iTEVA *Security* Software

Installation Manual

Version 5.8

Part number 8499 400 20021

Contents

Introduction

This manual explains how to install and configure the Thermo Scientific iTEVA *Security* software.

The iTEVA *Security* software can be thought of as a client-server application which consists of three separately installable components. These components are:

1. The Thermo Security Server and Security Administration Software

The Thermo Security Server software provides security information to client applications, such as iTEVA. It runs in the background as a Windows® service.

The Thermo Security Administration Software allows an administrator to define and manage the security policies for Thermo client applications.

Together, these two components provide the 'server' side of the client-server relationship with the iTEVA *Security* client software providing the client side.

2. The iTEVA *Security* Client Software

The iTEVA *Security* client software provides the functionality to control an iCAP 6000 series spectrometer and to collect and process its data. By communicating with the Thermo Security Server, it enforces the access control, system policy and electronic signature behaviour as defined by an administrator.

3. SQL Server Express

SQL Server Express is a database server that provides secure storage for the electronic records produced by the iTEVA client software.

Together, these components integrate with the security and auditing features of the Windows operating system to provide:

- Traceability of user operations through audit trails and event logs
- Access control via a secure user authentication process
- Prevention and detection of uncontrolled changes to electronic records
- Electronic signatures based on the user's Windows log-on credentials

When correctly installed and configured, these features help your laboratory meet regulatory requirements, such as FDA 21 CFR Part 11.

Installation Steps

Installation of the iTEVA *Security* software consists of the following steps:

1. Configure Windows Administration

The iTEVA *Security* software integrates with various security and auditing features provided by the Windows operating system, therefore it is essential that before installation begins, these features be reviewed and configured appropriately.

2. Install the Thermo Security Server and Administration Software

An administrator must install the Security Server and Administration software onto a designated server computer. Once installed the administrator can transfer the ability to run the administration software to any users or user groups as required.

3. Configure the Security settings for the iTEVA *Security* Client application

Once the Thermo Security Server and Administration Software has been installed, the client application's security settings must be configured to provide the access control, system policy and electronic signature behaviour required by your laboratory or regulatory body.

4. Install and configure SQL Server Express

SQL Server Express must be installed and configured appropriately in order to protect the integrity of your analytical data by preventing it from being modified by unauthorised individuals or in an uncontrolled manner.

Note If required, iTEVA *Security* can connect to an existing instance of SQL Server, in which case installation of SQL Server Express is not required. Any existing instance of SQL Server must however be configured as described in this manual.

5. Install and configure the iTEVA *Security* Client application

Instances of the iTEVA *Security* Client software are installed and configured to communicate with the Security Server and to access secure analytical databases hosted by SQL Server Express. Analysts may then use the software to collect, process store and review analytical data.

Note Failure to perform all of these steps correctly may compromise the security of the installation and the integrity of your analytical data, and may result in an inability to comply with regulatory requirements, such as FDA 21 CFR Part 11.0

The Installation Process

Configuring Windows Administration

iTEVA *Security* can be installed to operate in a number of different networked or stand-alone configurations.

The steps required to make Windows ready for installation of iTEVA *Security* should have already been taken as part of the customer pre-installation process. If for any reason they have not, then these are outlined below.

The configurations and the process of setting up Windows for each configuration are described in the following document which is supplied on the iTEVA *Security* installation CD:

```
Program Files>ThermoAdmin>SecAdminUserGuide.pdf
```

If you are unfamiliar with the concepts of Windows administration, please read the chapter *Overview of Windows Administration* first. This will explain the concepts behind the processes described later.

Follow the detailed instructions in the chapter *Setting up Windows Administration* for the configuration that matches your own environment.

Note

Be sure to follow the relevant instructions depending on whether your system is Windows XP or Windows Vista/Windows 7, networked, or stand-alone.

Disregard the chapter ‘Setting Service Accounts’ as this describes features of the Thermo Security and Administration software that are not used by iTEVA *Security*.

Power Users

iTEVA users must have membership of the ‘Power Users’ group. This is because Windows will only allow ‘users’ to run ‘certificated’ applications and iTEVA is not a ‘certificated’ application.

1. To grant iTEVA users membership of the Power Users group, through the **control panel** select **Administrative Tools**
2. Select **Computer Management** then **Local Users and Groups**.
3. In the list of Groups double-click on **Power Users** to open the **Power Users Properties Window**.

Add all the required users.

Disable Time and Date Changes

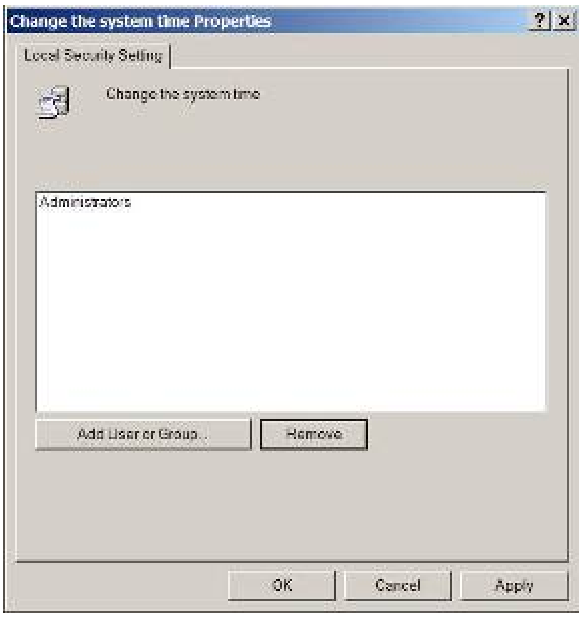
By default, 'Power Users' are able to change the system time and date settings. It is crucial for the integrity of iTEVA *Security* that only 'administrators' can do this.

Note In networked environments this functionality will be administered by the network administrators, and the following steps should only be necessary for stand-alone configurations.

1 To restrict this control to 'administrators' only, through the **control panel** select **Administrative Tools**

2 Select **Local Security Policy** > **Local Policies** > **User Rights Assignment**

3 Double-click on the policy, **Change the system time**



4 If the group 'Power Users' is there remove it from the list so that only 'Administrators' have permission to change the system time.

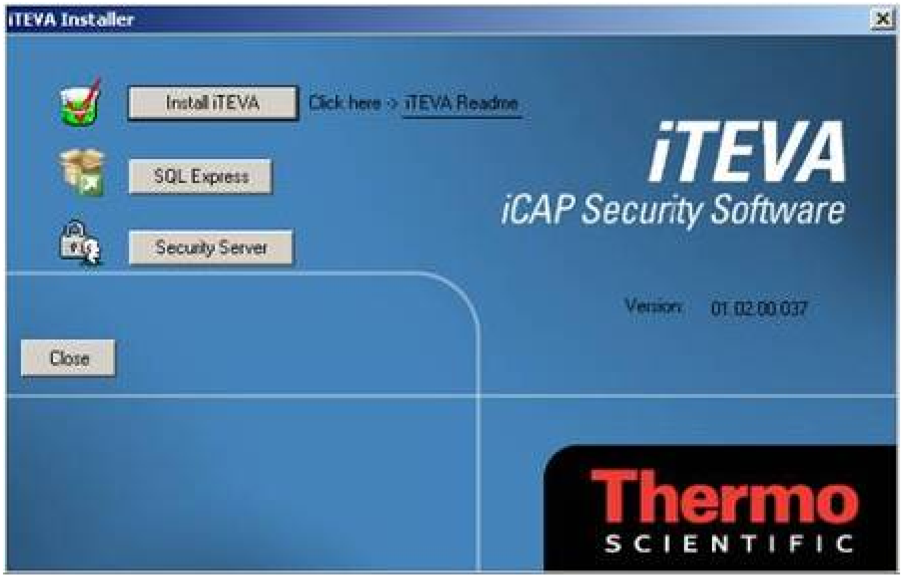
1 of 9 Complete

□

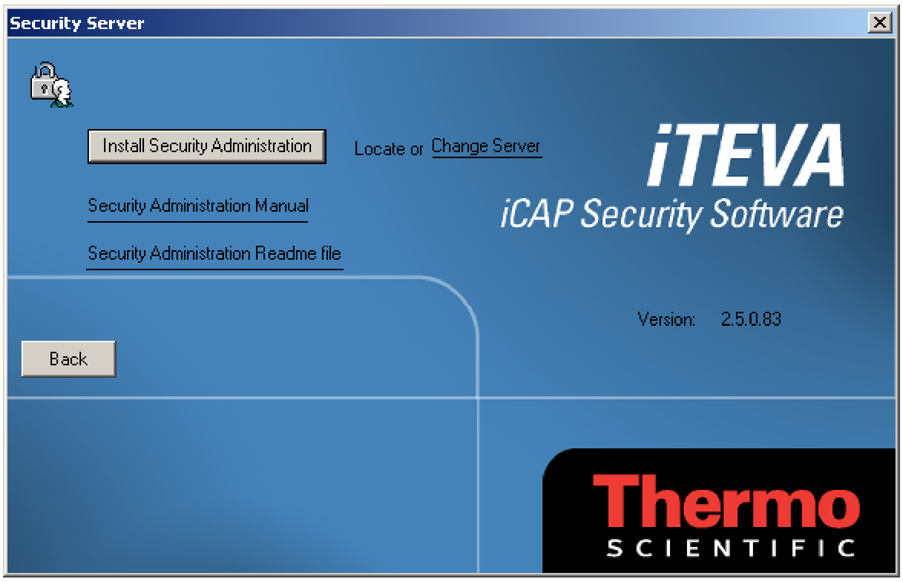
Installing the iTEVA *Security* Server and Administration Software

The Thermo Security Server and Administration software is installed from the iTEVA *Security* installation CD. It must be installed by someone who is a member of the *Administrators* group on the computer that it is being installed to and it must be installed on a disk or partition that is formatted with the NTFS file system as only this file system is capable of using security attributes on files, an essential capability for protecting the security administration database from unauthorised access.

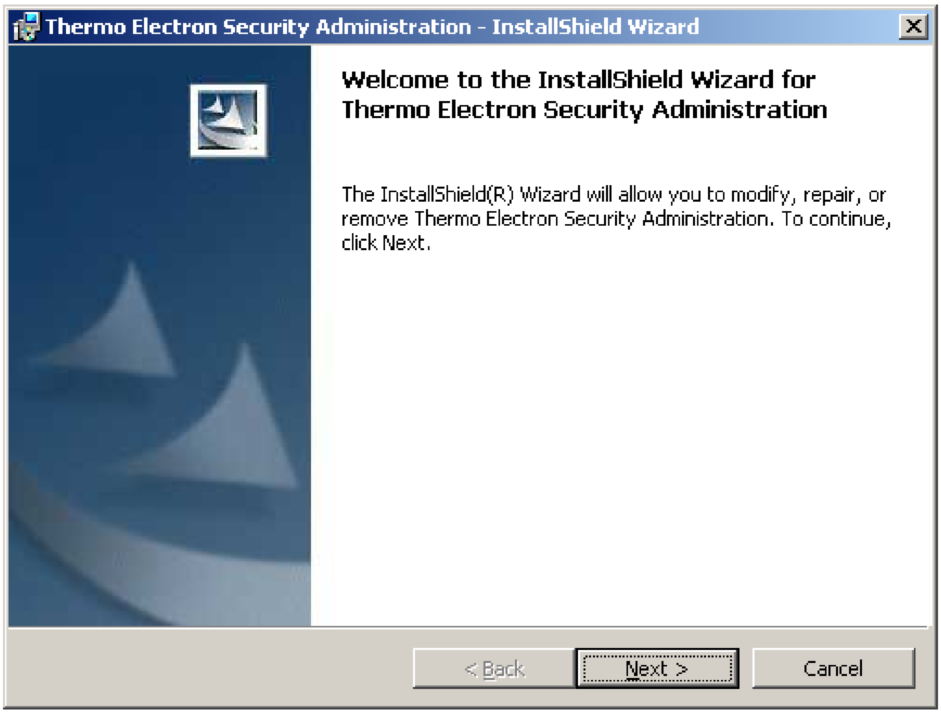
1 Insert the installation CD into the CD drive of the computer that will be used as the server. The installation program should start running automatically. If it does not, using windows explorer, navigate to the contents of the CD drive and double-click on the file: `setup.exe`.



2 Click **Security Server**.



3 Click **Install Security Administration**. The installation wizard should start.

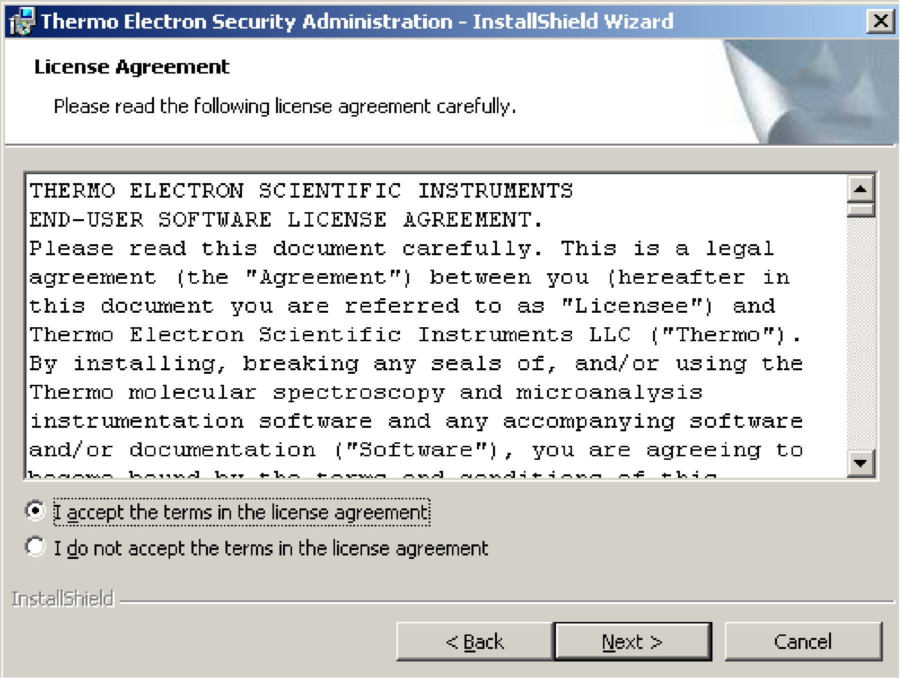


Thermo Electron Security Administration - InstallShield Wizard

Welcome to the InstallShield Wizard for Thermo Electron Security Administration

The InstallShield(R) Wizard will allow you to modify, repair, or remove Thermo Electron Security Administration. To continue, click Next.

