Security Suite with OMNIC Paradigm Software - System Owner Form

This document facilitates communication between the Thermo Scientific™ System Owner and the on-site IT Administrator to select a Security Suite configuration and complete any supporting Microsoft® Windows® administrative tasks before the Thermo Scientific software installation.

This form should be used when installing Security Suite software with OMNIC Paradigm software. If you are installing Security Suite with other instrument applications, see Getting Started with Security Suite.

Complete this form and have it available for our service representative to perform the installation. For detailed information about the software installation, see *Security Suite Installation Guide* in the Security Suite documentation set.

Note

You must have an IT Administrator present during the Thermo Scientific software installation!

Be prepared to provide an **administrative loginand password** for each instrument computer.

Installation Configurations

You can use the Security Suite to set and enforce security policies in two types of configurations:

- **Single Computer Installation**. Recommended for one or more Thermo Scientific instruments that will be controlled individually. Provides a secure environment with data integrity.
- **Distributed Installation**. Recommended for Thermo Scientific instruments that will be controlled as a group. All controlled instruments must be connected to the same (or a trusted) network domain. Provides the highest level of security and data integrity.

269-344200 Revision A
July 2020 Thermo Fisher Scientific

thermo scientific

Single Computer Installation

With a single computer installation, each Thermo Scientific instrument will have all of the Security Suite components installed. The instruments can be connected to a network domain but this is not a requirement for successful software installation.

Note Single computer configurations require an administrative login and password for each instrument computer. With this configuration,

Security settings must be applied individually for each Thermo Scientific instrument.

Each instrument will have a separate audit log.

Distributed Installation

With a distributed installation, networked computers or servers on the same domain are used to run the instrument and for Security Administration. Data from OMNIC Paradigm software is stored in a secure database. Files from other instrument applications, such as OMNICxi or OMNIC, can be stored in a secure data folder.

Note Thermo Scientific instruments intended for central Security Suite control should be connected to the same (or a trusted) network domain and the Security Administration software should be installed on that domain. With these configurations, security settings are applied globally for all connected instruments and all instruments send events to the same Thermo Scientific audit log.

All distributed installations require an administrative login and password for the network domain. A network server running the Windows Server operating system is preferred over one running the Professional version of Windows operating system software.

In the following options, instrument computers can include a Nicolet Summit spectrometer directly or can be a separate device running the Workstation version of OMNIC Paradigm software.

If you are also using other instrument applications alongside OMNIC Paradigm software, such as OMNICxi software or OMNIC software, you must also specify a location for secure data storage.

With a distributed installation, Security Server software is installed on the computer used to run Security Administration software and to manage the audit log. Security Client software is installed on any instrument computers, including the Nicolet Summit spectrometer directly or a workstation computer running OMNIC Paradigm software.

Domain account name: _____

Security Administration computer name (Security Server):_____

Data Storage computer name: _____

(required if using other instrument applications with OMNIC Paradigm software)

Windows Administrative Tasks

For all Security Suite installation configurations (Single Computer and Distributed), complete the following Windows administrative tasks **before** the Thermo Scientific service representative arrives to install the Security Suite software.

1. **(Optional) Create a database** for storing spectral and instrument data collected with OMNIC Paradigm software.

   If you plan to use the default Thermo Scientific Built-in database with a single installation configuration, OMNIC Paradigm software configures the database automatically. No other database information is required.

   If you are not using the default database option and are using a custom database, ensure that your database is configured to use the Unicode character set. Select UTF-8, UTF-16, or UTF-32 (not recommended) encoding, depending on the requirements of your organization.

   The database can be shared in a network location or on only the single instrument computer.

   Database name: _____

   (for example, ParadigmData)

Database engine: Maria DB SQL Server Oracle Amazon Aurora

(Select one)

The following table lists supported database engines:

Database Engine	Supported Versions
Maria DB	10.3

Database Engine	Supported Versions
	10.2 10.1 10.0
SQL Server	2017 2016 2014 2012
Oracle	18c 12c Release 2 12c Release 1 11g Release 2
Amazon Aurora	MySQL 5.7 compatible MySQL 5.6 compatible

Database version: _____

Database server name or URL: _____

Database port: _____

Use default port

2. If you are also using instrument applications other than OMNIC Paradigm software, such as OMNICxi or previous versions of OMNIC software, create a folder for storing acquired instrument data and associated files.

   For single computer configurations, create this folder on each Thermo Scientific instrument computer. This folder will be used for secure data storage for all Security Suite applications.

For distributed configurations, the folder location depends on the selected configuration (see the previous section for details). This folder may be used for secure data storage for all Thermo Scientific instruments and Security Suite applications on the selected network domain.

Data Storage Folder location: _____

(must be a UNC path, for example, \\servername\foldername)

3. If you created a secure storage folder, create a service account that has Full Control access to the Data Storage Folder specified in step 2 above (a managed service account is preferred for networked installations).

Note For single computer installations where the instrument computer is not connected to a network domain, the service account can be a dedicated local user account. For all other installations, the service account must be a domain account.

Data Storage Service account name: _____

(for example, domainname.accounttype.service name)

4. **Create a database** for the Thermo Scientific audit log.

   If you are using a single computer installation and using the default SQLite database for the audit log, the audit log database is configured automatically. No other database information is required.

   If you are using a distributed installation or a custom database, enter the database information here.

   If you are not using the default database option and are using a custom database, ensure that your database is configured to use the Unicode character set. Select UTF-8, UTF-16, or UTF-32 (not recommended) encoding, depending on the requirements of your organization.

   Database name: _____

   (for example, Audit Log Database)

   Database engine: SQLServer Oracle MariaDB SQLite

   (Select one) (SQLite is appropriate for single computer installations only)

Note If using the SQLite database engine (appropriate for Single Computer configurations only), the Security Suite creates the Audit Log database automatically and sets appropriate access rights for the Audit Log Service account you specify. No other database information is required.

The following table lists database engines that are supported by the Thermo Scientific Audit Log Service.

Database Engine	Supported Versions
Maria DB	10.2 10.1 10.0
SQL Server	2016 2014 2012
Oracle	12c Release 2 12c Release 1 11g Release 2

Database server name or URL: _____

(not required for SQLite)

Database port: _____

(not required for SQLite)

Use default port

Create a service account for the Audit Log database.

- If you are using the default SQLite database, Read/Write access is configured automatically.
- If you are using a custom database, configure the service account to have full Read/Write access.

Database service account name: _____

(for example, domainname.accounttype.service name)

Additional Tasks

Create network authorization groups, if desired, that will be used for security administration and secure instrument operation and then add user accounts to those groups. (If using the default Windows user groups (not recommended), then just add user accounts to those groups.)

Note For all distributed installation configurations, both authorization groups must be on the network domain. For single computer configurations, the authorization groups can be on the local computer. The default authorization groups (Administrators and Users) are on the local computer.

Each group must include at least one user.

Security Administrators group name: _____

(will have Full Control access to Security Administration software)

Instrument Operators group name: _____

(will have limited access to Thermo Scientific instrument applications)