GlobalProtect Configuration

Basic Setup

Backup Configuration (Device-Setup-Operations)

Navigate to Device->Setup->Operations

1. Save named configuration snapshot
    1. candidate config
2. Export Named Configuration
    2. Candidate Config
3. Save this somewhere you can find it. you can import this if a rollback is needed. Alternatively, you can just verify current configuration version
    1. Load Configuration version
    2. Verify Highest number and most recent date.
    3. Roll back to this number after any changes completed.

Zones (Network-Zones)

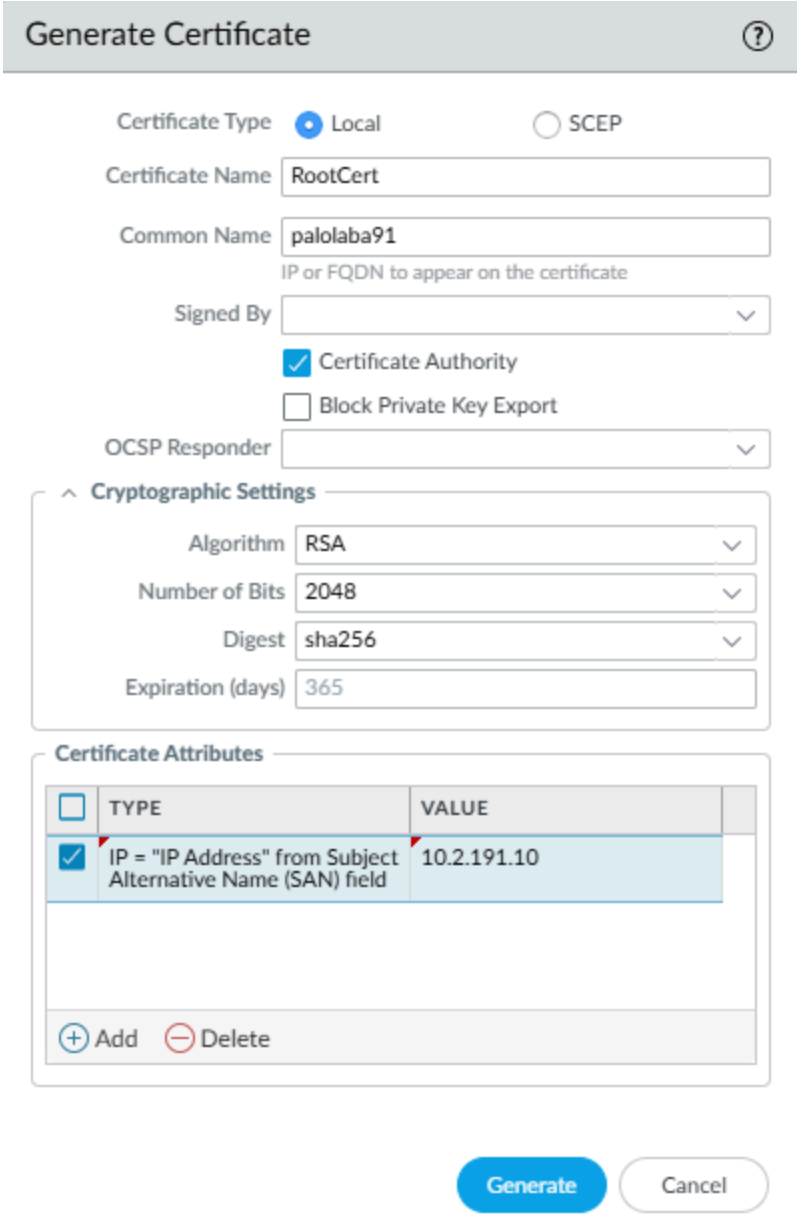
For the most control, we need to configure a zone for our GlobalProtect. This is *optional* however **HIGHLY** recommended.

							User-ID			Device-ID		
	NAME	TYPE	INTERFACES / VIRTUAL SYSTEMS	ZONE PROTECTION PROFILE	PACKET BUFFER PROTECTION	LOG SETTING	ENABLED	INCLUDED NETWORKS	EXCLUDED NETWORKS	ENABLED	INCLUDED NETWORKS	EXCLUDED NETWORKS
	DMZ	layer3	ethernet1/7		✓			any	none		any	none
	GP	layer3	tunnel.1 tunnel.2		✓		✓	any	none		any	none
	inside	layer3	ethernet1/1 ethernet1/2 tunnel		✓		✓	any	none		any	none
	Outside	layer3	ethernet1/3 ethernet1/4		✓		✓	any	none		any	none

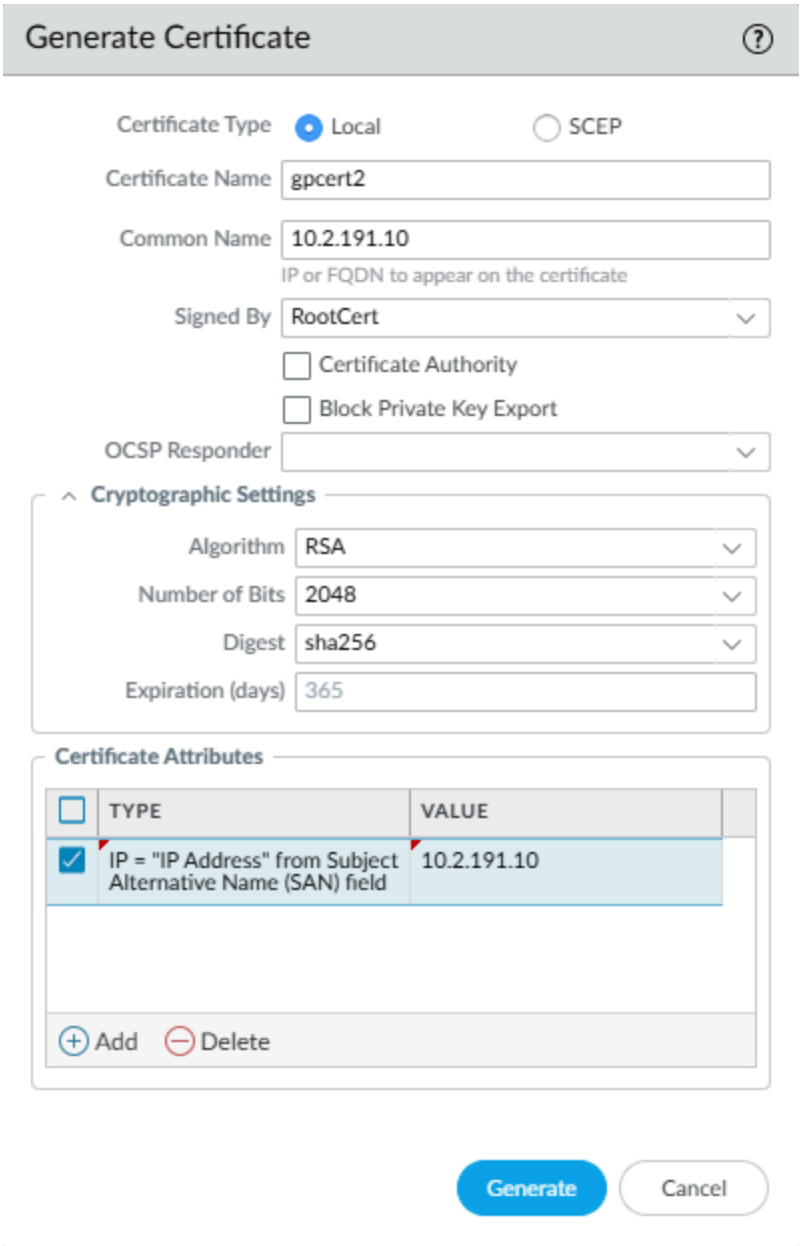
Certificates (Device-Certificate Management-Certificates)

Okay we need to generate two certificates. One is our root cert, and one will be our GlobalProtect Specific.