4 Click **Next** and accept the license Agreement.



Thermo Electron Security Administration - InstallShield Wizard

License Agreement

Please read the following license agreement carefully.

```
THERMO ELECTRON SCIENTIFIC INSTRUMENTS
END-USER SOFTWARE LICENSE AGREEMENT.
Please read this document carefully. This is a legal
agreement (the "Agreement") between you (hereafter in
this document you are referred to as "Licensee") and
Thermo Electron Scientific Instruments LLC ("Thermo").
By installing, breaking any seals of, and/or using the
Thermo molecular spectroscopy and microanalysis
instrumentation software and any accompanying software
and/or documentation ("Software"), you are agreeing to
become bound by the terms and conditions of this
```

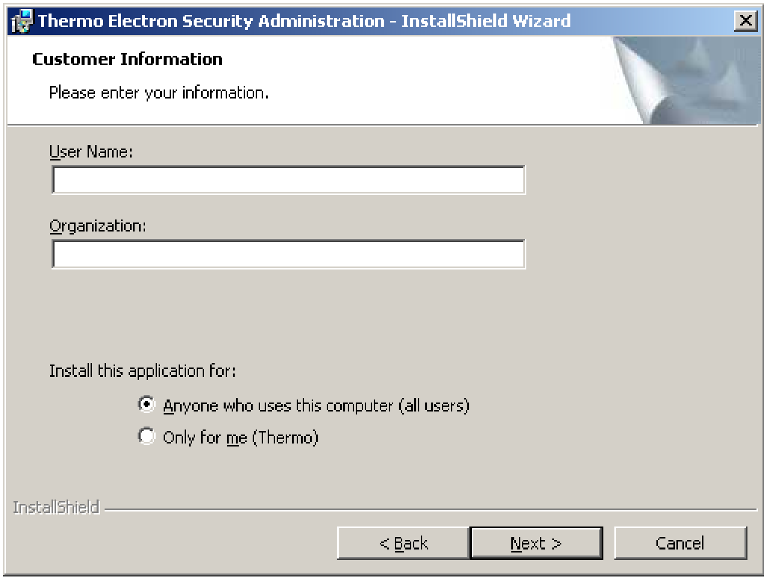
● I accept the terms in the license agreement

○ I do not accept the terms in the license agreement

5 Click **Next**. On the customer information page, enter your username and organisation name.

If the administration software is only ever to be accessible by the user performing the installation, select the **Only for me** button. If, on the other hand you envisage that other users will be performing administrative tasks, select **Anyone who uses this computer**.

Note This only controls whether or not a shortcut to the Administration software appears on the desktop and on the Windows start menu for the selected user(s). You will later be able to define exactly who can and cannot perform administrative tasks.



Thermo Electron Security Administration - InstallShield Wizard

Customer Information

Please enter your information.

User Name:

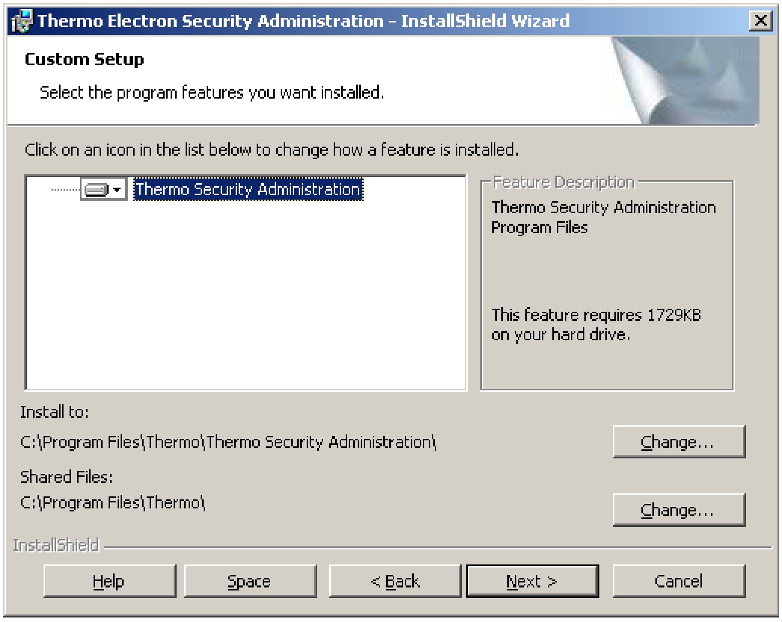
Organization:

Install this application for:

● Anyone who uses this computer (all users)

○ Only for me (Thermo)

6 Click **Next**. The custom setup dialogue allows you to change the location where files are installed. If you do this, always use the same location each time you install the software so that files are upgraded correctly when subsequent versions are installed. Typically, default locations are used for installation.



Thermo Electron Security Administration - InstallShield Wizard

Custom Setup

Select the program features you want installed.

Click on an icon in the list below to change how a feature is installed.

Thermo Security Administration

Feature Description

Thermo Security Administration Program Files

This feature requires 1729KB on your hard drive.

Install to:

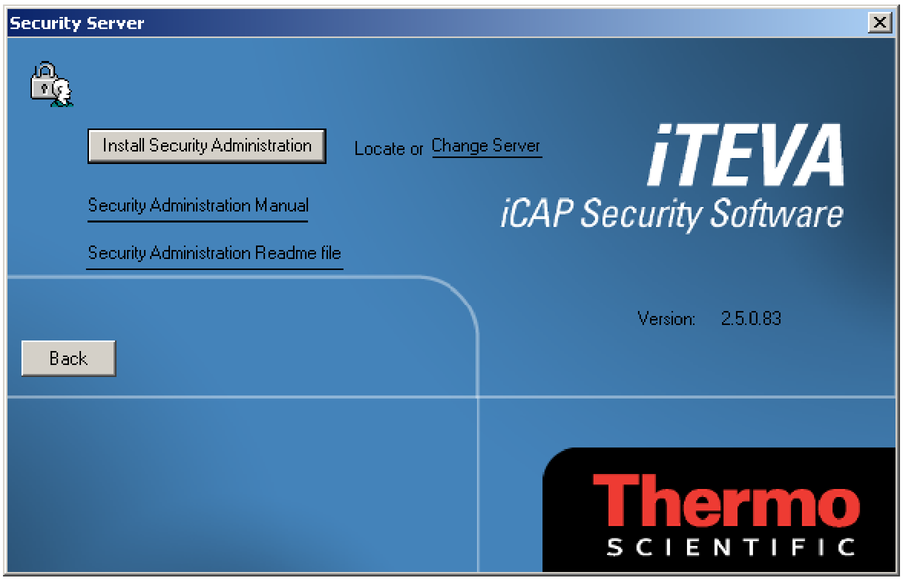
C:\Program Files\Thermo\Thermo Security Administration\

Shared Files:

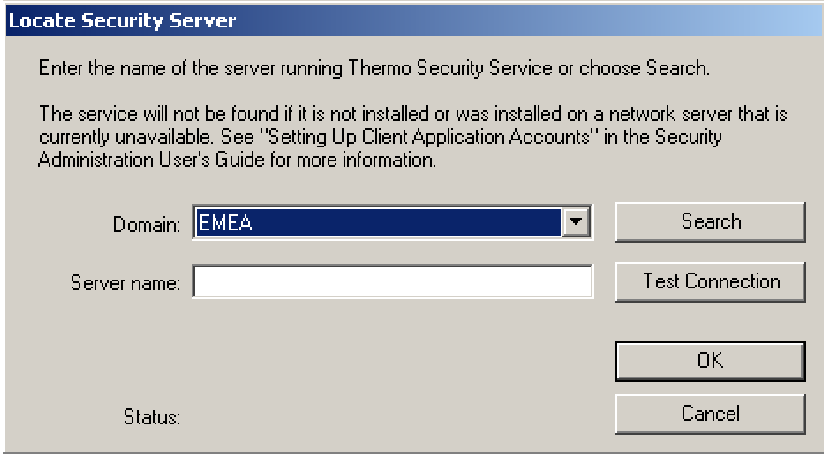
C:\Program Files\Thermo\

7 Click **Next** and then on the final install dialogue, click **Install**. The installation will now proceed. Click **Finish** to end the installation wizard when installation has run to completion.

8 From the installation window for the Security Server, click on **Locate or <u>Change Server</u>**, as in the screen shot below.



9 The Locate Security Server dialogue is displayed. Click **search** to find the local PC.


Locate Security Server

Enter the name of the server running Thermo Security Service or choose Search.

The service will not be found if it is not installed or was installed on a network server that is currently unavailable. See "Setting Up Client Application Accounts" in the Security Administration User's Guide for more information.

Domain: EMEA

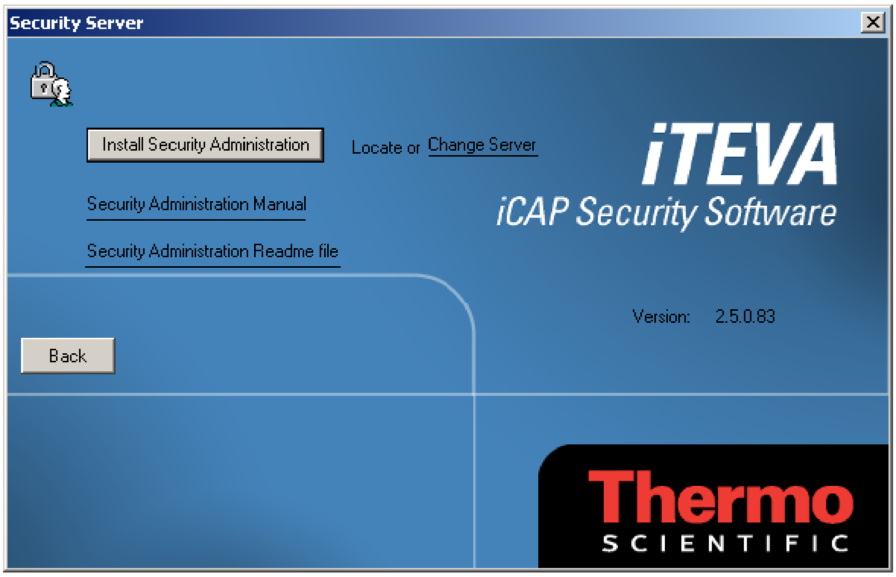
Server name:

Status:

In a networked configuration the *Domain* field will automatically default to the name of the domain that the computer belongs to. Accept the default and enter a dot '.' in the Server Name field and click **OK**.

In a stand-alone configuration both the Domain field and the Server Name field will default to the name of the stand alone computer. Accept the defaults and click **OK**. It may be necessary to click **Search** to fill the fields.

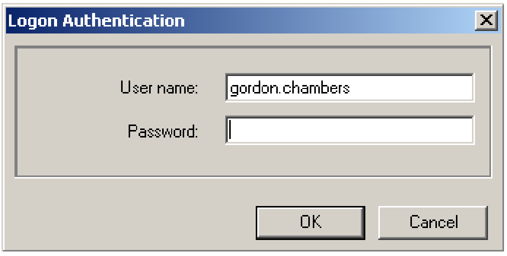
10 Click **Back** on the iTEVA *Security* installer.



11 Click **Close** on the iTEVA *Security* installer.

There should now be a shortcut on your desktop for the Thermo Security administration application. Double click this icon to start the application.

A Logon Authentication dialogue will be displayed.

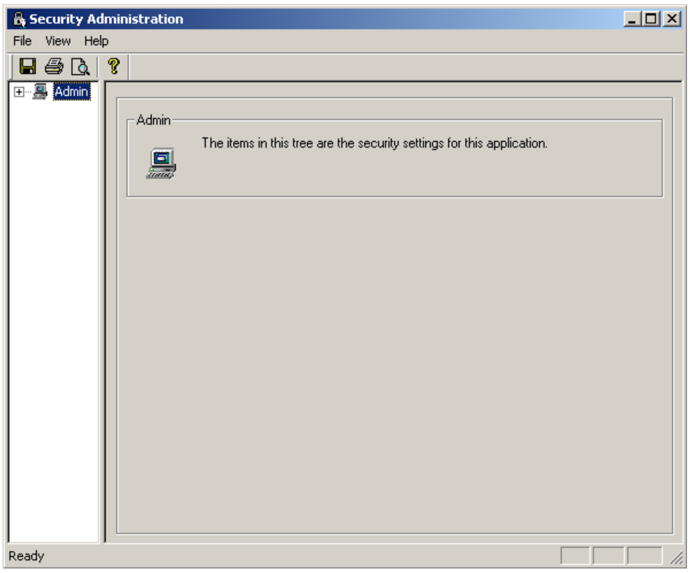


User name: gordon.chambers

Password:

Note: if the password has been created as blank, then this logon may fail.

12 Enter your Windows user name and password and click **OK**. The Security Administration software will now start.

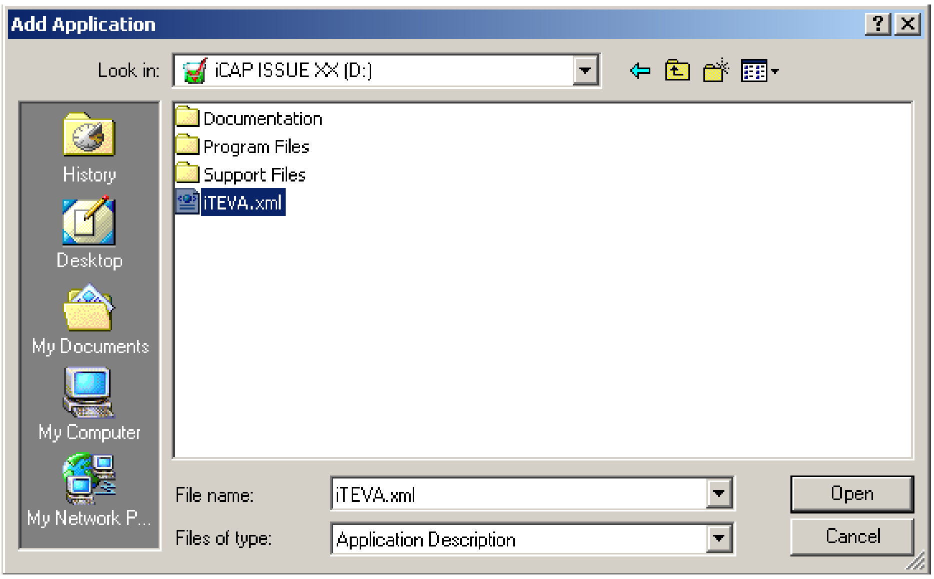


Admin

The items in this tree are the security settings for this application.

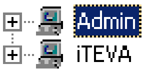
13 Select **Add Application** from the **file** menu and in the browser dialogue that is displayed, navigate to the CD drive containing the installation CD. Select the file `iTEVA.xml` and click **Open**.

The Navigation pane of the Security Administration software should now display an icon representing the iTEVA client application, in addition to the existing icon representing the Security Administration application itself:

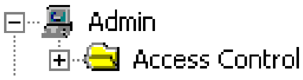


File name: iTEVA.xml

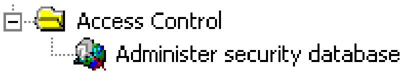
Files of type: Application Description



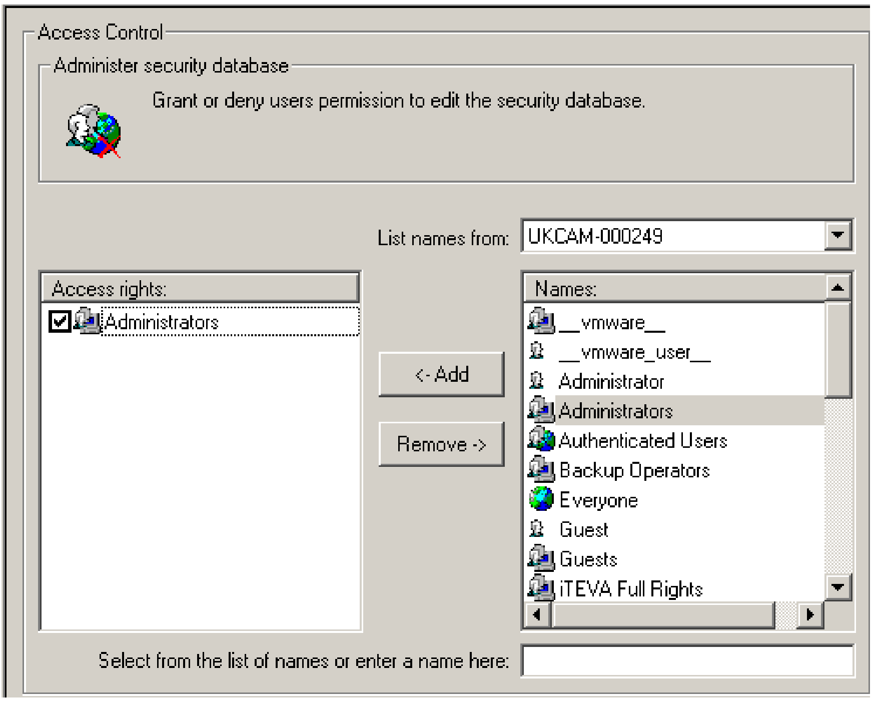
14 Click on the plus sign '+' next to the Admin icon. The access Control Folder appears:



15 Click on the plus sign '+' next to the Access Control folder. The Administer Security Database icon appears:



16 Click on the Administer Security Database icon. A list of access rights appears in the right hand pane. The built-in Windows group 'Administrators' should already be granted the right to administer the security database.



