Installing Security Suite

Contents

Preinstallation Tasks

These tasks should be completed before the service engineer arrives to install the instrument.

Task Overview

1. Determine the installation configuration to be used
2. Create dedicated accounts to run the Secure Data Storage and Audit Log services
3. Create the Secure Data Storage folder with appropriate permissions
4. If the Secure Data Storage folder will be on the network, set up the share
5. If using a database server for the audit log, set up the database

Task Details

Installation Configuration

There are 2 primary installation configurations: Single Computer and Distributed. The primary difference is whether all access control, policy management, and data storage will occur on the instrument computer or not.

Single Computer

All access control, policy management, and data storage will occur on the instrument computer. The computer may or may not be connected to a network. The customer's IT organization will only need to be involved if the computer is a member of a domain to set up an account that is a member of the local Administrators group to allow the software installation.

Distributed

If either access control and policy management or data storage will be in a centralized location, the installation is considered distributed. Distributed installations require the involvement of the customer's IT organization to set up domain accounts, network shares, and databases.

In a distributed configuration, there are 3 supported sub-configurations:

1. Option 1 – data storage is on a network folder, but access control and policy management are on the instrument computer
2. Option 2 – access control, policy management, and data storage are on a single network computer separate from the instrument computer. This may be a network server or another workstation
3. Option 3 – access control and policy management are on a network computer separate from the instrument computer and data storage is on another network computer separate from both. These may be network servers or other workstations

NOTE: Access control and policy management require administrative rights to the computer being used for this function.

NOTE: For options 2 and 3, a database engine is recommended for the audit data. Without a separate database engine, the audit information can only be reviewed on the computer used for access control and policy management.

In addition to these options, a distributed configuration may have multiple instruments or dedicated audit review workstations installed. When a distributed installation is chosen, these options are presented to the installer (see Installation Tasks below).

Security Server

Throughout this document, the term *Security Server* is used to indicate the computer used for access control and policy management.

Service Accounts

Security Suite requires at least one and, preferably, two service accounts to store data and the audit trail information in a secure manner. Two accounts are preferred since they are used for different kinds of data and two accounts allows the permissions to be very narrowly granted.

NOTE: If a database server without integrated security is being used for the audit log storage, only 1 service account is required.

In an environment where the computers are joined to a Microsoft Active Directory domain, a Managed Service Account (additional information here) is the preferred account type as the password management is automated.

If the computer is not joined to an Active Directory domain or the IT department is reluctant to use Managed Service Accounts, a standard user account will suffice. This account should:

1. Have password expiration disabled
2. Be granted the “Log on as a service” right
3. Be denied the “Log on locally” and “Log on through Remote Desktop Services” rights

Secure Data Storage Folder

The Secure Data Storage folder can either be on the local computer or on a server. If it is on a server, it must be shared so that the remote computers can access it and it will be referenced using the UNC path in Security Administrator (e.g. \\server\share)

NOTE: If the local computer is used, the folder cannot be the OMNIC Data Directory (typically C:\My Documents\OMNIC).

The security permissions for the folder must be modified to allow the service account that will be used for the Secure Data Storage service **Full Control** and all other users **Read & Execute**. If a backup service is being used and needs more permissions, that can be included, but typical network users should only have **Read & Execute** permissions.

NOTE: Granting users more permissions than this results in a data folder that can have datafiles modified or injected without proper audit logging.

Security permissions for the network share should be no more restrictive than the NTFS permissions. By default, Microsoft only grants the **Read** permission to **Everyone**. This is enough for the average user but prohibits the Secure Data Storage service from being able to write the data to the location.

Database Server

NOTE: This section only applies if a database server will be used to store the audit log.

If a database server will be used for the audit log storage (recommended for distributed installations), the database must be created before the installation. The schema will be created automatically by the Audit Log service once it is installed.

Currently, Security Suite supports Microsoft SQL Server 2012 or newer, Oracle 11g Release 2 or newer, and MariaDB 10 or newer.

Integrated Security

If integrated security will be used for the database (recommended), the service account used to run the Audit Log service must be granted **Read / Query**, **Write / Insert**, and **Create / Update Schema** privileges for the database. All other users must be granted **Read / Query** privileges for the database. Failure to grant a user the **Read / Query** privilege will result in that user being unable to review the audit log.

Dedicated Users

If integrated security will not be used for the database, 2 accounts will need to be created in the database:

1. An account for the log service to use. This account must be granted **Read / Query**, **Write / Insert**, and **Create /Update Schema** privileges
2. An account for the viewer to use. This account must be granted **Read / Query** privileges

Task Walkthrough

This section provides a detailed walkthrough of the preinstallation steps. It does not include database configuration, domain account creation, or Managed Service Account creation as these tasks require specialized permissions and knowledge.

NOTE: These walkthroughs assume that the user performing them is a member of the **Administrators** group on the local computer.

Service Account Creation

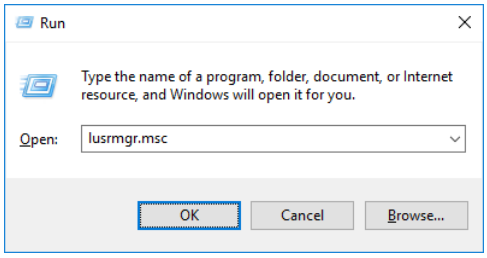
This section covers creating and configuring service accounts for a Single Computer installation.

Account Creation

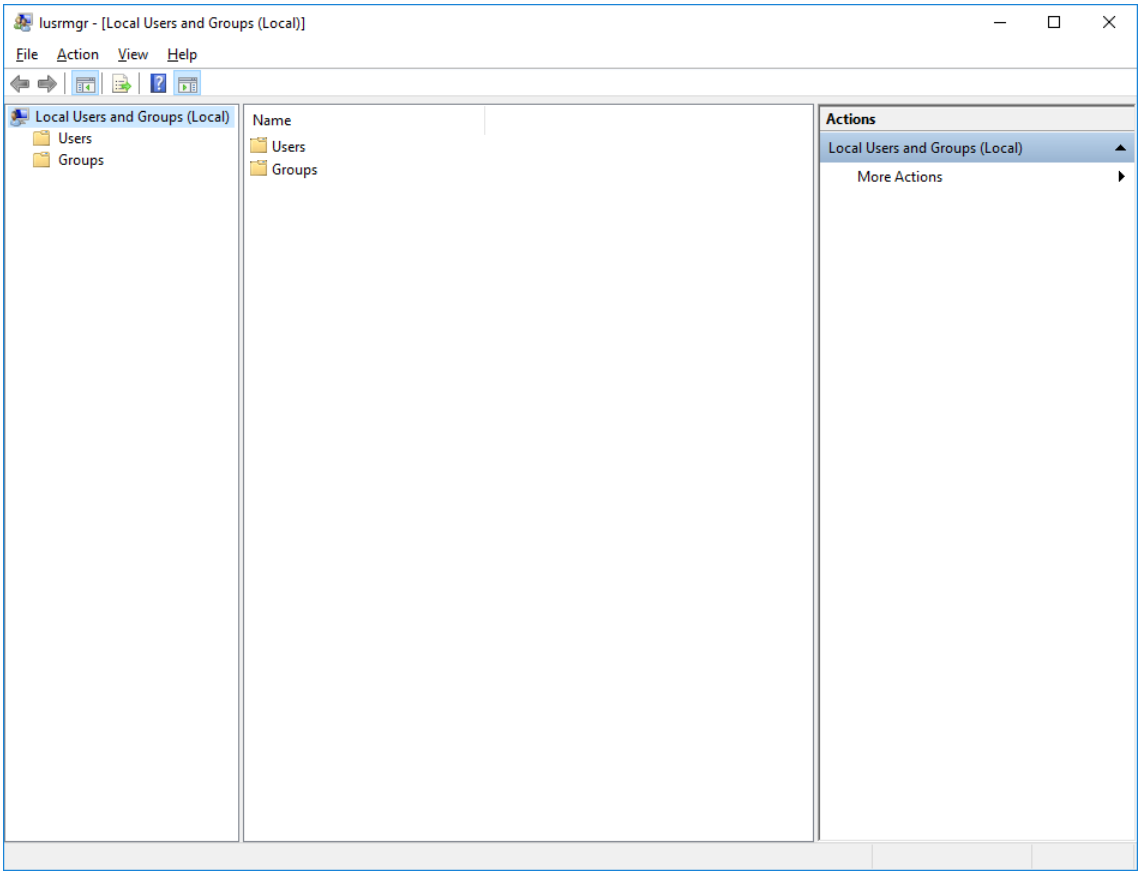
1. Open the Local Users and Groups management console:

a. Press ⊞+R

b. Type *lusrmgr.msc*

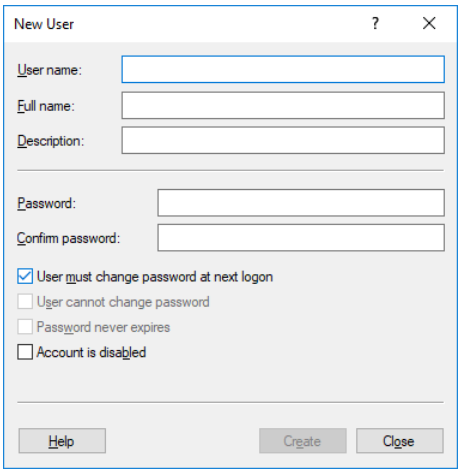


c. Click **OK**

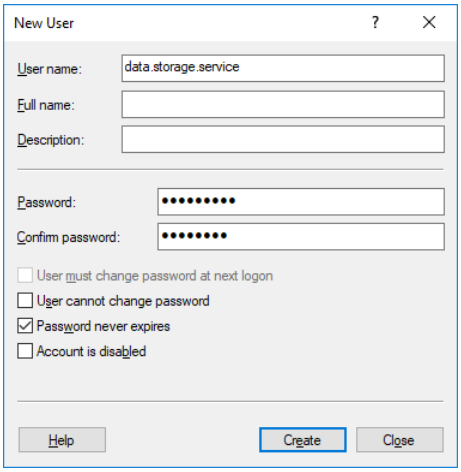


2. Open **Users**

3. Click **Action→New user…**



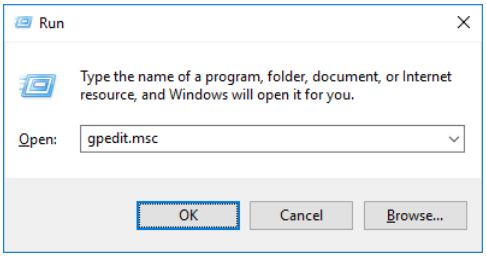
4. Set up the Secure Data Storage service account:
    a. Enter the **User name** (e.g. data.storage.service, audit.log.service, etc.)
    b. Enter the **Password** and **Confirm password**
    c. Uncheck **User must change password at next logon**
    d. Check **Password never expires**



