

Basic GlobalProtect Configuration

Version 1.1



Agenda

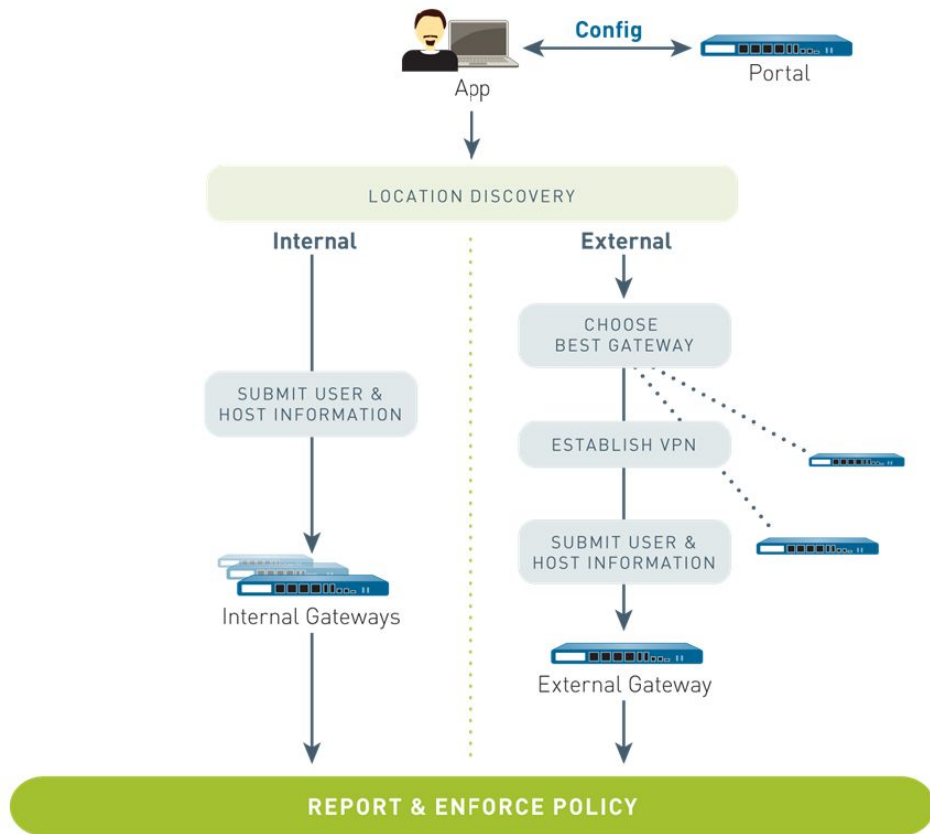
- GlobalProtect Components
- GlobalProtect License
- Interfaces, Zones, and Policies
- SSL Certificates
- User Authentication
- Gateway Configuration
- Portal Configuration
- GlobalProtect Clients
- Troubleshooting
- Resources
- Questions?

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

Interface Name	ethernet1/1			
Comment	Primary Outside Interface			
Interface Type	Layer3			
Netflow Profile	None			
Config	IPv4	IPv6	SD-WAN	Advanced

Assign Interface To	
Virtual Router	default_vRouter
Security Zone	outside

Interfaces

Interface (Cont.)

Interface Name	ethernet1/1		
Comment	Primary Outside Interface		
Interface Type	Layer3		
Netflow Profile	None		

Config **IPv4** | IPv6 | SD-WAN | Advanced

☒ Enable SD-WAN

Type ☒ Static ☐ PPPoE ☐ DHCP Client

☐	IP	NEXT HOP GATEWAY
☐	10.4.0.2/30	10.4.0.1

Interfaces

Network -> Interfaces -> Tunnel

Tunnel Interface

Interface Name

tunnel

11

Comment

Tunnel for GP Clients

Netflow Profile

None

Config

IPv4

IPv6

Advanced

Assign Interface To

Virtual Router

default_vRouter

Security Zone

gp-clients

OK

Cancel

Zones

Network -> Zones

Zone ?

