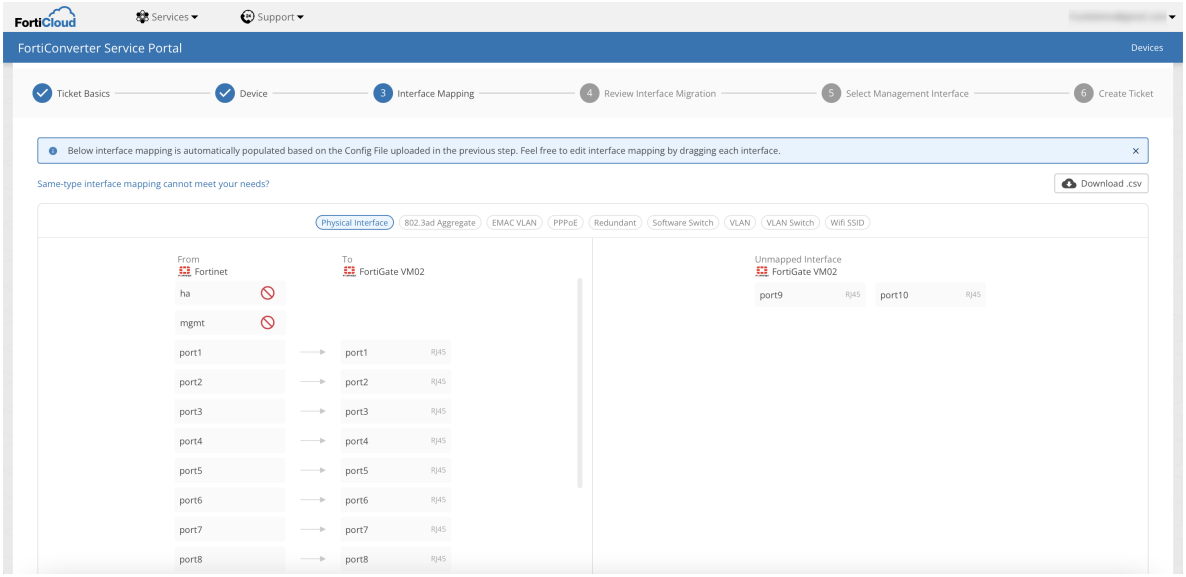
4. From the left panel, select source device vendor and model, click **browse** to upload source configuration file(s) from your local PC.
   Click FortiOS Version for <SN> drop down menu to select the target platform FortiOS version.



Note: **Check Point** conversion requires firewall or firewall cluster name, this can avoid back and forth confirmation during the ticket processing.

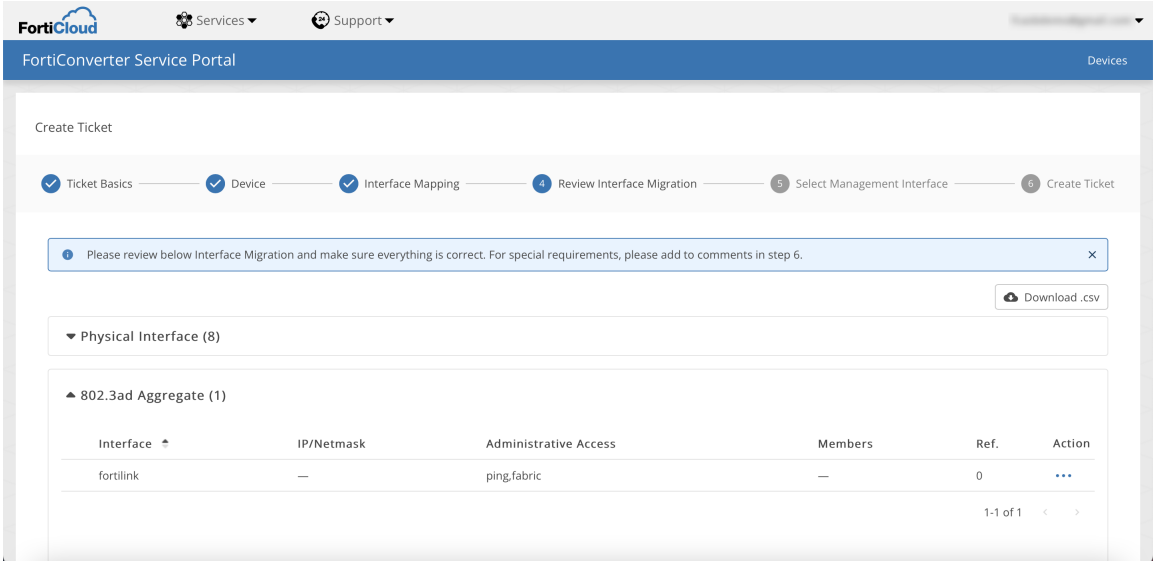


5. Drag and drop the physical interface from right to left. If some of the interfaces are no longer in-use, you can consider marking them as  (Do not migrate).
Various interface types extracted from the source config file will be displayed, such as vlan, tunnel, aggregate, redundant, and switch interfaces.

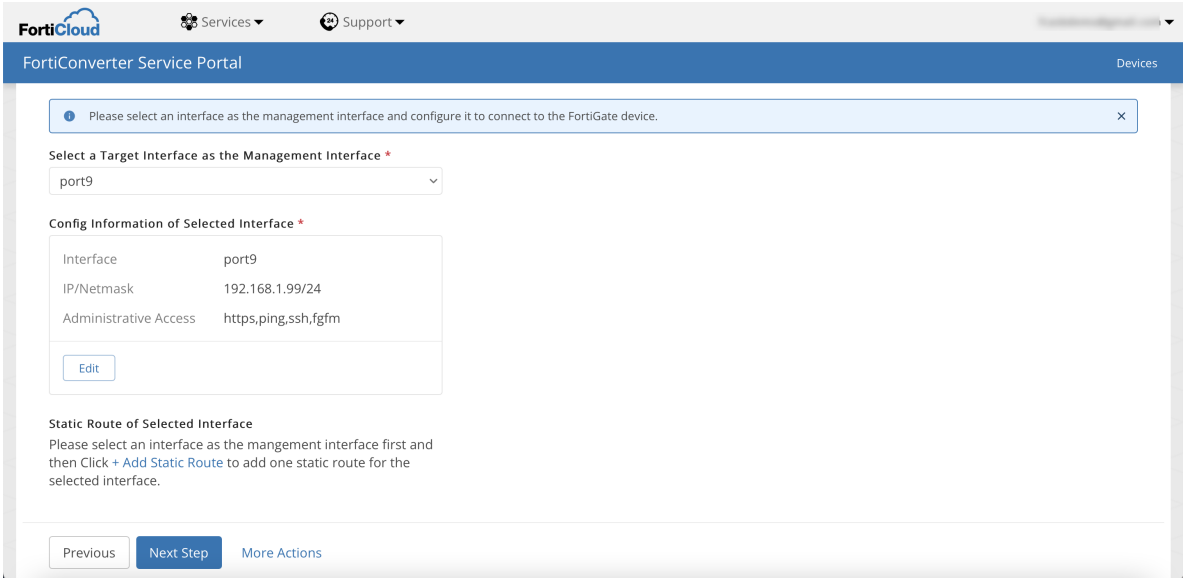


6. **Review Interface Migration**: This page displays how the interfaces look like after the configuration migration to the target FGT/FWF device.

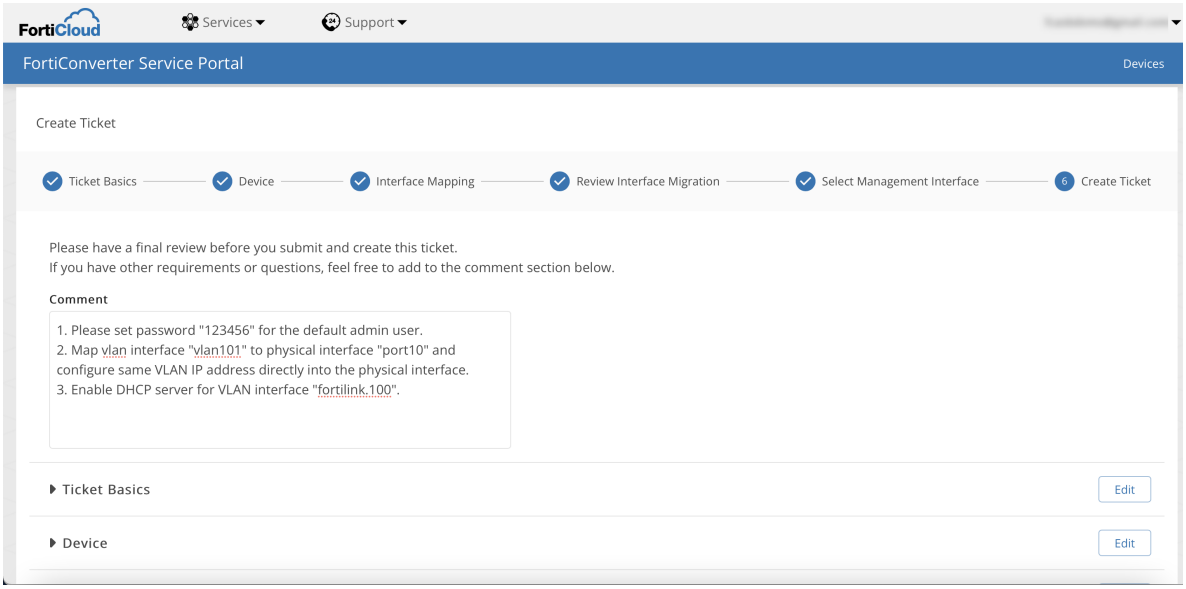
   Please update interface settings by clicking the button.



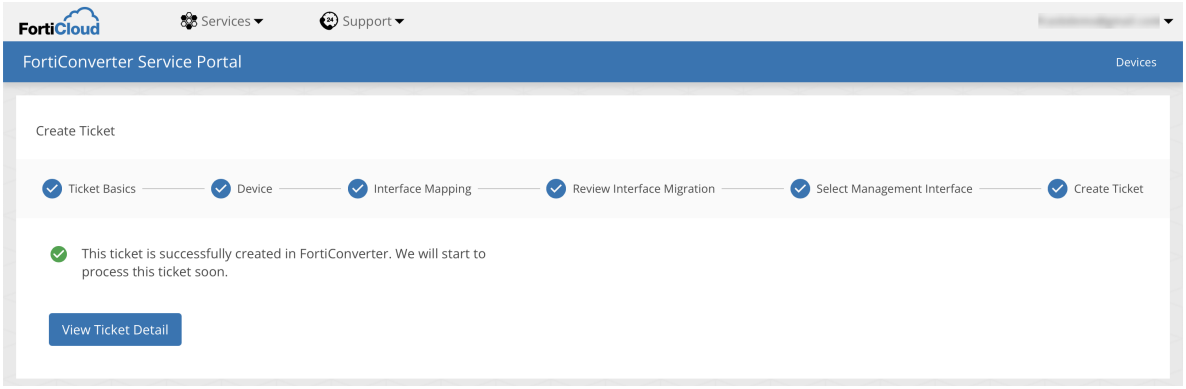
7. Select target FortiGate's management interface, configure interface IP address, administrative access and an optional static route, and click **Next Step**.



8. Add special migration instructions if necessary (optional). Review the service ticket summary and click **Create Ticket**.



9. The last page will show that you have created the ticket successfully, click **View Ticket Detail** to enter the ticket details page.



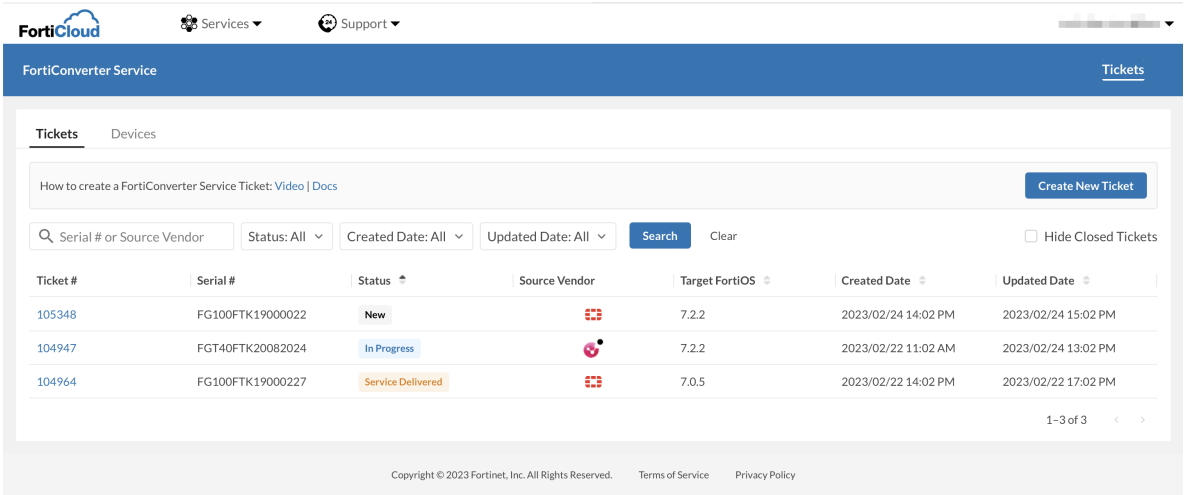
After service ticket is created, please refer to Review FortiConverter Service Ticket on page 38

Review FortiConverter Service Ticket

After submitting a FortiConverter service ticket, you may review the ticket status from the **FortiConverter Service Portal** home page.

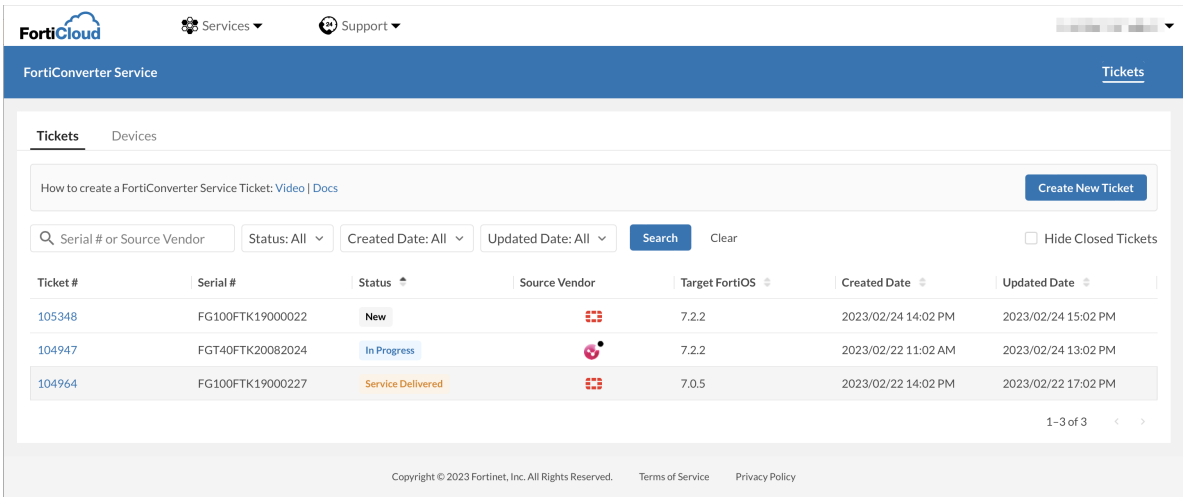
Steps to review FortiConverter Service Ticket:

1. Log in to **FortiConverter Service Portal** with your **FortiCloud account** user name and password - https://service.forticonverter.com/
2. From the **Tickets** tab, you can review the status of the conversion tickets submitted.

