



Palo Alto Networks Application Framework - Lab Guide

Table of contents

Full Lab Deployment Instructions

[Application-Framework-Lab](#)

Application Framework FAQs

[Application-Framework-FAQs](#)

API Usage Examples

[API-Curl-Examples](#)

API Explorer Only Deployment Instructions

[API-Explorer-Lab](#)

Application-Framework-Lab

Cortex Hub Full Lab Deployment via AWS CloudFormation

This document describes how to automatically set up a lab environment on Amazon Web Services that can be used to generate logs for Palo Alto Networks Cortex Hub. It is meant for Palo Alto Networks partners and customers that need a quick way to start developing on Application Framework.

It also provides instructions on how to pair the API Explorer application with Cortex Hub.

Doc Revision: 2019-03-01-21:34:38 (UTC)

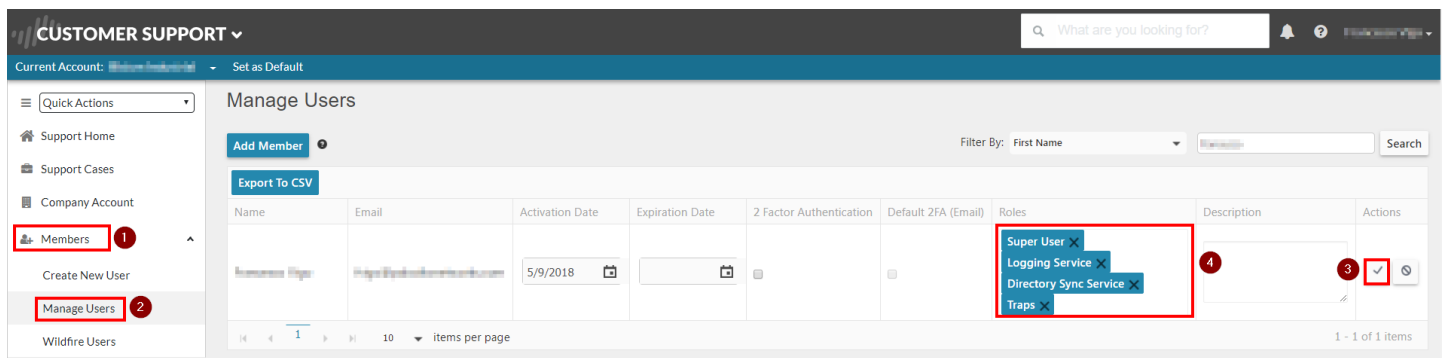
Please make sure you always use the latest revision of this document and the required files:

- Wiki home: <https://github.com/PaloAltoNetworks/appframeworklab/wiki>
- This document: <https://github.com/PaloAltoNetworks/appframeworklab/wiki/Application-Framework-Lab>
- Documentation PDF (incl FAQ): <https://github.com/PaloAltoNetworks/appframeworklab/blob/master/pdf/LabGuide.pdf> Cortex Hub Lab GitHub Repo: <https://github.com/PaloAltoNetworks/appframeworklab>
- AWS Full Lab CloudFormation Template JSON file: <https://raw.githubusercontent.com/PaloAltoNetworks/appframeworklab/master/cft/appframework-lab-v3.json>

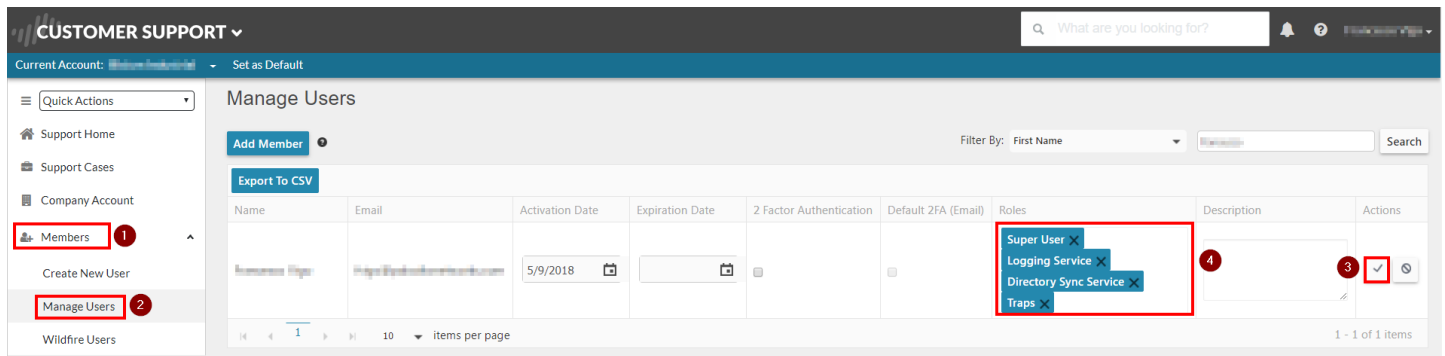
Prerequisites

This lab environment requires the following:

- A valid Palo Alto Networks Customer Support Portal (CSP) Account with the **SuperUser**, **Logging Service**, **Directory Sync Service** and **Traps** roles enabled for your organization (If you don't have one already, once you receive the licenses, you can create an account here: <https://support.paloaltonetworks.com/UserAccount/PreRegister>). The following picture shows how to configure the permissions in CSP:



Note: once you set up the CSP account, please write down the CSP ID (from the browser URL, as shown below), and communicate it to your Palo Alto Networks technical contact:



- A valid AWS Account with the following permissions:
 - Deploy EC2 Instances (at least 2 large)
 - AWS Region with at least 2 available Elastic IPs (EIP)
 - (optional) Route53 Hosted Zone Creation and Configuration
- Palo Alto Networks Licenses (provided by your Business Development or Developer Relations contact):
 - Panorama (serial number and support Auth Code)
 - VM-Series Firewall (2x Auth Codes per firewall (base and bundle))
 - Logging Services (Auth Code)
 - (optional) Traps (Auth Code)
- (optional) A second or third level domain configured in AWS Route53 (i.e. lab.yourcompany.com with NS records pointing to AWS Route 53 DNS Servers): ask your Palo Alto Networks representative for more details.

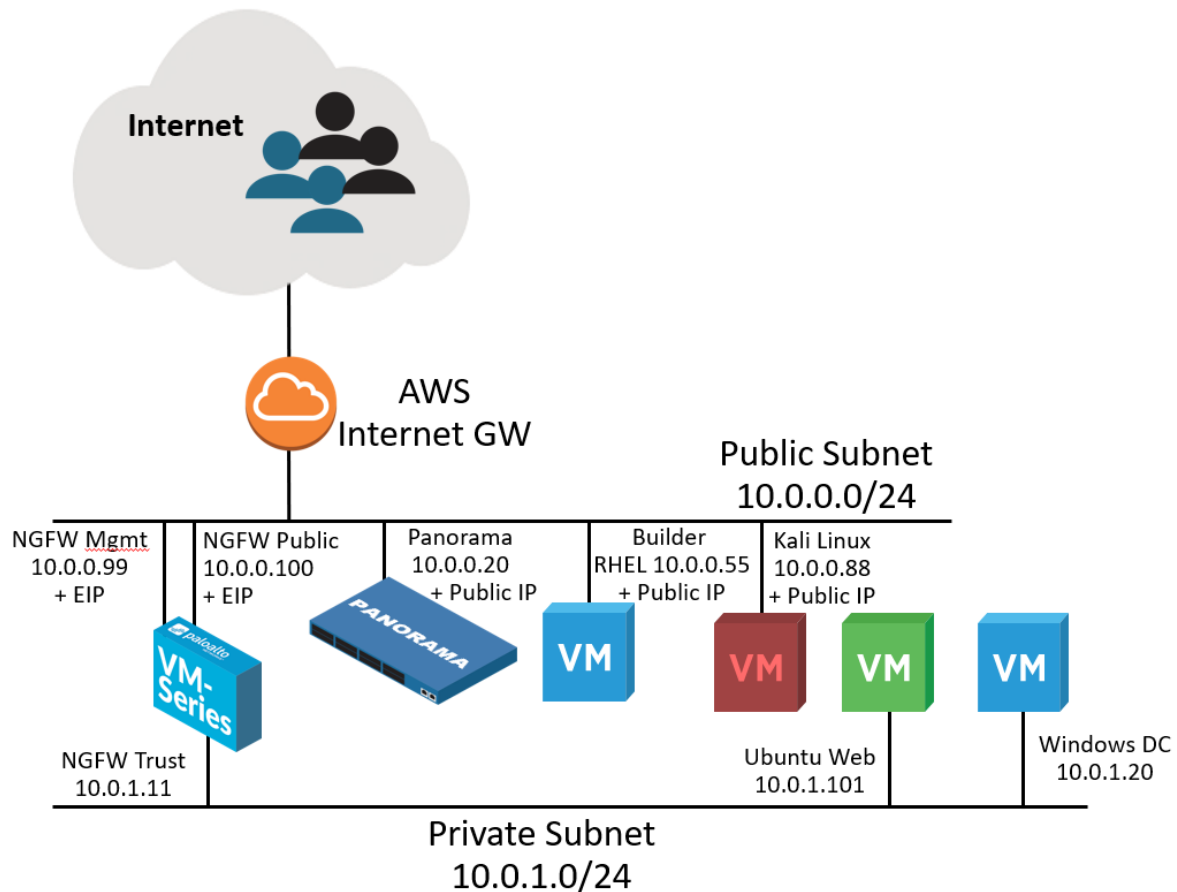
Lab Topology and features

The AWS CloudFormation template automatically deploys a network topology that can be used to generate different logs end events to be sent to the Palo Alto Networks Cortex Hub.

The following components are included in the template:

- Panorama (10.0.0.20 + public IP assigned for remote reachability). **Once the setup is complete, the Panorama VM can be shut down (not destroyed) to reduce the cost of the lab**
- Next-Generation Firewall VM Series with the following interfaces:
 - Management: 10.0.0.99 (+ EIP assigned for remote reachability)
 - Public (10.0.0.100) (+ EIP assigned for remote reachability)
 - Internal (10.0.1.11)
- builder VM running RHEL (10.0.0.55 + public IP assigned for remote reachability). **Once the setup is complete, the builder VM be shut down and terminated to reduce the cost of the lab**
- (optional) Kali Linux VM (10.0.0.88 + public IP assigned for remote reachability)
- Ubuntu Web Server behind the firewall (10.0.1.101, reachable via SSH through the firewall Public EIP on port 221)
- (optional) Windows Server 2012 R2 Domain Controller behind the firewall (10.0.1.20, reachable via RDP through the firewall Public EIP on port 3389)

The network topology is depicted in the following diagram:



Once created, the environment automatically starts generating traffic through a web crawler installed on the Ubuntu Web server VM. It automatically and periodically updates the User-to-IP mapping on the firewall via API, so the traffic logs will appear with "user1" as source user. The crawler also periodically downloads a sample test PE from the Palo Alto Networks web site, that will trigger a Wildfire event. SSL Decryption is automatically enabled on the firewall with SSL Forward Proxy, and all the web requests from the VMs in the private subnet are decrypted: both the Ubuntu Web server VM and the Windows Domain Controller trust the Firewall pre-created certificate for SSL Decryption. The certificate used by the NGFW for decryption is static and has been pre-added in the environment configuration to simplify the automation: it is possible to replace it post deployment (instructions are not provided in this document).

- For details on VM information and useful commands, see Appendix A
- For details on EIP associations, see Appendix B

Some URL categories (sports, finance-services) are configured to be blocked or to generate alerts on the firewall, and the web crawler will hit those categories, to automatically generate URL filter events.

A Kali Linux VM can also be deployed and used to generate attacks on the Ubuntu Web Server VM, in order to generate Threat Logs on the Firewall (need to be done manually, see Appendix A).

NAT rules are configured on the Firewall Public Interface (10.0.1.100, with an EIP associated to it) that allow reachability to the VMs behind it:

- Port 3389 to RDP into the Windows Domain Controller
- Port 221 to SSH on the ubuntu Web Server VM

The CloudFormation template allows to specify an Administrative password that is automatically configured on the following systems:

- Next-Generation Firewall (for the *admin* user)
- Panorama (for the *admin* user)
- Windows Domain Controller:
 - Domain Admin user (specified at deployment, default is 'paloalto')
 - Other users (user1, user2, user3 -- also with Domain Admin privileges)

Since the password is used widely, it's recommended to select one with a good level of complexity.

Note: if you delete the Stacks deployed through this CFT, make sure you manually delete the EC2 Volumes that are left for the NGFW VM, otherwise you will end up using space unnecessarily.

Security Hardening Considerations

This environment is meant for development use only, it's not security hardened for production. Specifically, the following security considerations should be known:

- Active Directory Password Complexity is disabled
- Administrative password is provided as an environment variable for the installation scripts on the builder VM, Ubuntu Web Server VM and Windows Server VM (`var/lib/cloud/instances/i-("instanceid")/scripts/part-001` script in Linux VMs, `c:\cfn\scripts\pw.txt` in Windows), so it may be visible in some of the log and configuration files (i.e. `/tmp/deploy/vars.yml` and `/var/log/user-data.log` on the builder and under the logs in `c:\cfn` on the Windows Server VM) - you can manually delete those files post deployment.
- The Panorama/NGFW SSH private key is generated by the Cloud Formation template and is still enabled to access Panorama and Firewall. The private key is also written in the bootstrap scripts (`var/lib/cloud/instances/i-("instanceid")/scripts/part-001` , `/tmp/deploy/vars.yml`) on the builder machine and also saved in `/tmp/deploy/key.pem` . - you can manually delete those files post deployment and modify the access credentials on Panorama and NGFW to disallow access via ssh key.

Summarizing, to perform additional hardening of the environment, the following post-deployment steps are suggested:

- Manually change the admin passwords on Panorama and NGFW
- Remove the bootstrap scripts from all VMs, and the `/tmp/deploy` folder from the builder VM
- Remove or replace the SSH key for authentication on NGFW and Panorama for admin users
- Re-enable Password complexity on Domain Controller
- Replace the Decryption SSL certificate on NGFW, and import it on both Ubuntu Web Server VMs and Domain Controller

This document does not provide instructions for the above steps.

Palo Alto Networks Customer Support Portal Configuration

This section describes how to register the licenses and activate the services on the Palo Alto Networks Customer Support Portal (CSP)

1. Login to <https://support.paloaltonetworks.com> using your CSP (Customer Support Portal) account
2. Navigate to "Assets", "Devices" and click on "Register New Device", then select "Register device using Serial Number or Authorization Code", then "Submit"

The screenshot shows the Palo Alto Networks Customer Support Portal interface. The top navigation bar includes 'CUSTOMER SUPPORT' and a search bar. The current account is 'Technical Business Development'. The left sidebar contains a 'Quick Actions' menu and a list of navigation items: 'Support Home', 'Support Cases', 'Company Account', 'Members', 'Groups', 'Assets', 'Devices', 'Line Cards/Optics/FRUs', 'Spares', 'Advanced Endpoint Protection', and 'VM-Series Auth-Codes'. The 'Assets' menu item is highlighted with a red box and a '1' callout. The 'Devices' sub-menu is also highlighted with a red box and a '2' callout. The main content area shows the 'Devices' page with a 'Register New Device' button highlighted with a red box and a '3' callout. Below this button are buttons for 'Deactivate License(s)', 'Device Tag', and 'Hide Expired License(s)'. A table lists devices with columns for 'Serial Number', 'Case History', 'Model Name', 'Device Name', 'Group', 'License', 'Actions', 'Auth Code', and 'Expiration Date'. A modal window titled 'Device Type' is open, showing two options: 'Register device using Serial Number or Authorization Code' (selected) and 'Register usage-based VM-Series models (hourly/annual) purchased from public cloud Marketplace or Cloud Security Service Provider (CSSP)'. The 'Submit' button in the modal is highlighted with a red box and a '5' callout.

3. Insert your Panorama serial number and fill in the other required fields. Then click on **Agree and Submit**:

The screenshot shows the 'DEVICE REGISTRATION' form. The form is titled 'DEVICE REGISTRATION' and has a close button in the top right corner. The form is divided into two sections: 'DEVICE INFORMATION' and 'EULA'. The 'DEVICE INFORMATION' section contains the following fields: 'Serial Number' (text input, highlighted with a red box and a '1' callout), 'Device Name' (text input, highlighted with a red box and a '2' callout), 'Device Tag' (dropdown menu, highlighted with a red box and a '2' callout), and 'Device will be used' (checkbox for 'Offline'). The 'EULA' section contains the text: 'By clicking "Agree and Submit" below, you agree to the terms and conditions of our [END USER LICENSE AGREEMENT](#) and [SUPPORT AGREEMENT](#).' Below the EULA text is a 'Required' label and three buttons: 'Agree and Submit' (highlighted with a red box and a '3' callout), 'Refuse', and 'Refuse'.