Root Certification Generation

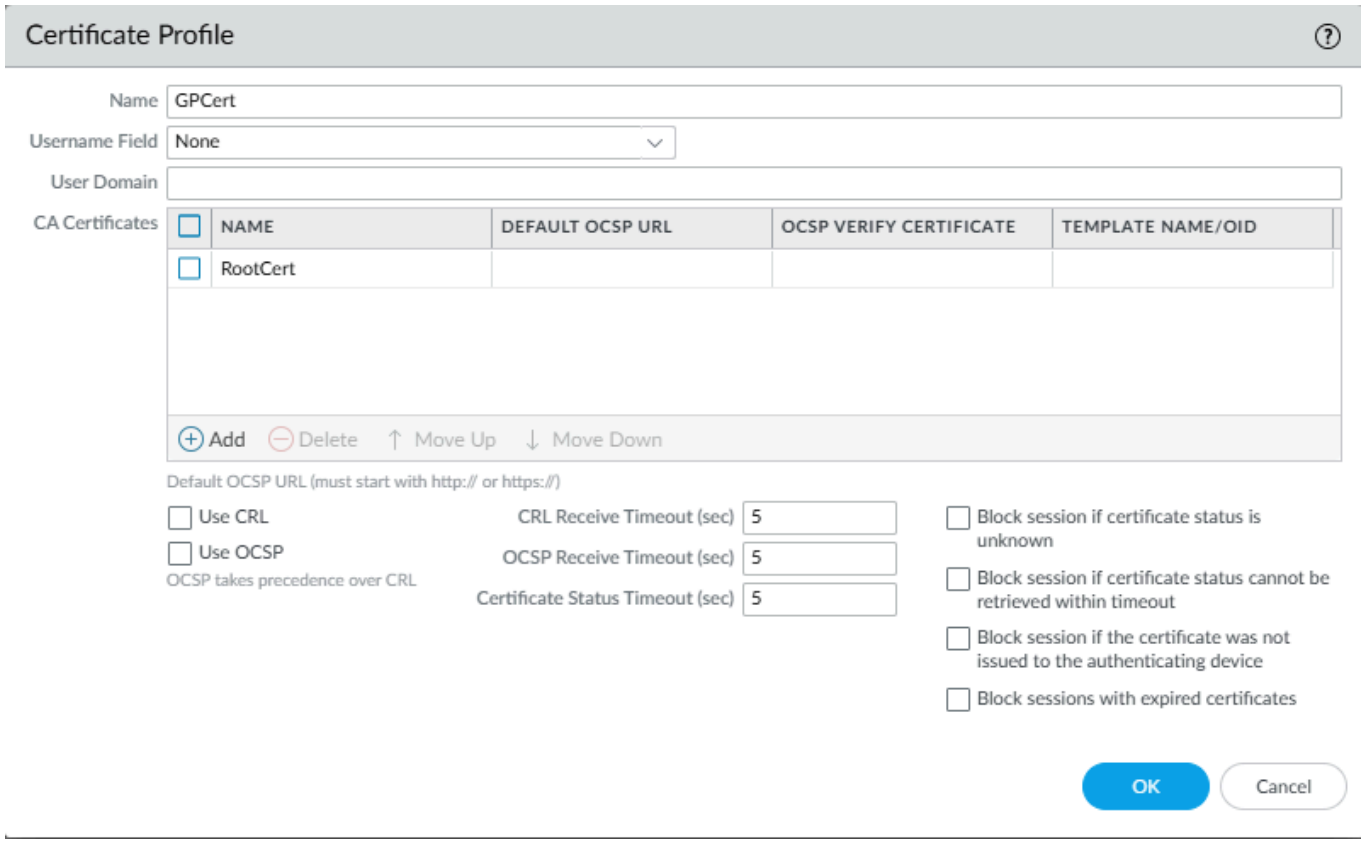


GP (GlobalProtect) Certification Generation



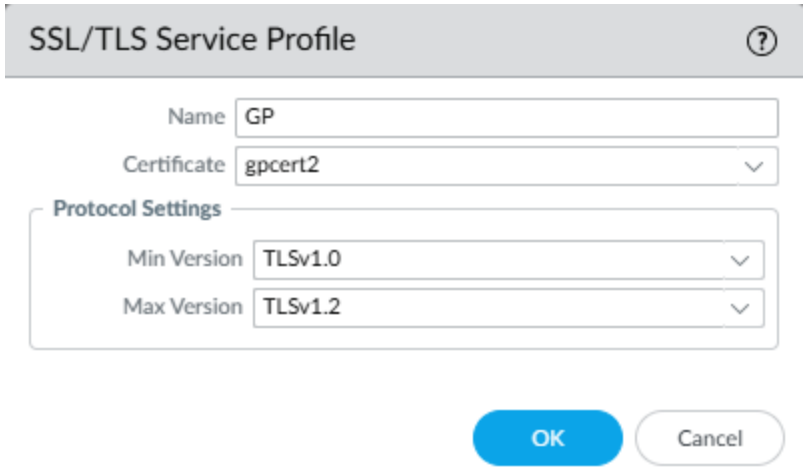
Certificate Profile (Device-Certificate Management-Certificate Profile)

Next up we will create a certificate profile, as shown below. We're referencing our Root Cert, and leaving everything else blank



SSL/TLS Service Profile (Device-Certificate Management-SSL/TLS Service Profile)

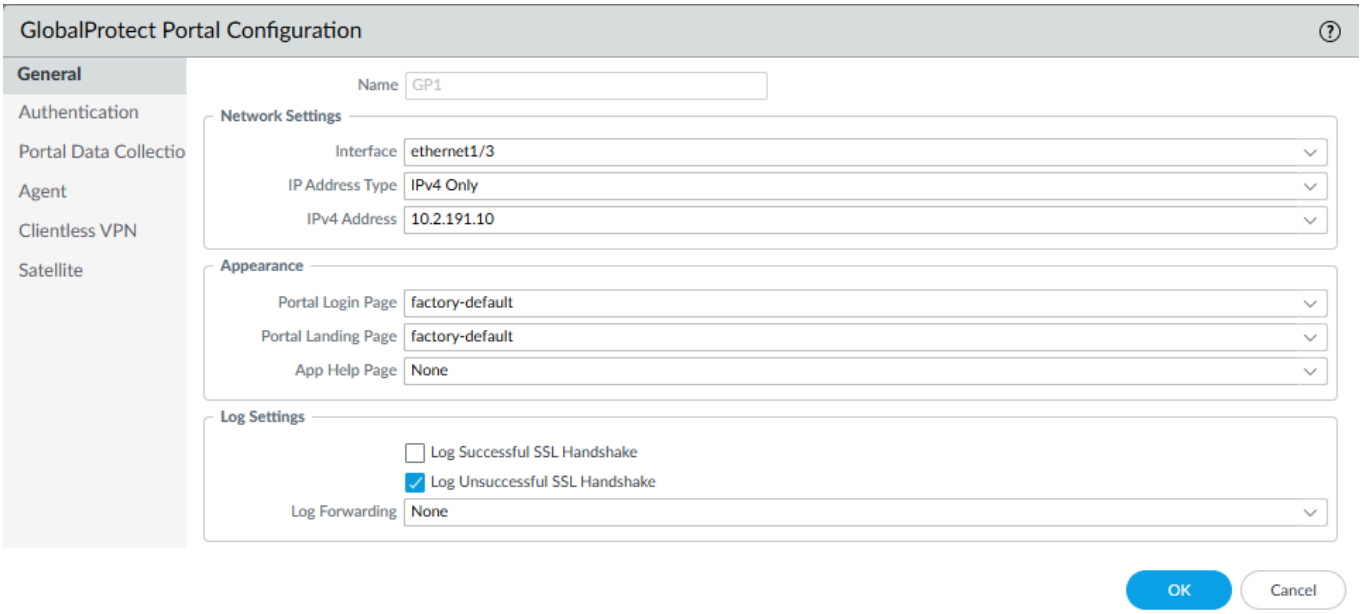
Configure this section as shown in the picture, reference the GPCert. and set the min/max versions.



