Comment

Ploera

08-28-2019 07:46 A

Expedition (updated to version 1.1.11)

User Guide

Version 1.2

What is Expedition?

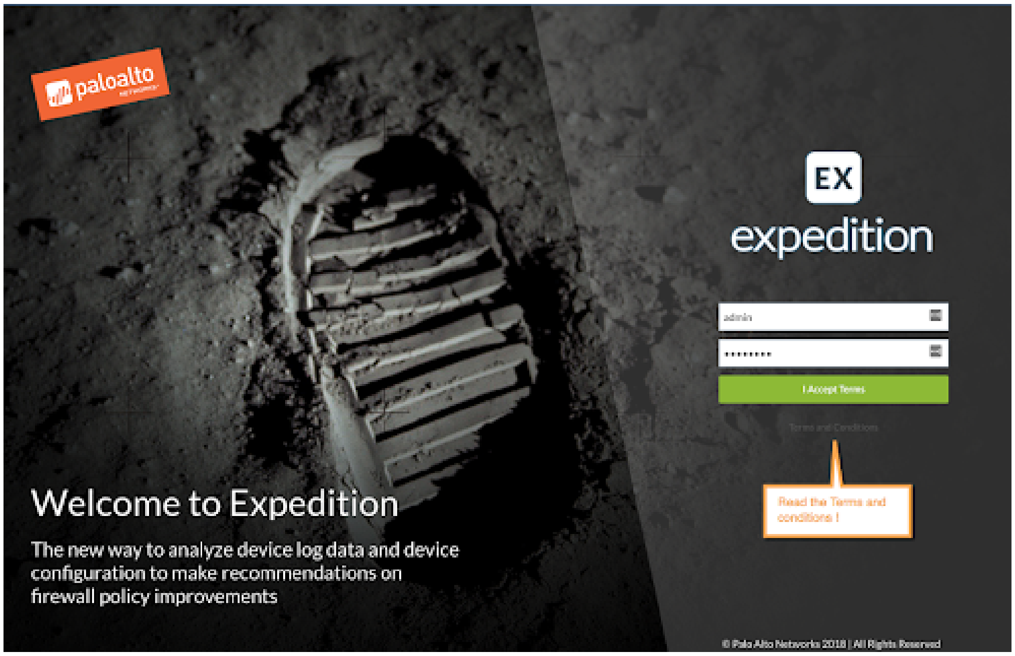
Expedition is the fourth evolution of the Palo Alto Networks Migration Tool. The original main purpose of this tool was to help reduce the time and effort to migrate a configuration from one of the supported vendors to Palo Alto Networks.

By using the Migration Tool, everyone can convert a configuration from Checkpoint or Cisco or any other vendor to a PAN-OS and give you more time to improve the results. Migration Tool 3 added some functionalities to allow our customers to enforce security policies based on App-ID and User-ID as well.

With Expedition, we have gone one step further, not only because we want to continue helping to facilitate the transition of a security policy from others vendors to PAN-OS but we want to ensure the outcome makes use of the most advanced features of the platform to get you closer to the best of the possible configurations. For this reason, we added a **Machine Learning module**, which can help you to generate new security policies based on real log traffic, and we have introduced the **Best Practices Assessment Tool**, which checks whether the configuration complies with the Best Practices recommended by our security experts.

With all these huge improvements, we expect the next time you use Expedition the journey to excellence will be easier.

Login



Read the Terms and conditions !

Welcome to Expedition

The new way to analyze device log data and device configuration to make recommendations on firewall policy improvements

© Palo Alto Networks 2018 | All Rights Reserved

Login From the Web Interface

Web Interface Login

This is only referencing the access via web interface

Username	**admin**
Password	**paloalto**

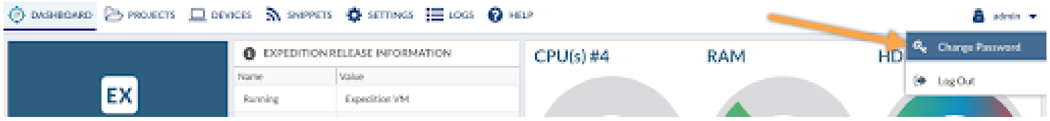
SECURITY WARNING: We encourage you to change the username and password after your first login.

Changing default credentials

As a best practice, we recommend that you change the default credentials as soon as possible (DP – upon first log in)

Web Interface Login

After you log in via the web browser, follow these instructions to change the password for the “admin” user.

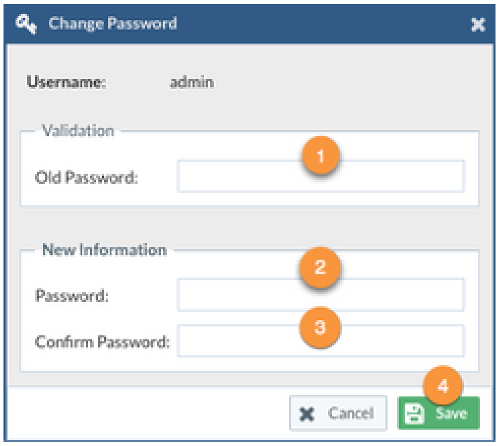


Name	Value
Running	Expedition VM

A new window to change the password will be shown:

1. Type the current password
2. Type NEW password
3. Re-type NEW password
4. Click on Save

Remember the password length has to be at least 10 characters long.



Let’s Migrate

Expedition can help you migrate pieces of configuration from other security vendors and import them into a Palo Alto Networks configuration. The goal is to reduce time and mistakes. Expedition results always need to be reviewed by a professional with knowledge of the vendor that has been migrated and with Palo Alto Networks technologies as well.

There is no easy button that magically converts a configuration from any vendor to Palo Alto Networks without applying the right methodologies and using qualified people.

Migration Workflow

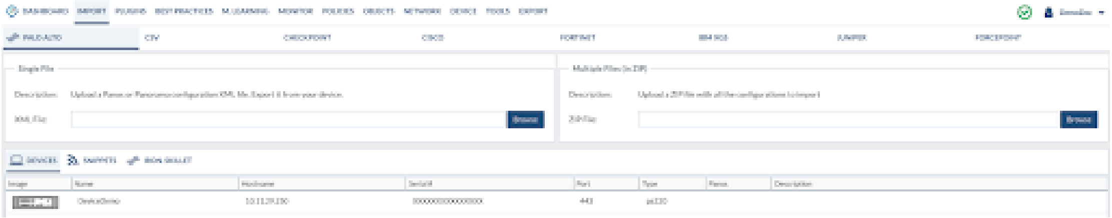
The migration workflow applies to all the vendors we support:

a. Import a Configuration (from a supported vendor)
b. Export Unused Objects Report
c. Remove Unused
d. Clean Invalid Objects
e. Rename, Remap Interfaces to PAN-OS Naming Convention
f. Import a Base Configuration (Palo Alto Networks configuration from the device that you are migrating to)
g. Move Objects From the Configuration Migrated to the Base Configuration.
h. Merge
i. Remove Duplicates (if any)

j. Generate the Output (XML, SET Commands, API Calls)

First step will be always creating a Project, then enter the project by double-click on it.

Importing a configuration into the project



Description: Upload a Panos or Panorama configuration XML file. Export it from your device.
XML File:

Description: Upload a ZIP File with all the configurations to import
ZIP File:

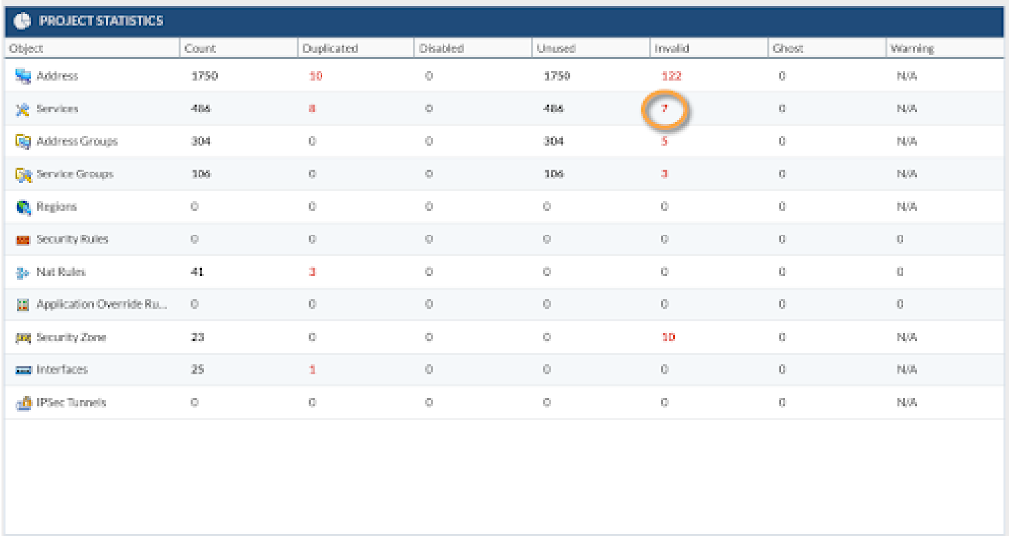
Image	Name	Hostname	SerialId	Port	Type	Panos	Description
	DeviceDemo	10.11.29.150	XXXXXXXXXXXXXXXX	443	pa220		

Expedition can read from different sources. For more specific insights on each vendor, go to the Appendix at the end of this document. Here we will describe the common procedure to migrate any configuration.

