Preparation

On this page:

Accounts needed to install ActiveEfficiency

To install ActiveEfficiency, you will need:

1. ActiveEfficiency installer account:
   - Must be a domain account and have local admin rights on the Web server where ActiveEfficiency is installed
   - Have Sysadmin rights on the SQL Server instance hosting the ActiveEfficiency database. Sysadmin is required to create:
     a. a new ActiveEfficiency database, with SQL login for the ActiveEfficiency service account
     b. a linked server used by Nomad Sync
   - If you are not using Nomad Sync then either:
     a. let the installer create a new database and SQL login, which requires CREATE DATABASE and ALTER ANY LOGIN rights on the instance
     b. use an existing database and SQL login which requires db_owner rights on the database
   - Have the ability to add the relevant service accounts described in granting access to the Configuration Manager site database. This concerns the `ConfigMgr_DViewAccess` localgroup on the SQL Server hosting the Configuration Manager database. This is achieved by either:
     a. this group is manually populated and configured as described
     b. the installer account has local admin rights in order to populate this group and grant rights before or after installation.
2. ActiveEfficiency service account:
   - ActiveEfficiency uses Network Service for its service account and web application pool. The installer will create a SQL login and grant the necessary rights on the ActiveEfficiency database if the installer account has the rights listed above.
   - If you need to use an alternative service account, then specify the SVCUSER and SVC PASSWORD installer properties on the MSI command-line.
   - If you are using Nomad Sync, then you must grant it access to the Configuration Manager site database

Accounts needed to install the Scout

> You only require the ActiveEfficiency Scout if you are using Shopping or AppClarity 5.2.

To install the Scout, you will need:

1. Scout installer account:
   - Must be a domain account and have local admin rights to install the Scout
   - When using the Scout in Configuration Manager mode, the installer account must have:
     a. Local admin rights to run the ActiveEfficiency synchronization manager.
     b. Configuration Manager database read-only permissions.
   - When installing in iQSonar mode the installer account must have:
     - iQDataHub database read-only and execute permissions on the dbo.DatabaseVersion_re stored procedure
2. A Scout service account is required when using the Scout in Configuration Manager mode. The ActiveEfficiency Synchronization Manager uses it as the Master Credentials account to run Task Scheduler tasks, which connect to and extract data from Configuration Manager. In order to run Task Scheduler tasks, this account needs the following:
   - Must be a domain account
   - Must be a member of the Administrators localgroup
   - Must have the following rights, either configured locally or using GPO, in order to run Task Scheduler tasks.
   - If the installer account is a local Administrator, then these rights will be granted automatically, otherwise they must be configured manually.
     - Log on as batch job
     - Replace a process level token
   - Additional rights may need to be configured manually:
     - Access the computer from the network
     - Log on as a service
     - Deny logon locally (optional)
     - Server security policy “Network Access: Do not allow storage of passwords and credentials for network authentication” must be disabled, to allow accounts to be stored for Task Scheduler
3. One or more Data capture accounts. If you are using the Scout in Configuration Manager mode, by default you can use the Master Credentials account, which needs the following:
   - Must grant it access to the Configuration Manager site database
   - Review data capture accounts to determine what additional requirements you may require for other Scout modes

Granting access to the Configuration Manager site database

In most configurations, ActiveEfficiency and its Scout require read access to the Configuration Manager site database. For a single-site hierarchy this is a standalone Primary Site, and for a multi-site hierarchy this is the CAS. When using the Scout to collect data for AppClarity, this can be a reporting Site, but other uses require a live Site to get the most recent data.

Access rights are required for the following service accounts depending on which features are used.

- If using Nomad Sync, grant the ActiveEfficiency service account. By default, the service account is Network Service, in which case the ActiveEfficiency server's computer account must be granted access. If using a domain account then this must be granted access instead.
- If using the Scout in Configuration Manager mode, grant the Scout service account (also known as as Master Credentials)

To grant rights to the ActiveEfficiency and Scout service accounts, do the following on the Configuration Manager site database server.

