RISCO
G R O U P

Configuration Software

Installation & User Guide

Visit us on the Web: http://www.riscogroup.com/products/product/95

Contents

Important Notice

This guide is delivered subject to the following conditions and restrictions:

- This guide contains proprietary information belonging to RISCO Group. Such information is supplied solely for the purpose of assisting explicitly and properly authorized users of the system.
- No part of its contents may be used for any other purpose, disclosed to any person or firm, or reproduced by any means, electronic or mechanical, without the express prior written permission of RISCO Group.
- The information contained herein is for the purpose of illustration and reference only.
- Information in this document is subject to change without notice.
- Corporate and individual names and data used in examples herein belong to their respective owners.

Chapter 1: Getting Started

This manual explains how to use the Configuration Software (CS) to configure RISCO systems from your own PC – at the client's premises with a direct link to a laptop computer, or from a remote location with a PC that communicates to the system via PSTN (phone connection using a modem), GSM, GPRS, or IP.

NOTE: Some RISCO systems may not support PSTN communication.

The CS also enables you to:

- Manage your clients and their databases
- Remotely monitor and update the status of every system device in real time.
- View client settings for purposes of customization, backup and upgrade
- Generate RRI reports

NOTE: All sections of this document refer to all the supported RISCO systems (LightSYS, ProSYS Plus, Agility, WiComm), unless otherwise specified.

For more information regarding definitions of (and programming) system parameters, installer operations and user-operations, refer to the relevant RISCO system documentation.

System Requirements

Recommended minimum system requirements:

CPU	P4 3GHz or AMD 3500+
RAM	2 GB Dual DDR 400 or above
Hard Disk	SATA2 with 5 GB free space
Display	PCI Express 256MB
Screen Resolution	1024 x 768
Network	Ethernet port
Operating System	Windows XP,Vista, Windows 7, 8, 8.1

Prerequisites

- Before installing the Configuration Software Program make sure that Microsoft.NET Framework 4 has been installed on the computer.
- Installation must be performed by the Administrator or by a user with Administrator privileges

Installing Configuration Software on your PC

NOTES:

- ProSYS Plus requires version 3.0 or above of the Configuration Software installed.
- For Microsoft Windows Vista users only, the User Account Control (UAC) feature must be turned off. Go to Control Panel > User Accounts > Turn User Account Control on or off. Uncheck the checkbox and click OK.

➢ **To Install the Configuration Software:**

1. Download the CS from the RISCO website:

   http://www.riscogroup.com/products/product/95

2. Double click the **setup.bat** file.
3. Advance to and accept the License agreement, and accept the terms.
4. Click **Finish** to open the Configuration Software setup wizard.
5. Click **Next;** the Select Installation Folder dialog box appears.
6. Browse for a location for the installation folder, or use the default location:
7. Select who can use the program on your computer (**Everyone** or **Just me),** then click **Next;** the Confirmation dialog box appears.
8. Click **Next** to begin installing, and click **Close** when installation is complete.

Initializing the System Database

➤ **To initialize the system database:**

1. Go to **Start → Programs → RISCO Group → Configuration Software → System Organizer.** After entering access credentials (default User Name is **Admin,** Password is **123**), the System Organizer screen appears.
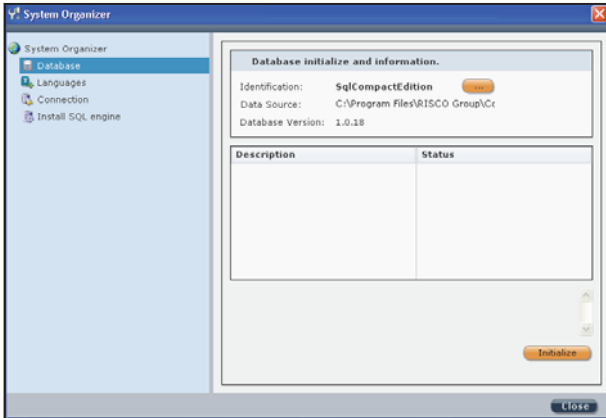
2. For new CS installations, in the left pane you can select **Database** for the Compact Edition (or click [...] to select SQL Express Edition from the resulting dropdown list that appears).

   NOTE: If your system requires support for multiple concurrent connections or enhanced performance, consider usage of SQL Server Express Edition 2005. See *Appendix B: SQL Server Express Edition 2005* Management, page *70* for upgrading existing databases, and for troubleshooting installation issues.