Navigate to the Import Tab and select from what vendor you want to migrate. After the configuration has been imported to Expedition, check for invalid objects and clean them before you move forward.

Project Dashboard

As a good starting point, it's recommended to take a look at the Project Statistics panel. We can search here for invalid, unused, and duplicate objects. We can go straight to review the invalid services by clicking on the number shown under the invalid column for the Services Row. That will move the view to Services, which is located under Objects and will apply a predefined filter to show only the Invalid Services.

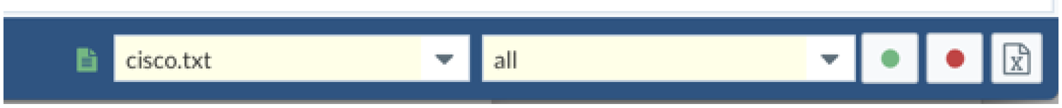


PROJECT STATISTICS

Object	Count	Duplicated	Disabled	Unused	Invalid	Ghost	Warning
Address	1750	10	0	1750	122	0	N/A
Services	486	8	0	486	7	0	N/A
Address Groups	304	0	0	304	5	0	N/A
Service Groups	106	0	0	106	3	0	N/A
Regions	0	0	0	0	0	0	N/A
Security Rules	0	0	0	0	0	0	0
Nat Rules	41	3	0	0	0	0	0
Application Override Ru...	0	0	0	0	0	0	0
Security Zone	23	0	0	0	10	0	N/A
Interfaces	25	1	0	0	0	0	N/A
IPSec Tunnels	0	0	0	0	0	0	N/A

Remove Unused Objects

Before searching how to fix those invalid services, it’s important to remove what was imported but not used in any security or NAT policy. Let's call them unused objects. To remove the unused objects, you have to navigate to the Objects Tab and look at the bottom right bar.



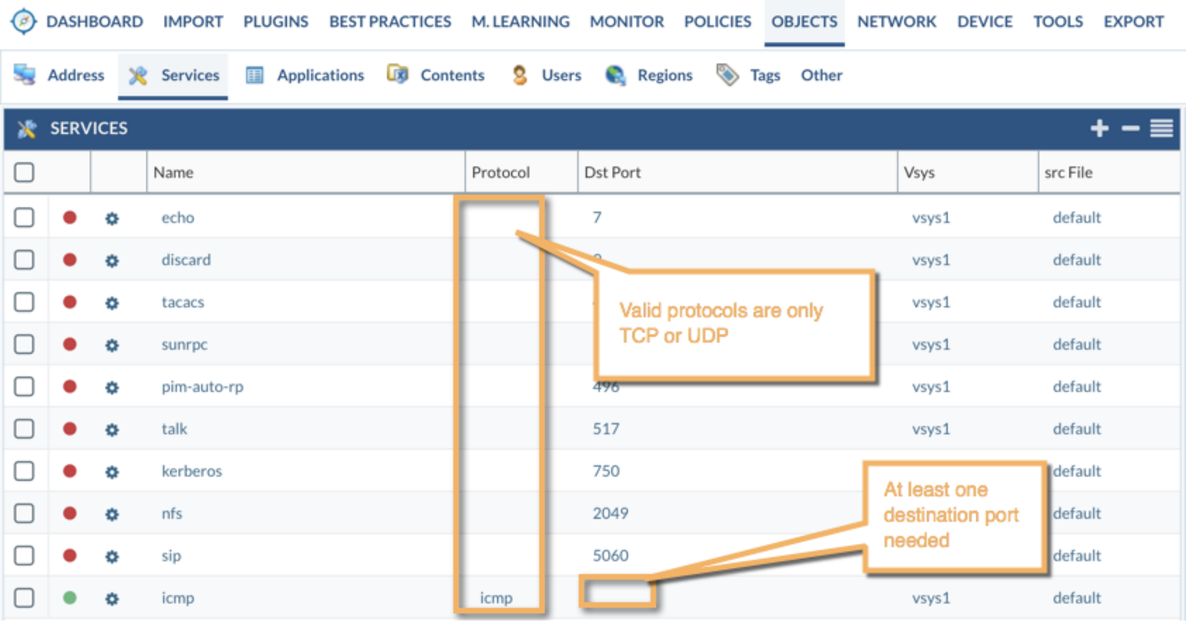
At the very end, you will find three buttons. The green button will recalculate the objects that are defined as used or not used. This should be used after changes have been made on the configuration, so Expedition can recalculate the used objects. The red button is will remove the unused objects from the configuration. The third button with the "X" on it will export a report with all the unused objects.

We recommend exporting the Excel file to track which objects will be removed from the configuration when you click on the red button, and it’s good to keep it for your migration records.

After export the Excel file, click the red button to remove all the unused, and recheck your dashboard to see if you reduced the number of fixes you have to make.

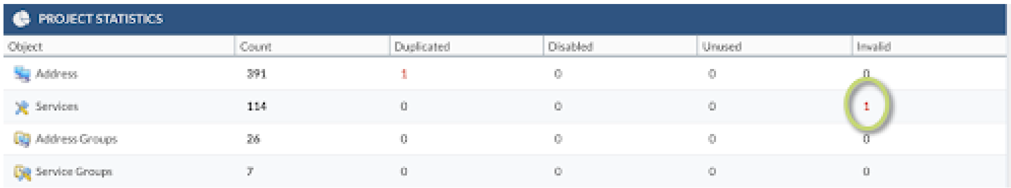
Fixing Invalid Services

Every time you import a configuration from a vendor other than Palo Alto Networks, it's common to have what we call invalid services. We consider invalid services all of those who were based on IP protocols other than TCP or UDP. For example, you can find ICMP services related or IPSec, GRE.



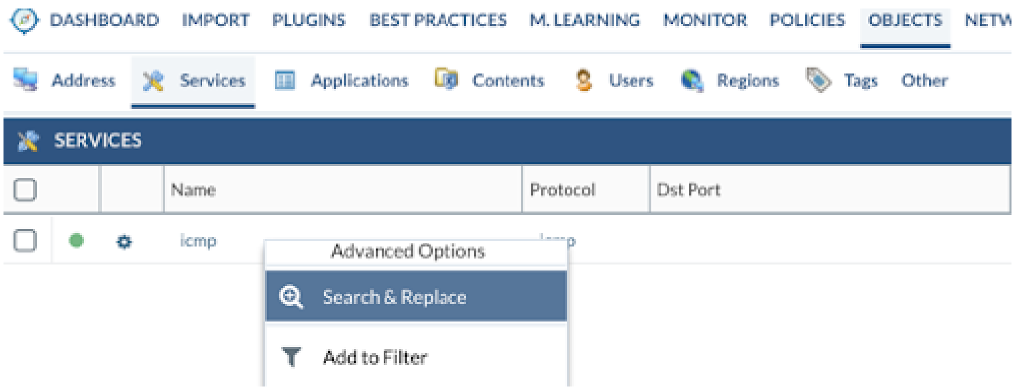
☐			Name	Protocol	Dst Port	Vsys	src File
☐	●	⚙	echo		7	vsys1	default
☐	●	⚙	discard		9	vsys1	default
☐	●	⚙	tacacs			vsys1	default
☐	●	⚙	sunrpc			vsys1	default
☐	●	⚙	pim-auto-rp		496	vsys1	default
☐	●	⚙	talk		517	vsys1	default
☐	●	⚙	kerberos		750		default
☐	●	⚙	nfs		2049		default
☐	●	⚙	sip		5060		default
☐	●	⚙	icmp	icmp		vsys1	default

After we have removed the Unused Objects, only the used ones will be kept for remediation. In the case of invalid services, the only way to fix it, in case the original service was not TCP or UDP, is change it to an App-ID from Palo Alto Networks.



