tecom
Security Commander

Security Commander Installation Manual

P/N 1070183 • REV 07 • ISS 12OCT15

Trademarks and patents The Security Commander name and logo are trademarks of UTC Fire & Security.

Other trade names used in this document may be trademarks or registered trademarks of the manufacturers or vendors of the respective products.

Manufacturer UTC Fire & Security Australia Pty Ltd t/a Interlogix
A UTC Building & Industrial Systems company
Ground Floor, 10 Ferntree Place, Notting Hill, VIC, 3168, Australia

Contact information For contact information, see www.interlogix.com.au.

Content

Important information

Scope of this manual

This manual provides information for Integration Technicians to:

- Install Security Commander on a server computer.
- Optionally install Security Commander on one or more client computers.
- Upgrade Security Commander to a later version (or to reinstall the same version).

The term “Security Commander” is used for either Security Commander or Security Commander Lite, except where noted. See “Software editions” on page 1 for details.

This manual provides sufficient information to install Security Commander, and to check that the installation was successful, for a user with the network permissions of Administrator.

This manual does not describe how to plan and structure an entire security and access control system.

Related documentation

Refer to the following:

- *Security Commander Help*: Provides reference information, such as screen and field descriptions, along with instructions for system administrator duties, such as configuring Challenger panels.
- *Security Commander Administration Manual and Operation Guide*: Provides information for both the system administrator and the operator to program, configure, and use the Security Commander system.
- *Security Commander Photo ID User Guide*: Provides instructions for users of the optional Photo ID package (not available in Security Commander Lite).
- *Security Commander CCTV Interface Guide*: Provides interface instructions for CCTV equipment (not available in Security Commander Lite).
- *Security Commander API Manual*: Security Commander API (Application-Program Interface) provides the ability to import data from external applications such as a Human Resource Management System (not available in Security Commander Lite).

Typographical conventions

This manual uses certain notational and typographical conventions to make it easier for you to identify important information.

Table 1: Notational and typographical conventions

Item	Description
Command sequences	Where appropriate, command sequences are abbreviated with the “>” symbol. For example, the command “Click Start, and then click Run” is written as “Click Start > Run”. The command Start > Run, means open a Windows command prompt. Some Windows versions do not have Run in the Start menu by default, but it may be added.
Command alternatives	Many commands can be executed in a variety of ways including menu bar, tool bar, shortcut keys, right click, or double-click. In general, commands are described from their menu bar location only, even when alternatives exist.
Keys	Capitalized, for example “press Enter”.
Keystrokes	Text that you type is indicated in Courier New font. For example, “Type `dcomcnfg`”.
Expanding a “tree” view	The word “expand” is used to indicate that selections may be hidden. For example, the command “Click the + box next to Computers” is written as “Expand Computers”.
Notes	Notes alert you to information that can save you time and effort.
Caution	Cautions are displayed to advise the user that failure to take or avoid a specified action could result in loss of data.

System introduction

Software editions

Security Commander Lite is a cut-down edition of system management software intended for small Challenger systems. Security Commander Lite runs on a single server computer, with no additional clients. The number of simultaneous connections to active Challenger panels is limited to five.

Certain features of the full Security Commander edition are not available in Security Commander Lite:

- Photo ID and badge design
- Video integration
- Client computers
- User import API
- Email notification
- Client monitor
- Graphic maps

Refer to the *Software Comparison Matrix* for a detailed comparison of Tecom's management software products.

Challenger panel versions

Security Commander may be used with the following types of Challenger panels:

- Challenger V8 control panels using firmware version 8.128 (or later) and fitted with a memory expansion module model TS0882, TS0883, or TS0884. This configuration is called "V8 Extended".
- Challenger10, ChallengerSE, or ChallengerLE control panels using firmware version V10-06 (or later). These panels are called "Challenger Series".

The term "Challenger Series" does not apply to legacy products such as Challenger V8.

Note: Challenger10, ChallengerSE, and ChallengerLE control panels have differing capacities. Refer to the topic "Challenger Series features" in Security Commander help for details.

System overview

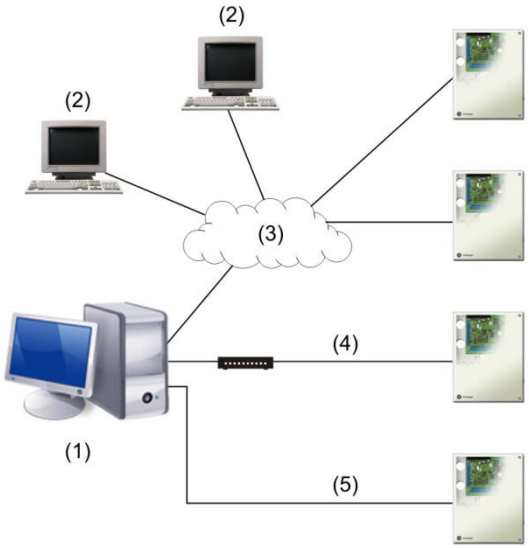
Subject to the limitations described in "Software editions" above, Security Commander management software is comprised of at least one computer (the server). The Security Commander server computer typically communicates with multiple client computers, to multiple Challenger control panels, and optionally to other security devices such as digital video recorders (DVRs).

Security Commander computers have a user interface and have background applications called services. A service can start automatically when the computer starts, and remains running in the background, regardless of whether a user is logged in. It is important to realise that logging out of the user interface and closing it does not stop the services. For more information about services, see “Configuring services” on page 18.

The Security Commander server computer must have access to a database server. The database server is installed by default on the Security Commander server computer, but may be on a different computer if required. The default installation process installs SQL Server 2012 Express Edition on the Security Commander server computer. Alternatively, the full version of SQL Server 2012 may be used if required (not provided with Security Commander).

Refer to Figure 1 below for an overview of a basic Security Commander system (Security Commander Lite does not support remote clients).

Figure 1: Security Commander system connection options



1. Security Commander server computer
2. Security Commander client computers (subject to licensing)
3. Connection to clients and control panels via IP
4. Connection to control panels via RS-232 to modem and PSTN to control panel
5. Connection to control panels via RS-232

Note: The number of simultaneous connections to client computers, control panels, and options like Photo ID is subject to licensing.

Refer to the *Security Commander Administration Manual and Operation Guide* for details about connecting to control panels.

Before you begin

This section lists the things you need to consider before you install Security Commander.

Note: The use of client computers does not apply Security Commander Lite.

Supported operating systems

The Security Commander server or client computer must use one of the following Microsoft Windows operating systems, with the latest service pack installed:

- Windows 7 Professional or above 32- or 64-bit
- Windows 8.1 Pro or above 64-bit
- Windows 10 Pro or above 64-bit
- Windows Server 2008 R2 64-bit (server only)
- Windows Server 2012 64-bit (server only)
- Windows 7 Professional or above 32- or 64-bit (server only)
- Windows 8.1 Pro or above 64-bit (server only)
- Windows 10 Pro or above 64-bit (server only)

Notes:

- Any Security Commander computer that hosts a Challenger control panel via IP must be configured to use a static IP address (except for Challenger Series control panels using the dynamic IP address option).
- A Security Commander server requires at least 3 GB of RAM. Security Commander clients require at least 2 GB of RAM.
- Review “Appendix A. Preparing the operating system” on page 27.

Does the computer have a Windows local group named "Administrators"?

The computer must have a Windows local group named “Administrators” with local administrator rights.

Ensure the required network ports are not blocked

When installing Security Commander a number of Windows Firewall ports are automatically configured. The required ports are:

- Port 135 (UDP and TCP) for RPC
- Port 137 and 138 (UDP), 139 (TCP) and 445 (TCP) for file sharing and computer browsing
- Port 1024 (TCP) for DVR connection
- Port 1434 (UDP) used by default for SQL
- Port 1433 (TCP) used by SQL (depending on how SQL was installed)
- 6700 to 6715 (TCP and UDP) for receiving communications from the Security Commander server to clients.

The Windows Firewall settings are created automatically (or can be re-applied) using SPInitClient.exe in the Security Commander program folder. Other firewall applications will need to be configured manually.