1. If it does not already exist, create a localgroup called the **`ConfigMgr_DViewAccess`** (this localgroup should already exist on a Primary site database server, but will not exist for a CAS or any CB 1710 site database servers)
2. Add the **ActiveEfficiency service account** to the localgroup
3. If you will be using 1E Shopping then also add the **Scout service account** to the localgroup
4. Execute the ConfigMgr_DViewAccess_permissions.SQL script against the Configuration Manager database – it creates a SQL login, if not already exists, and grants execute rights on fnGetSiteNumber, exactly the same way as found natively on standalone Primaries.

You can use your ActiveEfficiency installer account to configure the above rights before or after installation. Whatever installation account is used, it will need the following with respect to the `ConfigMgr_DViewAccess` localgroup.

- local administrator rights on the server to create the `ConfigMgr_DViewAccess` localgroup and add the service accounts
- sysadmin rights in order to create a login for the group and grant it execute rights on the Configuration Manager site database

Nomad Dashboard uses the following sources to populate its tiles:

- ActiveEfficiency database – uses the ActiveEfficiency application pool account, which is Network Service by default. See ActiveEfficiency service account for details.
- Configuration Manager database – uses the `ConfigMgr_DViewAccess` local group described in the paragraph above
- Configuration Manager SMS Provider – uses the logged on user's credentials in the Configuration Manager Console (the minimum privilege required is Read-only Analyst)
- If sufficient rights exist and there is no data, the tiles show No Data Available
- If rights have not been granted, or there is an issue with the linked server, then tiles show Error 500

MSMQ

Microsoft Message Queuing (MSMQ) Windows feature must be enabled in order to install the 1E ActiveEfficiency service component. This service is required by:

- Nomad Sync (dashboard and pre-cache features) even though it does not use MSMQ
- Nomad integration with WakeUp feature, which does use MSMQ and requires MSMQ to also be enabled on the NightWatchman server

MSMQ is only required to support the above features, and is no longer required by other 1E companion products that use ActiveEfficiency Server (AppClarity 5.x and Shopping 5.x).

AppV considerations

These considerations are only relevant if you are using the Scout to get data for AppClarity 5.2, which is no longer supported.

- The Scout must be installed with Configuration Manager mode enabled. Refer to Installing the Scout for more detail on Scout modes.
- AppV packages must have been sequenced in AppV 4.5, 4.6 or 5.0
- The Configuration Manager client must be installed on all the systems where the AppV packages are deployed.

Nomad considerations

- The Nomad Sync feature in ActiveEfficiency is used by
    - Nomad Dashboard
    - Nomad pre-cache
- ActiveEfficiency is also used by Nomad for
    - Single-Site Download (SSD)
    - Single-site Peer Backup Assistant
    - Nomad integration with 1E WakeUp
    - Nomad Download Pause

DNS alias

Nomad requires the FQDN of the ActiveEfficiency server to be configured in the PlatformURL setting of the Nomad agent on all machines. Therefore a DNS alias is recommended for the ActiveEfficiency server, but is not mandatory. This can be a CNAME or Host (A) record.

MSDTC

ActiveEfficiency Server requires Distributed Transaction Coordinator (MSDTC) to be enabled and configured on each of the SQL Servers used by:

