



## Using Terraform to Deploy a Simple GlobalProtect Infrastructure in GCP

Patrick Glynn – Public Cloud CE

April 2020

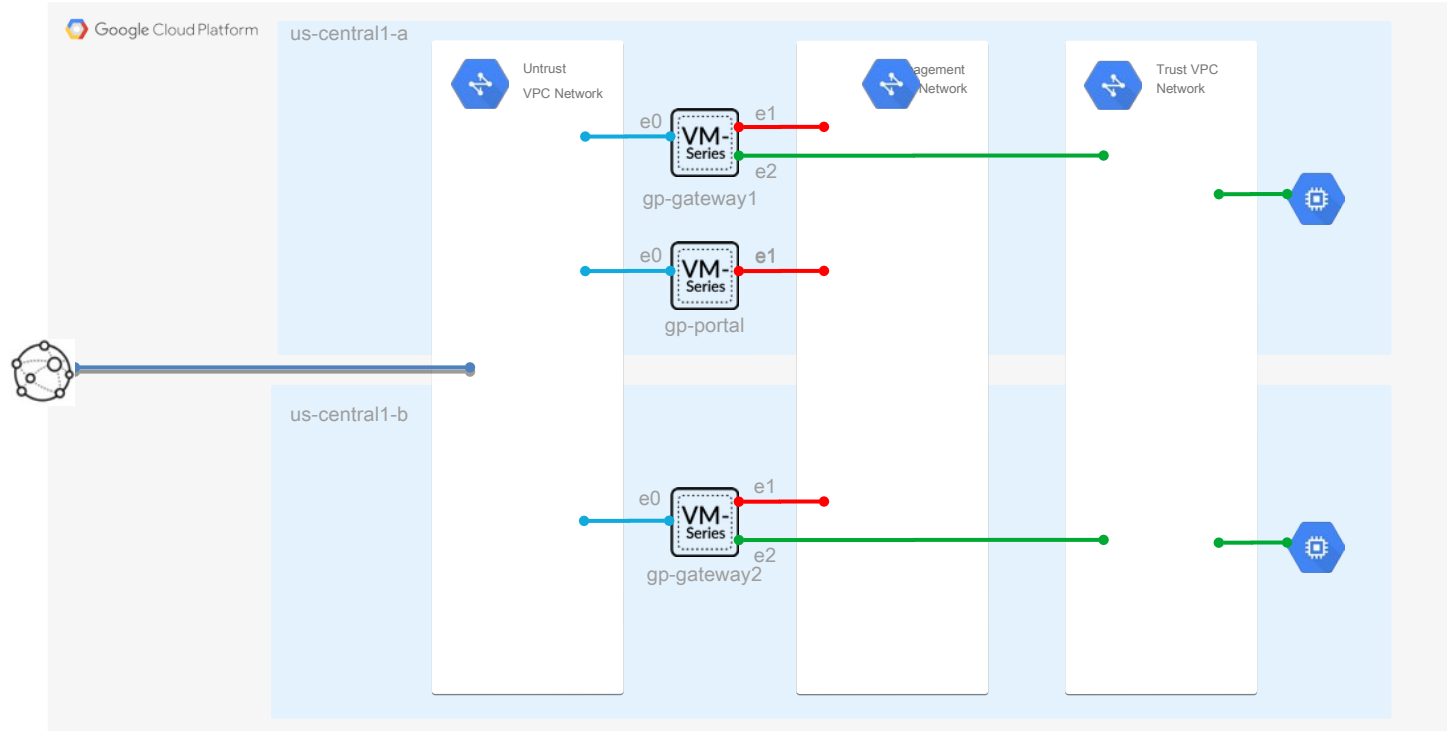


Customers are increasingly looking to the public cloud to provide scalable, flexible, on-demand infrastructure to support business-critical processes as well as disaster recovery on demand. The ability to establish scalable, secure connectivity to these environment is a critical element of enabling remote users.

Here, we demonstrate a simple GlobalProtect deployment consisting of a portal and two gateways in separate zones. Terraform is used to facilitate rapid, consistent deployment and bootstrapping is used to create pre-configured portals/gateways which reduces the post-deployment configuration steps required to get the solution up and running.



This is the infrastructure that will be built. A single GlobalProtect portal will be deployed to us-central1-a, two gateways to us-central1-a and us-central1-b, and two test Ubuntu hosts.



## Notes:

- The portal is displayed to us-central1-a and gateways are deployed to us-central1-a and us-central1-b. Alternate regions are supported by editing the tfvars file prior to deployment. The template will automatically pick the first two zones in the region.
- Two sample users have been created in the local database for testing purposes. Refer to published documentation for additional authentication options.
- The template creates a project with a unique ID and may be used as a stand-alone project or enabled as a host project for use with Shared VPC architectures.
- The template creates an entire sample deployment, including: a project, VPC networks, subnets, routes, GCP firewall rules, the GlobalProtect infrastructure, and two test ubuntu servers.
- A self-signed CA certificate is used for this example. For production use, a CA certificate signed by a corporate or public PKI is best practice.

Step 1: Navigate to the the GP-NoAutoscale directory and edit the file terraform.tfvars to suit requirements.

```
Billing_Account = "<GCP Billing Account>"
Base_Project_Name = "<Base Project Name>"
Public_Key_Path = "~/.ssh/id_rsa.pub"

#FW_PanOS = "byol-904"                # Uncomment for PAN-OS 9.0.4 - BYOL
FW_PanOS = "bundle1-904"              # Uncomment for PAN-OS 9.0.4 - PAYG Bundle 1
#FW_PanOS = "bundle2-904"              # Uncomment for PAN-OS 9.0.4 - PAYG Bundle 2

FW_Machine_Type = "<FW Machine Size>"
FW_Image = "https://www.googleapis.com/compute/v1/projects/paloaltonetworksgcp-public/global/images/"
GCP_Region = "<GCP Region>"
Management_Subnet_CIDR = "10.0.0.0/24"
Untrust_Subnet_CIDR = "10.0.1.0/24"
Trust_Subnet_CIDR = "10.0.2.0/24"
```

## Step 2: Authenticate to GCP.

```
bash-4.3# gcloud auth login
Go to the following link in your browser:

  https://accounts.google.com/o/oauth2/auth?code_challenge=uBJkH8p4pyeB1NZtFzfI8hxjKr5qm9FAZX8tdAfO
lRY&prompt=select_account&code_challenge_method=S256&access_type=offline&redirect_uri=urn%3Aietf%3Awg
%3Aoauth%3A2.0%3Aoob&response_type=code&client_id=32555940559.apps.googleusercontent.com&scope=openid
+https%3A%2F%2Fwww.googleapis.com%2Fauth%2Fuserinfo.email+https%3A%2F%2Fwww.googleapis.com%2Fauth%2Fcl
oud-platform+https%3A%2F%2Fwww.googleapis.com%2Fauth%2Fappengine.admin+https%3A%2F%2Fwww.googleapis.
com%2Fauth%2Fcompute+https%3A%2F%2Fwww.googleapis.com%2Fauth%2Faccounts.reauth

Enter verification code: 4/yQEQnp4mkB6jZC2wFi_ryxYj95q5jsMZTYzbILet9SDXvaXCpNxqGoI

You are now logged in as [ptglynn@cloudy.business].
Your current project is [adv-peering-2fw-2spoke-common]. You can change this setting by running:
  $ gcloud config set project PROJECT_ID

Updates are available for some Cloud SDK components. To install them,
please run:
  $ gcloud components update

bash-4.3#
```

Step 3: Apply the Terraform template to the environment. This process will take several minutes to complete as bootstrapping is used to perform the initial configuration of the portal/gateways. Once done, the output will include the management/untrust IP addresses of the portal/gateways as well as the private IP addresses of the test servers.

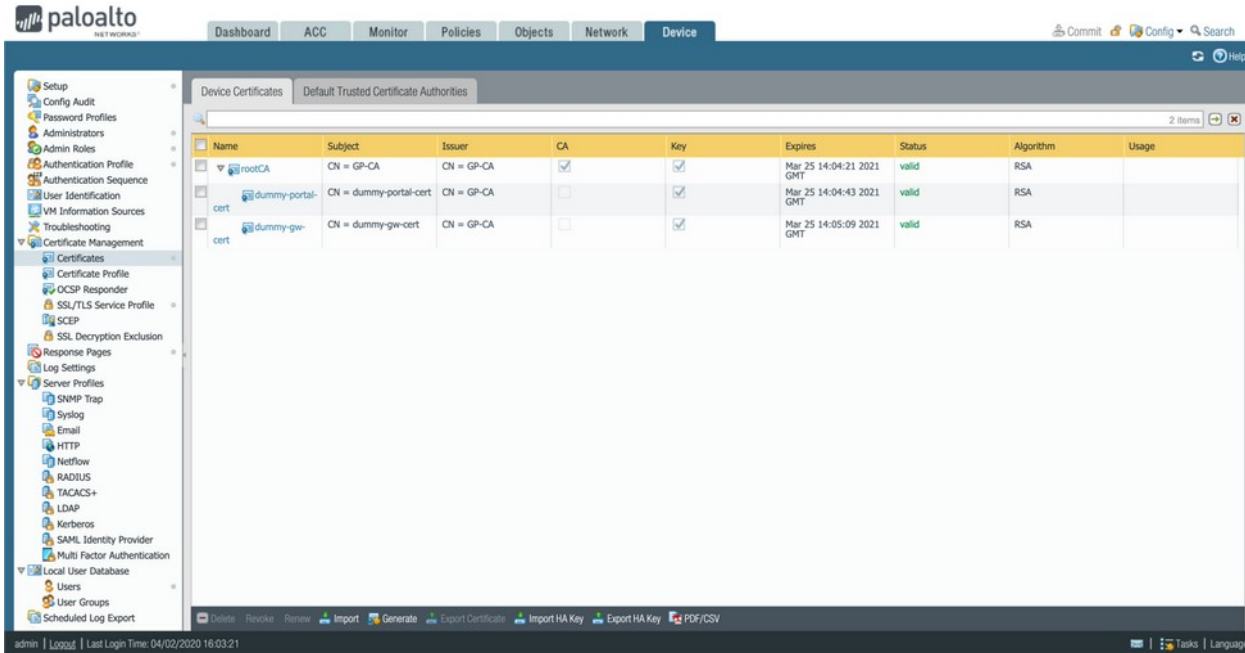
```
google_storage_bucket_object.portal_software: Refreshing state... [id=portal-55d9-software/null.txt]
google_storage_bucket_object.portal_license: Refreshing state... [id=portal-55d9-license/null.txt]
google_storage_bucket_object.portal_content: Refreshing state... [id=portal-55d9-content/null.txt]
google_compute_instance.server1: Refreshing state... [id=projects/782961236101/zones/us-central1-a/in
stances/server1]
google_compute_instance.server2: Refreshing state... [id=projects/782961236101/zones/us-central1-b/in
stances/server2]
google_compute_instance.gateway2: Refreshing state... [id=projects/782961236101/zones/us-central1-b/i
nstances/gp-gateway2]
google_compute_instance.gateway1: Refreshing state... [id=projects/782961236101/zones/us-central1-a/i
nstances/gp-gateway1]
google_compute_instance.portal: Refreshing state... [id=projects/782961236101/zones/us-central1-a/ins
tances/gp-portal]

Apply complete! Resources: 0 added, 0 changed, 0 destroyed.

Outputs:

Gateway1-Management-IP = 104.197.113.130
Gateway1-Untrust-IP = 35.184.52.74
Gateway2-Management-IP = 35.226.146.146
Gateway2-Untrust-IP = 104.154.69.217
Portal-Management-IP = 34.71.55.129
Portal-Untrust-IP = 35.223.117.106
Server1-IP = 10.0.2.5
Server2-IP = 10.0.2.4
bash - 4.3#
```

Step 4: Login to the portal ([admin/Pal0ALt0@123](#)) and navigate to the Device Tab > Certificates. Dummy certs have been added as placeholders and need to be replaced.