Portal Configuration

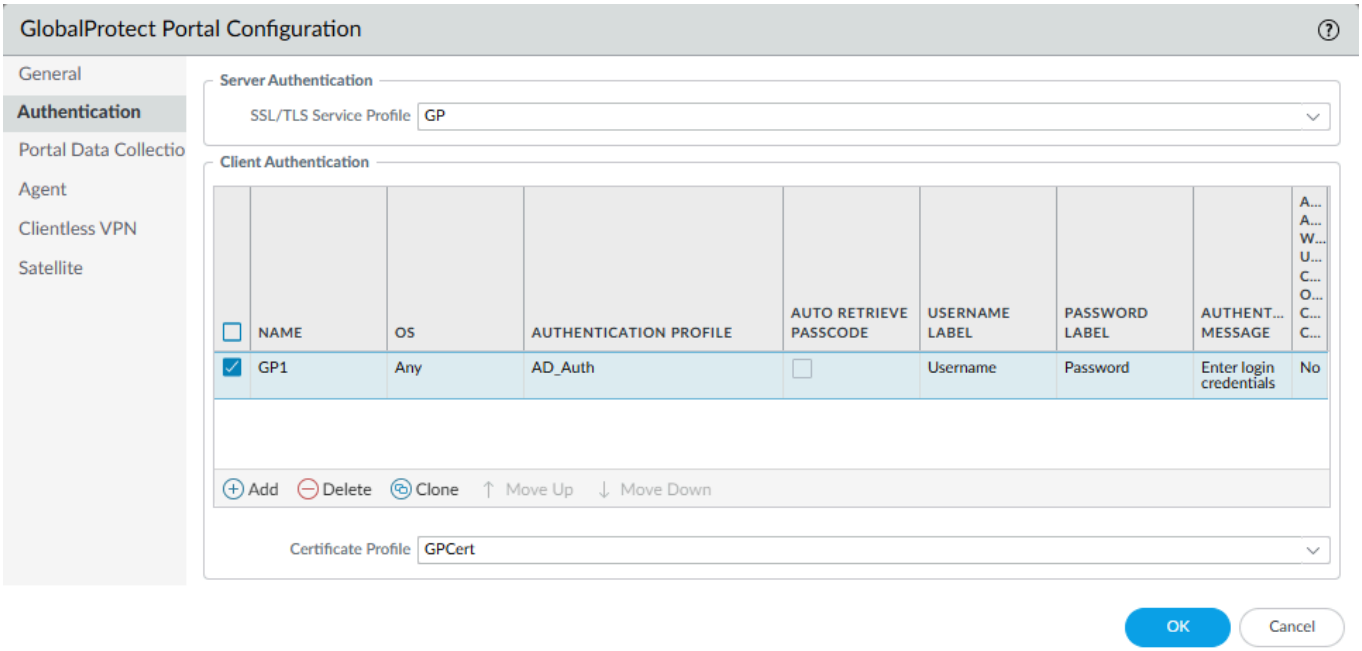
Configure as shown in the pictures below.

General

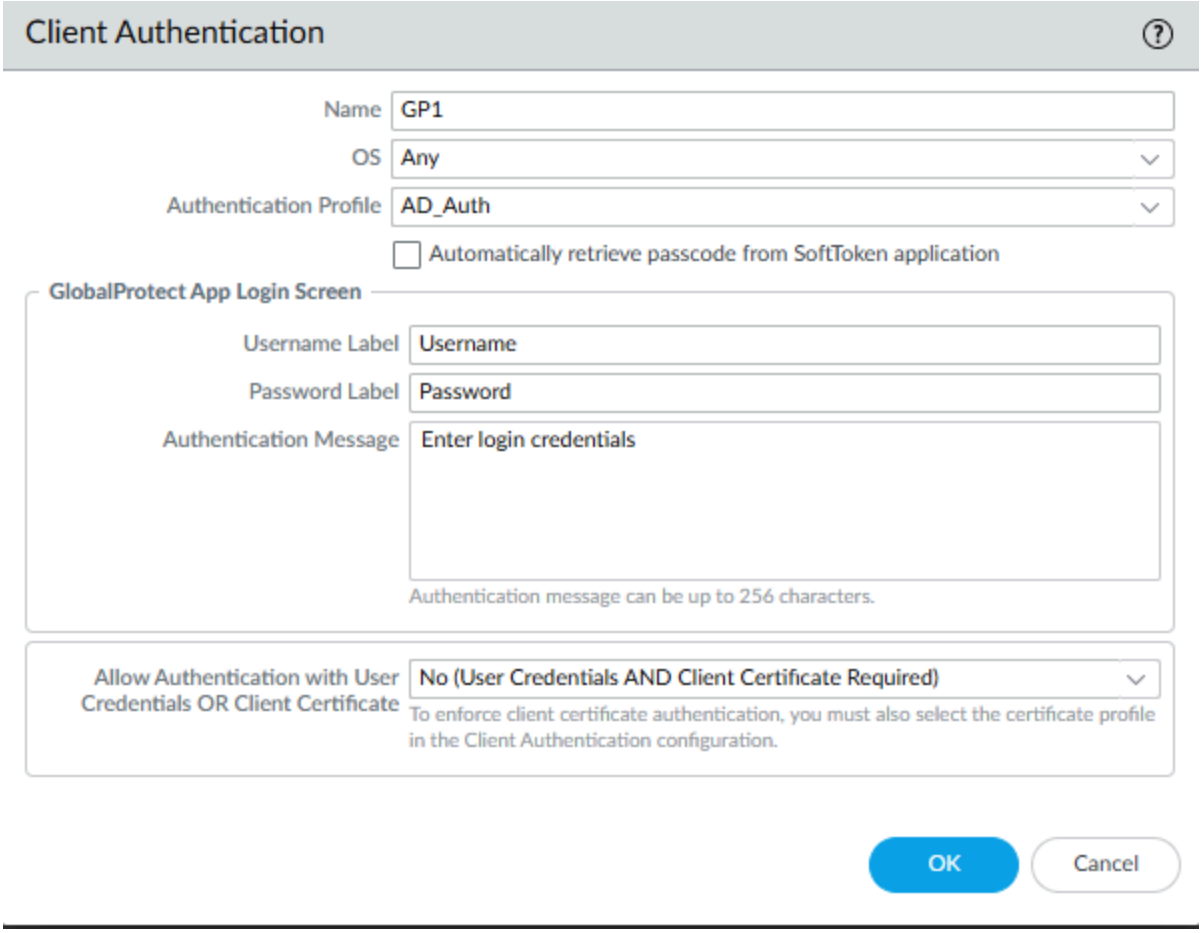


Authentication

Make sure we choose the Service and Certificate profiles then add a client authentication



For this we will reference our authentication profile tied to active directory that was previously made

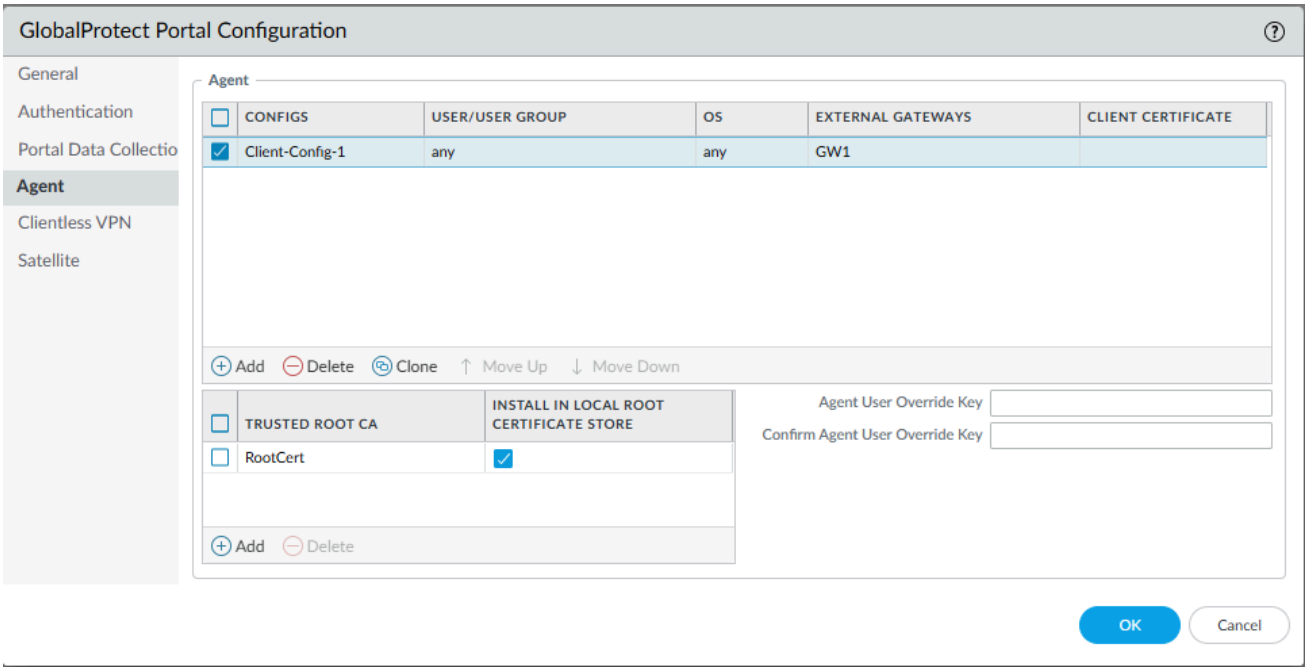


Please note: The bottom box has to be set to YES in order to skip the future "device configuration" section. This will, however, make our network less secure.

