Basic GlobalProtect Configuration

Version 1.1

Agenda

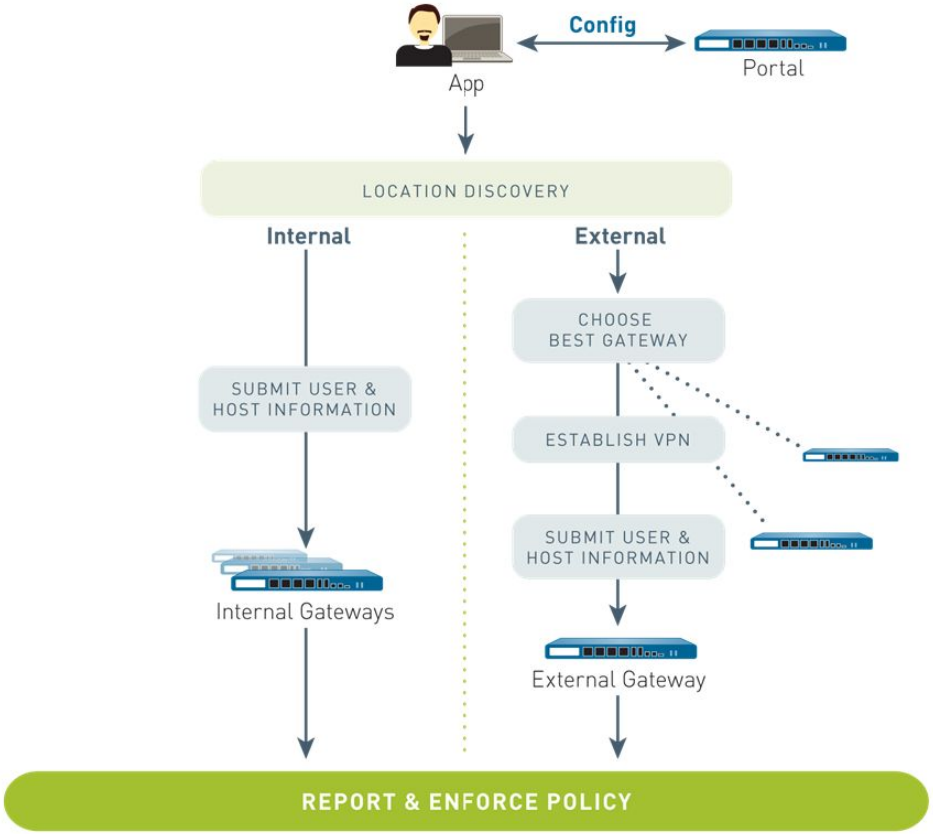
- GlobalProtect Components
- GlobalProtect License
- Interfaces, Zones, and Policies
- SSL Certificates
- User Authentication
- Gateway Configuration
- Portal Configuration
- GlobalProtect Clients
- Troubleshooting
- Resources
- Questions?

GlobalProtect Components

GlobalProtect Components

- GlobalProtect Portal
  - The GlobalProtect portal provides the management functions for your GlobalProtect infrastructure. Every endpoint that participates in the GlobalProtect network receives configuration information from the portal, including information about available gateways as well as any client certificates that may be required to connect to the GlobalProtect gateway. In addition, the portal controls the behavior and distribution of the GlobalProtect app software to both macOS and Windows endpoints. On mobile endpoints, the GlobalProtect app is distributed through the endpoint app store. If you're using the Host Information Profile (HIP) feature, the portal also defines what information to collect from the host, including any custom information you require.
- GlobalProtect Gateway
  - GlobalProtect gateways provide security enforcement for traffic from GlobalProtect apps. Additionally, if the HIP feature is enabled, the gateway generates a HIP report from the raw host data the apps submit and can use this information in policy enforcement. You can configure different Types of Gateways to provide security enforcement and virtual private network (VPN) access for your remote users, or to apply security policy for access to internal resources.
- GlobalProtect Client Application
  - The GlobalProtect app software runs on endpoints and enables access to your network resources through the GlobalProtect portals and gateways that you have deployed.

GlobalProtect Components



GlobalProtect License

GlobalProtect License

- Palo Alto default GlobalProtect
  - Support for Windows and macOS clients
  - Single or multiple internal gateways
  - Single or multiple external gateways
  - IPv6 for internal gateways
- GlobalProtect Gateway License
  - Support for Linux clients
  - Support for mobile device clients (iOS and Android)
  - HIP Checks
  - Clientless VPN
  - IoT Devices
  - IPv6 for external gateways
  - Split tunneling based on destination domain, client process, and video streaming application
  - Split DNS
  - Add a compromised device to a quarantine list

GlobalProtect -> Prisma Access Agent

GlobalProtect Gateway License is now Prisma Access Agent License PAA Docs

What does this mean:

- PAA license still supports all GP features and the GP client.
- GP client is not going away, only the license has changed names.
- GP license is not interchangeable with PAA license (necessary for HA configuration)
- New deployments will see the PAA License
- Will see current GP licenses change names in 1H26

Prisma Access Agent Features

- Anti-tampering: to prevent all users including admin privileged users from tampering the agent & bypassing security controls
- Endpoint Insights: to fast track resolution of endpoint related issues with remote shell & automatic log collection
- In-Product upgrades: with ability to do modular upgrades & rollback, streamlining the upgrade experience
- Complete always-on enforcement: by using an Embedded browser for completing the captive portal auth & avoid opening the network access for all apps
- Endpoint DLP: with peripheral controls & stop data loss at endpoint

At the time of GA (4/15/25), PA Agent does not have support for IPv6, Linux, FIPS/CC & FedRAMP certifications.

Interfaces, Zones, and Policies

Interfaces, Zones, and Policies

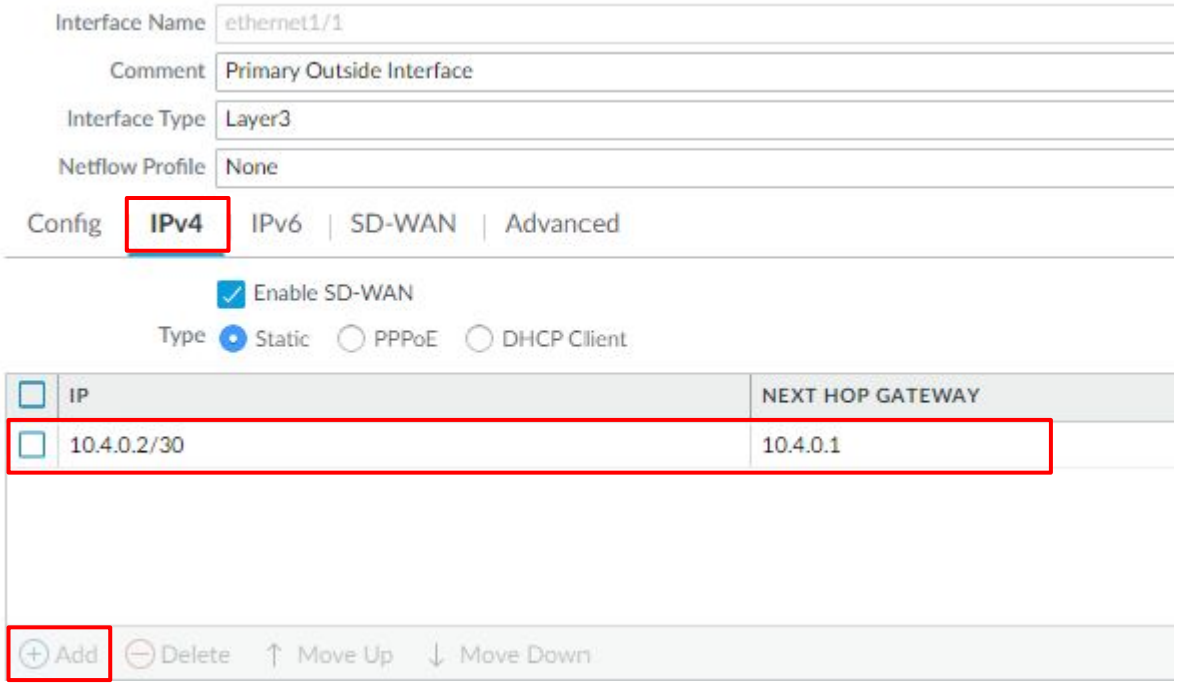
- GlobalProtect portal
  - Requires a Layer 3 or loopback interface for the GlobalProtect apps' connection. If the portal and gateway are on the same firewall, they can use the same interface. The portal must be in a zone that is accessible from outside your network, such as a DMZ.
- GlobalProtect gateways
  - External gateways requires a Layer 3 or loopback interface and a logical tunnel interface for the app to establish a connection. The Layer 3/loopback interface must be in an external zone, such as a DMZ. A tunnel interface can be in the same zone as the interface connecting to your internal resources (for example, trust). **For added security and better visibility, you can create a separate zone, such as corp-vpn**. If you create a separate zone for your tunnel interface, you must create security policies that enable traffic to flow between the VPN zone and the trust zone.
  - Internal gateways requires a Layer 3 or loopback interface in your trust zone. You can also create a tunnel interface for access to your internal gateways, but this isn't required.
- If the gateway and portal are on the same firewall, you can use a single interface for both. Best practice is to use a static IP address on the interface.

Interfaces

Network -> Interfaces -> Ethernet

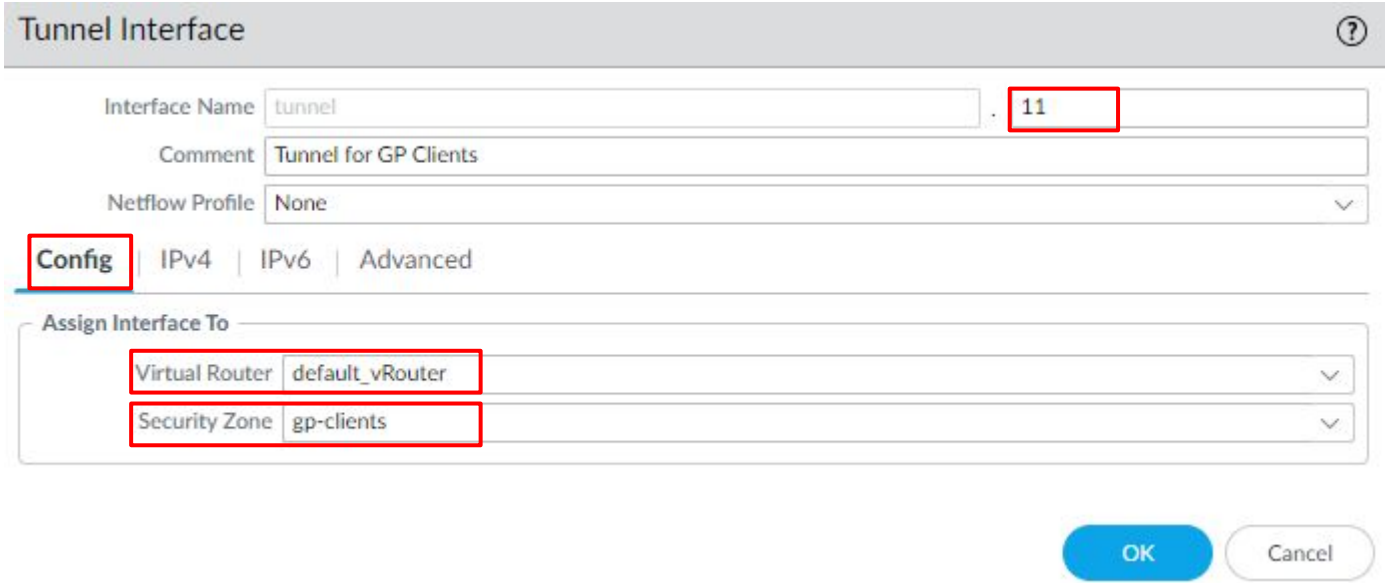
Interfaces

Interface (Cont.)



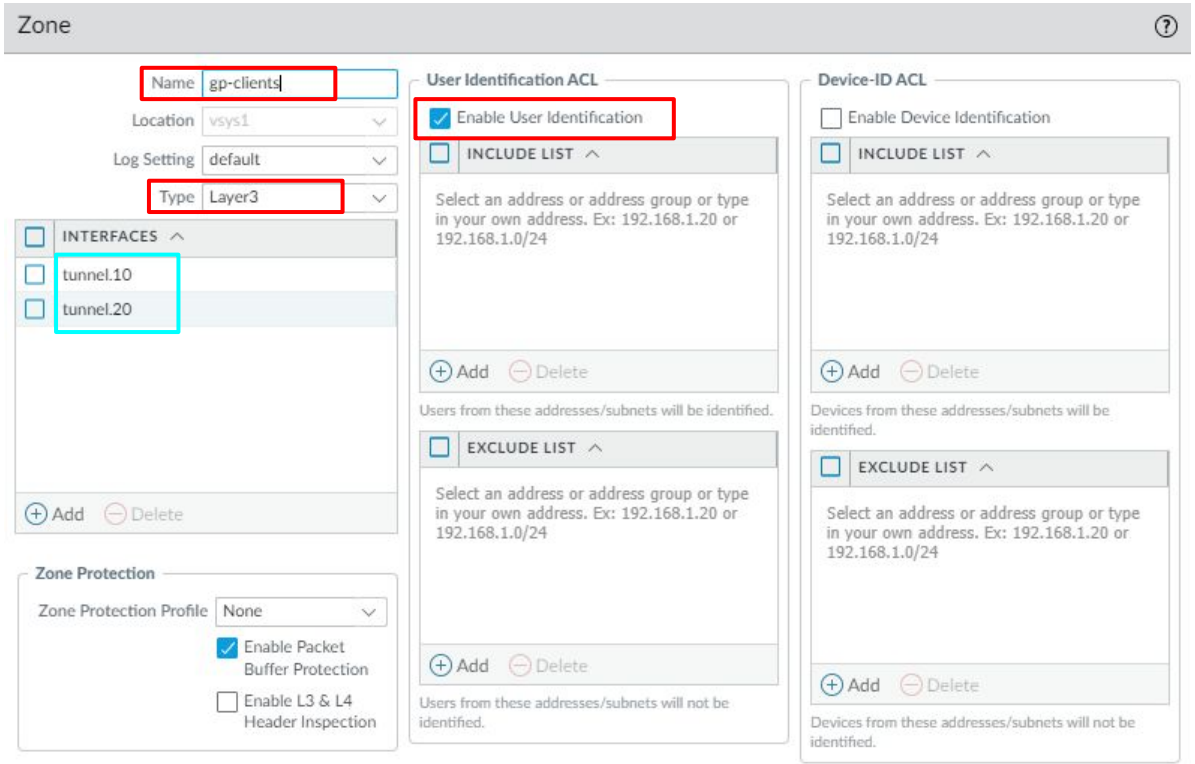
Interfaces

Network -> Interfaces ->Tunnel



Zones

Network -> Zones



Policies

Policies -> Security

Traffic between zones must be explicitly allowed by policy.