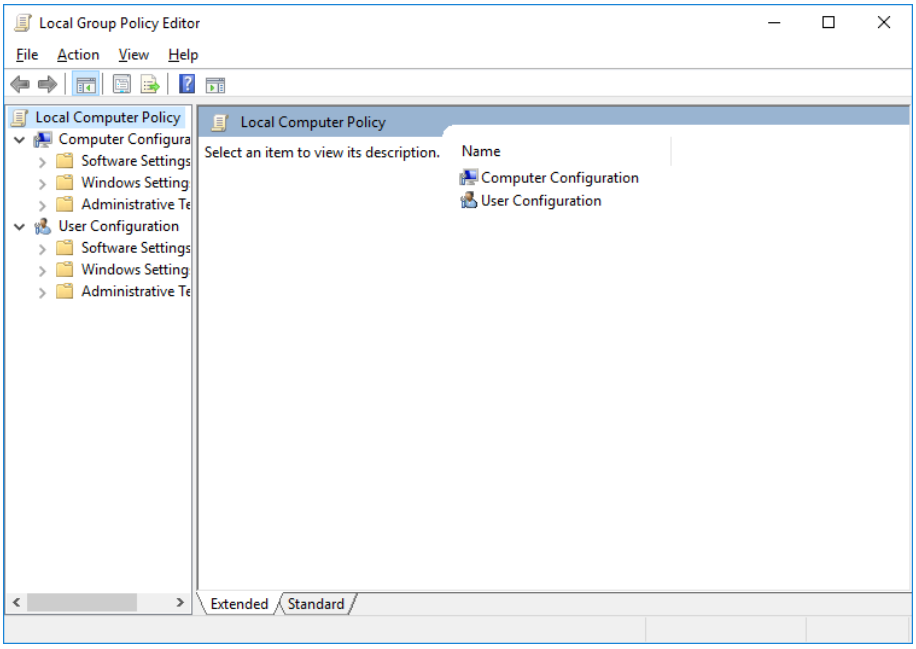
5. Click **Create**
6. Repeat Steps 4 and 5 for the Audit Log service account if one is needed
7. Click **Close**
8. Close the Local Users and Groups window

Configure Log on Rights

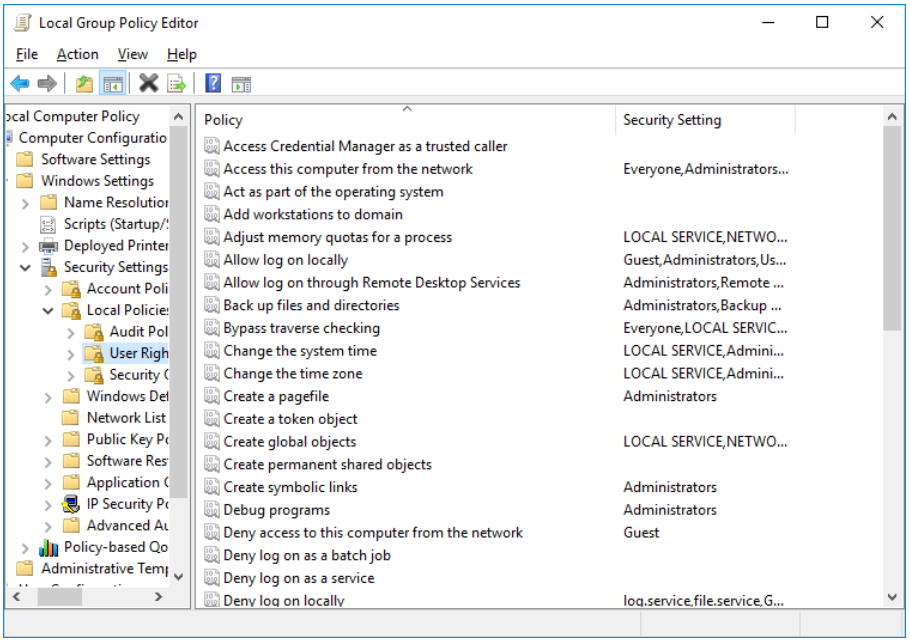
1. Open the Local Group Policy Editor management console:
    a. Press ⊞+R
    b. Type *gpedit.msc*



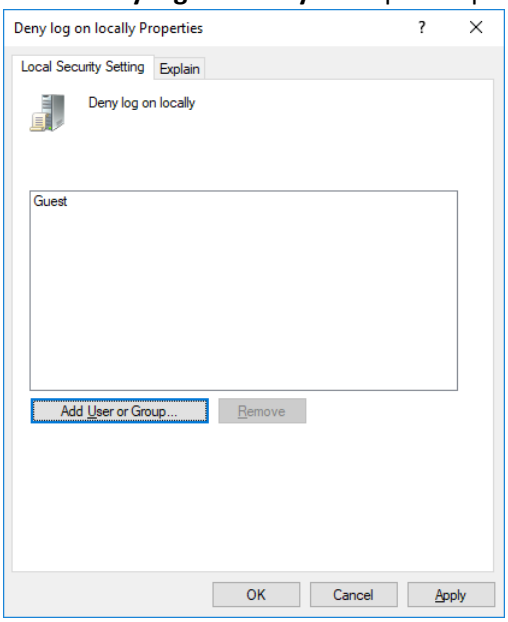
    c. Click **OK**



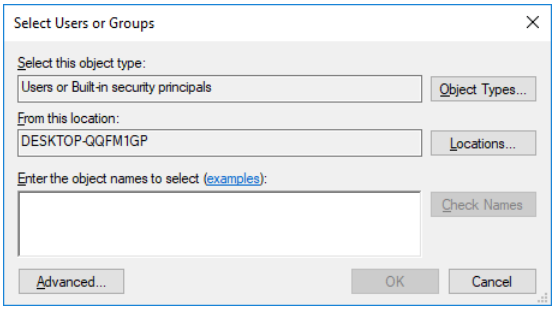
2. Navigate to **Computer Configuration→Windows Settings→Security Settings→Local Policies→User Rights**



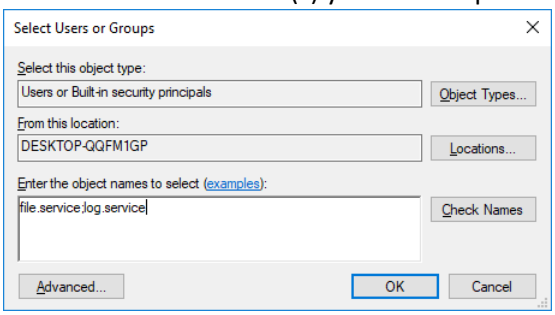
3. Select **Deny log on locally** and open its properties



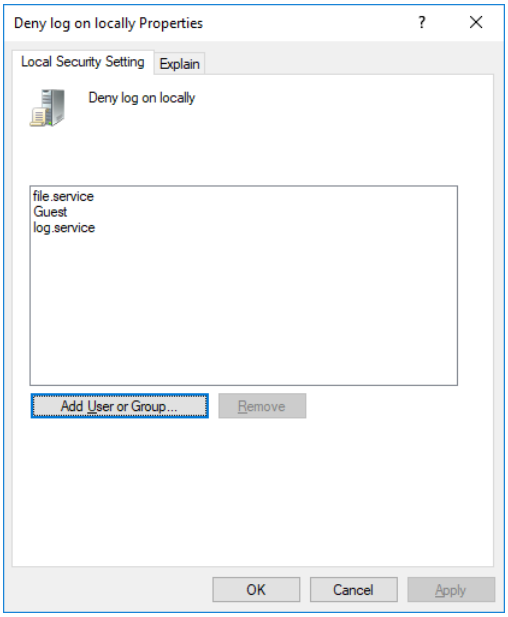
4. Click **Add User or Group…**



5. Enter the account name(s) you created previously separated by a semicolon



6. Click **OK**



7. Click **OK**
8. Repeat Steps 3 through 7 for **Deny log on through Remote Desktop Services** and **Log on as a service**
9. Close the Local Group Policy Editor window

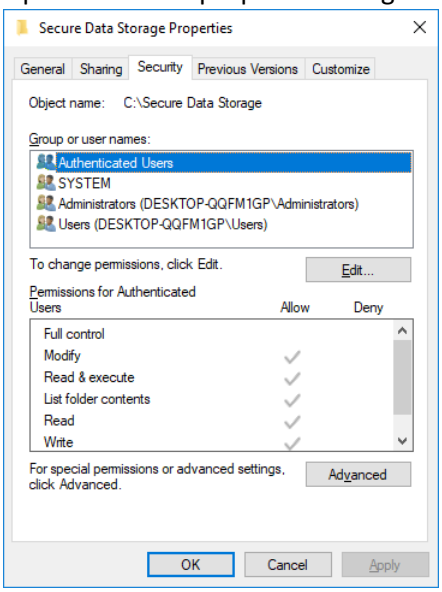
Secure Data Storage Folder Creation

This section covers creating the secure data storage folder and setting up its security appropriately. It is the same procedure for a local or network folder although a network folder will require administrator access to the network server.

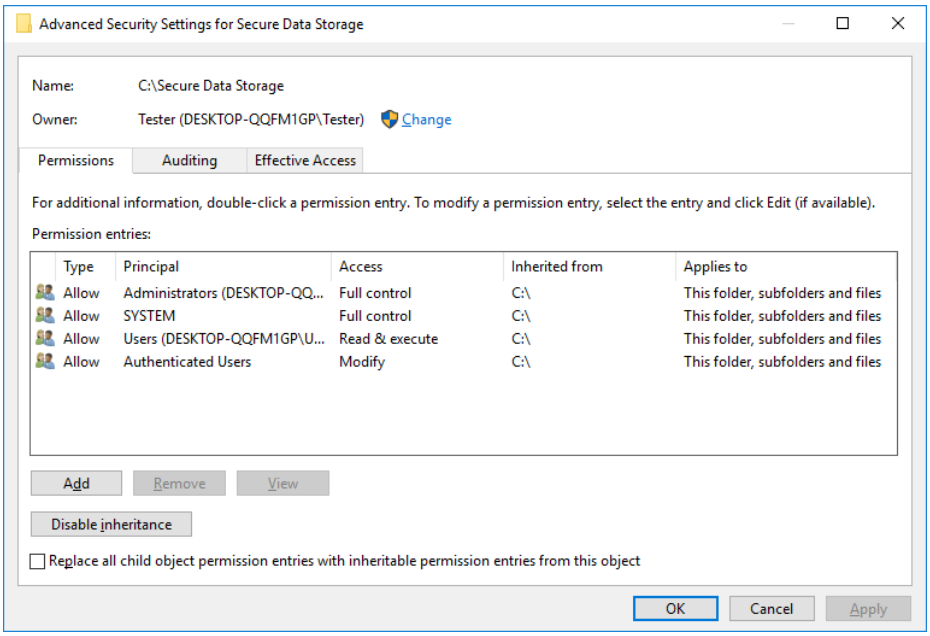
Windows 8 and Newer

1. Create the desired folder using Windows Explorer

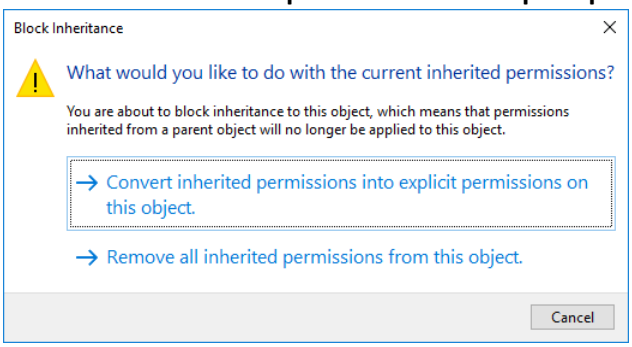
2. Open the folder properties and go to the **Security** tab