Name **gp-clients**

Location vsys1

Log Setting default

Type **Layer3**

INTERFACES ^

tunnel.10

tunnel.20

+ Add - Delete

Zone Protection

Zone Protection Profile None

☒ Enable Packet Buffer Protection

☐ Enable L3 & L4 Header Inspection

User Identification ACL

☒ Enable User Identification

☐ INCLUDE LIST ^

Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24

+ Add - Delete

☐ EXCLUDE LIST ^

Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24

+ Add - Delete

Users from these addresses/subnets will be identified.

Device-ID ACL

☐ Enable Device Identification

☐ INCLUDE LIST ^

Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24

+ Add - Delete

☐ EXCLUDE LIST ^

Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24

+ Add - Delete

Devices from these addresses/subnets will be identified.

© 2025 Palo Alto Networks, Inc. All rights reserved. Proprietary and confidential information.

 paloalto
NETWORKS

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

Device Certificates | Default Trusted Certificate Authorities

☐	NAME	LOCATION	SUBJECT	ISSUER	CA	KEY	EXPIRES	STATUS
☐	AD-Root-CA	vsys1	DC = us, DC = neta...	DC = us, DC = neta...	☒	☐	Jan 6 21:28:43 2027 G...	valid
☐	AD-Sub-Root	vsys1	C = US, ST = MS, C...	DC = us, DC = neta...	☒	☒	Dec 18 23:26:32 2025 ...	valid
☐	GP-Cert	vsys1	C = US, ST = MS, C...	DC = us, DC = neta...	☒	☒	Mar 26 20:02:00 2026 ...	valid
☐	untrusted-cert	vsys1	CN = untrusted-cert	CN = untrusted-cert	☒	☒	Dec 17 23:45:21 2024 ...	valid

Create CSR

SSL Certificates

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



SSL/TLS Service Profile ?

Name

☐ Shared

Certificate

Protocol Settings

Min Version

Max Version

- TLSv1.0
- TLSv1.1**
- TLSv1.2
- Max

Max is TLSv1.3

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

Local User

Name

gpuser

Mode

☒ Password ☐ Password Hash

Password

••••••••

Confirm Password

••••••••

☒ Enable

OK

Cancel

User Authentication

External User: LDAP

Device -> Server Profile -> LDAP

LDAP Server Profile

Profile Name LDAP-SVR-Profile

☐ Administrator Use Only

Server List

NAME	LDAP SERVER	PORT
Lab-AD	172.16.32.25	389

+ Add

- Delete

Enter the IP address or FQDN of the LDAP server

Server Settings

Typeactive-directory

Base DNDC=netadminlab,DC=us

Bind DNsvc_paloalto@netadminlab.us

Password••••••••

Confirm Password••••••••

Bind Timeout30

Search Timeout30

Retry Interval60

☒ Require SSL/TLS secured connection

☐ Verify Server Certificate for SSL sessions

active-directory

e-directory

sun

other

OK

Cancel

© 2025 Palo Alto Networks, Inc. All rights reserved. Proprietary and confidential information.

 paloalto
NETWORKS

User Authentication

Authentication Profile:

Device -> Authentication Profile

Authentication Profile

Profile NameGP-Auth-Profile

Authentication

Factors

Advanced

TypeLDAP

Server ProfileLab-DC01

Login Attribute

Password Expiry Warning7

Number of days prior to warning a user about password expiry.

User Domainnetadminlab.us

Username Modifier%USERINPUT%

Single Sign On

Kerberos Realm

Kerberos KeytabClick "Import" to configure this fieldX Import

None

Cloud Authentication Service

Local Database

RADIUS

LDAP

TACACS+

SAML

Kerberos

User Authentication

Authentication Profile (Cont.):

Authentication Profile

?

