FortiConverter - Admin Guide

Version 7.4.0

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 4th, 2025
FortiConverter 7.4.0 Admin Guide
00-400-000000-20181031

TABLE OF CONTENTS

About FortiConverter

This content explains how to install and use FortiConverter.

FortiConverter helps you migrate your network to Fortinet network security solutions, significantly reducing workload and minimizing errors. FortiConverter translates configuration files from other vendors' firewall products into a valid FortiGate or FortiManager configuration file. Because the output uses command line syntax, it can either be uploaded as a configuration file or piped to the CLI.

For additional assistance, contact fconvert_feedback@fortinet.com.

Supported versions and conversions

FortiConverter can translate configurations from the following vendors and models. Unless noted as an exception below, conversions only support IPv4 unicast policy.

If FortiConverter cannot properly translate some of the supported configurations listed from below table, please kindly contact our product support email alias fconvert_feedback@fortinet.com

FortiGate Conversions

Vendor	Models	Versions	Convertible Objects
Alcatel-Lucent	Brick	ALSMS v9.x	• Interface (physical, logical, loopback, PPPoE) • Addresses & Address Books • Partitions • Services & Service Books • Static Routes • Zone rule set
Bluecoat	SGOS	6.5.10 6.6.4.2 6.7.4 7.0	• Addresses & Address Groups • Proxy Address (group) • Service • Proxy Policy
CheckPoint	SmartCenter	NGX R65 onward	• Interface • Addresses & Address Groups • Local Users & Groups • NAT • Negate Cell • Policies (rulebases.fws/*.csv) • RADIUS, TACACS+, LDAP • Rules (rulebases.fws/*.csv)

Vendor	Models	Versions	Convertible Objects
			• Schedules • Services & Service Groups • Static Routes • Traditional IPSec sito-to-site VPN (Support only before R80.10) • Simplified IPSec sito-to-site VPN
	VSX		
	Provider-1		
Cisco	ASA	7.x onward	• ACLs • Addresses & Address Groups • DHCP Servers • DNS Servers • Interface • IP Pools • Local Users & Groups • NAT (Central NAT) • RADIUS, TACACS+, LDAP • Services & Service Groups • Static Routes • VPN
	FWSM	3.x onward	
	IOS	10.x to 12.x	
		15.x	
	PIX	5.x onward	
	FTD (LINA)	6.x onward	
	IOS XR	4.x/5.x/6.x	• Addresses & Address Groups & FQDNs • Interface • IPPools • Policies • Services & Service Groups • Static Routes
	Nexus	5.2/6.x/7.x	
	Meraki	N/A	• Addresses & Address Groups • Interfaces • L3 firewall rules • NAT (Central NAT only)

Vendor	Models	Versions	Convertible Objects
			• Services & Service Groups
Forcepoint	Sidewinder	7.x onward	• Addresses & Address Groups & FQDNs • Interfaces • IP Pools • Policies • Services & Service Groups • Static Routes • NAT (Policy NAT only)
	Stonesoft	5.7 onward	• Addresses & Address Groups • Interfaces • Policies/ Sub-policy • Alias • Services & Service Groups • Static Routes • NAT
FortiGate	FortiOS	FOS5.2 and above	FortiGate configuration can be converted based on the version of the target FortiGate device. However, note that • Older features might be deprecated and may not be fully converted over. • The review is necessary. After importing the converted configuration, any CLI commands that have not successfully imported can be reviewed on the page. • For more details, please see "FortiGate configuration migration" section in the admin guide.
Huawei	USG Series		• Interface • Zone • Addresses & Address Groups • Services & Service Groups • Policy • Route • Zone • IPSec Policy (VPN) • Security Context • Nat Policy (SNAT) • Nat Server (VIP)

Vendor	Models	Versions	Convertible Objects
IBM	PAM		IPS Sensor
Ivanti		N/A	• Addresses • Services • User groups • Policies
Juniper	SSG/ISG	ScreenOS 4.x, 5.x, 6.x	• Addresses & Address Groups & FQDNs • DHCP Servers & Clients & Relays Interfaces • Static Routes • Services & Service Groups • Policies • VIPs/MIPs • NAT • IP Pools • VPN • Local Users & Groups • RADIUS & LDAP • Zones
	SRX	JunOS 10.x onward	• Addresses & Address Groups & FQDNs • DHCP Servers & Client & Relay • Interfaces • IP Pools • Local Users & Groups • NAT • Policies • RADIUS & LDAP • Services & Service Groups • Static Routes • VIPs/MIPs • VPN (IPSec site-to-site) • Zones • Routing-instances (virtual-router)
	MX	Juno OS 10.x to 12.x	• Addresses & Address Groups & FQDNs • Interfaces • IP Pools • Policies • Services & Service Groups • Static Routes

Vendor	Models	Versions	Convertible Objects
Open Systems			• Addresses & Address Groups • Services & Service Groups
Palo Alto Networks	PAN OS	PAN-OS 1.x onward	• Addresses & Address Groups & FQDNs • Interfaces • Local Users & Groups • NAT • Policies • Schedules • Static Routes • Services & Service Groups • Zones • VPN (GlobalProtect VPN not supported) • Panorama
PFSense		15+	• Addresses & Address Groups • Interfaces • NAT (Central NAT only) • Policies • Services & Service Groups • Static routes
Snort			IPS rules
SonicWall	TZ Series NSA Series	SonicOS 4.x onward	• Addresses & Address Groups & FQDNs • DHCP Servers & Clients & Relays • Interfaces • Local Users & Groups • NAT • Policies • Schedules • Services & Service Groups • Static Routes • Zones • VPN (IPSEC site to site) • SSLVPN
Sophos	XG Series	SFOS 17.0 - 17.5 MR3	• Interface • Zone • Addresses & Address Groups • Service & Service Groups • Users & User Groups • Policy • NAT (XG supports traditional

Vendor	Models	Versions	Convertible Objects
	Cyberoam	Cyberoam OS 10.6.3 onward	NAT merge and SG model supports central NAT mode only)
	SG Series	6.6 onward	
Tipping Point	IPS	4.5	• Addresses & Address Groups • Policies • Services & Service Groups
	Firewall	TOS v6.5x onward	• Interfaces and zones • Addresses and Address groups • Services • Policies • Static Routes • DHCP server & Relay • Application-list
Vytta	VyOS	5.2 to 6.7	• Interface • Zone • Addresses & Address Groups • Services & Service Groups • Policy • Route
WatchGuard	Firebox Series XTM Series	Fireware 11.3 onward	• Interfaces • Addresses & Address Groups • Services & Service Groups • Policies • Static Routes • IPSec VPN • NAT
Zscaler		N/A	• Addresses & Address Groups • Services

Exception

- Check Point to FGT conversion can support IPv4 multicast policy.
- Check Point, Cisco, and Juniper (Junos only) to FGT conversion can support IPv6 unicast policy.
- Bluecoat conversion supports FortiProxy mode which the generated CLI would be slightly different to FortiGate mode.

FortiADC conversions (Beta feature)

Vendor	Models	Versions	Convertible Objects
Citrix NetScaler	MPX/SDX/VPX	NS12.1	• Interface • Real servers • Pools
F5		N/A	• Nodes • Pools • Virtual addresses • Virtual servers • Server policies (FortiWeb only)
Radware	Alteon	30.x	• Real servers • Server groups • Virtual servers

General limitations

FortiConverter is a migration tool, not a migration service. It’s designed to be used as part of a properly planned migration process.

Supported FortiOS conversions

FortiConverter supports conversions from other vendors to FortiOS 6.4, 7.0, 7.2, 7.4 and 7.6.

Creating final configurations

While FortiConverter significantly shortens the conversion process, a final, useable configuration requires you to review and audit the FortiConverter output conversion. The FortiConverter tuning capability can help with the review and audit process.

While you can use the FortiConverter tuning capability to review and fix errors in the conversion, it isn't designed to perform significant reconfiguration.

Incomplete routing information

In some cases, not all routing information that FortiConverter requires to make a decision about a policy interface is available. In these cases, it uses the **any** interface.

IPsec support

FortiConverter converts IPsec configurations to route-based or policy-based IPsec depending on which one the source configuration is closest to. Users can enable Route-based IPSec for Cisco ASA, PIX,FWSM, Juniper and Check Point conversions.

Licensing

The trial version of FortiConverter, allows you to complete a conversion and view the results in the Tuning page. CLI output is disabled, but is available in the fully-licensed version.

When you purchase a license, FortiConverter is unlocked and full functionality is enabled for all supported vendors. Your paid license entitles you to any new versions of FortiConverter that Fortinet releases until the license expires, as well as direct engineering support.

FortiConverter requires an Internet connection to verify its license. You can use the software for up to 30 days without validating the license online.

For more information, see Activating the license on page 21.

What's new

This release contains the following new features and enhancements:

- Updated the front end which is implemented by React.
- Supported the conversion of Open Systems firewalls.

Installation

Download the FortiConverter installer from the Fortinet Technical Support website:
https://support.fortinet.com

To install the FortiConverter application

1. Double-click the FortiConverter installer (.py.exe).
2. Click **Next**.
3. Read the license agreement, select **I accept the terms of the License Agreement**, then click **Next**.
4. Select settings if needed, and then click **Next**.

Setting	Description
Enable HTTPS	Use HTTPS instead of HTTP to communicate between the browser and the FortiConverter application.
Clear all history conversions	Delete all previous conversions and logs before installation starts.
Browse	This button has been disabled, which only allows FortiConverter to be installed at the path **C:\Program Files\Fortinet\FortiConverter**. This prevents non-administrator users modifying files in FortiConverter, which may cause some security issues.

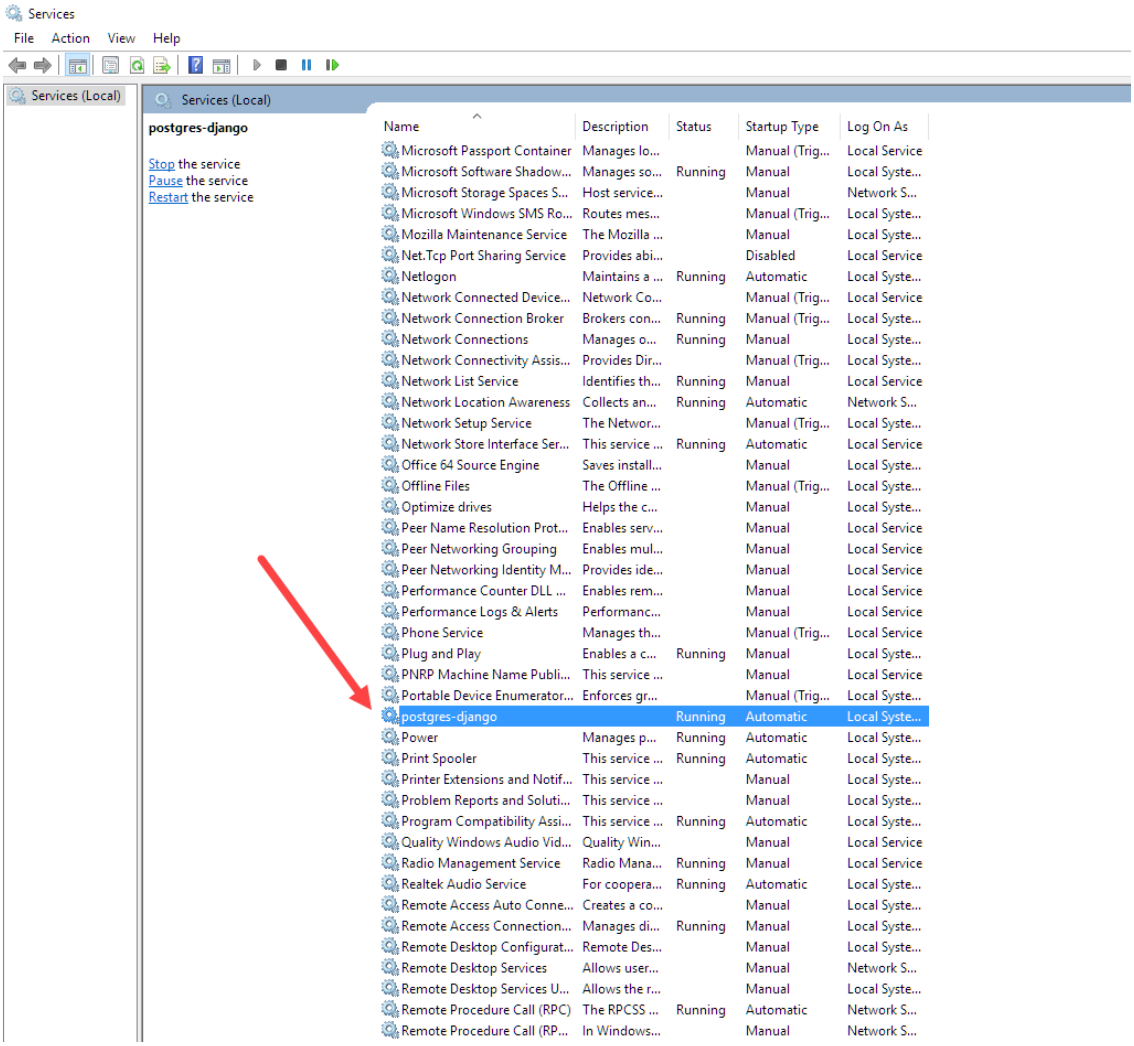
5. Click **Finish** to complete and exit the FortiConverter installer.

To completely remove FortiConverter application and data

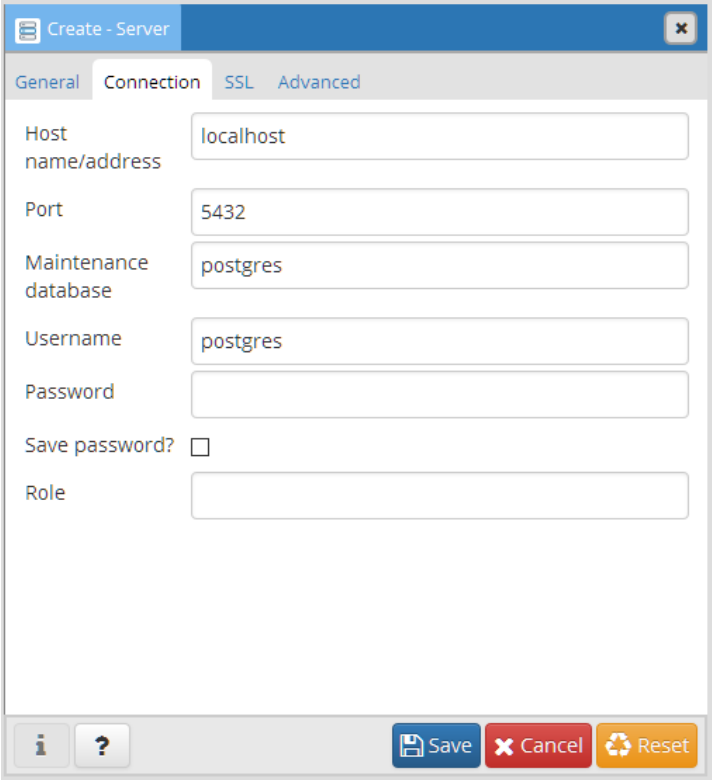
Uninstalling FortiConverter application from Windows only removes the application itself, it does not remove the conversion data or database. If you re-install the application later, the data can still be accessed.

To remove all conversion data

1. Stop the FortiConverter application.
2. Restart your local PostgreSQL database service.
   a. Open your Services desktop application.
   b. Right-click the service name **postgres-django**, and select **Restart**.



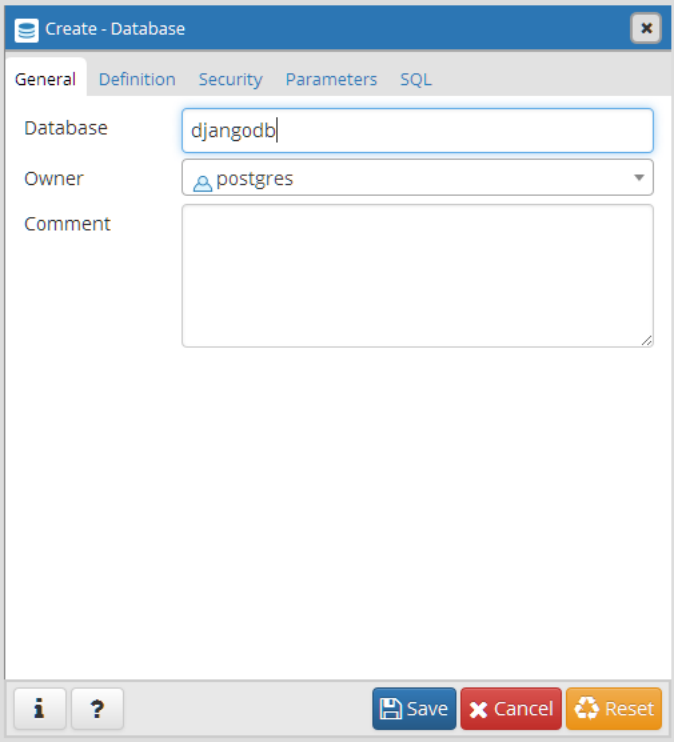
3. Install the latest version of pgAdmin 4, which can be downloaded at https://www.pgadmin.org/.
4. Using pgAdmin 4, create a server record.
   - Go to **Object > Create > Server**.
5. Set both the username and password to "postgres".



6. Open the newly created service record, right-click the database "djangodb", and select **Delete/Drop**.
7. Click **OK**.
8. If you receive the error message: "there is 1 other session xxx", terminate all other existing external connections, except for the connection from pgAdmin 4.
   a. Make sure FortiConverter has been stopped.
   b. Click the "djangodb" database.
   c. Go to **Tools > Query Tool**, then enter the following PSQL script.

```
SELECT
   pg_terminate_backend(pid)
FROM
   pg_stat_activity
WHERE--
   don't kill my own connection!
   pid <> pg_backend_pid()
   -- don't kill the connections to other databases
   AND datname = 'djangodb';
```

   d. Click **Execute**.
9. Restart the pgAdmin 4 tool, and drop "djangodb" again, if available.
10. Re-create a database with the name "djangodb" by going to **Object > Create > Database** .
11. Click **Save**.



12. Delete all existing conversion folders to avoid a name conflict.Conversions are, by default, stored at `C:\Users\<UserName>\AppData\Roaming\Fortinet\FortiConverter\conversions`.
13. Uninstall the program.
14. Delete all remaining files and folders in the FortiConverter folder, located at `C:\Program Files\Fortinet\FortiConverter`.

System requirements

FortiConverter requires one of the following Microsoft Windows 64-bit platforms:

- Microsoft Windows 11
- Microsoft Windows 10
- Microsoft Windows 8
- Microsoft Windows Server 2022
- Microsoft Windows Server 2019

- Microsoft Windows Server 2016
- Microsoft Windows Server 2012

A web browser is required.

An Internet connection is required to periodically verify the software license.

For any questions not covered in this content, contact FortiConverter customer support at fconvert_feedback@fortinet.com.

Activating the license

By default, FortiConverter is installed with a limited trial license. If you have purchased a full license, download it to unlock the complete feature set.

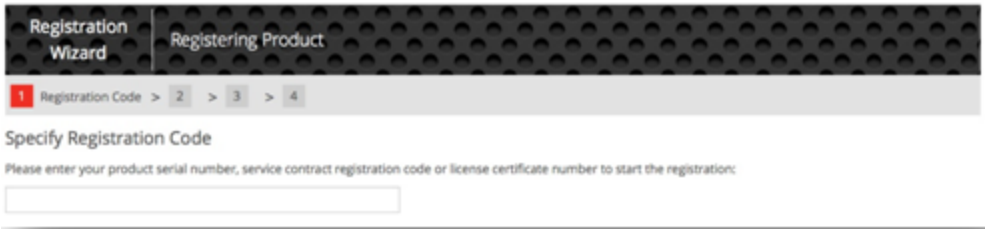
To purchase a license, use your usual Fortinet sales channel. For other licensing issues, see Licensing for more information.

If you have already activated a license for the legacy FortiConverter application on your device, the new application automatically uses that license when it's installed.

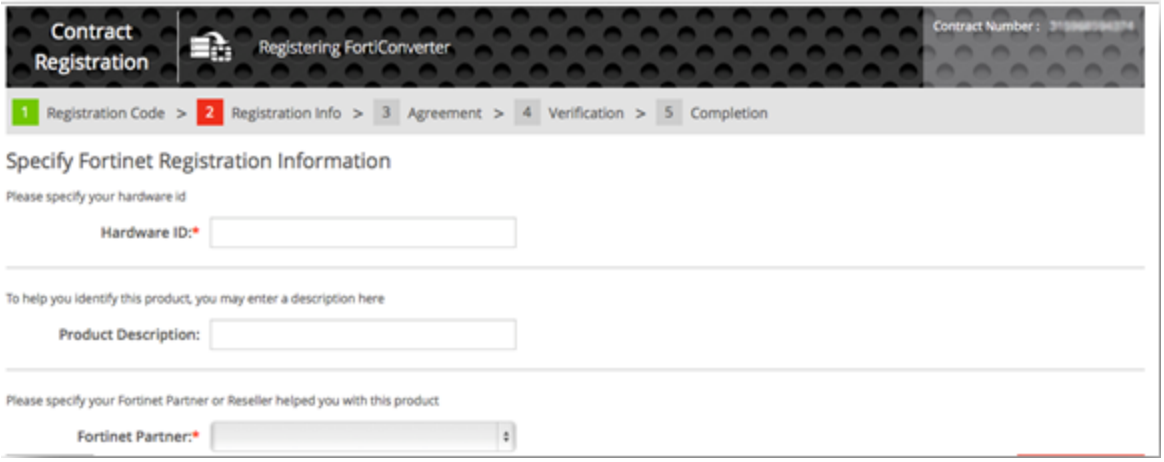
To activate the license

1. Double-click the FortiConverter shortcut.
2. Click **License**.
3. Copy the **Hardware ID** value to the clipboard.

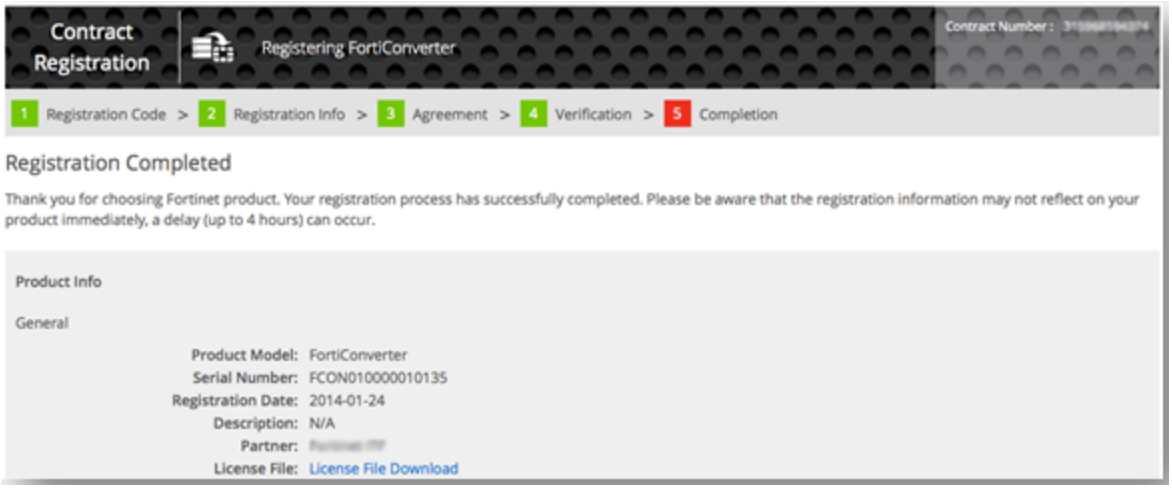
4. Ensure you have purchased a license, then sign in to the Fortinet Technical Support web site: https://support.fortinet.com/
   Registration uses a simple, four-step wizard that is commonly used for many Fortinet products.
5. On the first page of the wizard, enter the registration code you received when you purchased your FortiConverter product.



6. Enter the **Hardware ID** you copied earlier, an optional description, and choose your Fortinet partner from the list.



7. After you agree to the license terms, the final page of the wizard allows you to download the license file (.lic file).



8. In FortiConverter, from the **License** tab, click the icon next to **License File**, then navigate and select the .lic file.
9. Click **Activate**.
   FortiConverter validates the license file and changes your **Activation Status** from **Trial** to **Activate**. Your license is valid for all FortiConverter software updates released until the date specified by **License Expiry**

Date.After the license is activated, the expiry information is under the **License** tab.

Enabling remote connections

FortiConverter is designed as a web application. The application (FortiConverter.py) should be run with Administrator privileges because it reads and writes data from/to high privilege directories. For security concerns, the default configuration only allows connections from users on the localhost.

To enable remote access to the web application

1. Run notepad as an administrator and open the `start.bat` file located in the directory `C:\Program Files\Fortinet\FortiConverter\`.
2. Update the value of --host to 0.0.0.0 (the port change is optional).
   For example:
   ```
   call "%install_dir%\Python36\python.exe" start.py --host 0.0.0.0 --port
   8000
   ```
3. Run notepad.exe as an administrator and open `C:\Program Files\Fortinet\FortiConverter\converter\backend\mysite\mysite\settings.py`
4. Add the wildcard IP address **'*'** (match ANY) into allowed ALLOWED_HOSTS.
   For example:
   ```
   ALLOWED_HOSTS = [
      'localhost','127.0.0.1','*',
   ]
   ```

Run FortiConverter on different Windows users

From FortiConverter v6.0.1, you are able to run the FortiConverter as different Windows users of the same host.

Each user has an individual conversion list.

As long as a user with administrator privileges on the host installs the FortiConverter tool, all users including the standard users can run FortiConverter.

About PostgreSQL Version Upgrade

The FortiConverter version 7.0.6 upgrades from PostgreSQL version 16.2 to 16.4.

Please carefully examine the following before upgrading to FortiConverter 7.0.6 and above or rollback to an older version:

FortiConverter Installation Direction	PostgreSQL Database Data Migration
Upgrading FortiConverter from version 7.0.5 or above to the current version	The old conversion data will still be **preserved** and **accessible** in the new version's PostgreSQL database.
Upgrading FortiConverter from version 6.0.2 or above to the current version	The old conversion data **will be automatically migrated** to the new version's PostgreSQL database.
Upgrading FortiConverter from version 6.0.1 or below to the current version	The old conversion data **will not be migrated** to the new version's PostgreSQL database. There are too many differences between 6.0.1 and 7.0.6 so it would be better to redo the conversions with the current version. However, if the old data should be preserved, please first upgrade to a version between 6.0.2 and 7.0.4, and then upgrade to the current version.
Downgrade FortiConverter from the current version to version 7.0.4 or below	The new conversion data completed in the current version **will not be migrated back** to the older version's PostgreSQL database
Downgrade FortiConverter from the current version to version 7.0.5 or above	Please **first run the uninstaller on the existing build** and then install the older build. The conversions data of the existing build should still be **preserved and accessible** in PostgreSQL database after the installation.

- **If** you encountered a bug during the data migration, or for some other reason **you do not want to migrate the data**, please check the "**Clear all history conversion**" option during installing. This will skip the migration process and install a clean database instead.

If any additional assistance is required, Please contact fconvert_feedback@fortinet.com and send us the log file located in `C:\ProgramData\Fortinet\ForiConverter\temp\install.log`

Resolve PostgreSQL CVEs

Background

FortiConverter v7.0.3 GA release comes with PostgreSQL version v12.16, and these CVEs are detected with PostgresSQL v12.16 by FortiClient:

```
PostgreSQL CVE-2023-5869 Buffer Overflow Vulnerability
PostgreSQL CVE-2023-5868 Information Disclosure Vulnerability
PostgreSQL CVE-2023-5870 Denial of Service Vulnerability
```

FortiConverter application uses an embedded version of PostgreSQL.

Data folder: C:\ProgramData\Fortinet\PostgreSQL\12

Binary folder: C:\Program Files\Fortinet\FortiConverter\pgsql12

Precondition

You have FortiConverter v7.0.3 or earlier version installed.

Your FortiClient reported a high CVE risk and requires to upgrade to v12.17 or v15.5.

Solution 1: Upgrade to PostgreSQL v12.17

Upgrade to FortiConverter v7.0.4 patch release.

Then download and install the latest GA release v7.0.4 from Fortinet support portal.

Solution 2: Upgrade to PostgreSQL v15.5

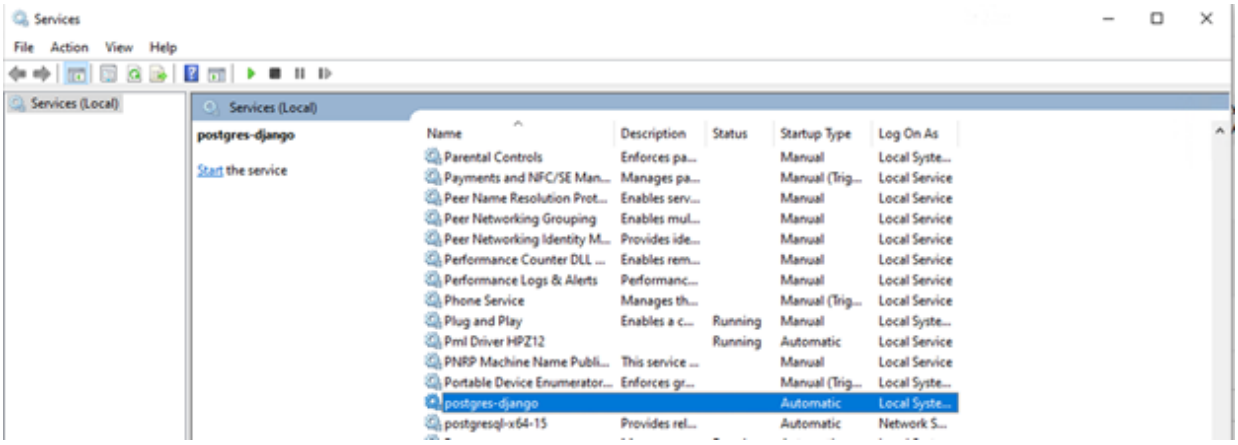
Currently FortiConverter still comes with PostgreSQL v12.x by default since upgrade to PostgreSQL v15.x requires data migration process.

If you would like to upgrade to a newer version of PostgreSQ, such as version 15.5, follow the steps below to complete the transition by installing a standalone version of PostgreSQL.

After the database transition, all previous/historical conversions will disappear.

Step 1 - Stop Postgres Services

1. Go to **Windows > Services** on your local computer and stop all the Postgres services.
2. The service named "postgres-django" was installed by FortiConverter application. Right click to stop this service.



Step 2 - Delete Binary Folder

After the service "postgres-django" is stopped , delete the binary folder "`C:\Program Files\Fortinet\FortiConverter\pgsql12`".

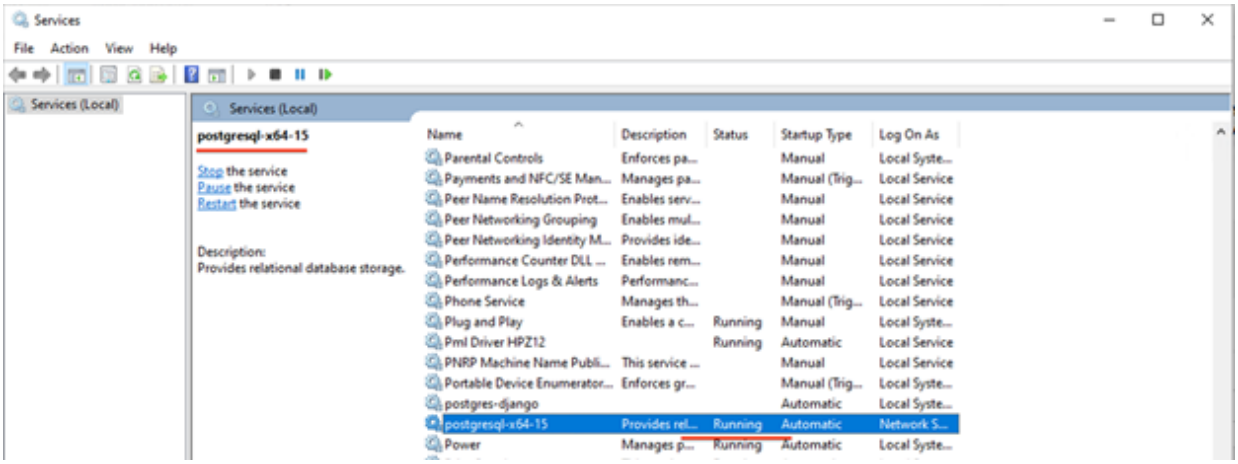
Step 3 - Download and Install New PostgreSQL

Download and install PostgreSQL 15.5-1 release from the EDB official site.

Step 4 - Check New PostgreSQL Status

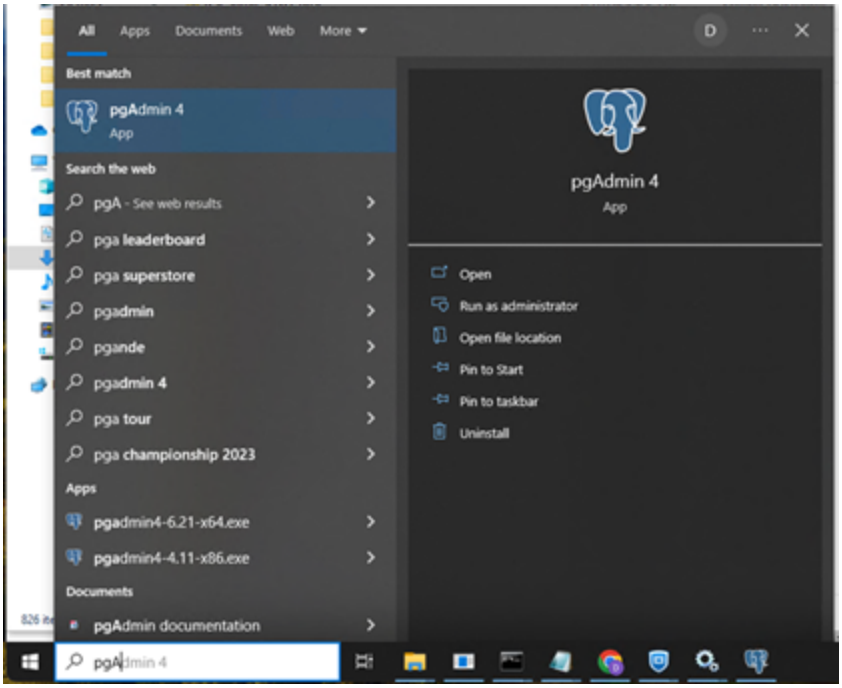
After the installation, double check if the new version of PostgreSQL v15.5 is running.

Go to **Windows > Services** again, make sure the service status is **Running**.



Step 5 - Run "pgAdmin4"

Run the "`pgAdmin 4`" application from your local computer.



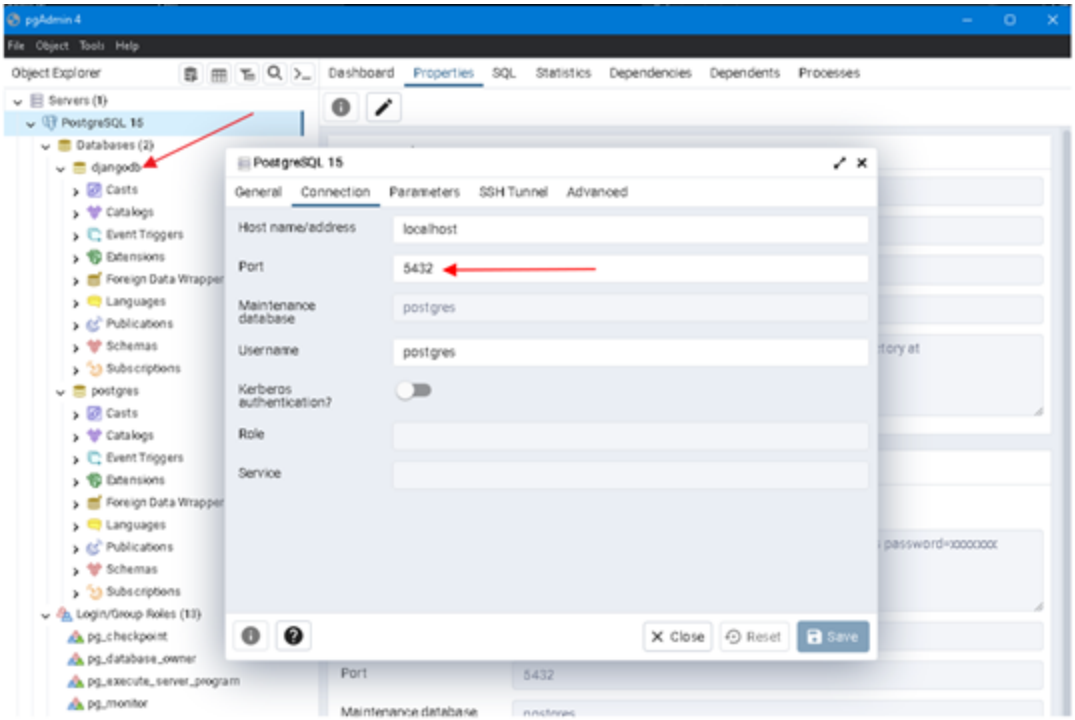
Step 6 - Check PostgreSQL Configurations

Connect to the server, right click over PostgreSQL 15 and make sure the configurations as following:

- username: postgres
- password: postgres
- server listening on localhost 5432

Step 7 - Create An Empty Database

Create an empty database named: djangodb



Step 8 - Correct the Python File Path

1. Open the windows command prompt.
2. Enter - > `cd "C:\Program Files\Fortinet\FortiConverter"`
3. Run -> more migrate.bat to display the migration scripts.
4. Copy the outputs from the above command and paste into a text editor.
5. Replace the 3rd line with below:
   `cd "%install_dir%\converter\backend\mysite"`
6. Replace the "`python.exe`" file path:

```
@echo on
set install_dir=%cd%
cd "%install_dir%\converter\backend\mysite"

"%~1\Python311\python.exe" manage.py migrate auth
"%~1\Python311\python.exe" manage.py migrate contenttypes
"%~1\Python311\python.exe" manage.py migrate bluecoat 0012_bcwarningtabs_referenced
"%~1\Python311\python.exe" manage.py migrate checkpoint 0033_auto_20231208_1730
"%~1\Python311\python.exe" manage.py migrate cisco 0066_ciscosnmpserver
"%~1\Python311\python.exe" manage.py migrate conversion 0020_auto_20230630_0208
"%~1\Python311\python.exe" manage.py migrate converter 0196_proxyaddrgrp_comment
"%~1\Python311\python.exe" manage.py migrate f5 0001_initial
"%~1\Python311\python.exe" manage.py migrate fileupload 0003_auto_20200113_0035
"%~1\Python311\python.exe" manage.py migrate forcepoint 0012_auto_20230714_1345
"%~1\Python311\python.exe" manage.py migrate fortigate 0001_initial
"%~1\Python311\python.exe" manage.py migrate homepage 0001_initial
"%~1\Python311\python.exe" manage.py migrate huawei 0019_hwinterface_eth_trunk
"%~1\Python311\python.exe" manage.py migrate ibm 0004_ibmrule_is_duplicate
"%~1\Python311\python.exe" manage.py migrate junos 0025_josifrange_disable
"%~1\Python311\python.exe" manage.py migrate screenos 0008_auto_20220815_1655
"%~1\Python311\python.exe" manage.py migrate license 0001_initial
"%~1\Python311\python.exe" manage.py migrate lucent 0002_alter_brickstaticroute_is_valid
"%~1\Python311\python.exe" manage.py migrate mcafee 0009_ipsec

Find: "%~1\\Python311\\python.exe"
Replace: call "%install_dir%\\Python311\\python.exe"
```

Step 9 - Run the Migration Script

1. Paste the rectified batch scripts into a Windows command prompt.
2. These scripts will create data tables for the FortiConverter database "djangodb".
   Alternatively, you can also save these scripts into a bat file and run the scripts from the command prompt. Make sure the execution path is "`C:\Program Files\Fortinet\FortiConverter`".

```
Command Prompt - call "C:\Program Files\Fortinet\FortiConverter\Python311\python.exe" manage.py runserver --insecure - call "C:\Program Files\Fortinet\FortiConverter...
c:\Program Files\Fortinet\FortiConverter>
c:\Program Files\Fortinet\FortiConverter>
c:\Program Files\Fortinet\FortiConverter>
c:\Program Files\Fortinet\FortiConverter>
c:\Program Files\Fortinet\FortiConverter>@echo on

c:\Program Files\Fortinet\FortiConverter>set install_dir=%cd%

c:\Program Files\Fortinet\FortiConverter>cd "%install_dir%\converter\backend\mysite"

c:\Program Files\Fortinet\FortiConverter\converter\backend\mysite>
c:\Program Files\Fortinet\FortiConverter\converter\backend\mysite>call "%install_dir%\Python311\python.exe" manage.py migrate auth
Operations to perform:
  Apply all migrations: auth
Running migrations:
  No migrations to apply.

c:\Program Files\Fortinet\FortiConverter\converter\backend\mysite>call "%install_dir%\Python311\python.exe" manage.py migrate contentt
ypes
Operations to perform:
  Apply all migrations: contenttypes
Running migrations:
  No migrations to apply.

c:\Program Files\Fortinet\FortiConverter\converter\backend\mysite>call "%install_dir%\Python311\python.exe" manage.py migrate bluecoat
 0012_bcwarningtabs_referenced
Operations to perform:
  Target specific migration: 0012_bcwarningtabs_referenced, from bluecoat
Running migrations:
  No migrations to apply.

c:\Program Files\Fortinet\FortiConverter\converter\backend\mysite>call "%install_dir%\Python311\python.exe" manage.py migrate checkpoi
nt 0033_auto_20231208_1730
Operations to perform:
  Target specific migration: 0033_auto_20231208_1730, from checkpoint
Running migrations:
  No migrations to apply.

c:\Program Files\Fortinet\FortiConverter\converter\backend\mysite>call "%install_dir%\Python311\python.exe" manage.py migrate cisco 00
66_ciscosnmpserver
```

Step 10 - Update FortiConverter Binaries

After PostgreSQL is updated to version 15.5, the FortiConverter application's binaries also need to be manually updated to accommodate the new version.

Copy the binaries below from the newly installed PostgreSQL 15.5 folder:

From folder:

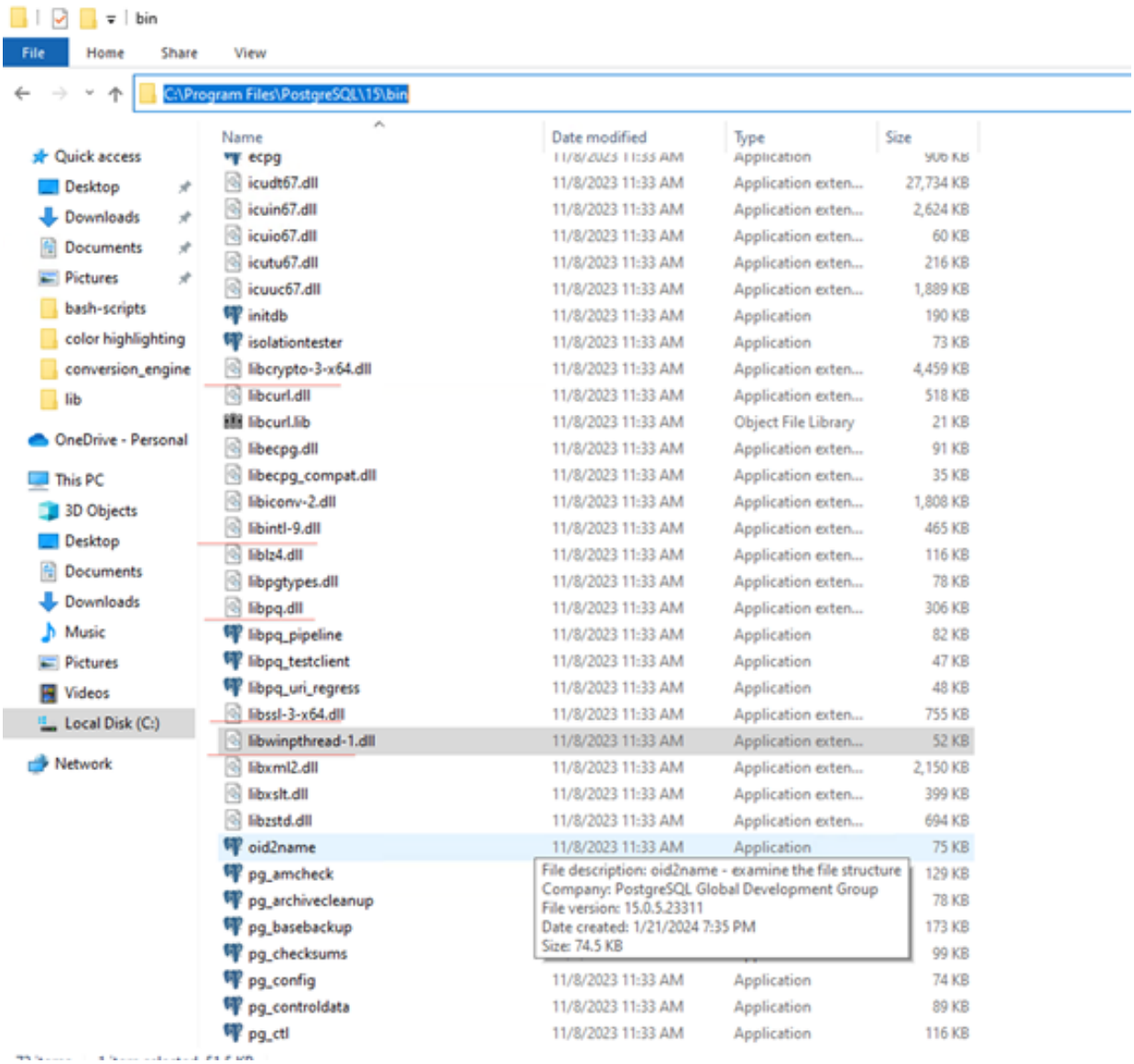
```
C:\Program Files\PostgreSQL\15\bin
```

To folder:

```
C:\Program Files\Fortinet\FortiConverter\converter\backend\mysite\conversion_engine
```

Binary file list:

```
Libcrypto-3-x64.dll
Libintl-9.dll
Libpq.dll
Libssl-3-x64.dll
Libwinpthread-1.dll
```



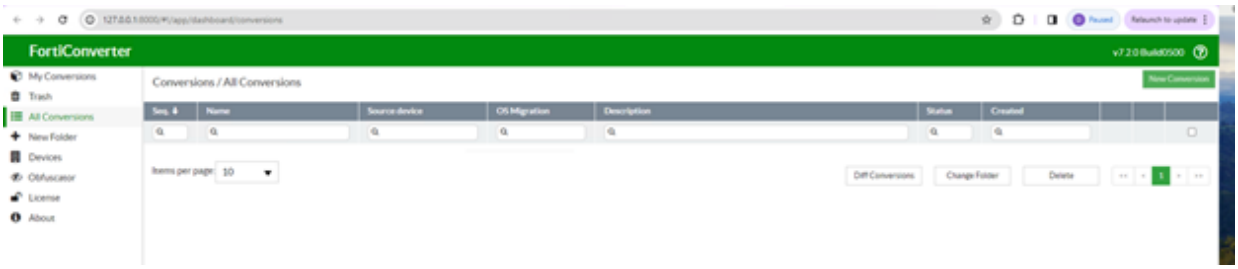
Step 11 - Test FortiConverter

Test and run the FortiConverter application from your desktop.

The previous conversions should no longer be there after the migration.

Now your FortiConverter application is running with a standalone PostgreSQL v15.5.

The default data folder is changed to: "`C:\Program Files\PostgreSQL\15\data`".

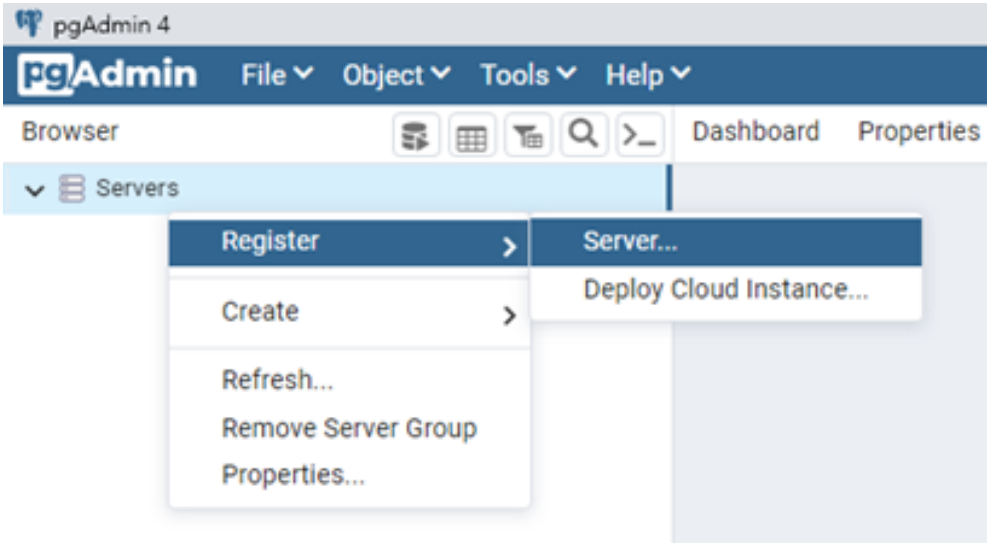


Backup and Restore History Conversions

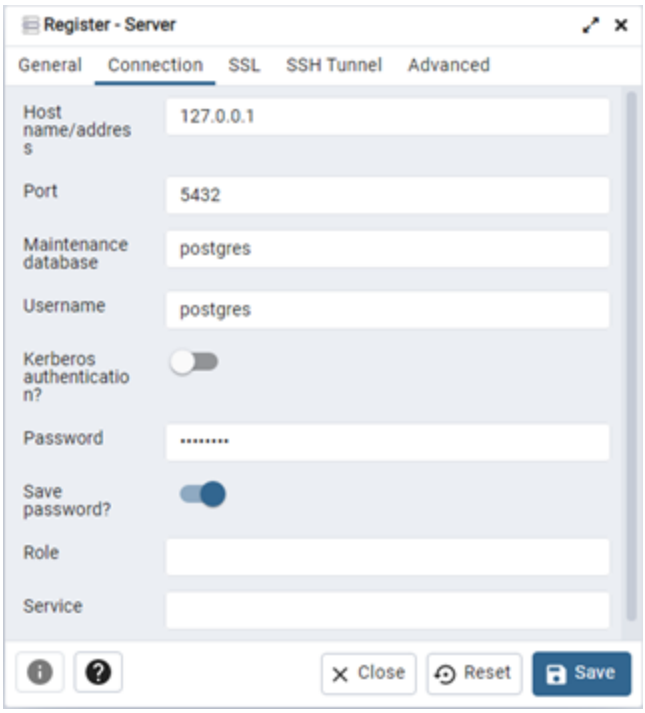
Please follow the steps below if you need to back up your history conversions and restore them to another computer.

Backup

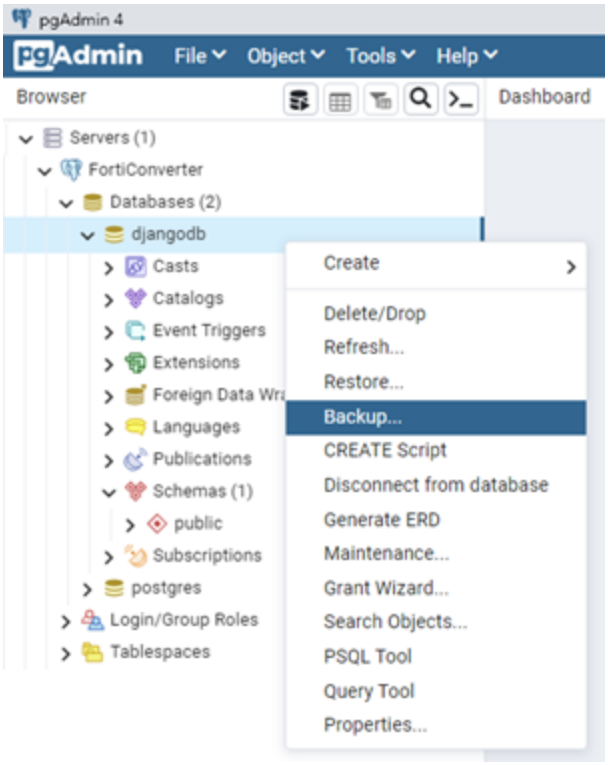
1. Install the latest version of pgAdmin 4, which can be downloaded at https://www.pgadmin.org/.
2. Right click on **Servers** and select **Register > Server** to connect to the database of FortiConverter:



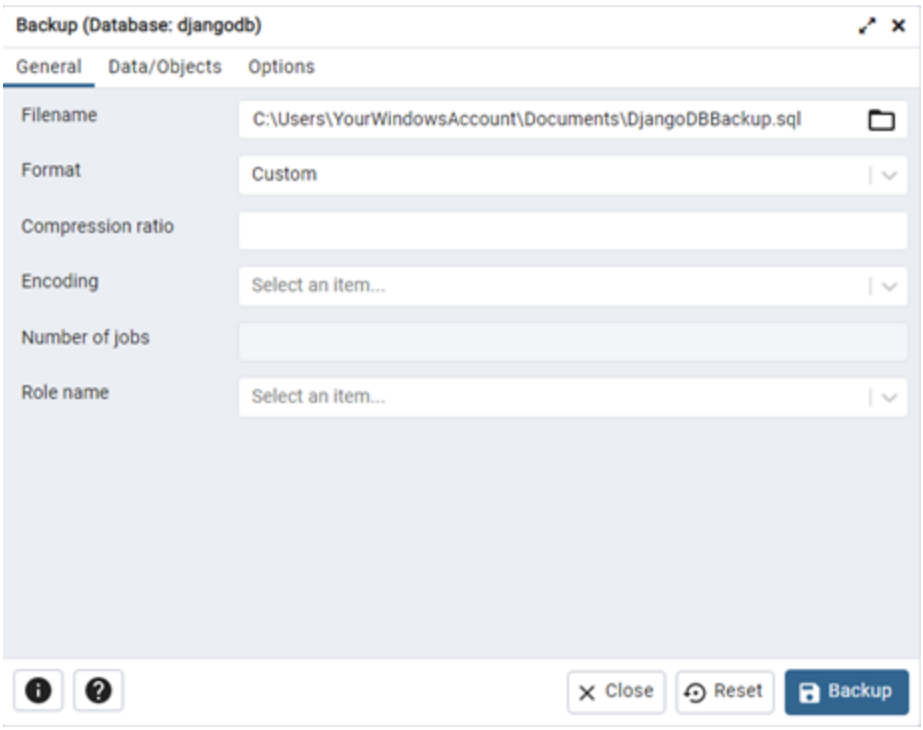
3. Input a name the server in tab **General**, click on tab **Connection** and input the following information:
   a. **Host name/address**:"127.0.0.1" (or “localhost”)
   b. **Username**: "postgres"
   c. **Password**: "portgres"
   d. Click **Save**.



4. Open the server, right-click on the database **django** and select **Backup…**:



5. Select a path in **Filename** and click **Backup**:

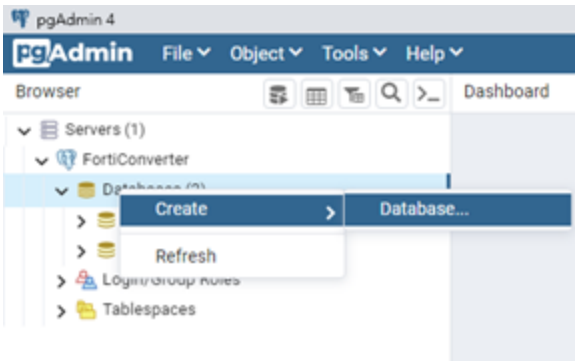


The backup file, which will be referred as **database backup file**, would be saved to the specified path.

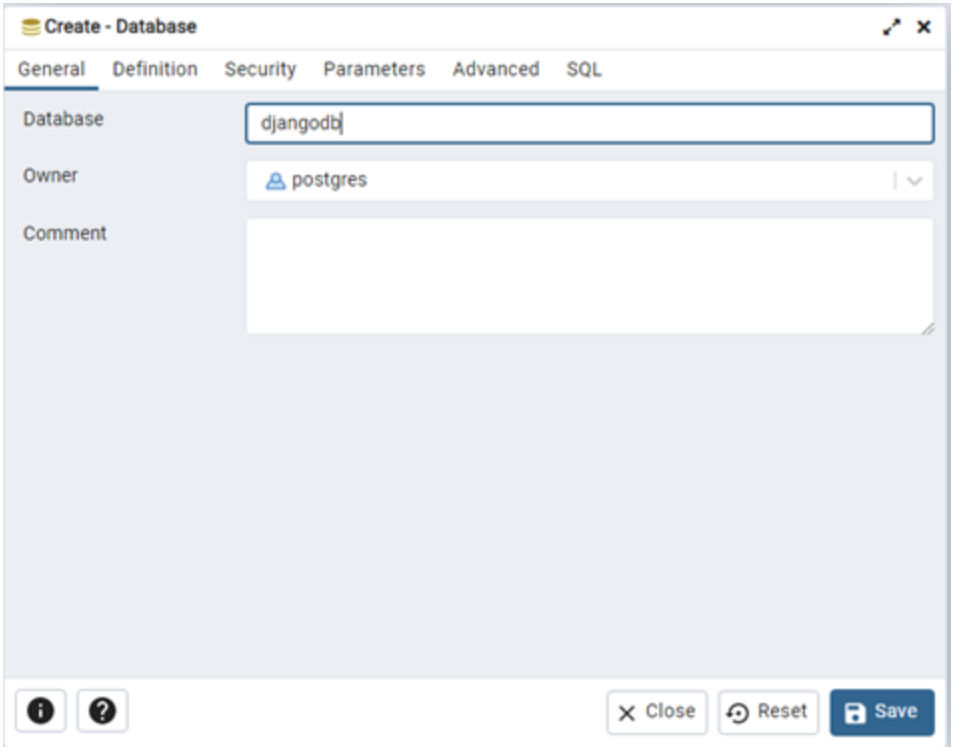
6. Go to path and backup all the folders, which will be referred as **conversion backup files**:
   `C:\Users\<Windows user name>\AppData\Roaming\Fortinet\FortiConverter\conversions`

Restore

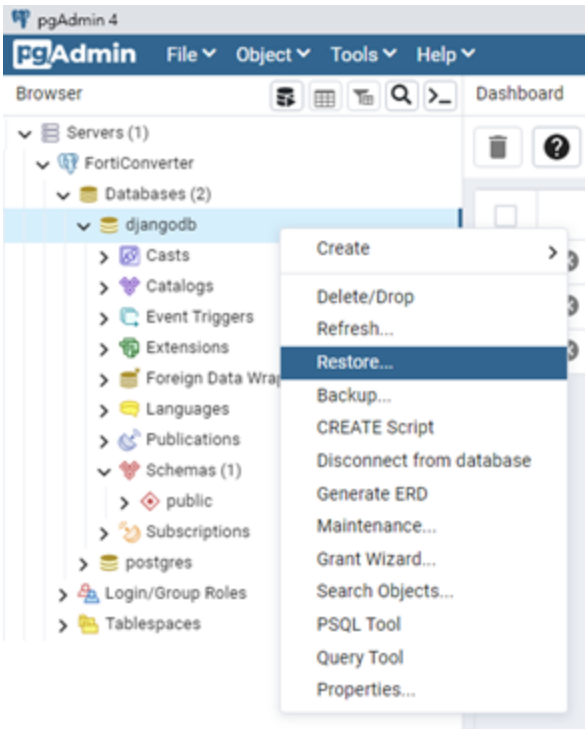
1. Move the **database backup file** and the **conversion backup files** to the computer you would like to restore FortiConverter.
2. Install **the same version of FortiConverter as the old computer** on the new one. Please do not do any conversion on FortiConverter before restoring the data.
3. Follow the same process in the backup steps to install pgAdmin and connect to the database of FortiConverter.
4. Open the server, right-click the database **djangodb** and select "Delete/Drop" to delete **djangodb**.
5. Right click on the database server of FortiConverter and select **Create > Database**.



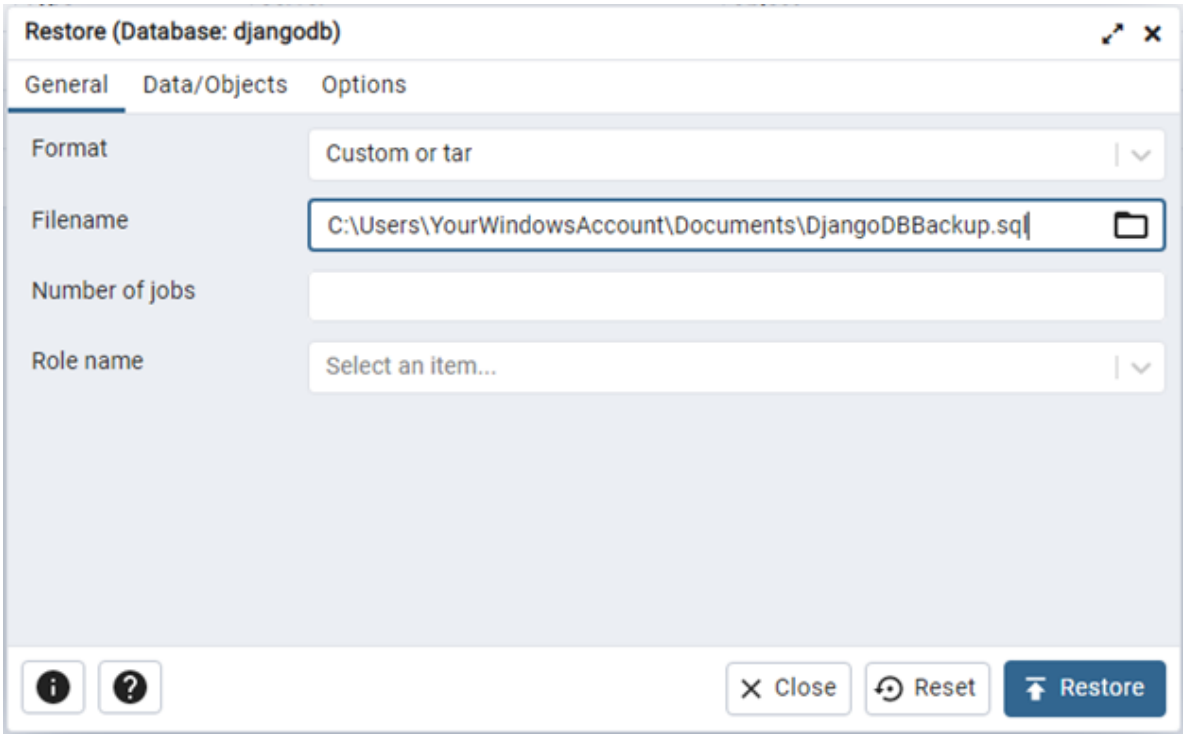
6. Input "djangodb" as the database name and click **Save** to recreate it.



7. Right click on **djangodb**, select **Restore**.



8. Select the path of the **database backup file** retrieved from the **Backup** process above, and click **Restore**:



9. Install the version of FortiConverter you want.
10. Go to path `C:\Users\<Windows user name>\AppData\Roaming\Fortinet\FortiConverter\conversions` and copy the **conversion backup files** into this folder.

11. Open FortiConverter, and the backup conversions should be accessible on the conversion page.

FortiGate Configuration Migration

To perform the FortiGate migration, you need to provide two input configurations: the source, and the default target device configuration. After running the conversion and proceed to the summary page, you can download the converted configuration and upload it to the device.

Fortinet Conversion Wizard

1. Start the FortiConverter. When the start-up is complete, a browser window automatically opens to http://127.0.0.1:8000.
2. At the top-right corner of the window, click **New Conversion**.
3. Enter the name for the conversion configuration.
4. Select **Fortinet** block from the below.
5. Click **OK**.

The page turns to the **Start page**.

Requirements

Configurations that are removed by default

Configurations that may block device-accessing can be removed by FortiConverter, you might need to configure these settings manually after the configuration restoration. The settings you should check on are:

- The administrator password
- The IP of interface "mgmt"
- The "accprofile" setting of administrators
- The "trusthost" setting of administrators

To preserve the administrator password and trusthosts, please enable the option **Preserve default admin user password and trusthost settings** at the start page.

For FortiGate conversion, the default admin account settings may be overwritten after the configuration restoration. For example, if the old FortiGate set the default admin access to disabled, you should temporarily enable this admin access before the restoration.

```
config system global
   set admin-maintainer enable
end
```

VDOM mode migration

If the source config has VDOM mode enabled, please also enable the VDOM mode on the target device and create all the user-defined VDOMs which you want to migrate on the target device with the same names. Then use the config backup as the target default config. As a result, both the source config and the target default config will contain the titles "config global" and "config vdom".

Transparent mode

```
#config-version=FGT60E-6.0.10-FW-build0365-200617:opmode=0:vdom=0:user=admin
```

The "**opmode=0**" in the configuration header does not affect the setting on the FortiGate.

If you want to change the opmode to transparent mode, you should add the CLI below.

```
config system settings
     set opmode transparent
     set manageip 172.23.1.111/255.255.255.0
end
```

FortiConverter does not change these CLI during the conversion. If the source configuration has been set to the transparent mode, then, it'll keep this settings in the configuration after the conversion.

The conversion output consists of two main parts:

1. The first part is the default configuration of the target device.
2. The second part starts with the commented out line "#migrated config starts", and follows with the migrated source configuration.

If you want to modify the output config manually, we suggest you modify only the second part because the definition from the first part will be overwritten by the following definition.

Importing output configuration into FortiGate

Please follow the steps in this video:
https://youtu.be/UBjSE-Kb9EM?t=2220

Fortinet Start Options

Setting	Description
Profile	
Description	Enter a description of the conversion.
Input	
Config mode change	Enable this option if you only need to convert the config from one mode to another mode instead of migrating the config into another device. When this option is enabled, only the source configuration needs to be input. Currently, 2 kinds of mode conversions are supported: 1. Policy mode to Profile mode conversion. 2. Interface Split conversion
Source Configuration	Select the input configuration file or a device.
Target Device Default Configuration	FortiConverter needs the default configuration of the target device to extract interface or other information of the target device. The default configuration should contain the same VDOM as those in the source config. So if the source device contains multiple VDOMs, users should also create VDOMs with the same name on the target device before back up the default configuration.
Migrate SSL VPN to IPsec VPN	Enable this option if you need to migrate the source config's SSL VPN into IPsec VPN. When this option is enabled, only the source configuration needs to be provided.
Conversion Options	
Append new object to avoid overwriting existing one	Enable this option to append configurations such as **interface**, **route**, **Central-Nat table**, and **DHCP Server** into the pre-exist configuration on the device.
Migrate device Hostname and Alias	Enable this option to migrate your hostname and alias in config system global setting. Note that if the hostname in source config is the Serial Number, it'll be skipped by converter even if this option is enabled.
Discard interfaces with neither references nor IP	When this option is enabled, those interfaces which do not have IPs and are not referenced anywhere in the config will be discarded directly.
Policy mode to Profile mode conversion	When selected, the config will be converted from FortiOS NGFW Policy mode to Profile mode, instead of converting to another device.

Setting	Description
Interface Split conversion	When this option is enabled, the policies with multiple source or destination interfaces will be split into equivalent policies with single source and destination interfaces. After splitting, the "Interface pair view" can be used in FortiGate GUI.
Preserve default admin user password and trusthost settings	By default, FortiConverter removes the password and trusthost settings in the default admin account to prevent accessing issues. Enable this option to preserve those settings.

Config Information

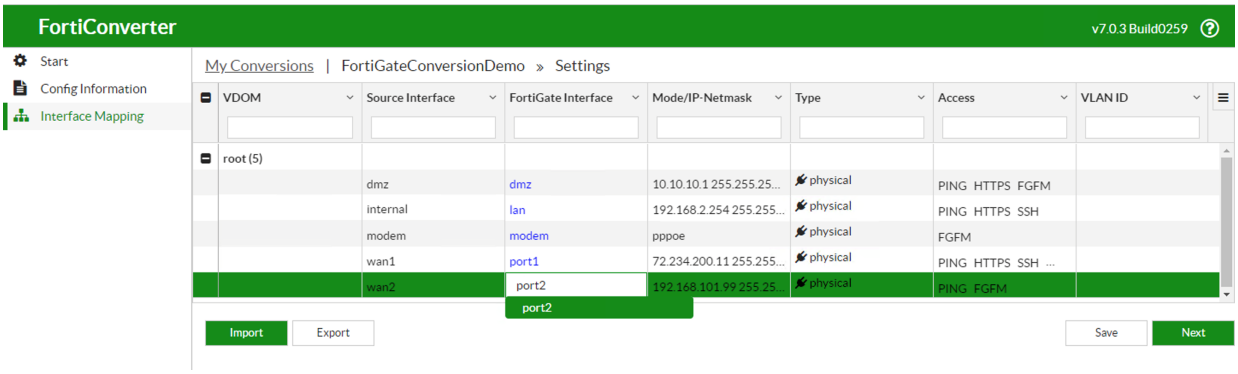
Setting	Description
Information of Configurations	The device model name and the firmware build information of the source and target devices are shown in this table. Configuration file names are shown in the table as a link. Click the link to see the content. The file won't show if it's too large.
Managed Device Name	The name of the managed device which the converted interface or route configuration would be imported in FortiManager. (Only available when the output format is **FortiManager**)
Detect Messages	Some warning or error message detected in the parser would be shown in this table. If an error message occurs, users would be blocked to process the conversion further. Users should fix the problem manually and restart a new conversion.
Source Configuration Preview	The number of each type of objects are shown in the preview table.

