SAP SNC Errors - Using Microsoft Kerberos instead of MIT Kerberos for Windows to access SAP

Q: SAP SNC Errors - Using Microsoft Kerberos instead of MIT Kerberos for Windows to access SAP

- Due to a compatibility issue with MIT Kerberos for Windows and the User Account Control (UAC), the UAC is disabled by default in win.mit.edu to avoid having users receive errors while trying to access SAP instances.
- The following fix allows users to access SAP via Microsoft Kerberos functionality built into the OS instead of MIT's Kerberos for Windows. Once this fix is in place the UAC can be enabled if desired in the case where MIT's Kerberos for Windows was only used for access to SAP.

Context

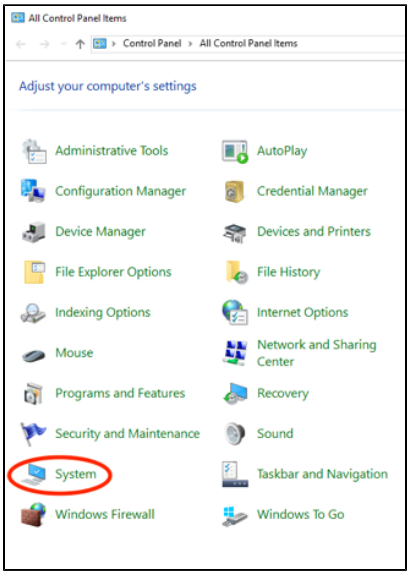
- This is due to an issue with MIT Kerberos and Windows. By using Microsoft Kerberos this issue is bypassed. **Please note this issue should only be used to resolve issues with SAP as other applications may need MIT Kerberos**. Other applications can continue to use the Kerberos for Windows software.
- This fix is generally applied via a group policy object and must be performed by an IT technician with the appropriate permissions to the GPO.
- Applying this fix allows UAC to be enabled on computers if desired.

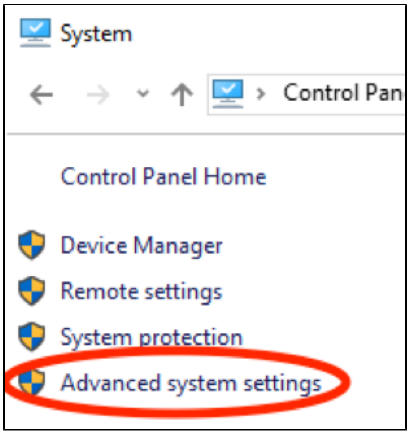
Answer

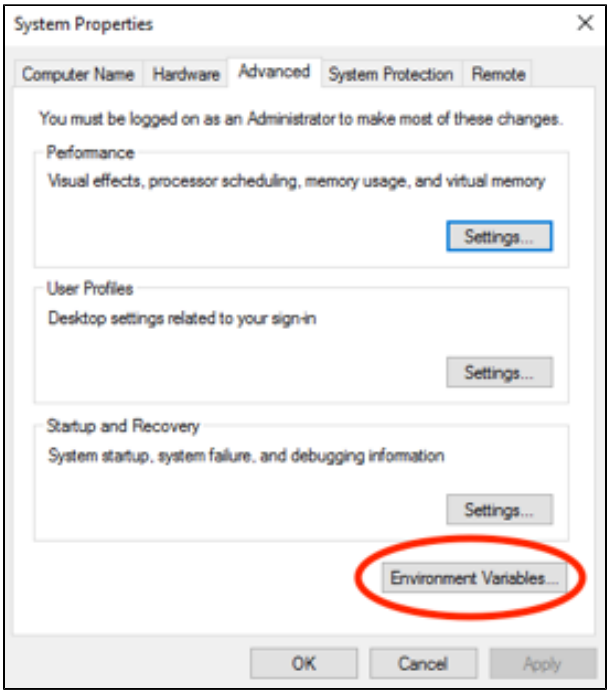
Note: Only one procedure below is needed. You do not apply both procedures. The individual computer change procedures apply to only the computer(s) you are working on whereas the group policy procedures will apply to all computers located in the related Organizational Unit (OU).

Individual computer change procedures:

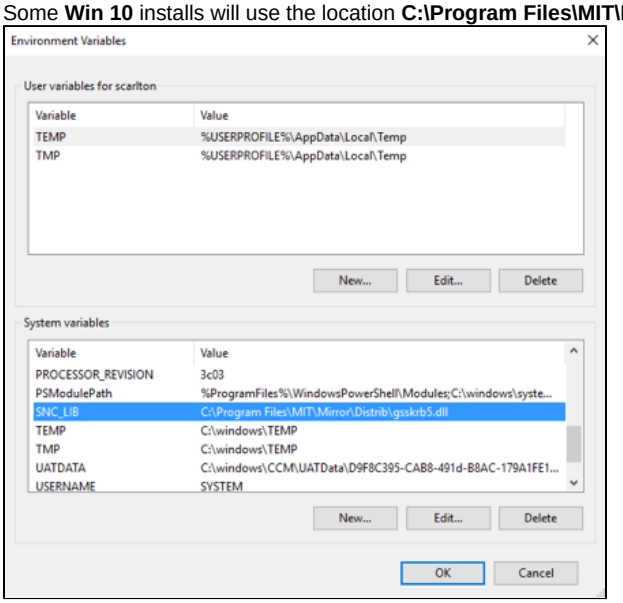
1. **Environment Variables** are located under **Advanced system settings**. This can be accessed through **System** within **Control Panel**







