Centrify Infrastructure Service

Privilege Service 18.3

Palo Alto Firewall Workshop

Contents

About these labs

In these labs we'll perform several activities related to new capabilities for Centrify Infrastructure Service/Privilege Service 18.3:

1. Launch a Palo Alto Networks Firewall instance in AWS.
2. Prepare the Public Key Infrastructure details to enable Palo Alto Networks Firewall Password Management.
3. Onboard a Palo Alto Networks firewall for Password Management and Secure SSH Access.

Lab Pre-Requisites

For All labs

- All labs require a **Centrify** tenant enabled for Infrastructure Services (formerly CPS). To request a Centrify tenant, visit www.centrify.com/free-trial and sign up for a free trial tenant.
- This tenant must have a Centrify connector capable of reaching the target system(s). E.g. outbound to AWS for Palo Alto.

The Palo Alto Firewall-related labs requires

- An AWS account to launch a Palo Alto Firewall in AWS (7.1 or 8.x). To be able to participate in the labs during the workshop, you must have completed Part I (below) PRIOR to the workshop. *Note that you ideally you have set up consolidated billing. The PANOS system should be available for you in a 15-day trial.*
- A set of Virtual Machines that represent your environment. For example, a domain controller (dc.centrify.vms in this example); a member server (running the connector). You will need to be able to create an A or CNAME DNS record to resolve the name of the PANOS system correctly for PKI purposes.
- Access to the Certification Authority or Certificate enrollment applets. This is to request an SSL certificate and to export the Root CA certificate.
  - The certificate template (Web Server) must allow the private key to be exportable.
  - Ideally, your CA has been upgraded to issue certificates with the SHA256 algorithm instead of SHA1.

    The examples in this guide use the Microsoft Certification Authority.

Part I: Launching & Configuring a Palo Alto Networks Firewall EC2 VM

You will perform the steps in AWS, in your Mac with the terminal (or PC with PuTTY) and with a Web browser.

1. Launch the EC2 Instance from the AWS Marketplace

a) Sign-in to your AWS account with your root account or with a role that has EC2 Full Access. **https://console.aws.amazon.com/ec2**

b) In the landing page, press the **Launch Instance** button 

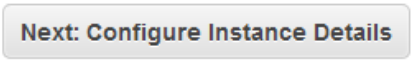
a) 1. Choose AMI: Click on the AWS Marketplace in the left pane.

b) In the Search function of the middle pane, type Palo Alto and press Enter.

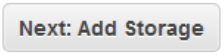
c) Press **Select** next to VM-**Series Next-Generation Firewall Bundle 1**

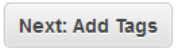
Press **Continue** in the Bundle details page.

d) 2. Choose Instance Type: Press **Next: Configure Instance Details**



e) 3. Configure Instance Details: Make sure the **Auto-Assign Public IP** is set to **Enable**.

Press **Next: Add Storage.** 

f) 4. Add Storage: Press **Add Tags.** 

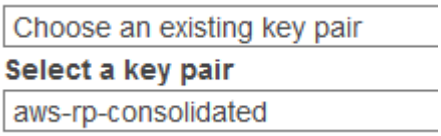
g) 5. Add Tags: Add tags as needed. E.g. Name, "May16Workshop PANOS" or simply press: **Next: Configure Security Group.** 

h) 6. Configure Security Groups: You can use the default security group that enables TCP 22 (SSH) and TCP 443 (HTTPS) inbound. If you use a different security group, make sure these rules are in place.

Press **Review and Launch.** 

i) 7. Review. Press Launch.

j) **Select Existing Key pair or new Key pair** (dialog box): Select your existing or new AWS key-pair. Very important that you have this, otherwise you won't be able to access.

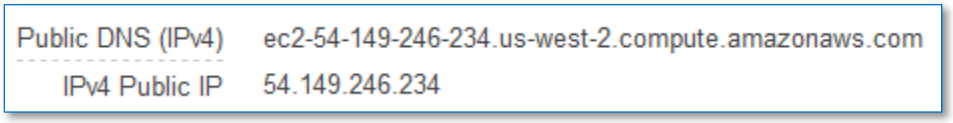


Press the **Launch** Button.

c) You will be notified over email that the subscription has been provisioned. It takes approximately 8-15 minutes for the image to be ready for the next steps.

2. Gather Information and Perform Initial Configuration of the Palo Alto EC2 VM

a) Gather the Public IP and DNS Name of our image.



b) Make sure the instance has passed the initial checks:

c) Connect to your EC2 Image using the SSH Key pair:

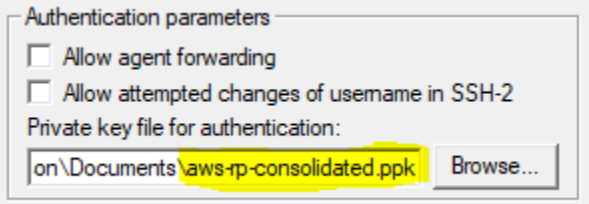
I. If using UNIX/Linux or Mac from the terminal:

```
$ ssh -i <privatekey.pem> admin@<EIP or private IP of eth0>
```

in the example above, if my key is called aws-rp-consolidated.pem

```
$ ssh -i /home/aws-rp-consolidated.pem admin@ec2-54-149-246-234.us-west-2.compute.amazonaws.com
```