Fortinet interface mapping

At the interface mapping step, double-click the table cell from the **FortiGate Interface** column to modify interface mapping.

You can either select an existing entry from the name list or manually input a desired interface name to map.

- To **select** the appropriate FortiGate interface, click the value in the FortiGate Interface column, and then select a value or enter a custom interface name.
- To **edit** other values, double-click the proper column. Use the toolbar icon on the right to show and hide columns. You can also use the Tuning page to create mappings after the conversion is complete.
- To **import** a set of interface mappings from a file, click **Import**.
- To **download** the current set of interface mappings, click **Export**.
- To **delete** an interface, select the entry and right-click to select **Delete Selected**. This is useful if your target FortiGate has fewer interfaces than the source configuration.



Setting	Description
VDOM	Shows the virtual domains used in the conversion. ("root" by default)
Source Interface	The original interface name extracted from the source configuration file. e.g. Cisco ASA conversion may display - "GigabitEthernet0/0" FortiGate conversion may have – "internal1" or "port1"
FortiGate Interface	This is the interface name to be mapped into the target FortiGate. Click to assign a FortiGate port or input the interface name manually for each interface. (Only available when the output format is **FortiGate**) e.g. Cisco ASA conversion you may map "GigabitEthernet0/0" to "port1" FortiGate conversion you may want to map "internal1" to "port1"
Members	Shows any members, if they are set.
IP-Netmask	Shows the IP address and netmask of the connection.
Type	Shows the type of interface.
Access	Shows which protocols has permission to access each interface.
Import	Click to load a set of interface mappings from a text file.
Export	Saves the current set of interface mappings to a text file.
Delete Selected	Click to delete the selected mapping item.

Fortinet Conversion Result

Setting	Description
Conversion Summary	Provides basic information about the conversion.
Device Summary	Provides statistics about the detected objects.

To download your finished conversion, click **Download Configurations**, located in the top-right corner. Your download conversion is a configuration file.

The conversion output consists of two main parts:

1. The first part is the default configuration of the target device.
2. The second part starts with the commented out line "**#migrated config starts**", and follows with the migrated source configuration.

If you want to modify the output config manually, we suggest you to modify only the second part because the definition from the first part will be overwritten by the following definition.

Migrate SSL VPN to IPsec VPN

This feature allows user to migrate existing SSL VPN configuration into IPsec VPN configuration. To perform the FortiGate SSL VPN to IPsec VPN migration, only src config is needed. After the migration then proceed to the summary page to download the migrated configuration. The following changes are made:

1. SSL VPN web portals are migrated into phase1 interfaces (the mapped ippool, user/user group, interface name can be edited)
2. A default phase2 object will also be generated.
3. VPN policies' source Interface ssl.<vdom_name> are replaced by corresponding migrated phase1-interface.

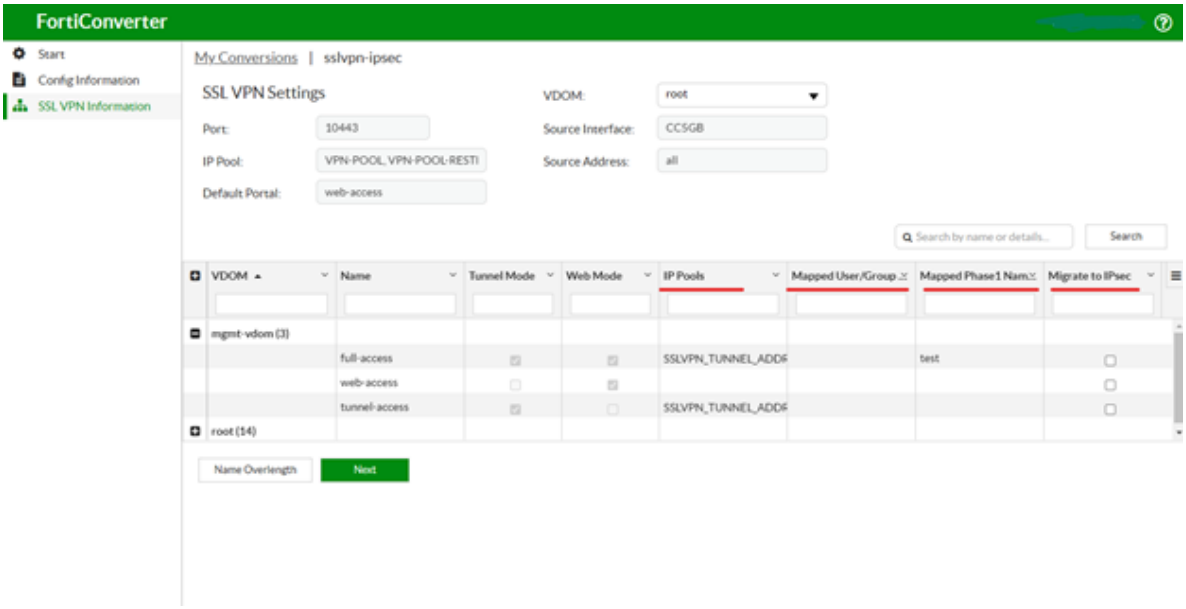
Migration process

1. Select the option **Migrate SSL VPN to IPsec VPN** at the start page and input.
2. Proceed the conversion to the page **SSL VPN Information**.

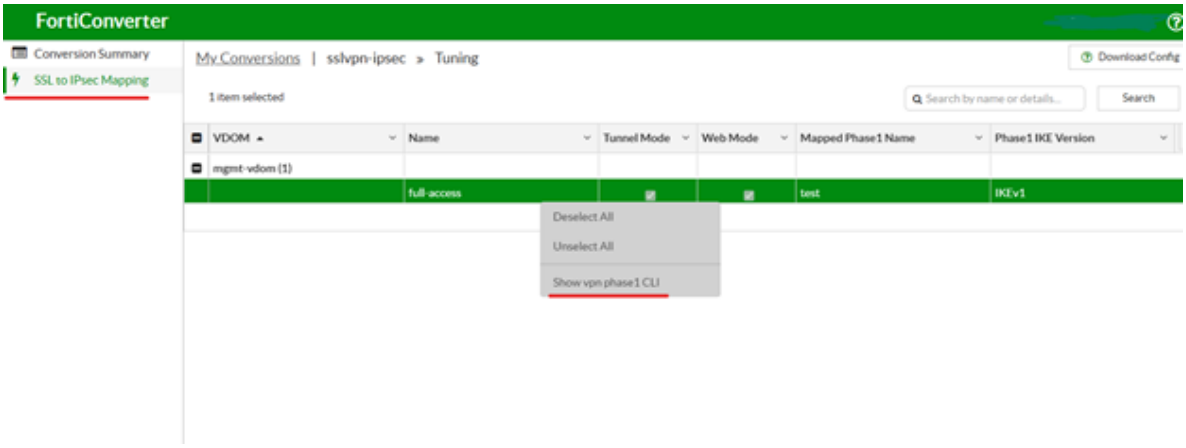
3. At the **SSL VPN Information** page, double-click the web portal table column headers: IP Pools, mapped User/Group, mapped phase1 name to edit the content.

Setting	Description
IP Pools	The selected ip pool will be used in the migrated VPN IPsec phase1 object as either ipv4-start-ip, ipv4-end-ip or ipv4-start-ip, ipv4-netmask
User/Group	The selected user/group will be used in the migrated VPN IPsec phase1 object as authusrgrp
Mapped Phase1 Name	The settings define the migrated VPN IPsec phase1 name, the length should be between 1 to 15 characters.
Migrate to IPsec	Check to migrate the selected web portal

At the **SSL VPN Information** page, double-click the web portal table column headers: **IP Pools**, **Mapped User/Group**, **Mapped Phase1 Name** to edit the content.



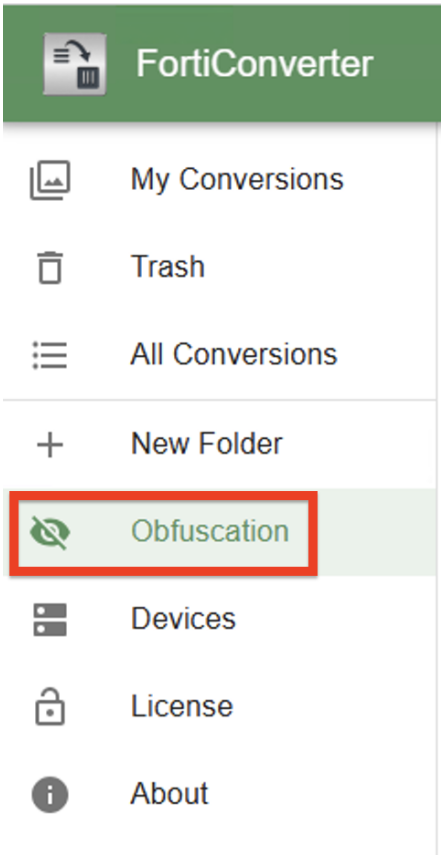
4. Click **Next**, and the converted VPN information will be displayed in the **SSL to IPSec Mapping** page.



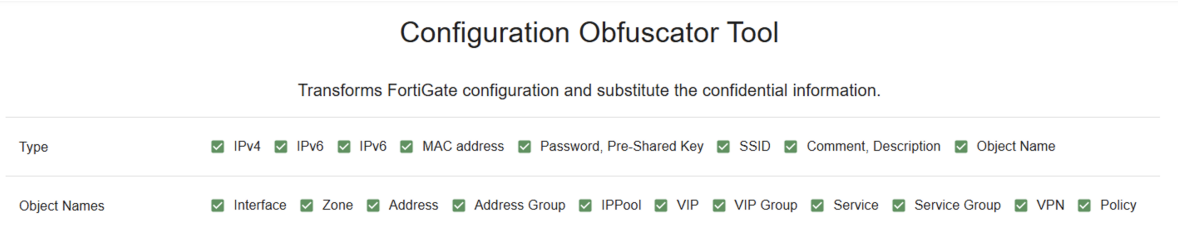
FortiGate Configuration Obfuscator Tool

This feature can be used to obfuscate IP addresses, object's names, and confidential information for the case when the configurations cannot be sent without scrubbing.

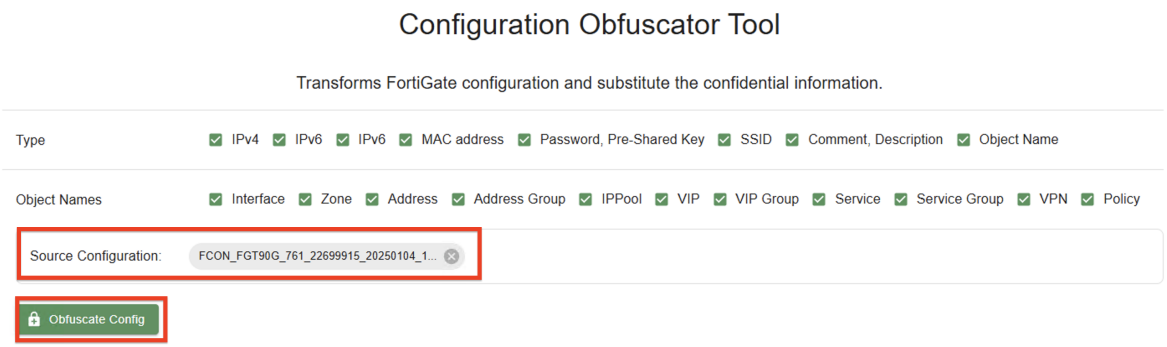
1. On the left-sidebar, select **Obfuscator** to enter the page.



2. 2. Select the types you want to obfuscate. Note that if the object name is unselected, the second row will be disabled.



3. 3. Upload the FortiGate configuration and click **Obfuscate Config.**



4. Options description

Type	
IPv4	Global find **IPv4** addresses include the unicast, multicast, private network, and address range pattern and substitute.
IPv6	Global find **IPv6** addresses and substitute.
FQDN	Global find **FQDN** and **Wildcard-FQDN** address and substitute.
MAC Address	Global find **MAC** addresses and substitute.
Password, Pre-Shared key	Global find **ENC ***** pattern and substitute with the string "012345678".
SSID	Global find **ssid** name and substitute.
Comment	Global find **set comment|comments** and remove the line.
Object Name	Global find object names according to the selected object name categories .

Object Name	
Interface	Find object names under the **config system interface** and substitute with INTERFACE_INDEX. It won't change the default FortiGate interface name like "wan1", "port2", "dmz," etc.
Zone	Find object names under the **config system zone** and substitute with ZONE_INDEX.
Address	Find object names under the **config firewall address** and substitute with ADDR_INDEX. It won't change the name like "all", "any", etc.
Address Group	Find object names under the **config firewall addrgrp** and substitute with ADDRGrp_INDEX.
IPPool	Find object names under the **config firewall ippool** and substitute with IPPool_INDEX.
VIP	Find object names under the **config firewall vip** and substitute with VIP_INDEX.

Object Name	
VIP Group	Find object names under the **config firewall vipgrp** and substitute with VIPGrp_INDEX.
Service	Find object names under the **config firewall service** custom and substitute with SERV_INDEX. It won't change the name like "all", "any", etc.
Service Group	Find object names under the **config firewall service** group and substitute with SERVGrp_INDEX.
VPN	Find object names under **config vpn ipsec phase1, config vpn ipsec phase2 config vpn ipsec phase1-interface, config vpn ipsec phase2-interface** and substitute with VPN_INDEX or VPN_INTF_INDEX.
Policy	Find "set name" under the **config firewall policy** and substitute with POLICY_INDEX.

*Note that the text substitution follows the order below.

IP Address > SSID > (substitute object name with the following order) > VPN > Interface > Zone > address and group > ippool > vip > vip and group > service and group

According to the substitution order above, if the object name contains an address string (commonly used in IPPool and VIP), it won't be replaced with the name IPPool_INDEX or VIP_INDEX because the IP address has higher order.

For example, in the case below, the output replaces the IP string in the object name instead of using IPPool_INDEX while other objects such as VIP remains the same.

```
config firewall ippool
   edit "ippool-10.161.192.11"
      set endip 10.161.192.11
      set startip 10.161.192.11
      set type overload
   next
end
```

(After run the obfuscator)

```
config firewall ippool
   edit "ippool-10.90.31.207"
      set endip 10.90.31.207
      set startip 10.90.31.207
      set type overload
   next
end
```

3rd Party Security Vendors Conversion

Alcatel-Lucent Conversion

Alcatel-Lucent differences

Conversion support

FortiConverter supports the conversion of the following Alcatel-Lucent Brick features:

- Interfaces
- Host Groups
- Service Groups
- Zone Brick Rulesets

Fortinet plans to support the following Lucent features in a future FortiConverter release:

- NAT
- Schedule
- VPN
- Hosts Behind Zone

Address and address group configuration

- Lucent host addresses are mapped to FortiGate addresses.
- Lucent host groups are mapped to FortiGate address groups.
- Virtual Brick Addresses (VBA) aren't supported.

Interface configuration

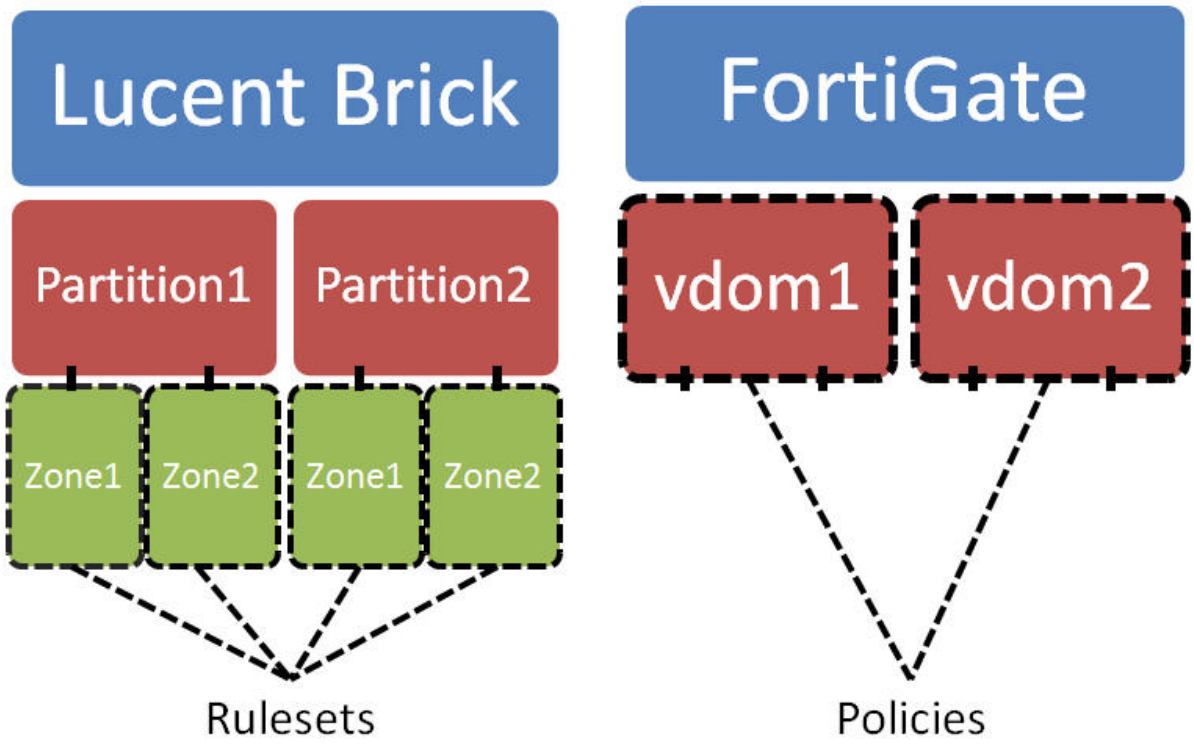
- FortiConverter assigns default VLAN configuration directly to physical interfaces.
- FortiConverter considers all VLANs named "*" or "Port Default" to be the default VLAN configuration.
- Domain Addresses aren't supported.

Service and Service Group configuration

- Lucent Service Groups are mapped to FortiGate Service Groups.
- Lucent service "*" maps to FortiGate service "any".

Policy configuration

Lucent Brick Zone Rulesets operate at the zone level, which has no direct equivalent in FortiGate. Zone rulesets need to be translated into equivalent FortiGate policies.



FortiConverter translates Lucent Brick rules by separating traffic into two categories: inter-partition and intra-partition.

- **Inter-partition traffic** behaves like inter-VDOM traffic, and is simple to convert to FortiGate policies.
- **Intra-partition traffic** is more complicated to convert because multiple zone rules can be applied.

FortiConverter handles the inter-partition traffic by creating a general policy for each rule.

FortiConverter handles the intra-partition traffic by looking for all matches between two zone rulesets. FortiConverter looks at 3 fields: source, destination, and service. All 3 fields must overlap for the rules to match. FortiConverter creates a policy for each match using the intersection of each field.

The action of the rules determines the action of the converted policy, as shown in the following table:

Rule 1	Rule 2	Policy
Pass	Pass	Accept
Pass	Drop	Deny
Drop	Pass	Deny
Drop	Drop	Deny

Inter-partition Deny policies have higher priority than intra-partition policies, while inter-partition Accept policies have lower priority than intra-partition policies.

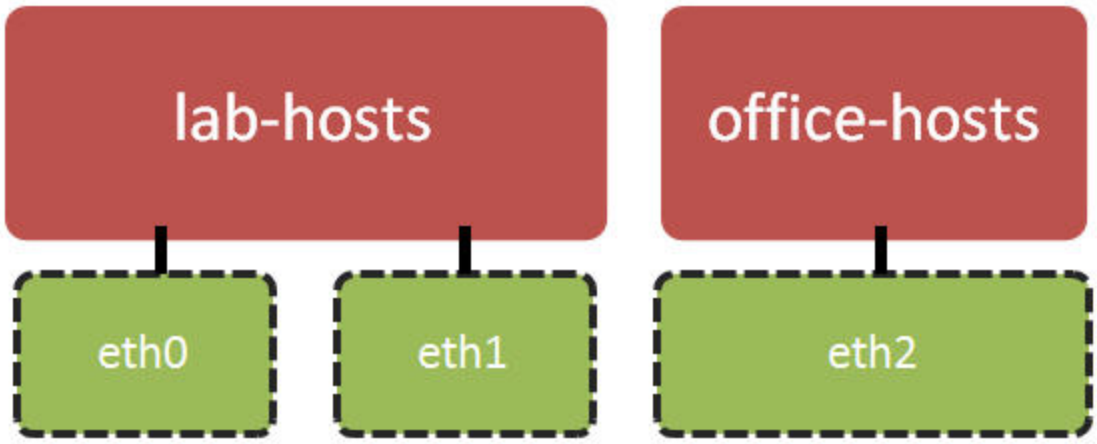
Lucent default ruleset "firewall" is currently unsupported.

VDOM configuration

- Lucent partitions map to FortiGate VDOMs.
- VDOM names are limited to 11 characters. FortiConverter truncates longer names to 11 characters.
- Lucent partition "*Default" maps to the FortiGate root VDOM.

Example conversion

The following block diagram and tables illustrates a Lucent configuration with 2 partitions and 3 zones.



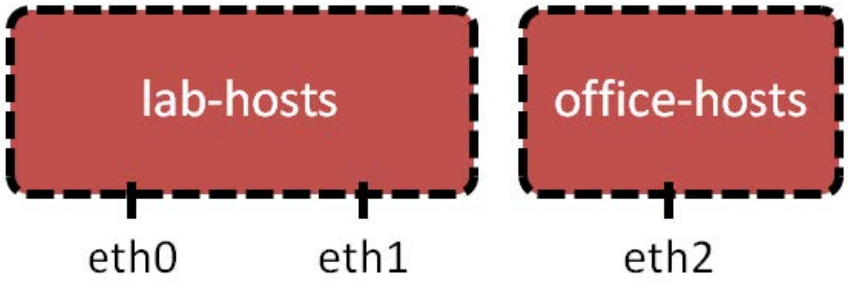
Zone eth0 Ruleset					
Rule Num	Direction	Source	Destination	Service	Action
1000	Out	192.168.1.15	172.30.10.1/24	*	Drop
1001	Both	192.168.1.0/24	172.30.10.1/24	*	Pass

Zone eth1 Ruleset					
Rule Num	Direction	Source	Destination	Service	Action
1000	In	*	172.30.10.5 - 172.30.10.20	TCP	Pass
1001	Both	192.168.1.132	172.30.10.9	*	Pass

Zone eth2 Ruleset

Rule Num	Direction	Source	Destination	Service	Action
1000	Both	*	10.10.15.0/24	HTTP	Pass

This Lucent configuration creates the following FortiGate configuration. Inter-partition rules are in **bold**.



VDOM lab-hosts Policies						
Policy Num	**Src Interface**	**Dst Interface**	**Source**	**Destination**	**Service**	**Action**
10000	**eth0**	**any**	**192.168.1.15**	**172.30.10.1/24**	*****	**Deny**
10001	eth0	eth1	192.168.1.0/24	172.30.10.5 - 172.30.10.20	TCP	Accept
10002	eth0	eth1	192.168.1.132	172.30.10.9	*	Accept
10003	**eth0**	**any**	**192.168.1.0/24**	**172.30.10.1/24**	*****	**Accept**
10004	any	eth0	192.168.1.0/24	172.30.10.1/24	*	Accept
10005	eth1	eth0	192.168.1.132	172.30.10.9	*	Accept
10006	**eth1**	**any**	**192.168.1.132**	**172.30.10.9**	*****	**Accept**
10007	**any**	**eth1**	**192.168.1.132**	**172.30.10.9**	*****	**Accept**

VDOM office-hosts Policies						
Policy Num	**Src Interface**	**Dst Interface**	**Source**	**Destination**	**Service**	**Action**
10000	any	eth2	any	10.10.15.0/24	HTTP	Accept
10001	eth2	any	10.10.15.0/24	any	TCP	Accept

Saving the Alcatel-Lucent source configuration file

Overview

This document provides a step-by-step guide for extracting your Lucent Brick configuration. Fortinet provides a Perl script, `extractConfig.pl` that will read the Brick configuration and extract it into a data format that the FortiConverter can use. FortiConverter can then convert the Brick configuration into its FortiGate equivalent.

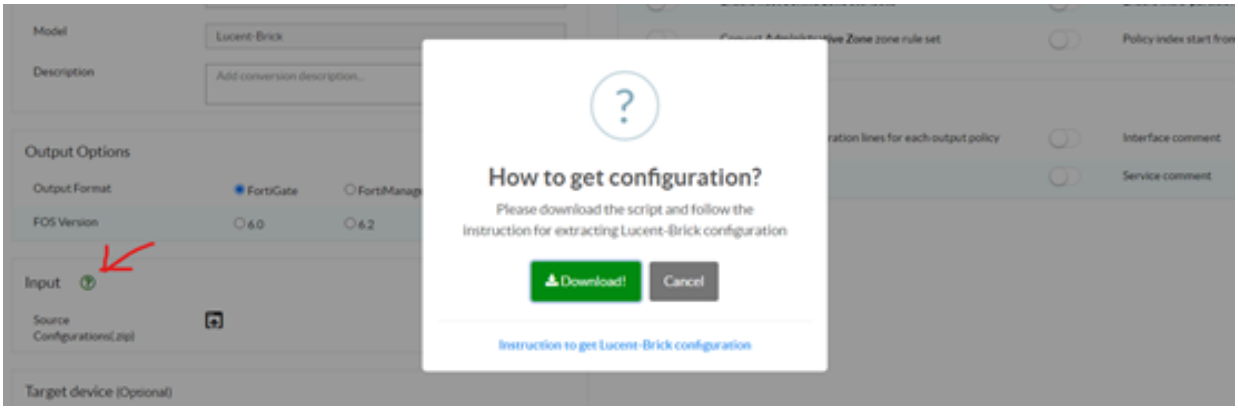
Prerequisites

Perl 5 needs to be installed on the machine for the script to run.

ActivePerl 5.16.3 was used for this example.

The machine also needs to have the Alcatel-Lucent CLI administration tools installed.

For `extractConfig.pl`, please download the script from the FortiConverter application. Click the question mark, a pop-up window will lead you to this instruction guide. At the same time, click download to get the script file.



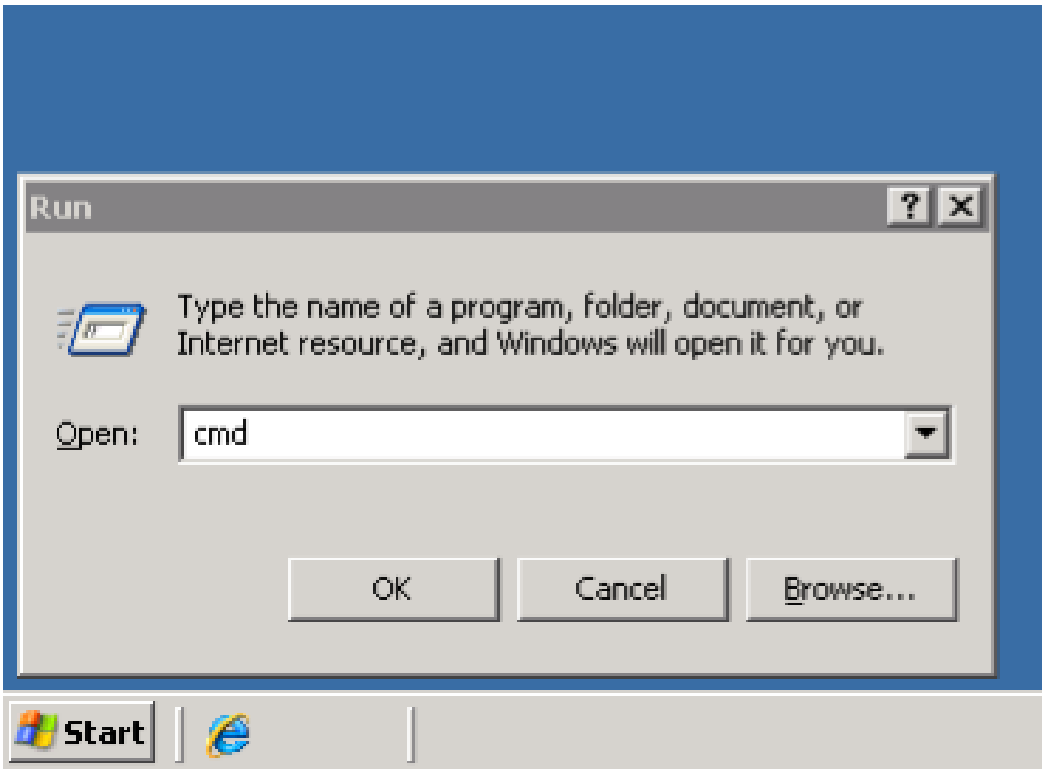
This script is also available in the FortiConverter tool's GitHub:

https://github.com/fortinet/forticonverter-tools/blob/main/extractConfig.pl

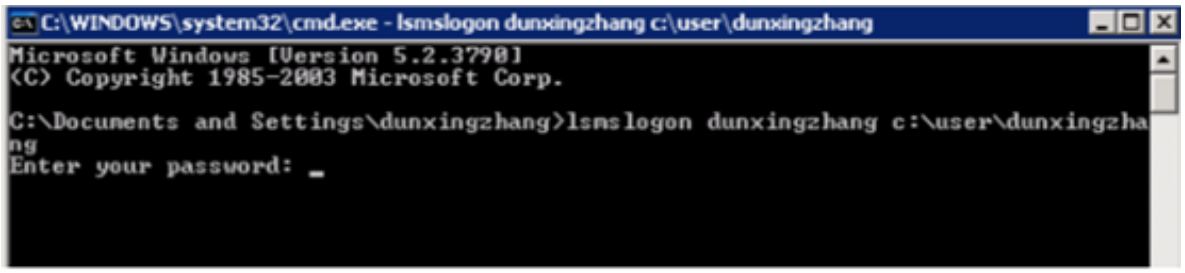
Example Procedure

1. In this example, the target configuration is in the "lab" group, as shown in the SMS GUI tool screenshot below. FortiConverter needs configuration information from the Brick Devices, the Brick Zone Rulesets, the Host Groups, and the Service Groups.

2. Open a command terminal.

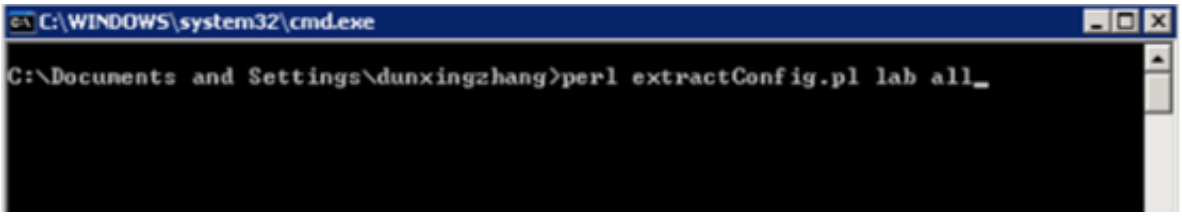


3. Log on to an SMS administrator account that has access to the target group.
   In the command line, type: `lsmslogon <admin> <outputDirectory>`.
   In this example, the admin account is "`dunxingzhang`". The output directory is `C:\users\dunxingzhang\`.

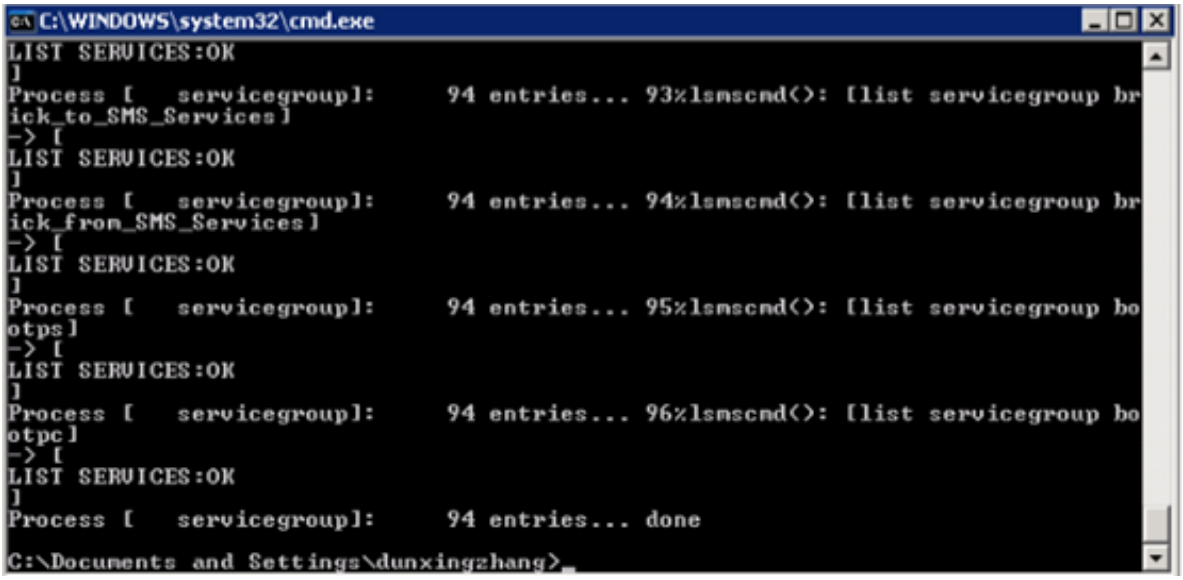


4. Run the Perl script in the command line by typing: `perl extractConfig.pl <systemGroup> all`
In this example, the target group is "`lab`", and the script has been copied to the admin's home directory, `C:\Documents and Settings\dunxingzhang`.

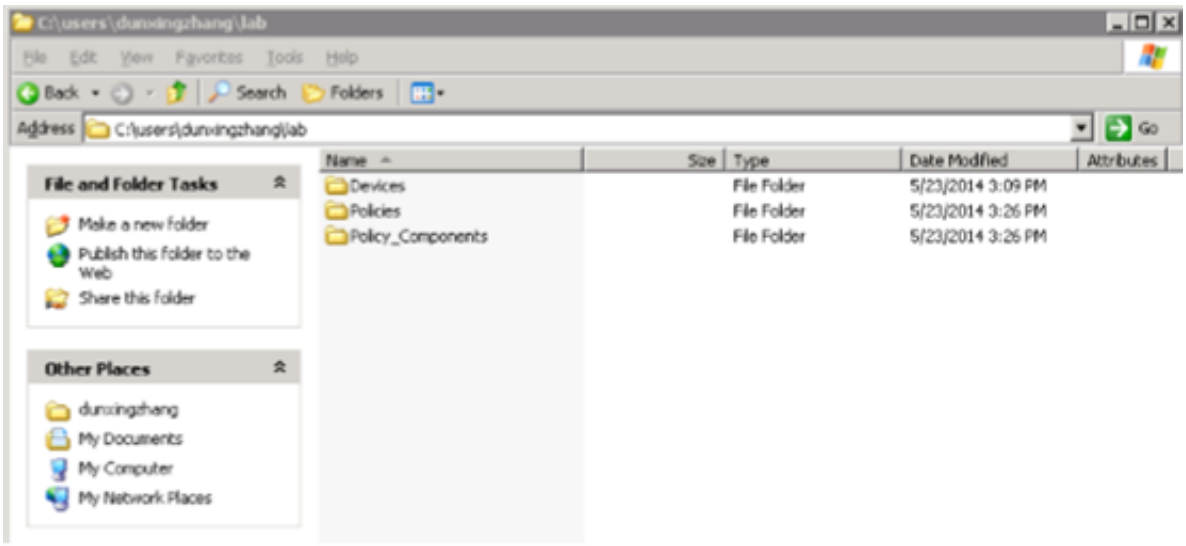
For a detailed instruction of the script, please see the README file in the link below: https://github.com/fortinet/forticonverter-tools/blob/main/README.md



The script will show its progress as it extracts each object and ruleset



5. When it is completed, the output will be saved in the output directory designated in step 3. A directory is created for each category, and each object in a category is saved to its own text file.



Congratulations!

You have successfully extracted your Lucent Brick configuration.

6. Compress all the directories as a zip file.

Alcatel-Lucent conversion wizard

> The administrator password is **not** set on the new configuration.
>
> For third-party conversions, the trusted host settings are converted. Check the trusted host settings to ensure they allow management access from the relevant network interfaces.

To start a new conversion

1. Start FortiConverter.
2. When start-up is complete, a browser window automatically opens to http://127.0.0.1:8000.
3. Click New Conversion **New Conversion**, located at the top right corner.
4. Enter a name for the conversion configuration.
5. For Vendor, choose **Alcatel-Lucent** block.
6. Choose a Model, if applicable.
7. Click **OK**.

The configuration page opens to the Start page, and you can input your settings.

Alcatel Start options

This table lists the start settings.

Setting	Description
Description	Enter a description for the configuration.
Output format	Select the appropriate output for your target Fortinet device.
FOS version	The configuration syntax is slightly different among FortiOS 6.4, 7.0, 7.2, 7.4 and 7.6. Select the version that corresponds to the FortiOS version on the target.
Source Configuration	Select the input file (.zip). Ensure the input configuration is in .zip format. See Saving the Alcatel-Lucent source configuration file on page 53
Discard unreferenced firewall objects	Specifies whether addresses, schedules, and services that aren't referenced by a policy are saved and added to the output. This option can be useful if your target device has table size limitations. You can view the unreferenced objects that FortiConverter removed on the Tuning page.
Enable host behind zone attribute	Specifies whether FortiConverter restricts the destination or source IP addresses in the firewall policy it generates to the ones specified by the "host behind zone" settings in the source configuration. When this option is disabled, FortiConverter ignores the "host behind zone" settings, and it uses the destination or source IP address specified by the source rule in the output policy.
Convert Administrative Zone ruleset	Specifies whether FortiConverter includes the default "administrative zone" ruleset in the output configuration. The "administrative zone" ruleset is designed for device management, in most cases, it isn't required in the output configuration.
Increase Address and Service Table Sizes for High-End Models	You can customize the maximum table sizes that FortiConverter uses when "Adjust table sizes" is selected. For more information, see Adjusting table sizes on page 232.
Enable intra-partition zone rule set merge	Specifies whether FortiConverter creates FortiGate policies for traffic within a partition that the source configuration applies the multiple zone rulesets to. For more information on how FortiConverter converts intra-partition zone rulesets to a FortiGate policy, see Alcatel-Lucent Conversion on page 50.
Include input configuration lines for each output policy	Specifies whether FortiConverter includes the input configuration lines used for each FortiGate policy in the FortiGate configuration as a policy comment.
Address comment	Specifies whether FortiConverter copies the address comment from source configuration to the converted FortiGate address.
Interface comment	Specifies whether FortiConverter copies the interface comment from the source configuration to the mapped FortiGate interface.
Service comment	Specifies whether FortiConverter copies the service comment from the source configuration to converted FortiGate service.

Setting	Description
Policy index start from 1 instead of 10000	When selected, the serial number of firewall policies will start from 1 instead of 10000.
Target device (optional)	Select the model of the target device, or select a device connected to FortiConverter.

Device selection

Setting	Description
Select the firewall to convert	Select a specific firewall to include in the conversion.
Source Configuration Preview	The numbers of each type of firewall object are shown in the preview table. Click the object number to see detailed information on each object. In each type of object, click the button **Export CSV** to export the current object info as CSV file.

Partition & Zone rule selection

Setting	Description
Select all partitions	Select to select all partitions or clear it to de-select all partitions
Partition selection	Select the partition to include the partition to the conversion. Include the individual zone rules within a partition.
Zone rule selection	Select or de-select the zone rule to include in the conversion.

Lucent Interface Mapping

You can manually map the interface.

- To **select** the appropriate FortiGate interface, click the value in the FortiGate Interface column, and then select a value or enter a custom interface name.
- To **edit** other values, double-click the proper column. Use the toolbar icon on the right to show and hide columns. You can also use the Tuning page to create mappings after the conversion is complete.
- To **import** a set of interface mappings from a file, click **Import**.
- To **download** the current set of interface mappings, click **Export**.
- To **delete** an interface, select the entries you would like to delete, **right click** and select **Delete Selected**. This is useful if your target FortiGate has fewer interfaces than the source configuration.

The limit of the length of interface names in FortiOS is 15 characters. Interfaces in the source config which have longer names should be trimmed to a shorter name. It is recommended to trim the names manually to ensure readability. But if a quick trimming is needed, please select the entries, **right click** and select **Trim Interface Name** to trim the names into 15 characters automatically.

Setting	Description
VDOM	Shows the virtual domains used in the conversion. ("root" by default)
Source Interface	Shows each interface on the Alcatel-Lucent firewall.
FortiGate Interface	The input field for corresponding FortiGate interface names. Click to assign a FortiGate port or input the interface name manually for each interface. (Only available when the output format is **FortiGate**)
Normalized interface	The input field for corresponding normalized interface names, which would be configured in the ADOM database in FortiManager. Click to assign a port or input the interface name manually for each interface. (Only available when the output format is **FortiManager**)
Device interface	The input field for corresponding interface names in the managed devices in FortiManager. Click to assign a port or input the interface name manually for each interface. (Only available when the output format is **FortiManager**)
Members	Shows any members, if they are set.
IP-Netmask	Shows the IP address and netmask of the connection.
Type	Shows the type of interface.
Access	Shows which protocols has permission to access each interface.
Import	Click to load a set of interface mappings from a text file.
Export	Saves the current set of interface mappings to a text file.
Delete Selected	Click to delete the selected mapping item.
Trim Interface Name	Trim the interface names which exceed 15 characters into 15 characters automatically.

Lucent Route Information

FortiConverter creates static routes in the output using the static routes it detects in the source configuration and any routing information you provide.

Double-click an item to edit it.

Setting	Description
New Route	Click to add a route.
Edit	Click to edit the selected route.
Delete	Click to delete the selected route.

Alcatel-Lucent Conversion result

Tab	Description
Conversion Summary	It provides statistics about the conversion.
Reports	Generate PDF reports including converted and unconverted objects list.
VDOM Information	It shows how VDMS were mapped from the source device to the new device.
Interface Mapping	It shows how interfaces were mapped for each VDOM from the source device.
Device Summary	It provides statistics about the detected objects.

FortiConverter includes error and warning messages into the conversion when an error occurs.

Review the `config-all.txt` file after each conversion for errors. These errors and warning messages might cause the import process to fail, if not corrected. See for more details.

Bluecoat Conversion

Conversion support

FortiConverter supports the following features:

- Address (group)
- Proxy Address(group)
- Service
- Proxy Policy

Forticonverter supports conversion to either Fortigate or FortiProxy devices. The converted config would be slightly different in interface and/or Proxy Policy category."

Saving the Bluecoat source configuration files

Backup Configurations

1. Make sure that the SSH client you are using is set to write the output to a file:
2. For example, in PuTTY, select **Session > Logging**. Ensure that All Session output radio button option is selected to log all session output.
3. Connect to the Edge SWG CLI via SSH.
4. Enter enable mode.
5. Type the following command: "`show configuration expanded noprompts with-keyrings unencrypted`"

Note: If you are running version 7.x, the above command will not work, it has been removed. In version 7.x, the Workaround is to set security private-key-display unencrypted option in config mode before running show configuration expanded noprompts command. After set that option you can see configuration output with keyring information.

```
Blue Coat#configure terminal
Blue Coat#(config)security private-key-display unencrypted
   ok
Blue Coat#(config)exit
Blue Coat#show configuration expanded noprompts
```

The expanded configuration will be written to the file you specified in step 1; this may take some time depending on the size of your configuration. This copies the entire configuration as well as the security keyrings (both private and public keys), unencrypted.

Reference: https://knowledge.broadcom.com/external/article/165964

Bluecoat conversion wizard

To start a new conversion

1. Start FortiConverter.
2. When start-up is complete, a browser window automatically opens to http://127.0.0.1:8000.
3. Click 

New Conversion, located at the top right corner.
4. Enter a name for the conversion configuration.
5. For Vendor, choose **Bluecoat** from the drop-down list.
6. Choose a Model, if applicable.
7. Click **OK**.

The configuration page opens to the Start page, and you can input your settings.

Bluecoat start options

Forticonverter supports conversion to either Fortigate or FortiProxy devices. The converted config would be slightly different in interface and/or Proxy Policy category.

This table lists the start settings.

Setting	Description
Profile	
Description	Enter a description of the configuration.
Output Options	
Output Format	Select whether to convert to FortiGate or FortiProxy device.
FOS Version	The configuration syntax is slightly different among FortiOS 6.4, 7.0, 7.2, 7.4 and 7.6. Select the version that corresponds to the FortiOS version on the target.
Input	
Source Configuration	Select the input file.
Conversion Options	
Discard unreferenced firewall objects	Specifies whether addresses, schedules, and services that are not referenced by a policy are saved and added to the output. This option can be useful if your target device has table size limitations. You can view the unreferenced objects that FortiConverter removed in the Tuning page.
Increase Address and Service Table Sizes for High-End Models	You can customize the maximum table sizes that FortiConverter uses when Adjust table sizes is selected. For more information, see Adjusting table sizes on page 232

Policy index start from 1 instead of 10000	When selected, the serial number of firewall policies will start from 1 instead of 10000.
Convert as custom local category	Bluecoat custom category URLs & URIs will be converted into FPX custom local category URLs
Use "webproxy" as default service	When this option is enabled, FortiConverter uses the predefined service "webproxy" by default as the service of proxy policies when no specific service is specified. When this option is disabled, FortiConverter uses service "ALL" by default
DNS is not in use in the migrated device	This option is for FortiProxy migration only. When the device cannot do DNS lookup by itself, the conversion result will have the following two differences: 1. FQDN addresses cannot be used, so the web URLs will be converted into proxy addresses with Regex matching. 2. When a forwarding layer is defined in the Bluecoat device, the forwarding will not be performed by proxy policies in FortiProxy, but by URL matches instead.
Comment Options	
Include input configuration lines for each output policy	Specifies whether FortiConverter includes the input configuration lines used for each FortiGate policy in the FortiGate configuration as a policy comment.
Domain Name Conversion Options	
Convert to FQDN addresses, **e.g: set fqdn "domain.name"**	Convert the Bluecoat objects which have domain names as contents into FQDN addresses.
Convert to FQDN addresses with wildcard prefix "*.", **e.g: set fqdn "*.domain.name"**	Convert the Bluecoat objects which have domain names as contents into FQDN addresses which start with “*.”.
Convert to host-regex proxy addresses, **e.g: set host-regex "domain\.name"**	Convert the Bluecoat objects which have domain names as contents into host-regex proxy addresses.
Convert to FQDN addresses with wildcard prefix and suffix "*", **e.g: set fqdn "*domain.name*"**	Convert the Bluecoat objects which have domain names as contents into FQDN addresses which start and end with “*”.

Bluecoat Interface Mapping

You can manually map the interface.

- To **select** the appropriate FortiGate interface, click the value in the FortiGate Interface column, and then select a value or enter a custom interface name.
- To **edit** other values, double-click the proper column. Use the toolbar icon on the right to show and hide columns. You can also use the Tuning page to create mappings after the conversion is complete.
- To **import** a set of interface mappings from a file, click **Import**.
- To **download** the current set of interface mappings, click **Export**.
- To **delete** an interface, select the entries you would like to delete, **right click** and select **Delete Selected**. This is useful if your target FortiGate has fewer interfaces than the source configuration.

The limit of the length of interface names in FortiOS is 15 characters. Interfaces in the source config which have longer names should be trimmed to a shorter name. It is recommended to trim the names manually to ensure readability. But if a quick trimming is needed, please select the entries, **right click** and select **Trim Interface Name** to trim the names into 15 characters automatically.

Setting	Description
VDOM	Shows the virtual domains used in the conversion. ("root" by default)
Source Interface	Shows each interface on the Bluecoat firewall.
FortiGate Interface	The input field for corresponding FortiGate interface names. Click to assign a FortiGate port or input the interface name manually for each interface. (Only available when the output format is **FortiGate**)
Normalized interface	The input field for corresponding normalized interface names, which would be configured in the ADOM database in FortiManager. Click to assign a port or input the interface name manually for each interface. (Only available when the output format is **FortiManager**)
Device interface	The input field for corresponding interface names in the managed devices in FortiManager. Click to assign a port or input the interface name manually for each interface. (Only available when the output format is **FortiManager**)
Members	Shows any members, if they are set.
IP-Netmask	Shows the IP address and netmask of the connection.
Type	Shows the type of interface.
Access	Shows which protocols has permission to access each interface.
Import	Click to load a set of interface mappings from a text file.
Export	Saves the current set of interface mappings to a text file.

Setting	Description
Delete Selected	Click to delete the selected mapping item.
Trim Interface Name	Trim the interface names which exceed 15 characters into 15 characters automatically.

Bluecoat conversion result

Tab	Description
Conversion Summary	Provides statistics about the conversion.
Device Summary	Provides statistics about the detected objects.

FortiConverter includes error and warning messages into the conversion when an error occurs.

Review the `config-all.txt` file after each conversion for errors. These errors and warning messages might cause the import process to fail, if not corrected. See for more details.

Bluecoat Layer Merge

FortiConverter is able to merge SSL intercept layer, authentication layer and forwarding layer in Bluecoat into the proxy policy list in FortiGate.

In Bluecoat proxy rules are separated into multiple layers, and each layer has different functions such as authentication, SSL intercept, web access and forwarding. A traffic needs to go through one layer to perform one function and go through the next layer to perform another function.

In FortiGate, those functions are performed by proxy policies and there is only one proxy policy list. When converting Bluecoat rules, FortiConverter first converts web access layers into proxy policies, then matches the proxy policies with other layers and applies the action of those layers into the proxy policies.

Currently FortiConverter supports the layer merge of SSL intercept layer, authentication layer and forwarding layer.

Specify web access layers by adding key strings on page 66

1. SSL Intercept layer merge on page 67
2. Authentication layer merge on page 68
3. Forwarding layer merge on page 70
4. The order of layer merge on page 71

Specify web access layers by adding key strings

To perform the layer merge, it is required to add the keyword "**Web Access Layer**" into the name of web access layers inside the config file. Since FortiConverter cannot always correctly identify web access layers in

the config, it is needed to manually specify them in the layer name. For example:

Originally, the definition of web access layer name is:

```
;; Tab: [User WAL]
```

Please add the keyword "Web Access Layer" into the layer name:

```
;; Tab: [User WAL Web Access Layer]
```

When FortiConverter finds the keyword in the layer name, the layer will be marked as a web access layer.

SSL Intercept layer merge

Currently FortiConverter supports merging the SSL intercept rules with the setting ssl.forward_proxy(no) into proxy policies, and enable SSL SSH inspection for other policies. For example:

If there is a web access rule:

```
client.address=1.1.1.0/24 url.domain=" fortinet.com" Allow ; Rule 1
```

It would be converted into a FortiGate proxy policy like this:

```
config firewall policy
edit 10001
   set type explicit-web
   set explicit-web-proxy "web-proxy"
   set dstintf "INTERNET"
   set srcaddr "n-1.1.1.0_24"
   set dstaddr " fortinet.com "
   set service "webproxy"
   set action accept
   set ssl-ssh-profile "deep-inspection"
next
end
```

The SSL SSH profile will be set to "deep inspection" by default.

SSL Intercept layer merge - Full match

If an SSL intercept rule is defined for domain "fortinet.com":

```
url.domain=" fortinet.com" ssl.forward_proxy(no) ; Rule 1
```

Then the SSL intercept rule covers the whole web access rule, which is a **full match**, so no SSL SSH inspection should be performed on the proxy policy. Hence after merging the SSL intercept rule into the web access rule, the converted proxy policy will become:

```
config firewall policy
edit 10001
   set type explicit-web
   set explicit-web-proxy "web-proxy"
   set dstintf "INTERNET"
   set srcaddr "h-1.1.1.1"
   set dstaddr " fortinet.com "
   set service "webproxy"
   set action accept
next
end
```

`set ssl-ssh-profile "deep-inspection"` would be removed from the proxy policy.

SSL Intercept layer merge - Partial match

If the SSL intercept rule is defined like this:

```
client.address=1.1.1.1/32 url.domain=" fortinet.com" ssl.forward_proxy(no) ; Rule 1
```

In the SSL intercept rule, only client host 1.1.1.1 is used, but in the web access layer, the whole subnet 1.1.1.0/24 is used, so this is a **partial match**. In this case, the original rule would not be changed, but another proxy policy will be created before the original proxy policy:

```
config firewall policy
edit 50010001 --- The prefix "5xx" is added for new SSL intercept rules.
   set type explicit-web
   set explicit-web-proxy "web-proxy"
   set dstintf "INTERNET"
   set srcaddr "h-1.1.1.1" --- The traffic of the SSL intercept rule.
   set dstaddr " fortinet.com "
   set service "webproxy"
   set action accept
next
edit 10001
   set type explicit-web
   set explicit-web-proxy "web-proxy"
   set dstintf "INTERNET"
   set srcaddr "n-1.1.1.0_24"
   set dstaddr "fortinet.com "
   set service "webproxy"
   set action accept
   set ssl-ssh-profile "deep-inspection"
next
end
```

The first proxy policy is created with no SSL SSH profile because host 1.1.1.1 does not need SSL incept according to the SSL intercept rule. The second proxy policy is converted from the original web access rule, which needs to do SSL intercept.

The newly created proxy policies from SSL intercept layer merge would have prefix "**5xx**". For example, if three proxy policies from SSL intercept are created for proxy policy 10001, their policy names will be 50010001, 50110001 and 50210001.

Authentication layer merge

For authentication layer, FortiConverter supports merging the authentication rules into proxy policies, and adds the user group into the matched proxy policies.

The user group mentioned in authentication rule would be converted into a user group with prefix “Domain Users”.

For example, an authentication rule with:

authenticate(Fortinet) authenticate.force(yes)

will be converted into a user group called “Domain Users Fortinet”. A member “Fortinet” will be added into the group, but users need to check if the configuration needs to be modified.

If proxy policy matches with an authentication rule, the proxy policy will use the user group from the authentication rule. If there is already a user configured in the proxy policy, but it matches with a rule with **authenticate(no)**, then the users inside the proxy policy will be removed.

An example of authentication layer merge:

For the web access rule (the same as the example in the previous section):

client.address=1.1.1.0/24 url.domain=" fortinet.com" Allow ; Rule 1

There is no user configured in the rule.

Authentication layer merge - Full match

If an authentication rule is defined for domain “fortinet.com”:

url.domain=" fortinet.com" authenticate(Fortinet) authenticate.force(yes) ; Rule 1

Then the authentication rule covers the whole web access rule, which is a full match, so the user group “Domain Users Fortinet” will be applied on the proxy policy. Hence after merging, the converted proxy policy will become:

```
config firewall policy
edit 10001
   set type explicit-web
   set explicit-web-proxy "web-proxy"
   set dstintf "INTERNET"
   set srcaddr "h-1.1.1.1"
   set dstaddr " fortinet.com "
   set service "webproxy"
   set groups "Domain Users Fortinet" --- the user group from the authentication rule
   set action accept
next
end
```

Authentication layer merge - Partial match

If the authentication rule is defined like this:

client.address=1.1.1.1/32 url.domain=" fortinet.com" authenticate(Fortinet) authenticate.force(yes) ; Rule 1

In this rule, only client host 1.1.1.1 is used, but in the web access layer, the whole subnet 1.1.1.0/24 is used, so this is a partial match. In this case, the original rule would not be changed, but another proxy policy will be created before the original proxy policy:

```
config firewall policy
edit 60010001 --- The prefix “6xx” is added for new authentication rules.
set type explicit-web
set explicit-web-proxy "web-proxy"
set dstintf "INTERNET"
set srcaddr "h-1.1.1.1" --- The traffic of the authentication rule.
set dstaddr " fortinet.com "
set service "webproxy"
set groups "Domain Users Fortinet" --- the user group from the authentication rule
set action accept
next
edit 10001
set type explicit-web
```

```
set explicit-web-proxy "web-proxy"
set dstintf "INTERNET"
set srcaddr "n-1.1.1.0_24"
set dstaddr "fortinet.com "
set service "webproxy"
set action acceptnext
end
```

The first proxy policy is created with the user group because only host 1.1.1.1 needs to authenticate according to the authentication rule. The second proxy policy is converted from the original web access rule, which does not need authentication.

The newly created proxy policies from authentication layer merge would have prefix "**6xx**". For example, if three proxy policies from authentication layer merge are created for proxy policy 10001, their policy names will be 60010001, 60110001 and 60210001.

Forwarding layer merge

For forwarding layer, FortiConverter supports merging the forwarding rules into proxy policies, and adds the forward server into the matched proxy policies.

An example of forwarding layer merge:

For the web access rule (the same as the example in the previous section):

```
client.address=1.1.1.0/24 url.domain=" fortinet.com" Allow ; Rule 1
```

There is no forward server configured in the rule.

Forwarding layer merge - Full match

If a forwarding rule is defined for domain "fortinet.com":

```
url.domain=" fortinet.com" forward("Fortinet") ; Rule 1
```

Then the forwarding rule covers the whole web access rule, which is a full match, so the forward server "Fortinet" will be applied on the proxy policy. Hence after merging, the converted proxy policy will become:

```
config firewall policy
edit 10001
   set type explicit-web
   set explicit-web-proxy "web-proxy"
   set dstintf "INTERNET"
   set srcaddr "h-1.1.1.1"
   set dstaddr " fortinet.com "
   set service "webproxy"
   set webproxy-forward-server "Fortinet" --- the forward server from the forwarding
        rule
   set action accept
next
end
```

Forwarding layer merge - Partial match

If the forwarding rule is defined like this:

```
client.address=1.1.1.1/32 url.domain=" fortinet.com" forward(Fortinet) ; Rule 1
```

In this rule, only client host 1.1.1.1 is used, but in the web access layer, the whole subnet 1.1.1.0/24 is used, so this is a partial match. In this case, the original rule would not be changed, but another proxy policy will be created before the original proxy policy:

```
config firewall policy
edit 70010001 --- The prefix “7xx” is added for new forwarding rules.
set type explicit-web
set explicit-web-proxy "web-proxy"
set dstintf "INTERNET"
set srcaddr "h-1.1.1.1" --- The traffic of the forwarding rule.
set dstaddr " fortinet.com "
set service "webproxy"
set webproxy-forward-server "Fortinet" --- the forward server from the forwarding rule
set action accept
next
edit 10001
   set type explicit-web
   set explicit-web-proxy "web-proxy"
   set dstintf "INTERNET"
   set srcaddr "n-1.1.1.0_24"
   set dstaddr "fortinet.com "
   set service "webproxy"
   set action acceptnext
end
```

The first proxy policy is created with the forward server because only host 1.1.1.1 needs to be forward according to the forwarding rule. The second proxy policy is converted from the original web access rule, which does not need to be forwarded.

The newly created proxy policies from forwarding layer merge would have prefix “**7xx**”. For example, if three proxy policies from forwarding layer merge are created for proxy policy 10001, their policy names will be 70010001, 70110001 and 70210001.

The order of layer merge

The order that FortiConverter merge the layers into proxy policies is: 1. SSL intercept layer, 2. Authentication layer and 3. Forwarding layer, and the merged policy list of the previous layer would become the input policy list of the next layer merge.

For example, if a proxy policy 10001 has one partial match to the SSL intercept layer, then the merged policy list will become:

50010001, 10001

Then this policy list will match with the authentication layer. If it is found that 50010001 has one partial match, and 10001 has two partial matches, then the created policies will be places just before the merged policies. The merged policy list will become:

60010001, 50010001, 60110001, 60210001, 10001

50010001 is the proxy policy created from 60010001, and 50110001 and 50210001 are created from 10001.

All these proxy policies will match with the forwarding layer. If there is one match with 5010001 and one match with 10001, then the merged policy list will become:

60010001, 50010001, 70010001, 60110001, 60210001, 70110001, 10001

After the layer merge, the proxy policy list becomes longer, but in this way, it approaches the behavior of the multi-layer rules configured in Bluecoat.

Check Point Conversions

Check Point system information

Check Point configuration files are exported from **Smart Center** or **Provider-1**, Smart Center contains the configuration of multiple firewalls and policy packages. In the conversion process, FortiConverter requires users to select the target firewall/firewall cluster and the corresponding policy package. Therefore, please find out the name of the target firewall/firewall cluster to be converted, and the name of the policy package installed on the target firewall/firewall cluster to ensure accuracy of the conversion results.

For the Smart Center with version above R80.10, the policy package configurations should be exported via Smart Console. Please navigate to the desired policy package and export into two CSV format files, saved into <firewall rules>.csv and <nat rules>.csv. For the steps to save Check Point configuration files, please see Saving the Check Point source configuration file on page 73.

Check Point differences

General

- The FortiGate `set allowaccess` command for interfaces doesn’t exist on Check Point. Because FortiGate requires this setting, FortiConverter enables all services for interfaces by default.
- The interface **Lead to Internet** is a default static route on FortiGate.
- FortiConverter supports Traditional Mode and Simplified Mode IPSec.

Schedule configuration

FortiConverter converts "Day in month" time schedules to FortiGate one-time schedules. It converts "Day in week" and "None" schedules to recurring schedules.

You assign a year range for the "Day in month" schedule. If the specified day doesn't exist for a certain month, FortiConverter doesn't generate the one-time schedule for that month.

NAT and policy configuration

FortiConverter supports the conversion of the following NAT types:

- Hide NAT
- Static NAT
- Manual NAT

FortiConverter doesn't convert NAT global properties.

VPN configuration

Both of the Check Point IPSec VPN modes are supported:

- **Traditional Mode*** (Support only before R80.10)

- **Simplified Mode**

Check Point doesn't configure VPN within a firewall rule. When FortiConverter converts the configuration to FortiGate, it generates several VPN policies from non-"Lead to Internet" interfaces to the "Lead to Internet" (default route) interface.

After FortiConverter converts the VPN configuration, the VPN policy destination interface refers to the "Lead to Internet" interface. If you changed the default route egress interface, you may need to update the VPN/Policy configuration manually.

FortiConverter can detect and convert meshed and star VPN topologies in Simplified form.

To convert Traditional Mode policies to Simplified Mode policies, use the Check Point Security Policy Converter Wizard. This can be found by clicking **Policy > Convert to > Simplified VPN** from the Check Point SmartDashboard.

Service objects

Unlike FortiGate service objects, Check Point service objects have a protocol type attribute. FortiGate uses a session helper object to provide the same functionality as the service objects with a protocol type attribute.

Saving the Check Point source configuration file

Before starting the conversion wizard, save a copy of your Check Point configuration file to the computer where FortiConverter is installed.

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 Provider 1 on page 74

Saving the Check Point source configuration file from Smart Center on page 77

Saving the Check Point source configuration file from VSX Gateway on page 85

Saving the Check Point source configuration file from Provider 1

1. Provider – 1 to Fortigate conversion

Usually used while converting a single checkpoint firewall to a Fortigate. In this case chose "Smartcenter" option while doing the conversion

1.1 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.

1.2 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.

1.3 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		

File	File name	Location	Path or command
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/**

2. Provider - 1 to FortiManager conversion

Usually used while converting a multiple checkpoint firewall configuration to Fortimanager output. In this case use "Provider-1" option while doing the conversion

- **MDS definitions** – "mdss.C" This file contains the MDS hierarchy.
- **MDS object definitions** – "objects_5_0.C" This file contains the definition of domains in each MDS.
- **Global object definitions** – "objects_5_0.C" This file contains the definition of objects used in global policies.
- **Global policy rule bases** – "rulebases_5_0.fws" This file contains the definition of global policies.
- **Global policy assignments** – "customers.C"
- **CMA domain files** – Every CMA needs a set of "objects_5_0.C", "rulebases_5_0.fws" and "fwauth.NDB" (optional) files as the input.

File Path:

File	File name	Path
MDS definitions	mdss.C	`$MDSDIR/conf/mdsdb`
MDS object definitions	objects_5_0.C	`$MDSDIR/conf/mdsdb`
Global object definitions	objects_5_0.C	`$MDSDIR/conf/`
Global policy rule bases	rulebases_5_0.fws	`$MDSDIR/conf/`

File	File name	Path
Global policy assignments	customers.C	`$MDSDIR/conf/mdsdb`
CMA object definitions	objects_5_0.C	Path format: "`/opt/<mds name>/customers/<Domain mgmt. server name>/<CMA>/<fw name>/conf`"
CMA policy rulebases rulebases_5_0.fws	CMA policy rulebases rulebases_5_0.fws	e.g. "`opt\CPmds-R76\customers\domain-1_Management_Server\CPsuite-R76\fw1\conf`"

Uploader Icons used in tool:

Saving the Check Point source configuration file from Smart Center

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/`

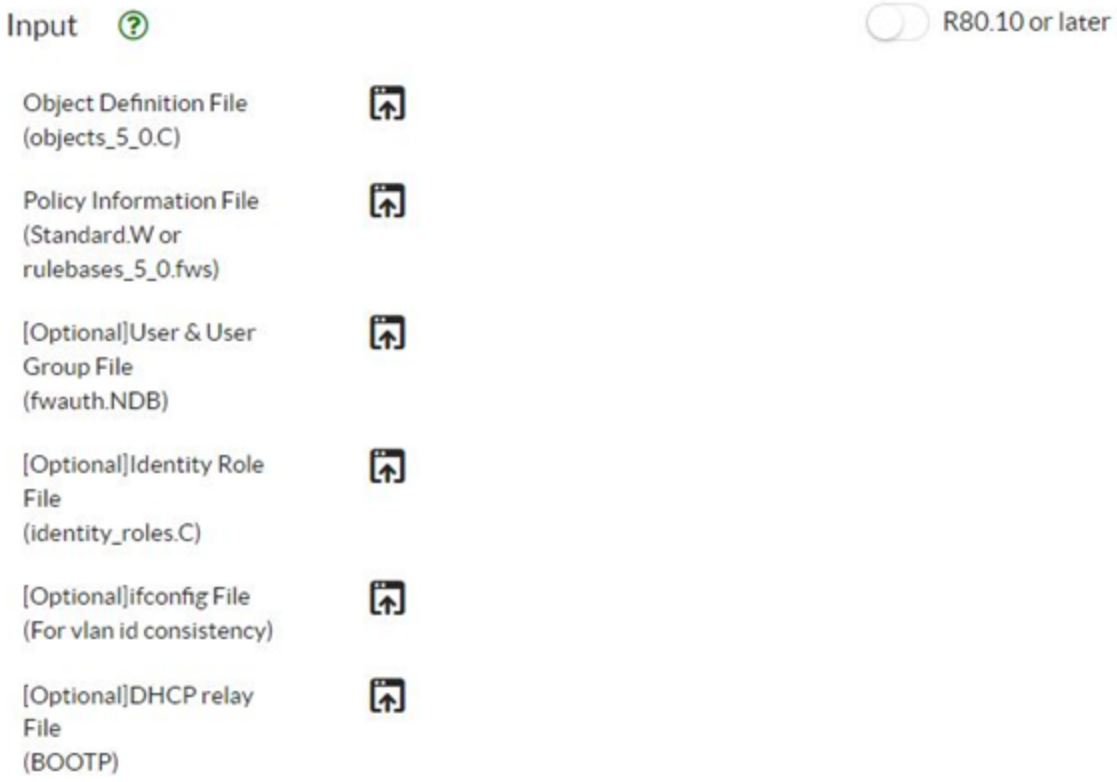
Policy rulebases	rulebase_5_0.fws <package name>.W	SmartCenter	`$FWDIR/conf`

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`

File	File name	Location	Path or Command
DHCP relay file	NA	Gateway	`show configuration bootp`

Uploader Icons used in tool:



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

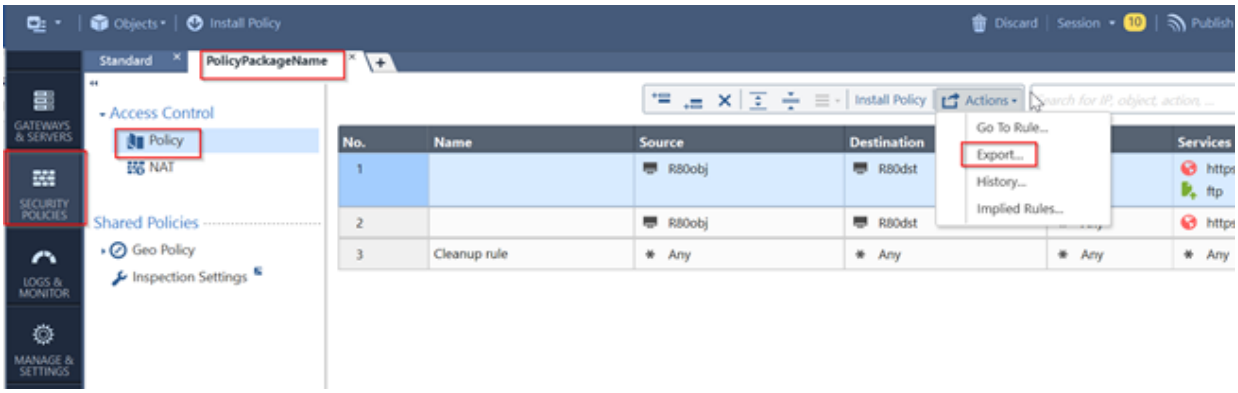
- **Object definitions** – "objects_5_0.C" (Check Point NG/NGX) or "objects.C" (Check Point 4.x) contains the firewall's object definitions.
- **Rule definitions** – "*.csv". The Policy and NAT CSV files can be exported from the Smart Console (refer screenshot below). Before exporting, please display all the columns of the rule tables to ensure that all necessary information is exported.
- **[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.