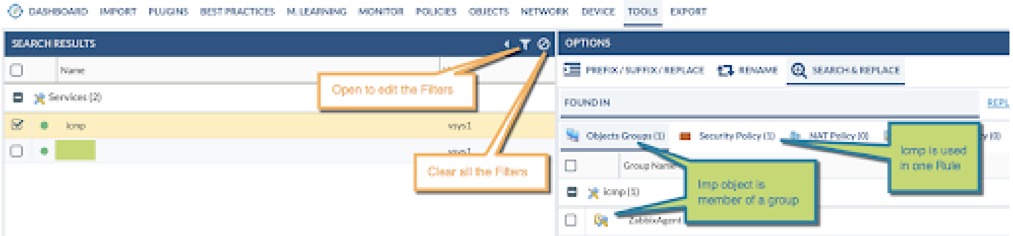
Object	Count	Duplicated	Disabled	Unused	Invalid
Address	391	1	0	0	0
Services	114	0	0	0	1
Address Groups	26	0	0	0	0
Service Groups	7	0	0	0	0

To update the App-IDs, just right-click on the invalid service and click Search and Replace from the advanced menu.



☐			Name	Protocol	Dst Port
☐	●	⚙	icmp	icmp	

This will open up the Tools Tab and show you the Search & Replace Tab. The view is divided in two panels: the left panel shows the output of the applied filters and the right panel will show you where the selected items from the left panel are used.



Open to edit the Filters

Clear all the Filters

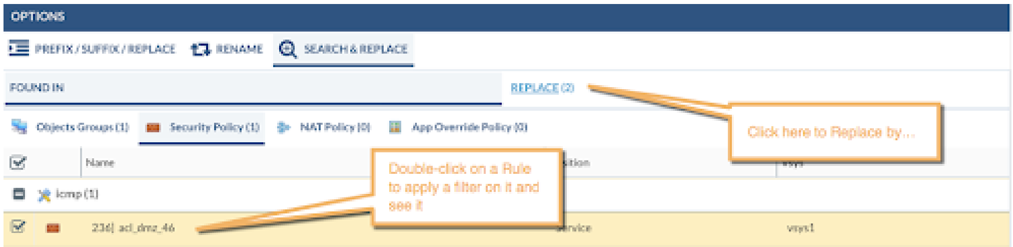
Imp object is member of a group

Icmp is used in one Rule

Replace Services by App-ID

Select the service to be replaced. For instance, in our example, we will select the Group where ICMP was a member and clicked the Replace button located on the bottom bar.

Click Security Policy (1) then select the rule where the service is used and click Replace again.



Click here to Replace by...

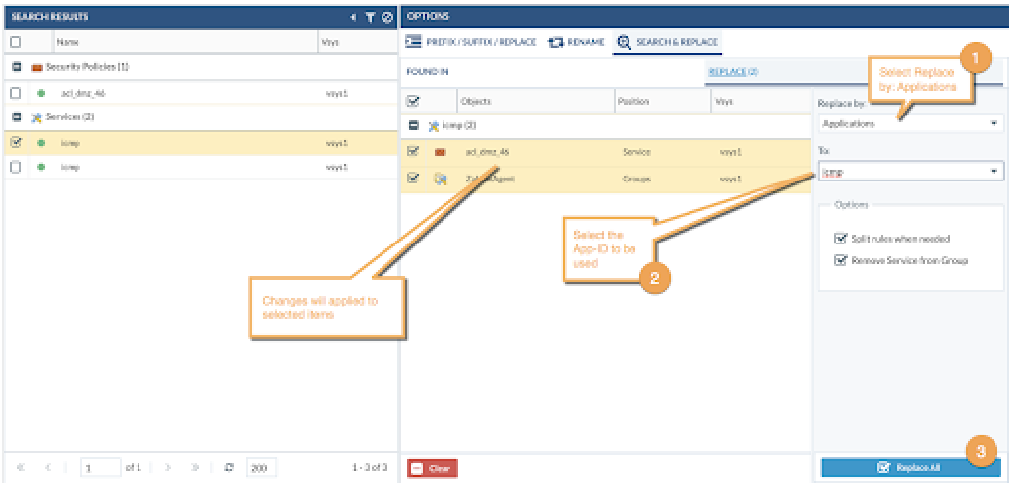
Double-click on a Rule to apply a filter on it and see it

If you want to see the rule(s) that use this object, just double-click on the rule and you will be redirected to the Policy Tab and a filter by that rule will be applied.

After review, move back to the Tools Tab, click the Search & Replace Tab, and click on Replace. In this example, we are replacing a service by an App-ID, so select Replace by "Applications" and then to "ICMP" and click Replace All.

There are a couple options enabled by default:

1. Split rules when needed – In case we are replacing services by App-ID, check if the rule where the invalid service is in use has more services defined. In that situation, the rule will be cloned to allow the new App-ID but removing all the other services from the cloned rule, and then the invalid service will be removed from the original rule. By doing this, we don't mix services with apps in the same rule which can lead to change the original behavior of the rule.
2. Remove Service from Group – In case the invalid service was a member of a group, it will be removed after the replace as a member.



1 Select Replace by: Applications

2 Select the App-ID to be used

Changes will applied to selected items

3

This procedure can be used in many other ways. For example, if we want to filter by a service or address and remove that object from the configuration, just select the object from the Search Results panel then add to Replace from where it was being used. To replace, select Replace by combo "Remove." That will remove the object from where it was used, or if you have an address-group or service-group and you want to replace it by the members instead, you will do the same but in the Replace and select "Members" then click Replace All.

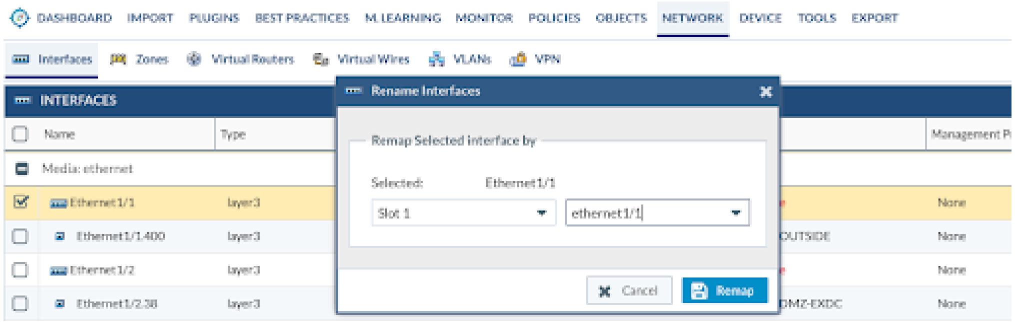
After replacement of the invalid objects, you can repeat the step for removing the unused objects since they will not be used anymore.

Remapping Interface Names

Expedition, when imports configurations from other vendors, keeps the original interface names to make the validation process easier after the import. The problem with that is naming usually doesn't match the one that Palo Alto Networks expects, so we have to rename them to ensure the changes will be captured by our Palo Alto Networks configuration.

For example, we import a configuration from Cisco, and the interface names are "Ethernet1/1" which is very similar to a Palo Alto Networks naming convention, but, in our case, it must be all in lowercase.

To convert it to the proper naming convention, you can select the Ethernet1/1 that is parent for more sub-interfaces (vlan tags) and click on the Remap Interface Name located at the bottom left-side bar. From there, select Slot 1 and ethernet1/1.



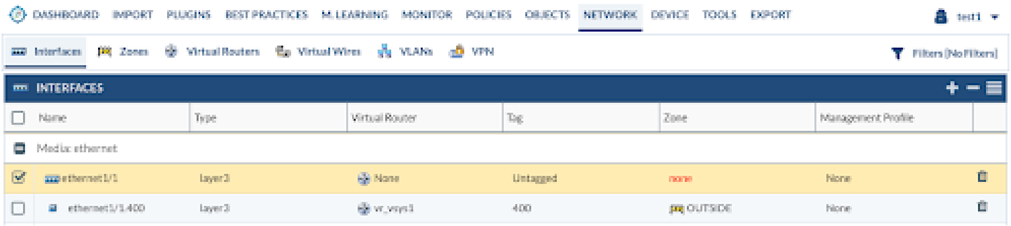
Remap Selected interface by

Selected: Ethernet1/1

Slot 1 | ethernet1/1

□	Name	Type		Management P
⊟	Media: ethernet			
☑	Ethernet1/1	layer3		None
□	Ethernet1/1.400	layer3	OUTSIDE	None
□	Ethernet1/2	layer3		None
□	Ethernet1/2.38	layer3	DMZ-EXDC	None

After clicking the Remap button, the Expedition tool will replace the name of the interface in the whole configuration, including any references to it and any subinterfaces.



