

Expedition

User Guide

Version 1.1



Contents

| | |
|--|-----------|
| What is Expedition? | 3 |
| Login from the web interface | 4 |
| GUI Login | 4 |
| Changing default credentials | 5 |
| GUI Login | 5 |
| Migration Workflow | 6 |
| Importing a configuration into the project | 6 |
| Project Dashboard..... | 7 |
| Remove Unused Objects | 7 |
| Fixing Invalid Services..... | 8 |
| <i>Replace Services by App-ID</i> | 9 |
| Remapping Interface names | 10 |
| Import your Base Configuration..... | 11 |
| Merge Objects to your Base Configuration..... | 12 |
| Find Duplicates after the merge and removing them..... | 13 |
| Generating the Output..... | 16 |
| Revision History | 22 |

What is Expedition?

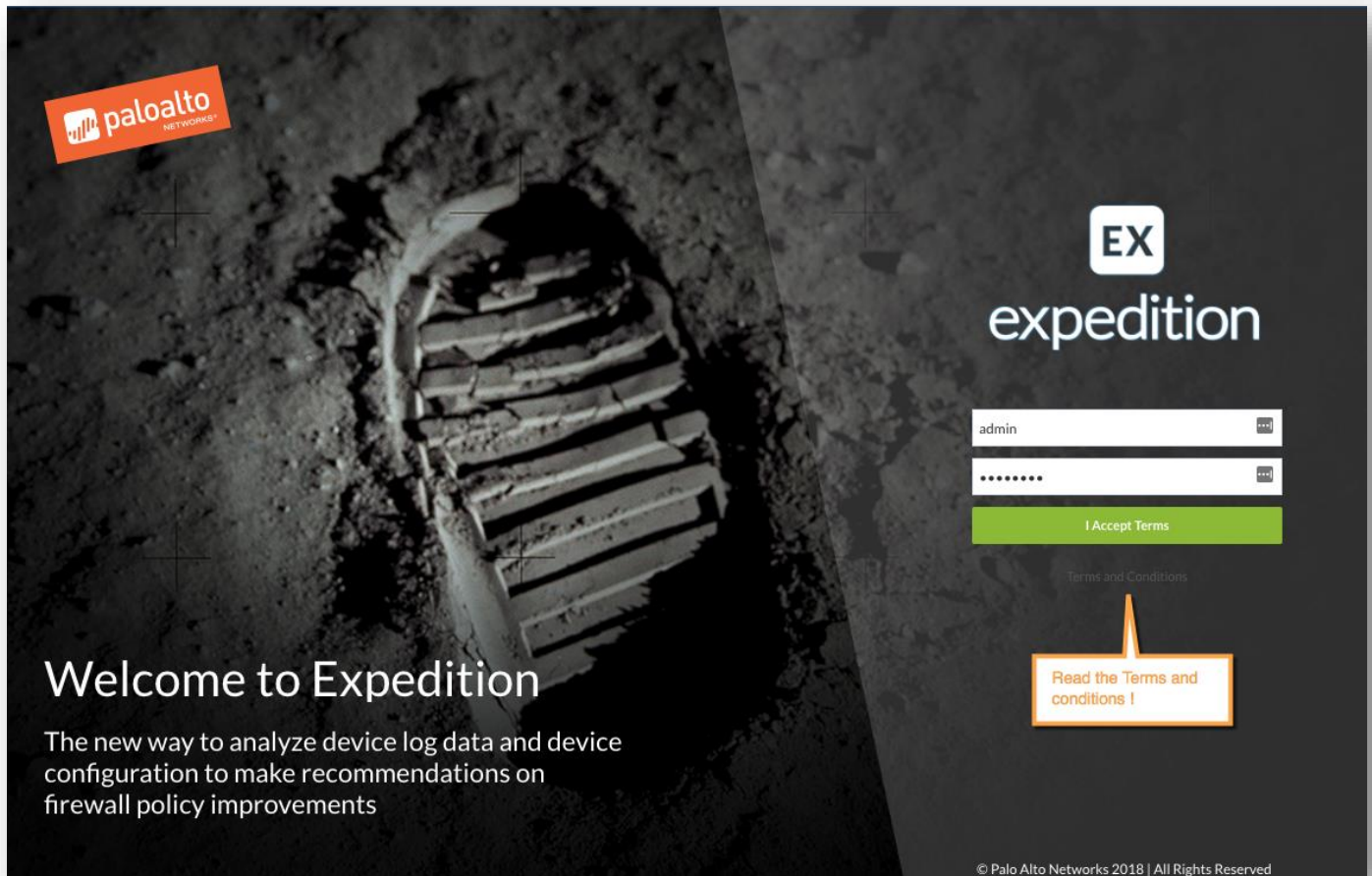
Expedition is the fourth evolution of the Palo Alto Networks Migration Tool. The main purpose of this tool was help reducing the time and efforts to migrate a configuration from one of the supported vendors to Palo Alto Networks.

By using the Migration Tool everyone can convert a configuration from Checkpoint or Cisco or any other vendor to a PanOS 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 PanOS but we want to ensure the outcome it's the best as possible, there is why we added a **Machine Learning module** who can help you to generate new security policies based on real log traffic and the introduction of the **Best Practices Assessment Tool** to check 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 the excellence will be easier.

