

Configuring Kerberos Authentication to Prevent the Double-Hop Issue

Symptoms

User cannot use any of the features that require direct SQL database read/write procedures (Workflow instance/Document ID preservation/Deleted AD user preservation).

The user can establish a connection to the Metalogix Extensions Web Service (MEWS) and can migrate content however they do not get the full set of features available.

Cause

When we make the SQL Database RPC T-SQL calls it is under the name of the migrating account for auditability (i.e DOMAIN\user). However this identity cannot be persisted from the Web Service to the SQL backend in an NTLM authentication scenario.

Resolution

1. Change your web application to use Kerberos

If your web app is not already using Negotiate (Kerberos) Authentication change your SharePoint Web Application to use mixed mode authentication (NTLM and Negotiate). This is the [recommended article](#):

IIS

1. Click **Start**, click **Run**, type **cmd**, and then press ENTER.
2. Locate the directory that contains the Adsutil.vbs file. By default, this directory is C:\inetpub\Adminscripts.
3. Use the following command to retrieve the current values for the **NTAuthenticationProviders** metabase property:

```
cscript adsutil.vbs get w3svc/ WebSite/root/NTAuthenticationProviders
```

In this command, *WebSite* is a placeholder for the Web site ID number. The Web site ID number of the default Web site is 1. To find the Web site ID go to IIS on the sites list folder there is an ID column in the features view box.

Warning Do not perform a copy-and-paste operation to paste the command from this article. This operation may cause issues with the property setting. To avoid these issues, type the whole command at a command prompt.

Note This command fails if the **NTAuthenticationProviders** metabase property is not defined. For more information, see the note earlier in this section.

If the Negotiate process is enabled, this command returns the following information:

```
NTAuthenticationProviders : (STRING) "Negotiate,NTLM"
```

4. If the command in step 3 does not return the string "Negotiate,NTLM," use the following command to enable the Negotiate process:

```
cscript adsutil.vbs set w3svc/Website/root/NTAuthenticationProviders "Negotiate,NTLM"
```

5. Repeat step 3 to verify that the Negotiate process has been enabled.

2. Create Service Principle Names (SPN) to allow constrained delegation.

SQL server

Create an SPN for the SQL service over port 1433 for the SQLserver account

```
setspn -A MSSQLSvc/<FQDN for SQL Server machine>:<Port number that SQL is running on, 1433 is the default> <Domain\Account>
```

e.g. setspn -A MSSQLSVC/SQLServer.Metalogix.Company:1433 TEST\MSSQLAccount

Application Server (Web front end with IIS6)

Create an SPN for the HTTP service over port 1433 for the Network service account

```
setspn -A HTTP /<FQDN for SharePoint Web front end server or NLB cluster name>:<port> <domain-user-account or computer account>
```

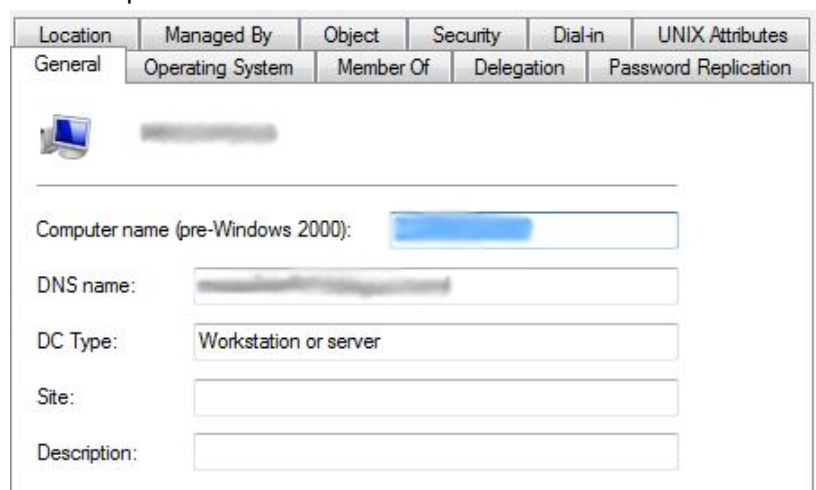
e.g. setspn -A HTTP/MossWFE.Metalogix.Company:1433 TEST\MossWFE\$

Note, you can list the existing SPNs for a given account by:

```
setspn -l <DOMAIN\Account>
```

3. Setup the Web Server computer account for delegation

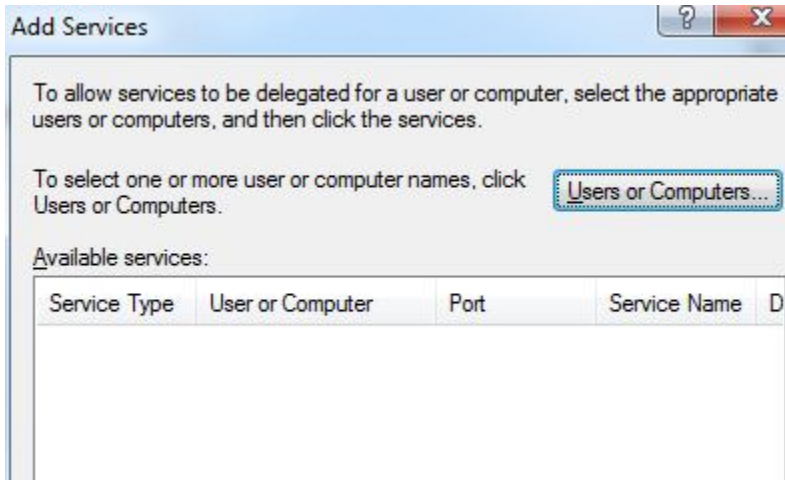
On the properties for the Web Front End server in Active Directory you should see a tab named "Delegation", if you do not then the Service Principle names have not been configured correctly so see step 2.



