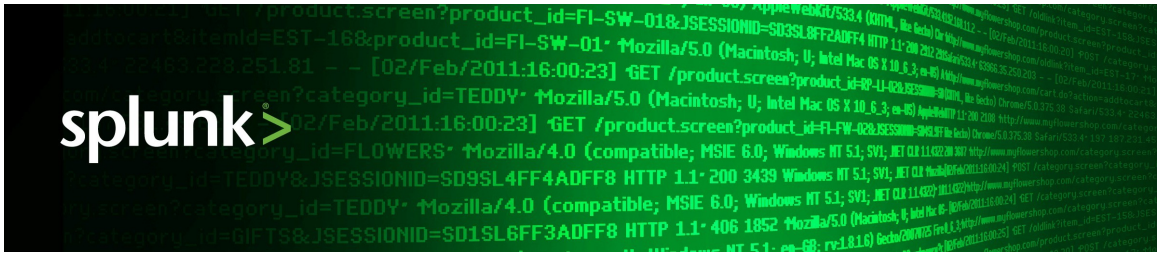

Splunk® Universal Forwarder Forwarder Manual 6.5.0

Control forwarder access

Generated: 10/19/2016 9:56 pm

Control forwarder access

If you have Splunk Enterprise, you can control how forwarders connect to receiving indexers with tokens. When you assign a token to a receiving indexer, any forwarders that connect to it must provide that token before they can forward data to it. Forwarder access control is different than a Secure Sockets Layer configuration and can be used in environments that do not have SSL enabled between Splunk instances.

Prerequisites to configuring forwarder access control

You must use the REST API to create, configure, and delete tokens. The commands in this topic use the `curl` command-line tool.

While this tool is available on most *nix systems, you must download a separate executable on Windows systems as there is no native default. You can get it at the cURL website.

You must reference tokens with configuration files.

Forwarder-indexer communication

When you configure tokens on the universal forwarder and indexer, the following communication happens when a forwarder connects to send data:

- The forwarder connects to the indexer.
- The indexer requests authentication.
- The forwarder provides the token to the indexer.
- The indexer compares the token it received with the token it has.
- If the tokens match, the indexer accepts the connection and sets up the data stream.
- If the tokens do not match, the indexer rejects the connection and logs an entry in `splunkd.log`.

Generate a token

Before you can configure token-based forwarding, you must generate at least one token to use.

1. From a command or shell prompt on the indexer where you want to generate the token, use the REST API to connect to a Splunk Enterprise indexer to create the token:

```
curl -v -k -u <user>:<password>
https://<host>:<management_port>/services/data/inputs/tcp/splunktcptoken
-d "name=<name>"
```
In this command:

- `user` and `password` are the credentials you use to log into the Splunk Enterprise indexer.
- `host` is the host name or IP address of the indexer.
- `management_port` is the TCP management port on the indexer.
- `name` is the friendly name that you want to assign the token.

For example, to create a token called `my_token` on the `idx1.mycompany.com` instance with the standard user and password for the `admin` user:

```
curl -v -k -u admin:changeme
https://idx1.mycompany.com:8089/services/data/inputs/tcp/splunktcptoken
-d "name=my_token"
```
The host responds with:

```
token=808F7BD7-1444-4910-B8F5-87B83D694E18
```
This is the Globally Unique Identifier (GUID).

Enable a token

1. From a command or shell prompt, run:

```
curl -v -k  -X "POST" -u <user>:<password>
https://idx1.mycompany.com:8089/services/data/inputs/tcp/splunktcptoken/tok1/enable
```
Disable a token

1. From command or shell prompt, run:

```
curl -v -k  -X "POST" -u <username>:<password>
https://idx1.mycompany.com/services/data/inputs/tcp/splunktcptoken/my_token/disable
```
Delete a token

To change a token, issue the following command:

```
curl -v -k -X "DELETE" -u <username>:<password>
https://idx1.mycompany.com:8089/services/data/inputs/tcp/splunktcptoken/my_token
```

Configure the indexer with the token

Before you can control forwarders with tokens, set up the indexer with the token you generated. Edit inputs.conf on the forwarder to specify a special stanza along with the token that you generated.

1. Configure the forwarder as a receiving indexer.

2. From a shell or command prompt on the indexer, edit `inputs.conf`:

```
vi $SPLUNK_HOME/etc/system/local/inputs.conf
```

3. In this file, add the following stanza:

```
[splunktcptoken://my_token]
disabled = 0
token = 808F7BD7-1444-4910-B8F5-87B83D694E18
```

4. Save `inputs.conf` and close it.

5. Restart the indexer.

Configure the forwarder with the token

Configure forwarders with the new token. You can specify tokens in `tcpout` and load balancing groups. See Configure forwarding with outputs.conf.

1. From a shell or command prompt on the forwarder, edit `outputs.conf`:

```
vi $SPLUNK_HOME/etc/system/local/outputs.conf
```

2. Add the following stanza:

```
[tcpout]
server=idx1.mycompany.com:9997
token = 08F7BD7-1444-4910-B8F5-87B83D694E18
...
```

3. Save the file and close it.

4. Restart the universal forwarder.

Confirm that the forwarder and indexer can communicate with the tokens

On the indexer, review `splunkd.log` for information about forwarder attempts to communicate with an indexer that has tokens enabled.

A forwarder that does not have the correct token generates this output:

```
ERROR TcpInputProc - Exception: Token sent by forwarder does not match
configured tokens src=127.0.0.1:58798! for data received from
src=127.0.0.1:58798
```

A forwarder that does not submit a token to an indexer that has an enabled token generates this output:

```
ERROR TcpInputProc - Exception: Token not sent by forwarder
src=127.0.0.1:58796! for data received from src=127.0.0.1:58796
```

In either case, the indexer terminates the connection to the forwarder.

A forwarder that does not submit the right token to an indexer that asks for one does not generate an error. It does not forward data to that indexer.