Server computer installation tasks

To set up a Security Commander server computer:

1. Check minimum hardware and software requirements. See page 5.
2. If you are not installing SQL Server 2012 Express Edition software provided on the Security Commander CD, refer to “Optional SQL Server” on page 5 before you install Security Commander.
3. Install Security Commander software (part 1). See page 6.
4. Install Security Commander software (part 2, database). See page 10.
5. Register the Security Commander license. See page 13.
6. Configure Security Commander services. See page 17.
7. Verify that services are running. See page 18.
8. Optional: Install Photo ID. See page 19.
9. Optional: Install Microsoft Access. See page 20.
10. Optional: Program modems. See page 20.
11. Optional: Install and program the CCTV software and hardware. Refer to the *Security Commander CCTV Interface Guide*.
12. Optional: Install and program printers. See page 28.
13. Optional: Install a backup device. Refer to the backup device’s instructions.

Client computer installation tasks

Note: This section does not apply to Security Commander Lite.

To set up a Security Commander client computer:

1. Check minimum hardware and software requirements. See page 22.
2. Install Security Commander software (part 1). See page 6.
3. Configure Security Commander services. See page 17.
4. Verify that services are running. See page 18.
5. Optional: Install Photo ID. See page 24.
6. Optional: Install and program the CCTV software and hardware. Refer to the *Security Commander CCTV Interface Guide*.

Preparing the server computer

This chapter provides important information on setting up a Windows computer for Security Commander. We recommend that you read these sections carefully before you begin the installation. Perform the steps in the order they appear.

This chapter describes how to prepare the server computer to run Security Commander as server and client applications, as well as running the optional Photo ID application.

Minimum requirements

Required hardware

Refer to the *Security Commander Data Sheet* for recommended minimum specifications for a Security Commander server computer.

Hard disk space will vary depending on your system environment. If you elect to partition your hard drive, verify that sufficient space remains in your system drive for your program files to load properly.

Required software

See “Supported operating systems” on page 3.

Optional SQL Server

Microsoft SQL Server 2012 Express Edition is provided on the Security Commander CD.

Note: If you choose to use the full version of Microsoft SQL Server 2012, then an instance of SQL Server named “SPSQL” must be installed before you install Security Commander. Refer to “Setting up Microsoft SQL Server 2012 (optional)” on page 13.

Installing Security Commander on the server

Note: Some tasks do not apply to Security Commander Lite. Refer to “Software editions” on page 1 for details.

The procedures for installing Security Commander on a server computer are listed in “Server computer installation tasks” on page 4.

When installing Security Commander on the server computer, always log in as Administrator to the local computer and use the same login name and password for the entire installation process on all computers. Make sure to reboot whenever indicated during the installation process. The instruction to “log in as Administrator” means that you must log in as a user with administrative rights.

For the initial installation of Security Commander on a server computer for evaluation purposes, registration may be deferred, in which case Security Commander may be used in trial mode for up to 14 days (see “Trial mode” on page 15). After that time, if not registered, Security Commander may be used only in demonstration mode (see “Demonstration mode” on page 16).

Installation, part 1

This section describes the Security Commander installation process for both server and client computers, and Security Commander Lite for server computers.

Insert the Security Commander CD in the computer’s CD drive to launch the AutoPlay window.

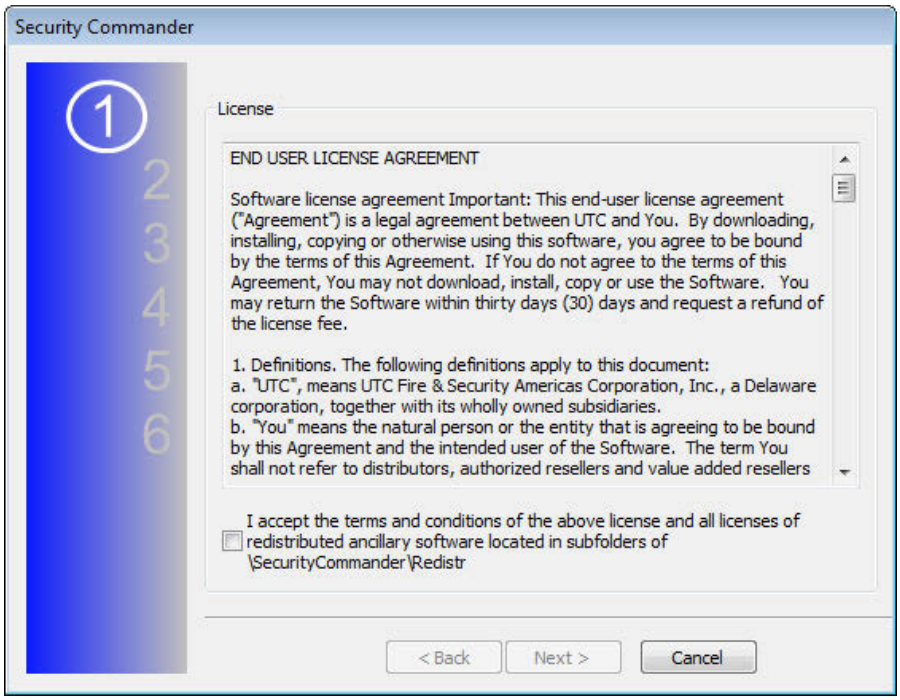
The AutoPlay window displays the following options:

- **Run setup.exe**. Select this option to immediately begin installing Security Commander.
- **Open folder to view files**. Select this option to display the files and folders on the CD. We recommend that you use this option to find and then open the web page “Before-you-begin” before you run setup.exe.

To install Security Commander:

1. At installation screen 1 (Figure 2 below) the End User License Agreement (EULA) displays. Read the license agreement, mark the “I accept …” check box to state that you agree, and then click Next (the Next button is inactive until the license is accepted).

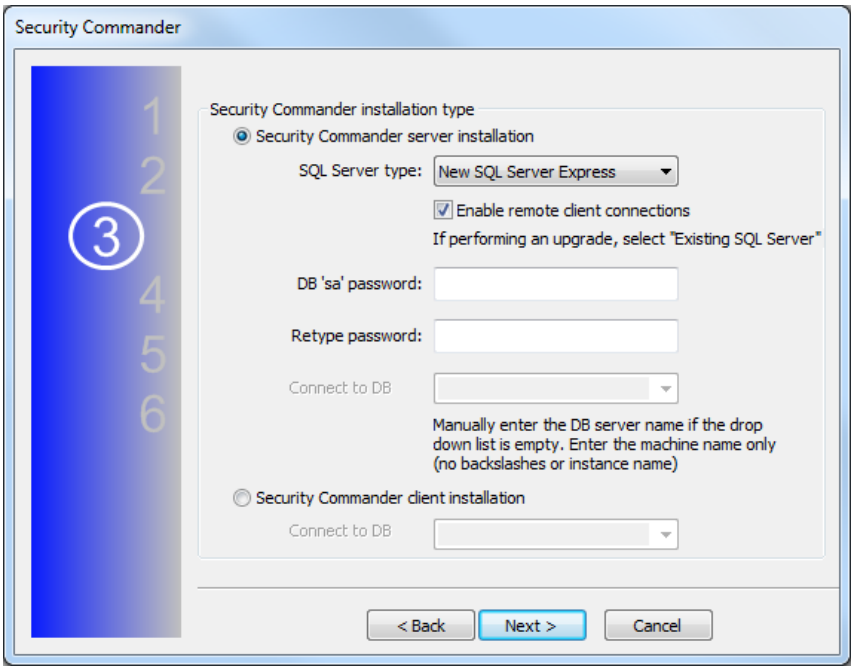
Figure 2: Installation screen 1



2. At installation screen 2 select the default destination path (or click the browse button to select a different destination), and then click Next.

3. At installation screen 3 your selections will be based on the type of installation:
   - Server installation including SQL Server 2012 Express Edition (Figure 3 below).
   - Server installation (or upgrade) using a previously installed version of SQL Server (Figure 4 on page 8).
   - Client installation (Figure 5 on page 9). **Note:** The use of client computers is not supported in Security Commander Lite.