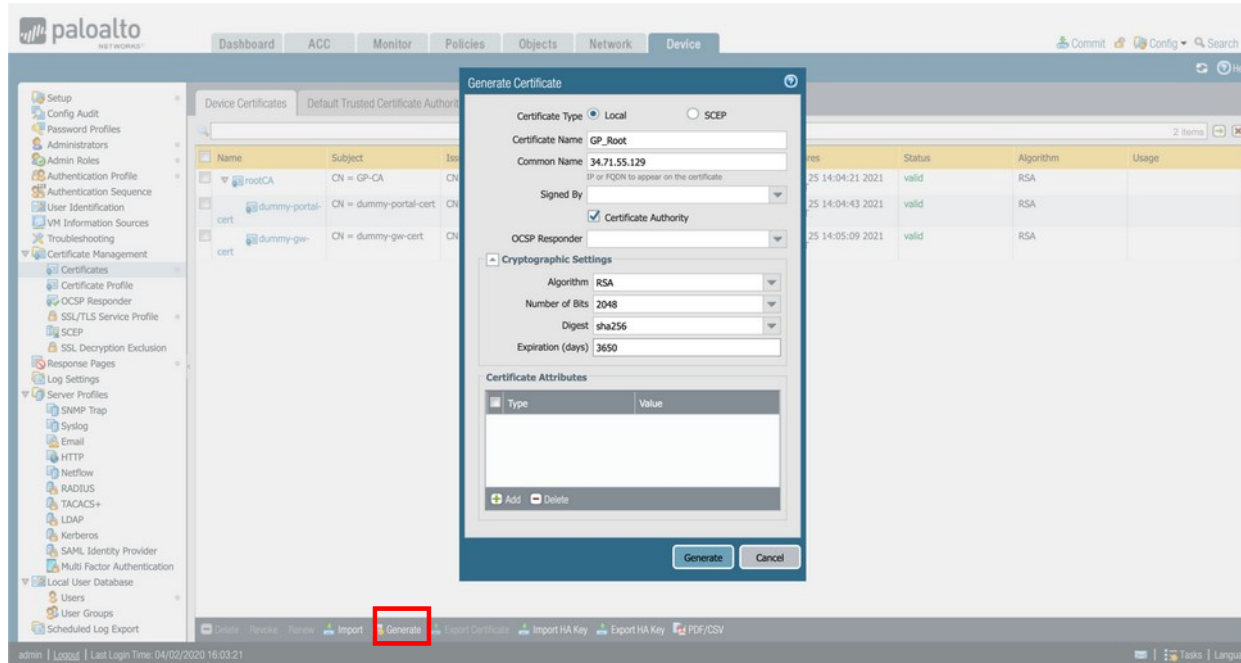
The screenshot shows the Palo Alto Networks management interface. The left sidebar contains a navigation menu with categories like Setup, Configuration, and Server Profiles. The main content area is titled 'Device Certificates' and shows a table of certificates. The table has the following columns: Name, Subject, Issuer, CA, Key, Expires, Status, Algorithm, and Usage. There are three certificates listed:

Name	Subject	Issuer	CA	Key	Expires	Status	Algorithm	Usage
rootCA	CN = GP-CA	CN = GP-CA	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Mar 25 14:04:21 2021 GMT	valid	RSA	
cert dummy-portal-cert	CN = dummy-portal-cert	CN = GP-CA	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Mar 25 14:04:43 2021 GMT	valid	RSA	
cert dummy-gw-cert	CN = dummy-gw-cert	CN = GP-CA	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Mar 25 14:05:09 2021 GMT	valid	RSA	

At the bottom of the interface, there is a status bar showing 'admin | Logout | Last Login Time: 04/02/2020 16:03:21' and a 'Tasks | Language' link.



Step 5: Click “Generate” at the bottom of the page and specify a descriptive name (e.g. “GP\_Root”), the public IP of the **management** interface of the portal, and optionally, set a longer expiration time. Tick the “Certificate Authority” box and then click “Generate”. This is the root CA certificate that will sign all other certificates.

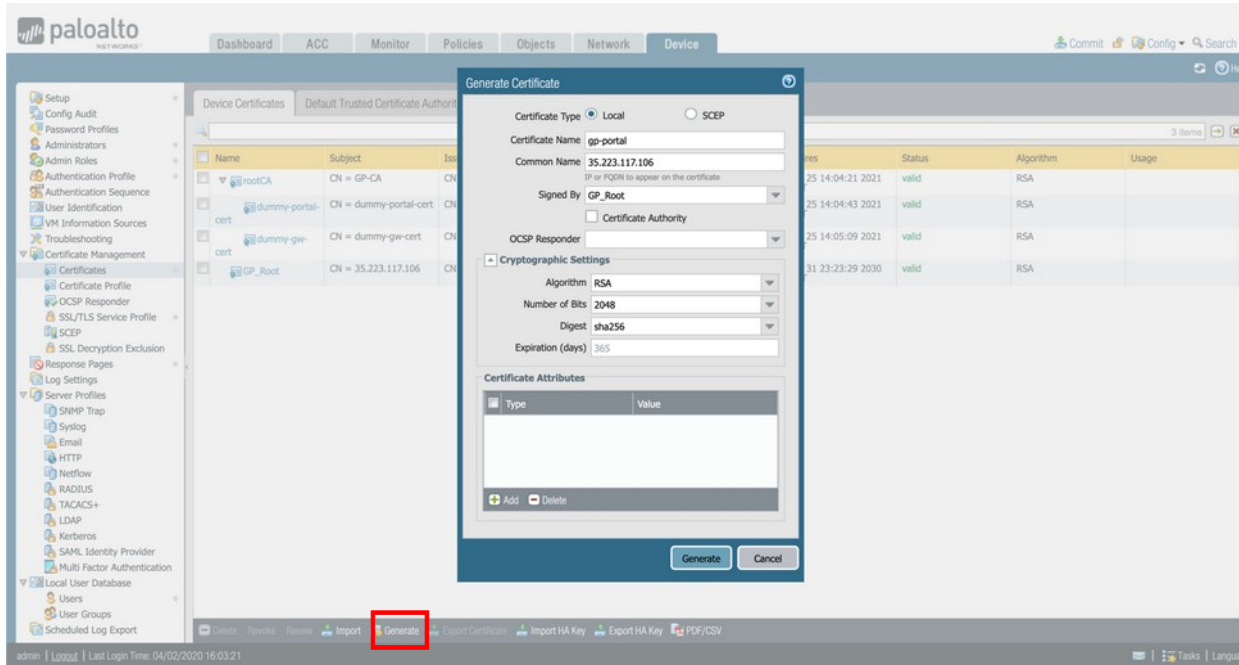


The screenshot shows the Palo Alto Networks management console with the 'Generate Certificate' dialog box open. The dialog box is titled 'Generate Certificate' and has a 'Certificate Type' dropdown set to 'Local'. The 'Certificate Name' field is 'GP\_Root' and the 'Common Name' field is '34.71.55.129'. The 'Signed By' dropdown is set to 'Certificate Authority'. The 'OCSP Responder' dropdown is set to 'Certificate Authority'. The 'Cryptographic Settings' section shows 'Algorithm' set to 'RSA', 'Number of Bits' set to '2048', 'Digest' set to 'sha256', and 'Expiration (days)' set to '3650'. The 'Certificate Attributes' section is empty. The 'Generate' button is highlighted with a red box at the bottom of the dialog box.

Name	Subject	Issued
rootCA	CN = GP-CA	CN
dummy-portal-cert	CN = dummy-portal-cert	CN
dummy-gw-cert	CN = dummy-gw-cert	CN

Expires	Status	Algorithm	Usage
25 14:04:21 2021	valid	RSA	
25 14:04:43 2021	valid	RSA	
25 14:05:09 2021	valid	RSA	

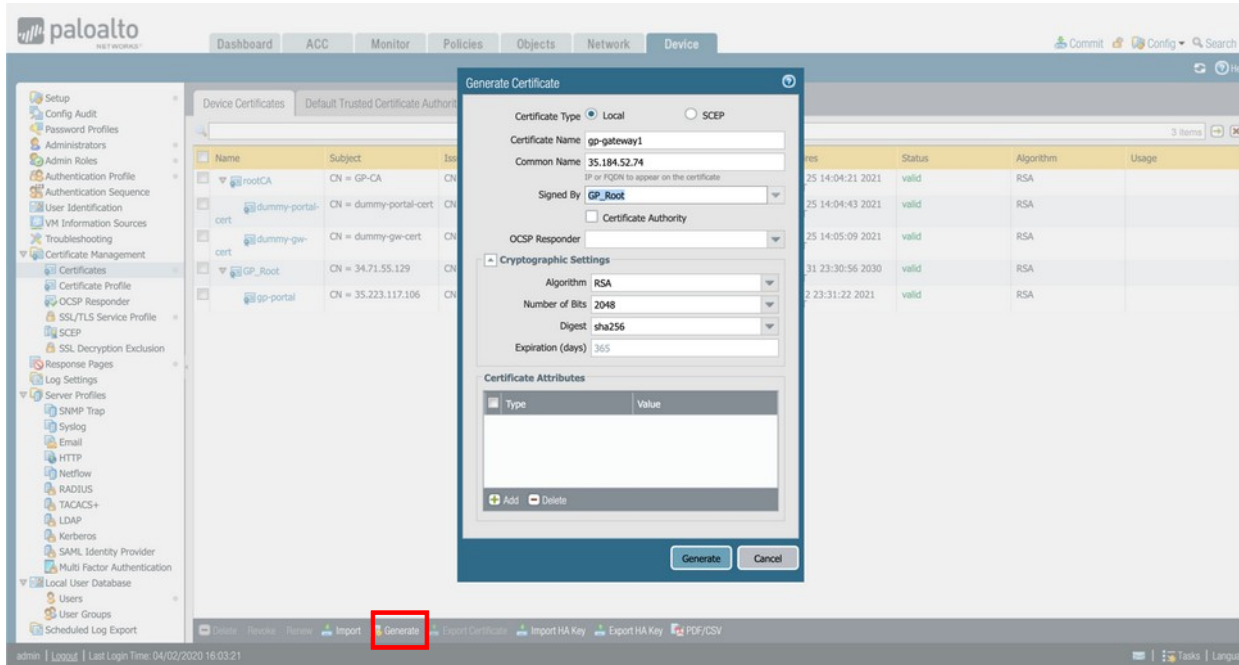
Step 6: Click “Generate” at the bottom of the page and specify a descriptive name (e.g. “gp-portal”), the public IP of the **untrust** interface of the portal. Select the recently-created root certificate from the “Signed By” drop-down and then click “Generate”. This is the certificate for the portal interface.



The screenshot shows the Palo Alto Networks GUI with the 'Generate Certificate' dialog box open. The dialog is titled 'Generate Certificate' and has a 'Local' radio button selected for 'Certificate Type'. The 'Certificate Name' is 'gp-portal' and the 'Common Name' is '35.223.117.106'. The 'Signed By' dropdown is set to 'GP\_Root'. The 'Cryptographic Settings' section shows 'Algorithm' as 'RSA', 'Number of Bits' as '2048', 'Digest' as 'sha256', and 'Expiration (days)' as '365'. The 'Generate' button at the bottom of the dialog is highlighted with a red box. In the background, the 'Device Certificates' page is visible, showing a table of certificates with columns for Name, Subject, Issued, and Status. The 'GP\_Root' certificate is listed with a status of 'valid'.

Name	Subject	Issued	Status	Algorithm	Usage
GP_Root	CN = GP-CA	25 14:04:21 2021	valid	RSA	
dummy-portal	CN = dummy-portal-cert	25 14:04:43 2021	valid	RSA	
dummy-gw	CN = dummy-gw-cert	25 14:05:09 2021	valid	RSA	
GP_Root	CN = 35.223.117.106	31 23:23:29 2030	valid	RSA	

Step 7: Click “Generate” at the bottom of the page and specify a descriptive name (e.g. “gp-gateway1”), the public IP of the **untrust** interface of the first gateway. Select the recently-created root certificate from the “Signed By” drop-down and then click “Generate”. This is the certificate for the first gateway interface.