II. If using PuTTY, you must export the key to PuTTY format; instructions here: https://devops.profitbricks.com/tutorials/use-ssh-keys-with-putty-on-windows/ and connect specifying the key here:



d) When you connect as admin, run these commands:

configure

sets the system in configuration mode

set mgt-config users admin password

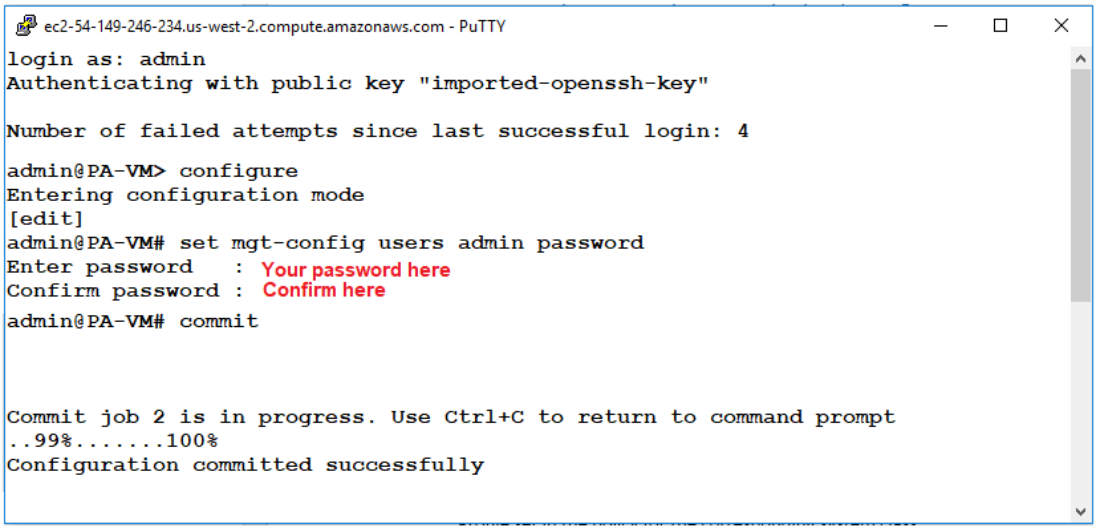
command to configure the admin password – will prompt to type and confirm.

Note: if you forget this password, you need to terminate and relaunch.

commit

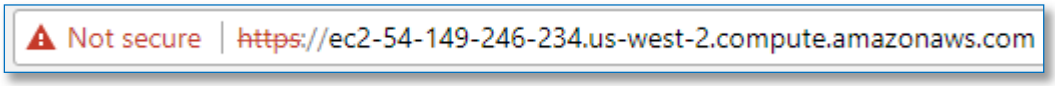
saves the configuration (new password change)

Sample output:



3. Verify Palo Alto EC2 access via Web Interface

I. Open your favorite browser and connect to your Palo Alto EC2 VM image.
Note: Because the SSL connection is with the firewall's self-signed certificate, you may have to add an exception (depending on the browser). The next section will correct that.



II. Type-in the admin credential. The password is the one set in step 4 in the prior section.

Note: if you forgot the admin password, you will need to terminate the instance and repeat all steps.

III. You will be placed in the PAN VM home. In the welcome page, feel free to check the "do not show again" and press Close.

IV. You are ready to start your Palo Alto CPS workshop.

Part II – Configure your DNS and PKI Environment for Palo Alto Firewall

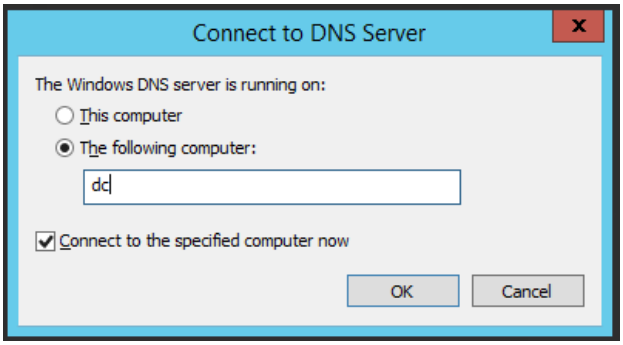
You will be working these steps from your centrify.vms environment from a system that has the DNS Management and Certification Authority tool (DC has it, but MEMBER may or may not have it depending on your setup).

Tip: If you want these tools to be installed on MEMBER, run this command in an Administrative PowerShell Window: **`Install-WindowsFeature RSAT-ADCS-Mgmt, RSAT-DNS-Server`**

1. Create an A (Host) record for your Palo Alto Firewall in centrify.vms

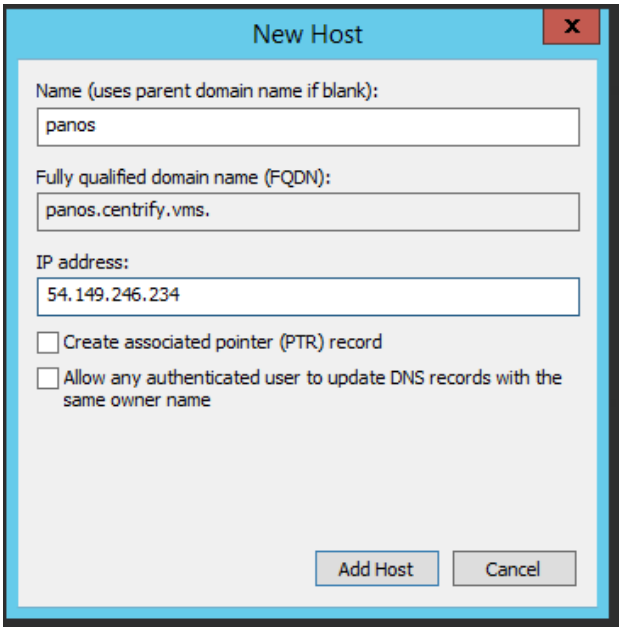
a) On your management system (MEMBER OR DC) log in with an administrative user.

b) Open DNS Management and connect to your DC.