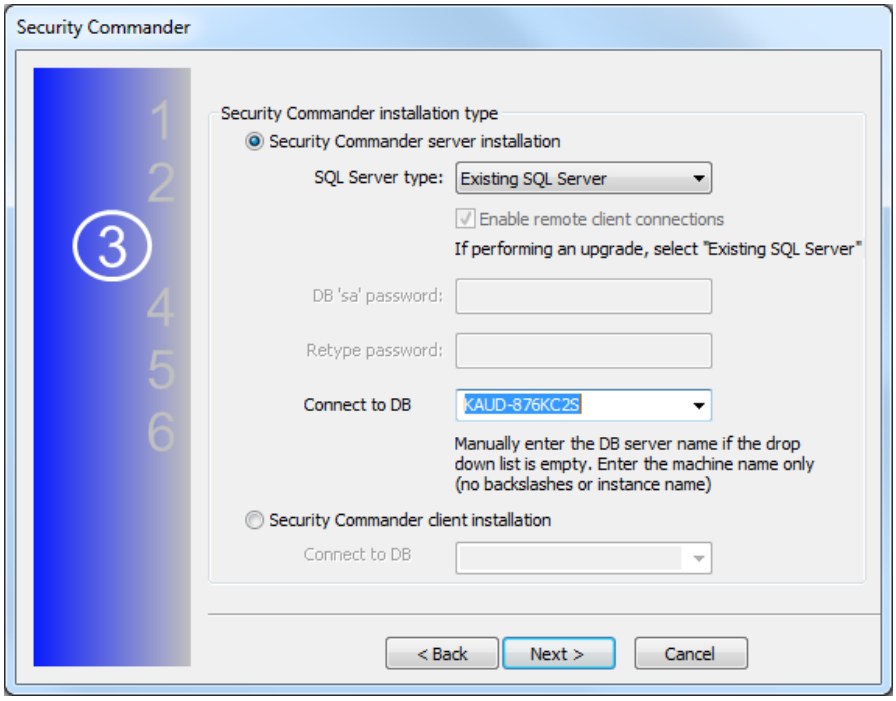
Figure 3: Installation screen 3 (server installation with SQL)



For a server installation using SQL Server 2012 Express Edition:

- Click the “SQL Server type” arrow, and then select “New SQL Server Express” from the list.
- Check the “Enable remote client connections” checkbox to enable remote Security Commander client computers to connect with the server. **Note**: If you do not check the “Enable remote client connections” checkbox, then Security Commander client computers will not be able to connect to the server.
- Type a password for “sa” DB user. **Note**: This password will be required during database operations and must comply with SQL server policy, otherwise the installation may fail. For example, the password may need to contain both letters and numerals, and the letters may need to contain both uppercase and lowercase characters.
- Click Next to continue.

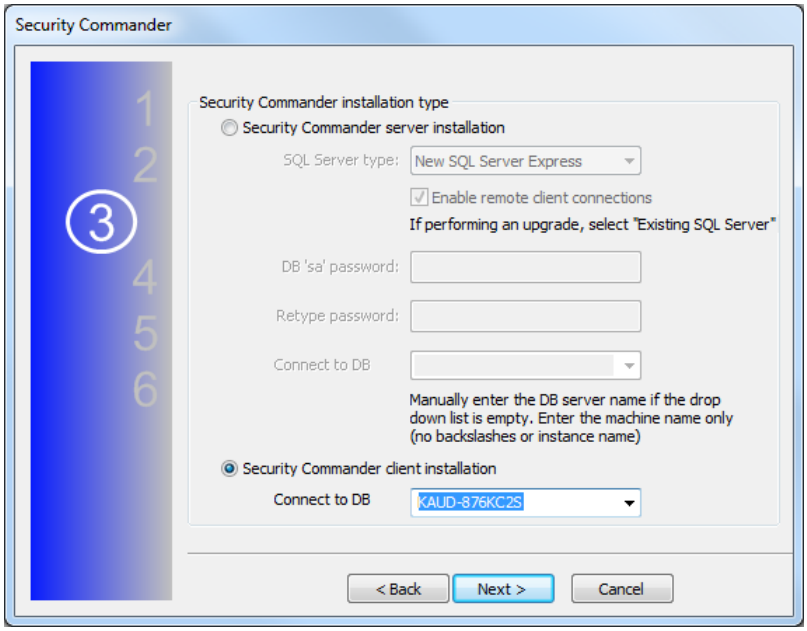
Figure 4: Installation screen 3 (server installation for existing SQL server)



For a server installation (or upgrading) using a previously-installed version of SQL Server:

- Click the “SQL Server type” arrow, and then select “Existing SQL Server” from the list. **Note**: An instance of SQL Server named “SPSQL” must exist prior to installing Security Commander or you cannot proceed with the installation.
- Click the “Connect to DB” arrow, and then select the name of the server from the list. Alternatively, if network servers are not listed, then you can type the server name in the “Connect to DB” field.
- Click Next to continue.

Figure 5: Installation screen 3 (client installation)

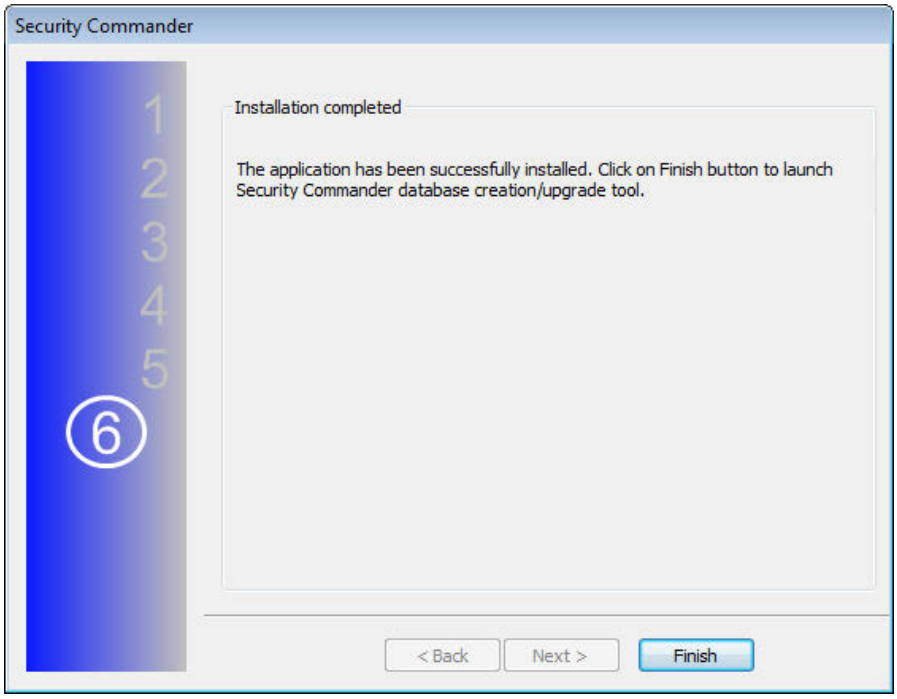


For a client installation:

- Click to populate the “Security commander client installation” radio button.
- Click the “Connect to DB” arrow, and then select the name of the server from the list. Alternatively, if network servers are not listed, then you can type the server name in the “Connect to DB” field.
- Click Next to continue.

4. At installation screen 4 review the installation details. If everything is correct, click Next to continue. Alternatively, click Back to change details on a previous screen.
5. At installation screen 5 details of the installation files are displayed along with a progress bar.
6. Installation screen 6 (Figure 6 on page 10) indicates that the installation completed. Click Finish to continue. If this is a server installation and you have installed the default SQL Server 2012 Express Edition, the Database Tools application runs automatically to create the database.

Figure 6: Server installation screen 6



Check the log file after installation to be sure everything went properly. The log file is (typically) C:\Program Files (x86)\Alliance8300Installation.log.

Note: If any part of the installation fails, then a window automatically displays a list of errors. You can review this list at any time from Alliance8300Installation.log.

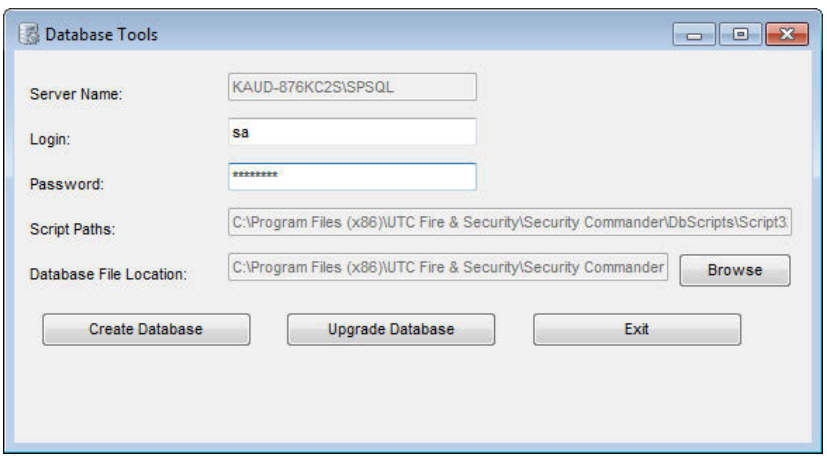
Installation, part 2 (server only)

The following steps describe the additional installation steps required for a Security Commander server computer.

To continue installation of Security Commander:

1. If installing on a server computer, the Database Tools application runs automatically to create or upgrade the database.