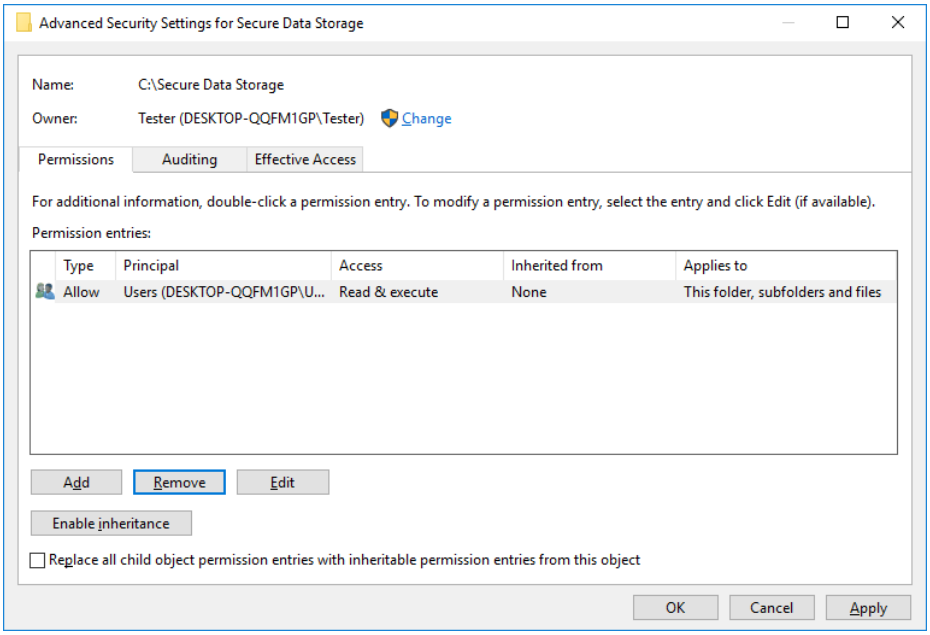
3. Click **Advanced**



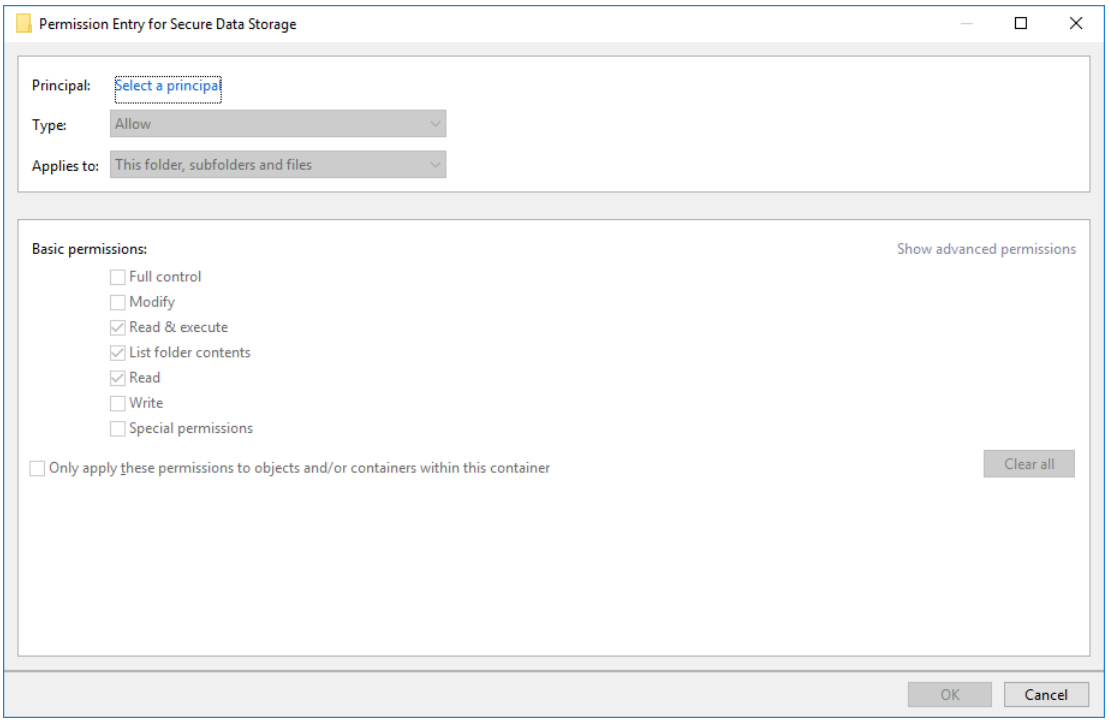
4. Click **Disable inheritance**
5. Click **Convert inherited permissions into explicit permissions on this object**



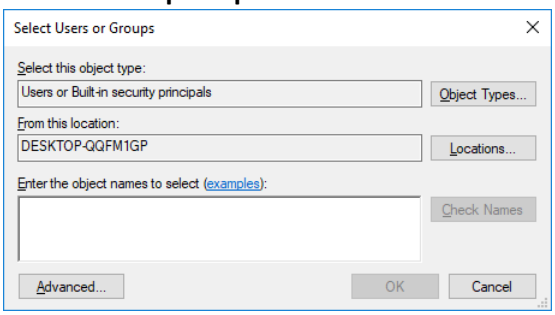
6. Select **Administrators** and click **Remove**
7. Repeat Step 6 for **SYSTEM** and **Authenticated Users**