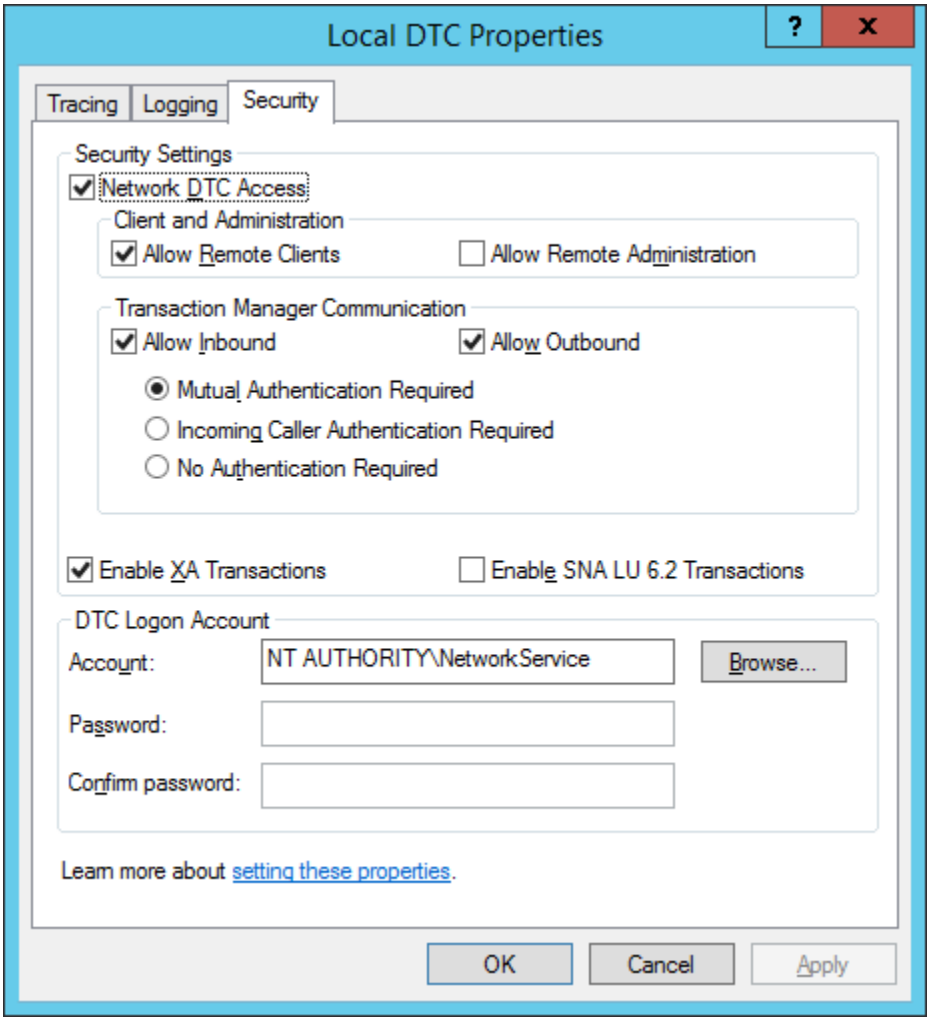
- ActiveEfficiency database

- Configuration Manager site database - specified in the Nomad Sync settings during installation of ActiveEfficiency. This would normally be the CAS in a multi-site hierarchy, or the Primary Site in a single-site hierarchy.

MSDTC is a feature of Windows Server and is used to track of transactional processes, usually over multiple resource managers on multiple computers. MSDTC ensures that the transactions are completed and can be rolled-back if any part of the process fails. Nomad Sync uses MSDTC to perform complex queries on Configuration Manager and ActiveEfficiency data. For example, to retrieve computers targeted with Nomad Pre-cache policies and Nomad Dashboard data.

> You must complete the following procedure on each SQL Server used by ActiveEfficiency and the Configuration Manager site.

1. Ensure the Distributed Transaction Coordinator (MSDTC) service is enabled and running.
2. Optionally use the registry import, which will set the values which you can then verify using the following steps.
3. Start **Component Services** (comexp.msc) and expand **Computers My Computer Distributed Transaction Coordinator Local DTC**.
4. Right-click **Local DTC** and from its context menu, choose **Properties**.
5. Select the **Security tab** and **enable the following**, leaving other settings as default.
    - Network DTC Access
    - Allow Remote Clients
    - Allow Inbound
    - Allow Outbound
    - Mutual Authentication Required
    - Enable XA Transactions
6. Click **OK** – if any changes were made this will restart the MSDTC service.
7. If you used the registry import, you will need to restart the MSDTC service.



```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MSDTC]
"FallbackToUnsecureRPCIfNecessary"=dword:00000000
"AllowOnlySecureRpcCalls"=dword:00000001
"TurnOffRpcSecurity"=dword:00000000

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MSDTC\Security]
"NetworkDtcAccess"=dword:00000001
"NetworkDtcAccessClients"=dword:00000001
"NetworkDtcAccessAdmin"=dword:00000000
"NetworkDtcAccessInbound"=dword:00000001
"NetworkDtcAccessOutbound"=dword:00000001
"NetworkDtcAccessTransactions"=dword:00000001
"NetworkDtcAccessTip"=dword:00000000
"XaTransactions"=dword:00000001
"LuTransactions"=dword:00000000
```

Service Principal Names and Delegation

Nomad Sync uses a SQL linked server on the same SQL instance as the ActiveEfficiency database, to connect to the Configuration Manager database. The linked server is created by the ActiveEfficiency installer if the Nomad Sync option is enabled. The service account used by the ActiveEfficiency SQL instance must be trusted to present delegated credentials to the Configuration Manager SQL instance.