Figure 7: Create database (server installation)

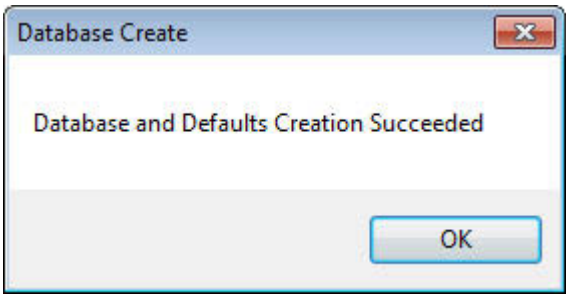


2. Type the database login “sa”, and then type the previously-defined password (the password displays as *****). Click Create Database to continue.

   Note: If you are upgrading Security Commander click the Upgrade Database button or the Exit button.

3. Database Tools creates the databases and defaults. This will take several minutes and progress may appear to stop. Please be patient.
4. Database Tools displays a confirmation message.

Figure 8: Create database confirmation



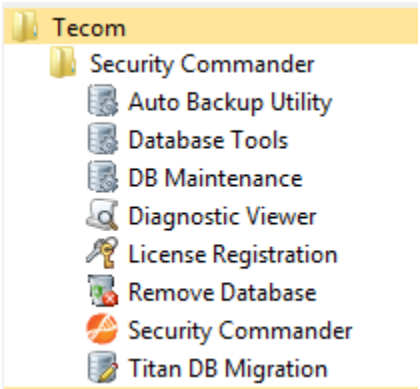
5. Click OK to continue, and then click Exit to close the Database Tools window.

Installation results

After installing Security Commander note the following new items:

- A default Security Commander operator named “secure” with a password “4346”.
- The Security Commander icon appears on your desktop.

- The Security Commander program group appears on your Start menu.



The Security Commander program group contains the following options:

- Auto Backup Utility, to schedule backups of Security Commander databases.
- Database Tools, to create the database for an initial installation or to upgrade a database.

- DB Maintenance, to perform diagnostic operations with the Security Commander database.
- Diagnostic Viewer, to run Diagview (it can also be run from within Security Commander).
- License Registration, to register the installation of Security Commander.
- Remove Database, to delete the Security Commander database.
- Security Commander, to run Security Commander.
- Titan DB Migration, to create Challenger panel data and person records from a Titan database back up file.

Security Commander folders

During installation of the Security Commander and Photo ID software, a number of folders are created. Some of the folders are shared to allow other computers to gain access to the information stored in these folders (as long as they logged in as an authorised user).

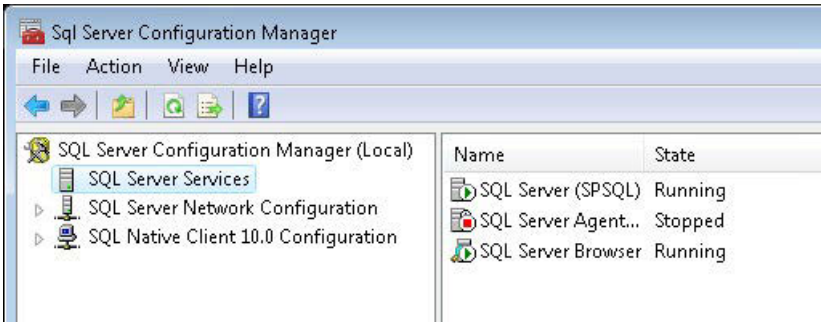
The following is a typical list of Security Commander server folders:

- Badge Designer: Contains the executable file for the Badge Designer program.
- Client: Contains the Photo ID installation program and a Microsoft troubleshooting tool.
- Database: Contains the Alliance database, archive database, and history database files.
- DbScripts: Contains the scripts, utilities, and programs used to create the database.
- Designs: Contains the badge design files used by the Photo ID stations.
- EnglishAU: Localised English language resource files.
- Externals: Contains Security Commander external reports.
- Firmware: Reserved for future use.
- Graphics: Contains the maps and icons used for alarm graphics.
- Images: Contains the captured badge holder pictures.
- Logs: Contains the Security Commander diagnostic log files. For more information on these logs, refer to the *Security Commander Administration Manual and Operation Guide*.
- Manuals: A folder containing the Security Commander manuals in PDF format.
- Reports: Contains report files used by Security Commander.
- Signature: Contains captured signature pictures.

Setting up Microsoft SQL Server 2012 Express Edition

After installation database server and database creation please check if MS SQL Express works properly. You need to run SQL Server Configuration Manager.

Figure 9: SQL Server Configuration Manager



SQL Server (SPSQL) and SQL Server Browser services must be running.

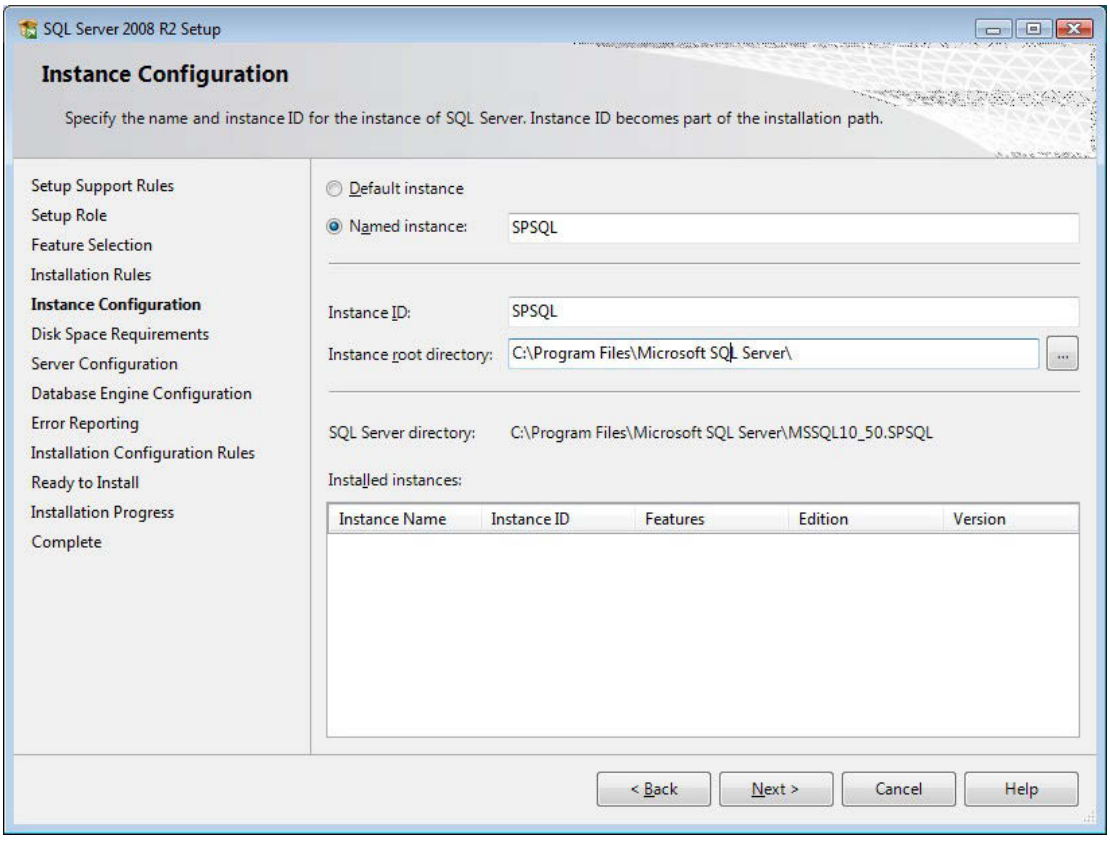
Setting up Microsoft SQL Server 2012 (optional)

As an alternative to Microsoft SQL Server 2012 Express Edition, Security Commander may be used with Microsoft SQL Server 2012.

Before you install Security Commander, you must create an instance of Microsoft SQL Server 2012 named “SPSQL”.