□	Name	Type	Virtual Router	Tag	Zone	Management Profile
⊟	Media: ethernet					
☑	ethernet1/1	layer3	None	Untagged	none	None
□	ethernet1/1.400	layer3	vr_vsys1	400	OUTSIDE	None

You will have to repeat the process to adapt all the interfaces that you want to migrate.

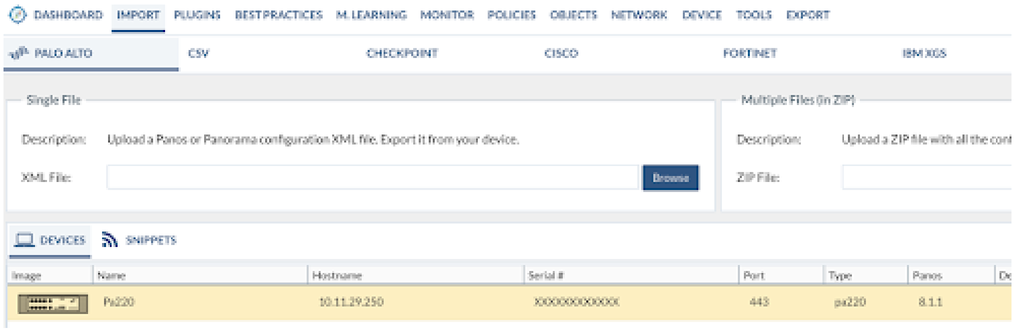
Import Your Base Configuration

What is the Base Configuration?

Base Configuration is a device's specific configuration that is usually taken from the Palo Alto Networks device that you are migrating to. The base configuration should be used, as the name suggests, as a base and should be merged with the imported third-party vendor configuration that you have imported and manipulated. The result of the merge should be a working and migrated Palo Alto Networks configuration.

The first PAN-OS configuration imported into the project will be assigned as Base Configuration. The Base Configuration is the one that will be used at the time to export the configuration out of Expedition or by generating an XML file or API calls. Any changes made to the Base Configuration will be applied to the output.

To import a Base Configuration, click the Import Tab from the PALO ALTO Tab and enter a link to your XML file that you previously exported from your PAN-OS device or just double click on one of the devices added to the project (if any) to import the config from the snapshot stored in Expedition.



Single File

Description: Upload a Panos or Panorama configuration XML file. Export it from your device.

XML File:

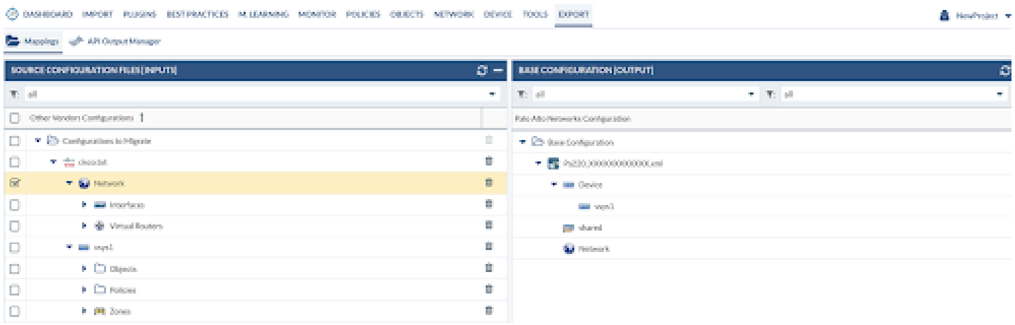
Multiple Files (in ZIP)

Description: Upload a ZIP file with all the conf

ZIP File:

Image	Name	Hostname	Serial #	Port	Type	Panos	De
	Pa220	10.11.29.250	XXXXXXXXXXXX	443	pa220	8.1.1	

After that, you can check from the Export Tab that the config has been set as Base Config by seeing if it has been placed in the right panel.



SOURCE CONFIGURATION FILES [INPUTS]

all

□ Other Vendors Configurations

□ Configurations to Migrate
□ checkist
☑ Network
□ Interfaces
□ Virtual Routers
□ vsys1
□ Objects
□ Policies
□ Zones

BASE CONFIGURATION [OUTPUT]

all all

Palo Alto Networks Configuration

Base Configuration
Pa220_XXXXXXXXXXXX.xml
Device
vsys1
shared
Network

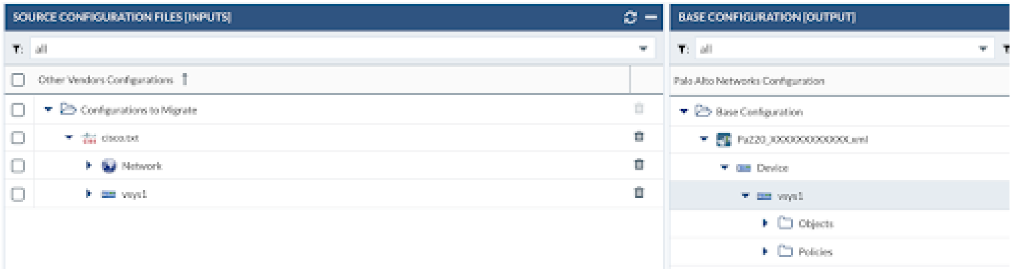
From there, you can select what objects we want to move from the left panel to the Base Configuration (right panel) by using drag and drop.

In case you want to move the objects from the left panel and convert them as shared objects, drop them into the Shared vsys/DG. After the merge, they will be transformed into shared objects, and all the references to them will point to the new shared objects (from policies, groups, etc).

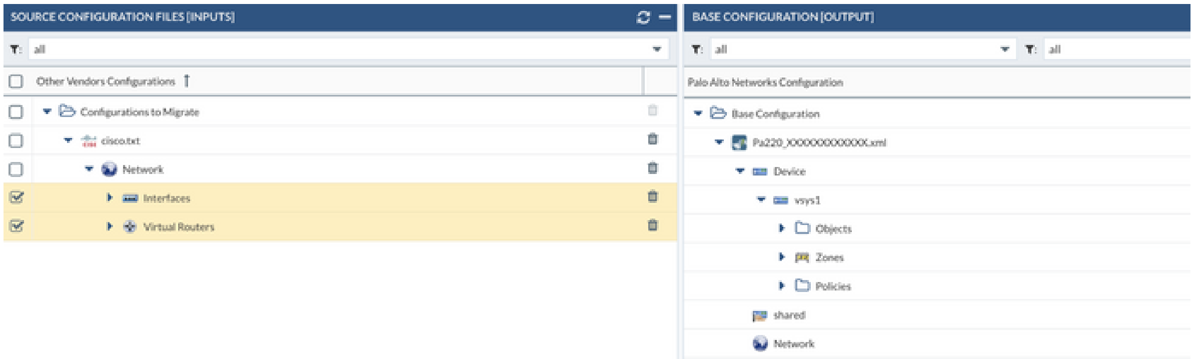
Merge Objects to your Base Configuration

All migrated objects should be visible on the left panel under the Export Tab. The right panel should have your Base Configuration that you previously imported. You just need to drag and drop the migrated objects and policies from the left to the right. You can select certain parts of the migrated configuration to be moved to the final configuration or all of them.

Please make sure you place the objects and policies into the desired vsys configuration.

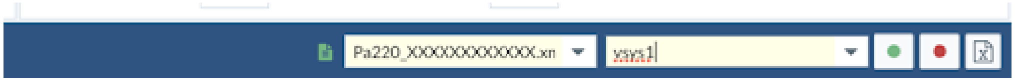

SOURCE CONFIGURATION FILES [INPUTS]
T: all
Other Vendors Configurations
Configurations to Migrate
cisco.txt
Network
vsys1
BASE CONFIGURATION [OUTPUT]
T: all
Palo Alto Networks Configuration
Base Configuration
Pa220_XXXXXXXXXXXXX.xml
Device
vsys1
Objects
Policies

Repeat the same procedure with the Zones, Interfaces, Virtual Router(s) and drop them into the correct vsys.


SOURCE CONFIGURATION FILES [INPUTS]
T: all
Other Vendors Configurations
Configurations to Migrate
cisco.txt
Network
Interfaces
Virtual Routers
BASE CONFIGURATION [OUTPUT]
T: all
T: all
Palo Alto Networks Configuration
Base Configuration
Pa220_XXXXXXXXXXXXX.xml
Device
vsys1
Objects
Zones
Policies
shared
Network

The final step is to merge the migrated configuration and your base configuration and create you final configuration. To do this, click the MERGE button.

After this action, all the selected objects will be transferred from one configuration to the Base Configuration. If you want to see how it looks, you need to change the selected configuration and the vsys to the Base Configuration from the bottom bar by going to the Objects Tab. This will filter and show you the objects and rules on the Base Configuration.