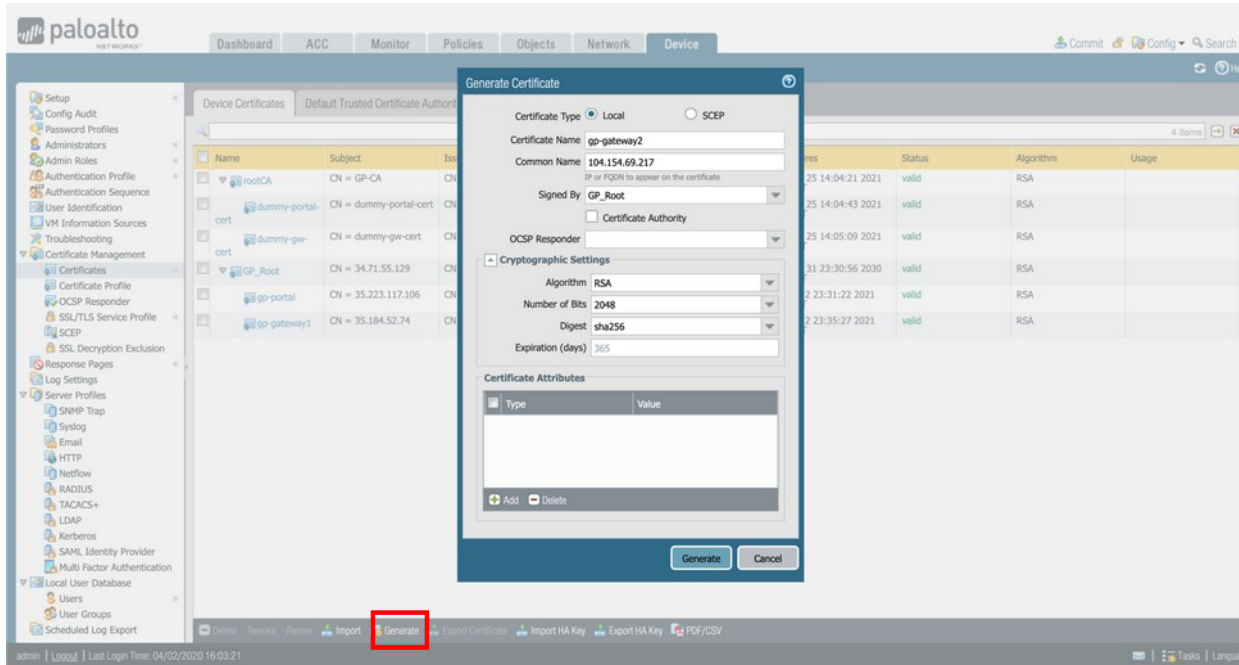
The screenshot shows the Palo Alto Networks configuration interface. The left sidebar contains a navigation menu with categories like Setup, Config Audit, Password Profiles, Administrators, Admin Roles, Authentication Profile, Authentication Sequence, User Identification, VM Information Sources, Troubleshooting, Certificate Management, Certificates, Certificate Profile, OSCP Responder, SSL/TLS Service Profile, SCEP, SSL Decryption Exclusion, Response Pages, Log Settings, Server Profiles, SNMP Trap, Syslog, Email, HTTP, Netflow, RADIUS, TACACS+, LDAP, Kerberos, SAML Identity Provider, Multi Factor Authentication, Local User Database, Users, User Groups, and Scheduled Log Export. The main content area is titled 'Device Certificates' and shows a table of certificates. A 'Generate Certificate' dialog box is open in the center, with the following fields and options:

- Certificate Type:** Local (selected), SCEP
- Certificate Name:** gp-gateway1
- Common Name:** 35.184.52.74
- Signed By:** GP\_Root (selected from a dropdown)
- OCSP Responder:** (empty dropdown)
- Cryptographic Settings:**
  - Algorithm:** RSA
  - Number of Bits:** 2048
  - Digest:** sha256
  - Expiration (days):** 365
- Certificate Attributes:** A table with columns 'Type' and 'Value'.

At the bottom of the dialog box are 'Generate' and 'Cancel' buttons. The 'Generate' button is highlighted with a red box. The background shows a table of certificates with columns: Name, Subject, Issued, Status, Algorithm, and Usage. The table contains three entries:

Name	Subject	Issued	Status	Algorithm	Usage
GP_Root	CN = GP-CA	25 14:04:21 2021	valid	RSA	
GP_Root	CN = GP-CA	25 14:04:43 2021	valid	RSA	
GP_Root	CN = GP-CA	25 14:05:09 2021	valid	RSA	

Step 8: Click “Generate” at the bottom of the page and specify a descriptive name (e.g. “gp-gateway2”), the public IP of the **untrust** interface of the second gateway. Select the recently-created root certificate from the “Signed By” drop-down and then click “Generate”. This is the certificate for the second gateway interface.



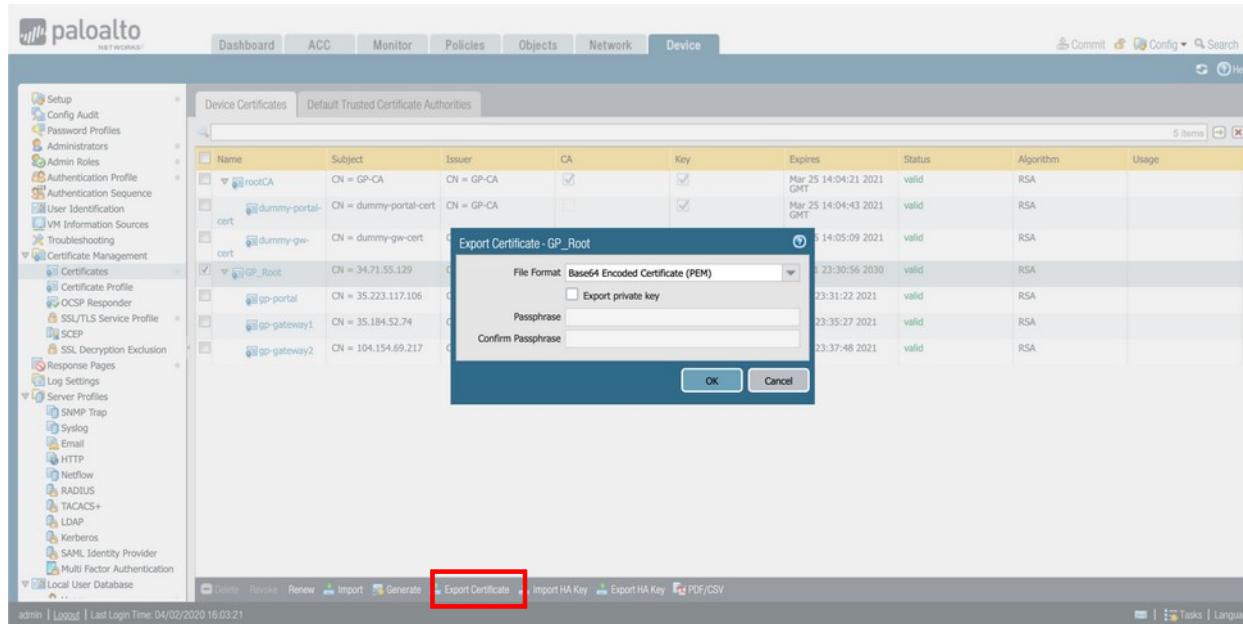
The screenshot shows the Palo Alto Networks GUI with the 'Generate Certificate' dialog box open. The dialog is titled 'Generate Certificate' and has a blue header. It contains the following fields and options:

- Certificate Type:** Local (selected), SCEP
- Certificate Name:** gp-gateway2
- Common Name:** 104.154.69.217
- Signed By:** GP\_Root (selected from a dropdown)
- OCSP Responder:** (empty)
- Cryptographic Settings:**
  - Algorithm: RSA
  - Number of Bits: 2048
  - Digest: sha256
  - Expiration (days): 365
- Certificate Attributes:** A table with columns 'Type' and 'Value'.

The 'Generate' button is highlighted with a red box at the bottom of the dialog. The background shows the 'Device Certificates' page with a table of certificates:

Name	Subject	Issued
GP_Root	CN = GP-CA	25 14:04:21 2021
GP_Root	CN = GP-CA	25 14:04:43 2021
GP_Root	CN = GP-CA	25 14:05:09 2021
GP_Root	CN = GP-CA	31 23:30:56 2030
GP_Root	CN = GP-CA	2 23:31:22 2021
GP_Root	CN = GP-CA	2 23:35:27 2021

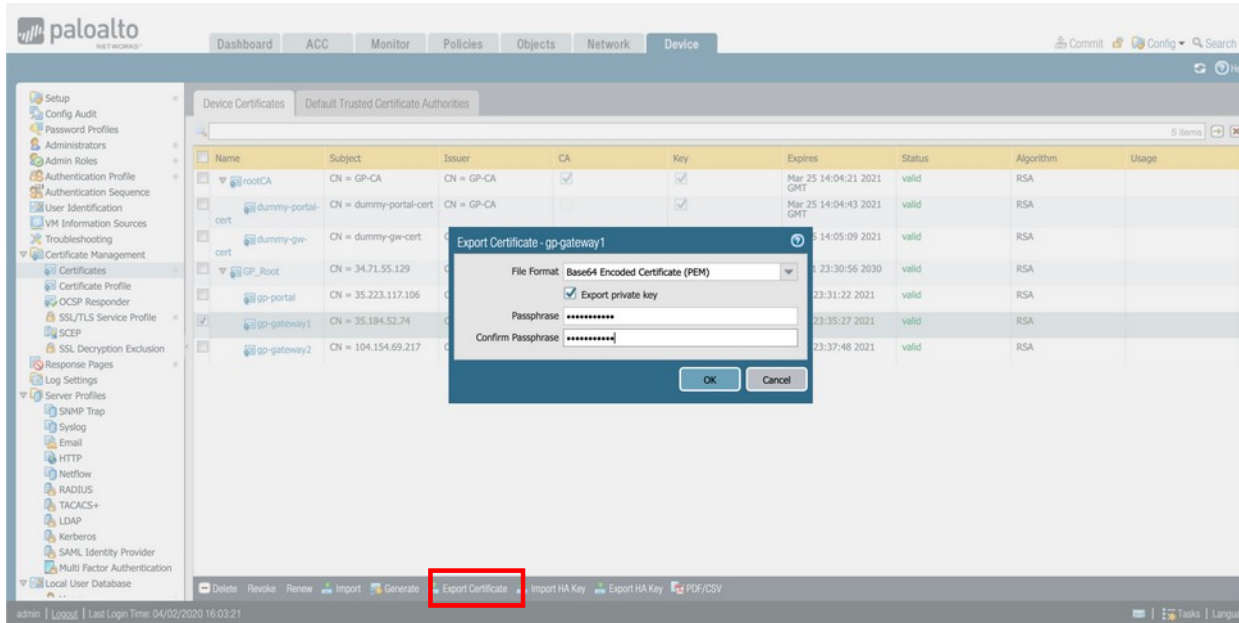
Step 9: Select the root certificate (GP\_Root in this example), and click “Export Certificate”. Save the certificate to a known location. This certificate must be imported into all of the gateways although the associated private key is not required.



The screenshot shows the Palo Alto Networks GUI with the 'Device' tab selected. The 'Device Certificates' section is active, displaying a table of certificates. The 'GP\_Root' certificate is selected, and the 'Export Certificate' dialog box is open. The dialog box shows the 'File Format' as 'Base64 Encoded Certificate (PEM)' and the 'Export private key' checkbox is unchecked. The 'Passphrase' and 'Confirm Passphrase' fields are empty. The 'OK' button is highlighted.