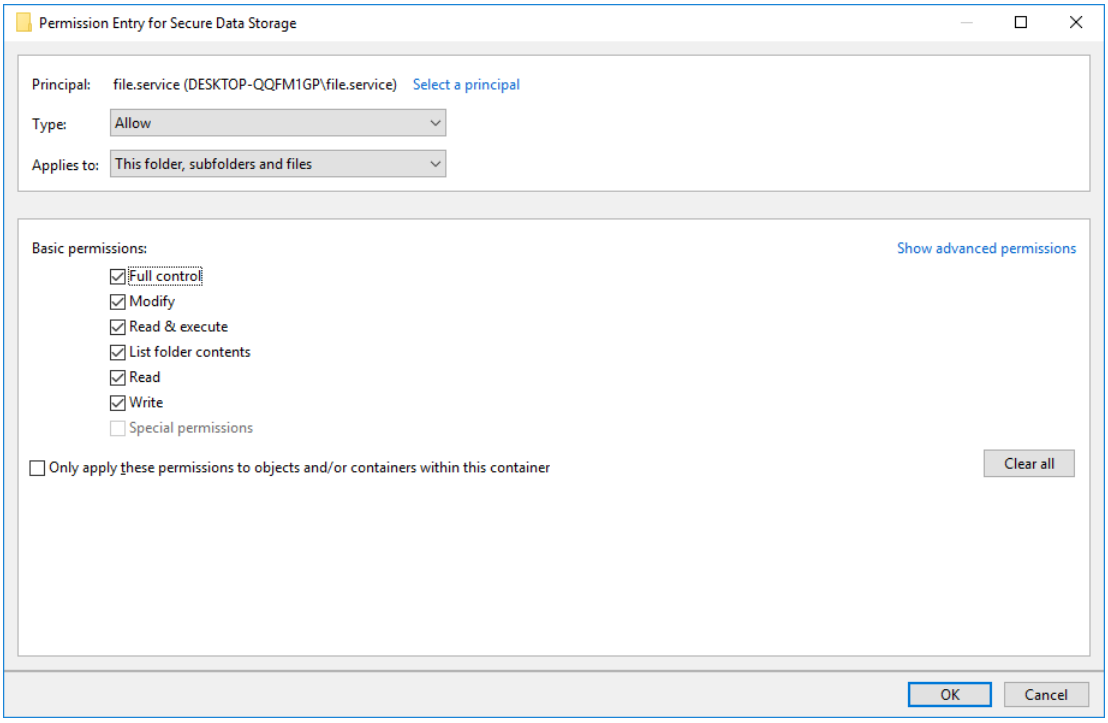
8. Click **Add**



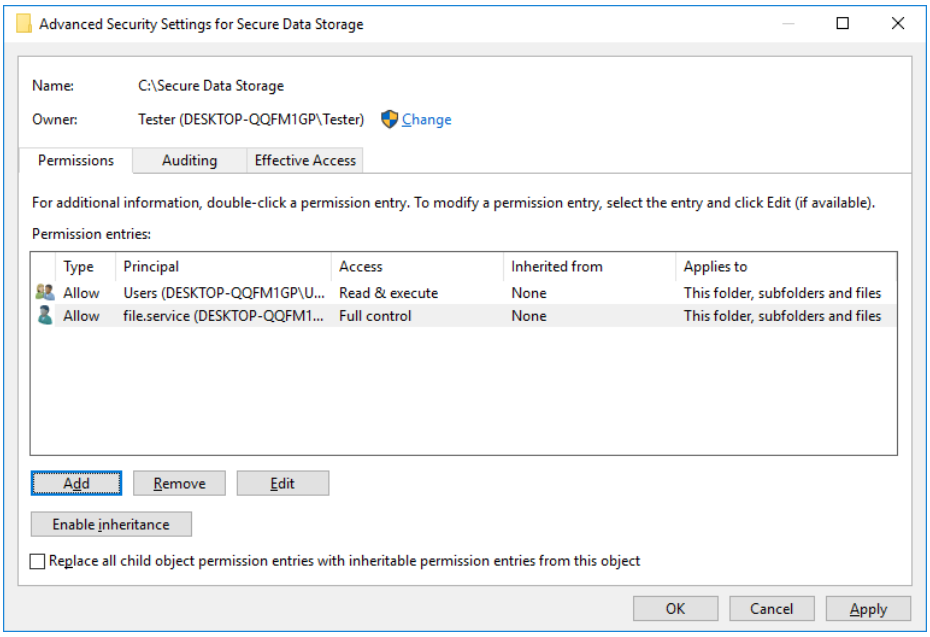
9. Click **Select a principal**



10. Enter the account name for the Secure Data Storage service
11. Click **OK**
12. Check **Full Control**



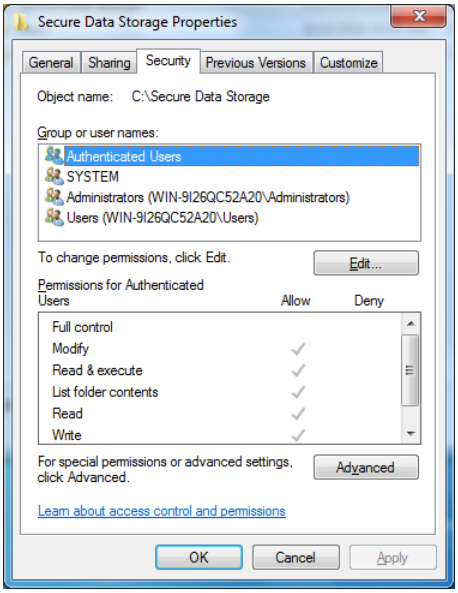
13. Click **OK**



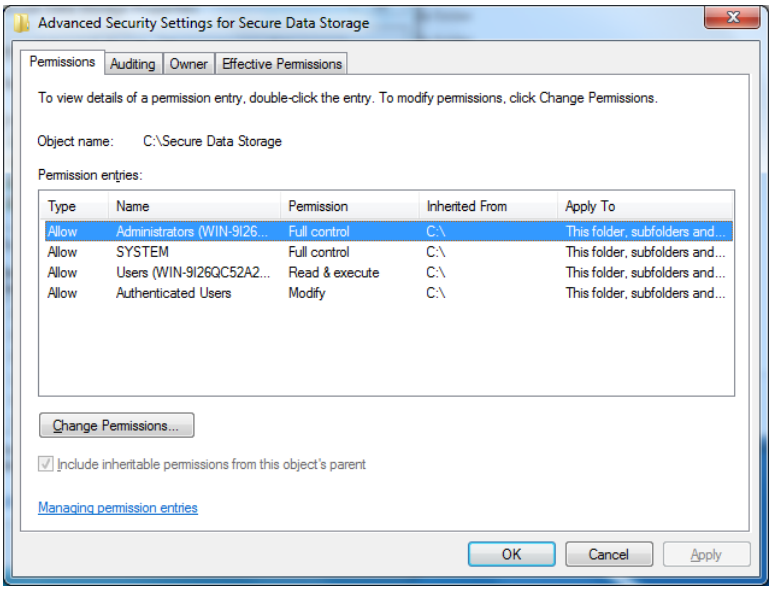
14. Add any additional users that need special rights (e.g. backup service accounts)
15. Click **OK**
16. Click **OK**

Windows 7

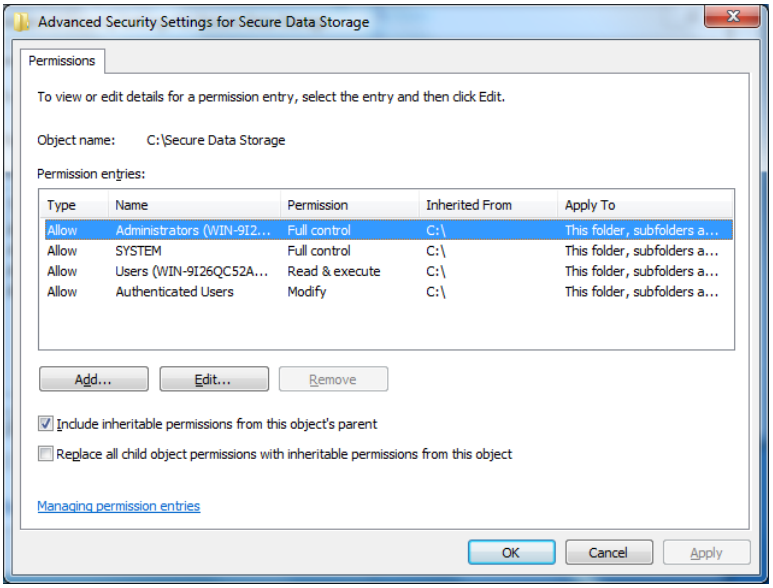
1. Create the desired folder using Windows Explorer
2. Open the folder properties and go to the **Security** tab



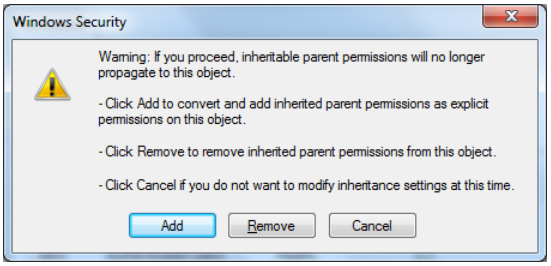
3. Click **Advanced**



4. Click **Change Permissions…**

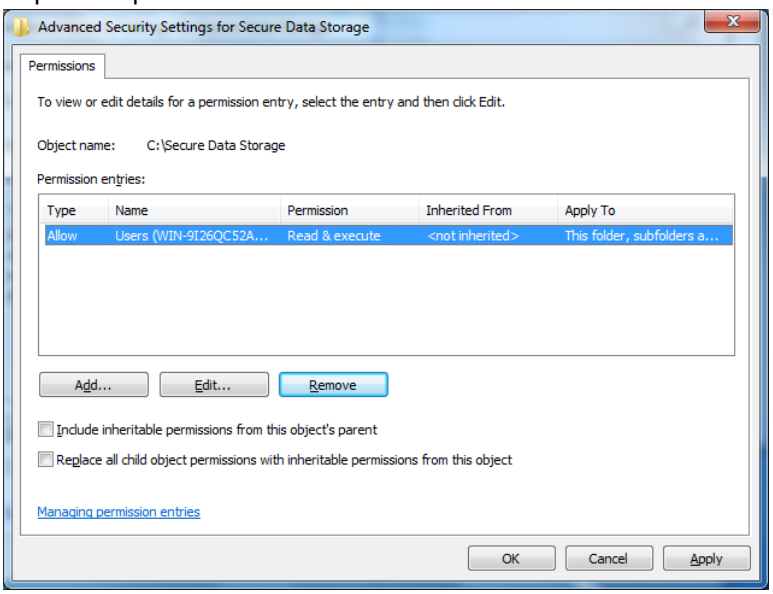


5. Uncheck **Include inheritable permissions from this object's parent**

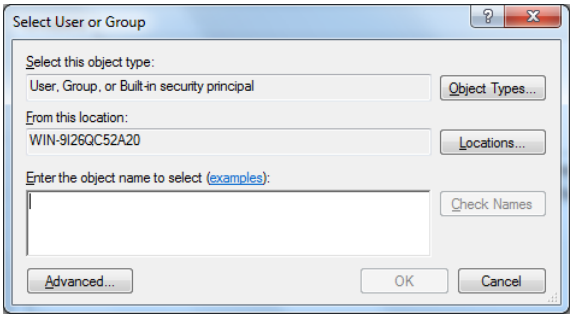


6. Click **Add**
7. Select **Administrators** and click **Remove**

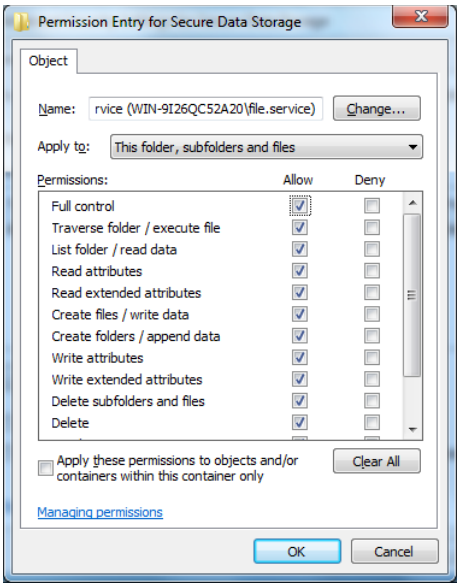
8. Repeat Step 6 for **SYSTEM** and **Authenticated Users**



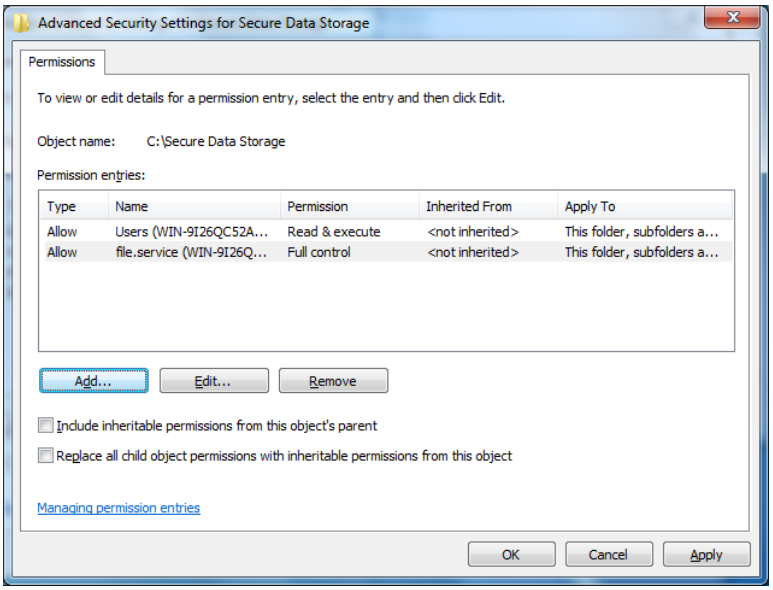
9. Click **Add…**



10. Enter the account name for the Secure Data Storage service
11. Click **OK**
12. Check **Full Control**



13. Click **OK**



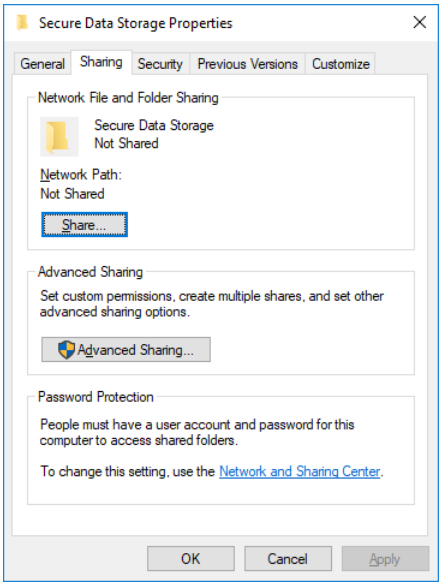
14. Add any additional users that need special rights (e.g. backup service accounts)
15. Click **OK**
16. Click **OK**
17. Click **OK**

Share Secure Data Storage Folder

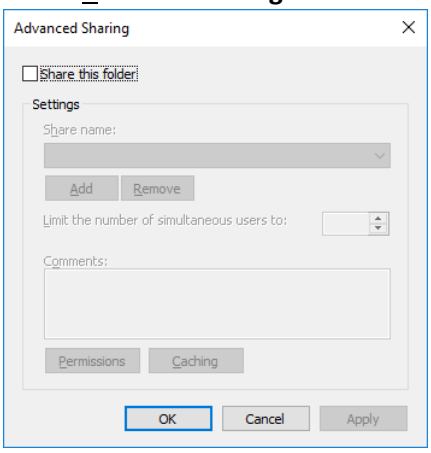
This section covers sharing the secure data storage folder.

NOTE: This only applies to distributed configurations where the data is stored on a network folder.