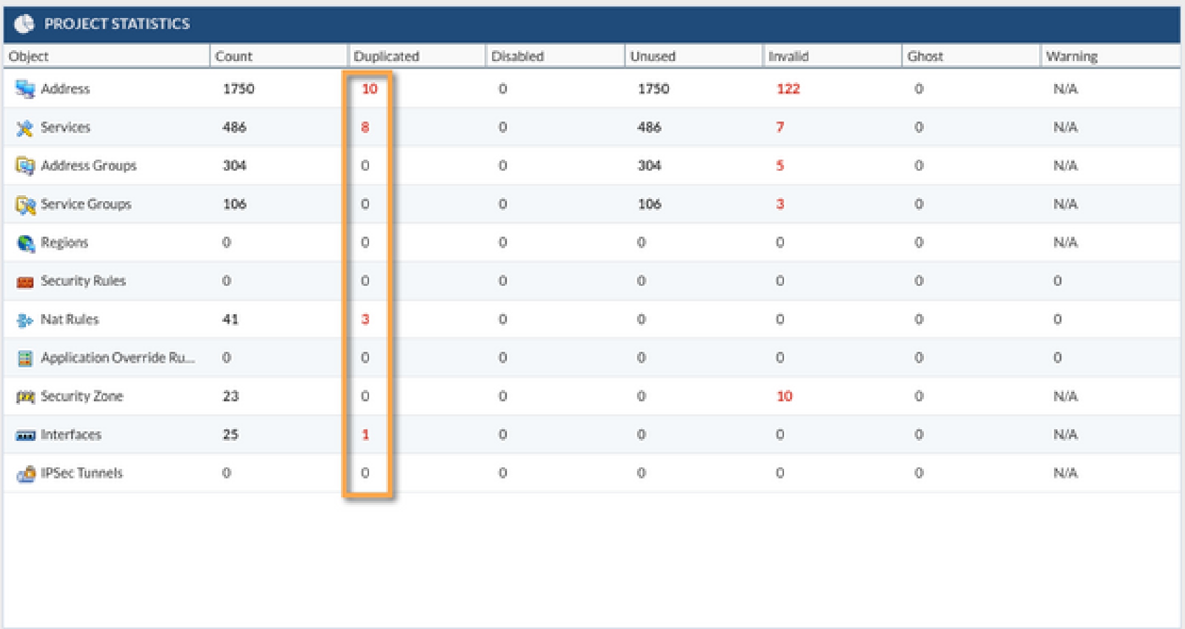


After you have created the final configuration, you have two options to deploy it. One option is a manual XML file export that can be deployed on the Palo Alto Networks device to which you are migrating, and the other option is to use API calls to send parts of the configuration or the whole configuration to the device if that Palo Alto Networks device is already connected to Expedition.

Find Duplicates After the Merge and Removing Them

It is recommended that you run another check for duplicates and remove or merge them after a configuration migration. A common scenario is to have duplicates amongst objects, services, and/or interfaces.

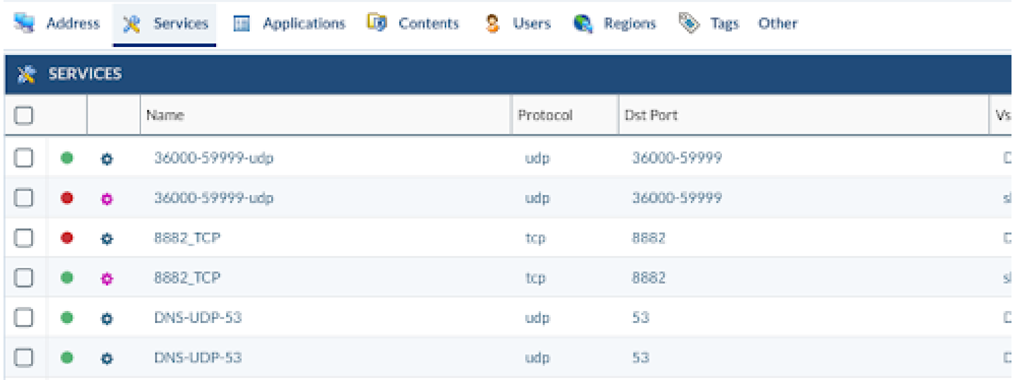
Using the dashboard from within the project, it will tell you how many duplicated objects you have in your current configuration. You can click on the duplicate object to go to the object view, and Expedition will filter by duplicate and by name predefined filter.



PROJECT STATISTICS

Object	Count	Duplicated	Disabled	Unused	Invalid	Ghost	Warning
Address	1750	10	0	1750	122	0	N/A
Services	486	8	0	486	7	0	N/A
Address Groups	304	0	0	304	5	0	N/A
Service Groups	106	0	0	106	3	0	N/A
Regions	0	0	0	0	0	0	N/A
Security Rules	0	0	0	0	0	0	0
Nat Rules	41	3	0	0	0	0	0
Application Override Ru...	0	0	0	0	0	0	0
Security Zone	23	0	0	0	10	0	N/A
Interfaces	25	1	0	0	0	0	N/A
IPSec Tunnels	0	0	0	0	0	0	N/A

Next, check the duplicated services to demonstrate the workflow to follow and get rid of them.

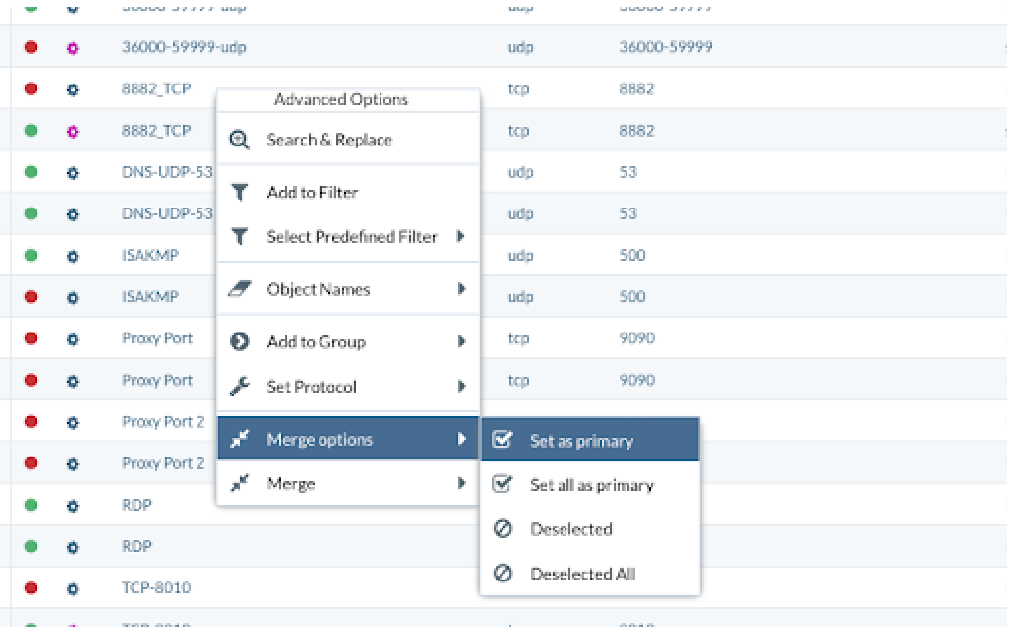


□			Name	Protocol	Dst Port	Vs
□	●	⚙	36000-59999-udp	udp	36000-59999	C
□	●	⚙	36000-59999-udp	udp	36000-59999	sl
□	●	⚙	8882_TCP	tcp	8882	C
□	●	⚙	8882_TCP	tcp	8882	sl
□	●	⚙	DNS-UDP-53	udp	53	C
□	●	⚙	DNS-UDP-53	udp	53	C

The object in Pink is a Shared object, so that means you have selected the vsys equal to all from the bottom bar. This will do a search across all the vsys/DG to find objects seen more than once.

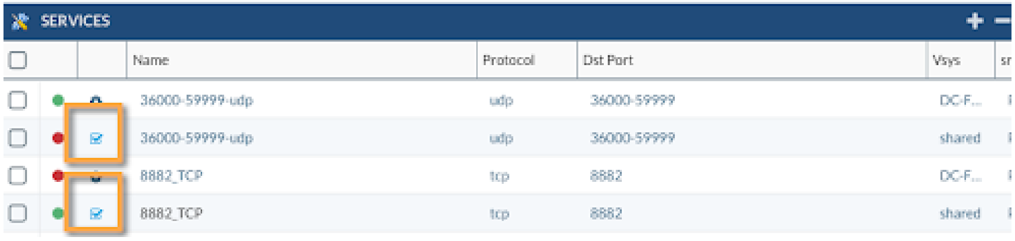
In our example, we want to keep the object that already exists as Shared and make all the references within the vsys/DG points after the merge to the Shared object only and finally the duplicated object out from the Shared will be removed.

