Configure the Moonshot SSP

The Moonshot Security Support Provider (SSP) on Windows has various configuration options. This page documents these options, including how to manually add account mappings.

Contents

1. Configuration Tools

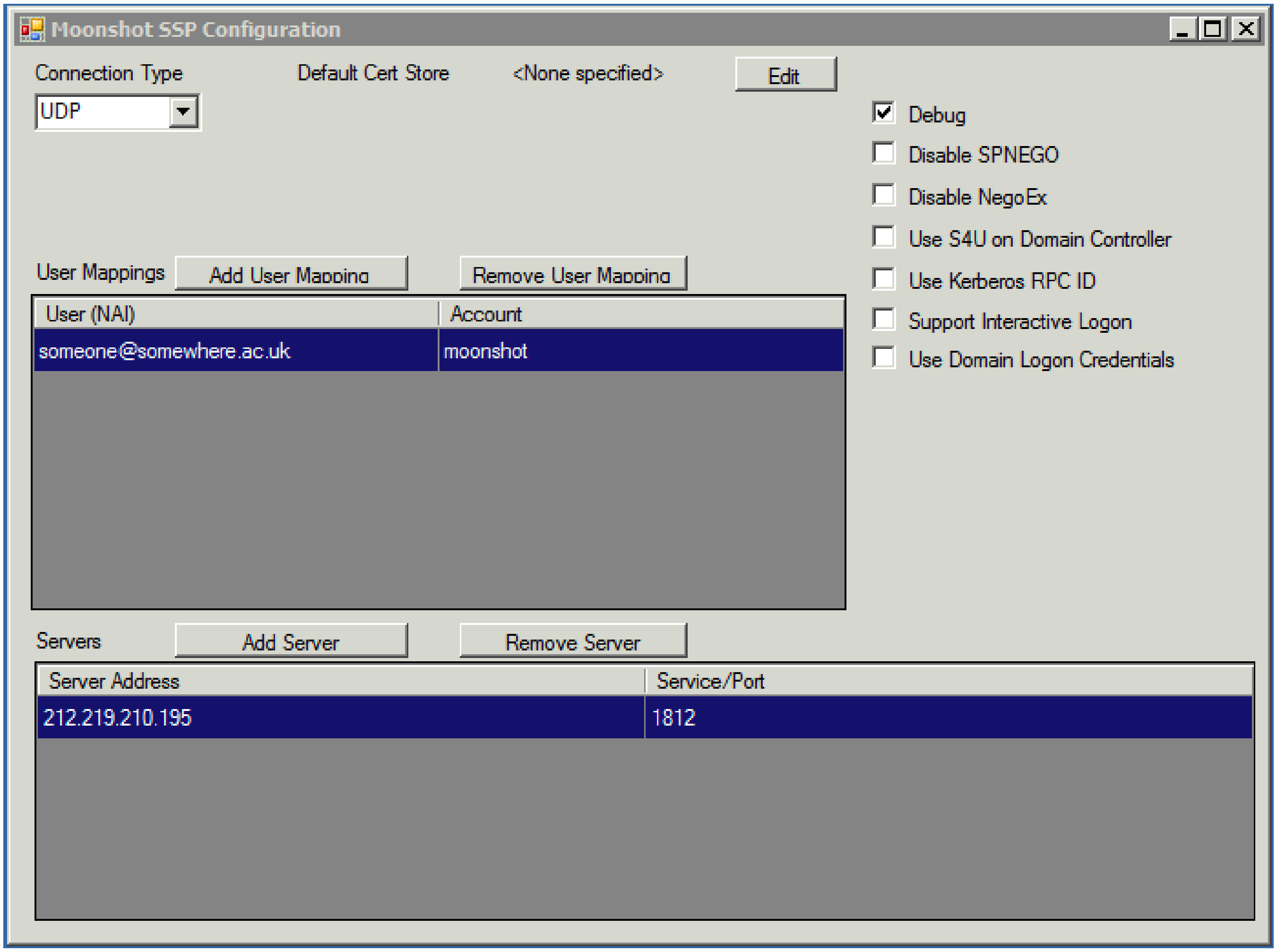
The Moonshot SSP ships with two tools for configuring the SSP. One is a GUI, and one a CLI. These tools allow you to:

- Set various configuration options about the way the SSP operates
- Configure your connection to a Moonshot RP Proxy
- Add manual account mappings.