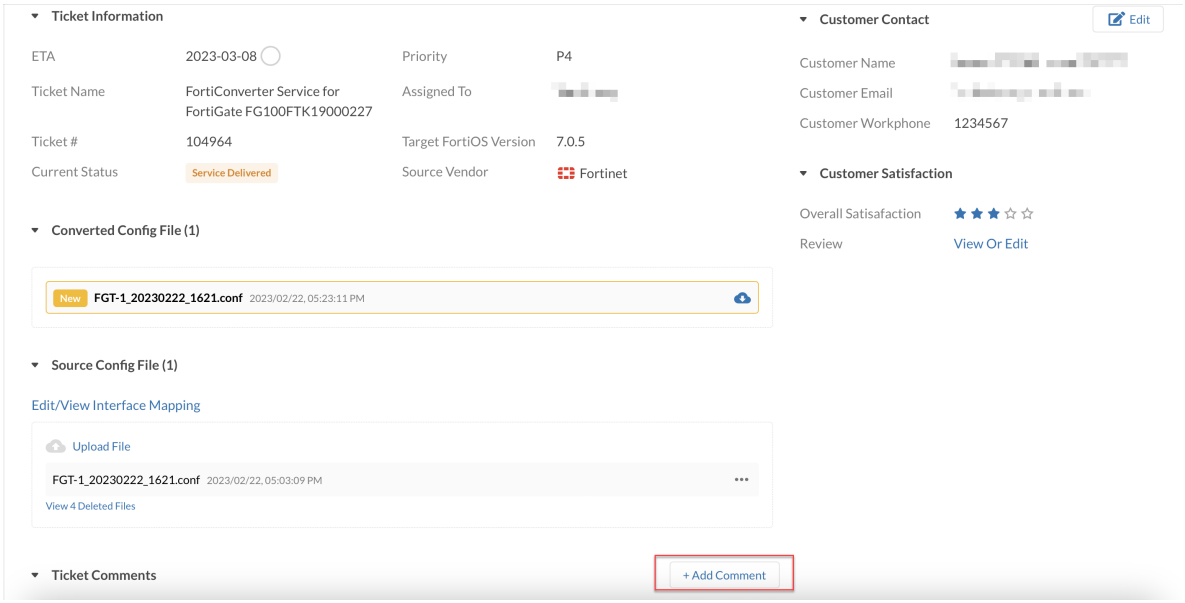


- The **Draft** ticket status shows the ticket has been initiated, but has not yet been submitted to the system. Service team will not process **Draft** ticket.
- The **New** ticket status shows the ticket has been created, but has not yet been assigned to any service team staff yet.

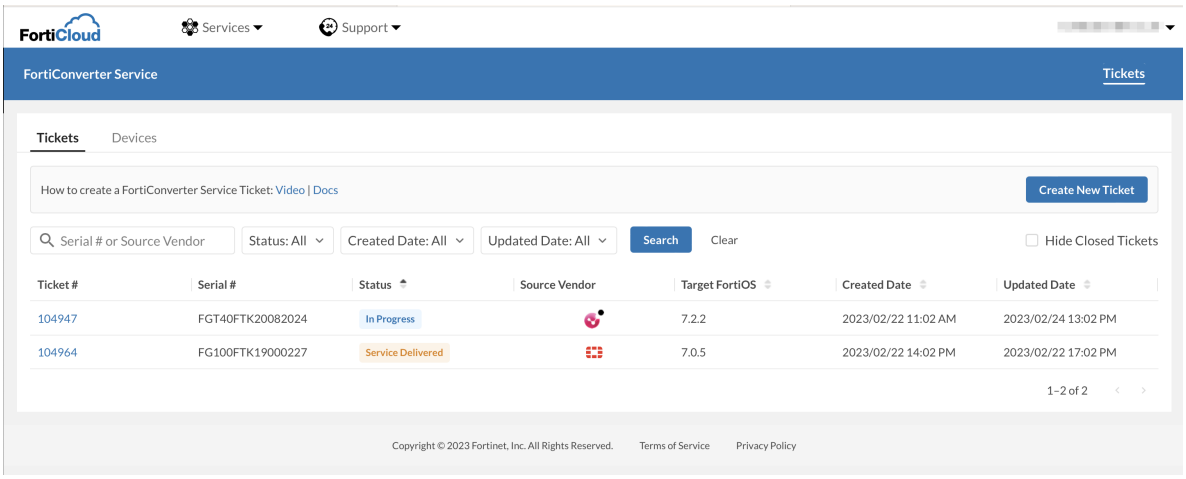
3. Click on each ticket to be redirected to the ticket details page.



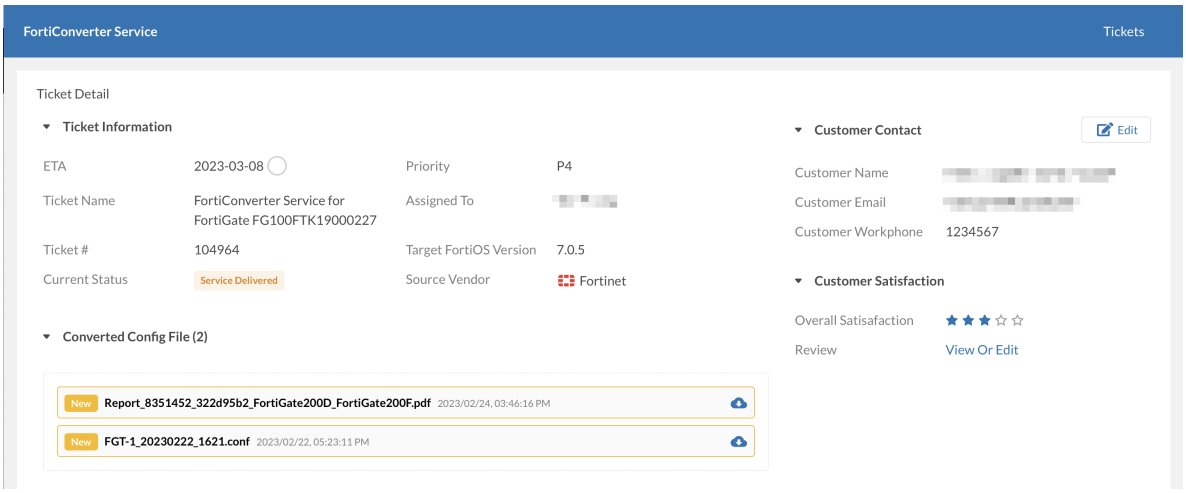
4. Click the **Add Comment** button to post a message to communicate with FortiConverter Service Team.



5. When the ticket status has changed to "**Service Delivered**", you can download the converted configuration file(s) inside the ticket details. Converted configuration file and report links can be found from the dedicated **Converted Configuration File** area.



Converted configuration file and report links can be found from the dedicated **Converted Configuration File** area

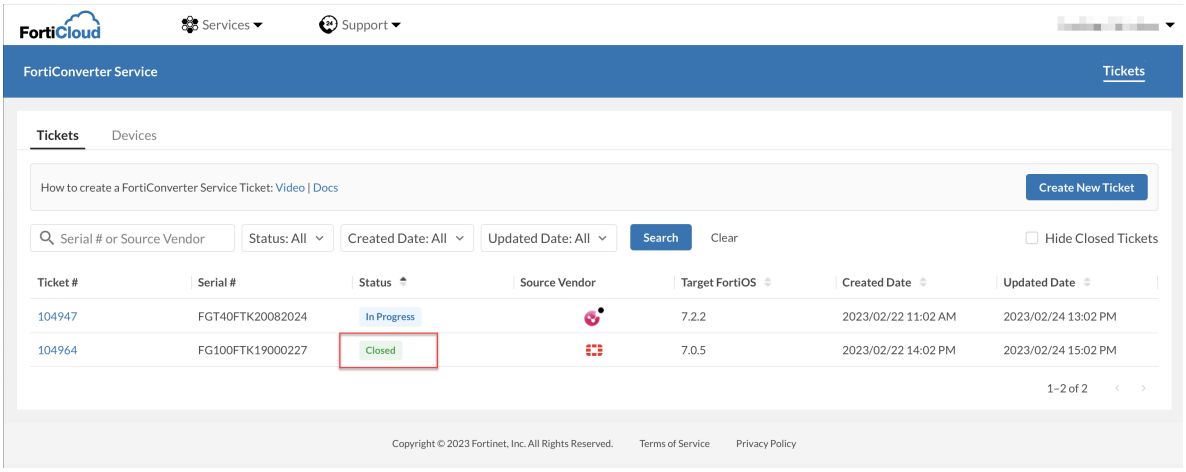


Reopen a FortiConverter Service Ticket

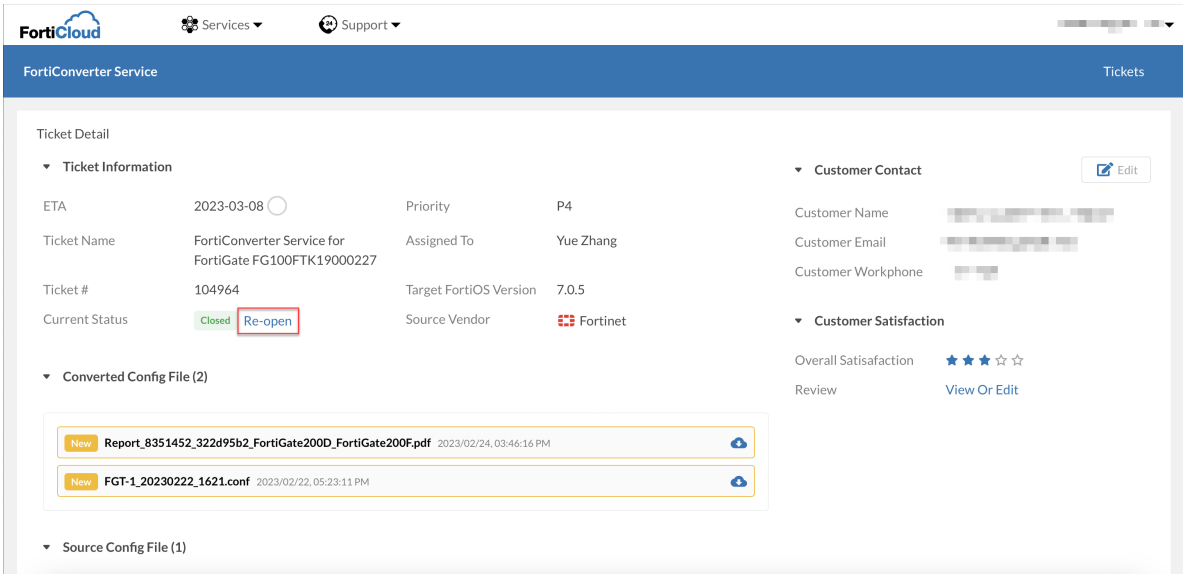
After the ticket status is changed to "**Service Delivered**", if there FortiConverter Service team could not get any further feedback from you after 14 days, the service ticket status will automatically changed to "**Closed**". You can reopen the "Closed" ticket when you get a chance to work on it again as long as the service contract is not expired.

Steps to reopen a FortiConverter Service ticket:

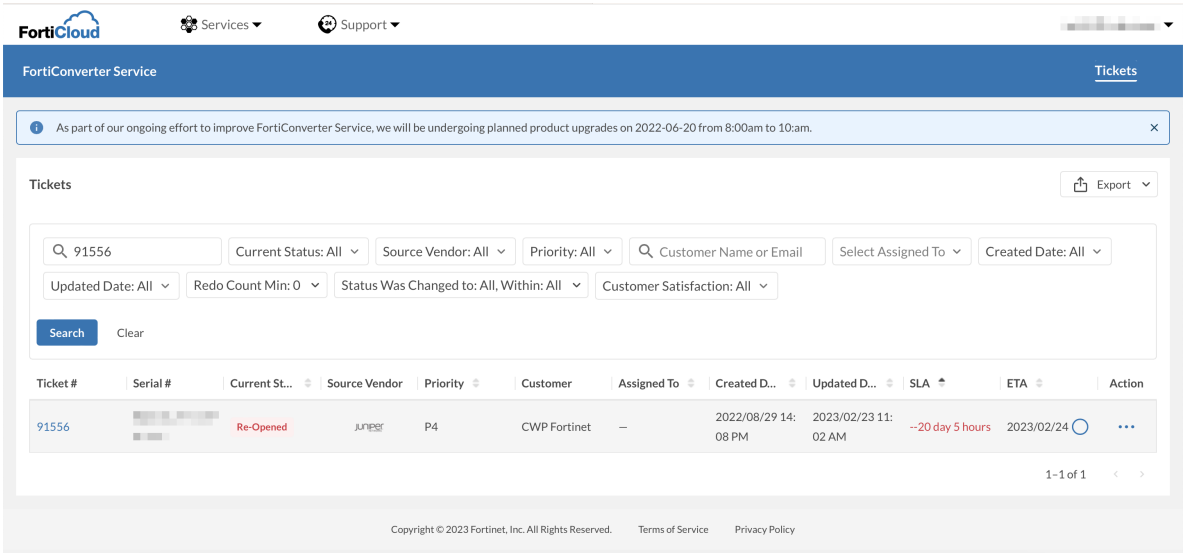
1. Locate the **Closed** ticket from the ticket table.



2. Click the desired ticket to enter ticket details page and then click **Re-open** button.



3. Go back to the service ticket page to track the reopened service ticket.



Configuration Migration

Migrate FortiToken on page 43

Import Certificate on page 44

Policy NAT vs Central NAT mode on page 45

Migrate FortiToken

FortiToken cannot be migrated by FortiConverter Service because it needs to be done on user's new device. Please follow the steps below to migrate and activate your FortiToken configs.

To import the FortiToken Hardware into your FortiGate:

1. Export the FortiToken config from the old device and import the config to the new device. The config can be output in the CLI console by the commands:
   `"config user fortitoken" -> "show".`
2. Remove the FortiTokens from the old device, or block the access of the old device to FortiGuard. This would prevent the old device from requesting the activation of the tokens after they are reset.
3. Reset the activation flags for the tokens through FortiCare.
   Create a FortiCare ticket on the Support Portal https://support.fortinet.com/, and ask TAC to help you reset the activation flags of the FortiTokens. The message should include the SN of the old device and the FortiTokens.
   The TAC would reset the activation flag and inform you after it is completed.
4. Connect the new device to FortiGuard, and the tokens would be activated.

To import the FortiToken into your FortiGate:

1. Transfer the FortiToken license from the old device SN to the new device SN through FortiCare.
   Create a FortiCare ticket on the Support Portal https://support.fortinet.com/, and ask TAC to help you migrate the FortiTokens from the old device to the new device. The message should include the SN of the old device, the new device, and the FortiTokens.
   The TAC would migrate the token and inform you after the migration is completed.

2. Activate the FortiToken on the new device.
   Go to the page **User & Authentication > FortiTokens** on the new device. Click **Create New** and input the activation code of the FortiTokens. The tokens would be imported into the new device.

3. Re-provision every user, which means to bind a new token to user's app again.
   Configure users on the new device, send the activation code through e-mails or SMS to do re-provision for all users, and the migration is completed. The seeds on the old device cannot be restored to the new device. This is designed to prevent possible fraudulent attacks.