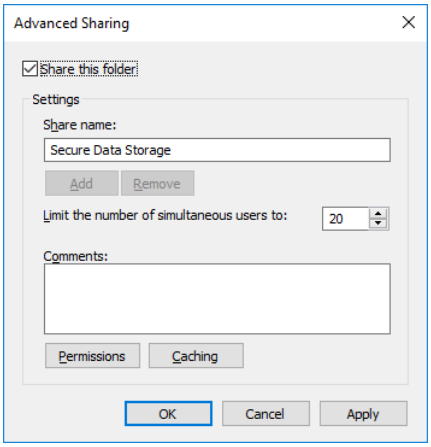
1. Open the Secure Data Folder properties in Windows Explorer and go to the **Sharing** tab



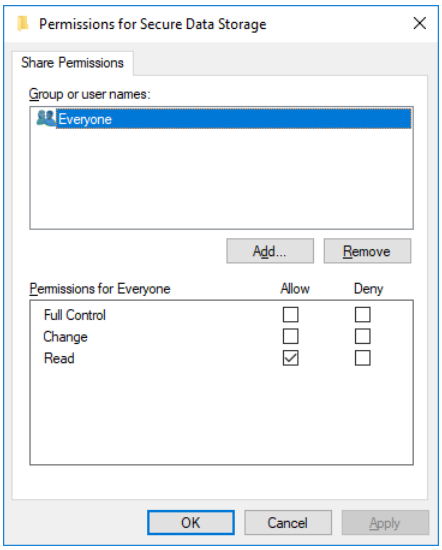
2. Click **Advanced Sharing…**



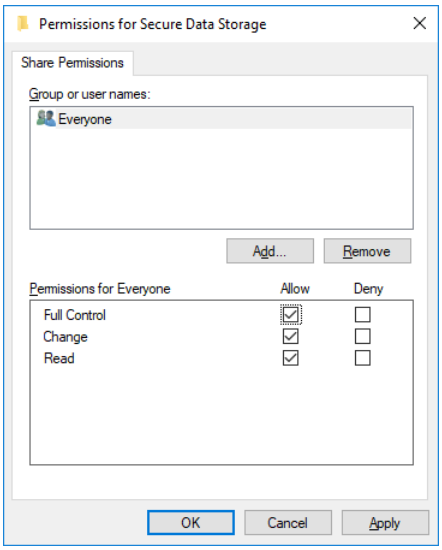
3. Check **Share this folder**



4. Update the **Share name** if desired
5. Click **Permissions**



6. Check **Full Control**



NOTE: If the customer site has other permission conventions for network shares, please observe them. Ensure that the account for the Secure Data Storage service is granted **Full Control** permissions.

7. Click **OK**
8. Click **OK**
9. Click **OK** or **Close**

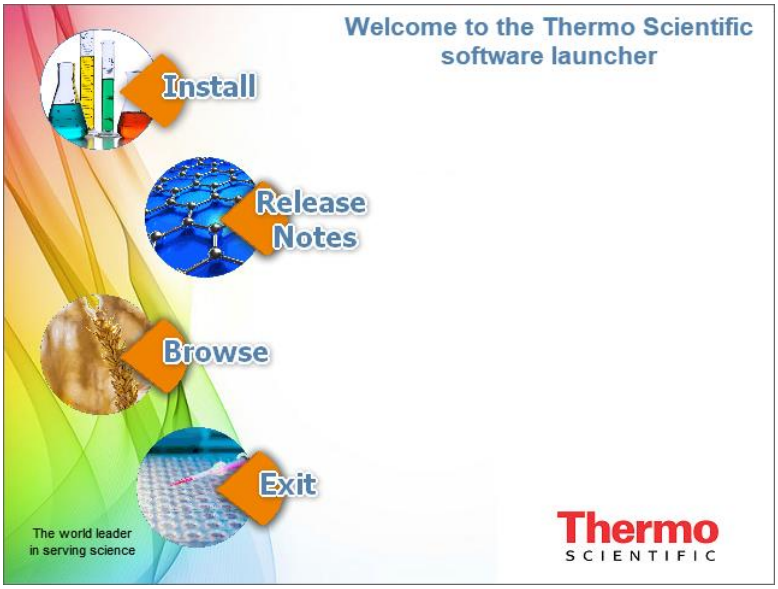
Installation Tasks

Once the pre-installation tasks have been completed, the software can be installed.

NOTE: All installations start on the Instrument Computer whether a distributed configuration is being used or not.

Single Computer

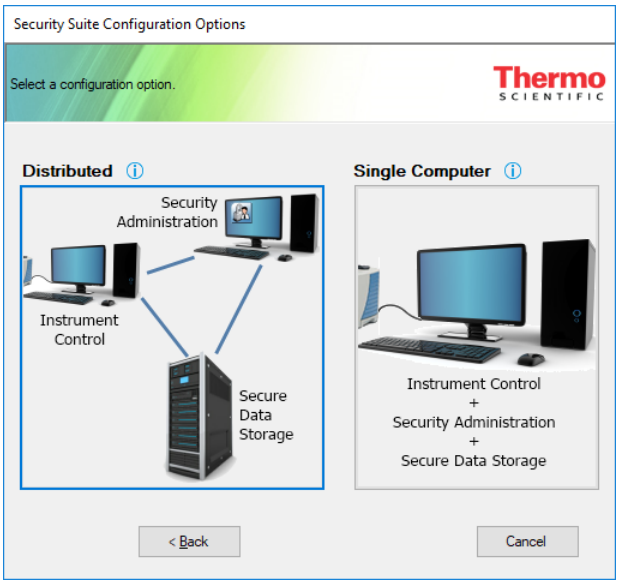
1. Run Start.exe from the installation media



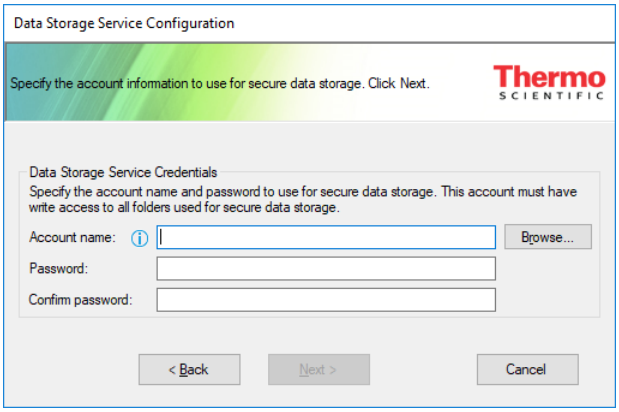
2. Click **Install**

   NOTE: If the .NET Framework needs to be upgraded for this installation, it will automatically install at this time. A reboot may be required, and the installation will proceed automatically after that is complete.

3. Step through the installation process to the *Security Suite Configuration Options* screen

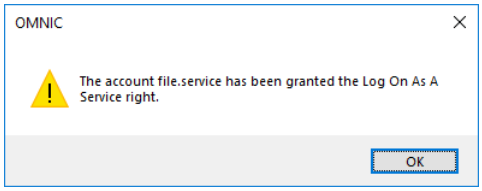


4. Choose **Single Computer**



5. Enter the Secure Data Storage service account name and password
6. Click **Next >**

   NOTE: You may see a dialog informing you that the Secure Data Storage service account has been granted the Log On as a Service right.



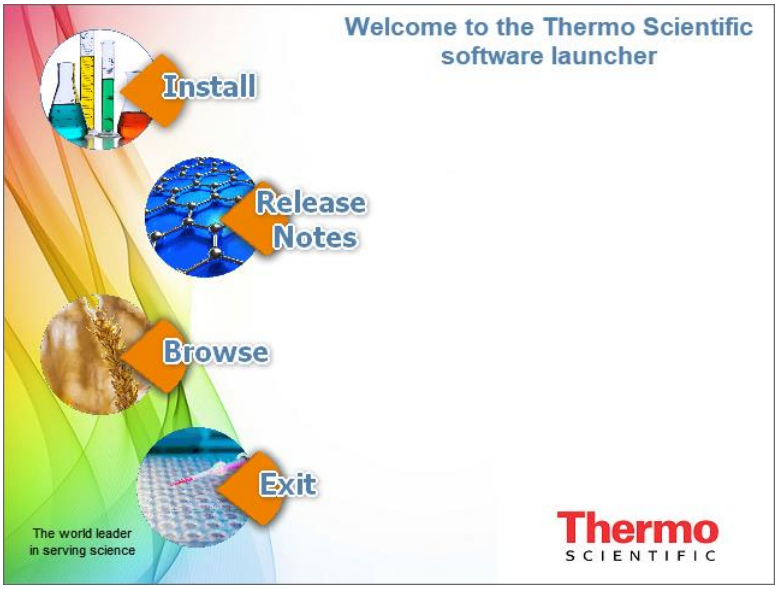
7. Continue the installation process.
8. After the software has installed, the Audit Log Service Database Configuration window will appear. Follow the instructions in (Re)configure the Audit Log Service below to set up the database connection.

9. Click **OK** to complete the installation
10. Follow the instructions in (Re)configure the Data Storage Folder below to configure the data storage location
11. Perform all remaining installation qualification tasks

    NOTE: The first time OMNIC opens, it will take extra time to copy the sample data and default configuration information to the Secure Data Folder

Distributed

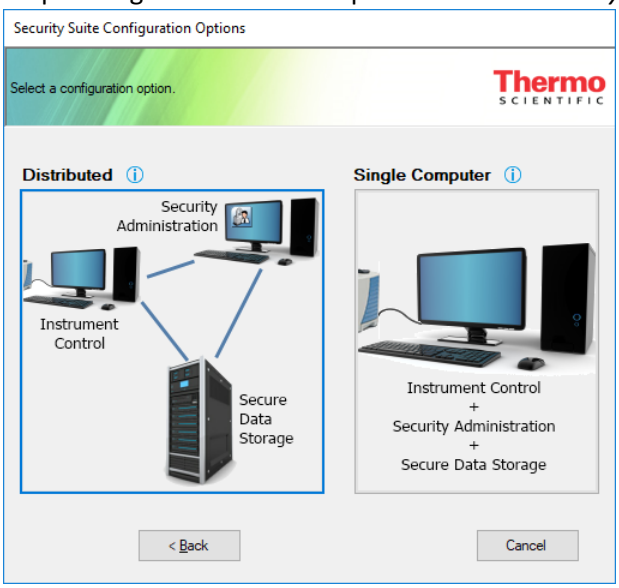
1. Run Start.exe from the installation media



2. Click **Install**

    NOTE: If the .NET Framework needs to be upgraded for this installation, it will automatically install at this time. A reboot may be required, and the installation will proceed automatically after that is complete.