2. **Edit** the System Variable **SNC_LIB** to **C:\Program Files\MIT\Mirror\Distrib\gsskrb5.dll**
   Some **Win 10** installs will use the location **C:\Program Files\MIT\Kerberos\bin\gssapi32.dll**

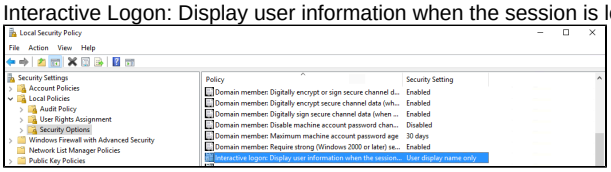


Additionally you'll want to change some settings that resolve the issue of Kerberos tickets breaking when a computer goes to sleep. Changing

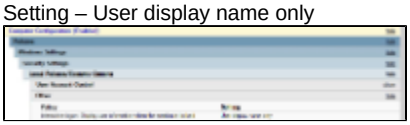
these settings will require a user to logon with a password every time wake from sleep. Go to the local group policy editor by running **gpedit.msc** on the local computer.

In the local group policy editor, browse to:

1. Computer Configuration, Policies, Windows Settings, Security Settings, Local Policies / Security Options / Other
2. Interactive Logon: Display user information when the session is locked

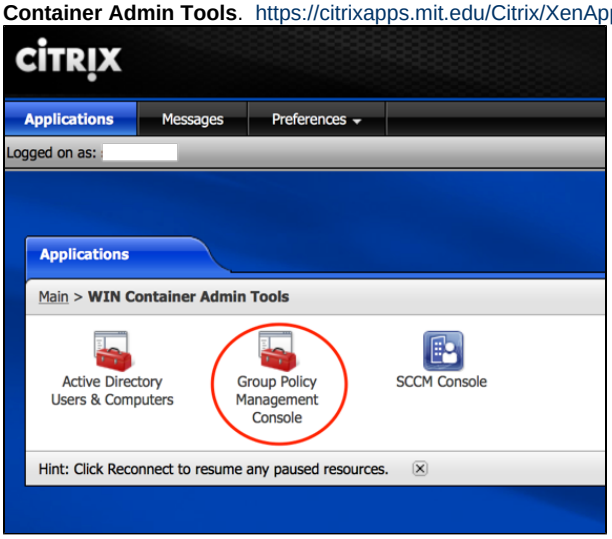


3. Setting – User display name only



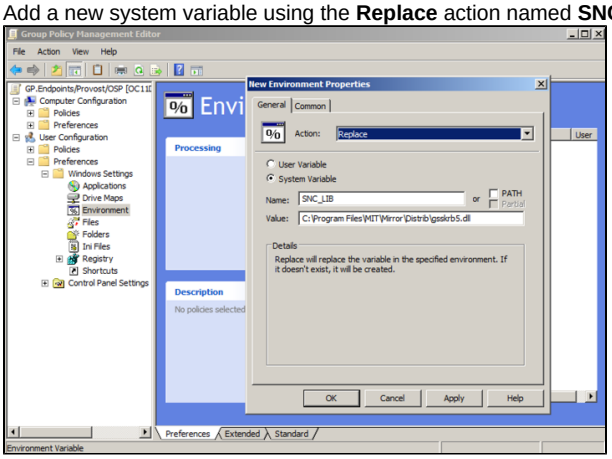
Group Policy change procedures (applies to all computers within the OU):

1. Access the related Organization Unit GPO through **Group Policy Management Console**. This is done through **Citrix** under the **WIN Container Admin Tools**. https://citrixapps.mit.edu/Citrix/XenApp/auth/login.aspx



Once you locate your related GPO **right click** and **select edit**

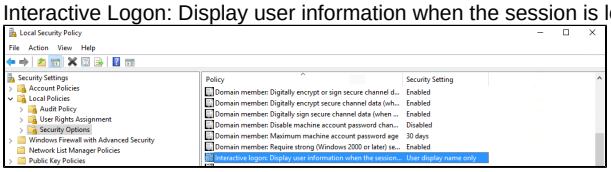
1. Navigate to **User Configuration/Preferences/Windows Settings/Environment**
2. Add a new system variable using the **Replace** action named **SNC_LIB** with the value **C:\Program Files\MIT\Mirror\Distrib\gsskrb5.dll**



Additionally you'll want to change some settings that resolve the issue of Kerberos tickets breaking when a computer goes to sleep. Changing these settings will require a user to logon with a password every time wake from sleep. Go to the GPO **right click** and **select edit**

In GPMC, browse to:

1. Computer Configuration, Policies, Windows Settings, Security Settings, Local Policies / Security Options / Other
2. Interactive Logon: Display user information when the session is locked



3. Setting – User display name only