Import Certificate

Background

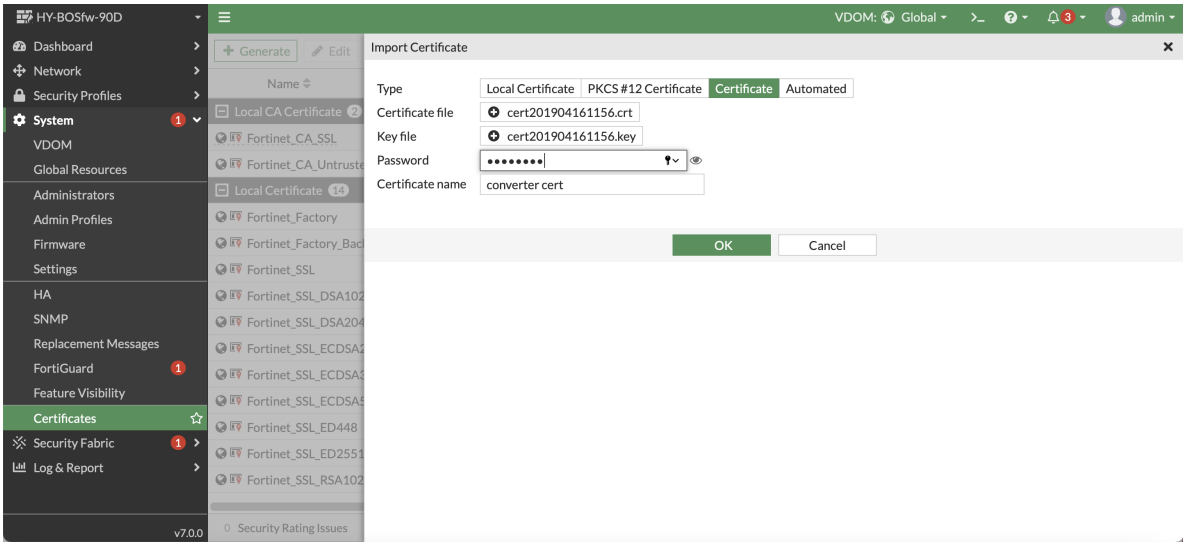
Certificates can be migrated and imported in most cases, but with a few exceptions. If a certificate cannot be imported, it will be replaced by the default certificate in the migrated config. When this happens, the certificate will need to be imported manually.

Wait until the migrated config is restored on the device, then follow the steps below to import the certificate manually:

Steps to import the signed certificate into your FortiGate:

Before importing the certificate, please prepare either your certificate (**.crt**) and private key (**.key**), or the PKCS#12 certificate (**.pfx**).

1. Log in to your FortiGate unit and go to **System > Certificates**.
   If there's no Certificates, please click **Feature Visibility** and enable the **Certificates**.
2. Click **Import > Local Certificate**.
3. Upload the local certificate file and private key, then click **OK**.
   If you use a password to encrypt the certificate file, please fill the password as well.



4. The certificate will be added and the status of the certificate will change from *PENDING* to *OK*.

FortiGate provides the capability to download the certificate. However, for security reasons, the private key encrypted in FortiGate cannot be accessed. To successfully restore the private key, you need to find the matched origin key to import the certificate to another FortiGate device.

Policy NAT vs Central NAT mode

There are 2 NAT modes in FortiGate: **policy NAT mode** and **central NAT mode**. Policy NAT mode requires NATs to be configured inside firewall policies, which is the default mode that FortiGate uses. Central NAT mode separates NATs and policies into 2 independent modules so policies do not reference NAT objects.

FortiConverter provides the option to control the NAT modes for the conversion of some 3rd party vendors, and the recommended mode is different depending on the vendor of the source configuration. **When the recommended mode of each vendor is selected, the NAT conversion is more straightforward.** It means that the NATs would be similar between the source and converted configuration. Hence, the number of policies and NAT objects do not change a lot, and it would be easier to review the conversion result.

In **Juniper SSG and Forcepoint Sidewinder**, NATs are configured inside firewall policies, which is similar to policy NAT mode. Therefore, **policy NAT mode is recommended**. WatchGuard allows NATs to be configured both inside policies and in an independent list at the same time. Currently, FortiConverter only converts it into the policy NAT mode.

In **Cisco, Check Point, Juniper SRX, Palo Alto, SonicWALL, Sophos, Huawei, and Forcepoint Stonesoft**, NATs and policies are configured separately. Therefore, **central NAT mode is recommended**. On the contrary, the number of policies may greatly increase after converting these vendors into the policy mode, because FortiConverter applies the “NAT merge” process to match the traffic of each NAT and each policy, and may create extra policies to perform the NAT behavior when the traffic overlaps. It is possible to get 2 or 3 times of policies after the NAT merge. For more details about NAT merge, please see the examples in **Check Point** and **Cisco**. **In order to prevent users from reviewing a much larger policy list, central NAT mode should be the first choice.**

However, in central NAT mode, FortiGate doesn’t allow dynamic NAT rules to translate a single internal address into different external addresses based on different services. For example, if there are 2 dynamic NATs in the source configuration, one translates 10.10.10.1 with HTTP into 20.10.10.1, and the other translates 10.10.10.1 with SMTP into 20.10.10.2, then there is no way to distinguish these NATs under central NAT mode. If there are many such dynamic NATs in the source configuration, please select policy mode instead.

The following table shows the difference between the 2 NAT modes:

	Policy NAT mode	Central NAT mode
Description	NATs are configured in policies.	NATs and policies are separated.
Related categories for dynamic NAT	config firewall ippool config firewall policy	config firewall ippool config firewall central-snat-map

	Policy NAT mode	Central NAT mode
Related categories for static NAT	config firewall vip config firewall policy	config firewall vip
Recommended in vendors	Juniper SSG, Forcepoint Sidewinder, WatchGuard	Cisco, Check Point, Juniper SRX, Palo Alto, SonicWALL, Sophos, Huawei, Forcepoint Stonesoft
Supported in vendors	Cisco, Check Point, Juniper, Palo Alto, SonicWALL, Sophos SG, WatchGuard, Forcepoint	Cisco, Check Point, Juniper, Palo Alto, SonicWALL, Sophos, Huawei, Forcepoint
Allow dynamic NAT based on services	Yes	No
May excessively increase the number of policies	Yes for Cisco, Check Point, Juniper SRX, Palo Alto, SonicWALL, Sophos SG, Huawei and Forcepoint Stonesoft	No

For more information about central NAT mode, please refer to the links(in FortiOS 7.2.4) below:

Central SNAT:

https://docs.fortinet.com/document/fortigate/7.2.4/administration-guide/421028/central-snat

Central DNAT:

https://docs.fortinet.com/document/fortigate/7.2.4/administration-guide/448790/central-dnat

Save Source Configuration File

This section provides detail instructions on saving the source configuration file of the 3rd party security vendor conversions.

Barracuda

Save the configuration from Barracuda

1. Extract Barracuda Source Config through JSON format 9.0 and above

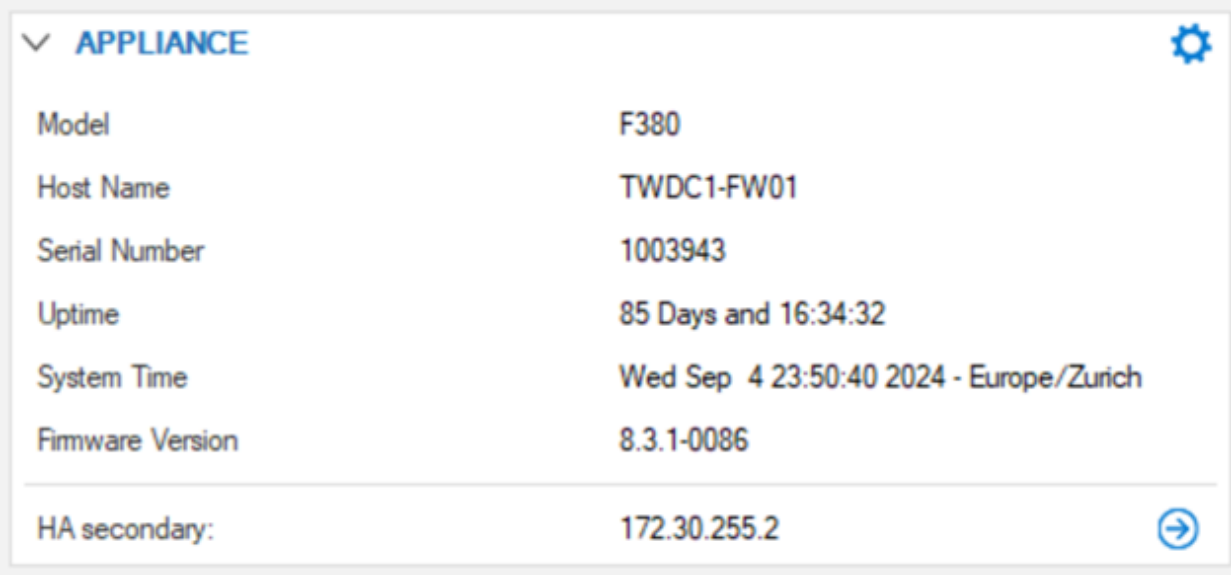
Export WAF Configuration to a JSON File

1. Go to **ADVANCED > Backups** page.
2. In the Export WAF Configuration File section, do the following:
   a. **Backup** - Choose a type of export for exporting the configuration changes.
      i. **Complete Configuration** - Exports the entire WAF configurations including the base configuration.
      ii. **Only Changes** - Export only the configuration changes that were made on the Barracuda Web Application Firewall after the selected checkpoint was created.
         i. **Changes After** - Select the checkpoint to export the changes that were made after it was created.
         ii. **Date** - Displays the date and time when the checkpoint was created.
3. Click **Ok**. The export process can take a few minutes for completion depending on the configurations installed. However, the status of completion is indicated on the User Interface. A Success/Failure message is displayed at the end of the export process.
4. Click **Download** to download and save the JSON file on your computer.

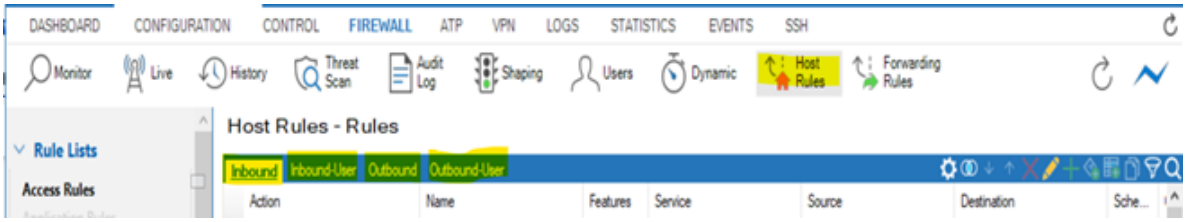
Reference - https://campus.barracuda.com/product/webapplicationfirewall/doc/168311026/backing-up-and-restoring-the-json-configuration-file/

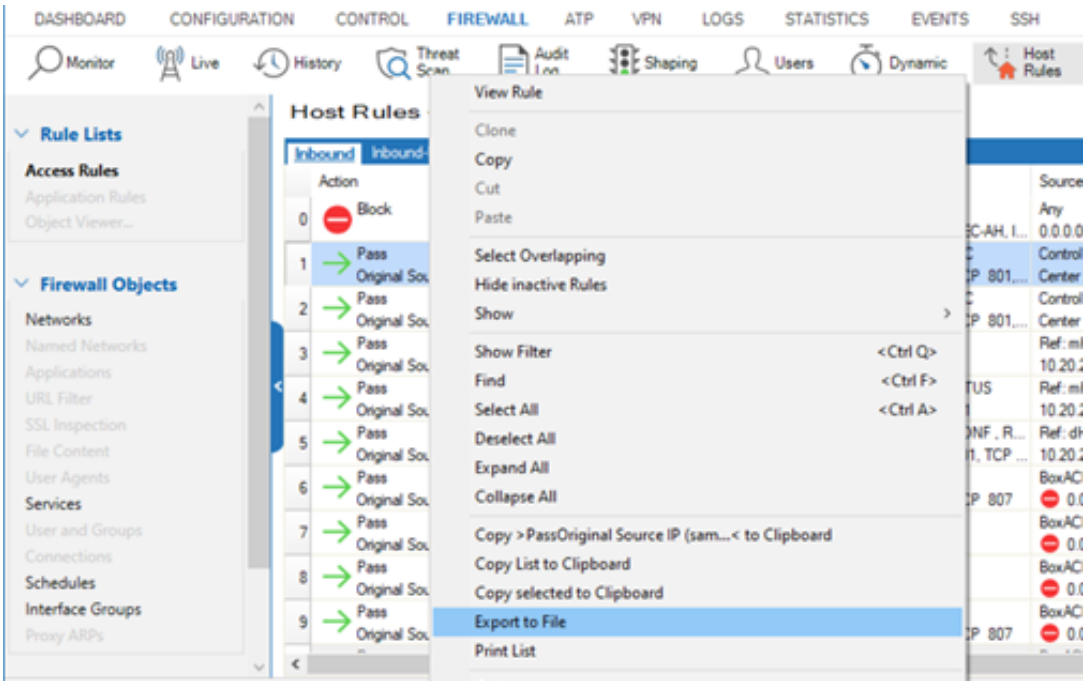
2. Extracting Barracuda Source config for JSON format version below 9.0

For Barracuda version 8.3 and before, instead of providing the default back up file **Box.par**, please use the instructions below to extract individual inbound, outbound and forward rule files.