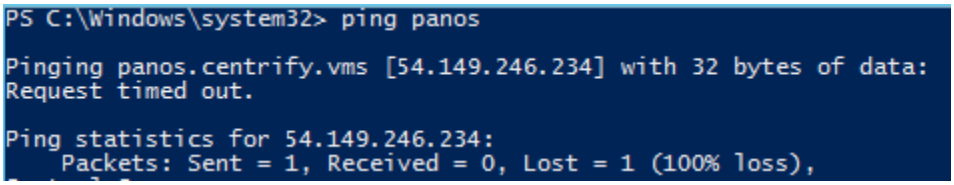
c) In DNS Manager, expand DC > Forward Lookup Zones > centrify.vms, then right click centrify.vms and select **New host (A or AAA) …**

d) Set up the following information:
Name: [your name here]; e.g. panos. IP Address: Your system's public IP. Then press **Add Host"**



e) Press **OK** in the successfully created dialog box.

f) From your **Centrify Connector,** perform a name resolution test. E.g. "`ping panos.centrify.vms`" in the command line; this will resolve the address, but won't respond to any ICMP requests (per AWS Security rules and Firewall settings).

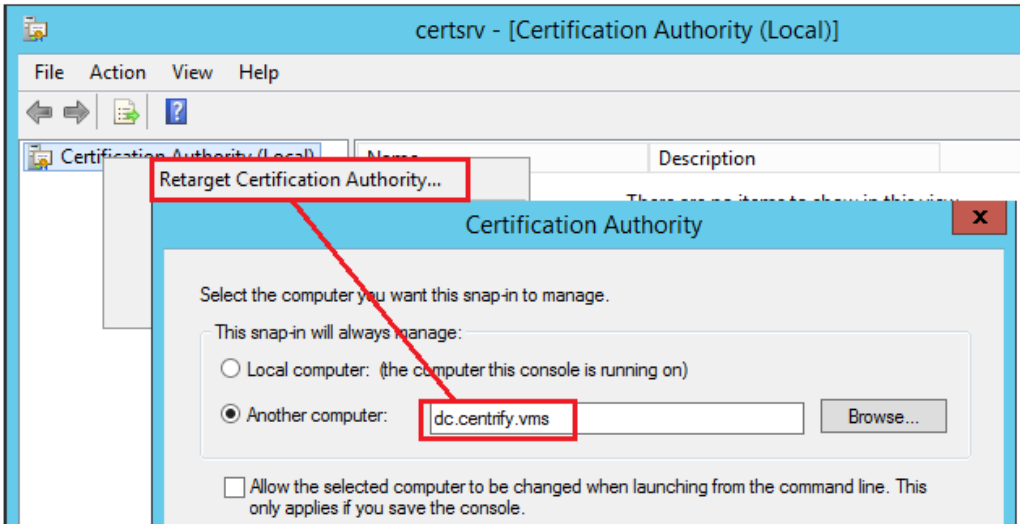


Note: This will ensure that your Centrify Connector can resolve the system by FQDN.

2. Export your Root Certification Authority Certificate

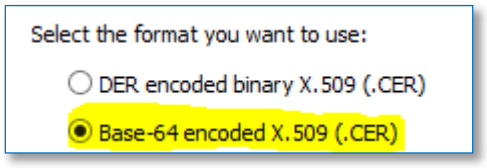
In the next steps, you will be exporting the root CA certificate for your environment. This will be used to establish PKI trust with the PANOS system. In addition, you'll be issuing an SSL/TLS certificate under the DNS name of your system.

a) On your management system, sign-in with an administrative user and open the **Certification Authority** administrative tool.
Note: If you are opening this tool from a system other than DC. You will get a "**Cannot Manage Active Directory Certificate Service"** this message (just press OK) and retarget the console to dc. Like this:



b) On the left pane, right click the Certification Authority (centrify-DC-CA) and select Properties > **View Certificate**, then go to the **Details** tab, and click the **Copy To file** button.

c) Follow the wizard, and make sure that you export the certificate as a Base-64 encoded X.509 .CER format.



d) Note the location of the certificate for a later step.

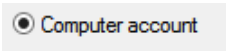
3. Request and Export a Web Server (SSL/TLS) certificate for your Palo Alto Firewall

You need a SSL/TLS certificate from your CA to be used during PANOS configuration for Password Management.

a) In MEMBER, open the mmc.exe program

b) In **MMC**, add the **Certificates (Computer)** snap-in

Make sure you're opening the Computer Account certificate store.

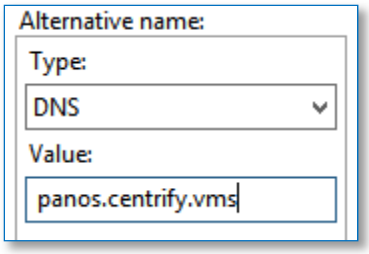


c) Under **Personal** > **Certificates**, right click and select request new certificate > **Active Directory Policy**

d) Select the "**Web Server**" certificate template that **allows for private key export**, and click on "more information…"

Note: If you have not modified your Web Server Certificate to have the private key to be exportable, check out the Appendix.

e) In **Subject** > **Common Name** > **Value** >
type the short name of your Palo Alto Networks system "e.g. panos" and press **Add**.



f) In **Subject** > **Alternative Name** > **DNS** >
type the fully-qualified name of your Palo Alto firewall (e.g. panos.centrify.vms) and press **Add**.

g) Press **OK** and press **Enroll**. You should see success.
Note: In some instances, this step will stall. This is observed in VMs that are suspended frequently; reboot your DC and then retry.

h) In the Certificates snap-in, navigate to **Personal** > **Certificates** and double-click the recently-created panos certificate.