Login



Login from the web interface

After you review the

GUI Login

GUI it's only referencing the access via web interface

| | |
|----------|----------|
| Username | admin |
| Password | paloalto |

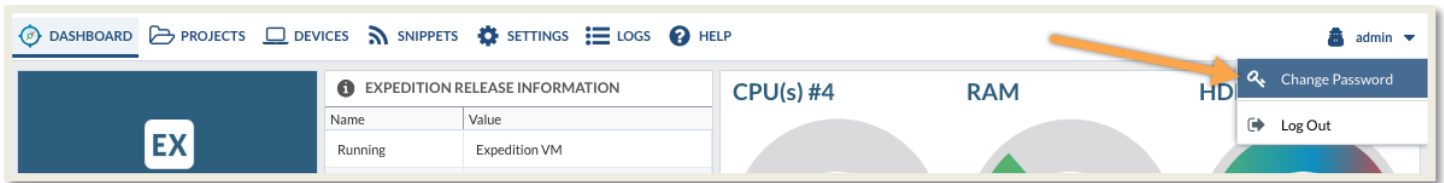
Security Warning! We encourage to change them after the first login.

Changing default credentials

As a good practice we recommend you to change the default credentials as soon as you can (DP – upon first log in)

GUI Login

After login via web browser follow these instructions to change the password for the “admin” user.

A screenshot of the 'Change Password' dialog box. It has a title bar with a search icon and a close button. The dialog is divided into two sections: 'Validation' and 'New Information'. The 'Validation' section has a 'Username' field with 'admin' and an 'Old Password' field. The 'New Information' section has 'Password' and 'Confirm Password' fields. At the bottom are 'Cancel' and 'Save' buttons. Numbered orange circles indicate the steps: 1. Old Password field, 2. Password field, 3. Confirm Password field, and 4. Save button.

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 will be at least 10 characters long

Let's Migrate

Expedition can help you to migrate pieces of configuration from other security vendors and import them into a Palo Alto Networks configuration. The goal is to reduce the time and mistakes a human can make by doing this by hand. Expedition result always needs to be reviewed by a professional with knowledge on the vendor 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 PanOS 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 in case 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

The screenshot shows the Expedition web interface. At the top is a navigation bar with tabs: DASHBOARD, IMPORT (selected), PLUGINS, BEST PRACTICES, M. LEARNING, MONITOR, POLICIES, OBJECTS, NETWORK, DEVICE, TOOLS, and EXPORT. Below the navigation bar is a sub-header with vendor tabs: PALO ALTO (selected), CSV, CHECKPOINT, CISCO, FORTINET, IBM XGS, JUNIPER, and FORCEPOINT. The main content area is divided into two sections: 'Single File' and 'Multiple Files (in ZIP)'. The 'Single File' section has a description 'Upload a Panos or Panorama configuration XML file. Export it from your device.' and a text input field for 'XML File' with a 'Browse' button. The 'Multiple Files (in ZIP)' section has a description 'Upload a ZIP file with all the configurations to import' and a text input field for 'ZIP File' with a 'Browse' button. Below these sections is a 'DEVICES' tab and a 'SNIPPETS' tab. The 'DEVICES' tab is active, showing a table with columns: Image, Name, Hostname, Serial #, Port, Type, Panos, and Description. The table contains one row with the following data: Image (Palo Alto logo), Name (Pa220), Hostname (10.11.29.250), Serial # (XXXXXXXXXXXX), Port (443), Type (pa220), Panos (8.1.1), and Description.












| Image | Name | Hostname | Serial # | Port | Type | Panos | Description |
|-------|-------|--------------|--------------|------|-------|-------|-------------|
| | Pa220 | 10.11.29.250 | XXXXXXXXXXXX | 443 | pa220 | 8.1.1 | |

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 it's time to check for Invalid objects and clean them before we move forward.

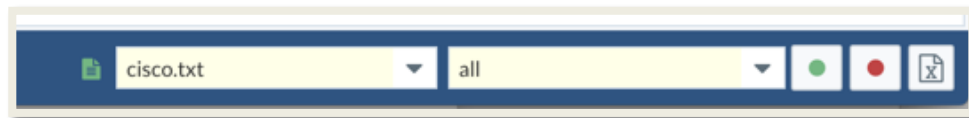
Project Dashboard

As a good starting point it's recommended to taking a look to the Project Statistics panel, we can search here for Invalid, Unused and Duplicated 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 located under Objects and will apply a predefined filter to show only the Invalid Services.

| PROJECT STATISTICS | | | | | |
|--|-------|------------|----------|--------|---------|
| Object | Count | Duplicated | Disabled | Unused | Invalid |
|  Address | 556 | 3 | 0 | 165 | 39 |
|  Services | 209 | 2 | 0 | 95 | 10 |
|  Address Groups | 98 | 0 | 0 | 72 | 0 |
|  Service Groups | 79 | 0 | 0 | 72 | 0 |
|  Regions | 0 | 0 | 0 | 0 | 0 |
|  Security Rules | 295 | 0 | 11 | 0 | 1 |
|  Nat Rules | 70 | 0 | 0 | 0 | 0 |
|  Application Override Rules | 0 | 0 | 0 | 0 | 0 |
|  Security Zone | 4 | 0 | 0 | 0 | 0 |
|  Interfaces | 4 | 0 | 0 | 0 | 0 |
|  IPSec Tunnels | 0 | 0 | 0 | 0 | 0 |

Remove Unused Objects

Before we think even how we will fix those invalid services it's important to try to remove whatever we imported but not used in any Security or Nat policy, we call them unused objects. To remove the unused objects, we have to navigate to the OBJECTS TAB and look at the bottom right bar.