1.1. The GUI - msetupgui.exe

The default location for the SSP setup GUI is `C:\Program Files\Moonshot\msetupgui.exe`.

To set the options as documented in Section 2, simply click to turn them on and off. Note that all settings require a reboot to take effect.



Moonshot SSP Configuration

Connection Type
UDP

Default Cert Store <None specified>

☑ Debug
☐ Disable SPNEGO
☐ Disable NegoEx
☐ Use S4U on Domain Controller
☐ Use Kerberos RPC ID
☐ Support Interactive Logon
☐ Use Domain Logon Credentials

User Mappings

User (NAI)	Account
someone@somewhere.ac.uk	moonshot

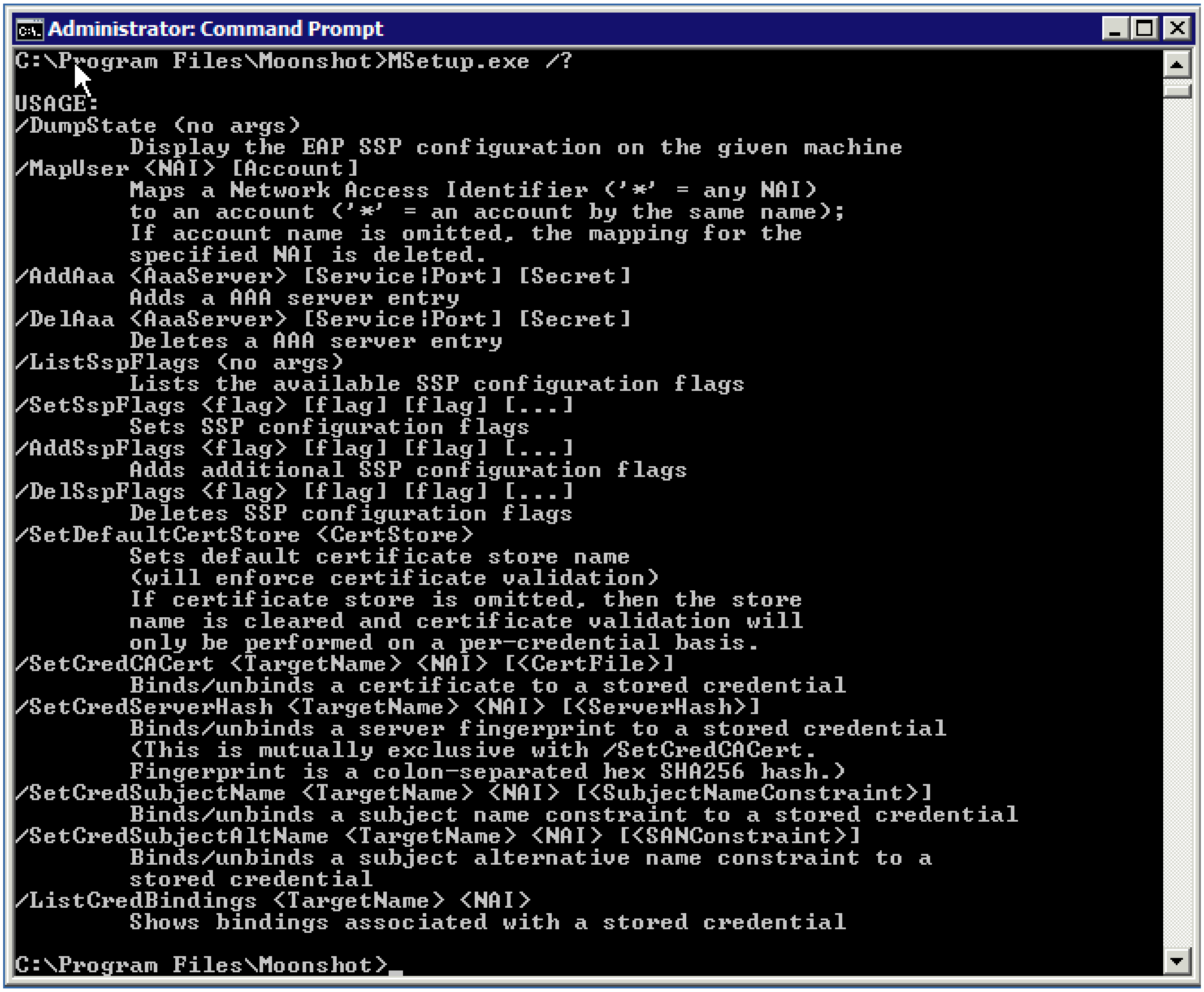
Servers

Server Address	Service/Port
212.219.210.195	1812

1.2. The CLI - msetup.exe

The SP setup CLI is located at `C:\Program Files\Moonshot\msetup.exe`

To set the options as documented in Section 2, run the msetup tool in a command prompt with the appropriate flags. Note that all settings require a reboot to take effect.



```
C:\Program Files\Moonshot>MSetup.exe /?

USAGE:
/DumpState (no args)
        Display the EAP SSP configuration on the given machine
/MapUser <NAI> [Account]
        Maps a Network Access Identifier ('*' = any NAI)
        to an account ('*' = an account by the same name);
        If account name is omitted, the mapping for the
        specified NAI is deleted.
/AddAaa <AaaServer> [Service|Port] [Secret]
        Adds a AAA server entry
/DelAaa <AaaServer> [Service|Port] [Secret]
        Deletes a AAA server entry
/ListSspFlags (no args)
        Lists the available SSP configuration flags
/SetSspFlags <flag> [flag] [flag] [...]
        Sets SSP configuration flags
/AddSspFlags <flag> [flag] [flag] [...]
        Adds additional SSP configuration flags
/DelSspFlags <flag> [flag] [flag] [...]
        Deletes SSP configuration flags
/SetDefaultCertStore <CertStore>
        Sets default certificate store name
        (will enforce certificate validation)
        If certificate store is omitted, then the store
        name is cleared and certificate validation will
        only be performed on a per-credential basis.
/SetCredCACert <TargetName> <NAI> [<CertFile>]
        Binds/unbinds a certificate to a stored credential