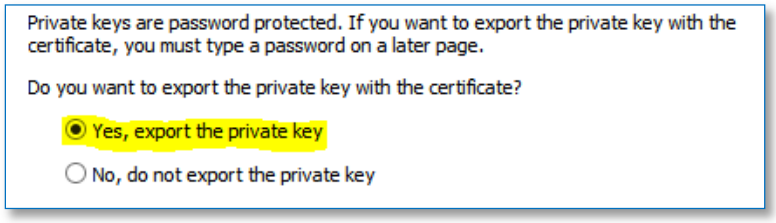
i) Keep the Certificates snap-in open for the export process.

4. Exporting the Certificate with the Private Key

a) Under **Personal** > **Certificates**, right click the recently-created certificate and select **Export**.

b) **Welcome Page** > Next

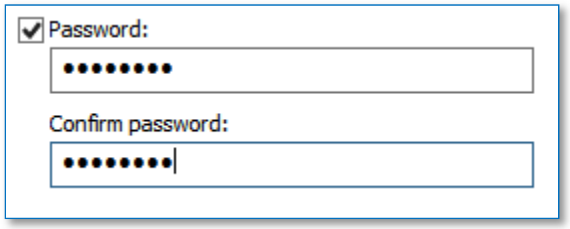
c) **Private Key** > Select "Yes, export the private key" and press Next.



If the "Yes, export the private key" option is not selectable, you used the wrong template or you have not modified the template to export the private key. Use the Appendix.

d) **File format** > Next

e) **Security** > This time, you'll set a password for the certificate. Make sure you don't forget it.



f) **File** > Select a location other than the nodes > Next
Make a note of this location, you'll need it during CPS setup. (e.g. c:\panos.pfx)

g) **Complete** > Finish

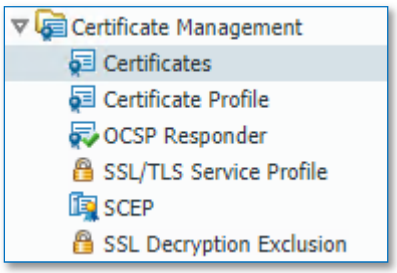
You are ready to start configuring your Palo Alto Firewall with Infrastructure Service.

Part III – Configure Palo Alto Firewall PKI (TLS/SSL) Certificate Settings

In this section, we will configure the Palo Alto Firewall to trust certificates issued by our Certification Authority, we'll also configure an SSL-TLS profile for the system. You'll need the root CA certificate, the newly-exported Web Server certificate and its password.

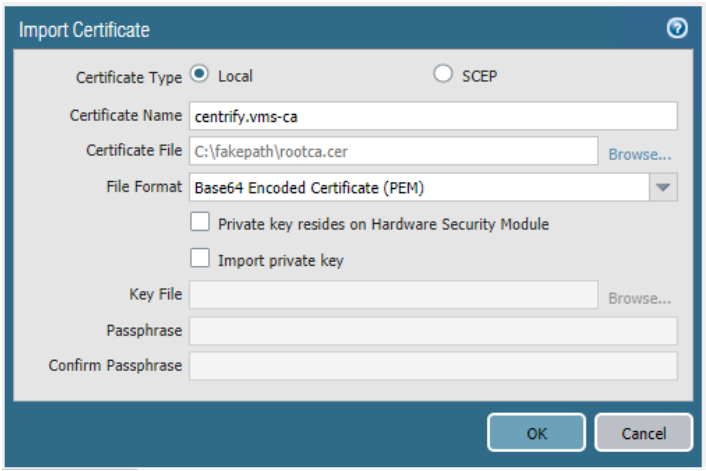
1. Add the Root CA Certificate to Palo Alto Firewall

a) Sign-in to the admin console of your Palo Alto Networks system as admin and go to **Device (tab) > Certificate Management > Certificates**

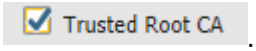


b) On the bottom pane, select **Import**

- Certificate name: type a descriptive name (e.g. centrify.vms-ca)
- Certificate File: Browse to the location of the exported Root CA cert.



c) Press OK. The Certificate will be listed, now double-click it.

d) Check the box next to "Trusted Root CA" 

.

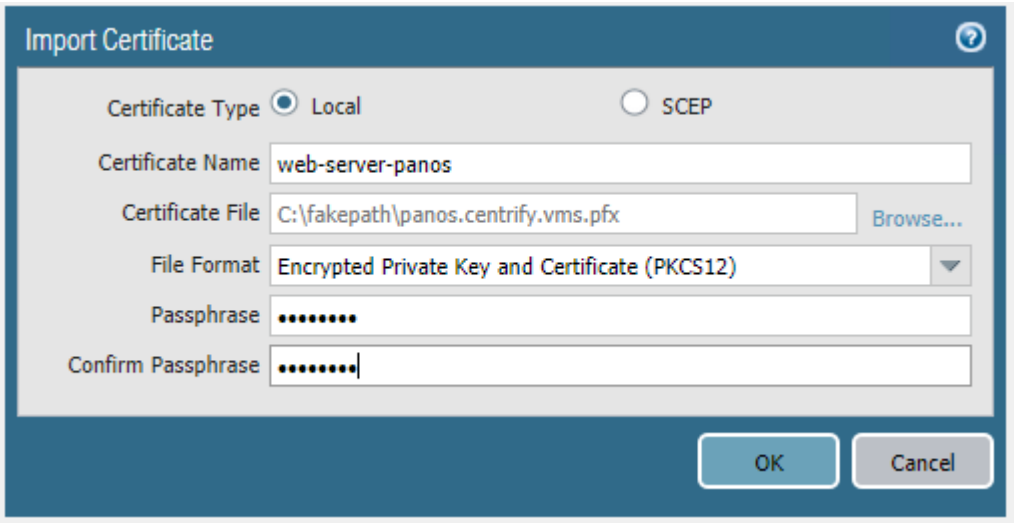
You have added the root CA to the PANOS system and it's now trusted by the device.