At the very end we will find 3 buttons, the green one will recalculate if the objects defined are or not still used, should be used after changes have been made on the configuration so Expedition can recalculate the used objects, the second one in red is the one will remove the unused objects from the configuration and the third will export a report with all the unused objects.

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

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

Fixing Invalid Services

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

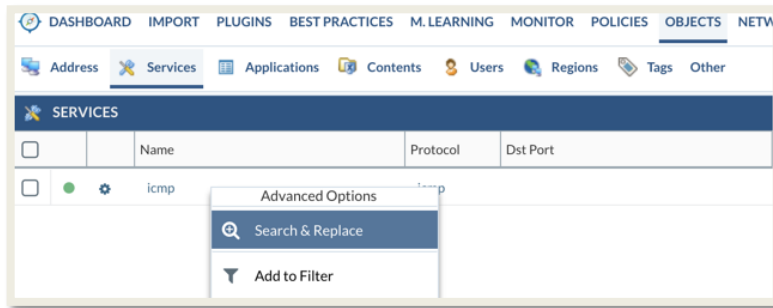
| | Name | Protocol | Dst Port | Vsys | src File |
|--------------------------|-------------|----------|----------|-------|----------|
| <input type="checkbox"/> | echo | | 7 | vsys1 | default |
| <input type="checkbox"/> | discard | | | vsys1 | default |
| <input type="checkbox"/> | tacacs | | | vsys1 | default |
| <input type="checkbox"/> | sunrpc | | | vsys1 | default |
| <input type="checkbox"/> | pim-auto-rp | | 496 | vsys1 | default |
| <input type="checkbox"/> | talk | | 517 | vsys1 | default |
| <input type="checkbox"/> | kerberos | | 750 | | default |
| <input type="checkbox"/> | nfs | | 2049 | | default |
| <input type="checkbox"/> | sip | | 5060 | | default |
| <input type="checkbox"/> | icmp | icmp | | vsys1 | default |

After we have removed the Unused Objects, only the used ones will be kept for remediation

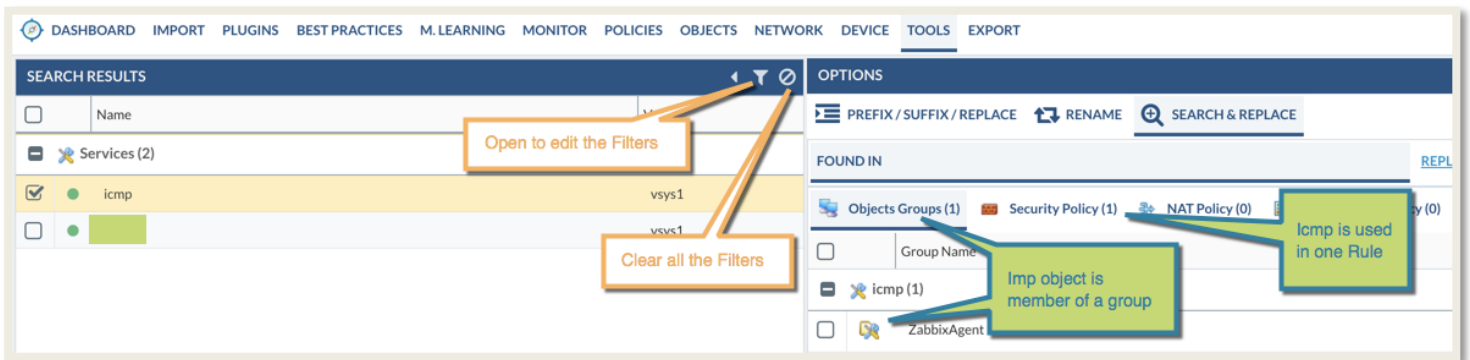
In the case of invalid services, the only way to fix in case the original service was not TCP or UDP, is change it to an App-ID from Palo Alto Networks.

| 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 do it just right click on the invalid service and click from the advanced menu Search and Replace



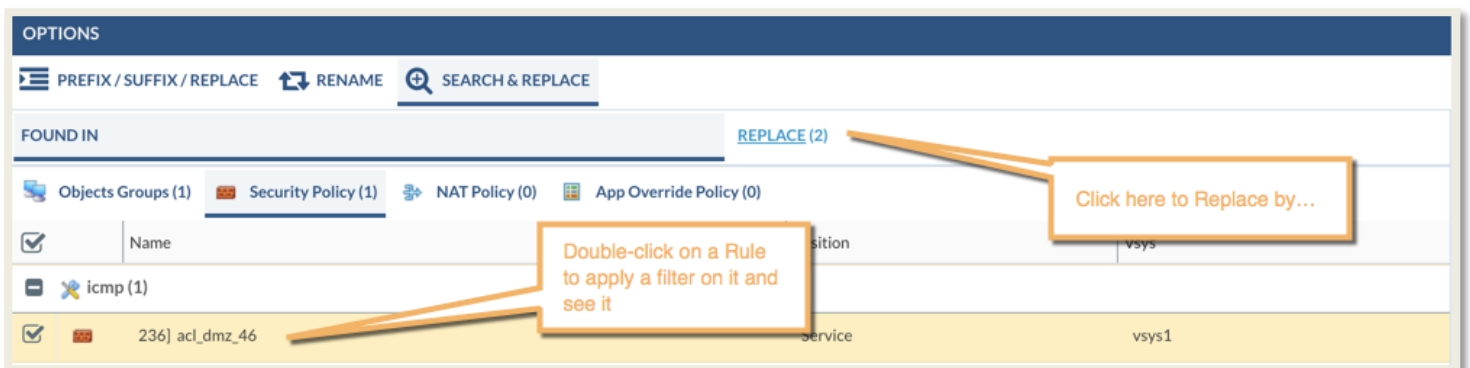
This will open up the TOOLS TAB and show you the Search & Replace TAB, the view is divided in two panels, the left panel shows the output of the applied filters and the right panel will show you where the selected items from the left panel are used.