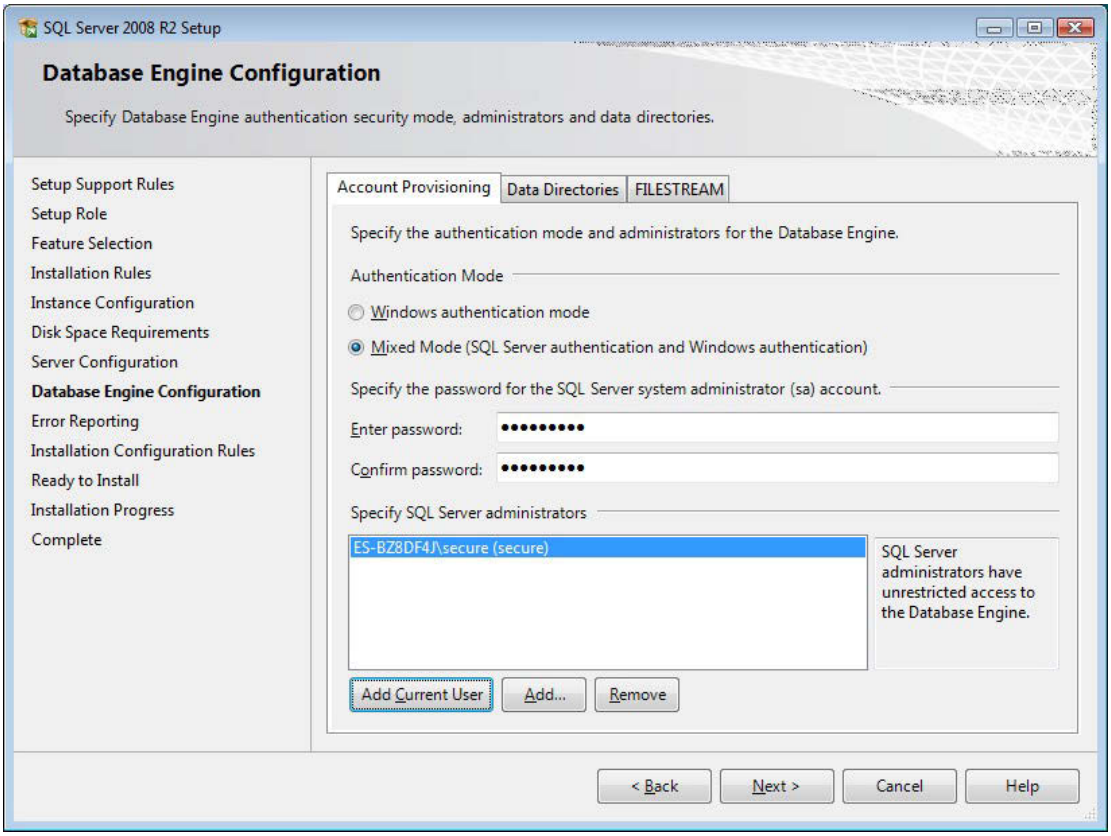
Refer to the figures below for additional details (images are based on SQL Server 2008).

Figure 10: Instance name in SQL Server



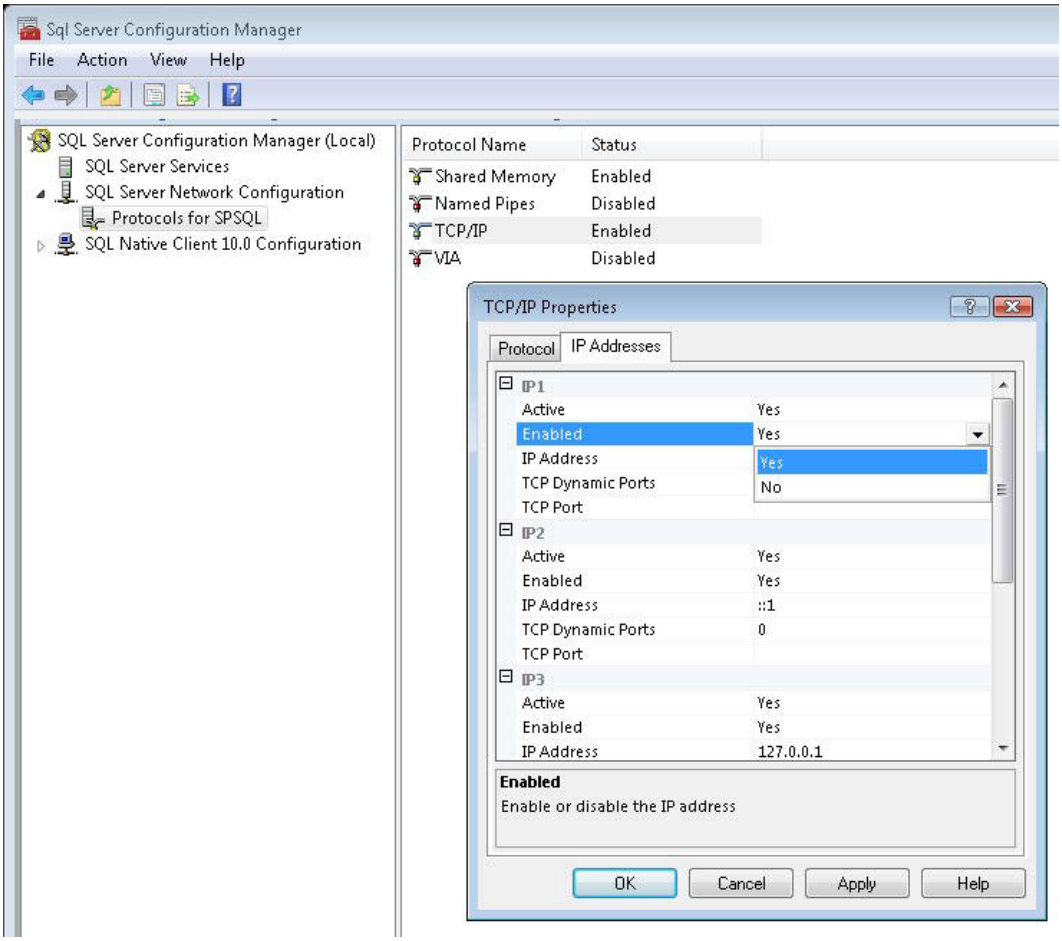
The user named “sa” is created automatically. Select Mixed Mode for authentication.

Figure 11: Authentication mode in SQL Server



Run SQL Server Configuration Manager. Click Start > Programs > Microsoft SQL Server 2012 > Configuration Tools > SQL Server Configuration Manager (Figure 12 on page 15).

Figure 12: SQL Server Configuration Manager



In SQL Server Network Configuration, select Protocols for SPSQL, and then disable the Named Pipes protocol.

Registering the Security Commander server

In order to use Security Commander outside of trial or demonstration modes (see “Trial mode” below and “Demonstration mode” on page 16) register the Security Commander’s 12-character serial number (called a base license) via the Web (www.interlogix.com.au/registerSC). The serial number is printed on the Standard or Professional Edition’s Base Licence card located within the product packaging.

Tip: If you don’t have access to the Web site, then you can register Security Commander by telephone on 1300 361 479.

Trial mode

When initially installed on the server computer (or if the database has been restored), Security Commander can be used in an unregistered state for 14 days. After 14 days, if not registered, Security Commander reverts to demonstration mode.

Demonstration mode

After 14 days, in demonstration mode, the following conditions apply:

- “Demo Mode” is displayed in the title bar
- Photo ID is not available
- Remote connections to client computers are not available
- The session time is limited to one hour
- DVR connection is not available
- 200 person records are available

Additional licence modules, such as Photo ID, can be purchased on separate licence cards. Add these modules’ serial numbers to a registered base licence via the Web in order to obtain an updated activation code to enable the feature. When registered and enabled, a workstation computer can use the license information stored on the server computer.

To check Security Commander’s license details, select Help > About Security Commander.

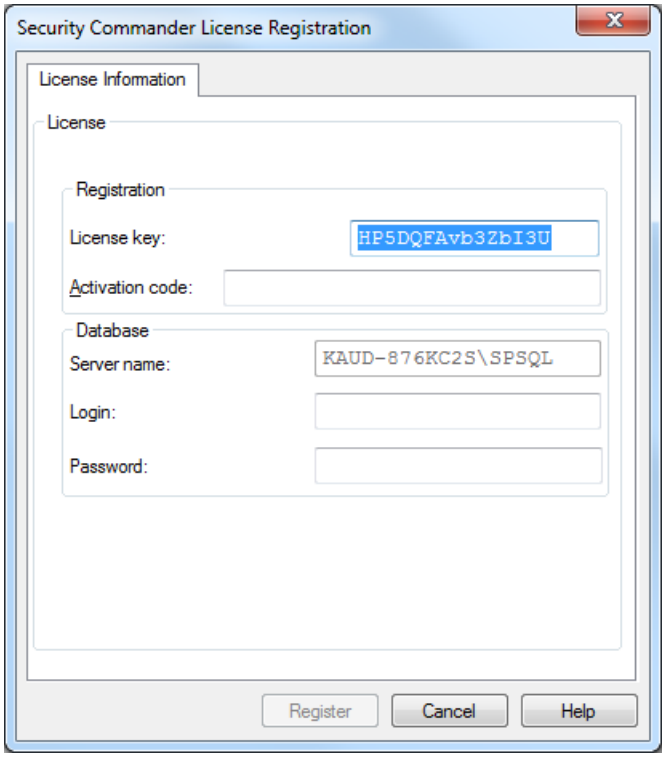
To register Security Commander:

1. Visit the registration Web site at www.interlogix.com.au/registerSC, and then enter the base licence serial number. The serial number is printed on the Standard or Professional Edition’s Base Licence card located within the product packaging.