2. Install and Configure the Web Server Certificate in your Palo Alto Firewall

a) Sign-in to the admin console of your Palo Alto Networks system as admin and go to **Device (tab) > Certificate Management > Certificates**

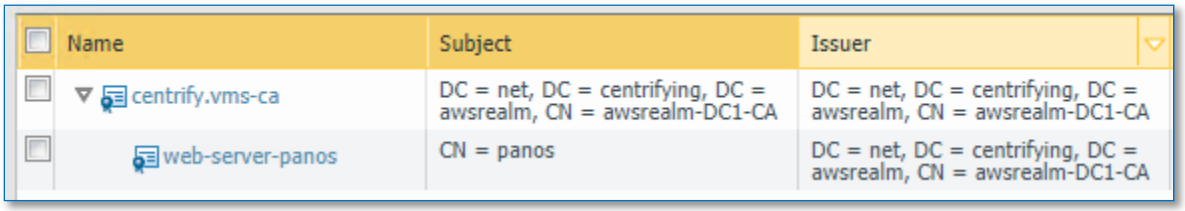
b) On the bottom pane, select **Import**

   a. Certificate name: type a descriptive name (e.g. web-server-cert)
   b. Certificate File: Browse to the location of the exported Web Server cert.
   c. File format: Select "Encrypted Private Key and Certificate (PKCs12)"
   d. Paraphrase and Confirm Paraphrase: Type the password set for this certificate.



If you forgot the password set for the Web Server certificate, you must repeat the previous section (Part II, section 4).

At this point, your window should display the RootCA certificate as the parent of the Web Server cert like this:



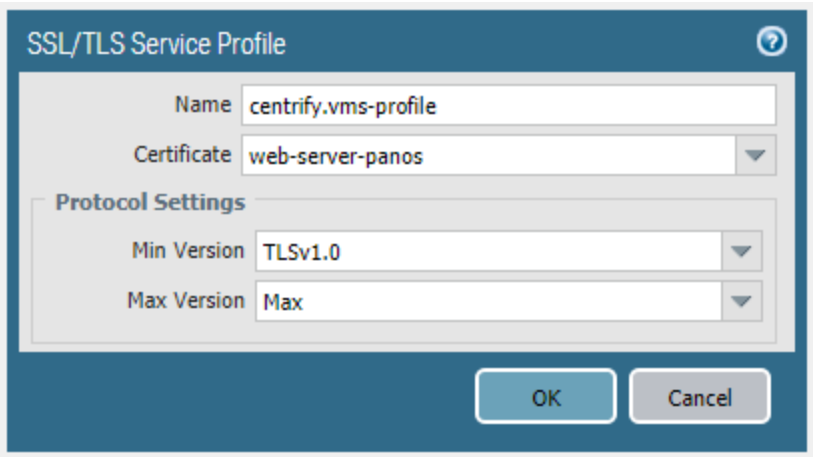
c) Keep the window open.

3. Create a new SSL/TLS Service Profile

a) Sign-in to the admin console of your Palo Alto Networks system as admin and go to **Device** (tab) > **Certificate Management** > **SSL/TLS Service Profile**.

b) Press **Add** in the lower bar and set the following information:

- Name: Set a descriptive name (e.g. “centrify.vms-profile”)
- Certificate: Select the certificate onboarded in the previous step.

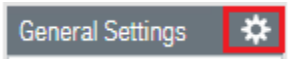


c) Press **OK.**

d) Leave the window open.

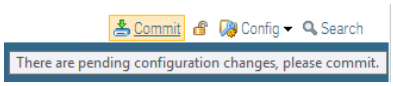
4. Update the SSL/TLS Profile of the Palo Alto Device

a) Sign-in to the admin console of your Palo Alto Networks system as admin and go to **Device** (tab) > **Setup** and click on the gears for the General Settings section.

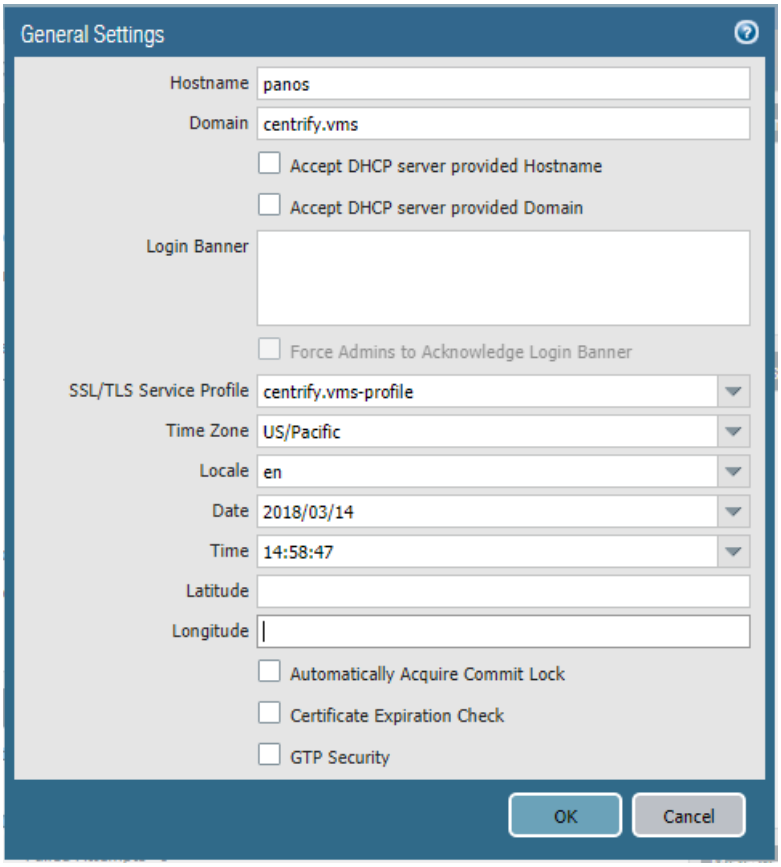


b) Set the following information:
Hostname: The short name you used (e.g. panos)
Domain: centrify.vms (if using the demo images)
SSL/TLS Service Profile: The profile created in the previous section (e.g. centrify.vms-profile)