Replace Services by App-ID

Select the service to be replaced, like in our example we will select the Group where ICMP was a member and click on Add to replace button located at the bottom bar.

Click on Security Policy (1) and select the rule where the service it's used and click on Add to replace again

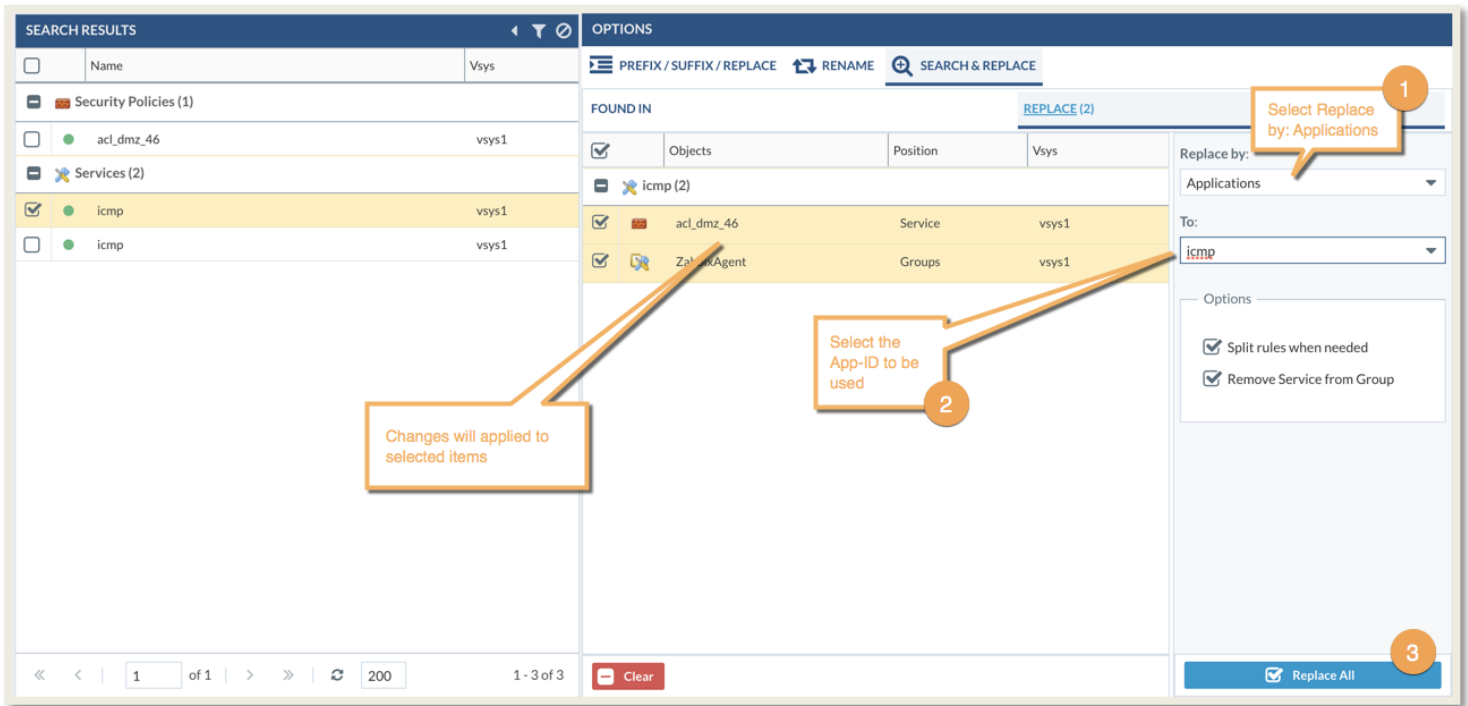


If you want to see the rule(s) that use this object, just double-click on the rule and you will be redirected to the POLICY TAB and a filter by that rule will be applied.

After review move back to TOOLS TAB and select 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 on Replace All.

There are couple of options enabled by default:

1. Split rules when needed: In case we are replacing services by app-id will 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, with this we don't mix services with apps in the same rule who 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.



This procedure can be used in many other ways, for example, 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 was being used and instead to replace select in the Replace by combo "Remove", that will remove the object from where was used or if we have an address-group or service-group and we want to replace it by the members instead so we will do the same but in the Replace by we will select "Members" and click Replace All.