NAME	LOCATION	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION	PROFILE
GP-to-Inside-Traffic	SD-WAN_Hub	gp-clients	universal	gp-clients	GP-Clients	any	any	inside	Jackson-LAN	any	any	application-...	Allow	

GP-Clients Zone -> Inside Zone

SSL Certificate

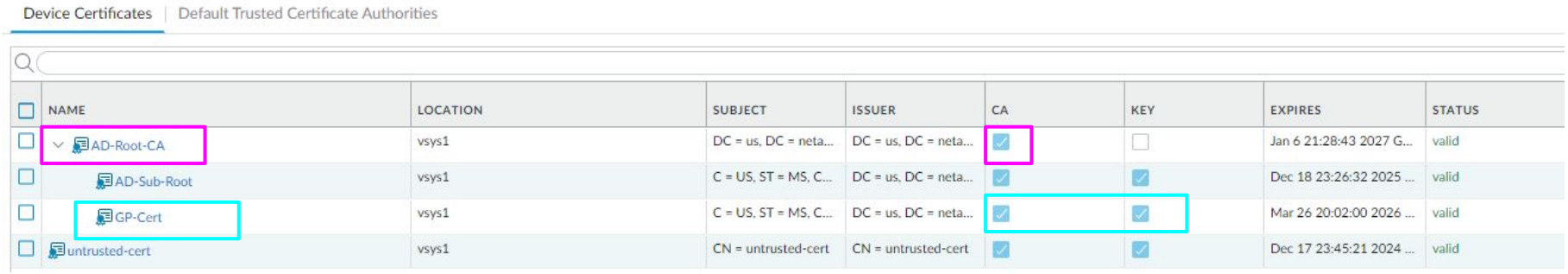
SSL Certificate

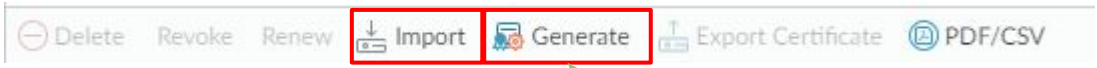
- All interaction between the GlobalProtect components occurs over an SSL/TLS connection. Therefore, you must generate and install the required certificates before configuring each component so that you can reference the appropriate certificate in the configurations.

- There are three basic approaches to Deploy Server Certificates to the GlobalProtect Components:
  - (Recommended) Combination of third-party certificates and self-signed certificates—Because the GlobalProtect app will be accessing the portal prior to GlobalProtect configuration, the app must trust the certificate to establish an HTTPS connection.
  - Enterprise CA—If you already have your own enterprise CA, you can use this internal CA to issue certificates for each of the GlobalProtect components and then import them onto the firewalls hosting your portal and gateway. In this case, you must also ensure that the endpoints trust the root CA certificate used to issue the certificates for the GlobalProtect services to which they must connect.
  - Self-Signed Certificates—You can generate a self-signed CA certificate on the portal and use it to issue certificates for all the GlobalProtect components. However, this solution is not recommended since it's less secure than the other options. If you do choose this option, end users will see a certificate error the first time they connect to the portal. To prevent this, you can deploy the self-signed root CA certificate to all endpoints manually or using some sort of centralized deployment, such as an Active Directory Group Policy Object (GPO).

SSL Certificates

Device -> Certificate Management -> Certificates





Create CSR

SSL Certificates

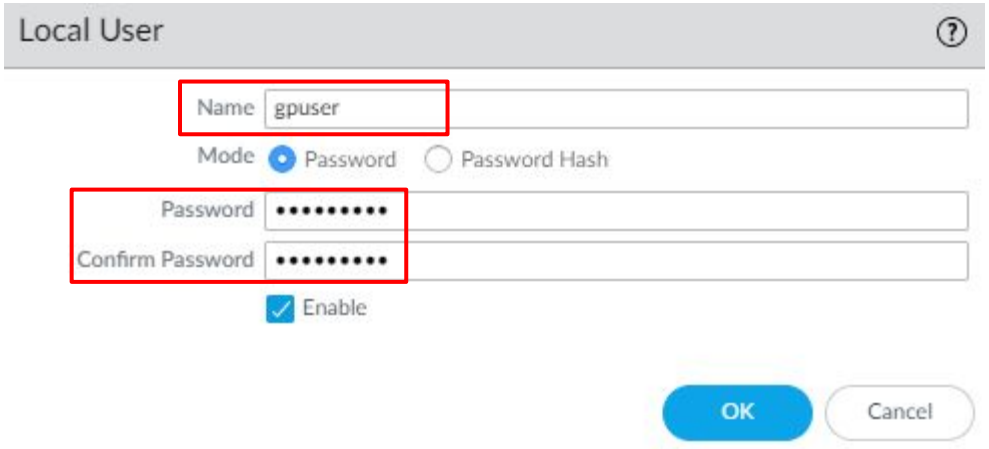
Device -> Certificate Management -> SSL/TLS Service Profile

User Authentication

User Authentication

- Local Authentication - Users are in the FW local database
- External Authentication - LDAP, SAML, Kerberos, Radius, or TACACS+,
- Client Certificate
- Two-Factor Authentication

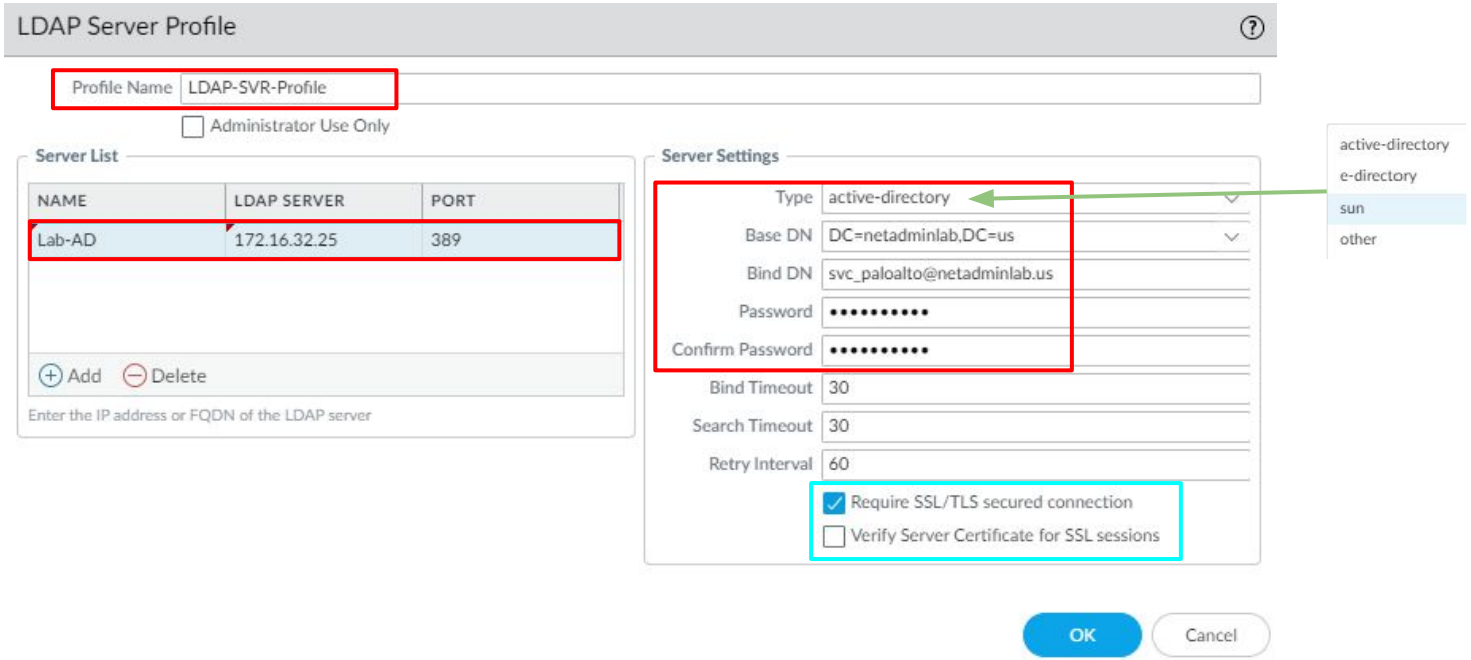
- Local Users: Device -> Local User Database -> Users