If the ActiveEfficiency service, the ActiveEfficiency database and the Configuration Manager database are on three separate servers and you plan to use the Nomad Dashboard or the Nomad pre-cache features or if you get the `Login failed for user NT AUTHORITY\ANONYMOUS LOGON` error message in the ActiveEfficiency service log (located in `C:\ProgramData\1E\ActveEfficiency`), follow this procedure:

1. Ensure the ActiveEfficiency SQL instance and the Configuration Manager SQL instance both use Kerberos authentication. Run this SQL query to verify the authentication method:

   ```
   select auth_scheme from sys.dm_exec_connections where session_id=@@spid
   ```

   > This query must be run remotely from the SQL Server – connect to ActiveEfficiency's SQL instance from the remote Configuration Manager SQL instance (or vice versa). If you run it on the SQL Server it will always return NTLM.

   It returns KERBEROS if the service is configured correctly. If it returns NTLM, the service principal names (SPNs) for the SQL Server service are not configured correctly for Kerberos authentication.
2. Determine the name of the SPN required by the service, by looking at the SQL Server logs (in the SQL instance, under Management node). SQL Server will attempt to self-register the correct SPNs when the service starts, and will succeed if the service account has permissions in Active Directory. A computer account normally has the necessary permissions to self-register, but a domain user account does not. You must create the SPN if self-registration fails.

   A self-registration failure is logged as follows:

   ```
   The SQL Server Network Interface library could not register the Service Principal Name (SPN) [
   MSSQLSvc/SQLServerFQDN:port ] for the SQL Server service. Windows return code: 0x200b, state: 15.
   Failure to register a SPN might cause integrated authentication to use NTLM instead of Kerberos. This
   is an informational message. Further action is only required if Kerberos authentication is required
   by authentication policies and if the SPN has not been manually registered.
   ```

   A self-registration success is logged as follows:

   ```
   The SQL Server Network Interface library successfully registered the Service Principal Name (SPN) [
   MSSQLSvc/SQLServerFQDN:port ] for the SQL Server service.
   ```

3. Use a domain admin account to execute a SetSPN command to create the SPN you need. Port is the TCP port used by the SQL instance. For example:

