Authentication

The authentication flow is modeled on that of SSH, specifically using keyfiles. The steps involved in authentication are as follows:

1. Install Network Fandango
2. Set up your Network Discovery
3. The first time the Network Fandango service (`nfsvc`) is started, it will create a root CA certificate, a TLS certificate and a JWT certificate.
4. You must copy the root CA certificate (`ca.pem`) to your workstation. Put it in `~/.nf/certs/[server]`
5. On your workstation, install the Network Fandango client tools
6. On your workstation, run `nf`

When you do this, `nf` will:

- Discover your server
- Verify that the server's TLS certificate is signed by the root CA certificate you copied to your workstation
- Create a public and private key file (in `~/.nf/certs/[server]`)
- Request a nonce from the server
- Sign the nonce using the private key
- Submit the signed nonce, public key and your username to the server

Because this is the first login, the key will be accepted without question, and the initial user account created. Your public key will be stored for future use.

The server will respond with a JWT token, signed with the JWT certificate. `nf` will verify the JWT against the JWT certificate by requesting it from the server's JWKS endpoint.

`nf` will cache the JWT, which are valid for 8 hours by default.

On subsequent requests to the server, `nf` will detect that the JWT exists and attempt to verify it. If it fails, it will repeat the above process. The difference is that the provided public key must match the previously provided one because this is not the first login.

Subsequent users must be made manually by the initial user. You have two options for doing this:

1. The first time the user logs in, their key is accepted without quesion.
2. You set a one time password on the new user, and the first time the user connects, they must provide this or their key will not be accepted. The password is not required for future use of the `nf` command line tool.

The authentication flow for the web app has not yet been designed.

Revision #4
Created 11 August 2025 02:00:44 by Neil Bullock
Updated 6 September 2025 17:16:35 by Neil Bullock