

## Manual Chapter : BIG-IP Edge Command Line Client for Linux

**Applies To:**

Show Versions 



[Table of Contents](#) | [<< Previous Chapter](#) | [Next Chapter >>](#)

### About BIG-IP Edge Client for Linux command line

The BIG-IP® Access Policy Manager® includes a BIG-IP Edge Client® command line for Linux. You can download and deploy this client to your organization's Linux desktops.

#### Task summary

##### Downloading the Linux command line client

You can download the BIG-IP® Edge command line client for Linux installer, as a gzipped .TAR file, and distribute it to clients for installation.

1. On the Main tab, click **Access Policy > Secure Connectivity > Client Downloads**. A list of available client downloads displays.
2. Click **BIG-IP Edge Command Line Client for Linux**. The file `linux_sslvpn.tgz` is downloaded to your local directory.

The Linux command line client is ready to be installed.

##### Installing the Linux command line client

You must download the file `linux_sslvpn.tgz` before you can install the command line client.

You can use various Linux client commands with the BIG-IP® Edge command line client for Linux.

1. Extract the file `linux_sslvpn.tgz` to your local directory.
2. Extract the file `linux_sslvpn.tar` to your local directory.
3. Run the install script `Install.sh` under the root account.

The following text appears when installation is complete:

```
--> f5fpc is installed in /usr/local/bin
--> Please check f5fpc --help command to get started
--> Uninstaller located in /usr/local/lib/F5Networks/uninstall_F5.sh
```

##### 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.

**Note:** 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]`

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

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

Arguments	Description
<code>--nonblock</code> <code>-b</code>	Returns the command line interface immediately after the command.
<code>--host [https://]hostname[:port]</code> <code>-t</code> <code>[https://]hostname[:port]</code>	The host name to which the client starts the VPN connection. This is required.
<code>--user username</code> <code>-u username</code>	The optional user name for the connection.
<code>--password password</code> <code>p password</code>	The optional password for the connection.
<code>--userhex hex-encoded-username</code> <code>-U hex-encoded-username</code>	The optional hex-encoded user name for the connection.
<code>--passwordhex hex-encoded-password</code> <code>-P hex-encoded-password</code>	The optional hex-encoded password for the connection.
<code>--cert certificate</code> <code>-r certificate</code>	Specifies an optional client certificate.

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

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.