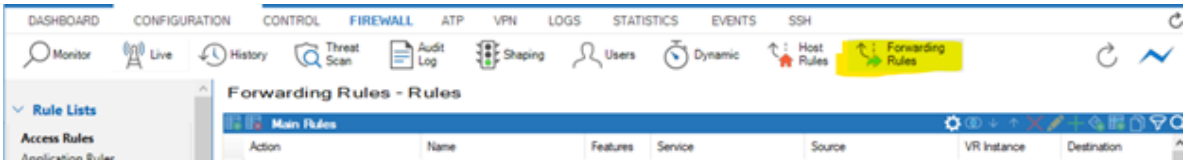


1. Log in to the GUI of the Barracuda firewall.
2. Extract the inbound host rules - Navigate to **FIREWALL > Host Rules > Inbound**, then right click on any rule and select **Export to File** and name the file as `Inbound.txt`.
3. Repeat the steps above for all highlighted section in the image below and name the files as
   - Inbound-User.txt
   - Outbound.txt
   - Outbound-User.txt

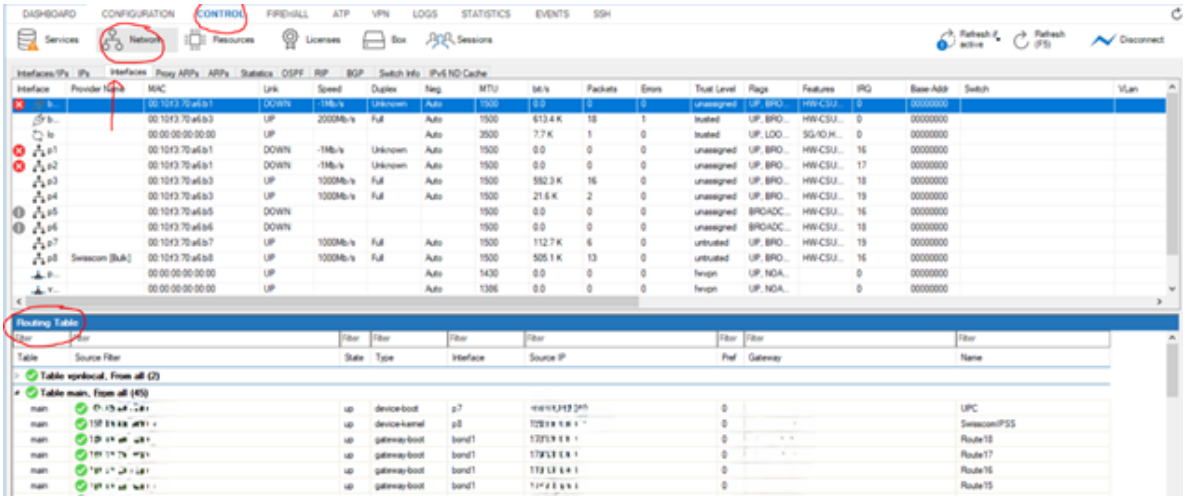


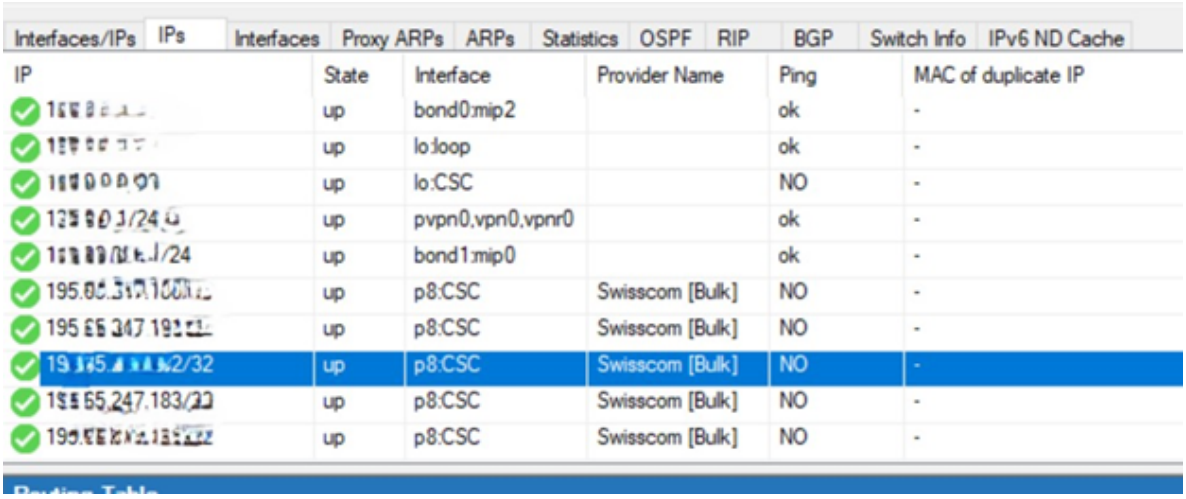


4. Extract the forwarding rules - Navigate to **FIREWALL > Forwarding Rules**, right click on any rule and select **Export to File** and name the file as `Forwarding_Rules.txt`



5. Extract the site-to-site VPN config - Navigate to **VPN > Site-to-Site**, right click on any entry and select **Export to File** and name the file as `Site-to-Site-VPN.txt`
6. Extract the interfaces and static routes -





a. Interfaces:

  i. Navigate to **CONTROL > Network > Interfaces**, right click on any interface and select **Export to File** and name the file as `interfaces.txt`.

  ii. Navigate to **CONTROL > Network > IPs**, right click on any interface and select **Export to File** and name the file as `ipaddress.txt`.

b. Static routes: In the routing table section, right click on any route entry and select **Export to File** and name the file as `routes.txt`.

Conversion Support

1. Interfaces
2. Address objects
3. Service objects
4. Firewall Policies [Forwarding rules, Host rules – Inbound and Outbound]
5. Static Routes
6. VPN IPSec

Bluecoat

Save the configuration from Bluecoat

1. In the web UI, go to **Backup & Firmware**.
2. Click **Import Export**.
3. Select **Export full configurations** in block **Export**.
4. Click **Export** and save the configuration file, which should be XML-formatted.

Check Point

To acquire the configuration, please download the following files from the management system, ensure the configuration is in a text format. FortiConverter can't take binary files.

Use the following command to find the files:

```
# find / -name "filename"
```

Saving the Check Point source configuration file from Smart Center on page 51

Saving the Check Point source configuration file from Provider 1 on page 57

Saving the Check Point source configuration file from VSX Gateway on page 58

Saving the Check Point source configuration file from Smart Center

1. Exporting configuration file in JSON format using the "ShowPolicyPackage" tool on page 52

2. Both Checkpoint Smart Center & Gateways with version before R80.10 on page 52

3. Both Checkpoint Smart Center & Gateways are in version R80.10 & Later on page 53

4. Smart Center is on R80.10 and later but Gateways are below R80 such as R77 on page 55

1. Exporting configuration file in JSON format using the "ShowPolicyPackage" tool

WARNING: For Check Point R80-R80.30, please do not use the ShowPolicyPackage tool to export the JSON config. Although Check Point R80-R80.30 supports JSON export, there are some issues in the web API so it could not export complete configurations

To setup “ShowPolicyPackage” tool:

1. Please navigate to Check Point’s GitHub of "ShowPolicyPackage": https://github.com/CheckPointSW/ShowPolicyPackage/releases
2. Find the latest version (which is currently v2.0.6) and download the file "web_api_show_package-jar-with-dependencies.jar".
3. Use a SCP tool you preferred to upload the file "web_api_show_package-jar-with-dependencies.jar" to the SmartCenter Server where Checkpoint R80 management is running.

Before running the tool, please read the file “README.md” in

https://github.com/CheckPointSW/ShowPolicyPackage to know more about how to run the tool, and please focus more on the section “Examples”.

To run “ShowPolicyPackage” tool:

1. Please check if the Check Point API is running. Please follow the steps in this article to check the status or enable the API: https://community.checkpoint.com/t5/API-CLI-Discussion/Enabling-web-api/td-p/32641
2. Run the tool from CLI as "expert":
   `java -jar web_api_show_package-jar-with-dependencies.jar -v`
   This command shows the list of packages which can be exported.
3. Run the command to export the selected package to JSON:
   `java -jar web_api_show_package-jar-with-dependencies.jar -k PACKAGE_NAME -d DOMAIN_NAME`
   ("-d DOMAIN_NAME" is needed only when multiple domains exist.)
4. A ".tar.gz" file would be generated, which contains the JSON config and can be used as the input of FortiConverter.

2. Both Checkpoint Smart Center & Gateways with version before R80.10

- **Object definitions** – "objects_5_0.C" (Check Point NG/NGX) or "objects.C" (Check Point 4.x) contains the firewall's object definitions.
- **Policy rulebases** – "*.w" or "rulebases_5_0.fws". The file name is "<package name>.W" (default "Standard.W") or "rulebases_5_0.fws".
- **[Optional] Route information** – Helps FortiConverter to correctly interpret the network topology being converted. To get this data, enter the route print command (for example, `"netstat -nr"`) on the firewall node and then copy and paste the output into a plain text file. Codes in the output indicate if the route is a directly connected interface, a host route, a network route, and so on. The output varies by the platform.

- **[Optional] User and user groups file** – "fwauth.NDB"
- **[Optional] Identity role file** - Helps FortiConverter to identify the identity role names referenced in Check Point policies and set them as policy user groups. However, FortiConverter cannot convert the identity roles themselves into FortiGate objects. Users should configure them manually using FSSO in FortiGate.
- **[Optional] ifconfig File (For vlan id consistency)** – This file can help the converter to determine the user-set vlan-id for interfaces, if the information is provided. To get this data, enter the command "`ifconfig -a`" then copy and paste the output into a plain text file.
- **[Optional] DHCP relay file** – This file contains the DHCP relay information of interfaces. To get this data, enter the command "`show configuration bootp`" then copy and paste the output into a plain text file.

File paths:

File	File name	Location	Path or Command
Object definitions	objects_5_0.C (Checkpoint NG/NGX) objects.C (Checkpoint 4.x_)	SmartCenter	`$FWDIR/conf` —or— `$FWDIR/database/`
Policy rulebases	rulebase_5_0.fws <package name>.W	SmartCenter	`$FWDIR/conf`
User and User Group file	fwauth.NDB	SmartCenter	`$FWDIR/conf/` —or— `$FWDIR/database/`
Identity role file	identity_roles.C	Gateway	`$FWDIR/conf/`
Route	NA	Gateway	`netstat -nr`
ifconfig file	NA	Gateway	`ifconfig -a`
DHCP relay file	NA	Gateway	`show configuration bootp`

3. Both Checkpoint Smart Center & Gateways are in version R80.10 & Later

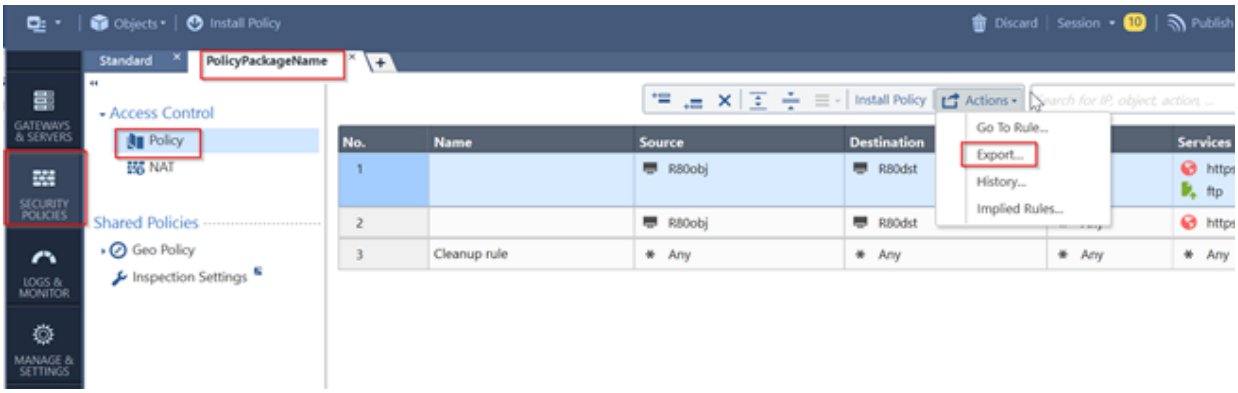
- **Object definitions** – "objects_5_0.C" (Check Point NG/NGX) or "objects.C" (Check Point 4.x) contains the firewall's object definitions.
- **Rule definitions** – "*.csv". The Policy and NAT CSV files can be exported from the Smart Console (refer screenshot below)

- **[Optional] Route information** – Helps FortiConverter to correctly interpret the network topology being converted. To get this data, enter the route print command (for example, "`netstat -nr`") on the firewall node and then copy and paste the output into a plain text file. Codes in the output indicate if the route is a directly connected interface, a host route, a network route, and so on. The output varies by the platform.
- **[Optional] User and user groups file** – "`fwauth.NDB`"
- **[Optional] Identity role file** - Helps FortiConverter to identify the identity role names referenced in Check Point policies and set them as policy user groups. However, FortiConverter cannot convert the identity roles themselves into FortiGate objects. Users should configure them manually using FSSO in FortiGate.
- **[Optional] ifconfig File (For vlan id consistency)** – This file can help the converter to determine the user-set vlan-id for interfaces, if the information is provided. To get this data, enter the command "`ifconfig -a`" then copy and paste the output into a plain text file.
- **[Optional] DHCP relay file** – This file contains the DHCP relay information of interfaces. To get this data, enter the command "`show configuration bootp`" then copy and paste the output into a plain text file.

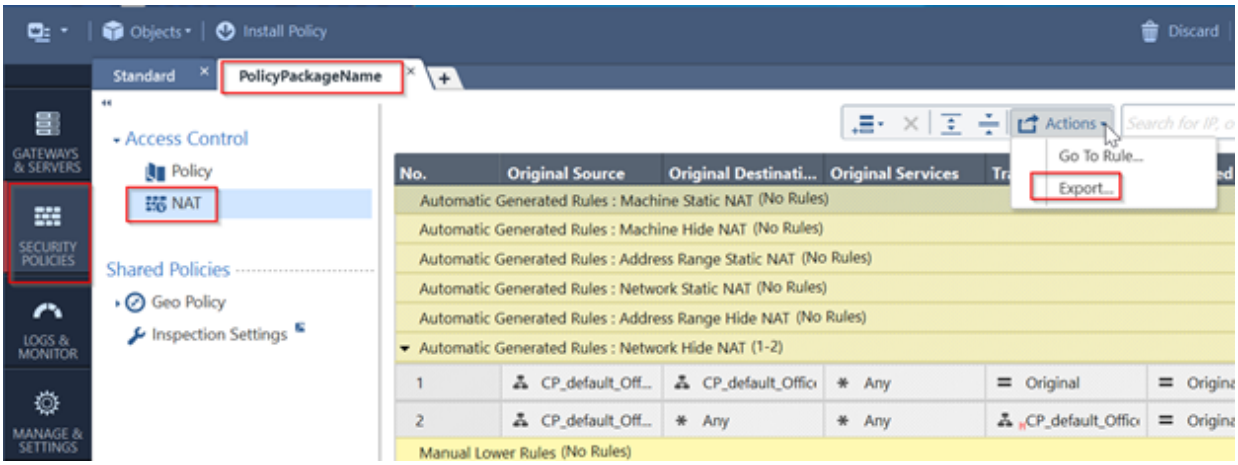
File Path:

File	File name	Location	Path or command
Object definitions	objects_5_0.C (Checkpoint NG/NGX)	SmartCenter	`$FWDIR/conf` —or— `$FWDIR/database/`
	objects.C (Checkpoint 4.x_)		
Policy and NAT files	NA	SmartConsole GUI	Refer to screenshots below
User and User Group file	fwauth.NDB	SmartCenter	`$FWDIR/conf/` —or— `$FWDIR/database/`
Identity Role file	identity_roles.C	SmartCenter	`$FWDIR/conf/`
Route	NA	Gateway	`netstat -nr`
ifconfig file	NA	Gateway	`ifconfig -a`
DHCP relay file	NA	Gateway	`show configuration bootp`

Export Policy file (CSV Format):



Export Nat file (CSV Format)



Note: Alternately, you can chose to download Policy and rule definitions file "`rulebases_5_0.fws`" from following path if you are interested to cross verify it with CSV file **`$FWDIR/conf/rulebase_5_0.fws`**

4. Smart Center is on R80.10 and later but Gateways are below R80 such as R77

- **Object definitions** – "objects_5_0.C" (Check Point NG/NGX) or "objects.C" (Check Point 4.x) contains the firewall's object definitions.
- **Policy rulebases** – "*.w" or "rulebases_5_0.fws". The file name is "<package name>.W" (default "Standard.W") or "rulebases_5_0.fws".
- **[Optional] Route information** – Helps FortiConverter to correctly interpret the network topology being converted. To get this data, enter the route print command (for example, "netstat -nr") on the firewall node and then copy and paste the output into a plain text file. Codes in the output indicate if the route is a directly connected interface, a host route, a network route, and so on. The output varies by the platform.
- **[Optional] User and user groups file** – "fwauth.NDB"
- **[Optional] Identity role file** - Helps FortiConverter t

- o identify the identity role names referenced in Check Point policies and set them as policy user groups. However, FortiConverter cannot convert the identity roles themselves into FortiGate objects. Users should configure them manually using FSSO in FortiGate.
- **[Optional] ifconfig File (For vlan id consistency)** – This file can help the converter to determine the user-set vlan-id for interfaces, if the information is provided. To get this data, enter the command "`ifconfig -a`" then copy and paste the output into a plain text file.
- **[Optional] DHCP relay file** – This file contains the DHCP relay information of interfaces. To get this data, enter the command "`show configuration bootp`" then copy and paste the output into a plain text file.