Access Control

Administer security database

Grant or deny users permission to edit the security database.

List names from: UKCAM-000249

Access rights:

☑ Administrators

<- Add

Remove ->

Names:

- __vmware__
- __vmware_user__
- Administrator
- Administrators
- Authenticated Users
- Backup Operators
- Everyone
- Guest
- Guests
- iTEVA Full Rights

Select from the list of names or enter a name here:

17 You may now specify the users and/or groups of users who will have the right to run the Security Administration software. To add a user or group, select the name of the user or group from the **Names** list and click the **Add** button. The check mark next to the name indicates that the user or group has been granted the right to run the Security Administration software.

To remove a user or group from the list, select the user or group from the Access Rights list and click the Remove button.

18 Select ‘Save Settings’ from the File menu. This will write the changes you have made into the security database. The Security Administration software can now be shut down by selecting ‘Exit’ from the file menu.

2 of 9 Complete

□

Configuring Security settings for the iTEVA *Security* client application

This process consists of:

- Granting the desired access rights to users or groups of users
- Setting the required system policies
- Configuring the use of electronic signatures

This process must be performed by someone who has been granted the right to run the Security Administration software.

Listed below is a description of the security settings that are specific to the iTEVA client application. For a general description of how to use the Security administration software, please refer to the chapter *Using Security Administration* in the document *SecAdminUserGuide.pdf.*

Configuring Access Control Settings

The following access control settings are available for the iTEVA client software.

- Run iTEVA *Security*

Users with this right are able to log in to the iTEVA client software.

- Edit System Settings

Users with this right are able to make changes to any of the parameters that appear on the **options** and **instrument options** pages in the iTEVA client software, **including the right to run the Database Wizard.** In a stand-alone configuration (client and server installed on the same computer), this allows the user to create analytical databases and to attach and detach them on SQL Server Express.

Note It is strongly recommended, that in a regulated environment, for example where compliance with 21 CFR Part 11 is required, this access right is only granted to those users who also have the right to administer security settings i.e. users who can run the Security administration software. This is because a user who creates an analytical database is, by default, the ‘owner’ of that database, and this confers certain privileges such as the ability to make uncontrolled edits to the contents of the database, from outside the controlled environment of the iTEVA *Security* software.

Users must have this right to be able to perform a firmware upgrade to the iCAP instrument.

Users with this right are able to change the default plasma conditions that are set following plasma ignition (post ignition conditions).

Users with this right are able to archive Full Frame sample data to a file that is separate from the analytical database, thereby removing it from the analytical database.

Users with this right are able to copy analytical methods and results between databases and to delete methods and samples from analytical databases. The ability to copy and delete samples, also requires the 'Edit Samples' access right to be granted.

- Edit Map Database

Users with this right are able to make changes to the **Map Database**. This allows a user to mark which emission lines are available for analysis, which lines are selected by default when the element is added to a method and to define the default width and height of the examination region for each emission line.

- Edit Methods

Users with this right are able to create and edit analytical methods.

- Edit Samples

Users with this right are able to make changes to sample data after the sample has been collected, such as deleting repeats, changing the regions of interest (central and background points), recalculating the sample with a different concentration factor or changing the sample identification.

- Edit Sequences

Users with this right are able to create and edit sequence automation sessions (auto-sessions). This includes the ability to add or delete samples from the auto-session.

- Create Reports

Users with this right are able to create analytical reports using the Publisher application.

- **Override method parameters on 'run sample' dialogues**

Users with this right are able to override some of the method parameters, such as the number of repeats and sample flush time when running samples. In a regulated environment, routine users would not ordinarily have this right granted as it allows samples to be collected under conditions that are not reflected in the method, thus removing traceability between the sample and the method. However, for those users involved in method development, it is often useful to be able to quickly override these parameters between samples at run time, without having to perform the normal method edit/save process.

Configuring System Policies

The following system policies are available for the iTEVA client software.

- **Audit Information Events**

By default, the iTEVA client application logs all significant system events in the Windows event log of the server computer (the one running the Thermo Security Server service.) Such events include all instrument errors (e.g. plasma went out during analysis, failed to connect to an analytical database etc.) and all successful and failed user authentications (i.e. entry of username and password for a given user account). By opting to audit information events, this information is supplemented by more detailed information about less critical events. This includes events such as plasma ignition, auto-sampler run started/completed, running sample x etc. Whilst this provides a more detailed account of all the activity associated with each instrument, it can result in very large amounts of data being stored in the event log.

As this information is already stored locally in the iTEVA journal on each client computer, it is recommended that most labs do not routinely audit information events.

- **Database Application Role Password**

When iTEVA writes data (methods, samples etc.) to an analytical database it provides a special password to the SQL Server that identifies the application as being the iTEVA application. SQL Server compares this password with one stored in the database and only grants access to write to the database if they match. If any other application attempts to write to the database, it will fail to do so as it cannot provide the correct password. This prevents analytical data from being modified in an uncontrolled manner, even by users who have been granted the right to access the database using the iTEVA application.

The default password, known as an *application role* password is complex, consisting of a random string of characters and. **Under normal circumstances this password need never be changed.**

However, if your regulated environment requires that all passwords related to data security be changed on a frequent basis, this can be achieved via this system policy.

If you specify a database application role password in the Security Administration software, the iTEVA client application will use this password instead of the original one. Any password you specify must adhere to certain rules regarding complexity.

- The password must be at least six characters long.
- The passwords must contain elements from three of the four following types of characters.

Character types	Examples
English uppercase letters	A, B, C, ... Z
English lowercase letters	a, b, c, ... z
Westernized Arabic numerals	0, 1, 2, ... 9
Non-alphanumeric characters (special characters)	$, ! , % ,^

After setting a new application role password, the iTEVA client application will automatically store this password in any new database that is created and attached to SQL Server using the database wizard. To change the password that is stored in existing analytical databases, you must use the database wizard to first detach, then re-attach the database.

Configuring Signature Meanings

Four example signature meanings are provided by default. If you wish to use electronic signatures, these should be reviewed and edited to suit the roles and responsibilities within you organisation. Signature meanings behave like access rights in that each signature meaning can be used only by those individuals who have been granted the right to do so.

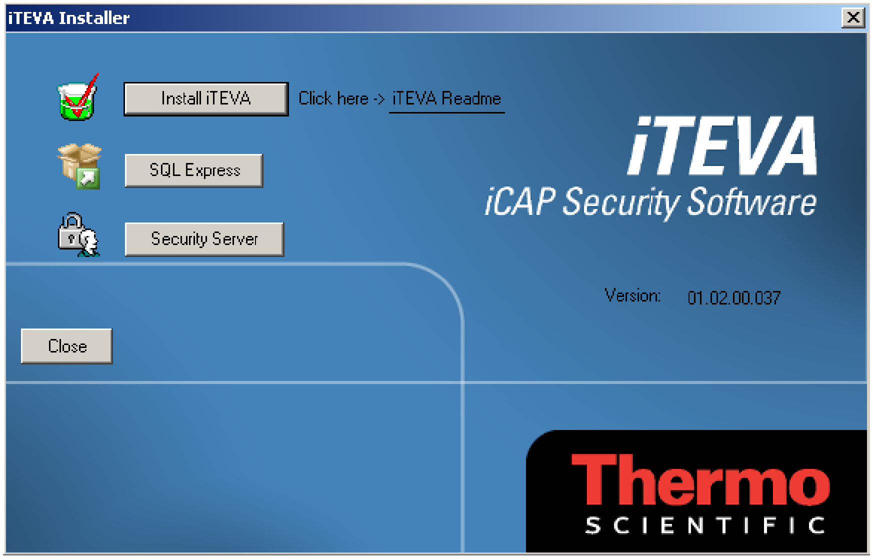
Installing and configuring SQL Server Express

SQL Server Express is installed from the iTEVA *Security* installation CD. It must be installed by someone who is a member of the **Administrators** group on the computer that it is being installed to.

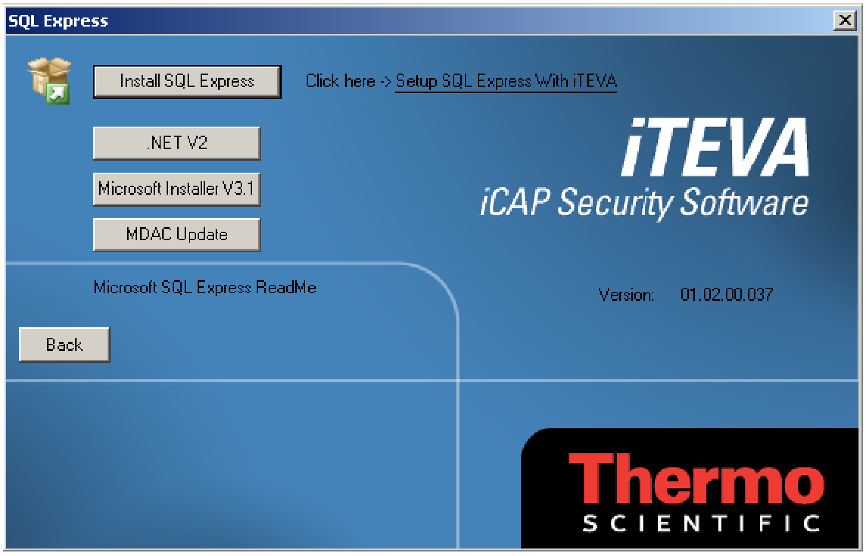
In a networked environment it is commonly installed on the same computer as the Thermo Security Server and Administration software as it is commonly administered by the same person(s).

In a stand-alone environment it is installed on the single computer that is acting as both client and server.

1 Insert the installation CD into the CD drive of the computer that will be used as the server. The installation program should start running automatically. If it does not, using windows explorer, navigate to the contents of the CD drive and double-click on the file: `setup.exe`.



2 Click **SQL Express**.



3 Install Pre-Requisite Components.

SQL Server express requires the following components to be installed. If you are unsure whether these components have already been installed on your system run the installation process for each anyway and they will be installed if necessary.

.NET V2 – if this is not installed then an error message will tell you when you try to run SQL Express Setup. In this case run the .NET update (Click .NET V2).

Microsoft Installer V3.1– if this is not installed then an error message will tell you when you try to run SQL Express Setup. In this case run the MSI update (Click Microsoft Installer V3.1).

MDAC Update – if this is not up-to-date then the installation program will signal that in the System Configuration Check stage (See below). In this case, click MDAC Update.

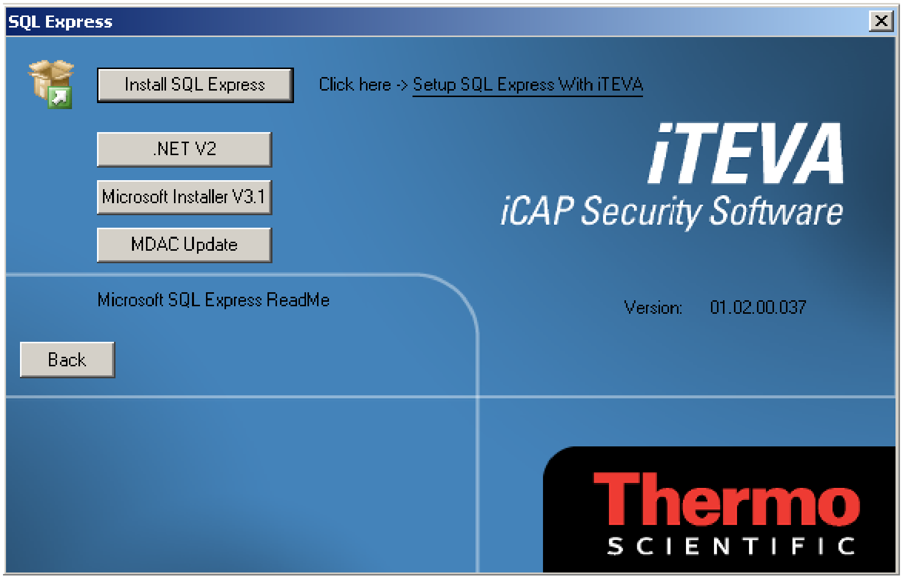
4 Open the instructions for installing SQL Server by clicking on the link Setup SQL Express With iTEVA.

Click **Install SQL Express** to start the installation program.

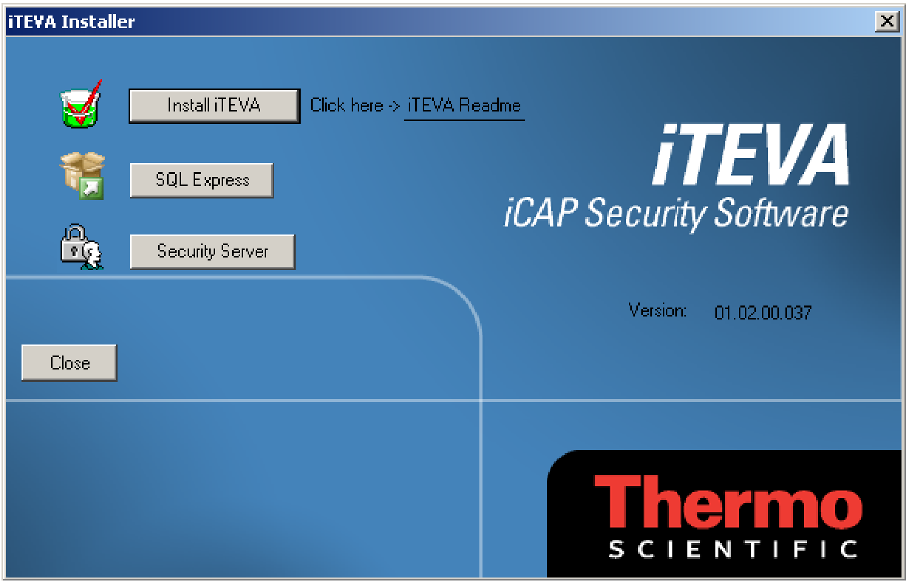
Follow the instructions in the opened document.

At this point if a required component is not installed the installer will indicate to you with an error message - refer to step 3 above and install the required update package by clicking on the respective links and following the installation instructions.

5 Click **Back** on the iTEVA *Security* installer.



6 Click **Close** on the iTEVA *Security* installer.



3 of 9 Complete

□

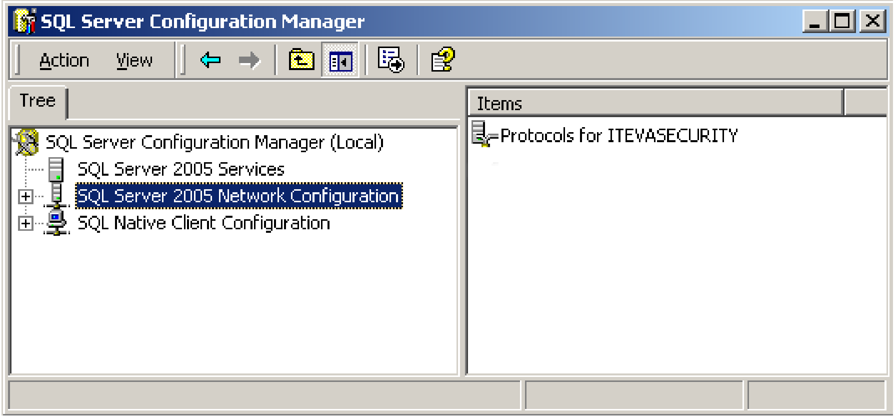
Configuring SQL Server Express for use with remote clients

If you have installed SQL Server express for use in a networked environment, it must be configured to communicate over your network.