/SetCredServerHash <TargetName> <NAI> [<ServerHash>]
        Binds/unbinds a server fingerprint to a stored credential
        (This is mutually exclusive with /SetCredCACert.
        Fingerprint is a colon-separated hex SHA256 hash.)
/SetCredSubjectName <TargetName> <NAI> [<SubjectNameConstraint>]
        Binds/unbinds a subject name constraint to a stored credential
/SetCredSubjectAltName <TargetName> <NAI> [<SANConstraint>]
        Binds/unbinds a subject alternative name constraint to a
        stored credential
/ListCredBindings <TargetName> <NAI>
        Shows bindings associated with a stored credential

C:\Program Files\Moonshot>_
```

2. Main configuration options

You can use either tool to set any of the options below.

SSP Option	*Explanation of Option*
Debug	Turns on Debug logging. See the Debugging the Moonshot SSP on Windows topic for further information.
Disable SPNEGO	GSS-EAP will not be advertised by the SPNEGO/Negotiate security package. This may avoid any potential incompatibilities that might arise from the SSP being negotiable at two layers (Negotiate and NegoEx).
Disable NegoEx	GSS-EAP will not be advertised by the NegoEx security package (as negotiated by SPNEGO)
Use S4U on Domain Controller	Normally, if running on a domain controller, the directory is interrogated directly. If this flag is set, however, then S4U2Self (protocol transition) will be used if that fails. Used for debugging
Use Kerberos RPC ID	Pretends to be Kerberos rather than GSS-EAP (e.g., required for Microsoft Exchange)
Support Interactive Login	Allows federated sign-in to the Windows desktop
Use Domain Login Credentials	Pass through the credentials of the currently logged in user (desktop SSO)

3. Configure the connection to your Moonshot RP Proxy

Your Moonshot SSP needs to connect to a local Moonshot RP Proxy in order to authenticate remote users. To do so, you can either use the GUI or the CLI, whichever you prefer. Adding a connection to a Moonshot RP Proxy consists of two steps: configuring the basic details for the Moonshot RP Proxy, then configuring whether to use a RADIUS or a RadSec connection.