3. Click **Initialize;** the Database Initialize Complete dialog box appears, or if this installation is an upgrade, the Database Initialize Options dialog box appears:
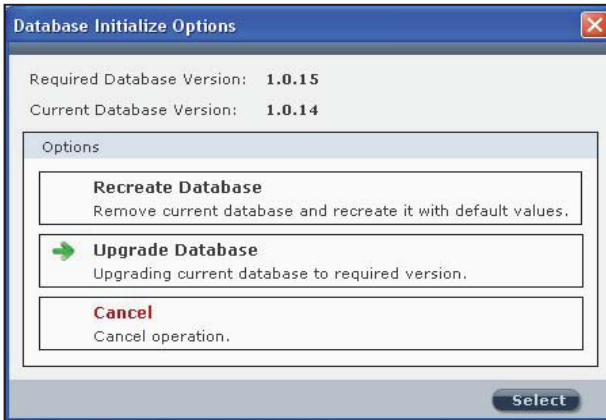
4. Click one of the following options:

   - **Recreate Database**: to remove the current database and recreate it with default values
   - **Upgrade Database**: to upgrade the current database to the required version
   - **Cancel**

5. Click **Select**. When initialization has been successfully completed the status of each action should display as **Succeed:**
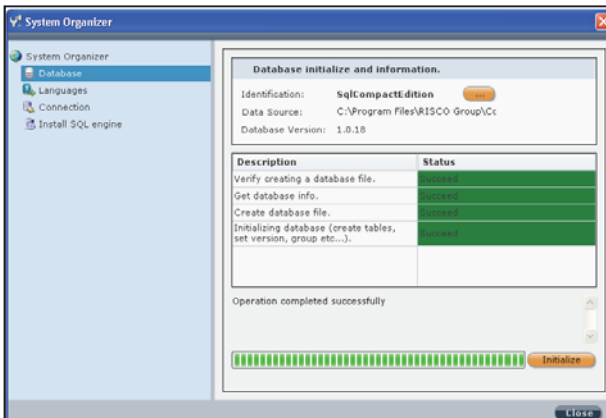
NOTE: For SQL Express edition, if initialization has failed go to:
My Computer → C → Program Files → Microsoft SQL Server → MSSQL.x → MSSQL → Data. Then delete the following files, which contain the Configuration Software's database information (in order to recreate these files they must first be deleted):

- **ConfigurationSoftware_Data**
- **ConfigurationSoftware_Log**

Using the Advanced Database Connection Utility

This feature is used to test the database parameters when database initialization has failed.

➢ **To test the database:**

1. In the System Organizer, in the left pane select **Connection**; the following dialog box appears:
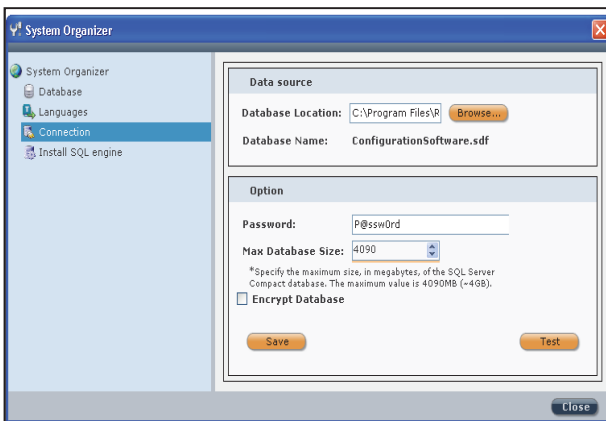
2. From the **Database Location** dropdown list, browse to the location of the desired database.

3. Ensure the default Database Name displayed is: **ConfigurationSoftware.sdf**.

4. Enter the password: **P@ssw0rd**

   NOTE: When testing database parameters prior to initializing the system database, the default user name will be **sa** and the default password will be **Syn0pY.**

5. You can edit the maximum size of the SQL server Compact Edition database (default maximum size is 4090 MB)

6. You can select the **Encrypt Database** checkbox.

7. Click **Test** to check the connection to the database; when a message appears indicating the test was successful, click **Save.**

Setting the Software Language

➢ **To set the software language:**

1. In the System Organizer, select **Languages** from the directory tree; the System Organizer dialog box appears.

2. Select the desired language from the Supported Languages dropdown list, and then click **Set Language**; "language setting will apply changes on next running" displays.