Agent

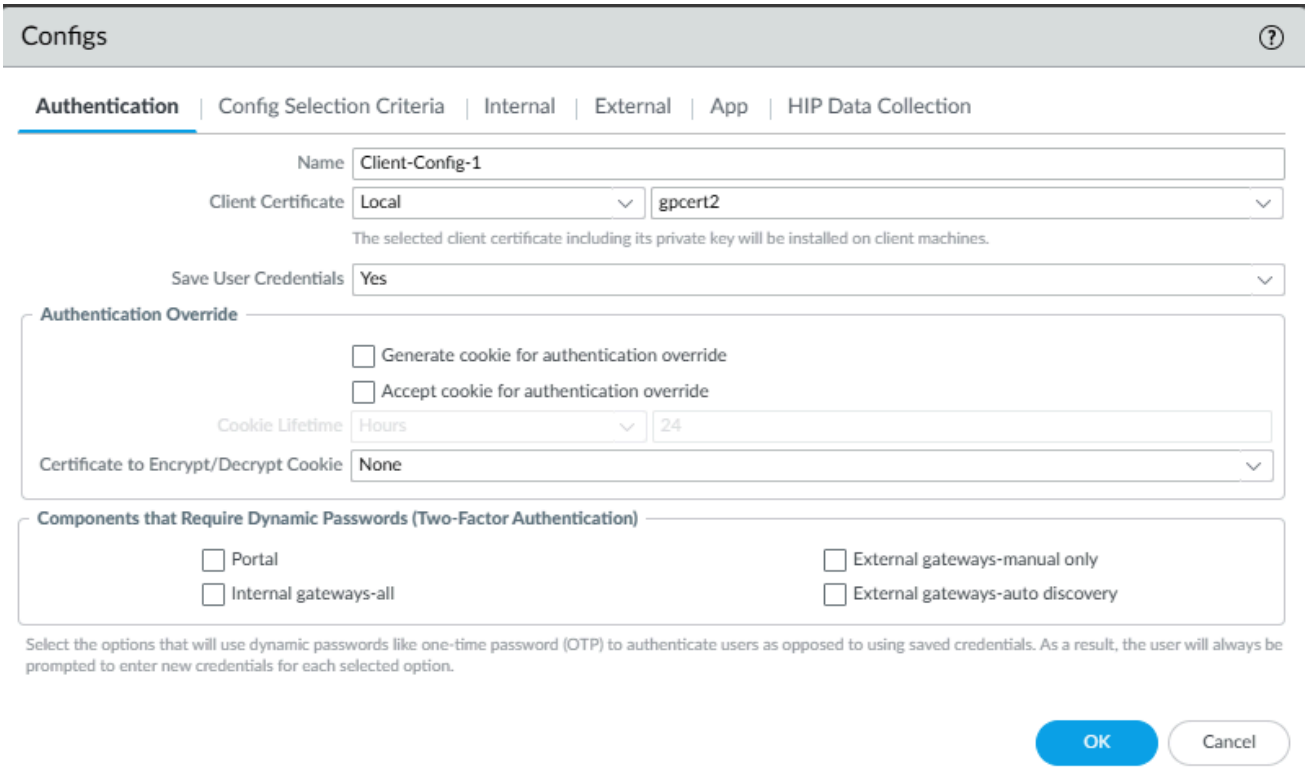
You can Skip the Portal Data Collection tab for now. Here in Agent, we need to do two things:

1. Configure an Agent
2. Add the root and have it install in local root store
   As you can see, you just add the trusted root ca, select RootCert and then check the box