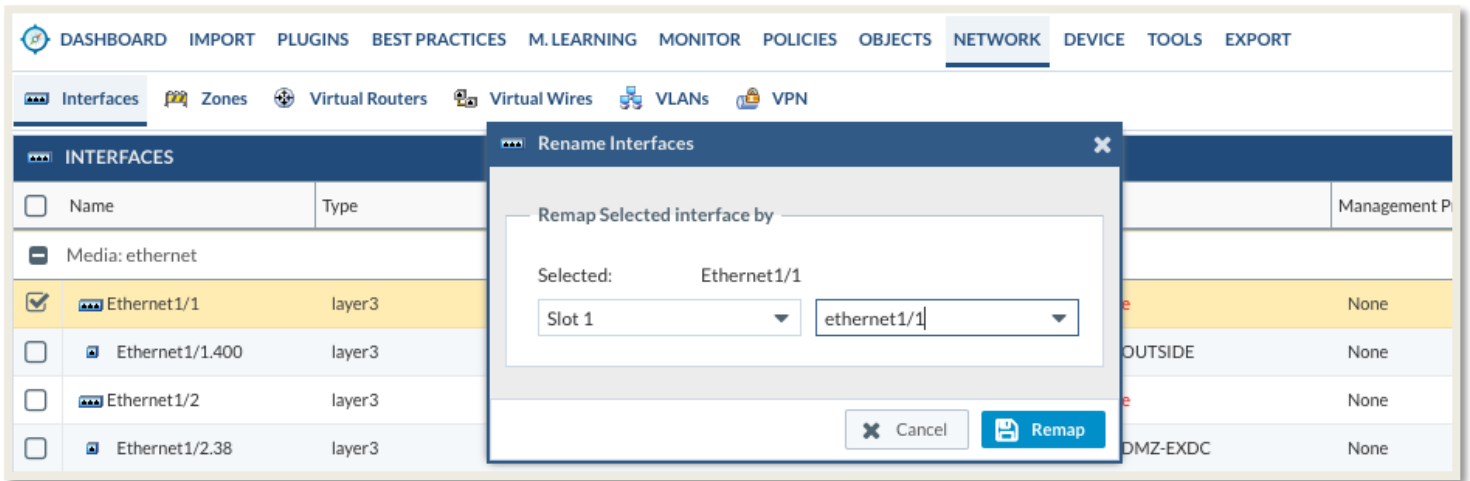
After replacement of the invalid objects we can repeat the step for removing the unused objects since they will not be used anymore

Remapping Interface names

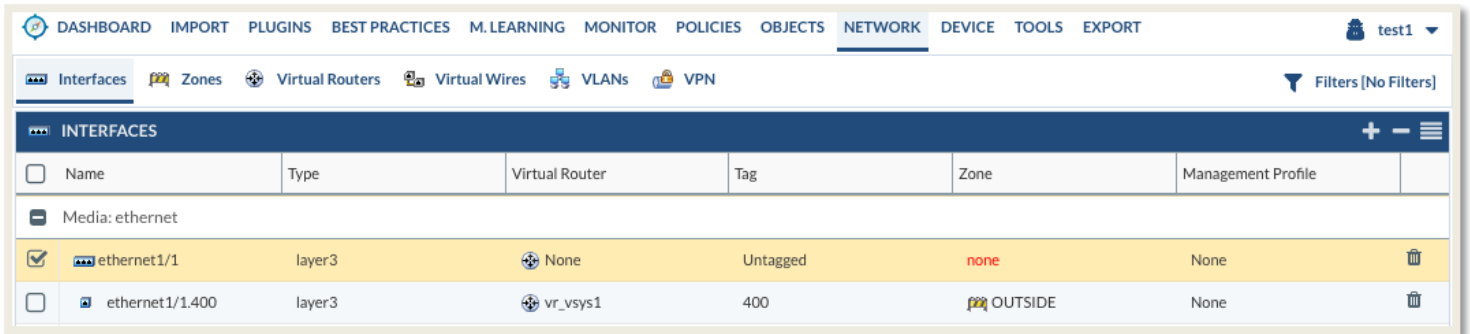
Expedition when imports configurations from other vendors keeps the original interface names to make the validation process easier after the import. Problem with that is that naming usually doesn't match the one that Palo Alto Networks expects so we have to rename them to ensure the changes will be captured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

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

To convert to the proper naming convention, we can select the Ethernet1/1 who 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.



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



We have to repeat the process to adapt all the interfaces we want to migrate.

Import your Base Configuration

What is the Base configuration?

Base configuration is devices specific configuration usually taken from the PA 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 we have imported and manipulated. The result of the merge should be a working and migrated Palo Alto configuration.

The first PanOS configuration imported into the project will be assigned as Base Configuration. The Base configuration is the one will be used at the time to export the configuration out from Expedition or by generating a XML file or API calls. Any change made to the Base Configuration will be applied to the Output.

To import a Base Configuration, you should select the IMPORT TAB from the PALO ALTO TAB and provide a link to your XML file that you previously exported from your PanOS device or just double click in one of the devices added to the project (if any) to import the config from the snapshot stored in Expedition.

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.

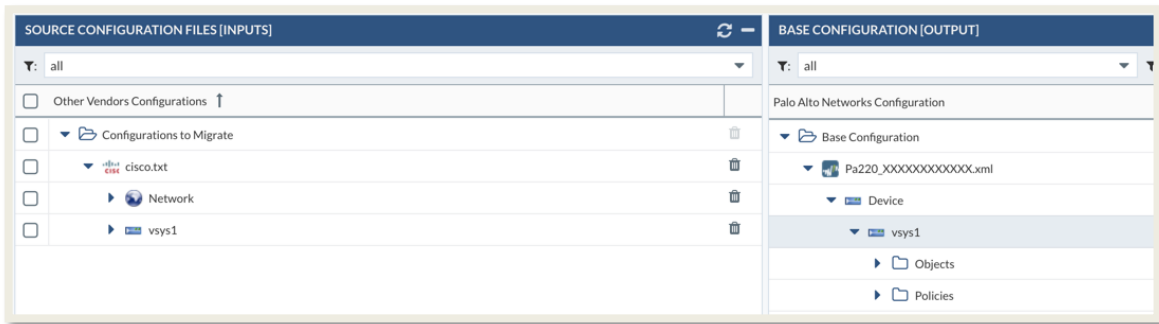
From there we can select what objects we want to move from the left panel to the Base configuration (right panel) by using drag and drop.