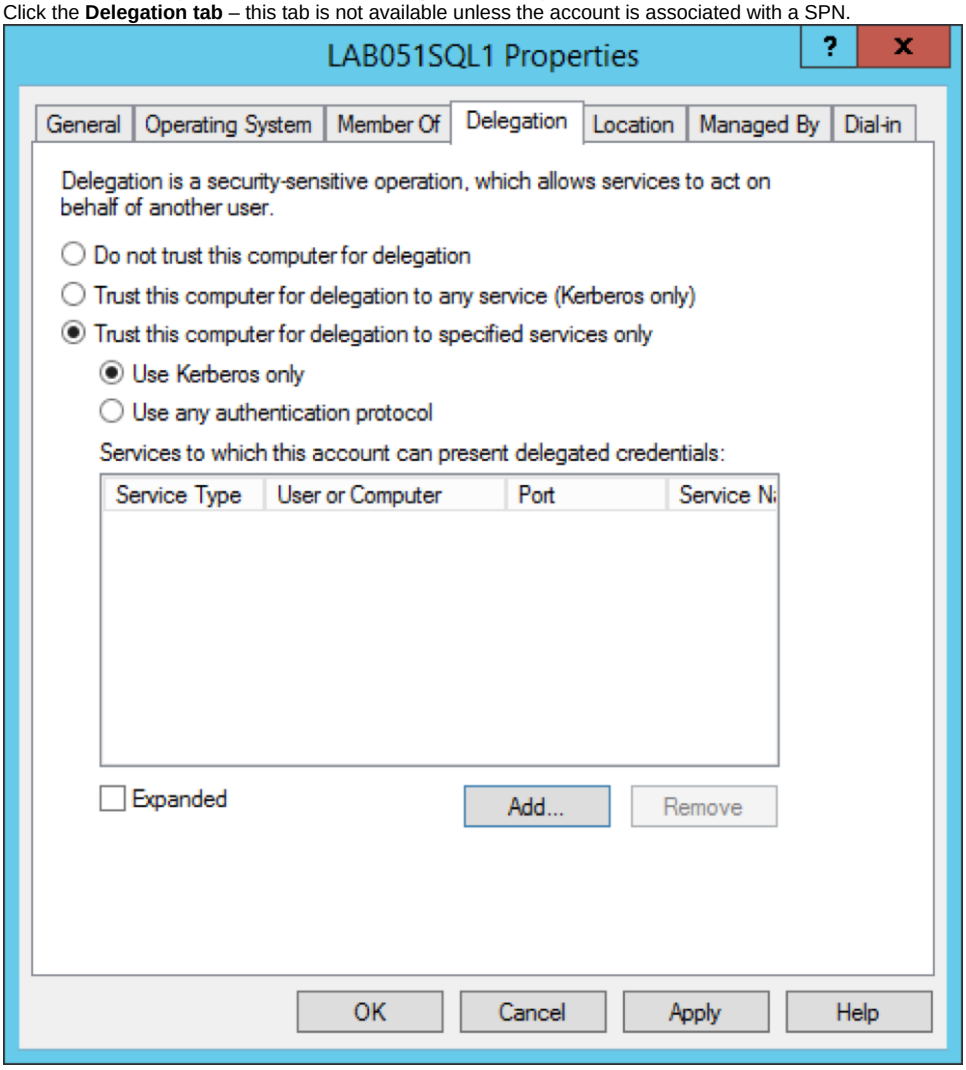
   ```
   setspn -S MSSQLSvc/SQLServerFQDN:port <domain\SQL service account>
   ```

   Verify the SPN has been created correctly with:

```
setspn -L <domain\SQL service account>
```

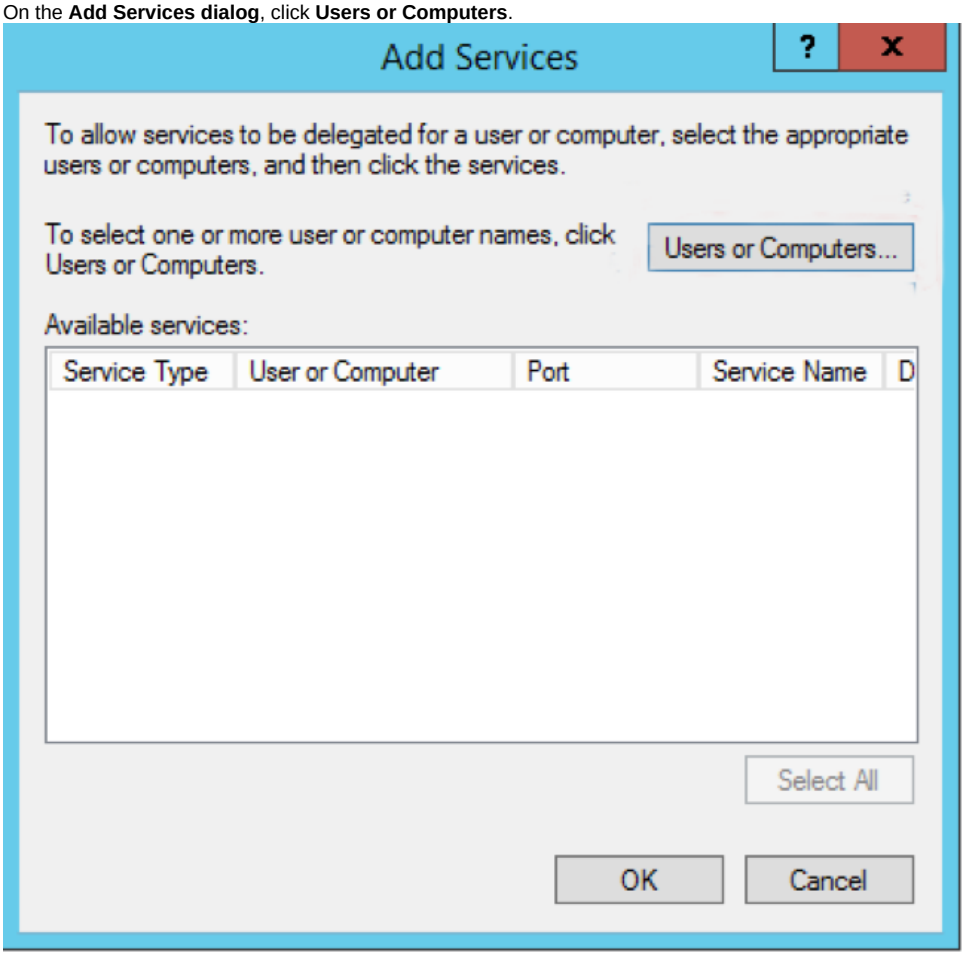
You must complete the above procedure for both the ActiveEfficiency SQL instance and Configuration Manager SQL instance before continuing.