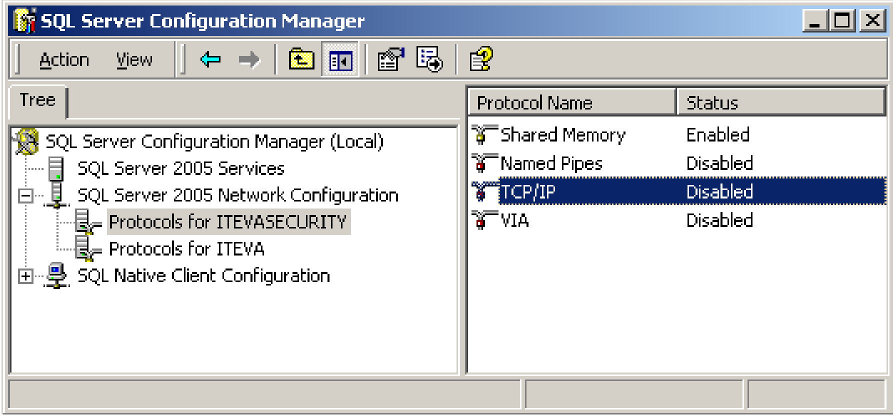
These steps are NOT required if SQL Server Express has been installed to operate in a stand-alone environment. If this is the case, skip steps 1-10 below and go to the section *Creating User Logins for SQL Server Express.*

1 On the computer on which SQL Server Express is installed, run SQL Server configuration manager:

```
Start>Programs>Microsoft SQL Server 2005>Configuration Tools>SQL
Server Configuration Manager
```

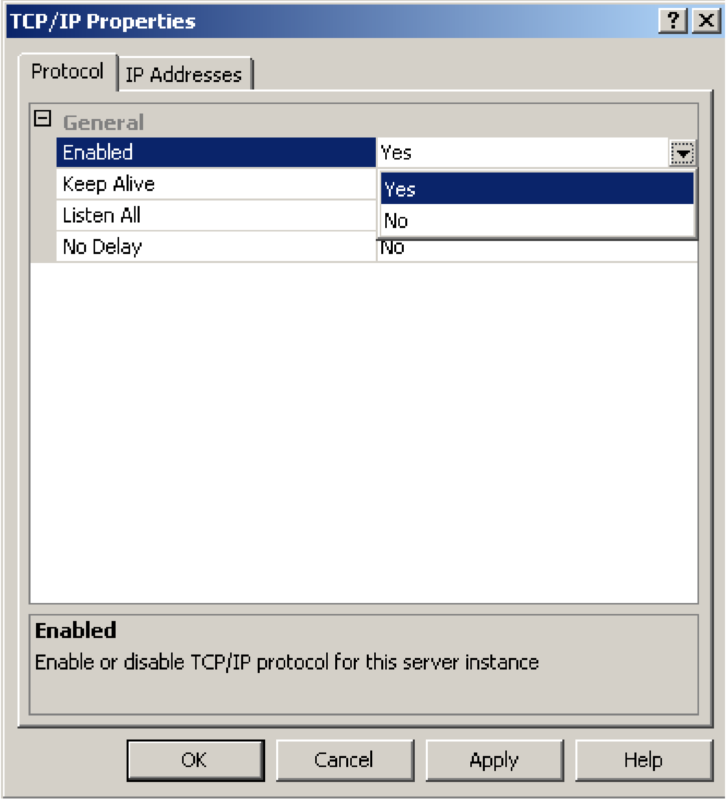

SQL Server Configuration Manager
Action View
Tree
SQL Server Configuration Manager (Local)
SQL Server 2005 Services
SQL Server 2005 Network Configuration
SQL Native Client Configuration
Items
Protocols for ITEVASECURITY

2 Click SQL Server 2005 Network Configuration, and then double-click on Protocols for iTEVASECURITY.


SQL Server Configuration Manager
Action View
Tree
SQL Server Configuration Manager (Local)
SQL Server 2005 Services
SQL Server 2005 Network Configuration
Protocols for ITEVASECURITY
Protocols for ITEVA
SQL Native Client Configuration

Protocol Name	Status
Shared Memory	Enabled
Named Pipes	Disabled
TCP/IP	Disabled
VIA	Disabled

3 Double click on TCP/IP to display the TCP/IP properties page:



TCP/IP Properties

Protocol | IP Addresses

⊟ General

Enabled	Yes
Keep Alive	
Listen All	
No Delay	No

Yes
No

Enabled

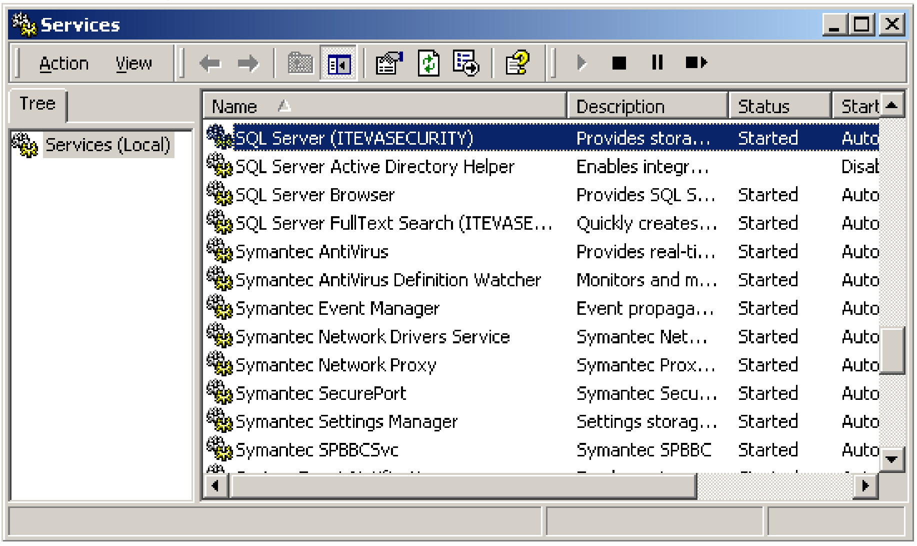
Enable or disable TCP/IP protocol for this server instance

4 Click to set the **Enabled** field to **Yes**. Then click **OK** and **OK** again to acknowledge the warning prompt.

5 Close SQL Server Configuration Manager.

6 The changes you have made will not become effective until you have stopped and re-started the SQL Server Service. To do this, open the Services applet in Windows control panel:

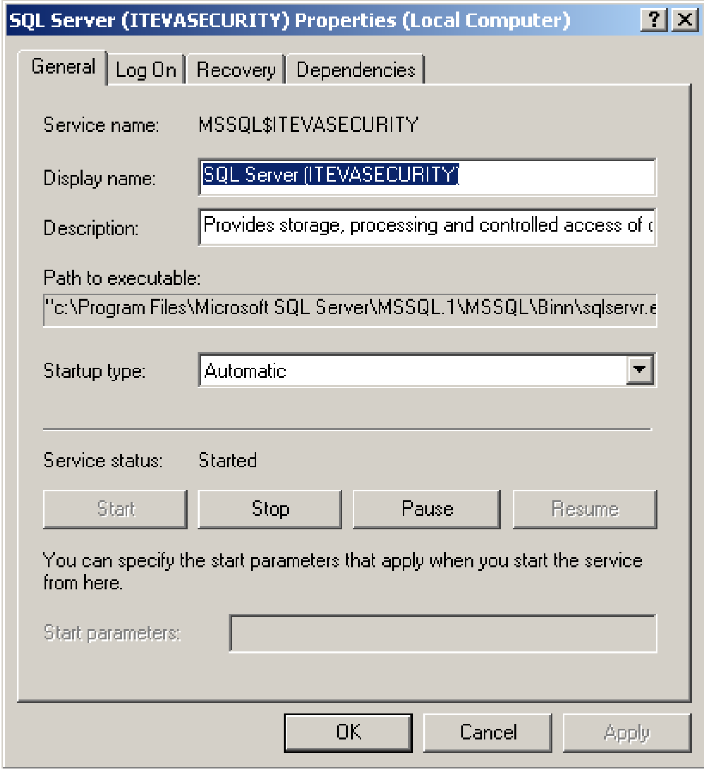
`Start>Settings>Control Panel>Administrative tools>Services`



Services

Name	Description	Status	Start
SQL Server (ITEVASECURITY)	Provides stora...	Started	Auto
SQL Server Active Directory Helper	Enables integr...		Disat
SQL Server Browser	Provides SQL S...	Started	Auto
SQL Server FullText Search (ITEVASE...	Quickly creates...	Started	Auto
Symantec AntiVirus	Provides real-ti...	Started	Auto
Symantec AntiVirus Definition Watcher	Monitors and m...	Started	Auto
Symantec Event Manager	Event propaga...	Started	Auto
Symantec Network Drivers Service	Symantec Net...	Started	Auto
Symantec Network Proxy	Symantec Prox...	Started	Auto
Symantec SecurePort	Symantec Secu...	Started	Auto
Symantec Settings Manager	Settings storag...	Started	Auto
Symantec SPBBCSvc	Symantec SPBBC	Started	Auto

7 Scroll down to the service named SQL Server (ITEVASECURITY) and double-click on the Service name. The service properties dialogue is displayed.



SQL Server (ITEVASECURITY) Properties (Local Computer)

Service name: MSSQL$ITEVASECURITY

Display name: SQL Server (ITEVASECURITY)

Description: Provides storage, processing and controlled access of d

Path to executable:
"c:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\Binn\sqlservr.e

Startup type: Automatic

Service status: Started

You can specify the start parameters that apply when you start the service from here.

Start parameters:

8 Click **Stop**. Windows will now attempt to stop the service, which should succeed. The Stop button will now be disabled and the **Start** button will become enabled.

9 Click **Start**. Windows will now attempt to start the service, which should succeed, resulting in the changes taking effect.

10 Click **OK** to close the Service Properties dialogue, and then close the Windows Services applet.

Complete (Networked installations only) □

Creating User Logins for SQL Server Express

All users of the iTEVA client software, who need to be able to access data stored in an analytical database, will need to have a log-in created for them in SQL Server Express. Log-ins can either be created individually for each user, or can be created for Windows user groups, thereby simplifying the administration process.

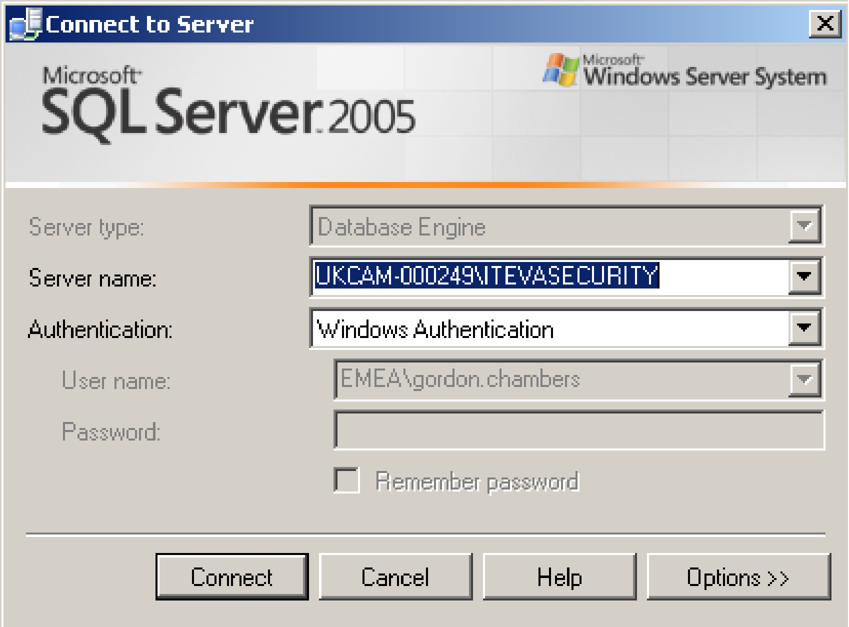
These steps must be performed by someone who is a member of the 'Administrators' group on the computer onto which SQL Server Express has been installed.

1 Start SQL Server Management Studio Express:

Note for Windows 7: You may need to run SQL Server Management Studio Express as an administrator. Use the Start menu as below, but instead of just running the Management Studio Express, **Right Click on it and select Run as administrator**.

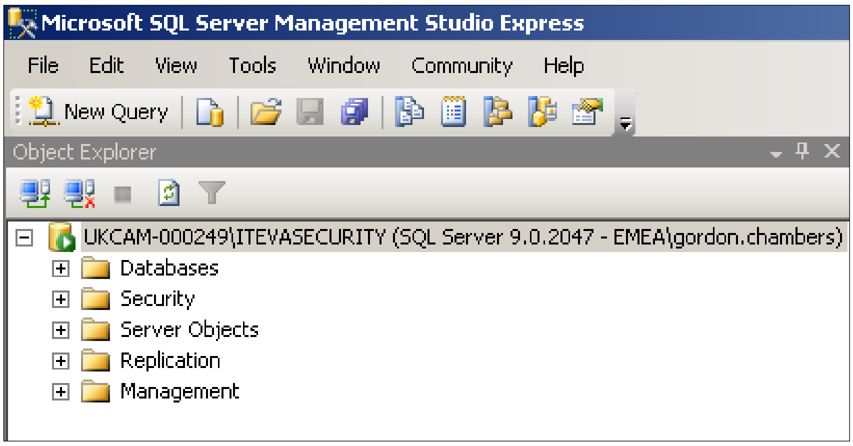
```
Start>Programs>Microsoft SQL Server 2005>SQL Server Management
Studio Express
```

The 'Connect to Server' dialogue will be displayed.

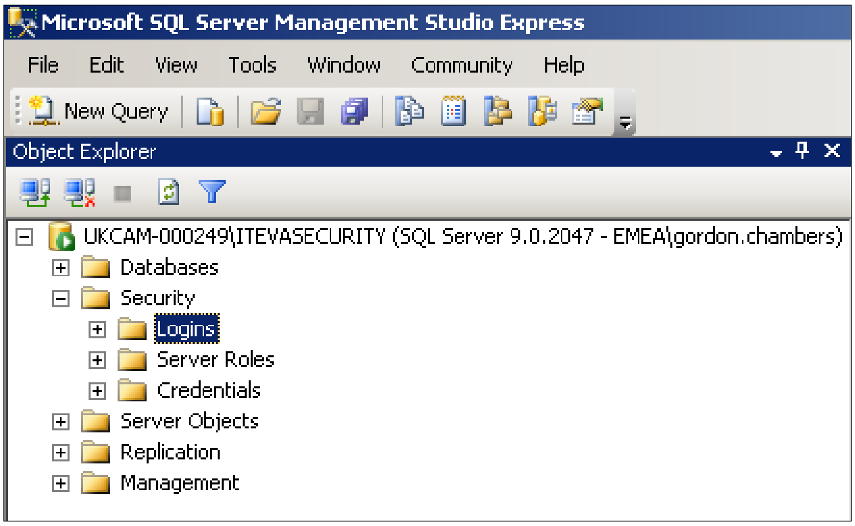


Server type: Database Engine
Server name: UKCAM-000249\ITEVASECURITY
Authentication: Windows Authentication
User name: EMEA\gordon.chambers
Password:
□ Remember password

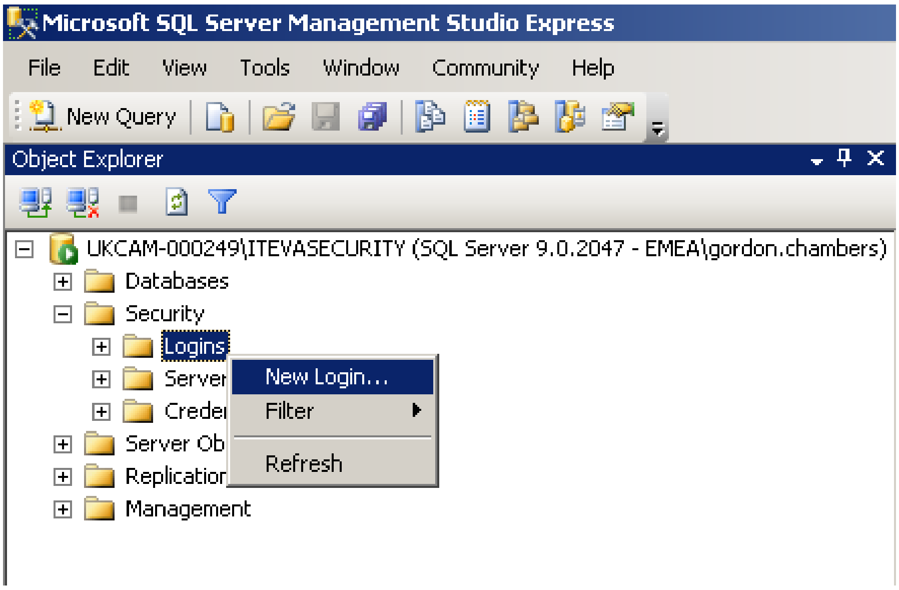
2 Select the server name that you wish to connect to, which will be in the form : <**computername>**ITEVASECURITY>. Select **Windows Authentication** as the authentication mode and click **Connect**. The Object Explorer window should then be displayed for the ITEVASECURITY instance of SQL Server.