Name	Subject	Issuer	CA	Key	Expires	Status	Algorithm	Usage
rootCA	CN = GP-CA	CN = GP-CA	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Mar 25 14:04:21 2021 GMT	valid	RSA	
dummy-portal-cert	CN = dummy-portal-cert	CN = GP-CA	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Mar 25 14:04:43 2021 GMT	valid	RSA	
dummy-gw-cert	CN = dummy-gw-cert							
GP_Root	CN = 34.71.55.129				14-05-09 2021	valid	RSA	
gp-portal	CN = 35.223.117.106				23:30:56 2030	valid	RSA	
gp-gateway1	CN = 35.184.52.74				23:31:22 2021	valid	RSA	
gp-gateway2	CN = 104.154.69.217				23:35:27 2021	valid	RSA	
					23:37:48 2021	valid	RSA	

Step 10: Select the first gateway certificate (gp-gateway1 in this example), tick “Export Private Key”, specify a password, and click “OK”. Save the certificate to a known location. This certificate will be imported into the first gateway.



The screenshot shows the Palo Alto Networks GUI with the 'Device' tab selected. The 'Device Certificates' section is active, displaying a table of certificates. The 'gp-gateway1' certificate is selected. A dialog box titled 'Export Certificate - gp-gateway1' is open, showing the 'File Format' as 'Base64 Encoded Certificate (PEM)', the 'Export private key' checkbox checked, and fields for 'Passphrase' and 'Confirm Passphrase'.

Name	Subject	Issuer	CA	Key	Expires	Status	Algorithm	Usage
rootCA	CN = GP-CA	CN = GP-CA	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Mar 25 14:04:21 2021 GMT	valid	RSA	
dummy-portal-cert	CN = dummy-portal-cert	CN = GP-CA	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Mar 25 14:04:43 2021 GMT	valid	RSA	
dummy-gw-cert	CN = dummy-gw-cert				14-05-09 2021	valid	RSA	
GP_Root	CN = 34.71.55.129				23-30-56 2030	valid	RSA	
gp-portal	CN = 35.223.117.106				23-31-22 2021	valid	RSA	
gp-gateway1	CN = 35.184.52.74				23-35-27 2021	valid	RSA	
gp-gateway2	CN = 104.154.69.217				23-37-48 2021	valid	RSA	

Export Certificate - gp-gateway1

File Format: Base64 Encoded Certificate (PEM)

☒ Export private key

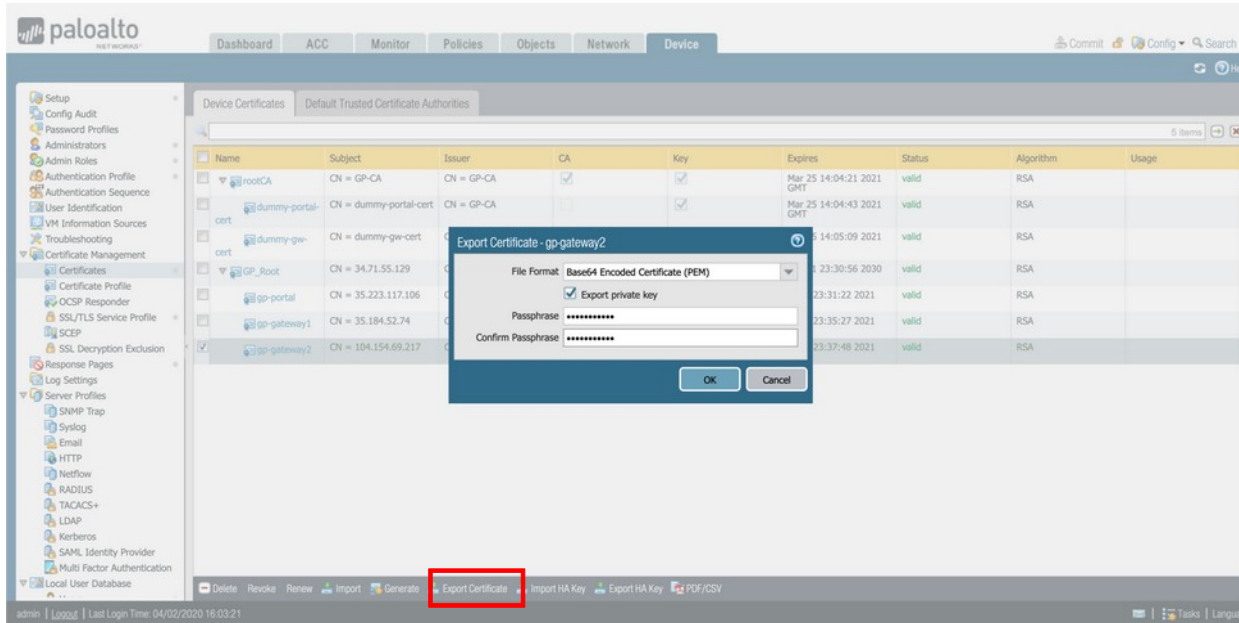
Passphrase: \*\*\*\*\*

Confirm Passphrase: \*\*\*\*\*

OK Cancel

Export Certificate

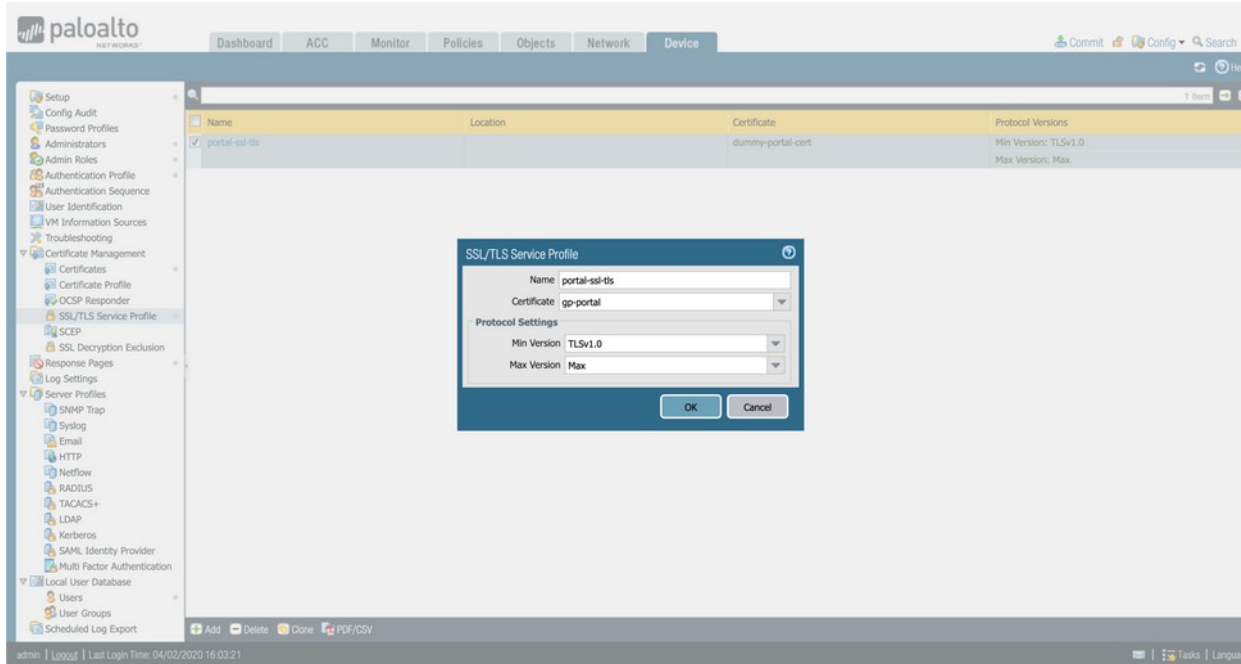
Step 11: Select the second gateway certificate (gp-gateway2 in this example), tick “Export Private Key”, specify a password, and click “OK”. Save the certificate to a known location. This certificate will be imported into the second gateway.



The screenshot shows the Palo Alto Networks configuration interface. The 'Device Certificates' table is displayed, showing a list of certificates. The 'gp-gateway2' certificate is selected. A dialog box titled 'Export Certificate - gp-gateway2' is open, showing the 'File Format' as 'Base64 Encoded Certificate (PEM)', the 'Export private key' checkbox is checked, and a 'Passphrase' field is visible. The 'OK' button is highlighted.

Name	Subject	Issuer	CA	Key	Expires	Status	Algorithm	Usage
rootCA	CN = GP-CA	CN = GP-CA	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Mar 25 14:04:21 2021 GMT	valid	RSA	
dummy-portal-cert	CN = dummy-portal-cert	CN = GP-CA	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Mar 25 14:04:43 2021 GMT	valid	RSA	
dummy-gw-cert	CN = dummy-gw-cert				14-05-09 2021	valid	RSA	
GP_Root	CN = 34.71.55.129				23-30-56 2030	valid	RSA	
gp-portal	CN = 35.223.117.106				23-31-22 2021	valid	RSA	
gp-gateway1	CN = 35.184.52.74				23-35-27 2021	valid	RSA	
gp-gateway2	CN = 104.154.69.217				23-37-48 2021	valid	RSA	

Step 12: Navigate to the **Device Tab > SSL/TLS Service Profile** and click on “portal-ssl-tls”. Click the Certificate drop-down and select the new portal certificate (gp-portal in this example).



The screenshot shows the Palo Alto Networks GUI with the **Device** tab selected. In the left sidebar, the navigation tree is expanded to **SSL/TLS Service Profile**. The main pane displays a table with one entry:

Name	Location	Certificate	Protocol Versions
portal-ssl-tls		dummy-portal-cert	Min Version: TLSv1.0 Max Version: Max

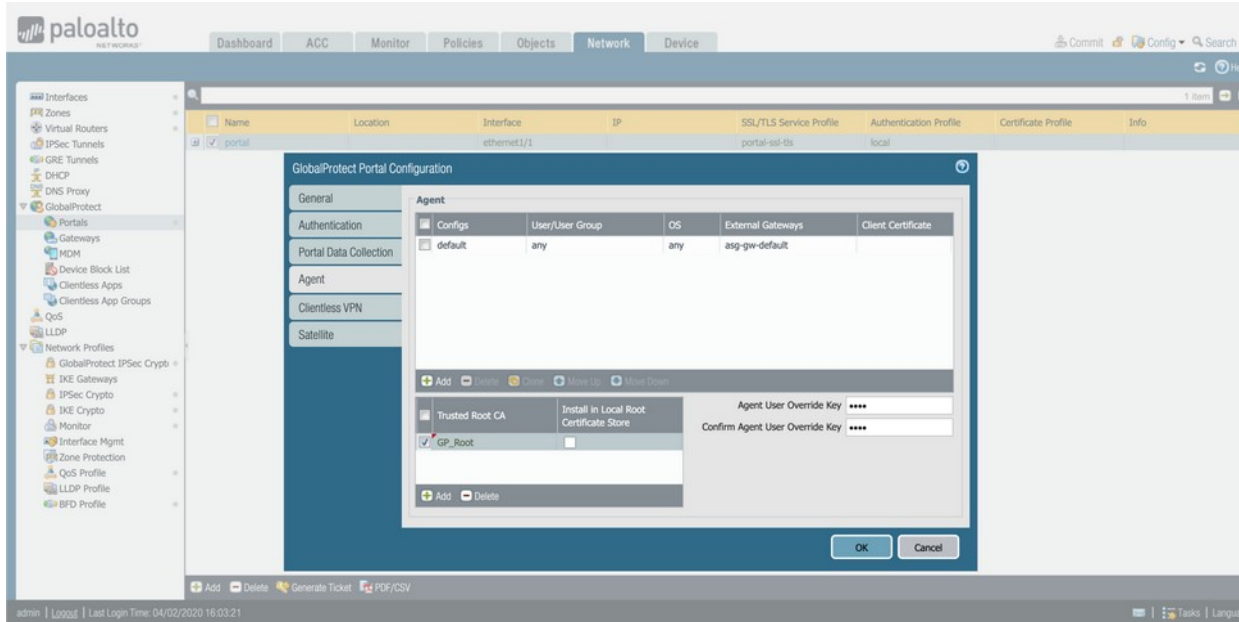
A modal window titled **SSL/TLS Service Profile** is open, showing the configuration for the selected profile:

- Name: portal-ssl-tls
- Certificate: gp-portal (selected from a dropdown)
- Protocol Settings:
  - Min Version: TLSv1.0
  - Max Version: Max

Buttons for **OK** and **Cancel** are at the bottom of the modal.