4. Open **Active Directory Users and Computers** to verify the service account for the ActiveEfficiency database SQL Server is trusted for delegation.
    a. The first step in the process is to determine if it is running under a system account or domain user account.
        i. If the ActiveEfficiency SQL Server service is using the Network Service built-in account:
            - In **AD Users and Computers**, locate the computer account for the Active Efficiency SQL Database server
            - Open the **Computer Properties dialog**
        ii. If the ActiveEfficiency SQL Server service is using a domain user service account:
            - In **AD Users and Computers**, locate the SQL Server service account
            - Open the **User Account Properties dialog**
    b. Click the **Delegation tab** – this tab is not available unless the account is associated with a SPN.

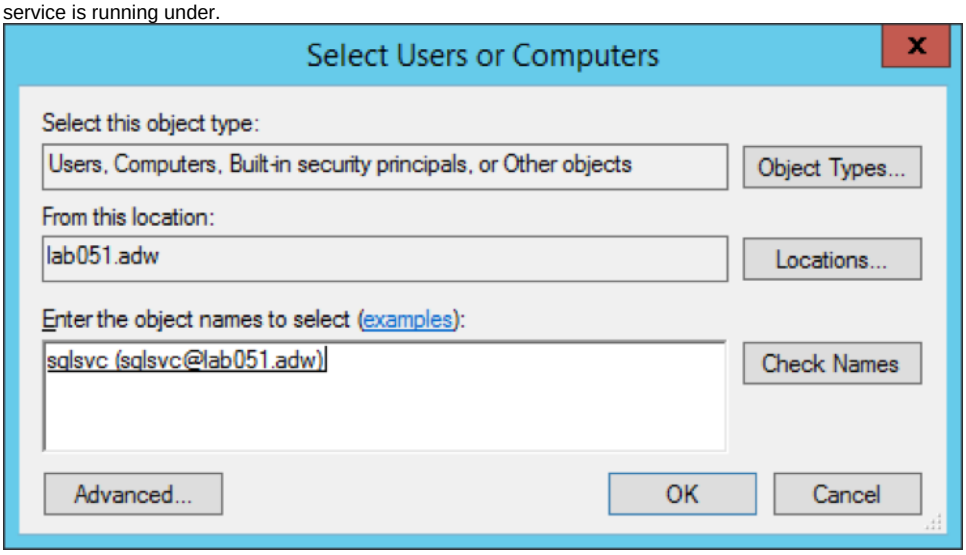


    c. Select **Trust this computer/user for delegation to specified services only**.
    d. Select **Use Kerberos only**.
    e. Click **Add**.

i. On the **Add Services dialog**, click **Users or Computers**.