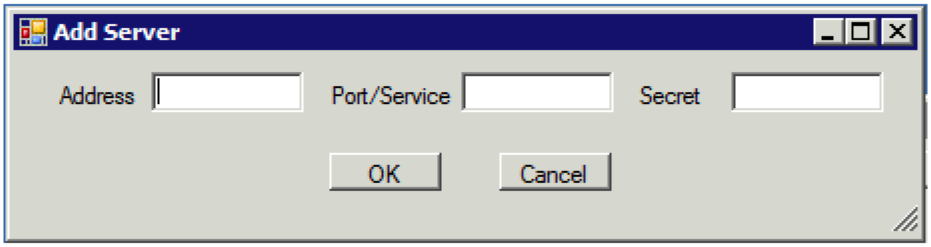
✓ Defining multiple Moonshot RP Proxy connections would give a simple fail-over mechanism; should the first Moonshot RP Proxy in the list not be available, the second would be consulted, and so on.

3.1. Basic Connection Details

3.1.1. Using the GUI

In the msetupgui.exe window, you will find an "Add Server" button. Click on this and a dialogue will pop up asking you to enter some information. Fill it in as follows:

- Address - the IP address of your AAA proxy
- Port/Service - the port that your RADIUS server is running on (often 1812 for RADIUS and 2083 for RadSec)
- Secret - the shared secret for your SSP as configured in the AAA proxy



3.1.2. Using the CLI

In a command prompt, issue the following command:

```
C:\Program Files\Moonshot\MSetup.exe /AddAaa server port secret
```

✓ **Example**

For a server located at 123.123.123.123, listening on port 1812 with a secret of "sharedsecret" you would run a command as follows:

```
C:\Program Files\Moonshot\MSetup.exe /AddAaa 123.123.123.123 1812 sharedsecret
```

3.2. Configuring RADIUS or RadSec

Your Moonshot libraries will need connect to a Moonshot RP Proxy. This can be a RADIUS or a RadSec connection.

✓ If you are unsure which to use, then RadSec is recommended as it is more flexible and more secure. It is slightly more complex to set up, however.

3.2.1. RadSec

3.2.1.1. Using the GUI

To configure a RadSec connection, make sure the "TCP" option is selected in the drop-down menu at the top left of the msetupgui.exe window.

⚠ **TODO**

Instructions on configuring certs in the SSP GUI

3.2.1.2. Using the CLI

> ⚠ **TODO**
>
> Instructions on configuring certs in the SSP CLI

3.2.2. RADIUS

3.2.2.1. Using the GUI

To configure a RADIUS connection, simply make sure the "UDP" option is selected in the drop-down menu at the top left of the msetupgui.exe window.

3.2.2.2. Using the CLI

> ⚠ **TODO**
>
> Need to check how to do this...

4. Add account mappings

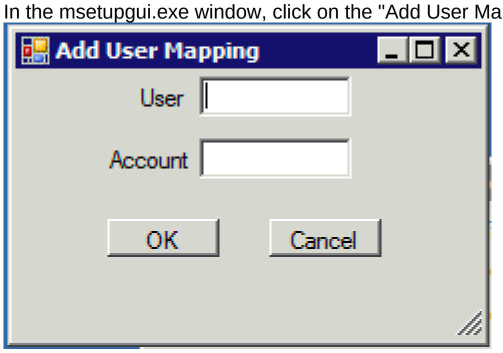
> ✓ Before doing any of the following, make sure you've read the User Account Mapping Options.

When a user authenticates via Moonshot, their remote identity (their NAI) must be mapped to an existing account on the Windows machine. If the machine is a standalone machine, this should be a local account; if the machine is a member of an AD domain, then it should be a domain account.

4.1. Mapping to a local account

4.1.1. Using the GUI

1. In the msetupgui.exe window, click on the "Add User Mapping" button. A dialogue box will appear:



2. Add the following information:

    - User - the full NAI of the user (e.g. johnsmith@example.com)
    - Account - the name of the local account you wish to map to (e.g. johns).

4.1.2. Using the CLI

1. In a command prompt, issue the following command:

```
C:\Program Files\Moonshot\MSetup.exe /MapUser NAI account
```

Example

To map a user with an incoming NAI of "johnsmith@example.com" to a local account of "johns" you would run a command as follows

```
C:\Program Files\Moonshot\MSetup.exe /MapUser johnsmith@example.com johns
```

4.2. Mapping to an AD domain account

To map to an AD account, you need to edit that account's attribute called "AltSecurityIdentities". Add a value of "EAP:[NAI]" to map an incoming user to that particular account (e.g., a value of "EAP:johnsmith@example.com" on a domain account of "DOMAIN\johns").

TODO

Tidy this last section up and add screenshot