Profile Name

GP-Auth-Profile

Authentication

Factors

Advanced

Allow List

☐

ALLOW LIST

^

☒

 all

Account Lockout

Failed Attempts

[0 - 10]

Lockout Time (min)

0

Gateway Configuration

Gateway Configuration

Network -> GlobalProtect -> Gateways

GlobalProtect Gateway Configuration ?

General
Authentication
Agent
Satellite

NameGP-Gateway

Network Settings

Interfaceethernet1/1

IP Address TypeIPv4 Only

IPv4 Address10.5.0.2/30

Log Settings

☐ Log Successful SSL Handshake

☒ Log Unsuccessful SSL Handshake

Log Forwardingdefault

© 2025 Palo Alto Networks, Inc. All rights reserved. Proprietary and confidential information.

 paloalto
NETWORKS

Gateway Configuration

General

Authentication

Agent

Satellite

Server Authentication

SSL/TLS Service ProfileGP-SSL-TLS-Profile

Client Authentication

	NAME	OS	AUTHENTICAT... PROFILE	AUTO RETRIEVE PASSCODE	USERNAME LABEL	PASSWORD LABEL	AUTHENTIC... MESSAGE	ALLOW AUTHENTIC... WITH USER CREDENTIALS OR CLIENT CERTIFICATE
☐	GP-Client-Auth	Any	Auth_Profile	☐	Username	Password	Enter login credentials	Yes

+ Add

- Delete

🔄 Clone

↑ Move Up

↓ Move Down

Certificate ProfileGP-Cert-Profile

☒ Block login for quarantined devices

Next Slide

Gateway Configuration

Client Auth Profile:

Client Authentication



Name GP-Client-Auth

OS Any

Authentication Profile Auth_Profile

☐ Automatically retrieve passcode from SoftToken application

GlobalProtect App Login Screen

Username Label Username

Password Label Password

Authentication Message Enter login credentials

You can change this message

Authentication message can be up to 256 characters.

Allow Authentication with User Credentials OR Client Certificate Yes (User Credentials OR Client Certificate Required)

To enforce client certificate authentication, you must also select the certificate profile in the Client Authentication configuration.

No (AND)

Gateway Configuration

Agent: Tunnel Settings

GlobalProtect Gateway Configuration

General

Authentication

Agent

Satellite

Tunnel Settings

Client Settings

Client IP Pool

Network Services

Connection Settings

Video Traffic

HIP Notifi

☒ Tunnel Mode

Tunnel Interface

tunnel.10

Max User

[>= 1]

☒ Enable IPSec

GlobalProtect IPSec Crypto

default

☐ Enable X-Auth Support

Group Name

Group Password

Confirm Group Password

☒ Skip Auth on IKE Rekey

Gateway Configuration

Agent: Client Settings

GlobalProtect Gateway Configuration ?

General
Authentication
Agent
Satellite

Tunnel Settings

Client Settings

Client IP Pool

Network Services

Connection Settings

Video Traffic

HIP Notifi

1 item → ×

				Source Address			
				REGION	IP ADDRESS		
☐	CONFIGS	USERS	OS			IP POOL	INCLUDE ACCESS ROUTE
☐	GP-Users	any	any			172.16.28.0/24	

+ Add

- Delete

⌕ Clone

↑ Move Up

↓ Move Down

Gateway Configuration

Client Settings (Cont.)

Config Selection Criteria

Authentication Override | IP Pools | Split Tunnel | Network Services

Name

Config Selection Criteria

any

☐ SOURCE USER ^

☒ Any

☐ OS ^

+ Add - Delete

+ Add - Delete

Source Address

☐ REGION ^

☐ IP ADDRESS ^

+ Add - Delete

+ Add - Delete

Gateway Configuration

Client Settings (Cont.)