Microsoft SQL Server Management Studio Express
File
Edit
View
Tools
Window
Community
Help
New Query
Object Explorer
UKCAM-000249\ITEVASECURITY (SQL Server 9.0.2047 - EMEA\gordon.chambers)
Databases
Security
Server Objects
Replication
Management

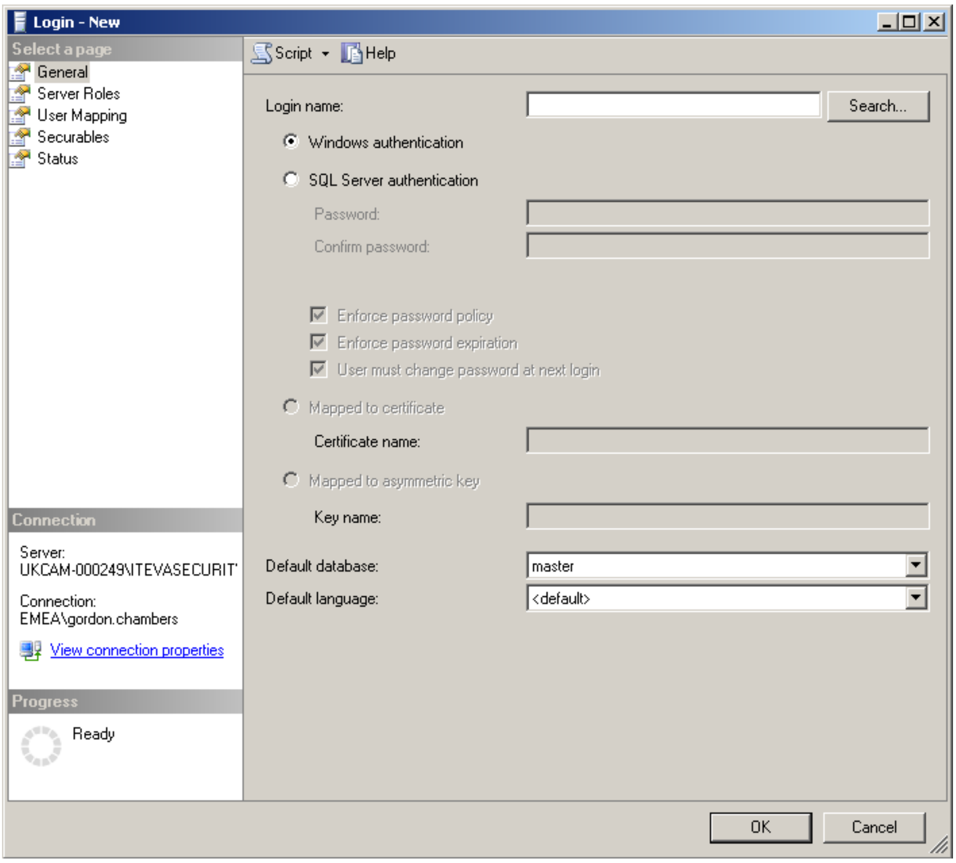
3 Click on the + next to **Security** to expand the Security branch of the object explorer tree.



4 Right-click on the **Logins** branch of the tree to display the logins popup menu.



5 Click on **New Login…** to display the Login – New dialogue.



Login name:

● Windows authentication

○ SQL Server authentication

Password:

Confirm password:

☑ Enforce password policy

☑ Enforce password expiration

☑ User must change password at next login

○ Mapped to certificate

Certificate name:

○ Mapped to asymmetric key

Key name:

Default database: master

Default language: <default>

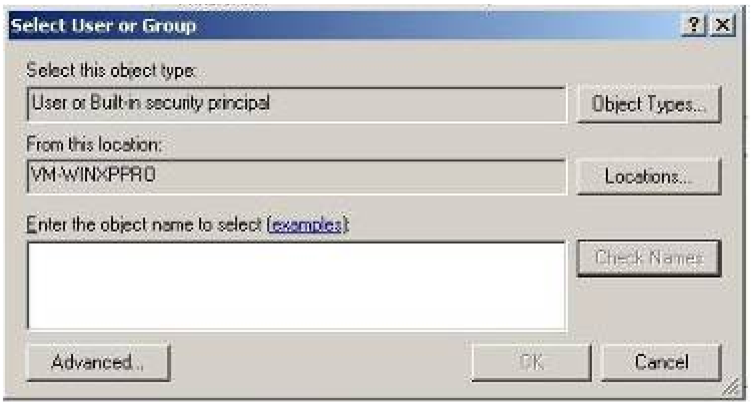
Server:
UKCAM-000249\ITEVASECURIT

Connection:
EMEA\gordon.chambers

Ready

6 Click on **Search…** to search for a user or group for which you wish to create a SQL Server log-in.

The "Select User or Group" below will be shown.



Select this object type:
User or Built-in security principal

From this location:
VM-WINXPPRO

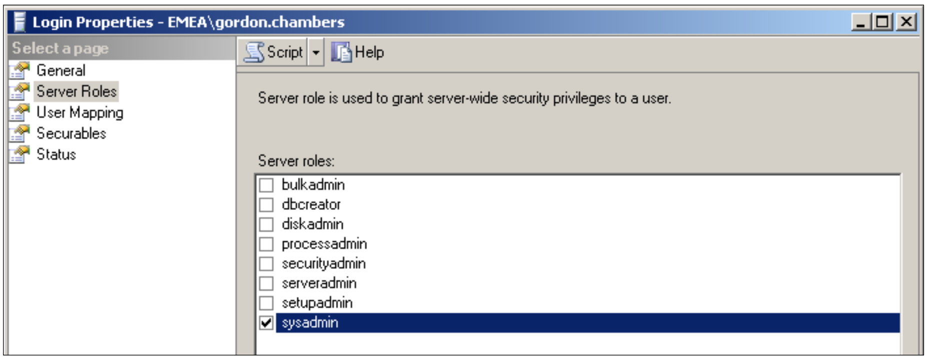
Type names into the 'object name' field and click **Check Names** to confirm name. Alternatively, click **Advanced…** and the **Find Now** for a list of available names. Choose a name and then click **OK**, then **OK** again to close both windows.

7 Click **OK** on the Login – New window, leaving all other settings at their default values.

The newly created login will be shown in the Logins list.

8 If the user or group that you have selected needs to be able to create and attach new analytical databases to SQL Server, then they must have the sysadmin server role assigned to their login. It is strongly recommended that this ability be restricted to those users who have the right to run the Thermo Security administration software.

Double-click on the user in the **Logins** list then click on the **Server Roles** page. To assign the sysadmin role, click to select the **Server Roles** page and check the box **sysasdmin**.



Server role is used to grant server-wide security privileges to a user.

Server roles:

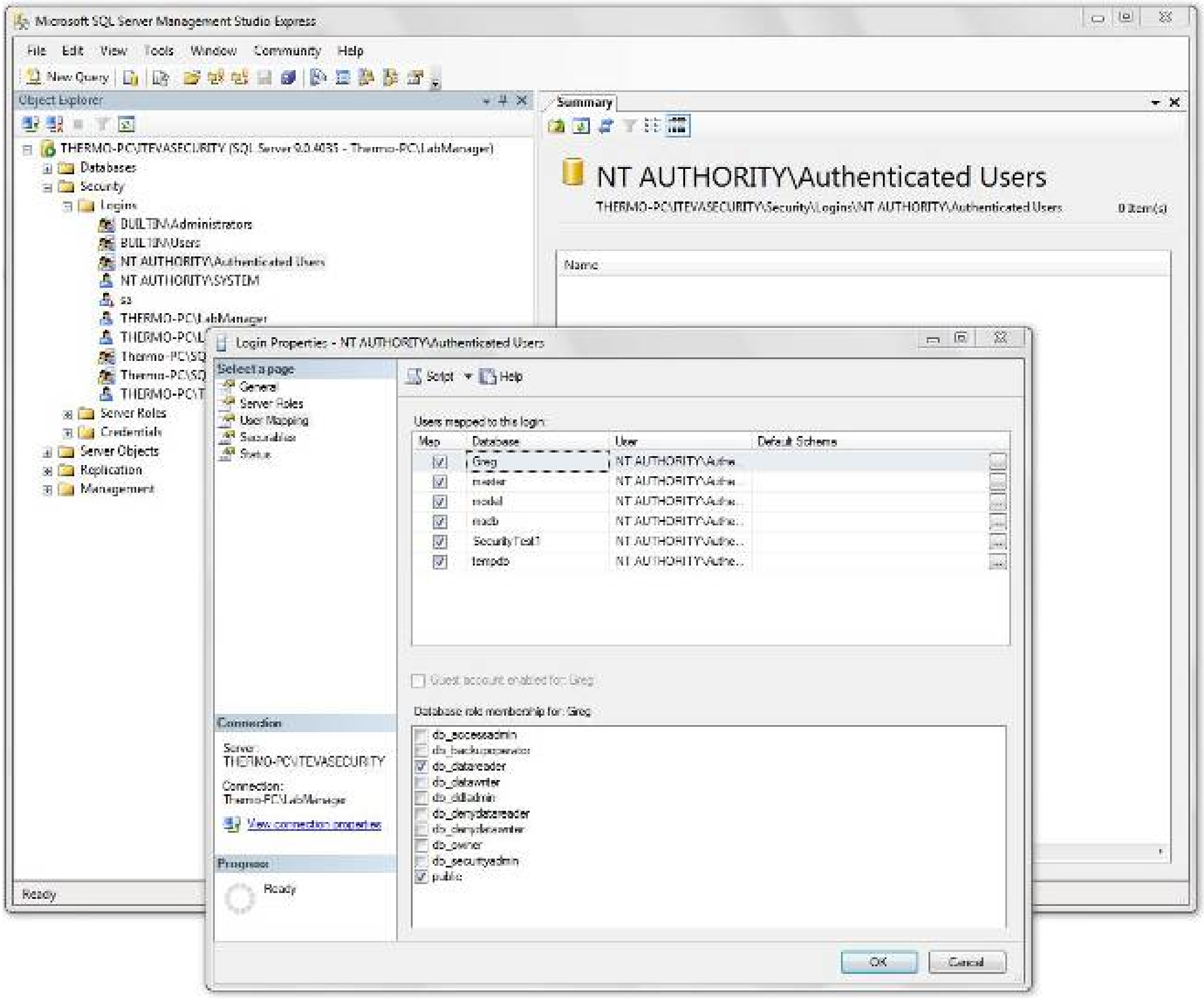
- □ bulkadmin
- □ dbcreator
- □ diskadmin
- □ processadmin
- □ securityadmin
- □ serveradmin
- □ setupadmin
- ☑ sysadmin

9 Click **OK** to close the login properties dialogue. The selected user or group will now be added to the list of SQL Server logins.

10 Repeat steps 4 to 8 for each user or group for which you wish to create a login.

11 Users must be mapped to each database in order to read data from them. A quick way to do this is to take the existing group **Authenticated Users** and map the group to each required database. Alternatively, individuals or other groups can be mapped separately.

Add the group **Authenticated Users** by right-clicking on **Logins** and selecting **New Login…**. Search for **Authenticated Users** and add it to the list of logins.


Microsoft SQL Server Management Studio Express
File Edit View Tools Window Community Help
New Query
Object Explorer
THERMO-PC\ITEVASECURITY (SQL Server 9.0.4035 - Thermo-PC\LabManager)
Databases
Security
Logins
BUILTIN\Administrators
BUILTIN\Users
NT AUTHORITY\Authenticated Users
NT AUTHORITY\SYSTEM
sa
THERMO-PC\LabManager
Server Roles
Credentials
Server Objects
Replication
Management
Ready
Summary
NT AUTHORITY\Authenticated Users
THERMO-PC\ITEVASECURITY\Security\Logins\NT AUTHORITY\Authenticated Users
0 Item(s)
Name
Login Properties - NT AUTHORITY\Authenticated Users
Select a page
General
Server Roles
User Mapping
Securables
Status
Script
Help
Connection
View connection properties
Progress
Ready
OK
Cancel

Server: THERMO-PC\ITEVASECURITY

Connection: Thermo-PC\LabManager

Users mapped to this login:

Map	Database	User	Default Schema
☑	Greg	NT AUTHORITY\Authe	
☑	master	NT AUTHORITY\Authe	
☑	model	NT AUTHORITY\Authe...	
☑	msdb	NT AUTHORITY\Authe...	
☑	SecurityTest1	NT AUTHORITY\Authe...	
☑	tempdb	NT AUTHORITY\Authe...	

☐ Guest account enabled for: Greg

Database role membership for: Greg

☐ db_accessadmin
☐ db_backupoperator
☑ db_datareader
☐ db_datawriter
☐ db_ddladmin
☐ db_denydatareader
☐ db_denydatawriter
☐ db_owner
☐ db_securityadmin
☑ public

12 Double click on **NT AUTHORITY\Authenticated Users** and in the **User Mapping** window make sure that **db-datareader** is ticked for all the databases required.

13 Save the changes by clicking on **File>Save All**, then close Microsoft SQL Server Management Studio Express.

4 of 9 Complete

□

Installing and Configuring the iTEVA *Security* client application

The iTEVA *Security* client software is installed from the iTEVA *Security* installation CD.

In a networked environment the client application is installed on one or more client computers on the network, which are normally the computers that are being used to control an iCAP spectrometer. In addition, it is often useful to install the client software on the server computer that is running SQL Server Express, as this provides an easy way for an administrator to create and attach analytical databases, using the Database Wizard in the client software.

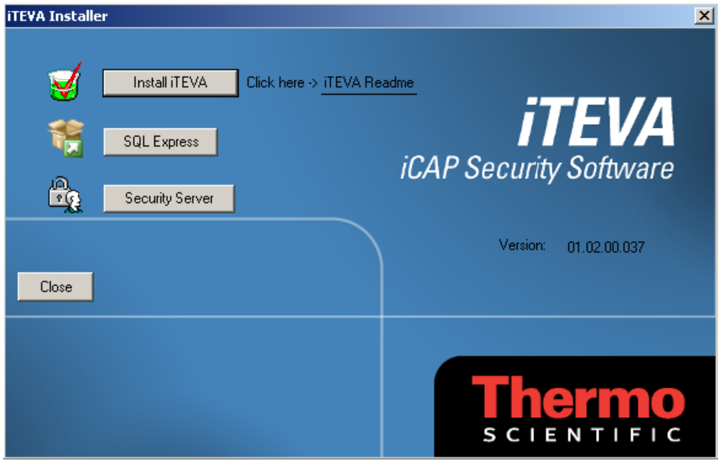
Installing the iTEVA *Security* client application

In a stand-alone environment the client application is installed on the single computer that is acting as both client and server.