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

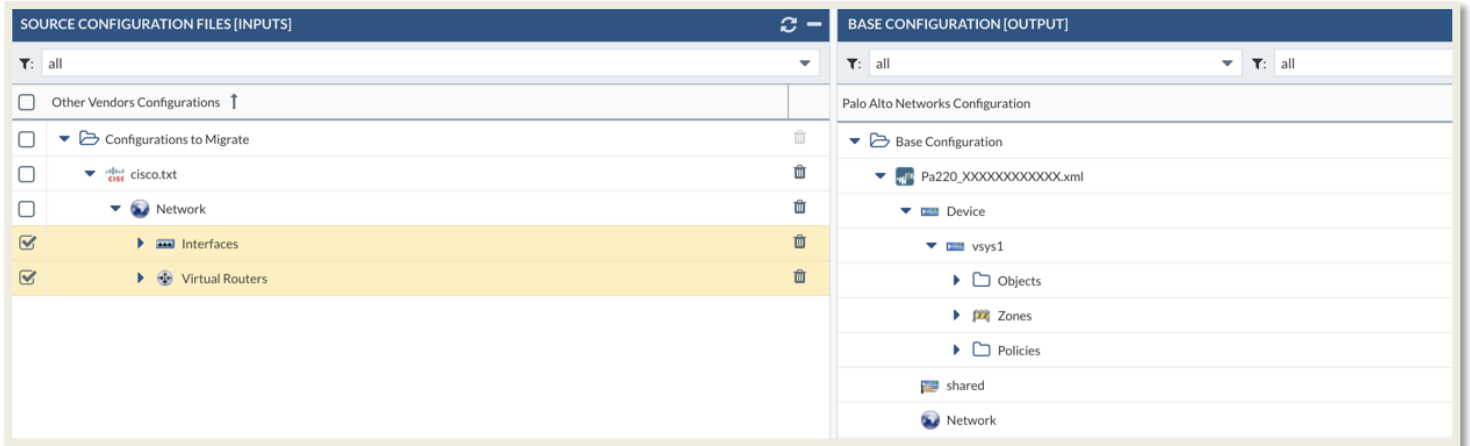
Merge Objects to your Base Configuration

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

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

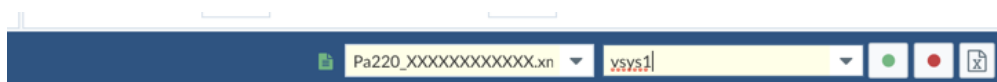


Repeat the same procedure with the Zones, Interfaces, Virtual router(s) and drop them into the correct vsys



The final step is to Merge the migrated configuration and your base configuration and create you final configuration. Just click on the MERGE button

After this action, all the selected objects will be transferred from one configuration to the Base configuration. So, if we want to see how it looks we need to change from the bottom bar the selected configuration and the vsys to the Base Configuration 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 to options to deploy it, one is manual XML file export that can be deployed on the PA device that we are migrating to, or if that PA device is already connected to Expedition, we can use API calls to send parts of the configuration or the whole configuration to the device.

Find Duplicates after the merge and removing them

It is recommended that you run another check for duplicates and remove/merge them after a configuration migration. A common scenario is to have duplicates amongst objects/services/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 in the duplicated object to go to the object view and Expedition will filter by duplicated by name predefined filter.

| PROJECT STATISTICS | | | | | |
|----------------------------|-------|------------|----------|--------|---------|
| Object | Count | Duplicated | Disabled | Unused | Invalid |
| Address | 3856 | 0 | 0 | 532 | 0 |
| Services | 1598 | 346 | 0 | 339 | 0 |
| Address Groups | 965 | 220 | 0 | 237 | 0 |
| Service Groups | 307 | 79 | | 133 | 0 |
| Regions | 6 | 1 | | 6 | 0 |
| Security Rules | 3357 | 671 | 5 | 0 | 0 |
| Nat Rules | 2 | 0 | 0 | 0 | 0 |
| Application Override Rules | 2 | 1 | 0 | 0 | 0 |
| Security Zone | 0 | 0 | 0 | 0 | 0 |
| Interfaces | 0 | 0 | 0 | 0 | 0 |
| IPSec Tunnels | 0 | 0 | 0 | 0 | 0 |

Click on the number

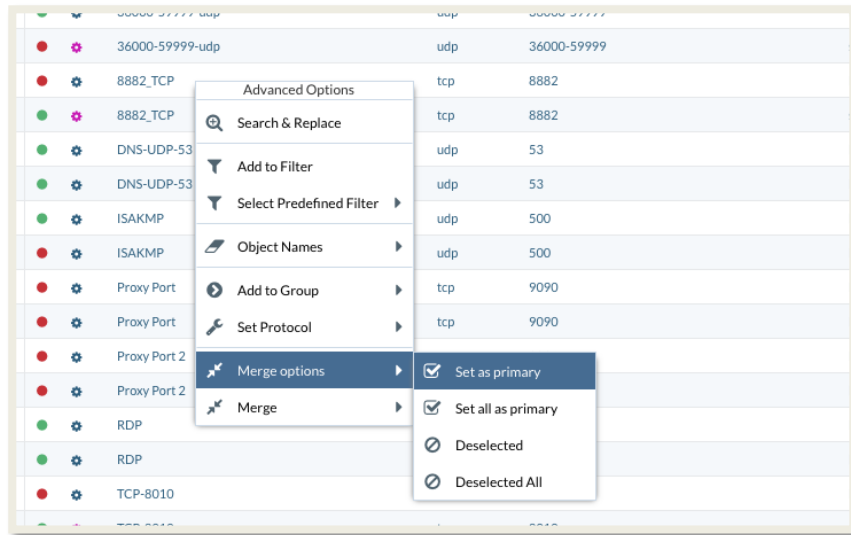
We will check Duplicated services to demonstrate the workflow to follow to get rid of them