Step 12: Navigate to the Network **Tab** > **GlobalProtect** > **Portals** and click on “portal”. Click on the **Agent** tab. Update the “Trusted Root CA” to the recently created one. Click on “default”.



The screenshot shows the Palo Alto Networks management console. The left sidebar displays the navigation tree with 'GlobalProtect' expanded and 'Portals' selected. The main content area shows the 'GlobalProtect Portal Configuration' window for a portal named 'portal'. The 'Agent' tab is active, displaying a table of agent configurations.

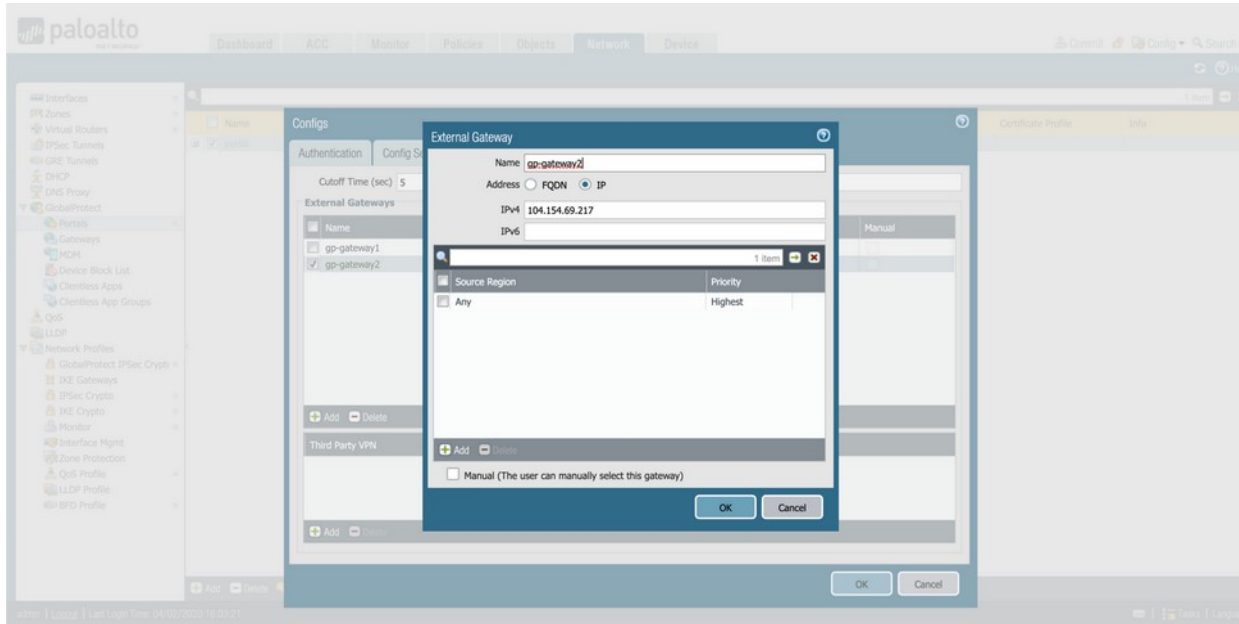
Configs	User/User Group	OS	External Gateways	Client Certificate
<input type="checkbox"/> default	any	any	asp-gw-default	

Below the table, there are buttons for 'Add', 'Delete', 'Clone', 'Move Up', and 'Move Down'. The 'Trusted Root CA' section shows a list of certificates:

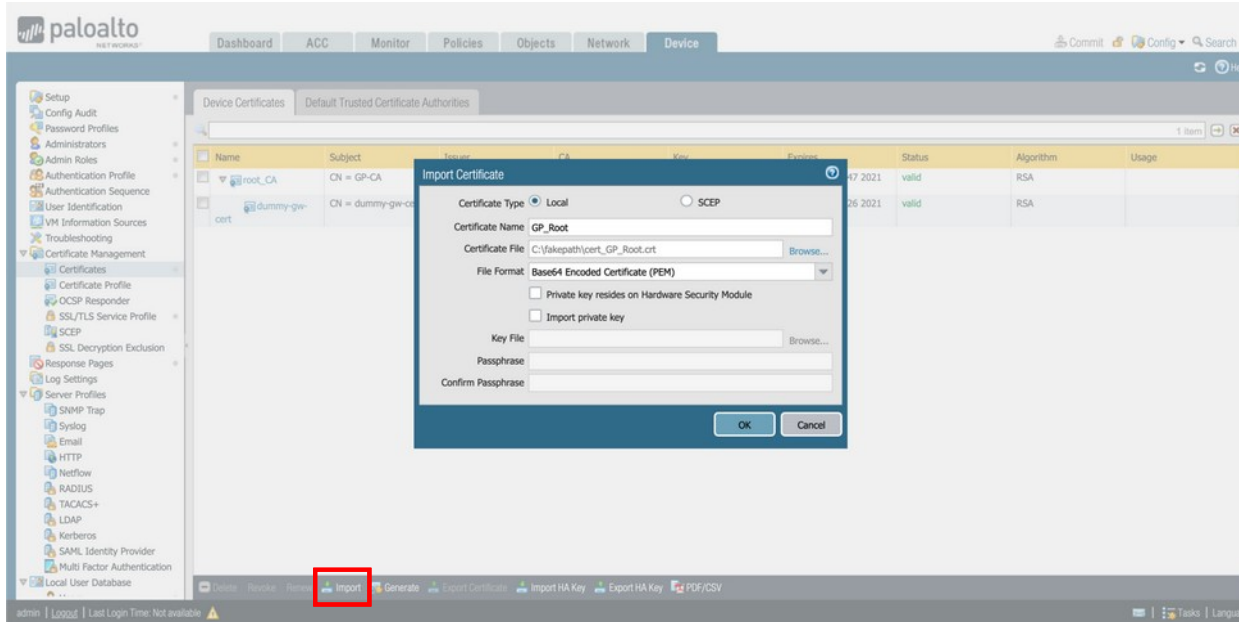
Trusted Root CA	Install in Local Root Certificate Store
<input checked="" type="checkbox"/> GP_Root	<input type="checkbox"/>

There are also input fields for 'Agent User Override Key' and 'Confirm Agent User Override Key', both containing four asterisks (\*\*\*\*). At the bottom of the window are 'OK' and 'Cancel' buttons.

Step 12: Click on the **External** tab, delete the existing external gateway and add the IP addresses of the two new gateways, specifying them by IP address. Commit the changes when done.



Step 13: Login to the first gateway ([admin/Pal0Alt0@123](http://admin/Pal0Alt0@123)) and navigate to the Device Tab > Certificates. Click “Import”. Provide a name for the certificate (e.g. GP\_Root), and browse to the location of the exported root certificate. Click “OK”.

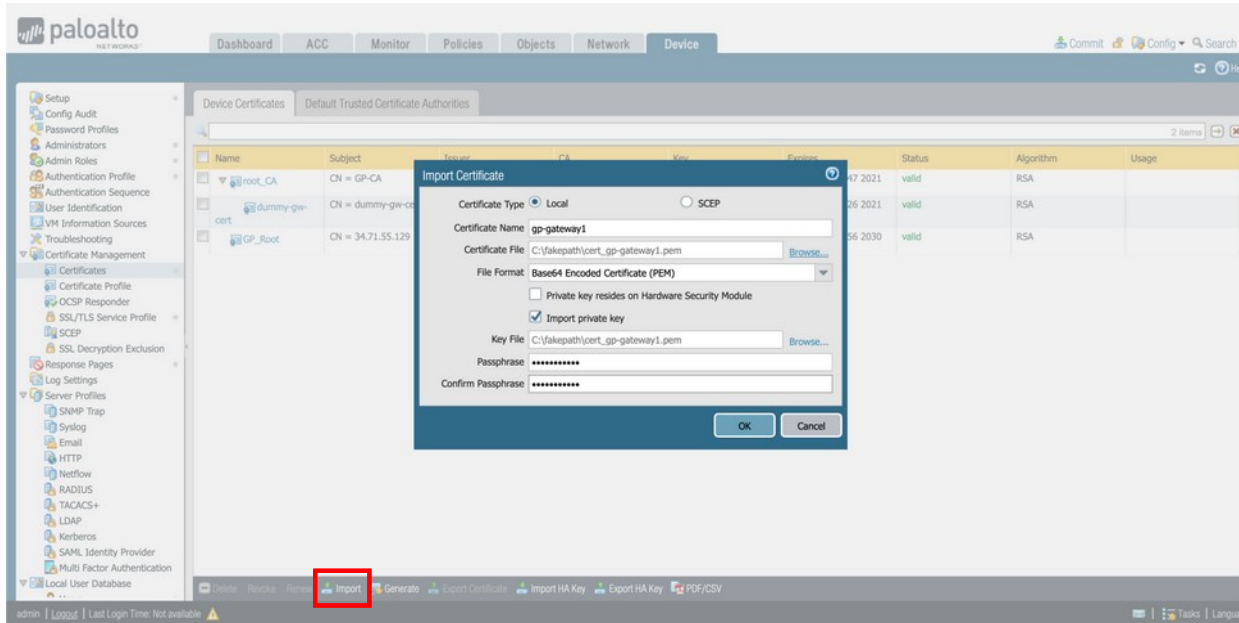


The screenshot shows the Palo Alto Networks management interface. The left sidebar contains a tree view with categories like Setup, Configuration, and Server Profiles. The main content area is titled 'Device Certificates' and shows a table of certificates. An 'Import Certificate' dialog box is open in the center, with the following fields and options:

- Certificate Type:** Local (selected), SCEP
- Certificate Name:** GP\_Root
- Certificate File:** C:\fakepath\cert\_GP\_Root.crt (with a 'Browse...' button)
- File Format:** Base64 Encoded Certificate (PEM)
- ☐ Private key resides on Hardware Security Module
- ☐ Import private key
- Key File:** (with a 'Browse...' button)
- Passphrase:** (text field)
- Confirm Passphrase:** (text field)
- Buttons:** OK, Cancel

At the bottom of the interface, there is a toolbar with buttons for 'Delete', 'Revoke', 'Import', 'Generate', 'Export Certificate', 'Import HA Key', 'Export HA Key', and 'PDF/CSV'. The 'Import' button is highlighted with a red box.

Step 14: Click “Import”. Provide a name for the certificate (e.g. gp-gateway1), and browse to the location of the exported certificate for the first gateway. Tick “Import private key”, browse to the location of the exported certificate for the first gateway, and input the password used to secure the certificate. Click “OK”.



The screenshot shows the Palo Alto Networks configuration interface. The left sidebar contains a navigation tree with categories like Setup, Configuration, and Certificate Management. The main pane displays the 'Device Certificates' table. An 'Import Certificate' dialog box is open in the foreground, allowing for the import of a local certificate. The dialog includes fields for Certificate Name, Certificate File, File Format, Key File, Passphrase, and Confirm Passphrase. The 'Import private key' checkbox is checked. The 'OK' button is highlighted with a red box in the bottom toolbar.