3. Step through the installation process to the *Security Suite Configuration Options* screen



4. Choose **Distributed**

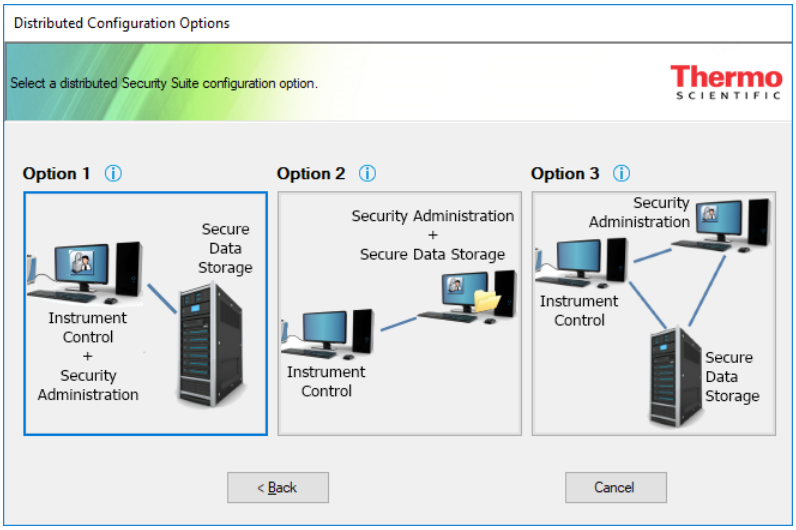
5. Choose the appropriate step:
    a. **Initial Instrument** is for the first instrument to be installed using a given set of computers
    b. **Subsequent Instruments** is for any additional instruments that will utilize the previously installed security server and data storage computer(s)
    c. **Audit Manager** is to install just the Audit Manager on a workstation to be used for reviewing the audit data

Initial Instrument

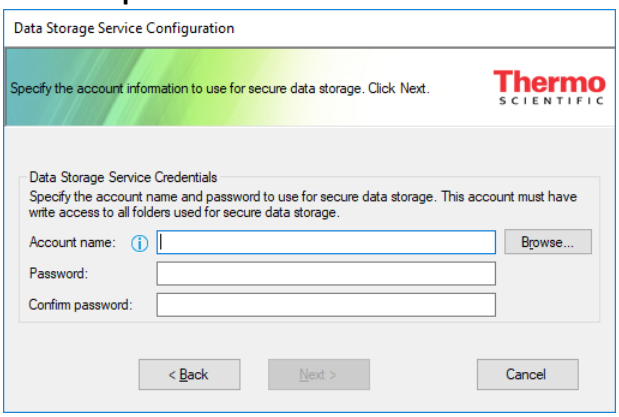
See Distributed above for a description of the options.

Option 1

1. Clicking **Initial Instrument** brings up the *Distributed Configuration Option* screen

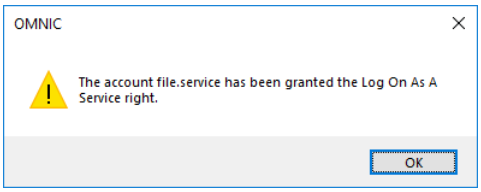


2. Click on **Option 1**

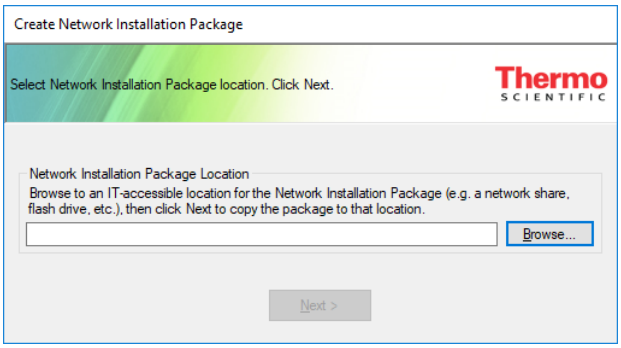


3. Enter the Secure Data Storage service account name and password
4. Click **Next >**

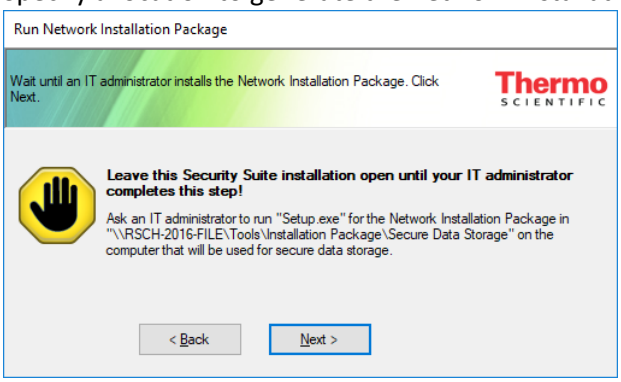
NOTE: You may see a dialog informing you that the Secure Data Storage service account has been granted the Log On as a Service right.



5. Continue the installation process.
6. After the software has installed, the Create Network Installation Package screen will appear



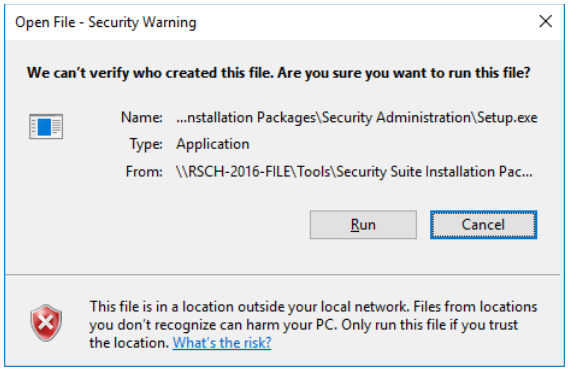
7. Specify a location to generate the network installation package in and click **Next >**



8. Have the customer's IT organization install the generated package on the computer to be used for secure data storage

   NOTE: There are no steps or prompts in this installation that differ from a typical software install.

   NOTE: If the IT organization receives a notification like the one below, they will need to copy the installation folder to the computer they are installing the package on and try again.

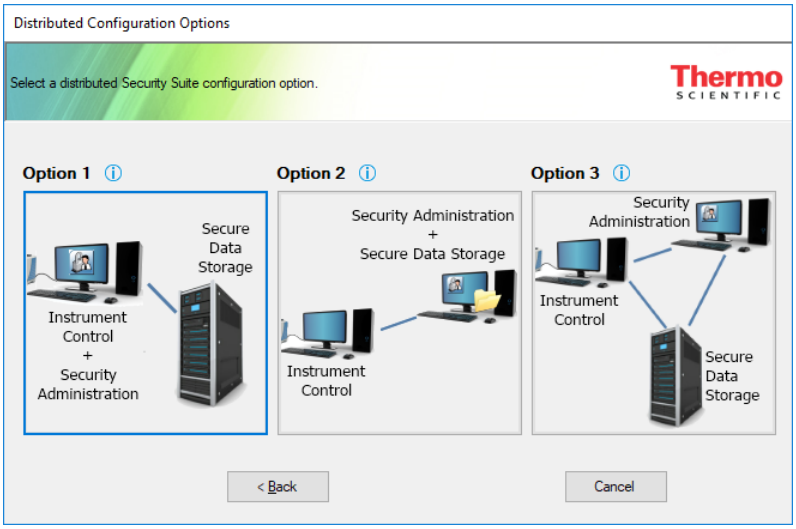


9. Once the customer IT organization has completed the installation, click **Next >**.
10. The Audit Log Service Database Configuration window will appear. Follow the instructions in (Re)configure the Audit Log Service below to set up the database connection.
11. Click **OK** to complete the installation
12. Follow the instructions in (Re)configure the Data Storage Folder below to configure the data storage location
13. Perform all remaining installation qualification tasks

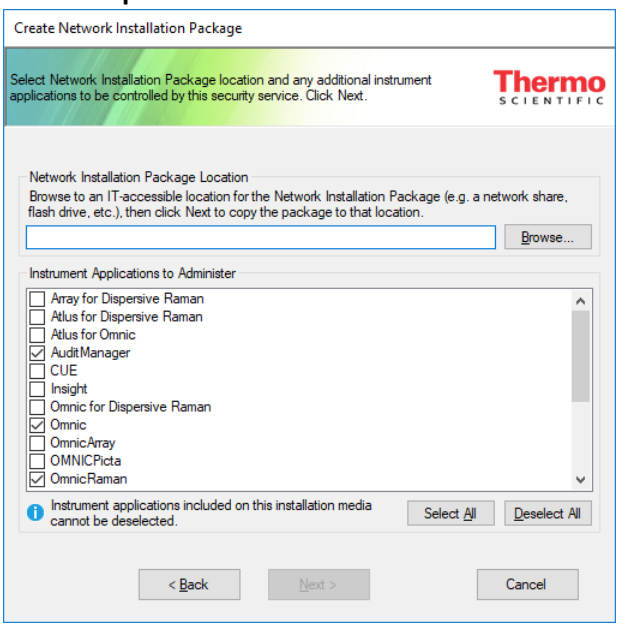
    NOTE: The first time OMNIC opens, it will take extra time to copy the sample data and default configuration information to the Secure Data Folder

Option 2

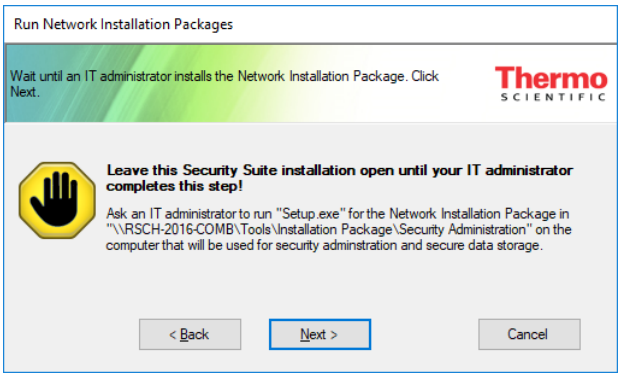
1. Clicking **Initial Instrument** brings up the *Distributed Configuration Option* screen



2. Click on **Option 2**



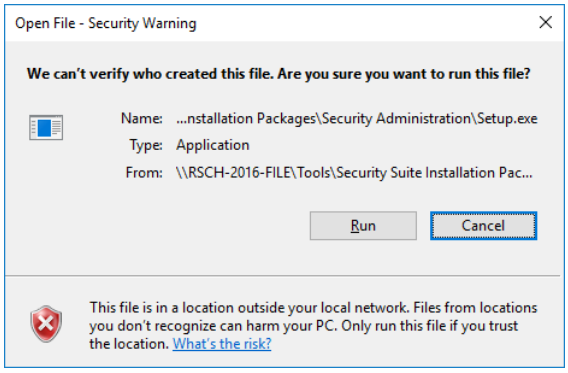
3. Specify a location where the network installation package will be created
4. Select any additional products that will be administered using this computer
5. Click **Next >**



6. Have the customer's IT organization install the generated package on the computer to be used for access control, policy management, and data storage

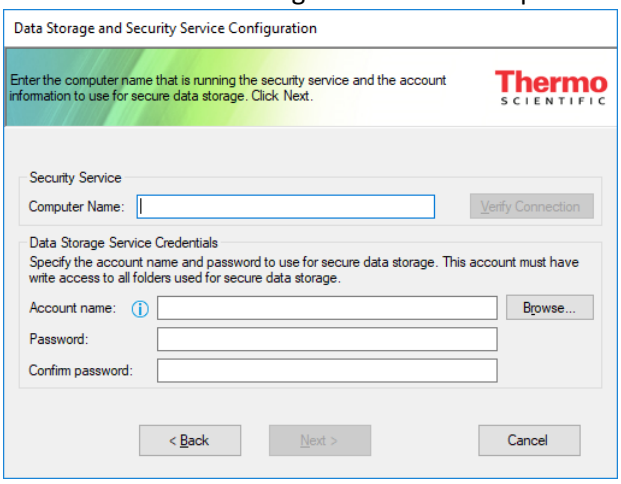
   NOTE: This process will require configuring the audit log service and access controls and policies at the end.