First, select the duplicated objects you want to keep and then right-click and select Merge Options and “Set as Primary.” That will tell Expedition to keep the one we set as Primary after Merging the duplicated objects.



●	⚙	36000-59999-udp	udp	36000-59999
●	⚙	8882_TCP	tcp	8882
●	⚙	8882_TCP	tcp	8882
●	⚙	DNS-UDP-53	udp	53
●	⚙	DNS-UDP-53	udp	53
●	⚙	ISAKMP	udp	500
●	⚙	ISAKMP	udp	500
●	⚙	Proxy Port	tcp	9090
●	⚙	Proxy Port	tcp	9090
●	⚙	Proxy Port 2		
●	⚙	Proxy Port 2		
●	⚙	RDP		
●	⚙	RDP		
●	⚙	TCP-8010		

When the object has been set as Primary, you will notice a new icon appear.



□			Name	Protocol	Dst Port	Vsys
□	●		36000-59999-udp	udp	36000-59999	DC-F...
□	●	☑	36000-59999-udp	udp	36000-59999	shared
□	●		8882_TCP	tcp	8882	DC-F...
□	●	☑	8882_TCP	tcp	8882	shared

Now you can apply the Merge type. In our case, we will use Merge by Name and Value to validate only the same duplicated object is merged. Right-click and select "Merge" then click "By Name & Value." This will be applied to the selected objects or, in case you didn't select any, it will be applied to all the results from the filter applied.

You can change the filter and add a predefined filter to show only the duplicated services by name only and then apply the merge by the same concept, only by name as well.

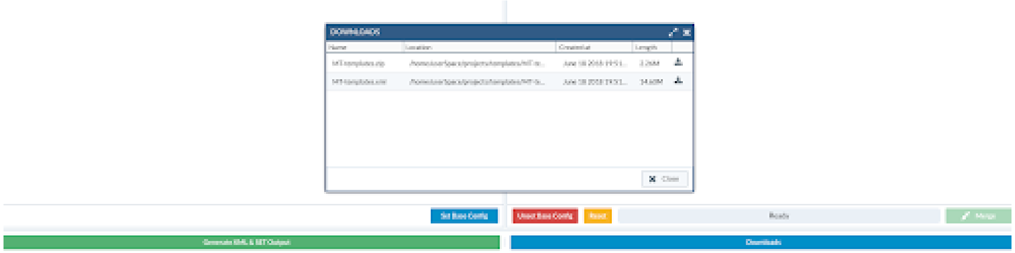
All this can be done with the right-click "Select predefined filter."

Generating the Output

When you are finished cleaning your configuration, it's time to get the results and export from Expedition and import into your Palo Alto Networks device (Firewall or Panorama).

Navigate to the Export TAB.

Under the Mapping Tab, there is a button at the bottom bar-left titled "Generate XML & SET Output." By pressing this button, Expedition will generate a XML configuration file and based on that configuration (and using a script called Pan-Python made by Kevin Steves https://github.com/kevinsteves/pan-python) it will generate the Set commands as well. After the generation, a new window with the download links will appear. Click the Downloads button to get access to that window as well.



DOWNLOADS

Name	Location	Created at	Length
MT-templates.zip	/home/userSpace/projects/templates/MT-te...	June 18 2018 19:51...	3.26M
MT-templates.xml	/home/userSpace/projects/templates/MT-te...	June 18 2018 19:51...	14.60M

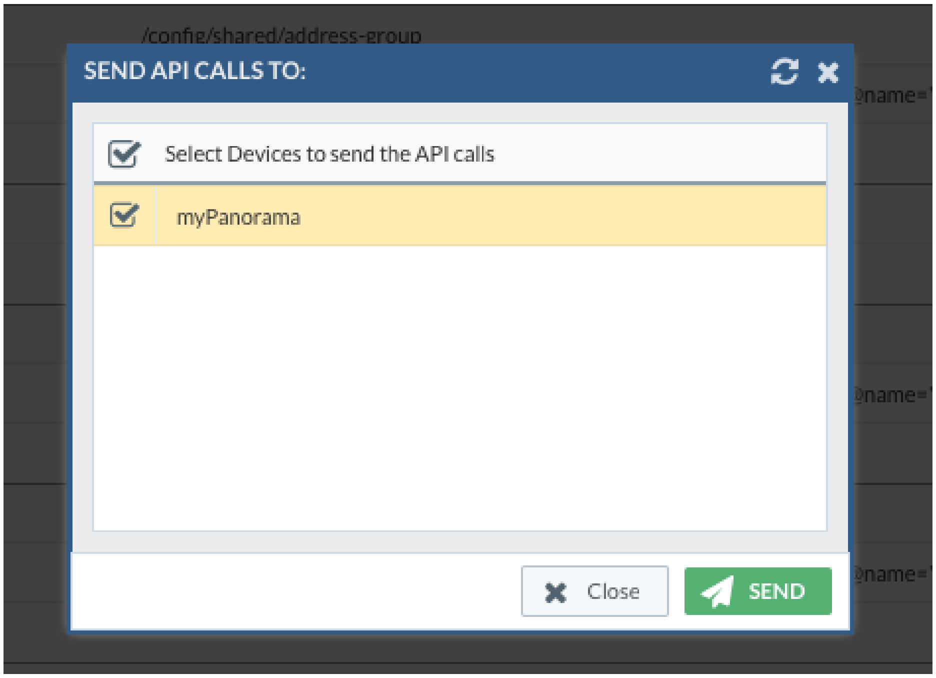
You can generate API Calls to be sent to your devices in case you created them before and you added to the project you are working on. In that case, you will need to go under the tab titled, “API Output Manager.”

Here, you have several options. We will start covering Atomic and Subatomic.

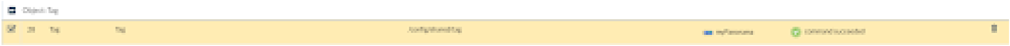
Atomic calls will be API calls where with a single API call will add all the address, for instance, to a specific vsys/DG. If you select subatomic, you will get one API call by element you have. If you have 500 addresses, you will get 500 API calls, one for each address. With Atomic, you will get just one API call containing the 500 addresses inside.

Step One: Click on “Atomic” or “Subatomic” and click the “Step 1” button to create all the API calls.
After that, the ID of each API call will tell you the order in which you have to send the API call. Yes, order matters. If you don’t select any, all API calls will be sent in the proper order.

Step Two: Click “Step 2” button and select the DEVICE where you want to send the API calls and send them all.


/config/shared/address-group
SEND API CALLS TO:
☑ Select Devices to send the API calls
☑ myPanorama
✖ Close
SEND
@name='
@name='
@name='

After the API call is sent, you will get the response from the device itself. If it was successful, you will see in the output.



```
Object: Tag
☑ 29 Tag Tag /config/shared/tag myPanorama command succeeded
```

Appendix A: Import

Importing CSV files

From within a project, it's possible to import CSV files containing objects that you want to add to you current configuration.

Requirements

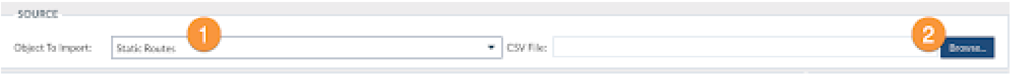
You must have a configuration previously loaded in order to import something else on top by using CSV files.

