

Enterprise Deployment Options

1. Introduction

For large-scale deployments of Moonshot authentication, it is recommended that user credentials are pre-provisioned, i.e. that users are issued with a credential file that is imported into their local keyring and/or local identity storage. This method also allows the deployment of trust anchors, without which credentials could be exposed to malicious resource providers.

2. Moonshot Credential Files (.msht)

The Moonshot credential file is simple XML. The format of the file is described on the [Moonshot identity file format](#) page.

A sample of the file can be found at `/usr/share/moonshot-ui/default-identity.msht`

This credential format is also used to secure communication between RPs, IdPs and trust routers in the Moonshot infrastructure.

The Moonshot credential file may contain multiple identities.



Keeping identity files safe

Identity files are simple XML, which may include passwords in plain-text (encoded for valid XML). As such, credential files should be kept safe.

3. Importing Credential Files

3.1. Linux

Moonshot ships with a tool, `moonshot-webp`, to securely and correctly provision credentials onto clients.

The command-line of the tool is very simple:

moonshot-webp command-line

```
moonshot-webp [-f] credential-file.xml
```

The optional `-f` parameter directs the tool to store the credential in `identities.txt` instead of the keyring (the default).

3.2. macOS

The Moonshot Identity Manager for macOS currently does not support automatic provisioning of credentials onto clients.

To provision credentials, open the Moonshot Identity Manager app and click the Import button to select an identity file to import.