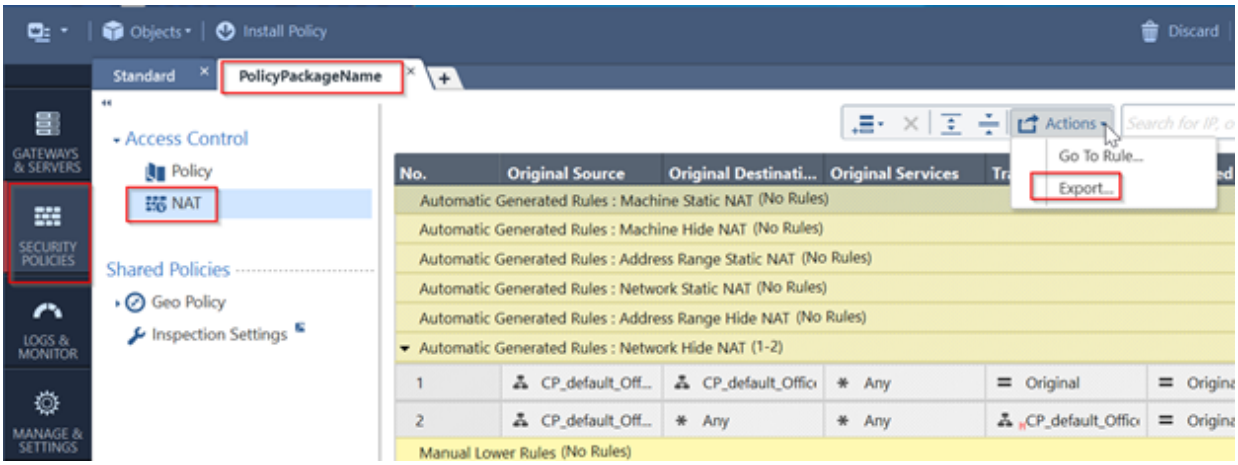
File Path:

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`

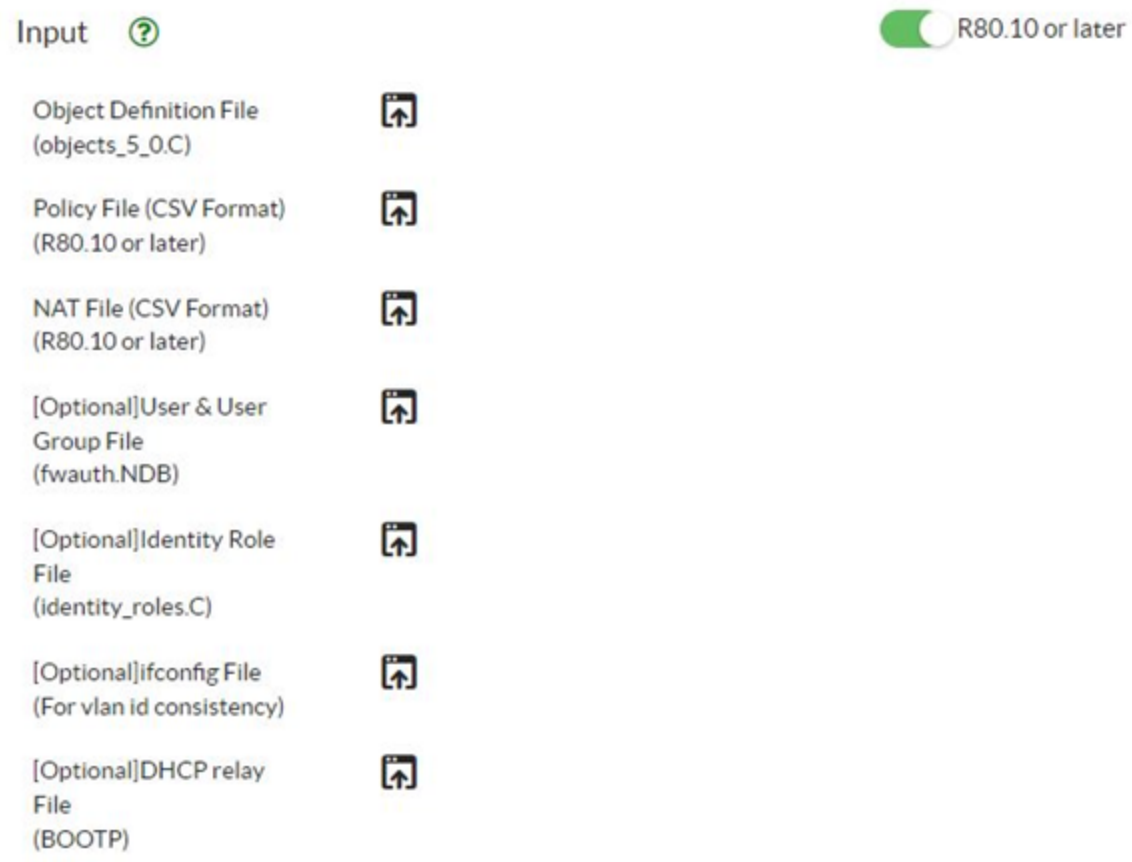
Export Policy file (CSV Format):



Export Nat file (CSV Format)



Uploader Icons used in tool:



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`**

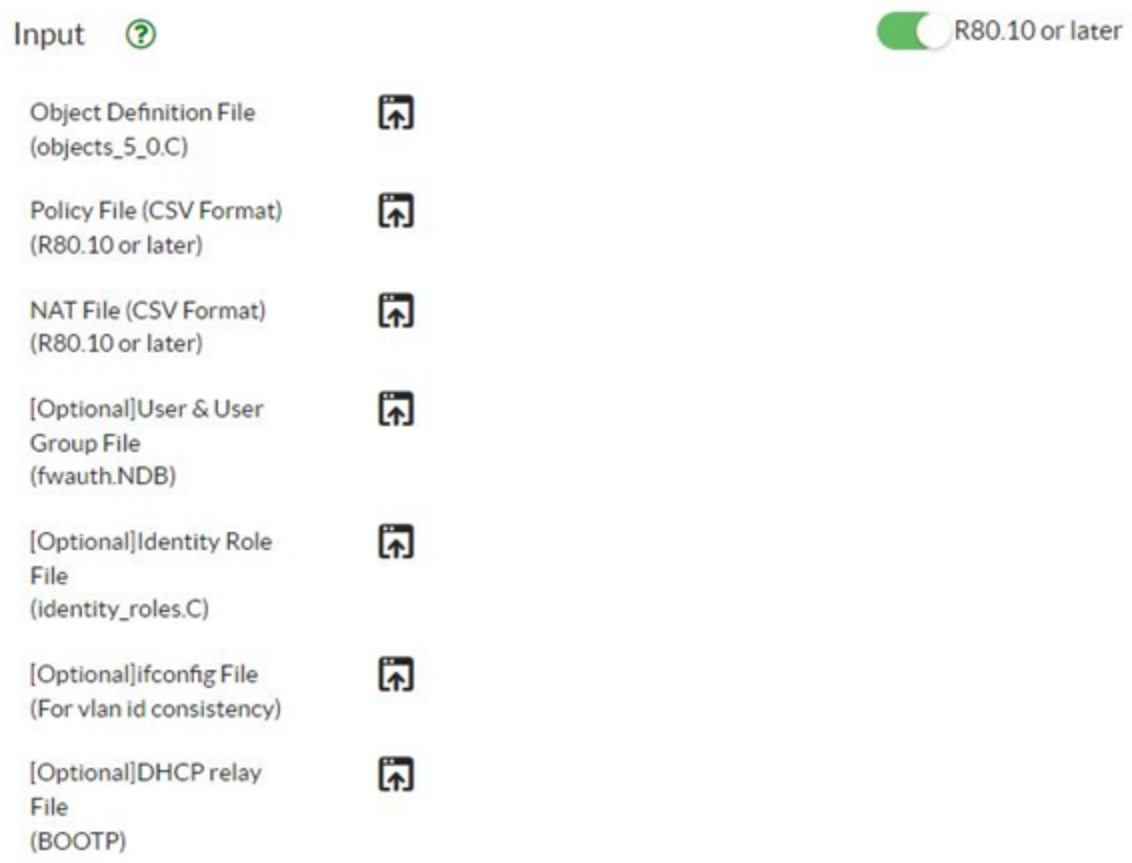
4. Smart Center is on R80.10 and later but Gateways are below R80 such as R77

- **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`



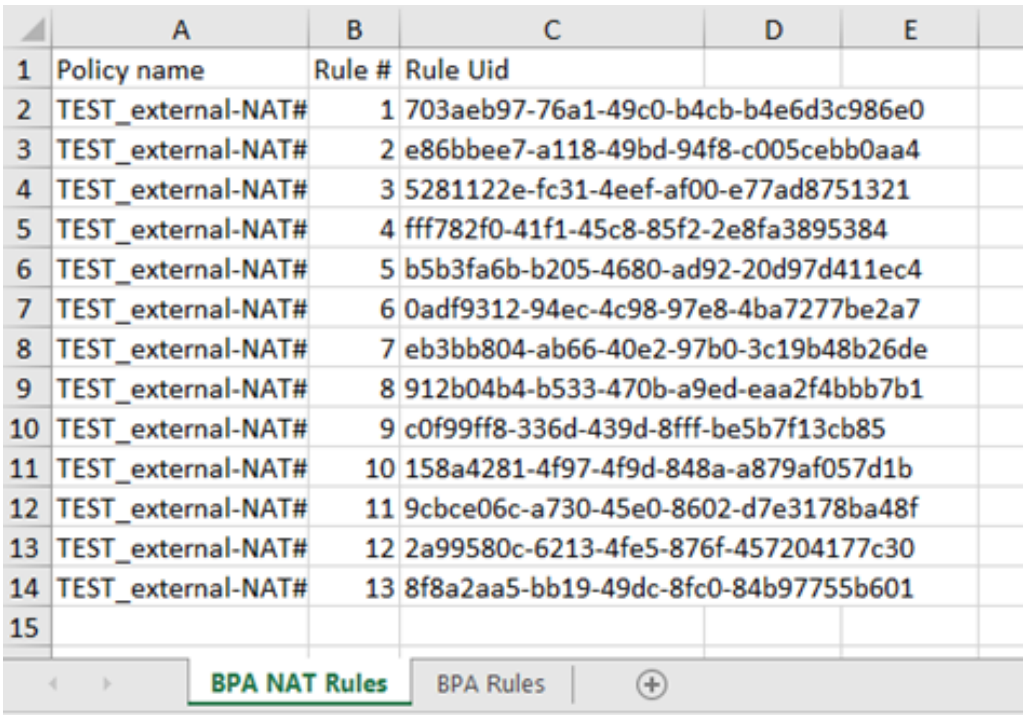
Note: Alternately, you can choose to download Policy and rule definitions file "`rulebases_5_0.fws`" from following path if you are interested to cross verify it with CSV file: **/opt/CPR77CMP-R80/conf**

[Optional] Policy and NAT Rule File with UUIDs

This input file entry accepts an Excel worksheet which contains the UUID of firewall and NAT rules. The format of this file is as below:

1. The Excel file can contain 2 sheets, one for firewall rules and one for NAT rules. The sheet which contains the keyword "NAT" in its name is the NAT rule table, and the other is the policy table.
2. There can be multiple columns in the sheets, but FortiConverter needs to read 2 columns inside. The first one is "Rule #" which shows the rule number in Check Point and this number should be consistent with the rule number in the CSV files. The second one is "Rule Uid", which shows the UUID of the rules.
3. The number and order of the rules are always the same as the rules in the CSV files so the tool can always correlate them based on the rule number instead of checking the content.

Please see an example of the file below:



	A	B	C	D	E
1	Policy name	Rule #	Rule Uid		
2	TEST_external-NAT#	1	703aeb97-76a1-49c0-b4cb-b4e6d3c986e0		
3	TEST_external-NAT#	2	e86bbee7-a118-49bd-94f8-c005cebb0aa4		
4	TEST_external-NAT#	3	5281122e-fc31-4eef-af00-e77ad8751321		
5	TEST_external-NAT#	4	fff782f0-41f1-45c8-85f2-2e8fa3895384		
6	TEST_external-NAT#	5	b5b3fa6b-b205-4680-ad92-20d97d411ec4		
7	TEST_external-NAT#	6	0adf9312-94ec-4c98-97e8-4ba7277be2a7		
8	TEST_external-NAT#	7	eb3bb804-ab66-40e2-97b0-3c19b48b26de		
9	TEST_external-NAT#	8	912b04b4-b533-470b-a9ed-eaa2f4bbb7b1		
10	TEST_external-NAT#	9	c0f99ff8-336d-439d-8fff-be5b7f13cb85		
11	TEST_external-NAT#	10	158a4281-4f97-4f9d-848a-a879af057d1b		
12	TEST_external-NAT#	11	9cbce06c-a730-45e0-8602-d7e3178ba48f		
13	TEST_external-NAT#	12	2a99580c-6213-4fe5-876f-457204177c30		
14	TEST_external-NAT#	13	8f8a2aa5-bb19-49dc-8fc0-84b97755b601		
15					

BPA NAT Rules | BPA Rules

Saving the Check Point source configuration file from VSX Gateway

When VSX feature is enabled and multiple Virtual Systems are part of the VSX gateway, FortiConverter supports migrating multiple Virtual Systems with one conversion.

1. Both Checkpoint Smart Center & VSX Gateways(VS) are in version R80.10 & Later on page 85

2. Both Checkpoint Smart Center & VSX Gateways(VS) with version before R80.10 on page 87

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

- **Rule definitions** – "*.csv" or "*.zip". The Policy and NAT CSV files can be exported from the Smart Console (refer screenshot below). Before exporting, please display all the columns of the rule tables to ensure that all necessary information is exported.
  If only one VSYS needs to be converted, or all VSYS's share one policy package, input the CSV file exported from the policy package.
  If multiple VSYSs need to be converted in one shot, and they use multiple policy packages, input a ZIP file which contains multiple CSV files, each one exported from a policy package. Please see Input multiple CSV files as multiple policy packages on page 87 for more information.
- **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

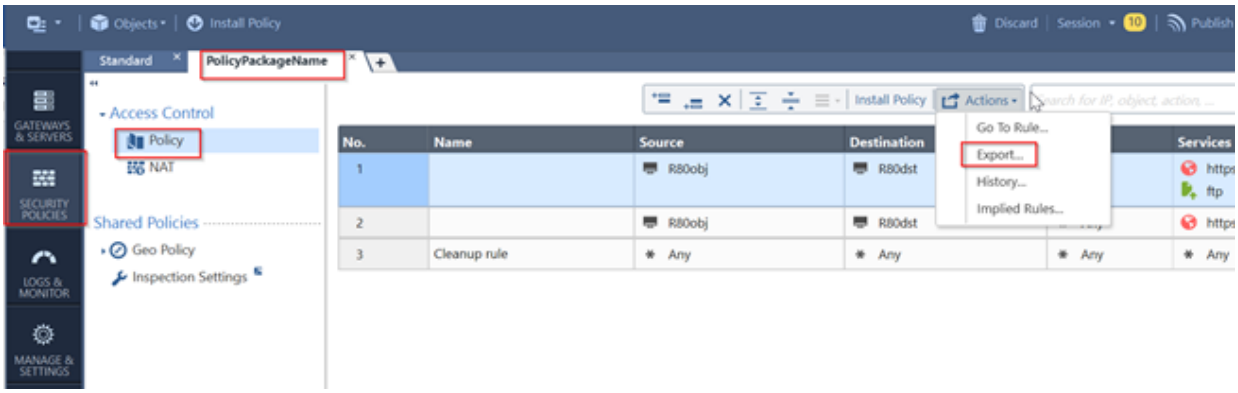
and then copy and paste the output into a plain text file. Codes in the output indicate if the route is a directly connected interface, a host route, a network route, and so on. The output varies by the platform.

- **User and user groups file (optional)** – "fwauth.NDB"

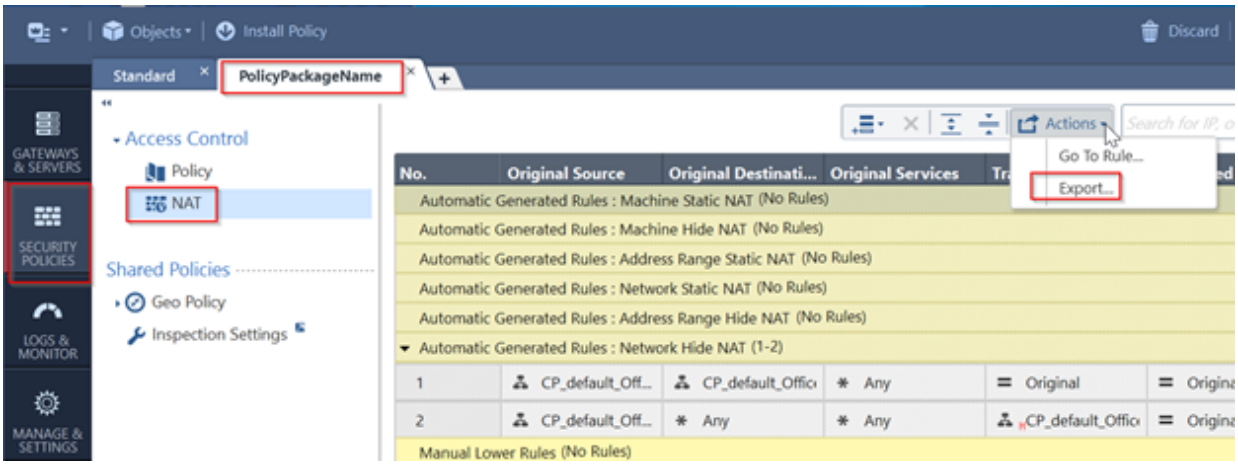
File Path

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)



Input multiple CSV files as multiple policy packages

When multiple Virtual Systems are converted in one shot, and they use multiple policy packages, we need multiple firewall rule CSV files and multiple NAT rule CSV files. To input multiple CSV files into FortiConverter, we need to archive the CSV files into ZIP files. Please follow the steps below to prepare the ZIP files:

Firewall rule ZIP file:

1. Export the firewall rules in each package into a CSV file.
2. Use the package name as the file name of each firewall rule CSV file.
3. Archive all the firewall rule CSV files into a ZIP file as the policy file input.

NAT rule ZIP file:

1. Similarly, export the NAT rules in each package into a CSV file.
2. Use the package name as the file name of each NAT rule CSV file.
3. Archive all the NAT rule CSV files into another ZIP file as the NAT file input.

For each firewall rule and NAT rule CSV file, FortiConverter uses its file name as the policy package name of the rules inside. Therefore, the firewall rule CSV file and NAT rule CSV file from the same policy package should use the same name. Although they are archived in two separate ZIP files, FortiConverter can recognize that they belong to the same package after parsing.

For example, if there is a file "package1.csv" in the firewall rule ZIP file, and there is also a file "package1.csv" in the NAT rule ZIP file, then FortiConverter would categorize those firewall rules and NAT rules into a package named "package1".

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	`$FWDIR/conf/`
			—or—
			`$FWDIR/database/`

Route	NA	Gateway	`netstat -nr`

Check Point conversion wizard

The pages that the Check Point conversion wizard shows depend on whether your source configuration is SmartCenter or Provider-1.

Because Provider-1 uses global and device-level virtual domains that are similar to FortiManager ADOMs, you convert Provider-1 configurations to policy packages and objects for your source firewalls in the FortiManager Policy & Objects database. You can only select FortiManager as the output format on the Start options page.

The administrator password is **not** set on the new configuration.

For third-party conversions, the trusted host settings are converted. Check the trusted host settings to ensure they allow management access from the relevant network interfaces.

To start a new conversion

1. Start FortiConverter.
2. When start-up is complete, a browser window automatically opens to http://127.0.0.1:8000.
3. Click New Conversion **New Conversion**, located at the top right corner.
4. Enter a name for the conversion configuration.
5. For Vendor, choose **Check Point** block.
6. Choose a Model, if applicable.
7. Click **OK**.

The configuration page opens to the Start page, and you can input your settings.

Check Point Start options

This table lists the start settings.

Setting	Description
Profile	
Description	Enter a description of the configuration.
Output Options	
Output Format	Select the appropriate output for your target Fortinet device.
FOS Version	The configuration syntax is slightly different among FortiOS 6.4, 7.0, 7.2, 7.4 and 7.6. Select the version that corresponds to the FortiOS version on the target.
Smart Center and VSX Input	
Before R80.10	Select this option if the configuration is from a SmartCenter device with version before R80.10.
R80.10 or later	Select this option if the configuration is from a SmartCenter with version R80.10 or later device.

Setting	Description
JSON Export	Select this option if the configuration is an archived JSON file exported from the Check Point “ShowPolicyPackage” tool.
Object Definition File (objects_5_0.C)	Select the object definition file. This file should include the definition of firewalls, interfaces and firewall objects.
Policy Information File (Standard.W or rulebases_5_0.fws)	Select the policy information file. This file should include the policy informations and manual NAT rules in each policy package. This is only needed for devices with SmartCenter version before R80.
Policy File (CSV Format) (R80.10 or later)	Select the policy file in CSV format. This is only needed when "R80.10 or later" is selected.
NAT File (CSV Format) (R80.10 or later)	Select the NAT rule file in CSV format. This is only needed when "R80.10 or later" is selected.
[Optional] User & User Group File(fwauth.NDB)	Select the user and user group file.
[Optional] Identity Role File (identity_roles.C)	Select the identity role file.
[Optional] ifconfig File (For vlan id consistency)	Select the result text file from linux command "ifconfig" output. The file would help to determine the vlan-id of interfaces if provided. (Smart Center only)
[Optional]DHCP relay File (BOOTP)	Select the file which contains the DHCP relay information of interfaces. (Smart Center only)
[Optional] Policy and NAT Rule File with UUIDs	An Excel file which contains the UUIDs of policies and NAT rules in Check Point.
Provider-1 Input	
MDS Definition File (mdss.c)	Select the MDS definition file. This file should include the MDS hierarchy.
MDS Object File (objects_5_0.c)	Select the MDS object definition file.
Global Policy Object File (objects_5_0.c)	Select the global object definition file. This file should include the definition of global objects.
Global Policy Rulebase File (rulebases_5_0.fws)	Select the global policy information file. This file should include the information of policies and manual NAT rules in each global policy package.
Global Policy Assignment(customer.C)	Select the global policy assignment file.

Setting	Description
Target device (Optional)	
Target device	Select the model of the target device, or select a device connected to FortiConverter.
Conversion Options	
Discard unreferenced firewall objects	This option can be useful if your target device has table size limitations. You can view the unreferenced objects that FortiConverter removed on the Tuning page.
Automatically generate policy interfaces	Specifies whether FortiConverter generates policy interfaces using a Check Point route file. (For example, a file you obtained using the netstat -nr command.) You select the route file on the Policy package page. Check Point policies define rules for network-to-network communication. When you migrate a Check Point configuration to FortiGate, which uses policies that define rules for interface-to-interface communication, you can use the Check Point router information to determine which interface a policy uses. If you disable this option, or router information isn't available, FortiConverter uses the "any" interface. This option is disabled in Provider-1 conversion.
Increase Address and Service Table Sizes for High-End Models	You can customize the maximum table sizes that FortiConverter uses when **Adjust table sizes** is selected. For more information, see Adjusting table sizes on page 232.
Route-based IPSec	Specifies whether Route-based IPSec is used for this conversion.
Generate global objects in a separate file	FortiConverter can distinguish global objects in the configuration and output the converted global objects into a separated file.
Remove self-traffic addresses and polices	Self-traffic polices should be configured in Check Point, but they are not necessary in FortiOS. FortiConverter comments out the self-traffics policies or remove self-traffic addresses from policies when this option is enabled.
Number of year-long schedules from day in month schedules	Specifies how many years of one-time schedules to generate. The wizard converts Check Point "day in month" schedules into

Setting	Description
	equivalent one-time FortiGate schedules.
Policy index start from 1 instead of 10000	When selected, the serial number of firewall policies will start from 1 instead of 10000.
Split Address group From VPN Phase2 selector	If the remote side of VPN is not a FortiGate but a device of other vendor, setting an address group in the VPN phase2 quick selector does not work. When this option is enabled, a VPN phase2 object with an address group in the selector would be split into multiple objects with subnet or a range in selector.
Get routing info from source configuration file	Fet the routing information from the source configuration file instead from nstats command
Add prefix to the address objects which will trigger VIP/DNAT	Adds "v-" prefix to the name if an address would be referenced in a VIP.
NGFW policy-based mode	When selected, the conversion will be in NGFW policy-based mode. "`firewall policy`" will become "`firewall security-policy`" instead, and "`set application 00000`" will be generated in policies, which requires manual processing. There will also be some other minor differences adapted for the NGFW policy-based CLI.
Enable merging of parent inner layer policy to child policies	When a policy has action "inner layer", and its child has src/dst address as "any", the policy's address will apply to the child's.
Generate configurations with all VDOMs merged	Select this option if a merged config folder of all the converted VDOMs is required in the output config folder. When you migrate a Check Point configuration to FortiManager. You can use this option to get a merged folder including policies and firewall objects. (SmartCenter and Povider-1 only)
Use FQDN instead of URI in firewall address	When this option is enabled, the names will be trimmed from URI to FQDN in firewall address objects.
Comment Options	
Interface Comment	Specifies whether FortiConverter copies the interface comment from the source

Setting	Description
	configuration to the mapped FortiGate interface.
Address Comment	Specifies whether FortiConverter copies the address comment from source configuration to the converted FortiGate address.
Service Comment	Specifies whether FortiConverter copies the service comment from the source configuration to converted FortiGate service.
Policy comment - Add policy package name and rule number	Include policy package name, policy number and NAT rule number in the comment of output policy.
Policy comment - Preserve the original comment	Include the original comment in source file in the comment of the output policy.
Policy comment - Preserve UUID from the original rule	Append the policy UUID given in the Check Point source config as part of policy comments to make it easier to correlate source and converted policies .
Separate multiple comments into different lines	When a policy is merged from multiple firewall or NAT rules, the original comments of the rules would be concatenated directly as the comment of the new policy. Enable this option to separate the original comments into different lines inside the new comment.
NAT Merge Options	
Enable Central NAT merge	Specifies whether FortiConverter converts NATs to FortiGate central NATs instead of policy-based NATs.
Ignore firewall policies with all or any addresses when processing NAT rules	Specifies whether FortiConverter ignores firewall policies with an "all" or "any" address when it merges a NAT rule and a firewall policy to create a FortiGate NAT policy. FortiConverter creates new policies in the output configuration based on where NAT rules to firewall policies intersect. Because firewall policies that use "all" or "any" as the address create many intersections, Fortinet recommends that you ignore them.

Setting	Description
Convert Static NATs into VIP/source NAT pairs	When this option is enabled, a static NAT rule would be converted into a central SNAT rule and an unidirectional VIP object. Otherwise it would be converted into a bidirectional VIP object
Disable arp-reply for all IP pools and VIPs	Add "set arp-reply disable" for all IPPool and VIPs
Use translated source addresses in NAT rules as IP pool names	When this option is enabled, IP pool names will be the translated source address names in NAT rules instead of their IP values.
Generate central NAT rules with "set nat disable" for destination NAT rules	If a destination NAT rule in Check Point is only converted into a VIP in FortiGate, the traffic may accidentally hit a central NAT rule and its source address may be translated by mistake. This is because source and destination NATs are included in one NAT rule list in Check Point, but VIP and central NAT are separated modules in FortiGate. When this option is enabled, central NAT rules with "set nat disable" will be generated for destination NAT rules to prevent unnecessary source address translation.
Enable identity match of NAT policy	Specifies whether FortiConverter converts or ignores any identity NAT rules in the source configuration. The "range" and "network" address objects in a Check point configuration can include hide NAT and static NAT. Check Point performs NAT only when a host in the IP range of the address object communicates with a host outside that range. To disable NAT for traffic with both source and destination inside the address range, Check Point generates an automatic rule called an "identity NAT rule". By default, FortiConverter excludes this type of rule from the conversion because it performs no NAT after it is converted and generates redundant policies. You can enable this option to generate policies based on the identity NAT rules.
NAT Merge Depth	

Setting	Description
Hide NAT **Static NAT** **Rule NAT**	Specifies which types of NAT FortiConverter merges with the output firewall policies, or whether FortiConverter performs NAT merge based on object names or values. • Off – FortiConverter converts firewall policies only and doesn't perform NAT merge for this type of NAT. This is useful for performing a quick, initial conversion to discover any conversion issues. • Object Names – FortiConverter performs NAT merge based on matching address names in firewall policies and NAT rules. • Object Values – FortiConverter performs NAT merge based on matching address values in firewall policies and NAT rules. It generates the most accurate matching of NAT rules and policies, but in most cases, it also generates more NAT policies. Because it can take FortiConverter several hours to complete a conversion that include a large number of NAT rules, Fortinet recommends that you turn off or limit NAT merge for your initial conversion. Then, resolve any issues with the conversion before you run it again with NAT merge enabled. For more information, including example matches, see NAT merge options on page 233.

MDS selection (Provider-1 only)

Setting	Description
Select the MDS to convert	Choose the domain to convert.

Global policy collection (Provider-1)

Setting	Description

Standard_Global_Policy	Specifies whether FortiConverterconverts the Standard Global Policy. You can select both **Standard Global Policy** and **Simple Global Policy**.
Simple_Global_Policy	Specifies whether FortiConverter converts the **Simple Global Policy**.

Check Point Source Configuration (Provider-1)

A Provider-1 configuration contains multiple domains. Input the object definition, policy package information, and user file in this page.

Ensure the configuration is in a text format. FortiConverter can't use binary files.

See Saving the Check Point source configuration file

Setting	Description
Browse	Click to navigate to the domain source configuration file. See Saving the Check Point source configuration file.

Firewall selection

Setting	Description
(firewall items)	Please select one or more firewalls to convert from the source configuration.
Information of Configurations	Source configuration file names are shown in the table. Click the file name to see the content. But if the file size is too large, the file can't be shown.
Mapped VDOM Name	The converted VDOM name for the firewall in FortiGate.
Hostname	The name of the managed device which the converted interface or route configuration would be imported in FortiManager. (Only available when the output format is **FortiManager**) If the hostname is not input, the policy installation and the dynamic mapping of normalized interfaces in FortiManager would not be correctly converted.
Manage IP	When the firewall is configured in transparent mode, the management IP needs to be input for the converted FortiGate VDOM.
Source Configuration Preview	The numbers of each kind of firewall objects are shown in the table above. By clicking the object number, the detailed information of each object is listed in the table below. In each type of object, click the button **Export CSV** to export the current object info as CSV file.

Policy collection

Setting	Description
(policy collection item)	Select the policy collections to convert.
Route File (optional)	Select the file of the route information exported from the selected firewalls using the **netstat -nr** command. If the format of the route file is incorrect, there would be a document pop up and please follow the instruction inside to correct the route format. If **Automatically generate policy interfaces** is selected on the Start options page, the route file would be required. FortiConverter needs the route information to correctly calculate the interfaces.
Policy packages viewer	Select the policy package name and the detail of each policy in the package listed in the table.

Check Point Interface mapping

You can manually map the interface.

- To **select** the appropriate FortiGate interface, click the value in the FortiGate Interface column, and then select a value or enter a custom interface name.
- To **edit** other values, double-click the proper column. Use the toolbar icon on the right to show and hide columns. You can also use the Tuning page to create mappings after the conversion is complete.
- To **import** a set of interface mappings from a file, click **Import**.
- To **download** the current set of interface mappings, click **Export**.
- To **delete** an interface, select the entries you would like to delete, **right click** and select **Delete Selected**. This is useful if your target FortiGate has fewer interfaces than the source configuration.

The limit of the length of interface names in FortiOS is 15 characters. Interfaces in the source config which have longer names should be trimmed to a shorter name. It is recommended to trim the names manually to ensure readability. But if a quick trimming is needed, please select the entries, **right click** and select **Trim Interface Name** to trim the names into 15 characters automatically.

Setting	Description
VDOM	Shows the virtual domains used in the conversion. ("root" by default)
Source Interface	Shows each interface on the Check Point firewall.
FortiGate Interface	The input field for corresponding FortiGate interface names. Click to assign a FortiGate port or input the interface name manually for each interface. (Only available when the output format is **FortiGate**)
Normalized interface	The input field for corresponding normalized interface names, which would be configured in the ADOM database in FortiManager. Click to assign a port or input the interface name manually for each interface. (Only available when the output format is **FortiManager**)
Device interface	The input field for corresponding interface names in the managed devices in FortiManager. Click to assign a port or input the interface name manually for each interface. (Only available when the output format is **FortiManager**)
Members	Shows any members, if they are set.
IP-Netmask	Shows the IP address and netmask of the connection.
Type	Shows the type of interface.
Access	Shows which protocols has permission to access each interface.
Import	Click to load a set of interface mappings from a text file.
Export	Saves the current set of interface mappings to a text file.
Delete Selected	Click to delete the selected mapping item.
Trim Interface Name	Trim the interface names which exceed 15 characters into 15 characters automatically.

Check Point Route information

FortiConverter creates static routes in the output using the static routes it detects in the source configuration and any routing information you provide.

Double-click an item to edit it.

Setting	Description
New Route	Click to add a route.
Delete Selected	Click to delete the selected route.

Check Point Conversion result

Tab	Description
Conversion Summary	Provides information about the conversion.
Reports	Generate PDF reports including converted and unconverted objects list.
VDOM Mapping	Shows how VDOMs were mapped from the source device to the new device.
Interface Mapping	Shows how interfaces were mapped for each VDOM from the source device.
Device Summary	Provides statistics about the objects detected.

For more information, see View Conversion Summary on page 248

FortiConverter includes error and warning messages into the conversion when an error occurs.

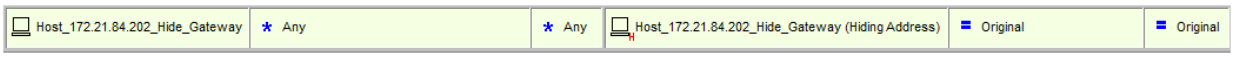
Review the `config-all.txt` file after each conversion for errors. These errors and warning messages might cause the import process to fail, if not corrected. See for more details.

Check Point NAT merge examples

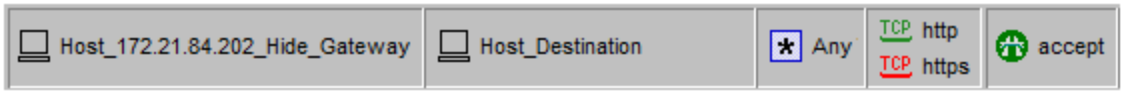
For more information on how handles NAT merges, see NAT merge options on page 233.

Host address hides behind gateway

The source configuration hides the host address object `Host_172.21.84.202_Hide_Gateway` behind the gateway.



It also has a firewall rule that matches the object to source addresses.



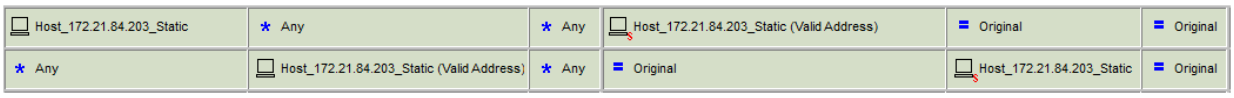
FortiConverter generates the following policy, for which NAT is enabled (`set nat enable`). However, because it doesn't specify an IP pool, the source address uses the interface IP address to perform NAT:

```
edit 10002
   set srcintf "port2"
   set dstintf "port1"
   set srcaddr "Host_172.21.84.202_Hide_Gateway"
   set dstaddr "Host_Destination"
   set service "http" "https"set schedule "always"
   set logtraffic allset status enableset action acceptset comments "Example of address
        hides behind gateway."
   set global-label "FW1"
   set nat enable
next
```

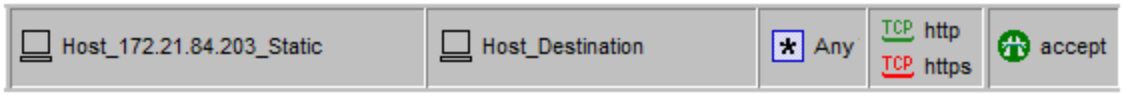
When a policy has NAT enabled, it attempts to match a source address to a VIP object. If it finds a match, it performs static NAT using the VIP object. If it doesn't find a match, it uses the interface IP address. (See the next section for an example with a VIP object.)

Address with static NAT matches policy source address

The source configuration static NAT settings translate the IP address of the host address object `Host_172.21.84.203_Static` to `210.61.82.160`.



It also has a firewall rule that matches the object to source addresses.



FortiConverter generates the following VIP object and policy:

```
edit "vip-Host_172.21.84.203_Static"
   set extip 210.61.82.160
   set mappedip 172.21.84.203
   set extintf port1
   set nat-source-vip enable
next
```

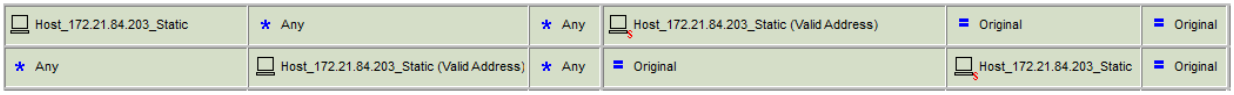
```
edit 10003
   set srcintf "port2"
   set dstintf "port1"
   set srcaddr "Host_172.21.84.203_Static"
   set dstaddr "Host_Destination"
   set service "http" "https"set schedule "always"
   set logtraffic all
   set status enable
   set action accept
```

```
   set comments "Example of address with static NAT in source address."
   set global-label "FW1"
   set nat enable
next
```

When a policy has NAT enabled, it attempts to match a source address to a VIP object. If it finds a match, it performs static NAT using the VIP object. If it doesn't find a match, it uses the interface IP address. (See Host address hides behind gateway for an example without a VIP object.)

Address with static NAT matches policy destination address

Like the example where static NAT matches the policy destination address, the source configuration static NAT settings translate the IP address of the host address object `Host_172.21.84.203_Static` to `210.61.82.160`.



It also has a firewall rule that matches the object to destinations.

FortiConverter generates the following VIP object and policy. The policy replaces the destination address with the VIP object:

```
edit "vip-Host_172.21.84.203_Static"
   set extip 210.61.82.160
   set mappedip 172.21.84.203
   set extintf port1
   set nat-source-vip enable
next
```

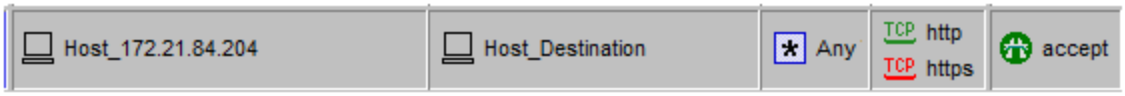
```
edit 10004
   set srcintf "port1"
   set dstintf "port2"
   set srcaddr "Host_Source"
   set dstaddr "vip-Host_172.21.84.203_Static"
   set service "http" "https"
   set schedule "always"
   set logtraffic all
   set status enable
   set action accept
   set comments "Example of address with static NAT in destination address."
   set global-label "FW1"
next
```

In this case, the destination address is used directly.

Manual NAT rule matches policy source address with one-to-one mapping

A source configuration has a manual NAT rule that translates a source address:

It also has the following firewall rule:



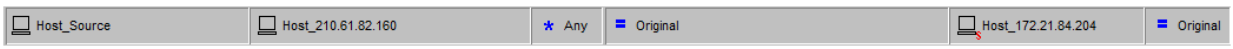
This configuration is a one-to-one mapping because both the original address and translated address are host addresses.

FortiConverter generates the following IP address pool and policy. NAT is enabled for the policy and it uses the pool to perform NAT:

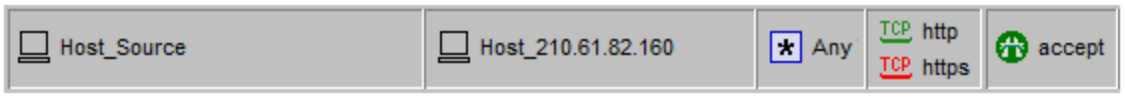
```
edit "ippool-210.61.82.160"
   set endip 210.61.82.160
   set startip 210.61.82.160
   set type overload
next


edit 10005
   set srcintf "port2"
   set dstintf "port1"
   set srcaddr "Host_172.21.84.204"
   set dstaddr "Host_Destination"
   set service "http" "https"
   set schedule "always"
   set logtraffic all
   set status enable
   set action accept
   set comments "Example of one to one source NAT rule ."
   set global-label "FW1"
   set nat enable
   set poolname "ippool-210.61.82.160"
next
```

Manual NAT rule matches policy destination address

A source configuration has a manual NAT rule that translates a destination address:



It also has the following firewall rule:



FortiConverter generates the following VIP object and policy:

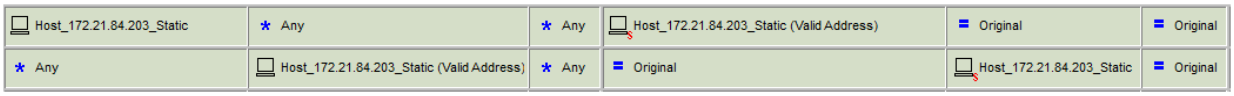
```
edit "vip-Host_210.61.82.160"
   set extip 210.61.82.160
   set mappedip 172.21.84.204
   set extintf any
   set nat-source-vip enable
next

edit 10007
```

```
   set srcintf "port1"
   set dstintf "port2"
   set srcaddr "Host_Source"
   set dstaddr "Host_172.21.84.204"
   set service "http" "https"
   set schedule "always"
   set logtraffic all
   set status enable
   set action accept
   set comments "Example of one to one destination NAT rule ."
   set global-label "FW1"
next
```

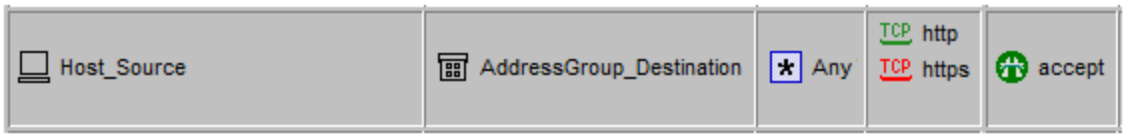
The translated address is used as the destination address because it is in internal network.

NAT rule and policy addresses don't match: Destination address of the policy contains the NAT object

A source configuration has a host address object Host_172.21.84.203_Static that Static NAT translates to 210.61.82.160.



It also has the following firewall rule:



AddressGroup_Destination is a group that contains the members `Host_172.21.84.203_Static`, `Host_Member3`, and `Host_Member4`.

FortiConverter generates the following VIP object and NAT policy:

```
edit "vip-Host_172.21.84.203_Static"
   set extip 210.61.82.160
   set mappedip 172.21.84.203
   set extintf port1
   set nat-source-vip enable
next

edit 110009
   set srcintf "port1"
   set dstintf "port2"
   set srcaddr "Host_Source"
   set dstaddr "vip-Host_172.21.84.203_Static"
   set service "http" "https"
   set schedule "always"
   set logtraffic all
   set status enable
   set action accept
   set global-label "FW1"
next
```

```
edit 10009
   set srcintf "port1"
   set dstintf "port2"
   set srcaddr "Host_Source"
   set dstaddr "AddressGroup_Destination"
   set service "http" "https"
   set schedule "always"
   set logtraffic all
   set status enable
   set action accept
   set comments "Example of name overlap in destination address."
   set global-label "FW1"
next
```

FortiConverter converts policy 10009 directly from the original firewall rule. Policy 11009 is a copy of policy 10009 with the destination address field changed to `vip-Host_172.21.84.203_Static` to reflect the static NAT object conversion.

Unused VIP objects generate policy

In some cases, the final policy in an output configuration is one that FortiConverter generates from VIP objects that aren't used as a destination address in at least one policy. For example:

```
edit 001
   set srcintf "port1"
   set dstintf "any"
   set srcaddr "all"
   set dstaddr "vip-Host_172.21.84.24" " vip-Host_172.21.84.25" " vip-Host_172.21.84.26"
   set service "ALL"
   set schedule "always"
   set logtraffic all
   set status enable
   set action deny
   set comments "This policy is auto-generated by FortiConverter to activate static-NAT
        VIPs that aren't referenced in other policies."
next
```

This type of policy enables the source static NAT mapping by capturing all the VIP objects that other policies don't reference.

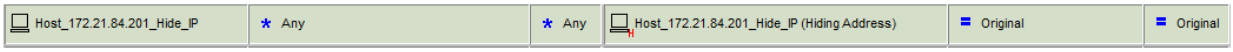
In some conversions, FortiConverter generates more than one of this kind of policy – one for each external interface that is referenced by an unreferenced VIP object.

Check Point NAT merge examples with central NAT

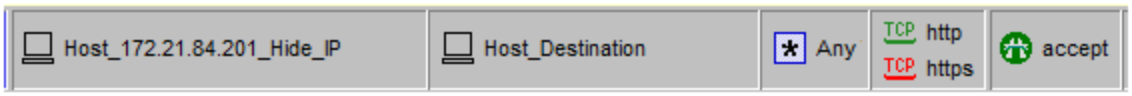
From FOS v6.0.0 release, the central NAT feature was enhanced. You don’t need to add a "set nat enable" clause into each firewall policy command view. This makes the central NAT module run as a separated functional part.

Host address hides behind IP

The source configuration hides the host address object `Host_172.21.84.201_Hide_IP` behind the IP address `210.61.82.139`.



It also has a firewall rule that matches the object to source addresses.



FortiConverter captures the hide NAT IP address 210.61.82.139 in an IP pool:

```
edit "ippool-210.61.82.139"
   set endip 210.61.82.139
   set startip 210.61.82.139
   set type overload
next
```

FortiConverter also creates a central NAT object that uses the IP pool:

```
edit 3
   set srcintf "port2" (generated from route information)
   set dstintf "port1" (generated from route information)
   set orig-addr "Host_172.21.84.201_Hide_IP"
   set dst-addr "all"
   set nat-ippool "ippool-210.61.82.139"
next
```

FortiConverter converts the Check Point firewall rule into the following policy:

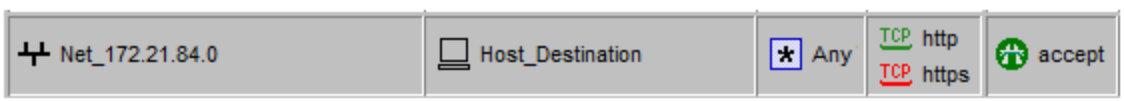
```
edit 10001
   set srcintf "port2" (generated from route information)
   set dstintf "port1" (generated from route information)
   set srcaddr "Host_172.21.84.201_Hide_IP"
   set dstaddr "Host_Destination"
   set service "http" "https"
   set schedule "always"
   set logtraffic all
   set status enable
   set action accept
   set comments "Example of address hides behind IP."
   set global-label "FW1"
next
```

Manual NAT rule matches policy source address with many-to-one mapping

A source configuration has a manual NAT rule that translates a source address:

`Net_172.21.84.0` is a network object with the IP address `172.21.84.0/24`.

The configuration also has the following firewall rule, which matches the object to source addresses:



FortiConverter converts many-to-one rules to an IP pool.

For this configuration, FortiConverter generates the following IP pool, central NAT object, and policy:

```
edit "ippool-210.61.82.130"
   set endip 210.61.82.130
   set startip 210.61.82.130
   set type overload
next

edit 2
   set srcintf "port2"
   set dstintf "port1"
   set orig-addr "Net_172.21.84.0"
   set dst-addr "Host_Destination"
   set nat-ippool "ippool-210.61.82.130"
next

edit 10006
   set srcintf "port2"
   set dstintf "port1"
   set srcaddr "Net_172.21.84.0"
   set dstaddr "Host_Destination"
   set service "http" "https"
   set schedule "always"
   set logtraffic all
   set status enable
   set action accept
   set comments "Example of one to many source NAT."
   set global-label "FW1"
next
```

Cisco Conversions

Cisco differences

General

- FortiGate's `set allowaccess` command for interfaces doesn't exist on Cisco firewalls. Because FortiGate requires this setting, FortiConverter enables all services for interfaces by default.
- The postfix "_conflict" used for services prevents a service and a service group from having the same name. It is recommended that you rename these objects.
- On Cisco IPSec VPNs, Phase 1 (ISAKMP) supports more than two types of authentication methods. FortiGate supports only two types: `pre-share` and `rsa-sig`. Therefore, you must assign methods for each VPN connection. The wizard converts Cisco EZVPN configuration to FortiGate VPN policies with the `srcintf` "<tunnel-interface-name>" (i.e. phase1-interface object name) and `dstintf` "any".
- FortiConverter doesn't support the following Cisco configuration elements:
- Wild card netmasks for `access-list` and `object- group` objects

Cisco FTD support

Cisco FTD (Firepower Threat Defense) has two modules and maintain policies on both modules:

1. LINA (layer 4 only)
2. SNORT (layer 7 inspection)

FortiConverter tool can only support FTD's LINA component but not SNORT IPS engine rules.

NAT support

Software	Supported NAT types
PIX **FWSM** **ASA (8.2 and earlier)**	Dynamic NAT (NAT exemption, policy dynamic NAT, regular) Static NAT (Static NAT, Static PAT, Identity Static NAT)
ASA (8.3 and later)	Object NAT (Dynamic, Static) Twice NAT
IOS	Dynamic NAT Static NAT
FTD (LINA)	Object NAT(Dynamic, Static) Twice NAT

FortiConverter doesn't support the following NAT features:

- Identity NAT, and NAT Exemption

To reduce the number of NAT polices a conversion generates, FortiConverter doesn't convert Static NAT rules in which the source and mapped IPs are the same.

Saving the Cisco source configuration file

Before starting the conversion wizard:**Cisco**, save a copy of your configuration file to the computer where FortiConverter is installed.

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.

For more information about Route file, please see Route File on page 243.

Save the LINA configuration from Cisco FTD

Cisco FTD (Firepower Threat Defence) has two modules and maintain policies on both modules:

1. LINA (layer 4 only)
2. SNORT (layer 7 inspection)

FortiConverter tool can only support FTD's LINA component but not SNORT IPS engine rules.

To extract FTD LINA module configuration, please use the CLI commands:

```
system support diagnostic-cli
enable(press enter)
show running-config
```

Copy and paste the outputs into a plain text file.

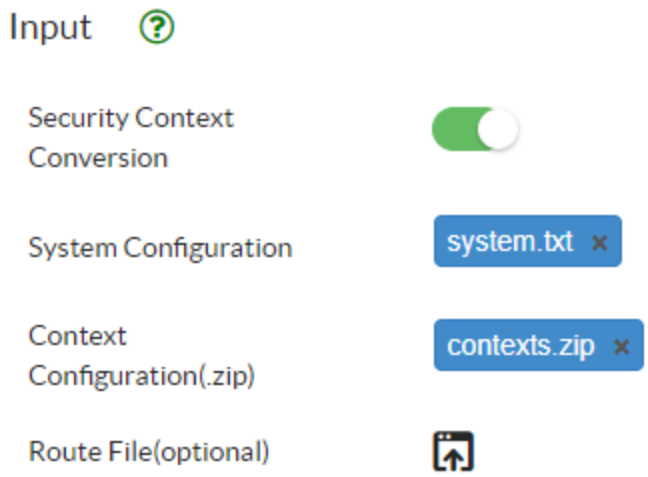
Saving and naming for multi-context configuration file

If your Cisco device contains multiple contexts, please follow the steps below to prepare the input files of FortiConverter:

1. Switch to the system execution space using the command:
   ```
   changeto system
   ```
   Then use the commands given previously to show the system configuration, and save it into a single file.
2. Switch to each context using the command:
   ```
   changeto context <context-name>
   ```
   Save the configuration of each context into a single file separately. It is fine to skip the contexts you don't want to convert.
3. Open the system file and find the context definitions inside, and rename the context config file using the names after keyword **config-url disk0:/**.
   For example, in the screen shot below, the system file contains the definition of context "admin", "test_second" and "third". Then according to the definition, rename the config of the context "admin" as "admin.cfg", context "test_second" as "test_second.cfg", and context "third" as "third.cfg".

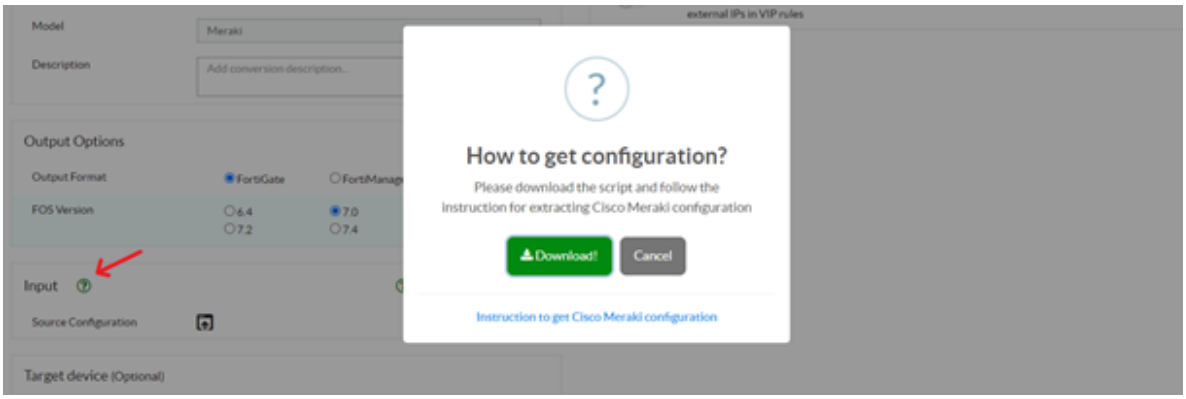
```
admin-context admin
context admin
  allocate-interface TestIntf1 outside
  config-url disk0:/admin.cfg
!

context test_second
  allocate-interface TestIntf2 Inside
  allocate-interface TestIntf3 Outside
  config-url disk0:/test_second.cfg
!

context third
  allocate-interface TestIntf4 PS-VM-PUB_175
  config-url disk0:/third.cfg
!
```

4. Archive all the context config files into a ZIP file.
5. Input the configs as below to do the conversion:



Save the configuration from 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

Cisco conversion wizard

The administrator password is **not** set on the new configuration.

For third-party conversions, the trusted host settings are converted. Check the trusted host settings to ensure they allow management access from the relevant network interfaces.

To start a new conversion

1. Start FortiConverter.

2. When start-up is complete, a browser window automatically opens to http://127.0.0.1:8000.
3. Click New Conversion **New Conversion**, located at the top right corner.
4. Enter a name for the conversion configuration.
5. For Vendor, choose **Cisco** block.
6. Choose a Model, if applicable.
7. Click **OK**.

The configuration page opens to the Start page, and you can input your settings.

Cisco Start options

This table lists the start settings.

Setting	Description
Profile	
Description	Enter a description of the configuration.
Output Options	
Output Format	Select the appropriate output format for your FortiGate device.
FOS Version	The configuration syntax is slightly different among FortiOS 6.4, 7.0, 7.2, 7.4 and 7.6. Select the version that corresponds to the FortiOS version on the target.
Input	
Security Context Conversion	Enable this option to convert configurations with multiple security contexts.
Source Configuration	Select the input file or files. This option only appears if Security Context Conversion is disabled.
System Configuration	Select the system configuration file. This file should include interfaces and config file names for each security context. This option only appears if Security Context Conversion is enabled.
Bulk Conversion	If there are many devices to be converted where all of them are the same model, sharing the same interface mapping relationship in conversion, then bulk conversion can convert all of them at once. Collect all the configuration files to be converted, compress them into a ZIP file and use the ZIP file as the input.
Context Configuration(.zip)	Select the .zip file containing all the config files. The file name for each context should match the name given in the system configuration file. This option only appears if Security Context Conversion is enabled. Please see example below in Cisco

	Start options on page 111.
Route File (Optional)	Select a route file that FortiConverter uses to determine the interfaces used in output policies, in addition to routes it detects in the source configuration. Because Cisco devices apply access-lists to source interfaces, FortiConverter can determine the source interfaces for output policies, but not the destination interfaces. When you specify a route file, FortiConverter uses the information in the file to determine the destination interface.
Target device(Optional)	
Target device	Select the model of the target device, or select a device connected to FortiConverter.
Conversion Options	
Discard unreferenced firewall objects	Specifies whether addresses, schedules, and services that aren't referenced by a policy are saved and added to the output. This option can be useful if your target device has table size limitations. You can view the unreferenced objects that FortiConverter removed on the Tuning page.
Increase Address and Service Table Sizes for High-End Models	You can customize the maximum table sizes that FortiConverter uses when **Increase Address and Service Table Sizes for High-End Models** is selected. For more information, see Adjusting table sizes on page 232
Automatically generate policy interfaces	Specifies whether FortiConverter automatically generates policy interfaces.
Route-based IPSec	Specifies whether Route-based IPSec is used for this conversion.
Suppress auto grouped items from Cisco ASDM/CSM	When an ACL contains multiple objects in its source address, destination address or service field, Cisco ASDM and CSM may automatically group them in to a group object because Cisco ASA only allows single object in each field. This option expands the grouped objects after conversion.
Combine expanded multi-object policies	When an ACL contains multiple objects in its source address, destination address or service field, Cisco CSM may expand the ACL into equivalent multiple ACLs because Cisco ASA only allows single object in each field. This option combines those ACLs into the original one automatically.
Combine policies generated by NAT merge	FortiConverter may generate multiple NAT policies after merging NAT rules into ACLs. This option combines and simplifies the output policies.

Split Address group From VPN Phase2 selector	If the remote side of VPN is not a FortiGate but a device of other vendor, setting an address group in the VPN phase2 quick selector does not work. When this option is enabled, a VPN phase2 object with an address group in the selector would be split into multiple objects with subnet or a range in selector.
Add default "accept all" rules from high to low security level interfaces	In Cisco firewalls, traffic from high security level interfaces to lower security level interfaces is allowed by default. Enable this option to create rules to allow this kind of traffic when no access list is specified.
Policy index start from 1 instead of 10000	When selected, the serial number of firewall policies will start from 1 instead of 10000.
NGFW policy-based mode	When selected, the conversion will be in NGFW policy-based mode. "`firewall policy`" will become "`firewall security-policy`" instead, and "`set application 00000`" will be generated in policies, which requires manual processing. There will also be some other minor differences adapted for the NGFW policy-based CLI.
Collect unreferenced access lists	FortiConverter typically converts those Cisco access lists which are referenced by access groups into firewall policies. However, sometimes access lists are configured on the authentication server side and would not have explicit reference in the config file, so they would not be converted. After enabling this option, FortiConverter would collect those access lists which are not reference by any part of the config, and list them in the context selection page. Users can select those access lists and convert them into firewall policies.
Enable send-deny-packet for resetoutside	When this option is enabled and config line "service resetoutside" is present in the config file, the policies with "deny" will have "send-deny-packet" enabled.
Generate SNAT when mapped IP linked to multiple external IPs in VIP rules	When same mapped IP is repeating in multiple VIP rules, but the external IP used in those rules are different. If "set nat-source-vip enable" has been added in those rules. After enabling this option, FortiConverter would create SNAT rules from those VIP rules and remove "set nat-source-vip enable".
Set extintf to "any" under "config firewall vip"	When selected, all vip extintf value will be set to “any”. Only available when central NAT mode is enabled.
Comment Options	
Address comment	Specifies whether FortiConverter copies the address comment from the source configuration to the converted FortiGate address.
Interface comment	Specifies whether FortiConverter copies the interface

	comment from the source configuration to the converted FortiGate address.
Service comment	Specifies whether FortiConverter copies the service comment from the source configuration to the converted FortiGate address.
Policy comment - Add policy package name and rule number	Specifies whether FortiConverter includes the input configuration lines used for each FortiGate policy in the FortiGate configuration as a policy comment.
Policy comment - Preserve the original comment	Include the original comment in source file in the comment of the output policy.
NAT Merge Options	
Ignore firewall policies with all or any addresses when processing NAT rules	Specifies whether FortiConverter ignores firewall policies with an "all" or "any" address when it merges a NAT rule and a firewall policy to create a FortiGate NAT policy. FortiConverter creates new policies in the output configuration based on where NAT rules to firewall policies intersect. Because firewall policies that use "all" or "any" as the address create many intersections, Fortinet recommends that you ignore them.
Enable central NAT merge	Specifies whether FortiConverter converts NATs to FortiConverter central NATs instead of policy-based NATs.
Convert Static NATs into VIP/Central NAT pairs	When this option is enabled, a static NAT rule would be converted into a central SNAT rule and an unidirectional VIP object. Otherwise it would be converted into a bidirectional VIP object
Generate central NAT rules with 'set nat disable' for destination NAT rules	If a destination NAT rule in Cisco is only converted into a VIP in FortiGate, the traffic may accidentally hit a central NAT rule and its source address may be translated by mistake. This is because source and destination NATs are included in one NAT rule list in Cisco, but VIP and central NAT are separated modules in FortiGate. When this option is enabled, central NAT rules with "set nat disable" will be generated for destination NAT rules to prevent unnecessary source address translation.
NAT Merge Depth	
Mode	Specify the source version number. This option is available only when **Model** is **ASA**.

NAT exemption	Specifies which types of NAT FortiConverter merges with the output firewall policies, or whether FortiConverter performs NAT merge based on object names or values. • **Object Name Match** – FortiConverter performs NAT merge based on matching address names in firewall policies and NAT rules. • **Object Content Overlap** – FortiConverter performs NAT merge based on matching address values in firewall policies and NAT rules. It generates the most accurate matching of NAT rules and policies, but in most cases, it also generates more NAT policies. Because it can take FortiConverter several hours to complete a conversion that include a large number of NAT rules, Fortinet recommends that you turn off or limit NAT merge for your initial conversion. Then, resolve any issues with the conversion before you run it again with NAT merge enabled. For more information, including sample matches, see NAT merge options on page 233.
Dynamic NAT	
Static NAT	
Dynamic ACL NAT	
Static ACL NAT	
Object Dynamic NAT	
Object Static NAT	
Twice Dynamic NAT	
Twice Static NAT	
Static ACL NAT	

Context selection

This page shows the source configuration before conversion.

By default, all virtual contexts are mapped to VDOMs with the same name.

Click an option under **Source Configuration Preview** to view it. Use the search bars to filter the search.

Setting	Description
VDOM Select	Select/Unselect the VDOM item.
VDOM Rename	Rename the VDOM name.
VDOM Mode	Change the VDOM mode in the output result.
Information of Configurations	Source configuration file names are shown in the table as a link. Click the link to see the content. The file won't show if it's too large.

Unreferenced Access List	When the option "Collect unreferenced access lists" is selected, FortiConverter collect access lists which are not referenced in the configuration. If you need to convert some of them into firewall policies, please select those access lists in the table.
Managed Device Name	The name of the managed device which the converted interface or route configuration would be imported in FortiManager. (Only available when the output format is FortiManager)
Manage IP	When the context is configured in transparent mode, the management IP needs to be input for the converted FortiGate VDOM.
Target Device Switch Interface - Interface/Port	If there are virtual switches in the selected target device, FortiConverter will list the member ports of the virtual switches. If an interface in the list is going to be used in the configuration, it should first be detached from the virtual switch. Click "**X**" on the interface to detach it. Please note that a detached interface cannot be re-added later by FortiConverter.
Source Configuration Preview	The numbers of each type of firewall object are shown in the preview table. Click the object number to see detailed information on each object. In each type of object, click the button **Export CSV** to export the current object info as CSV file.

Cisco Interface mapping

You can manually map the interface.

- To **select** the appropriate FortiGate interface, click the value in the FortiGate Interface column, and then select a value or enter a custom interface name.
- To **edit** other values, double-click the proper column. Use the toolbar icon on the right to show and hide columns. You can also use the Tuning page to create mappings after the conversion is complete.
- To **import** a set of interface mappings from a file, click **Import**.
- To **download** the current set of interface mappings, click **Export**.
- To **delete** an interface, select the entries you would like to delete, **right click** and select **Delete Selected**. This is useful if your target FortiGate has fewer interfaces than the source configuration.

The limit of the length of interface names in FortiOS is 15 characters. Interfaces in the source config which have longer names should be trimmed to a shorter name. It is recommended to trim the names manually to ensure readability. But if a quick trimming is needed, please select the entries, **right click** and select **Trim Interface Name** to trim the names into 15 characters automatically.

Setting	Description
VDOM	Shows the virtual domains used in the conversion. ("root" by default)

Setting	Description
Source Interface	Shows each interface on the Cisco firewall.
FortiGate Interface	The input field for corresponding FortiGate interface names. Click to assign a FortiGate port or input the interface name manually for each interface. (Only available when the output format is **FortiGate**)
Normalized interface	The input field for corresponding normalized interface names, which would be configured in the ADOM database in FortiManager. Click to assign a port or input the interface name manually for each interface. (Only available when the output format is **FortiManager**)
Device interface	The input field for corresponding interface names in the managed devices in FortiManager. Click to assign a port or input the interface name manually for each interface. (Only available when the output format is **FortiManager**)
Members	Shows any members, if they are set.
IP-Netmask	Shows the IP address and netmask of the connection.
Type	Shows the type of interface.
Access	Shows which protocols has permission to access each interface.
Import	Click to load a set of interface mappings from a text file.
Export	Saves the current set of interface mappings to a text file.
Delete Selected	Click to delete the selected mapping item.
Trim Interface Name	Trim the interface names which exceed 15 characters into 15 characters automatically.

Cisco Routing Information

FortiConverter creates static routes in the output using the static routes it detects in the source configuration and any routing information you provide.

Double-click an item to edit it.

Setting	Description
New Route	Click to add a route.
Delete Selected	Click to delete the selected route.

Cisco Conversion result

Some columns can be selected, sorted, and filtered.

Tab	Description
Conversion Summary	Shows information about the conversion.
Reports	Generate PDF reports including converted and unconverted objects list.
VDOM Mapping	Shows how VDOMs were mapped from the source device to the new device.
Interface Mapping	Shows how interfaces were mapped for each VDOM from the source device.
Device Summary	Shows statistics about the objects detected.

For more details on how to fine-tune your conversion, see .

To download your finished conversion, click **Download Configurations**, located in the top-right corner. Your downloaded conversion is a .zip file.

FortiConverter includes error and warning messages into the conversion when an error occurs.

Review the `config-all.txt` file after each conversion for errors. These errors and warning messages might cause the import process to fail, if not corrected. See for more details.

Cisco PIX and ASA NAT merge examples

For more information about how FortiConverter handles NAT merges, see NAT merge options on page 233

For ASA, these examples are valid only for source configurations created using software versions 8.2.x and earlier.

Identity NAT

Dynamic NAT with ID 0 is the identity NAT and specifies that the address doesn't need to be translated. For example:

```
nat (inside) 0 172.17.3.68 255.255.255.255
```

Currently, because FortiConverter doesn't merge this kind of NAT, it ignores the settings when it converts the configuration.

Static identity NAT

In the following settings, in the two static NAT settings, the real address and the mapped address are the same.

```
static (inside,outside) 200.251.129.33 200.251.129.33 netmask 255.255.255.255

static (inside,outside) 172.17.3.69 access-list inside_nat0_static

access-list inside_nat0_static extended permit ip host 172.17.3.69 object-
group Group0
```

FortiConverter doesn't support this kind of static NAT and it ignores the settings when it converts the configuration.

Dynamic NAT with NAT IP

A source configuration has the following dynamic NAT settings:

```
global (outside) 1 172.31.242.69 netmask 255.255.255.255
```

```
nat (inside) 1 172.17.3.120 255.255.255.255
```

It also has the following firewall rule:

```
access-list acl_inside extended permit tcp host 172.17.3.120 object-group
Group_Destination eq http
```

```
access-group acl_inside in interface inside
```

FortiConverter generates the following IP pool and NAT policy from the source configuration:

```
edit "ippool-172.31.242.69"
   set endip 172.31.242.69
   set startip 172.31.242.69
   set type one-to-one
next

edit 10001
   set srcintf "port1" (corresponds to the interface "inside")
   set dstintf "port2" (corresponds to the interface "outside")
   set srcaddr "h_172.17.3.120"
   set dstaddr "Group_Destination"
   set service "HTTP"
   set schedule "always"
   set logtraffic disable
   set status enable
   set action accept
   set nat enable
   set ippool enable
   set poolname "ippool-172.31.242.69"
next
```

The interface and address of the dynamic NAT matches the firewall rule, so FortiConverter inserts the IP pool into policy 10001.

Dynamic NAT with mapped IP is "interface"

A source configuration has the following dynamic NAT settings:

```
global (outside) 2 interface
```

```
nat (inside) 2 172.17.40.73 255.255.255.255
```

It also has the following firewall rule:

```
access-list acl_inside extended permit tcp host 172.17.40.73 object-group
Group_Destination eq http
```

```
access-group acl_inside in interface inside
```

FortiConverter generates the following NAT policy from the source configuration:

```
edit 10002
   set srcintf "port1"
   set dstintf "port2"
   set srcaddr "h-172.17.40.73"
   set dstaddr "Group_Destination"
   set service "HTTP"
   set schedule "always"
   set logtraffic disable
   set status enable
   set action accept
   set nat enable
next
```

The interface and address of the dynamic NAT matches the firewall rule. NAT is enabled for policy 10002, but because there is no IP pool specified, the source address uses the interface IP address to perform NAT.

