



Configuring Host Input Clients

In addition to accepting host input commands from users on the Defense Center, the Defense Center's host input service also accepts batch import files from authenticated host input clients on external hosts. You can use a host input client to process import files created for the host input import tool and then send the data to the Defense Center to add the information to your network map.

You can use the provided host input API reference client to process and send CSV data or to test your host input client connection to the Defense Center.

Perform the following tasks to manage Defense Center and input client interaction:

1. Establish an authenticated connection to the Defense Center.

See [Registering the Host Input Client with the Defense Center, page 4-1](#) for information about generating authentication credentials to establish an authenticated connection to the Defense Center.

2. Set up a host input client:

- To use the Cisco-provided host input reference client, set up the reference client on the computer where you plan to run it. For more information, see [Using the Host Input Reference Client, page 4-2](#).

For information on creating import files (also referred to as command files) that you will use your reference client to process, see [Writing Host Input Import Files, page 3-3](#).

- To use your own custom client, make sure it can locate and process the certificate to connect to the Defense Center. For information, see [Registering the Host Input Client with the Defense Center, page 4-1](#).

Registering the Host Input Client with the Defense Center

License: FireSIGHT

Before you can use a host input client, you must register the computer on which the client runs with the Defense Center. The Defense Center then generates an authentication certificate, which you download to your client computer.

To add a host input client:

Access: Admin

1. Select **Local > Registration > Host Input Client**.

The Host Input Client page appears.

2. Click **Create Client**.


The Create Client page appears.

3. In the **Hostname** field, enter the host name or IP address of the host running the host input client.


Note: If you use a host name, the host input server **must** be able to resolve the host to an IP address. If you have not configured DNS resolution, you should configure it first or use an IP address.

4. If you want to encrypt the certificate file, enter a password in the **Password** field.
5. Click **Save**.

The host input service allows the client computer to access port 8307 on the Defense Center and creates an authentication certificate to use during client-server authentication. The Host Input Client page re-appears, with the new client listed under **Host Input Clients**.

6. Click the download icon () next to the certificate file.
7. Save the certificate file to the directory used by your client computer for SSL authentication.

The client can now connect to the Defense Center.

Note: To revoke access for a client, click the delete icon () next to the host you want to remove. Note that you do not need to restart the host input service on the Defense Center; access is revoked immediately.

Connecting the Client to the Defense Center

The host input service on the Defense Center reads a version from the client when the client connects. If the client sends a version newer than the version of the server, the service rejects the connection.

In addition, during the initial exchange, the host input service communicates the maximum allowed data size per transaction to the client. If the client attempts to send a data block bigger than the maximum size, the server closes the connection.

Using the Host Input Reference Client

The reference client provided with the host input SDK is a set of sample client scripts and Perl modules that illustrate how you can use the host input API. You can run them to familiarize yourself with host input import, or you can use them to debug problems with installations of your custom-built client. You can also use one of the scripts to process a host input command file from the client.

For more information on setting up reference clients, see the following sections:

- [Setting Up the Host Input Reference Client, page 4-2](#)
- [Running the Host Input Reference Client, page 4-4](#)

Setting Up the Host Input Reference Client

To use the host input reference client, you must first install the sample scripts and configure your client to fit the script requirements.

For more information, see the following sections:

- [Understanding the Host Input Reference Client, page 4-3](#)
- [Configuring Communications for the Host Input Reference Client, page 4-3](#)

- [Loading General Prerequisites for the Host Input Reference Client, page 4-3](#)
- [Downloading and Unpacking the Host Input Reference Client, page 4-4](#)
- [Creating a Certificate for the Host Input Reference Client, page 4-4](#)

Understanding the Host Input Reference Client

You can download the `HostInputClientSDK.zip` package, which contains the host input reference client, from the [Cisco support site](#). The [Table 4-1 Host Input Reference Client Files, page 4-3](#) lists the files included in the `HostInputClientSDK.zip` package.

