Debugging the Moonshot SSP on Windows

Debugging the Moonshot SSP can be a tricky task. There are three potential ways to do it. This page presents each of them, in order of increasing difficulty.

Contents

1. System Preparation

1.1. Turning on Debug

Before you use any of the three methods, the first task it to load the Moonshot configuration GUI (usually located in `C:\Program Files\Moonshot\msetupgui.exe`) and tick the "Debug" option. You will need to reboot for this to take effect.

1.2. Setting the Registry

You now need to add the following items into the Windows Registry:

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa]
"SPMInfoLevel"=dword:0000101F
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa]
"LogToFile"=dword:00000001
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\]
"NegEventMask"=dword:0000000F
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\Kerberos]
"LogToFile"=dword:00000001
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\Kerberos]
"LogLevel"=dword:00000001
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\Kerberos\Parameters]
"LogToFile"=dword:00000001
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\Kerberos\Parameters]
"LogLevel"=dword:00000001
```

2. Debugging

2.1. Option 1 - Log to lsass.log

After doing the preparation steps above, reboot the machine. SSP debug logging should now appear in C:\WIndows\System32\lsass.log.

The lines relevant to the Moonshot SSP begin with "EAP-SSP" (before v1.1.135), or "EapSSP" (v1.1.135 or later).

> ⊘ This option is probably the easiest way to view the debug logging from the Moonshot SSP.

2.2. Option 2 - Gather trace information

If you just wish to see the Moonshot SSP logging in its own file, this option may be the best.

Once you have performed the above preparation work, start a Command Prompt session as an Administrator:

1. Click Start, All Programs, Accessories.
2. Right-click the Command Prompt entry, select Run as administrator.

> ⚠️ **User Access Control**
>
> You may be prompted to confirm whether you want to allow the program to make changes to the computer. Choose Yes.

3. Run the following command from the command prompt to start gathering trace information:

```
logman start mysession -p {b85c67ff-f395-4e75-8836-dc395f022125} -o eapssp.etl -ets
```

4. Once you've performed the actions you wish to debug, stop this by issuing the following command:

```
logman stop mysession -ets
```

5. Now run the following common to create the trace log for you to look at.

```
tracerpt eapssp.etl
```

> ✅ If you just wish to see the Moonshot SSP logging in its own file - so that you don't have to sift through other non-relevant logs, this option may be the best.

2.3. Option 3 - Using DebugView

1. Once you've done the preparation work above, download DebugView from Microsoft (get it at Microsoft's site).
2. Run DebugView as Administrator and capture global Win32 events.

> ⊘ This final option is the trickiest and requires extra tools to be installed. It is, however, required to debug particularly thorny SSP issues.