File Path:

File	File name	Location	Path or command
Object definitions	objects_5_0.C (Checkpoint NG/NGX)	SmartCenter	`/opt/CPR77CMP-R80/conf`
Policy rulebases	rulebase_5_0.fws <package name>.W	SmartCenter	`/opt/CPR77CMP-R80/conf`
User and User Group file	fwauth.NDB	SmartCenter	`/opt/CPR77CMP-R80/conf`
Identity role file	identity_roles.C	SmartCenter	`/opt/CPR77CMP-R80/conf`
Route	NA	Gateway	`netstat -nr`
ifconfig file	NA	Gateway	`ifconfig -a`
DHCP relay file	NA	Gateway	`show configuration bootp`

Note: Alternately, you can choose to download Policy and rule definitions file "`rulebases_5_0.fws`" from following path if you are interested to cross verify it with CSV file: **/opt/CPR77CMP-R80/conf**

Saving the Check Point source configuration file from Provider 1

Provider – 1 to FortiGate conversion

Usually used while converting a single checkpoint firewall to a FortiGate.

1. Both MDS/CMA & Gateways are on version before R80.10

MDS is running with multiple CMA domains and we need to convert a single CMA to FortiGate, please refer Section-1 to fetch the files.

2. Both MDS/CMA & Gateways are on version R80.10 Or later

MDS is running with multiple CMA domains and we need to convert a single CMA to FortiGate, please refer Section-2 to fetch the files.

3. MDS/CMA is on R80.10 but Gateways running below R80 such as R77

- We can fetch policy and Nat csv files as mentioned above as the management server running with R80.
- Object definitions and user files are available in the below table.

File Path:

File	File name	Location	Path or command
Object definitions	objects_5_0.C (Checkpoint NG/NGX)	MDS/CMA	`/opt/CPmds-R80/customers/<CMA_Server>/CPR77CMP-R80/conf/`
Policy rulebases	rulebase_5_0.fws	MDS/CMA	`/opt/CPmds-R80/customers/<CMA_Server>/CPR77CMP-R80/conf/`
	<package name>.W		
User and user group file	fwauth.NDB	MDS/CMA	`/opt/CPmds-R80/customers/<CMA_Server>/CPR77CMP-R80/conf/`
Identity role file	identity_roles.C	MDS/CMA	`/opt/CPmds-R80/customers/<CMA_Server>/CPR77CMP-R80/conf/`
Route	NA	Gateway	`netstat -nr`
ifconfig file	NA	Gateway	`ifconfig -a`
DHCP relay file	NA	Gateway	`show configuration bootp`

Note: Alternately, you can choose to download Policy and rule definitions file "`rulebases_5_0.fws`" from following path if you are interested to cross verify it with CSV file: **/opt/CPmds-R80/customers/<CMA_Server>/CPR77CMP-R80/conf/**

Saving the Check Point source configuration file from VSX Gateway

To achieve this, we need to fetch Policy file for each corresponding VSYS. The direction to export such file is outlined below.

All objects belonging to different VSYS (excluding to Security rule and NAT rules) are maintained in one common file. **For example**, Object.c

1. Both Checkpoint Smart Center & VSX Gateways(VS) are in version R80.10 & Later on page 58

2. Both Checkpoint Smart Center & VSX Gateways(VS) with version before R80.10 on page 60

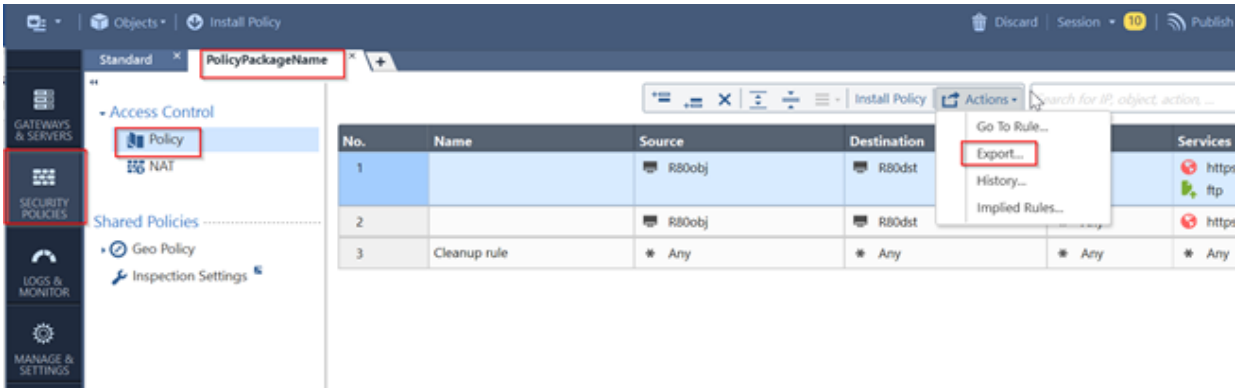
1. Both Checkpoint Smart Center & VSX Gateways(VS) are in version R80.10 & Later

- **Policy and rule definitions** – "*.csv". The Policy and NAT CSV files can be exported from the Smart Console (refer screenshot below)
- **Object definitions** – "objects_5_0.C" (Check Point NG/NGX) or "objects.C" (Check Point 4.x) contains the firewall's object definitions.
- **Route information (optional)** – Helps FortiConverter to correctly interpret the network topology being converted. To get this data, enter the route print command (for example, "netstat -nr") on the firewall node and then copy and paste the output into a plain text file. Codes in the output indicate if the route is a directly connected interface, a host route, a network route, and so on. The output varies by the platform.
- **User and user groups file (optional)** – "fwauth.NDB"

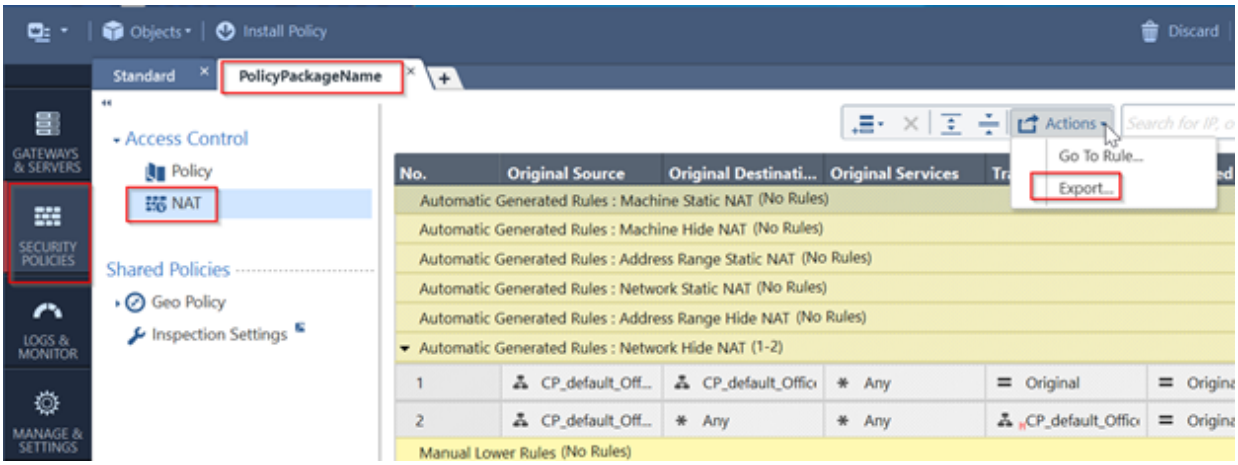
File Path

File	File name	Location	Path or Command
Object definitions	objects_5_0.C (Checkpoint NG/NGX)	SmartCenter	`$FWDIR/conf` —or— `$FWDIR/database/`
	objects.C (Checkpoint 4.x_)		
Policy and NAT files	NA	SmartConsole GUI	`Refer to screenshots below`
User and user Group file	fwauth.NDB	SmartCenter	`$FWDIR/conf/` —or— `$FWDIR/database/`
Route	NA	Gateway	`netstat -nr`

Export Policy file (CSV Format):



Export Nat file (CSV Format)



2. Both Checkpoint Smart Center & VSX Gateways(VS) with version before R80.10

- **Object definitions** – "objects_5_0.C" (Check Point NG/NGX) or "objects.C" (Check Point 4.x) contains the firewall's object definitions.
- **Policy rulebases** – "*.w" or "rulebases_5_0.fws". The file name is "<package name>.W" (default "Standard.W") or "rulebases_5_0.fws".
- **Route information (optional)** – Helps FortiConverter to correctly interpret the network topology being converted. To get this data, enter the route print command (for example, "netstat -nr") on the firewall node and then copy and paste the output into a plain text file. Codes in the output indicate if the route is a directly connected interface, a host route, a network route, and so on. The output varies by the platform.
- **User and user groups file (optional)** – "fwauth.NDB"

File paths:

File	File name	Location	Path or Command
Object definitions	objects_5_0.C (Checkpoint NG/NGX) objects.C (Checkpoint 4.x_)	SmartCenter	`$FWDIR/conf` —or— `$FWDIR/database/`
Policy rulebases	rulebase_5_0.fws <package name>.W	SmartCenter	`$FWDIR/conf`
User and user Group file	fwauth.NDB	SmartCenter	`$FWDIR/conf/` —or—

File	File name	Location	Path or Command
			`$FWDIR/database/`
Route	NA	Gateway	`netstat -nr`

Ciena (Vyatta)

Save the configuration from Ciena

1. Use an SSH terminal and connect to the device.
2. Input command "`set terminal length 0`".
3. Input "`show configuration all`" and save the output configuration.

Please note that FortiConverter requires the structural configuration file as a valid input.

For example:

```
firewall {
   all-ping enable
   broadcast-ping disable
   config-trap disable
   group {
   address-group ADDR_GRP1 {
      address 10.58.14.15
      address 10.58.14.16
      address 10.58.14.17
   }
   address-group ADDR_GRP2 {
      address 10.58.186.41
      address 10.58.186.52
   }
   ............
   ............
```

CIPA Firewall

Customer can reach out to CIPA filter support team for a decrypted source file

Cisco

Cisco ASA, FWSM, and PIX

Save the configuration from Cisco

To get the configuration, you can use the CLI commands:

```
terminal length 0
show running-config
```

Copy and paste the outputs into a plain text file.

Cisco FTD

Part 1: Save LINA configuration

To get the configuration, you can use the CLI commands:

```
terminal length 0
show running-config
```

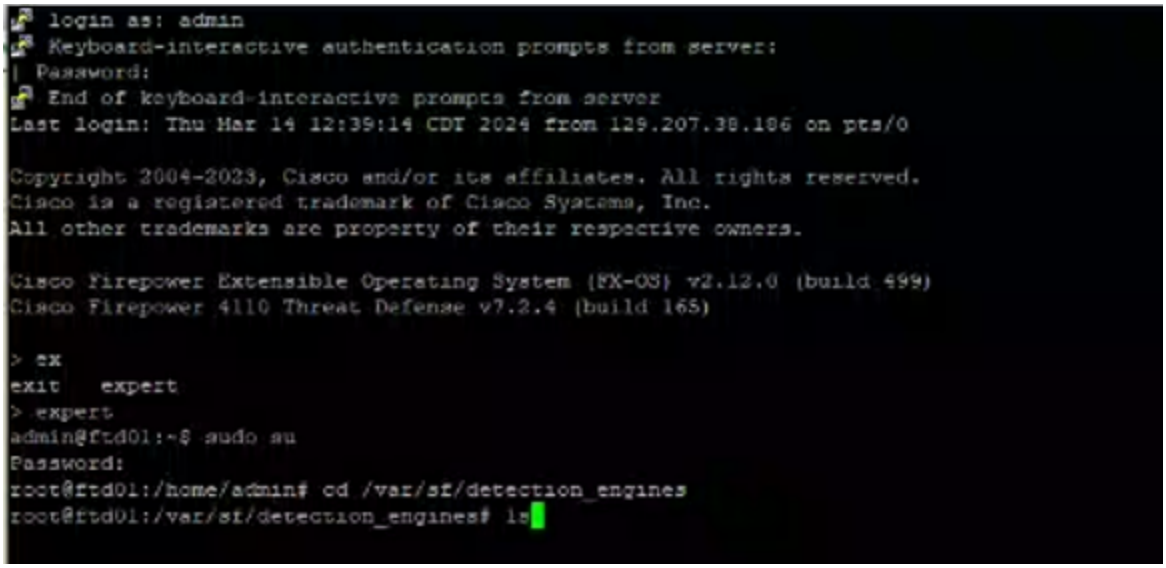
Copy and paste the outputs into a plain text file.

Part 2: Backup the NGFW Rules, Snort3, FQDN from FTD

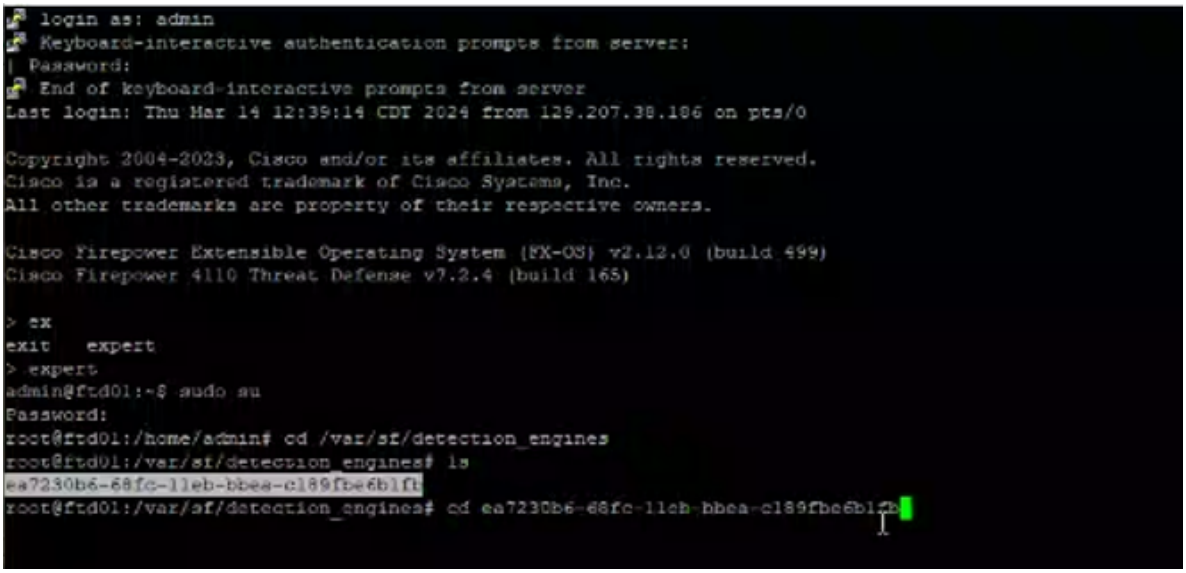
This guide briefly shows where to find the NGFW Rules, IPS, FQDN and how to save in a txt file.

