



Manual Chapter : Clients for Linux

Applies To:

Show Versions



Clients for Linux

About Linux clients

Access Policy Manager (APM) supports two Linux clients, a CLI and Network Access client components for browser-based access. On the CLI for Linux, APM supports logon with user name and password only and does not support any endpoint security features.

On the client component for Linux, APM supports all of the primary Network Access features, except for Drive Mappings and some endpoint security features. For endpoint security support for the web client for Linux, refer to *BIG-IP APM Client Compatibility Matrix* on AskF5 at <http://support.f5.com/>. For information about Network Access features, refer to *BIG-IP Access Policy Manager: Network Access* on AskF5 at <http://support.f5.com/>.

About browser-based connections from Linux, Mac, and Windows clients

For Linux, Mac OS X, and Windows-based systems, the Network Access client component is available for automatic download from the BIG-IP[®] system.

The client component supports secure remote web-based access to the network. It is not the same as the customizable client package that is associated with the connectivity profile.

The first time a remote user starts Network Access, APM[®] downloads a client component. This client component is designed to be self-installing and self-configuring. If the browser does not meet certain requirements, APM prompts the user to download the client component and install it manually.

Requirements for client installation and use on Linux

The table lists requirements for installing Network Access client components on a Linux system and using them for web-based access.

Requirement	Specification
Browser	Use Firefox for installing the client component. The browser must support the installation of plugins.
Firewall settings	If you have a firewall enabled [®] on your Linux system, you must enable access on IP address 127.0.0.1, port 44444.

Requirement	Specification
PPP	The system must support PPP. (This is usually the case.) The user must have permission to run the PPP daemon.
Installation privilege	The remote user must have superuser authority, or, must be able to supply an administrative password to successfully install the Network Access client.

About Network Access features for Linux clients

Access Policy Manager (APM) supports two Linux clients, a CLI and Network Access client components that support web-based access. On the CLI for Linux, APM supports logon with user name and password only and does not support any endpoint security features.

With the web-based client components for Linux, APM supports all of the primary Network Access features, except for Drive Mappings and some endpoint security features. For endpoint security support for the web client for Linux, refer to *BIG-IP APM Client Compatibility Matrix* on AskF5 at <http://support.f5.com/>. For information about Network Access features, refer to *BIG-IP Access Policy Manager: Network Access* on AskF5 at <http://support.f5.com/>.

Specifying applications to start on a Linux client

You can specify applications to start when the client begins a Network Access session. You might do this when you have remote clients that routinely use Network Access to connect to an application server, such as a mail server.

1. On the Main tab, click **Access** > **Connectivity / VPN** > **Network Access (VPN)** > **Network Access Lists** .
The Network Access Lists screen opens.
2. In the Name column, click the name of the network access resource you want to edit.
3. To configure applications to start for clients that establish a Network Access connection with this resource, click **Launch Applications** on the menu bar.
4. Click **Add** to add an application list.
A screen opens showing the Add Application To Launch area.
5. In the **Application Path** field type an application to launch.
For example, type `/usr/bin/mozilla` to start Mozilla.
6. In the **Parameters** field, type a parameter.
For example, type `http://www.f5.com`.
7. From the **Operating System** list, select **Unix**.
8. Click **Finished** to add the configuration.

Now, when remote users with assigned resources make a Network Access connection, the application you configured starts automatically.

Overview: Installing and using the CLI for Linux

The BIG-IP[®] Access Policy Manager[®] includes a CLI for Linux. With the CLI, users can initiate VPN connections through APM[®] from the command line. You can download and deploy this client to your organization's Linux desktops.

Task summary

Downloading the Linux command line client

Beginning with BIG-IP 14.1.0, you can directly download the **Command Line Client for Linux** installer packages in either *rpm* and *deb* format and distribute it to clients for installation.

1. On the Main tab, click **Access > Connectivity / VPN > Connectivity > Client Downloads** .
A list of available client downloads displays.
2. Click the required **Command Line Client for Linux rpm/deb** file to download.
The *rpm/deb* file is downloaded to your local directory. Open the package using software installer and proceed with the installation or you may choose to use command line utility to install the package.

Importing a certificate to the local trust store

You can import an untrusted certificate to the local trust store and change it into a trusted certificate.

1. Using operating system commands, place the certificate in any folder in the operating system.
For example, `/etc/certs`.
2. Change the directory.
For example, `cd /etc/certs`.
3. Type the command `c_rehash ./`.

The certificate is installed.

Alternatively, instead of installing the certificate, you can specify the `--cacert` option to import a certificate to the local store.

Linux client commands

The following commands are supported by the Linux command line client. All commands that are invoked on the Linux command line client begin with the command `f5fpc`.

To start a VPN connection, type either of the following commands:

- `f5fpc --start [arguments]`
- `f5fpc -s [arguments]`

This requires the `--host` or `-t` argument at the minimum.

Use the following table to assign arguments to the Linux commands.