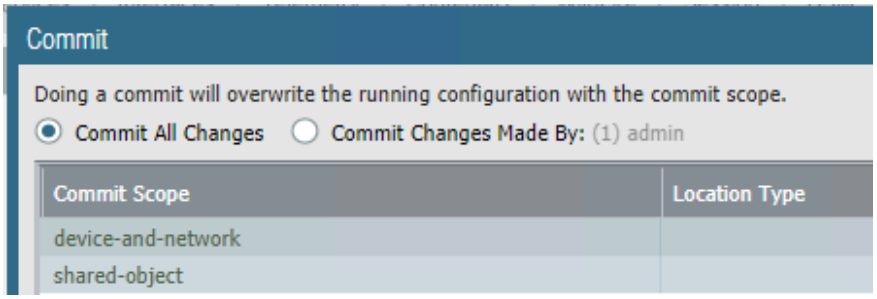
c) Press **OK**.
Note: Your changes aren't saved yet.



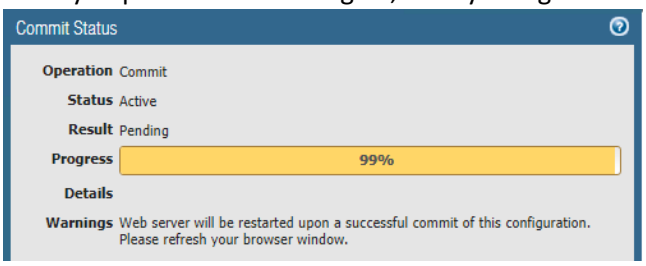
d) On the upper-right corner, click the **Commit** button.



The system will show you a preview of the changes. Then press **Commit** again.



Once you press the button again, then you'll get this status window:



e) You can now wait until the Palo Alto Firewall reboots the web service.

5. Verifying the SSL/TLS profile and clean SSL connectivity from Centrify Connector

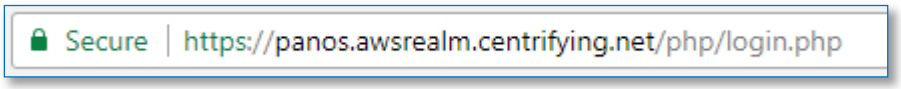
Perform these steps from your Centrify Connector system.

a) Sign out of the Palo Alto Firewall (if you have the old session).

Now access the URL using the designated DNS name. E.g. https://panos.centrify.vms (this will work only from your demo environment).

If you did not perform the DNS changes outlined in Part II, section I, you will not get the proper DNS name resolution.

b) At this point you should be able to get to the Palo Alto firewall portal. A key distinction is that now you have a clean browser experience.



c) At this point, you have successfully configured your Palo Alto firewall for enterprise PKI trust and fulfilled the pre-requisite for Password Management.

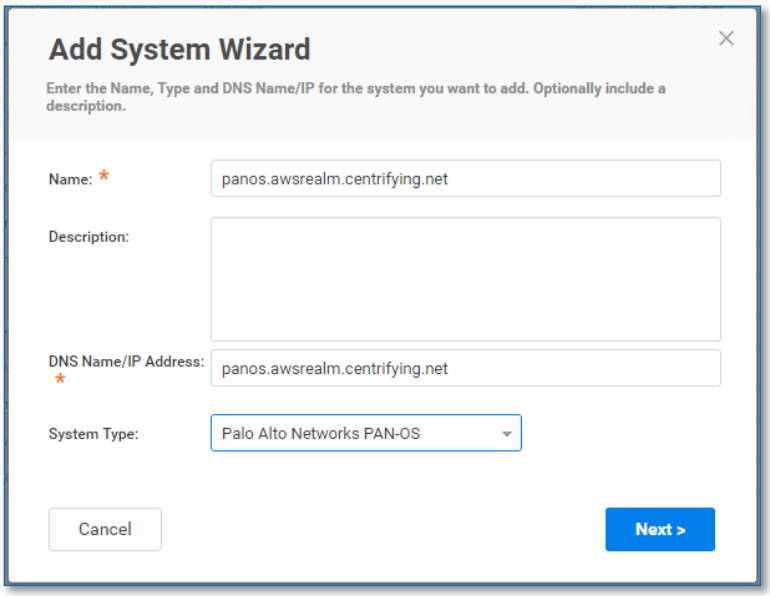
Part IV – Add and Configure Palo Alto Firewall to Privilege Service

In this section you use the “Add Device” wizard to onboard your Palo Alto firewall into Privilege Service.