4. You will need to associate the Panorama Support Authcode with the Panorama serial that you registered. From the **Devices** page under the **Assets** tab, click on the **Actions** icon on the line that correspond to the Panorama serial number you just added:

CUSTOMER SUPPORT Q What are y

Current Account: XXXXXXXXXX Set as Default

Quick Actions

- Support Home
- Support Cases
- Company Account
- Members
- Groups
- Assets
- Devices
- Line Cards/Optics/FRUs
- Spares
- Advanced Endpoint Protection
- VM-Series Auth-Codes

Devices

Register New Device Deactivate License(s) Device Tag Hide Expired License(s) Filter By: Serial Number

[Export To CSV](#)

Serial Number	Case History	Model Name	Device Name	Group	License	Actions	Auth Code	Expiration Date
XXXXXXXXXX		PAN-PA-200	accessPA		Threat Prevention Premium Partner Support Lab Bundle Threat Prevention		XXXXXXXXXX XXXXXXXXXX	6/28/2013 11/28/2013
XXXXXXXXXX		PAN-PA-200-LAB	New-PA-200		PAN-DB URL Filtering GlobalProtect Gateway GlobalProtect Portal Standard Support WildFire License		XXXXXXXXXX	7/25/2017 7/25/2017 7/25/2017 Perpetual 7/25/2017
XXXXXXXXXX		PAN-PRA-25-NFR			Device Management License Logging Service NFR Support	1	XXXXXXXXXX XXXXXXXXXX	Perpetual 4/24/2019 4/24/2019

5. Select "Activate Auth-Code", insert the Panorama support Auth-Code (the one that corresponds to the PAN-SVC-NFR-PRA-25 SKU) and click on "Agree and Submit":

Device Licenses

Device Licenses

Serial Number: XXXXXXXXXX

Model: PAN-PRA-25-NFR

Device Name:

Feature Name	Authorization Code	Expiration Date	Actions
Logging Service	XXXXXXXXXX	04/24/2019	
NFR Support	XXXXXXXXXX	04/24/2019	
Device Management License	XXXXXXXXXX	Perpetual	

To activate the license feature for DNS Security, the OS version for the firewall must be 9.0 or above

Activate Licenses

Activate Auth-Code 1

Auth-Code Activation

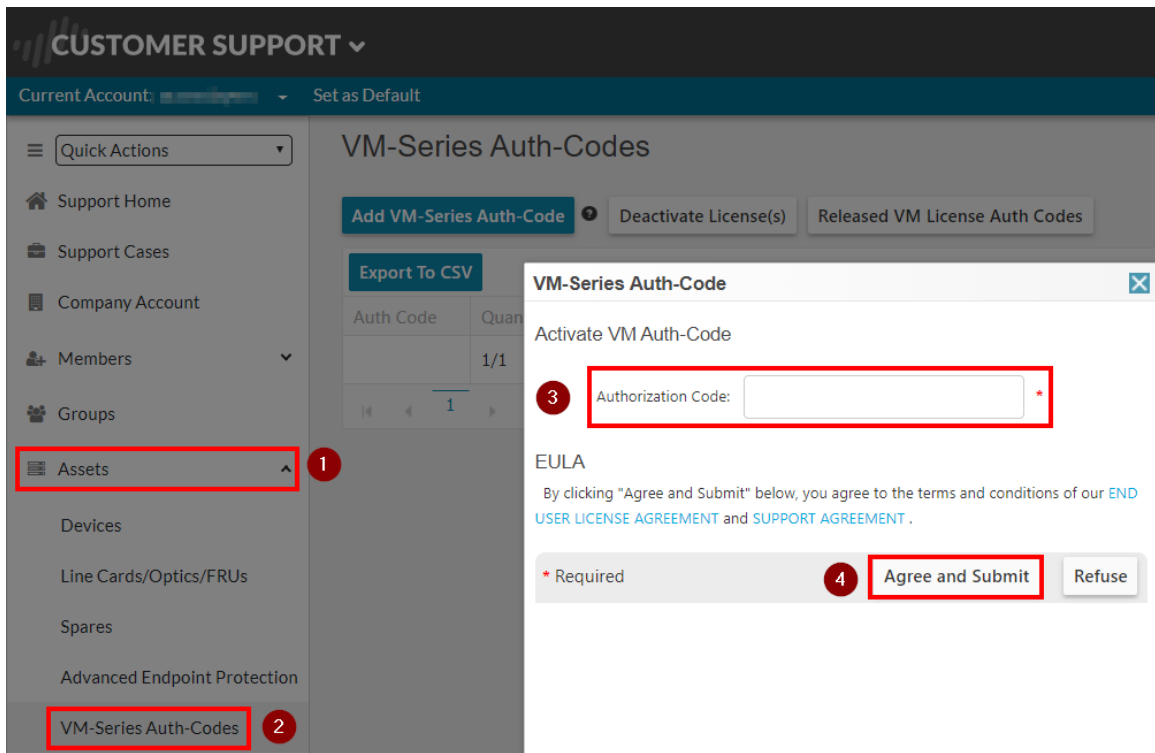
Authorization Code: * 2

EULA

By clicking "Agree and Submit" below, you agree to the terms and conditions of our [END USER LICENSE AGREEMENT](#) and [SUPPORT AGREEMENT](#).

3

6. Navigate to "Assets", then go to "VM-Series Auth-Codes", select "Add VM-Series Auth-Code". Enter the VM-Series Auth-Code (the one that corresponds to the PAN-VM-100-NFR SKU) and click on "Agree and Submit":



7. Navigate to "Assets", then select "Cortex Hub" and click on "Activate Cortex Hub Auth-Code".
8. Enter the Logging Service Auth-Code. Then select the serial number of the Panorama device that you entered in the previous step, and the region (americas). Then click on "Agree and Submit":

ACTIVATE CLOUD SERVICES AUTH-CODE

Upon activation of your Cloud Service, please go to the Logging Service app on [Cloud Services Portal](#) to adjust log quota for this app. [More details](#)

Authorization

Code: * 1

Panorama: * 2

Logging Region: * 3

EULA

By clicking "Agree and Submit" below, you agree to the terms and conditions of our [END USER LICENSE AGREEMENT](#) and [SUPPORT AGREEMENT](#).

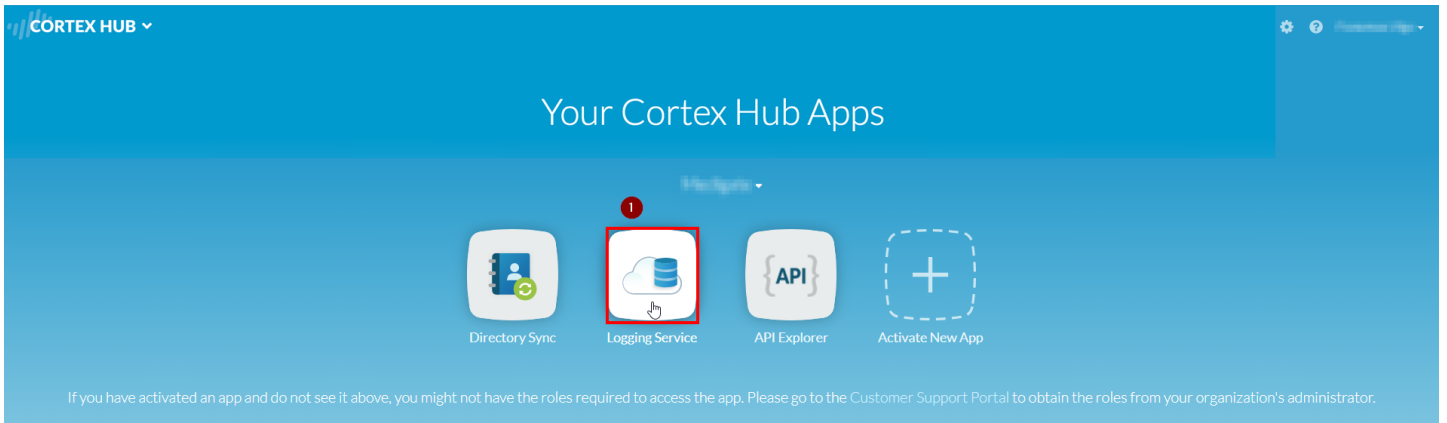
* Required

Note: If you don't see the option to activate the Cortex Hub, you might not have the required permissions in the Support Portal (CSP). You need the *Super User* permission. If the Panorama instance doesn't show in the list, make sure that you added the support Authcode (Step 5).

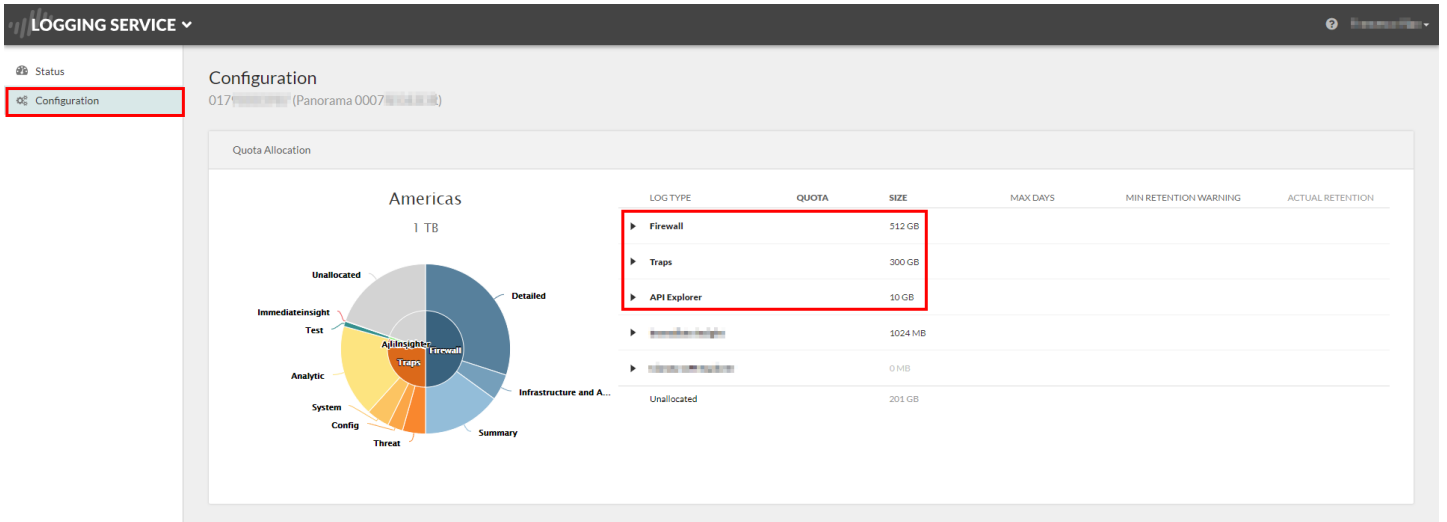
Logging Service Quota

Before moving forward, set up the Logging Service Quota to make sure that logs can be received successfully.

1. Navigate to the Cortex Hub at <https://apps.paloaltonetworks.com> and sign in with your CSP account credentials.
2. Click on the "Logging Service" icon in the screen:



3. In the "Logging Service" page, click on **Configuration**, and assign some quota (100 GB) to *Firewall*, *Traps* and *API Explorer*, as shown in the following picture:



Note: if you don't see API Explorer, it means that the app hasn't been activated yet by your Palo Alto Networks technical contact. You will configure this later.

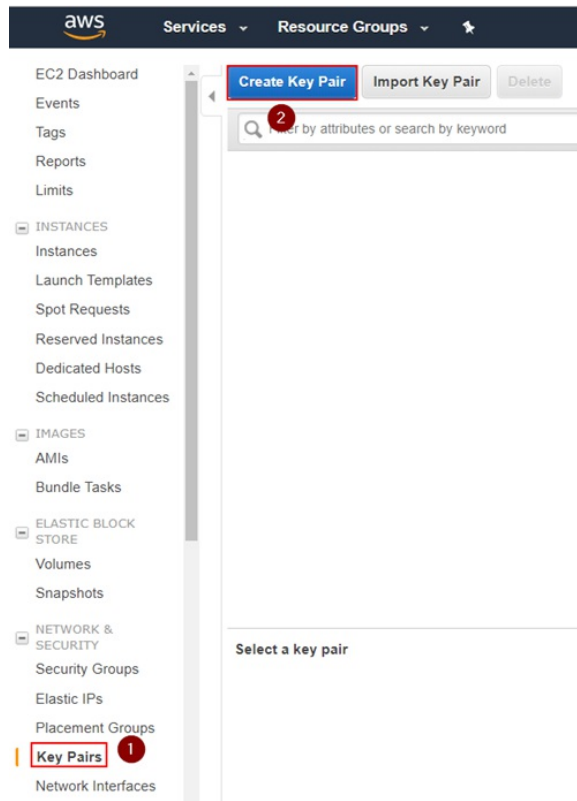
AWS Configuration

This section describes the configuration of the AWS required components to deploy the lab components. You'll need a Key Pair (either existing or new) and (optionally) a Route53 Hosted Zone. You'll also need to accept the terms for Palo Alto Networks VM-Series, Panorama and Kali Linux in the AWS Marketplace in order to deploy the required VMs.

Key Pair Creation

It's recommended to use a dedicated key pair for this deployment, but you can use an existing one if you prefer. If using an existing one (that needs to be present in the same region as you will use to deploy the lab), skip this section.

1. Navigate to your selected region (i.e. us-east-1), select the EC2 service and under **Network & Security** select **Key Pairs** and click on **Create Key Pair**:



2. Insert a keypair name and click on "Create". In the example, we use "paloalto". This will create a "paloalto.pem" private key and the AWS Web UI will prompt you to download it.



3. Download the Private Key to your local machine. The file name of this example will be **paloalto.pem**, but you can choose an arbitrary name. You will need this key later to SSH into the deployed linux VMs and, optionally, on the NGFW and Panorama.

Route53 Zone Configuration

The CloudFormation Template deploys a series of VMs (Firewall, Panorama, API Explorer, Kali Linux, etc.) and AWS can automatically associate DNS names to the Elastic and Public IPs that are used by EC2. To do that, you need a Route53 public Hosted Zone configured in your AWS environment. This step is optional: you can just connect to the VMs via their Elastic/Public IP addresses, or manually configure your DNS entries at a later stage if you're not using Route53.

The public DNS zone you use can either be an existing second-level domain (i.e. yourcompanylab.com), or a third-level domain (lab.yourcompany.com). It must be publicly resolvable, so you need to be the registered owner of the domain. As an option, you can register a new domain directly through the AWS console and add it automatically in Route53.

If you don't have the opportunity to use a second or third level domain in Route53, and you still want to use FQDNs instead of IPs to access your lab, ask your Palo Alto Networks technical contact for support to get a fourth level domain delegated to your Route53 DNS Servers (i.e. yourcompany.dev.appframework.rocks).

To create a Hosted zone in AWS Route 53, proceed through the following steps:

1. Navigate to AWS "Route53", go to "Hosted zones" and click on "Create Hosted Zone". Enter the domain name: it must be a public domain name (second or third level) where you have permissions configure name servers for (i.e. yourcompanylab.com or lab.yourcompany.com). The type must be "Public Hosted Zone." Then click on **Create**:

2. Look at the AWS Name Servers listed in the NS record and configure your Domain Hosting provider platform to use them for the selected domain:

Name	Type	Value	Evaluate Target Health	Health Check ID	TTL	Region	Weight	Geolocat
lab.hhq.cloud	NS	ns-829.awsdns-39.net. ns-1192.awsdns-21.org. ns-2012.awsdns-59.co.uk. ns-36.awsdns-04.com.	-	-	172800			
lab.hhq.cloud	SOA	ns-36.awsdns-04.com. awsdns-hostmaster.amazon.	-	-	900			

In this example we are using the third-level domain `lab.hhq.cloud`.

Note: if you registered the domain through AWS, you don't need any additional configuration as it will be automatically registered in Route

53. If you're using a different domain hosting platform (i.e. GoDaddy, NameCheap, etc.), the configuration on how to configure your domain to use AWS Route53 DNS servers will be different depending on your provider.

If you're being helped by Palo Alto Networks to use a fourth level domain (i.e. `yourcompany.dev.apptframework.rocks`), you can skip this step as the Route53 configuration will happen automatically as part of the template deployment.

Activate Palo Alto Networks VMs Series, Panorama and Kali Linux on AWS Marketplace

To deploy some of the VMs, you first need to activate them on the AWS marketplace. Note that deploying Kali Linux is optional (is useful to generate threats in the firewall logs) so, if you don't need it, you can skip the step for Kali Linux (but not for Next Generation Firewall and Panorama).