   Tip: If you don’t have access to the Web site, then you can register Security Commander by telephone on 1300 361 479.

2. Follow the directions on the Web site to register your contact details; being careful to provide the correct e-mail address for the end user (this is necessary for receiving licence information).
3. Enter any additional licence module serial numbers on the configuration options page. The serial number is printed on the module’s licence card.
4. When prompted to provide your licence key, click Start > All Programs > Tecom > Security Commander > License Registration. The Security Commander License Registration screen displays (Figure 13 on page 17).

Figure 13: Security Commander License Registration screen



5. Record the contents of the License Key field.

   Tip: You don't need to keep this screen open until you receive the activation code because the original license key remains valid even if this screen is closed and reopened.

6. Obtain the activation code from the registration Web site (or via telephone to Customer Service on 1300 361 479). The activation code is specific to the server computer's configuration.

   Tip: Record the activation code in case you need to reinstall Security Commander on this computer.

7. Type or paste the code into the Activation code field, and then click Register.
8. Type "sa" as the database login, type the previously-defined password (see page 7), and then click Register.
9. License Registration displays a progress bar showing services being restarted, then displays a message to indicate whether the installation was successful. Click OK.

After a successful installation, you can start Security Commander (no need to restart the computer).

Note: The activation code will work only on the computer that produced the licence key. If Security Commander is installed on a different computer (for example, after a hardware change) the customer will need to contact Customer Service on 1300 361 479 to have the registration applied to the new computer.

Configuring services

Windows computers use special programs called services. A service is a process that can start automatically when the system boots and remains running as a background process independent of anyone being logged in. These services must be running in order for Security Commander server to communicate with Security Commander client computers and with control panels.

All computers running Security Commander software use three services, listed here in the order in which they must be started (if started individually):

- Alliance 8300 Diagnostics controls the diagnostic information log.
- Alliance 8300 System Manager coordinates the communications of data between server and client computers and handles licensing.
- Alliance 8300 Manager controls the communications between Security Commander and Challenger control panels.

Starting one service will automatically start any other service that needs to be running. For example, starting Alliance 8300 Manager will automatically start all three services.

Stopping services manually

You might need to stop the services, for example, to restore a database. If you need to individually stop the Security Commander services, do so in the following order:

1. Alliance 8300 Manager
2. Alliance 8300 System Manager
3. Alliance 8300 Diagnostics

Verifying that services are running

To verify that services are running:

1. Click Start > Control Panel > Administrative Tools.
2. Double-click Component Services.
3. Select Services (Local) in the left-hand panel, and then find the Alliance 8300 services in the right-hand panel.

The status will be either Started or blank. If it is blank, then the service is not running.

Starting Security Commander

To start Security Commander:

1. Select Start > All Programs > Tecom > Security Commander > Security Commander to run the application. Alternatively, double-click the Security Commander desktop icon.

2. The login screen displays automatically when Security Commander starts. Type your operator login ID and password, and then click OK. Alternatively, use the default login ID “secure” with a password “4346”.

Optional server applications

Installing Photo ID

Note: This option is not available in Security Commander Lite.

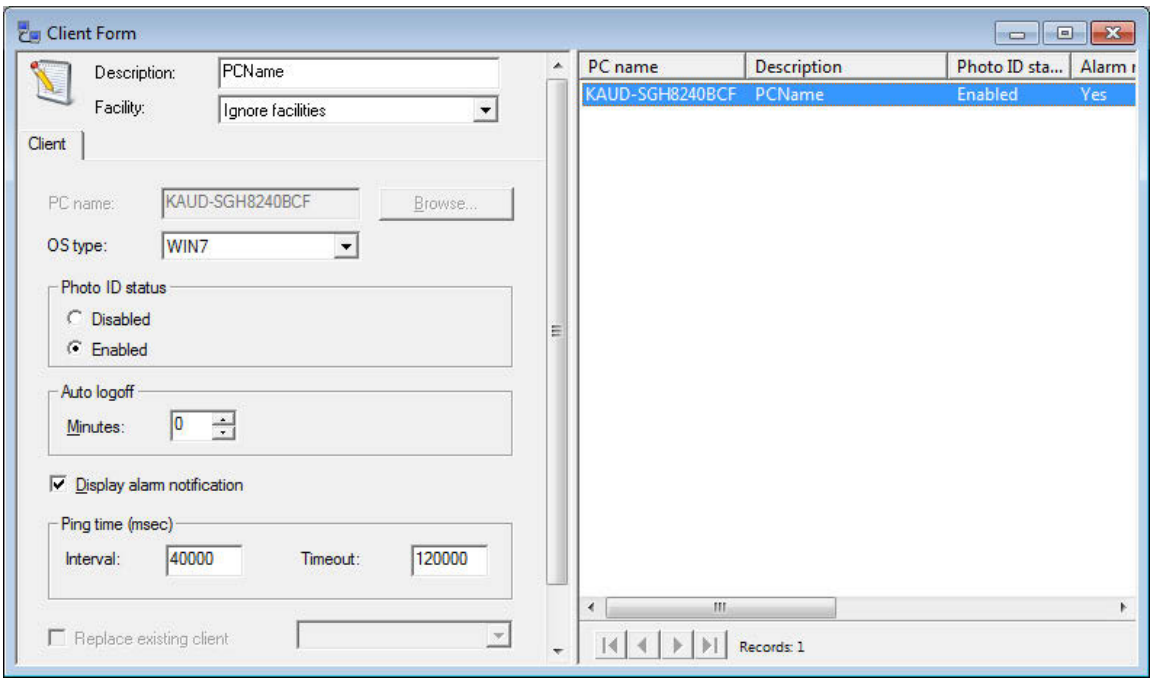
The next step during the installation process is to install Photo ID on the server computer. Photo ID is used on either server or client computers to add images such as photographs and signatures to Security Commander badge designs and person records.

If Photo ID is to be used on any server or client computer it must first be installed on the server computer followed by installation on each client computer that may need to use it.

The required number of Photo ID licenses must be issued via the Security Commander License Registration process prior to using Photo ID (Photo ID licenses are floating and may be enabled and disabled on various Security Commander client computers or the server computer, as required).

After installing Photo ID, use the Client Form on the Security Commander server to set the client’s Photo ID status to Enabled before Photo ID can be used on that computer (see Figure 14 below).

Figure 14: Client Form used to enable Photo ID



Notes

- If Photo ID was previously installed on this computer you must uninstall it before proceeding.

- You must have Security Commander installed and working before you install Photo ID. If you have not installed Security Commander, do so now.

To install Photo ID:

1. Close all applications, and then log on to the computer as Administrator.
2. Click Start > Run > Browse.
3. Select the file C:\Program Files (x86)\UTC Fire & Security\Security Commander\Client\setup.exe.
4. Click Open, click OK, and then follow the on-screen instructions.

Installing API

Note: This option is not available in Security Commander Lite.

API (Application-Program Interface) enables data (such as personnel data contained in external databases) to be imported into the Security Commander system via XML files (appropriately formatted text files with an .XML file extension).

Refer to the *Security Commander API Installation and Operation Manual* for details.

Installing Microsoft Access

Microsoft Access is used optionally for database maintenance and for creating custom reports.

Refer to the *Security Commander Administration Manual and Operation Guide* for details of how to create new projects and to connect your Security Commander database files with Microsoft Access.

Setting up dial-up modems

A Security Commander computer may be connected via modem and PSTN to the Challenger panel's onboard dialler.

Challenger Series panels have onboard modems that support 56 kbps. Challenger V8 panels have onboard modems that support either 300 bps or 2400 bps (depending on the firmware version). You may need to set the Security Commander computer's modem to communicate at the appropriate speed. Refer to the modem's user manual for details about these settings.