From FTD CLI expert mode navigate to the directory `ngfw/var/sf/detection_engines/<UUID>/ngfw.rules` by following the steps below:

1. Log in to FTD CLI as Expert Mode.



2. Navigate to the directory `ngfw/var/sf/detection_engines/` by using `cd` command.
3. Verify the uuid by `ls` command.



4. List all the files and folders in the current directory using the `ls -l` command.

```
dir = os.getenv('SNORT_LUA_PATH')
if ( not dir ) then
    dir = '.'
end

-- IPS/NAP configuration from Access rules
include('policies.lua')

-- Global modules
include('snort3.global.lua')

cat: snort3.sock: No such device or address
root@ftd01:/var/sf/detection_engines/ea7230b6-68fc-11eb-bbea-c189fbe6b1fb# ls -l ips
```

5. Get the files, for example, if we are trying to fetch NGFW_rules use the command `cat NGFW_rules`.

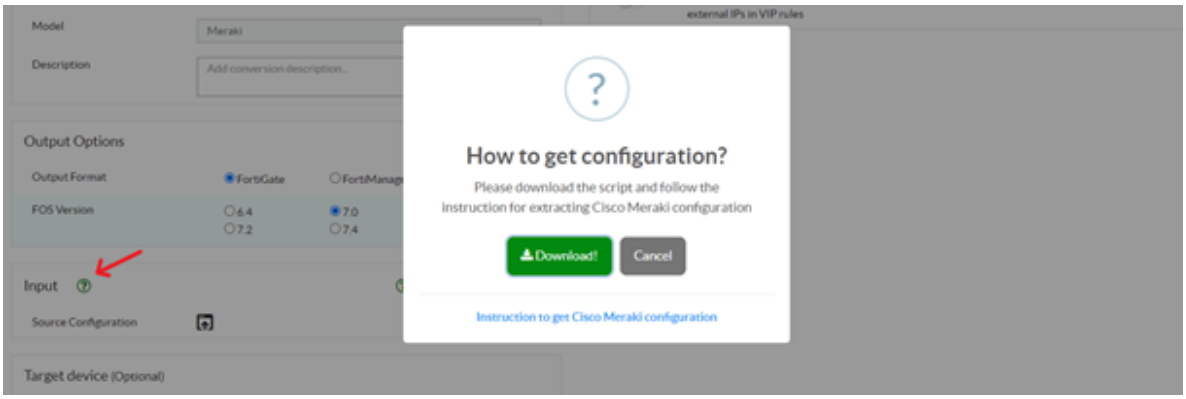
```
root@ftd01:/var/sf/detection_engines/ea7230b6-68fc-11eb-bbea-c189fbe6b1fb/plugins# ls -l
total 14896
-rw-r--r-- 1 root root   85660 Jul  3  2023 appid_navl.so
-rw-r--r-- 1 root root  110160 Jul  3  2023 captive_portal.so
-rw-r--r-- 1 root root   18704 Jul  3  2023 cd_pdts.so
-rw-r--r-- 1 root root  163536 Jul  3  2023 crashhandler.so
-rw-r--r-- 1 root root  529592 Jul  3  2023 dns_si.so
-rw-r--r-- 1 root root   43520 Jul  3  2023 efd.so
-rw-r--r-- 1 root root 3293496 Jul  3  2023 firewall.so
-rw-r--r-- 1 root root   31184 Jul  3  2023 lab.so
-rw-r--r-- 1 root root 1453752 Jul  3  2023 identity.so
-rw-r--r-- 1 root root 1297048 Jul  3  2023 insight.so
-rw-r--r-- 1 root root   52096 Jul  3  2023 izm.so
-rw-r--r-- 1 root root   89728 Jul  3  2023 mercury.so
-rw-r--r-- 1 root root  603384 Jul  3  2023 qos.so
-rw-r--r-- 1 root root 1498232 Jul  3  2023 rna_util.so
-rw-r--r-- 1 root root  509016 Jul  3  2023 url_si.so
-rw-r--r-- 1 root root 5443064 Jul  3  2023 xtls.so
root@ftd01:/var/sf/detection_engines/ea7230b6-68fc-11eb-bbea-c189fbe6b1fb/plugins#
```

6. Copy and paste in a text file.

Cisco Meraki

Save the configuration on Cisco Meraki

1. Please follow the steps in the Meraki documentation below to generate an API key: https://documentation.meraki.com/General_Administration/Other_Topics/Cisco_Meraki_Dashboard_API
2. Fortinet provides a Python script, `fcon_meraki_backup.py`, which exports backup config files which can be converted by FortiConverter. Please download the script from the FortiConverter application:



This script is also available in the FortiConverter tool's GitHub:
https://github.com/fortinet/forticonverter-tools/blob/main/fcon_meraki_backup.py

3. Run the script file and select the organization and network you would like to backup.
Example procedure:

```
(MerakiBackup) C:\>py fcon_meraki_backup.py [API_KEY]
Welcome to Meraki config backup tool for FortiConverter.

The following organizations are fetched by the API key:
1.      1365006: CWP

Only one organization is fetched. Selecting "CWP" automatically.

The following networks are fetched from organization "CWP":
1.      L_3705899543372501083: nac

Only one network is fetched. Selecting "nac" automatically.

Backup config file is saved as "meraki_backup_CWP_nac_20231128161249.json".
```

For a detailed instruction of the script, please see the README file in the link below:
https://github.com/fortinet/forticonverter-tools/blob/main/README.md

Forcepoint

Save the source configuration files on Forcepoint Sidewinder on page 66

Save the source configuration files on Forcepoint Stonesoft on page 67

Save the source configuration files on Forcepoint Sidewinder

The following is for **McAfee Firewall Enterprise 8**. The config is binary therefore the output of the following commands must be saved to a text file for FortiConverter.

- Interface and Zone (`cf interface|zone|zonegroup query`)
- Address object and address group object (`cf domain|ipaddr|iprange|subnet|host|geolocation|netgroup query`)
- Service object and service group object (`cf application|appgroup query`)
- NAT objects (cf netmap query)
- Admin users and firewall users & user groups (`cf adminuser query, cf udb query, cf usergroup query`)
- Static routes (`cf route query`)
- Firewall Policy (`cf policy query`)

Syntax difference on Sidewinder's CLI between v7 and v8

McAfee Firewall Enterprise v7	McAfee Firewall Enterprise v8
cf interface query	cf interface query
cf burb query	**cf zone query**
cf burbgroup query	**cf zonegroup query**
cf domain query	cf domain query
cf ipaddr query	cf ipaddr query
cf iprange query	cf iprange query
cf subnet query	cf subnet query
cf host query	cf host query
cf geolocation query	cf geolocation query
cf netgroup query	cf netgroup query
cf service query	**cf application query**
cf servicegroup query	**cf appgroup query**
cf netmap query	cf netmap query
cf adminuser query	cf adminuser query
cf udb query	cf udb query
cf usergroup query	cf usergroup query
cf static query	**cf route query**
cf policy query	cf policy query

Sample CLI commands to retrieve configurations from Sidewinder and upload to a SCP server.

```
cf interface query > fc_interface.txt
cf burb query > fc_burb.txt
cf burbgroup query > fc_burbgroup.txt
cf domain query > fc_domain.txt
cf ipaddr query > fc_ipaddr.txt
cf iprange query > fc_iprange.txt
cf subnet query > fc_subnet.txt
cf netgroup query > fc_netgroup.txt
cf service query > fc_service.txt
cf servicegroup query > fc_servicegroup.txt
cf adminuser query > fc_adminuser.txt
cf udb query > fc_udb.txt
cf usergroup query > fc_usergroup.txt
cf static query > fc_static.txt
cf policy query > fc_policy.txt
cf ipsec query show_clear_passwords=true > fc_ipsec.txt
cf geolocation list > fc_geoloc_list.txt
cf geolocation query > fc_geoloc_query.txt
cf netmap query > fc_netmap.txt
cat fc_*.txt > forticonverter.txt
scp -v forticonverter.txt <username>@xxx.xxx.xxx.xxx:/
```

Save the source configuration files on Forcepoint Stonesoft

To get the XML format configuration file, you can find the export function from the web GUI:

Choose **Menu > File > Export > Export All Elements**

Huawei

Exporting config through web operation

1. Choose **System** > **Configuration File Management**.
2. Click **Export** in **Current Configuration**.
3. Click **Save** and select a path on the terminal to save the configuration file.

Juniper

Save the configuration from Juniper

To get the configuration, for both ScreenOS and Junos, in the web UI, go to **Configuration> Update > ConfigFile**.

Alternatively, for ScreenOS only, you can use the `get conf` CLI command and paste the output into a plain text file.

For Junos, FortiConverter requires the structural configuration file as a valid input.

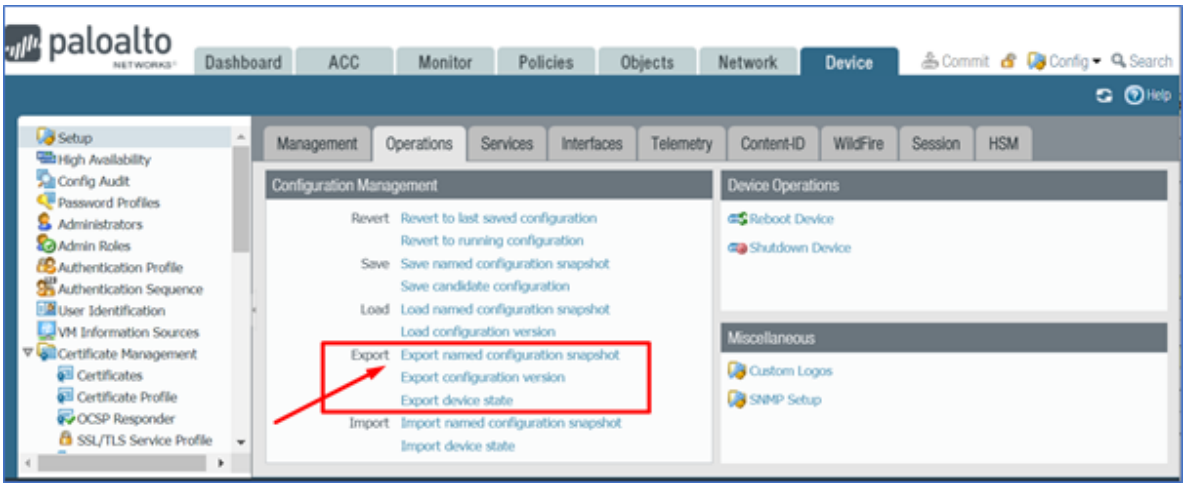
For example:

```
show configuration
   ## Last commit: 2013-06-05 11:28:53 CST by master
   version 10.2S7;
   groups {
      node0 {
         system {
               host-name SRX3400-Active;
               backup-router 172.16.1.254 destination 0.0.0.0/0;
         }
            interfaces {
               fxp0 {
                  unit 0 {
                     family inet {
                        address 172.16.1.1/24;
                  }
            }
         }
      }
   }
   ............
   ............
```

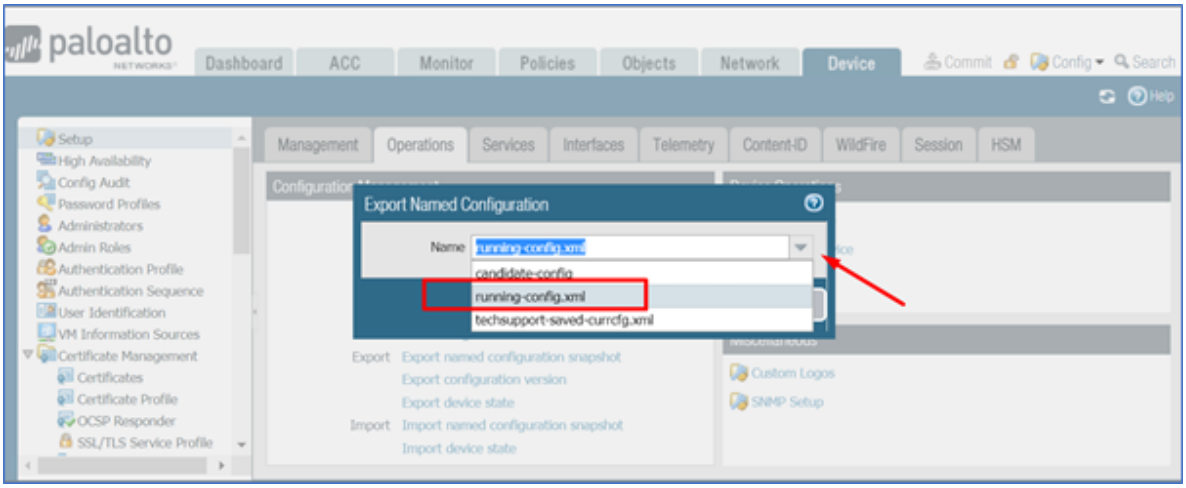
Palo Alto Networks

Configuration File from Palo Alto FW (Not Managed by Panorama)

1. Log-in to **Palo Alto FW** web UI using super-user account.
2. In the web UI, go to **Device > Setup > Operations**, then click **Export named configuration snapshot**.



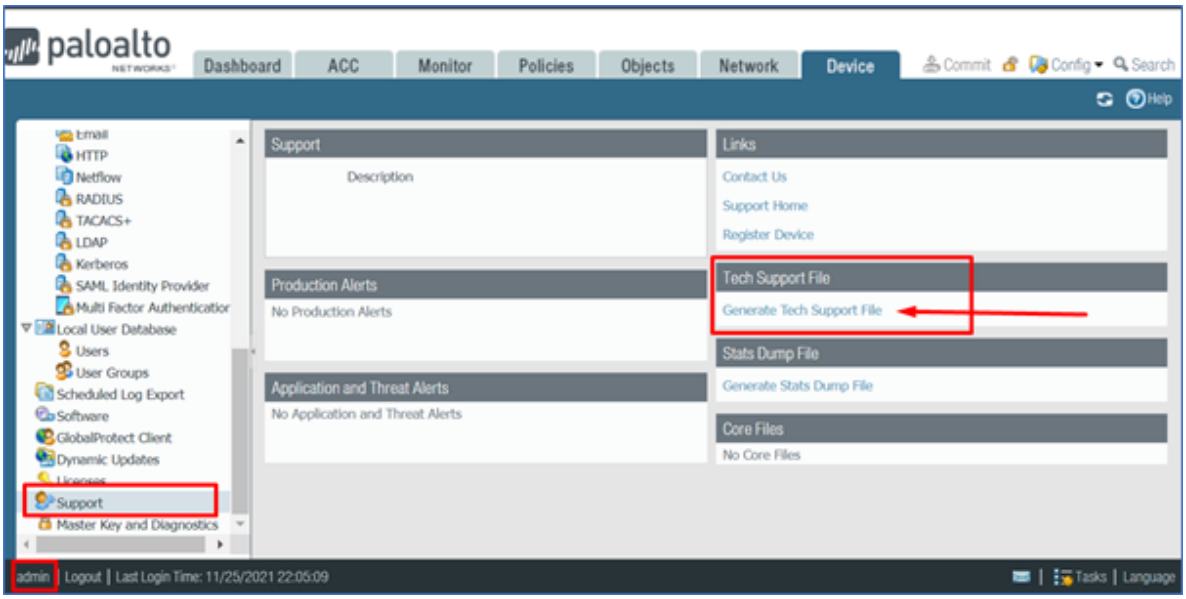
3. Select the **running-config.xml** from the dropdown menu.