To activate the solutions on the AWS Marketplace, follow this procedure:

1. Navigate to the AWS Marketplace (<https://aws.amazon.com/marketplace>), search for "kali" and click on the search icon:

2. In the results page, click on **Kali Linux**:

3. In the Kali Linux page, click on **Continue to Subscribe**:



Kali Linux

Sold by: [Kali Linux](#) Latest Version: Kali Linux 2018.1*

Kali Linux is a Debian-based Linux distribution aimed at advanced Penetration Testing and Security Auditing.

Linux/Unix ★★★★☆ (5)

Free Tier



Continue to Subscribe

Save to List

Typical Total Price

\$0.046/hr

Total pricing per instance for services hosted on t2.medium in US East (N. Virginia). [View Details](#)

4. Click on "Accept Terms":

You will be subscribed to this software and agree that your use of this software is subject to the pricing terms and the seller's End User License Agreement (EULA) and your use of AWS services is subject to the [AWS Customer Agreement](#)



Accept Terms

This table shows pricing information for the listed software components. You will be charged separately for your use of each component.

5. Repeat the same procedure for both Palo Alto Networks "VM-Series Next-Generation Firewall (BYOL)" and "Palo Alto Networks Panorama"

VM-Series Next-Generation Firewall (BYOL)

Manual Launch

With EC2 Console, API or CLI

Service Catalog

Copy to SC and Launch

Launch Options

You can click the "Launch with EC2 Console" buttons below and follow the instructions to launch an instance of this software.

You can also find and launch these AMIs by searching for the AMI IDs (shown below) in the "Community AMIs" tab of the EC2 Console Launch Wizard.

You can view this information at a later time by visiting the Your Software page. For help, see step-by-step instructions for launching Marketplace Products from the AWS Console.

▼ Version

PAN-OS 8.1.0, released 03/13/2018

Usage Instructions

Palo Alto Networks Panorama

1-Click Launch
Review, modify and launch **Manual Launch**
With EC2 Console, API or CLI **Service Catalog**
Copy to SC and Launch

Click "Accept Software Terms & Launch with 1-Click" to launch this software with the settings below

Once you accept the terms, you will have access to launch any version of this software in any supported region. For future launches, you can return to this page or launch directly from the EC2 console, APIs or CLI.

► **Version**
Panorama 8.1.0, released 03/13/2018

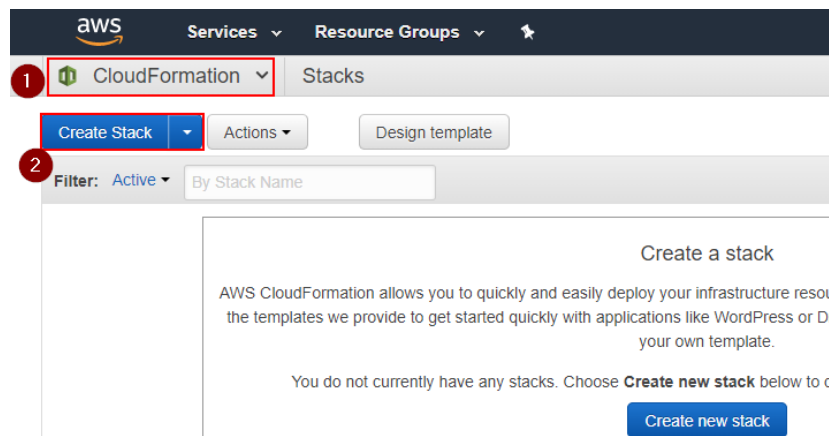
Before continuing, make sure you're able to see the subscriptions by navigating to your AWS Marketplace Software Subscriptions page here https://aws.amazon.com/marketplace/library?ref_=header_user_your_software

Deploy the CloudFormation Template

You can now deploy the AWS CloudFormation Template (CFT) to create the lab environment. Before starting, make sure that you have 2 Elastic IPs (EIPs) available in the region you want to deploy the CFT (by default AWS limits EIPs to 5 per region per account. If you don't have enough EIPs available, you can request more via AWS support: usually takes only a few minutes).

Note: this tutorial is displaying screenshots of the older CloudFormation console. If you use the redesigned console, the output will be slightly different, but the process is identical. Proceed with the following steps:

1. Navigate to "AWS CloudFormation" and select "Create Stack":



2. Select "Specify an Amazon S3 template URL", and input the following URL: <https://s3.amazonaws.com/applicationframework-conf/templates/appframework-lab-v3.json>. Then click on **Next**:

Select Template

Select the template that describes the stack that you want to create. A stack is a group of related resources that you manage as a single unit.

Design a template Use AWS CloudFormation Designer to create or modify an existing template. [Learn more.](#)

Design template

Choose a template A template is a JSON/YAML-formatted text file that describes your stack's resources and their properties. [Learn more.](#)

Select a sample template

Upload a template to Amazon S3

Choose File No file chosen

1 Specify an Amazon S3 template URL

2 [View/Edit template in Designer](#)

Cancel

3 Next

1. Input the required parameters. Please pay attention on inserting the right values in the right order (i.e Authcodes), in order to avoid failed deployments:

- **Stack name:** an arbitrary name for this lab deployment (i.e. AppFrameworkLab)
- **Admin Password:** an arbitrary password that will be used for the following systems:
 - NGFW admin user
 - Panorama admin user
 - Windows Domain Controller admin (the default username is "paloalto", but can be changed in the advanced parameters below)
 - Windows Domain Users (user1, user2, user3)
- **EC2 VMs Key Name:** from the drop down menu, select the Key Pair that you want to use to SSH in the Linux VMs. It can be the Key Pair that you previously created in EC2, or an existing one.
- **AuthCode1:** Insert the VM Series capacity license Authcode you received from Palo Alto Networks and previously registered in the Support Portal (the SKU is **PAN-VM-100-NFR**)
- **AuthCode2:** Insert the VM Series services and support Authcode you received from Palo Alto Networks. Note that this hasn't been registered on the portal (the SKU is **PAN-VM-100-BND-NFR**)
- **Panorama Serial:** Insert the Panorama Serial number that was provided by Palo Alto Networks and previously registered in the Support Portal.
- **DNS Domain Name:** Insert the domain name zone that you have configured on Route53. If you don't have it, add a random name and select *false* under the **"Map FQDNs to Public/Elastic IPs in Route53"** field in the *"Advanced DNS Configuration"* section. In the example we use the **lab.appframework.rocks** domain.

The following screenshot shows an example configuration:

Specify Details

Specify a stack name and parameter values. You can use or change the default parameter values, which are defined in the AWS CloudFormation template. [Learn more.](#)

Stack name AppFrameworkLab

Parameters

Basic Configuration - REQUIRED

Admin Password	
	Password for NGFW/Panorama admin user, Windows DC admin and users. Must be at least 8 characters containing letters, numbers and symbols	
AuthCode1	<input type="text"/>	
	VM-Series Capacity Licence AuthCode (SKU: PAN-VM-100-NFR)	
AuthCode2	<input type="text"/>	
	VM-Series Bundle AuthCode (SKU: PAN-VM-100-BND-NFR4)	
EC2 VMs Key Name	appframeworklab-oregon	
	Name of an existing EC2 KeyPair to enable SSH access to VMs. Except NGFW and Panorama	
Panorama Serial	0007	<input type="text"/>
	Panorama Serial Number (provided by Palo Alto Networks)	
DNS Domain Name	test.appframework.rocks	
	DNS Domain Name or Route53 Hosted Zone Name (i.e. appframework.mycompany.com)	

There are some advanced options that could be useful, such as the Timezone for Firewall and Panorama and the toggles to deploy the Kali Linux VM and the Windows VMs. By default the Kali Linux VM is deployed, while the Windows Domain Controller is not:

Advanced Configuration: Options

Deploy Kali VM	<input type="text" value="true"/>	Deploy Kali Linux VM?
Deploy Windows DC	<input type="text" value="false"/>	Deploy W2012R2 Domain Controller?
NGFW and Panorama Timezone	<input type="text" value="US/Pacific"/>	Firewall and Panorama timezone

Leave all the other parameters to the default values unless you are a power user and you know what you're doing.

2. Click on "Next".

3. In the options page, expand the **Advanced** options and select **No** under **Rollback on failure**. This will allow you to try to recover manually if a failure occurs late in the stage of deployment:

Advanced

1 You can set additional options for your stack, like notification options and a stack policy. [Learn more.](#)

Notification options

No notification

New Amazon SNS topic

Topic

Email

Existing Amazon SNS topic

Existing topic ARN

Termination Protection ⓘ Enabled

Disabled

Timeout ⓘ Minutes

Rollback on failure ⓘ Yes

No 2

Note: if a failure occurs immediately (i.e. within the first 5 minutes of the deployment), it's likely that something is wrong with the parameters or AWS configuration/permissions. The recommended procedure is to delete the stack and redeploy once the problem is solved. Trying to recover from a failed deployment is recommended only after the entire AWS setup completes (~5-10 minutes) and the process gets stuck during the configuration phase. For more details, please reach out to your Palo Alto Networks technical contact.

4. Click on "Next".

5. In the Review page, at the bottom, under "Capabilities", check the both **1 acknowledge that AWS CloudFormation might create IAM resources with custom names** and **1 acknowledge that AWS CloudFormation might require the following capability: CAPABILITY_AUTO_EXPAND** boxes, and click on "Create":

Capabilities

1 ⓘ The following resource(s) require capabilities: [AWS::IAM::Role, AWS::CloudFormation::Stack]

This template contains Identity and Access Management (IAM) resources. Check that you want to create each of these resources and that they have the minimum required permissions. In addition, they have custom names. Check that the custom names are unique within your AWS account. [Learn more.](#)

For this template, AWS CloudFormation might require an unrecognized capability: CAPABILITY_AUTO_EXPAND. Check the capabilities of these resources.

1 acknowledge that AWS CloudFormation might create IAM resources with custom names.

1 acknowledge that AWS CloudFormation might require the following capability: CAPABILITY_AUTO_EXPAND

[Quick Create Stack](#) (Create stacks similar to this one, with most details auto-populated)

Cancel Previous **2** Create

Note: the CFT will create some IAM roles to allow some of the VMs to Read configuration files from S3 buckets and execute Lambda functions that will create the temporary key pairs.

6. Sit down and relax, the whole process will take up to an hour to complete. If it fails within the first 5-10 minutes, look at the Event logs for errors and try to solve the problem. Early failures often result in missing permissions in AWS, failure to subscribe to the marketplace items or lack of available Elastic IPs in the region.

Note that the deployment might spawn a child template after several minutes, in case the optional Windows Domain controller VM is being deployed as well, as shown in the following screenshot:

CloudFormation ▾ Stacks

Create Stack ▾ Actions ▾ Design template

Filter: Active ▾ By Stack Name

Showing 2 stacks

Stack Name	Created Time	Status	Description
PartnerLab1-DomainControll... NESTED	2018-03-22 21:13:19 UTC-0700	CREATE_IN_PROGRE...	This template creates 1 Active Directory Domain Controller in a private subnet. The d...
PartnerLab1	2018-03-22 21:12:13 UTC-0700	CREATE_IN_PROGRE...	Palo Alto Networks AppFramework PlayGround with API Explorer

8. You can keep refreshing the deployment status and check the **Events**. Once you see the **WebVMWaitCondition** creation initiated, as shown in the following pictures, you can optionally SSH into the builder VM and check the deployment status for errors:

Overview Outputs Resources **Events** Template Parameters Tags Stack Policy Change Sets Rollback Triggers

Filter by: Status ▾ Search events

2019-02-06	Status	Type	Logical ID	Status Reason
08:45:48 UTC-0800	CREATE_IN_PROGRESS	AWS::CloudFormation::WaitCondition	WebVMWaitCondition	Resource creation Initiated
08:45:47 UTC-0800	CREATE_IN_PROGRESS	AWS::CloudFormation::WaitCondition	WebVMWaitCondition	
08:45:42 UTC-0800	CREATE_COMPLETE	AWS::EC2::Instance	WebVM	
08:45:42 UTC-0800	CREATE_COMPLETE	AWS::Route53::RecordSet	BuilderFQDN	
08:45:11 UTC-0800	CREATE_IN_PROGRESS	AWS::Route53::RecordSet	BuilderFQDN	Resource creation Initiated
08:45:10 UTC-0800	CREATE_IN_PROGRESS	AWS::EC2::Instance	WebVM	Resource creation Initiated
08:45:10 UTC-0800	CREATE_IN_PROGRESS	AWS::CloudFormation::Stack	DomainControllerTemplate	Resource creation Initiated
08:45:10 UTC-0800	CREATE_IN_PROGRESS	AWS::Route53::RecordSet	BuilderFQDN	

9. (optional) Use the SSH Private Key (`appframework-oregon.pem` in the example) to connect from your computer to the builder Linux machine, using the `ec2-user` account. If you have enabled the Route53 configuration, the FQDN will automatically resolve in `builder.lab.yourdomain.com`, using the Route53 configured domain (`lab.appframework.rocks` in the example). If you didn't configure Route53, you will need to check in EC2 which is the Public IP address of the builder VM.

```
ec2-user@ip-10-0-0-55~
root@BLLMR:~# ssh -i appframeworklab-oregon.pem ec2-user@builder.
The authenticity of host 'builder.lab.appframework.rocks ( )' can't be established.
ECDSA key fingerprint is .
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'builder.lab.' (ECDSA) to the list
of known hosts.
[ec2-user@ip-10-0-0-55 ~]$
```

10. (optional) You can run the command `tail -f /tmp/deploy/ansible.log` to check the status of the configuration. There will be errors and timeouts, don't worry. If there are new messages being displayed every minute, the process is still ongoing. If nothing appears for more than a couple of minutes, there might be an issue. Also, if the `ansible.log` file doesn't exist, check the output of the `/var/log/user-data.log` file for errors, and reach out to your Palo Alto Networks technical contact.

```
ec2-user@ip-10-0-0-55~
[ec2-user@ip-10-0-0-55 ~]$ tail -f /var/log/user-data.log

TASK [Start Configure Panorama] *****
changed: [localhost]

TASK [Panorama Configure Firewall] *****
changed: [localhost]

TASK [wait_for_firewall] *****
FAILED - RETRYING: wait_for_firewall (57 retries left).
FAILED - RETRYING: wait_for_firewall (56 retries left).
```

11. (optional) If the automated configuration completes, the `ansible.log` file should show a message similar to the one displayed in the following screenshot (note the `failed=0` in the last line). If something goes wrong, you can explore the content of the `/tmp/deploy` folder to check if the variables in `vars.yml` are correct. Reach out to your Palo Alto Networks technical contact for troubleshooting. If everything goes well, the CloudFormation will complete shortly after you see the final output message.

```

ec2-user@ip-10-0-0-55~
*****
2019-02-06 17:17:12,200 p=12313 u=root | ok: [localhost]
2019-02-06 17:17:12,206 p=12313 u=root | TASK [ansible-pan : pip] *****
*****
2019-02-06 17:17:16,438 p=12313 u=root | ok: [localhost]
2019-02-06 17:17:16,443 p=12313 u=root | TASK [ansible-pan : pip] *****
*****
2019-02-06 17:17:17,354 p=12313 u=root | ok: [localhost]
2019-02-06 17:17:17,360 p=12313 u=root | TASK [Lab Include variables (free-form)] *****
*****
2019-02-06 17:17:17,399 p=12313 u=root | ok: [localhost]
2019-02-06 17:17:17,404 p=12313 u=root | TASK [appframework lab] *****
*****
2019-02-06 17:17:30,048 p=12313 u=root | changed: [localhost]
2019-02-06 17:17:30,053 p=12313 u=root | TASK [Lab Commit All] *****
*****
2019-02-06 17:17:32,097 p=12313 u=root | FAILED - RETRYING: Lab Commit All (5 retries left).
2019-02-06 17:19:11,048 p=12313 u=root | changed: [localhost]
2019-02-06 17:19:11,051 p=12313 u=root | PLAY RECAP *****
*****
2019-02-06 17:19:11,051 p=12313 u=root | localhost : ok=6 changed=2 un
reachable=0 failed=0

```

12. Eventually, the deployment will show **CREATE_COMPLETE** once everything is done:

Stack Name	Created Time	Status	Drift Status	Description
AppFrameworkLab-DomainC... <small>NESTED</small>	2019-02-06 08:45:10 UTC-0800	CREATE_COMPLETE	NOT_CHECKED	Palo Alto Networks Application Framework Lab Domain Controller Nested Template
AppFrameworkLab	2019-02-06 08:39:50 UTC-0800	CREATE_COMPLETE	NOT_CHECKED	Palo Alto Networks Application Framework Developer Lab

Note: if you run in an error, make sure you added the right licenses and Auth-Codes, check the FAQ document and reach out to your Palo Alto Networks contact for support.