How the CSV file must be created:

- The character used to split by columns is the semi-colon “;”
- The character used to split members inside a column is the comma “,”

Process

1. Select the object type you want to import. Example: Static Routes
2. Select the CSV file from your laptop

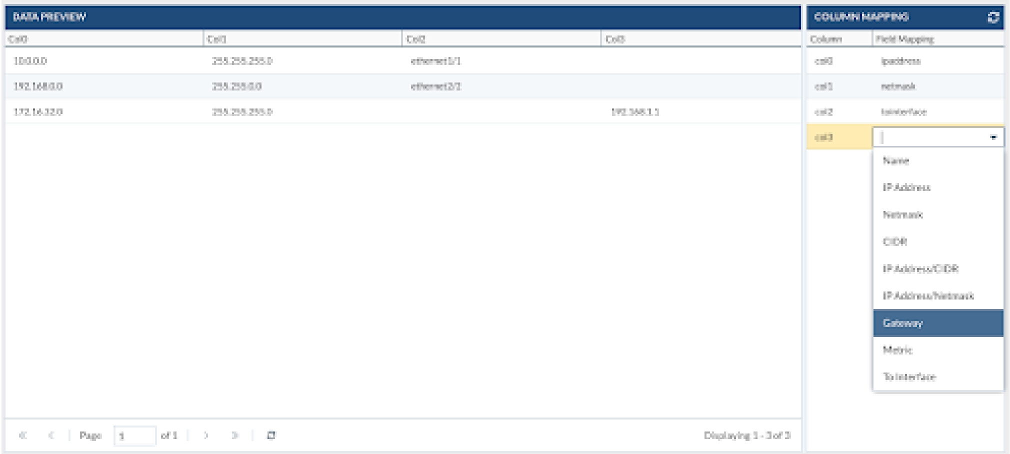


SOURCE

Object To Import: Static Routes

CSV File:

3. Map your columns with the predefined fields from the right panel



DATA PREVIEW

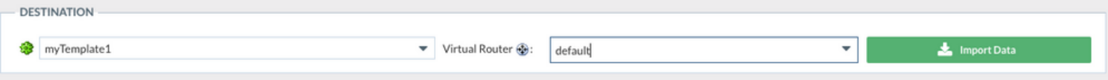
Col0	Col1	Col2	Col3
10.0.0.0	255.255.255.0	ethernet1/1	
192.168.0.0	255.255.0.0	ethernet2/2	
172.16.32.0	255.255.255.0		192.168.1.1

Page 1 of 1 Displaying 1 - 3 of 3

COLUMN MAPPING

Column	Field Mapping
col0	ipaddress
col1	netmask
col2	tointerface
col3	

4. Select where to import the new data loaded from the CSV and mapped



DESTINATION

myTemplate1 Virtual Router: default

In this example, routes are part of Templates and need to be imported into a Virtual-Router. Plus, select the virtual-system where your VR is located. Then click Import Data.

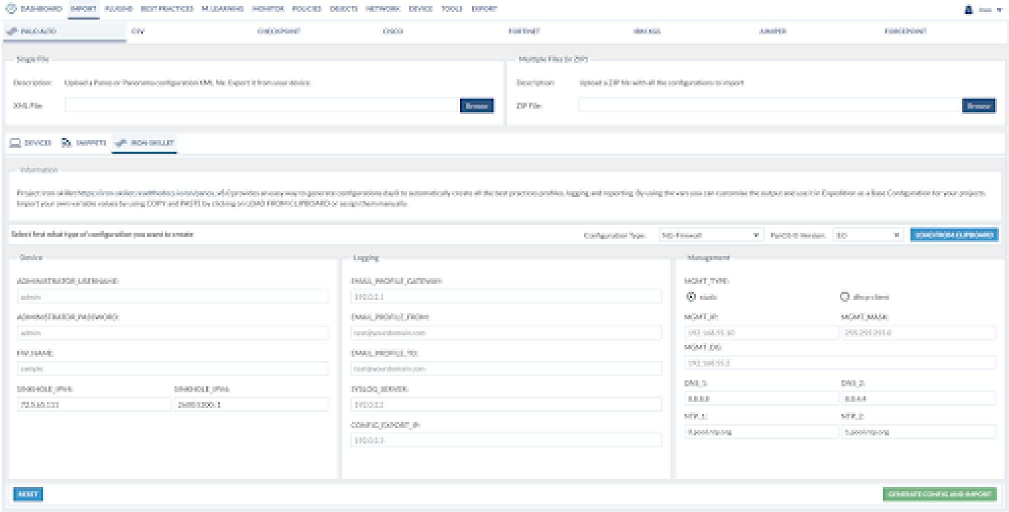
Order matters! If want to import Service Groups, you need to first import the services used on those Groups or the import will not be successful.

Importing an IronSkillet Day1 Configuration

IronSkillet is a project made by Palo Alto Networks to create a configuration that is already configured with some of the best practices recommended by our security experts. If you need to add a Base Configuration into Expedition to use it as a base to migrate something else, it's very simple now with the integration built in Expedition.

Process

Create a project and click to get in. After you enter the project, go to IMPORT. Then click the Tab title "Iron-Skillet."



Single File

Description: Upload a Panos or Panorama configuration XML file. Export it from your device.

XML File:

Multiple Files (in ZIP)

Description: Upload a ZIP file with all the configurations to import

ZIP File:

Information

[illegible]