Arguments	Description
<code>--non-block</code> <code>-b</code>	Returns the command line interface immediately after the command.
<code>--host [https://]hostname[:port]</code> <code>-t [https://]hostname[:port]</code>	The host name to which the client starts the VPN connection. This is required.

Arguments	Description
<pre>-- user user- name -u user- name</pre>	<p>The optional user name for the connection.</p>
<pre>-- pass- word pass- word p pass- word</pre>	<p>The optional password for the connection.</p>
<pre>--user- hex hex- en- coded- user- name -U hex- en- coded- user- name</pre>	<p>The optional hex-encoded user name for the connection.</p>
<pre>-- pass- word- hex hex- en- coded- pass- word -P hex- en- coded- pass- word</pre>	<p>The optional hex-encoded password for the connection.</p>

Arguments	Description
--cert cer- tifi- cate -r cer- tifi- cate	Specifies an optional client certificate.
--key certificate_key -k certificate_key	Specifies the key for an optional client certificate.
--keypass SSL_certificate_password -y SSL_certificate_password	Specifies the password for an optional SSL certificate.
--cacert trusted_CA_certificate -a trusted_CA_certificate	Specifies a certificate from a trusted certificate authority (CA). If --cacert or --cacertdir is specified, then the server certificate validates for trust against the specified certificate or directory. If --cacert or --cacertdir is not specified, then the default location <code>/etc/ssl/certs</code> is checked to verify trust. The --nocheck option can be specified if a server certificate check is not desired, though this is not recommended.
--cacertdir trusted_CA_certificate_directory -d trusted_CA_certificate_directory	Specifies a certificate directory that contains a certificate from a trusted CA. If --cacert or --cacertdir is specified, then the server certificate validates for trust against the specified certificate directory. If --cacert or --cacertdir is not specified, then the default location <code>/etc/ssl/certs</code> is checked to verify trust. The --nocheck option can be specified if a server certificate check is not desired, though this is not recommended.
--nocheck -x	Specifies that the trusted CA certificate is not verified for trust at all. If --cacert or --cacertdir is specified, then the server certificate validates for trust against the specified certificate or directory. If --cacert or --cacertdir is not specified, then the default location <code>/etc/ssl/certs</code> is checked to verify trust. The --nocheck option can be specified if a server certificate check is not desired, though this is not recommended.

To stop the VPN connection, type either of the following commands:

- `f5fpc --stop`
- `f5fpc --o`

To display the connection status, type either of the following commands:

- `f5fpc --info`
- `f5fpc --i`

To display the command line client help, type either of the following commands:

- `f5fpc --help`

- f5fpc --h

Info command status and error codes

The following status codes and error codes might be displayed when you run the --info command.

Error code/command status	Hex value	Shell value	Description
CLI_ERROR_SUCCESS	0x0	0	The command line operation was successful.
CLI_ERROR_USERS_DISCONNECT	0x150	80	The user was disconnected
CLI_ERROR_LOGON_FAILURE	0x151	81	Login failed due to incorrect authentication information or login errors.
CLI_ERROR_ATTENTION_REQUIRED	0x154	84	The user's attention is required.
CLI_ERROR_GENERIC_FAILURE	0x155	85	An error occurred in the system API.
CLI_ERROR_UNKNOWN_PARAMETER	0x156	86	An incorrect or unknown parameter was passed to the command line.
CLI_ERROR_WRONG_VALUE	0x157	87	This is an undefined error.
CLI_ERROR_UNKNOWN_SESSION_ID	0x158	88	An unknown session ID was encountered. The user should reconnect to the server.
CLI_ERROR_NO_PROFILE	0x15B	91	No such profile exists.
CLI_ERROR_MSGQ_OPEN_FAILURE	0x15D	93	The system failed to open the message queue.
CLI_ERROR_OPERATION_IN_PROGRESS	0x15F	95	An operation is in progress, please retry.
kss_Initialized	1	1	The session is initialized.
kss_LogonInProgress	2	2	The user login is in progress.
kss_Idle	3	3	The session is idle.
kss_Established	5	5	The session is established.
kss_AttentionReq	6	6	The session requires the user's attention.
kss_LogonDenied	7	7	Login was denied.
kss_LoggedOut	8	8	The user is logged out of the server.

Editing the log level for Edge Client on Linux

You can edit log settings in the configuration file on Linux systems.

1. In the `/usr/local/lib/F5Networks` directory, open the `f5networks.conf` file.
2. Edit the settings to change the log level.

By default, the values are 0 (zero). For debugging purposes, set the values to 5.

VPN component installation and log locations on Linux

On Linux operating systems, the client installs the VPN components and writes VPN logs to the locations listed in the table.

Category	Location
VPN component	<code>/usr/local/lib/F5Networks</code>
VPN logs	<code>~/.F5Networks</code>

[Contact Support](#)

HAVE A QUESTION?

[Support and Sales >](#)

FOLLOW US