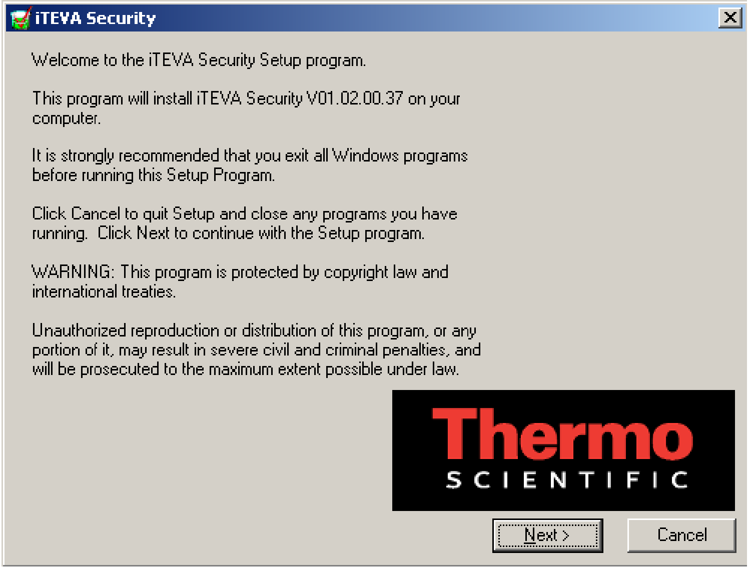
The client application must be installed by someone who is a member of the 'Administrators' group on the computer that it is being installed to.

Note If you purchased a PC from Thermo Fisher Scientific when you purchased your iCAP instrument, this will have the **iTEVA Routine** software pre-installed on it. It is recommended that you uninstall this software first (from Add/Remove programs) and then follow the instructions below to install **iTEVA *Security*** in its place.

1 Insert the installation CD into the CD drive of the client computer. The installation program should start running automatically. If it does not; using windows explorer, navigate to the contents of the CD drive and double-click on the file: `setup.exe`.



2 Click **Install iTEVA**.



Welcome to the iTEVA Security Setup program.

This program will install iTEVA Security V01.02.00.37 on your computer.

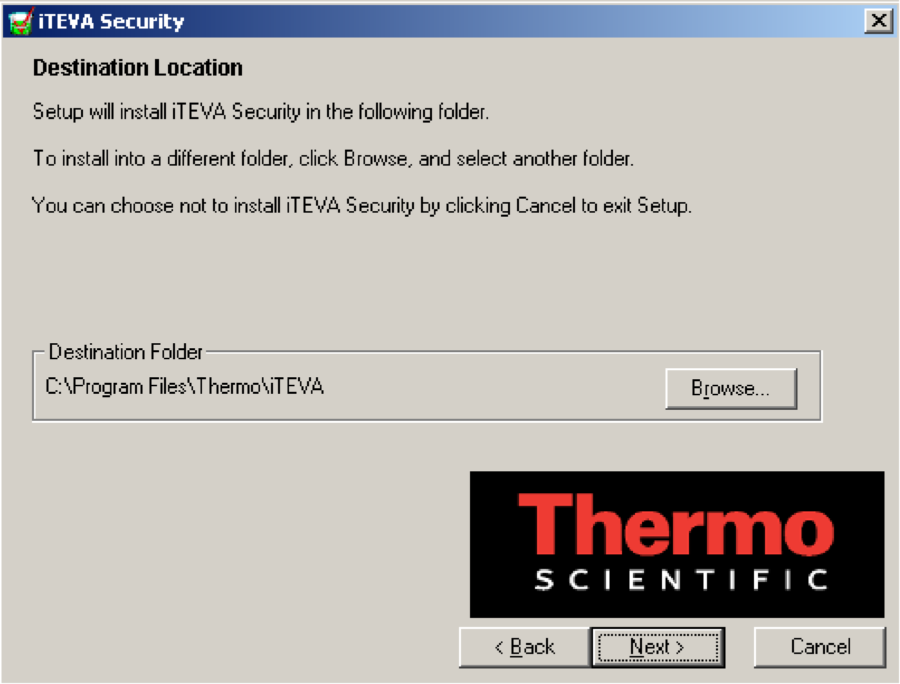
It is strongly recommended that you exit all Windows programs before running this Setup Program.

Click Cancel to quit Setup and close any programs you have running. Click Next to continue with the Setup program.

WARNING: This program is protected by copyright law and international treaties.

Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.

3 Click **Next**. The Destination Location dialogue allows you to change the location where files are installed. If you do this, always use the same location each time you install the software so that files are upgraded correctly when subsequent versions are installed. Typically, default locations are used for installation.



Destination Location

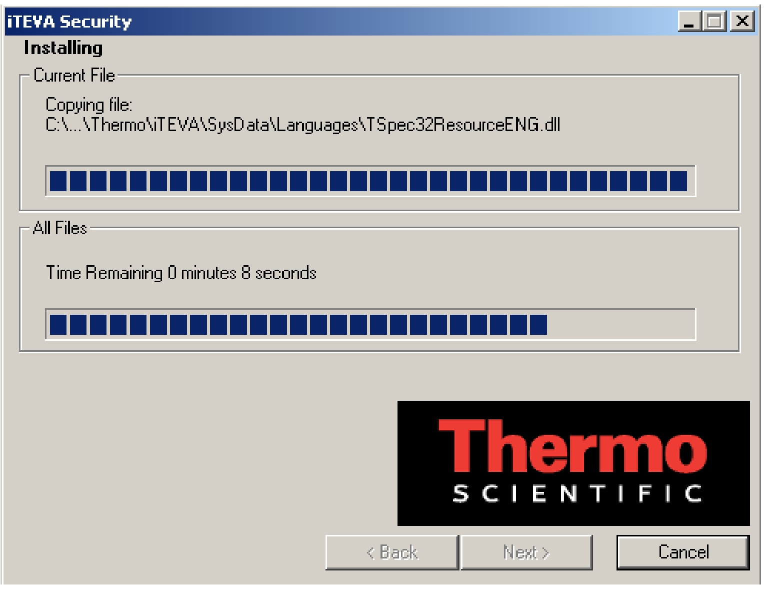
Setup will install iTEVA Security in the following folder.

To install into a different folder, click Browse, and select another folder.

You can choose not to install iTEVA Security by clicking Cancel to exit Setup.

Destination Folder
C:\Program Files\Thermo\iTEVA

4 Click **Next**. The iTEVA *Security* client application will now proceed to install.



iTEVA Security

Installing

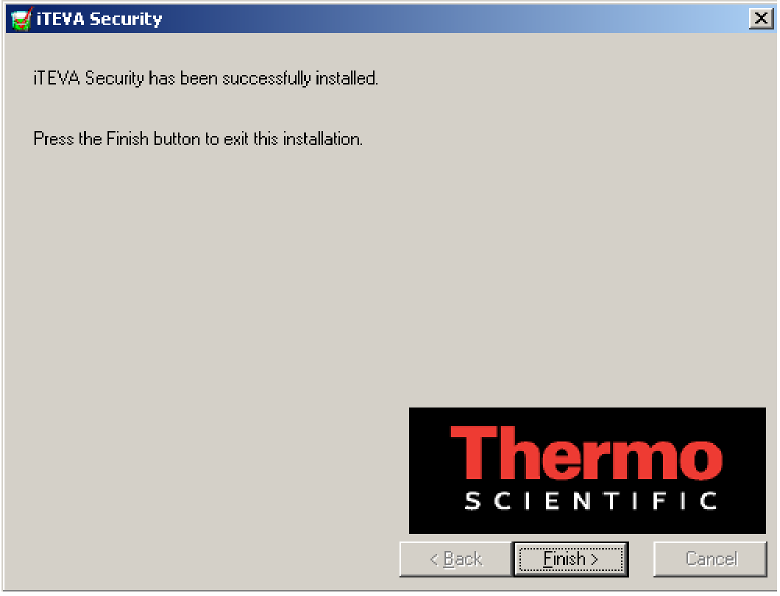
Current File

Copying file:
C:\...\Thermo\iTEVA\SysData\Languages\TSpec32ResourceENG.dll

All Files

Time Remaining 0 minutes 8 seconds

5 Click **Finish** after installation has completed. You will now be prompted to install the Thermo Security Client component.

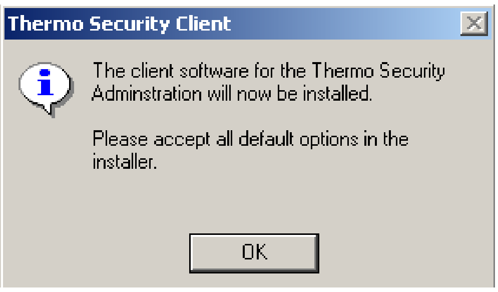


iTEVA Security

iTEVA Security has been successfully installed.

Press the Finish button to exit this installation.

6 Click **OK**. The installation Wizard will begin.

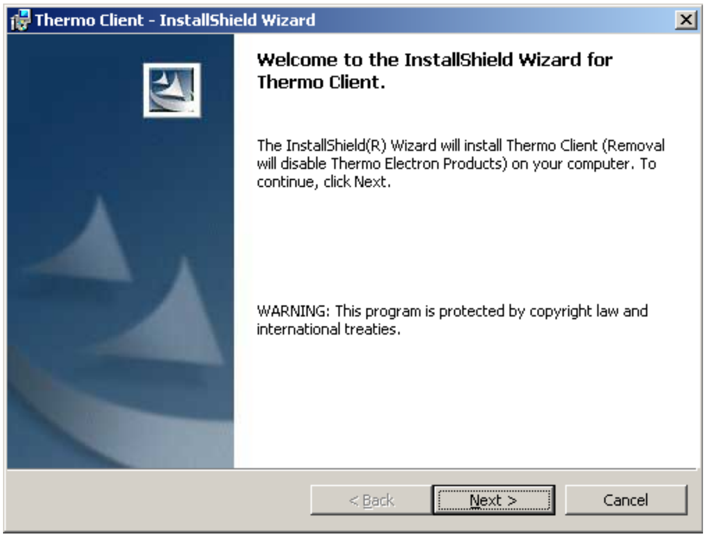


Thermo Security Client

The client software for the Thermo Security Adminstration will now be installed.

Please accept all default options in the installer.

7 Click **Next**.



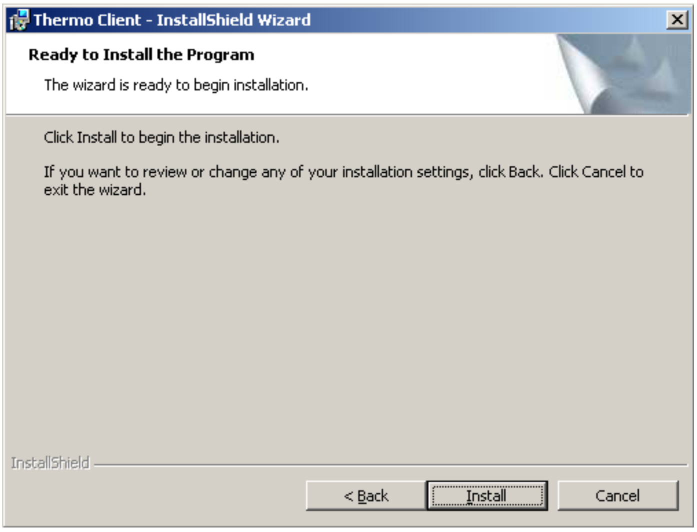
Thermo Client - InstallShield Wizard

Welcome to the InstallShield Wizard for Thermo Client.

The InstallShield(R) Wizard will install Thermo Client (Removal will disable Thermo Electron Products) on your computer. To continue, click Next.

WARNING: This program is protected by copyright law and international treaties.

8 Click **Install**. The Thermo Security client application will be installed.



Thermo Client - InstallShield Wizard

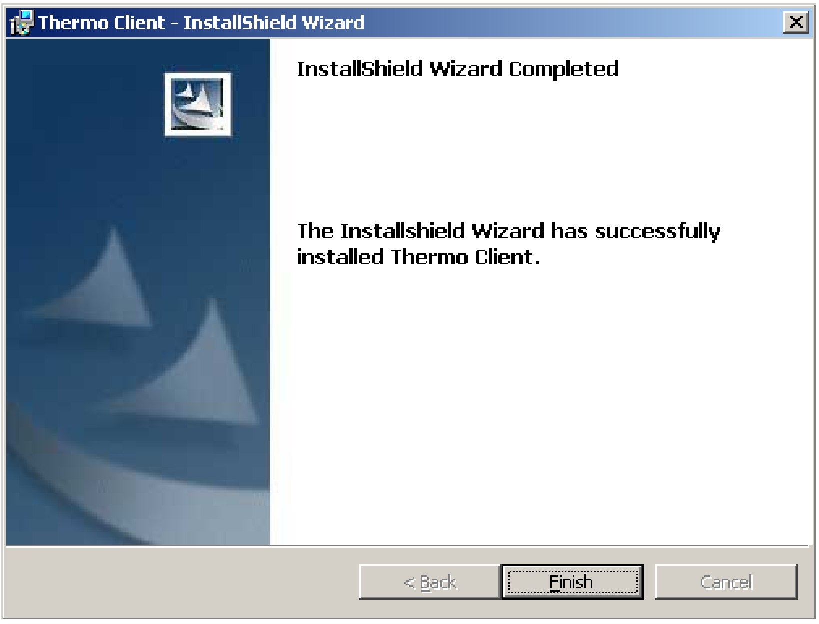
Ready to Install the Program

The wizard is ready to begin installation.

Click Install to begin the installation.

If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

9 Click **Finish**.

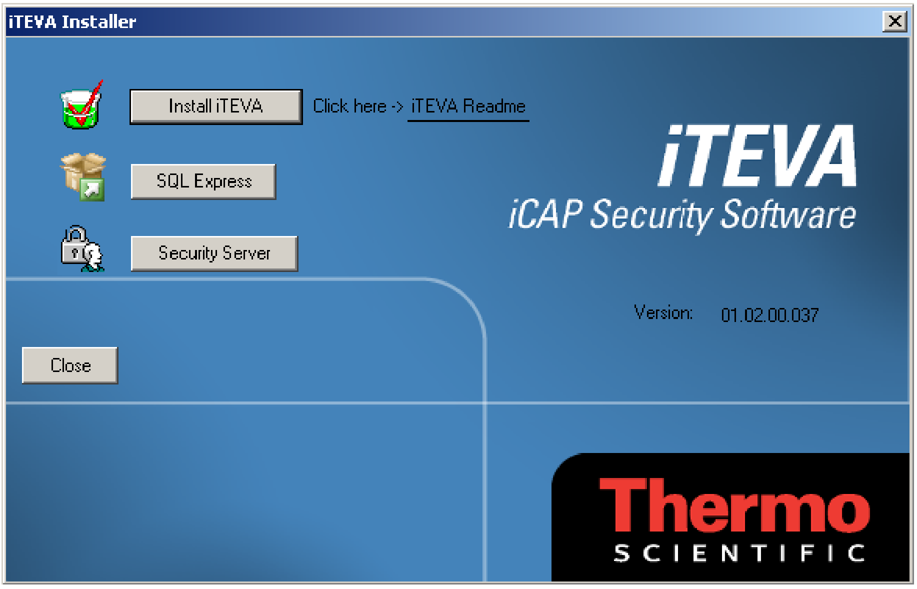


Thermo Client - InstallShield Wizard

InstallShield Wizard Completed

The Installshield Wizard has successfully installed Thermo Client.