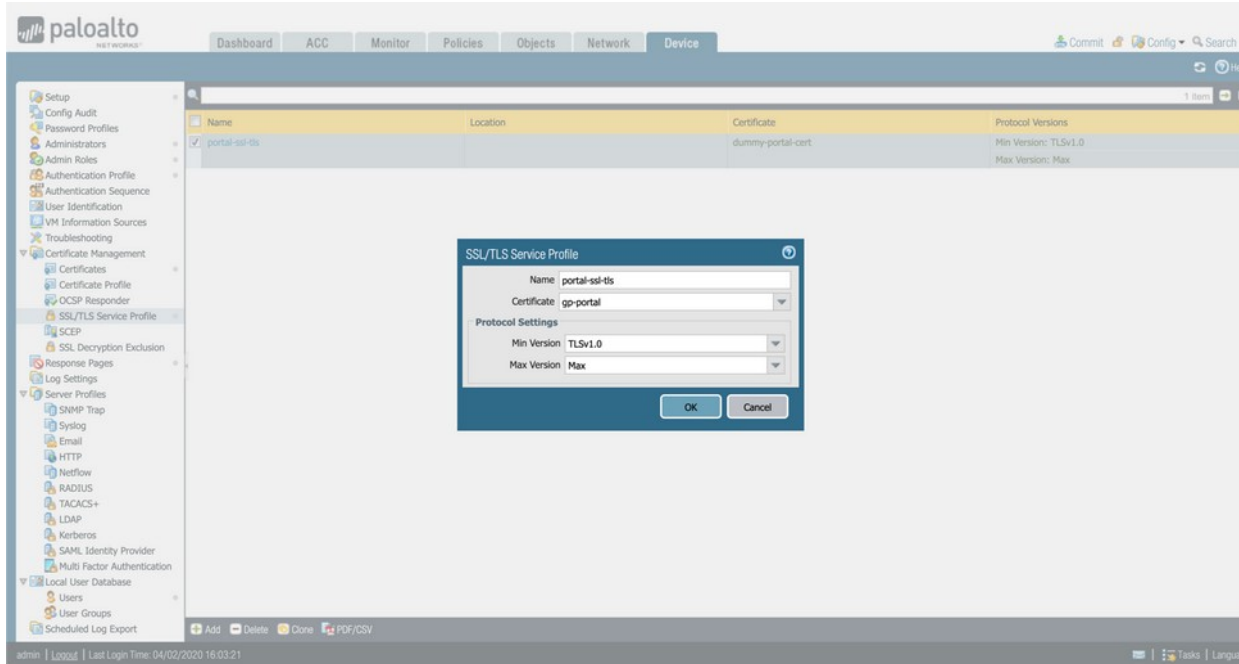
Name	Subject	Issuer	CA	Key	Expiry	Status	Algorithm	Usage
root_CA	CN = GP-CA				47 2021	valid	RSA	
dummy-gw-cert	CN = dummy-gw-cert				26 2021	valid	RSA	
GP_Root	CN = 34.71.55.129				56 2030	valid	RSA	

**Import Certificate Dialog:**

- Certificate Type: ☒ Local ☐ SCEP
- Certificate Name: gp-gateway1
- Certificate File: C:\fakepath\cert\_gp-gateway1.pem
- File Format: Base64 Encoded Certificate (PEM)
- ☐ Private key resides on Hardware Security Module
- ☒ Import private key
- Key File: C:\fakepath\cert\_gp-gateway1.pem
- Passphrase: \*\*\*\*\*
- Confirm Passphrase: \*\*\*\*\*

Buttons: OK, Cancel

Step 15: Navigate to the **Device Tab > SSL/TLS Service Profile** and click on “gateway-ssl-tls”. Click the Certificate drop-down and select the new portal certificate (gp-gateway1 in this example). Commit all changes.



The screenshot shows the Palo Alto Networks configuration interface. The left sidebar contains a navigation tree with categories like Setup, Configuration, and Server Profiles. The 'SSL/TLS Service Profile' is selected under the 'Certificates' section. The main panel displays a table of existing profiles, with 'portal-ssl-tls' highlighted. A modal dialog titled 'SSL/TLS Service Profile' is open, showing the configuration for the selected profile. The 'Name' field is 'portal-ssl-tls', the 'Certificate' dropdown is set to 'gp-portal', and the 'Protocol Settings' are 'Min Version: TLSv1.0' and 'Max Version: Max'. The 'OK' and 'Cancel' buttons are at the bottom of the dialog.

Name	Location	Certificate	Protocol Versions
portal-ssl-tls		dummy-portal-cert	Min Version: TLSv1.0 Max Version: Max

**SSL/TLS Service Profile**

Name: portal-ssl-tls

Certificate: gp-portal

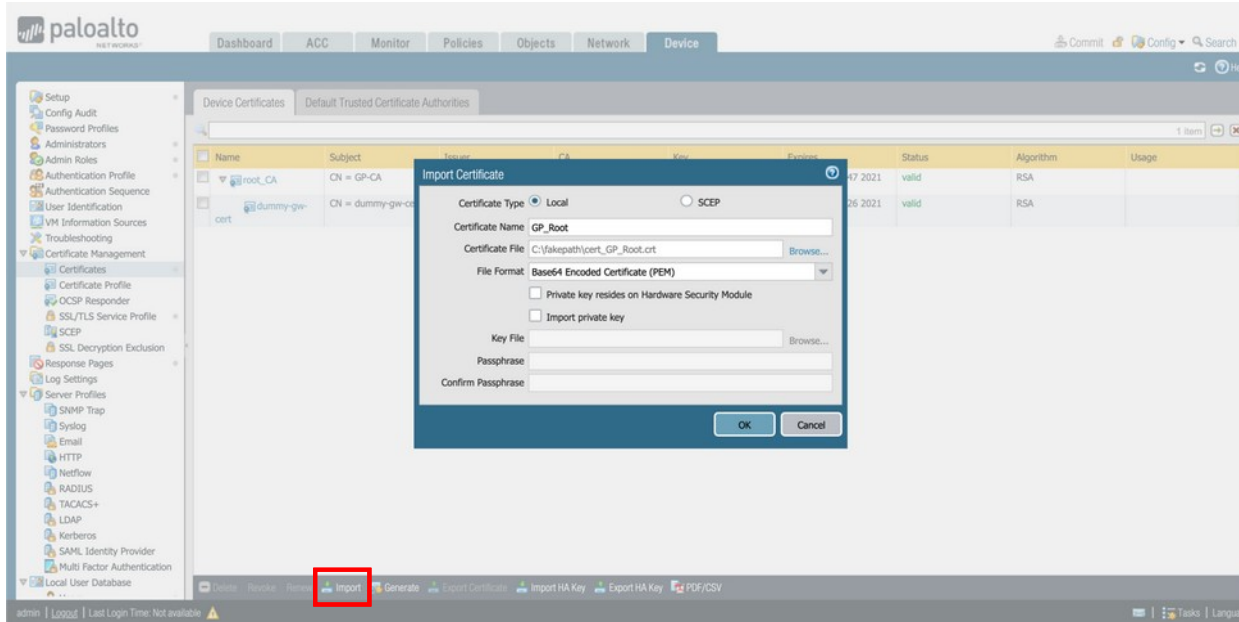
Protocol Settings

Min Version: TLSv1.0

Max Version: Max

OK Cancel

Step 16: Login to the second gateway ([admin/Pal0ALt0@123](#)) and navigate to the Device Tab > Certificates. Click “Import”. Provide a name for the certificate (e.g. GP\_Root), and browse to the location of the exported root certificate. Click “OK”.

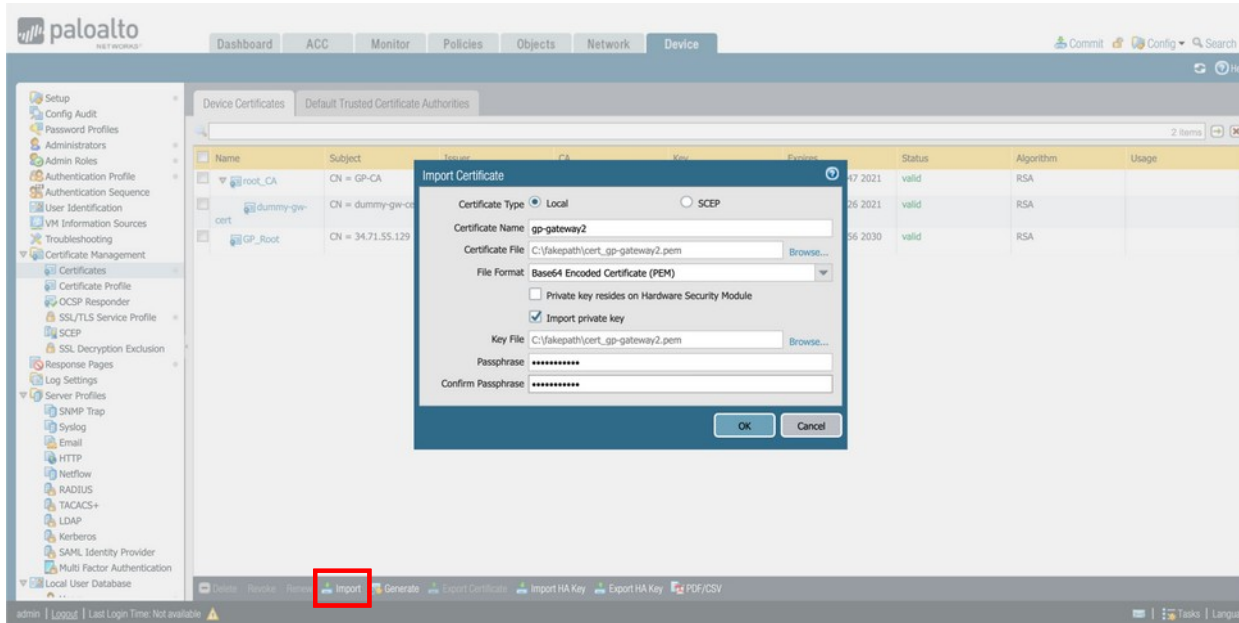


The screenshot shows the Palo Alto Networks management console interface. The left sidebar contains a navigation tree with categories like Setup, Configuration, and Troubleshooting. The main panel is titled 'Device Certificates' and shows a table of certificates. An 'Import Certificate' dialog box is open in the center, with the following fields and options:

- Certificate Type:** Local (selected), SCEP
- Certificate Name:** GP\_Root
- Certificate File:** C:\fakepath\cert\_GP\_Root.crt (with a 'Browse...' button)
- File Format:** Base64 Encoded Certificate (PEM) (dropdown menu)
- ☐ Private key resides on Hardware Security Module
- ☐ Import private key
- Key File:** (with a 'Browse...' button)
- Passphrase:** (text field)
- Confirm Passphrase:** (text field)

At the bottom of the console, there is a toolbar with buttons: Delete, Revoke, **Import** (highlighted with a red box), Generate, Export Certificate, Import HA Key, Export HA Key, and PDF/CSV. The status bar at the very bottom shows 'admin | Logout | Last Login Time: Not available'.

Step 17: Click “Import”. Provide a name for the certificate (e.g. gp-gateway2), and browse to the location of the exported certificate for the second gateway. Tick “Import private key”, browse to the location of the exported certificate for the first gateway, and input the password used to secure the certificate. Click “OK”.



The screenshot shows the Palo Alto Networks configuration interface. The left sidebar contains a tree view with categories like Setup, Configuration, and Certificate Management. The main pane displays the 'Device Certificates' section with a table of certificates. An 'Import Certificate' dialog box is open in the foreground, allowing for the import of a new certificate.