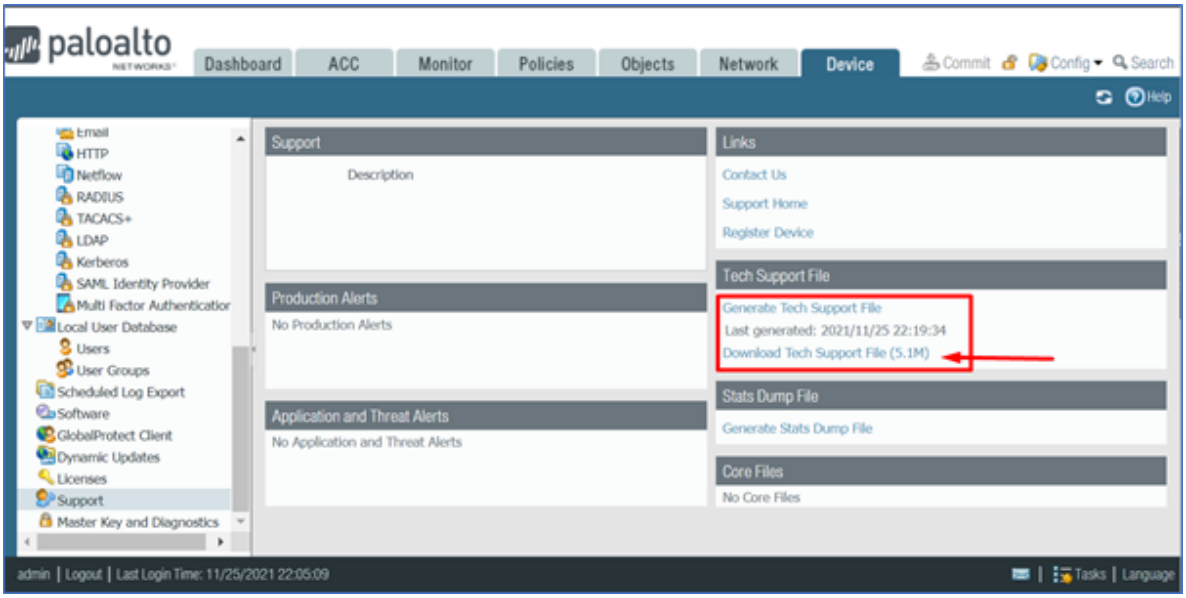
4. Download the file above and upload to FortiConverter through the source configuration tab and follow the steps in conversion process.

Configuration File from Palo Alto FW Web UI (Managed by Panorama)

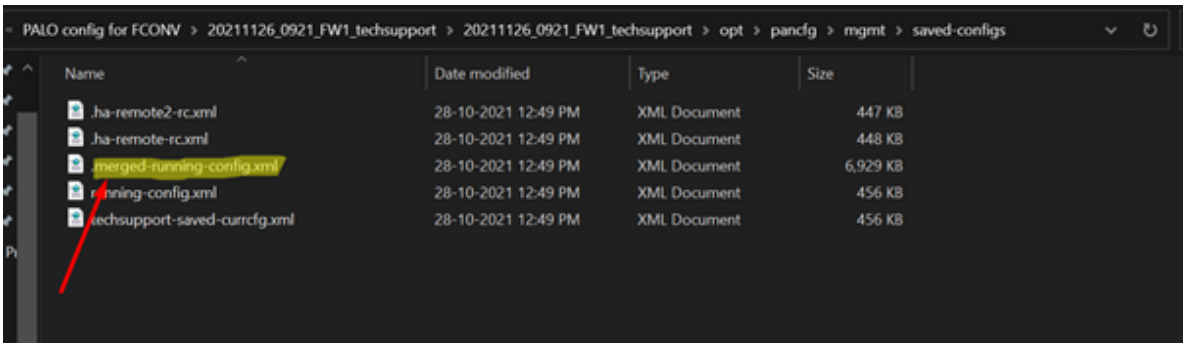
1. Log in to the **Palo Alto FW** web UI using super-user account.
2. In the web UI, go to **Device > Support > Tech Support File**, then click **Generate Tech support File**.



3. Once the file is generated and become available, click **Download Tech Support File**.



4. Unzip and Untar the file and then navigate to the path `\opt\pancfg\mgmt\saved-configs\` to fetch a file named "merged-running-config.xml".



5. Use the file above to upload to FortiConverter through the source configuration tab and follow the steps in conversion process.

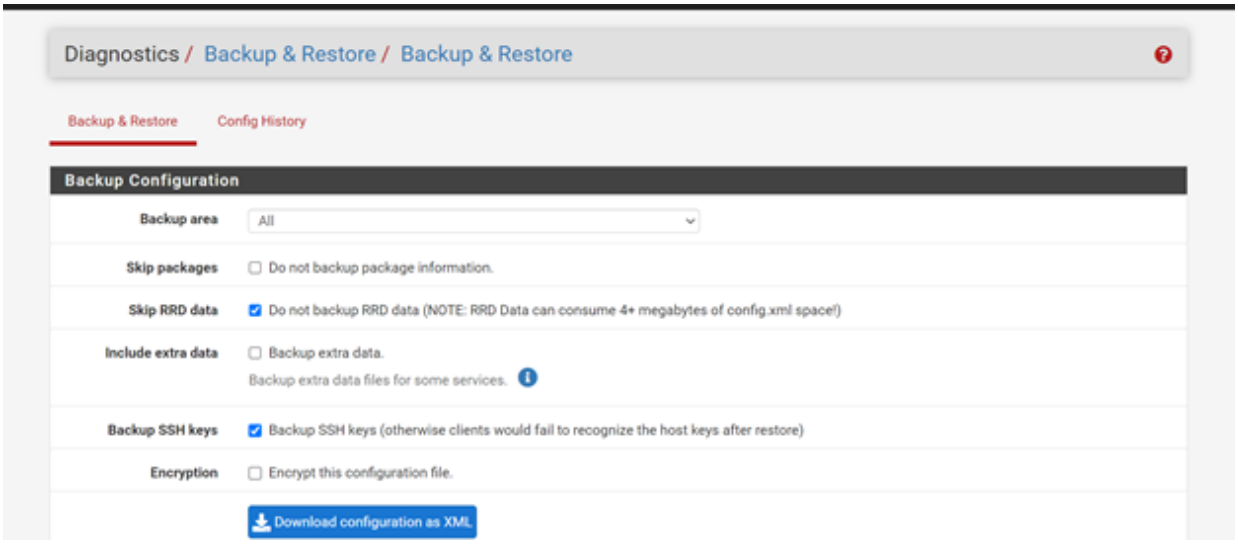
Configuration File from Palo Alto FW CLI (Managed by Panorama)

1. Log-in to the **Palo Alto FW** CLI using super-user account.
2. Use these commands to generate or export "tech-support-file" to TFTP server or SCP server:
   ```
   > tftp export tech-support to <tftp host>
   > scp export tech-support to <username@host:path>
   ```
3. Unzip and Untar the file and then navigate to path `\opt\pancfg\mgmt\saved-configs\` to fetch a file named ".merged-running-config".
4. Use the file above to upload to FortiConverter through source configuration tab and follow the steps in conversion process.

PFSense

Save the source config on PFsense

STEP 1: In the web UI, go to Diagnostics > Backup & Restore

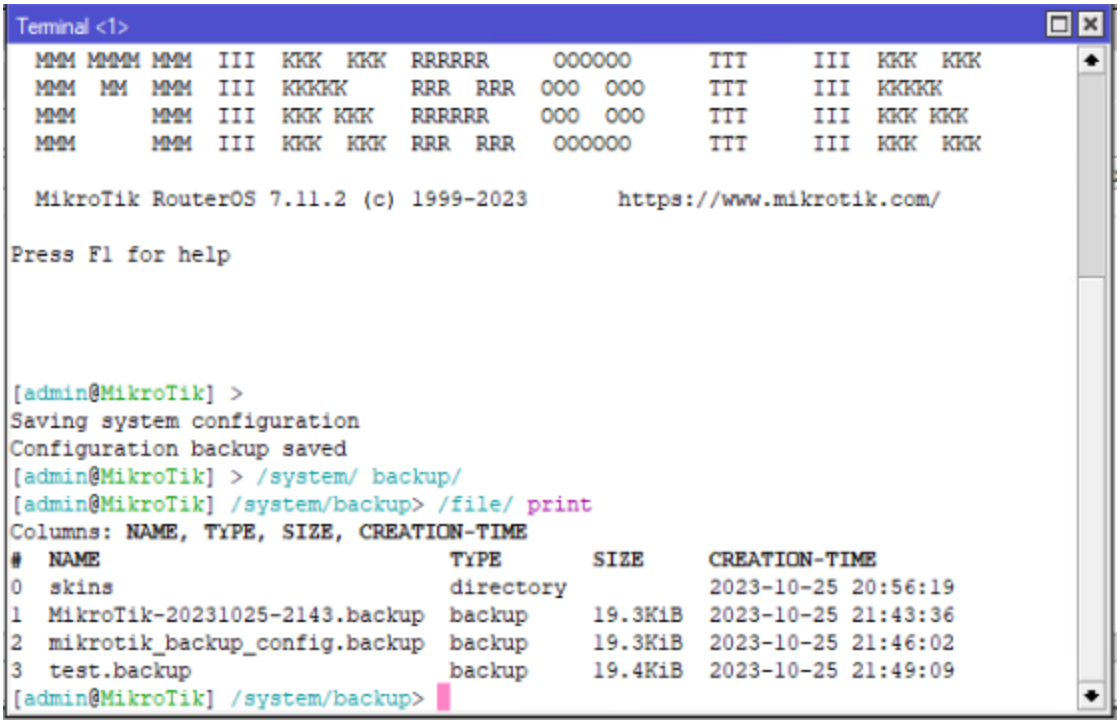


STEP 2: Click on "Download configuration as XML"

Mikrotik

Saving the source config files on Mikrotik

STEP 1: In terminal, go to `/system backup`



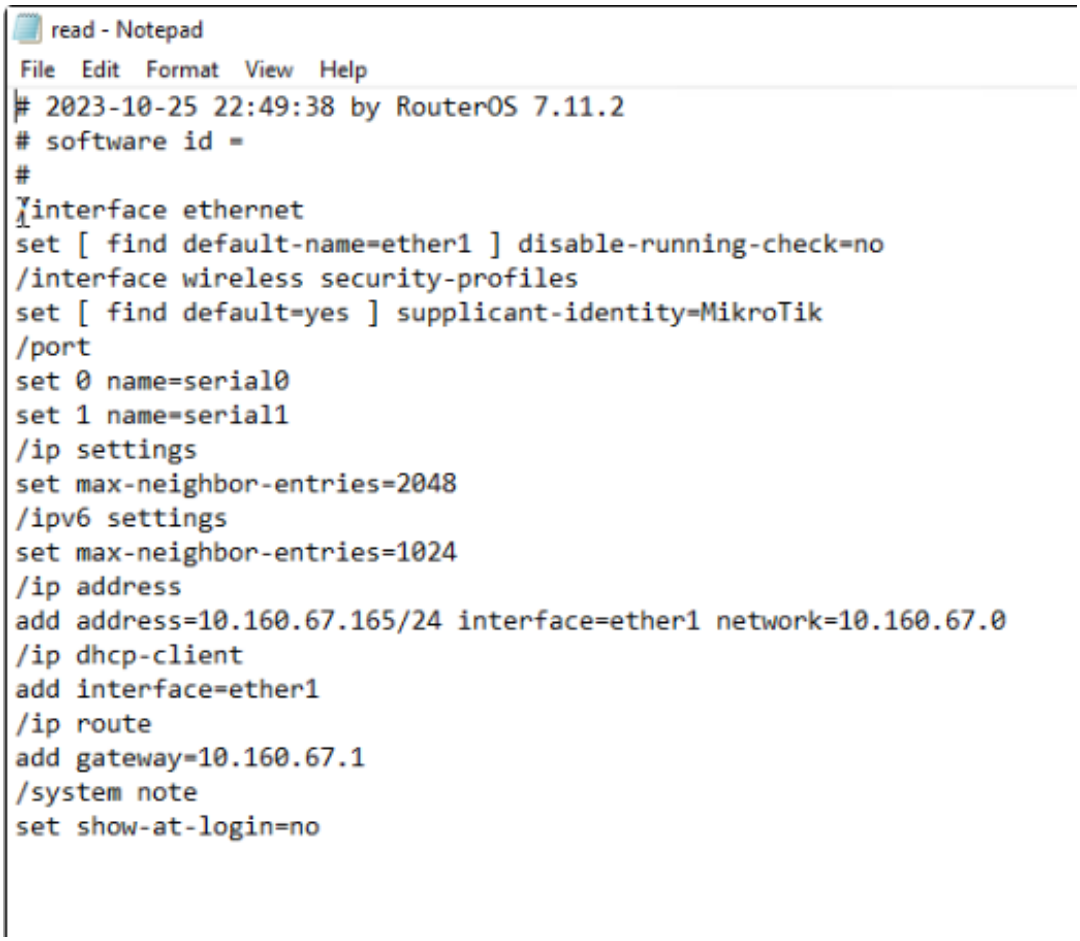
STEP 2: Export the source config into readable format

Execute: `/export file=read`

```
[admin@MikroTik] /system/backup> export fi=test.rsc
bad command name export (line 1 column 1)
[admin@MikroTik] /system/backup> /export file=read
[admin@MikroTik] /system/backup> /file/ print
Columns: NAME, TYPE, SIZE, CREATION-TIME
#  NAME                          TYPE       SIZE     CREATION-TIME
0  skins                         directory           2023-10-25 20:56:19
1  MikroTik-20231025-2143.backup backup     19.3KiB  2023-10-25 21:43:36
2  mikrotik_backup_config.backup backup     19.3KiB  2023-10-25 21:46:02
3  test.backup                   backup     19.4KiB  2023-10-25 21:49:09
4  read.rsc                      script     567      2023-10-25 22:49:38
5  pub                           directory           2023-10-25 22:49:38
[admin@MikroTik] /system/backup>
```

`read.rsc` is readable format of source config

Config looks like below:



SmoothWall

Steps to extract the Smoothwall source configuration files

Login via SSH and retrieve the .json files in the `/settings/` directory of the Smoothwall's linux OS.

All the configurations will be located inside `/settings/`

1. **Interfaces**
   Interfaces_ethernet.json: `/settings/ethernet.json`
2. **Addresses and Address groups**
   AddressObjects_namedaddresses.json: `/settings/namedaddresses.json`
3. **Service and Service groups**
   ServiceObjects_namedservices.json: `/settings/namedservices.json`

4. **DNS**
   LocalDNSHosts_dnsmasq.json: `/settings/dnsmasq.json`
5. **Firewall Policies**
   FirewallRules_ipfilter.json: `/settings/ipfilter.json`
6. **Virtual IPs / Destination NAT**
   PortForwards_dnat.json: `/settings/dnat.json`
7. **Source NAT**
   SourceNAT_LoadBalance_snat.json: `/settings/snat.json`

Shorewall

Save the configuration from Shorewall

There are two methods to save the Shorewall configuration. Follow one of the methods blow based on your preference.

Method 1 - Extract files from CLI

When accessing the device remotely, use SSH to connect: **`#ssh user@device-ip`**

The Shorewall configuration files are typically located in `/etc/shorewall`, navigate to this directory using: **`#cd /etc/shorewall`**

Below are the paths for each file:

```
Policy - /etc/shorewall/policy
Rules - /etc/shorewall/rules
Hosts - /etc/shorewall/hosts
Zones - /etc/shorewall/zones
Interfaces - /etc/shorewall/interfaces
```

Use scp(secure copy) command to transfer the files from the device to your local machine.