13. You can select template and click on the **Outputs** tab of the to view the deployment information (IP addresses and FQDNs) of the lab.

14. You can also see all the DNS records added to Route53 Hosted zone (in case you enabled Route53 configuration)

Panorama Pairing with Logging Service

The last step of the process requires to pair your Panorama Instance with Logging Service:

1. Navigate back to <https://support.paloaltonetworks.com> and login with your CSP credentials
2. Go to "Assets", "Cloud Services" and click "Generate OTP". Select the Panorama instance you've created (corresponding to the Panorama Serial Number) and click on "Generate OTP":

CUSTOMER SUPPORT ▾

Current Account: *Test User at Palo Alto Networks, Palo Alto* ▾

Quick Actions ▾

Support Home

Support Cases

Company Account

Members ▾

Groups

Assets **5**

Devices

Line Cards/Optics/FRUs

Spares

Advanced Endpoint Protection

VM-Series Auth-Codes

Cloud Services **4**

Site Licenses

Enterprise Agreements

Asset History

Search Current Account

Cloud Services

Activate Cloud Services Auth-Code **3** Generate OTP Try a Product ⓘ

Export To CSV

Auth Code	Serial Number	Model Name	Quantity	License Description
...	...	Logging Service	1 TB	Logging Service with 1TB of storage, 1-year, includes Premium Support
...	...	Logging Service		
...	...	Logging Service		
...	...	Logging Service		
...	...	Logging Service		
...	...	Logging Service		
...	...	Logging Service		
...	...	Logging Service		
...	...	Logging Service		
...	...	Logging Service		
...	...	Logging Service		

Generate Cloud Services One Time Password ✕

Generate Cloud Services One Time Password

The OTP provides users the password to input into the Cloud Services. This is a required step to enable secure use of the cloud services. This password is only valid for 10 minutes. If the time has expired before you have use this password, please generate a new password.

Panorama : 000 *Test User* **2**

Password : `dcae6fa03a3feba15d9b2cf2dc2a79
8ae9d74df2b5372a3347a2fb2db52
55296cca0d2468cffe05243e05152c
b2a47e843ec6e9de8cef2b32a0bd
00ea9a59106e988f27f44674811372`

Expires On : 2/6/2019 10:01:11 AM **1**

Copy to Clipboard **1** Generate OTP Close

3. Copy the generated One Time Password in your browser clipboard by clicking on **Copy to Clipboard**:

CUSTOMER SUPPORT ▾

Current Account: *Test User at Palo Alto Networks, Palo Alto* ▾

Quick Actions ▾

Support Home

Support Cases

Company Account

Members ▾

Groups

Assets

Devices

Line Cards/Optics/FRUs

Spares

Advanced Endpoint Protection

VM-Series Auth-Codes

Cloud Services

Site Licenses

Enterprise Agreements

Asset History

Search Current Account

Cloud Services

Activate Cloud Services Auth-Code Generate OTP Try a Product ⓘ

Export To CSV

Auth Code	Serial Number	Model Name	Quantity	License Description
...	...	Logging Service	1 TB	Logging Service with 1TB of storage, 1-year, includes Premium Support
...	...	Logging Service		
...	...	Logging Service		
...	...	Logging Service		
...	...	Logging Service		
...	...	Logging Service		
...	...	Logging Service		
...	...	Logging Service		
...	...	Logging Service		
...	...	Logging Service		

Generate Cloud Services One Time Password ✕

Generate Cloud Services One Time Password

The OTP provides users the password to input into the Cloud Services. This is a required step to enable secure use of the cloud services. This password is only valid for 10 minutes. If the time has expired before you have use this password, please generate a new password.

Panorama : 000 *Test User*

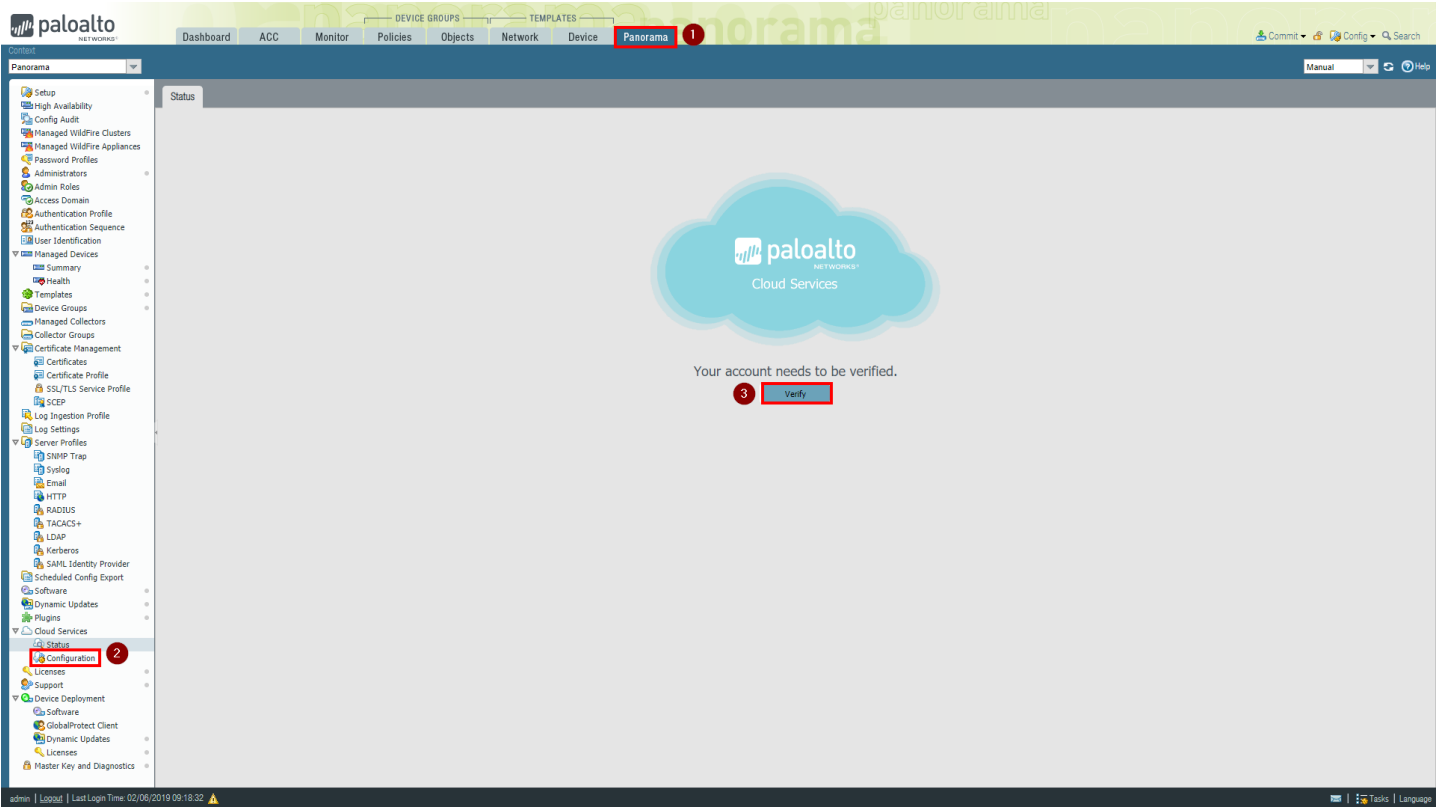
Password : `dcae6fa03a3feba15d9b2cf2dc2a79
8ae9d74df2b5372a3347a2fb2db52
55296cca0d2468cffe05243e05152c
b2a47e843ec6e9de8cef2b32a0bd
00ea9a59106e988f27f44674811372`

Expires On : 2/6/2019 10:01:11 AM

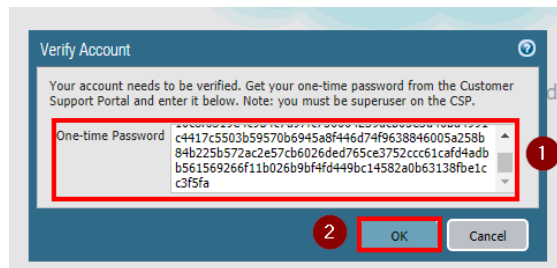
1 Copy to Clipboard Generate OTP Close

4. Login to Panorama via the web UI, navigating to <https://panorama.lab.yourdomain.com> (assuming that Route53 has used to automatically create the FQDN, otherwise look at the EIP of the Panorama instance). Use the "admin" user and the password you have configured in the template.

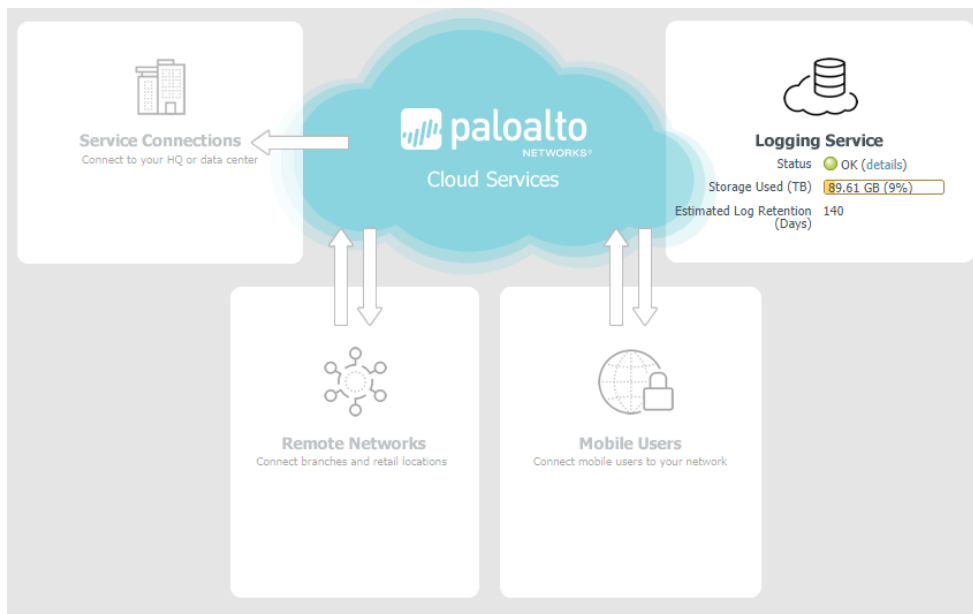
- On the Panorama UI, navigate to **Panorama**, **"Cloud Services"**, **"Configuration"** (If you don't have the option to **"Verify"** go to **"Licenses"** directly below **"Configuration"** and select **"Retrieve license keys from license server"** before verifying):



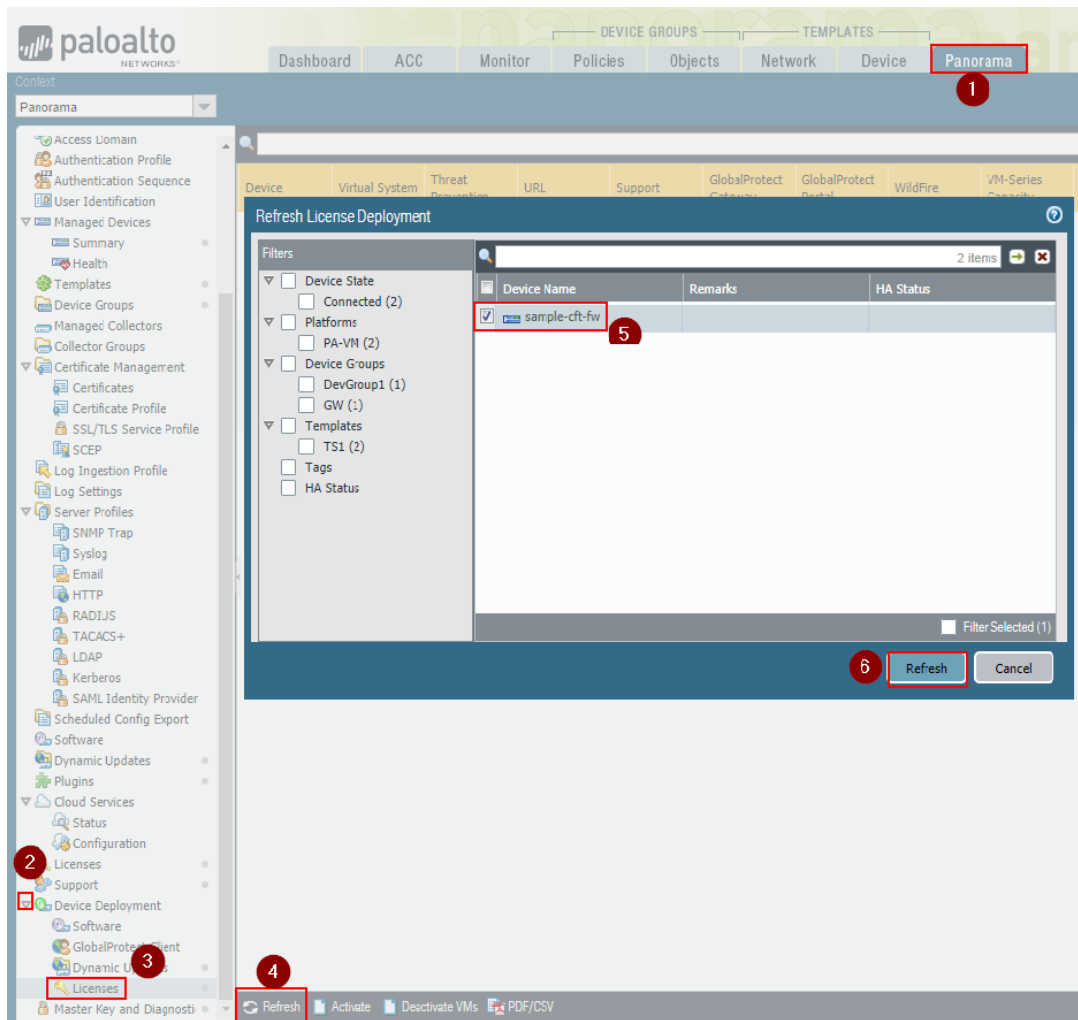
- Insert the previously copied One Time Password (OTP) to complete the pairing and click on **OK**:



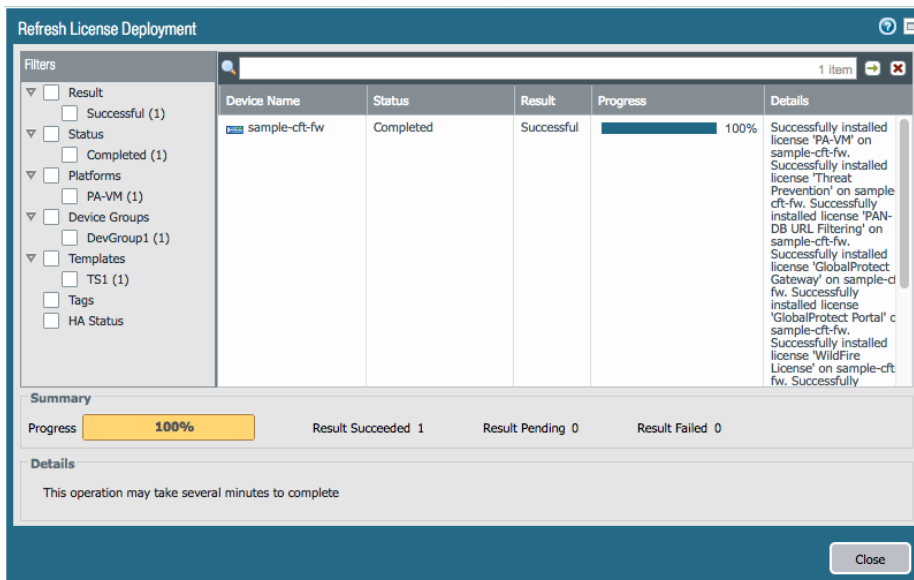
After the pairing is complete, in the "Status" page under "Cloud Services", you should see a dashboard similar to the following:



- On the Panorama UI, navigate to **Panorama**, **"Device Deployment"**, **"Licenses"** and click on **Refresh**.
- Select the firewall (**ngfw** or **sample-ct-fw** in the example) and click on **"Refresh"** to refresh the licenses:



The refresh process will take a few seconds. Wait until it completes:



After the license refresh is complete, wait a few minutes.

Under the Monitor tab in Panorama you should be able to view Logs (see Appendix C)

Congratulations, the setup is complete!

You can work with your Palo Alto Networks contact to make sure that the API Explorer application is active in your Application Portal.