10 Click **Close** on the iTEVA Security installer. When prompted to restart Windows, click **OK**.



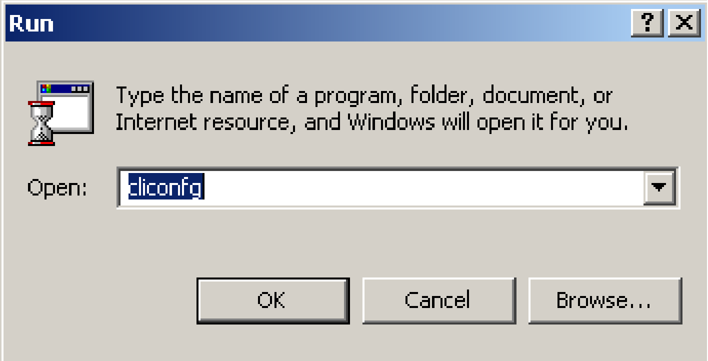
5 of 9 Complete
□

Configuring the iTEVA *Security* client application

If you have installed the iTEVA *Security* client application for use in a **networked environment**, it must be configured to communicate over your network. This involves making sure it can that it can communicate with SQL Server Express and that it can communicate with the Thermo Security Server application.

If you have installed iTEVA *Security* on **stand-alone system**, skip steps 1-4 and see the section *Running the iTEVA* Security *Client Application*.

1 To run the SQL Server Client Network utility, click **Run** from the Windows **Start** button and type '**cliconfg**' in the run dialogue.

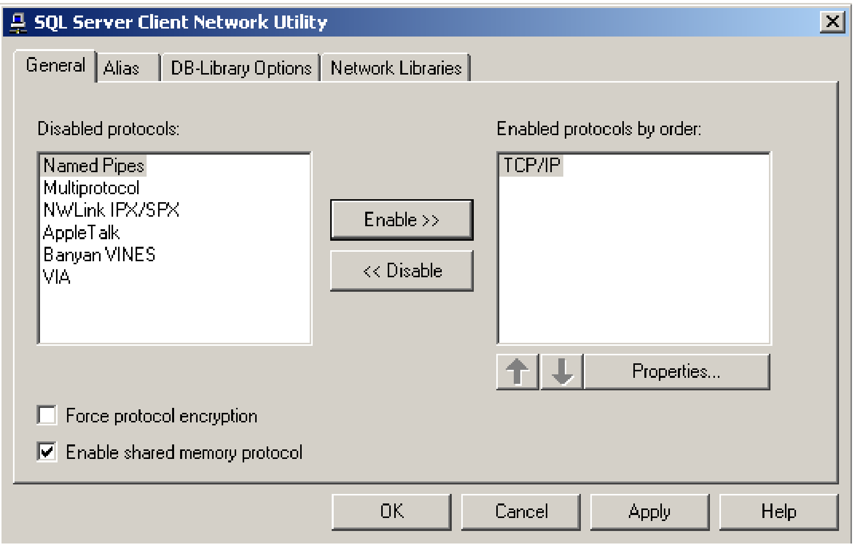


Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: cliconfg

2 Click **OK**. The SQL Server Client Network Utility starts.

3 Select TCP/IP in the list of disabled protocols and click **Enable** to add it in to the list of enabled protocols.



Disabled protocols:

Named Pipes
Multiprotocol
NWLink IPX/SPX
AppleTalk
Banyan VINES
VIA

Enabled protocols by order:

TCP/IP

☐ Force protocol encryption

☑ Enable shared memory protocol

4 Click **OK** to close the Client Network Utility

Complete (networked installations only)

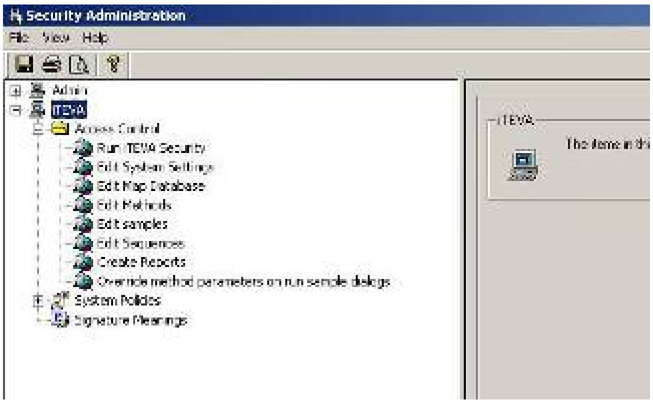
□

Before running the iTEVA *Security* Client Application

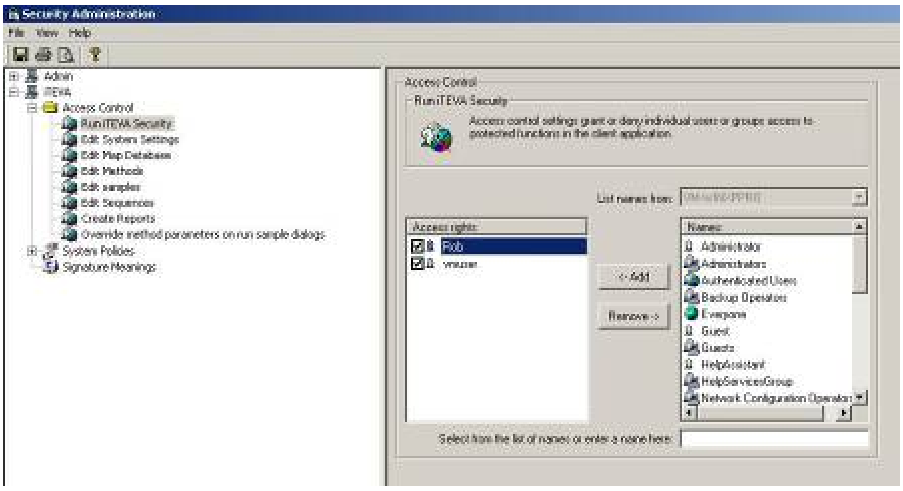
Before you are able to run the iTEVA *Security* client, user access must be granted in the Security Administration application. By default no users are given access to run iTEVA *Security*, so even administrators must be assigned access by the following method.

1 Open the Security Administration software by double clicking on the icon on the desktop. (For Windows 7 a login is required at this point.)

2 In the Security Administration software click on the + next to iTEVA and then the + next to Access Control. The various access control parameters will be shown.



3 To enable users to run iTEVA *Security* Client click on **Run iTEVA Security**. The Access Control Dialogue for “Run iTEVA Security” will be shown.



Access control settings grant or deny individual users or groups access to protected functions in the client application.

List names from:

Access rights:
☑ Rob
☑ vmuser

Names:
Administrator
Administrators
Authenticated Users
Backup Operators
Everyone
Guest
Guests
HelpAssistant
HelpServicesGroup
Network Configuration Operator

Select from the list of names or enter a name here:

4 Choose individual users or groups from the list of names and click **Add** to grant access rights.

5 Repeat the above steps to grant access rights to **Edit System Settings**.

6 In the toolbar select **File>Save Settings**, and then close the Security Administration Application.

6 of 9 Complete □

Running the iTEVA *Security* Client Application

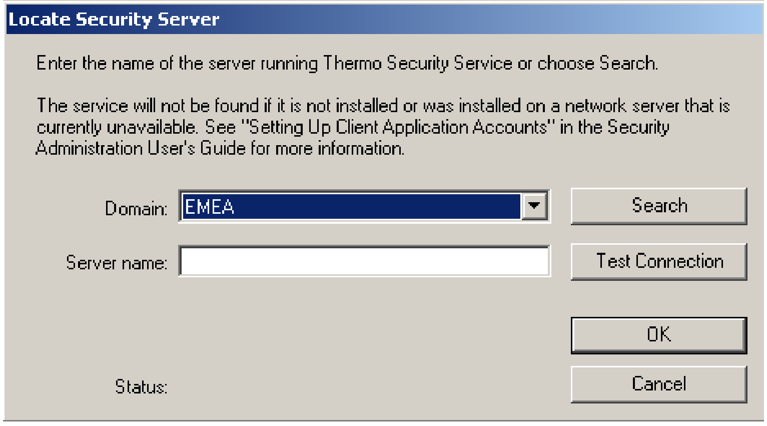
Once you have granted access to the current user, the iTEVA *Security* client can be opened.

The first time you run the iTEVA *Security* client application from any client computer, you must allow the client to locate the Thermo Security server.

1 Start the iTEVA *Security* client application:

```
Start>Programs>Thermo iTEVA Security>iTEVA Security
```

The Locate Security Server dialogue may be displayed. If this is not displayed skip to Step 5 below.


Locate Security Server

Enter the name of the server running Thermo Security Service or choose Search.

The service will not be found if it is not installed or was installed on a network server that is currently unavailable. See "Setting Up Client Application Accounts" in the Security Administration User's Guide for more information.

Domain: EMEA

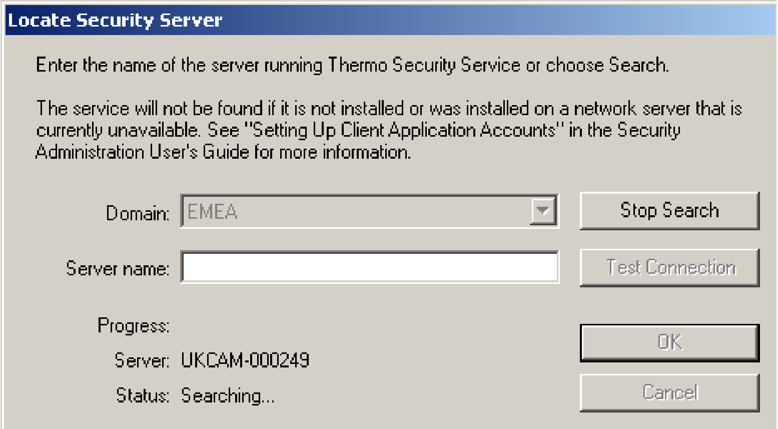
Server name:

Status:

2 Select the domain on which the Security Service is running, and then click **Search** to start the search process.

For **stand-alone configurations**, the local system will be shown when clicking search, and you can skip to step 5 below.

For a **networked configuration**, continue to step 3.



Locate Security Server

Enter the name of the server running Thermo Security Service or choose Search.

The service will not be found if it is not installed or was installed on a network server that is currently unavailable. See "Setting Up Client Application Accounts" in the Security Administration User's Guide for more information.

Domain: EMEA

Server name:

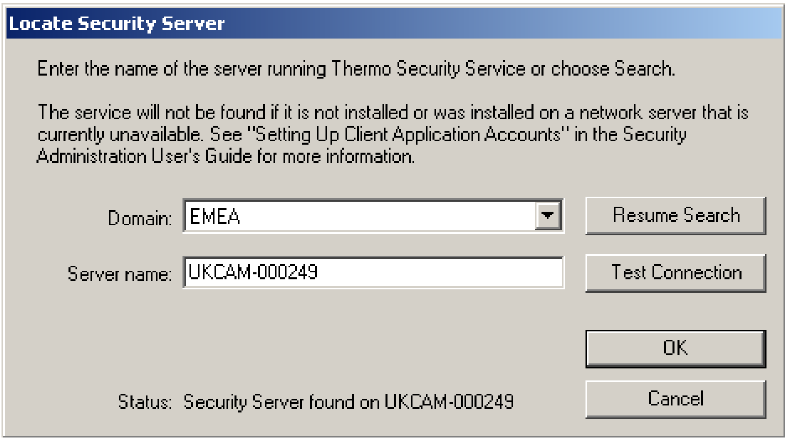
Progress:

Server: UKCAM-000249

Status: Searching...

Note If the domain that you are searching is very large (i.e. it has many computers that belong to it), the search process may take some considerable time. However, if you know the name of the server computer on which the security service is running, you can type it in to the Server name field directly, instead of searching for it. The server name can be found by logging on to the server and then right clicking on the **My Computer** icon and selecting the **Network Identification** tab.

3 When a valid server is found on the domain (i.e. one which is running the Thermo Security Server service) its name will appear in the server name field and the **Stop Search** button will be replaced by a **Resume Search** button.



Locate Security Server

Enter the name of the server running Thermo Security Service or choose Search.

The service will not be found if it is not installed or was installed on a network server that is currently unavailable. See "Setting Up Client Application Accounts" in the Security Administration User's Guide for more information.

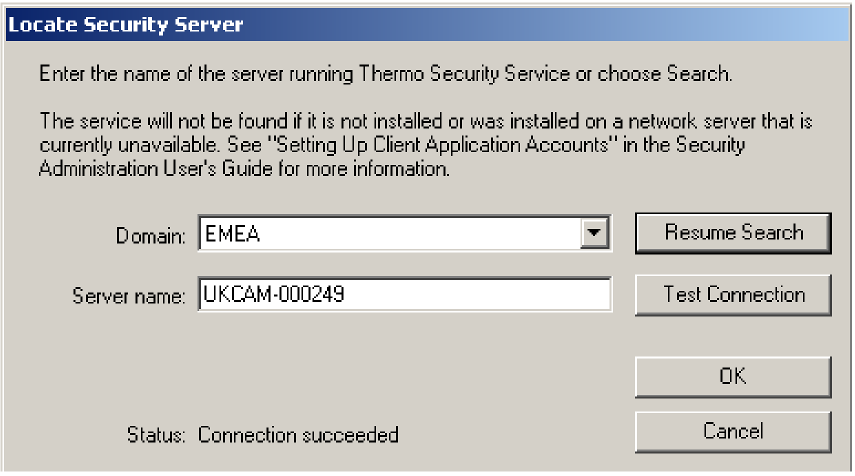
Domain: EMEA

Server name: UKCAM-000249

Status: Security Server found on UKCAM-000249

4 If the server that was found is not the correct server, click **Resume Search** to continue searching.

Once the correct server appears in the Server name field, click **Test Connection** and if the connection is valid the status area will report: **Connection Succeeded**.



Locate Security Server

Enter the name of the server running Thermo Security Service or choose Search.

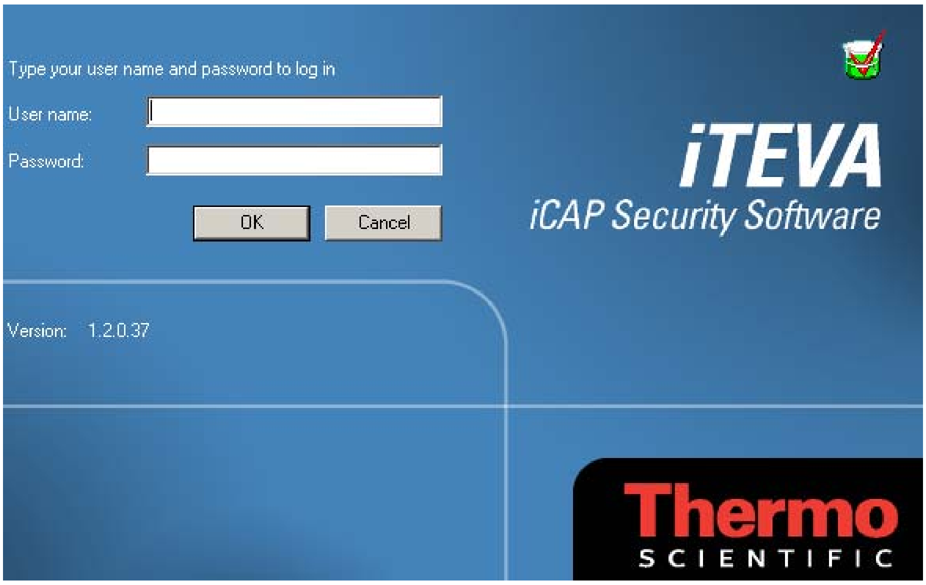
The service will not be found if it is not installed or was installed on a network server that is currently unavailable. See "Setting Up Client Application Accounts" in the Security Administration User's Guide for more information.