| Address Services Applications Contents Users Regions Tags Other | | | | | |
|---|--|-----------------|----------|-------------|--------------------------|
| SERVICES | | | | | |
| <input type="checkbox"/> | | Name | Protocol | Dst Port | Vs |
| <input type="checkbox"/> | | 36000-59999-udp | udp | 36000-59999 | <input type="checkbox"/> |
| <input type="checkbox"/> | | 36000-59999-udp | udp | 36000-59999 | <input type="checkbox"/> |
| <input type="checkbox"/> | | 8882_TCP | tcp | 8882 | <input type="checkbox"/> |
| <input type="checkbox"/> | | 8882_TCP | tcp | 8882 | <input type="checkbox"/> |
| <input type="checkbox"/> | | DNS-UDP-53 | udp | 53 | <input type="checkbox"/> |
| <input type="checkbox"/> | | DNS-UDP-53 | udp | 53 | <input type="checkbox"/> |

The object in PINK is a SHARED object, so that means we have selected from the bottom bar the VSYS equal to ALL, this will do the 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 we can select the duplicated objects we want to keep and after that right click and select Merge Options and “Set as Primary”, that will tell Expedition that after Merge the duplicated objects keep the one we set as Primary.



When the object has been set as Primary you will notice because a new icon will show up.

| SERVICES | | | | | | |
|--------------------------|--|-----------------|----------|-------------|---------|----|
| <input type="checkbox"/> | | Name | Protocol | Dst Port | Vsys | sr |
| <input type="checkbox"/> | | 36000-59999-udp | udp | 36000-59999 | DC-F... | |
| <input type="checkbox"/> | | 36000-59999-udp | udp | 36000-59999 | shared | |
| <input type="checkbox"/> | | 8882_TCP | tcp | 8882 | DC-F... | |
| <input type="checkbox"/> | | 8882_TCP | tcp | 8882 | shared | |

Now we 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” -> “By Name & Value”, this will be applied or to the selected objects or in case you didn’t select any will be applied to all the results from the filter applied.

We 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.

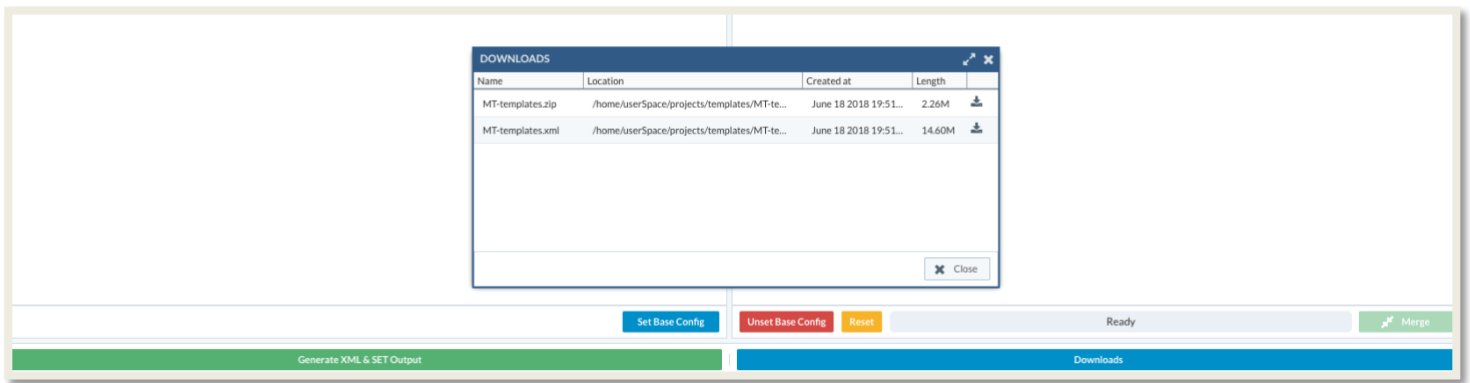
All this can be done with the right click “Select predefined filter”.

Generating the Output

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

We have to navigate to the Export TAB.

Under Mapping TAB there is a button at the bottom bar-left named "Generate XML & SET Output". Pressing this button Expedition will generate the 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 show up. You can click on the Downloads button to get access to that window as well



We can generate API Calls to be send to our devices in case we had created them before and we added to the project we are working on. In that case we will go under the TAB called "API Output Manager"

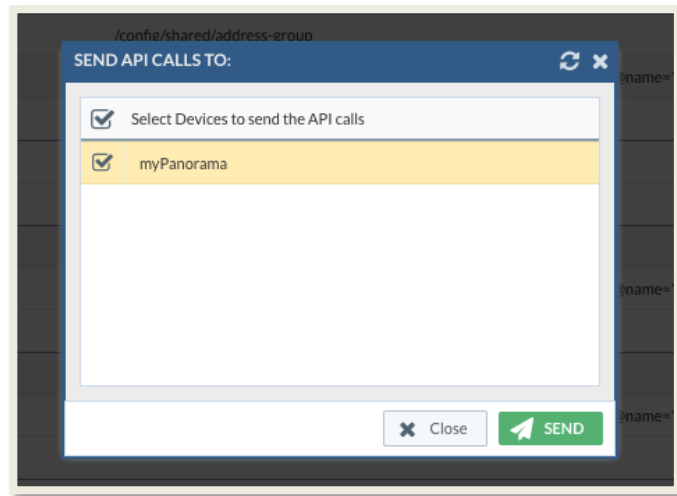
Here you have several options, we will start covering Atomic and Subatomic.