User Authentication

External User: LDAP

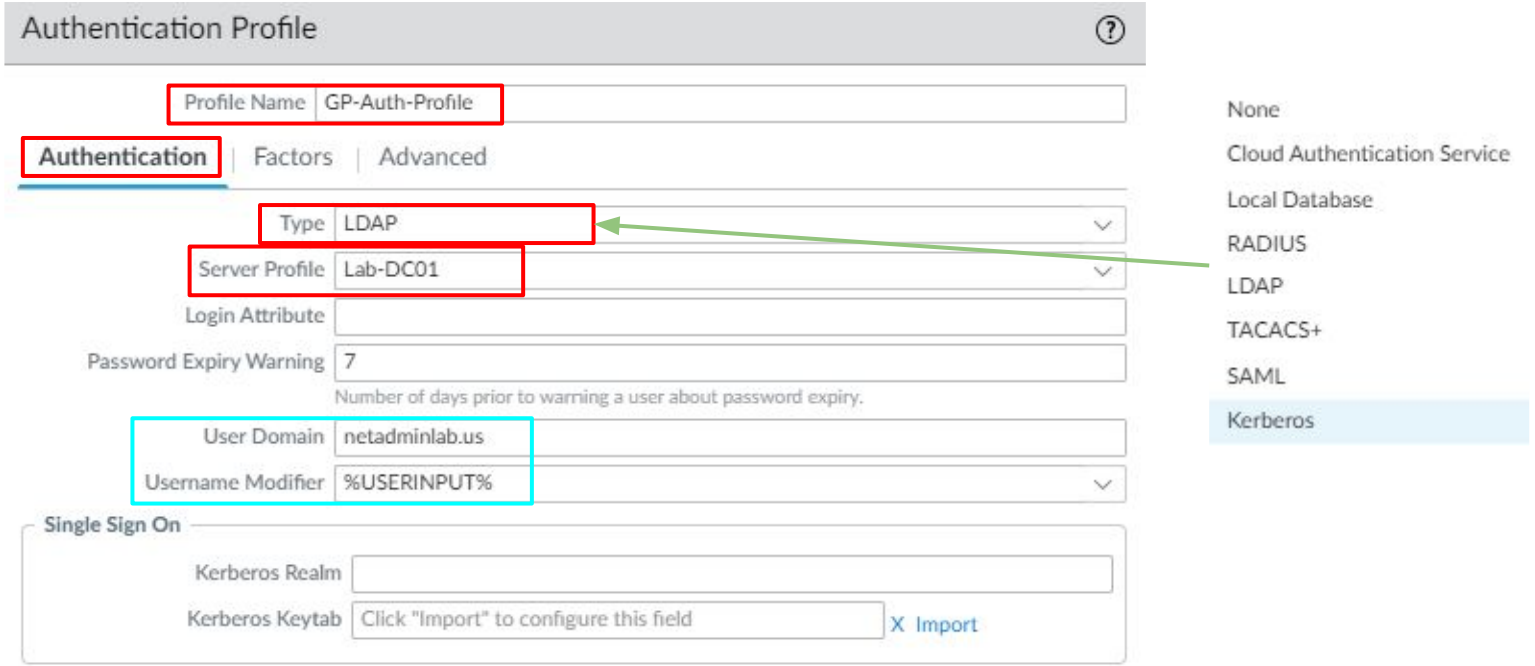
Device -> Server Profile -> LDAP



User Authentication

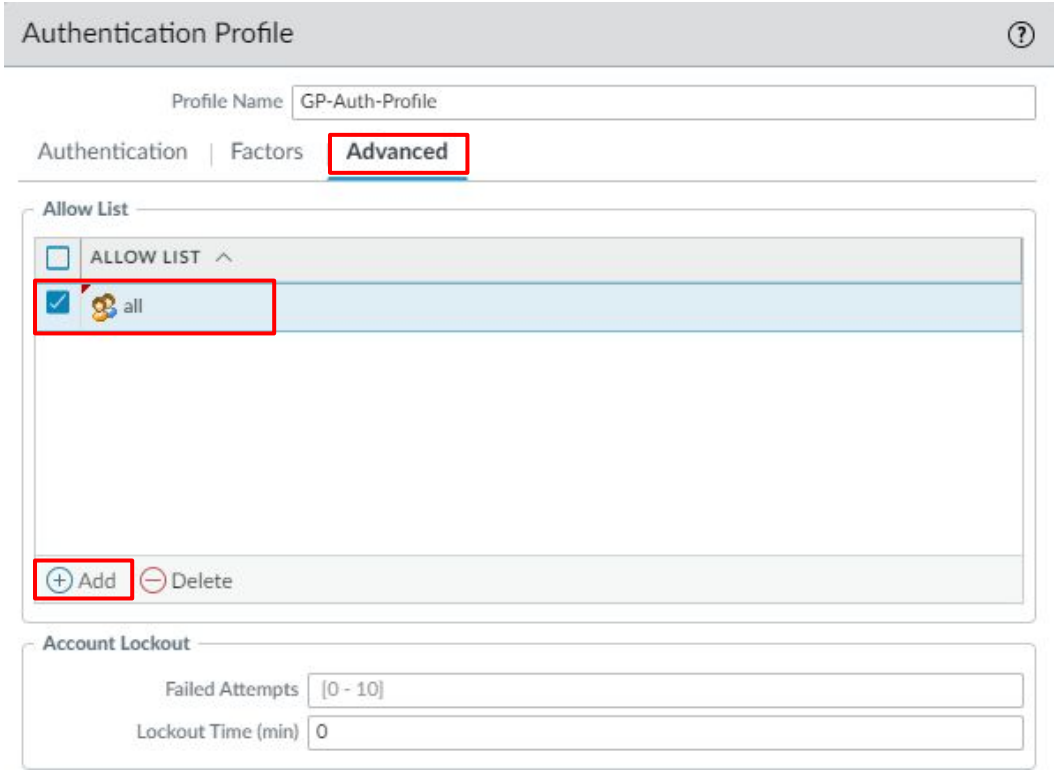
Authentication Profile:

Device -> Authentication Profile



User Authentication

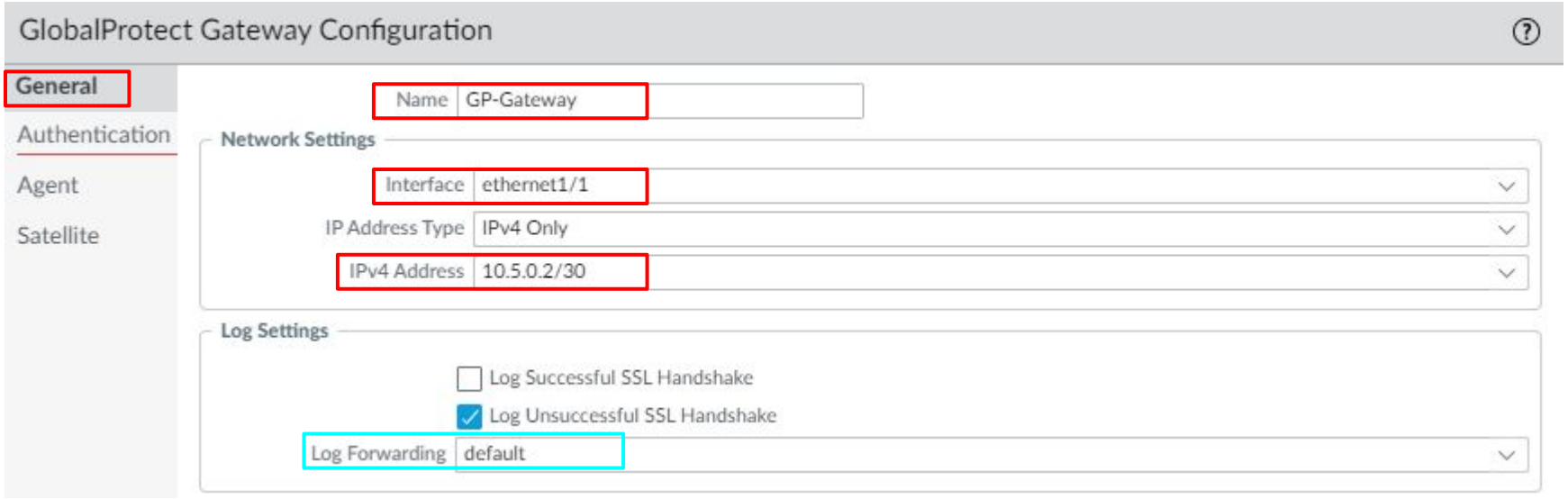
Authentication Profile (Cont.):



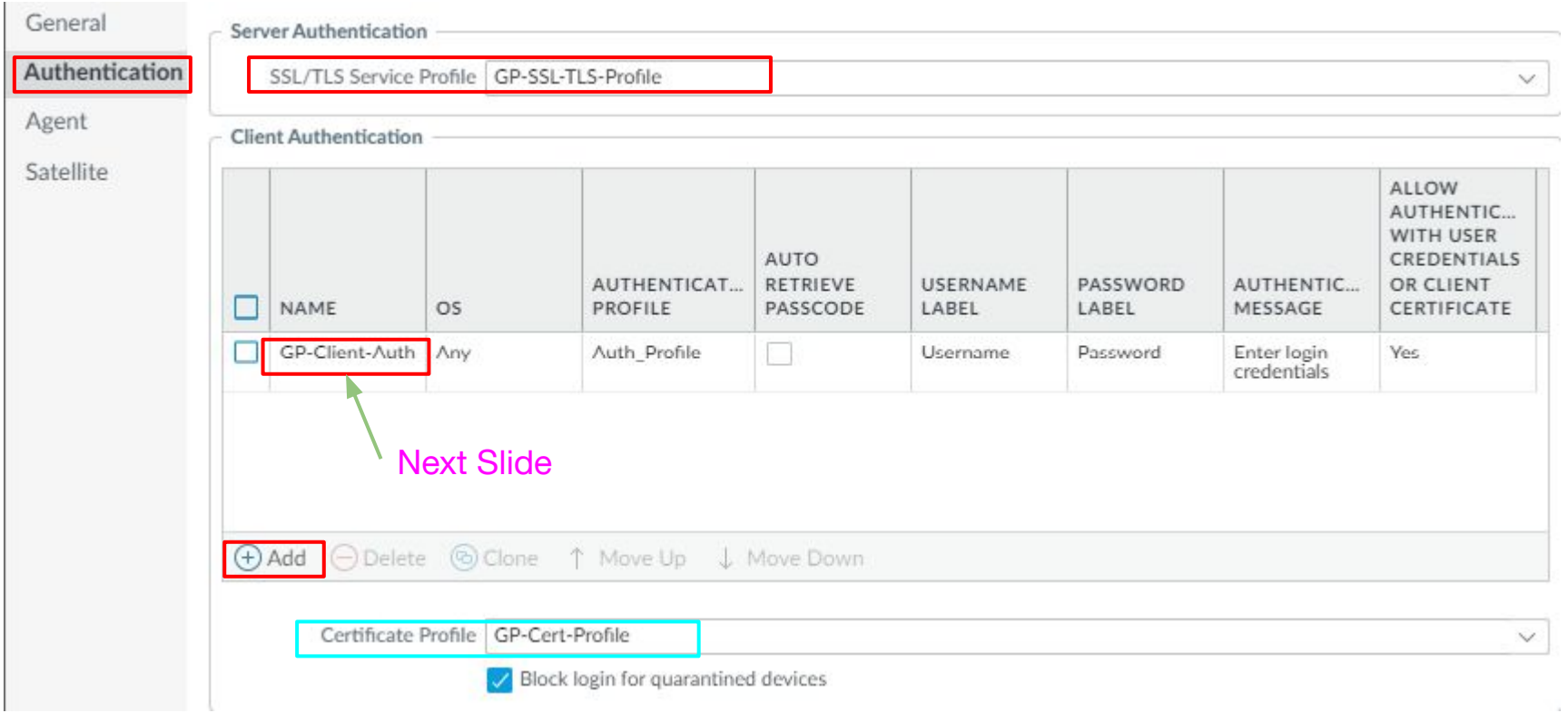
Gateway Configuration

Gateway Configuration

Network -> GlobalProtect -> Gateways

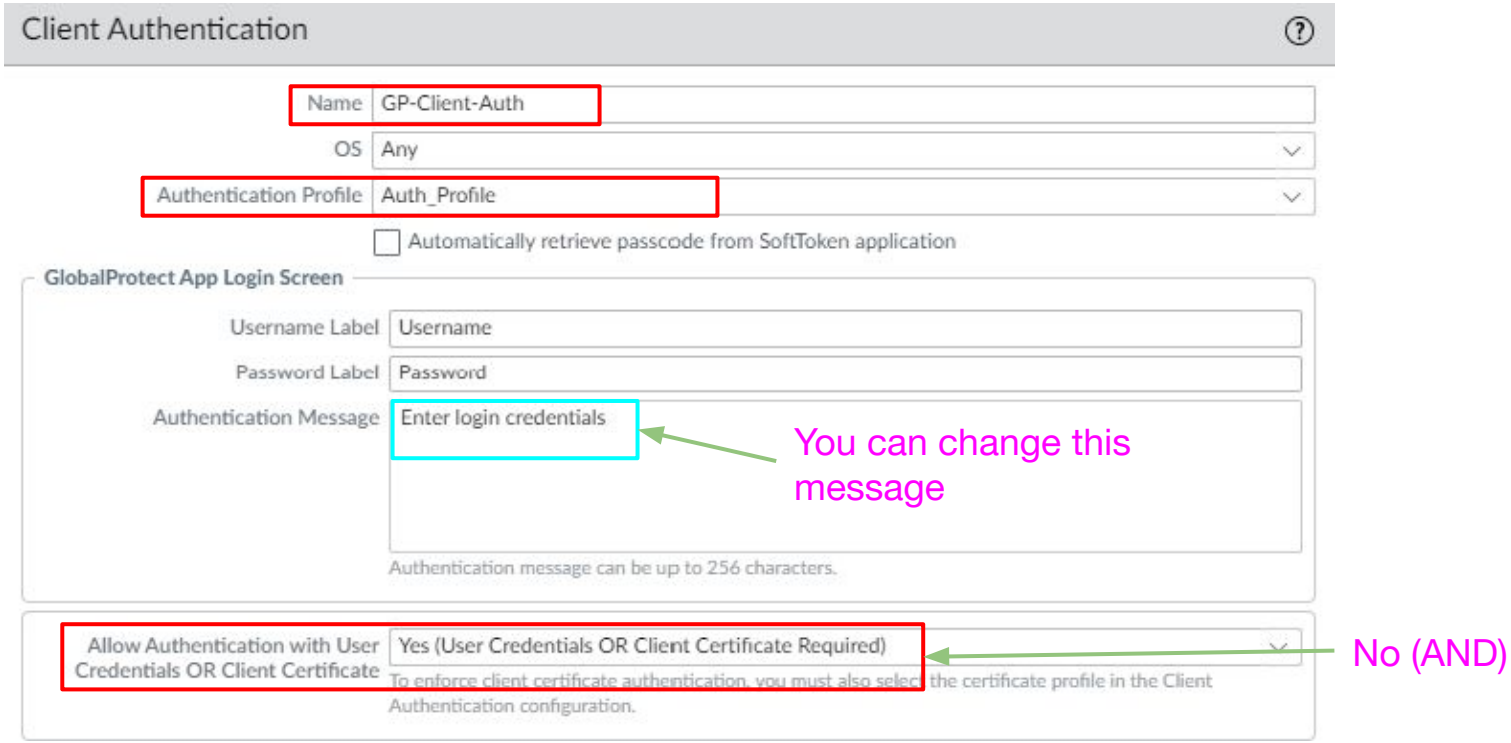


Gateway Configuration



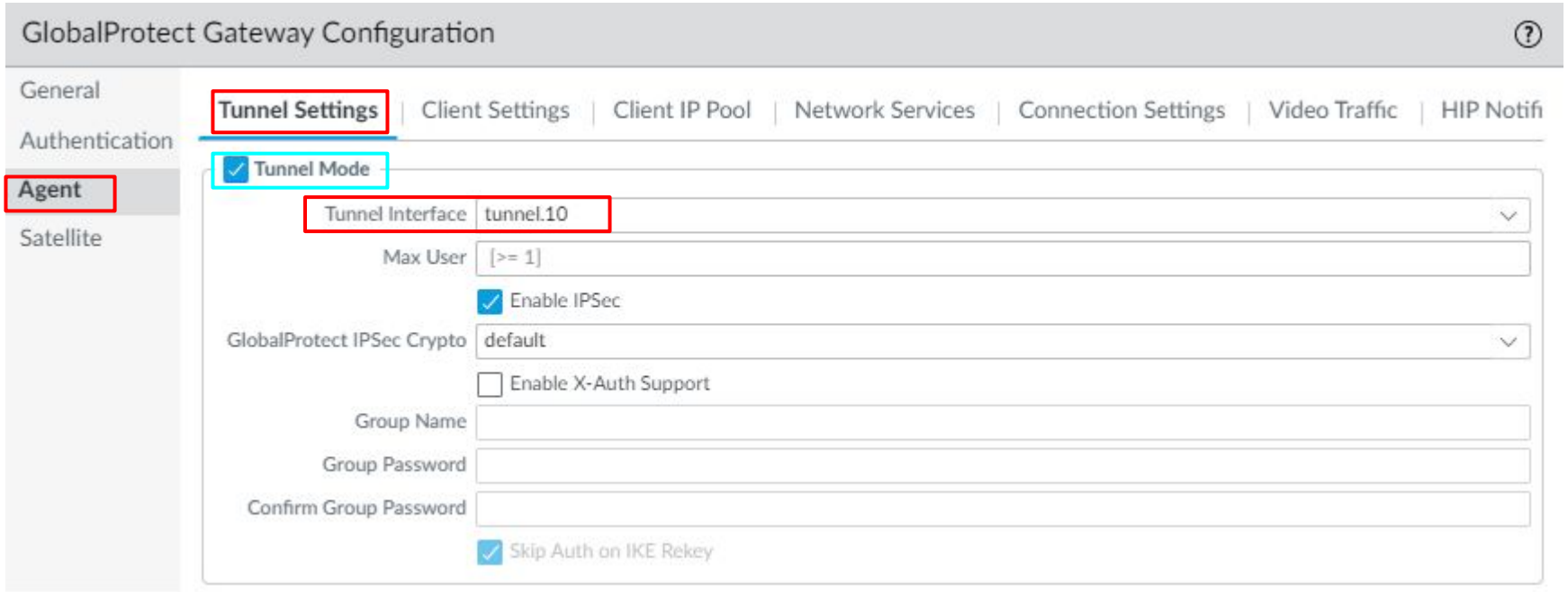
Gateway Configuration

Client Auth Profile:



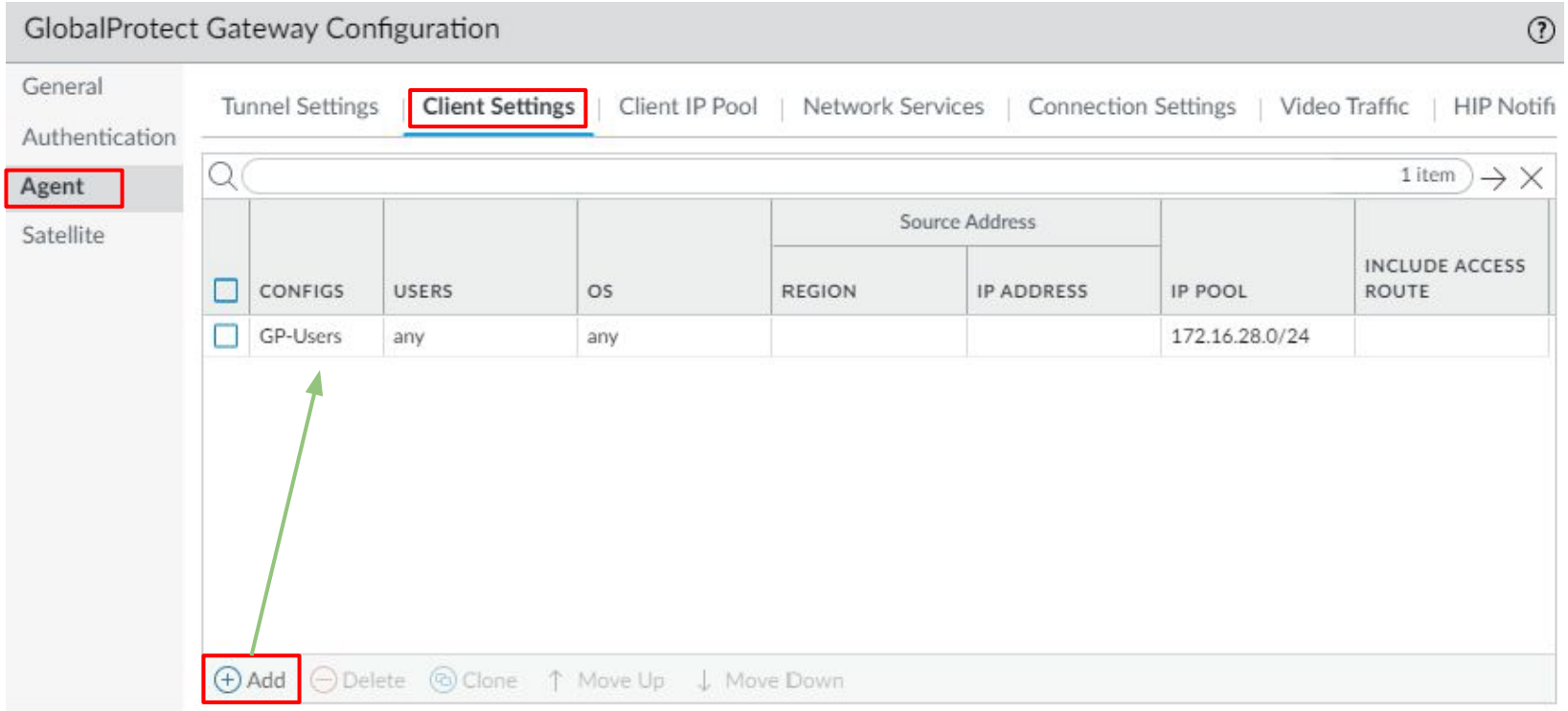
Gateway Configuration

Agent: Tunnel Settings



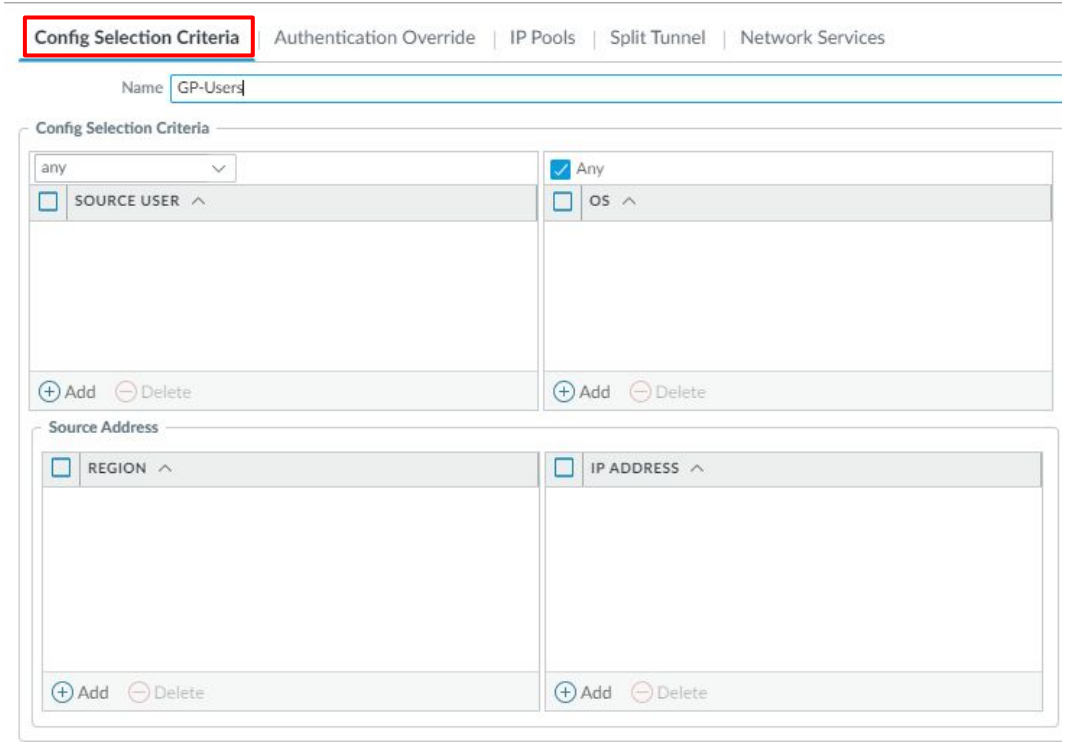
Gateway Configuration

Agent: Client Settings



Gateway Configuration

Client Settings (Cont.)

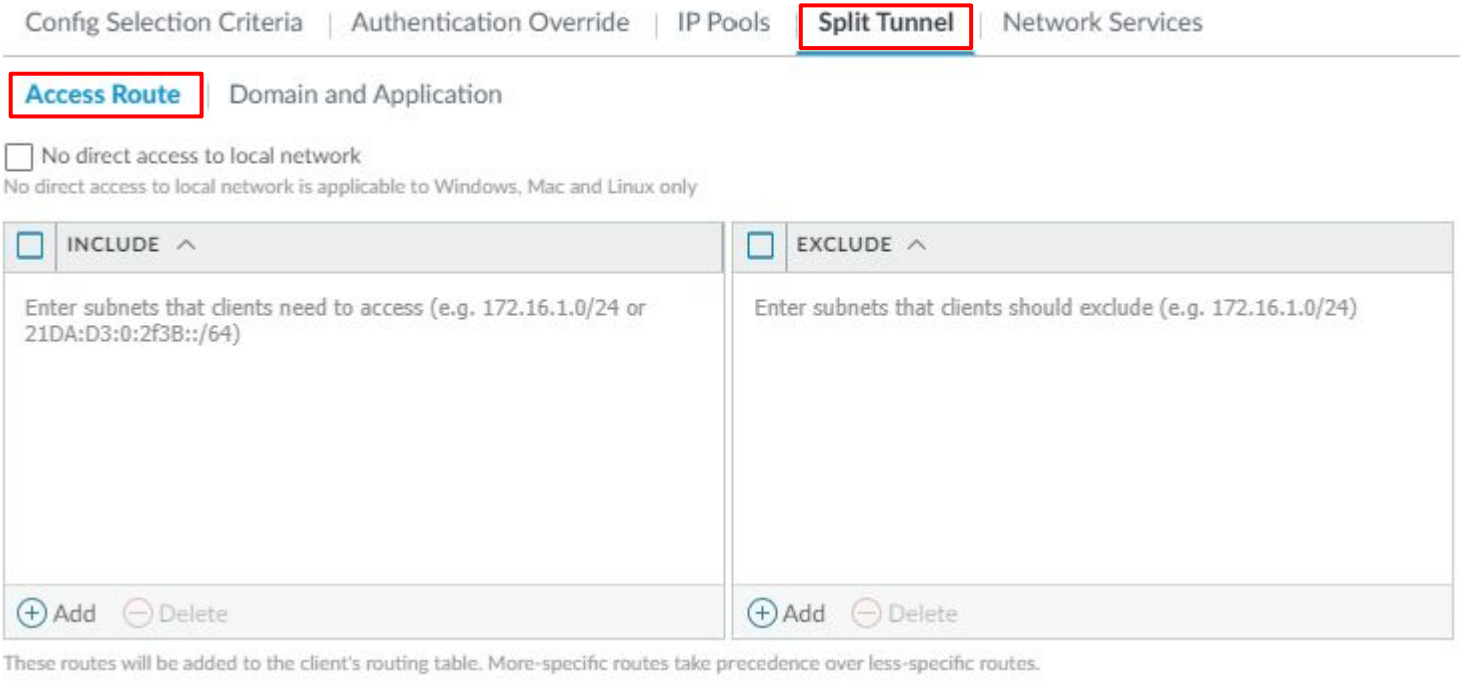


Gateway Configuration

Client Settings (Cont.)

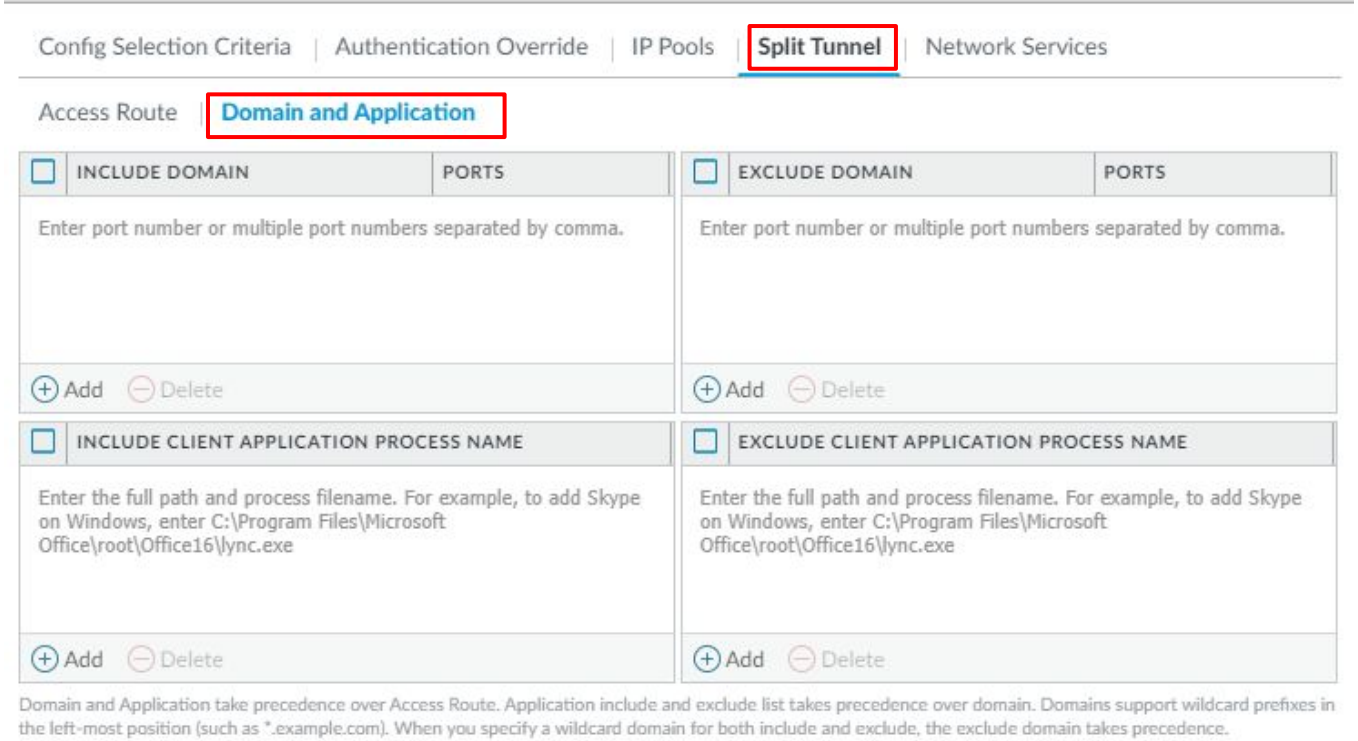
Gateway Configuration

Client Settings (Cont.)