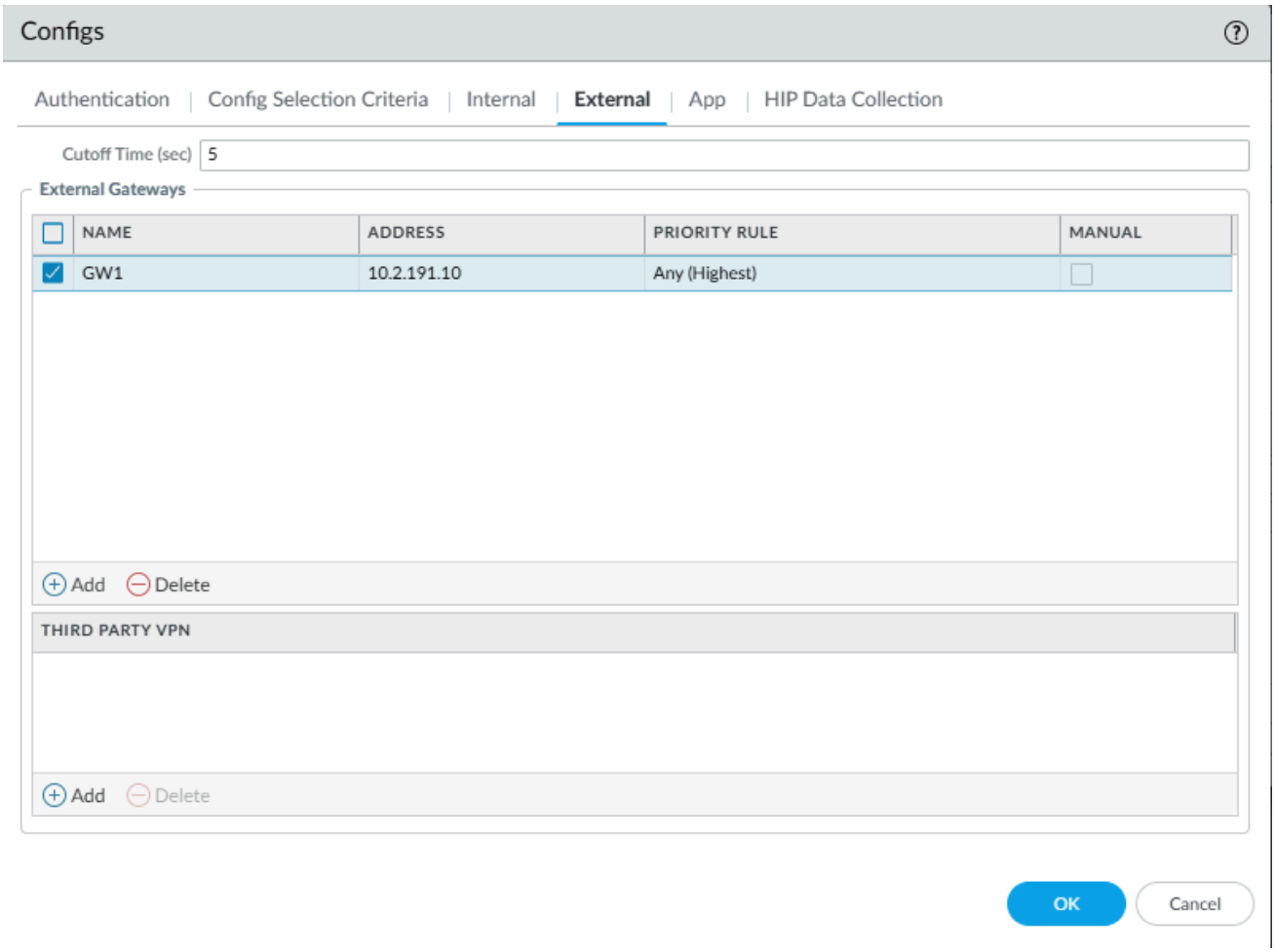


Now for the agent, go ahead and add

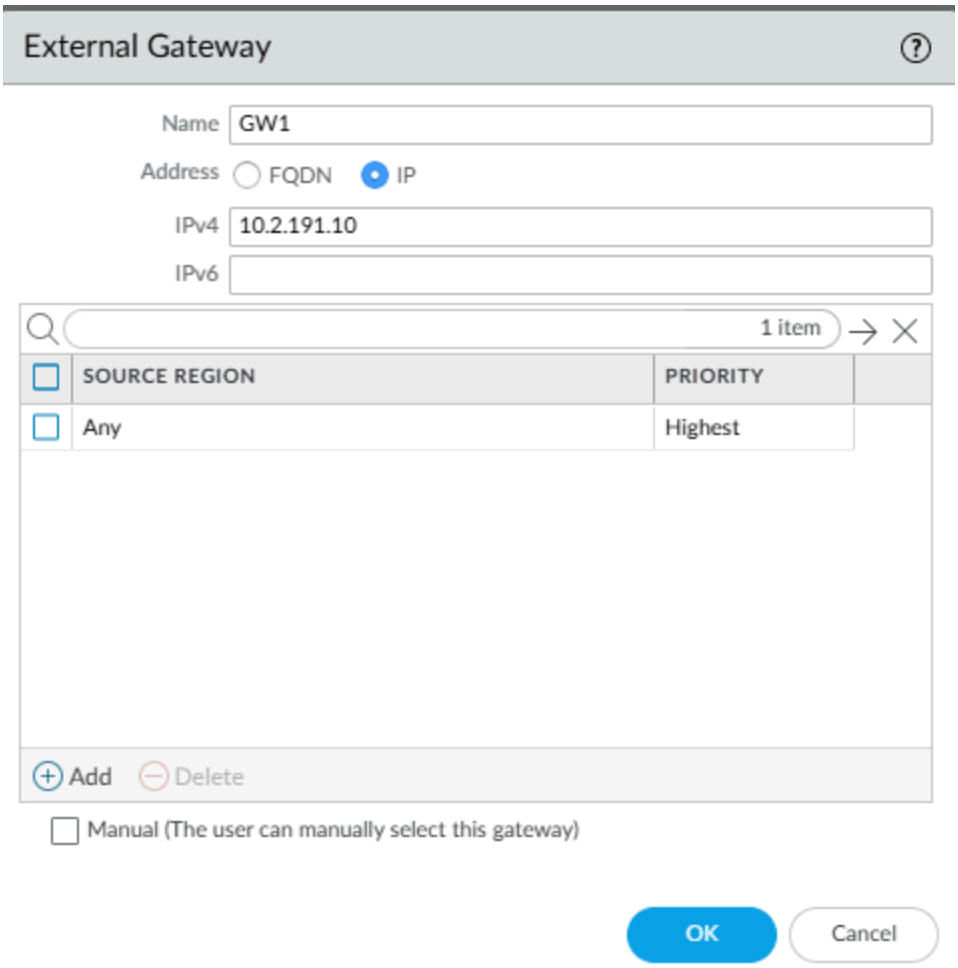
- Name: Arbitrary, I used Client-Config-1
- Client certificate - local - pick your GPCert
- Everything else can be left alone on this tab



Jump to the "External" tabs and add



Here you would put your FQDN or IP, however you want the portal reachable. I used my outside Interfaces IP of 10.2.191.10 with a source region of any.



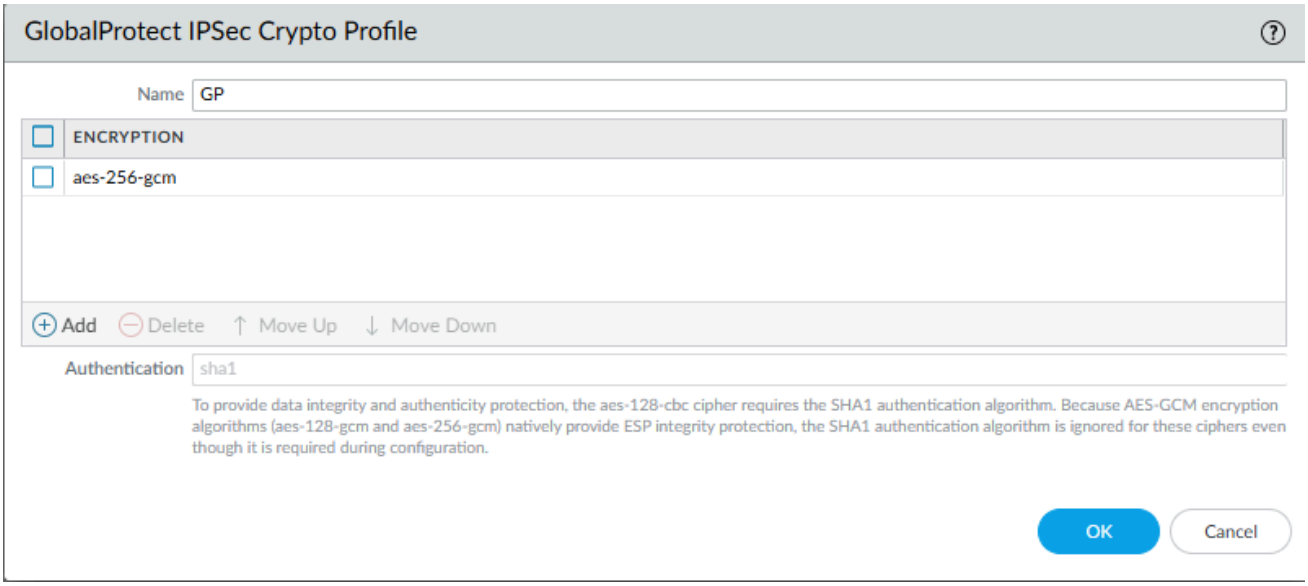
At this point you can go ahead and click okay until you reach the main page and commit. you are done configuring the portal.

Before we get started with the gateway we need to configure a few things.

IPSec Crypto Policy (network-network profiles-GlobalProtect IPSec Crypto)

- Add a new profile
- Select aes-256-gcm as this is the best option

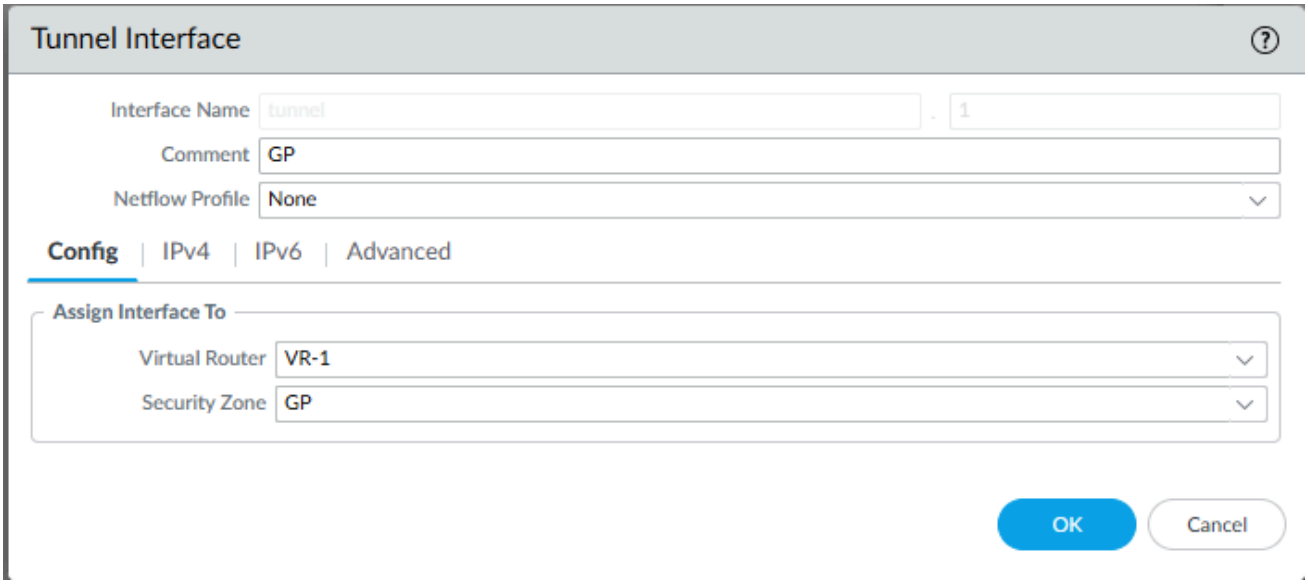
- Name the Profile (I named it GP)



Tunnel interface (Network-Interfaces-Tunnel)

We need to create two tunnel interfaces, one for the GlobalProtect base and one for the satellite. Create and name accordingly