NOTE: If the IT organization receives a notification like the one below, they will need to copy the installation folder to the computer they are installing the package on and try again.



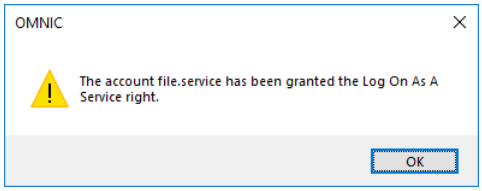
a. When the Audit Log Service Database Configuration window appears, follow the instructions in (Re)configure the Audit Log Service below to set up the database connection
b. Click **OK** to complete the installation
c. Follow the instructions in (Re)configure the Data Storage Folder below to configure the data storage location

7. Once the customer IT organization has completed the installation, click **Next >**



8. Enter the name of the computer used as the security server
9. Enter the Secure Data Storage service account name and password
10. Click **Next >**

NOTE: You may see a dialog informing you that the Secure Data Storage service account has been granted the Log On as a Service right.

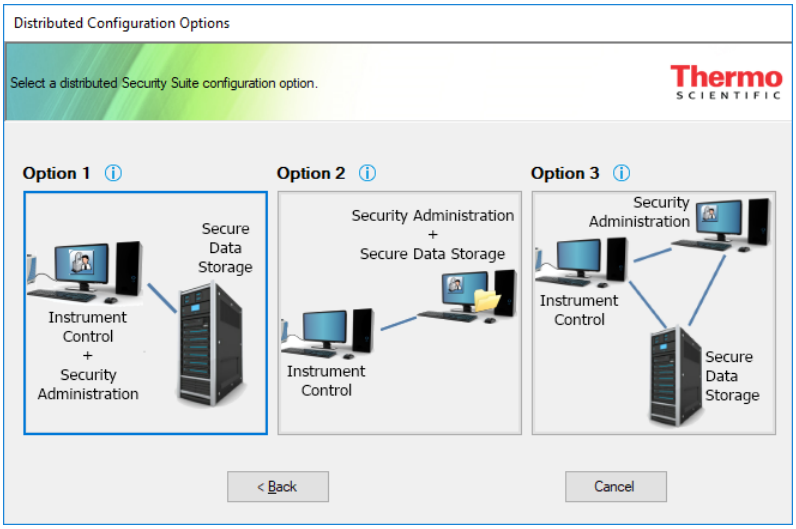


11. Complete the installation process
12. Perform all remaining installation qualification tasks

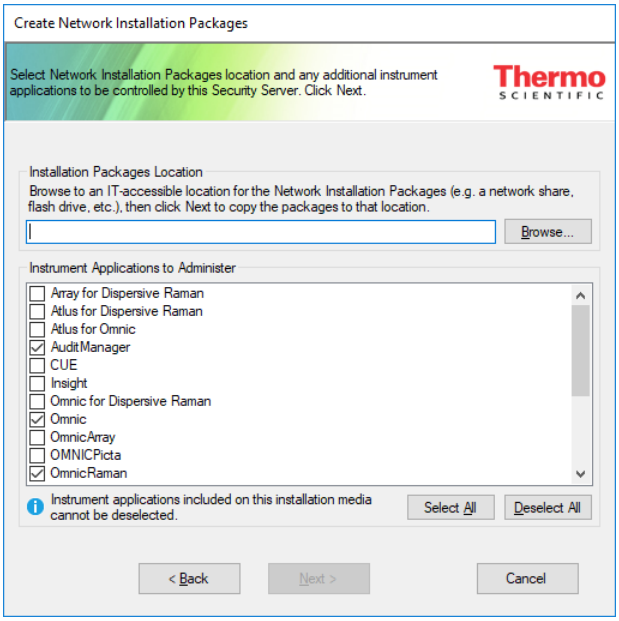
NOTE: The first time OMNIC opens, it will take extra time to copy the sample data and default configuration information to the Secure Data Folder

Option 3

1. Clicking **Initial Instrument** brings up the *Distributed Configuration Option* screen

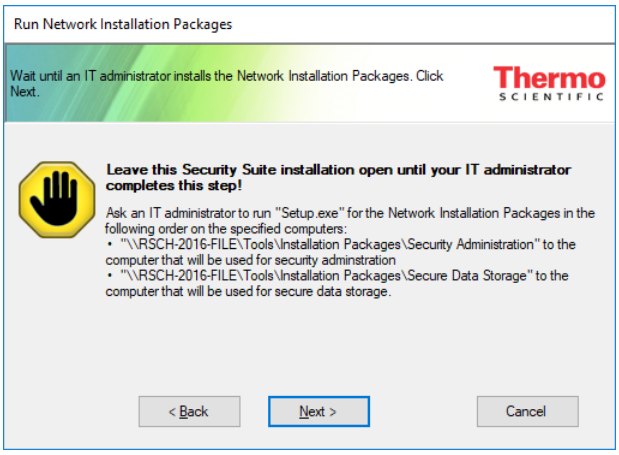


2. Click on **Option 3**



3. Specify a location where the network installation packages will be created
4. Select any additional products that will be administered using this computer

5. Click **Next >**

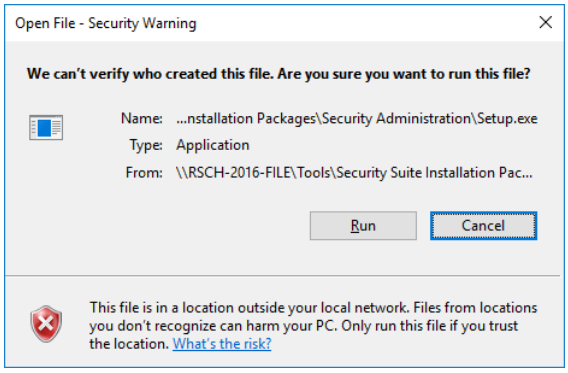


6. Have the customer's IT organization install the generated packages on the computers to be used as the security server and for data storage

   NOTE: The Security Server package must be installed first.

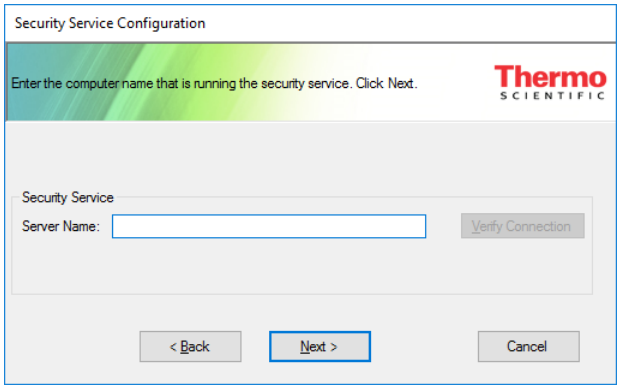
   NOTE: This process will require configuring the audit log service and access controls and policies at the end.

   NOTE: If the IT organization receives a notification like the one below, they will need to copy the installation folder to the computer they are installing the package on and try again.

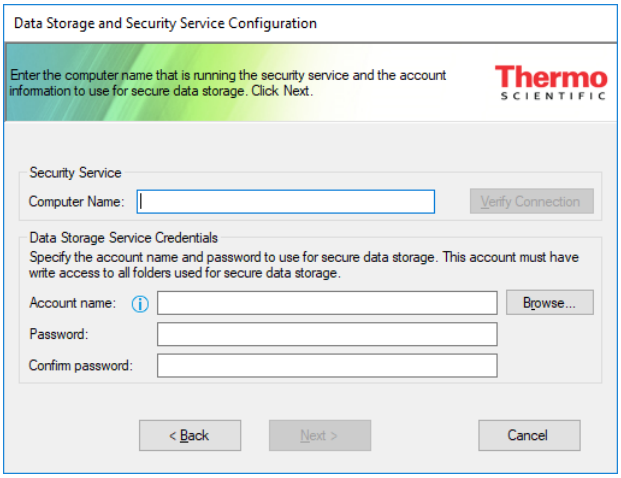


   a. When the Audit Log Service Database Configuration window appears, follow the instructions in (Re)configure the Audit Log Service below to set up the database connection
   b. Click **OK** to complete the installation
   c. Follow the instructions in (Re)configure the Data Storage Folder below to configure the data storage location

d. When prompted during the data storage computer installation, enter the name of the computer used as the security server

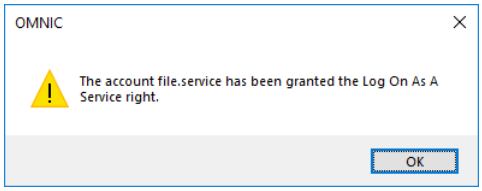


7. Once the customer IT organization has completed the installation, click **Next >**



8. Enter the name of the computer used as the security server
9. Enter the Secure Data Storage service account name and password
10. Click **Next >**

NOTE: You may see a dialog informing you that the Secure Data Storage service account has been granted the Log On as a Service right.

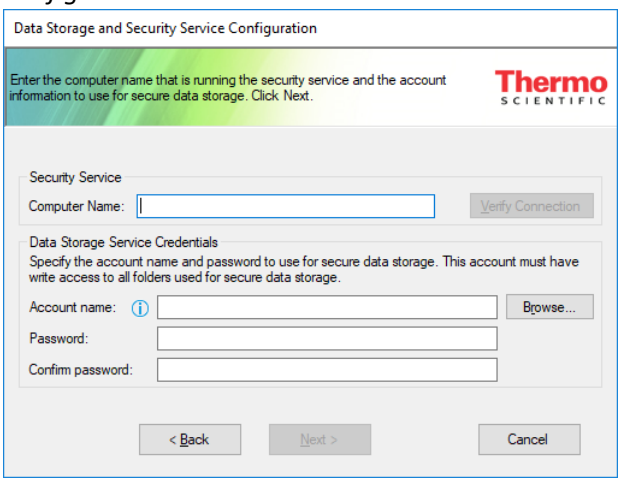


11. Complete the installation process
12. Perform all remaining installation qualification tasks

NOTE: The first time OMNIC opens, it will take extra time to copy the sample data and default configuration information to the Secure Data Folder

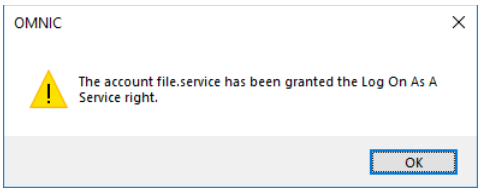
Subsequent Instruments

1. Choosing **Subsequent Instruments** will bring up the *Data Storage and Security Service Configuration* screen



2. Enter the name of the computer used as the security server
3. Enter the Secure Data Storage service account name and password
4. Click **Next >**

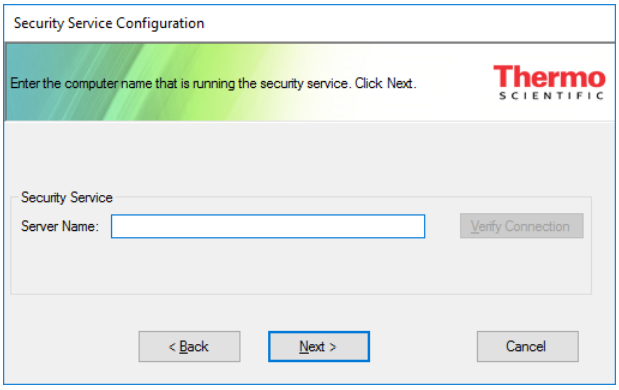
   NOTE: You may see a dialog informing you that the Secure Data Storage service account has been granted the Log On as a Service right.