If you haven't done already, please write down the CSP ID (from the browser URL, as shown below), and communicate it to your Palo Alto Networks technical contact:

CUSTOMER SUPPORT What are you looking for? Set as Default

Current Account: Set as Default

Quick Actions

Support Home

Support Cases

Company Account

Members 1

Create New User

Manage Users 2

Wildfire Users

Manage Users

Add Member

Export To CSV

Filter By: First Name Search

Name	Email	Activation Date	Expiration Date	2 Factor Authentication	Default 2FA (Email)	Roles	Description	Actions
Resuman Raju	Raju.Palathal@paloaltonetworks.com	5/9/2018				Super User Logging Service Directory Sync Service Traps		3 4 5

10 items per page

1 - 1 of 1 items

If done, please move on to the activation phase.

API Explorer App Activation Process

This section describes how to Activate the API Explorer application and start interacting with the APIs.

Note: Before proceeding, please make sure you have assigned some Logging Service quota to the API Explorer app in the Logging Service configuration, as described in the *Logging Service Quota* section of this document.

To activate the API Explorer, follow this process:

1. Navigate to the Cortex Hub beta environment: <https://apps.paloaltonetworks.com> and Sign in with your Customer Support Portal credentials:

Welcome to Cortex Hub

Now you can collaborate between different apps, share threat context and intelligence, and drive automated response and enforcement. [Learn more](#)


[Sign In](#)

[Have an Auth Code? Activate](#)


2. Activate an instance of Directory Sync Service by clicking on the **Activate** button in the **Directory Sync** tile:

CORTEX HUB

Your Cortex Hub Apps




Logging Service



Activate New App


If you have activated an app and do not see it above, you might not have the roles required to access the app. Please go to the Customer Support Portal to obtain the roles from your organization's administrator.

More Available Palo Alto Networks Apps




Directory Sync
Allow Palo Alto Networks Cloud Services to access your organization's directory

1 [Activate](#) [Learn More](#)



Magnifier
Discover malicious activity and stop attackers and malware operating inside your network

[Learn More](#)



Traps
Advanced, multi-method malware prevention that protects users and endpoints

[Learn More](#)

3. Enter an arbitrary **Instance Name** and select **Americas** as **Region**, then click on **OK**:

Directory Sync

* Instance Name: 1

Description:

* Region: 2

Cancel 3

Note: You don't need to actually register an Active Directory agent to it if you don't need to interact with AD data to build your integration. Or you can deploy the Directory Sync Agent on the windows Domain Controller, by following the Getting Started Guide, not covered by this manual

4. Review the configuration by clicking on the Settings icon in the top right corner:



Make sure that you have a Logging Service instance, and a Directory Sync instance.

5. Go back to the main page and navigate to the bottom of the Application Portal page, under **Partner Apps on the Cortex Hub**. Select the application (API Explorer) and click on the **Activate** icon:



Partner Apps on the Application Framework

<p>Zero Trust SOC The ON2IT Zero Trust SOC-as-a-Service offers customers an economical, highly automated Security Operations Center.</p> <p>Activate Learn More →</p>	<p>Silverfort Silverfort enables MFA and AI-based adaptive authentication even for systems that don't support it, without installing...</p> <p>Activate Learn More →</p>	<p>Seclytics The Seclytics app for the Palo Alto Networks® Application Framework delivers forward-deployed predictive intelligence...</p> <p>Activate Learn More →</p>	<p>Microsoft Graph Building on our long-standing partnership, the Microsoft Graph app enables the seamless sharing of data and alerts with integrate...</p> <p>Activate Learn More →</p>
<p>Immediate Insight Immediate Insight is an analytics-enabled threat hunting and investigation platform for the Palo Alto Networks Application...</p> <p>Activate Learn More →</p>	<p>Recorded Future Lookup The Recorded Future Lookup App lets you search traffic and threat logs for evidence of specific IOCs in your network...</p> <p>Activate Learn More →</p>	<p>Portnox CLEAR A leading risk management, access control and network visibility capability delivered seamlessly as a cloud-based app.</p> <p>Activate Learn More →</p>	<p>Critical Start ATAP Critical Start's Advanced Threat Analytics Platform Application for the Application Framework orchestrates the investigation o...</p> <p>Activate Learn More →</p>
<p>Cybeats IoT Radar The Cybeats IoT Radar app utilizes contextual data derived from Application Framework to provide better visibility into IoT...</p> <p>Activate Learn More →</p>	<p>SecBI Threat Detection SecBI enables PAN users, gain visibility to their network, to quickly understand the full scope of a cyber attack.</p> <p>Activate Learn More →</p>	<p>API Explorer Take the Application Framework for a test drive!</p> <p>1 Activate Learn More →</p>	

Note: if you don't see your API Explorer App, reach out to your Palo Alto Networks technical contact for support.

1. Enter the required parameters, choosing the correct Logging Service and Directory Sync Service instances, then click on **Agree and Submit**:

Activate API Explorer



License Type: apiexplorer

Company Name: Technical Business Development

* Instance Name: ApiExplorer1 **1**

Description: API Explorer **2**

* Region: Americas **3**

* Logging Service: Instance 017... (Panorama 0007...)

If not all Logging Service instances appear, you may need to [activate purchased licenses](#).

* Directory Sync: devrel_dss **4**

* Description: API Explorer

EULA: By clicking "Agree and Activate", you accept the terms of the [End User License Agreement](#).

5 Cancel Agree and Activate

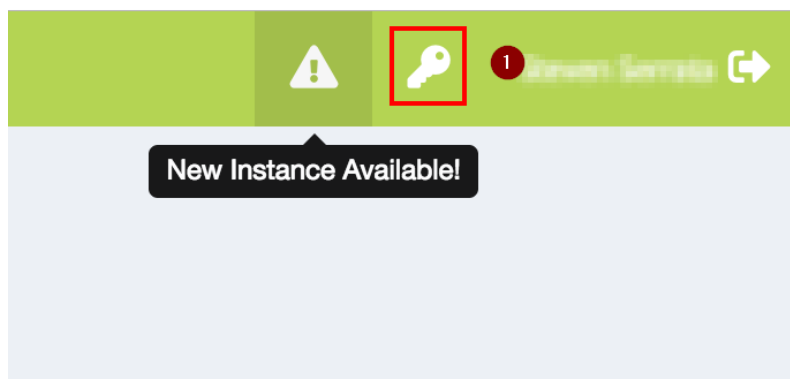
7. At this point you should see the instance of your "API Explorer" App in the "Your Cortex Hub Apps" section of the App Portal:



8. Click on your API Explorer App icon and you will be redirected to the API Explorer application. You should be able to login with the same Palo Alto Networks credentials you used for the Support Portal and Cortex Hub.

Note: Make sure that you login on the API explorer App for the first time through link on the Cortex Hub. Do not login on the API Explorer by navigating to the FQDN directly with your browser, as some required tokens must be passed to the API Explorer by the Cortex Hub through the link.

9. At the first Login, the API explorer app will notify you that a new instance is available. Click on the "Key" icon:



10. In the Authorization page, on the corresponding Instance, click on "Authorize":

AUTHORIZATION





Active Account (select one)

Select account ▼

Active Instance (select one)

Select instance ▼

Manage Instances

ACCOUNT ↑↓	DESCRIPTION ↑↓	INSTANCE ID ↑↓	SCOPE ↑↓	REGION ↑↓	TOKEN ↑↓	↑↓
TBD	New Instance		TBD	americas		 Authorize 

Showing 1 to 1 of 1 entries

11. Insert the required scopes (all of them, or at least the "read" ones) and click on **Authorize**:

API EXPLORER Authorization

Account (select one)

Note: Instances are organized by account ID. Try to select the account the instance was activated under. If you select the wrong account, don't worry, it can be changed later.

Scope * (select one or more)

× logging-service:read × logging-service:write × event-service:read 1
× directory-sync-service:read

Authorize 2

Note: If successful, API EXPLORER will receive tokens necessary for interacting with your Logging, Event and Directory Sync service instances.

12. The "Request for Approval" page on the Identity Provider will show up. Click on "Allow":

Request for Approval

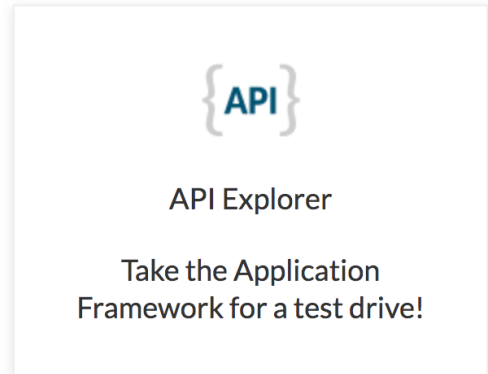
API Explorer is requesting permission for the following:

- Read Logging Service
- Write Logging Service
- Read Event Service
- Read Directory Sync Service

Consent info:

- **API Explorer: apiexplorer_test**
- Region: Americas
- Logging Service: (no name)
- Directory Sync Service: devrel_dss

1



13. If the authorization is successful, you should see the Active Instance and Tokens in the Authorization page, and the application should work:

AUTHORIZATION

Active Account (select one)
Technical Business Development

Active Instance (select one)
48888888-47455-4641104 (New Instance)

Manage Instances

ACCOUNT	DESCRIPTION	INSTANCE ID	SCOPE	REGION	TOKEN
Technical Business Development	New Instance	48888888-47455-4641104	logging-service:read logging-service:write event-service:read directory-sync-service:read	americas	

Congratulations: You can now use the functions of the API Explorer. For example, the "Query Explorer" from the left menu.

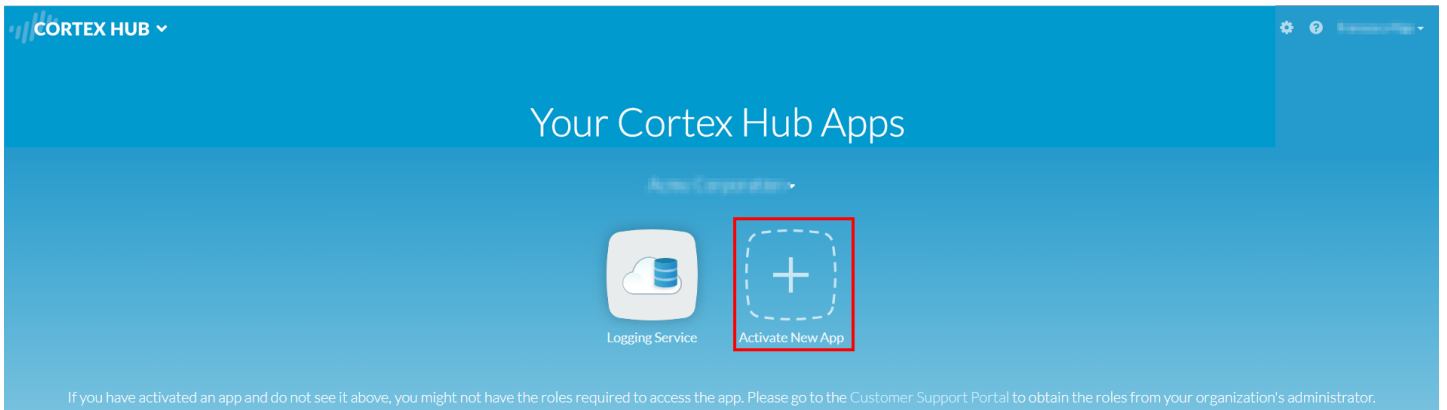
Make sure you look at the [Application-Framework-FAQs](#) for additional details.

(Optional) Traps Configuration

In case you want to enable Endpoint data on Logging Service, you can configure Traps. It doesn't require firewall data and can be done independently from the Firewall setup.

To activate Traps, follow this procedure:

1. Navigate to the Cortex Hub at <https://apps.paloaltonetworks.com> and sign-in with your CSP credentials.
2. Click on "Activate New App":



3. Insert the AuthCode you have received for Traps and click on **Continue**:

Activation - Step 1 of 2

If you've purchased a license from your sales representative, and received a sales order email, enter the auth code from the email.

* Auth Code:

1

2

Cancel **Continue**

4. Insert the required information, including your Traps FQDN prefix, as well the Region, the Logging Service instance you previously configured and, optionally, the Directory Sync Service instance. Then click on **Agree and Activate**:

Activation - Step 2 of 2

To start using the app, please enter the following information.

License Type: Traps

Auth Code:

* Company Name: Palo Alto Networks

1

* Instance Name:

Description:

2

* Subdomain:

3

* Region:

3

* Logging Service:

4

If not all Logging Service instances appear, you may need to [activate purchased licenses](#).

Directory Sync:

EULA: By clicking "Agree and Activate", you accept the terms of the [End User License Agreement](#).

5

Cancel **Agree and Activate**

The setup will take several minutes to complete, then you will be able to navigate to the Traps Management Service console by browsing to the FQDN you configured in the previous step (i.e. <https://yourcompany.traps.paloaltonetworks.com>).

You can then install the Traps Agent on any client machine, including the Windows 2012 Domain Controller VM, in case you have deployed it.

For more information on how to configure and deploy Traps, please follow the product documentation <https://docs.paloaltonetworks.com/traps/tms/traps-management-service-admin.html>

Additional links:

- Traps Licensing: <https://docs.paloaltonetworks.com/traps/tms/traps-management-service-admin/get-started-with-tms/license-the-tms.html>
- Traps Agent Administration Guide: <https://docs.paloaltonetworks.com/traps/5-0/traps-agent-admin.html>

Appendix A: Explanation of the CFT services and usage

Kali Linux VM

Used to generate exploits to trigger Threat events on NGFW

Access server directly with SSH private key with the **ec2-user** user:

```
# ssh -i paloalto.pem ec2-user@kali.lab.yourcompany.com
```

Run threats against web server:

```
# sudo uniscan -u http://10.0.0.100 -esqdw
```

Builder/Installer VM

Installes and configures the lab

You can also access directly with SSH private key with the **ec2-user** user:

```
# ssh -i paloalto.pem ec2-user@apiexplorer.lab.yourcompany.com
```

Public IP

Public IP of the NGFW eth1 interface :

- Use port 221 to access WEB VM through SSH (username is **ubuntu**)
- Use port 3389 to access Windows Domain controller through RDP

Next-Generation Firewall (NGFW)

Palo Alto Networks Next-Generation Firewall

Access directly with SSH private key with the **admin** user:

```
# ssh -i paloalto.pem admin@ngfw.lab.yourcompany.com
```

Or via the WebUI: <https://ngfw.lab.yourcompany.com>

Panorama

Palo Alto Networks Panorama

Access directly with SSH private key with the **admin** user:

```
# ssh -i paloalto.pem admin@panorama.lab.yourcompany.com
```

Or via the WebUI: <https://panorama.lab.yourcompany.com>

Ubuntu Web Server

Traffic generation VM and Web Server

Internal address that can be reached through NGFW public interface (see above)

A web crawler runs on it (for URL and traffic logs, etc)

Access server with SSH private key through firewall mapped port 221 with the **ubuntu** user:

```
# ssh -i paloalto.pem ubuntu@public.lab.yourcompany.com -p 221
```

Useful commands:

- `# crontab -l` (shows the command in the crontab to register IP-to-User mapping with the NGFW API every 15 minutes)
- `# /home/ubuntu/web-traffic-generator` (web traffic generator. It's started during the first boot and it will restart at VM reboot). Configuration is in `config.py`
- If required, manually restart the Web traffic Generator with the following command: `REQUESTS_CA_BUNDLE=/etc/ssl/certs/ca-certificates.crt nohup python /home/ubuntu/web-traffic-generator/gen.py 1>>/tmp/webgen.stdout 2>>/tmp/webgen.stderr &`

Domain Controller:

Windows 2012R2 Domain Controller

Internal IP that can be reached via RDP through NGFW public interface (see above)

Login as yourdomain\youruser (default **PANWDOMAIN\paloalto**), or as user1, user2 or user3

The password is the one you configured in the CFT.

You can install the Directory Sync Service agent on this VM if you want to use it.

Appendix B: Default hostname to IP and VM Mapping

Public Hostname	Internal IP	EIP assigned?	Public IP?	Description
kali	10.0.0.88	N	Y	Kali Linux VM
builder	10.0.0.55	N	Y	Builder/Installer VM

Public Hostname	Public IP?	Description
public	Y	NGFW Public Interface
ngw	N	NGFW Management Interface
panorama	Y	Panorama Management Interface
N/A	N	Ubuntu Web Server VM
N/A	N	Windows Domain Controller VM

Appendix C: Sample log outputs in the monitor tab

Traffic

The screenshot shows the Palo Alto Networks Monitor tab with the 'Traffic' log selected. The table displays log entries with columns: Generate Time, Type, From Zone, To Zone, Source, Source User, Destination, To Port, Application, Action, Rule, Session End Reason, Bytes, Device SN, and Device Name.