1. Add the system

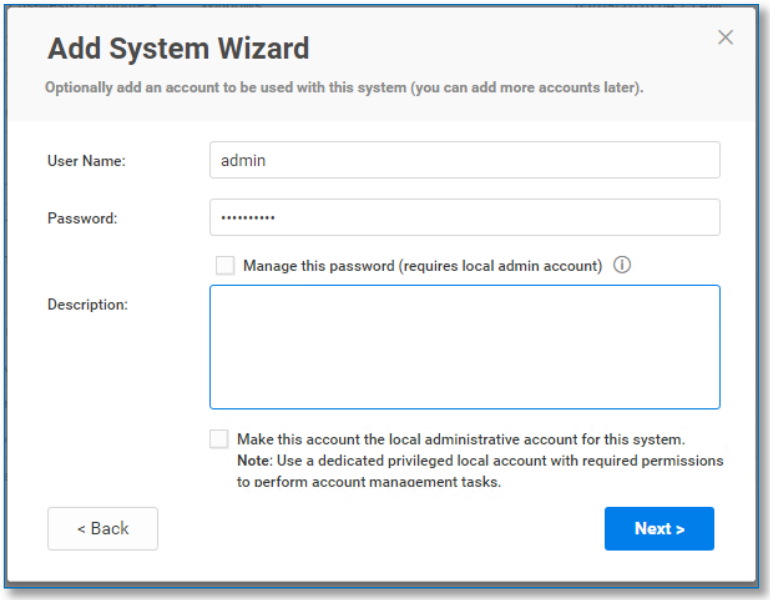
a) In IS/CPS go to Admin Portal > Infrastructure > Systems and press Add System

b) In the first panel, make sure you populate the Name, FQDN and System Type, then press Next.

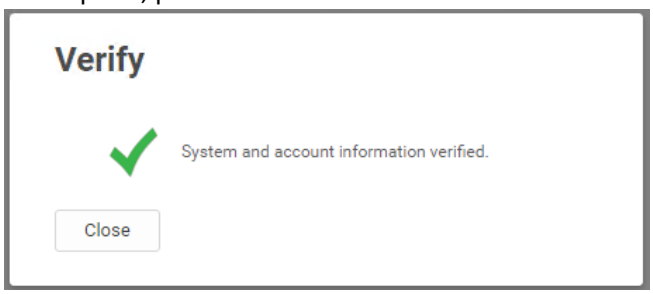


To enable password management, you must use the FQDN that is listed as the alternative name in the SSL/TLS cert used by the Palo Alto Firewall.

c) In the second panel, onboard your admin credential. Don’t check Password Management. This will be done later. Press Next



d) Press Next in the verification step (make sure the checkbox is set), once the verification is complete, press Close.

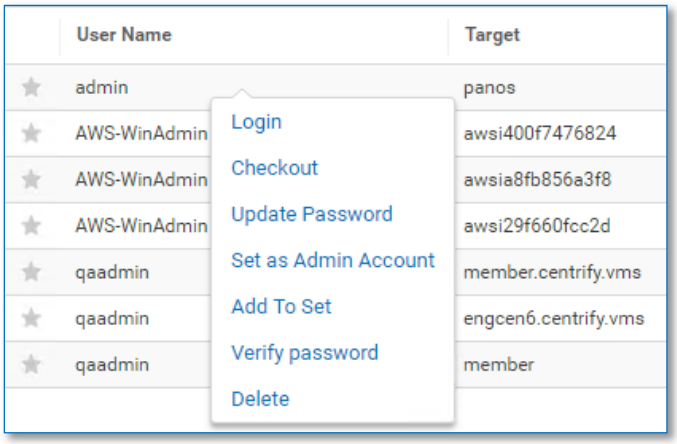


e) Leave this system standing by.

2. Verify Secure SSH Access

a) Go the Admin Portal > Infrastructure > Accounts and look your admin account.

b) Right-click and select login.



c) You should be placed in the SSH terminal of the Palo Alto Firewall system.

3. Set up Password Management

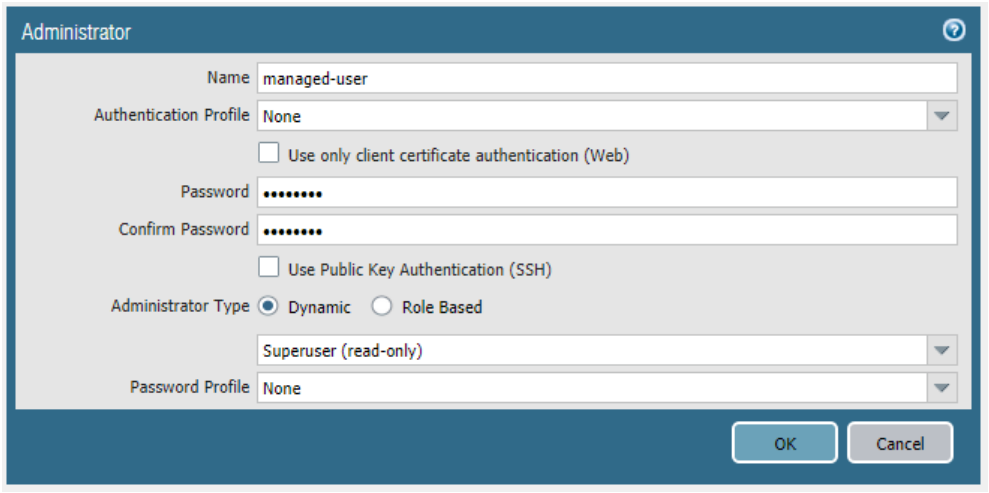
Note: Password Management in Palo Alto Firewall, just like Check Point requires a designated administrative account. In addition, a PKI relationship needs to be in place due to the use of REST APIs for Password operations. In this section, we create an account in Palo Alto First (our managed account) and we'll designate the admin account as the "management or administrative" account.