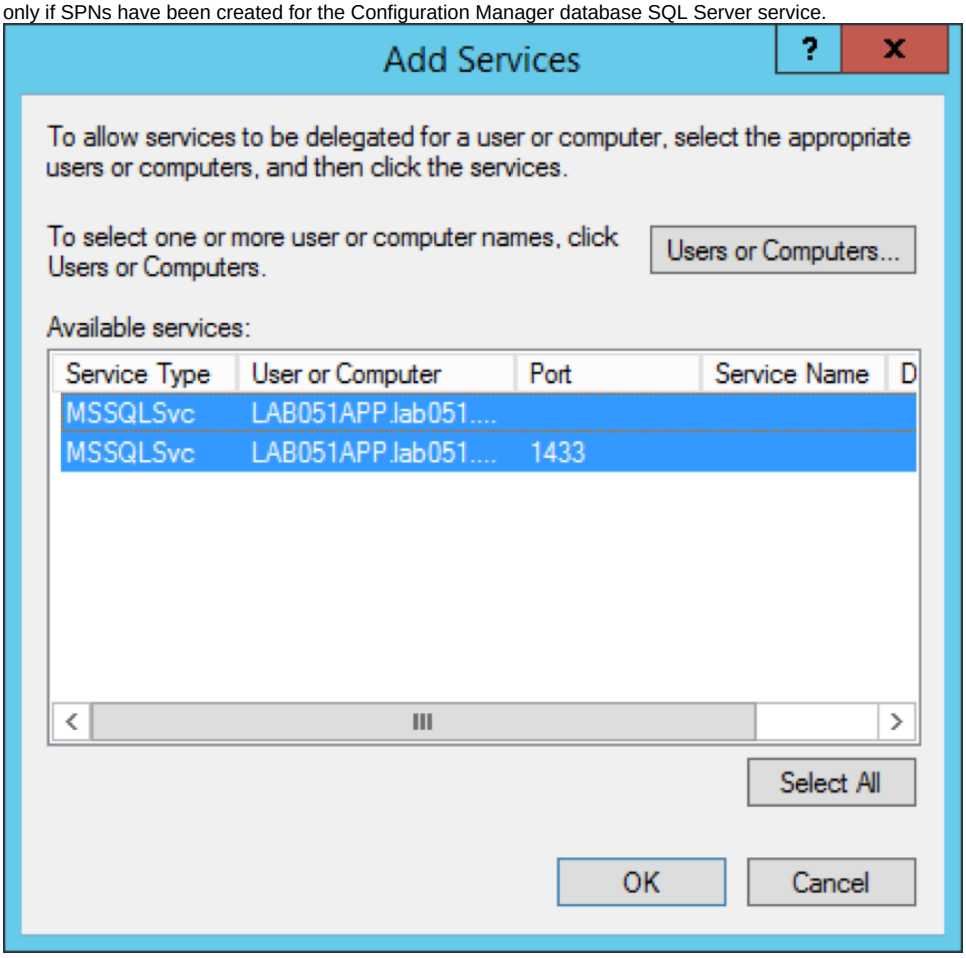


ii. On the **Select Users or Computers dialog**, enter the service account the Configuration Manager database SQL Server service is running under.



iii. Click **OK**.