Generate Time	Type	From Zone	To Zone	Source	Source User	Destination	To Port	Application	Action	Rule	Session End Reason	Bytes	Device SN	Device Name
03/26 15:16:59	end	L3-Trust	L3-Untrust	10.0.1.101	panwdomain\user1	23.210.101.240	443	web-browsing	allow	Allow Outbound Browsing	tcp-fin	11.9k	0070550000401...	sample-ct-fw
03/26 15:16:58	end	L3-Trust	L3-Untrust	10.0.1.101	panwdomain\user1	10.0.0.2	53	dns	allow	Allow all outbound	aged-out	412	0070550000401...	sample-ct-fw
03/26 15:16:58	end	L3-Trust	L3-Untrust	10.0.1.101	panwdomain\user1	23.210.101.240	443	web-browsing	allow	Allow Outbound Browsing	tcp-fin	11.3k	0070550000401...	sample-ct-fw
03/26 15:16:57	end	L3-Trust	L3-Untrust	10.0.1.101	panwdomain\user1	10.0.0.2	53	dns	allow	Allow all outbound	aged-out	406	0070550000401...	sample-ct-fw
03/26 15:16:56	end	L3-Trust	L3-Untrust	10.0.1.101	panwdomain\user1	23.210.101.240	443	web-browsing	allow	Allow Outbound Browsing	tcp-fin	14.3k	0070550000401...	sample-ct-fw
03/26 15:16:55	end	L3-Trust	L3-Untrust	10.0.1.101	panwdomain\user1	10.0.0.2	53	dns	allow	Allow all outbound	aged-out	642	0070550000401...	sample-ct-fw
03/26 15:16:54	end	L3-Trust	L3-Untrust	10.0.1.101	panwdomain\user1	23.210.101.240	443	web-browsing	allow	Allow Outbound Browsing	tcp-fin	13.5k	0070550000401...	sample-ct-fw
03/26 15:16:54	end	L3-Trust	L3-Untrust	10.0.1.101	panwdomain\user1	10.0.0.2	53	dns	allow	Allow all outbound	aged-out	572	0070550000401...	sample-ct-fw
03/26 15:16:52	end	L3-Trust	L3-Untrust	10.0.1.101	panwdomain\user1	10.0.0.2	53	dns	allow	Allow all outbound	aged-out	410	0070550000401...	sample-ct-fw

Threat

The screenshot shows the Palo Alto Networks Monitor tab with the 'Threat' log selected. The table displays log entries with columns: Receive Time, Type, Name, From Zone, To Zone, Source address, Source User, Destination address, To Port, Application, Action, Severity, and File Name.

Receive Time	Type	Name	From Zone	To Zone	Source address	Source User	Destination address	To Port	Application	Action	Severity	File Name	URL
03/26 15:37:23	vulnerability	Joomla Visites Component Remote File Include Vulnerability	L3-Untrust	L3-Trust	10.0.0.88		10.0.0.100	80	web-browsing	reset-both	critical	10.0.0.100/admi...	
03/26 15:37:23	vulnerability	Joomla Visites Component Remote File Include Vulnerability	L3-Untrust	L3-Trust	10.0.0.88		10.0.0.100	80	web-browsing	reset-both	critical	10.0.0.100/admi...	
03/26 15:37:23	vulnerability	Joomla Visites Component Remote File Include Vulnerability	L3-Untrust	L3-Trust	10.0.0.88		10.0.0.100	80	web-browsing	reset-both	critical	10.0.0.100/admi...	
03/26 15:37:22	vulnerability	Joomla Visites Component Remote File Include Vulnerability	L3-Untrust	L3-Trust	10.0.0.88		10.0.0.100	80	web-browsing	reset-both	critical	10.0.0.100/admi...	
03/26 15:37:22	vulnerability	Joomla Visites Component Remote File Include Vulnerability	L3-Untrust	L3-Trust	10.0.0.88		10.0.0.100	80	web-browsing	reset-both	critical	10.0.0.100/admi...	
03/26 15:37:22	vulnerability	Joomla Visites Component Remote File Include Vulnerability	L3-Untrust	L3-Trust	10.0.0.88		10.0.0.100	80	web-browsing	reset-both	critical	10.0.0.100/admi...	
03/26 15:37:22	vulnerability	PHP Remote File Include Vulnerability	L3-Untrust	L3-Trust	10.0.0.88		10.0.0.100	80	web-browsing	reset-both	medium	10.0.0.100/zoo...	

Note: to see these you should generate some threats with Kali Linux, as explained in Appendix A.

URL Filtering

The screenshot shows the Palo Alto Networks Monitor tab with the 'URL Filtering' log selected. The table displays log entries with columns: Generate Time, Category, URL, From Zone, To Zone, Source, Source User, Destination, Application, Action, Headers Inserted, Device SN, and Device Name.

Generate Time	Category	URL	From Zone	To Zone	Source	Source User	Destination	Application	Action	Headers Inserted	Device SN	Device Name
03/26 15:17:22	society	www.condenast....	L3-Trust	L3-Untrust	10.0.1.101	panwdomain\us...	151.101.40.239	web-browsing	allow		0070550000401...	sample-ct-fw
03/26 15:17:20	society	www.condenast....	L3-Trust	L3-Untrust	10.0.1.101	panwdomain\us...	151.101.40.239	web-browsing	allow		0070550000401...	sample-ct-fw
03/26 15:17:19	society	www.condenast....	L3-Trust	L3-Untrust	10.0.1.101	panwdomain\us...	151.101.40.239	web-browsing	allow		0070550000401...	sample-ct-fw
03/26 15:17:18	society	www.condenast....	L3-Trust	L3-Untrust	10.0.1.101	panwdomain\us...	151.101.40.239	web-browsing	allow		0070550000401...	sample-ct-fw
03/26 15:17:17	news	www.wired.com...	L3-Trust	L3-Untrust	10.0.1.101	panwdomain\us...	151.101.190.194	web-browsing	allow		0070550000401...	sample-ct-fw
03/26 15:17:17	society	www.condenast....	L3-Trust	L3-Untrust	10.0.1.101	panwdomain\us...	151.101.40.239	web-browsing	allow		0070550000401...	sample-ct-fw
03/26 15:17:17	society	www.condenast....	L3-Trust	L3-Untrust	10.0.1.101	panwdomain\us...	151.101.40.239	web-browsing	allow		0070550000401...	sample-ct-fw
03/26 15:17:15	news	digg.com/	L3-Trust	L3-Untrust	10.0.1.101	panwdomain\us...	184.169.136.19	web-browsing	allow		0070550000401...	sample-ct-fw
03/26 15:17:13	shopping	www.craigslis...o...	L3-Trust	L3-Untrust	10.0.1.101	panwdomain\us...	208.82.238.17	web-browsing	allow		0070550000401...	sample-ct-fw
03/26 15:17:13	shopping	www.craigslis...o...	L3-Trust	L3-Untrust	10.0.1.101	panwdomain\us...	208.82.238.17	web-browsing	allow		0070550000401...	sample-ct-fw
03/26 15:17:11	shopping	www.craigslis...o...	L3-Trust	L3-Untrust	10.0.1.101	panwdomain\us...	208.82.238.17	web-browsing	allow		0070550000401...	sample-ct-fw

Wildfire Submissions

paloalto NETWORKS

Dashboard ACC Monitor Policies Objects Network Device Panorama

Context: Panorama Device Group: All

Logs

- Traffic
- Threat
- URL Filtering
- WildFire Submissions
- Data Filtering
- HIP Match
- User-ID
- Tunnel Inspection
- System
- Configuration
- Authentication
- Unified
- External Logs
- Traps ES
- Threat
- System
- Policy

Generate Time	File Name	URL	Source Zone	Destination Zone	Source address	Source User	Destination address	Dest... Port	Application	Rule	Verdict	Action	Severity	Sc
03/26 15:16:26	wildfire-test-pe-f...		L3-Trust	L3-Untrust	10.0.1.101	panwdomain(us...	52.8.161.117	80	web-browsing	Allow Outbound Browsing	malicious	allow	high	.
03/26 15:12:27	wildfire-test-pe-f...		L3-Trust	L3-Untrust	10.0.1.101	panwdomain(us...	52.8.161.117	80	web-browsing	Allow Outbound Browsing	malicious	allow	high	.
03/26 15:10:27	wildfire-test-pe-f...		L3-Trust	L3-Untrust	10.0.1.101	panwdomain(us...	52.8.161.117	80	web-browsing	Allow Outbound Browsing	malicious	allow	high	.
03/26 15:08:27	wildfire-test-pe-f...		L3-Trust	L3-Untrust	10.0.1.101	panwdomain(us...	52.8.161.117	80	web-browsing	Allow Outbound Browsing	malicious	allow	high	.
03/26 15:06:27	wildfire-test-pe-f...		L3-Trust	L3-Untrust	10.0.1.101	panwdomain(us...	52.8.161.117	80	web-browsing	Allow Outbound Browsing	malicious	allow	high	.
03/26 15:04:27	wildfire-test-pe-f...		L3-Trust	L3-Untrust	10.0.1.101	panwdomain(us...	52.8.161.117	80	web-browsing	Allow Outbound Browsing	malicious	allow	high	.
03/26 15:00:27	wildfire-test-pe-f...		L3-Trust	L3-Untrust	10.0.1.101	panwdomain(us...	52.8.161.117	80	web-browsing	Allow Outbound Browsing	malicious	allow	high	.

Application-Framework-FAQs

Application Framework Partner Beta Program - Frequently Asked Questions

Doc Revision: 2019-03-01-21:34:38 (UTC)

Please make sure you always download the latest revision of this document and the required files:

- Wiki home: <https://github.com/PaloAltoNetworks/appframeworklab/wiki>
- This document: <https://github.com/PaloAltoNetworks/appframeworklab/wiki/Application-Framework-FAQs>

What is the Application Framework Partner Beta Program?

- As Ignite 2018 draws near, Palo Alto Networks is providing partners preview access to the Application Framework to work on their specific integrations.

Where can I go to find/acquire X?

- API reference and Getting-Started documentation (ask your Palo Alto Networks representative to get access to the shared folder if you cannot reach it)
 - <https://paloaltonetworks.app.box.com/folder/46344564211>
- Authorization codes/serials/licenses
 - Please contact your Palo Alto Networks representative.
- pancloud SDK
 - <https://github.com/PaloAltoNetworks/pancloud>
- API Explorer (sample app)
 - <https://github.com/PaloAltoNetworks/apiexplorer>
- Lab Deployment Documentation
 - <https://github.com/PaloAltoNetworks/appframeworklab/wiki>

How can I report an issue/bug with X?

- APIs
 - Please contact your Palo Alto Networks representative.
- pancloud SDK
 - Create a GitHub issue following the submission guidelines published in the repo.
 - Gitter: <https://gitter.im/PaloAltoNetworks/pancloud>
 - Contact your Palo Alto Networks representative.
- API explorer
 - Create a GitHub issue following the submission guidelines published in the repo.
 - Gitter: <https://gitter.im/PaloAltoNetworks/pancloud>
 - Contact your Palo Alto Networks representative.

How can I deploy X?

- API Explorer
 - <https://paloaltonetworks.box.com/s/s0hc5umuxsumjb6t3vcwtknzh9isbkcf>
- Developer Environment on AWS
 - <https://paloaltonetworks.box.com/s/s0hc5umuxsumjb6t3vcwtknzh9isbkcf>

How can I register my own app?

- Work with your Palo Alto Networks representative to generate the required manifest.json file.

Where do I find my client_id, client_secret, etc., needed for authorization/OAuth?

- Contact your Palo Alto Networks representative.

How are we tracking customers who click from the app portal to the 3rd-party app.

- Although the Cortex Hub logs the username of the person that "Activates" a 3rd-party app, it will be up to the vendor/partner to record tracking/accounting data when a user "Signs Up" or "Signs In" for/to the 3rd-party app from the CSP.

How does a 3rd-party partner get paid for app usage?

- This has not been defined yet.

Can we develop with dummy data/sample logs in Logging Service?

- Yes, we have the option to stream any log type to any Logging Service instance (using jlogger). The sample logs are derived from our Palo Alto Networks demo labs and do not contain sensitive data.
- However, unless the circumstances require it, it is recommended for 3rd-party developers to deploy or configure a lab suitable for generating logs. We provide an AWS CloudFormation Template (CFT) that can be used for the purpose.

What region is the Logging Service data center physically located?

- North America.

Are Logging Service column names supported in SQL filter SELECT expressions?

- Please refer to the official API documentation for supported features. Undocumented features are not supported and subject to change without notice. Developers should avoid using undocumented features.
- Column names in SELECT expressions are not supported but may return valid results. For example, to return only the source and destination IP address columns, include those column name in the SELECT expression, e.g:
 - `SELECT src,dst FROM panw.traffic`
 - For names that conflict with SQL keywords, prepend the underscore character to the field name, e.g:
 - `SELECT _from FROM panw.traffic`

How often can the Event Service API be polled? Why doesn't Event Service API push data?

- Push will not be available in 1.0. You should poll as often as needed by your app.

Why does the Event Service poll return an empty list even when logs are present?

- There are subtle but significant differences in the Event Service and Logging Service SQL filters that can produce unexpected results.
- For the Event Service, the table reference must be enclosed in back quotes. For example:
 - `{ "filters": [{"panw.traffic": "SELECT * FROM panw.traffic"}] }` will return no results.
 - `{ "filters": [{"panw.traffic": "SELECT * FROM `panw.traffic`"}] }` works as expected.

Where do I get the "channelID" for the Event Service?

- Use the static value `"EventFilter"`

What is the duration of the OAuth Authorization Token?

- 1 hour (3600 seconds). You can use the `refresh token` to generate a new `authorization token`

How can the app framework protect against real time threats?

- Please continue to rely on a properly configured NGFW, Traps, WildFire, for protection against real-time threats.
- Retroactive protection is possible using a combination of MineMeld,

EDLs, or a 3rd-party supplied on-premise agent capable of updating NGFW [firewall](#) security policy.

Why I cannot generate the OTP on Customer Support Portal?

- Please make sure that your account has **SuperUser**, **Logging Service** and **Directory Sync Service** permissions on Cortex Hub

Logging Service doesn't work (I can't see logs on Panorama):

- Check that you have the proper licenses registered in Panorama (navigate to "Panorama" - "Licenses" and make sure you have both "Logging Service" licenses and Support (can be either "Standard" or "Premium")):

The screenshot shows the Palo Alto Networks Panorama configuration interface. The left sidebar contains a navigation tree with 'Licenses' highlighted. The main content area displays four license cards:

- AutoFocus Device License:** Date Issued: March 29, 2018; Date Expires: October 27, 2020; Description: AutoFocus Device License.
- Device Management License:** Date Issued: March 29, 2018; Date Expires: Never; Description: VM Panorama license to manage up to 25 devices.
- Premium:** Date Issued: March 29, 2018; Date Expires: March 29, 2019; Description: 24 x 7 phone support; advanced replacement hardware service.
- Logging Service:** Date Issued: March 29, 2018; Date Expires: March 29, 2019; Description: Cloud Service; Log Storage TB: 1.

- Check that you have the proper licenses registered in the Firewall (navigate to "Panorama" - "Device Deployment" - "Licenses" and make sure you have "Support", "URL", "Threat Prevention", "WildFire", "VM-Series Capacity" and "Logging Service" licenses enabled:

The screenshot shows the Palo Alto Networks Firewall configuration interface. The 'Licenses' section is expanded, showing a table of license status for various services:

Device	Virtual System	Threat Prevention	URL	Support	GlobalProtect Gateway	GlobalProtect Portal	WildFire	VM-Series Capacity	AutoFocus	Logging Service	Decryption Port Mirror	Decryption Broker
sample-cft-fw		Expires: 4/2/2019	PaloAlto Networks Expires: 4/2/2019	Expires: 4/2/2019	Expires: 4/2/2019		Expires: 4/2/2019			Expires: 5/9/2028		

- On the Panorama CLI, run the following commands and provide the output to your Palo Alto Networks Representative:
 - `show plugins cloud_services logging-service info`
 - `request plugins cloud_services logging-service status`
 - `show system state | match lcaas`
 - `show system state | match cust`
- On the Firewall CLI, run the command "`show logging-status`". The output should be like the one in following picture:

```
admin@sample-cft-fw> show logging-status
```

```
-----
```

Type	Last Log Created	Last Log Fwdd	Last Seq Num Fwdd	Last Seq Num Ackd	Total Logs Fwdd
> CMS 0	Not Sending to CMS 0				
> CMS 1	Not Sending to CMS 1				
>Log Collection Service					
'Log Collection log forwarding agent' is active and connected to 74.217.90.118					
config	2018/04/02 00:21:17	2018/04/02 16:01:19	11	11	1
system	2018/04/02 18:57:26	2018/04/02 18:57:26	15026	15026	136
threat	2018/04/02 18:57:43	2018/04/02 18:57:46	204109	204101	2724
traffic	2018/04/02 18:57:41	2018/04/02 18:57:46	409905	409899	5277
hipmatch	Not Available	Not Available	0	0	0
gtp-tunnel	Not Available	Not Available	0	0	0
userid	2018/04/02 18:45:10	2018/04/02 18:45:26	405	405	12
auth	Not Available	Not Available	0	0	0
sctp	Not Available	Not Available	0	0	0

- Other useful Firewall CLI commands (provide the output to your Palo Alto Networks Representative):

- `request logging-service-forwarding certificate info`
- `request logging-service-forwarding status`
- `request logging-service-forwarding customerinfo show`
- `show system state | match cust`
- `show system state | match lcaas`
- `less mp-log lcaas_agent.log`
- `tail mp-log ms.log`
- `debug log-receiver rawlog_fwd_dpi stats global show verbose`
- **Restart Log Receiver on Firewall:**
- `debug software restart process log-receiver`

API-Curl-Examples

Palo Alto Networks Application Framework API Explorer Curl Examples

This document describes some examples on how to interact with the Application Framework API using *curl*.