**Device Certificates Table:**

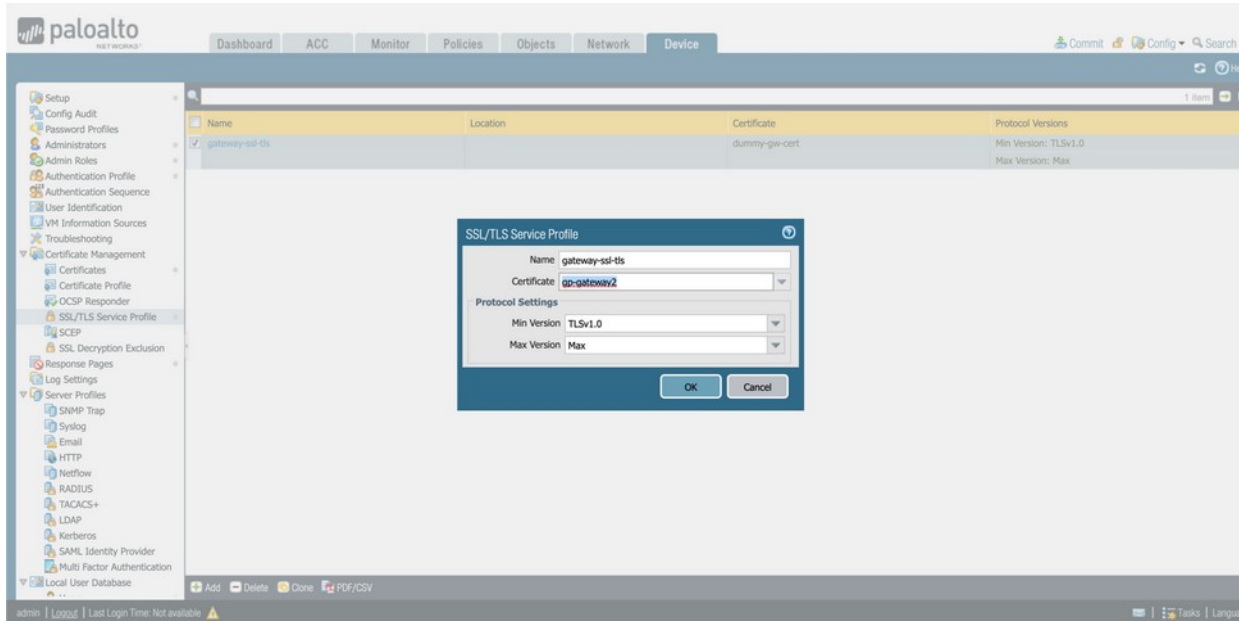
Name	Subject	Issuer	CA	Key	Expires	Status	Algorithm	Usage
root_CA	CN = GP-CA				47 2021	valid	RSA	
dummy-gw-cert	CN = dummy-gw-cert				26 2021	valid	RSA	
GP_Root	CN = 34.71.55.129				56 2030	valid	RSA	

**Import Certificate Dialog Box Fields:**

- Certificate Type:** Local (selected), SCEP
- Certificate Name:** gp-gateway2
- Certificate File:** C:\fakepath\cert\_gp-gateway2.pem (Browse...)
- File Format:** Base64 Encoded Certificate (PEM)
- Private key resides on Hardware Security Module:** ☐
- Import private key:** ☒
- Key File:** C:\fakepath\cert\_gp-gateway2.pem (Browse...)
- Passphrase:** [Redacted]
- Confirm Passphrase:** [Redacted]

At the bottom of the configuration pane, the 'Import' button is highlighted with a red box. Other buttons visible include 'Generate', 'Export Certificate', 'Import HA Key', 'Export HA Key', and 'PDF/CSV'.

Step 18: Navigate to the **Device Tab > SSL/TLS Service Profile** and click on “gateway-ssl-tls”. Click the Certificate drop-down and select the new portal certificate (gp-gateway2 in this example). Commit all changes.



The screenshot shows the Palo Alto Networks management interface. The left sidebar contains a navigation tree with categories like Setup, Configuration, and Server Profiles. The 'SSL/TLS Service Profile' is selected under the 'Certificates' section. The main panel displays a table with one entry: 'gateway-ssl-tls'. A modal window titled 'SSL/TLS Service Profile' is open, showing the configuration for this profile. The 'Name' field is 'gateway-ssl-tls', the 'Certificate' dropdown is set to 'gp-gateway2', and the 'Protocol Settings' show 'Min Version' as 'TLSv1.0' and 'Max Version' as 'Max'. The bottom status bar indicates the user is 'admin' and the last login time is 'Not available'.

Name	Location	Certificate	Protocol Versions
gateway-ssl-tls		dummy-gw-cert	Min Version: TLSv1.0 Max Version: Max

**SSL/TLS Service Profile**

Name: gateway-ssl-tls

Certificate: gp-gateway2

Protocol Settings

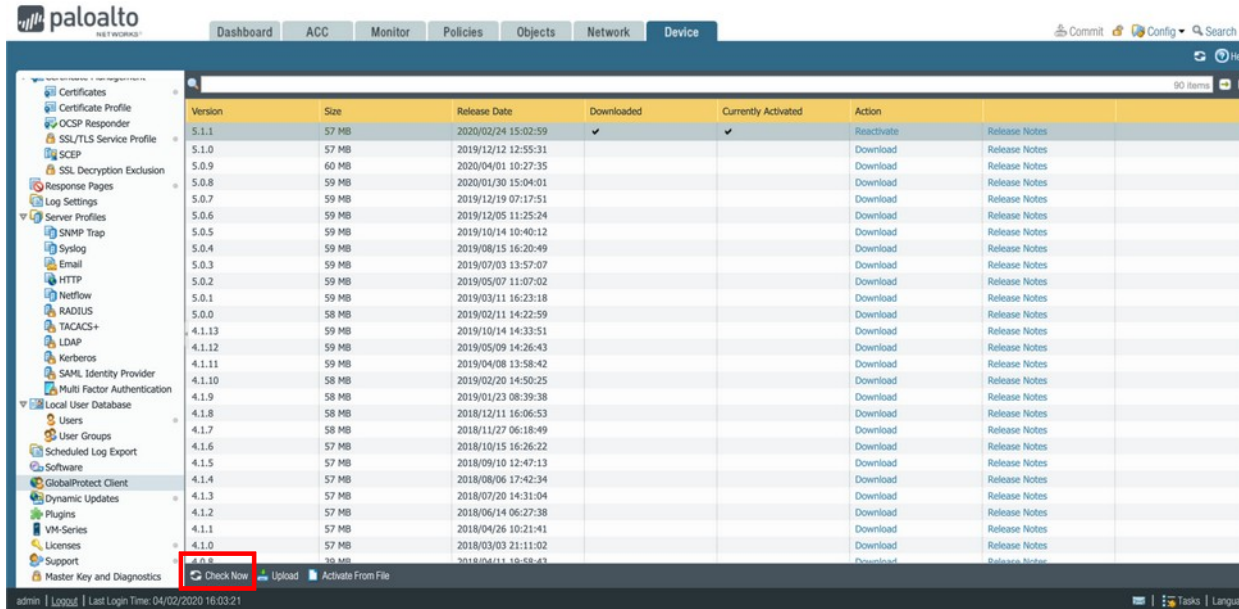
Min Version: TLSv1.0

Max Version: Max

OK Cancel



Step 19: Login to the portal and Navigate to the **Device Tab > GlobalProtect Client** and click on “Check Now”. Download and then activate the desired client version. If you see the error “The device is not found or not registered, please try after some time”, acknowledge the error and click “Check Now” again.

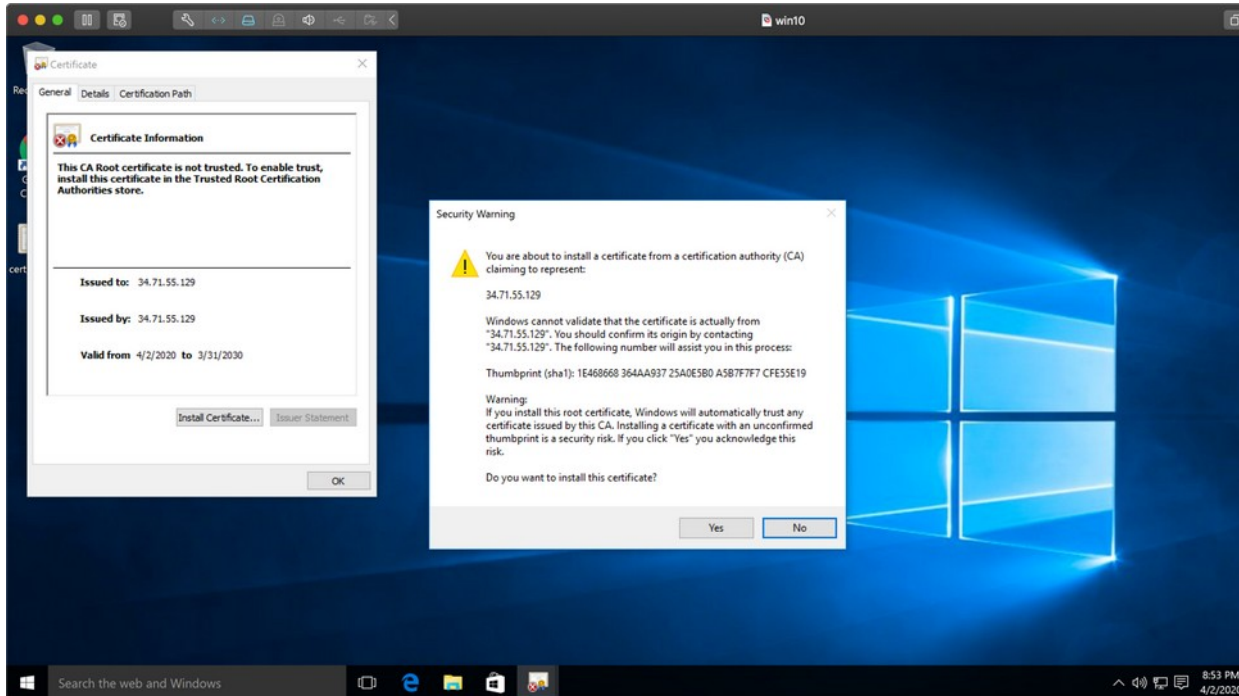


The screenshot shows the Palo Alto Networks management interface. The 'Device' tab is selected, and the 'GlobalProtect Client' section is expanded. A table lists various client versions and their details. The 'Check Now' button at the bottom of the table is highlighted with a red box.