Config Selection Criteria

Authentication Override

IP Pools

Split Tunnel

Network Services

☐ Retrieve Framed-IP-Address attribute from authentication server

☐ AUTHENTICATION SERVER IP POOL ^

Enter IP subnets or ranges to match the Framed IP attribute of the authentication server. Supports IPv4 private/public addresses (e.g. 192.168.74.0/24, 192.168.75.1-192.168.75.100) or IPv6 unique local/public addresses (e.g. 2001:aa::1-2001:aa::10)

+ Add

- Delete

These IPs will be added to the firewall's routing table

☐ IP POOL

☐ 172.16.28.0/24

+ Add

- Delete

↑ Move Up

↓ Move Down

These IPs will be added to the firewall's routing table

Gateway Configuration

Client Settings (Cont.)

Config Selection Criteria | Authentication Override | IP Pools | **Split Tunnel** | Network Services

Access Route | Domain and Application

☐ No direct access to local network

No direct access to local network is applicable to Windows, Mac and Linux only

☐ INCLUDE ^	☐ EXCLUDE ^
Enter subnets that clients need to access (e.g. 172.16.1.0/24 or 21DA:D3:0:2f3B::/64)	Enter subnets that clients should exclude (e.g. 172.16.1.0/24)
 Add  Delete	 Add  Delete

These routes will be added to the client's routing table. More-specific routes take precedence over less-specific routes.

Gateway Configuration

Client Settings (Cont.)

Config Selection Criteria

Authentication Override

IP Pools

Split Tunnel

Network Services

Access Route

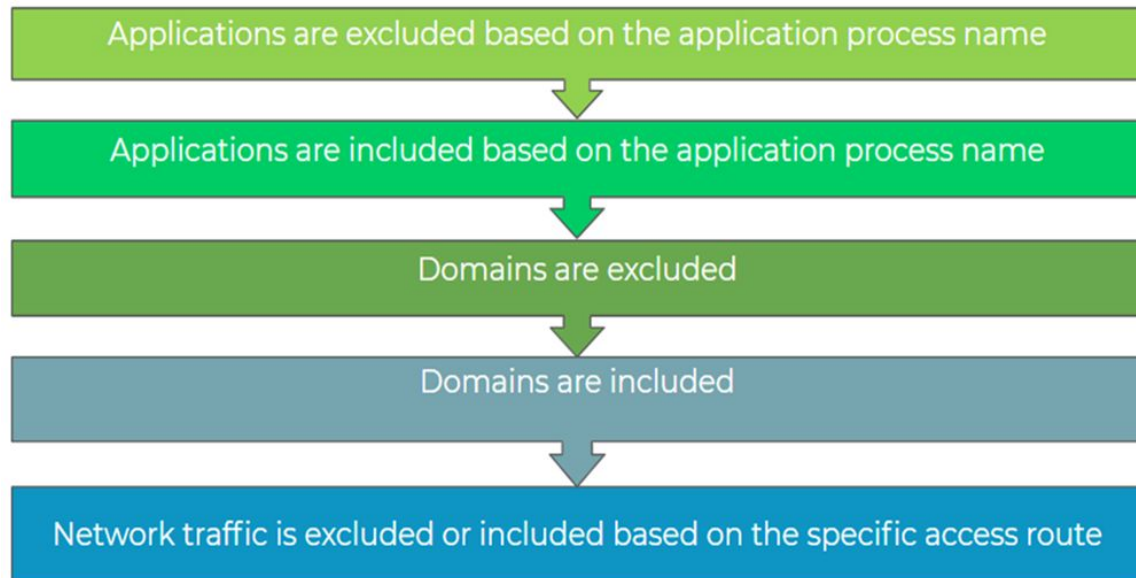
Domain and Application

☐ INCLUDE DOMAIN	PORTS	☐ EXCLUDE DOMAIN	PORTS
Enter port number or multiple port numbers separated by comma.		Enter port number or multiple port numbers separated by comma.	
+ Add - Delete		+ Add - Delete	
☐ INCLUDE CLIENT APPLICATION PROCESS NAME		☐ EXCLUDE CLIENT APPLICATION PROCESS NAME	
Enter the full path and process filename. For example, to add Skype on Windows, enter C:\Program Files\Microsoft Office\root\Office16\lync.exe		Enter the full path and process filename. For example, to add Skype on Windows, enter C:\Program Files\Microsoft Office\root\Office16\lync.exe	
+ Add - Delete		+ Add - Delete	

Domain and Application take precedence over Access Route. Application include and exclude list takes precedence over domain. Domains support wildcard prefixes in the left-most position (such as *.example.com). When you specify a wildcard domain for both include and exclude, the exclude domain takes precedence.

