* Connect to a GlobalProtect portal.

Use the

globalprotect connect --portal

*<gp-portal>*

command where

*<gp-portal>*

is the IP address or FQDN of your GlobalProtect portal.

For example:

user@linuxhost:~$

globalprotect

connect --portal myportal.example.com

Retrieving configuration...

Disconnected

myportal.example.com - portal:local:Enter login credentials

username:user1

Password:

Retrieving configuration...

Discovering network...

Connecting...

Connected

When you use certificate-based authentication, the first time you connect without a root CA certificate, the GlobalProtect app and GlobalProtect portal exchange certificates. The GlobalProtect app displays a certificate error, which you must acknowledge before you authenticate. When you next connect, you will not be prompted with the certificate error message.

user@linuxhost:~$

globalprotect

connect --portal myportal.example.com

Retrieving configuration...

Disconnected

There is a problem with the security certificate, so the identity of 10.3.188.61 cannot be verified. Please contact the Help Desk for your organization to have the issue rectified.

Warning: The communication with 10.3.188.61 may have been compromised. We recommend that you do not continue with this connection.

Error details:Do you want to continue(y/n)?

y

Retrieving configuration...

Disconnected

10.3.188.61 - portal:local:Enter login credentials

username:

user1

Password:

Retrieving configuration...

Discovering network...

Connecting...

Connected

You can also specify a username in the command using the

--username

*<username>*

option. The GlobalProtect app prompts you to authenticate and, if you specified the username option, confirm your username.

* Import a certificate.

When you want to pre-deploy a client certificate to an endpoint for certificate-based authentication, you can copy the certificate to the endpoint and import it for use by the GlobalProtect app. Use the

globalprotect import-certificate --location

*<location>*

command to import the certificate on the endpoint. When prompted you must supply the certificate password.

user@linuxhost:~$

globalprotect

import-certificate --location /home/mydir/Downloads/cert\_client\_cert.p12

Please input passcode:

Import certificate is successful.

* Connect to a gateway.
  1. (

Optional

) Display the manual gateways to which you can connect using the

globalprotect show--manual-gateway

command.

* 1. Connect to a gateway using the

globalprotect connect--gateway

*<gp-gateway>*

command where

*<gp-gateway>*

is the IP address or FQDN of the GlobalProtect gateway.

* 1. View details about your connection using the

globalprotectshow --details

command.

* user@linuxhost:~$
* globalprotect show --manual-gateway
* Name Address
* ------------------------------
* gw1 192.168.1.180
* gw2 192.168.1.181
* user@linuxhost:~$
* globalprotect connect --gateway 192.168.1.180
* Retrieving configuration...
* Discovering network...
* Connecting...
* Connected
* Verify the status of and view details about your connection.

user@linuxhost:~$

globalprotect show --status

GlobalProtect status: Connected

user@linuxhost:~$

globalprotect show --details

Assigned IP address: 192.168.1.132

Gateway IP address: 192.168.1.180

Protocol: IPSec

Uptime(sec): 231

* Rediscover the network.

Use the

globalprotect rediscover-network

command to disconnect and reconnect from GlobalProtect.

user@linuxhost:~$

globalprotect

rediscover-network

Disconnecting...

Retrieving configuration...

Retrieving configuration...

Discovering network...

Connecting...

Connecting...

Connected

GlobalProtect status: Connected

* Clear the credentials for the current user.

Use the

globalprotect remove-user

command to clear the credentials used to authenticate with the portal and gateways. After you confirm that the GlobalProtect app should clear your credentials, the GlobalProtect app disconnects the tunnel and then requires you to enter your credentials the next time you connect.

user@linuxhost:~$

globalprotect

remove-user

Credential will be cleared and current tunnel will be terminated.

Do you want to continue(y/n)?

y

Clear is done successfully.

user@linuxhost:~$

globalprotect connect --portal 192.168.1.179

Retrieving configuration...

Disconnected

192.168.1.179 - portal:local:Enter login credentials

username:

user1

Password:

Retrieving configuration...

Discovering network...

Connecting...

Connected

* Resubmit host information to the gateway.

Use the

globalprotect show --host-state

command the current host information about your endpoint and the

globalprotectresubmit-hip

command to resubmit information about the endpoint to the gateway. This is useful in cases where HIP-based security policy prevents users from accessing resources because it allows the user to fix the compliance issue on the endpoint and then resubmit the HIP.

user@linuxhost:~$

globalprotect

show --host-state

generate-time: 09/28/2017 11:24:07

categories

host-info

client-version: 4.1.0

os: Linux Ubuntu 16.04.3 LTS

os-vendor: Linux

domain:

host-name: linuxhost

host-id: 4C4C4544-0034-4D10-804C-\*\*\*\*\*\*\*\*\*\*\*\*

network-interface

enp0s31f6

description: enp0s31f6

mac-address: D4:81:D7:D4:5A:A5

wlp2s0

description: wlp2s0

mac-address: 14:AB:C5:DE:D1:0E

user@linuxhost:~$

globalprotect resubmit-hip

Resubmit is successful.

* View any GlobalProtect notifications.

Use the

globalprotect show --notification

command to view notifications.

* View the Welcome page.

Use the

globalprotect show --welcome-page

command. The GlobalProtect app displays the Welcome page in a browser if a Welcome page exists or displays a notification if the Welcome page does not exist.

* View errors.

Use the

globalprotect show --error

command to view errors reported by the app.

user@linuxhost:~$

globalprotect

show --error

Error: Cannot connect to GlobalProtect Portal

* Collect logs.

The app stores the PanGPA and PanGPI log files in the

/home/

*<user>*

/.Globalprotect

directory. Use the

globalprotect collect-logs

command to enable the GlobalProtect app for Linux to package these logs and other useful information. You can then use the logs to troubleshoot issues or forward them to a Support engineer for expert analysis.

user@linuxhost:~$

globalprotect

collect-log

Start collecting...

collecting network info...

collecting machine info...

copying files...

generating final result file...

The support file is saved to /home/user/.GlobalProtect/Collect.tgz

* Display the version of the GlobalProtect app for Linux.

user@linuxhost:~$

globalprotect show --version

GlobalProtect: 4.1.0-23

Copyright(c) 2009-2017 Palo Alto Networks, Inc.