Domain: EMEA

Server name: UKCAM-000249

Status: Connection succeeded

5 Click **OK**. The iTEVA *Security* log-in screen will be displayed.



Type your user name and password to log in

User name:

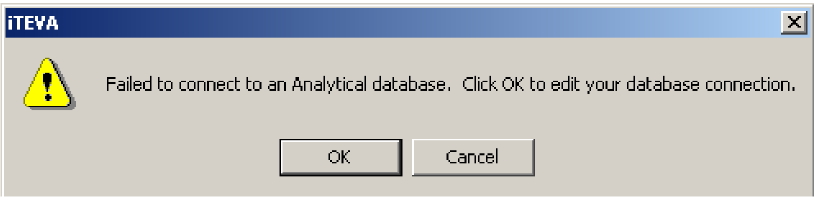
Password:

Version: 1.2.0.37

6 Enter your Windows username and password log to in to the iTEVA *Security* Client application.

You will now be prompted to create a connection to an analytical database.

Click **OK** to proceed. This will display the database options dialogue from where connections to analytical databases can be managed. This process is described in the following sections.



Failed to connect to an Analytical database. Click OK to edit your database connection.

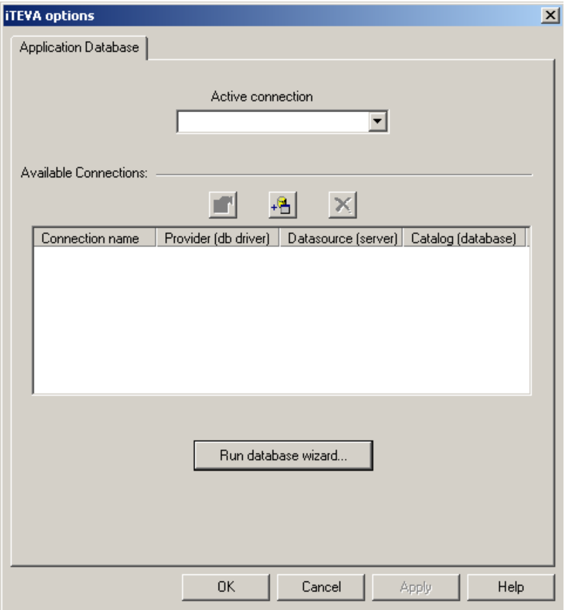
7 of 9 Complete

□

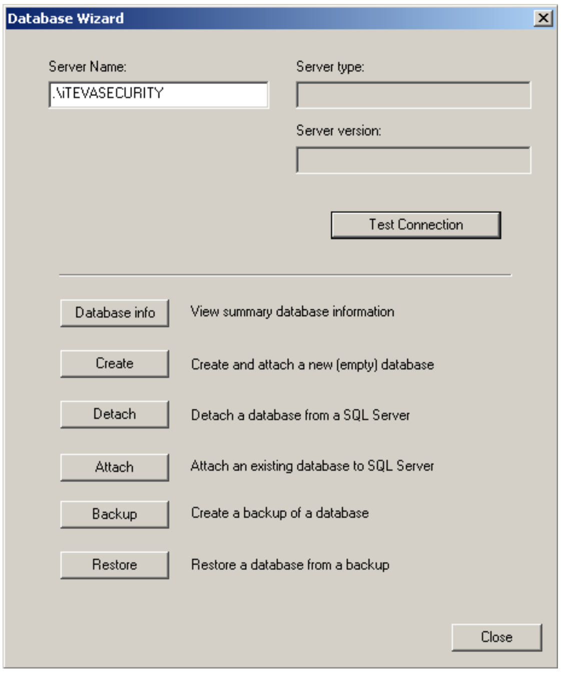
Creating an analytical database

To create an analytical database and attach it to SQL Server Express using the Database Wizard in the iTEVA *Security* client application, the iTEVA *Security* Client application must be installed on the same computer as SQL Server Express. It will subsequently be possible to connect to the newly created database from other instances of the iTEVA *Security* Client application, installed on other client computers on the network.

1 Click **Run Database Wizard…** from the Application Database options dialogue. The Database Wizard dialogue is displayed.



2 Click **Create** to create and attach a new empty database.



Server Name: .\iTEVASECURITY

Database info — View summary database information

Create — Create and attach a new (empty) database

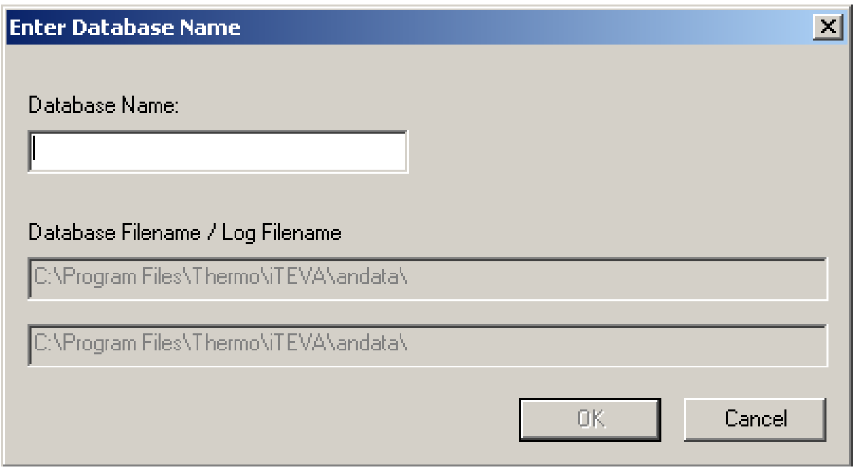
Detach — Detach a database from a SQL Server

Attach — Attach an existing database to SQL Server

Backup — Create a backup of a database

Restore — Restore a database from a backup

3 Enter a meaningful name for your database and click **OK**. SQL Server Express will now create and attach a new empty database and you will be returned to the Database Wizard Page.



Enter Database Name

Database Name:

Database Filename / Log Filename

C:\Program Files\Thermo\iTEVA\andata\

C:\Program Files\Thermo\iTEVA\andata\

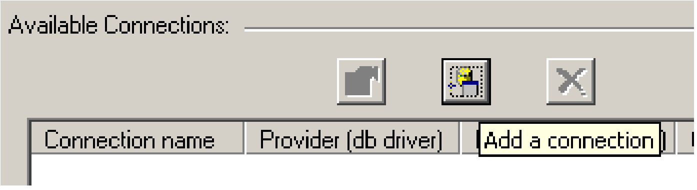
4 Click **Close** on the database Wizard. You may now create a connection to the newly created database on any client computer that requires it.

8 of 9 Complete

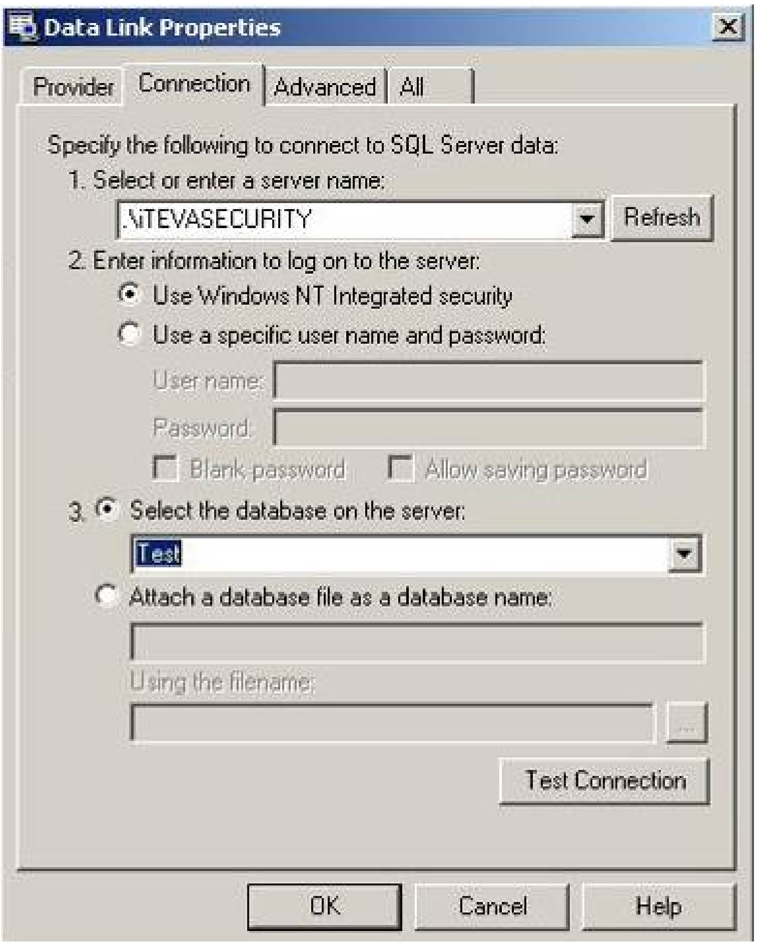
□

Creating a connection to an analytical database

1 Click the **Add a connection** button from the Application Database options dialogue.



A **Data Link Properties** dialogue is displayed.


Data Link Properties

Provider | Connection | Advanced | All

Specify the following to connect to SQL Server data:

1. Select or enter a server name: .\ITEVASECURITY [Refresh]

2. Enter information to log on to the server:

● Use Windows NT Integrated security

○ Use a specific user name and password:

User name:

Password:

□ Blank password □ Allow saving password

3. ● Select the database on the server: Test

○ Attach a database file as a database name:

Using the filename:

[Test Connection]

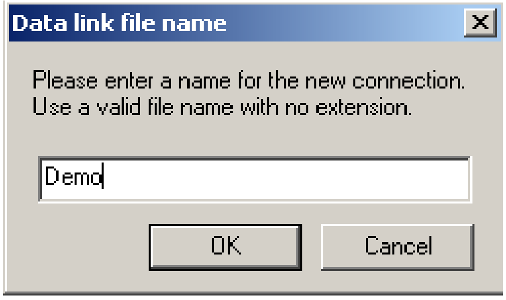
[OK] [Cancel] [Help]

2 **Select or enter the server name** of the instance of SQL Server to which the database has been attached. By default this will be ".\ITEVASECURITY" which is the instance on the local computer. If you are connecting to a database on another networked computer, select the appropriate entry from the list.

3 Make sure **Use Windows NT Integrated Security** is checked.

4 **Select the database on the server** from the drop-down list that you wish to connect to.

5 Click **OK**. You will be prompted to give a name to the new connection. To avoid confusion we recommend giving the connection the same name as the database.



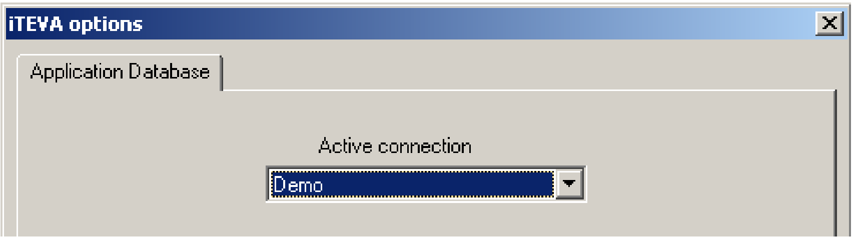
Data link file name

Please enter a name for the new connection.
Use a valid file name with no extension.

Demo

6 Click **OK** to create the connection. The connection will now appear in the list of available connections.

7 To make this connection the active connection (i.e. the one that you are currently connected to) select it from the drop-down **Active connection** list.



iTEVA options

Application Database

Active connection: Demo

8 Click **OK**.

9 Depending on the access rights of the user, when creating a new database it may be necessary to grant access to users by following step 12 in the **Creating User Logins for SQL Server Express** section above.

9 of 9 Complete □

Please ensure you have completed all 9 sections of the installation procedure and the two extra sections if you are installing iTEVA *Security* on a network.

Troubleshooting Guide

Problem

A ‘Password does not match’ error is reported when attempting to log in to the iTEVA *Security* client application or the Security Administration application. I know the password is correct.

Likely Cause

This may be caused by failing to correctly set the sharing and security model for local accounts. Or, the PC will not accept a user with a blank password.

Solution

On the client computer, double-click local security policy in the administrative tools window: `Start>Settings>Control Panel>Administrative tools>Local Security Policy`. The local security settings dialog box appears. Open the ‘Local Policies’ folder and then click on the ‘Security Options’ folder. Scroll down to ‘Network Access: Sharing And Security Model For Local Accounts’ on the right hand pane and double click on it. A ‘Network Access’ dialog appears. In the list box, select ‘Classic – Local Users Authenticate as themselves’ and then click OK. Close the local security settings dialog and then close the Administrative tools window. You will need to log out of Windows and back in again for the settings to take effect.

Problem

I have been granted the right to run the iTEVA *Security* client application, but when I try to run it – nothing happens.

Likely Cause

You do not have the necessary Windows security group membership to run the iTEVA *Security* client application. It is not sufficient for iTEVA users to have membership of the windows ‘users’ security group; they must have membership of the ‘Power Users’ group. This is because Windows will only allow ‘users’ to run ‘certificated’ applications and iTEVA is not a ‘certificated’ application.

Solution

To grant membership of the Power Users group, follow the instructions appropriate to your Windows configuration in Setting up Windows Administration in the document SecAdminUserGuide.pdf.

Problem

I have been granted the right to Edit System Settings in the Security Administration software but when I attempt to create and attach a database using the iTEVA database Wizard, I get an error reported: ‘Cannot alter the application role iTEVA’ because it does not exist or you do not have permission’.

Likely Cause

The SQL Server login for your user account has not been assigned the sysadmin server role.

Solution

Log into the computer that is running SQL Server Express as a user who is a member of the administrators group on that machine. Start SQL Server Management Studio Express and connect to the ITEVASECURITY instance of SQL Server:

`Start>Programs>Microsoft SQL Server 2005`

Expand the security branch of the tree in Object Explorer and then expand the logins branch. Double-click on the login name for the user account that you wish to modify.

On the Login Properties dialog, select the Server Roles page and check the sysadmin checkbox. Click OK and shut down Sequel Server Management Studio Express.

Problem

I have been granted an access right in the Security Administration software - but when I log on to the iTEVA *Security* client application I find that I cannot perform the corresponding operation.

Likely Cause

It is likely that you have ‘inherited’ an access control setting through being a member of a Windows security group that has been denied the access right in question.

Solution

Review the group membership for your Windows account and check that none of the groups that you belong to have been denied the access right in question. Care is required when denying an access right to a group, since an ‘access denied’ setting will always take precedence over an ‘access granted’ setting. You can always check the value of the accumulated access rights for your user account from the iTEVA client application. Go to `Tools>Options>Access Rights`.

Problem

SQL Server Management Studio Express does not run.

Likely Cause

The Windows component, Internet Information Services (IIS) is required for certain aspects of SQL Server to work. Not having IIS installed will not affect any functionality of the iTEVA *Security* software, but may cause the installation of SQL Server Management Studio Express to fail.

Solution

Install IIS through Control Panel>Add or Remove Programs>Add Remove Windows Components. If not available here, it will need to be installed from your Windows installation CD.

Problem

Following an upgrade of the iTEVA Security software the application database upgrade fails.

Likely Cause

The database needs to be detached and reattached to the SQL server prior to attempting to upgrade the database.

Solution

Enter the Database Wizard via Control Center, `Tools>Options>Application Database` and detach the database you wish up upgrade. Once the detach process is completed, reattach the database and set the active connection to the database you wish to upgrade (the one that has just been detached and reattached) and select ok. The database should upgrade successfully.