I. Create a test user

a) Sign-in to the admin console of your Palo Alto Networks system as admin and go to **Device** (tab) > **Certificate Management** > **Administrators**

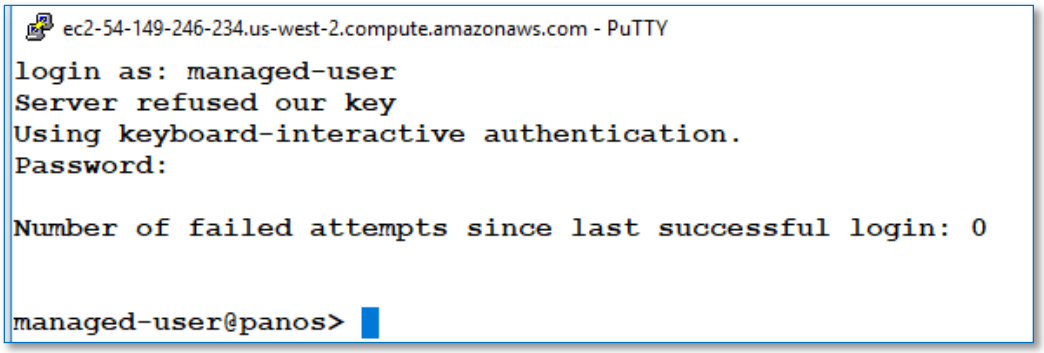
b) Press the **Add** button in the lower pane and set up the following info:

- Name: use a descriptive name (e.g. managed-user)
- Password: set up a password.
- Administrator type: SuperUser (read-only)
- Press OK.



II. Verify your test user

a) Use PuTTY or SSH in your terminal to verify that the user can connect over SSH correctly.

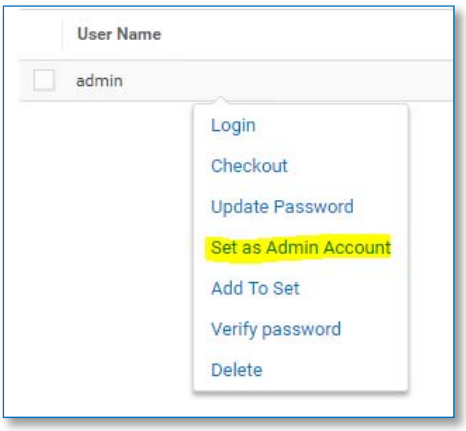


III. Configure the Super User account (Admin) as the Palo Alto Firewall Admin Account

a) In Privilege Service, go to Admin Console > Infrastructure > Systems > Double-click your PANOS system > Go to the Accounts tab.

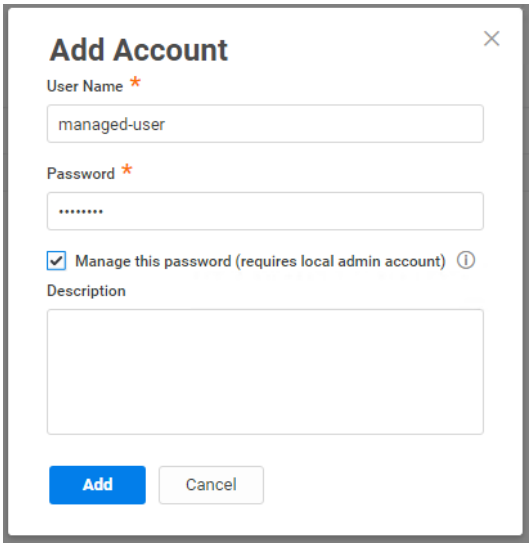
b) Right click the Super User Account (Admin) and select "Set as Admin Account"

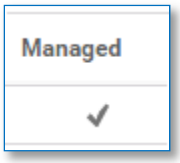
c) Keep the window open.



IV. Onboard a new managed account

a) In the existing Window (or under the **Accounts** section of the PANOS system), press **Add**.
b) Add the account set in the previous step (e.g. managed-user).
c) Set up the name/password, and make sure you check the “Manage this password (requires local admin account” box.
d) Press **Add**.
e) If you set up the system correctly and the network settings allow for HTTPS communication, the account should be managed.

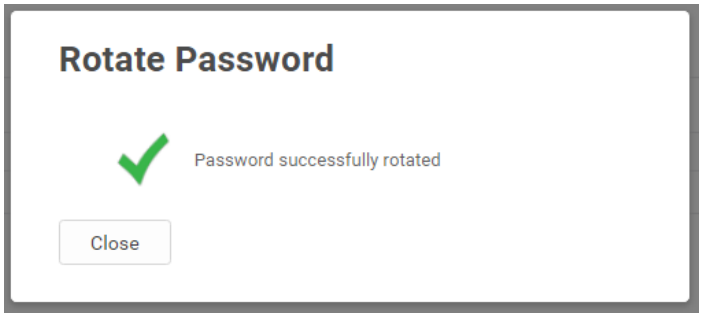




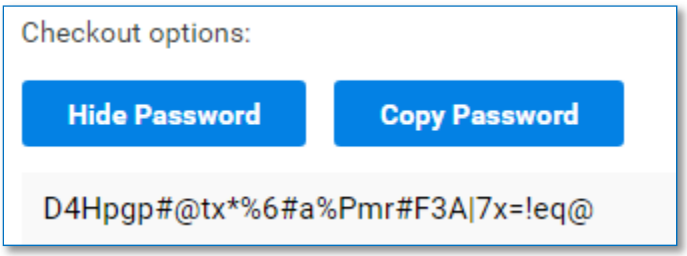
f) Leave the window open.

V. Testing Palo Alto Firewall Password Management.

a) Right-click your newly-created account and select Rotate. Confirm when prompted.



b) Once the password is rotated, verify the value by using the checkout function.



You have successfully tested your Palo Alto Firewall for Session Access and Password Management.