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

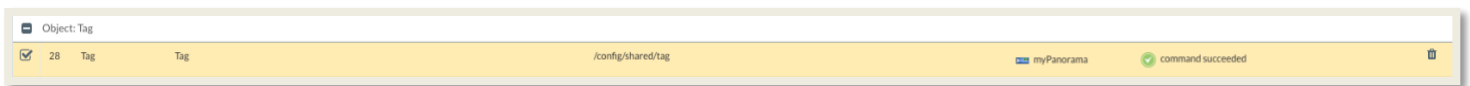
First Step click on "Atomic" or "Subatomic" and click on the "Step 1" button to create all the API calls.

After that the ID of each API call will tell us the order in what we have to send the API call, order matters. Or if you don't select any ALL API calls will be sent in the proper order.

Click "Step 2" button and select the DEVICE where you want to send the API calls and Send them All.



After send the API call you will get the response from the device itself, if was successful you will see in the output



Appendix A: Import

Importing CSV files

From within a Project its possible to import CSV files containing objects we want to add to our 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. First select the object type you want to import. Ex. Static Routes.
2. Select the CSV file from your Laptop

SOURCE

Object To Import: Static Routes CSV File: Browse...

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

| 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 |

| Column | Field Mapping |
|--------|---------------|
| col0 | ipaddress |
| col1 | netmask |
| col2 | tointerface |
| col3 | Gateway |

Displaying 1 - 3 of 3

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

In this example routes are part of Templates and need to be imported into a Virtual-Router plus select the virtual-system where our VR is located. Then we can click on Import Data.

Order matters, if want to import Service Groups we need to first import the services used on those Groups if not the fail will not successful.

Importing an Iron-Skillet Day1 Configuration

Iron-Skillet it's a project made by Palo Alto Networks to create a configuration that it's 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 base to migrate something else on top its super simple now with the integration we built in Expedition.

Process

Create a project and click to get in. After you enter the project go to IMPORT. Then locate the TAB called IRON-SKILLET and click there.

From here we can configure some parameters before the configuration is created. We can modify the parameters by hand or if we have an Iron-Skillet configuration file we can load it to automatically fill the fields.

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

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

```
# 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 <sshoad@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": "forthe love of all things holy changeme",
    # 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",
}
```

The screenshot displays the 'IRON-SKILLET' configuration page in the Expedition tool. The top navigation bar includes 'DASHBOARD', 'IMPORT', 'PLUGINS', 'BEST PRACTICES', 'M. LEARNING', 'MONITOR', 'POLICIES', 'OBJECTS', 'NETWORK', 'DEVICE', 'TOOLS', and 'EXPORT'. Below this, a sub-navigation bar lists various vendors: 'PALO ALTO', 'CSV', 'CHECKPOINT', 'CISCO', 'FORTINET', 'IBM XGS', 'JUNIPER', and 'FORCEPOINT'. The 'PALO ALTO' tab is active.

The main content area is divided into two sections. The top section, 'Single File', has a description: 'Upload a Panos or Panorama configuration XML file. Export it from your device.' It includes an 'XML File:' input field with a 'Browse' button. The bottom section, 'Multiple Files (in ZIP)', has a description: 'Upload a ZIP file with all the configurations to import.' It includes a 'ZIP File:' input field with a 'Browse' button.

Below these sections is the 'IRON-SKILLET' configuration area. It starts with an 'Information' section containing a project description and instructions. This is followed by a 'Select first what type of configuration you want to create' section with a 'Configuration Type' dropdown set to 'NG-Firewall' and a 'PanOS © Version' dropdown set to '8.0'. A 'LOAD FROM CLIPBOARD' button is also present.

The configuration area is divided into three columns: 'Device', 'Logging', and 'Management'. The 'Device' column contains fields for 'ADMINISTRATOR_USERNAME' (iron-skillet), 'ADMINISTRATOR_PASSWORD' (fortheloveofalldthingsholychangeme), 'FW_NAME' (firewall), 'SINKHOLE_IPV4' (72.5.65.111), and 'SINKHOLE_IPV6' (2600:5200::1). The 'Logging' column contains fields for '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), and 'CONFIG_EXPORT_IP' (192.0.2.3). The 'Management' column contains fields for 'MCMT_TYPE' (static selected), 'DNS_1' (8.8.8.8), 'DNS_2' (8.8.4.4), 'NTP_1' (0.pool.ntp.org), and 'NTP_2' (1.pool.ntp.org).

At the bottom left is a 'RESET' button, and at the bottom right is a green 'GENERATE CONFIG AND IMPORT' button.

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

Revision History

| Date | Revision | Comment |
|-----------------|----------|---------------------------------|
| June 22, 2018 | A | First release of this document. |
| October 16,2018 | B | Added Appendix A |