Setting up the power options

A Security Commander computer can be a communication server, a database server, and a license server. In each case, the computer's power options must be configured such that the hard disks never turn off and the system does not go into standby or hibernate modes.

Adding Security Commander clients

Note: This section does not apply to Security Commander Lite.

The Security Commander server computer may connect with remote client computers (subject to the Security Commander license). The Security Commander server must be registered (or in trial mode) before adding clients.

Note: Create client records on the Security Commander server before installing the Security Commander software on the client computers. Client computers must be on the network.

To create a client record:

1. On the Security Commander server computer, click Start > All Programs > Tecom > Security Commander > Security Commander.
2. Log in as “secure”, using the default password “4346” (or the subsequently changed password).
3. Select Administration > Client.
4. Select File > New Record.
5. Type the name of the client computer. Alternatively, browse the network, select the client computer, and then click OK.
6. Save the Client form.

Modifying or removing clients

To modify client details or to remove a client from the network, the client must be disconnected. This can be done by having that client log out of Security Commander.

Alternatively, the operator on the server computer can select the client on the Client Monitor Form and use the Disconnect command to disconnect the client from Security Commander (subject to the permissions settings for the operator).

Enabling Photo ID

You can enable or disable the Photo ID application on a client without disconnecting. You may have more Photo ID stations set up than you have licenses. However, if not all the clients require the license at the same time, you can enable and disable the license for the appropriate clients.

Open the client computer’s Client Form. In the Photo ID Status section, select Enabled. Alternatively, select Disabled to disable the license for a client computer (see Figure 14 on page 19).

Completion of server setup

This completes the Security Commander server computer setup. You will now set up the client computers (if applicable). Continue with “Preparing a client computer” on page 22.

Preparing a client computer

Note: This section does not apply to Security Commander Lite.

The procedures for installing Security Commander on a client computer are listed in “Client computer installation tasks” on page 4.

This chapter describes how to prepare a client computer to run Security Commander as a client application, as well as installing the optional Photo ID application.

Note: Create client records on the Security Commander server before installing the Security Commander software on the client computers (see “Adding Security Commander clients” on page 20). Client computers must be on the network.

Minimum requirements

Required hardware

Refer to the *Security Commander Data Sheet* for recommended minimum specifications for a Security Commander client computer.

Note: If using the Digital Video Surveillance option, increasing the processor speed and memory will be required to maintain performance in your specific system.

Required software

See “Supported operating systems” on page 3.

Installing Security Commander on a client

When installing Security Commander on a client computer, always log in as Administrator to the local computer and use the same login name and password for the entire installation process on all computers. Make sure to reboot whenever indicated during the installation process. The instruction to “log in as Administrator” means that you must log in as a user with administrative rights.

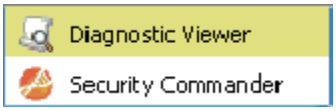
To install Security Commander on a client computer, follow the steps in “Installation, part 1” on page 6, except for the server-only steps (as noted).

Installation results

After installing Security Commander and restarting the computer, note the following new items:

- A default Security Commander operator named “secure” with a password “4346”.
- The Security Commander icon appears on your desktop.

- The Security Commander program group appears on your Start menu.



The Security Commander program group contains the following options:

- Diagnostic Viewer: To run Diagview (it can also be run from within Security Commander).
- Security Commander: To run Security Commander.

Security Commander folders

During installation of the Security Commander and Photo ID software, a number of folders are created. If other languages are installed, other language-specific folders display. Some of the folders are shared to allow other computers to gain access to the information stored in these folders (as long as they logged in as an authorised user).

The following is a typical list of Security Commander client folders:

- Badge Designer: Contains the executable file for the Badge Designer program.
- Client: Contains the Photo ID installation program and a Microsoft troubleshooting tool.
- Designs: Contains the badge design files used by the Photo ID stations.
- EnglishAU: Localised English language resource files.
- Externals: Contains Security Commander external reports.
- Graphics: Contains the maps and icons used for alarm graphics.
- Images: Contains the captured badge holder pictures.
- Logs: Contains the Security Commander diagnostic log files. For more information on these logs, refer to the Security Commander Administrator's Guide.
- Manuals: A folder containing the Security Commander manuals in PDF format.
- Reports: A folder containing report files used by Security Commander.

Configuring services

Windows computers use special programs called services. A service is a process that can start automatically when the system boots and remains running as a background process independently of anyone being logged in. These services must be running in order for connection to the client computers and for Security Commander to communicate with control panels.

See "Configuring services" on page 18 for details.

Starting Security Commander on a client

The procedures and requirements to run Security Commander on a client computer are the same as for the server computer. See “Starting Security Commander” on page 18.

Optional client applications

Installing Photo ID

The next step during the installation process is to install Photo ID on the client computer. Photo ID is used to add images such as photographs and signatures to Security Commander badge designs and person records.

Note: You must have Security Commander installed and working before you proceed. If you have not installed Security Commander, do so now. Before installing Photo ID, verify that the server is running and the client computer can connect to it. The Security Commander server must already have Photo ID installed.

See “Installing Photo ID” on page 19 for details about installing Photo ID.

Installing API

API (Application-Program Interface) enables data (such as personnel data contained in external databases) to be imported into the Security Commander system via XML files (appropriately formatted text files with an .XML file extension).

Refer to the *Security Commander API Installation and Operation Manual* for details.

Shutting down

Logging out of Security Commander

The Security Commander File > Logoff command allows an operator to log out from the Security Commander user interface so that another operator can log in without exiting the program.

During the time when an operator is not logged in to Security Commander, the Security Commander services are still running in the background. However, you will not receive any alarm notifications because these require an operator to be logged in.

Note: If you also want to log out of Windows so that another Windows user can log in, see “Logging out of Windows” below.

Exiting the Security Commander user interface

The Security Commander File > Exit command logs out the currently logged in operator and shuts down the Security Commander user interface.

During the time when the Security Commander user interface is shut down, the Security Commander services are still running in the background. However, you will not receive any alarm notifications because these require an operator to be logged in.

Stopping services

If you need to stop the Security Commander services manually, refer to “Verifying that services are running” on page 18.

Do not stop the Security Commander services when the Security Commander user interface is running.

Logging out of Windows

To log out the current Windows user:

1. Exit Security Commander (see “Exiting the Security Commander user interface” above).
2. Click Start > Shut Down.
3. From the Shut Down Windows form, select Log off nnnn (where nnnn is the Windows user name that you used to log in), and then click OK.

Result: This logs off the current user and allows another user to log on. Keep in mind that the Security Commander services are still running but you will not receive any alarm notifications.

Shutting down

To do a total shutdown of Security Commander and your computer:

1. Exit Security Commander (see “Exiting the Security Commander user interface” on page 25).
2. Click Start > Shut Down.
3. From the Shut Down Windows form, select Shut Down, and then click OK.

Note: You can cause serious damage to your computer if you do not follow the procedure above. In fact, the resulting damage may require that you reload all the software on your computer.

Appendix A. Preparing the operating system

Install your operating system and any specified service packs (see “Supported operating systems” on page 3).

Suggested and required settings

The following items are provided for your guidance only, and may vary depending on the specific operating system:

- The file system type should be NTFS.
- Use the default settings for network services and binding.

Windows user password

When installing and configuring the Windows operating system, the user “Administrator” must be assigned a password. For Security Commander to work correctly, all Windows login IDs used in conjunction with Security Commander must have assigned passwords.

Setting the network properties

It is highly recommended that the Security Commander server and clients are either all on the same domain or all in the same workgroup.

Appendix B. Installing printers

This section provides information about connecting printers to your computer or your network.

You may use either a printer directly connected to your computer or a printer on the network. For example, you may have two Photo ID stations but only one printer.

If you plan on printing either badge or alarm activity, at least one of those printers must be a dot matrix that supports a width of 133 characters either by using a wide carriage or printing in compressed mode.

Note: The printer used for transaction printing must be installed on the Security Commander server computer. All transactions will be printed on that printer. You cannot print badge transactions or alarms transactions from a client printer.

If you plan on printing badges, you must use a UTC-approved Photo ID printer. Currently, UTC supports the DataCard ImageCard Express and the DataCard III printers. For directions on installing printer drivers, refer to the instructions that came with your printer.

To print badges, the default printer must be the Photo ID printer. However, this means that the report preview will not display accurately. You will need to select your report printer before you preview a report.

In Security Commander, click File > Print Setup to select your report printer.