Gateway Configuration

Split Tunnel Rule Processing:



[Split Tunnel Behavior Doc](#)

Gateway Configuration

Client Settings (Cont.)

Config Selection Criteria	Authentication Override	IP Pools	Split Tunnel	Network Services
DNS Server	Enter comma-separated DNS server for client (e.g. 192.168.75.1, 2001:aa::1-2001:aa::10)			
DNS Suffix	Enter comma-separated DNS suffix for client (e.g. hr.mycompany.com, mycompany.com)			

Gateway Configuration

Agent: Client IP Pool

GlobalProtect Gateway Configuration

General
Authentication
Agent
Satellite

Tunnel Settings | Client Settings | **Client IP Pool** | Network Services | Connection Settings | Video Traffic | HIP Notifi

☐ IP POOL

Enter IP subnets or ranges (e.g. 192.168.74.0/24, 192.168.75.1-192.168.75.100)

+

Add

-

Delete

↑

Move Up

↓

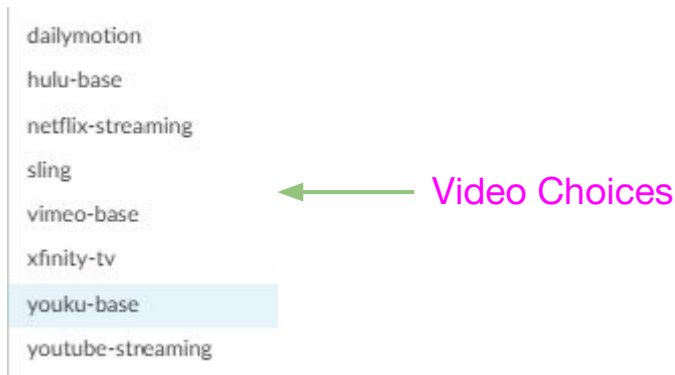
Move Down

These IPs will be added to the firewall's routing table

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

General
Authentication
Portal Data Collection
Agent
Clientless VPN
Satellite

Profile NameGP-Portal

Network Settings

Interfaceethernet1/1

IP Address TypeIPv4 Only

IPv4 Address10.4.0.2/30

Appearance

Portal Login Pagefactory default

Portal Landing Pagefactory-default

App Help PageNone

Log Settings

☐ Log Successful SSL Handshake

☒ Log Unsuccessful SSL Handshake

Log ForwardingNone

Portal Configuration

Authentication:

General

Authentication

Portal Data Collection

Agent

Clientless VPN

Satellite

Server Authentication

SSL/TLS Service ProfileGP-SSL-TLS-Profile

Client Authentication

	NAME	OS	AUTHENTIC... PROFILE	AUTO RETRIEVE PASSCODE	USERNAME LABEL	PASSWORD LABEL	AUTHENTI... MESSAGE	ALLOW AUTHENTI... WITH USER CREDENTI... OR CLIENT CERTIFICA...
☐	GP-Clients	Any	Auth_Profile	☐	Username	Password	Enter login credentials @ the portal.	Yes

+ Add

- Delete

🔄 Clone

↑ Move Up

↓ Move Down

Certificate ProfileGP-Cert-Profile

Portal Configuration

Agent:

GlobalProtect Portal Configuration

?