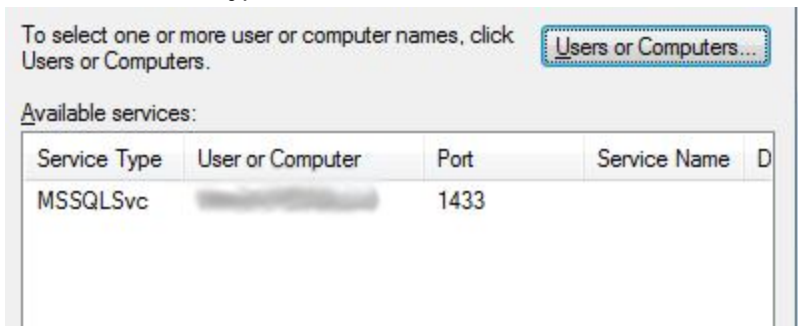
On the delegation tab, by default its set to "Do not trust the computer to delegation". Change that to "Trust this computer for delegation to specified services only", and select "Use Kerberos only".

- ☒ Do not trust this computer for delegation
- ☐ Trust this computer for delegation to any service (Kerberos only)
- ☐ Trust this computer for delegation to specified services only
 - ☒ Use Kerberos only
 - ☐ Use any authentication protocol

Click the "Add..." button



Click on Users and Computers button, and specify the account being used for the SQL server. Select the service type MSSQLSvc and click OK.



The screen should look like this -

☐ Do not trust this computer for delegation
☐ Trust this computer for delegation to any service (Kerberos only)
☒ Trust this computer for delegation to specified services only

☒ Use Kerberos only
☐ Use any authentication protocol


Services to which this account can present delegated credentials:

Service Type	User or Computer	Port	Service Name
MSSQLSvc		1433	

☐ Expanded

Next setup the SQL Server computer account for delegation by going to the properties for the SQL server computer account in Active Directory.

Location	Managed By	Object	Security	Dial-in	UNIX Attributes
General	Operating System	Member Of	Delegation	Delegation	Password Replication



Computer name (pre-Windows 2000):

DNS name:

DC Type: Workstation or server

Site:

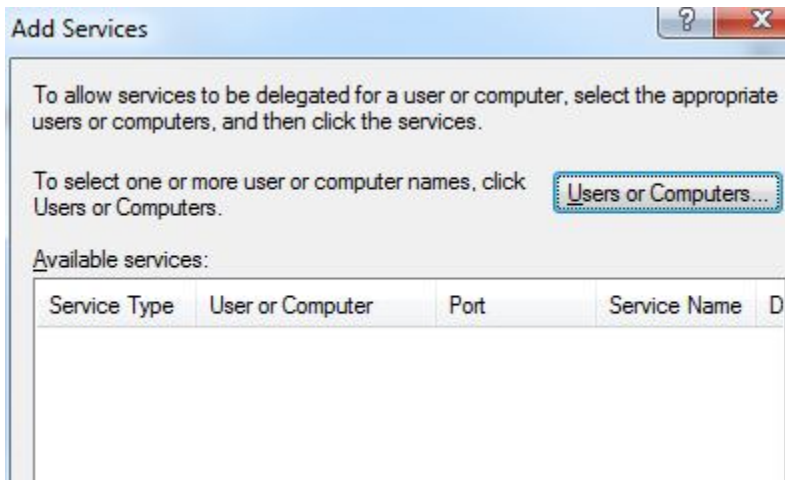
Description:

On the delegation tab, by default its set to "Do not trust the computer to delegation". Change that to "Trust this computer for delegation to specified services only", and select "Use Kerberos only".

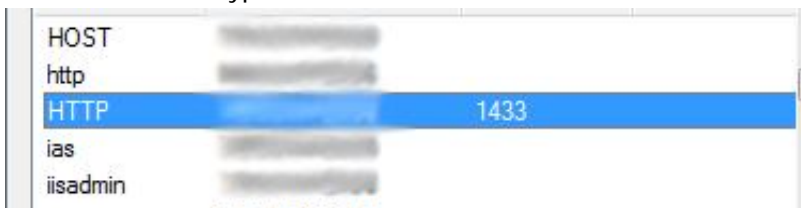
☒ Do not trust this computer for delegation
☐ Trust this computer for delegation to any service (Kerberos only)
☐ Trust this computer for delegation to specified services only

☒ Use Kerberos only
☐ Use any authentication protocol

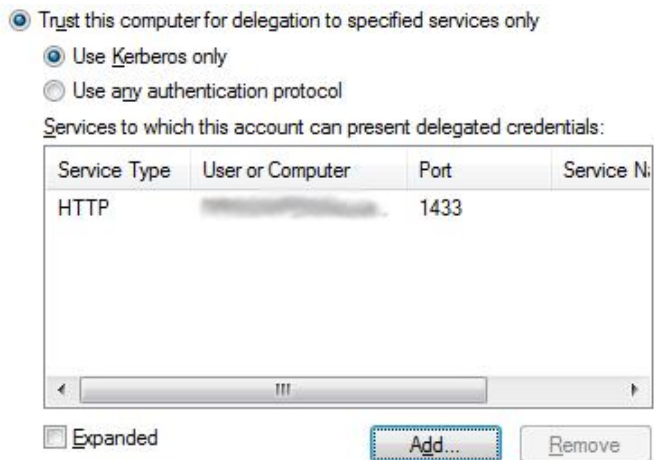
Click the "Add..." button



Click on Users and Computers button, and specify the account being used for the web server. Select the service type HTTP and click OK.



The Delegation tab should now look like this:



More Information