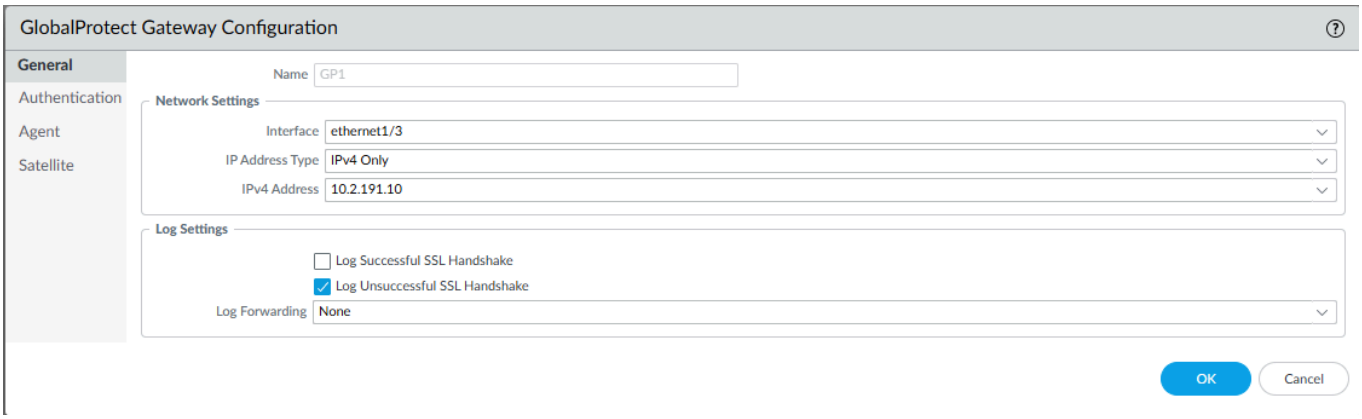
- Assign to VR-1 virtual router
- Place both into the GP security zone



Gateway

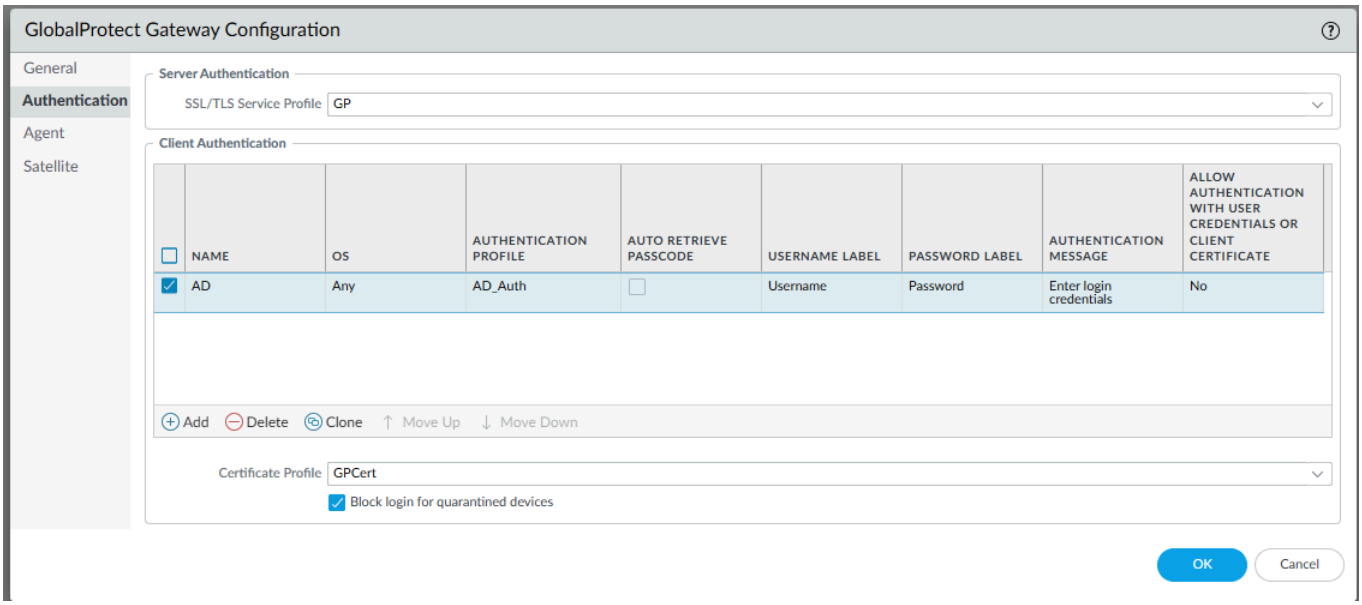
General

We're going to pick our interface, select ipv4 only and then use the IP on this interface, keep everything else the same.



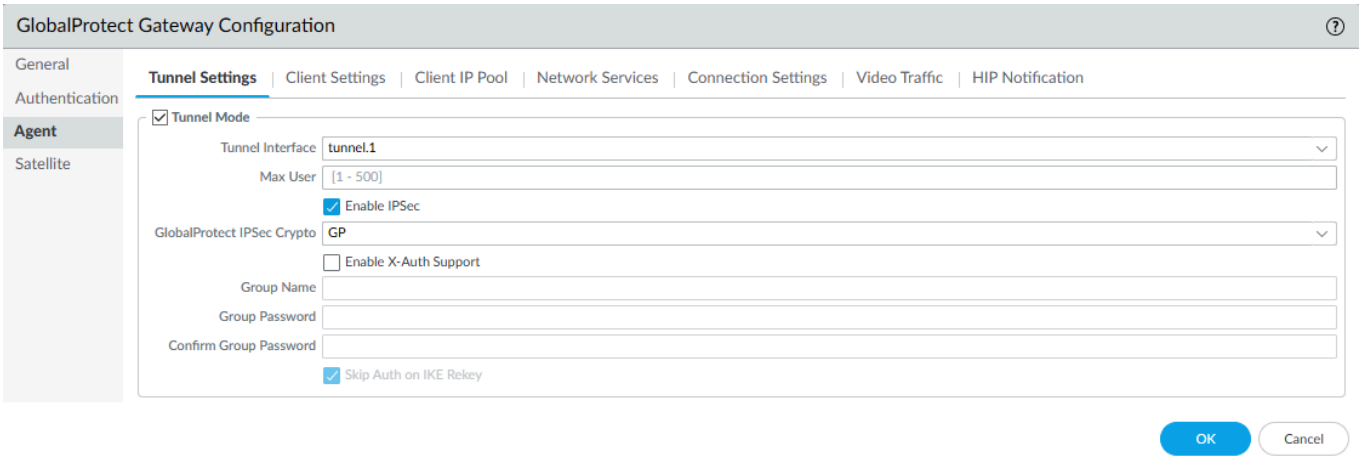
Authentication

We're going to once again select our SSL/TLS Service profile, our standard Certificate profile, and and setup our authentication as was done in the previous step.



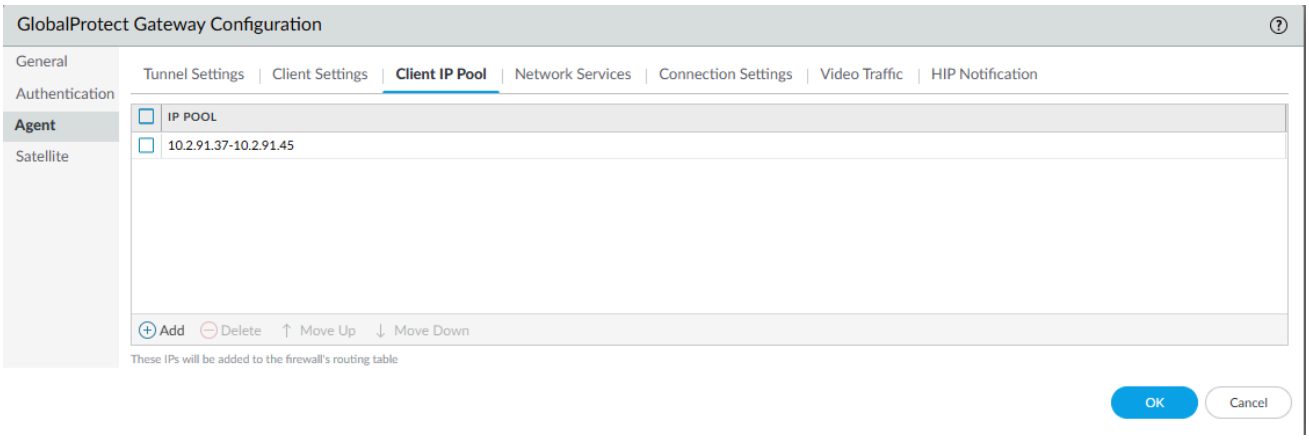
Agent

We're going to go ahead and check "tunnel mode" and choose our tunnel interface 1 (Or whichever one you created for the GlobalProtect base). Make sure we select the IPSec profile we created and enable IPSec is checked. Then move on to "Client IP Pool"