Appendix C. Upgrading or Uninstalling

Upgrading Security Commander

A typical Security Commander upgrade has the following steps:

1. Uninstall the old version (see “Removing Security Commander” on page 30), without checking the “Remove database” and “Remove Crystal Reports” check boxes shown in Figure 15 on page 30)
2. Install the new version (see either “Installing Security Commander on the server” on page 5 or “Installing Security Commander on a client” on page 22, as applicable).

When upgrading Security Commander on the server:

- Use a previously installed version of SQL Server, which is selected as “Existing SQL Server” (Figure 4 on page 8).
- In Database Tools, select either Upgrade Database or Exit (Figure 7 on page 10).

Note: Security Commander is shipped with Microsoft SQL Server 2012 Express Edition, but you do not need to upgrade from an earlier version when upgrading Security Commander.

Uninstalling Security Commander

A complete Security Commander removal has the following steps (some items are optional and may not have been installed):

1. Remove installed patches.
2. Remove Photo ID, if installed. See “Removing Photo ID” below.
3. Remove API (Dir Watcher) application, if installed. Refer to the *Security Commander API Installation and Operation Manual* for details.
4. Remove Security Commander. See “Removing Security Commander” on page 30.
5. Remove SQL. For a server, refer to “Removing SQL” on page 31. For a client, refer to “Removing SQL Server 2012 Native Client” on page 31.

Removing Photo ID

To remove Photo ID:

1. Log in to Windows with administrative privileges.
2. Open the Control Panel and double-click Add/Remove Programs.
3. Select Imaging, and then click Change/Remove.

Removing Security Commander

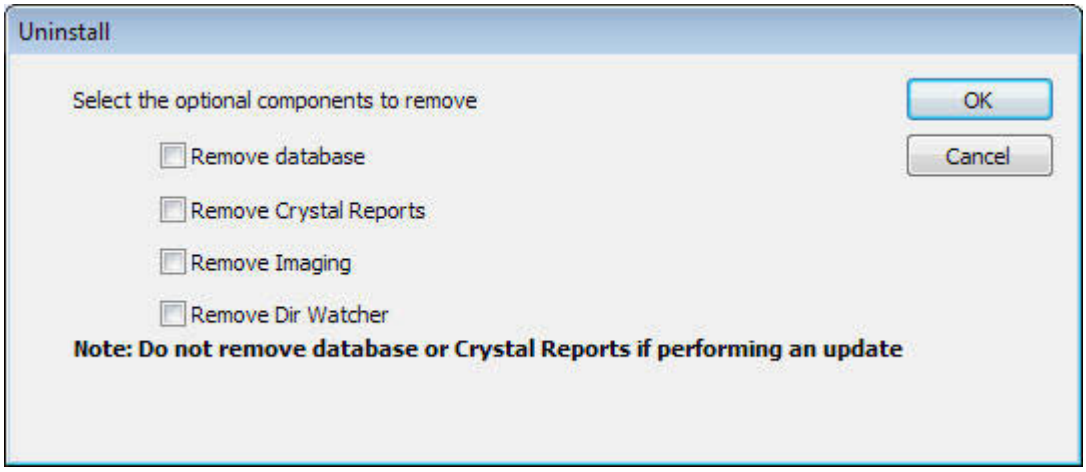
Note: Make a backup of your database before performing this procedure if you want to preserve data.

To remove Security Commander:

1. Log in to Windows with administrative privileges.
2. Exit from the Security Commander user interface and related applications, such as DiagView.
3. Open the Control Panel and double-click Add/Remove Programs.
4. Select Security Commander, and then click Uninstall (Figure 15 below). If performing a full uninstallation, check all of the check boxes.

   Tip: If you are upgrading Security Commander do not check any of the check boxes.

Figure 15: Uninstall options



5. Click OK. Windows will uninstall Security Commander and any selected options.

Removing the Security Commander databases

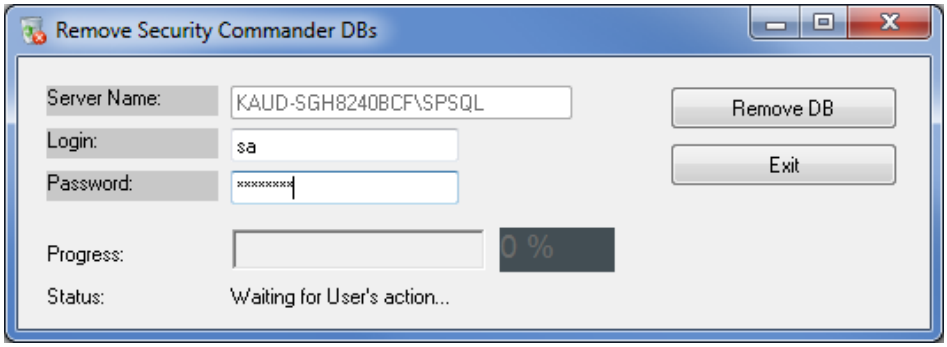
Database removal is optionally performed during the removal of Security Commander. This section describes how to do it separately, if required.

Note: Make a backup of your database before performing this procedure if you want to preserve data.

To delete the Security Commander databases from the server:

1. Click Start > All Programs > Tecom > Security Commander > Remove Database (Figure 16 on page 31).

Figure 16: Remove database



2. Type the password for the user name “sa”.
3. Click Remove DB.

Removing SQL

SQL Server 2012 Express Edition

Microsoft SQL Server 2012 Express Edition is used for the Security Commander server computer. If Security Commander is removed, you can also remove Microsoft SQL Server 2012 Express Edition.

Notes

- If you remove SQL components in preparation for installing Security Commander, then you must restart the computer before installing Security Commander.
- Removing Microsoft SQL Server 2012 Express Edition does not delete Security Commander databases; however, the database files become unusable because the engine to access and control the database will be removed.

To remove Microsoft SQL Server 2012 Express Edition software:

1. Open the Control Panel and double-click Add/Remove Programs.
2. Select Microsoft SQL Server 2012 from the Currently Installed Programs list and click Remove.
3. Select the SPSQL instance, and then click Next.

Removing SQL Server 2012 Native Client

Microsoft SQL Server 2012 Native Client is used for the Security Commander client computers. If Security Commander is removed, you can also remove Microsoft SQL Server 2012 Native Client.

Note: If a Security Commander client computer needs to be used as the Security Commander server, then you must remove Microsoft SQL Server 2012 Native Client before installing Security Commander as a server.

To remove Microsoft SQL Server 2012 Native Client software:

1. Open the Control Panel and double-click Add/Remove Programs.
2. Select Microsoft SQL Server 2012 Native Client from the Currently Installed Programs list and click Remove.

Appendix D. Troubleshooting

Security Commander has diagnostic viewing facilities to assist in troubleshooting.

The use of Diagnostic Viewer is described in the Security Commander Help.

Services

Problem: One or more of the Security Commander services is not running. Start Diagnostic Viewer to see details.

Solution: Ensure the services are set to automatically start and restart the computer.

Licensing

Problem: After registering the license, Security Commander does not recognize the License Key and remains in trial or demonstration mode.

Solution: Restart the computer.

Server and client installations

The general server installation failure may occur when the ‘sa’ password does not comply with SQL Server policy (for example, the password must contain both letters and numerals, and the letters must contain both uppercase and lowercase characters). The installation process is interrupted by SQL Server installation application, therefore this information is not recorded in the Security Commander installation log file, but it can be found in Windows application log.

Problems that may occur with Security Commander client computers include the following:

- If the client computers are remote, make sure you set up the client network properties before setting up the computer systems.
- Failure to add and configure client computers in the Security Commander server database prior to installing Security Commander on client workstations. See “Adding Security Commander clients” on page 20.

Errors may be caused by one or more of the following:

- The server is not running.
- The server is not accessible using the network.
- The database was not created on the server (or is not accessible on another computer).
- The Security Commander software was not licensed on the server.
- Clients are not added and configured in the database on the server.
- The installation instructions were not carried out correctly.

Photo ID

If Photo ID is to be used anywhere on the Security Commander system, the Photo ID application must first be installed on the server computer followed by installation on each client workstation that may need to use Photo ID.

The computer where Photo ID is required has a corresponding Client Form on the Security Commander server, and the Photo ID status must be set to Enabled. A Photo ID license is not used until the status is Enabled.

The number of Photo ID licenses being used (enabled) and the total number of Photo ID licenses is displayed on the Client Monitor Form. The difference between these numbers is the number of licenses available for other Security Commander workstations (for example, if Photo ID licenses = 1 and Photo ID Workstations = 1, then there are no Photo ID licenses available.

Index

S

T

U

W