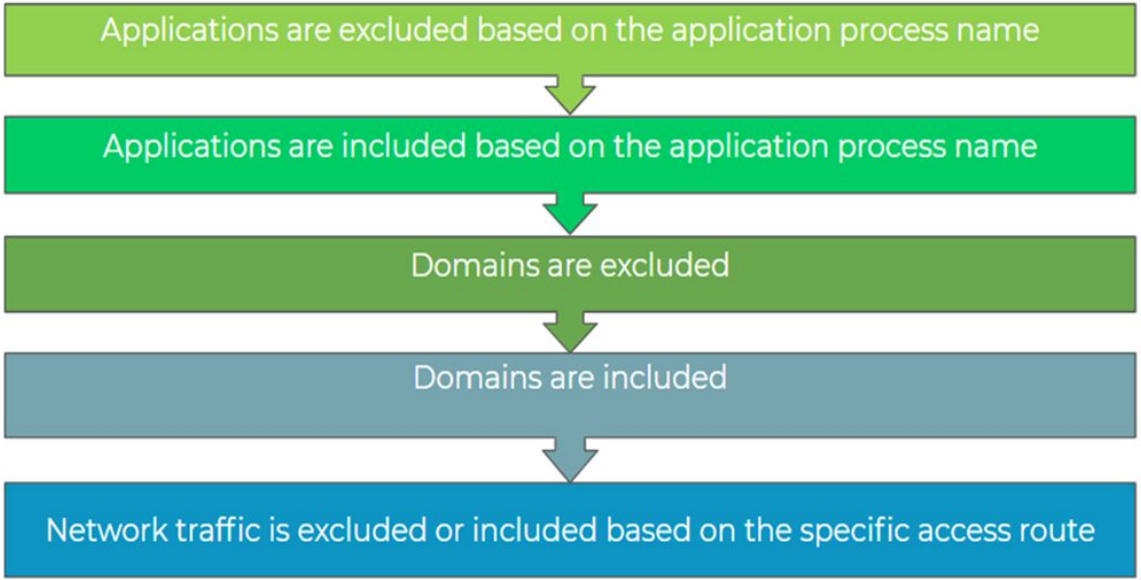
Gateway Configuration

Client Settings (Cont.)



Gateway Configuration

Split Tunnel Rule Processing:



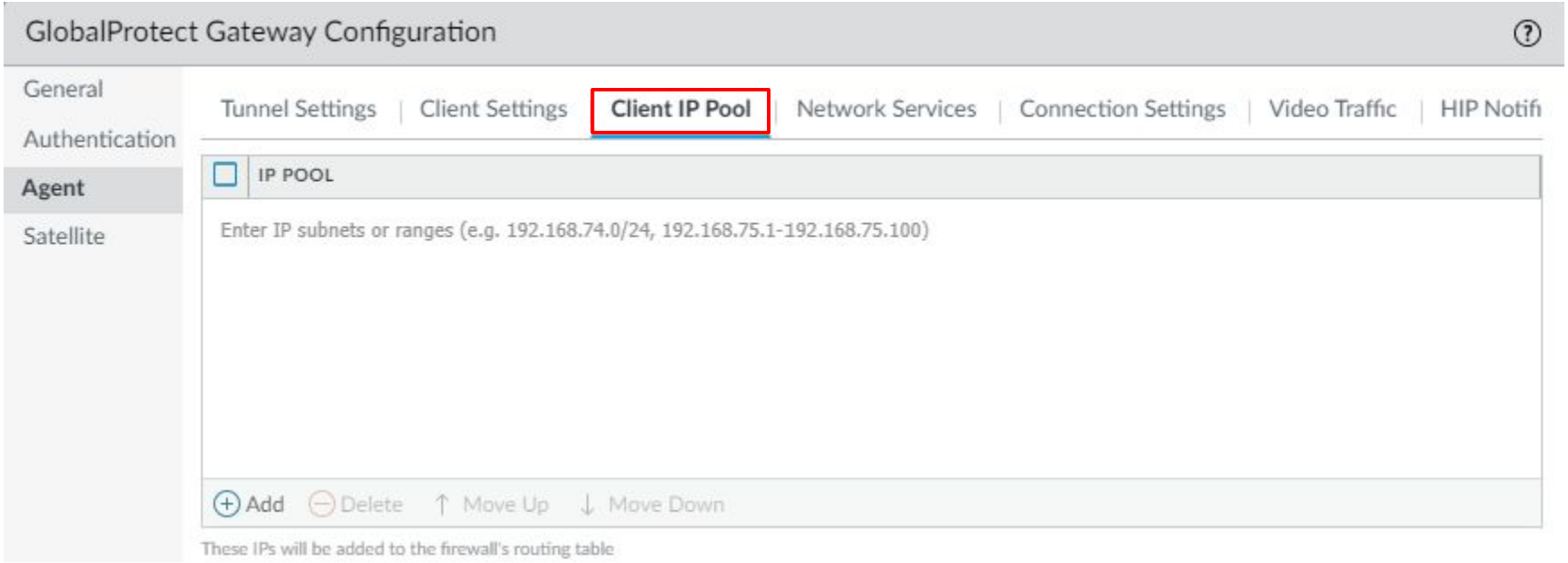
Split Tunnel Behavior Doc

Gateway Configuration

Client Settings (Cont.)

Gateway Configuration

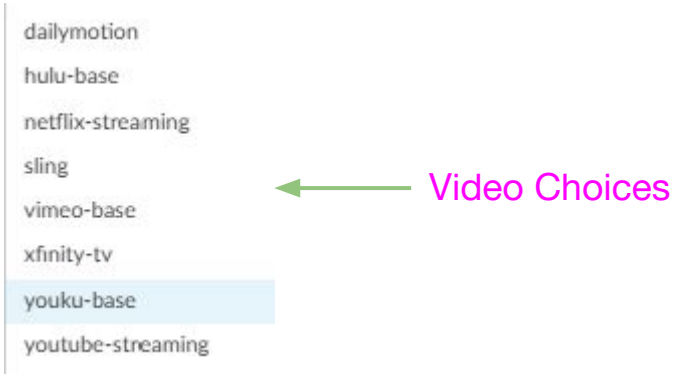
Agent: Client IP Pool



Gateway Configuration

Agent: Other Tabs

- Network Services - DNS, WINs, and domain name
- Connection Settings - Connectivity timers and messages
- Video Traffic - Allows video traffic to be split out from the tunnel. Default is all video traffic or you can select.

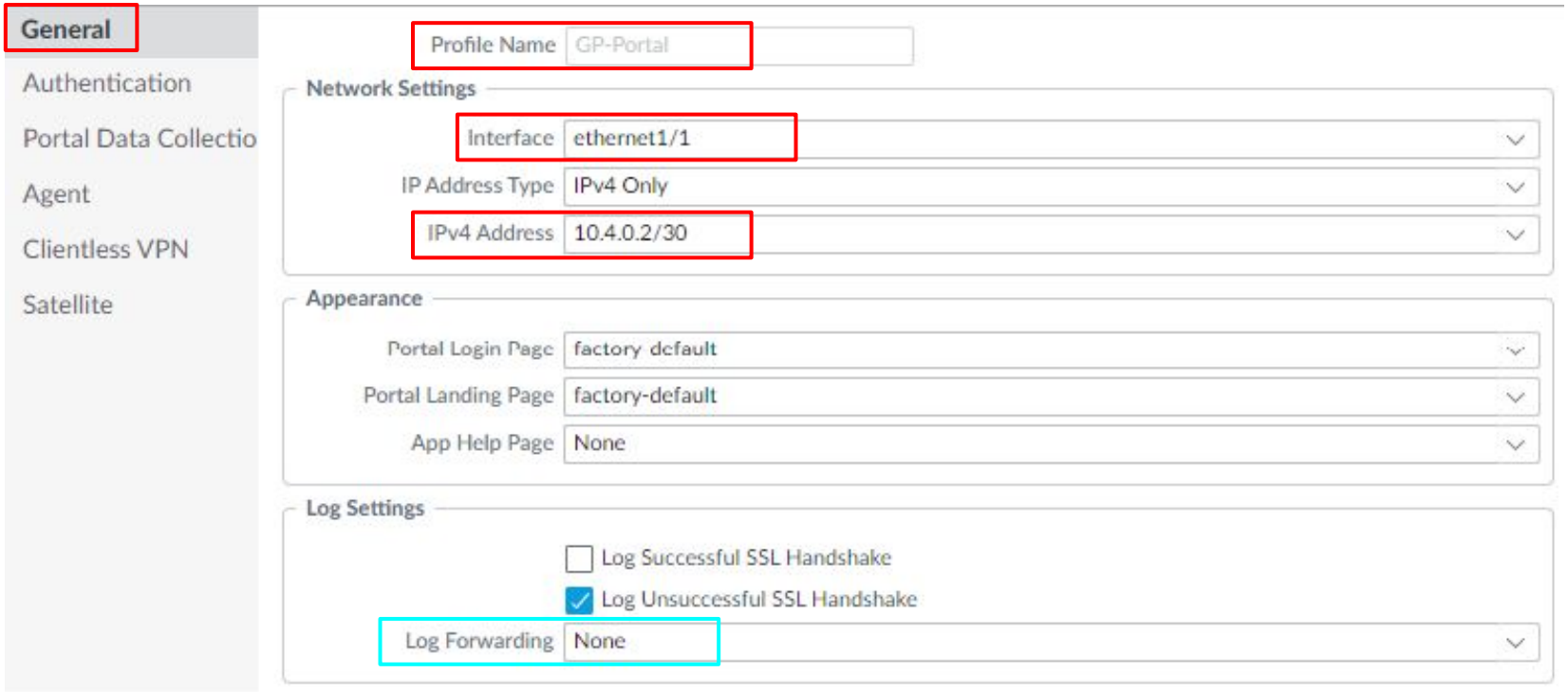


- HIP Notifications - Messages based on “Match/No-Match” criteria
- Satellite - Used for LSVPN configuration