Doc Revision: 2019-03-01-21:34:38 (UTC)

Please make sure you always download the latest revision of this document and the required files:

- Wiki home: <https://github.com/PaloAltoNetworks/appframeworklab/wiki>
- This document: <https://github.com/PaloAltoNetworks/appframeworklab/wiki/API-Curl-Examples>

Logging Service

Create a query

The following example shows how to run a query for 10 logs from the *panw.traffic* table. Note that the **AUTH_TOKEN** must be provided. *startTime* and *endTime* are used to determine the time window during which logs are searched.

```
curl -X POST -H "Content-Type: application/json" -H "Authorization: Bearer AUTH_TOKEN" -d '{"startTime": 0, "endTime": 1609459200, "maxWaitTime": 0, "query": "SELECT * FROM panw.traffic LIMIT 10"}' "https://apigw-stg4.us.paloaltonetworks.com/logging-service/v1/queries"
```

The response will look similar to:

```
{"queryId": "a8c81c89-0a2e-419c-b771-9283a2722e9a", "sequenceNo": 0, "queryStatus": "RUNNING", "clientParameters": {}, "result": {"esResult": null, "esQuery": {"table": ["panw.traffic"], "query": {"aggregations": {}, "size": 10, "selections": [], "params": {}}}}
```

You can extract the *queryId* (*a8c81c89-0a2e-419c-b771-9283a2722e9a*) and use it to collect results.

Get Poll results

To poll for a query result, use the following command (specifying the right *queryId*):

```
curl -X GET -H "Content-Type: application/json" -H "Authorization: Bearer AUTH_TOKEN" "https://apigw-stg4.us.paloaltonetworks.com/logging-service/v1/queries/a8c81c89-0a2e-419c-b771-9283a2722e9a/0"
```

The response will look similar to:

```
{"queryId": "a8c81c89-0a2e-419c-b771-9283a2722e9a", "sequenceNo": 0, "queryStatus": "JOB_FINISHED", "clientParameters": {}, "result": {"esResult": {"took": 335, "hits": {"total": 6489137, "maxScore": 2, "hits": [{"LOGS_HERE}], "id": "a8c81c89-0a2e-419c-b771-9283a2722e9a", "from": 0, "size": 10, "completed": true, "state": "COMPLETED", "time_out": false}, "esQuery": {"table": ["panw.traffic"], "query": {"aggregations": {}, "size": 10, "selections": [], "params": {}}}}
```

If the status is still *RUNNING* wait until it completes and try again. If the status is *FINISHED* there will be other results in additional sequences. If the status is *JOB_FINISHED* it is the last result set. Please look at the documentation for more details.

Delete Query

To delete a query, use the following command (specifying the right *queryId*):

```
curl -X DELETE -H "Content-Type: application/json" -H "Authorization: Bearer YOUR_TOKEN" "https://apigw-stg4.us.paloaltonetworks.com/logging-service/v1/queries/a8c81c89-0a2e-419c-b771-9283a2722e9a"
```

A successful response will be:

```
{"success": true}
```

API-Explorer-Lab

Palo Alto Networks Application Framework API Explorer Deployment via AWS CloudFormation

This document describes how to automatically set up an Application Framework API Explorer instance on Amazon Web Services. It is meant for Palo Alto Networks Partners that need a quick way to start developing for Application Framework.

It also provides instructions on how to pair the API Explorer application with Application Framework.

Doc Revision: 2019-03-01-21:34:38 (UTC)

Please make sure you always download the latest revision of this document and the required files:

- Wiki home: <https://github.com/PaloAltoNetworks/appframeworklab/wiki>
- This document: <https://github.com/PaloAltoNetworks/appframeworklab/wiki/API-Explorer-Lab>
- Documentation PDF: <https://github.com/PaloAltoNetworks/appframeworklab/blob/master/pdf/LabGuide.pdf>
- API Explorer JSON file: <https://raw.githubusercontent.com/PaloAltoNetworks/appframeworklab/master/ctf/apiexplorer-ctf.json>

Prerequisites

This lab environment requires the following:

- A valid AWS Account
- A Palo Alto Networks Enabled Network Instance
- AWS Region with 1 available Elastic IP
- (Not mandatory but highly recommended) A second or third level domain configured in AWS Route53 (i.e. lab.yourcompany.com with NS records pointing to AWS Route 53 DNS Servers): ask your Palo Alto Networks representative for more details.

Security Hardening Considerations

This environment is meant for development use only, it's not security hardened for production. Specifically, the following security considerations should be known:

- Administrative password is provided as an environment variable for the installation scripts on the API Explorer and Ubuntu Web Server VMs, so it may be visible in some of the log files (i.e. /tmp/panorama_setup.log on the API Explorer VM)

To perform manual hardening of the environment, the following post-deployment steps are suggested:

- Manually change all the passwords

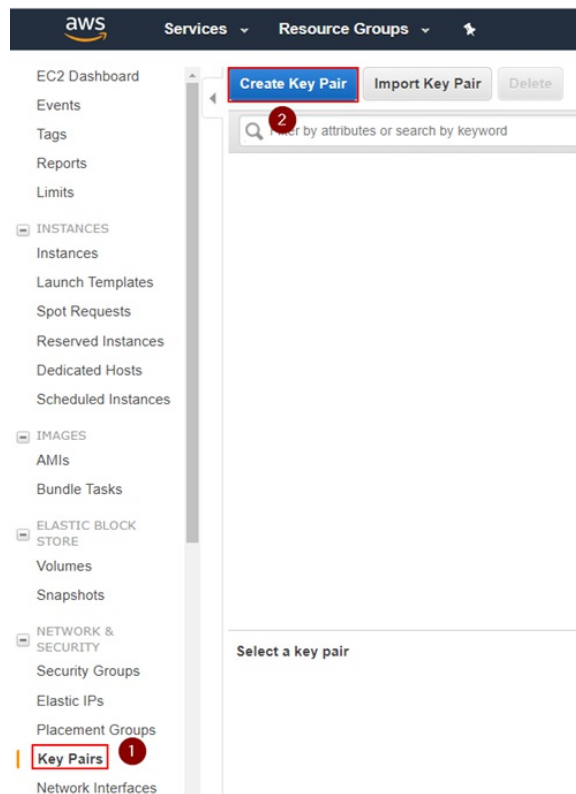
This document is not meant to provide instructions for the above steps.

AWS Configuration

This section describes the configuration of the AWS required components to deploy the lab components. You'll need a KeyPair and (optional) a Route53 Hosted Zone. Y

Key Pair Creation

1. Navigate to your selected region (i.e. us-east-1), select the EC2 service and under "Network & Security" select "Key Pairs" and click on "Create Key Pair":



2. Insert a keypair name and click on "Create". In the example, we use "paloalto". This will create a "paloalto.pem" private key and the AWS Web UI will prompt you to download it.



3. Download the Private Key to your local machine. The file name of this example will be `paloalto.pem`, but you can choose an arbitrary name. Y

Route53 Zone Configuration

The CloudFormation Template deploys a VM (API Explorer) and AWS can automatically associate DNS names to the Elastic IPs that are used by EC2. To do that, you need a Route53 public Hosted Zone configured in your AWS environment. This step is optional: you can just connect to the VMs via their Elastic IP addresses, or manually configure your DNS entries at a later stage if you're not using Route53. However, this step is highly recommended.

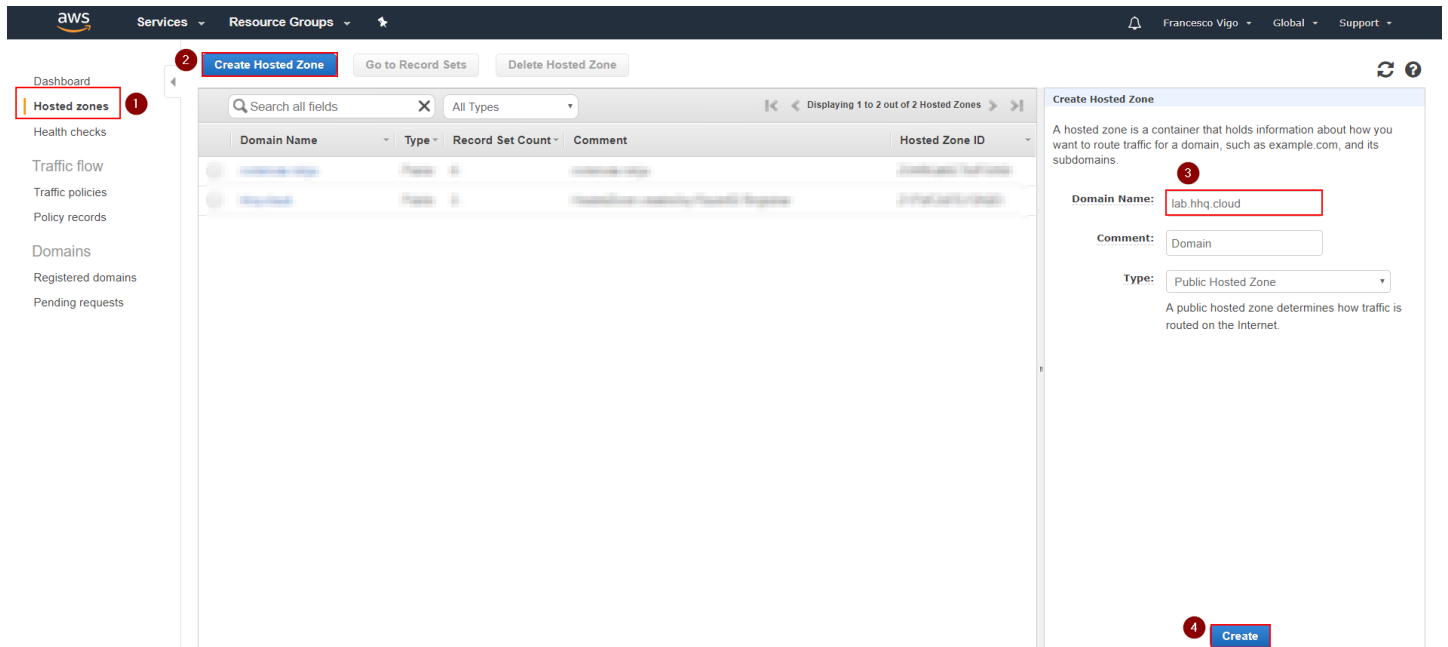
The public DNS zone you use can either be an existing second-level domain (i.e. `yourcompanylab.com`), or a third-level domain (`lab.yourcompany.com`). It must be publicly resolvable, so you need to be the registered owner of the domain. As an option, you can register a new domain directly through the AWS console and add it automatically in Route53.

If you don't have the opportunity to use a second or third level domain in Route53, ask your Palo Alto Networks contact for support to get a fourth level domain delegated to your Route53 DNS Servers.

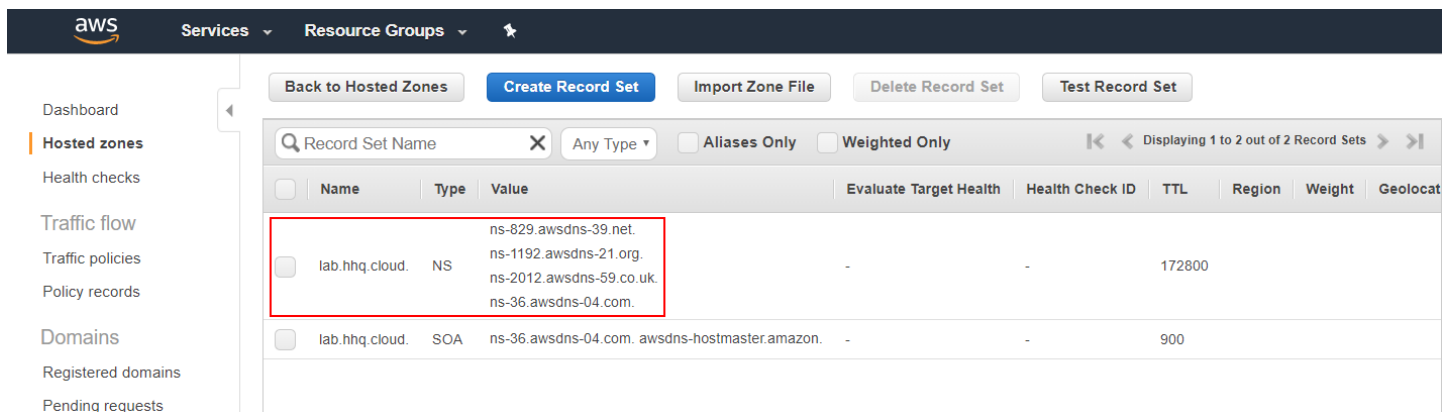
Note: the CFT can automate the creation and registration of a valid SSL certificate that corresponds to the FQDN of your API Explorer instance (this way the browser won't provide warnings when you connect to it), through a free service called "Let's Encrypt" (<https://letsencrypt.org>). If you want to automatically generate the Let's Encrypt certificate through the CFT, you must have the Route53 configuration enabled, otherwise the process will fail. Hence, if you don't want to use Route53 for this step, the API Explorer certificate must be a self-signed one. The CFT parameters provide options to disable the configuration of Route53 and Let's Encrypt.

To configure a Hosted zone in AWS Route 53, proceed through the following steps:

1. Navigate to AWS "Route53", go to "Hosted zones" and click on "Create Hosted Zone". Enter the domain name: it must be a public domain name (second or third level) where you have permissions configure name servers for (i.e. `yourcompanylab.com` or `lab.yourcompany.com`). The type must be "Public Hosted Zone." Then click on **Create**:



2. Look at the AWS Name Servers listed in the NS record and configure your Domain Hosting provider platform to use them for the selected domain:



In this example we are using the third-level domain `lab.hhq.cloud`.

Note: if you registered the domain through AWS, you don't need any additional configuration as it will be automatically registered in Route

53. If you're using a different domain hosting platform (i.e. GoDaddy, NameCheap, etc), the configuration on how to configure your domain to use AWS Route53 DNS servers will be different depending on your provider.

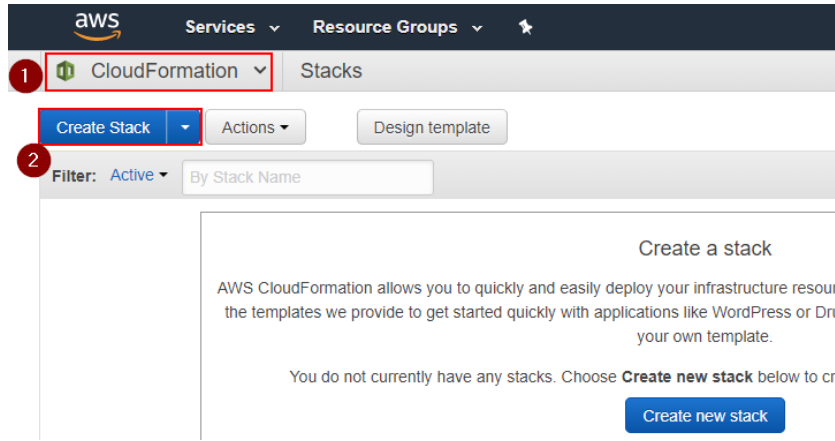
If you're being helped by Palo Alto Networks to use a fourth level domain, please provide the Name Servers to your contact.

Deploy the CloudFormation Template

You can now deploy the AWS CloudFormation Template (CFT) to create the lab environment. Before starting, make sure that you have one Elastic IP (EIP) available in the region you want to deploy the CFT (by default AWS limits EIPs to 5 per region per account).