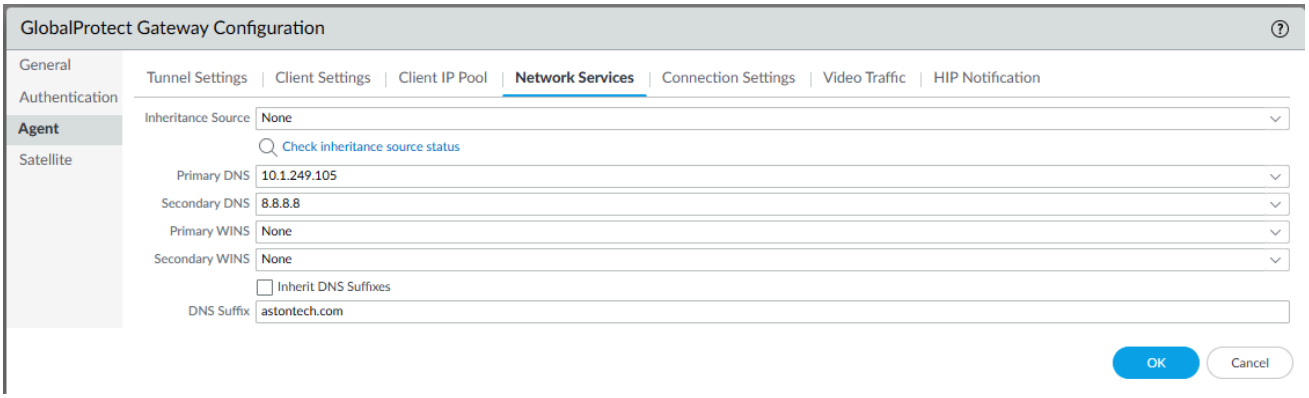


We need to create a pool of IPs for the devices, these will be added to the firewalls routing tables but remember: ***if you place them on their own network any other routers will need to add a static route or learn through dynamic routing!***

- For this example, I used some available IPs in my internal network

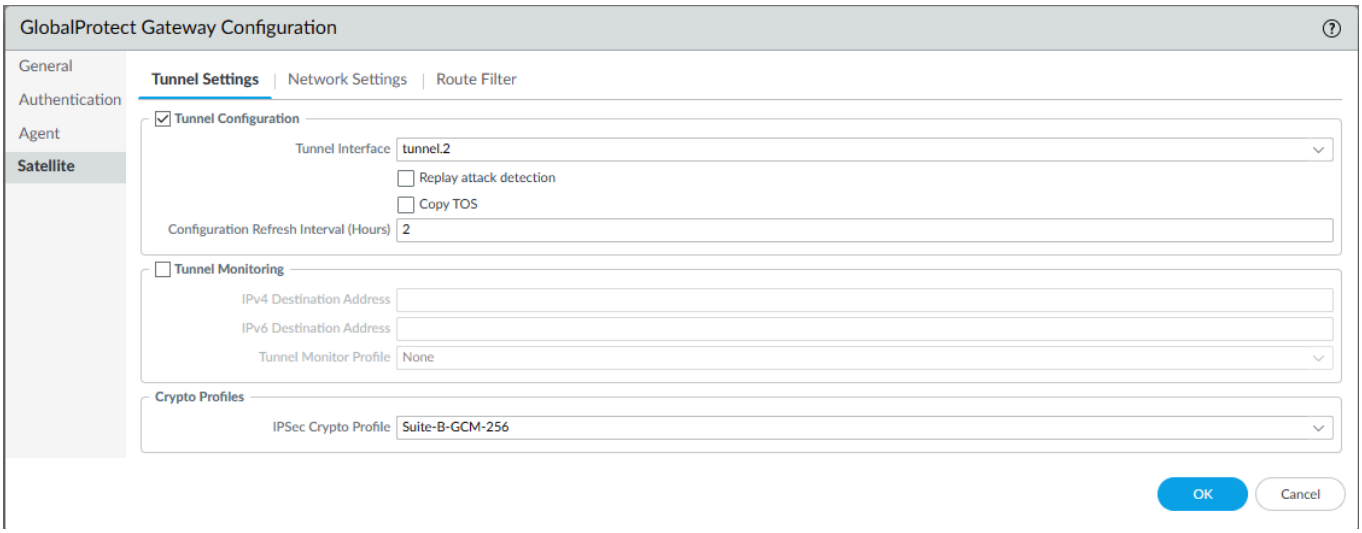


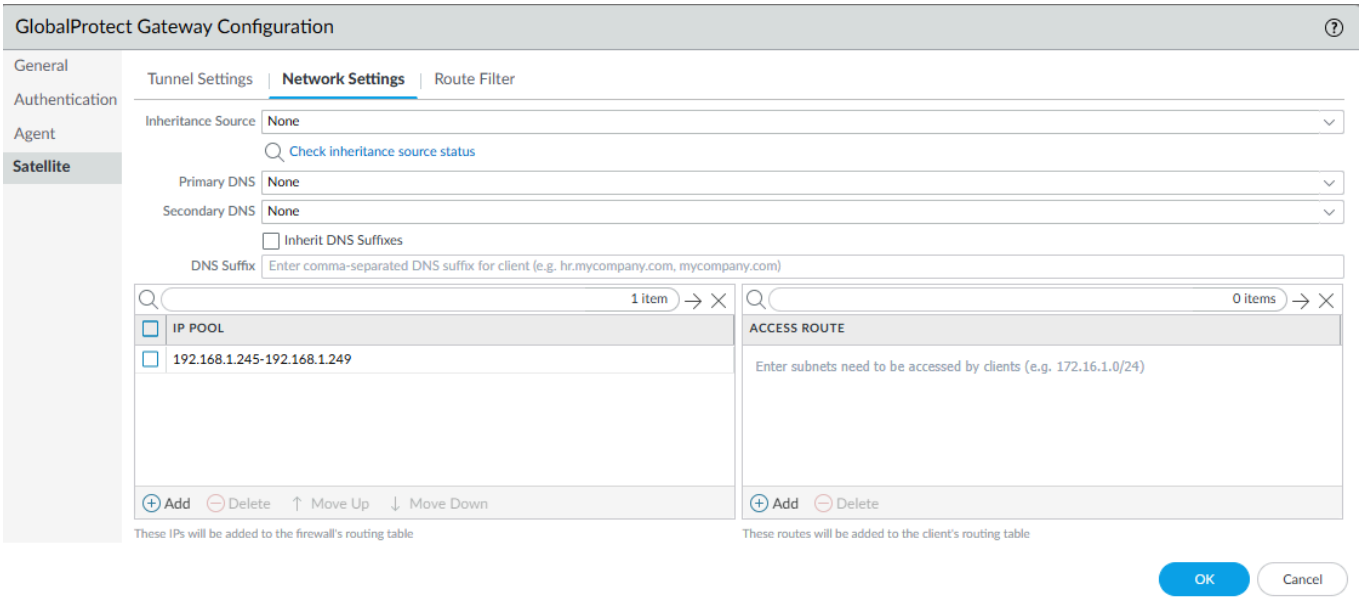
Finally, in the network services tab, add your primary and secondary DNS so your clients can resolve!



Satellite

Although we are not using the satellite functionality at this time, it still is required to setup here. Pick our interface we setup for the satellite (tunnel.2), configure a range of IPs to use, and keep everything else the same for now.





Click OK and commit all changes. You are now ready for the PC side configuration

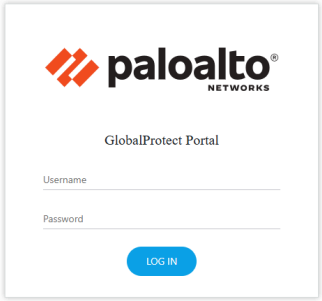
PC configuration

This section isn't needed if deploying GlobalProtect through Group policy

Due to the way we set up this deployment, upon joining the portal your PC will download the certificates once authenticated by user.