Select first what type of configuration you want to create

Configuration Type: NG-Firewall ▾ PanOS-8 Version: 8.0 ▾

Device

ADMINISTRATOR_USERNAME: admin

ADMINISTRATOR_PASSWORD: admin

FW_NAME: sample

SINKHOLE_IPV4: 72.5.65.111 SINKHOLE_IPV6: 2600:5200::1

Logging

EMAIL_PROFILE_GATEWAY: 192.0.2.1

EMAIL_PROFILE_FROM: test@yourdomain.com

EMAIL_PROFILE_TO: test@yourdomain.com

SYSLOG_SERVER: 192.0.2.2

CONFIG_EXPORT_IP: 192.0.2.3

Management

MGMT_TYPE: ● static ○ dhcp-client

MGMT_IP: 192.168.55.10 MGMT_MASK: 255.255.255.0

MGMT_DG: 192.168.55.2

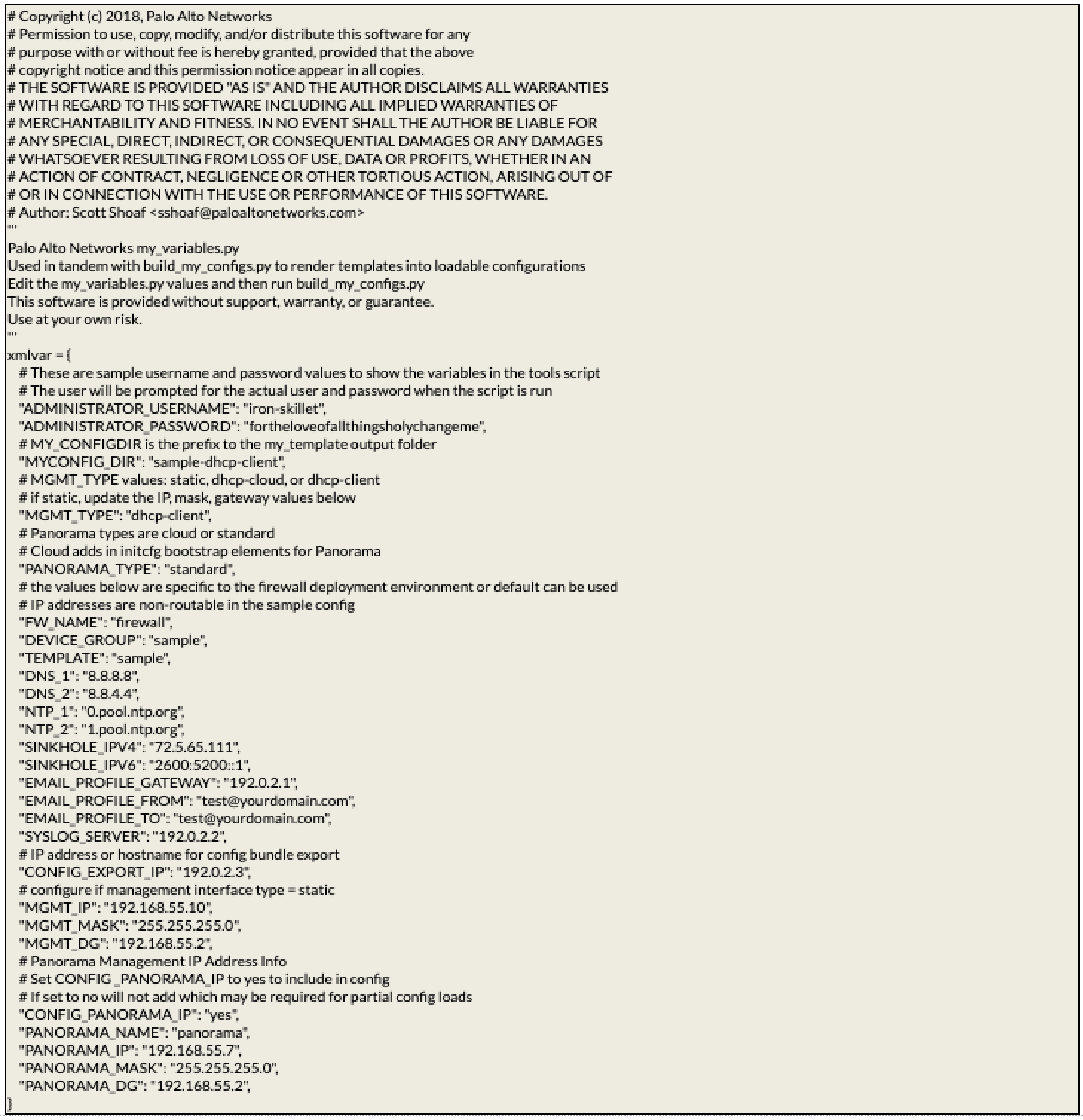
DNS_1: 8.8.8.8 DNS_2: 8.8.4.4

NTP_1: 0.pool.ntp.org NTP_2: 1.pool.ntp.org

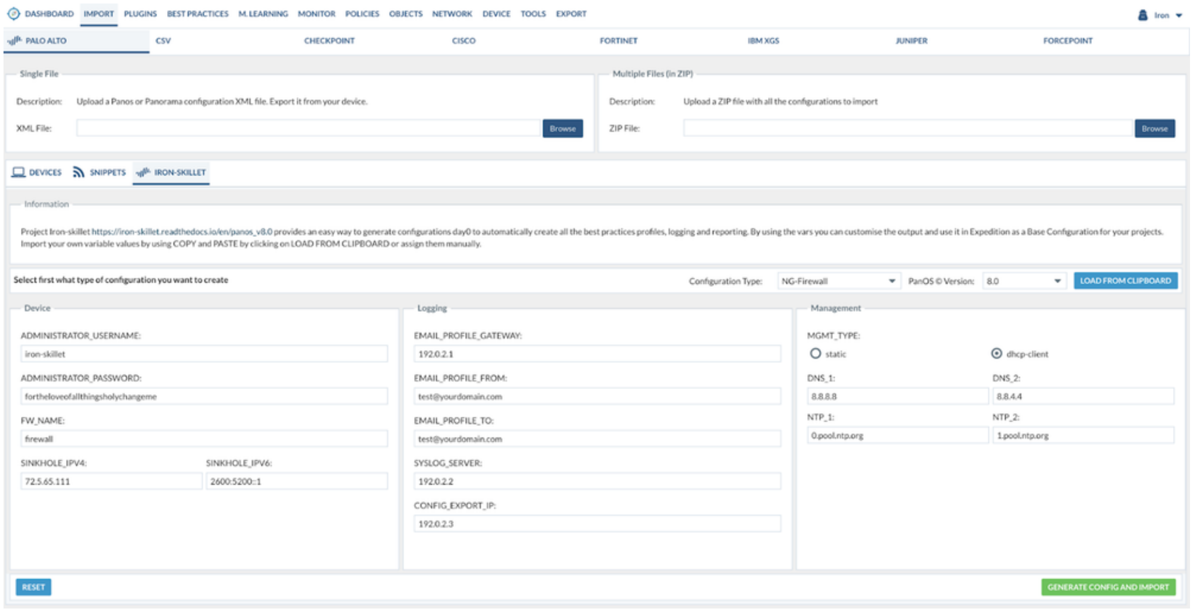
From here, you can configure some parameters before the configuration is created. You can modify the parameters by hand, or, if you have an IronSkillet configuration file, you can load it to automatically fill the fields.

- Select the Configuration Type (Firewall or Panorama) this will generate the type of configuration selected.
- PAN-OS Version. You can select if the configuration you need but it must be 8.0 or 8.1 or X.X
- If you have an IronSkillet configuration, you can click LOAD FROM CLIPBOARD and paste the content from the file and then click SAVE. That will automatically fill the fields configured.

Example: https://raw.githubusercontent.com/PaloAltoNetworks/iron-skillet/panos_v8.0/my_configs/sample-mgmt-dh...



```
# Copyright (c) 2018, Palo Alto Networks
# Permission to use, copy, modify, and/or distribute this software for any
# purpose with or without fee is hereby granted, provided that the above
# copyright notice and this permission notice appear in all copies.
# THE SOFTWARE IS PROVIDED "AS IS" AND THE AUTHOR DISCLAIMS ALL WARRANTIES
# WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF
# MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR
# ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES
# WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN
# ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF
# OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.
# Author: Scott Shoaf <sshoaf@paloaltonetworks.com>
'''
Palo Alto Networks my_variables.py
Used in tandem with build_my_configs.py to render templates into loadable configurations
Edit the my_variables.py values and then run build_my_configs.py
This software is provided without support, warranty, or guarantee.
Use at your own risk.
'''
xmlvar = {
  # These are sample username and password values to show the variables in the tools script
  # The user will be prompted for the actual user and password when the script is run
  "ADMINISTRATOR_USERNAME": "iron-skillet",
  "ADMINISTRATOR_PASSWORD": "fortheloveofallthingsholychangeme",
  # MY_CONFIGDIR is the prefix to the my_template output folder
  "MYCONFIG_DIR": "sample-dhcp-client",
  # MGMT_TYPE values: static, dhcp-cloud, or dhcp-client
  # if static, update the IP, mask, gateway values below
  "MGMT_TYPE": "dhcp-client",
  # Panorama types are cloud or standard
  # Cloud adds in initcfg bootstrap elements for Panorama
  "PANORAMA_TYPE": "standard",
  # the values below are specific to the firewall deployment environment or default can be used
  # IP addresses are non-routable in the sample config
  "FW_NAME": "firewall",
  "DEVICE_GROUP": "sample",
  "TEMPLATE": "sample",
  "DNS_1": "8.8.8.8",
  "DNS_2": "8.8.4.4",
  "NTP_1": "0.pool.ntp.org",
  "NTP_2": "1.pool.ntp.org",
  "SINKHOLE_IPV4": "72.5.65.111",
  "SINKHOLE_IPV6": "2600:5200::1",
  "EMAIL_PROFILE_GATEWAY": "192.0.2.1",
  "EMAIL_PROFILE_FROM": "test@yourdomain.com",
  "EMAIL_PROFILE_TO": "test@yourdomain.com",
  "SYSLOG_SERVER": "192.0.2.2",
  # IP address or hostname for config bundle export
  "CONFIG_EXPORT_IP": "192.0.2.3",
  # configure if management interface type = static
  "MGMT_IP": "192.168.55.10",
  "MGMT_MASK": "255.255.255.0",
  "MGMT_DG": "192.168.55.2",
  # Panorama Management IP Address Info
  # Set CONFIG _PANORAMA_IP to yes to include in config
  # If set to no will not add which may be required for partial config loads
  "CONFIG_PANORAMA_IP": "yes",
  "PANORAMA_NAME": "panorama",
  "PANORAMA_IP": "192.168.55.7",
  "PANORAMA_MASK": "255.255.255.0",
  "PANORAMA_DG": "192.168.55.2",
}
```



Single File

Description: Upload a Panos or Panorama configuration XML file. Export it from your device.

XML File:

Multiple Files (in ZIP)

Description: Upload a ZIP file with all the configurations to import

ZIP File:

Information

Project Iron-skillet https://iron-skillet.readthedocs.io/en/panos_v8.0 provides an easy way to generate configurations day0 to automatically create all the best practices profiles, logging and reporting. By using the vars you can customise the output and use it in Expedition as a Base Configuration for your projects. Import your own variable values by using COPY and PASTE by clicking on LOAD FROM CLIPBOARD or assign them manually.

Select first what type of configuration you want to create

Configuration Type: NG-Firewall PanOS © Version: 8.0

Device

ADMINISTRATOR_USERNAME: iron-skillet

ADMINISTRATOR_PASSWORD: fortheloveofallthingsholychangeme

FW_NAME: firewall

SINKHOLE_IPV4: 72.5.65.111

SINKHOLE_IPV6: 2600:5200::1

Logging

EMAIL_PROFILE_GATEWAY: 192.0.2.1

EMAIL_PROFILE_FROM: test@yourdomain.com

EMAIL_PROFILE_TO: test@yourdomain.com

SYSLOG_SERVER: 192.0.2.2

CONFIG_EXPORT_IP: 192.0.2.3

Management

MGMT_TYPE: ○ static ● dhcp-client

DNS_1: 8.8.8.8

DNS_2: 8.8.4.4

NTP_1: 0.pool.ntp.org

NTP_2: 1.pool.ntp.org

After the changes are made, you have to click on GENERATE CONFIG AND IMPORT. This will create a Palo Alto Networks configuration file based on your selection (Firewall or Panorama) and with the selected version and all the changes made in the parameters will be applied to it. After IronSkillet generates the new configuration, Expedition will Encrypt it and automatically imported into the Project. If this is the first Palo Alto Networks configuration loaded on the Project, Expedition will set it as the Base Configuration.

Revision History

Date	Revision	Comment
June 22, 2018	A	First release of this document.
October 16,2018	B	Added Appendix A
April 1,2019	C	Updated Screenshots
August 27, 2019	D	Created LIVEcommunity Article and Editorial Revisions

★★★★★ (1) 15,720 Views