Portal Configuration

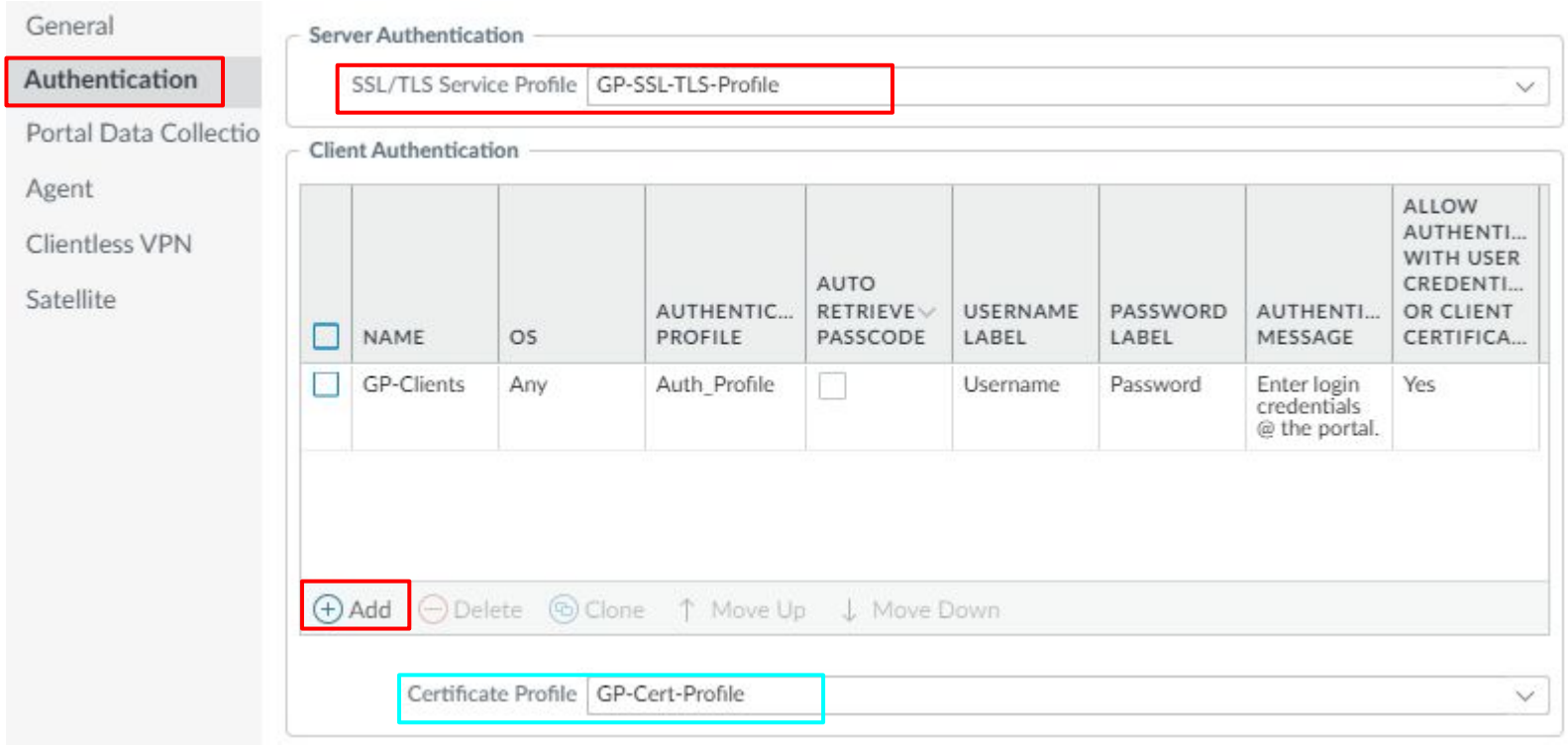
Portal Configuration

Network -> GlobalProtect -> Portals: General



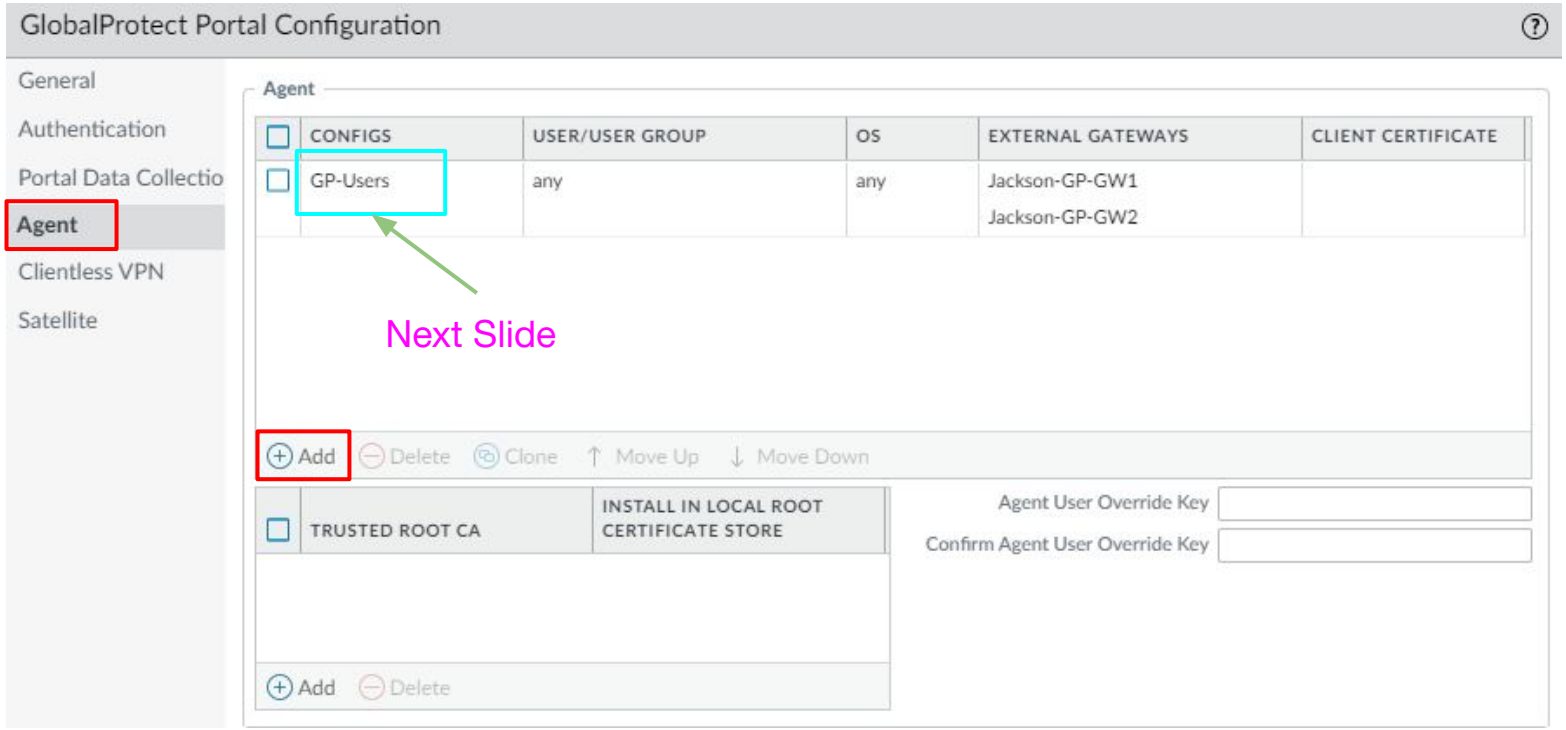
Portal Configuration

Authentication:



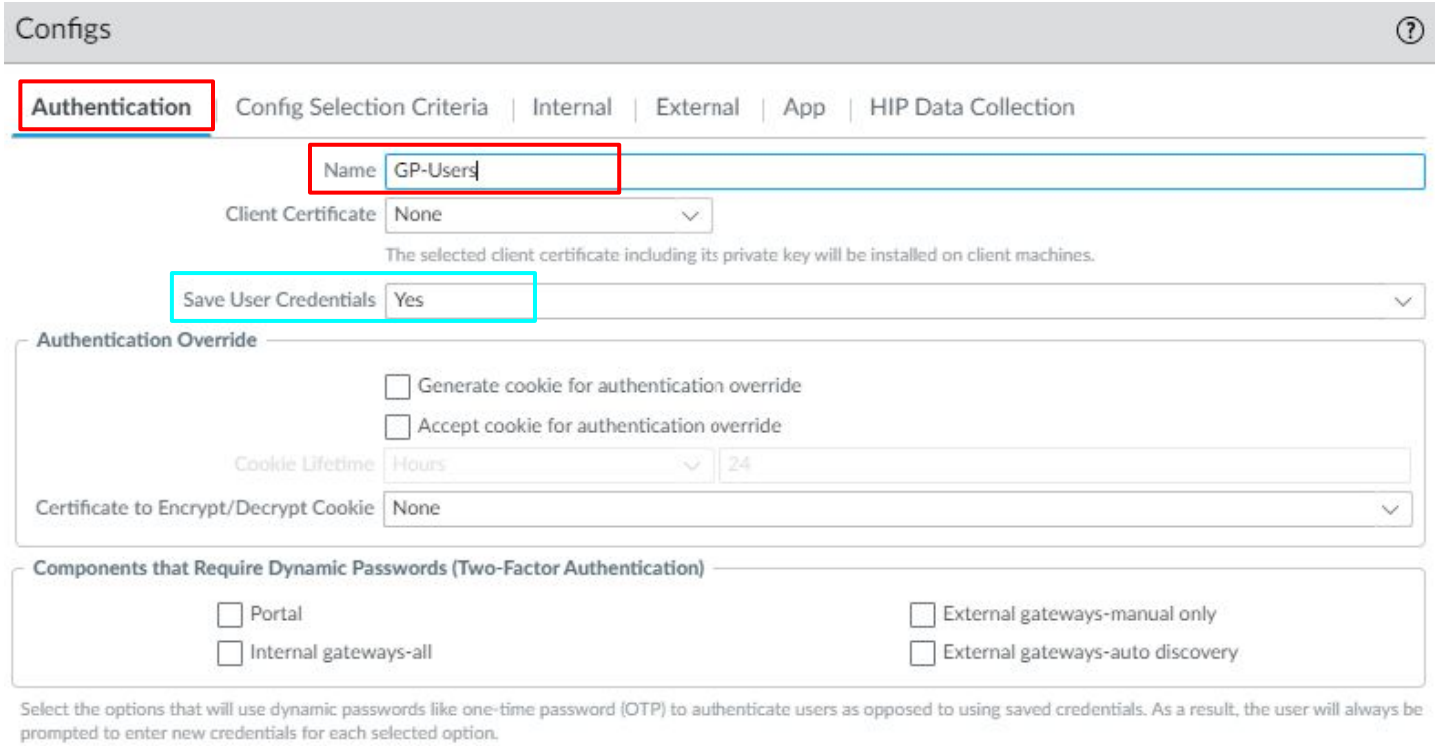
Portal Configuration

Agent:



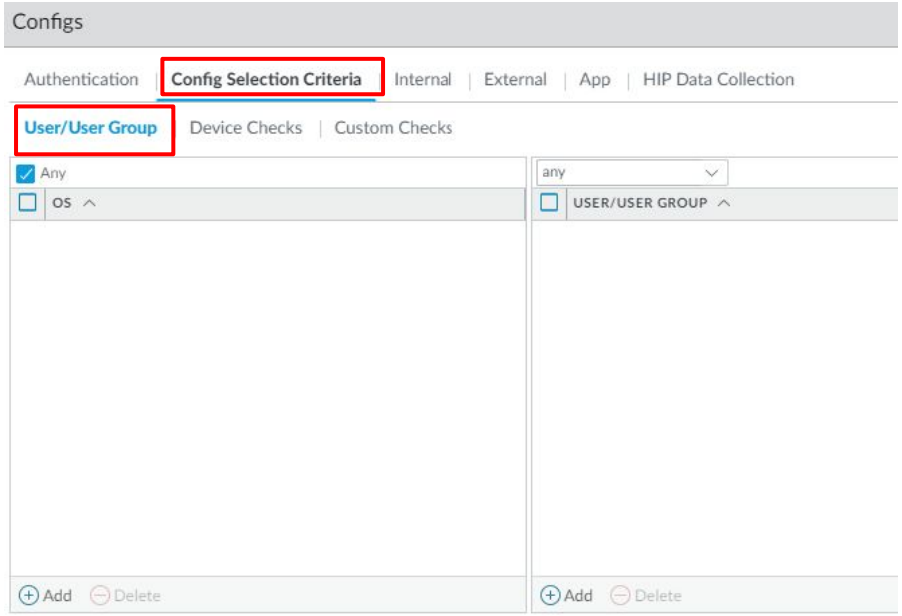
Portal Configuration

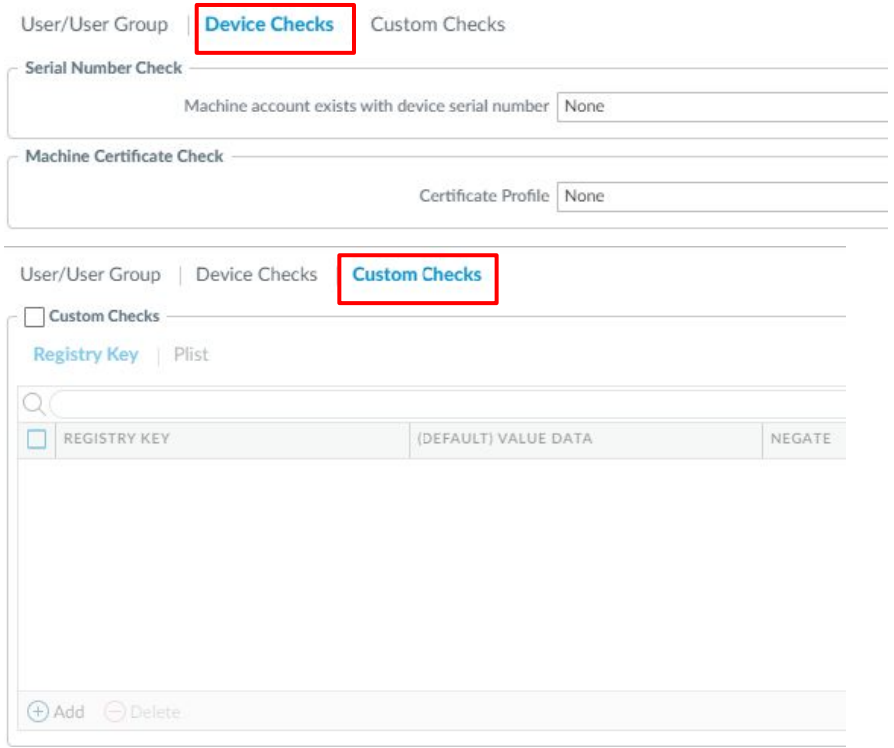
Agent: Agent Configuration



Portal Configuration

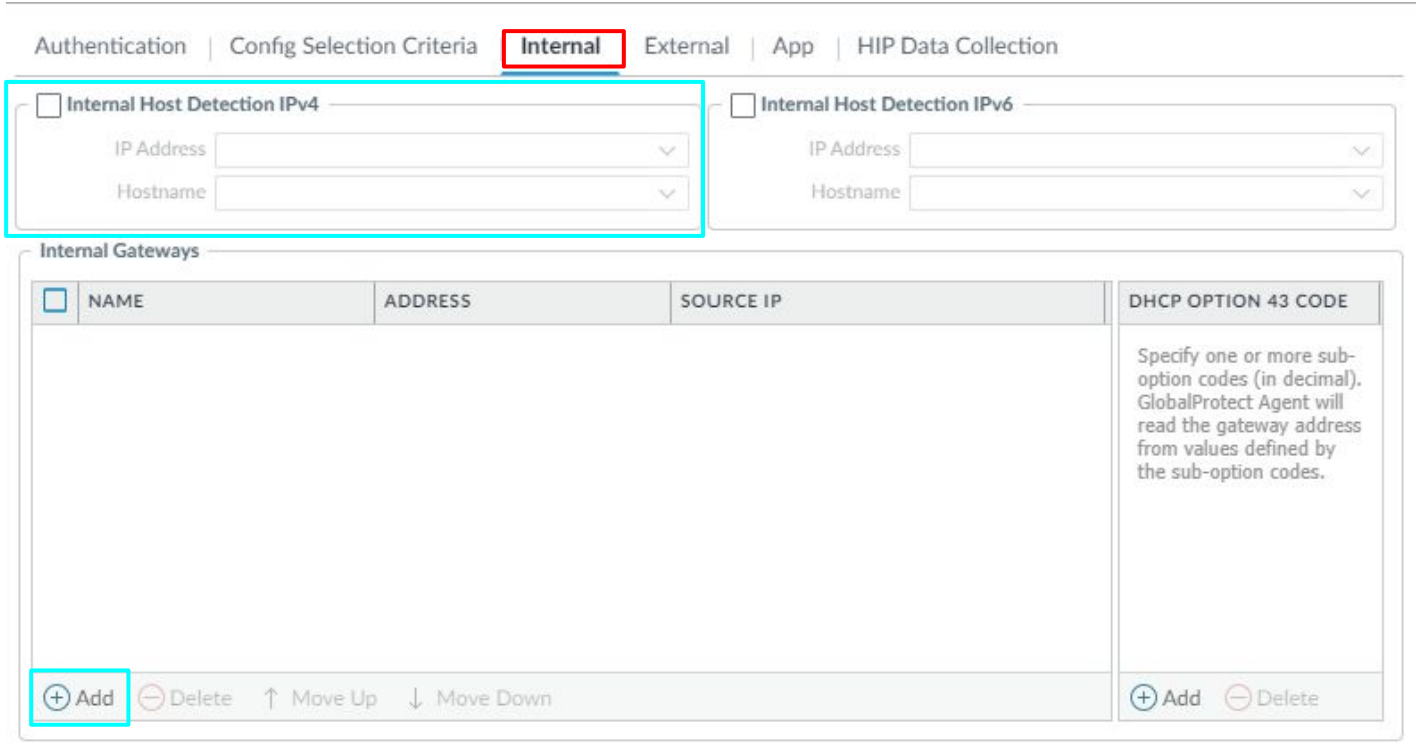
Agent: Agent Configuration





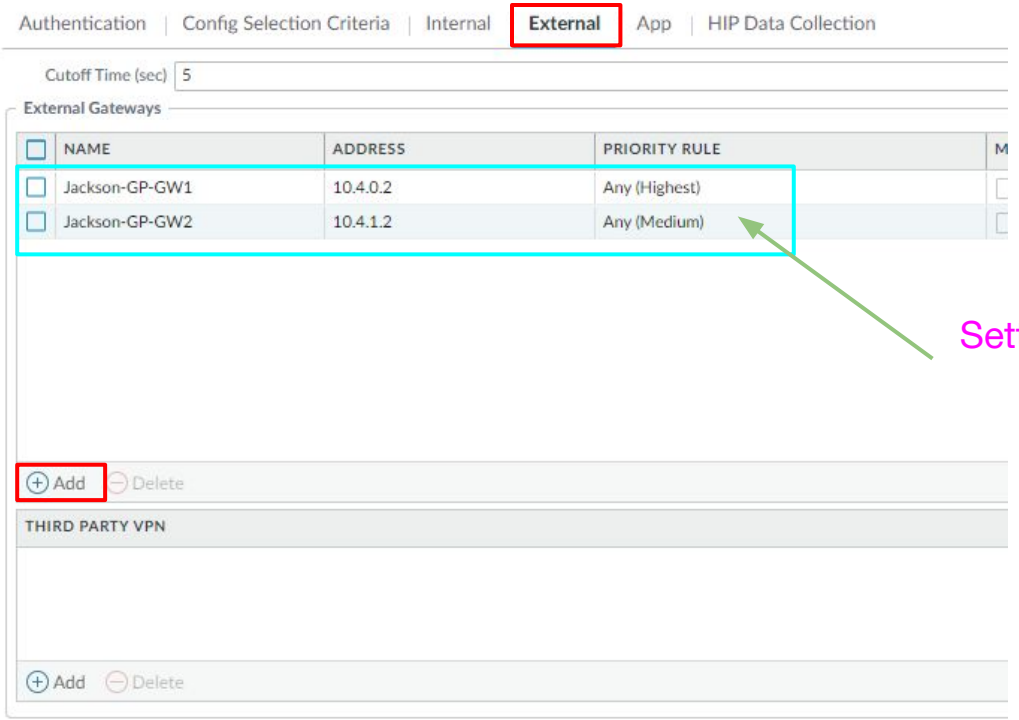
Portal Configuration

Agent: Agent Configuration



Portal Configuration

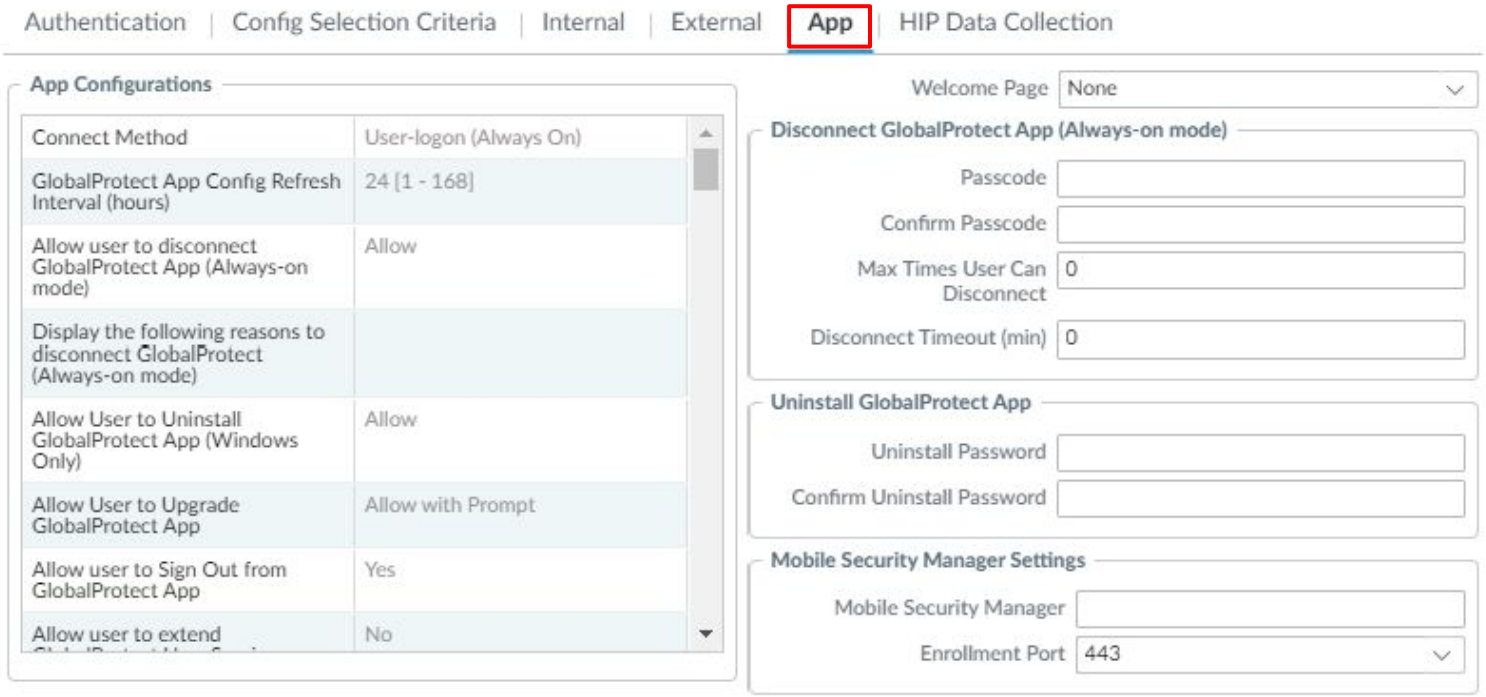
Agent: Agent Configuration



Setting Priority for multiple gateways

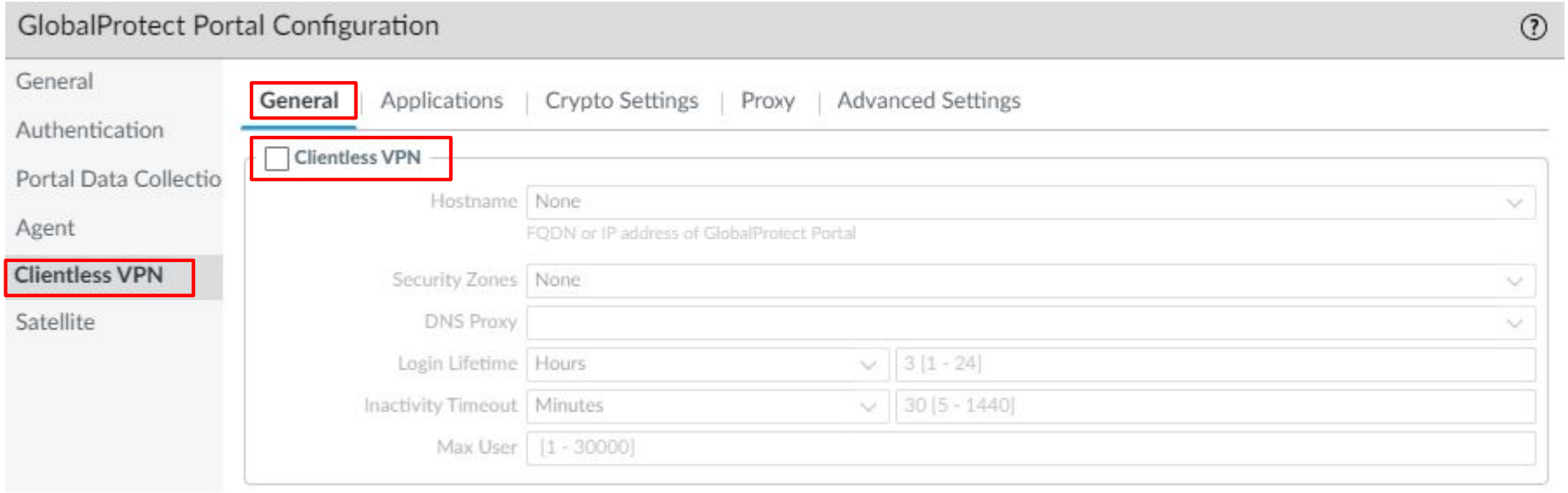
Portal Configuration

Agent: Agent Configuration - App Configurations Documentation



Portal Configuration

Clientless VPN:



Portal Configuration

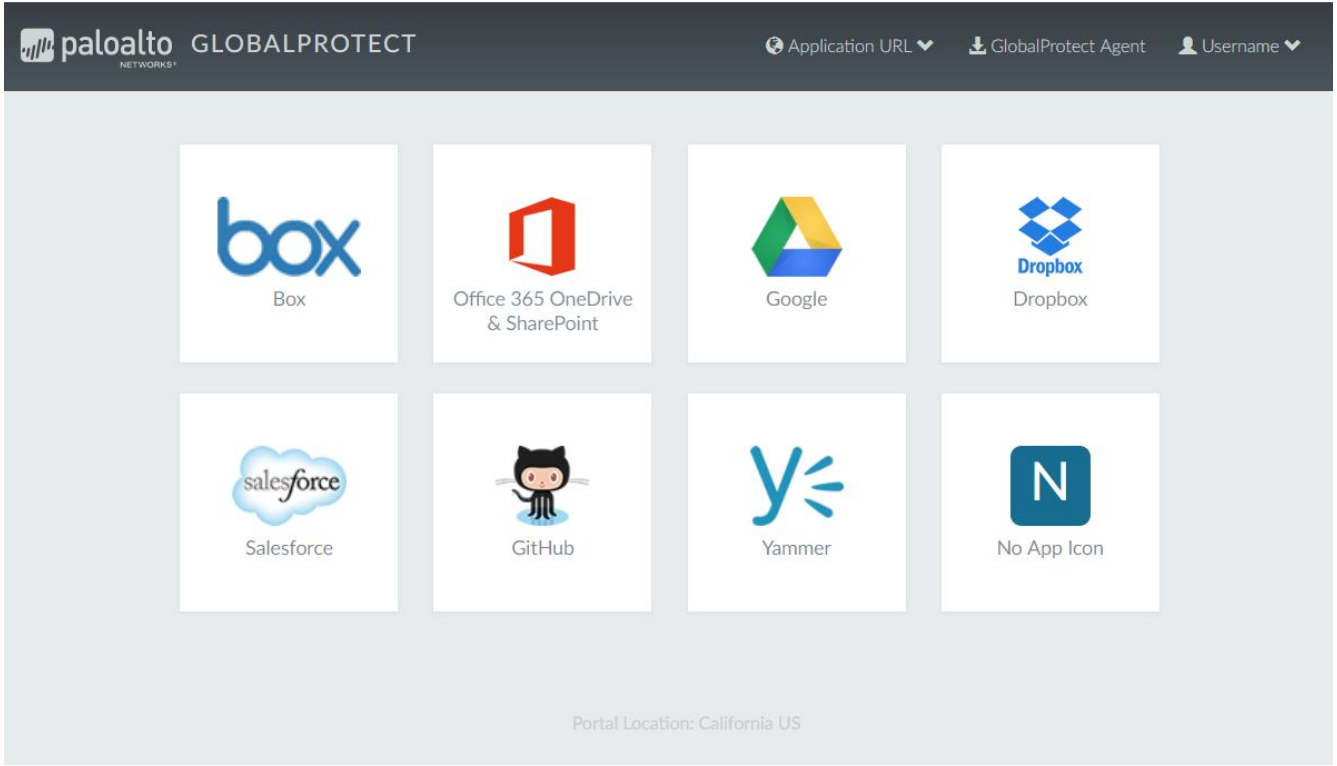
Clientless VPN: Applications

- Before you add applications in the Portal configuration, you need to add the clientless apps/groups.
  - Network -> GlobalProtect -> Clientless Apps
  - Network -> GlobalProtect -> Clientless App Groups
- Supported Technologies