1. Navigate to the IP you set for your portal (10.2.191.10)

2. You should see the below screen



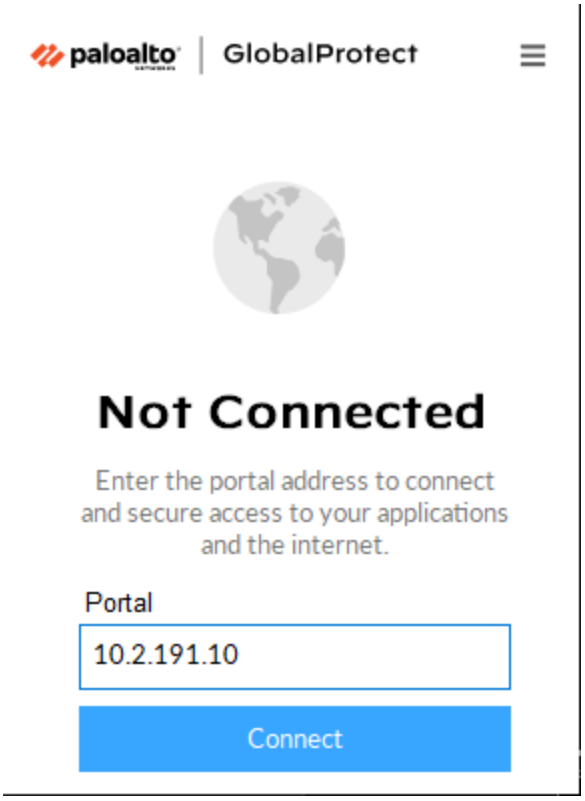
3. Login using your Active Directory Credentials, which will bring you to the below screen

4. Download the corresponding agent to your OS

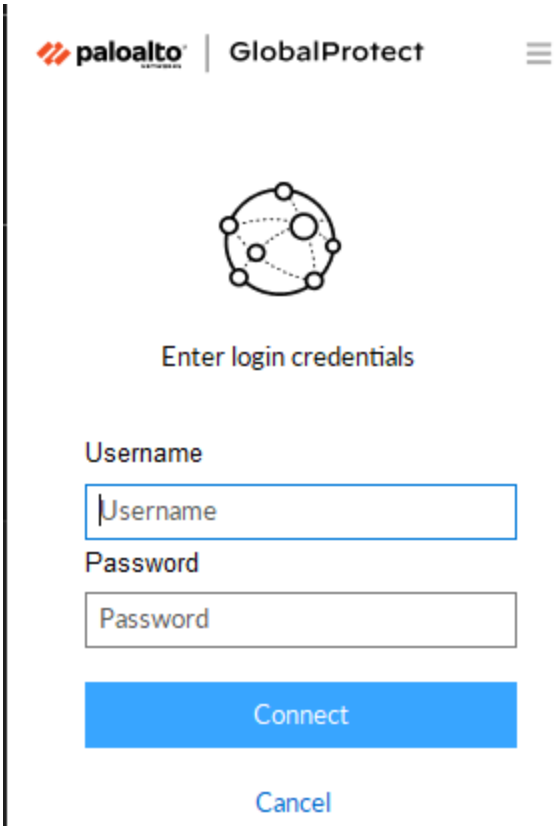
1. You do not have to change anything so just next through the installer and let it install.

5. Click get started

6. Enter Portal address (10.2.191.10) and connect



7. It will ask for your credentials once again, enter them and hit connect.



It will now show you connected to the portal.

Verifications

1. For our first verification we can refer to the above picture. If it shows connected then we are working.

2. We can also look in the logs located at *Monitor-Logs-GlobalProtect*

RECEIVE TIME	PORTAL/GATE...	STATUS	STAGE	EVENT	SOURCE USER	SOURCE REGION	HOST NAME	PUBLIC IPV4	PUBLIC IPV6	HOST ID	AUTH METHOD	ERROR
04/17 08:20:00	GP1	success	host-info	gateway-hip-report	s237.training.ast...	10.0.0.0-10.255.255.255	8FQH7Y2	10.8.128.41	0.0.0.0	b361539b-1785-44fe-a01b-bc892bd56300		
04/17 08:20:00	GP1	success	host-info	gateway-hip-check	s237.training.ast...	10.0.0.0-10.255.255.255	8FQH7Y2	10.8.128.41	0.0.0.0	b361539b-1785-44fe-a01b-bc892bd56300		
04/17 08:20:00	GP1	success	tunnel	gateway-tunnel-latency	s237.training.ast...	10.0.0.0-10.255.255.255	8FQH7Y2	10.8.128.41	0.0.0.0	b361539b-1785-44fe-a01b-bc892bd56300		
04/17 08:19:40	GP1	success	host-info	gateway-hip-report	s237.training.ast...	10.0.0.0-10.255.255.255	8FQH7Y2	10.8.128.41	0.0.0.0	b361539b-1785-44fe-a01b-bc892bd56300		
04/17 08:19:40	GP1	success	host-info	gateway-hip-check	s237.training.ast...	10.0.0.0-10.255.255.255	8FQH7Y2	10.8.128.41	0.0.0.0	b361539b-1785-44fe-a01b-bc892bd56300		
04/17 08:19:40	GP1	success	tunnel	gateway-tunnel-latency	s237.training.ast...	10.0.0.0-10.255.255.255	8FQH7Y2	10.8.128.41	0.0.0.0	b361539b-1785-44fe-a01b-bc892bd56300		
04/17 08:19:40	GP1	success	connected	gateway-connected	s237.training.ast...	10.0.0.0-10.255.255.255	8FQH7Y2	10.8.128.41	0.0.0.0	b361539b-1785-44fe-a01b-bc892bd56300	ldap	
04/17 08:19:40	GP1	success	tunnel	gateway-setup-ipsec	s237.training.ast...	10.0.0.0-10.255.255.255	8FQH7Y2	10.8.128.41	0.0.0.0	b361539b-1785-44fe-a01b-bc892bd56300		
04/17 08:19:40	GP1	success	agent-msg	gateway-agent-msg	s237.training.ast...	10.0.0.0-10.255.255.255		10.8.128.41	0.0.0.0			
04/17 08:19:35	GP1	success	configuration	gateway-getconfig	s237.training.ast...	10.0.0.0-10.255.255.255	8FQH7Y2	10.8.128.41	0.0.0.0	b361539b-1785-44fe-a01b-bc892bd56300		
04/17 08:19:34	GP1	success	login	gateway-register	s237.training.ast...	10.0.0.0-10.255.255.255	8FQH7Y2	10.8.128.41	0.0.0.0	b361539b-1785-44fe-a01b-bc892bd56300		
04/17 08:19:34	GP1	success	login	gateway-auth	calehamm	10.0.0.0-10.255.255.255	8FQH7Y2	10.8.128.41	0.0.0.0	b361539b-1785-44fe-a01b-bc892bd56300	ldap	
04/17 08:19:34	GP1	success	before-login	gateway-prelogin		10.0.0.0-10.255.255.255		10.8.128.41	0.0.0.0	b361539b-1785-44fe-a01b-bc892bd56300	Certificate	
04/17 08:19:33	GP1	success	configuration	portal-getconfig	s237.training.ast...	10.0.0.0-10.255.255.255	8FQH7Y2	10.8.128.41	0.0.0.0	b361539b-1785-44fe-a01b-bc892bd56300	ldap	
04/17 08:19:33	GP1	success	login	portal-auth	calehamm	10.0.0.0-10.255.255.255	8FQH7Y2	10.8.128.41	0.0.0.0	b361539b-1785-44fe-a01b-bc892bd56300	ldap	
04/17 08:19:32	GP1	success	before-login	portal-prelogin		10.0.0.0-10.255.255.255		10.8.128.41	0.0.0.0	b361539b-1785-44fe-a01b-bc892bd56300	Certificate	
04/17 08:18:52	GP1	success	before-login	portal-prelogin		10.0.0.0-10.255.255.255		10.8.128.41	0.0.0.0	b361539b-1785-44fe-a01b-bc892bd56300	Certificate	

We're looking specifically for the log showing "calehamm" (or your user) and "gateway auth" showing successful

3. Finally we can navigate to *ACC-Network Activity*
    1. This will show us the traffic being sent over our user.