General

Authentication

Portal Data Collection

Agent

Clientless VPN

Satellite

Agent

☐	CONFIGS	USER/USER GROUP	OS	EXTERNAL GATEWAYS	CLIENT CERTIFICATE
☐	GP-Users	any	any	Jackson-GP-GW1 Jackson-GP-GW2	

Next Slide

☐ Add

☐ Delete

☐ Clone

☐ Move Up

☐ Move Down

☐	TRUSTED ROOT CA	INSTALL IN LOCAL ROOT CERTIFICATE STORE

☐ Add

☐ Delete

Agent User Override Key

Confirm Agent User Override Key

Portal Configuration

Agent: Agent Configuration

Configs



Authentication

Config Selection Criteria

Internal

External

App

HIP Data Collection

Name GP-Users

Client Certificate

None

The selected client certificate including its private key will be installed on client machines.

Save User Credentials Yes

Authentication Override

☐ Generate cookie for authentication override

☐ Accept cookie for authentication override

Cookie Lifetime

Hours

24

Certificate to Encrypt/Decrypt Cookie

None

Components that Require Dynamic Passwords (Two-Factor Authentication)

☐ Portal

☐ Internal gateways-all

☐ External gateways-manual only

☐ External gateways-auto discovery

Select the options that will use dynamic passwords like one-time password (OTP) to authenticate users as opposed to using saved credentials. As a result, the user will always be prompted to enter new credentials for each selected option.

Portal Configuration

Agent: Agent Configuration

Configs

Authentication | **Config Selection Criteria** | Internal | External | App | HIP Data Collection

User/User Group | Device Checks | Custom Checks

☒ Any	any
☐ OS ^	☐ USER/USER GROUP ^

+ Add - Delete

User/User Group | **Device Checks** | Custom Checks

Serial Number Check

Machine account exists with device serial number

Machine Certificate Check

Certificate Profile

User/User Group | Device Checks | **Custom Checks**

☐ Custom Checks

Registry Key | Plist

☐ REGISTRY KEY	(DEFAULT) VALUE DATA	NEGATE
---------------------------------------	----------------------	--------

+ Add - Delete

Portal Configuration

Agent: Agent Configuration

Authentication

Config Selection Criteria

Internal

External

App

HIP Data Collection

☐ Internal Host Detection IPv4

IP Address

▼

Hostname

▼

☐ Internal Host Detection IPv6

IP Address

▼

Hostname

▼

Internal Gateways

☐	NAME	ADDRESS	SOURCE IP	DHCP OPTION 43 CODE
				Specify one or more sub-option codes (in decimal). GlobalProtect Agent will read the gateway address from values defined by the sub-option codes.

+

Add

-

Delete

↑

Move Up

↓

Move Down

+

Add

-

Delete

Portal Configuration

Agent: Agent Configuration

Authentication | Config Selection Criteria | Internal | **External** | App | HIP Data Collection

Cutoff Time (sec) 5

External Gateways

☐	NAME	ADDRESS	PRIORITY RULE	M
☐	Jackson-GP-GW1	10.4.0.2	Any (Highest)	☐
☐	Jackson-GP-GW2	10.4.1.2	Any (Medium)	☐

Setting Priority for multiple gateways

THIRD PARTY VPN

Portal Configuration

Agent: Agent Configuration - [App Configurations Documentation](#)

Authentication | Config Selection Criteria | Internal | External | **App** | HIP Data Collection

App Configurations

Connect Method	User-logout (Always On)
GlobalProtect App Config Refresh Interval (hours)	24 [1 - 168]
Allow user to disconnect GlobalProtect App (Always-on mode)	Allow
Display the following reasons to disconnect GlobalProtect (Always-on mode)	
Allow User to Uninstall GlobalProtect App (Windows Only)	Allow
Allow User to Upgrade GlobalProtect App	Allow with Prompt
Allow user to Sign Out from GlobalProtect App	Yes
Allow user to extend	No

Welcome Page None

Disconnect GlobalProtect App (Always-on mode)

Passcode

Confirm Passcode

Max Times User Can Disconnect

Disconnect Timeout (min)