Table 4-1 *Host Input Reference Client Files*

Filename	Description
SFHIClient.pm	This Perl module contains the functions called by the Perl clients.
SFPkcs12.pm	This Perl module parses the client certificate and allows the client to connect to the Defense Center.
ssl_host_input_api_test.pl	You can use this Perl script to import CSV data by specifying the appropriate input plugin and a command file.
InputPlugins/csv.pm	You can call this Perl module to run a command file that imports CSV data.

Configuring Communications for the Host Input Reference Client

The reference client uses the Secure Sockets Layer (SSL) protocol for data communication. You must install OpenSSL on the computer you plan to use as a client and configure it appropriately for your environment.

To set up SSL on your client:

1. Download OpenSSL from <http://openssl.org/source/>.
2. Unpack the source to `/usr/local/src`.
3. Configure the source by running the `Configure` script.
4. Make and install the compiled source.

Loading General Prerequisites for the Host Input Reference Client

Before you can run the host input reference client, you must install the `IO::Socket::SSL` Perl module on the client computer. You can install the module manually or use `cpan` to do so.

Note: If the `Net::SSLLeay` module is not installed on the client computer, install that module as well. `Net::SSLLeay` is required for communication with OpenSSL.

You also need to install and configure OpenSSL to support an SSL connection to the Defense Center. For more information, see [Configuring Communications for the Host Input Reference Client, page 4-3](#).

In addition, if you plan to use the Qualys plugin with the host input client, you must install the `XML::Smart` Perl module and its prerequisites. If you plan to use IPv6 to communicate between the client and the Defense Center, you must also install the `IO::Socket::INET6` Perl module.

Downloading and Unpacking the Host Input Reference Client

You can download the `HostInputClientSDK.zip` file that contains the host input reference client from the Support site.

Unpack the zip file to a computer running the Linux operating system, where you plan to run the client.

Creating a Certificate for the Host Input Reference Client

License: FireSIGHT

Before you can use the host input reference client, you need to create a certificate on the Defense Center for the computer where you want to run the client. You then download that file to the client computer.

To create a certificate for the reference client:

Access: Admin

1. Select **Local > Registration > Host Input Client**.

The Host Input Client page appears.

2. Click **Create Client**.


The Create Client page appears.

3. In the **Hostname** field, enter the host name or IP address of the host running the host input reference client.

If you use a host name, the Defense Center **must** be able to resolve the host to an IP address. If you have not configured DNS resolution on the Defense Center or if a reverse lookup is not available, you should configure DNS first or use an IP address. Refer to the *FireSIGHT System User Guide* or the online help for more information about configuring DNS settings.

4. Click **Save**.

The Defense Center now allows the host to access the Defense Center and creates an authentication certificate to use during client-server authentication. The Host Input Client page appears again, with the new client listed under **Hostname**.

5. Click the download icon () next to the client hostname to download the certificate file.
6. Save the certificate file to the directory where you put the reference client.

The client can now connect to the Defense Center. You do not need to restart the host input service.

Note: To revoke access for a client, click **Delete** next to the host you want to remove. Note that you do not need to restart the host input service on the Defense Center; access is revoked immediately.

Running the Host Input Reference Client

The Host Input Perl reference client scripts are designed for use on an operating system with the Linux kernel but should work on any POSIX-based operating system, as long as the client machine meets the prerequisites defined in [Setting Up the Host Input Reference Client, page 4-2](#).

You can use the reference client to import CSV data from a remote client to the network map on a Defense Center.

Use the following syntax to run the `ssl_host_input_api_test.pl` script:

```
./ssl_host_input_api_test.pl csv CSVCommandFile Defense Center IPAddress
```

For example, to import using a CSV file named `csv_file.txt` to a Defense Center with an IP address of 10.10.0.4:

```
./ssl_host_input_api_test.pl csv csv_file.txt 10.10.0.4
```