Proceed with the following steps:

1. Navigate to "AWS CloudFormation" and select "Create Stack":



2. Select "Upload a template to Amazon S3", and upload the template JSON file provided by Palo Alto Networks `apiexplorer-cft.json` in the example), then click on **Next**:

Select Template

Select the template that describes the stack that you want to create. A stack is a group of related resources that you manage as a single unit.

Design a template Use AWS CloudFormation Designer to create or modify an existing template. [Learn more.](#)

Design template

Choose a template A template is a JSON/YAML-formatted text file that describes your stack's resources and their properties. [Learn more.](#)

Select a sample template

Upload a template to Amazon S3

Choose File `apiexplorer-cft.json`

Specify an Amazon S3 template URL

Cancel

Next

3. Insert the required parameters:

- **Stack name:** an arbitrary name for this deployment (i.e. PartnerLab1)
- **Admin Password:** an arbitrary password that will be used for the API Explorer application admin user.
- **EC2 VMs Key Name:** from the drop down menu, select the KeyPair that you want to use for the non-Palo Alto Networks VMs (Kali Linux, API Explorer VM, Ubuntu VM). It can be the KeyPair that you previously created in EC2, or a different one of your choice.
- **DNS Domain Name:** Insert the domain name zone that you have configured on Route53. If you don't have it, add a domain name and select "false" under both the "Configure Route53" AND the "Create API Explorer LetsEncrypt Cert" fields in the Advanced Configuration section. In the example we use the `hhq.cloud` domain.
- **LetsEncrypt Email:** Insert your (valid) email address that will be used to request a Let's Encrypt SSL certificate for the API Explorer.

Leave the other parameters to the default values unless you are a power user and you know what you're doing.

The following screenshot shows an example configuration:

Specify Details

Specify a stack name and parameter values. You can use or change the default parameter values, which are defined in the AWS CloudFormation template. [Learn more](#).

Stack name

Parameters

Basic Configuration - REQUIRED

Admin Password

Password for API Explorer: Must be at least 8 characters containing letters, numbers and symbols

EC2 VM Key Name

Name of an existing EC2 KeyPair to enable SSH access to the VM

DNS Domain Name

DNS Domain Name or Route53 Hosted Zone Name (i.e. panwlab.mycompany.com)

LetsEncryptEmail

Email address to provide to Letsencrypt for API Explorer SSL certificate generation (i.e. user@mycompany.com)

4. Click on "Next" twice.

5. In the Review page, Click on "Create":

[Quick Create Stack](#) (Create stacks similar to this one, with most details auto-populated)

Cancel Previous Create

6. Sit down and relax, the whole process will take a few minutes to complete:

Stack Name	Created Time	Status	Description
<input checked="" type="checkbox"/> PartnerLab1	2018-04-09 08:37:53 UTC-0700	CREATE_IN_PROGRE...	Palo Alto Networks Application Framework ...

7. The deployment will show **CREATE_COMPLETE** once everything is done:

Stack Name	Created Time	Status	Description
<input checked="" type="checkbox"/> PartnerLab1	2018-04-09 08:37:53 UTC-0700	CREATE_COMPLETE	Palo Alto Networks Application Framework ...

8. Select the template and click on the **Outputs** tab of the to view the deployment information (IP addresses and FQDNs) of the lab:

Stack Name	Created Time	Status	Description
<input checked="" type="checkbox"/> PartnerLab1	2018-04-09 08:37:53 UTC-0700	CREATE_COMPLETE	Palo Alto Networks Application Framework ...

Key	Value	Description	Export Name
APIExplorerAppURL	https://apiexplorer.hhq.cloud	API Explorer URL	

###AT THIS STAGE YOU SHOULD STOP AND MAKE SURE THAT THE CLOUD ENVIRONMENT IS READY. PLEASE REACH OUT TO YOUR PALO ALTO NETWORKS TECHNICAL CONTACT FOR THIS.

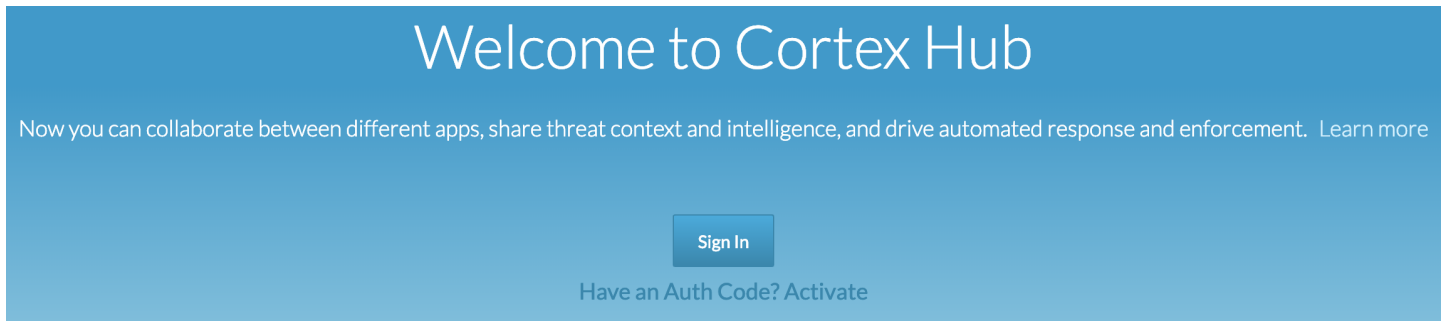
API Explorer App Activation Process

This section describes how to Activate the API Explorer application and start interacting with the APIs.

Note: this section requires the manifest file activation part to be already configured, otherwise you will not see your API Explorer application in the App Portal. You will also be provided a **Client ID** and a **Client Secret** by your Palo Alto Networks contact.

To activate the API Explorer, follow this process:


1. Navigate to the App Portal beta environment: <https://apps-stg4.app-portal-beta.us.paloaltonetworks.com> and Sign in with your Customer Support Portal credentials:




2. Activate an instance of Directory Sync Service by clicking on the **Activate** button in the **Directory Sync** tile:

CORTEX HUB

Your Cortex Hub Apps




Logging Service



Activate New App


If you have activated an app and do not see it above, you might not have the roles required to access the app. Please go to the Customer Support Portal to obtain the roles from your organization's administrator.

More Available Palo Alto Networks Apps




Directory Sync
Allow Palo Alto Networks Cloud Services to access your organization's directory

1 Activate [Learn More →](#)



Magnifier
Discover malicious activity and stop attackers and malware operating inside your network

[Learn More →](#)



Traps
Advanced, multi-method malware prevention that protects users and endpoints

[Learn More →](#)

3. Enter an arbitrary **Instance Name** and select **Americas** as **Region**, then click on **OK**:

Directory Sync ×

* Instance Name: DirSyncInstance1 **1**

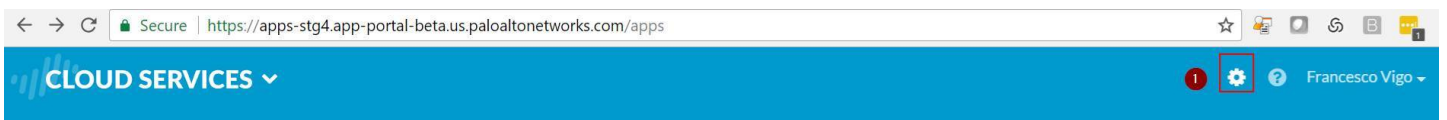
Description:

* Region: Americas **2**

Cancel OK **3**

Note: You don't need to actually register an Active Directory agent to it if you don't need to interact with AD data to build your integration. Or you can deploy the Directory Sync Agent on the windows Domain Controller, by following the Getting Started Guide, not covered by this manual

4. Review the configuration by clicking on the Settings icon in the top right corner:














The screenshot shows a browser window with the URL <https://apps-stg4.app-portal-beta.us.paloaltonetworks.com/apps>. The top navigation bar includes 'CLOUD SERVICES' and a user profile 'Francesco Vigo'. A red circle highlights the Settings icon in the top right corner.

Make sure that you have a Logging Service instance, and a Directory Sync instance.

5. Go back to the main page and navigate to the bottom of the Application Portal page, under **Partner Apps on the Application Framework**. Select the application (i.e. YourCompany - API Explorer) and click on the **Activate** icon:

Partner Apps on the Application Framework

 <p>Zero Trust SOC The ON2IT Zero Trust SOC-as-a-Service offers customers an economical, highly automated Security Operations Center.</p> <p>Activate Learn More →</p>	 <p>Silverfort Silverfort enables MFA and AI-based adaptive authentication even for systems that don't support it, without installing...</p> <p>Activate Learn More →</p>	 <p>Seclytics The Seclytics app for the Palo Alto Networks® Application Framework delivers forward-deployed predictive intelligence...</p> <p>Activate Learn More →</p>	 <p>Microsoft Graph Building on our long-standing partnership, the Microsoft Graph app enables the seamless sharing of data and alerts with integrate...</p> <p>Activate Learn More →</p>
 <p>Immediate Insight Immediate Insight is an analytics-enabled threat hunting and investigation platform for the Palo Alto Networks Application...</p> <p>Activate Learn More →</p>	 <p>Recorded Future Lookup The Recorded Future Lookup App lets you search traffic and threat logs for evidence of specific IOCs in your network...</p> <p>Activate Learn More →</p>	 <p>Portnox CLEAR A leading risk management, access control and network visibility capability delivered seamlessly as a cloud-based app.</p> <p>Activate Learn More →</p>	 <p>Critical Start ATAP Critical Start's Advanced Threat Analytics Platform Application for the Application Framework orchestrates the investigation o...</p> <p>Activate Learn More →</p>
 <p>Cybeats IoT Radar The Cybeats IoT Radar app utilizes contextual data derived from Application Framework to provide better visibility into IoT...</p> <p>Activate Learn More →</p>	 <p>SecBI Threat Detection SecBI enables PAN users, gain visibility to their network, to quickly understand the full scope of a cyber attack.</p> <p>Activate Learn More →</p>	 <p>API Explorer Take the Application Framework for a test drive!</p> <p>1 Activate Learn More →</p>	

Note: if you don't see your API Explorer App, reach out to your Palo Alto Networks technical contact for support.

6. Enter the required parameters, then select **"Agree and Submit"**:

Activate API Explorer ×

License Type: `apixplorer`

Company Name: `Technical Business Development`

* Instance Name: 1

Description: 2

* Region: 3

* Logging Service: 3

If not all Logging Service instances appear, you may need to [activate purchased licenses](#).

* Directory Sync: 4

* Description:

EULA: By clicking "Agree and Activate", you accept the terms of the [End User License Agreement](#).

Cancel
Agree and Activate 5

7. At this point you should see the instance of your "API Explorer" App in the "Cortex Hub Apps" section of the App Portal:

Your Cortex Hub Apps

Technical Business Development ▾



Directory Sync



Logging Service



API Explorer



Activate New App

8. Click on your API Explorer App icon and you will be redirected to your API Explorer instance (the FQDN of your AWS API Explorer instance). Login as **admin** (the password is the one you set as part of the CloudFormation Template parameters, same as Firewall and Panorama):

Note: Make sure that you login on the API explorer App for the first time through link on the Cortex Hub. Do not login on the API Explorer by navigating to the FQDN directly with your browser, as some required tokens must be passed to the API Explorer by the Cortex Hub through the link.

9. At the first Login, the API explorer app will ask you to perform the Activation. Click on the **Activate** button:

⚠ FURTHER ACTIVATION STEPS REQUIRED ⚠

NOTICE: Some features of your API EXPLORER will have limited functionality until the activation steps are completed.

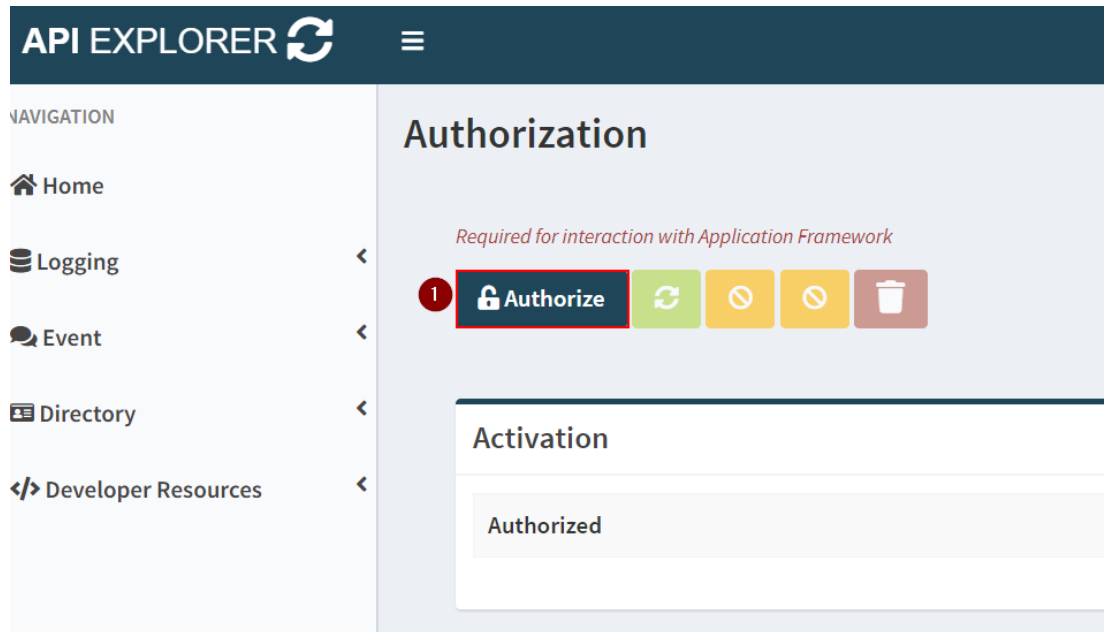
Activation Steps:

1. Click **Activate** button.
2. Click the **Authorize** button and provide the following to begin authorization:
 - Client ID
 - Client Secret
 - Redirect URI
 - Scope
3. When prompted, authenticate using your CSP credentials.
4. Complete and submit the "Request for Approval" form.

Note: If successful, your API EXPLORER will receive tokens necessary for interacting with your Logging, Event and Directory-Sync instances.

Cancel**1** **Activate**

10. In the Authorization page, click on "Authorize":



11. Insert the required parameters:

a. **Client ID** and **Client Secret** that you obtained from your

[Palo Alto Networks technical contact](#)

b. Redirect URI should be correspond to your API Explorer instance

with the /auth-callback route (i.e.
-<https://apiexplorer.lab.yourcompany.com/auth-callback> --
https://apiexplorer-stg4.lab.hhq.cloud/auth-callback in this
example)

c. Scope must be "logging-service:read", "event-service:read"

and "***directory-sync-service:read***". Do not select write scopes
at the moment.

12. Click on "Authorize":

API EXPLORER Authorization

Contact your Developer Relations representative if you are missing any of the required fields.

Client ID *

api_explorer_fv2 1

Client Secret *

..... 2

Redirect URI * /auth-callback

https://apiexplorer-stg4.lab.hhq.cloud/auth-callback 3

Scope * (select one or more)

logging-service:read event-service:read directory-sync-service:read 4

Authorize 5

Note: If successful, API EXPLORER will receive tokens necessary for interacting with your Logging, Event and Directory-Sync instances.

Cancel

13. The "Request for Approval" page on the Identity Provider will show up. Click on "Allow":

Request for Approval

APIExpFV-STG4 is requesting permission for the following:

- Read Logging Service
- Read Event Service
- Read Directory Sync Service

Consent info:

- APIExpFV-STG4: fvigo-stg4-test
- Logging Service: (no name)
- Directory Sync Service: DirSyncInstance1

1



APIExpFV-STG4

Take the Application Framework for a test drive!

14. If the authorization is successful, you should see the Tokens in the Authorization page, and the application should work:



Authorization

SUCCESS

Required for Interaction with Application Framework

Authorize   

Activation	
Scope	logging-service:read event-service:read directory-sync-service:read
Instance ID	4623954708994114687
Client ID	api_explorer
Authorized	True

Tokens	
Refresh-Token 
Access-Token 
Token-Type	bearer
Expires-At	Tuesday, April 3rd, 2018 1:03:49 PM

Congratulations: You can now use the functions of the API Explorer. For example, the "Query Explorer" from the left menu.

Appendix A: Explanation of the CFT services and usage

API Explorer VM

Runs the API Explorer application

Access the WebUI: <https://apiexplorer.lab.yourcompany.com>

You can also access directly with SSH private key with the `ec2-user` user:

```
# ssh -i paloalto.pem ec2-user@apiexplorer.lab.yourcompany.com
```

Appendix B: Default hostname to IP and VM Mapping

Public Hostname	Internal IP	EIP assigned?	VM
apiexplorer	10.0.0.55	Y	API Explorer VM