Using Global Managed Service Accounts with Fix My Session

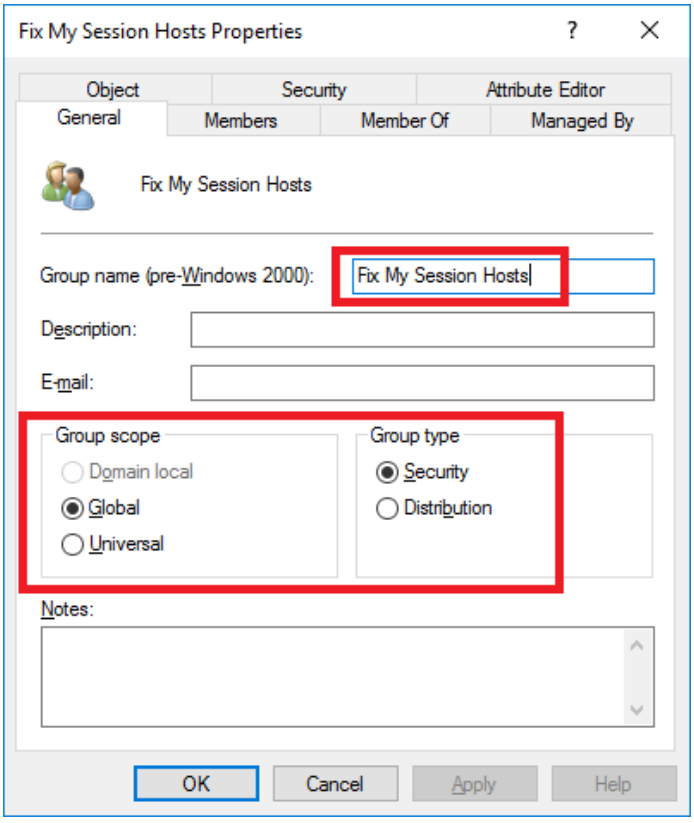
Organizations may wish to use a Global Managed Service Account (gMSA) with Fix My Session for many reasons, including:

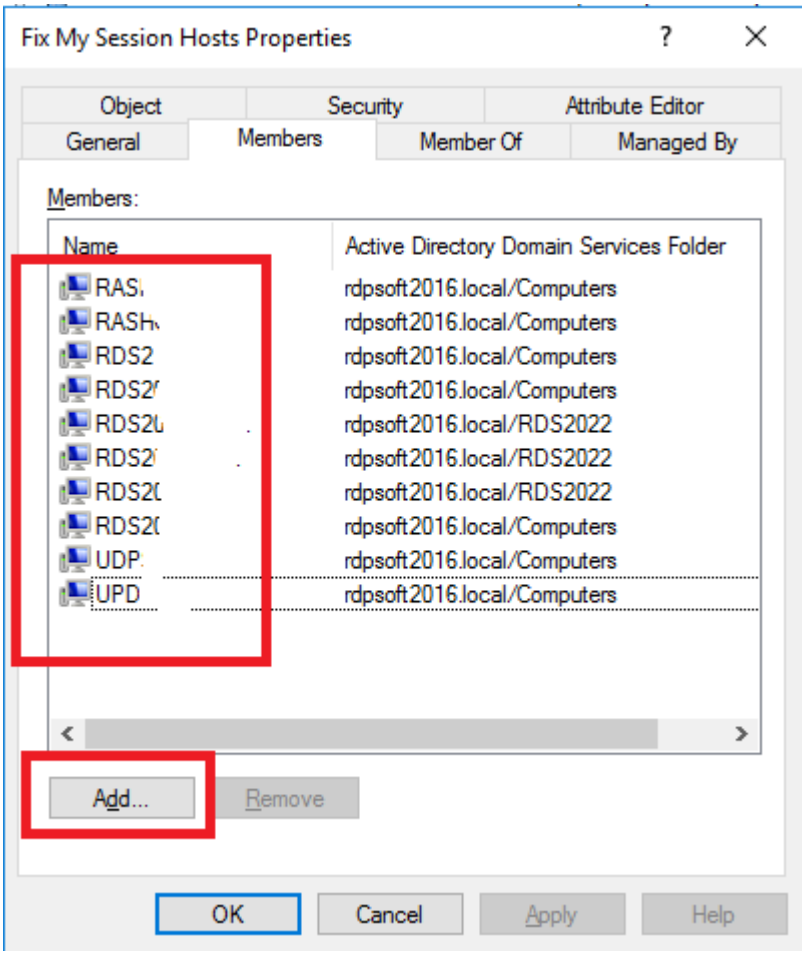
1.) No need to manage service account passwords manually or deal with unexpected password expiration due to policies,
2.) gMSAs use highly complex passwords, which are very resistant to brute force attacks, and
3.) gMSAs allow admins of EUC environments that use non-persistent session hosts (e.g. AVD hosts that are rebuilt each morning from a golden image) to script the automated deployment and configuration of the Fix My Session agent without needing to reference passwords, which could be inherently insecure.

Note, if you have an orchestrated EUC environment, such as Azure Virtual Desktop with non-persistent hosts that are re-provisioned daily or weekly, please also review the Performing Scripted Deployments of the Fix My Session Agent on Non Persistent Hosts help topic.

Here are the steps you need to take to utilize a gMSA with Fix My Session.