For example:

```
scp user@device-ip:/etc/shorewall/hosts /local/path/hosts
scp user@device-ip:/etc/shorewall/zones /local/path/zones
scp user@device-ip:/etc/shorewall/policies /local/path/policies
```

Replace `/local/path/` with the directory on your local machine where you want to save the files.

Method 2 - Extract Files Using GUI

There are a couple of places to choose from to extract files from the GUI.

1. Shorewall Web Interface

If you have a web-based management tool set up for Shorewall, such as **Shorewall Web**, follow these steps:

1. Log into the **Shorewall Web** interface by navigating to the appropriate URL on your browser.
2. Navigate to the section related to configuration or settings. The interface should have options to view or export configuration files.
3. Export files - If the web interface provides an option to export or download the configuration files, use it to save hosts, zones, and policy files to your local machine.

2. Web-Based Firewall Management

Some firewall management systems that integrate with Shorewall may offer a GUI with configuration section.

In a firewall management system that integration with Shorewall:

1. **Find Configuration Section**: Locate the section where you can view or manage the Shorewall configuration.
2. **Download or Export**: Use any available options to download or export configuration files.

3. Using Dedicated GUI Tools

Option 1: Webmin

Webmin is a web-based interface for system administration. If it is set up to manage Shorewall, Shorewall configuration can be exported from Webmin. Instruction on exporting Shorewall configuration from Webmin:

1. **Access Webmin** - Open your browser and go to the Webmin interface (e.g., `http://your-server-ip:10000`).
2. **Navigate to Shorewall** - Go to the Networking section and find Shorewall or firewall-related modules.
3. **Download Configuration** - Webmin might have options to view or download the Shorewall configuration files.

Option 2: Firewall Management GUI

There are certain Linux distributions of third-party tools with a firewall management GUIs that supports Shorewall.

Instruction on exporting Shorewall configuration from these Linux distributions or third-party tools firewall management GUI:

1. Access the GUI application.
2. Locate Shorewall Settings: Find the section for managing Shorewall.
3. Export or View Files: Use the export or download functionality to download the configuration files.

SonicWall

In the web UI, go to **System > Settings > Export Settings** to export the settings file.

Sophos

Save the source configuration files on SFOS on page 77

Save the source configuration files on Cyberoam OS on page 78

Save the source configuration files on SG on page 78

Save the source configuration files on SFOS

1. In the web UI, go to **Backup & Firmware**.
2. Click **Import Export**.
3. Select **Export full configurations** in block **Export**.
4. Click **Export** and save the configuration file, which should be XML-formatted.

Please note that the Sophos backups are no longer xml format, it is encrypted now. This minor security enhancement was introduced since v17.5 MR4, April 2019.

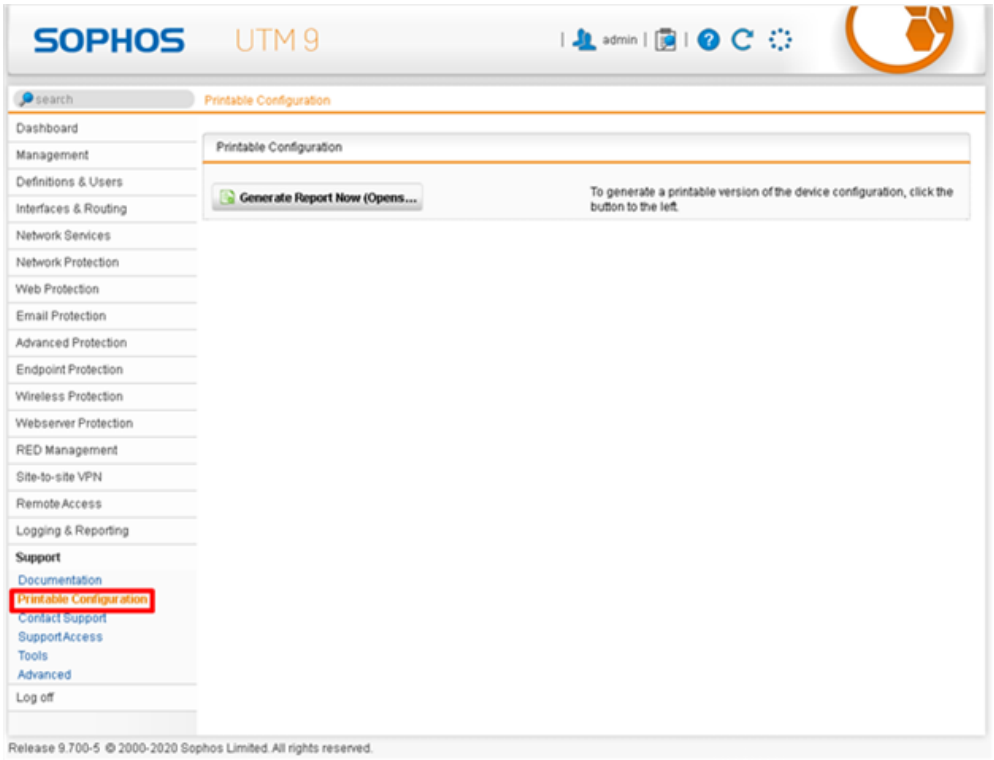
Save the source configuration files on Cyberoam OS

1. In the web UI, go to **System**.
2. Click **Maintenance**.
3. Click **Import Export** and save the configuration file, which should be XML-formatted.

Save the source configuration files on SG

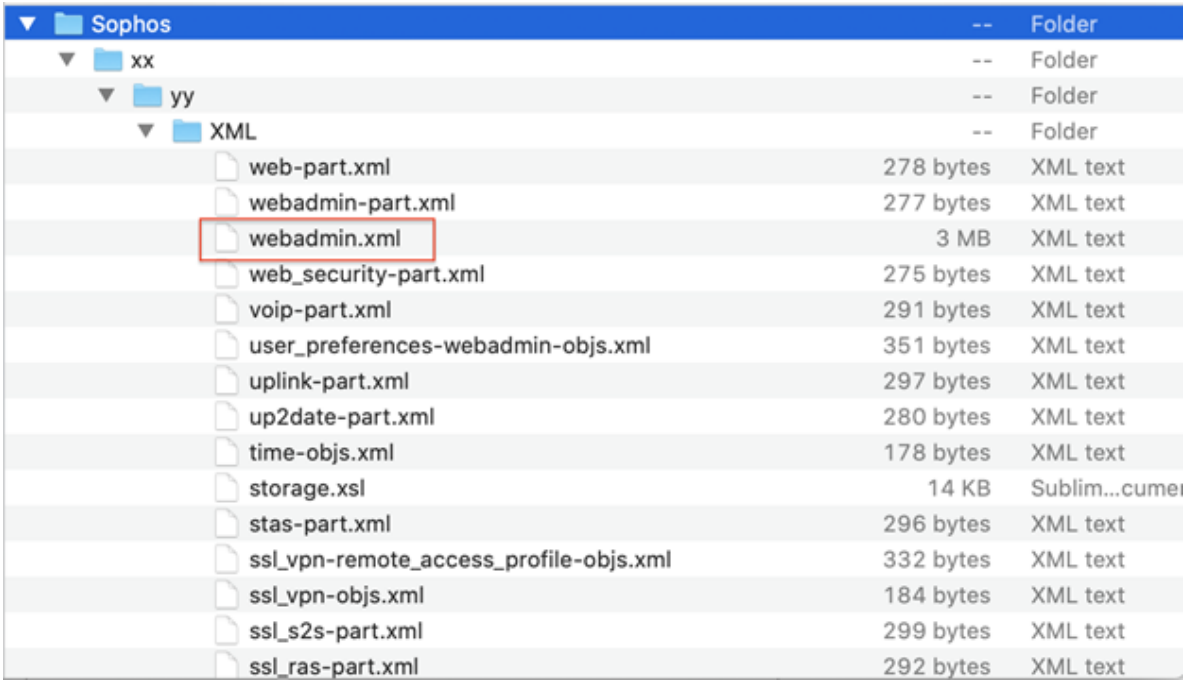
Option 1 (through WinSCP):

1. In **Webadmin**, open the printable configuration.



   Download a printable configuration from the GUI under **Support > Printable Configuration** on UTM 9 firewall.
2. Use WinSCP to connect to the FileSystem of your appliance using SSH.
3. Navigate to `/var/chroot-httpd/var/webadmin`
4. Create a new folder xx on your computer, and store all the necessary files. Create a subdirectory yy
5. Copy the folder "printable_configuration" into directory xx
6. On your appliance, move to the subfolder var (`/var/chroot-httpd/var/webadmin/var`). There you will find a directory with a cryptic name e.g.[:$]LIHKeSjlOjzQrjuMESn, double click on it.
7. Copy all the folders from that directory (downloads,objectcache,uploads,xml) to your local folder yy.

8. On your computer navigate in the folder ….xx\yy\xml\
9. Open webadmin.xml in a browser to access the offline configuration.
   (This process contains plain text passwords and pre-shared keys, please be mindful of it)



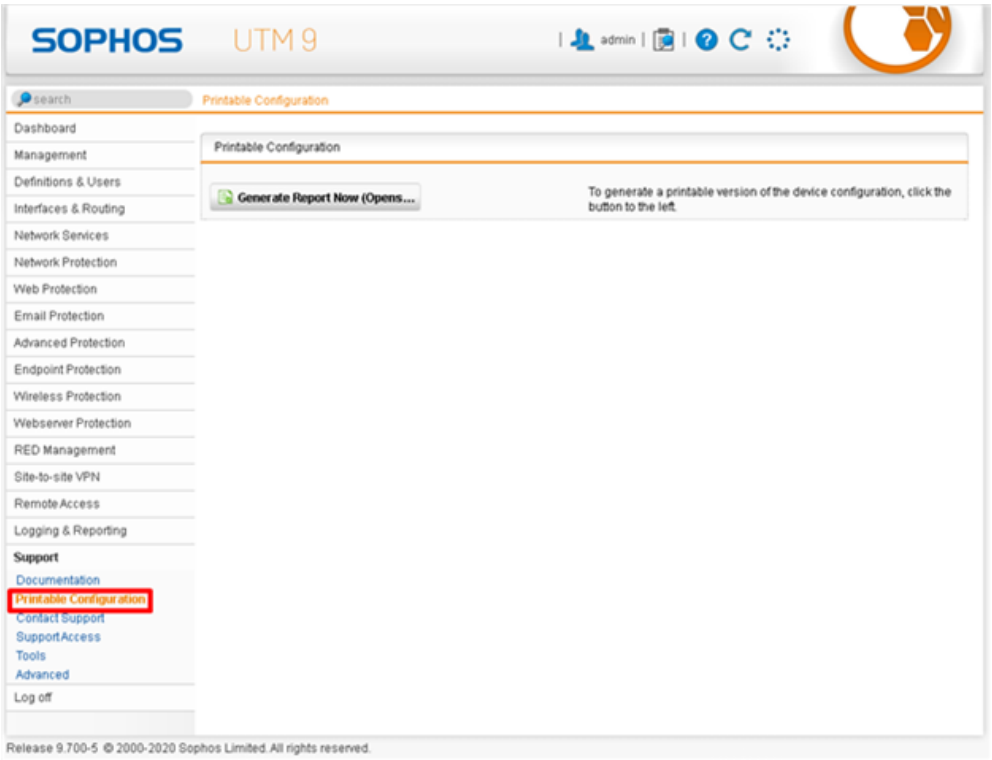
10. Use the file "webadmin.xml" as the input for the FortiConverter tool.

If you have any question, please kindly contact Sophos customer support.

Reference: https://community.sophos.com/utm-firewall/f/general-discussion/22706/howto-export-complete-printable-configuration

Option 2 (through SSH):

1. In **Webadmin**, open the printable configuration.



   Download a printable configuration from the GUI under **Support > Printable Configuration** on UTM 9 firewall.
2. Use **ssh** command to connect to the SG appliance, if the current login user is not "admin", you may consider to run "`su admin`" to obtain file system access permission.
3. Navigate to `/var/chroot-httpd/var/webadmin`
4. On your appliance, move to the subfolder var (`/var/chroot-httpd/var/webadmin/var`). There you will find a directory with a cryptic name e.g.[:$]LIHKeSjlOjzQrjuMESn, double click on it.
5. Run "`cat webadmin.xml`", then copy & paste the outputs into a text file.
6. Use the file as an input for the FortiConverter.

If you are using Putty to access the appliance, please enable logging to preserve all the outputs.

When you want putty to log all your session output, you have to change the default settings:

1. Open putty and go to **Session -> Logging**.
2. Select all session output and specify a log file.

Ubiquiti

Save the configuration from Ubiquiti

GUI: Access the **EdgeRouter** Web UI.

1. Navigate to the **System** tab in the bottom-left of the Web UI to download the backup configuration archive.
2. Go to **System > Configuration Management & Device Maintenance > Back Up Config**
3. Download the backup config file by clicking on the **Download** button.
4. The EdgeRouter will prompt you to save the .zip file archive on your computer.

For more information, please refer to:

https://help.ui.com/hc/en-us/articles/360044753453-EdgeRouter-Backing-Up-the-Config-Directory

Watch Guard

Save the configuration from Watch Guard

Use Policy Manager to download your configuration file.

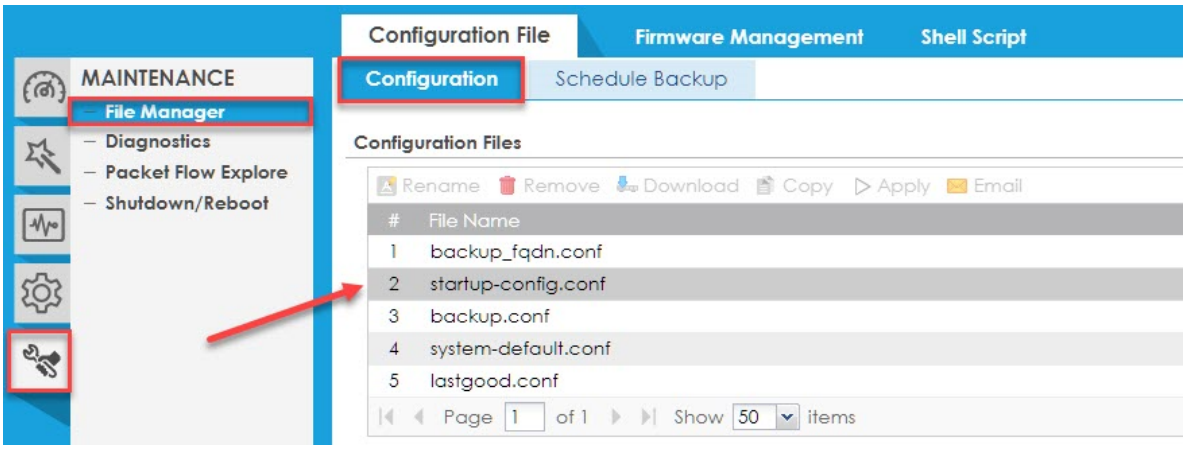
1. Select **File > Save > As File**.
2. Type the name of the file.
3. Click **Save**.

Zyxell

USG/ATP/VPN - Save the source configuration on Zyxell

Detailed instructions on where to find the current configuration and download it:

1. Log into the device and navigate to **Maintenance > File Manager > Configuration**.
2. The current configuration is saved on the device in the file named `startup-config.conf`



3. The configuration for the factory settings is saved under `system-default.conf`
4. The configuration can be downloaded via the **Download** button.