Dynamic policy NAT

A source configuration has the following dynamic NAT settings, which define NAT using an access list:

nat (inside) 1 access-list inside_nat_outboundaccess-list inside_nat_outbound extended permit tcp host 172.17.40.70 host 200.185.36.43 eq httpglobal (outside) 1 172.31.242.69 netmask 255.255.255.255

It also has the following firewall rule, which matches the NAT settings:

access-list acl_inside extended permit tcp host 172.17.40.70 host 200.185.36.43 eq http

access-group acl_inside in interface inside

FortiConverter generates the following IP pool and NAT policy from the source configuration:

```
edit "ippool-172.31.242.69"
   set endip 172.31.242.69
   set startip 172.31.242.69
   set type one-to-one
next

edit 10003
   set srcintf "port1"
   set dstintf "port2"
   set srcaddr "h-172.17.40.70"
   set dstaddr "h-200.185.36.43"
   set service "HTTP"
   set schedule "always"
   set logtraffic disable
   set status enable
   set action accept
   set nat enable
   set ippool enable
   set poolname "ippool-172.31.242.69"
next
```

The converted configuration is similar to when the source configuration specifies dynamic NAT with a NAT IP address.

FortiConverter converts the IP pool based on the dynamic NAT.

Static NAT matches policy source address

A source configuration has the following static NAT settings:

```
static (inside,outside) 200.251.129.95 172.17.60.85 netmask 255.255.255.255
```

It also has the following firewall rule:

```
access-list acl_inside extended permit ip host 172.17.60.85 object-group
Group_Destination

access-group acl_inside in interface inside
```

FortiConverter converts the static NAT rule to a VIP object and generates a NAT policy:

```
edit "vip-200.251.129.95"
   set extip 200.251.129.95
   set mappedip 172.17.60.85
   set extintf port2
   set nat-source-vip enable
next

edit 10004
   set srcintf "port1"
   set dstintf "port2"
   set srcaddr "h-172.17.60.85"
   set dstaddr "Group_Destination"
   set service "ALL"
   set schedule "always"
   set logtraffic disable
   set status enable
   set action accept
   set nat enable
next
```

The NAT-enabled policy tries to match the source address to a VIP object. If it finds a match, it performs static NAT as the VIP object specifies. Otherwise, it uses the interface IP for NAT.

Static NAT matches policy destination address

A source configuration has the following static NAT settings (which are the same as the example that matches by source address):

```
static (inside,outside) 200.251.129.95 172.17.60.85 netmask 255.255.255.255
```

It also has the following firewall rule:

```
access-list acl_outside extended permit ip any host 200.251.129.95

access-group acl_outside in interface outside
```

FortiConverter creates the same VIP object it does for the source address example, and the following NAT policy, which uses the VIP object as a destination address:

```
edit "vip-200.251.129.95"
set extip 200.251.129.95
set mappedip 172.17.60.85
set extintf port2
set nat-source-vip enable
next

edit 10005
set srcintf "port2"
set dstintf "port1"
set srcaddr "all"
```

```
set dstaddr "vip-200.251.129.95"
set service "ALL"
set schedule "always"
set logtraffic disable
set status enable
set action accept
next
```

Static NAT that uses access list matches policy source address

A source configuration has the following settings, which define static NAT using an access list:

```
static (inside,outside) 172.31.242.69 access-list inside_nat_static
```

```
access-list inside_nat_static extended permit ip host 10.100.128.97 object-group Group_Destination
```

It also has the following firewall rule:

```
access-list acl_inside extended permit ip host 10.100.128.97 object-group Group_Destination
```

```
access-group acl_inside in interface inside
```

FortiConverter converts the static NAT settings to the following VIP object and policies:

```
edit "vip-172.31.242.69_ip"
   set extip 172.31.242.69
   set mappedip 10.100.128.97
   set extintf port2
   set nat-source-vip enable
next

edit 10006
   set srcintf "port1"
   set dstintf "port2"
   set srcaddr "h-10.100.128.97"
   set dstaddr "Group_Destination"
   set service "ALL"
   set schedule "always"
   set logtraffic disable
   set status enable
   set action accept
   set nat enable
next
```

The NAT-enabled policy tries to match the source address to a VIP object. If it finds a match, it performs static NAT as the VIP object specifies. Otherwise, it uses the interface IP for NAT.

Static NAT specified by access list matches policy source address

The following source configuration settings define static NAT using an access list (they are the same as the example where static policy NAT matches the policy source address):

```
static (inside,outside) 172.31.242.69 access-list inside_nat_static
```

```
access-list inside_nat_static extended permit ip host 10.100.128.97 object-group Group_Destination
```

It also has the following firewall rule, which matches the NAT in source address:

access-list acl_outside extended permit ip object-group Group_Destination host 172.31.242.69

access-group acl_outside in interface outside

FortiConverter creates the same VIP object it does for the source address example, and the following NAT policy, which uses the VIP object as a destination address:

```
edit "vip-172.31.242.69_ip"
   set extip 172.31.242.69
   set mappedip 10.100.128.97
   set extintf port2
   set nat-source-vip enable
next

edit 110007
   set srcintf "por2"
   set dstintf "port1"
   set srcaddr "Group_Destination"
   set dstaddr "vip-172.31.242.69_ip"
   set service "ALL"
   set schedule "always"
   set logtraffic disable
   set status enable
   set action acceptnext edit 10007
   set srcintf "port2"
   set dstintf "any"
   set srcaddr "Group_Destination"
   set dstaddr "h-172.31.242.69"
   set service "ALL"
   set schedule "always"
   set logtraffic disable
   set status enable
   set action accept
next
```

NAT rule and policy addresses don't match exactly

When a NAT rule address doesn't match a policy address exactly, FortiConverter calculates where the addresses intersect (overlap) and uses the result as the address for the NAT policy it generates.

NAT rule address contains policy address

For example, a source configuration includes the following dynamic NAT configuration:

global (outside) 1 193.205.32.10 netmask 255.255.255.255

nat (inside) 1 10.1.2.0 255.255.255.0

It also contains the following firewall rule:

access-list acl_inside extended permit tcp host 10.1.2.1 host 193.205.23.66 eq smtp

access-group acl_inside in interface inside

The NAT rule address 10.1.2.0 255.255.255.0 contains the firewall rule source address 10.1.2.1.

FortiConverter converts the source NAT and firewall rules to the following IP pool and policies:

```
edit "ippool-193.205.32.0-193.205.32.255"
   set endip 193.205.32.10
   set startip 193.205.32.10
```

```
   set type one-to-one
next

edit 10001
   set srcintf "port1"
   set dstintf "port2"
   set srcaddr "h-10.1.2.1"
   set dstaddr "h-193.205.23.66"
   set service "SMTP"
   set schedule "always"
   set logtraffic disable
   set status enable
   set action accept
   set nat enable
   set ippool enable
   set poolname "ippool-193.205.32.10"
next
```

The source address of rule 10001 is the intersection of the NAT rule and original rule, which is "`h-10.1.2.1`".

Policy address contains the NAT rule address

A source configuration includes the following NAT settings (which are the same as the example where the NAT rule address contains the policy address):

```
global (outside) 1 193.205.32.10 netmask 255.255.255.255
```

```
nat (inside) 1 10.1.2.0 255.255.255.0
```

It also contains the following firewall rule:

```
access-list acl_inside extended permit tcp 10.1.0.0 255.255.0.0 host
193.205.23.66 eq smtp
```

```
access-group acl_inside in interface inside
```

The firewall rule source address `10.1.0.0 255.255.0.0` contains the NAT rule address `10.1.2.0 255.255.255.0`.

FortiConverter converts the source NAT and firewall rules to the following IP pool and policies:

```
edit "ippool-193.205.32.0-193.205.32.255"
   set endip 193.205.32.10
   set startip 193.205.32.10
   set type one-to-one
next

edit 110002
   set srcintf "port1"
   set dstintf "port2"
   set srcaddr "n-10.1.2.0_24"
   set dstaddr "h-193.205.23.66"
   set service "SMTP"
   set schedule "always"
   set logtraffic disable
   set status enable
   set action accept
   set nat enable
```

```
   set ippool enable
   set poolname "ippool-193.205.32.10"
   next

edit 10002
   set srcintf "port1"
   set dstintf "any"
   set srcaddr "n-10.1.2.0_16"
   set dstaddr "h-193.205.23.66"
   set service "SMTP"
   set schedule "always"
   set logtraffic disable
   set status enable
   set action accept
next
```

The policy 00110002 source address "n-10.1.2.0_24" is the intersection of NAT rule and firewall rule 10002.

NAT rule matches address "all" in policy

A source configuration includes the following NAT settings (which are the same as the example where the NAT rule address contains the policy address):

global (outside) 1 193.205.32.10 netmask 255.255.255.255

nat (inside) 1 10.1.2.0 255.255.255.0

It also contains the following firewall rule:

access-list acl_inside extended permit tcp any host 193.205.23.66 eq smtp

access-group acl_inside in interface inside

The source address field is "any", which contains the NAT rule.

FortiConverter converts the source NAT and firewall rules to the following IP pool and policies:

```
edit 110003
   set srcintf "port1"
   set dstintf "port2"
   set srcaddr "n-10.1.2.0_24"
   set dstaddr "h-193.205.23.66"
   set service "SMTP"
   set schedule "always"
   set logtraffic disable
   set status enable
   set action accept
   set nat enable
   set ippool enable
   set poolname "ippool-193.205.32.10"
next

edit 10003
   set srcintf "port1"
   set dstintf "any"
   set srcaddr "all"
   set dstaddr "h-193.205.23.66"
   set service "SMTP"
   set schedule "always"
```

```
   set logtraffic disable
   set status enable
   set action accept
next
```

The policy 110003 source address "n-10.1.2.0_24" is the intersection of NAT and firewall rules.

Static NAT overlaps policy destination address

A source configuration has the following settings, which define static NAT using an access list:

static (inside,outside) 172.31.242.69 access-list inside_nat_static

access-list inside_nat_static extended permit ip host 10.100.128.97 object-group Group_Destination

It also includes the following firewall rule:

access-list acl_outside extended permit ip object-group Group_Destination 172.31.242.0 255.255.255.0

access-group outside in interface outside

The firewall rule destination address 172.31.242.0 255.255.255.0 contains the static NAT mapped IP 172.31.242.69.

FortiConverter generates the following VIP object and policies that use the object as a destination:

```
edit "vip-172.31.242.69_ip"
   set extip 172.31.242.69
   set mappedip 10.100.128.97
   set extintf port2
   set nat-source-vip enable
next

edit 110004
   set srcintf "port2"
   set dstintf "port1"
   set srcaddr "Group_Destination"
   set dstaddr "vip-172.31.242.69_ip"
   set service "ALL"
   set schedule "always"
   set logtraffic disable
   set status enable
   set action accept
next

edit 10004
   set srcintf "port2"
   set dstintf "any"
   set srcaddr "Group_Destination"
   set dstaddr "n-172.31.242.0_24"
   set service "ALL"
   set schedule "always"
   set logtraffic disable
   set status enable
   set action accept
next
```

Static NAT overlaps address group object

A source configuration has the following settings, which define a static NAT using an access list:

```
static (inside,outside) 172.31.242.69 access-list inside_nat_static
```

```
access-list inside_nat_static extended permit ip host 10.100.128.97 object-
group Group_Destination
```

The access list destination address Group_Destination contains two members:

```
object-group network Group_Destination
   network-object 10.255.253.0 255.255.255.0
   network-object 10.255.254.0 255.255.255.0
```

The source configuration also has a firewall rule that matches the static NAT rule and its destination is a member of the group `Group_Destination.`

```
access-list acl_inside extended permit ip host 10.100.128.97 10.255.253.0 255.255.255.0
access-group acl_inside in interface inside
```

FortiConverter generates the following NAT policy, which has the destination address `10.255.253.0 255.255.255.0.`

```
edit 10009
   set srcintf "port1"
   set dstintf "port2"
   set srcaddr "h-10.100.128.97"
   set dstaddr "n-10.255.253.0_24"
   set service "ALL"
   set schedule "always"
   set logtraffic disable
   set status enable
   set action accept
   set nat enable
next
```

NAT exemption

NAT exemption is a dynamic policy NAT with ID 0. In most cases, you use NAT exemption to do one of the following:

- Exempt from NAT an address that is located in a NAT rule address range.
- In environments that use NAT control to block traffic to which no NAT rule applies, to permit this type of traffic.

Exempt an address from a NAT rule

A source configuration has the following NAT exemption configuration:

```
nat (inside) 0 access-list inside_nat_exemption
```

```
access-list inside_nat_exemption extended permit ip host 172.13.100.88
object-group Group_Destination
```

It also has the following dynamic NAT rule:

```
nat (inside) 4 172.13.100.0 255.255.255.0
global (outside) 4 172.80.80.8 netmask 255.255.255.255
```

Both the NAT exemption and the dynamic NAT rule match the following firewall rule:

```
access-list acl_inside extended permit ip 172.13.100.0 255.255.255.0 object-group Group_
     Destination
access-group acl_inside in interface inside
```

FortiConverter generates the following policies:

```
edit 110001
   set srcintf "port1"
   set dstintf "port2"
   set srcaddr "h-172.13.100.88"
   set dstaddr "Group_Destination"
   set service "ALL"
   set schedule "always"
   set logtraffic disable
   set status enable
   set action accept
next

edit 10001
   set srcintf "port1"
   set dstintf "port2"
   set srcaddr "n-172.13.100.0_24"
   set dstaddr "Group_Destination"
   set service "ALL"
   set schedule "always"
   set logtraffic disable
   set status enable
   set action accept
   set nat enable
   set ippool enable
   set poolname "ippool-172.80.80.8"
next
```

The NAT exemption configuration generates policy 110001 with no NAT behavior. The dynamic NAT configuration generates policy 10001, which references an IP pool. Because 00110001 comes first in the configuration, it applies to address "h-172.13.100.88" before the policy used for address "n-172.13.100.0_24" (which applies dynamic NAT) is applied.

Allowing traffic without NAT when PIX enables NAT control

When NAT control is enabled in PIX, traffic from an interface with high-level security to an interface with low-level security isn't allowed if no NAT rule is configured. To allow traffic that doesn't require NAT, a NAT exemption is required.

The following NAT configuration is a source configuration, which includes NAT control and a NAT exemption:

```
nat-control
nat (inside) 0 access-list inside_nat_exemption
```

```
access-list inside_nat_exemption extended permit ip host 172.14.100.88
object-group Group_Destination
```

It also has the following firewall rule:

```
access-list acl_inside extended permit ip 172.14.100.0 255.255.255.0 object-group Group_
     Destination
access-group acl_inside in interface inside
```

The interface security level has the following configuration:

```
nameif ethernet0 outside security0
nameif ethernet1 inside security100
```

FortiConverter generates the following policies:

```
edit 110002
   set srcintf "port1"
   set dstintf "port2"
   set srcaddr "h-172.14.100.88"
   set dstaddr "Group_Destination"
   set service "ALL"
   set schedule "always"
   set logtraffic disable
   set status enable
   set action accept
next

edit 10002
   set srcintf "port1"
   set dstintf "port2"
   set srcaddr "n-172.14.100.0_24"
   set dstaddr "Group_Destination"
   set service "ALL"
   set schedule "always"
   set logtraffic disable
   set status disable
   set action accept
   set comments "This policy is disabled as not allowed by NAT-Control."
next
```

The source interface of the firewall rule is "inside"(port1), which has security level 100. The destination interface of this firewall rule is calculated to be "outside"(port2), which has security level 0. Since "inside" has a higher security level than "outside", traffic from "n-172.14.100.0_24" to "Group_Destination" isn't allowed if NAT isn't configured (even if the firewall rule allows it). Only traffic from "h-172.14.100.88" to "Group_Destination" is allowed because a NAT exemption is configured for it. Since other traffic isn't allowed, FortiConverter disables policy 10002, and adds a comment to show the reason.

Unused VIP objects generate policy

In some cases, the final policy in an output configuration is one that FortiConverter generates from VIP objects that aren't used as a destination address in at least one policy. For example:

```
edit 001
   set srcintf "port1"
   set dstintf "any"
   set srcaddr "all"
   set dstaddr "vip- 172.21.84.24" " vip- 172.21.84.25" " vip- 172.21.84.26"
   set service "ALL"
   set schedule "always"
   set logtraffic all
   set status enable
   set action deny
   set comments "This policy is auto-generated by FortiConverter to activate static-NAT
        VIPs that aren't referenced in other policies."
next
```

This type of policy enables the source static NAT mapping by capturing all VIP objects that other policies don't reference.

In some conversions, FortiConverter generates more than one of this kind of policy – one for each external interface that is referenced by an unreferenced VIP object.

F5 Conversions (Beta feature)

Conversion Support

FortiConverter supports the following features:

- Nodes
- Pools
- Virtual addresses
- Virtual servers
- Server policies (FortiWeb conversions only)

F5 Conversion Wizard

The administrator password is **not** set on the new configuration.

For third-party conversions, the trusted host settings are converted. Check the trusted host settings to ensure they allow management access from the relevant network interfaces.

To start a new conversion

1. Start FortiConverter.
2. When start-up is complete, a browser window automatically opens to http://127.0.0.1:8000.
3. Click 

New Conversion, located at the top right corner.
4. Enter a name for the conversion configuration.
5. For Vendor, choose **NetScaler** block.
6. Choose a Model, if applicable.
7. Click **OK**.

The configuration page opens to the Start page, and you can input your settings.

F5 Start Options

This table lists the start settings.

Setting	Description
Profile	
Description	Enter a description of the configuration.
Output Options	
Output Format	Select the appropriate output for your target Fortinet device. FortiADC and FortiWeb conversions are available.
FOS Version	The configuration syntax of the output. Only v5 is available currently.
Input	
Source Configuration	Select the input file

F5 Source Preview

This table shows the information inside the configuration.

Setting	Description
File Name	Source configuration file names are shown in the table as a link. Click the link to see the content. The file won't show if it's too large.
Model	The model of the configuration.
Source Configuration Preview	The number of each type of object is shown in the preview table. Click the object number to see detailed information about each object. In each type of object, click the Export CSV button to export the current object info as a CSV file.

F5 Conversion Result

Setting	Description
Conversion Summary	Provides information about the conversion.
Device Summary	Provides statistics about the detected objects.

Forcepoint Conversion

Forcepoint differences

VPNs

StoneSoft VPNs aren't converted.

Conversion support

FortiConverter supports the following features:

- Interface
- Address (group)
- Service (group)
- Policy / Sub-Policy
- NAT
- Route

Saving the Forcepoint source configuration files

Before starting the conversion wizard, save a copy of your Forcepoint configuration file (XML format) to the computer where FortiConverter is installed.

Saving the Forcepoint Stonesoft source configuration files on page 133

Saving the Forcepoint Sidewinder source configuration file on page 133

Saving the Forcepoint Stonesoft source configuration files

Before starting the conversion wizard, save a copy of your Forcepoint Stonesoft configuration file (XML format) to the computer where FortiConverter is installed.

Saving the Forcepoint Sidewinder source configuration file

Before starting the conversion wizard, save a copy of your configuration file to the computer where FortiConverter is installed.

The following is for **Forcepoint Sidewinder 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

Forcepoint Sidewinder v7	Forcepoint Sidewinder 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:/
```

Forcepoint Conversion Wizard

The administrator password is **not** set on the new configuration.

For third-party conversions, the trusted host settings are converted. Check the trusted host settings to ensure they allow management access from the relevant network interfaces.

To start a new conversion

1. Start FortiConverter.
2. When start-up is complete, a browser window automatically opens to http://127.0.0.1:8000.
3. Click New Conversion **New Conversion**, located at the top right corner.
4. Enter a name for the conversion configuration.
5. For Vendor, choose **Forcepoint** block.
6. Choose a Model: **Stonesoft**, **Sidewinder v7** or **Sidewinder v8**.
7. Click **OK**.

The configuration page opens to the Start page, and you can input your settings.

Forcepoint Start options

The following table lists the start settings.

Setting	Description
Profile	
Description	Enter a description of the configuration.
Output Options	
Output Format	Select the appropriate output for your target Fortinet device.
FOS Version	The configuration syntax is slightly different among FortiOS 6.4, 7.0, 7.2, 7.4 and 7.6. Select the version that corresponds to the FortiOS version on the target.
Input	
Source Configuration	Select the input file.

Setting	Description
Bulk Conversion	If there are many devices to be converted where all of them are the same model, sharing the same interface mapping relationship in conversion, then bulk conversion can convert all of them at once. Collect all the configuration files to be converted, compress them into a ZIP file and use the ZIP file as the input.
Target device (Optional)	
Target device	Select the model of the target device, or select a device connected to FortiConverter.
Conversion Options	
Discard unreferenced firewall objects	Specifies whether addresses and services that aren't referenced by a policy are saved and added to the output. This option can be useful if your target device has table size limitations. You can view the unreferenced objects that FortiConverter removed on the Tuning page.
Increase Address and Service Table Sizes for High-End Models	You can customize the maximum table sizes that FortiConverter uses when **Adjust table sizes** is selected. For more information, see Adjusting table sizes on page 232.
Automatically generate policy interfaces (Stonesoft only)	Specifies whether FortiConverter automatically generates policy interfaces.
Policy index start from 1 instead of 10000	When selected, the serial number of firewall policies will start from 1 instead of 10000.
Split Address group From VPN Phase2 selector (Sidewinder only)	If the remote side of the VPN is not a FortiGate but a device of another vendor, setting an address group in the VPN phase2 quick selector does not work. When this option is enabled, a VPN phase2 object with an address group in the selector would be split into multiple objects with a subnet or a range in the selector.
NGFW policy-based mode	When selected, the conversion will be in NGFW policy-based mode. "`firewall policy`" will become "`firewall security-policy`" instead, and "`set application 00000`" will be generated in policies, which requires manual processing. There will also be some other minor differences adapted for the NGFW policy-based CLI.
Remove self-traffic addresses and policies	Self-traffic polices, which use the address "Firebox" as source or destination address, are not necessary in FortiOS. FortiConverter comments out the self-traffics policies or remove self-traffic addresses from policies when this option is enabled.

Setting	Description
Nat Merge Options (Stonesoft Only)	
Ignore firewall policies with all or any addresses when processing NAT rules	Specifies whether FortiConverter ignores firewall policies with an "all" or "any" address when it merges a NAT rule and a firewall policy to create a FortiGate NAT policy. FortiConverter creates new policies in the output configuration based on where NAT rules to firewall policies intersect. Because firewall policies that use "all" or "any" as the address create many intersections, Fortinet recommends that you ignore them.
Enable central NAT merge	Specifies whether FortiConverter converts NATs to FortiGate central NATs instead of policy-based NATs. It is recommended to enable this option.
Comment Options	
Policy comment - Preserve the original comment	Include the original comment in source file in the comment of the output policy.

Source Preview

This page shows the information inside the configuration.

Setting	Description
Information of Configurations	Source configuration file names are shown in the table as a link. Click the link to see the content. The file won't show if it's too large.
VDOM Select	Select/Unselect the VDOM item.
VDOM Rename	Rename the VDOM name.
VDOM Mode	Change the VDOM mode in the output result.
Source Configuration Preview	The numbers of each type of firewall object are shown in the preview table. Click the object number to see detailed information on each object. In each type of object, click the download icon to export the current object info as CSV file.

Policy Package Assignment (Stonesoft only)

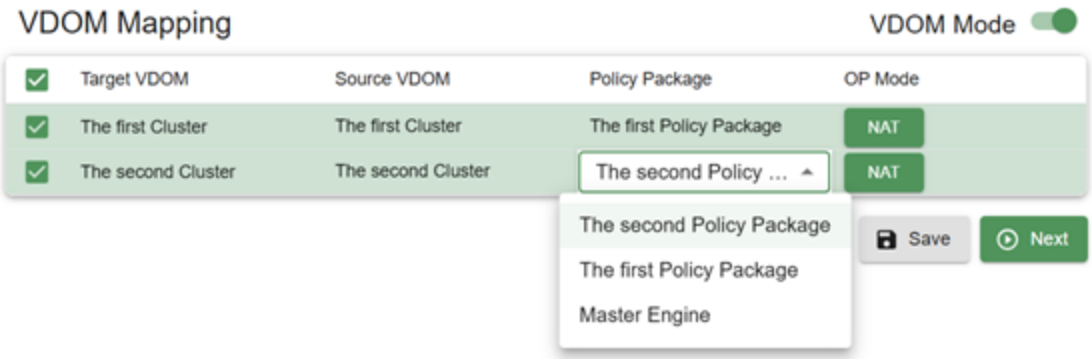
Because a single Stonesoft config could contain multiple configurations for multiple devices, an explicit info of mapping from firewall names (e.g. <fw_cluster> or <fw_single> or <virtual_fw>) to policy package names (<fw_policy>) is required. Otherwise, policy packages that are missing mapping information will fail to apply.

There are two ways to specify the mapping:

1. 1. Before the conversion, for each firewall-policy pair, manually modify the config by adding <granted_policy_ref> tag with the following format to the end of the config.

```
966
967 <granted_policy_ref engine_ref="***Enter Firewall Name here***">
968     <list>
969       <list_entry type="fw_policy" value="***Enter Mapped Policy Package Name here***"/>
970     </list>
971 </granted_policy_ref>
972
973 </generic_import_export>
```

2. If <granted_policy_ref> tags are not found while parsing, it is possible to select them from the dropdown list in VDOM mapping page. (For <master_engine> tag, just choose "Master Engine" from the dropdown list.)



Forcepoint Interface mapping

You can manually map the interface.

- To **select** the appropriate FortiGate interface, click the value in the FortiGate Interface column, and then select a value or enter a custom interface name.
- To **edit** other values, double-click the proper column. Use the toolbar icon on the right to show and hide columns. You can also use the Tuning page to create mappings after the conversion is complete.
- To **import** a set of interface mappings from a file, click **Import**.
- To **download** the current set of interface mappings, click **Export**.
- To **delete** an interface, select the entries you would like to delete, **right click** and select **Delete Selected**. This is useful if your target FortiGate has fewer interfaces than the source configuration.

The limit of the length of interface names in FortiOS is 15 characters. Interfaces in the source config which have longer names should be trimmed to a shorter name. It is recommended to trim the names manually to ensure readability. But if a quick trimming is needed, please select the entries, **right click** and select **Trim Interface Name** to trim the names into 15 characters automatically.

Setting	Description
VDOM	Shows the virtual domains used in the conversion. ("root" by default)
Source Interface	Shows each interface on the Forcepoint firewall.
FortiGate Interface	The input field for corresponding FortiGate interface names. Click to assign a FortiGate port or input the interface name manually for each interface. (Only available when the output format is **FortiGate**)
Normalized interface	The input field for corresponding normalized interface names, which would be configured in the ADOM database in FortiManager. Click to assign a port or input the interface name manually for each interface. (Only available when the output format is **FortiManager**)
Device interface	The input field for corresponding interface names in the managed devices in FortiManager. Click to assign a port or input the interface name manually for each interface. (Only available when the output format is **FortiManager**)
Members	Shows any members, if they are set.
IP-Netmask	Shows the IP address and netmask of the connection.
Type	Shows the type of interface.
Access	Shows which protocols has permission to access each interface.
Import	Click to load a set of interface mappings from a text file.
Export	Saves the current set of interface mappings to a text file.
Delete Selected	Click to delete the selected mapping item.
Trim Interface Name	Trim the interface names which exceed 15 characters into 15 characters automatically.

Forcepoint Route Information

FortiConverter creates static routes in the output using the static routes it detects from the source configuration as well as routing information you provided.

Double-click an item to edit it.

Setting	Description
New Route	Click to add a route.
Delete	Click to delete the selected route.

Forcepoint Conversion result

Tab	Description
Conversion Summary	Provides statistics about the conversion.
Reports	Generate PDF reports including converted and unconverted objects list.
Interface Mapping	Shows how interfaces were mapped for each VDOM from the source device.
Device Summary	Provides statistics about the detected objects.

FortiConverter includes error and warning messages into the conversion when an error occurs.
Review the `config-all.txt` file after each conversion for errors. These errors and warning messages might cause the import process to fail, if not corrected. See for more details.

Huawei USG Firewall Conversion

Conversion support

FortiConverter supports the following features:

- Interface
- Zone
- Address (group)
- Service (group)

- Policy
- Route
- Zone
- IPSec Policy (VPN)
- Security Context
- Nat Policy (Converted to Fortigate SNAT)
- Nat Server (Converted to Fortigate VIP)

Saving the Huawei source configuration files

Before starting the conversion wizard, save a copy of your Huawei configuration file to the computer where FortiConverter is installed.

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.

Huawei conversion wizard

To start a new conversion

1. Start FortiConverter.
2. When start-up is complete, a browser window automatically opens to http://127.0.0.1:8000.
3. Click 

New Conversion, located at the top right corner.
4. Enter a name for the conversion configuration.
5. For Vendor, choose **Huawei** block.
6. Choose a Model, if applicable.
7. Click **OK**.

The configuration page opens to the Start page, and you can input your settings.

Huawei Start options

This table lists the start settings.

Setting	Description
Profile	

Setting	Description
Description	Enter a description of the configuration.
Output Options	
Output Format	Select the appropriate output for your target Fortinet device.
FOS Version	The configuration syntax is slightly different among FortiOS 6.4, 7.0, 7.2, 7.4 and 7.6. Select the version that corresponds to the FortiOS version for the target.
Input	
Source Configuration	Select the input file.
Virtual System Conversion	Enable this option to convert configurations with multiple virtual systems.
Root Configuration	Select the system configuration file. This file should include interfaces and config file names for each security context. This option only appears if Virtual System Conversion is enabled.
Vsys Configuration (.zip)	Select the .zip file containing all the config files. The file name for each context should match the name given in the root configuration file. This option only appears if Virtual System Conversion is enabled. Please see example in Input and naming for vsys file on page 143.
Bulk conversion	If there are many devices to be converted where all of them are the same model, sharing the same interface mapping relationship in conversion, then bulk conversion can convert all of them at once. Collect all the configuration files to be converted, compress them into a ZIP file and use the ZIP file as the input.
Target device (Optional)	
Target device	Select the model of the target device, or select a device connected to FortiConverter.
Conversion Options	
Discard unreferenced firewall objects	Specifies whether addresses and services that aren't referenced by a policy are saved and added to the output. This option can be useful if your target device has table size limitations. You can view the unreferenced objects that FortiConverter removed on the Tuning page.

Setting	Description
Increase Address and Service Table Sizes for High-End Models	You can customize the maximum table sizes that FortiConverter uses when "Adjust table sizes" is selected. For more information, see Adjusting table sizes on page 232.
Route-based IPSec	Specifies whether Route-based IPSec is used for this conversion.
Policy index start from 1 instead of 10000	When selected, the serial number of firewall policies will start from 1 instead of 10000.
NGFW policy-based mode	When selected, the conversion will be in NGFW policy-based mode. "`firewall policy`" will become "`firewall security-policy`" instead, and "`set application 00000`" will be generated in policies, which requires manual processing. There will also be some other minor differences adapted for the NGFW policy-based CLI.
Service Comment	Specifies whether FortiConverter copies the service comment from the source configuration to converted FortiGate service.
Comment Options	
Include input configuration lines for each output policy	Specifies whether FortiConverter includes the input configuration lines used for each FortiGate policy in the FortiGate configuration as a policy comment.
Address Comment	Specifies whether FortiConverter copies the address comment from source configuration to the converted FortiGate address.
Service Comment	Specifies whether FortiConverter copies the service comment from the source configuration to the converted FortiGate service.
Nat Merge Options	
Enable central NAT merge	Specifies whether FortiConverter converts NATs to FortiGate central NATs instead of policy-based NATs. It is recommended to enable this option with FOS 6.0 or later.

Input and naming for vsys file

Here is an example on inputting vsys file and naming convention, please note that the file name should match the root:

Suppose the root config (test-FW-01) contains the following vsys information:

```
vsys first 1
 assign interface GigabitEt
 assign interface GigabitEt
#
vsys test_sec 2
 assign interface GigabitEt
 assign interface GigabitEt
 assign interface GigabitEt
#
vsys something 3
 assign interface GigabitEt
 assign interface GigabitEt
 assign interface GigabitEt
```

Then test-FW-01.zip should contain config files `"test-FW-01-first", "test-FW-01-test_sec", "test-FW-01-something"`.

i.e. vsys filename = root file name and vsys name joined by dash.

The files should not have a filename extension (for example .txt), otherwise the filename-vsys matching would fail.

VPN Instance

Map the VPN instances in the source configuration to VDOMs in the output configuration.

By default, all VPN instances are mapped to VDOMs with the same name. You can modify this default mapping as required by renaming VDOMs and removing VPN instances from the conversion.

Setting	Description
VDOM Select	Select/Unselect the VDOM item.
VDOM Rename	Rename the VDOM name.
VDOM Mode	Change the VDOM mode in the output result.

Information of Configurations	Source configuration file names are shown in the table as a link. Click the link to see the content. The file won't show if it's too large.
Managed Device Name	The name of the managed device which the converted interface or route configuration would be imported in FortiManager. (Only available when the output format is FortiManager)
Target Device Switch Interface - Interface/Port	If there are virtual switches in the selected target device, FortiConverter will list the member ports of the virtual switches. If an interface in the list is going to be used in the configuration, it should first be detached from the virtual switch. Click "**X**" on the interface to detach it. Please note that a detached interface cannot be re-added later by FortiConverter.
Source Configuration Preview	The numbers of each type of firewall object are shown in the preview table. Click the object number to see detailed information on each object. In each type of object, click the button **Export CSV** to export the current object info as CSV file.

Huawei Interface mapping

You can manually map the interface.

- To **select** the appropriate FortiGate interface, click the value in the FortiGate Interface column, and then select a value or enter a custom interface name.
- To **edit** other values, double-click the proper column. Use the toolbar icon on the right to show and hide columns. You can also use the Tuning page to create mappings after the conversion is complete.
- To **import** a set of interface mappings from a file, click **Import**.
- To **download** the current set of interface mappings, click **Export**.
- To **delete** an interface, select the entries you would like to delete, **right click** and select **Delete Selected**. This is useful if your target FortiGate has fewer interfaces than the source configuration.

The limit of the length of interface names in FortiOS is 15 characters. Interfaces in the source config which have longer names should be trimmed to a shorter name. It is recommended to trim the names manually to ensure readability. But if a quick trimming is needed, please select the entries, **right click** and select **Trim Interface Name** to trim the names into 15 characters automatically.

Setting	Description
VDOM	Shows the virtual domains used in the conversion. ("root" by default)
Source Interface	Shows each interface on the Huawei firewall.
FortiGate Interface	The input field for corresponding FortiGate interface names. Click to assign a FortiGate port or input the interface name manually for each interface. (Only available when the output format is **FortiGate**)
Normalized interface	The input field for corresponding normalized interface names, which would be configured in the ADOM database in FortiManager. Click to assign a port or input the interface name manually for each interface. (Only available when the output format is **FortiManager**)
Device interface	The input field for corresponding interface names in the managed devices in FortiManager. Click to assign a port or input the interface name manually for each interface. (Only available when the output format is **FortiManager**)
Members	Shows any members, if they are set.
IP-Netmask	Shows the IP address and netmask of the connection.
Type	Shows the type of interface.
Access	Shows which protocols has permission to access each interface.
Import	Click to load a set of interface mappings from a text file.
Export	Saves the current set of interface mappings to a text file.
Delete Selected	Click to delete the selected mapping item.
Trim Interface Name	Trim the interface names which exceed 15 characters into 15 characters automatically.

Huawei Route Information

FortiConverter creates static routes in the output using the static routes it detects in the source configuration and any routing information you provide.

Double-click an item to edit it.

Setting	Description
New Route	Click to add a route.
Delete	Click to delete the selected route.

Huawei Conversion result

Tab	Description
Conversion Summary	Provides statistics about the conversion.
Reports	Generate PDF reports including converted and unconverted objects list.
Interface Mapping	Shows how interfaces were mapped for each VDOM from the source device.
Device Summary	Provides statistics about the detected objects.

FortiConverter includes error and warning messages into the conversion when an error occurs.

Review the `config-all.txt` file after each conversion for errors. These errors and warning messages might cause the import process to fail, if not corrected. See for more details.

IBM IPAM IPS Signature Conversion

IBM Security Event example

```
<securityEventsList
securityEventID='xxxxxxxx-XXXX-XXXX-XXXX-XXXXXXXXXXXX' issueID='XXXXXXX'
      Enabled='false' virtualSensor='Extranet' isAttack='Attack' checkName='HTTP_
      Htaccess' risk='medium' protocol='url' ignore='false' display='WithoutRaw'
      block='true' xpu='0.0' eventThrottling='0' checkDate='2/2005'
      defaultQuarantine='Block' logEvidence='None' isUserOverride='true'
      noDelete='false' ><responses />
</securityEventsList>
```

Supported Keywords

IBM Keyword	Corresponding Fortigate Field
Enabled	set status
risk	set severity
block	set action
logEvidence	set log-packet
display	set log
protocol	set protocol

Unsupported Keywords

The following keywords are not supported in IBM conversion.

Unsupported Keywords
virtualSensor
checkName
ignore
xpu
eventThrottling
checkDate

Unsupported Keywords
defaultQuarantine
isUserOverride
noDelete
xpu
securityEventID
issueID

Supported Protocol Types

IBM Conversion supported protocol types:

Supported Protocol Types
bo
capwap
dcerpc
dhcp
dnp3
dns
ftgd
ftp
ftps
h323
http
https
icmp
iec104
im

Supported Protocol Types
imap
imaps
ldap
misc
modbus
mssql
nbss
nntp
other
p2p
pop3
pop3s
radius
rawtcp
rdt
rpc
rtcp
rtp
rtsp
sccp
sip
smtp
smtps
snmp
ssh
ssl
tcp
telnet
tfn
udp

Rule Overview

This page shows the information inside the configuration.

Click the "Export CSV"  button to export the current object info as CSV file.

IBM Conversion Result

Page Tab	Description
IBM IPS Sensor	Shows the parsed IBM IPS sensors, separated into two tables based on whether the protocol is supported by Fortigate.
Fortigate IPS Sensor	Shows only the supported FGT IPS sensors and the conversion results.

Ivanti Conversions (Beta feature)

Conversion Support

FortiConverter supports the following features:

- Address
- Services
- User groups
- Policies

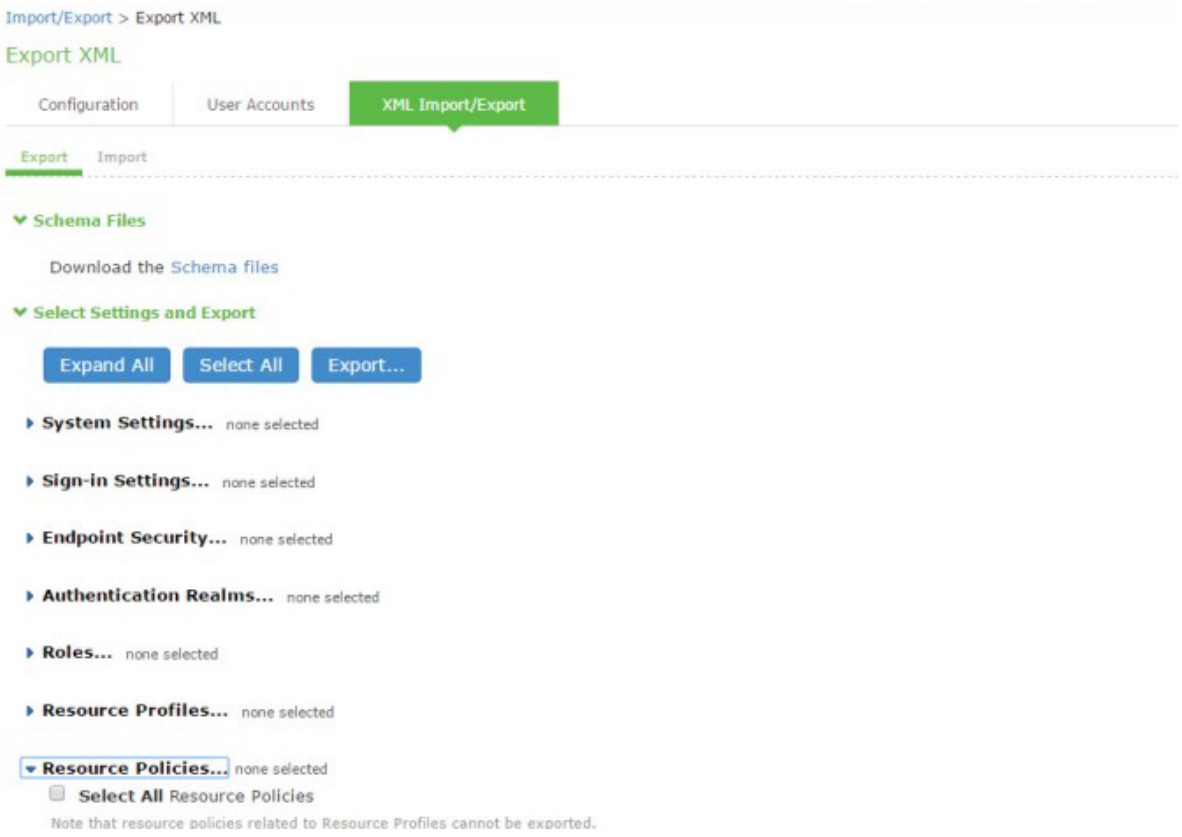
The conversion result can be output in the format of FortiOS CLI or in the format of FortiSASE API.

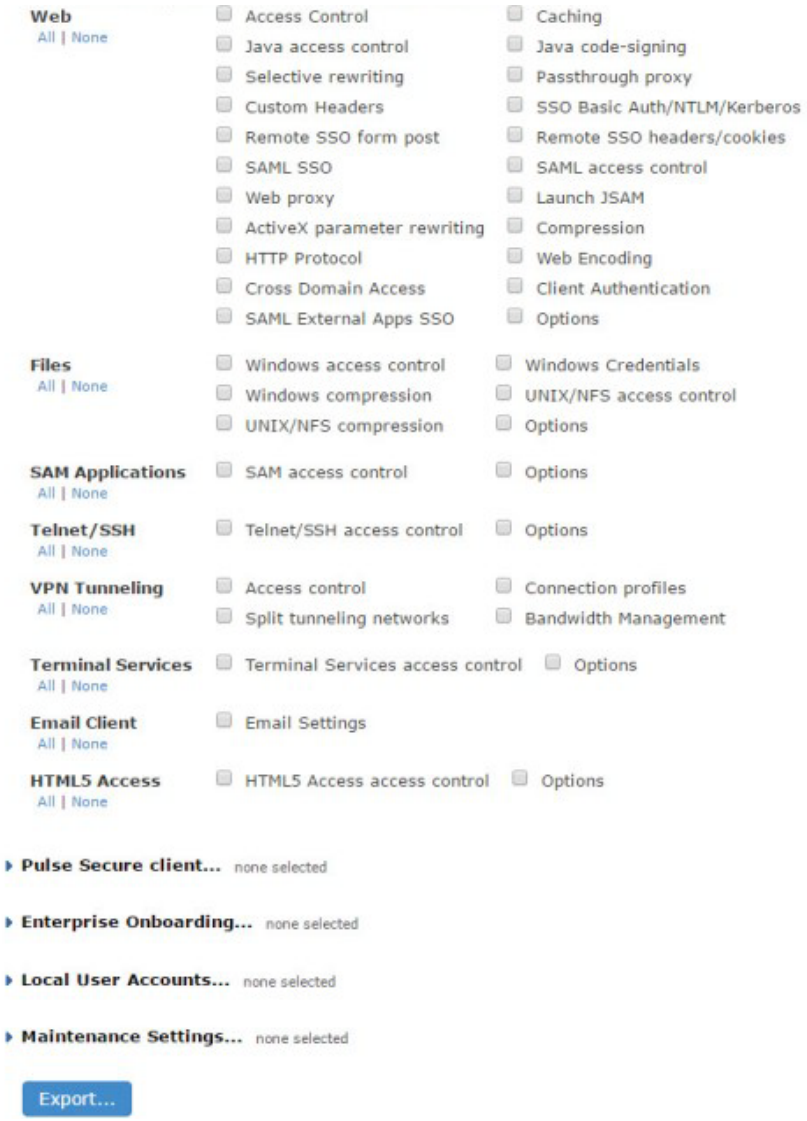
Saving the Ivanti Source Configuration Files

Before starting the conversion wizard, save a copy of your Ivanti configuration file to the computer where FortiConverter is installed.

To export an XML configuration file:

1. Select **Maintenance > Import/Export > Export XML** to display the configuration page.
2. Select the required options on the **Export XML File Configuration Page**.

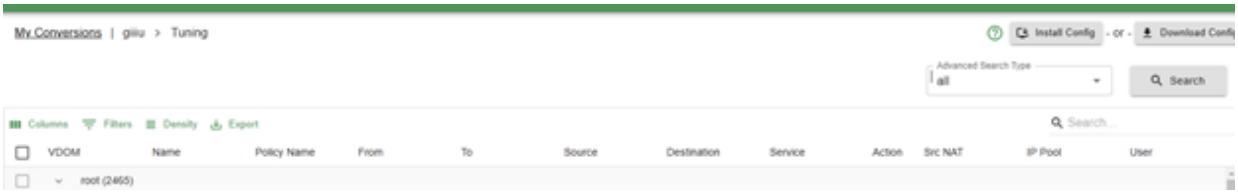

Import/Export > Export XML
Export XML
Configuration
User Accounts
XML Import/Export
Export
Import
Schema Files
Download the Schema files
Select Settings and Export
Expand All
Select All
Export...
System Settings... none selected
Sign-in Settings... none selected
Endpoint Security... none selected
Authentication Realms... none selected
Roles... none selected
Resource Profiles... none selected
Resource Policies... none selected
Select All Resource Policies
Note that resource policies related to Resource Profiles cannot be exported.



3. Click **Export** to export the selected configuration data to an XML file.

Ivanti Policy Tuning Filter

In the **Ivanti** policy tuning page, there is a filter titled **Advanced Search Type**.



The **Advanced Search Type** filter has the options **SIA/SPA/all**. Choosing any of them and then click **Search** on the right will filter out the desired policies to display.

"SPA" policies are policies that have destination address in private IP range, and "SIA" policies are policies that have destination address in public IP range, while "all" shows every policy.

Ivanti Conversion Wizard

The administrator password is **not** set on the new configuration.

For third-party conversions, the trusted host settings are converted. Check the trusted host settings to ensure they allow management access from the relevant network interfaces.

To start a new conversion

1. Start FortiConverter.
2. When start-up is complete, a browser window automatically opens to http://127.0.0.1:8000.
3. Click 

New Conversion, located at the top right corner.
4. Enter a name for the conversion configuration.
5. For Vendor, choose **Ivanti** block.
6. Choose a Model, if applicable.
7. Click **OK**.

The configuration page opens to the Start page, and you can input your settings.

Ivanti Start Options

This table lists the start settings.

Setting	Description
Profile	
Description	Enter a description of the configuration.
Output Options	
Output Format	Select the appropriate output for your target Fortinet device. If FortiGate or FortiManager is selected, the output would be in the format of FortiOS CLI. If FortiSASE is selected, the output would be in the format of JSON payload of FortiSASE import API.

Setting	Description
FOS Version/ API Versoin	The configuration syntax is slightly different for FortiOS 6.4, 7.0, 7.2, 7.4 and 7.6. Select the version that corresponds to the FortiOS version on the target. If FortiSASE is selected, the selection would become the API Version of FortiSASE API and "v2" would be the only option available.
Input	
Source Configuration	Select the input file
Conversion Options	
Discard unreferenced firewall objects	Specifies whether addresses, schedules, and services that aren't referenced by a policy are saved and added to the output. This option can be useful if your target device has table size limitations. You can view the unreferenced objects that FortiConverter removed on the Tuning page.
Policy index start from 1 instead of 10000	When selected, the serial number of firewall policies will start from 1 instead of 10000.
Public destination interface name (FortiOS only)	When the destination address of a policy is a public address, FortiConverter would set the input value as the destination interface. The default public interface in FortiSASE is "port2".
Private destination interface name (FortiOS only)	When the destination address of a policy is a private address, FortiConverter would set the input value as the destination interface.
JSON services per file (FortiSASE only)	When the input value is empty, all the services would be output into one file. If a number is given, the output file would be split into multiple files and each file contains the given number of services.
JSON addresses per file (FortiSASE only)	When the input value is empty, all the addresses would be output into one file. If a number is given, the output file would be split into multiple files and each file contains the given number of addresses.
JSON policies per file (FortiSASE only)	When the input value is empty, all the policies would be output into one file. If a number is given, the output file would be split into multiple files and each file contains the given number of policies.

Setting	Description
JSON users per file (FortiSASE only)	When the input value is empty, all the users would be output into one file. If a number is given, the output file would be split into multiple files and each file contains the given number of users.
Profile group name (FortiSASE only)	The profile group name which is needed in FortiSASE API.
Comment Options	
Policy comment - Preserve the original comment	Include the original comment in the source file in the comment of the output policy.

Ivanti Source Preview

This table shows the information inside the configuration.

Setting	Description
File Name	Source configuration file names are shown in the table as a link. Click the link to see the content. The file won't show if it's too large.
Model	The model of the configuration.
Source Configuration Preview	The number of each type of object is shown in the preview table. Click the object number to see detailed information about each object. In each type of object, click the **Export CSV** button to export the current object info as a CSV file.

Ivanti Conversion Result

Setting	Description
Conversion Summary	Provides information about the conversion.

Setting	Description
Device Summary	Provides statistics about the detected objects.

Juniper Conversions

Juniper ScreenOS or Junos OS differences

VLAN logical interfaces

FortiConverter recognizes interface names starting with "vlan" as logical interfaces.

Service objects

Junos OS service objects support MS-RPS and SUN-RPC, where program-numbers (SUN) and UUID (MS) are used instead of ports.

FortiOS supports this configuration using Application Control with an application override.

Example of Junos service object conversion

```
config application list
   edit "MS-ActiveDirectory"
      config entries
         edit 1
            set application 152305667
            config parameters
            edit 1
               set value "45f52c28-7f9f-101a-b52b-08002b2efabe"
            next
            edit 2
               set value "811109bf-a4e1-11d1-ab54-00a0c91e9b45"
            next
            end
            set action pass
         next
      end
   next
end

edit 10012
   set srcintf "trust"
   set dstintf "mgn"
   set srcaddr "MEI-Novi-172.24.81.0-24" "MEI-Novi-172.24.80.0-24" "MEI-Novi-
        172.24.252.112-28"
   set dstaddr "MEI-WAN"
   set service "MS-ActiveDirectory"
```

```
   set schedule "always"
   set logtraffic all
   set status enable
   set action accept
   set comments "95"
   set application-list "MS-ActiveDirectory"
next
```

NAT support

For SRX Series gateways, supports the FortiConverter conversion of the following NAT types:

- Destination NAT
- Source NAT
- Static NAT

In ScreenOS, source NAT is implicitly enabled when: the destination zone is in the untrust-vr, the source zone is trust zone and the destination zone is untrust zone, and both belong to the trust-vr.

Saving the Juniper source configuration file

Before starting the conversion wizard, save a copy of your Juniper configuration file to the computer where FortiConverter is installed.

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;
                  }
               }
         }
      }
   }
   ............
   ............
```

Juniper conversion wizard

The administrator password is **not** set on the new configuration.

For third-party conversions, the trusted host settings are converted. Check the trusted host settings to ensure they allow management access from the relevant network interfaces.

To start a new conversion

1. Start FortiConverter.
2. When start-up is complete, a browser window automatically opens to http://127.0.0.1:8000.
3. Click New Conversion **New Conversion**, located at the top right corner.
4. Enter a name for the conversion configuration.
5. For Vendor, choose **Juniper** block.
6. Choose a Model, if applicable.
7. Click **OK**.

The configuration page opens to the Start page, and you can input your settings.

Juniper Start options

This table lists the start settings.

Setting	Description
Profile	
Description	Enter a description of the configuration.
Output Options	
Output Format	Select the appropriate output for your target Fortinet device.
FOS Version	The configuration syntax is slightly different among FortiOS 6.4, 7.0, 7.2, 7.4 and 7.6. Select the version that corresponds to the FortiOS version on the target.
Input	
Source Configuration	Select the input file or files.
Bulk Conversion	If there are many devices to be converted where all of them are the same model, sharing the same interface mapping relationship in conversion, then bulk conversion can convert all of them at once. Collect all the configuration files to be converted, compress them into a ZIP file and use the ZIP file as the input.
Target device (Optional)	

Target device	Select the model of the target device, or select a device connected to FortiConverter.
Conversion Options	
Discard unreferenced firewall objects	Specifies whether addresses, schedules, and services that aren't referenced by a policy are saved and added to the output. This option can be useful if your target device has table size limitations. You can view the unreferenced objects that FortiConverter removed on the Tuning page.
Increase Address and Service Table Sizes for High-End Models	You can customize the maximum table sizes that FortiConverter uses when Adjust table sizes is selected. For more information, see Adjusting table sizes on page 232
Route-based IPSec	Specifies whether Route-based IPSec is used for this conversion.
Enable consolidated policy mode	Enable consolidated mode in FortiOS and convert security rules into consolidated policies which are able to reference both IPv4 and IPv6 addresses in a single policy.
Use Zone name instead of number to distinguish duplicate address names (SRX only)	Juniper SRX may have multiple address objects with the same name but tied to different zones. When this option is enabled, duplicate address name will be converted to `origname_zonename`. When disabled, they will be converted to `origname_1, origname_2` ... etc.
Enable consolidated policy mode	(Only available for FortiOS 6.2 conversions) Enable consolidated mode in FortiOS and convert security rules into consolidated policies which are able to reference both IPv4 and IPv6 addresses in a single policy.
Migrate VIP src-filter into policy src-addr	When this option is enabled, a policy using VIPs as destinations would use the source filter of the VIPs as source addresses.
Set src/dst interfaces to "any" in policies	When this option is enabled, the source and destination interfaces of all the policies would be set to "any".
Set extintf to "any" under "config firewall vip"	When selected, all vip extintf value will be set to “any”. Only available when central NAT mode is enabled.
Virtual Router Options	
Merge virtual routers into the default VRF	When this option is enabled, all the interfaces and routes assigned to virtual routers will be converted with no VRF(Virtual Routing and Forwarding) settings, which means they will all belong to the default VRF.
Convert virtual routers into FOS virtual domains	It is an approach to convert a virtual router into independent VDOMs in FortiOS. When this option is enabled, each virtual router would be converted into a VDOM.
Convert virtual routers into FOS VRFs	When this option is enabled, each virtual router would be converted into a VRF in FortiOS.
Comment Options	
Include input configuration lines for each output	Specifies whether FortiConverter includes the input configuration lines used for each FortiGate policy in the FortiGate configuration as a policy

policy	comment.
Interface Comment	Specifies whether FortiConverter copies the interface comment from the source configuration to the mapped FortiGate interface.
Address Comment	Specifies whether FortiConverter copies the address comment from source configuration to the converted FortiGate address.
Service Comment	Specifies whether FortiConverter copies the service comment from the source configuration to converted FortiGate service.
Rule comment	Specifies whether FortiConverter copies the security rule comment from the source configuration to converted FortiGate service.
Rule annotated comment (SRX only)	Specifies whether FortiConverter copies the annotated lines in rules from the source configuration to converted FortiGate policies.
NAT Merge Options	
Ignore firewall policies with all or any addresses when processing NAT rules (SRX only)	Specifies whether FortiConverter ignores firewall policies with an "all" or "any" address when it merges a NAT rule and a firewall policy to create a FortiGate NAT policy. FortiConverter creates new policies in the output configuration based on where NAT rules to firewall policies intersect. Because firewall policies that use "all" or "any" as the address create many intersections, Fortinet recommends that you ignore them.
Enable Central NAT merge	Specifies whether FortiConverter converts NATs to FortiGate central NATs instead of policy-based NATs.
Convert Static NATs into VIP/source NAT pair	When this option is enabled (in policy NAT mode only), a static NAT rule would be converted into a central SNAT rule and an unidirectional VIP object. Otherwise it would be converted into a bidirectional VIP object
NAT Merge Depth (SRX only)	

Source NAT	Specifies which types of NAT FortiConverter merges with the output firewall policies, or whether FortiConverter performs NAT merge based on object names or values. • Off – FortiConverter converts firewall policies only and doesn't perform NAT merge for this type of NAT. This is useful for performing a quick, initial conversion to discover any conversion issues. • Object Names – FortiConverter performs NAT merge based on matching address names in firewall policies and NAT rules. • Object Values – FortiConverter performs NAT merge based on matching address values in firewall policies and NAT rules. It generates the most accurate matching of NAT rules and policies, but in most cases, it also generates more NAT policies. Because it can take FortiConverter several hours to complete a conversion that include a large number of NAT rules, Fortinet recommends that you turn off or limit NAT merge for your initial conversion. Then, resolve any issues with the conversion before you run it again with NAT merge enabled. For more information, including example matches, see NAT merge options on page 233.
Static NAT	
Destination NAT	

LSYS (Junos OS) or VSYS (ScreenOS) selection

Map the logical or virtual systems in the source configuration to VDOMs in the output configuration.

By default, all logical or virtual systems are mapped to VDOMs with the same name. You can modify this default mapping as required by renaming VDOMs and removing logical or virtual systems from the conversion.

Setting	Description
VDOM Select	Select/Unselect the VDOM item.
VDOM Rename	Rename the VDOM name.
VDOM Mode	Change the VDOM mode in the output result.
Information of Configurations	Source configuration file names are shown in the table as a link. Click the link to see the content. The file won't show if it's too large.
Managed Device Name	The name of the managed device which the converted interface or route configuration would be imported in FortiManager. (Only available when the output format is FortiManager)
Target Device Switch Interface - Interface/Port	If there are virtual switches in the selected target device, FortiConverter will list the member ports of the virtual switches. If an interface in the list is going to be used in the configuration, it should first be detached from the virtual switch. Click "**X**" on the interface to detach it. Please note that a detached interface cannot be re-added later by FortiConverter.

Source Configuration Preview	The numbers of each type of firewall object are shown in the preview table. Click the object number to see detailed information on each object. In each type of object, click the button **Export CSV** to export the current object info as CSV file.

Juniper Interface mapping

You can manually map the interface.

- To **select** the appropriate FortiGate interface, click the value in the FortiGate Interface column, and then select a value or enter a custom interface name.
- To **edit** other values, double-click the proper column. Use the toolbar icon on the right to show and hide columns. You can also use the Tuning page to create mappings after the conversion is complete.
- To **import** a set of interface mappings from a file, click **Import**.
- To **download** the current set of interface mappings, click **Export**.
- To **delete** an interface, select the entries you would like to delete, **right click** and select **Delete Selected**. This is useful if your target FortiGate has fewer interfaces than the source configuration.

The limit of the length of interface names in FortiOS is 15 characters. Interfaces in the source config which have longer names should be trimmed to a shorter name. It is recommended to trim the names manually to ensure readability. But if a quick trimming is needed, please select the entries, **right click** and select **Trim Interface Name** to trim the names into 15 characters automatically.

Setting	Description
VDOM	Shows the virtual domains used in the conversion. ("root" by default)
Source Interface	Shows each interface on the Juniper firewall.
FortiGate Interface	The input field for corresponding FortiGate interface names. Click to assign a FortiGate port or input the interface name manually for each interface. (Only available when the output format is **FortiGate**)
Normalized interface	The input field for corresponding normalized interface names, which would be configured in the ADOM database in FortiManager. Click to assign a port or input the interface name manually for each interface. (Only available when the output format is **FortiManager**)
Device interface	The input field for corresponding interface names in the managed devices in FortiManager. Click to assign a port or input the interface name manually for each interface. (Only available when the output format is **FortiManager**)

Setting	Description
Members	Shows any members, if they are set.
IP-Netmask	Shows the IP address and netmask of the connection.
Type	Shows the type of interface.
Access	Shows which protocols has permission to access each interface.
Import	Click to load a set of interface mappings from a text file.
Export	Saves the current set of interface mappings to a text file.
Delete Selected	Click to delete the selected mapping item.
Trim Interface Name	Trim the interface names which exceed 15 characters into 15 characters automatically.

Juniper Route Information

FortiConverter creates static routes in the output using the static routes it detects in the source configuration and any routing information you provide.

Double-click an item to edit it.

Setting	Description
New Route	Click to add a route.
Delete	Click to delete the selected route.

Juniper Conversion result

Tab	Description
Conversion Summary	Provides statistics about the conversion.
Reports	Generate PDF reports including converted and unconverted objects list.
VDOM Mapping	Shows how VDMS were mapped from the source device to the new device.
Interface Mapping	Shows how interfaces were mapped for each VDOM from the source device.
Device Summary	Provides statistics about the detected objects.

FortiConverter includes error and warning messages into the conversion when an error occurs.

Review the `config-all.txt` file after each conversion for errors. These errors and warning messages might cause the import process to fail, if not corrected. See for more details.

NetScaler Conversions (Beta feature)

Conversion Support

FortiConverter supports the following features: (Convertible Objects)

- Interface
- Real servers
- Pools

Saving the NetScaler source configuration files

Before starting the conversion wizard, save a copy of your NetScaler configuration file to the computer where FortiConverter is installed.

Exporting config through web operation

1. Choose **Configurations > System**.
2. Click the **Save** icon (floppy button) on the right-hand side.
3. Click **Save** and select a path on the terminal to save the configuration file.

NetScalar Conversion Wizard

The administrator password is **not** set on the new configuration.

For third-party conversions, the trusted host settings are converted. Check the trusted host settings to ensure they allow management access from the relevant network interfaces.

To start a new conversion

1. Start FortiConverter.
2. When start-up is complete, a browser window automatically opens to http://127.0.0.1:8000.
3. Click New Conversion **New Conversion**, located at the top right corner.
4. Enter a name for the conversion configuration.
5. For Vendor, choose **NetScaler** block.
6. Choose a Model, if applicable.
7. Click **OK**.

The configuration page opens to the Start page, and you can input your settings.

NetScaler Start Options

This table lists the start settings.

Setting	Description
Profile	
Description	Enter a description for NetScaler
Output Options	
Output Format	The output format of the converted configuration. Only FortiADC is currently available currently.
FOS Version	The configuration syntax of the output. Only v5 is available currently.
Input	
Source Configuration	Select the input file

NetScaler Source Preview

This table shows the information inside the configuration.

Setting	Description
File Name	Source configuration file names are shown in the table as a link. Click the link to see the content. The file won't show if it's too large.
Model	The model of the configuration.
Source Configuration Preview	The number of each type of object is shown in the preview table. Click the object number to see detailed information about each object. In each type of object, click the Export CSV button to export the current object info as a CSV file.

NetScaler Conversion Result

Setting	Description
Conversion Summary	Provides information about the conversion.
Device Summary	Provides statistics about the detected objects.

Open Systems Conversions (Beta feature)

Conversion Support

FortiConverter supports the following features for Open Systems conversions:

- Addresses
- Address groups
- Services
- Service groups

Open Systems Conversion Wizard

To start a new conversion

1. Start FortiConverter.
2. When start-up is complete, a browser window automatically opens to http://127.0.0.1:8000.
3. Click New Conversion **New Conversion**, located at the top right corner.
4. Enter a name for the conversion configuration.
5. For Vendor, choose **Open Systems** block.
6. Choose a Model, if applicable.
7. Click **OK**.

The configuration page opens to the Start page, and you can input your settings.

Open Systems Start Options

This table lists the start settings.

Setting	Description
Profile	
Description	Enter a description of the configuration.
Output Options	
Output Format	Select the appropriate output for your target Fortinet device.
FOS Version	The configuration syntax is slightly different for FortiOS 6.4, 7.0, 7.2, 7.4 and 7.6. Select the version that corresponds to the FortiOS version on the target.
Input	
Source Configuration	Select the input file.
Target Device (Optional)	
Target Device	Select the model of the target device.

Open Systems Source Preview

This table shows the information inside the configuration.

Setting	Description
File Name	Source configuration file names are shown in the table as a link. Click the link to see the content. The file won't show if it's too large.
Model	The model of the configuration.
Source Configuration Preview	The number of each type of object is shown in the preview table. Click the object number to see detailed information about each object. In each type of object, click the **Export CSV** button to export the current object info as a CSV file.

Open Systems Conversion Result

Setting	Description
Conversion Summary	Provides information about the conversion.
Device Summary	Provides statistics about the detected objects.

Palo Alto Networks Conversion

Conversion support

FortiConverter supports the following features

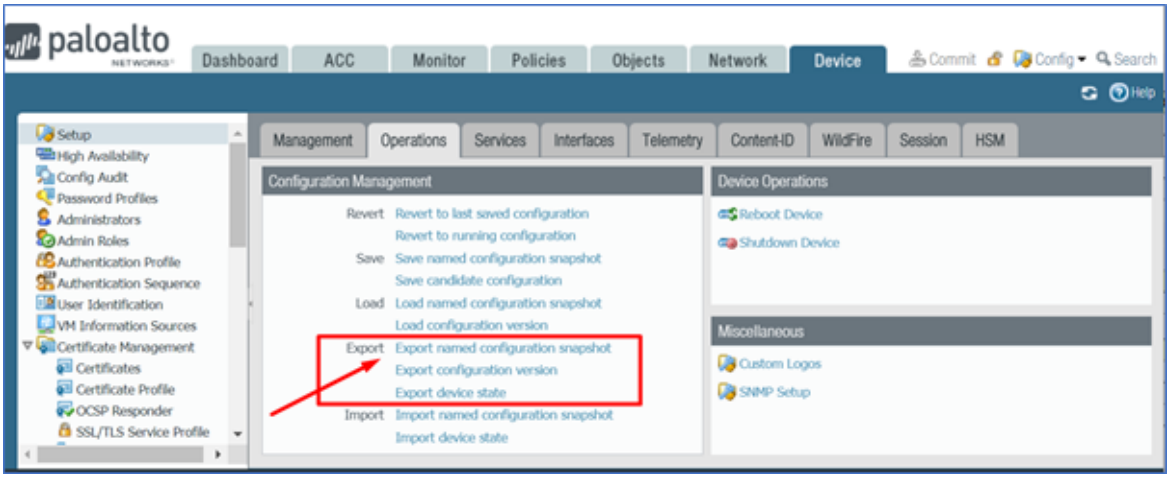
- Interface
- Zone
- Address(group) (Including IPV6)
- Service(group)
- Policy
- NAT (Rule NAT only)
- VPN
- Route
- Schedule
- User

Saving the PAN source configuration files

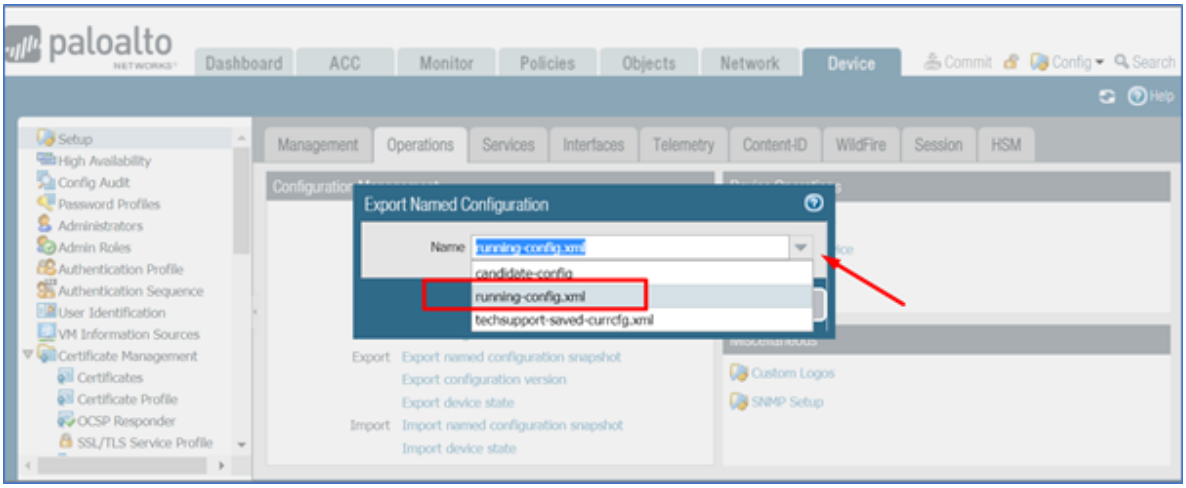
Before starting the conversion wizard:**Palo Alto**, save a copy of your configuration file to the computer where FortiConverter is installed.

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**.