- HTML
- HTML5
- HTML5-Web-Sockets
- Javascript ES5 or earlier
- RDP, VNC, or SSH
  - Virtual Desktop Infrastructure (VDI) and Virtual Machine (VM) environments, such as Citrix XenApp and XenDesktop, VMWare Horizon and vCenter support access natively through HTML5. You can RDP, VNC, or SSH to these machines through Clientless VPN without requiring additional third-party middleware.
  - In environments that do not include native support for HTML5 or other web application technologies supported by Clientless VPN, you can use third-party vendors, such as Thinfinity, to RDP through Clientless VPN.
- Adobe Flash—With Clientless VPN, browsers can serve content that uses Adobe Flash, Microsoft Word documents, or Adobe PDFs. However, Clientless VPN cannot rewrite HTML URLs or links within Adobe Flash, Microsoft Word documents, or Adobe PDFs, which can prevent the content from rendering correctly.
- Content encodings (for example, `Accept-Encoding: gzip`)

Portal Configuration

Clientless VPN: Landing Page



GlobalProtect Clients

GlobalProtect Clients

- Where can I install GlobalProtect
  - Apple macOS
  - Microsoft Windows
  - Linux
  - Apple iOS and iPadOS
  - Google Android
  - Google Chrome
  - Internet of Things (IoT)
  - Hypervisors

GlobalProtect Clients

- Supported client OS and supported GP client application information can be found on the compatibility Matrix.
  - Palo Alto Compatibility Matrix

Microsoft Windows

The following table shows which Microsoft Windows versions support which versions of the GlobalProtect app. For instructions on installing the GlobalProtect app on a macOS endpoint, see the installation instructions for 5.1, 5.2 6.0, 6.1, and 6.2.

OS	GP APP 5.1	GP APP 5.2	GP APP 6.0	GP APP 6.1	GP APP 6.2
Windows 7	√ Service Pack 1	– Upgrades from 5.1.10 to 5.2.x or later are blocked.	–	–	–
Windows 8	–	–	–	–	–
Windows 8.1	√	√	–	–	–
Windows 10	√	√	√ 64-bit (x64), 32-bit (x86), and ARM64 devices	√ 64-bit (x64), 32-bit (x86), and ARM64 devices	√ 64-bit (x64), 32-bit (x86), and ARM64 devices
Windows 10 UWP	√ x86 and ARM devices	√ x86 and ARM devices	√	√	√
Windows 11	–	√ x86 devices only on 5.2.10 & later	√ 64-bit (x64) and ARM64 devices	√ 64-bit (x64) and ARM64 devices	√ 64-bit (x64) and ARM64 devices

Troubleshooting

Troubleshooting

Monitor -> GlobalProtect Log

RECEIVE TIME	PORTAL/GATE...	STATUS	STAGE	EVENT	SOURCE USER	SOURCE REGION	HOST NAME	PUBLIC IPV4	PUBLIC IPV6	HOST ID	AUTH METHOD
03/26 17:33:38	Jackson-GP-GW1	success	logout	gateway-logout	netadminlab.us\sue	10.0.0.0-10.255.255.255	GP-CLIENT	10.25.0.100	0.0.0.0	34f15520-150d-49e1-88c3-205556eb78ee	
03/26 17:33:38	Jackson-GP-GW1	success	configuration	gateway-config-release	netadminlab.us\sue	10.0.0.0-10.255.255.255	GP-CLIENT	10.25.0.100	0.0.0.0	34f15520-150d-49e1-88c3-205556eb78ee	
03/26 17:31:29	Jackson-GP-GW1	success	host-info	gateway-hip-report	netadminlab.us\sue	10.0.0.0-10.255.255.255	GP-CLIENT	10.25.0.100	0.0.0.0	34f15520-150d-49e1-88c3-205556eb78ee	
03/26 17:31:29	Jackson-GP-GW1	success	host-info	gateway-hip-check	netadminlab.us\sue	10.0.0.0-10.255.255.255	GP-CLIENT	10.25.0.100	0.0.0.0	34f15520-150d-49e1-88c3-205556eb78ee	
03/26 17:31:29	Jackson-GP-GW1	success	tunnel	gateway-tunnel-latency	netadminlab.us\sue	10.0.0.0-10.255.255.255	GP-CLIENT	10.25.0.100	0.0.0.0	34f15520-150d-49e1-88c3-205556eb78ee	
03/26 17:31:29	Jackson-GP-GW1	success	connected	gateway-connected	netadminlab.us\sue	10.0.0.0-10.255.255.255	GP-CLIENT	10.25.0.100	0.0.0.0	34f15520-150d-49e1-88c3-205556eb78ee	ldap
03/26 17:31:29	Jackson-GP-GW1	success	tunnel	gateway-setup-ipsec	netadminlab.us\sue	10.0.0.0-10.255.255.255	GP-CLIENT	10.25.0.100	0.0.0.0	34f15520-150d-49e1-88c3-205556eb78ee	
03/26 17:31:29	Jackson-GP-GW1	success	agent-msg	gateway-agent-msg	netadminlab.us\sue	10.0.0.0-10.255.255.255		10.25.0.100	0.0.0.0		
03/26 17:31:21	Jackson-GP-GW1	success	configuration	gateway-getconfig	netadminlab.us\sue	10.0.0.0-10.255.255.255	GP-CLIENT	10.25.0.100	0.0.0.0	34f15520-150d-49e1-88c3-205556eb78ee	
03/26 17:31:21	Jackson-GP-GW1	success	login	gateway-register	netadminlab.us\sue	10.0.0.0-10.255.255.255	GP-CLIENT	10.25.0.100	0.0.0.0	34f15520-150d-49e1-88c3-205556eb78ee	
03/26 17:31:21	Jackson-GP-GW1	success	login	gateway-auth	sue	10.0.0.0-10.255.255.255	GP-CLIENT	10.25.0.100	0.0.0.0	34f15520-150d-49e1-88c3-205556eb78ee	ldap
03/26 17:31:21	Jackson-GP-GW1	success	before-login	gateway-prelogin		10.0.0.0-10.255.255.255		10.25.0.100	0.0.0.0	34f15520-150d-49e1-88c3-205556eb78ee	Certificate
03/26 17:31:18	GP-Portal	success	configuration	portal-getconfig	netadminlab.us\sue	10.0.0.0-10.255.255.255	GP-CLIENT	10.25.0.100	0.0.0.0	34f15520-150d-49e1-88c3-205556eb78ee	ldap
03/26 17:31:18	GP-Portal	success	login	portal-auth	sue	10.0.0.0-10.255.255.255	GP-CLIENT	10.25.0.100	0.0.0.0	34f15520-150d-49e1-88c3-205556eb78ee	ldap
03/26 17:31:16	GP-Portal	success	before-login	portal-prelogin		10.0.0.0-10.255.255.255		10.25.0.100	0.0.0.0	34f15520-150d-49e1-88c3-205556eb78ee	Certificate

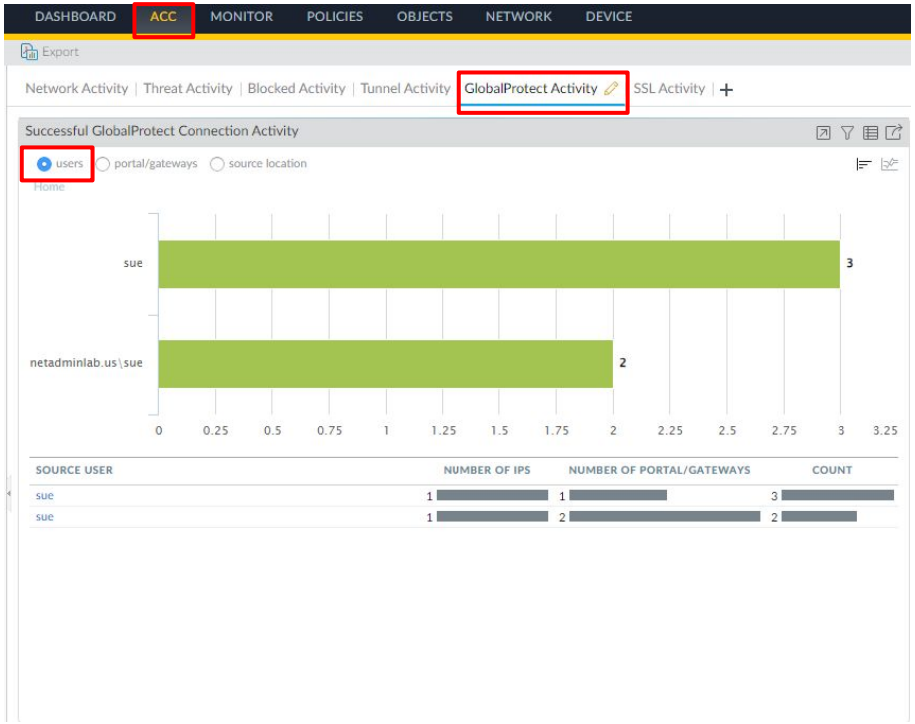
Troubleshooting

Session Browser:

START TIME	FROM ZONE	TO ZONE	SOURCE	DESTINATION	FROM PORT	TO PORT	PROTOCOL	APPLICATION	RULE	INGRESS I/F	EGRESS I/F	BYTES
04/02 16:56:28	gp-clients	outside	172.16.28.1	8.8.8.8	56849	53	17	dns-base	GP-to-Outside-Traffic	tunnel.10	sdwan.901	273
04/02 16:56:34	gp-clients	outside	172.16.28.1	8.8.8.8	55992	53	17	dns-base	GP-to-Outside-Traffic	tunnel.10	sdwan.901	276
04/02 16:56:31	gp-clients	outside	172.16.28.1	172.253.124.147	62451	443	17	quic	Block-QUIC-Traffic	tunnel.10	sdwan.901	6460
04/02 16:56:30	gp-clients	outside	172.16.28.1	8.8.8.8	59170	53	17	dns-base	GP-to-Outside-Traffic	tunnel.10	sdwan.901	382
04/02 16:56:30	gp-clients	outside	172.16.28.1	8.8.8.8	56888	53	17	dns-base	GP-to-Outside-Traffic	tunnel.10	sdwan.901	238
04/02 16:56:21	gp-clients	outside	172.16.28.1	8.8.8.8	64062	53	17	dns-base	GP-to-Outside-Traffic	tunnel.10	sdwan.901	208
04/02 16:56:34	gp-clients	outside	172.16.28.1	8.8.8.8	64416	53	17	dns-base	GP-to-Outside-Traffic	tunnel.10	sdwan.901	230
04/02 16:56:30	gp-clients	outside	172.16.28.1	23.2.23.210	61252	443	6	ssl	GP-to-Outside-Traffic	tunnel.10	sdwan.901	7258
04/02 16:53:30	gp-clients	outside	172.16.28.1	52.159.126.152	61153	443	6	windows-push-notifications	GP-to-Outside-Traffic	tunnel.10	sdwan.901	8713
04/02 16:56:30	gp-clients	outside	172.16.28.1	8.8.8.8	54234	53	17	dns-base	GP-to-Outside-Traffic	tunnel.10	sdwan.901	193
04/02 16:56:30	gp-clients	outside	172.16.28.1	142.250.9.95	61251	443	6	google-base	GP-to-Outside-Traffic	tunnel.10	sdwan.901	11015

Troubleshooting

ACC:



Troubleshooting

Network -> GlobalProtect -> Gateways

☑	Jackson-GP-GW1		ethernet1/1	10.4.0.2/30	tunnel.10		Remote Users
☐	Jackson-GP-GW2		ethernet1/2	10.4.1.2/30	tunnel.20		Remote Users

User Information - Jackson-GP-GW1

Current User | Previous User

1 item

DOMAIN	USER	PRIMARY USERNAME	COMPUTER	CLIENT	PRIVATE IP	PUBLIC IP	SOURCE REGION	TUNNEL TYPE	LOGIN AT	LIFETIME (S)	LOGOUT
netadminlab.us	sue	netadminlab.us\...	GP-CLIENT	Microsoft Windows 10 Pro N , 64-bit	172.16.28.1 ::	10.25.0.100 ::	10.0.0.0-10.255.255.255	IPSec	Apr.02 16:53:18	2592000	

Resources

Resources

- GlobalProtect Documentation Home Page
- GlobalProtect Administration Document
- GlobalProtect Quick Configs
- GlobalProtect 6.1 User's Guide (Windows)
- GlobalProtect 6.1 User’s Guide (macOS)
- Prisma Access Agent Administrator Guide
- Prisma Access Agent User Guide

Questions?

Thank You

paloaltonetworks.com