Step 1 - Create a Global Security Group in Active Directory, which must contain the computer accounts of all the session hosts where Fix My Session is running, as well as the primary host where Fix My Session was installed (e.g. the master host).





Step 2 - On an Active Directory Domain Controller, check to see if a Key Distribution Root Key already exists, by running the *Get-KDSRootKey* PowerShell command. If no such Key Distribution Root Key exists (empty results from the PowerShell command, run the *Add-KDSRootKey* PowerShell command on the DC as follows:

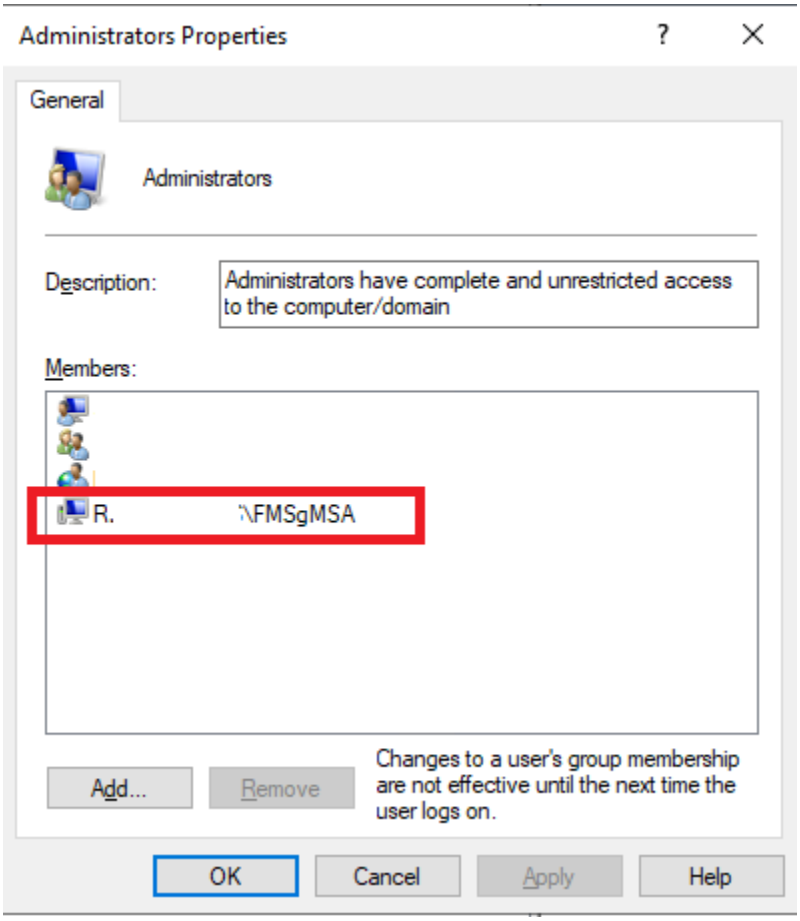
```
Add-KdsRootKey -EffectiveTime ((get-date).addhours(-10))
```

Step 3 - Once a KDS Root Key exists, create the gMSA for the Fix My Session agents and master service by using the New-ADServiceAccount PowerShell command as follows on your domain controller:

```
new-adserviceaccount -Name 'FMSgMSA' -DNSHostName 'FixMySessiongMSA.yourdomain.com' -
PrincipalsAllowedToRetrieveManagedPassword "Fix My Session Hosts" -Enabled $True
```

In this example, a new Fix My Session gMSA is created with the account name of **FMSgMSA**. It receives a DNS Host Name of **FixMySessionMSA.yourdomain.com**. Any computer account in the **Fix My Session Hosts** group you created in Step 1 above has the right to retrieve the managed password from the domain controller securely.

Step 4 - Make sure this new gMSA account is added to the Administrators group on the host running Fix My Session, on any file servers, and on all session hosts managed by Fix My Session. You can do this through group membership, or direct inclusion in the Administrators local group on those hosts. The account should show with a computer icon in the membership list, like so:



Step 5 - Finally, on any Session Host AND the computer hosting the Fix My Session application (e.g. master server), you will need to run the Install-ADServiceAccount PowerShell command so that those hosts can utilize the gMSA you created in Step 3, and so the Fix My Session Profile Fixer Service can run under this account.

First, it is important to note that the RSAT tools for PowerShell must first be installed on each host, in order to call the Install-ADServiceAccount PowerShell command.

For hosts running Windows Server operating systems, please run this command first before running the Install-ADServiceAccount PowerShell command:

```
Install-WindowsFeature RSAT-AD-Powershell
```

For hosts running Windows 10 or Windows 11 operating sysetms (e.g. AVD multiuser hosts), please run this command first before running the Install-ADServiceAccount PowerShell command:

```
Add-WindowsCapability -Online -Name Rsat.ActiveDirectory.DS-LDS.Tools~~~~0.0.1.0
```

Next, run the Install-ADServiceAccount PowerShell command like so to install your Global Managed Service Account on to this host:

```
Install-ADServiceAccount "YOURDOMAIN\FMSgMSA$"
```

Where **YOURDOMAIN** is the short, NetBIOS version of your domain, and **FMSgMSA$** is the gMSA you created in Step 3.

If you receive an Access Denied error running Install-ADServiceAccount, you may need to clear the local Kerberos ticket cache for the local computer where you are installing the gMSA, then try the Install-ADServiceAccount command again. This can be done with the following syntax:

```
c:\windows\system32\klist.exe -lh 0 -li 0x3e7 purge
```