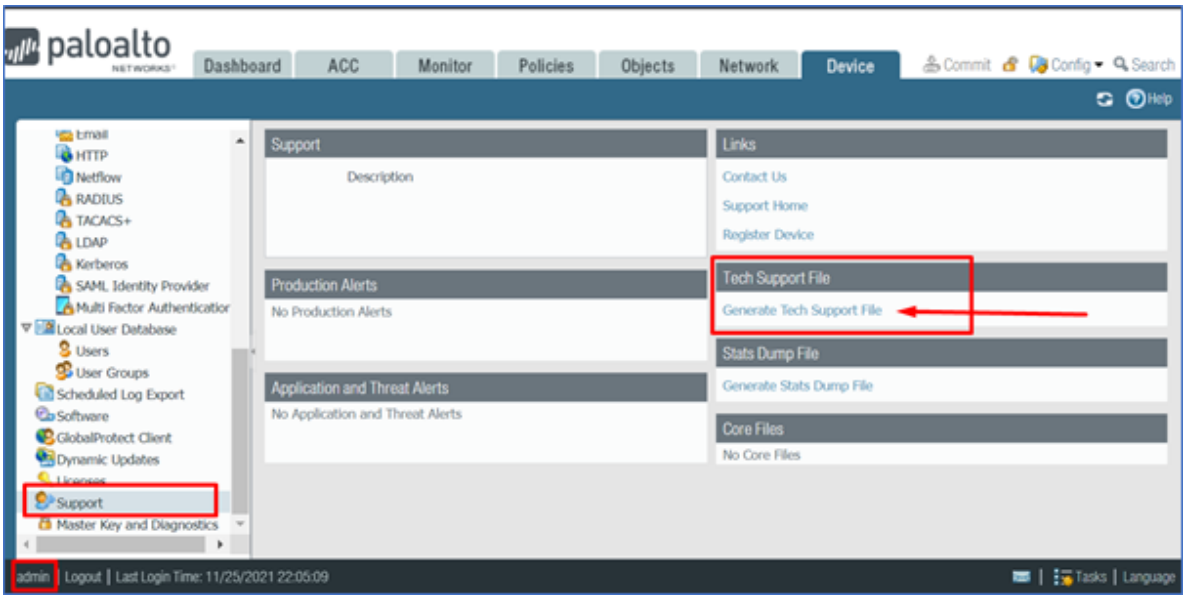
3. Select the **running-config.xml** from the dropdown menu.



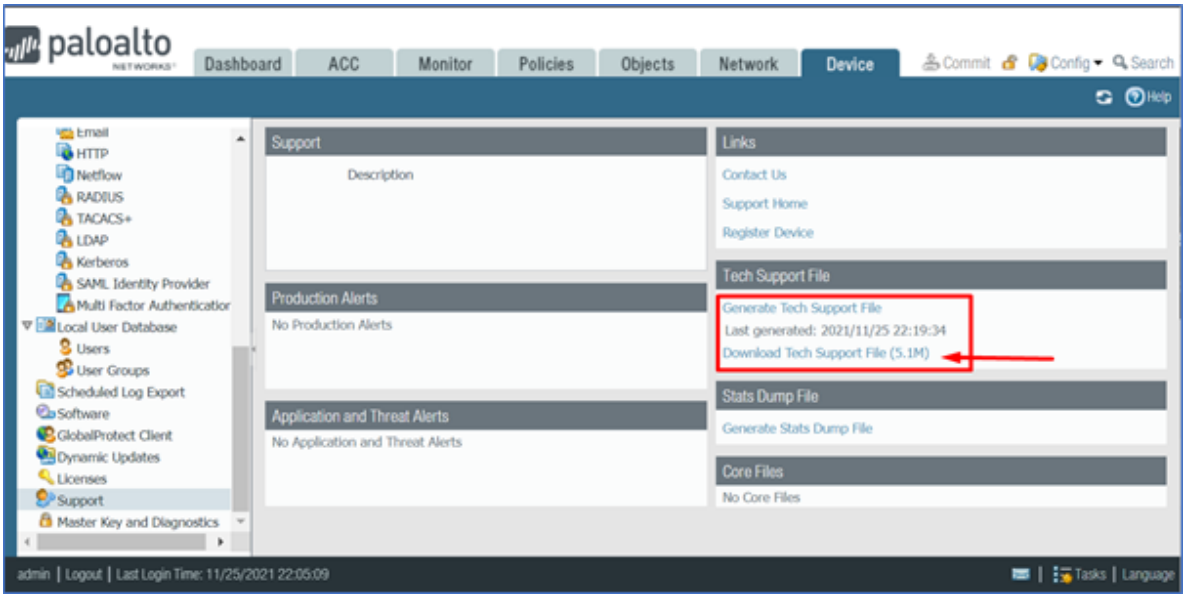
4. Download the file above and upload to FortiConverter through the source configuration tab and follow the steps in conversion process.

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

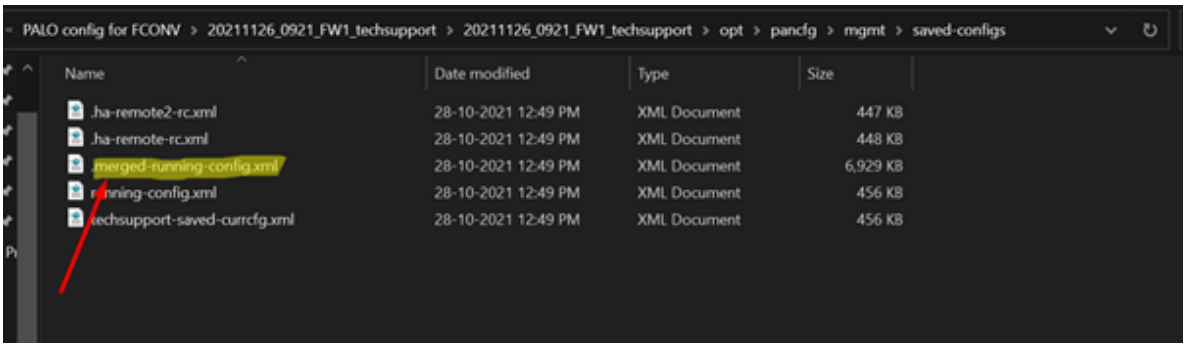
1. Log in to the **Palo Alto FW** web UI using super-user account.
2. In the web UI, go to **Device > Support > Tech Support File**, then click **Generate Tech support File**.



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.

Saving the Application Default Services Table

Saving a PAN application name mapping FortiGate service name file which includes the PAN application names and standard ports information. The mapping can be exported into a csv file from Palo Alto FW. Then upload the file to FortiConverter through application default services table tab on the start page.

Palo Alto conversion wizard

The administrator password is **not** set on the new configuration.

For third-party conversions, the trusted host settings are converted. Check the trusted host settings to ensure they allow management access from the relevant network interfaces.

To start a new conversion

1. Start FortiConverter.

2. When start-up is complete, a browser window automatically opens to http://127.0.0.1:8000.

3. Click New Conversion **New Conversion**, located at the top right corner.
4. Enter a name for the conversion configuration.
5. For Vendor, choose **PaloAlto** block.
6. Choose a Model, if applicable.
7. Click **OK**.

The configuration page opens to the Start page, and you can input your settings.

Palo Alto Start options

This table lists the start settings.

Setting	Description
Profile	
Description	Enter a description of the configuration.
Output Options	
Output Format	Select the appropriate output for your target Fortinet device.
FOS Version	The configuration syntax is slightly different among FortiOS 6.4, 7.0, 7.2, 7.4 and 7.6. Select the version that corresponds to the FortiOS version on the target.
Input	
Source Configuration	Select the input file.
Bulk Conversion	If there are many devices to be converted where all of them are the same model, sharing the same interface mapping relationship in conversion, then bulk conversion can convert all of them at once. Collect all the configuration files to be converted, compress them into a ZIP file and use the ZIP file as the input.
Panorama Configuration(optional)	Upload the panorama config to be converted together with device config.
Application Default Services Table (csv format) (optional)	Select the application default services table in CSV format. This file should include the PAN application names and standard ports information. FortiConverter uses the information in the file to convert PAN application names to FortiGate service names.
Target device (Optional)	
Target device	Select the model of the target device, or select a device connected to FortiConverter.
Conversion Options	

Discard unreferenced firewall objects	Specifies whether addresses and services that aren't referenced by a policy are saved and added to the output. This option can be useful if your target device has table size limitations. You can view the unreferenced objects that FortiConverter removed on the Tuning page.
Increase Address and Service Table Sizes for High-End Models	You can customize the maximum table sizes that FortiConverter uses when Adjust table sizes is selected. For more information, see Adjusting table sizes on page 232.
Policy index start from 1 instead of 10000	When selected, the serial number of firewall policies will start from 1 instead of 10000.
Converted source vendor's application ID as-is	When selected, the converter will generate "`set application <original app-name as-is>`" into firewall policy, if an application is defined for it. The output still requires manual processing.
NGFW policy-based mode	When selected, the conversion will be in NGFW policy-based mode. "`firewall policy`" will become "`firewall security-policy`" instead, and "`set application 00000`" will be generated in policies, which requires manual processing. There will also be some other minor differences adapted for the NGFW policy-based CLI.
Convert "log-start" or "log-end" to "set logtraffic-start enable" in policy	When a policy has "<log-end>" or "<log-start>", it will be converted as "set logtraffic-start enable".
Convert URL filters into FQDNs and external resources	When this option is enabled, the URL filters in the Palo Alto configs would be converted. For those URL categories which only have domain names, they will be converted into a group containing FQDN objects. For those URL categories which contain URL with path, they will be converted into external resources. User will need to set up a server to maintain the URL list externally.
Set extintf to "any" under "config firewall vip"	When selected, all vip extintf value will be set to "any". Only available when central NAT mode is enabled.
Convert URL category to webfilter profile	When selected, url categories will be converted to webfilter profile instead of to address objects/groups.
Convert policy tag to global-label	PaloAlto exclusive option, covert PAN policy's tag into FGT policy's global-label for grouping policies
Expand profile group in policies	Replace the profile groups configured in firewall policies into the individual security profiles in the group.
Virtual Router Options	

Merge virtual routers into the default VRF	When this option is enabled, all the interfaces and routes assigned to virtual routers will be converted with no VRF(Virtual Routing and Forwarding) settings, which means they will all belong to the default VRF.
Convert virtual routers into FOS VRFs	When this option is enabled, each virtual router would be converted into a VRF in FortiOS.
Comment Options	
Include input configuration lines for each output policy	Specifies whether FortiConverter includes the input configuration lines used for each FortiGate policy in the FortiGate configuration as a policy comment.
Interface Comment	Specifies whether FortiConverter copies the interface comment from the source configuration to the mapped FortiGate interface.
Address Comment	Specifies whether FortiConverter copies the address comment from source configuration to the converted FortiGate address.
Service Comment	Specifies whether FortiConverter copies the service comment from the source configuration to converted FortiGate service.
Nat Merge Options	
Ignore firewall policies with all or any addresses when processing NAT rules	Specifies whether FortiConverter ignores firewall policies with an "all" or "any" address when it merges a NAT rule and a firewall policy to create a FortiGate NAT policy. FortiConverter creates new policies in the output configuration based on where NAT rules to firewall policies intersect. Because firewall policies that use "all" or "any" as the address create many intersections, Fortinet recommends that you ignore them.
Enable central NAT merge	Specifies whether FortiConverter converts NATs to FortiGate central NATs instead of policy-based NATs. It is recommended to enable this option with FOS 6.0.

PAN Source Configuration

Source Preview

Setting	Description
VDOM Select	Select/Unselect the VDOM item.
VDOM Rename	Rename the VDOM name.
VDOM Mode	Change the VDOM mode in the output result.
Information of Configurations	Source configuration file names are shown in the table as a link. Click the link to see the content. The file won't show if it's too large.

Managed Device Name	The name of the managed device which the converted interface or route configuration would be imported in FortiManager. (Only available when the output format is **FortiManager**)
Target Device Switch Interface - Interface/Port	If there are virtual switches in the selected target device, FortiConverter will list the member ports of the virtual switches. If an interface in the list is going to be used in the configuration, it should first be detached from the virtual switch. Click "**X**" on the interface to detach it. Please note that a detached interface cannot be re-added later by FortiConverter.
Source Configuration Preview	The numbers of each type of firewall object are shown in the preview table. Click the object number to see detailed information on each object. In each type of object, click the button **Export CSV** to export the current object info as CSV file.

Palo Alto Interface mapping

You can manually map the interface.

- To **select** the appropriate FortiGate interface, click the value in the FortiGate Interface column, and then select a value or enter a custom interface name.
- To **edit** other values, double-click the proper column. Use the toolbar icon on the right to show and hide columns. You can also use the Tuning page to create mappings after the conversion is complete.
- To **import** a set of interface mappings from a file, click **Import**.
- To **download** the current set of interface mappings, click **Export**.
- To **delete** an interface, select the entries you would like to delete, **right click** and select **Delete Selected**. This is useful if your target FortiGate has fewer interfaces than the source configuration.

The limit of the length of interface names in FortiOS is 15 characters. Interfaces in the source config which have longer names should be trimmed to a shorter name. It is recommended to trim the names manually to ensure readability. But if a quick trimming is needed, please select the entries, **right click** and select **Trim Interface Name** to trim the names into 15 characters automatically.

Setting	Description
VDOM	Shows the virtual domains used in the conversion. ("root" by default)
Source Interface	Shows each interface on the PaloAlto firewall.
FortiGate Interface	The input field for corresponding FortiGate interface names. Click to assign a FortiGate port or input the interface name manually for each interface. (Only available when the output format is **FortiGate**)

Setting	Description
Normalized interface	The input field for corresponding normalized interface names, which would be configured in the ADOM database in FortiManager. Click to assign a port or input the interface name manually for each interface. (Only available when the output format is **FortiManager**)
Device interface	The input field for corresponding interface names in the managed devices in FortiManager. Click to assign a port or input the interface name manually for each interface. (Only available when the output format is **FortiManager**)
Members	Shows any members, if they are set.
IP-Netmask	Shows the IP address and netmask of the connection.
Type	Shows the type of interface.
Access	Shows which protocols has permission to access each interface.
Import	Click to load a set of interface mappings from a text file.
Export	Saves the current set of interface mappings to a text file.
Delete Selected	Click to delete the selected mapping item.
Trim Interface Name	Trim the interface names which exceed 15 characters into 15 characters automatically.

Palo Alto Route Information

FortiConverter creates static routes in the output using the static routes it detects in the source configuration and any routing information you provide.

Double-click an item to edit it.

Setting	Description
New Route	Click to add a route.
Delete	Click to delete the selected route.

Palo Alto Conversion result

Tab	Description
Conversion Summary	Provides statistics about the conversion.
Reports	Generate PDF reports including converted and unconverted objects list.
Interface Mapping	Shows how interfaces were mapped for each VDOM from the source device.
Device Summary	Provides statistics about the detected objects.

FortiConverter includes error and warning messages into the conversion when an error occurs.

Review the `config-all.txt` file after each conversion for errors. These errors and warning messages might cause the import process to fail, if not corrected. See for more details.

Palo Alto Application Mapping

Applications can be configured in Palo Alto policies, and FortiConverter supports converting Palo Alto policies into FortiGate policies in policy-based mode. The mapping relationship between Palo Alto applications and FortiGate applications needs to be maintained manually, and FortiConverter automatically applies the mapping relationship in the policies.

Before setting the application mapping, please extract the definitions of FortiOS applications from the target FortiGate device. The application definitions are downloaded and updated from FortiGuard every week. It is highly recommended to connect the target FortiGate device to FortiGuard, install security updates, and import the updated definitions to FortiConverter before setting the application mapping.

Steps to extract the definitions of FortiOS applications from the target FortiGate device

1. Switch the FortiGate to **NGFW policy mode**.
2. Connect to the console of the target FortiGate.
3. Input the following commands to show the definitions of FortiOS applications:

```
config global (only when the device is in multi-vdom mode)
   config firewall security-policy
           edit 1
              set application ?
```

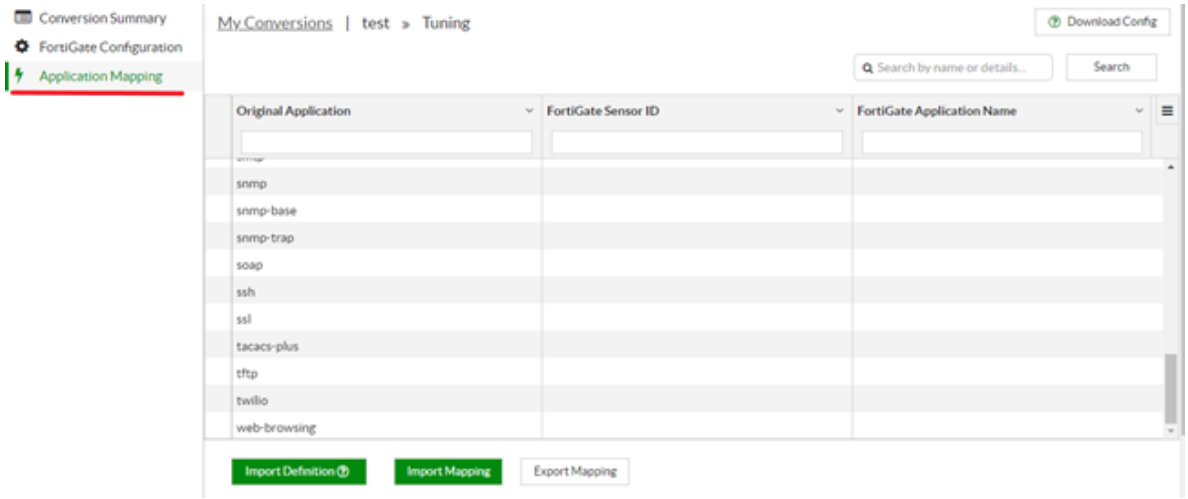
4. Save the output into a file.

   Any type of terminal application is applicable as long as it supports saving the output. The following screenshot is an example to save the output using the FortiGate CLI console.

5. Remove irrelevant lines and only keep the lines which starts from "ID / Select application ID". This file can be imported directly to the application mapping table. Alternatively, the output can be saved into a CSV file with headers in the first line, ID in the first column, and application name in the second column. The import result will be the same.

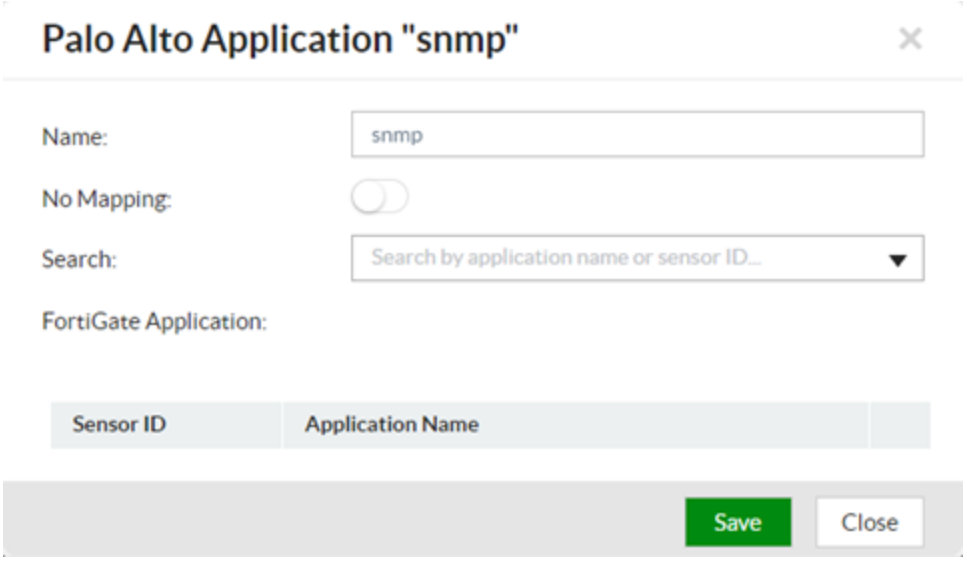
Steps to convert Palo Alto policies with applications and set application mapping relationship

1. Choose the option **Converted source vendor's application ID as-is** at the start page. This converts the configuration into policy-based mode in FortiGate.
2. Proceed the conversion to the tuning page.
3. Click **Application mapping** in the left column to show the mapping table then the Palo Alto applications used in the policies would be listed.

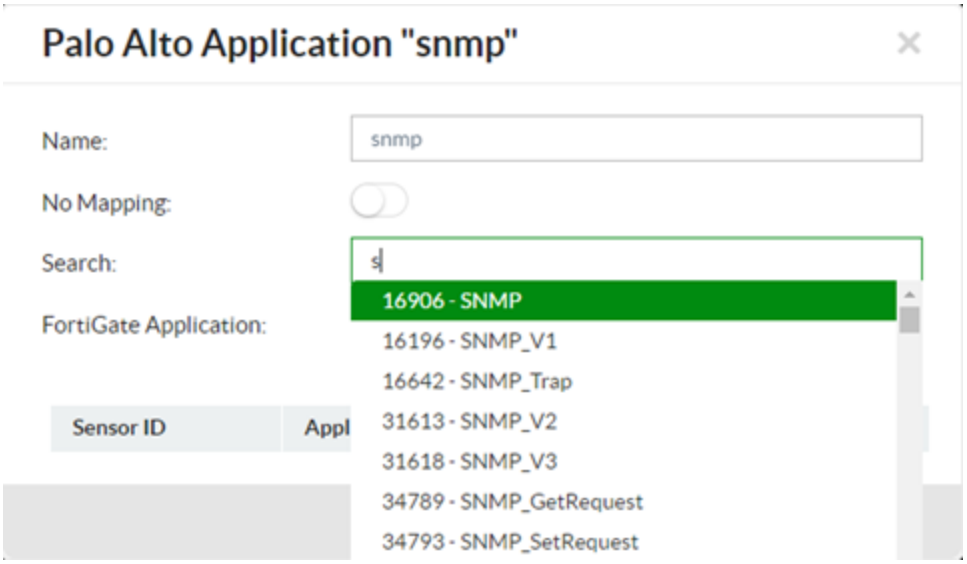


4. Click **Import Definition** and import the file with the FortiOS applications definitions extracted from the target FortiGate device. When the dialog window pops up, select whether to save the definition as default definition.
   Please note that the default definitions will only be used in future conversions with the same FortiOS version because each FortiOS version has a different application list.
   For example, if the current conversion uses FortiOS 7.2, and the definitions are saved as default, then the default definitions will only be applied on 7.2 conversions in the future, not on 7.4 conversions or other FortiOS versions. (If no definitions are imported, FortiConverter uses its own default definitions from FortiOS applications. However, this method is not recommended because some of the default definitions may be obsolete.)

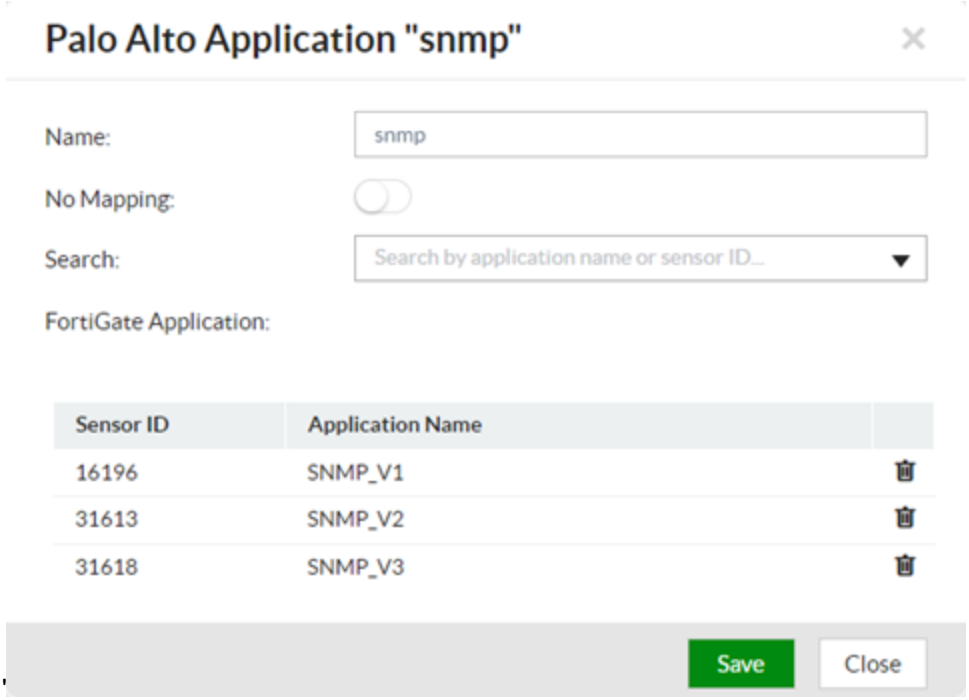
5. Click on the rows to specify the mapping of the Palo Alto application:



6. Type the FortiGate application name or ID to search the corresponding FortiGate applications.

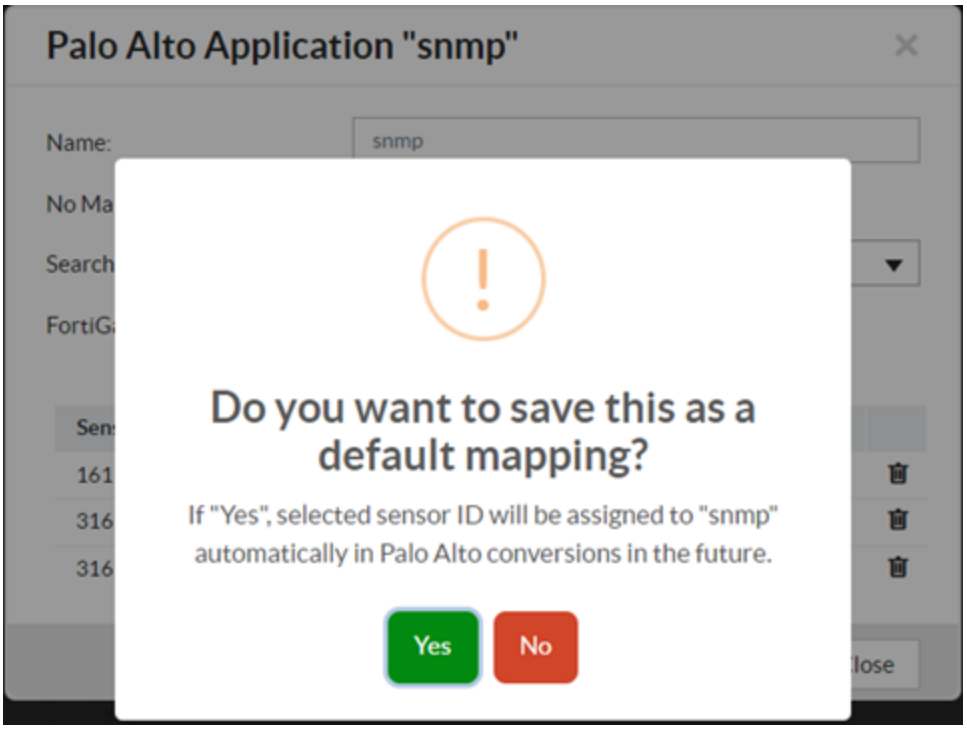


7. Select and add one or more FortiGate applications to the mapping list.

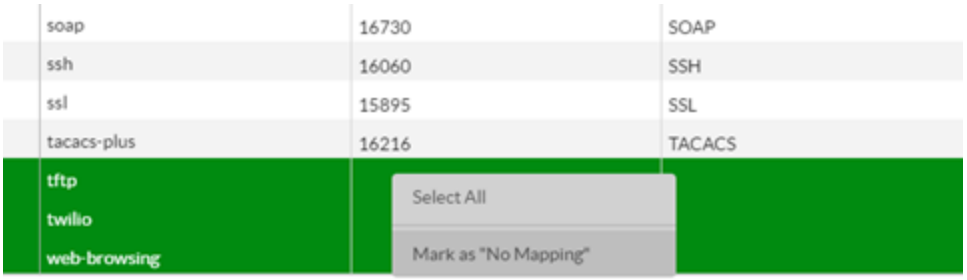


8. If the Palo Alto application is not mapped into any FortiGate applications, please enable **No Mapping** in the table. FortiConverter would skip this application in the output config.

9. Click **Save** to save the mapping relationship. If **Yes** is selected, the mapping relationship becomes the default mapping of Palo Alto conversions, and it will be applied to all Palo Alto conversions directly in the future.
   Please note that the default mapping only applies to Palo Alto conversions with the same FortiOS version because each FortiOS version has a different application list.
   For example, if the current conversion uses FortiOS 7.2, and a default mapping is saved in this conversion, then the default mapping will only be applied on 7.2 conversions in the future, but not on conversions using 7.4 or other FortiOS versions.



10. If there are multiple applications marked as "No Mapping", it is not necessary to click into each application. It can be done by selecting rows on the table, right click and select **Mark as No Mapping**.



11. After setting up the mapping relationships click **Download config** and review the converted policies, the FortiGate application IDs specified in the application mapping table would be used in the policies. However, if the mapping of a Palo Alto application is not specified (just like "radius" in the picture below), and it is not marked as "No Mapping", then FortiConverter would still use the Palo Alto application name in the policy with a warning message.

```
# Warning: Unmapped application "radius"
edit 10020
 set name "TEST policy"
 set srcintf "SrcZone"
 set dstintf "DstZone"
 set srcaddr "all"
 set application "radius" "16906" "16642" "16216"
 set dstaddr "all"
 set service "ALL"
 set schedule "always"
 set logtraffic all
 set status enable
 set action accept
next
```

12. The mapping can be exported into a CSV file and can be reused in the future Palo Alto Conversion. Please click **Export Mapping** and **Import Mapping** to export and import mapping CSV files.
Please note that it would be better to use the same definition of the FortiOS applications in the conversions that export and import the mapping. If a different definition was used, some application IDs in the exported CSV file may not exist in the imported conversion and those mappings would not be applied.

PFSense Conversion

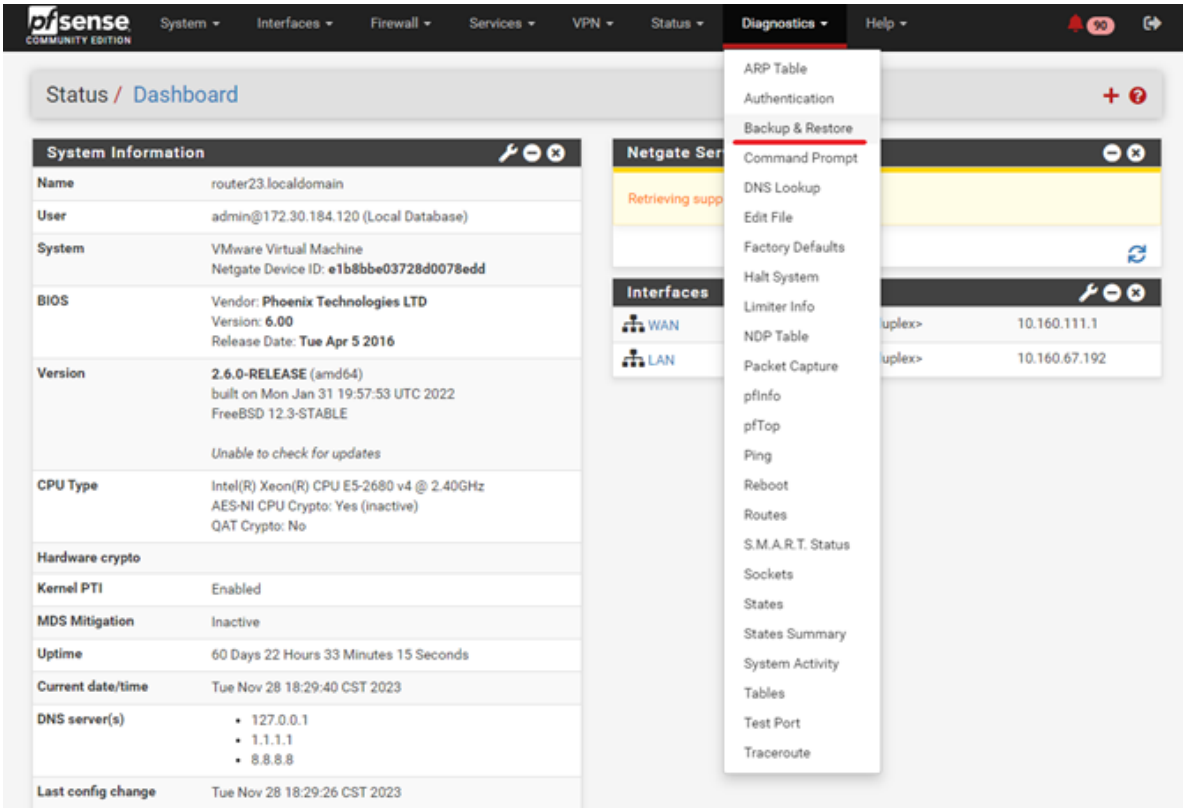
Conversion support

FortiConverter supports the following tag conversions:

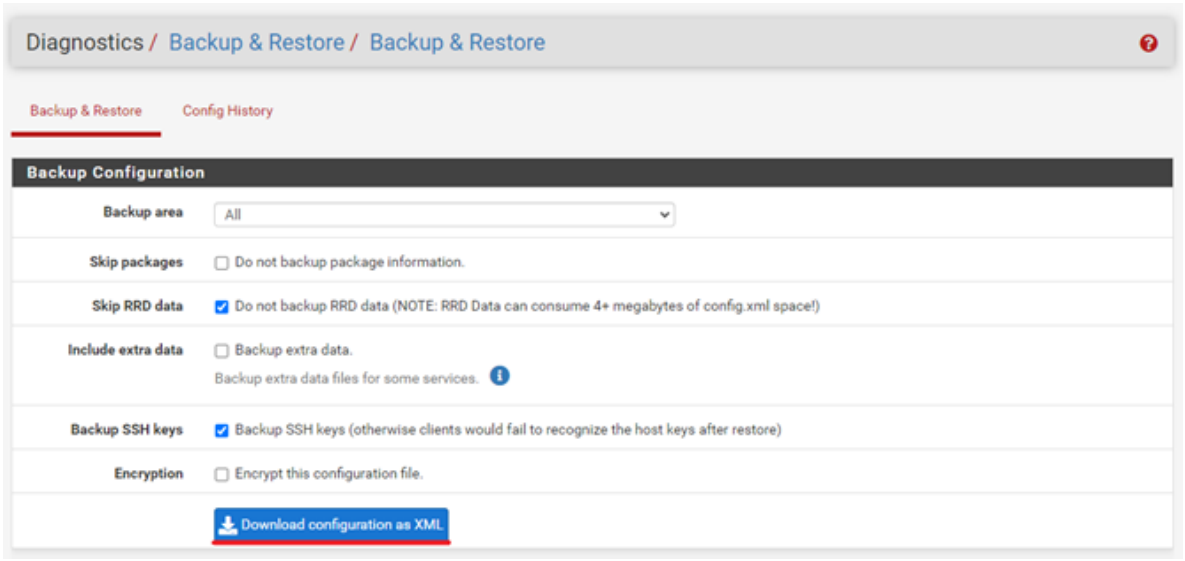
- system
- interface
- gateway / staticroutes
- dhcpd
- alias
- nat
- filter

Saving the PFSense Source Config File

1. Log into PFSense web portal.
2. Click **Diagnostics** > **Backup & Restore**



3. Click **Download configuration as XML** to download the configuration file.



PFSense Conversion Wizard

The administrator password is **not** set on the new configuration.

For third-party conversions, the trusted host settings are converted. Check the trusted host settings to ensure they allow management access from the relevant network interfaces.

To start a new conversion

1. Start FortiConverter.
2. When start-up is complete, a browser window automatically opens to http://127.0.0.1:8000.
3. Click 

New Conversion, located at the top right corner.
4. Enter a name for the conversion configuration.
5. For Vendor, choose **PFSense** block.
6. Choose a Model, if applicable.
7. Click **OK**.

The configuration page opens to the Start page, and you can input your settings.

PFSense start options

This table lists the start settings.

Setting	Description
Profile	
Description	Enter a description of the configuration.
Output Options	
Output Format	The output format of the converted configuration.
FOS Version	The configuration syntax of the output.
Input	
Source Configuration	Select the input file
Conversion Option	

Setting	Description
Discard unreferenced firewall objects	If selected, firewall objects not referenced by any policy would be converted as "unreferenced" and not show in downloaded config.
Policy index start from 1 instead of 10000	If selected, policy serial number will start from 1 instead of 10000.
Increase address and service group member sizes for high-end models	You can customize the maximum table sizes that FortiConverter uses when **Adjust table sizes** is selected. For more information, see Adjusting table sizes on page 232.
Nat Merge Option	
Enable Central NAT merge	Currently only Central NAT mode is supported for PFSense. Cannot be disabled.

PFSense Source Preview

This table shows the information inside the configuration.

Setting	Description
File Name	Source configuration file names are shown in the table as a link. Click the link to see the content. The file won't show if it's too large.
Model	The model of the configuration.
Source Configuration Preview	The number of each type of object is shown in the preview table. Click the object number to see detailed information about each object. In each type of object, click the Export CSV button to export the current object info as a CSV file.

PFSense Conversion Result

Setting	Description
Conversion Summary	Provides information about the conversion.
Device Summary	Provides statistics about the detected objects.

Radware Conversions (Beta feature)

Conversion support

FortiConverter supports the following features:

- Real servers
- Server groups
- Virtual servers

Radware Conversion Wizard

The administrator password is **not** set on the new configuration.

For third-party conversions, the trusted host settings are converted. Check the trusted host settings to ensure they allow management access from the relevant network interfaces.

To start a new conversion

1. Start FortiConverter.
2. When start-up is complete, a browser window automatically opens to http://127.0.0.1:8000.
3. Click 

New Conversion, located at the top right corner.
4. Enter a name for the conversion configuration.
5. For Vendor, choose **Radware** block.
6. Choose a Model, if applicable.
7. Click **OK**.

The configuration page opens to the Start page, and you can input your settings.

Radware Start Options

This table lists the start settings.

Setting	Description
Profile	
Description	Enter a description of the configuration.
Output Options	
Output Format	The output format of the converted configuration. Only FortiADC is available currently.
FOS Version	The configuration syntax of the output. Only v5 is available currently.
Input	
Source Configuration	Select the input file

Radware Source Preview

This table shows the information inside the configuration.

Setting	Description
File Name	Source configuration file names are shown in the table as a link. Click the link to see the content. The file won't show if it's too large.
Model	The model of the configuration.
Source Configuration Preview	The number of each type of object is shown in the preview table. Click the object number to see detailed information about each object. In each type of object, click the Export CSV button to export the current object info as a CSV file.

Radware Conversion Result

Setting	Description
Conversion Summary	Provides information about the conversion.

Setting	Description
Device Summary	Provides statistics about the detected objects.

Snort IPS Signature Conversion

Snort conversion wizard

Basic outline of a snort rule

```
[action][protocol][sourceIP][sourceport] -> [destIP][destport] ( [Rule options] )
| ---------------- Rule Header ------------------------------ |- Rule Options - |
```

SNORT rule example

```
alert tcp $EXTERNAL_NET $FILE_DATA_PORTS -> $HOME_NET any (msg:"FILE-FLASH
Adobe Flash Player ActionScript virtual machine opcode verifying code
execution attempt"; flow:to_client,established; flowbits:isset,file.swf;
file_data; content:"|01 09 0A 2E D0 30 D0 5D 04 4A 04 00 68 01 D0 92 90 4E|";
fast_pattern:only; metadata:policy balanced-ips drop, policy connectivity-ips
drop, policy security-ips drop, service ftp; reference:cve,2012-5271;
reference:url,adobe.com/support/security/bulletins/apsb12-22.html;
classtype:attempted-user; sid:24874; rev:3;)
```

FGT custom IPS signature

```
config ips custom
   edit "S24874R3"
      set signature "F-SBID(--name \"S24874R3\"; --protocol tcp; --service FTP; --flow
           from_server; --tag test,file.swf; --pattern \"|01 09 0A 2E D0 30 D0 5D 04 4A
           04 00 68 01 D0 92 90 4E|\";)"
      set action block
      set status enable
      set log enable
      set comment ''
   next
end
```

Warning: The character "?" is a special character in the interactive console on FortiGate, so if it's in the pcre of a signature, it won't be saved. The workaround is to upload the IPS signature through the web GUI.

"action" field

Supported keyword

```
   alert
```

Unsupported keyword

```
log
```

"protocol" field

Supported keyword

```
tcp/udp/ip/icmp/HTTP/FTP/POP3/SMTP/TELNET/SSH/IMAP/SNMP/RADIUS
HTTP/FTP/POP3/SMTP/TELNET/SSH/IMAP ->; tcp
SNMP/RADIUS ->; udp
```

"sourceIP", "sourceport", "destIP" and "destport" fields

Supported keyword

```
Either "any" or "$xxxx" variable
```

"Rule options" field

Supported keywords

Option	Test input	Test output
byte_test	byte_test:1,!&,0xF8,2;	--byte_test 1,~,0xF8,2;
byte_jump	byte_jump:4,-10,relative,little;	--byte_jump 4,-10,little,relative;
threshold	threshold:type limit, track by_src, count 1, seconds 60;	--track SRC_IP; --rate 1,60;
nocase	nocase;	--no_case;
isdataat	isdataat:50,relative;	--data_at 50,relative;
http_raw_uri	http_raw_uri;	--context uri;
http_raw_cookie	http_raw_cookie;	--context header;
http_raw_header	http_raw_header;	--context header;
http_stat_code	http_stat_code;	--context banner;
http_stat_msg	http_stat_msg;	--context banner;
sip_header	sip_header;	--context header;
sip_body	sip_body;	--context body;
id	id:123456;	--ip_id 123456;
dsize	dsize:<400;	--data_size <400;
ipopts	ipopts:lsrr;	--ip_option lsrr;
flags	flags:SF,CE;	--tcp_flags SF,CE;

seq	seq:0;	--seq 0;
ack	ack:0;	--ack 0;
window	window:55808;	--window_size 55808;
itype	itype:>30;	--icmp_type >30;
icode	icode:>30;	--icmp_code >30;
icmp_id	icmp_id:0;	--icmp_id 0;
icmp_seq	icmp_seq:0;	--icmp_seq 0;
rpc	rpc:100000, *, 3;	--rpc_num 100000, *, 3;
sameip	sameip;	--same_ip;
ttl	ttl:<3;	--ip_ttl <3;
tos	tos:!4;	--ip_tos !4;
content	content:"OK LOGIN";	--pattern \"OK LOGIN\";
flowbits	flowbits:set,logged_in; flowbits:noalert;	--tag set,logged_in; --tag quiet;
flow	flow:to_server,established;	--flow from_client;
pcre	pcre:"/^User-Agent\x3A[^\r\n]*malware/miH";	--pcre \"/^User-Agent\x3A [^\r\n]*malware/mi\";
uricontent	uricontent:"testurl";	--pattern "testurl"; --context uri;
ip_proto	ip_proto:igmp;	--protocol igmp;
depth	depth:8;	--within 8,packet;
offset	offset:4;	--distance 4,packet;
within	within:10;	--within 10;
distance	distance:4;	--distance 4;
http_client_ body	http_client_body;	--context body;
http_cookie	http_cookie;	--context header;
http_method	http_method;	--context uri;
urilen	urilen:5;	--data_size 5,uri;
metadata	metadata:impact_flag red, service dns;	--service DNS;
sid	sid:19644;	--name \"S19644R4\";
rev	rev:4;	--name \"S19644R4\";
byte_extract	byte_extract:1, 0, str_offset;	--extract 1,0,$0;
rawbytes	rawbytes;	--context packet_origin;

msg	msg:"Bad Stuff detected within field";	et comment "Bad Stuff detected within field"
file_data	file_data;	--context file;
pkt_data	pkt_data;	--context packet;
detection_filter	detection_filter:track by_src, count 30, seconds 60;	--rate 30,60; --track SRC_IP;

Unsupported keywords:

Option	Test input
replace	
stream_reassemble	
stream_size	
cvs	
ftpbounce	
asn1	
fragbits	
fragoffset	
base64_decode	
base64_data	
sip_method	
sip_stat_code	
gtp_type	
gtp_info	
gtp_version	
ssl_state	
reference	
classtype	
priority	
gid	
fast_pattern	
logto	
session	
resp	

react
tag
activites
activites_by
http_encode
count
dce_iface
dce_opnum
dce_stub_data
metadata
protected_content
hash
length
modbus_func
dnp3_ind

Snort Start options

This table lists the start settings.

Setting	Description
Profile	
Description	Enter a description of the configuration.
Input	
Snort Rules	Select the input file.
Snort Variable Definition (optional)	Select the file that defines IPS and port files. Undefined variables will be converted into "any".
Conversion Options	
Add extra backslash "\" for special characters	FortiConverter adds an extra back slash for special characters in the conversion.
Convert annotated	Select to disable rules that are annotated in the source

rules as status disable	configuration.
NGFW policy-based mode	When selected, the conversion will be in NGFW policy-based mode. "`firewall policy`" will become "`firewall security-policy`" instead, and "`set application 00000`" will be generated in policies, which requires manual processing. There will also be some other minor differences adapted for the NGFW policy-based CLI.

Source Preview

This page shows the information inside the configuration.

Setting	Description
IP Variables	The definitions of IP variables parsed from the variable definition file.
Port Variables	The definitions of port variables parsed from the variable definition file.
Snort IPS Signature	IPS signatures parsed from the input Snort rule files.

Snort Conversion result

Tab	Description
Snort IPS Signature	Shows variable definitions and Snort IPS signature contents.
FortiGate IPS Signature	Shows converted FortiGate IPS signatures.

SonicWall Conversion

SonicWall differences

Special characters

FortiGate reserves '#' (hash sign), '(', and ')' (open and close curved brackets) as special characters. You can't use them in the configuration unless an escape sequence precedes them. FortiConverter replaces these characters with the characters: '*' (star), '[' and ']' (open and close square brackets).

Examples:

- The address book "SNWL #1" becomes "SNWL *1".
- The service book "Citrix TCP (Session Reliability)" becomes "Citrix TCP [Session Reliability]".

Address book configuration

- FortiConverter generates two extra address book entries: "Any" and "_Address_Null".
- "Any" is added because it is a default address book in SonicWall.
- FortiConverter generates "_Address_Null" because FortiGate address groups don't allow a group without any members. Only empty address groups can refer to "_Address_Null".

Service book configuration

FortiConverter doesn't migrate SonicWall service objects that are predefined on FortiGate. For example, HTTP port 80 and HTTPS port 443.

Schedule configuration

- A SonicWall schedule group can contain only one "one-time" schedule and multiple "recur" schedules. The "one-time" schedule is an implicit object that you can embed in the schedule group. Because FortiGate defines each schedule group explicitly, FortiConverter automatically generates "one-time" schedules for the SonicWall implicit schedules.
- FortiGate time schedule configuration doesn't support "24:00" (equal to the next day's 00:00). It uses "00:00" instead. When FortiConverter converts a SonicWall "recur" time schedule such as "M 00:00 to 24:00", it sets the end time to "00:00".

Local User and User Group

- Because FortiConverter can't parse the local user's password string, it sets all passwords to "123456".
- Unlike FortiConverter, SonicWall allows you to nest user groups.

For example, in SonicWall, usergroup1 can be a member of usergroup1. FortiConverter removes any nested configurations.

Route configuration

- FortiConverter doesn't convert automatically generated routes like connected route and host route.

Saving the SonicWall source configuration file

Before starting the conversion wizard:**SonicWall**, save a copy of your configuration file to the computer where FortiConverter is installed.

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

SonicWall Conversion Wizard

The administrator password is **not** set on the new configuration.

For third-party conversions, the trusted host settings are converted. Check the trusted host settings to ensure they allow management access from the relevant network interfaces.

To start a new conversion

1. Start FortiConverter.
2. When start-up is complete, a browser window automatically opens to http://127.0.0.1:8000.
3. Click New Conversion **New Conversion**, located at the top right corner.
4. Enter a name for the conversion configuration.
5. For Vendor, choose **SonicWall** block.
6. Choose a Model, if applicable.
7. Click **OK**.

The configuration page opens to the Start page, and you can input your settings.

SonicWall Start options

This table lists the start settings.

Setting	Description
Profile	
Description	Enter a description of the configuration.
Output Options	
Output Format	Select the appropriate output for your target Fortinet device.
FOS Version	The configuration syntax is slightly different among FortiOS 6.4, 7.0, 7.2, 7.4 and 7.6. Select the version that corresponds to the FortiOS version on the target.
Input	
Source Configuration	Select the input file.

Bulk Conversion	If there are many devices to be converted where all of them are the same model, sharing the same interface mapping relationship in conversion, then bulk conversion can convert all of them at once. Collect all the configuration files to be converted, compress them into a ZIP file and use the ZIP file as the input.
Target device (Optional)	
Target device	Select the model of the target device, or select a device connected to FortiConverter.
Conversion Options	
Discard unreferenced firewall objects	Specifies whether addresses, schedules, and services that aren't referenced by a policy are saved and added to the output. This option can be useful if your target device has table size limitations. You can view the unreferenced objects that FortiConverter removed on the Tuning page.
Increase Address and Service Table Sizes for High-End Models	You can customize the maximum table sizes that FortiConverter uses when Adjust table sizes is selected. For more information, see Adjusting table sizes on page 232.
Policy index start from 1 instead of 10000	When selected, the serial number of firewall policies will start from 1 instead of 10000.
NGFW policy-based mode	When selected, the conversion will be in NGFW policy-based mode. "`firewall policy`" will become "`firewall security-policy`" instead, and "`set application 00000`" will be generated in policies, which requires manual processing. There will also be some other minor differences adapted for the NGFW policy-based CLI.
Split Address group From VPN Phase2 selector	If the remote side of VPN is not a FortiGate but a device of other vendor, setting an address group in the VPN phase2 quick selector does not work. When this option is enabled, a VPN phase2 object with an address group in the selector would be split into multiple objects with subnet or a range in selector.
Ignore auto-added VPN access rules	Ignore all the Auto-added VPN inbound and outbound rules in conversion.
Ignore auto-added NAT access rules	Ignore Auto NATs generated by SonicWall in conversion.
Keep original policy ID	Use the same policy ID as policies configured in SonicWALL.
Replace zone with member interfaces	When this option is disabled by default, FortiConverter replaces all interfaces configured in central NAT rules into the zones they belong to. When this option is enabled, FortiConverter discards all zone objects in SonicWALL and directly uses interfaces as the source and destination interface of firewall policies.

Convert CFS web filters	SonicWall exclusive option, when enabled, SonicWall CFS web filters and CFS polices will be converted into FGT url filters and app polices
Comment Options	
Include input configuration lines for each output policy	Specifics whether FortiConverter uses SW_RULE_ID as policy comment for each FortiGate policy or the original comment from rules in SonicWall configuration.
Policy comment - Preserve the original comment	Include the original comment in source file in the comment of the output policy.
NAT Merge Options	
Ignore firewall policies with all or any addresses	Specifies whether FortiConverter ignores firewall policies with an "all" or "any" address when it merges a NAT rule and a firewall policy to create a FortiGate NAT policy. FortiConverter creates new policies in the output configuration based on where NAT rules to firewall policies intersect. Because firewall policies that use "all" or "any" as the address create many intersections, Fortinet recommends that you ignore them.
Enable Central NAT merge	Specifies whether FortiConverter converts NATs to FortiGate central NATs instead of policy-based NATs
Nat Merge Depth	
Identical NAT **Source NAT** **Destination NAT** **Double NAT**	Specifies which types of NAT FortiConverter merges with the output firewall policies, or whether FortiConverter performs NAT merge based on object names or values. • Off -FortiConverter converts firewall policies only and doesn't perform NAT merge for this type of NAT. This is useful for performing a quick, initial conversion to discover any conversion issues. • Object Names–FortiConverter performs NAT merge based on matching address names in firewall policies and NAT rules. • Object Values–FortiConverter performs NAT merge based on matching address values in firewall policies and NAT rules. It generates the most accurate matching of NAT rules and policies, but in most cases, it also generates more NAT policies.

SonicWall Source Configuration

Source Preview

Setting	Description
VDOM Select	Select/Unselect the VDOM item.
VDOM Rename	Rename the VDOM name.
VDOM Mode	Change the VDOM mode in the output result.
Information of Configurations	Source configuration file names are shown in the

	table.
Managed Device Name	The name of the managed device which the converted interface or route configuration would be imported in FortiManager. (Only available when the output format is **FortiManager**)
Target Device Switch Interface - Interface/Port	If there are virtual switches in the selected target device, FortiConverter will list the member ports of the virtual switches. If an interface in the list is going to be used in the configuration, it should first be detached from the virtual switch. Click "**X**" on the interface to detach it. Please note that a detached interface cannot be re-added later by FortiConverter.
Source Configuration Preview	The number of each type of firewall object are shown in the preview table. Click the object number to see detailed information about each object. In each type of object, click the button **Export CSV** to export the current object info as CSV file.

SonicWall Interface mapping

You can manually map the interface.

- To **select** the appropriate FortiGate interface, click the value in the FortiGate Interface column, and then select a value or enter a custom interface name.
- To **edit** other values, double-click the proper column. Use the toolbar icon on the right to show and hide columns. You can also use the Tuning page to create mappings after the conversion is complete.
- To **import** a set of interface mappings from a file, click **Import**.
- To **download** the current set of interface mappings, click **Export**.
- To **delete** an interface, select the entries you would like to delete, **right click** and select **Delete Selected**. This is useful if your target FortiGate has fewer interfaces than the source configuration.

The limit of the length of interface names in FortiOS is 15 characters. Interfaces in the source config which have longer names should be trimmed to a shorter name. It is recommended to trim the names manually to ensure readability. But if a quick trimming is needed, please select the entries, **right click** and select **Trim Interface Name** to trim the names into 15 characters automatically.

Setting	Description
VDOM	Shows the virtual domains used in the conversion. ("root" by default)
Source Interface	Shows each interface on the SonicWall firewall.
FortiGate Interface	The input field for corresponding FortiGate interface names. Click to assign a FortiGate port or input the interface name manually for each interface. (Only available when the output format is **FortiGate**)

Setting	Description
Normalized interface	The input field for corresponding normalized interface names, which would be configured in the ADOM database in FortiManager. Click to assign a port or input the interface name manually for each interface. (Only available when the output format is **FortiManager**)
Device interface	The input field for corresponding interface names in the managed devices in FortiManager. Click to assign a port or input the interface name manually for each interface. (Only available when the output format is **FortiManager**)
Members	Shows any members, if they are set.
IP-Netmask	Shows the IP address and netmask of the connection.
Type	Shows the type of interface.
Access	Shows which protocols has permission to access each interface.
Import	Click to load a set of interface mappings from a text file.
Export	Saves the current set of interface mappings to a text file.
Delete Selected	Click to delete the selected mapping item.
Trim Interface Name	Trim the interface names which exceed 15 characters into 15 characters automatically.

SonicWall Route Information

FortiConverter creates static routes in the output using the static routes it detects in the source configuration and any routing information you provide.

Double-click an item to edit it.

Setting	Description
New Route	Click to add a route.
Delete	Click to delete the selected route.

SonicWall Conversion result

Tab	Description
Conversion Summary	Provides statistics about the conversion.
Reports	Generate PDF reports including converted and unconverted objects list.
VDOM Mapping	Shows how VDMS were mapped from the source device to the new device.

Interface Mapping	Shows how interfaces were mapped for each VDOM from the source device.
Device Summary	Provides statistics about the detected objects.

FortiConverter includes error and warning messages into the conversion when an error occurs.

Review the `config-all.txt` file after each conversion for errors. These errors and warning messages might cause the import process to fail, if not corrected. See for more details.

Sophos Conversion

Sophos Networks differences

Conversion support

FortiConverter supports the following features:

- Interface
- Zone
- Address
- Address group
- Service
- Service group
- User
- User group
- Policy
- Route

VPN and route conversions are not currently supported. NAT rules are not converted, but MASQ in policies can be converted into SNAT of interface in policies.

Saving the Sophos source configuration files

Before starting the conversion wizard, save a copy of your Sophos configuration file to the computer where FortiConverter is installed.

Here are the tutorial of the 3 models that you can save Sophos configuration files to:

Saving the source configuration files on SFOS on page 203

Saving the source configuration files on Cyberoam OS on page 203

Saving the source configuration files on SG on page 204

Saving 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 after v17.5 MR4, Sophos backups are encrypted. Please reach out to the Sophos support team to get a decrypted configuration file.

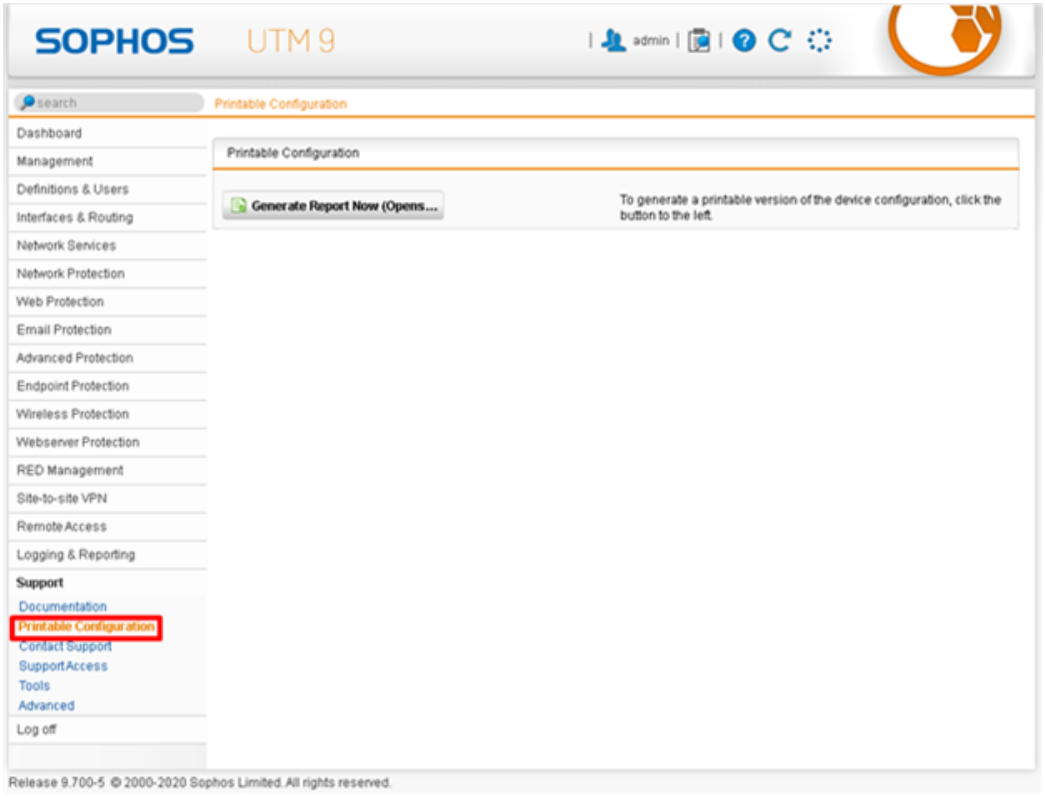
Saving the source configuration files on Cyberoam OS

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.

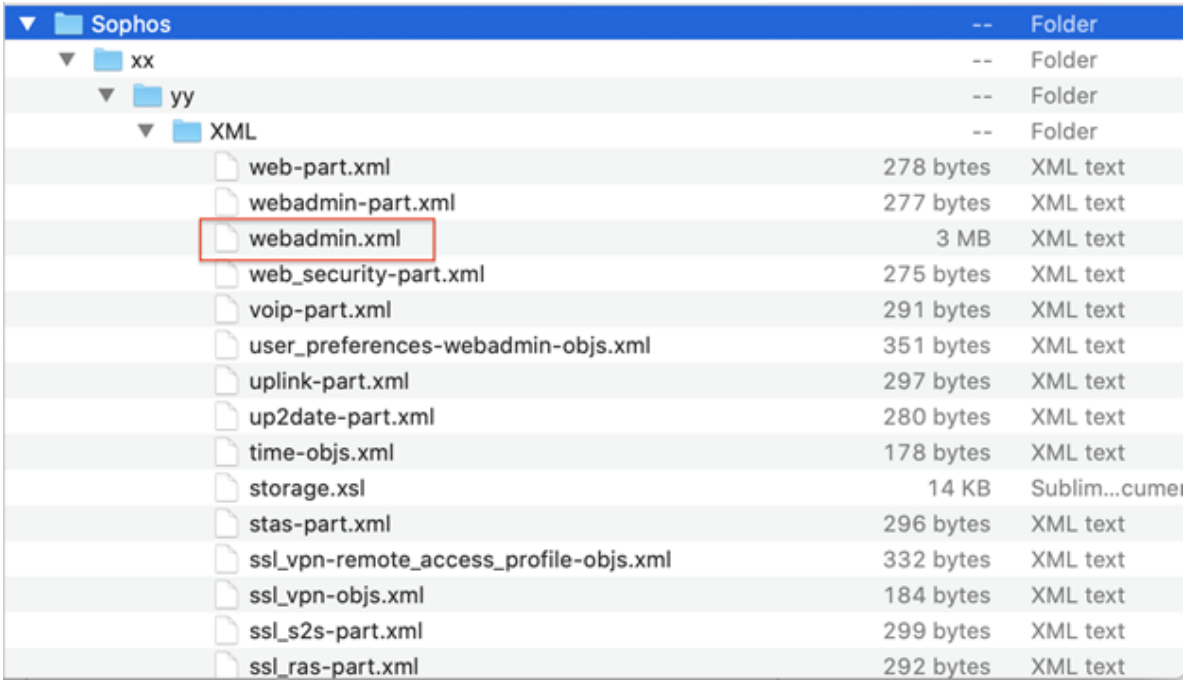
Saving the source configuration files on SG

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)



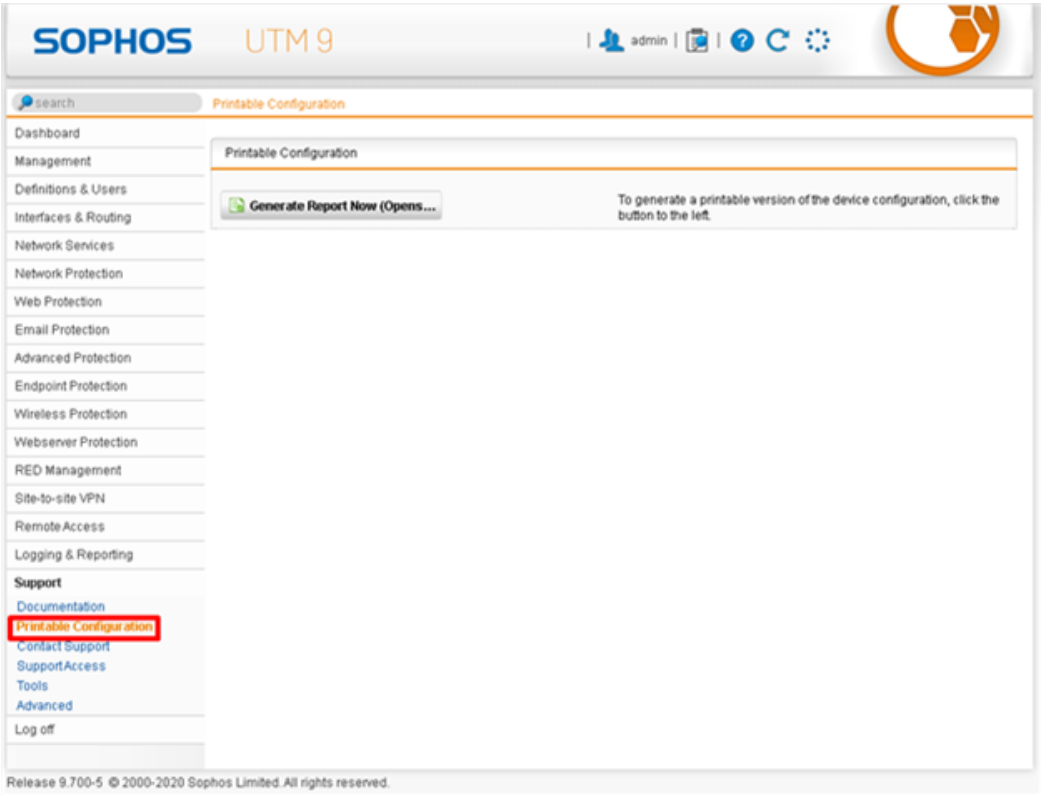
10. Use the file "webadmin.xml" as the input for the FortiConverter tool.

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 sub folder var (`/var/chroot-httpd/var/webadmin/var`). There you will find a directory with a cryptic name e.g.[:$]LIHKeSjIOjzQrjuMESn, 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.

Sophos conversion wizard

To start a new conversion

1. Start FortiConverter.
2. When start-up is complete, a browser window automatically opens to http://127.0.0.1:8000.
3. Click 

New Conversion, located at the top right corner.
4. Enter a name for the conversion configuration.
5. For Vendor, choose **Sophos** block.
6. For Model, choose **XG** or **SG**.
7. Click **OK**.

The configuration page opens to the Start page, and you can input your settings.

Sophos start options

This table lists the start settings.

Setting	Description
Profile	
Description	Enter a description of the configuration.
Output Options	
Output Format	Select the appropriate output for your target Fortinet device.
FOS Version	The configuration syntax is slightly different among FortiOS 6.4, 7.0, 7.2, 7.4 and 7.6. Select the version that corresponds to the FortiOS version on the target.
Input	
Source Configuration	Select the input file.
Bulk Conversion	If there are many devices to be converted where all of them are the same model, sharing the same interface mapping relationship in conversion, then bulk conversion can convert all of them at once. Collect all the configuration files to be converted, compress them into a ZIP file and use the ZIP file as the input.
Target device (Optional)	
Target device	Select the model of the target device, or select a device connected to FortiConverter.

Conversion Options	
Discard unreferenced firewall objects	Specifies whether addresses and services that aren't referenced by a policy are saved and added to the output. This option can be useful if your target device has table size limitations. You can view the unreferenced objects that FortiConverter removed on the Tuning page.
Increase Address and Service Table Sizes for High-End Models	You can customize the maximum table sizes that FortiConverter uses when Adjust table sizes is selected. For more information, see Adjusting table sizes on page 232.
Policy index start from 1 instead of 10000	When selected, the serial number of firewall policies will start from 1 instead of 10000.
NGFW policy-based mode	When selected, the conversion will be in NGFW policy-based mode. "`firewall policy`" will become "`firewall security-policy`" instead, and "`set application 00000`" will be generated in policies, which requires manual processing. There will also be some other minor differences adapted for the NGFW policy-based CLI.
Automatically generate policy interfaces	Specifies whether FortiConverter automatically generates policy interfaces.
Comment Options	
Service Group Comment	Specifies whether FortiConverter copies the service group comment from the source configuration to the FortiGate service group.
Nat Merge Options	
Enable central NAT merge	Specifies whether FortiConverter converts NATs to FortiGate central NATs instead of policy-based NATs. Currently only central NAT mode is supported, and NAT is available only for the SG model.

Source preview

This table shows the information inside the configuration.

Setting	Description
VDOM Select	Select/Unselect the VDOM item.
VDOM Rename	Rename the VDOM name.

VDOM Mode	Change the VDOM mode in the output result.
Information of Configurations	Source configuration file names are shown in the table as a link. Click the link to see the content. The file won't show if it's too large.
Managed Device Name	The name of the managed device which the converted interface or route configuration would be imported in FortiManager. (Only available when the output format is **FortiManager**)
Target Device Switch Interface - Interface/Port	If there are virtual switches in the selected target device, FortiConverter will list the member ports of the virtual switches. If an interface in the list is going to be used in the configuration, it should first be detached from the virtual switch. Click "**X**" on the interface to detach it. Please note that a detached interface cannot be re-added later by FortiConverter.
Source Configuration Preview	The number of each type of firewall object are shown in the preview table. Click the object number to see detailed information about each object. In each type of object, click the button **Export CSV** to export the current object info as CSV file.

Sophos Interface mapping

You can manually map the interface.

- To **select** the appropriate FortiGate interface, click the value in the FortiGate Interface column, and then select a value or enter a custom interface name.
- To **edit** other values, double-click the proper column. Use the toolbar icon on the right to show and hide columns. You can also use the Tuning page to create mappings after the conversion is complete.
- To **import** a set of interface mappings from a file, click **Import**.
- To **download** the current set of interface mappings, click **Export**.
- To **delete** an interface, select the entries you would like to delete, **right click** and select **Delete Selected**. This is useful if your target FortiGate has fewer interfaces than the source configuration.

The limit of the length of interface names in FortiOS is 15 characters. Interfaces in the source config which have longer names should be trimmed to a shorter name. It is recommended to trim the names manually to ensure readability. But if a quick trimming is needed, please select the entries, **right click** and select **Trim Interface Name** to trim the names into 15 characters automatically.

Setting	Description
VDOM	Shows the virtual domains used in the conversion. ("root" by default)
Source Interface	Shows each interface on the Sophos firewall.

Setting	Description
FortiGate Interface	The input field for corresponding FortiGate interface names. Click to assign a FortiGate port or input the interface name manually for each interface. (Only available when the output format is **FortiGate**)
Normalized interface	The input field for corresponding normalized interface names, which would be configured in the ADOM database in FortiManager. Click to assign a port or input the interface name manually for each interface. (Only available when the output format is **FortiManager**)
Device interface	The input field for corresponding interface names in the managed devices in FortiManager. Click to assign a port or input the interface name manually for each interface. (Only available when the output format is **FortiManager**)
Members	Shows any members, if they are set.
IP-Netmask	Shows the IP address and netmask of the connection.
Type	Shows the type of interface.
Access	Shows which protocols has permission to access each interface.
Import	Click to load a set of interface mappings from a text file.
Export	Saves the current set of interface mappings to a text file.
Delete Selected	Click to delete the selected mapping item.
Trim Interface Name	Trim the interface names which exceed 15 characters into 15 characters automatically.

Sophos Route Information

FortiConverter creates static routes in the output using the static routes it detects in the source configuration and any routing information you provide.

Double-click an item to edit it.

Setting	Description
New Route	Click to add a route.
Delete	Click to delete the selected route.

Sophos conversion result

Tab	Description
Conversion Summary	Provides statistics about the conversion.

Reports	Generate PDF reports including converted and unconverted objects list.
Interface Mapping	Shows how interfaces are mapped for each VDOM from the source device.
Device Summary	Provides statistics about the detected objects.