Uninstall GlobalProtect App

Uninstall Password

Confirm Uninstall Password

Mobile Security Manager Settings

Mobile Security Manager

Enrollment Port 443

Portal Configuration

Clientless VPN:

GlobalProtect Portal Configuration

General

Authentication

Portal Data Collection

Agent

Clientless VPN

Satellite

General

Applications

Crypto Settings

Proxy

Advanced Settings

☐ Clientless VPN

Hostname

None

FQDN or IP address of GlobalProtect Portal

Security Zones

None

DNS Proxy

Login Lifetime

Hours

3 [1 - 24]

Inactivity Timeout

Minutes

30 [5 - 1440]

Max User

[1 - 30000]

Portal Configuration

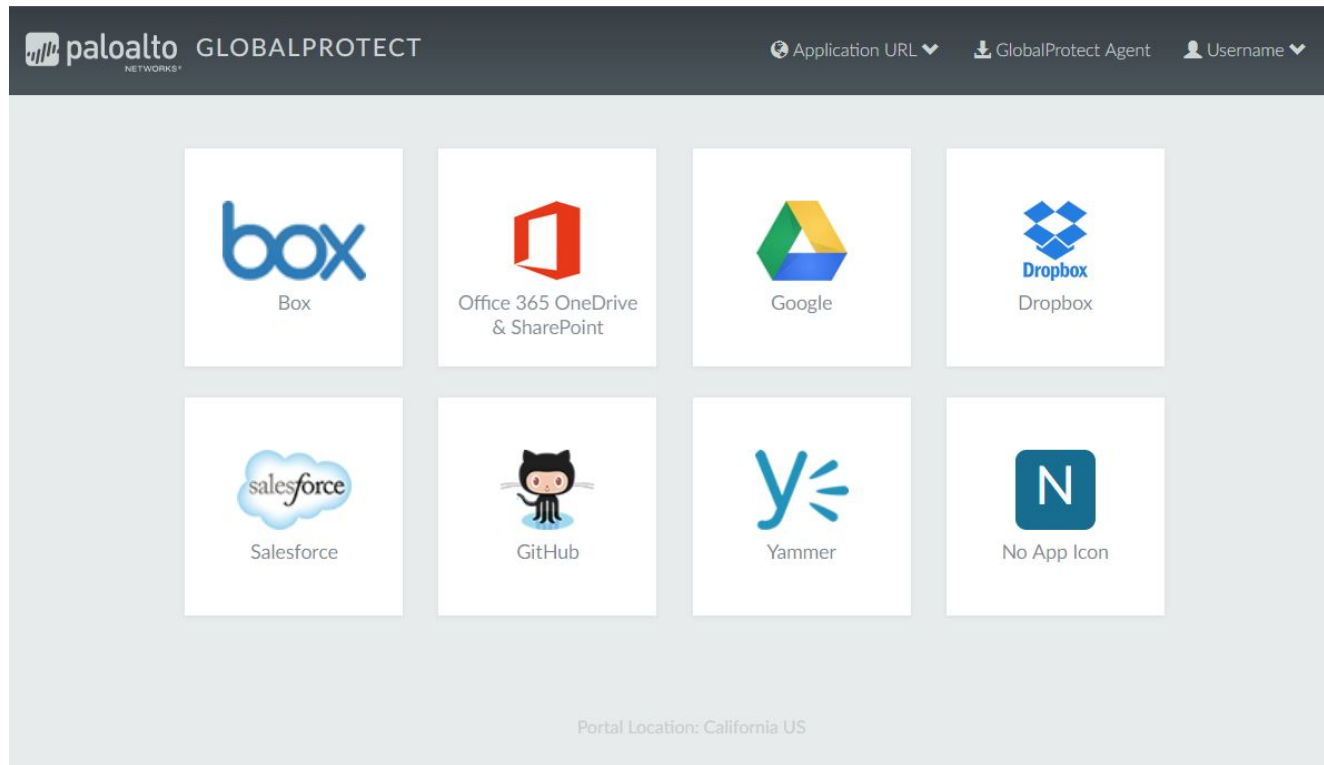
Clientless VPN: Applications

- 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

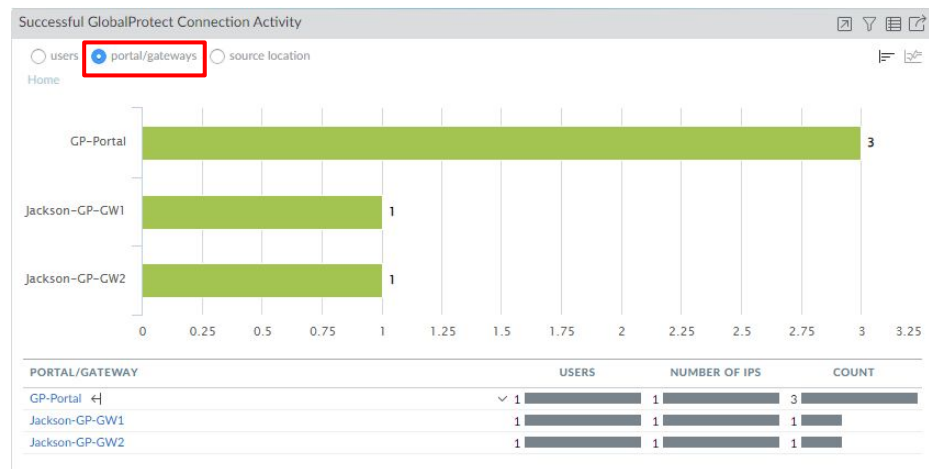
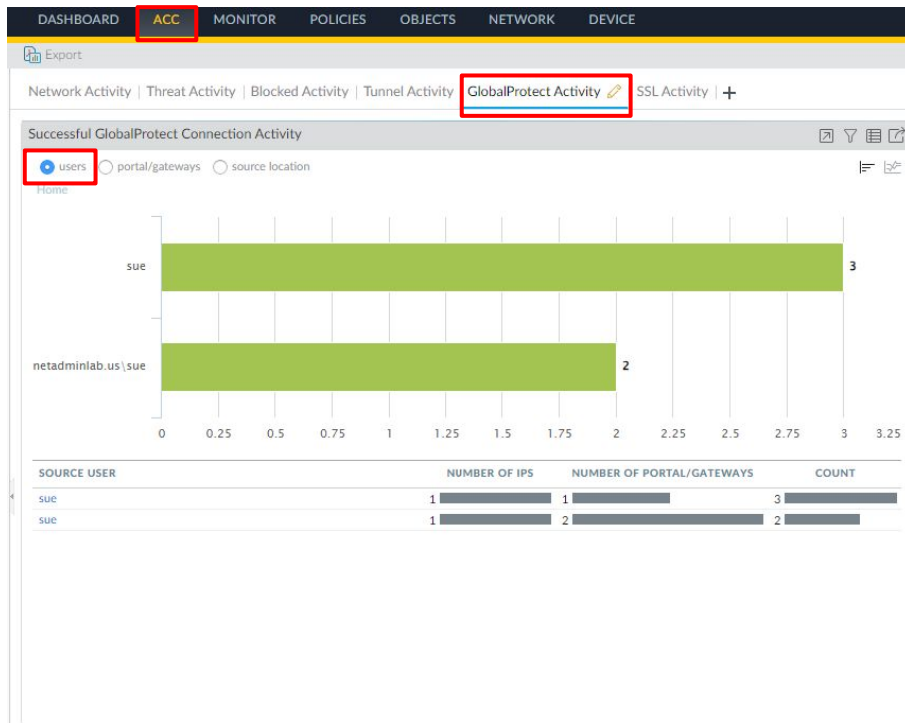
Troubleshooting

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

Q 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