5. Complete the installation process
6. Perform all remaining installation qualification tasks

Audit Manager

1. Choosing **Audit Manager** will bring up the *Security Service Configuration* screen



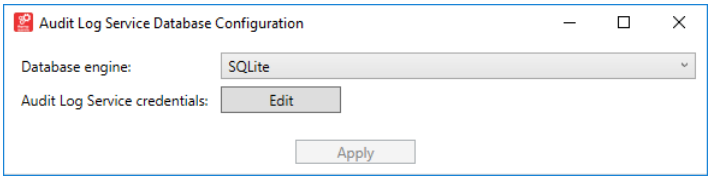
2. Enter the name of the computer used as the security server
3. Click **Next >**
4. Complete the installation process
5. Perform all remaining installation qualification tasks

Configuration Tasks

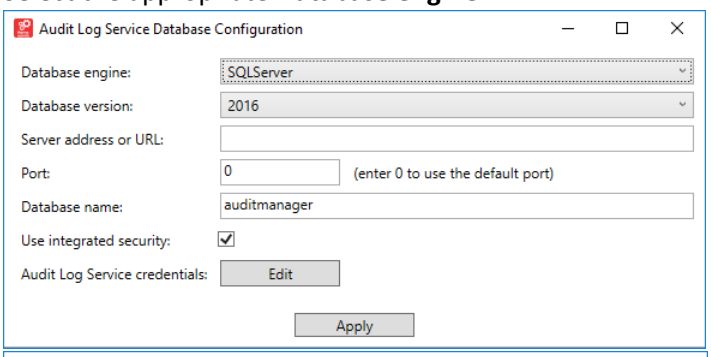
The following sections are used by all the installation scenarios and are consolidated here for simplicity.

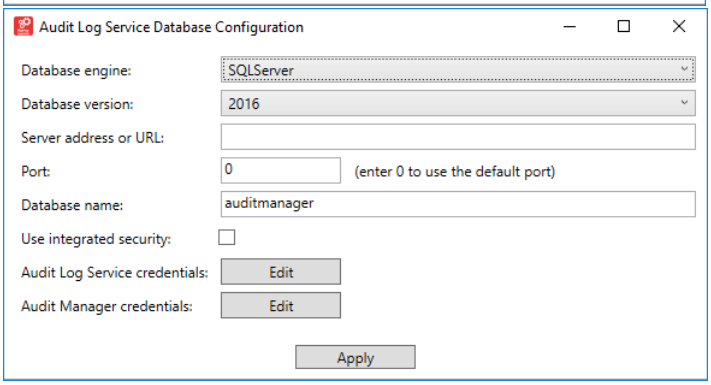
(Re)configure the Audit Log Service

1. If you are reconfiguring the Audit Log Service:
    a. Launch %ProgramFiles(x86)%\Thermo Scientific\Audit Log Service\Configuration Utility.exe
    b. Log in to the utility using the current username and password



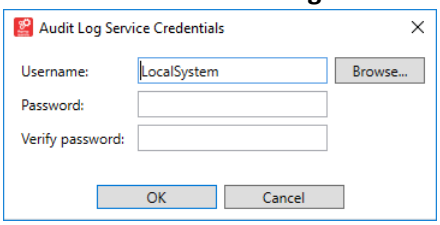
2. Select the appropriate **Database engine**





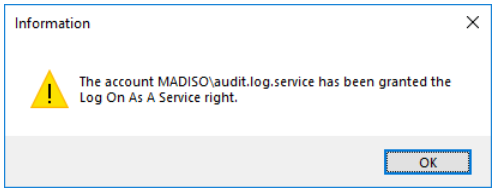
3. If an engine other than *SQLite* is chosen, do the following: (the customer's IT organization will provide this information):
    a. Select the appropriate **Database version**
    b. Enter the **Server address or URL**. This could be a machine name (e.g. USMAD-SQL02) or a full URL (e.g. mydatabase.myserver.com)
    c. If the database engine was configured to use a custom **Port**, enter it
    d. Enter the **Database name**
    e. Check or uncheck **Use integrated security** as appropriate

4. Click **Edit** for the **Audit Log Service credentials**

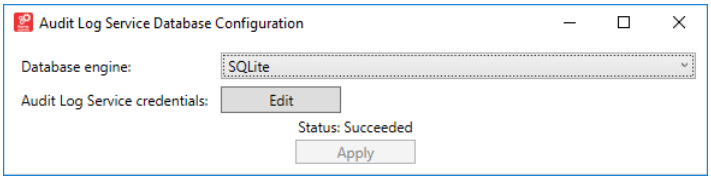


5. If using SQLite or integrated security, enter the Audit Log service account name and password; otherwise, enter the username and password created for the writing to the database
6. If <u>not</u> using integrated security, click **Edit** for the **Audit Manager credentials** and enter the username and password created for reading the database
7. Click **Apply**

   NOTE: You may see a dialog informing you that the Audit Log service account has been granted the Log On as a Service right.

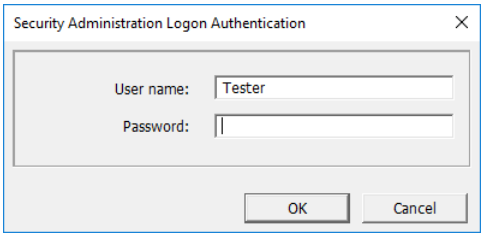


8. When the *Status: Succeeded* message appears, close the window

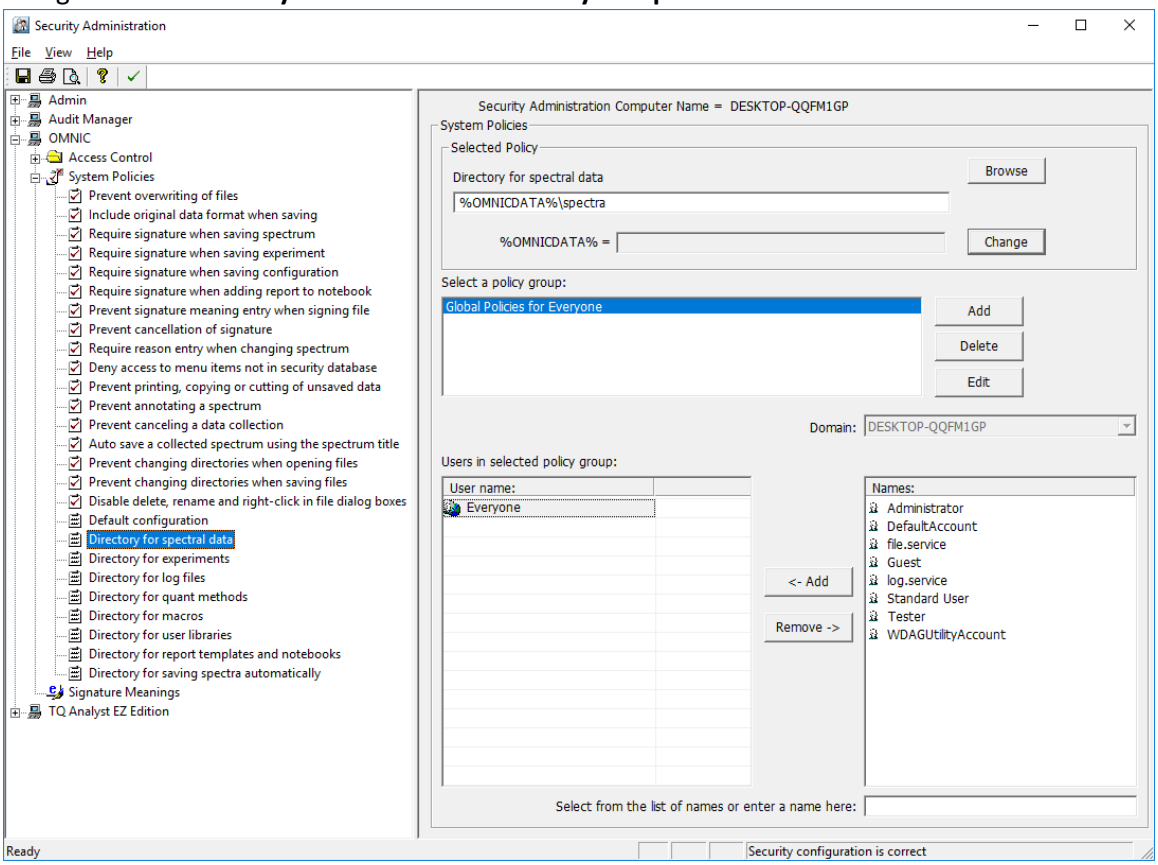


(Re)configure the Data Storage Folder

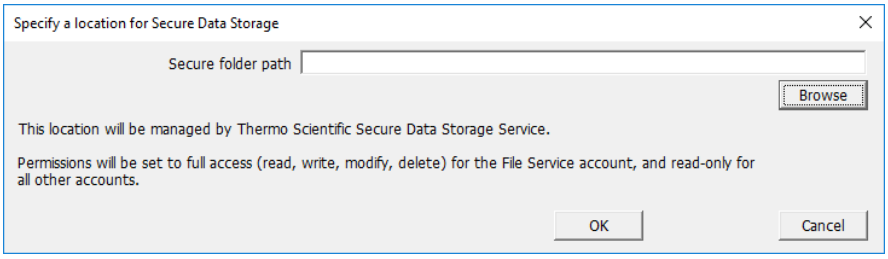
1. If you are reconfiguring the data storage folder, launch Security Administration
2. Log in to Security Administration



3. Navigate to **OMNIC→System Policies→Directory for spectral data**



4. Click **Change** for **%OMNICDATA%**



5. Enter the path to the Secure Data Folder
6. Click **OK**
7. Configure any other access controls and policies as required
8. Save the configuration
9. Close Security Administrator