FortiConverter includes error and warning messages into the conversion when an error occurs.

Review the `config-all.txt` file after each conversion for errors. These errors and warning messages might cause the import process to fail, if not corrected. See for more details.

Tipping Point Conversion

Tipping Point IPS differences

Interface and schedule conversion

Source interfaces and destination interfaces are set to "any" after conversion.

Schedules are set to "always" in all policies after conversion.

Action Set

If "Block" or "Drop" appears in an action set, the FortiGate policy `strAction` is set to "deny". Otherwise, the policy is set to "accept".

If "rsyslog" is found in an action set, the FortiGate policy `strLogTraffic` is set to "enable". Otherwise, it is disabled.

Ignored fields

The following fields are parsed but ignored:

- Zone
- Users
- Apps
- Security
- Reputation
- Install On

Save the Tipping Point Source Configuration Files

Before starting the conversion wizard, save a copy of your Tipping Point configuration file to the computer where FortiConverter is installed.

Here are the tutorial of the 2 models that you can save Tipping Point configuration files to:

Saving the source configuration files on IPS on page 212

Saving the source configuration files on Firewall on page 213

Saving the source configuration files on IPS

Make sure the file contents are arranged by the order of "**Addresses and Address groups**", "**Services and Service groups**" and "**Policies**".

You can use text editor such as Notepad or Notepad++, and only use plain text file as input file for FortiConverter Tool.

If you encounter problems with your TippingPoint configuration file, send it to FortiConverter support at fconvert_feedback@fortinet.com. The FortiConverter team will help improve your conversion for you.

Part 1: download Addresses and Address groups

1. Click the **Admin** tab, located at the top.
2. Click **Named resources**.
3. Click the address or address group.
4. Press Ctrl + A to select all.
5. Copy and paste the selected address or address group to a plain text editor like Notepad, Notepad++, etc.
6. Repeat for all other addresses or address groups.

Part 2: download Service and Service groups

1. Click the **Profile** tab, located at the top.
2. Click **Expand profiles**.
3. Click on **Shared settings**.
4. Click on the service or service group.
5. Press Ctrl + A to select all.
6. Copy and paste the selected service or service group to the same text file from Part 1.
7. Repeat for all other services and service groups.

Part 3: download Policies

1. Click the **Profile** tab, located at the top.
2. Click **Firewall profiles**.
3. Select a policy from the list.
4. Click on an item.
5. Press Ctrl + A to select all.
6. Copy and paste the policy to the same text file from Part 1 and 2.
7. Repeat for all other policies.

Saving the source configuration files on Firewall

If you encounter problems with your TippingPoint configuration file, send it to FortiConverter support at fconvert_feedback@fortinet.com. The FortiConverter team will help improve your conversion for you.

1. Login to Tipping Point Firewall via SSH
2. Run the command: `display config-running`
3. Save the config into `.txt` format on the computer where FortiConverter installed.

Tipping Point IPS Conversion Wizard

To start a new conversion

1. Start FortiConverter.
2. When start-up is complete, a browser window automatically opens to http://127.0.0.1:8000.
3. Click New Conversion **New Conversion**, located at the top right corner.
4. Enter a name for the conversion configuration.
5. For Vendor, choose **Tipping Point** block.
6. Choose a Model, if applicable.

7. Click **OK**.

The configuration page opens to the Start page, and you can input your settings.

Tipping Point IPS Start options

This table lists the start settings.

Setting	Description
Profile	
Description	Enter a description of the configuration.
Output Options	
Output Format	Select the appropriate output for your target Fortinet device.
FOS Version	The configuration syntax is slightly different among FortiOS 6.4, 7.0, 7.2, 7.4 and 7.6. Select the version that corresponds to the FortiOS version on the target.
Input	
Source Configuration	Select the input file
Bulk Conversion	If there are many devices to be converted where all of them are the same model, sharing the same interface mapping relationship in conversion, then bulk conversion can convert all of them at once. Collect all the configuration files to be converted, compress them into a ZIP file and use the ZIP file as the input.
Target device (Optional)	
Target device	Select the model of the target device, or select a device connected to FortiConverter.
Conversion Options	
Discard unreferenced firewall objects	Specifies whether addresses, schedules, and services that are not referenced by a policy are saved and added to the output. This option can be useful if your target device has table size limitations. You can view the unreferenced objects that FortiConverter removed in the Tuning page.
Increase Address and Service Table Sizes for High-End Models	You can customize the maximum table sizes that FortiConverter uses when Adjust table sizes is selected. For more information, see Adjusting table sizes on page 232
Policy index start from 1 instead of 10000	When selected, the serial number of firewall policies will start from 1 instead of 10000.
Comment Options	

Setting	Description
Include input configuration lines for each output policy	Specifies whether FortiConverter includes the input configuration lines used for each FortiGate policy in the FortiGate configuration as a policy comment.

Tipping Point IPS Source preview

This table shows the information inside the configuration.

Setting	Description
VDOM Select	Select/Unselect the VDOM item.
VDOM Rename	Rename the VDOM name.
VDOM Mode	Change the VDOM mode in the output result.
Information of Configurations	Source configuration file names are shown in the table as a link. Click the link to see the content. The file won't show if it's too large.
Source Configuration Preview	The number of each type of firewall object are shown in the preview table. Click the object number to see detailed information about each object. In each type of object, click the button **Export CSV** to export the current object info as CSV file.

Tipping Point IPS Conversion result

Tab	Description
Conversion Summary	Provides statistics about the conversion.
Reports	Generate PDF reports including converted and unconverted objects list.
Device Summary	Provides statistics about the detected objects.

FortiConverter includes error and warning messages into the conversion when an error occurs.

Review the `config-all.txt` file after each conversion for errors. These errors and warning messages might cause the import process to fail, if not corrected. See for more details.

Tipping Point Firewall Conversion Wizard

To start a new conversion

1. Start FortiConverter.
2. When start-up is complete, a browser window automatically opens to http://127.0.0.1:8000.
3. Click 

New Conversion, located at the top right corner.
4. Enter a name for the conversion configuration.
5. For Vendor, choose **Tipping Point** block.
6. Choose a Model, if applicable.
7. Click **OK**.

The configuration page opens to the Start page, and you can input your settings.

Tipping Point Firewall Start Options

Setting	Description
Profile	
Description	Enter a description of the configuration..
Output Options	
Output Format	The output format of the converted configuration
FOS Version	The configuration syntax is slightly different among FortiOS 6.4, 7.0, 7.2, 7.4 and 7.6. Select the version that corresponds to the FortiOS version on the target
Input	
Source Configuration	Select the input file

Tipping Point Firewall Source Preview

This table shows the information inside the configuration.

Setting	Descriptions
File Name	Source configuration file names are shown in the table as a link. Click the link to see the content. The file won't show if it's too large.
Model	The model of the configuration.
Source Configuration Preview	The number of each type of object is shown in the preview table. Click the object number to see detailed information about each object. In each type of object, click the Export CSV button to export the current object info as a CSV file.

Tipping Point Firewall Conversion Result

Setting	Description
Conversion Summary	Provides information about the conversion.
Device Summary	Provides statistics about the detected objects.

Vyatta Networks Conversion

Vyatta Networks (VyOS) differences

Conversion support

FortiConverter supports the following features:

- Interface
- Zone
- Address group
- Service group
- Policy
- Route

NAT and VPN conversions are not currently supported.

Configuration notes

Vyatta does not provide outgoing interface in static route configuration. FortiConverter uses the next-hop address and the network of each interface to determine the outgoing interface. However, since VPN conversions are not supported, and tunnel interfaces are not converted, routes to tunnel interfaces cannot be calculated. The interface fields of those kind of routes are empty in the output field and require you to fill them manually before the config is imported.

Saving the Vyatta source configuration files

Before starting the conversion wizard, save a copy of your Vyatta configuration file to the computer where FortiConverter is installed.

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
   }
   ............
   ............
```

Vyatta conversion wizard

To start a new conversion

1. Start FortiConverter.
2. When start-up is complete, a browser window automatically opens to http://127.0.0.1:8000.
3. Click New Conversion **New Conversion**, located at the top right corner.
4. Enter a name for the conversion configuration.
5. For Vendor, choose **Vyatta** block.
6. Choose a Model, if applicable.
7. Click **OK**.

The configuration page opens to the Start page, and you can input your settings.

Vyatta Start options

This table lists the start settings.

Setting	Description
Profile	
Description	Enter a description of the configuration.
Output Options	
Output Format	Select the appropriate output for your target Fortinet device.
FOS Version	The configuration syntax is slightly different among FortiOS 6.4, 7.0, 7.2, 7.4 and 7.6. Select the version that corresponds to the FortiOS version on the target.
Input	
Source Configuration	Select the input file.
Bulk Conversion	If there are many devices to be converted where all of them are the same model, sharing the same interface mapping relationship in conversion, then bulk conversion can convert all of them at once. Collect all the configuration files to be converted, compress them into a ZIP file and use the ZIP file as the input.
Target device (Optional)	
Target device	Select the model of the target device, or select a device connected to FortiConverter.
Conversion Options	
Discard unreferenced firewall objects	Specifies whether addresses and services that aren't referenced by a policy are saved and added to the output. This option can be useful if your target device has table size limitations. You can view the unreferenced objects that FortiConverter removed on the Tuning page.
Increase Address and Service Table Sizes for High-End Models	You can customize the maximum table sizes that FortiConverter uses when Adjust table sizes is selected. For more information, see Adjusting table sizes on page 232.
Policy index start from 1 instead of 10000	When selected, the serial number of firewall policies will start from 1 instead of 10000.
NGFW policy-based mode	When selected, the conversion will be in NGFW policy-based mode. "firewall policy" will become "firewall security-policy" instead, and "set application 00000" will be generated in policies, which requires manual processing. There will also be some other minor differences adapted for the NGFW policy-based CLI.

Source preview

This table shows the information inside the configuration.

Setting	Description
VDOM Select	Select/Unselect the VDOM item.
VDOM Rename	Rename the VDOM name.
VDOM Mode	Change the VDOM mode in the output result.
Information of Configurations	Source configuration file names are shown in the table as links. Click the link to see file contents. Files that are too large are not shown.
Target Device Switch Interface - Interface/Port	If there are virtual switches in the selected target device, FortiConverter will list the member ports of the virtual switches. If an interface in the list is going to be used in the configuration, it should first be detached from the virtual switch. Click "**X**" on the interface to detach it. Please note that a detached interface cannot be re-added later by FortiConverter.
Source Configuration Preview	The number of each type of firewall object are shown in the preview table. Click the object number to see detailed information about each object. In each type of object, click the button **Export CSV** to export the current object info as CSV file.

Vyatta interface mapping

You can manually map the interface.

- To **select** the appropriate FortiGate interface, click the value in the FortiGate Interface column, and then select a value or enter a custom interface name.
- To **edit** other values, double-click the proper column. Use the toolbar icon on the right to show and hide columns. You can also use the Tuning page to create mappings after the conversion is complete.
- To **import** a set of interface mappings from a file, click **Import**.
- To **download** the current set of interface mappings, click **Export**.
- To **delete** an interface, select the entries you would like to delete, **right click** and select **Delete Selected**. This is useful if your target FortiGate has fewer interfaces than the source configuration.

The limit of the length of interface names in FortiOS is 15 characters. Interfaces in the source config which have longer names should be trimmed to a shorter name. It is recommended to trim the names manually to ensure readability. But if a quick trimming is needed, please select the entries, **right click** and select **Trim Interface Name** to trim the names into 15 characters automatically.

Setting	Description
VDOM	Shows the virtual domains used in the conversion. ("root" by default)
Source Interface	Shows each interface on the Vyatta firewall.
FortiGate Interface	The input field for corresponding FortiGate interface names. Click to assign a FortiGate port or input the interface name manually for each interface. (Only available when the output format is **FortiGate**)
Normalized interface	The input field for corresponding normalized interface names, which would be configured in the ADOM database in FortiManager. Click to assign a port or input the interface name manually for each interface. (Only available when the output format is **FortiManager**)
Device interface	The input field for corresponding interface names in the managed devices in FortiManager. Click to assign a port or input the interface name manually for each interface. (Only available when the output format is **FortiManager**)
Members	Shows any members, if they are set.
IP-Netmask	Shows the IP address and netmask of the connection.
Type	Shows the type of interface.
Access	Shows which protocols has permission to access each interface.
Import	Click to load a set of interface mappings from a text file.
Export	Saves the current set of interface mappings to a text file.
Delete Selected	Click to delete the selected mapping item.
Trim Interface Name	Trim the interface names which exceed 15 characters into 15 characters automatically.

Vyatta route information

FortiConverter creates static routes in the output by using the static routes it detects in the source configuration, and any routing information you provide.

Double-click item to edit it.

Setting	Description
New Route	Click to add a route.
Delete	Click to delete the selected route.

Vyatta conversion result

Tab	Description
Conversion Summary	Provides statistics about the conversion.
Reports	Generate PDF reports including converted and unconverted objects list.
Interface Mapping	Shows how interfaces were mapped for each VDOM from the source device.
Device Summary	Provides statistics about the detected objects.

WatchGaurd Conversion

Conversion support

FortiConverter supports the following features:

- Interface
- Address (group)
- Service (group)
- Policy
- Route

Saving the WatchGuard source configuration files

Before starting the conversion wizard, save a copy of your WatchGuard configuration file (in XML format) to the computer where FortiConverter is installed.

You can use Policy Manager to download your configuration file.

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

WatchGuard conversion wizard

To start a new conversion

1. Start FortiConverter.
2. When start-up is complete, a browser window automatically opens to http://127.0.0.1:8000.
3. Click New Conversion **New Conversion**, located at the top right corner.
4. Enter a name for the conversion configuration.
5. For Vendor, choose **WatchGuard** block.
6. Choose a Model, if applicable.
7. Click **OK**.

The configuration page opens to the Start page, and you can input your settings.

WatchGuard Start options

This table lists the start settings.

Setting	Description
Profile	
Description	Enter a description of the configuration.
Output Options	
Output Format	Select the appropriate output for your target Fortinet device.
FOS Version	The configuration syntax is slightly different among FortiOS 6.4, 7.0, 7.2, 7.4 and 7.6. Select the version that corresponds to the FortiOS version on the target.
Input	
Source Configuration	Select the input file.
Bulk Conversion	If there are many devices to be converted where all of them are the same model, sharing the same interface mapping relationship in conversion, then bulk conversion can convert all of them at once. Collect all the configuration files to be converted, compress them into a ZIP file and use the ZIP file as the input.
Target device (Optional)	
Target device	Select the model of the target device, or select a device connected to FortiConverter.
Conversion Options	

Discard unreferenced firewall objects	Specifies whether addresses and services that aren't referenced by a policy are saved and added to the output. This option can be useful if your target device has table size limitations. You can view the unreferenced objects that FortiConverter removed on the Tuning page.
Increase Address and Service Table Sizes for High-End Models	You can customize the maximum table sizes that FortiConverter uses when Adjust table sizes is selected. For more information, see Adjusting table sizes on page 232.
Policy index start from 1 instead of 10000	When selected, the serial number of firewall policies will start from 1 instead of 10000.
NGFW policy-based mode	When selected, the conversion will be in NGFW policy-based mode. "`firewall policy`" will become "`firewall security-policy`" instead, and "`set application 00000`" will be generated in policies, which requires manual processing. There will also be some other minor differences adapted for the NGFW policy-based CLI.

Source Preview

This page shows the information inside the configuration.

Setting	Description
VDOM Select	Select/Unselect the VDOM item.
VDOM Rename	Rename the VDOM name.
VDOM Mode	Change the VDOM mode in the output result.
Information of Configurations	Source configuration file names are shown in the table as a link. Click the link to see the content. The file won't show if it's too large.
Target Device Switch Interface - Interface/Port	If there are virtual switches in the selected target device, FortiConverter will list the member ports of the virtual switches. If an interface in the list is going to be used in the configuration, it should first be detached from the virtual switch. Click "**X**" on the interface to detach it. Please note that a detached interface cannot be re-added later by FortiConverter.

Source Configuration Preview	The numbers of each type of firewall object are shown in the preview table. Click the object number to see detailed information on each object. In each type of object, click the button **Export CSV** to export the current object info as CSV file.

WatchGuard Interface mapping

You can manually map the interface.

- To **select** the appropriate FortiGate interface, click the value in the FortiGate Interface column, and then select a value or enter a custom interface name.
- To **edit** other values, double-click the proper column. Use the toolbar icon on the right to show and hide columns. You can also use the Tuning page to create mappings after the conversion is complete.
- To **import** a set of interface mappings from a file, click **Import**.
- To **download** the current set of interface mappings, click **Export**.
- To **delete** an interface, select the entries you would like to delete, **right click** and select **Delete Selected**. This is useful if your target FortiGate has fewer interfaces than the source configuration.

The limit of the length of interface names in FortiOS is 15 characters. Interfaces in the source config which have longer names should be trimmed to a shorter name. It is recommended to trim the names manually to ensure readability. But if a quick trimming is needed, please select the entries, **right click** and select **Trim Interface Name** to trim the names into 15 characters automatically.

Setting	Description
VDOM	Shows the virtual domains used in the conversion. ("root" by default)
Source Interface	Shows each interface on the WatchGuard firewall.
FortiGate Interface	The input field for corresponding FortiGate interface names. Click to assign a FortiGate port or input the interface name manually for each interface. (Only available when the output format is **FortiGate**)
Normalized interface	The input field for corresponding normalized interface names, which would be configured in the ADOM database in FortiManager. Click to assign a port or input the interface name manually for each interface. (Only available when the output format is **FortiManager**)
Device interface	The input field for corresponding interface names in the managed devices in FortiManager. Click to assign a port or input the interface name manually for each interface. (Only available when the output format is **FortiManager**)
Members	Shows any members, if they are set.
IP-Netmask	Shows the IP address and netmask of the connection.
Type	Shows the type of interface.

Setting	Description
Access	Shows which protocols has permission to access each interface.
Import	Click to load a set of interface mappings from a text file.
Export	Saves the current set of interface mappings to a text file.
Delete Selected	Click to delete the selected mapping item.
Trim Interface Name	Trim the interface names which exceed 15 characters into 15 characters automatically.

WatchGuard Route Information

FortiConverter creates static routes in the output using the static routes it detects in the source configuration and any routing information you provide.

Double-click an item to edit it.

Setting	Description
New Route	Click to add a route.
Delete	Click to delete the selected route.

WatchGuard Conversion result

Tag	Description
Conversion Summary	Provides statistics about the conversion.
Reports	Generate PDF reports including converted and unconverted objects list.
Interface Mapping	Shows how interfaces were mapped for each VDOM from the source device.
Device Summary	Provides statistics about the detected objects.

FortiConverter includes error and warning messages into the conversion when an error occurs.
Review the `config-all.txt` file after each conversion for errors. These errors and warning messages might cause the import process to fail, if not corrected. See for more details.

Zscaler Conversions (Beta feature)

Conversion Support

FortiConverter supports the following features:

- IP Source Groups
- IP Destination Groups
- Network Services
- Users
- Groups (user group)
- Firewall Filtering Rules

Saving the Zscaler Source Configuration File

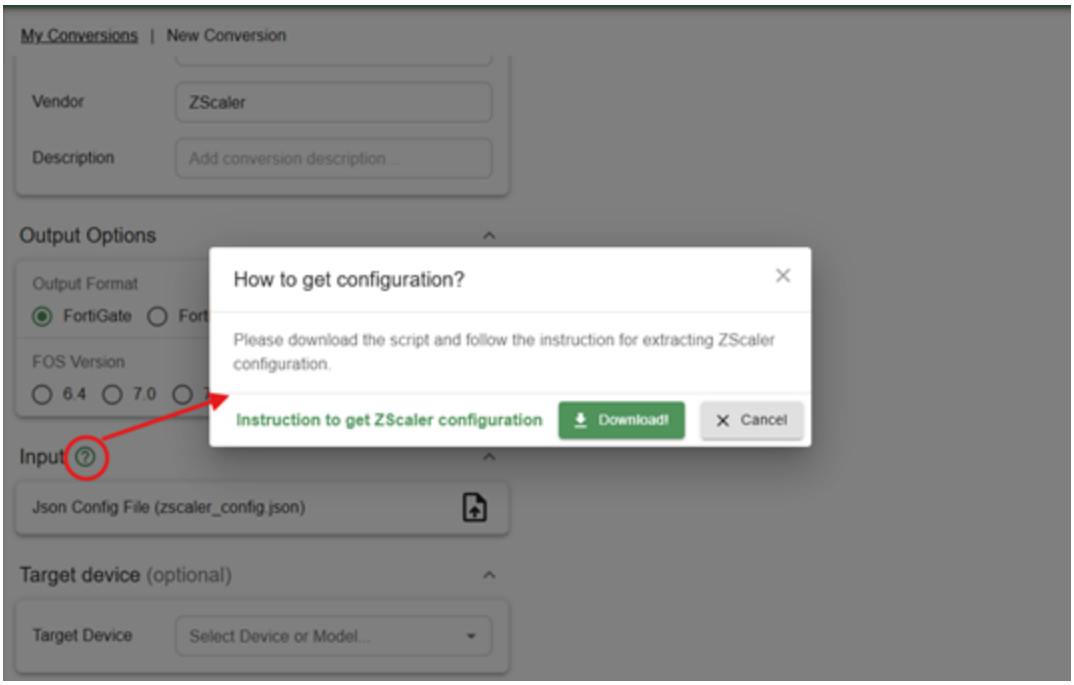
Overview

This document provides a step-by-step guide for dumping the Zscaler configuration file in JSON format. Fortinet provides a Python script, `fcon_Zscaler_backup.py` that downloads the configuration from Zscaler resource server.

Prerequisites

Python 3.11.6 with requests 2.32.3 needs to be installed on the machine for the script to run.

For `fcon_Zscaler_backup.py` , please download the script from the FortiConverter application. Click the question mark, a pop-up window will lead you to this instruction guide. At the same time, click **download** to get the script file.



Zscaler Conversion Wizard

To start a new conversion

1. Start FortiConverter.
2. When start-up is complete, a browser window automatically opens to http://127.0.0.1:8000.
3. Click New Conversion **New Conversion**, located at the top right corner.
4. Enter a name for the conversion configuration.
5. For Vendor, choose **Zscaler** block.
6. Choose a Model, if applicable.
7. Click **OK**.

The configuration page opens to the Start page, and you can input your settings.

Zscaler Start Options

This table lists the start settings.

Setting	Description
Profile	
Description	Enter a description of the configuration.
Output Options	
Output Format	Select the appropriate output for your target Fortinet device. For FortiSASE JSON output, please choose FortiSASE and API version v2
FOS Version	The configuration syntax is slightly different for FortiOS 6.4, 7.0, 7.2, 7.4 and 7.6. Select the version that corresponds to the FortiOS version on the target.
API Version	The section is only applicable to FortiSASE output and only version 2 is available.
Input	
Json Config File	Select the input file of Zscaler JSON configuration file (Zscaler_config.json which can be obtained from provided script fcon_Zscaler_backup.py)
Target Device (Optional)	
Target Device	Select the model of the target device.

Zscaler Source Preview

This table shows the information inside the configuration.

Setting	Description
File Name	Source configuration file names are shown in the table as a link. Click the link to see the content. The file won't show if it's too large.
Model	The model of the configuration.
Source Configuration Preview	The number of each type of object is shown in the preview table. Click the object number to see detailed information about each object. In each type of object, click the **Export CSV** button to export the current object info as a CSV file.

Zscaler Conversion Result

Setting	Description
Conversion Summary	Provides information about the conversion.
Device Summary	Provides statistics about the detected objects.

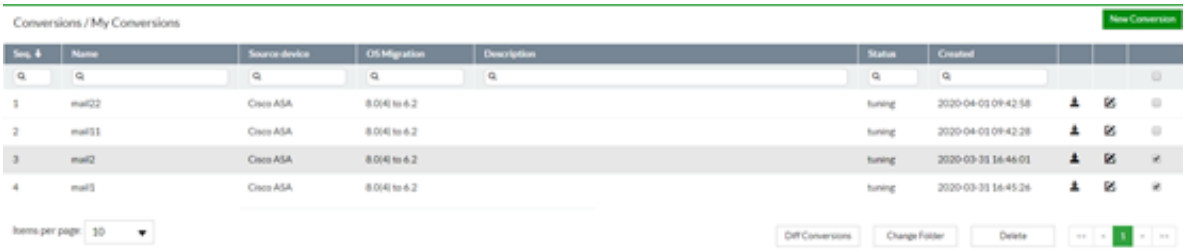
Conversion General

Compare Two Conversions

This feature can be used to compare two similar conversions from the same vendor/model and show the differences between them.

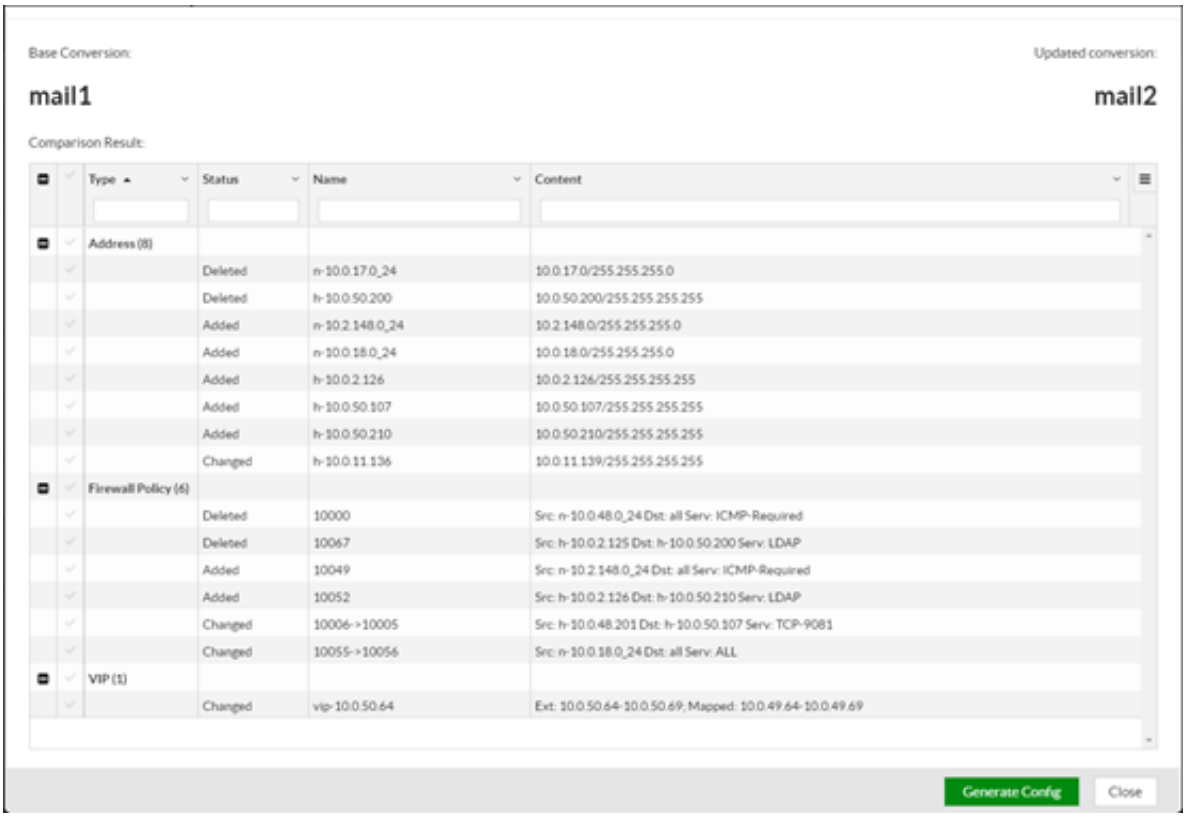
To use the feature:

1. Select exactly two conversions to be compared and press the **Diff Conversions** button.



2. By default, the converter assumes the older conversion is the base conversion and the newer one is the updated conversion. This means that objects that only exists in the updated conversion will be displayed as **Added** and the objects that only exists in the older conversion will be displayed as **Deleted**. Clicking on the  button allows the base/updated conversion to be swapped.

3. Press **Confirm** to start the calculation of differences between the two conversions.



4. The diff result would then be generated. A firewall object being marked as **Changed** means the object have the same name in both conversions, but its actual content differs. However, for Policy, Central NAT and static routes, **Changed** means they have the same relative order to other unchanged (Policy/Central NAT/static routes), with their actual content differs.
5. You may select the object(s) you want to generate CLI with the Checkbox on the left. After that, press **Generate Config** Button to download the desired CLI as `.zip` file. If no specific object is selected, all objects' CLI will be generated.

Adjusting table sizes

The conversion wizard Start options page allows you to specify whether FortiConverter allows larger table sizes and group membership than default in the output configuration.

This is useful when, for example, the source configuration has a large address group and the target configuration can accommodate the larger group. Otherwise, FortiConverter converts the large address group into two or more smaller address groups for a single policy.

For example, FortiConverter uses the following default maximum table sizes by default:

- **Address groups** – 2500
- **Addresses per group** – 300
- **Custom service objects** – 1024

When this option is selected, FortiConverter uses the following maximum table sizes:

- **Address groups** – 20000
- **Addresses per group** – 1500
- **Custom service objects** – 4096

Viewing maximum table sizes for your target device

On your target system, enter the following command:

```
print tablesize
```

The maximum table sizes are displayed in a response similar to the following output:

```
firewall addrgrp: 0 20000 20000
firewall addrgrp: member: 1500 0 0
firewall service custom: 0 4096 0
```

NAT merge options

For Check Point and Cisco PIX conversions, you can select which types of NAT configuration FortiConverter uses to generate output firewall policies, or whether FortiConverter derives its NAT-based policies based on object names or object values.

Because it can take FortiConverter several hours to complete a conversion that includes a large number of NAT rules, Fortinet recommends that you turn off NAT merge for **all** types of NAT for your initial conversion. Then, after you resolve any issues with the conversion, run it again at a convenient time with NAT merge enabled.

NAT merge depth

The FortiConverter NAT merge feature compares the firewall policy source and destination address with addresses in NAT rules. When these addresses overlap, FortiConverter uses the NAT rules to generate additional policies in the output configuration.

If a policy has an address with a large range, it can overlap with many NAT rules, which generates many NAT policies. Because output that includes a large number of NAT policies can be hard to review, FortiConverter provides NAT merge depth options that can reduce the number of NAT policies.

The merge depth policies control both the type of NAT to merge and the scope of the merge:

- When you select **Off** for a type of NAT, FortiConverter doesn't perform NAT merge using NAT rules of that type. If it's turned off for all types, the output conversion contains the converted source configuration policies only.
- When you select **Object Names**, FortiConverter generates policies based on NAT rules only where the address name the rules use is found in a policy. For Cisco PIX, this option can also match NAT rules and policies if they contain addresses that match exactly. For example, a source configuration NAT rule dynamically translates the object "address1"(IP 10.10.10.10) to "200.200.200.200". The source configuration also has three polices:

- policy1: source address is "address1"
- policy2: source address is "10.10.10.0-10.10.10.255"
- policy3: source address is "all"

Only policy1 matches the NAT rule, because it shares the address object name, and policy2 and policy3 don't match

because they don't reference the name "address1".

Cisco PIX allows you to use an IP address to configure a NAT rule instead of a name. For example, the NAT rule 10.10.10.10 to 200.200.200.200. When **Object Names** is selected, this NAT rule matches a policy with source address 10.10.10.10, even though it doesn't refer to a object name because they have the exactly the same IP range. This is a useful option if you make use of supernet addresses that would match many address objects.

- When you select **Object Values**, FortiConverter generates policies based on NAT rules that have address values that fall anywhere in the range specified by a policy (overlap).

  For the example above, when **Object Values** is selected, the NAT rule that translates the object "address1"(IP 10.10.10.10) to "200.200.200.200" matches both policy2 and policy3.

  Object Values generates the most accurate matching of NAT rules and policies, but in most cases, it also generates more NAT policies.

Create new conversion folder

The FortiConverter application allows you to create separate folders for your conversions.

To add a folder

1. Click the **New Folder** option from the menu on the left.
2. Enter a name for your new folder and press **OK**.

Your new folder appears in the left menu.

To move conversions to a folder

1. Select a conversion.
2. Click the **Change Folder** button, located at the bottom.
3. Select a folder for your conversion and press **OK**.

Error Messages

If an error occurs, FortiConverter inserts error messages and warnings into the conversion output file `config-all.txt`.

These warnings aren't inserted in any configuration branch files.

Review the `config-all.txt` file after each conversion for errors. These errors and warning messages might cause the import process to fail, if not corrected.

Undefined objects

```
# Error: Undefined interface/address/service/ippool object <NAME>;
```

This error occurs when an object used in the policy isn't previously defined. Make sure the object name is correct.

Interface

```
# Warning: Please input vlan interface
```

This warning means the physical interface of a vlan interface isn't specified.

Zone

```
# Warning: Interface exists in other Zone.
```

This warning means an interface belongs to two zones simultaneously. An interface should not belong to more than one zone at a time.

Service

```
# Error: The number of service custom is <NUMBER>, exceed <NUMBER>
limitation.
```

The number of services exceeds the maximum number supported by the selected FortiGate model.

Service group

```
# Error: Unconverted members in service group <NAME>
```

This error occurs when objects in the mentioned service group aren't converted and the service group becomes empty.

User

```
# Warning: can't support radius server group
```

This warning means the source configuration contains a radius server group. FortiGate doesn't support radius server groups. This warning only appears in Check Point conversions.

```
# Warning: can't find out radius server
```

This warning means the radius server of the user isn't defined in the source configuration. This warning only appears in Check Point conversions.

```
# Warning: Please reset the shared secret key.
```

This warning means the password in the source configuration is encrypted. Reset the shared secret key.

VIP

```
# Warning: Public IP confliction for below objects.
```

This warning appears when different VIP objects have the same public IP. Different VIP objects should not have the same public IP in FortiOS. To fix this issue, add port forwarding or source filter information to the conflicted VIP object.

VPN phase1

```
# Warning: <NAME> exceed 35 characters"
```

This warning means the Phase1 name exceeds 35 characters. Manually fix the name.

```
# Warning: remote-gw should be IP address, object <NAME> was not defined
```

This error occurs when the source configuration provides an address name for the remote-gw field. The remote-gw field should be an IP address.

```
# Warning: Please reset the pre-shared key.
```

All pre-shared keys are set to "123456" in the converted VPN object, if the password in source config is encrypted. Users should reset the pre-shared keys.

VPN phase2

```
# Warning: <NAME> exceed 35 characters
```

This warning appears when a Phase2 name exceed 35 characters. To fix this issue, fix the name manually.

Policy

```
# set utm-status enable
# set application-list NAME1 NAME2
# Application-list support only one item, please recheck config file.
```

This error means there are multiple items in the application list. There should be only one item in the application list. If there are multiple items given in the source configuration, reset the items.

```
# Warning: Removed self traffic object <NAME> from address list
# Warning: Comment out self traffic policy - object name <NAME>
```

Check Point policies may contain "self traffic" policies, but those policies aren't needed in FortiOS.

```
# Warning: Comment out default drop all policy
```

There may be a "drop all" policy in the end of the policy list for some vendors. But FortiOS has its own "drop all" policy by default, so the one in source configuration should be commented out.

Route static

```
# Warning: Please input field <device>
```

FortiOS requires the "device" (interface) route field.

Snmp sysinfo

```
# Warning: Community <NAME> has <NUMBER> hosts, beyond the limitation <NUMBER>.
```

The number of hosts in a community exceeds the maximum number supported by the FortiGate selected model.

Other warnings

Name length

```
# Warning: truncate <OBJECT> name <NAME> to <NUMBER> characters
```

```
# Warning: Trim <NAME> to <NUMBER> characters
```

When FortiConverter detects an object name that is longer than the limit given in FortiOS, FortiConverter renames the object.

Route BGP

```
# Warning: Please reset the password.
```

This warning appears when the password of route BGP neighbors in the source configuration is encrypted. Reset the password of the route BGP neighbors.

Route OSPF

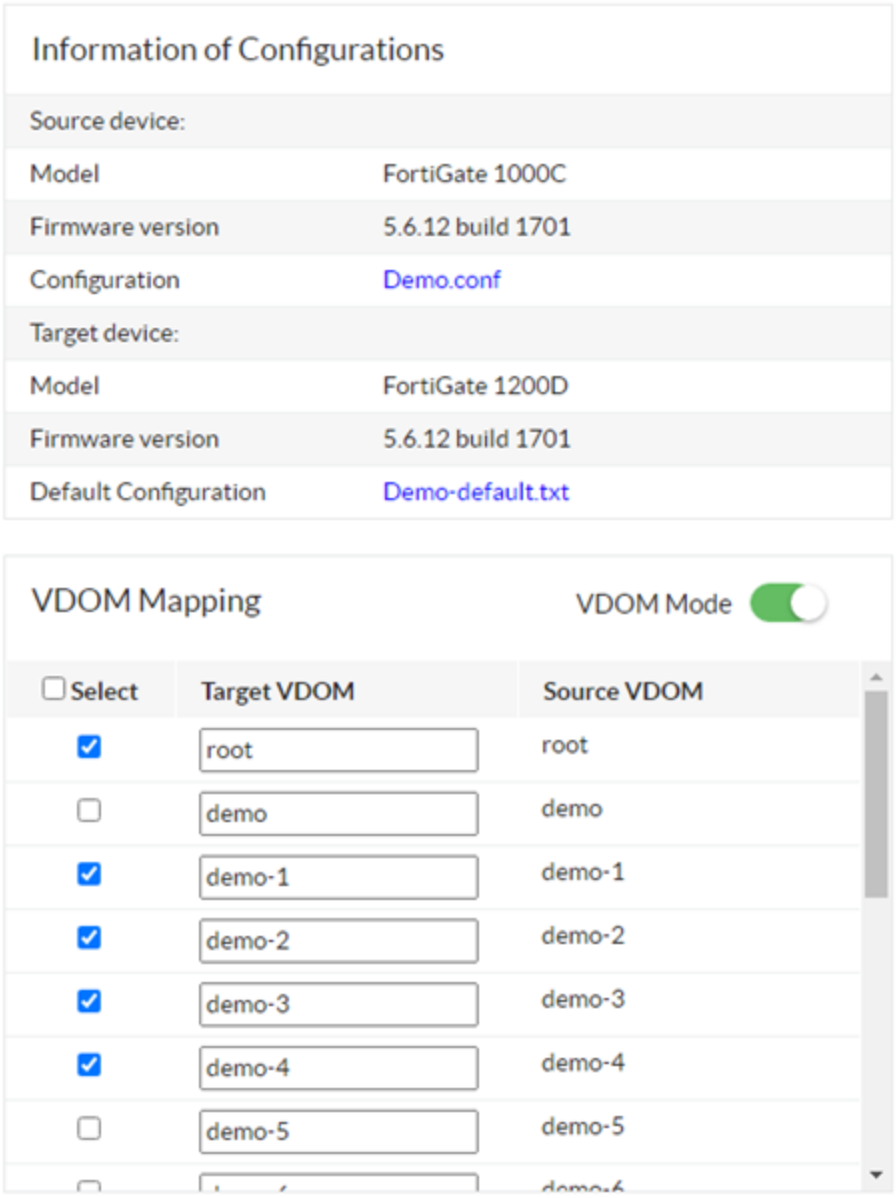
```
# Warning: Please reset the md5 key.
```

This warning appears when the md5 key of the OSPF interface in the source configuration is encrypted. Reset the md5 key.

VDOM Mapping

During conversion, after the configuration parsing, you can select the VDOMs that you want to convert and do VDOM name mapping.

If you unselect a VDOM, FortiConverter will not convert and generate the corresponding configuration in the output result.



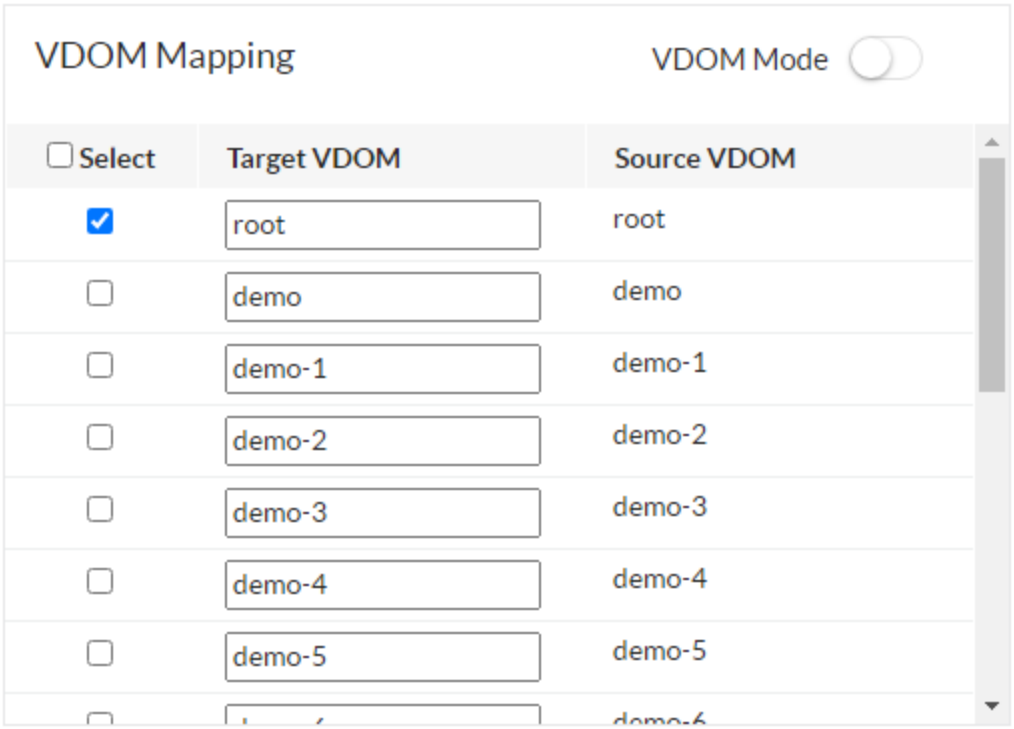
Note: VDOM Mapping does not support adding a new empty VDOM. For 3rd party conversion, an empty VDOM can add to the tuning page.

VDOM Mode Setting

The **VDOM mode** switch allows you to enable the VDOM mode or vice versa.

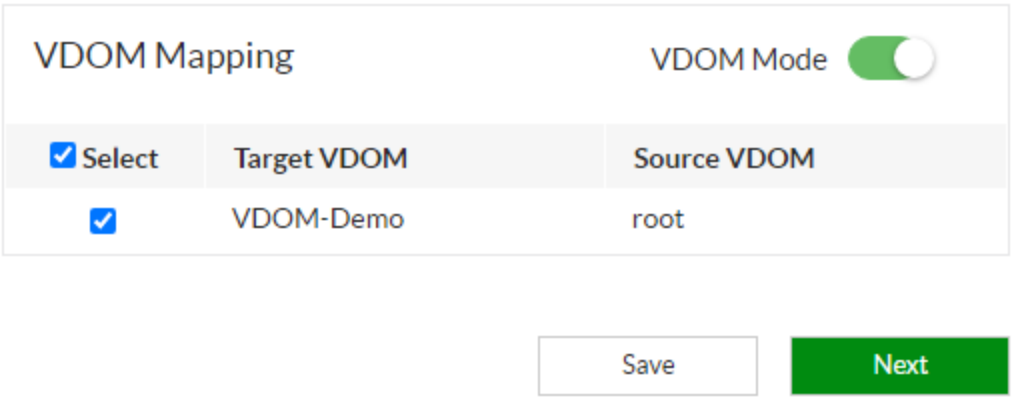
Example

1. Convert VDOM mode from the source to a target device without VDOM.
   a. Select a VDOM you want to upload to the root of the target device
   b. Disable the VDOM mode.
   c. Continue the conversion and get the converted configuration.



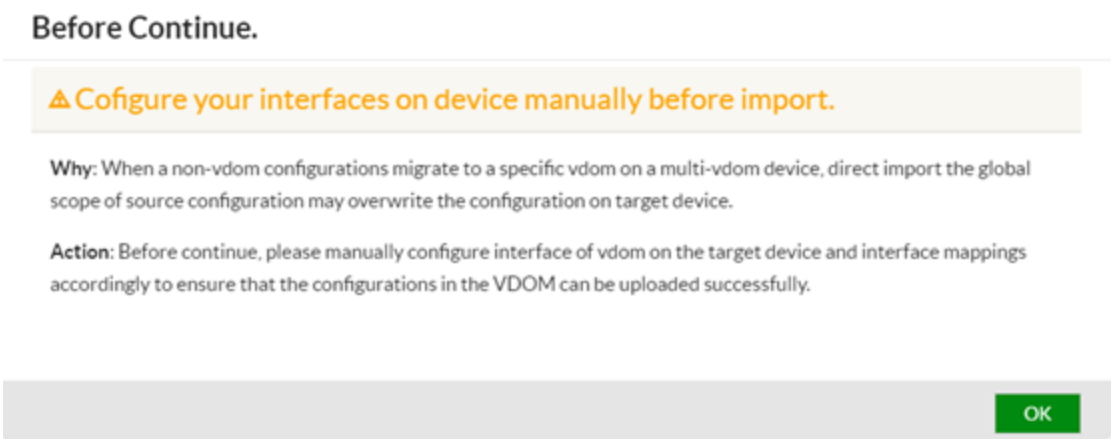
Remark: If you want to upload the "demo" of source VDOM to the target device's root, you can rename the target VDOM to "root" and continue with the conversion.

2. Convert the source device without VDOM to a target device with VDOM mode.
   a. Rename the name of the VDOM to the target device's VDOM you want to import.
   b. Enable VDOM Mode.
   c. Continue with the conversion and get the converted configuration.



Warning

1. In Fortinet migration, when a target device without VDOM enabled migrates to a specific vdom device with VDOM mode enabled, it means there have been existing configurations on the target device and FortiConverter will ignore the global scope of the configuration to avoid overwriting the global settings on the target device. In the device mode, you can utilize the partial import or push those configurations as you want.
2. In the Fortinet migration, if you enable the vdom mode, the "config system interface" under the global scope would not import to the device, please make sure to configure the device's interfaces and do the proper interface mapping before the import process. Otherwise, the object import may fail by the improper interface setting.



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 **Enable Central NAT merge** 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, the option is disabled by default. 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, the option is enabled by default. 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. This 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
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, WatchGuard, Forcepoint	Cisco, Check Point, Juniper, Palo Alto, SonicWALL, Sophos, Huawei, Forcepoint

	Policy NAT mode	Central NAT mode
Allow dynamic NAT based on services	Yes	No
May greatly increase the number of policies	Yes for Cisco, Check Point, Juniper SRX, Palo Alto, SonicWALL, Sophos, 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

Route File

Cisco ASA Routing Table

To display the routing table on a Cisco ASA, the command `show route` or `show ip route` can be used. These command will show you the current routing information, including static routes, directly connected routes, and routes learned via dynamic routing protocols. The output will display the destination network, subnet mask, gateway (next hop), interface, and administrative distance.

Check Point Routing Table

To obtain Check Point routing table, 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.

Route File Remedy Instruction

FortiConverter will make every effort to parse the route file. However, due to variations in output formats across different operating systems, users may occasionally need to make minor adjustments to ensure successful conversion.

Please refer to the following 5 formats and perform the fix accordingly.

Format 1:

Linux/Unix platform's output, use command `route` or `netstat -rn`.

```
Destination     Gateway         Netmask         Flags   Metric   Ref  Use  Iface
172.17.24.1     192.168.2.15    255.255.255.255 UGH     1        0    0    ethN18
```

Format 2:

"Destination" field with IP/netmask format, and "Gateway" is blank for connected route:

```
    Destination     Gateway     Flags    Refs    Use     Netif Expire
    10.11.11/24                 rCGSU    0       0       eth2c0 ----------Original Line.
=>
    10.11.11/24     *           rCGSU    0       0       eth2c0
    Add a character "*" for the connected route.
```

Format 3:

```
    0.0.0.0/0 192.168.1.1      ---------- Original Line
=>
    Destination     Gateway    ----------  Add title
    0.0.0.0/0       192.168.1.1

    Default    Normal    10.254.254.24   ---------- Original Line.
=>
    Destination     UnknowOptions    Gateway ---------- Add title
    Default         Normal           10.254.254.24
```

Format 4:

```
        172.17.24.1 255.255.255.255 192.168.2.15 ethN18 ---------- Original Line.
=>
        Destination     Netmask         Gateway       Iface ---------- Add title
        172.17.24.1     255.255.255.255 192.168.2.15  ethN18
```

Format 5:

```
S   0.0.0.0/0        via 172.31.224.19, eth-s1p1c0, cost 0, age 3294754---------- Original line.
C   127.0.0.1/32     is directly connected, loop0c0