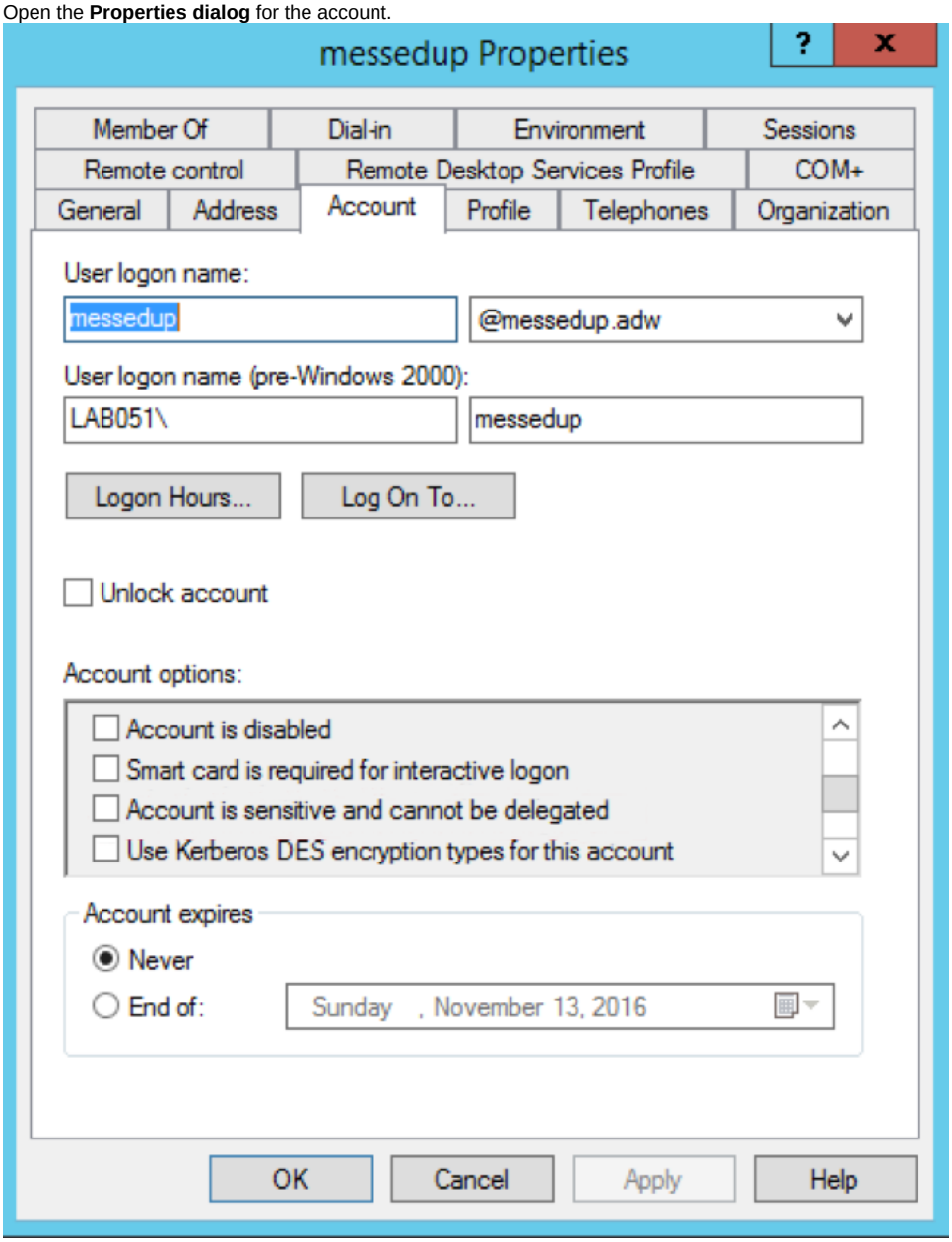
iv. The Add Services dialog displays all of the services associated with that service account. MSSQLSvc services will exist only if SPNs have been created for the Configuration Manager database SQL Server service.



v. Click **OK** to save and close the **Add Services dialog**.
vi. Ensure the MSSQLSvc services you selected are listed.
vii. Click **OK** to save and close the **Properties dialog**.

5. Open **Active Directory Users and Computers** to verify that the account you are using as the ActiveEfficiency service account can be delegated:

a. Open the **Properties dialog** for the account.



b. Under **Account options**, ensure that check box for **Account is sensitive and cannot be delegated** is **not ticked**.

> This step is required only if the Active Efficiency service is running under a domain user account. This is not usually the case.

c. Click **OK**.

6. Close **Active Directory and Users**.
7. If SQL Server is already installed, restart the ActiveEfficiency database server.
8. If ActiveEfficiency isn't already installed, install it now.
9. If ActiveEfficiency is already installed and you are troubleshooting the `Login failed for user 'NT AUTHORITY\ANONYMOUS LOGON` error message, restart the ActiveEfficiency service.
10. Open the ActiveEfficiency `service.log`
    - Ensure that the Nomad synchronization process completes successfully
    - Shortly after the service starts, you should see an entry like: `INFO : Started Nomad sync, type: Modified`. This should be followed by a `INFO : Finished Nomad sync`

Sizing and deployment considerations

Please review the documentation for each 1E product that uses ActiveEfficiency. If you are using ActiveEfficiency for multiple 1E products, ensure you add together each of the separate resource requirements.