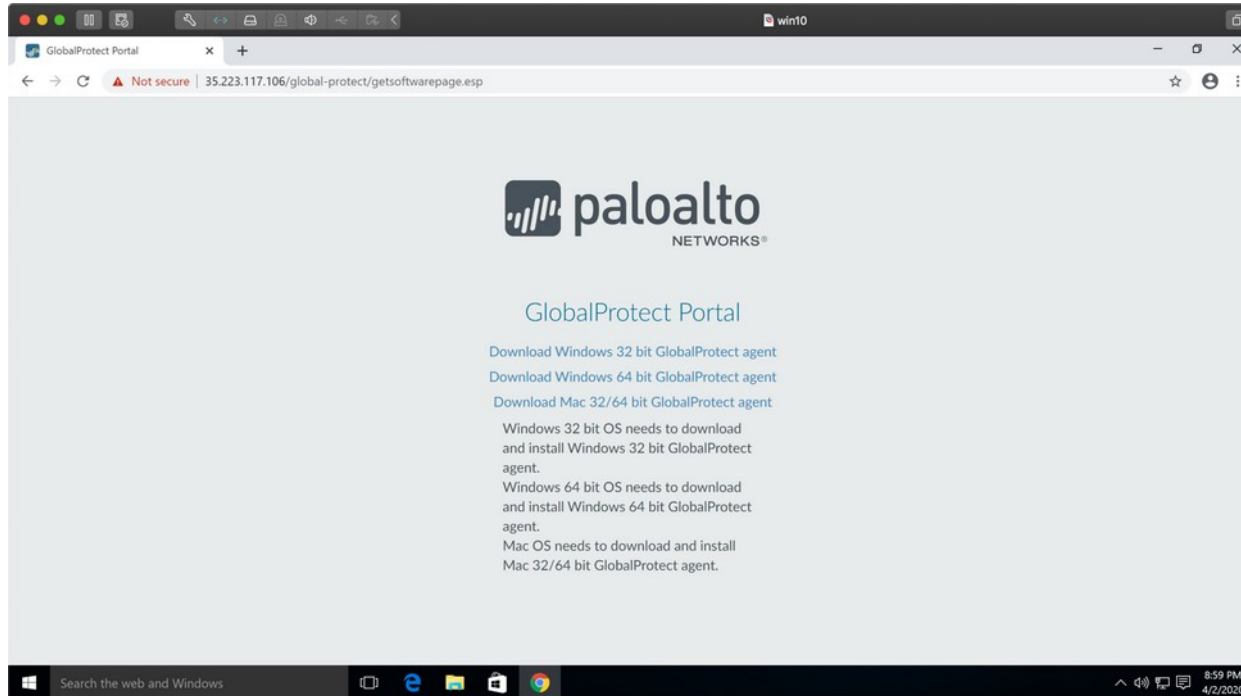
Version	Size	Release Date	Downloaded	Currently Activated	Action	Release Notes
5.1.1	57 MB	2020/02/24 15:02:59	✓	✓	Reactivate	Release Notes
5.1.0	57 MB	2019/12/12 12:55:31			Download	Release Notes
5.0.9	60 MB	2020/04/01 10:27:35			Download	Release Notes
5.0.8	59 MB	2020/01/30 15:04:01			Download	Release Notes
5.0.7	59 MB	2019/12/19 07:17:51			Download	Release Notes
5.0.6	59 MB	2019/12/05 11:25:24			Download	Release Notes
5.0.5	59 MB	2019/10/14 10:40:12			Download	Release Notes
5.0.4	59 MB	2019/08/15 16:20:49			Download	Release Notes
5.0.3	59 MB	2019/07/03 13:57:07			Download	Release Notes
5.0.2	59 MB	2019/05/07 11:07:02			Download	Release Notes
5.0.1	59 MB	2019/03/11 16:23:18			Download	Release Notes
5.0.0	58 MB	2019/02/11 14:22:59			Download	Release Notes
4.1.13	59 MB	2019/10/14 14:33:51			Download	Release Notes
4.1.12	59 MB	2019/05/09 14:26:43			Download	Release Notes
4.1.11	59 MB	2019/04/08 13:58:42			Download	Release Notes
4.1.10	58 MB	2019/02/20 14:50:25			Download	Release Notes
4.1.9	58 MB	2019/01/23 08:39:38			Download	Release Notes
4.1.8	58 MB	2018/12/11 16:06:53			Download	Release Notes
4.1.7	58 MB	2018/11/27 06:18:49			Download	Release Notes
4.1.6	57 MB	2018/10/15 16:26:22			Download	Release Notes
4.1.5	57 MB	2018/09/10 12:47:13			Download	Release Notes
4.1.4	57 MB	2018/08/06 17:42:34			Download	Release Notes
4.1.3	57 MB	2018/07/20 14:31:04			Download	Release Notes
4.1.2	57 MB	2018/06/14 06:27:38			Download	Release Notes
4.1.1	57 MB	2018/04/26 10:21:41			Download	Release Notes
4.1.0	57 MB	2018/03/03 21:11:02			Download	Release Notes
4.0.9	57 MB	2018/02/11 10:40:43			Download	Release Notes

At the bottom of the table, there are buttons for 'Check Now', 'Upload', and 'Activate From File'. The 'Check Now' button is highlighted with a red box.


Step 20: Copy the exported CA certificate to the test machine and import it as a trusted CA certificate. This is required to ensure that the client trusts the certificates presented by the portal and gateways.



Step 21: Login to the portal using one of the two pre-created GlobalProtect users (gp-user1/paloalto) or (gp-user2/paloalto). Once authenticated, download and install the relevant client software.



Step 22: Enter one of the ample username/password combinations and click “Sign In”.

GlobalProtect 

Sign In

Enter login credentials

Portal: 35.223.117.106

Sign In

Cancel

Step 23: Enter one of the ample username/password combinations and click “Sign In”.

GlobalProtect

## Sign In

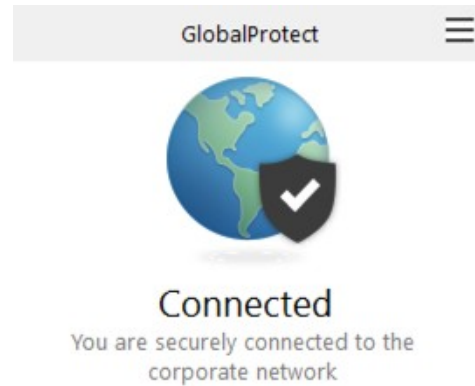
Enter login credentials

Portal: 35.223.117.106

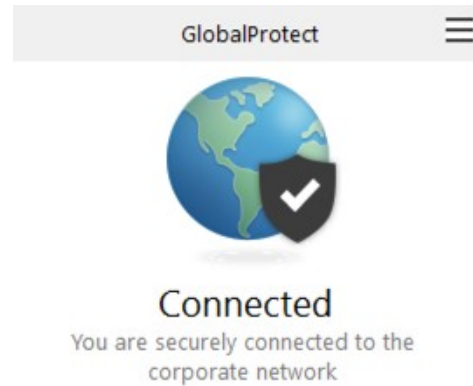
Sign In

Cancel

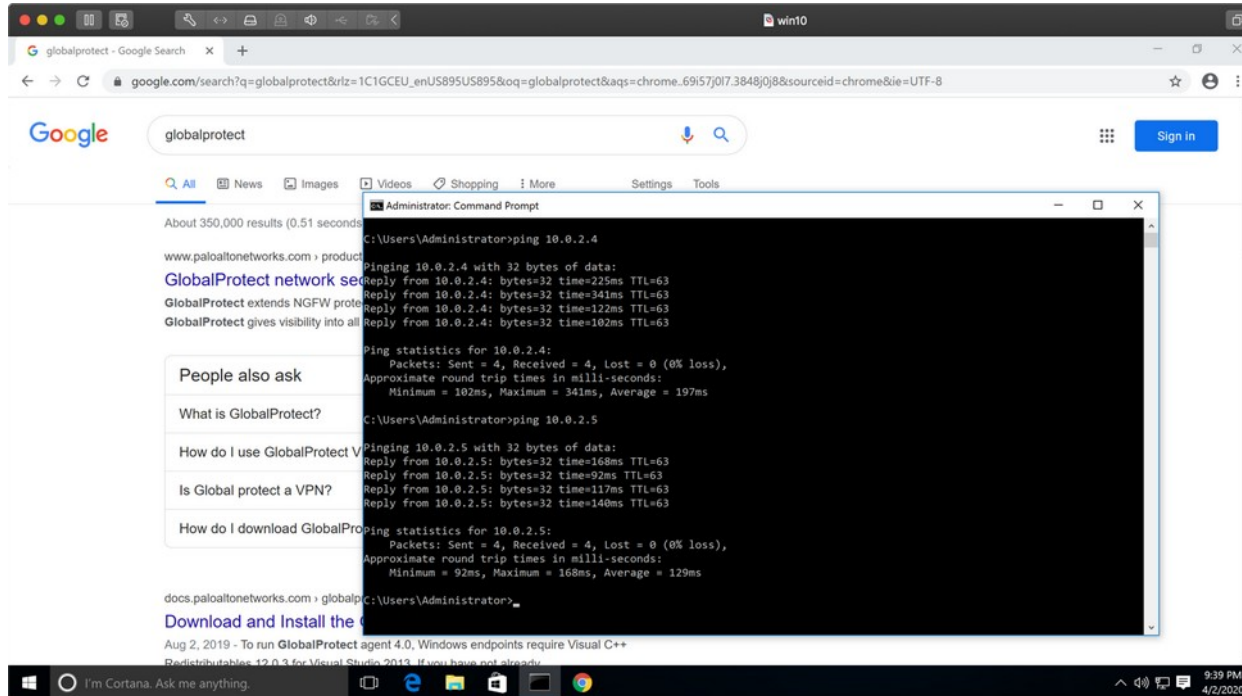
The client will reflect a successful connection.



The client will reflect a successful connection.



The Firewall policy allows internet traffic outbound as well as in to the trusted subnet.





The traffic logs will show the relevant logs in addition to user attribution.

**paloalto** NETWORKS

Dashboard ACC Monitor Policies Objects Network Device

Commit Config Search

10 Seconds Help

[ zone.src eq tunnel-zone ]

Logs

- Traffic
- Threat
- URL Filtering
- WildFire Submissions
- Data Filtering
- HIP Match
- IP-Tag
- User-ID
- Tunnel Inspection
- Configuration
- System
- Alarms
- Authentication
- Unified
- Packet Capture
- App Scope
- Summary
- Change Monitor
- Threat Monitor
- Threat Map
- Network Monitor
- Traffic Map
- Session Browser
- Botnet
- PDF Reports
- Manage PDF Summary
- User Activity Report
- SaaS Application Usage
- Report Groups
- Email Scheduler
- Manage Custom Reports

	Receive Time	Type	From Zone	To Zone	Source	Source User	Destination	To Port	Application	Action	Rule	Session End Reason	Bytes	HTTP/2 Connection Session ID
	04/02 18:40:26	end	tunnel-zone	untrust	192.168.16.10	gp-user1	192.168.10.160	53	dns	allow	allow-out	aged-out	304	0
	04/02 18:40:26	end	tunnel-zone	untrust	192.168.16.10	gp-user1	192.168.10.163	53	dns	allow	allow-out	aged-out	228	0
	04/02 18:40:15	end	tunnel-zone	untrust	192.168.16.10	gp-user1	192.168.10.163	53	dns	allow	allow-out	aged-out	228	0
	04/02 18:40:15	end	tunnel-zone	untrust	192.168.16.10	gp-user1	192.168.10.163	53	dns	allow	allow-out	aged-out	261	0
	04/02 18:40:15	end	tunnel-zone	untrust	192.168.16.10	gp-user1	192.168.10.160	53	dns	allow	allow-out	aged-out	304	0
	04/02 18:40:15	end	tunnel-zone	untrust	192.168.16.10	gp-user1	192.168.10.160	53	dns	allow	allow-out	aged-out	348	0
	04/02 18:40:12	end	tunnel-zone	untrust	192.168.16.10	gp-user1	64.233.177.95	443	google-base	allow	allow-out	tcp-fin	4.7k	0
	04/02 18:40:12	end	tunnel-zone	untrust	192.168.16.10	gp-user1	64.233.177.95	443	google-base	allow	allow-out	tcp-fin	14.1k	0
	04/02 18:40:04	end	tunnel-zone	untrust	192.168.16.10	gp-user1	192.168.10.160	53	dns	allow	allow-out	aged-out	364	0
	04/02 18:40:04	end	tunnel-zone	untrust	192.168.16.10	gp-user1	192.168.10.163	53	dns	allow	allow-out	aged-out	273	0
	04/02 18:39:53	end	tunnel-zone	untrust	192.168.16.10	gp-user1	74.125.21.106	443	unknown-udp	allow	allow-out	aged-out	499.9k	0
	04/02 18:39:52	end	tunnel-zone	untrust	192.168.16.10	gp-user1	192.168.10.160	53	dns	allow	allow-out	aged-out	304	0
	04/02 18:39:52	end	tunnel-zone	untrust	192.168.16.10	gp-user1	192.168.10.163	53	dns	allow	allow-out	aged-out	228	0
	04/02 18:39:49	end	tunnel-zone	trust	192.168.16.10	gp-user1	10.0.2.5	0	ping	allow	allow-in	aged-out	592	0
	04/02 18:39:49	start	tunnel-zone	untrust	192.168.16.10	gp-user1	64.233.177.95	443	google-base	allow	allow-out	n/a	823	0
	04/02 18:39:49	start	tunnel-zone	untrust	192.168.16.10	gp-user1	64.233.177.95	443	ssl	allow	allow-out	n/a	823	0

admin | Logout | Last Login Time: Not available

Displaying logs 1-20 per page DESC