Flags  Destination    Gateway          Iface---------- Add title and remedy the file line.
S      0.0.0.0/0      172.31.224.19    eth-s1p1c0
C      127.0.0.1/32   *                loop0c0
```

Note: FortiConverter only takes care of these keywords from title line, and parses out the corresponding fields by the keyword's order.

1. "Destination"
2. "Gateway"
3. "Genmask"
4. "Netmask"
5. "Mask"
6. "Iface"
7. "Interface"
8. "Netif"

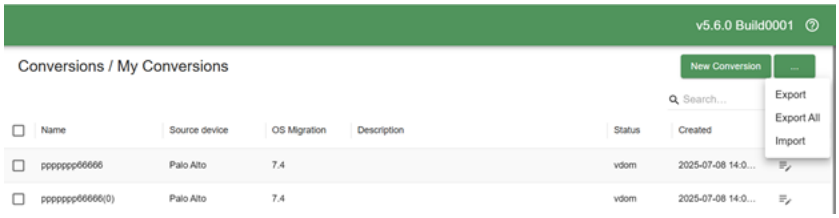
Backup and restore previous conversions

FortiConverter tool provides the capability to backup existing conversions by exporting them to local files. These conversions can be restored later by importing the backup file. Here are some typical use cases where backup/restore feature might become handy:

- Installing FortiConverter software to new instances. You can export the conversion history from old instance and import it to the new instance.
- Backup all the conversions before FortiConverter software upgrade to prevent any possible data loss.

Backup conversions by export

- Select the conversions you want to backup by selecting the check boxes in front of the conversions.
- Select "Export" from the dropdown menu on the up-right corner.
- If you want to backup all the existing conversions, select "Export All" from the drop down menu.



- A backup zip will be downloaded.

Please note that only conversions without any problem will be backed up. If a conversion contains problems like missing source configuration, the conversion will be skipped during exporting.

Restore conversions by import

- Select "Import" from the drop down menu on the up-right corner
- Select a backup zip file that needs to be stored in the popup dialog
- Click "OK"

If the name of a restoring conversion conflicts with an already existing conversion, the restoring conversion will be renamed by adding a number at the end of the original name.

3rd Party Vendor Conversion Tuning

Introduction

Although FortiConverter automatically converts as much of the source configuration as possible, in some cases, your input is required to complete the conversion. The Tuning page automatically opens when the conversion is complete. (**Currently this feature is available only in the conversion of 3rd party vendors**.)

From the Tuning page, you can:

View Conversion Summary

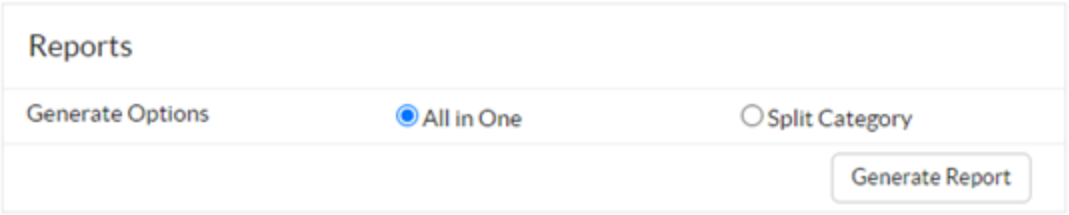
The Conversion Summary page displays a summary of the conversion, including VDOM mapping and Interface mapping, as well as a device summary.

- To fine-tune the conversion, click **FortiGate Configuration** from the menu on the left, then select an option.
- To download the final, converted configuration files, click the **Download Configurations** button, located on the top-right of the conversion page, or the icon in the home page.

Generate reports for 3rd party conversion

Reports can be generated in 3rd party vendor conversions to review the object content. After the conversion is completed, you are able to see the panel of report generation in the conversion summary page. Currently, the feature is supported with vendors below:

Alcatel-Lucent, **Check Point**, **Cisco**, **Forcepoint**, **Huawei**, **Juniper**, **McAfee**, **Palo Alto**, **SonicWall**, **Sophos**, **Tipping Point**, **Vyatta**, and **WatchGuard**.



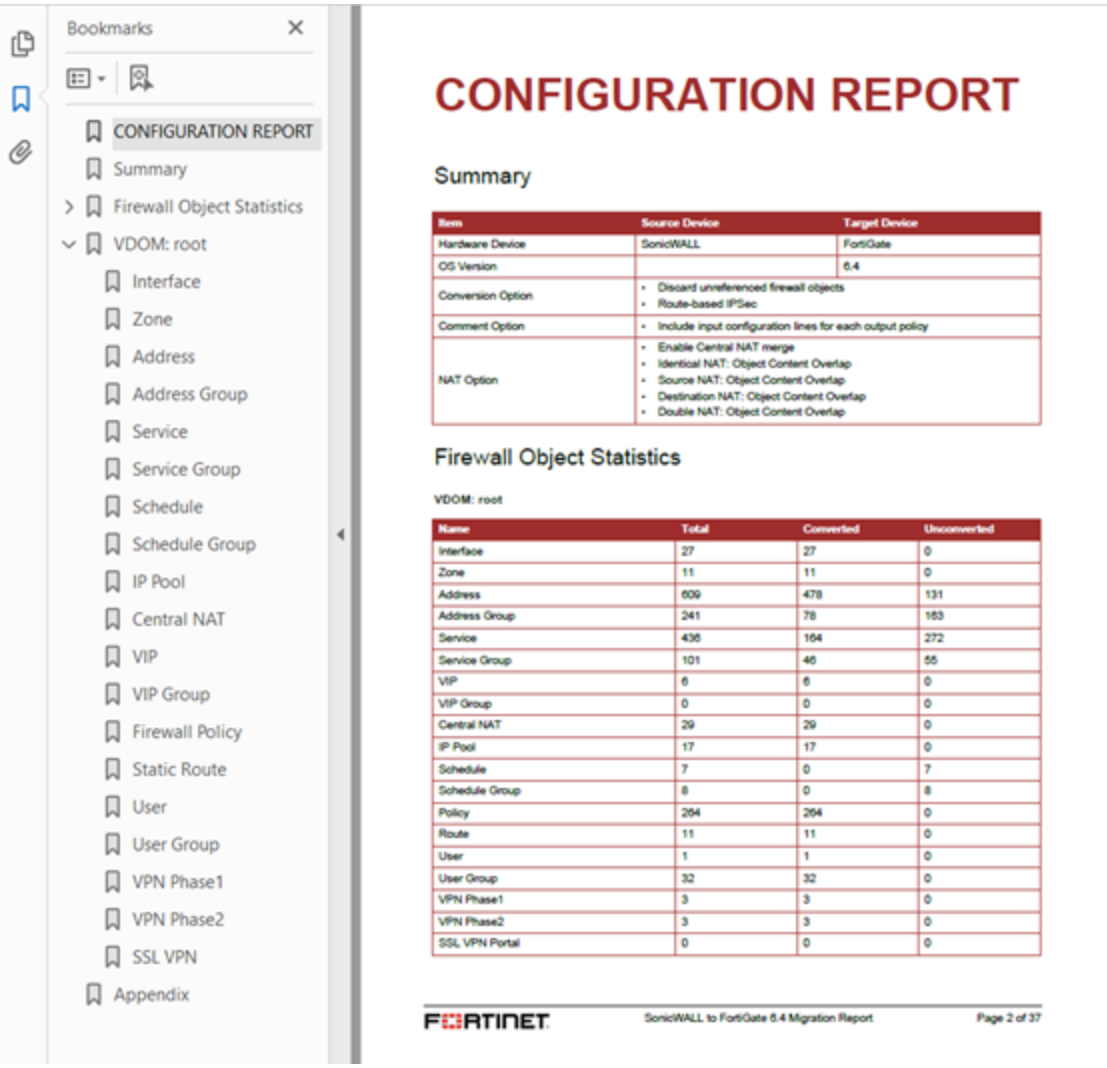
Generate Options	Description
All in One	"All in One" option would generate two PDF reports, converted and unconverted reports. **Converted Report**: lists the objects that are output in the result configuration. **Unconverted Report**: lists the objects that are removed by the feature "Discard unreferenced firewall objects", which can be enabled at the start page. Those objects are removed because they're not referenced by any policies or NAT rules, and they would not show up in the result configuration.

Generate Options	Description
Split Category	"Split Category" would generate PDF reports individually according to each object category. **Converted Report**: splits into multiple reports. **Unconverted Report**: remain the same as in "All in One" option.

Click **Generate Report**, It'll start to the generate report of the conversion result.

Please note that generate PDF reports may take processing time depending on the number of objects. Generally, it may take a while if it's over a thousand objects in a category.

The report might be lengthy if there is a large amount of objects in the conversion. It would be easier to use the bookmarks in the PDF file to jump between different sections of the report.



Manage your firewall objects

The Tuning page has several features enabling you to view, add, edit, and delete your various firewall objects.

To review the converted objects

1. In the upper-left corner, click **FortiGate Configuration**.

   A list of object categories loads in the menu bar, and a table of interface is displayed.
2. Select the object category you want to review.
   A table containing information about that object category loads.

VDOM	Name	Type	Details
AUECKASDWN005 (2236)			
	h-10.132.72.31	ipmask	10.132.72.31 255.255.255.255
	h-10.132.72.32	ipmask	10.132.72.32 255.255.255.255
	h-10.130.72.56	ipmask	10.130.72.56 255.255.255.255
	h-10.130.72.53	ipmask	10.130.72.53 255.255.255.255
	NET_10.10.204.0_24	ipmask	10.10.204.0 255.255.255.0
	NET_10.123.80.0_24	ipmask	10.123.80.0 255.255.255.0
	h-10.130.72.54	ipmask	10.130.72.54 255.255.255.255
	h-10.130.72.57	ipmask	10.130.72.57 255.255.255.255
	NET_10.123.81.0_24	ipmask	10.123.81.0 255.255.255.0
	NET_10.123.84.0_24	ipmask	10.123.84.0 255.255.255.0
	NET_10.127.144.0_21	ipmask	10.127.144.0 255.255.248.0
	NSIP01	ipmask	10.132.38.240 255.255.255.255

In the address, address group, service, and service group tables, some object rows are highlighted in yellow. Highlighted rows indicate objects that were automatically created by the FortiConverter tool during the conversion process. You cannot find the definition for these kinds of objects from the original inputted configuration files.

To edit an existing object in your configuration

1. In the table, double-click the object row you want to edit.
   A window containing configurable fields loads.
2. Update the fields as needed.
3. Click **Save** to save your changes.

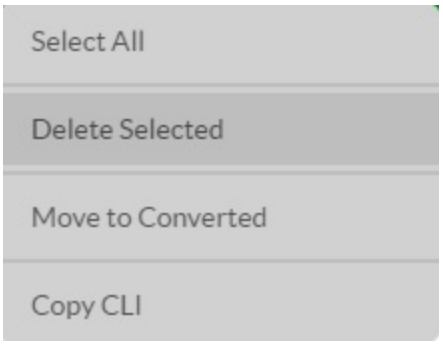
To add an object

At the bottom of every object category table is a button that enables you to add a new object. The button's name is dependent on which object category you want to add to. The directions below outline the steps to add a new address.

1. At the bottom of the object table, click **New Address**.
   A window loads, enabling you input information about the object you want to add.
2. Complete the fields as needed.
3. Click **Save** to save your changes.

To delete an object

1. From the table, select the object you want to delete.
2. Right-click to view the context menu.



3. Click **Delete Selected** from the context menu.
   A confirmation window loads, asking you to confirm your deletion. If the object you want to delete is referenced by other objects, the information will be displayed there.
4. Click **OK** to confirm your deletion.

Zone Configuration on Tuning Page

Switch zone-based and policy-based policies

Fortinet supports both zone-based policies and policy-based policies. If it is required to change a zone-based policy firewall to an interface-based policy firewall or vice versa, it can be done by deleting or creating zones in the Tuning page.

Change zone-based policies into interface-based policies

When users delete a zone in the tuning page, FortiConverter would find zone references in the policies, and change them into the zone member interfaces.

For example, the zones "trust" and "untrust" are configured as the follows:

Name	Interface Members	Intra-Zone Traffic
trust	port1	Deny
untrust	port2 port3	Deny

And there are 2 policies in the converted configuration:

Name	From	To	Source	Destination	Service	Action
1	trust	untrust	Bogon-192.0.2.0-24	X-195.93.178.6	ALL	deny
2	untrust	trust	X-60.169.3.16	Bogon-169.254.0.0-16	ALL	accept

When "trust" and "untrust" zones are deleted from the zone tuning page, FortiConverter would automatically replace all "trust" referenced policies into "port1", and replace all "untrust" referenced polices into "port2" and "port3". Hence the previous policies become:

Name	From	To	Source	Destination	Service	Action
1	port1	port2 port3	Bogon-192.0.2.0-24	X-195.93.178.6	ALL	deny
2	port2 port3	port1	X-60.169.3.16	Bogon-169.254.0.0-16	ALL	accept

Please note that an empty zone cannot be deleted if it is referenced by policies, because deleting an empty zone may result in policies with no interface and would result in import errors.

Change interface-based policies into zone-based policies

When users create a zone in the tuning page, FortiConverter would find references of the zone member interfaces in policies, and change them into the zone names.

For example, there are 2 policies in the converted configuration:

Name	From	To	Source	Destination	Service	Action
1	port1	port2	10.168.168.27	CTN_DEV	ALL	accept
2	port3	port1	AD-173	10.168.168.27	ALL	deny

A zone for "port1", and another zone for "port2" and "port3" are created in the zone tuning page:

Name	Interface Members	Intra-Zone Traffic
Zone1	port1	Deny
Zone2	port2 port3	Deny

FortiConverter would automatically replace all "port1" referenced in policies into "Zone1", and replace all "port2" and "port3" referenced in polices into "Zone2". Hence the previous policies become:

Name	From	To	Source	Destination	Service	Action
1	Zone1	Zone2	10.168.168.27	CTN_DEV	ALL	accept
2	Zone2	Zone1	AD-173	10.168.168.27	ALL	deny

Please note that deleting a zone after it is created may change some policies permanently.

For example, deleting "Zone1" and "Zone2" above would get the following policies:

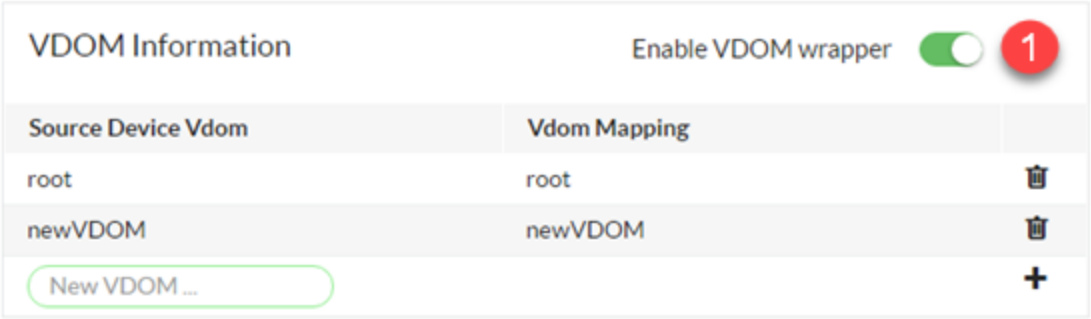
Name	From	To	Source	Destination	Service	Action
1	port1	port2 port3	10.168.168.27	CTN_DEV	ALL	accept
2	port2 port3	port1	AD-173	10.168.168.27	ALL	deny

It turns out that the policy interfaces are different from the previous ones. So please be careful while creating and deleting zones.

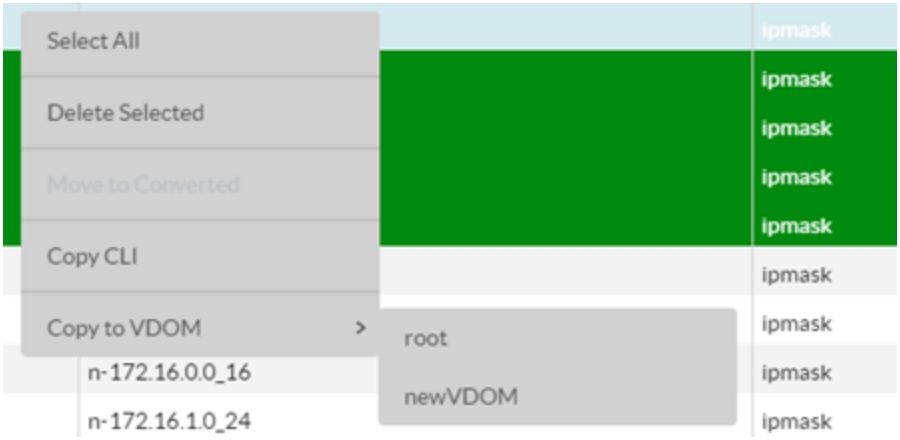
Copy an object to another VDOM

To copy objects to another VDOM

1. In the VDOM information section, toggle the **Enable VDOM** wrapper switch.



   Note: In order to enable the VDOM wrapper, the output requires at least two VDOMs. If the original configuration only has one VDOM, you can manually add a new VDOM.
2. From the table of objects, select the object(s) you want to copy to another VDOM.
3. Right-click to view the context menu.

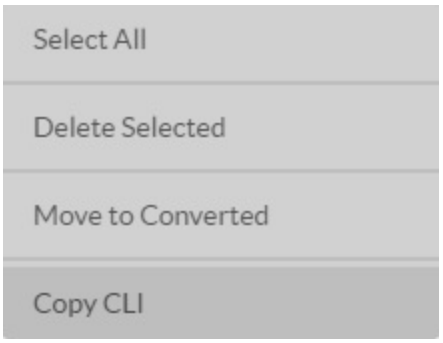


4. Expand the **Copy to VDOM** sub-menu.
   Your accessible VDOMs are listed in the sub-menu.
5. Select the VDOM you want to copy to.
   Your selected object(s) will be included in the selected VDOM output.

Copy an object's CLI configuration

To copy the CLI configuration of an object

1. From the list of objects, select the object that you want to copy the CLI from.
2. Right-click to view the context menu.



3. Click **Copy CLI**.
4. From the prompted window, click **Save** to save the configuration as a text file, or click **Copy** to copy the configuration to the clipboard.

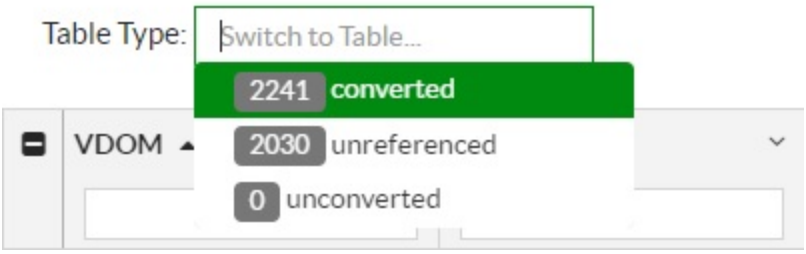
Output an unreferenced object

You can output unreferenced objects from the address, address group, service, and service group categories. To do so, you must move unreferenced objects from the unreferenced table to the converted objects table.

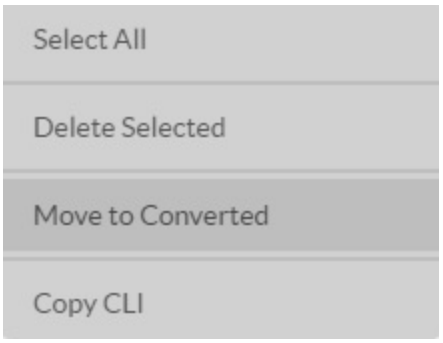
If you enable the "Discard unreferenced objects" option in the start page, FortiConverter scans each object and checks whether it is referenced by policies, central NAT rules or other objects.

To output an unreferenced object

1. Select the object category you want to include in your output.
   Note: You can only output unreferenced objects from the address, address group, service, and service group categories.
2. In the Table Type field, select "unreferenced".



   - **converted** - Objects are referenced and can be generated to the outputs.
   - **unreferenced** - Objects are not referenced and generally cannot be generated to the outputs.
   - **unconverted** - Objects cannot be converted by FortiConverter tool. They are not supported by FortiOS, or by FortiConverter.
3. Select the object(s) you want to output.
   You can select the entire table by right-clicking and selecting **Select All** from the context menu.
4. Right-click to view the context menu.



5. Select **Move to Converted**.
   FortiConverter moves the selected objects to the converted category.
6. In the upper-right of the page, click **Download Configuration**.
   The configuration of the objects are included in the output.

Rename an object

FortiOS sets different maximum characters length for object names. Object names that exceed the character limit are known as *overlengthed*, and must be renamed before they can be uploaded to a FortiGate device. The tuning summary table displays overlengthed objects numbers in red.

Device Summary

VDOM	Object Name	Detected	Overlengthed
root (12)			
	Interface	5	0
	Zone	0	0
	Address	198	2
	Address Group	28	1
	Service	22	0
	Service Group	4	1
	VIP	14	0

There are two ways see which objects are marked as overlengthed. You can:

1. Click the red number from Overlengthed column, or
2. Go to the table of the object, and click the button **Name Overlength**.
   Overlengthed object names are identified with a red background color.

Once you located the overlengthed objects, there are three ways to rename the object: (1) manually, and (2) automatically, (3)manually via CSV file export and import.

To manually rename an object

1. Double-click the object row.
2. In the prompt window, shorten the object name.
3. Click **OK**.

To automatically rename an object

1. Select the object row.
2. Right-click to view the context menu.
3. Click **Trim Object Name Automatically**.
   FortiConverter automatically deletes the last few characters from the tail-end of the object name so it falls under the character limit.

To manually rename an object via CSV file export and import

1. Select the object row.
2. Right-click to view the context menu.
3. Click **Export Names to CSV File** to download the CSV file of the selected objects' name.
4. Open the CSV file and only edit the new names in the **New Legal Names** column.

	A	B
1	Old Overlength Names	New Legal Names
2	Old Overlength Names 1	New Legal Names 1
3	Old Overlength Names 2	New Legal Names 2
4		

5. Save and close the edited CSV file
6. Return to the FortiConverter client, click **Import Edited Names** from CSV file and select the edited CSV file to change the names.

Find and merge duplicate objects

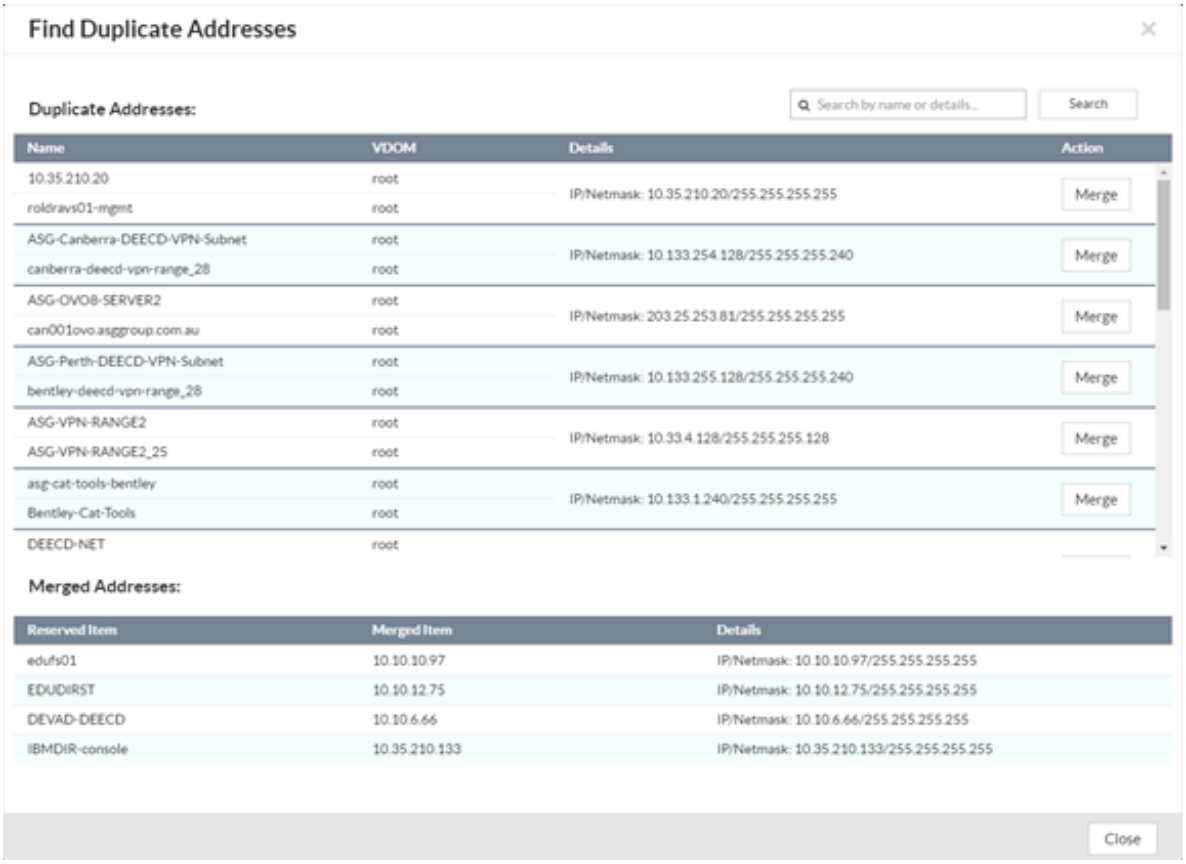
This feature helps you to find duplicate addresses, services, and groups which have the same name or content.

Find and merge duplicate objects in the converted objects

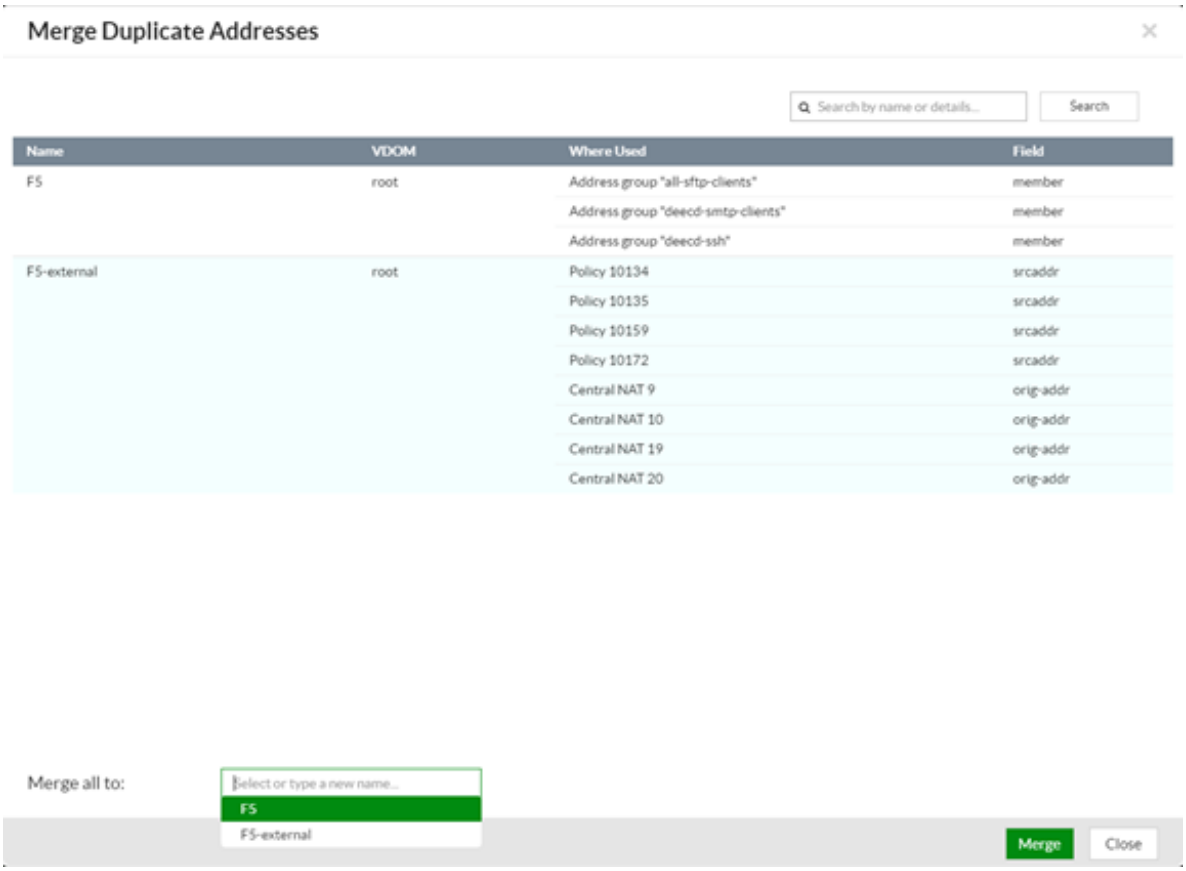
This feature helps you to find duplicate addresses, services, groups which have the same content, and merge them into a single object.

To merge duplicate objects:

1. Click **Find Duplicate** in the tuning page. This feature is available for addresses, address groups, services and service groups.
2. Duplicate objects would be shown in the pop-out window.



3. To merge a group of duplicate objects, click **Merge** in the table.
4. The detail of the duplicate objects would be shown in another pop-out window. All the objects (policies, groups, NAT rules) that references the duplicate objects in all VDOMs would be listed.



5. There is a droplist in the bottom of the window. Users can either select one of the name of the duplicate objects, or type a new name in the box.
6. Click **Merge**, and all the duplicate objects would be unified into the specified name.
7. After the merging is complete, the detail window would be closed and back to the duplicate table window. The record of this merging would be created and all the merging records would be shown in the merging history at the bottom.

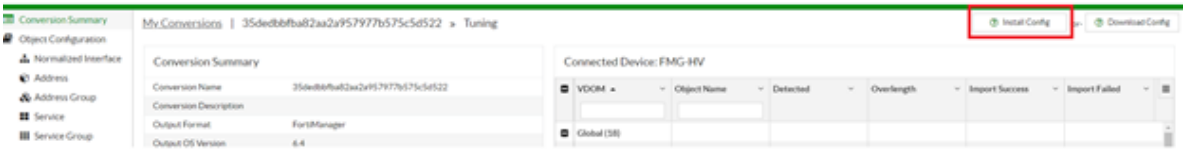
Find duplicate objects to the connected device

This feature helps you to compare the addresses, services and groups in the converted config with the FortiGate or FortiManager device connected, then find the objects which have the same name but different content. You can choose not to import those objects to prevent the objects already on the device being overwritten after the import.

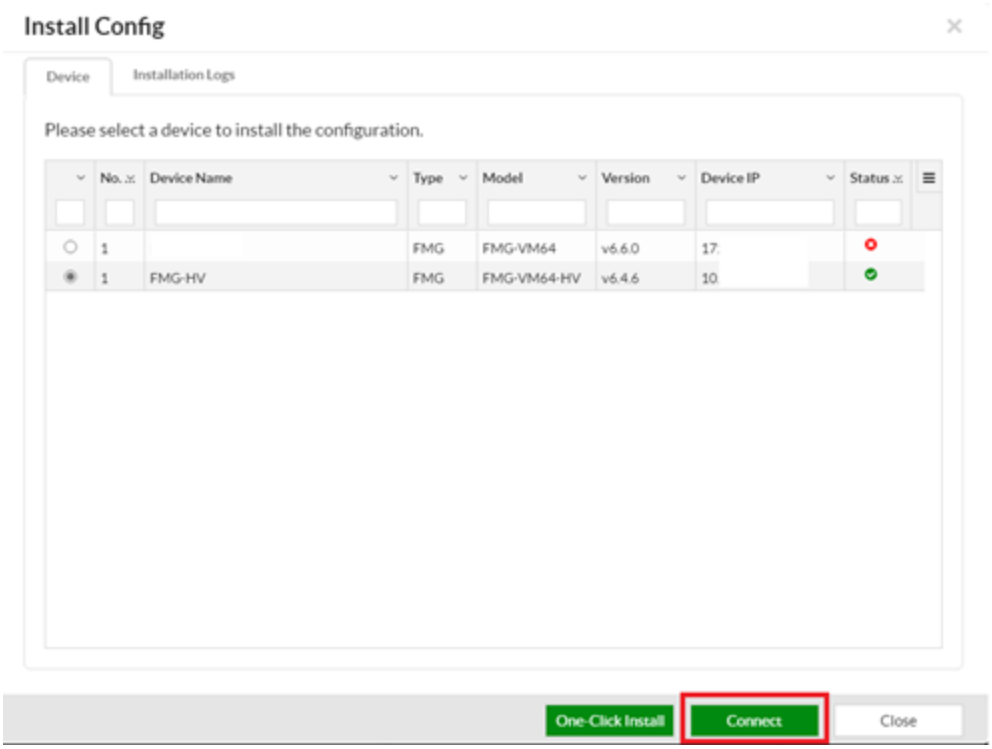
To use this feature, FortiConverter needs to connect to a FortiGate or FortiManager device via REST API. For "How to connecting the FortiGate/FortiManager device to FortiConverter", please refer to Connecting FortiGate devices on page 279.

After the conversion is completed, go to the conversion tuning page:

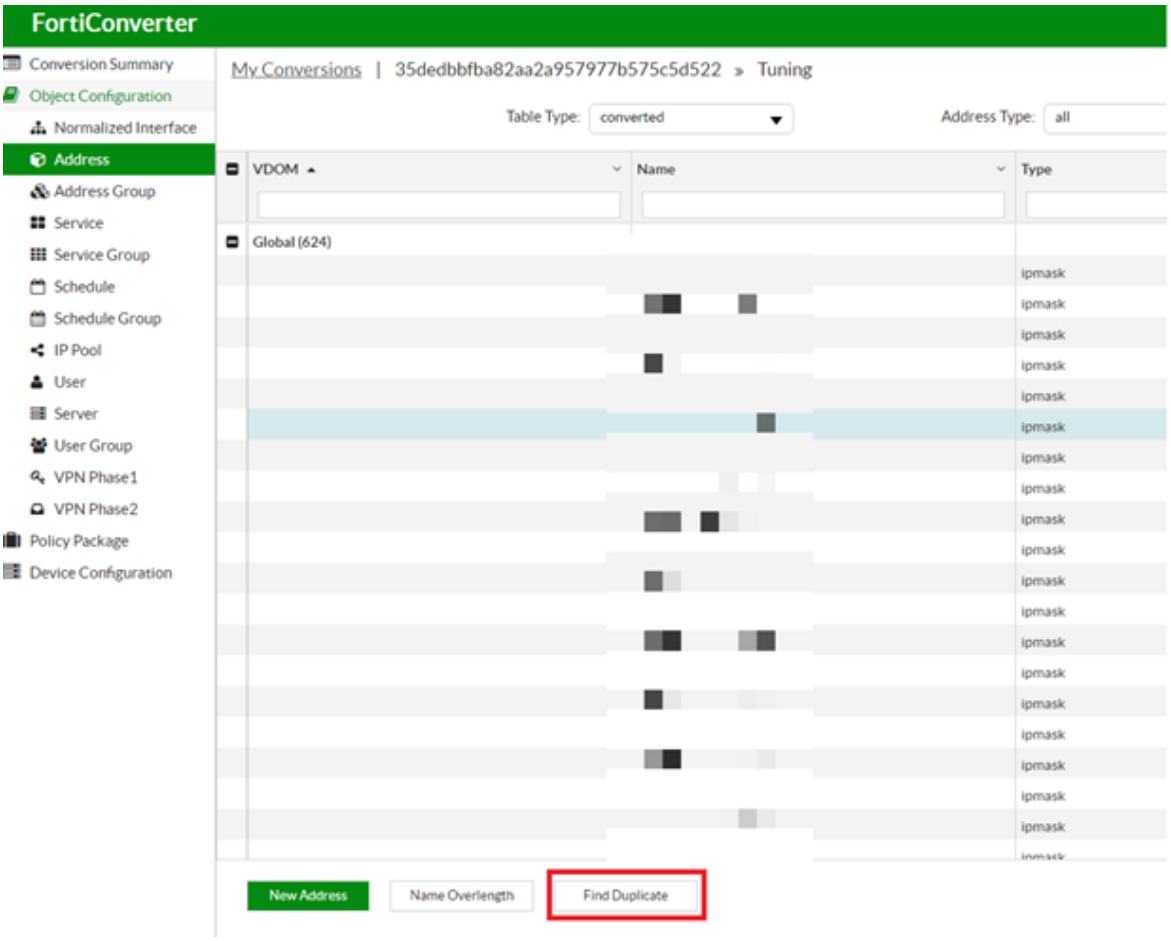
1. If you're not connect to the device, click **Install Config** on the right-top side.



2. Select the target device and click **Connect**.

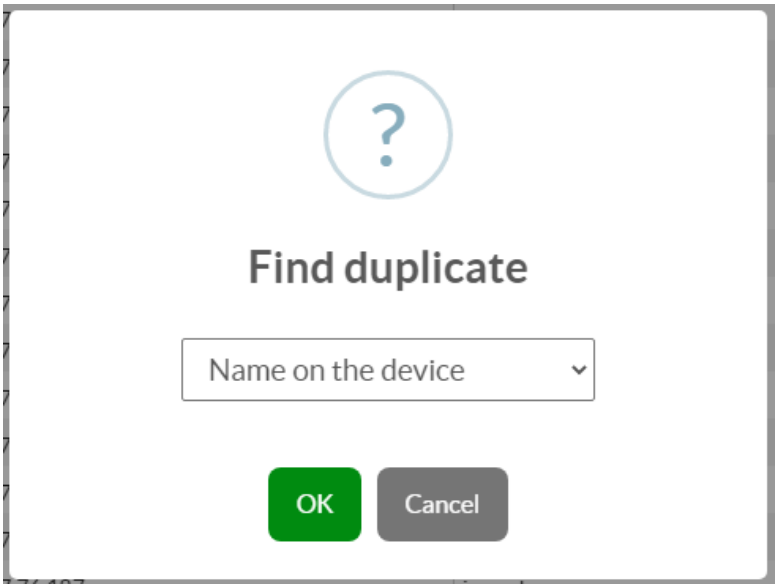


3. Go to category tuning page.

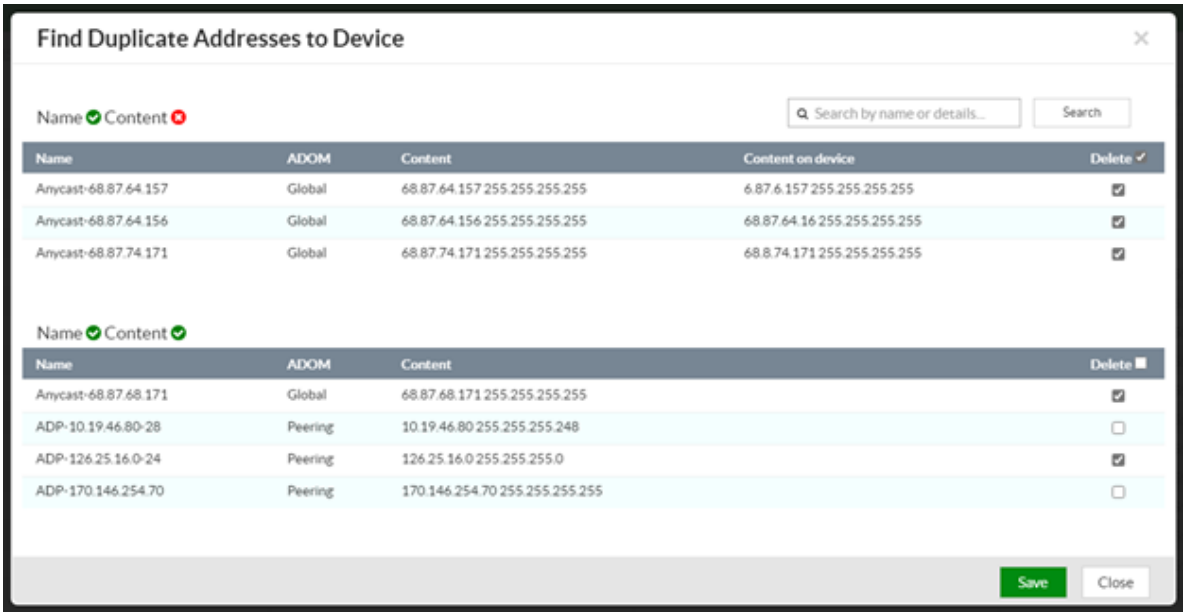


4. There's a button called **Find Duplicate**. In the dropdown menu, you'll need to select the search strategy.
   a. **Name on the device (Compare to device objects)**
      Search the device objects with duplicate names.
      (You have to connect FortiConverter with the FortiGate/FortiManager device)
   b. **Content on the device (Compare to device objects)**
      Search the device objects with duplicate content.
      Note: If the name and content are both duplicate, you should instead do a search by **a. Name on the device** to delete the duplicate items.
      (The content duplicate search would not search for duplicate name and content items simultaneously.)
   c. **Content in the current list (conversion result comparison)**
      This performs the same feature as Find and merge duplicate objects in the converted objects on page

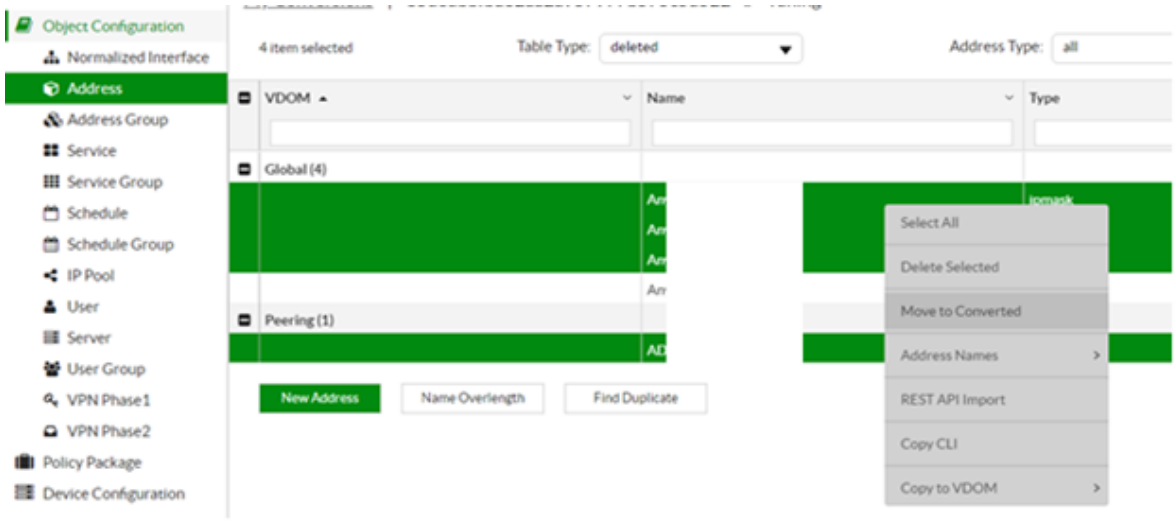
259.



5. Please select **Name on the device** and click **OK**.
6. It'll search the object name and content, and show the duplicate objects.
   The first table shows the objects with the same name but different content.
   The second table shows the duplicate objects with the same name and content.



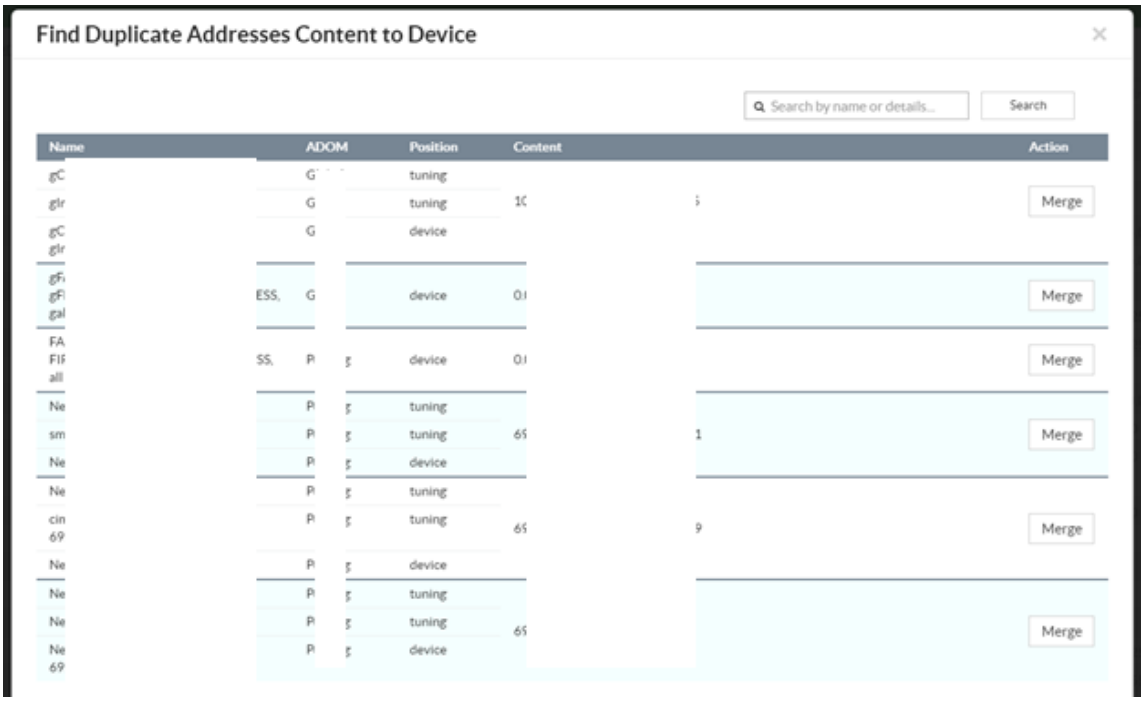
7. Select the objects you don't want to import to the target device, and click **Save**.
   The objects will not be deleted permanently, you can always restore them later.
8. The deleted object will not be present in the conversion result or be imported to the target device.
9. If you want to restore the deleted object to the conversion result. You can switch to the deleted table by selecting **Table Type**.
10. Right click the deleted objects and select **Move to Converted**.
    It'll be restored to the converted table.



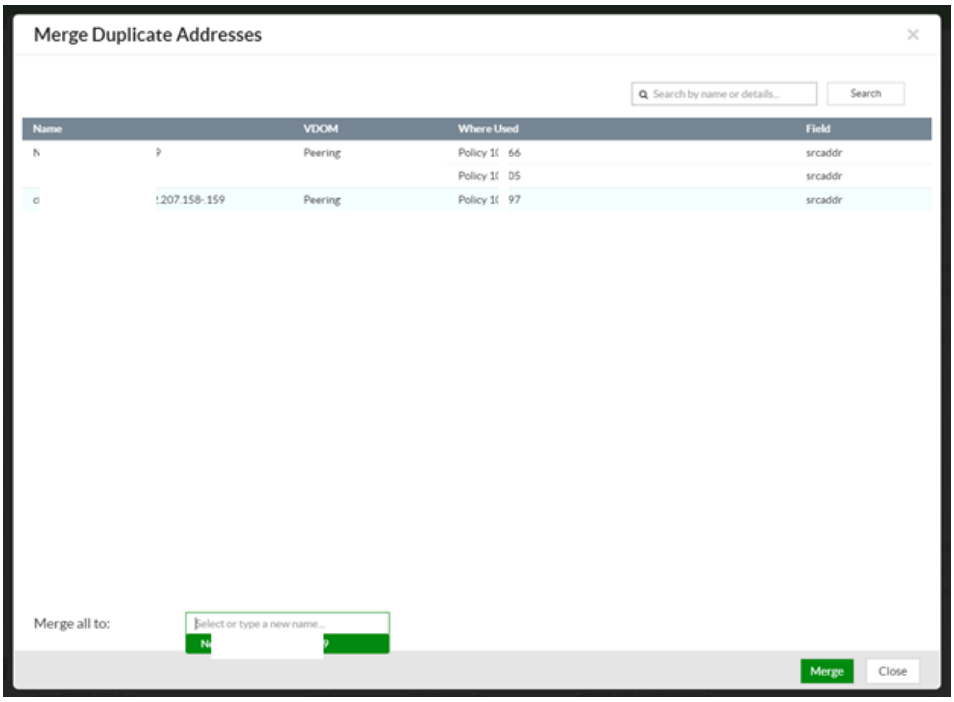
Find duplicate contents to the connected device

This feature helps you to compare the addresses, services and groups in the converted config with the FortiGate or FortiManager device connected, then find the objects which have the same content but different name. You can choose to merge those objects in the converted config to the object on the device.

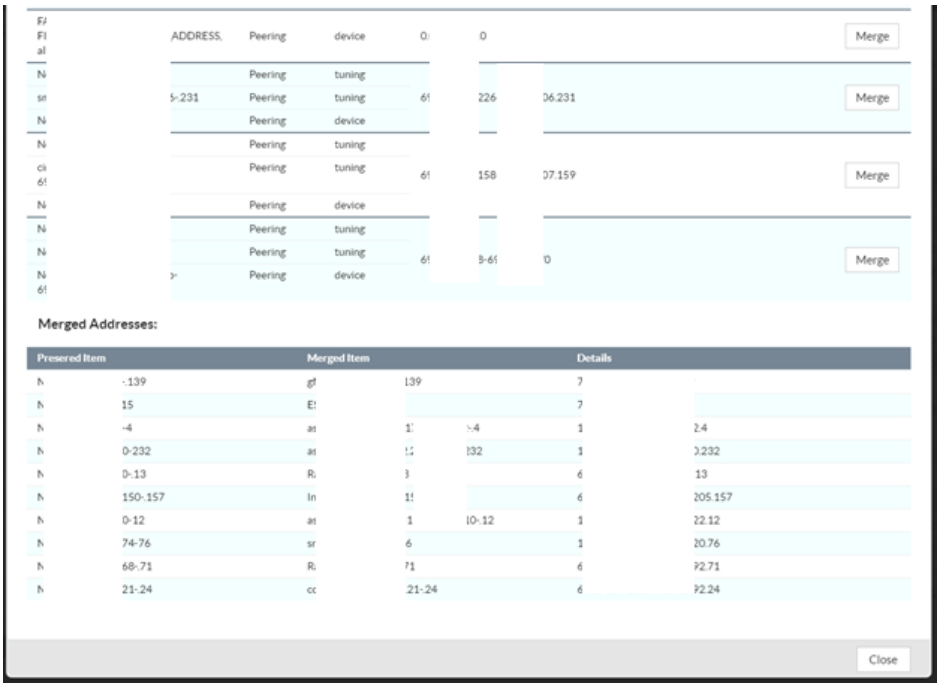
1. Follow the steps above to connect to a FortiGate or FortiManager.
2. Click **Find Duplicate** on the tuning page, select **Content on the device** and click **OK**.
3. It'll search the object with the same content and allow you to merge(rename) the object to the existing object name on the device.



4. On each row, you can **Merge** all the duplicate item(s) on the tuning position to one name.
   The best part is we'll find all the places where reference to these objects and update them accordingly.



5. You can select the existing name on the device or create a new name as you merge. All the objects on the tuning page would be merged to this one name.
   Note: The merged object cannot be recovered.
6. The merge record also shows as below.
   After the merge, you cannot merge again based on the same content.



If you want to remove objects with the same content, first go to Find duplicate contents to the connected device on page 264, merge the object with the same name to the device. Then, turn to Find and merge duplicate objects in the converted objects on page 259, it'll list all the objects with the same name and content, select the object and delete it.

Interface pair view split for policies

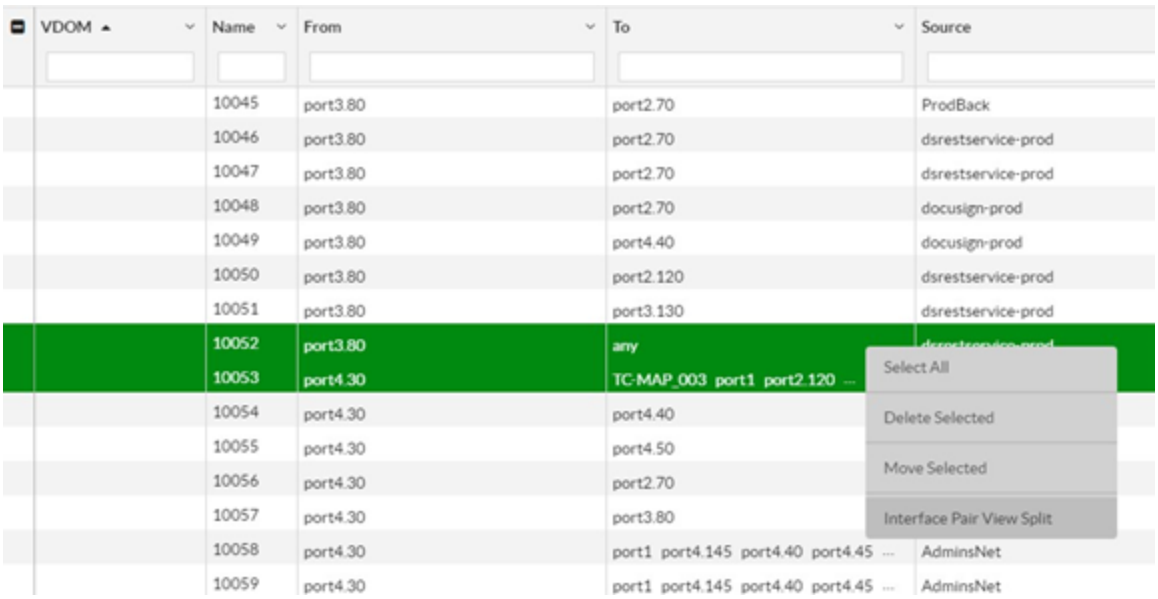
There are 2 modes to show policies in FortiOS: "**Interface Pair View**" and "**By Sequence**".

"**Interface Pair View**" categorizes policies by their source and destination interfaces, so it is more straight forward to manage.

However, "Interface Pair View" can only be used when all the policies contain only one interface in both source and destination interface fields. If there are multiple interfaces in a converted policy, "Interface Pair View Split" can split the policy into equivalent policies with single interface.

Please follow the steps below to split the policies:

1. Go to the tuning page of policies.
2. Click **Interface Pair View Check** to list all the policies which have multiple source or destination interfaces. (Optional)
3. Select the policies you want to split and right click.
4. Click **Interface Pair View Split**.



5. Select Options:
   a. Discard hairpin policies

      Hairpin policies refer to policies from and to the same interface.

      For example, a policy from **port1** to **port1 and port2** can be split into 2 policies: one is from **port1** to **port1** and the other is from **port1** to **port2**. If this option is enabled, the first policy would be discarded.

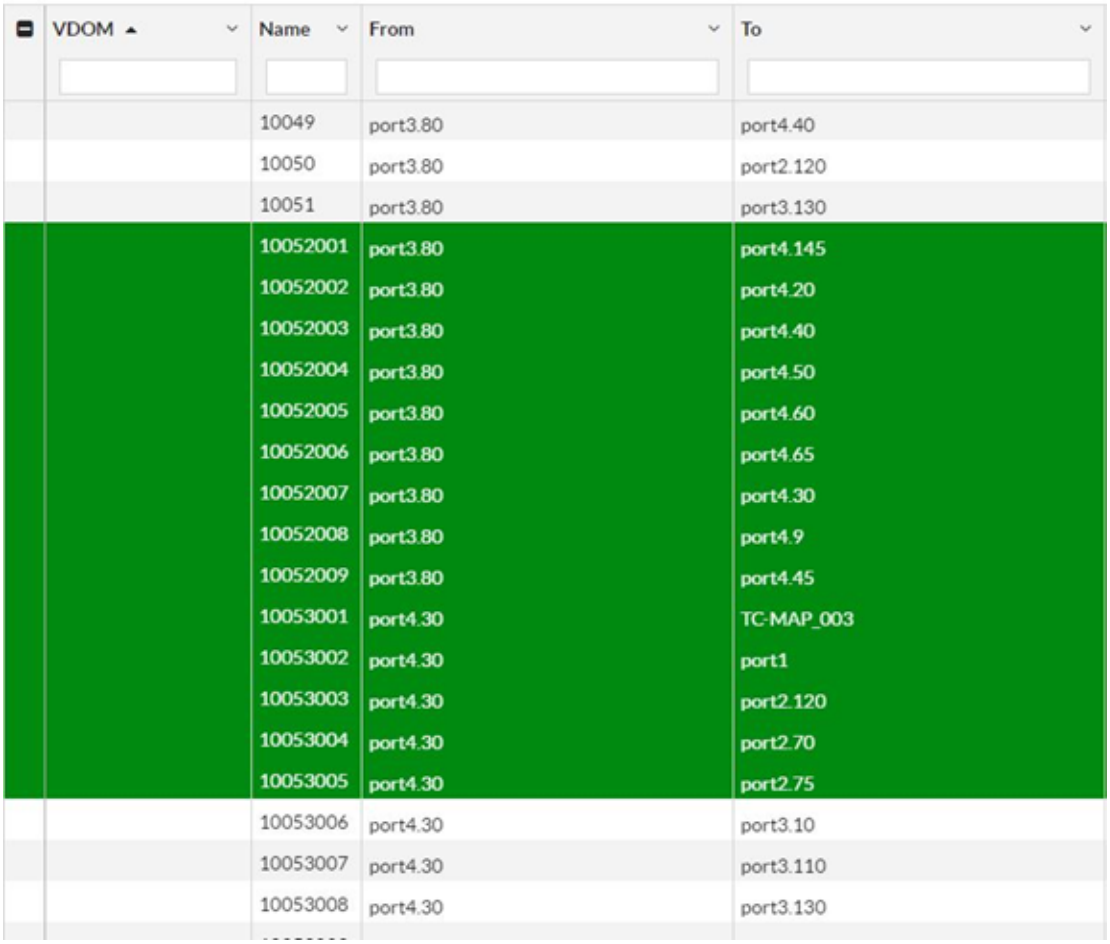
      This option is enable by default.

   b. Split interface "any" into multiple policies.

      If the source or destination interface of a policy is "any", you can choose to either split "any" into a list of interfaces, or not split the policy. If you want to split "any" into a list of interfaces, please select the interface names that represent to "any".

      For example, if **port1** and **port2** are selected, a policy from port1 to any can be split into 2 policies: one is from **port1** to **port1** and the other is from **port1** to **port2**. If this option is disabled, the policy would not be split.

      This option is disable by default. Please note that there may be a lot of policies generated if many interfaces are selected.
6. The selected policies will be split.



VDOM	Name	From	To
	10049	port3.80	port4.40
	10050	port3.80	port2.120
	10051	port3.80	port3.130
	10052001	port3.80	port4.145
	10052002	port3.80	port4.20
	10052003	port3.80	port4.40
	10052004	port3.80	port4.50
	10052005	port3.80	port4.60
	10052006	port3.80	port4.65
	10052007	port3.80	port4.30
	10052008	port3.80	port4.9
	10052009	port3.80	port4.45
	10053001	port4.30	TC-MAP_003
	10053002	port4.30	port1
	10053003	port4.30	port2.120
	10053004	port4.30	port2.70
	10053005	port4.30	port2.75
	10053006	port4.30	port3.10
	10053007	port4.30	port3.110
	10053008	port4.30	port3.130

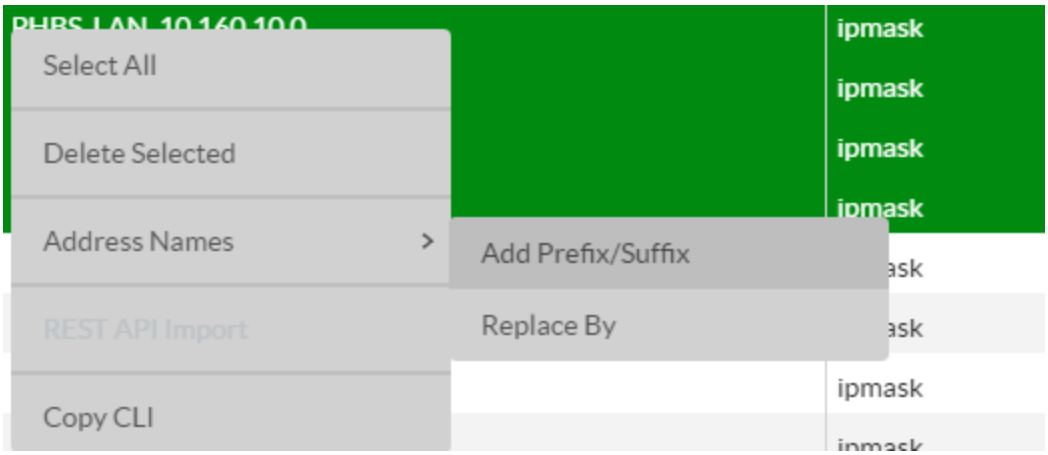
Add Prefix/Suffix or Replace Object Name

Add Prefix/Suffix to object(s) name on page 269

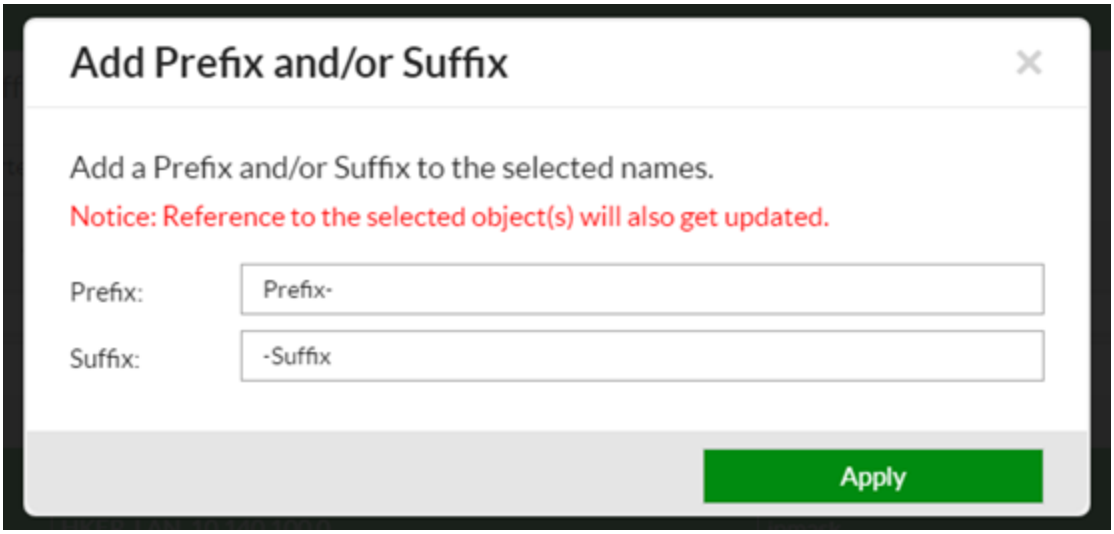
Find and replace the object(s) name on page 269

Add Prefix/Suffix to object(s) name

1. Go to the address (group) or service (group) tuning page.
2. From the table of objects, select the object(s) you want to add the prefix/suffix name.
3. Right-click to view the context menu and select **Add Prefix/Suffix**.



4. Enter the Prefix or Suffix string you want to add to the object name, both prefix or suffix addition are supported.

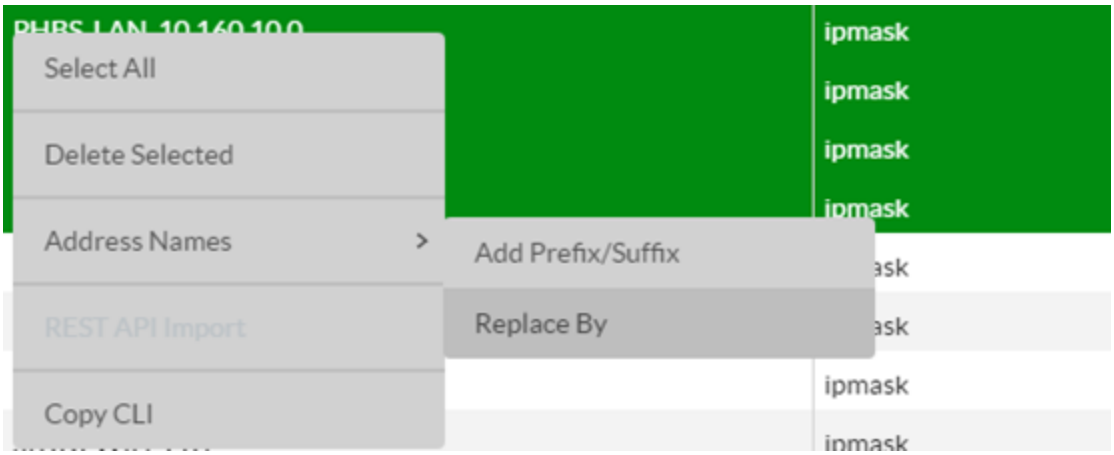


5. Click Apply to apply the changes.

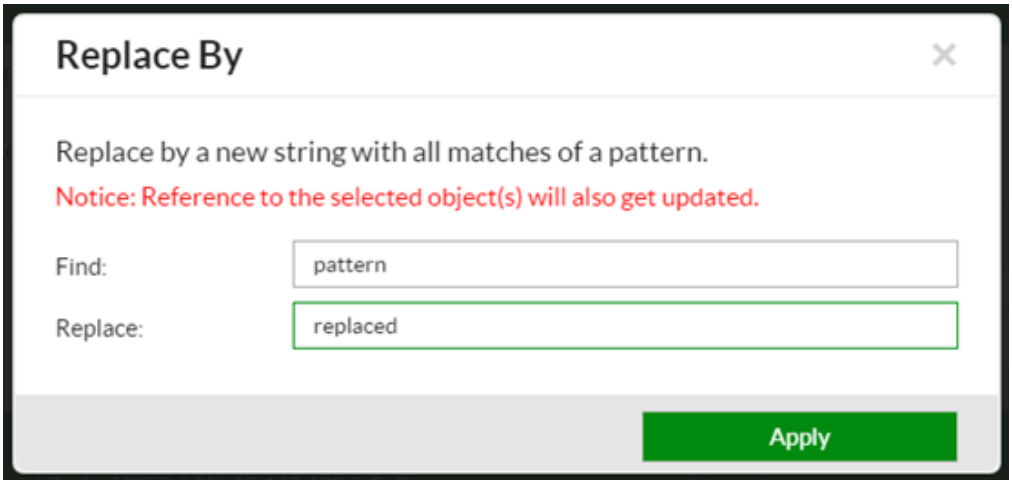
Find and replace the object(s) name

1. Got to the address(group) or service(group) tuning page.
2. From the table of objects, select the object(s) you want to replace the name.

3. Right-click to view the context menu and select **Replace By**.



4. Enter the string pattern and the string you want to replace.



5. Click **Apply** to apply the changes.

Find undefined object references that requires manual tuning adjustment

Background

After the conversion, there might be some object references that weren't defined in the configuration or cannot be converted. In this case, the summary page would be highlighted to indicate that some object(s) within the

highlighted category require manual adjustment in the tuning page before the configuration could be properly imported into a device.

Device Summary

VDOM	Object Name	Detected	Overlength
root (19)			
	Interface	7	0
	Zone	0	0
	Address	201	0
	Address Group	36	0
	Service	192	0
	Service Group	23	0
	VIP	24	1
	VIP Group	0	0
	Central NAT	34	0
	IP Pool	9	0
	Schedule	0	0
	Schedule Group	0	0
	Policy	195	0
	Route	22	0
	User	2	0
	User Group	5	0
	SSL VPN Portal	0	0
	VPN Phase 1	0	0
	VPN Phase 2	0	0

In each object tuning page, the entries/fields with undefined object references will be highlighted for faster object tracking experience.

VDOM	Name	From	To	Source	Destination	Service
root (195)						
	10000	Ethernet0/0.251	any	canberra-net	all	ALL
	10001	Ethernet0/0.251	any	asg-melb-office1	all	ALL
	10002	Ethernet0/0.251	any	Perth1-net	all	ALL
	10003	Ethernet0/0.251	any	asg-perth-net	all	ALL
	10004	Ethernet0/0.251	any	Oracle-enterprise-manager	npman01	OEM-console-ports
	10005	Ethernet0/0.251	any	ASG-legacy-net1	DEECD-NET	net-mgt
	10006	Ethernet0/0.251	any	asg-melb-office	DEECD-NET	net-mgt
	10007	Ethernet0/0.251	any	ASG-VPN-Range-Legacy	DEECD-NET	net-mgt
	10008	Ethernet0/0.251	any	ASG-VPN-RANGE2	DEECD-NET	net-mgt
	10009	Ethernet0/0.251	any	pa0240mcs.asggroup.com.au-1	DEECD-NET	net-mgt
	10010	Ethernet0/0.251	any	asg-melb-office1	DEECD-NET	net-mgt
	10011	Ethernet0/0.251	any	canvads011-1	DEECD-NET	net-mgt
	10012	Ethernet0/0.251	any	canberra-net	DEECD-NET	net-mgt
	10013	Ethernet0/0.251	any	canvads011-2	DEECD-NET	net-mgt
	10014	Ethernet0/0.251	any	asg-perth-net	DEECD-NET	net-mgt
	10015	Ethernet0/0.251	any	Bentley-DC-subnet1	DEECD-NET	net-mgt
	10016	Ethernet0/0.251	any	Bentley-Cat-Tools	DEECD-NET	net-mgt
	10017	Ethernet0/0.251	any	ASG-Canberra-DEECD-VPN-Subnet	DEECD-NET	net-mgt
	10018	Ethernet0/0.251	any	ASG-Perth-DEECD-VPN-Subnet	DEECD-NET	net-mgt

The downloaded configuration will also provide a commented warning line for undefined objects.

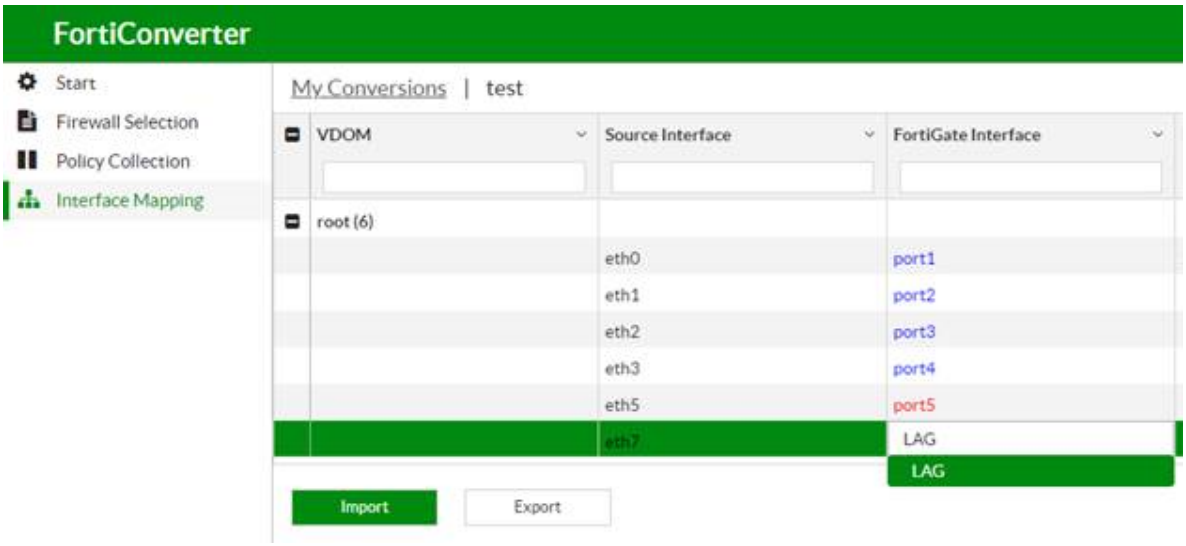
For this specific example, the configuration of policy 10000 would show:

```
edit 10000
   set srcintf "Ethernet0/0.251"
   set dstintf "any"
   set srcaddr "canberra-net"
   set status enable
   set action accept
   set comments "access-list NextGen_authentication extended permit ip object canberra-
        net any"
   set groups "LOCAL"
   set dstaddr "all"
   set service "ALL"
   set schedule "always"
   set logtraffic disable
   # Error: Undefined srcaddr object "canberra-net"
next
```

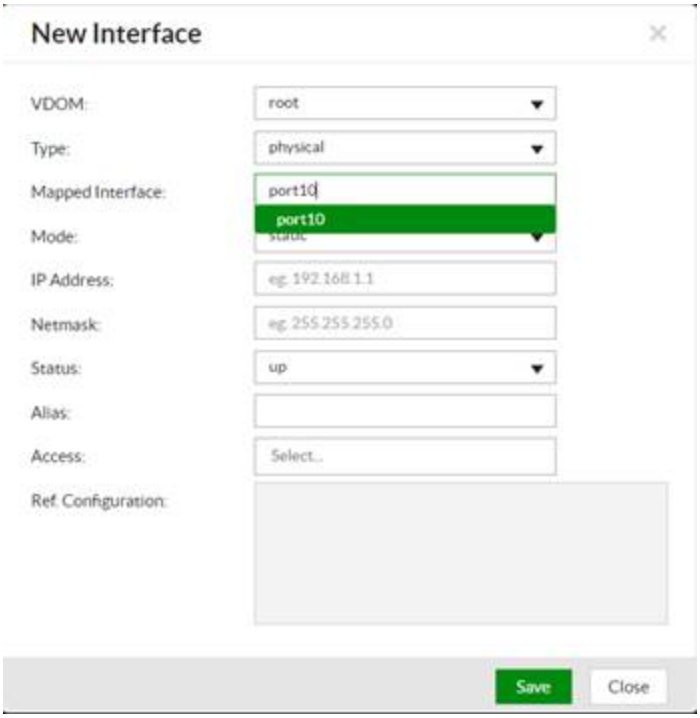
Change Interface Types

For 3rd party conversions, FortiConverter doesn't allow users to change the interface types in the interface mapping page, but it can be completed in the tuning page. Various kinds of interface type changes can be performed. This section shows the way to change a physical interface into an aggregate interface as an example.

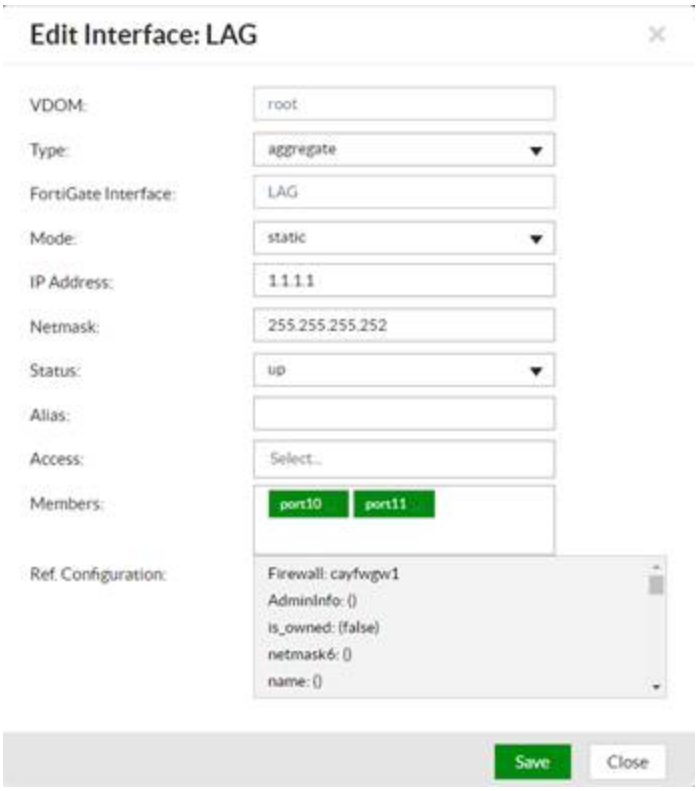
1. Map the interface name in the source configuration into the new interface name ("LAG", as an example) in the interface mapping page:
   FortiConverter doesn't support changing the interface type in the interface mapping page, so we can only change the name first.



2. Proceed the conversion to the tuning page, and go the tuning table of interfaces.
3. If the members in the aggregate interface are not in the source configuration and thus not in the table, please click "New interface" to create them:



4. Double click the interface that will be changed to an aggregate interface, change its type into "aggregate" and add members into it.



5. FortiConverter will output the aggregate interface and the newly created members as config lines.

Import Configuration

Connect FortiGate device via API Token

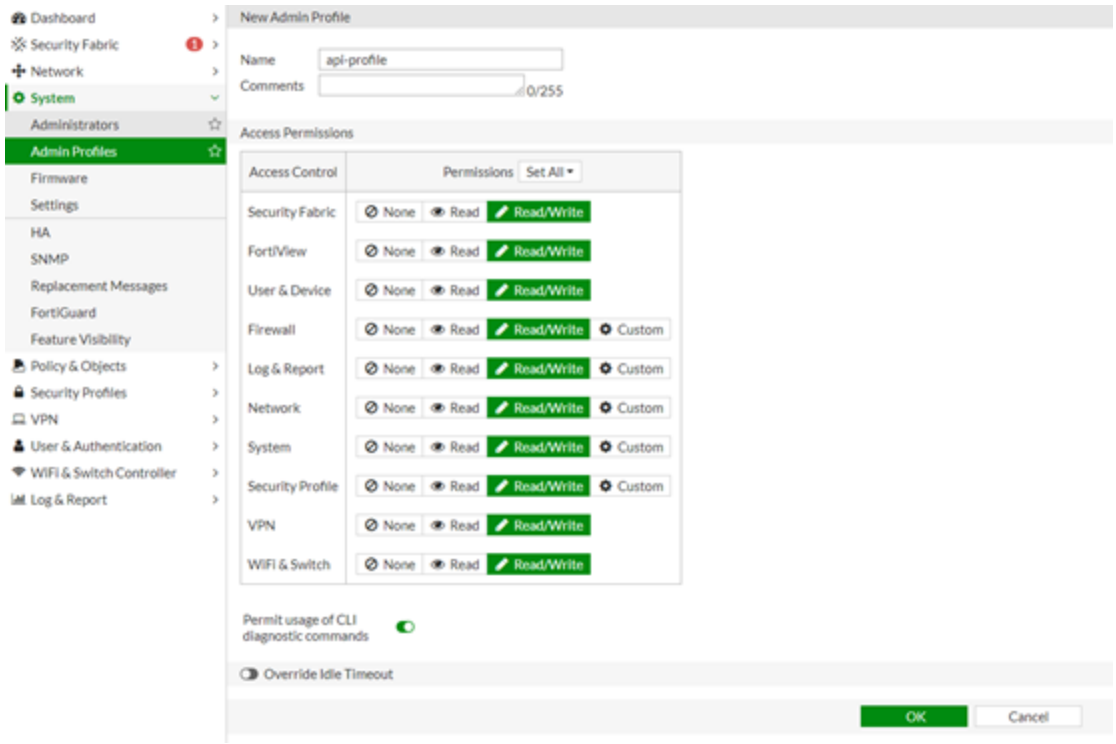
FortiConverter can import configurations through REST-API. Each API request can use an API token to be authenticated.

An API token is generated by creating a new REST API admin on FortiGate GUI.

Create new REST API admin

Step 1: Create an administrator profile

1. On the FortiGate GUI, select **System > Admin Profiles > Create New**.
2. Create a New Profile.
3. Enter a profile name and enable all the **Read/Write** permissions. Please note the profile name, it will be used in **Step 2**.



4. Click **OK**.

Step 2: Set up the global scope in the admin profile:

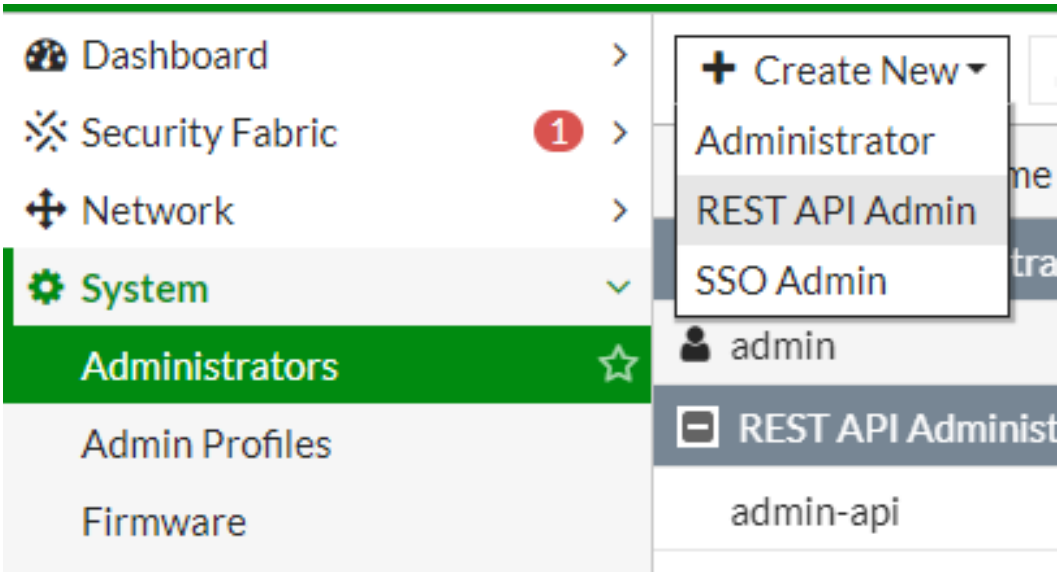
If your device is in multiple VDOM mode, please set the scope of the admin profile into "global":

1. Open the CLI console.
2. Input the following commands:

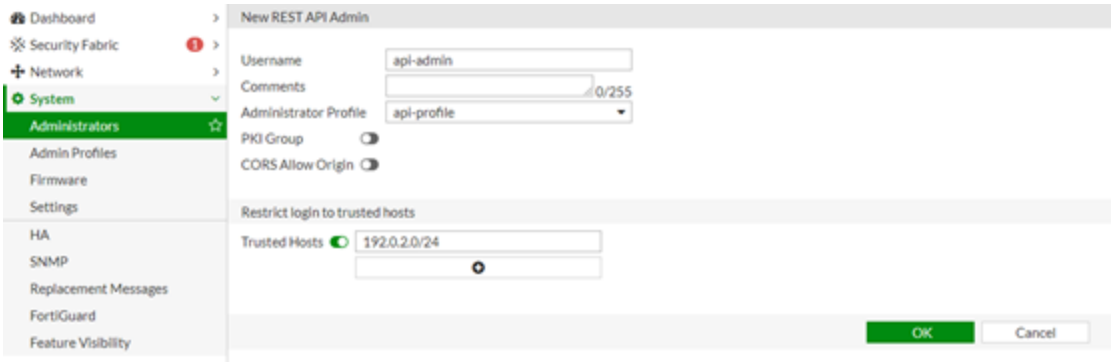
```
config global
   config system accprofile
      edit <your admin profile>
         set scope global
      next
   end
end
```

Step 3: Create a REST API Admin:

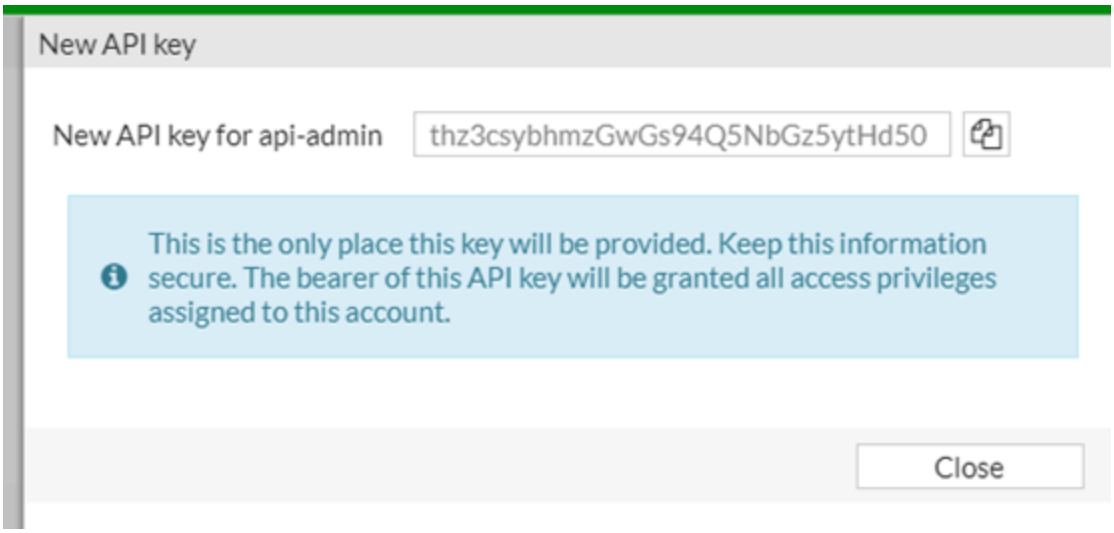
1. On the FortiGate GUI, select **System > Administrators > Create New > REST API Admin**.



2. Enter the API-user's name and select the profile name you created from **Step 1**.
3. The trusted host must be specified to ensure that the machine of your FortiConverter installed can reach the FortiGate.



4. Click **OK** and an API token will be generated.



5. Make a note of the API token as it's only shown once and cannot be retrieved.
6. Click **Close** to complete creation of the REST API Admin.

Regenerate an API token for API-user:

In FortiGate GUI, go to **System > Administrators**.

1. Edit your REST API admin user
2. Click **Regenerate**.

In CLI console, use the CLI command below:

```
execute api-user generate-key [API user name]
```

The steps above must be performed from the FortiGate GUI as an administrator with the **super_admin** profile.

Next: Connecting FortiGate devices on page 279

Connecting FortiGate devices

Before REST API imports, FortiConverter needs to connect to FortiGate devices first. The connected devices can be used as the source devices of FortiGate migration or the target devices of REST API imports.

Please follow the steps below to connect your devices to FortiConverter.

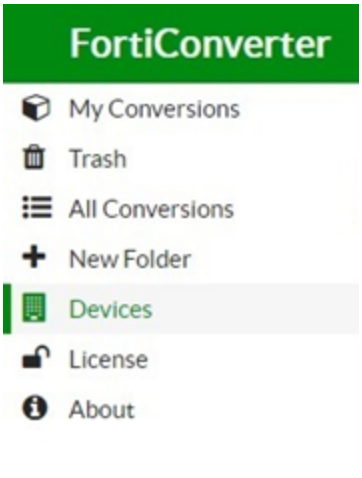
There're two ways to authenticate your REST API request:

- Username/Password
- API-Token.

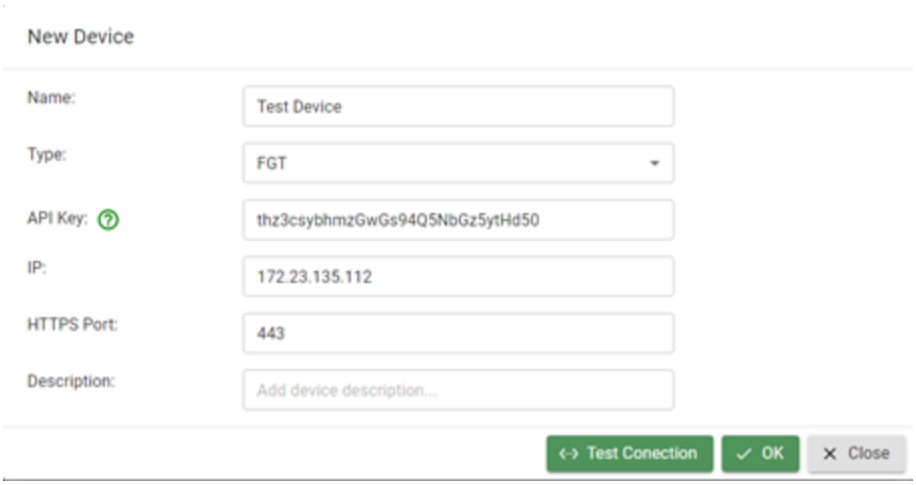
To use API-Token authorization, please follow steps in Create new REST API admin on page 275.

Please note that the devices with FortiOS v5.2 or older are not valid devices for REST API feature because minimium REST APIs are supported in those FortiOS versions.

1. Go to the FortiConverter dashboard and click the tab **Device** in the left side.



2. Click the button **New Device** at the top-right corner.
3. Input the network address and Token authorization information. If the HTTPS port of the device is changed by the command `config system global -> "set admin-sport"`, please fill in the field `HTTPS port`.



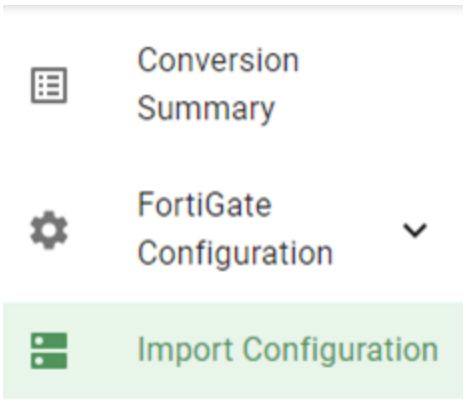
4. Click **Test Connection** to see if the device can be connected and authenticated.
5. Click **OK** to save the device information.

Import config to FortiGate via RESTful APIs

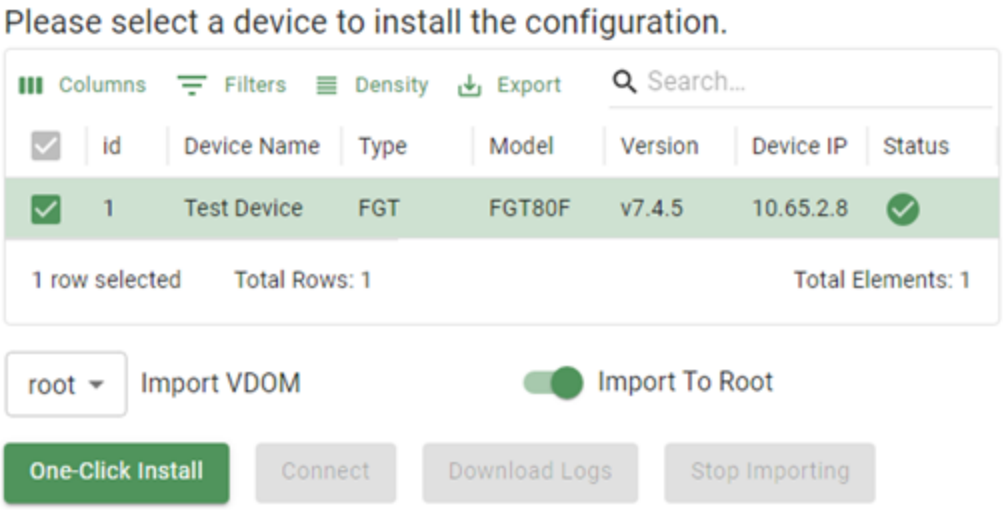
FortiConverter can use REST API provided by FortiOS to import the converted objects from 3rd party vendors into your FortiGate.

Start Installation

1. In the tuning page of the conversion, click **Install Config** at the top-right corner or **Import Configuration** on side bar. This button would exist only when there is at least one connectable device saved in FortiConverter.



2. Select the device to be imported and click **Connect**.
3. Click **One-Click Install** to start importing.



Multiple VDOM: If there are multiple VDOMs in the converted configuration, users can select the VDOM to be imported. When selecting to import "All VDOMs", all VDOMs would be created in the connected device, and all objects would be imported.

Single VDOM: When users select a single VDOM, an option "Import To Root" would show up. When this option is enabled, the objects in the VDOM would be imported to the root VDOM of the connected device. Otherwise, the VDOM would be created.

Root VDOM: If the converted result has only the root VDOM, the options above would not show up.

Special Case: In Snort conversion, FortiConverter would detect the VDOM in the connected device automatically, and users can select the IPS custom rules are imported to which VDOM.

4. View the installation logs and wait for the importing to be completed.
5. To interrupt the installation, click **Stop Importing** to stop the installation.
6. If an object failed to be imported because it contains invalid values, then it can be edited by clicking the icon **Edit**.

After editing the object, it can be imported again by clicking the icon **Import**.

7. **Download Logs** can be clicked to download the log file of importing. The CLI of failed objects would be printed in the file, and user can copy and paste the CLI into the terminal of the device to see what error occurs.

View Import Result

When the REST API import is finished, the statistic of imported objects would be shown in the table of conversion summary page.

VDOM	Object Name	Detected	Import Success	Import Failed
root (18)				
	Interface	11	11	0
	Zone	0	0	0
	Address	849	848	1
	Address Group	143	142	1
	Service	93	93	0
	Service Group	169	169	0
	VIP	44	44	0
	VIP Group	0	0	0
	Central NAT	7	7	0
	IP Pool	1	1	0
	Schedule	0	4	0
	Schedule Group	0	0	0
	Policy	354	353	1
	Route	26	26	0
	User	52	52	0
	User Group	1	1	0
	VPN Phase 1	6	6	0
	VPN Phase 2	7	7	0

By clicking the number in the **Import Failed** column, the failed objects would be listed in a table. In the table of each kind of object, the import result would be shown in the right column.

VDOM	Group Name	Members	Comments	Import Status
	Airwatch_Remote	n-199.106.140.0_23 h-202.80.1...		✓
	DM_INLINE_NETWORK_9	h-10.0.98.178 h-10.0.98.85		✓
	DM_INLINE_NETWORK_90	h-10.0.24.115 h-10.0.24.116 h-...		✓
	Blacklisted_Sites	h-123.114.240.33 h-60.191.80....	Blacklisted_Sites	✗
	BranchSupport_PCs	h-10.0.98.100 h-10.0.98.134 h-...		✓

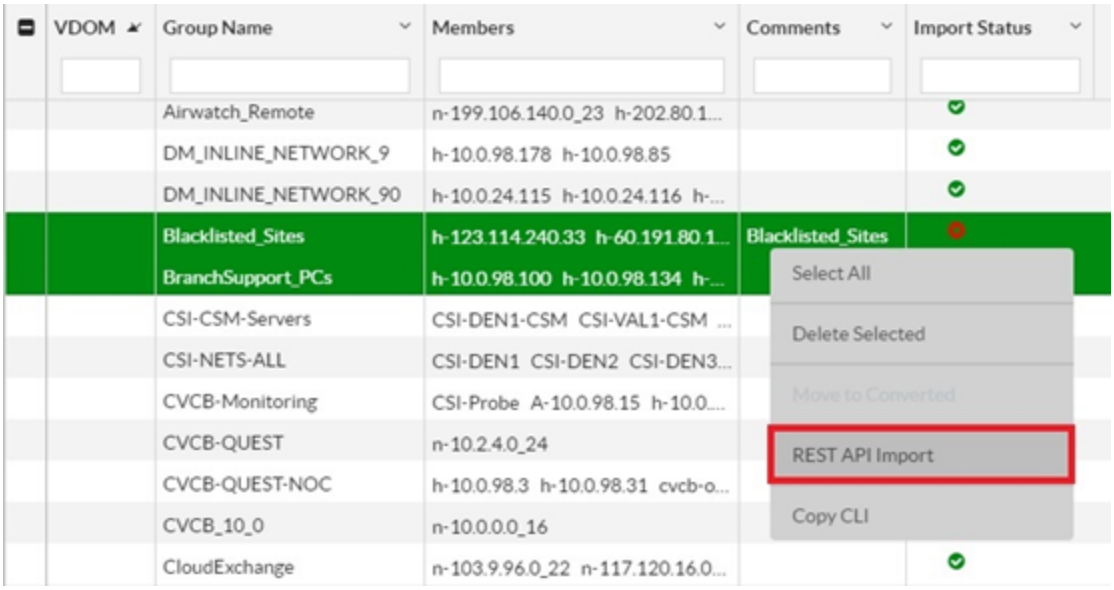
Import Individual objects

Users can also import objects individually in the object pages.

1. Select objects to be imported into the FortiGate.
2. Right click and select **REST API Import**.

It should be reminded that the prerequisite objects should be imported at first.

For example, before importing an address group, all the address objects inside the address group should be imported.



Import config to FortiGate by restoring migrated file

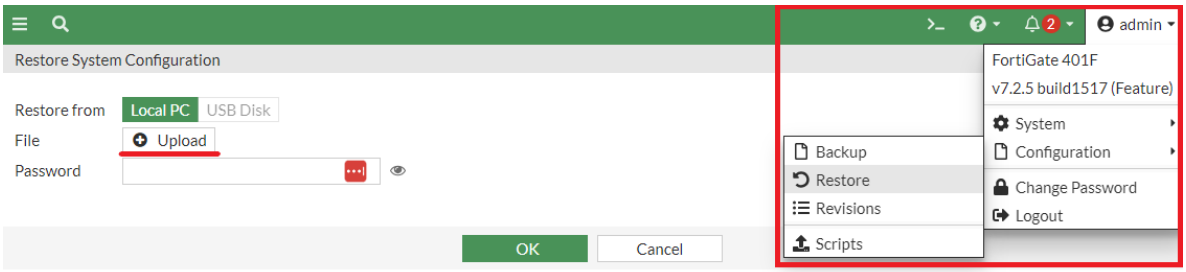
This section is only valid for FortiGate to FortiGate conversion.

Restoring the migrated file

After migrated file from FortiConverter is saved locally, please open the target FortiGate Web GUI and follow the steps below:

1. In the upper-right corner, click **admin -> Configuration -> Restore** to access **Restore System Configuration**.

2. In **Restore System Configuration**, click **Upload** and upload your converted file.



3. Wait for the system to reboot.

CLI debugging

After the system is rebooted, connect to the console and input this CLI command to review the error logs of the restoration:

```
diagnose debug config-error-log read
```

```
diagnose debug config-error-log read
>>> "set" "dlp-sensor" "[redacted]" @ 7717:firewall.policy.101000:value parse error (error -3)
>>> "set" "dlp-sensor" "[redacted]" @ 7732:firewall.policy.102000:value parse error (error -3)
>>> "set" "dlp-sensor" "[redacted]" @ 7747:firewall.policy.103000:value parse error (error -3)
>>> "set" "dlp-sensor" "[redacted]" @ 7792:firewall.policy.106000:value parse error (error -3)
>>> "set" "dlp-sensor" "[redacted]" @ 7807:firewall.policy.107000:value parse error (error -3)
>>> "set" "dlp-sensor" "[redacted]" @ 7824:firewall.policy.108000:value parse error (error -3)
>>> "set" "dlp-sensor" "[redacted]" @ 7839:firewall.policy.149000:value parse error (error -3)
```

The error logs show the information about the command line, line number, config path, and the error description.

For example, for this error log:

```
>>> "set" "dlp-sensor" "test" @ 7717:firewall.policy.101000:value parse error
    (error -3)
```

The error log description is as the following:

Error Log Section	Description
"set" "dlp-sensor" "test"	The command line "set dlp-sensor test" is failed to be imported.
7717	This command line is the 7717th line in the restored configuration file.

firewall.policy.101000	This command is located in the following config path:
	`config firewall policy`
	`edit 101000`
	`set dlp-sensor "test"`

value parse error (error -3)	The system returned error description. It is recommend to input the command again manually in the console for a more detailed error message.

The error message shown in the error log is usually unclear. Please manually run the CLI command again for a more detailed error message. In this example, the error is generated due to DLP sensors are no longer referenced in the newer version.

Import config to FortiGate by upload CLI scripts file

This section is only valid in 3rd party vendor to FortiGate conversion.

Conversion to FortiGate output

When you convert a source configuration to a FortiGate configuration, the resulting conversion files are placed into the directory FGT/ folder. File `config-all.txt` contains all converted CLI configuration, and all kinds of objects are also output into divided files such as `02-config-system-interface.txt` and `04-config-firewall-address.txt`.

Preparing the output configuration file for import

Before you import the output configuration, search the file for any comments that indicate issues that FortiConverter detected during the conversion (such as missing objects or conflicting object values) and fix them. To locate these comments, search for lines that start with # (number/hash symbol). You can't successfully import the configuration if you don't fix these issues.

Importing the configuration file sections

To import the sections of the output configuration file(s), please go to the admin dropdown menu in the top right corner, and then select **Configuration > Scripts > Run Script** to upload and run the CLI scripts file

Fortinet also recommends you not to import the file `config-all.txt` directly, but import each divided configuration such as `02-config-system-interface.txt` and `04-config-firewall-address.txt` separately instead. This makes troubleshooting easier if an error occurs.

A section of configuration cannot be successfully imported if an object it references doesn't already exist in the configuration. For example, interfaces, addresses, users, services, IPsec phase1 objects should be imported before policies being imported. To prevent this kind of failure, please import the configuration sections following the order given in the script file name. For example, import file `01-config-system-settings.txt` firstly and import `02-config-system-interface.txt` secondly. This order ensures that all the referenced objects exist when a configuration section is imported.

CLI debugging

To make troubleshooting easier when there are import errors, before you import sections, enable CLI

debugging.

By default, CLI debugging is level 3. This is the level to use under normal conditions.

You can use this command to view the current debug level:

```
# diagnose debug info
```

A response similar to the following appears:

```
debug output: disable
console timestamp: disable
console no user log message: disable
CLI debug level: 3
```

For the configuration importing process, the appropriate debug level is 8. Use this command to change the debug level:

```
diag debug enable
diag debug CLI 8
```

When the import process is complete, use this command to return the debug level to the default (3):

```
diag debug reset
```

Importing process

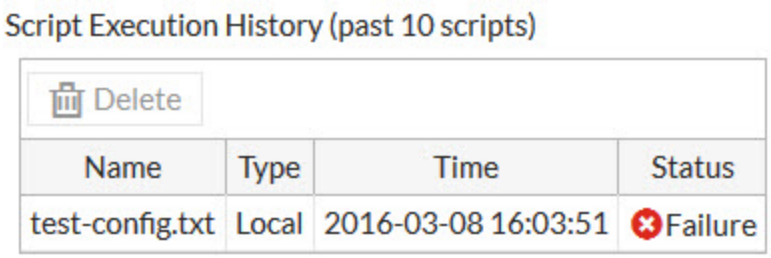
Import the sections of the conversion output systematically. For each section you import, check for import failures in the web UI Script Execution History. Use CLI debugging to diagnose and fix any errors. When the import is successful, continue with to next section of the configuration.

Example import error and troubleshooting

The following simple configuration generates an error because Test3 isn't defined:

```
config firewall address
   edit "Test1"
      set subnet 1.1.1.1 255.255.255.255
   next
   edit "Test2"
      set subnet 1.1.1.2 255.255.255.255
   next
end
config firewall addrgrp
   edit "Test-Addresses"
         set member "Test1" "Test2" "Test3"
   next
end
```

When you save this configuration as a file and import it, the Failure status indicator shows:



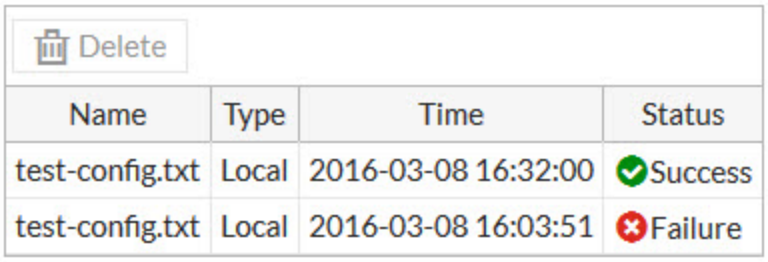
The following CLI output captures detailed information about the error:

```
0: config firewall address
0: edit "Test1"
0: set subnet 1.1.1.1 255.255.255.255
0: next
0: edit "Test2"
0: set subnet 1.1.1.2 255.255.255.255
0: next
0: end
0: config firewall addrgrp
0: edit "Test-Addresses"
-3: set member "Test1" "Test2" "Test3"
1: next
0: endwrite config file success, prepare to save in flash
```

The error code `-3` indicates that FortiGate did not find the object and the return code `1` indicates that an error occurred.

Notice that FortiGate creates the address objects Test1 and Test2. The failure status only relates to the address group.

When you fix the script by adding the missing Test3 object and import it again, the Success status indicator shows.



When the configuration is fixed, all return codes in the CLI debugging are 0, indicating no errors.

```
0: config firewall address
0: edit "Test1"
0: set subnet 1.1.1.1 255.255.255.255
0: next
0: edit "Test2"
0: set subnet 1.1.1.2 255.255.255.255
0: next
0: edit "Test3"
0: set subnet 1.1.1.3 255.255.255.255
0: next
0: end
0: config firewall addrgrp
```

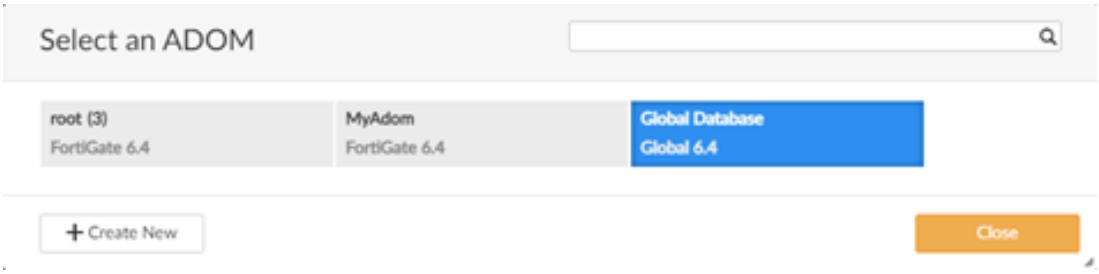
```
0: edit "Test-Addresses"
0: set member "Test1" "Test2" "Test3"
0: next
0: endwrite config file success, prepare to save in flash
```

Import config to FortiManager by upload CLI scripts file

The example in the procedures uses FortiManager 6.4 and global policies and objects. The procedures are similar for environments that don't use the global feature.

To configure FortiManager

On FortiManager, enable the ADOM feature and create an ADOM for each source domain that you want to migrate.Ensure that all the ADOMs (including the global ADOM) use the same version of FortiOS.



The output folder

The output folder provides a global folder and a folder for each source domain. Both folders contain the subfolder `FMGR\`.

Object configuration is located in the `FMGR\FWObject\` folder, which contains the following files:

- Several text and HTML files that are used for reporting. They aren't used to import the configuration.
- The text file `config-all` , which contains all the CLI commands for the object configuration.
- Text files that duplicate sections of the `config-all` file: `addresses`, `address groups`, `services`, `schedules`, and so on. When there are many objects (for example, most environments have many firewall address objects), these sections are divided into multiple, indexed files. To make the import process simpler, Fortinet recommends that you import configurations using the files for individual sections.

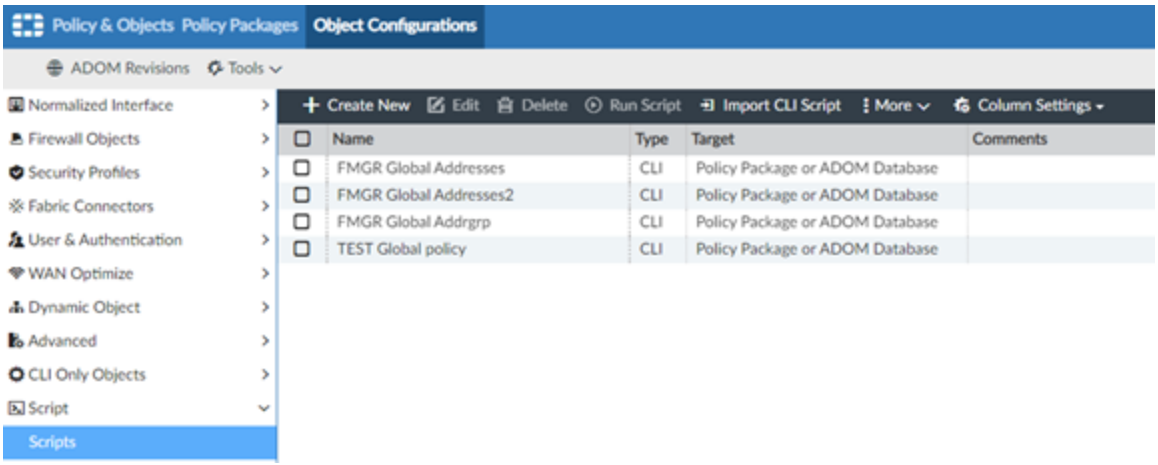
Policy scripts are located in policy package folders in `\FMGR\Policy` as one or more firewall policy files (`config-firewall-policy-1`, `config-firewall-policy-2`, and so on).These files are the same content as the conversion output file `config-all` in smaller, indexed files that are easier to import.

Configuration which relates to interfaces are located in `FMGR\DeviceList\` folder, including `interfaces, zones, static routes and dynamic interfaces` configuration.

To import policies and objects

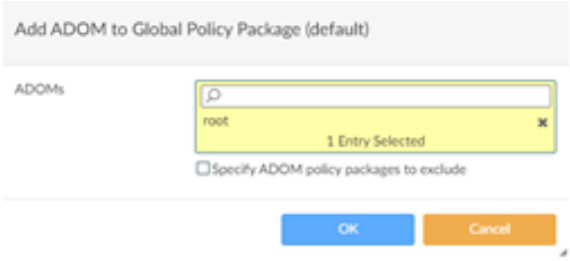
Import to Global Database

1. Display the scripts in the panel: from the **Policy & Objects** page, go to **Tools > Display Options > All On**.
2. Go to the script page: **Object Configurations > Script > Scripts**.

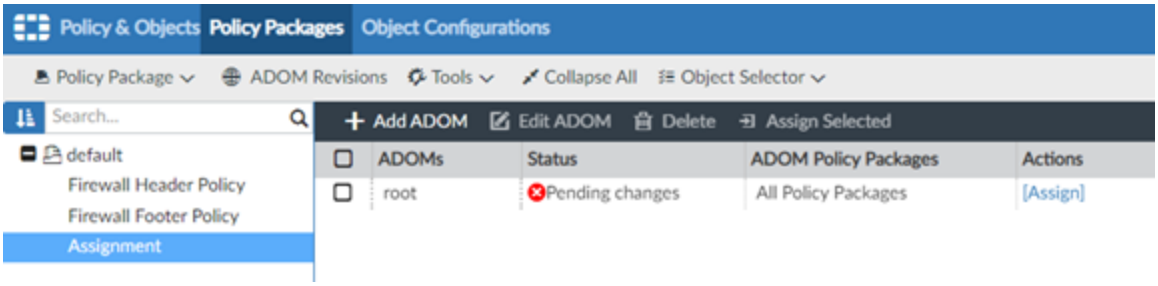


3. Click **Import CLI Script** and add a script file in the folder `FMGR\FWObject` on the page. Edit the script name, select **Policy Package or ADOM Database** for the field **Run Script On** and then click Import to save the script.
   For more information on the output folders and files, see The output folder on page 288.
4. On the table of scripts, select the imported script and click **Run Script**. For those object definition scripts, choose the policy package "default", the imported objects are sharable to all policy packages. Click **Run Now** to start running the script file.
5. If the script fails, click **View Details** to review error messages. For more information, see To troubleshoot script import and execution errors on page 292
6. Repeat the script import and run process for all scripts in `the Global\FMGR\FWObject` folder. If there are many address or service objects, there would be multiple scripts because the address file is split and indexed to keep the files at a manageable size.Please import the configuration sections following the order given in the script file name. For example, import file `04-config-firewall-address.txt` before importing `05-config-firewall-addrgrp.txt` since addresses would be referenced by address groups.
7. When all the objects are imported, policy packages can be imported. Use the same procedures to import and run the policy scripts using files `config-global-header-policy` and `config-global-footer-policy` located in the `Global\FMGR\Policy` folder, which contains a folder for each policy package.
8. After the scripts have run successfully, review the policies.

9. When the policy packages are correct, click **Assignment > Add ADOM** to assign it to your ADOM. By default, FortiManager assigns the selected policy package to all policy packages in the ADOM.



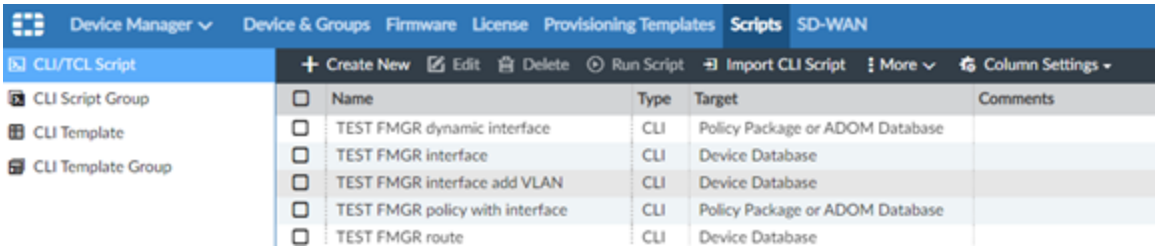
10. To complete the ADOM assignment, on the selected ADOM, click **Assign**.



11. Switch to the assigned ADOM and review the assigned global policies.

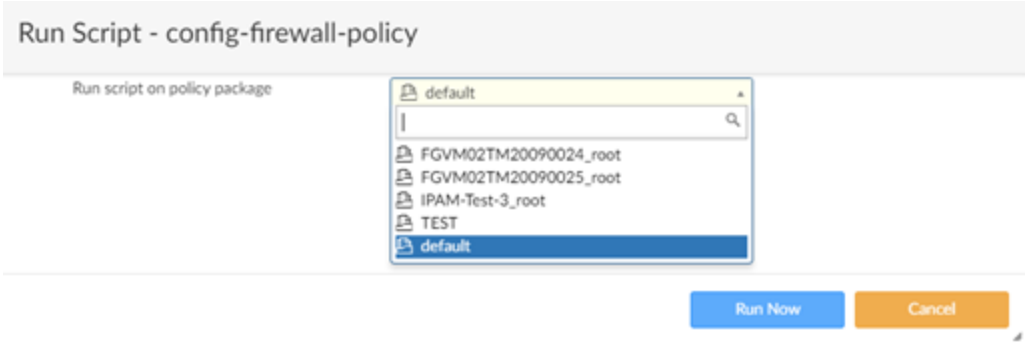
Import To ADOMS

1. Display the scripts in the panel: on the **System Settings** page, go to **Admin > Admin Settings**. Under **Display Options on GUI**, select **Show Script**.
2. Go to the script page: on the **Device Manager** page, Click on **Scripts**.



3. Follow steps 3-6 in Import to Global Database on page 289 to import the firewall object scripts in folder `<domain_name>\FMGR\FWObject`.
4. When all the objects are imported, please check if there are interfaces referenced in the policies. If policy is needed, please follow the steps in Import To Managed Device on page 291 and import the interface scripts in folder `<domain_name>\FMGR\DeviceList`.
   To create referenced interfaces on the **Policy & Objects** page, go to **Policy & Objects > Object configurations > Normalized interface > Normalized interface > Create New.**
5. When the objects and interfaces are imported, policy packages can be imported. If there are multiple policy packages to be imported, go to **Policy Packages > Policy Package > New** to create new policy packages other than the default one.
6. Use the same procedures to import and run the policy scripts using file `config-firewall-policy` located in the `<domain_name>\FMGR\Policy` folder, which contains a folder for each policy package. Remember to select the corresponding policy package after clicking **Run Script**. If there are many

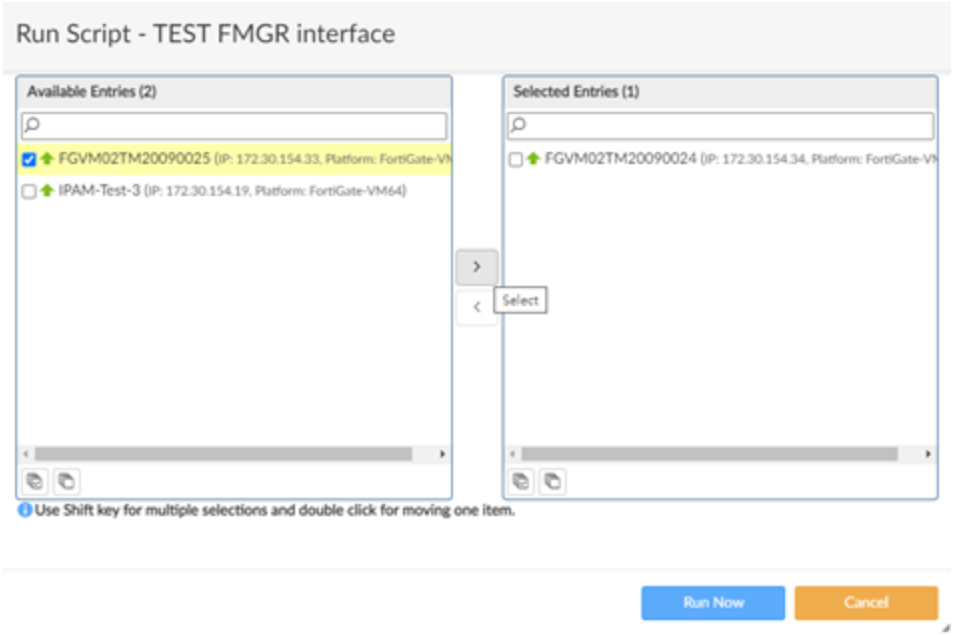
policies, there would be multiple scripts because the policy file is split and indexed to keep the files at a manageable size.



7. If the script fails, click **View Details** to review error messages. For more information, see To troubleshoot script import and execution errors on page 292
8. After the scripts have run successfully, review the policies.

Import To Managed Device

1. Follow step 1-2 in Import To ADOMS on page 290 to enter the script page.
2. Click **Import CLI Script** and add a script file in the folder `FMGR\DeviceList` on the page. Edit the script name, select **Device Database** for the field **Run Script On** and then click **Import** to save the script.
   For more information on the output folders and files, see The output folder on page 288.
3. On the table of scripts, select the imported script and click **Run Script**. Select the device which the script applies to and click **Run Now** to start running the script file.



4. If the managed device names have been inputted during the conversion, then the dynamic interface mapping file `config-dynamic-interface` would be generated. This script maps the interfaces in a managed device to the normalized interfaces in the ADOM database. If the normalized interfaces have not

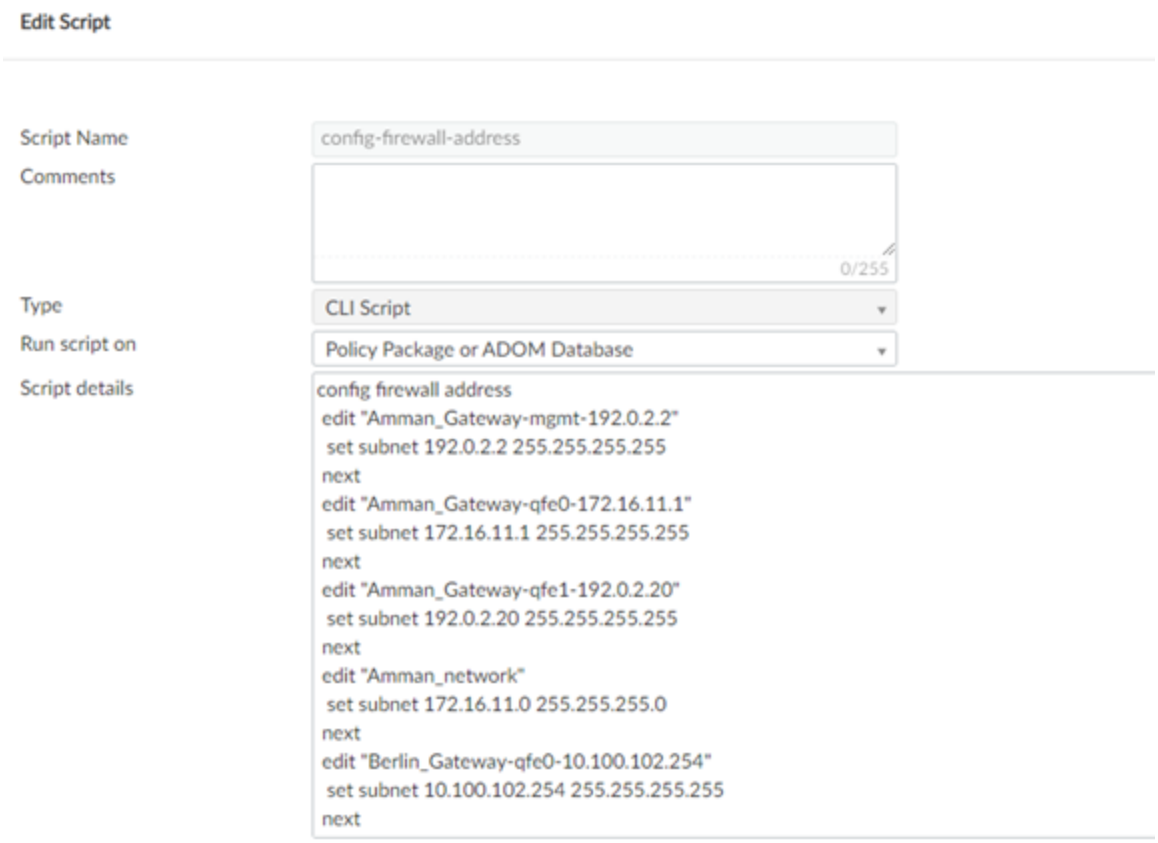
been created in the ADOM database, then this script also creates them.

5. After the scripts have run successfully, review the imported settings.

To troubleshoot script import and execution errors

FortiConverter inserts error messages in output scripts as comments.

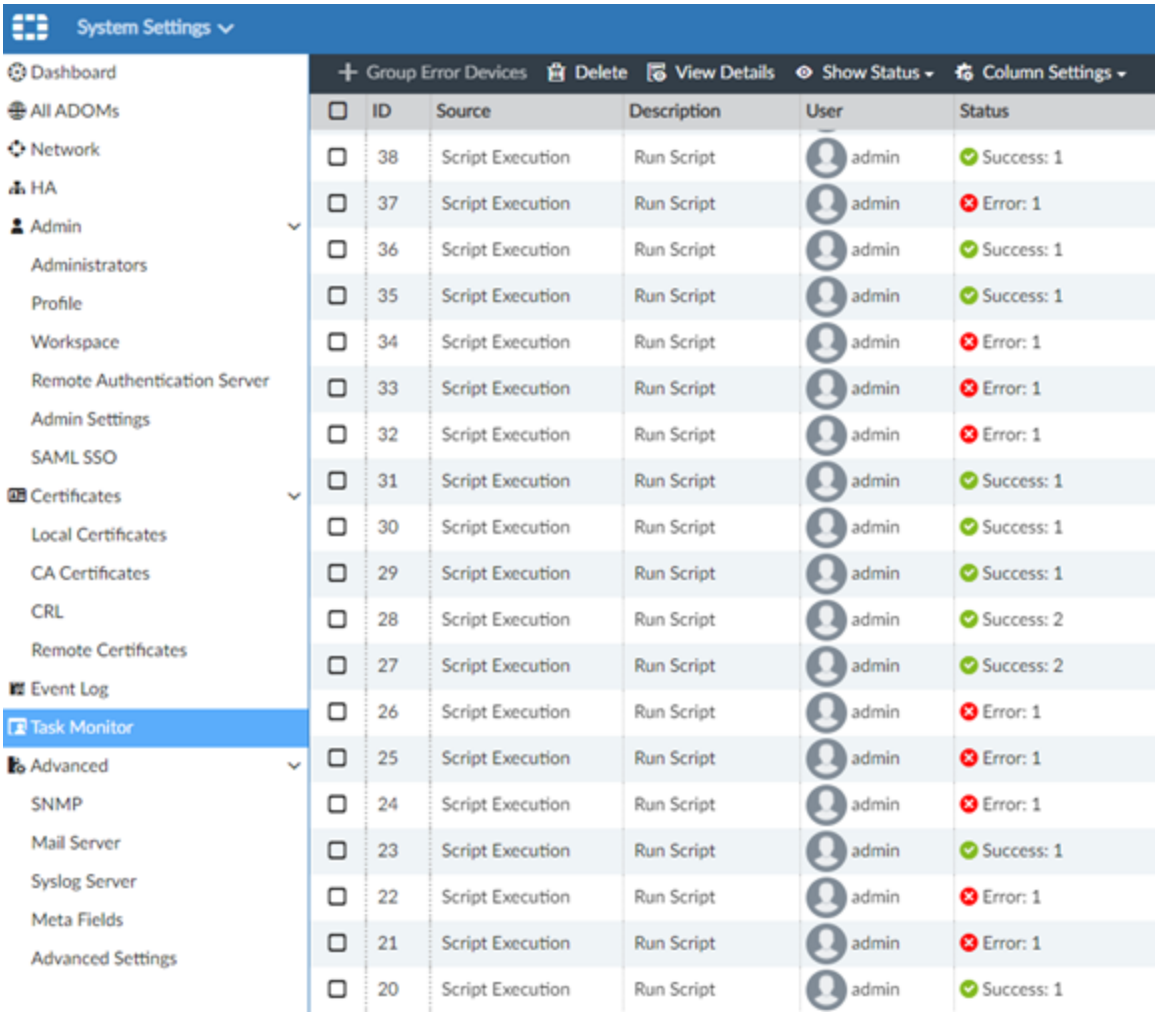
In some cases, the script can't run unless you edit it to correct the errors. Double-click the name of the script in the list of scripts to edit it.



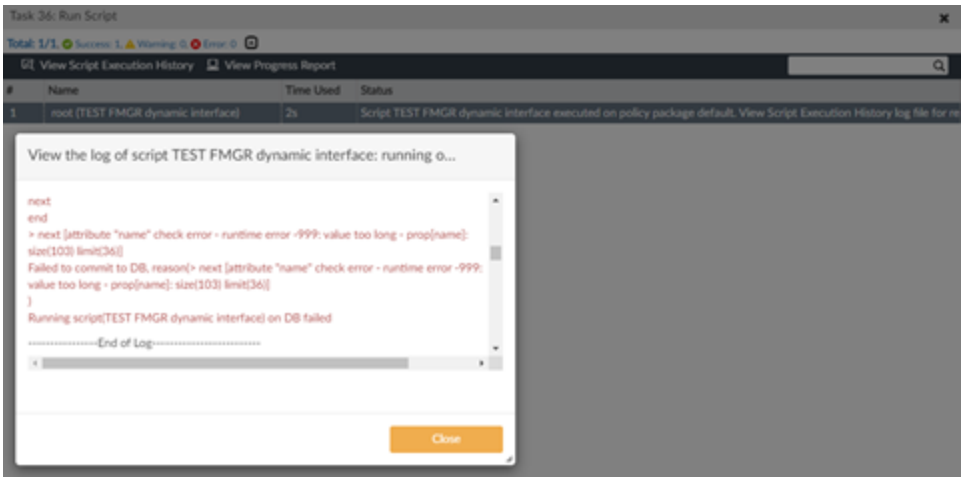
In the following example, the address objects that generate the errors are assigned using the global objects and can be ignored.

```
next
edit "
 set n
 # Error: Undefined address object "
next
edit "gV
 set me
 # Error: Undefined address object "ge
next
edit "globa
 set memb
 # Error: Undefined address objec
next
end
```

If an error occurs during script execution, on the page **System Settings**, click **Task Monitor** to view the error message and identify the error. Unlike a FortiGate import, which creates an object up to the point of failure, FortiManager does not create object or policy if the script execution fails.



Double click the records of script failure, and the error message can be found in the column status. For detailed error logs, click **View Script Execution History**.



Once the cause of the error is identified through the error log, please go back to the script page and fix the script. If the object which cause the problem is unnecessary, you can delete it or use #(hash) at the start of the appropriate lines to convert them to comments. Then, try to run the script again. Repeat the troubleshooting process until the script execution is successful.

If there is no obvious error in the output, try dividing the script into two smaller scripts. If only one script runs successfully, you have narrowed the focus of your troubleshooting to the content of the failed script. To divide a script, right-click it and select **Clone**. Using the policy numbers to determine and keep track of which policies you delete, edit the files so that they each contain a different section of the script. Then, run both scripts.

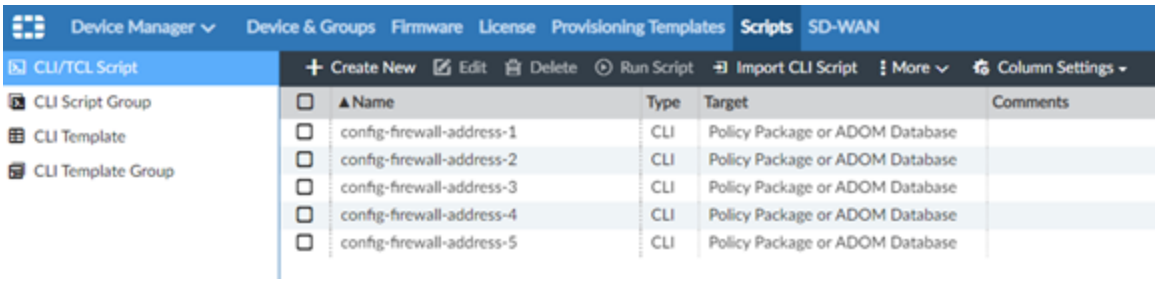
Dividing scripts into two or more smaller scripts is also useful if you suspect the length of a script is causing the execution to fail. Scripts that are too long fail without generating an error message.

In some cases, if a script fails, Fortinet recommends that you create a new script instead of editing or deleting it, because sometimes files can remain after you delete it. If you preserve the failed script, you can review it and the error it generates later. In the following example, the following `config user server` objects took several attempts to run successfully.

service1	CLI	Policy Package, ADOM Database
service2	CLI	Policy Package, ADOM Database
session-helper	CLI	Device Database
user-servera	CLI	Policy Package, ADOM Database
user-serverb	CLI	Policy Package, ADOM Database
user-serverc	CLI	Policy Package, ADOM Database

Working with object output in indexed files

In some cases, output files are split into smaller, indexed files to make it easier to import them.



If a configuration contains nested groups, script execution can fail because groups defined in one file are dependent on groups defined in another file.

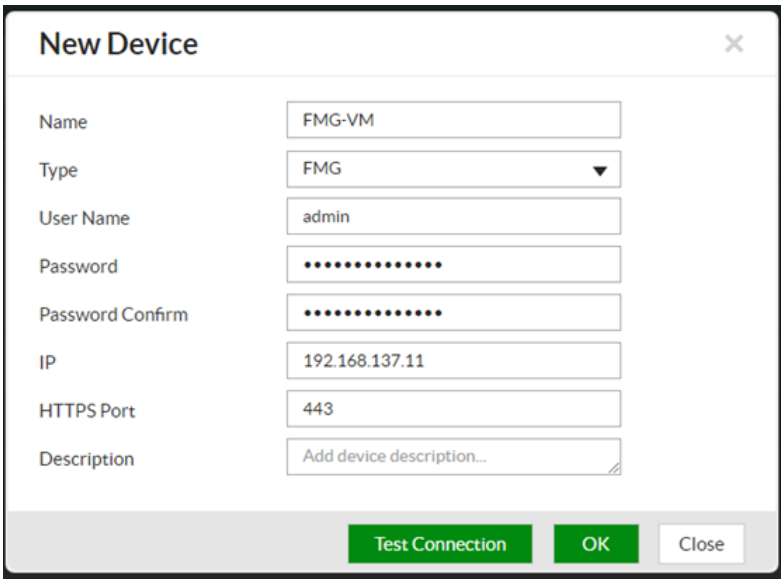
If a script fails because of a missing dependency, remove the object that causes the failure. When you have finished importing the scripts for the object type, delete the script you edited and import it again. Then, run the script without editing it. Because the dependency is now included in the imported configuration, the unedited script can execute successfully.

Import Config to FortiManager via RESTful APIs

FortiConverter can use REST API to import the converted objects from 3rd party vendors into your FortiManager.

Before the Installation

1. 1. Please create a new FMG device connection on the Device page.



2. After creating the necessary device connection, please start a new conversion and select **FortiManager** as the output format.

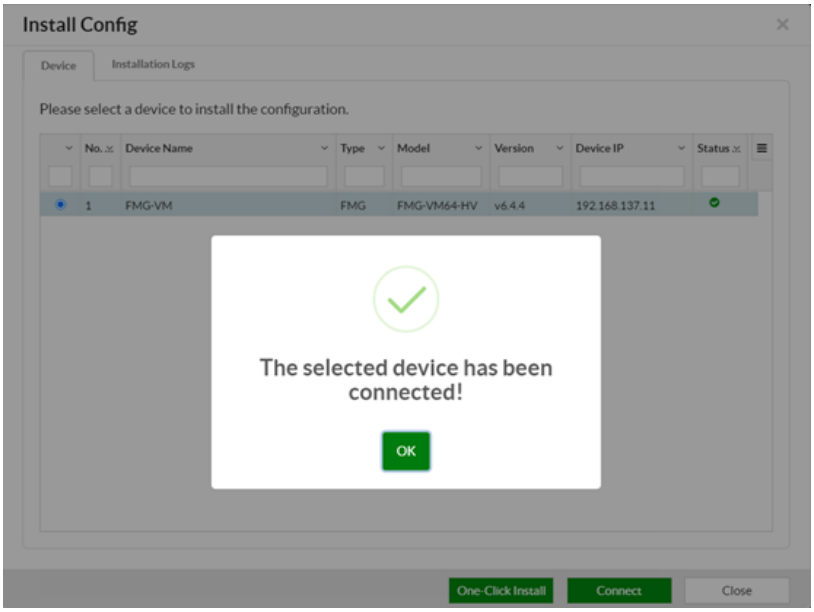
3. Complete the conversion and enter the conversion summary page.
4. You can choose either to install all config at once or one-by-one on each tuning page.

Please Note:

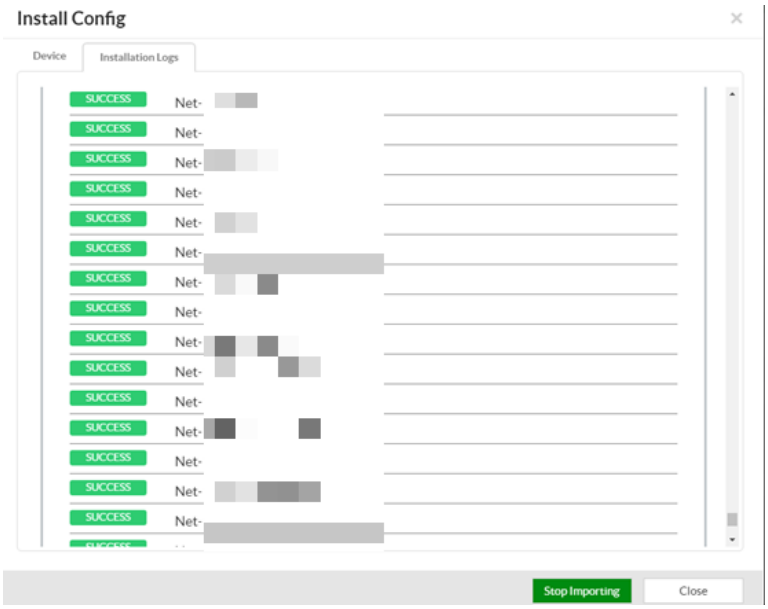
- REST API Import does not support importing dynamic mapping on normalized interface. Please manually tune the interface mapping on the FortiManager.
- FortiConverter does not support VPN objects importing or converting to VPN Manager nodes on FortiManager.

Start Installation

1. On the tuning page of the conversion, click **Install Config** at the top-right corner. This button would exist only when there's at least one connectable device saved in the FortiConverter.
2. Select the FMG device to be imported and click **Connect**.



3. Click **One-Click Install** to start importing.
4. View the installation logs and wait for the importing to be completed.
5. To interrupt the installation, click **Stop Importing** to stop the installation.



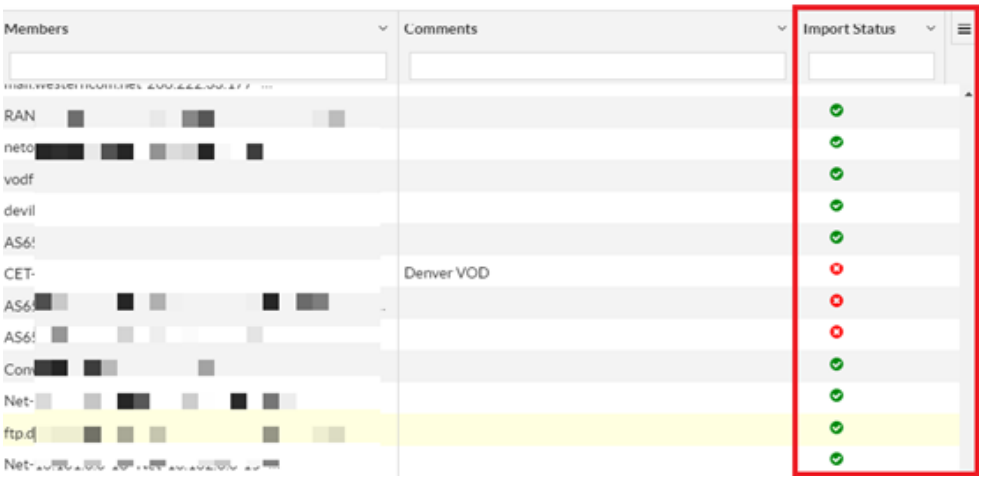
6. **Download Logs** can be clicked to download the log file of importing. The CLI of failed objects would be printed in the file, and users can upload the CLI script onto the device to see what error occurs.

View Import result

When the REST API import is finished, the statistics of imported objects would be shown in the conversion table summary page.

VDOM	Object Name	Detected	Overlength	Import Success	Import Failed
Global (18)					
	Interface	0	0	0	0
	Zone	0	0	0	0
	Address	623	0	623	0
	Address Group	15	0	15	0
	Service	51	0	51	0
	Service Group	2	0	2	0
	VIP	0	0	0	0
	Central NAT	0	0	0	0
	IP Pool	0	0	0	0
	Schedule	0	0	0	0
	Schedule Group	0	0	0	0
	Policy	33	0	31	1
	Route	0	0	0	0
	User	0	0	0	0
	Server	4	0	4	0
	User Group	1	0	1	0
	VPN Phase 1	0	0	0	0
	VPN Phase 2	0	0	0	0

The failed objects would be listed in a table by clicking the **Import Failed** row. For each object, the import result would be shown in the right column.



Import Individual object

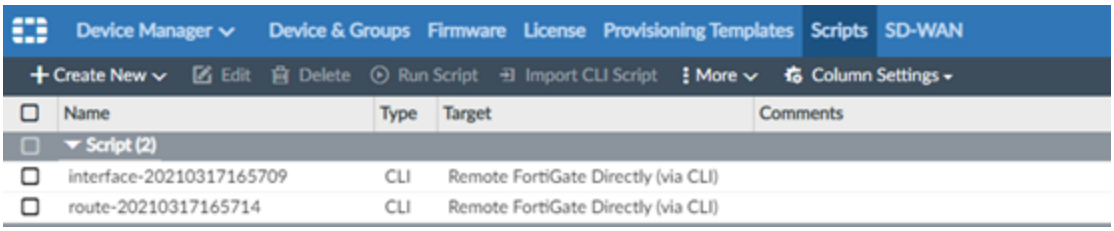
Users can also import objects individually in each object tuning page.

1. Select objects to be imported into the FortiManager.
2. Right click and select **REST API Import**.

Review on the FortiManager

In the **Policy & Objects** page, you can see objects and policy packages to be imported onto FortiManager database.

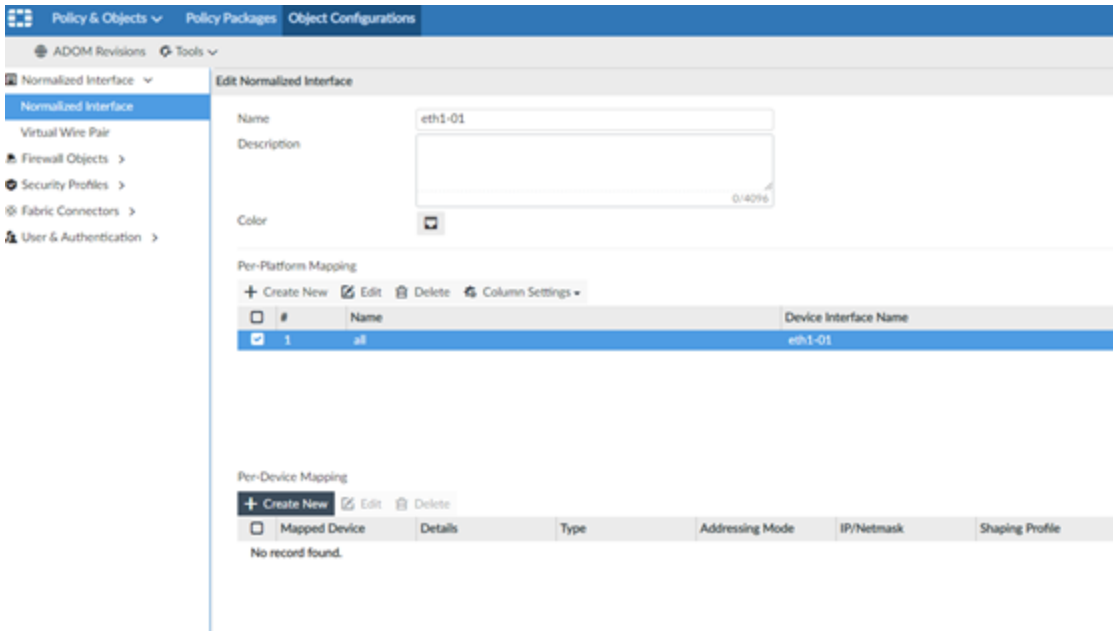
For Device Configuration, please go to **Device Manager**, you can see the device CLI script is listed by category plus a timestamp.



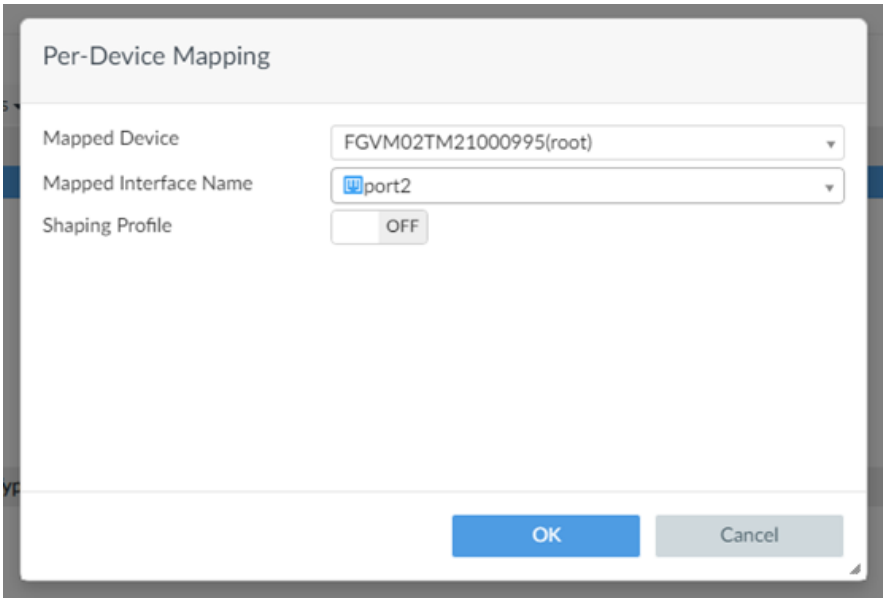
Config dynamic mapping on normalized interface

Before configuring your dynamic mapping, add your managed device to the Device Manager and upload the necessary Device CLI via Scripts page.

1. On the normalized interface, select the normalized interface you would like to create the dynamic mapping.



2. On the Pre-Device Mapping, click on the **Create New**.
3. Select the mapped device you added on the device manager and mapped interface.



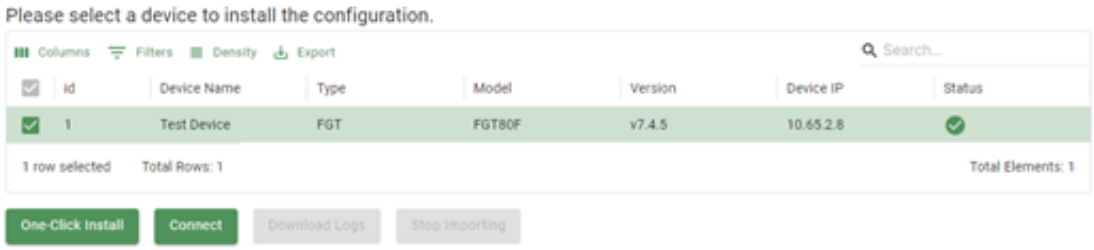
4. Click **OK** to complete the mapping.

Import config to FortiProxy via RESTful APIs

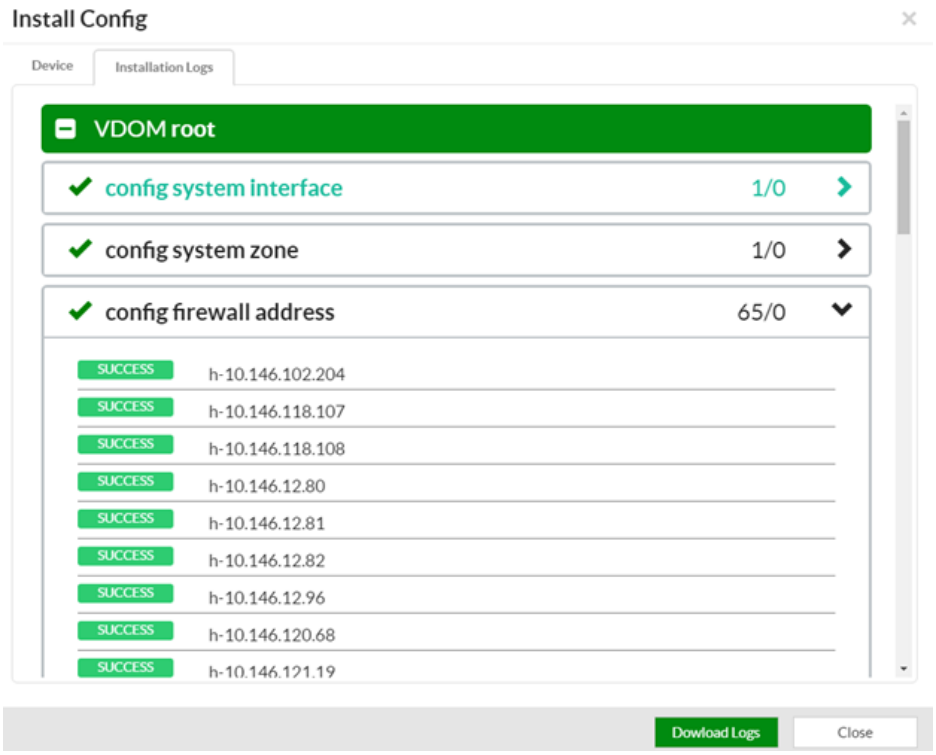
FortiConverter can use the REST API provided by FortiOS to import the converted objects from Bluecoat conversions into your FortiProxy.

Start Installation

1. In the tuning page of the conversion, click **Install Config** at the top-right corner. This button would exist only when there is at least one connectable device saved in FortiConverter.
2. Select the device to be imported and click **Connect**.
3. Click **One-Click Install** to start importing.



4. View the installation logs and wait for the importing to be completed.
5. To interrupt the installation, click **Stop Importing** to stop the installation.



6. **Download Logs** can be clicked to download the log file from importing. The CLI of failed objects would be printed in the file, and the user can copy and paste the CLI into the terminal of the device to see what error occurs.

View Import Result

When the REST API import is finished, the statistics of imported objects would be shown in the conversion summary page.

Connected Device: aerte

VDOM	Object Name	Detected	Import Success	Import Failed
root (14)				
	Interface	1	1	0
	Zone	1	1	0
	Address	489	65	0
	Address Group	64	0	0
	Proxy Address	1601	0	0
	Proxy Address Group	24	0	0
	Service	2	0	0
	Service Group	1	0	0
	Schedule	0	0	0
	Schedule Group	0	0	0
	Proxy Policy	27	0	0
	User	0	0	0
	Server	0	0	0
	User Group	0	0	0

By clicking the number in the **Import Failed** column, the failed objects would be listed in a table. In the table of each kind of object, the import result would be shown in the right column.

VDOM	Group Name	Members	Comments	Import Status
	Airwatch_Remote	n-199.106.140.0_23 h-202.80.1....		✓
	DM_INLINE_NETWORK_9	h-10.0.98.178 h-10.0.98.85		✓
	DM_INLINE_NETWORK_90	h-10.0.24.115 h-10.0.24.116 h-...		✓
	Blacklisted_Sites	h-123.114.240.33 h-60.191.80....	Blacklisted_Sites	✗
	BranchSupport_PCs	h-10.0.98.100 h-10.0.98.134 h-...		✓

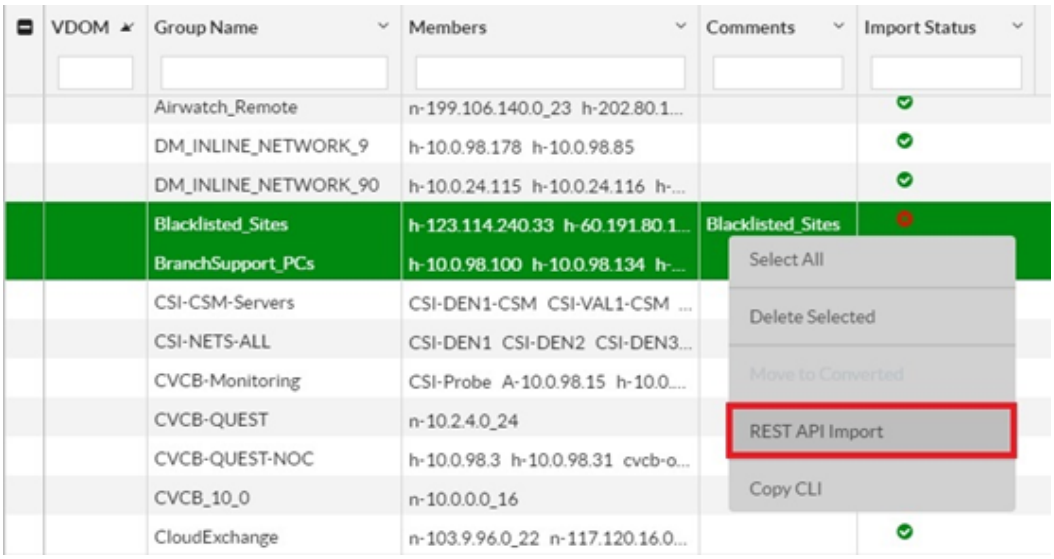
Import Individual objects

Users can also import objects individually in the object pages.

1. Select objects to be imported into the FortiProxy.
2. Right click and select **REST API Import**.

It should be reminded that the prerequisite objects should be imported first.

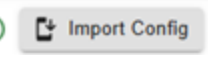
For example, before importing an address group, all the address objects inside the address group should be imported.



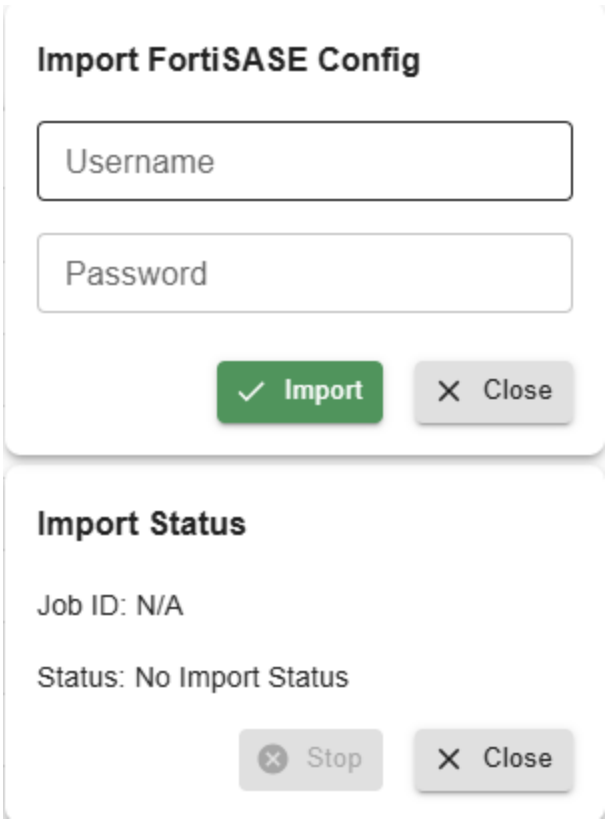
Import Config to FortiSASE with API User Credentials

For **Zscaler** conversion, FortiConverter can import the JSON format outputs into FortiSASE instance.

Initiation of Import Job

1. Click 

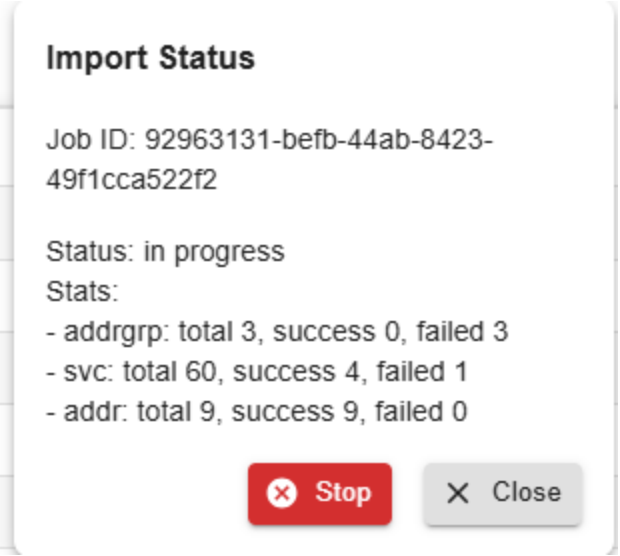
from the Conversion Summary page.
2. Input API user credentials:



3. Click **Import** to initialize the import job

View Import Result/Status

Import job status and object importing stats can be checked from the lower section of the Import job popup window



Terminate a Running Import Job

Please click **Stop** button to terminate the current running job.

Manual Configuration Migration Prerequisite

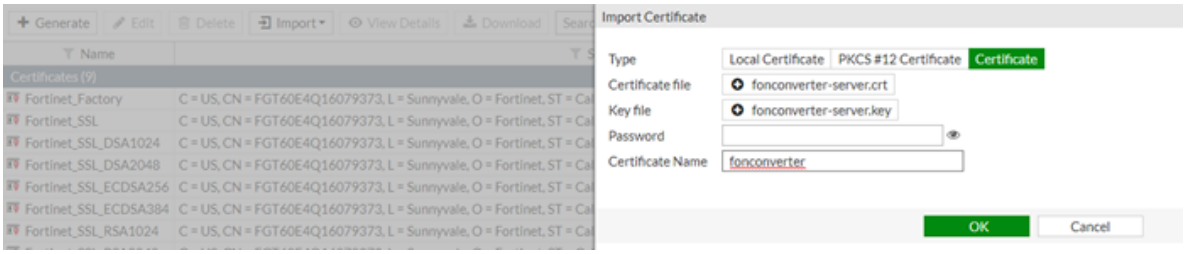
Some configurations cannot be converted by FortiConverter but need to be configured manually. Please follow the steps below to import certificates and migrate FortiToken to new device.

Import your Certificate

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

Steps to import the signed certificate into your FortiGate:

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.

Migrate FortiToken

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.

Troubleshooting

For any questions not covered in this content, contact FortiConverter customer support at fconvert_feedback@fortinet.com.

Licensing Issues

FortiConverter is a single-user application. Using more than one user account may invalidate the Hardware ID. If multiple users require the application, Fortinet recommends that you install it using a single, shared account, on a remotely accessible host.

- A hardware layer change generates a new hardware identifier. For a physical host, this could occur when installing the application on a new laptop, or installing a memory extension or a new network card. For a virtual host, such as VMware, the hardware identified may change because of an update in the virtualization software, or because of a change to the virtual hardware configuration for that virtual host.
- Windows updates might affect the hardware ID, particularly .Net framework updates.
- If your license does change, contact customer services, cs@fortinet.com, include your serial number, previous hardware identifier, and new hardware identifier. Customer services can update your FortiCare records and you can then download the replacement license from the support portal.

Accessing conversion logs

In most cases, when FortiConverter has an internal problem, the application displays a message in the web UI and adds an error message to a log file.

The logs capture all the conversion steps, including initialization, parsing (two logs), conversion, and reporting.

If the log indicates that FortiConverter encountered an internal error, or for help resolving other errors, contact the FortiConverter team at fconvert_feedback@fortinet.com.

Conversion Logs

Log location

The log of FortiConverter is stored at the following location ("AppData" is a hidden folder):

```
C:\Users\<Windows user name>\AppData\Roaming\Fortinet\FortiConverter
```

Log file "syslog.txt" is the log file of the application.

Normal log records

[2019-10-23 13:39:00,665] [INFO] --- --Start new conversion "TEST"---

[2019-10-23 13:39:00,666] [INFO] --- Vendor: SonicWALL Model:

[2019-10-23 13:39:00,666] [INFO] --- ---Starting Parse process---

[2019-10-23 13:39:00,815] [INFO] --- Parsing input configurations

[2019-10-23 13:39:01,294] [INFO] --- ---Parse completed---

[2019-10-23 13:39:01,298] [INFO] --- ---Save conversion completed---

[2019-10-23 13:39:11,630] [INFO] --- ---Starting convert process---

[2019-10-23 13:39:11,631] [INFO] --- Converting source configuration

[2019-10-23 13:39:11,634] [INFO] --- Converting domain root

[2019-10-23 13:39:12,247] [INFO] --- Start tuning job…

[2019-10-23 13:39:12,509] [INFO] --- Start nat tuning job…

[2019-10-23 13:39:12,518] [INFO] --- Start nat merge…

[2019-10-23 13:39:12,519] [INFO] --- Start nat merge parallelizer

[2019-10-23 13:39:19,897] [INFO] --- Nat tuning for policy package: root

[2019-10-23 13:39:21,338] [INFO] --- Merging policies with NAT rules…

[2019-10-23 13:39:24,544] [INFO] --- Process id 18252 nat merge and optimize all done

[2019-10-23 13:39:24,721] [INFO] --- Process id 13956 nat merge and optimize all done

[2019-10-23 13:39:24,820] [INFO] --- Process id 8044 nat merge and optimize all done

[2019-10-23 13:39:28,597] [INFO] --- Clean up objects by policy reference…

[2019-10-23 13:39:30,498] [INFO] --- Saving NAT merged policy…

[2019-10-23 13:39:32,782] [INFO] --- ---Conversion complete---

[2019-10-23 13:39:33,797] [INFO] --- ---Getting tuning data---

[2019-10-23 13:40:11,105] [INFO] --- Report: FGT

Log with error

[2019-10-23 13:37:29,963] [INFO] --- --Start new conversion "TEST"---

[2019-10-23 13:37:29,964] [INFO] --- Vendor: SonicWALL Model:

[2019-10-23 13:37:29,964] [INFO] --- ---Starting Parse process---

[2019-10-23 13:37:30,045] [INFO] --- Parsing input configurations

[2019-10-23 13:37:30,393] [INFO] --- Parser failed.

[2019-10-23 13:37:30,398] [ERROR] --- Parse failed.

Traceback (most recent call last):

File "C:\Users\<Windows use name>\Documents\FortiConverter\NewApplication\Django\backend\mysite\applications\converter\models\convert_job.py", line 112, in do_convert_for_first_phase raise Exception (engine_invoker.get_err_message(result))

Exception: Input Parameter Error

[2019-10-23 13:37:30,407] [ERROR] --- Parse request failed.

[2019-10-23 13:37:30,408] [INFO] --- ---Parse completed---

[2019-10-23 13:37:30,411] [INFO] --- ---Save conversion completed---

Troubleshooting application crashes

In many cases, disabling NAT merge options can resolve an application crash that occurs during a conversion.

For example, for a Cisco PIX conversion, on the wizard Start Option page, click **More**, and then for each type of NAT, select **Off**.

See the FortiConverter logs for detailed information about the cause of a crash. See Accessing conversion logs on page 308.