3. Click **OK,** and then click **Close**.

Activating Configuration Software from your Desktop

➢ **Logging in to the Configuration software:**

1. Double-click the CS icon on your desktop; the login dialog box appears.

2. Enter the user name (default is **Admin**) and the password (default is **123**).

3. Click the **Login** button to activate the program. If this is an initial installation, the Client dialog box appears to configure a (new) client (see *Creating a New Client,* page *29*).

   NOTE: If you have more than one client, the Find Client dialog box opens with a list of all the clients to select from.

Debug Window

Configuration Software enables utilization of the (optional) debug window.

➢ **To enable the debug window:**

1. Open the following file for editing:

   C:\Program Files\RISCO Group\Configuration Software\CS.exe.config.

2. Change the value of the DEBUG setting from False to **True.**

3. Display the DEBUG window – right-click on any directory tree node, and then select **DEBUG.**

Chapter 2: CS Main Screen

Main Menu

Tool Bar

Path

Directory (Navigation Tree Map)

Main Screen

Client List

Connection Indication

Elapsed Time

Trouble Indication

Status Indication

Partition Indication
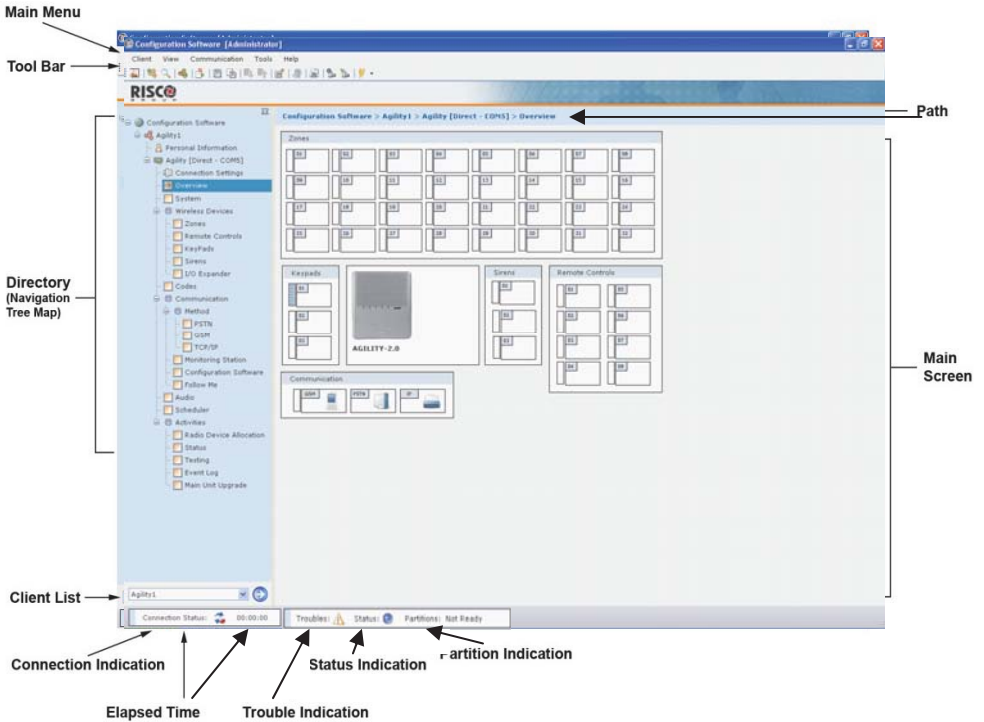
Tool Bar

Tool Bar Icon	Description
/	Open/Close Navigation Tree
	New Client
	Find Client
	Refresh
	View Previous Screen
	Save Client
	Save Current Screen
	Send Current Screen
	Receive Current Screen
	Restore Defaults To Current Screen
	Verify Screen
	Report Screen
	Capture Screen
	Load Screen
	Connect/Disconnect: Direct / GSM/Modem / TCP/IP / GPRS

Directory Tree

The directory tree is a hierarchical list of the client's configurable attributes. It provides for easy navigation between the different screens.
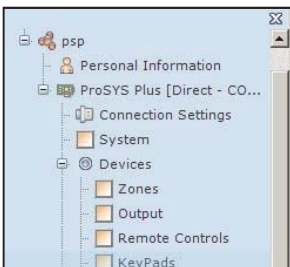
> ➢ **To use the directory tree:**
>
> 1. Click the checkbox for feature you want to configure; the respective screen appears.
>
> 2. Click 🔲 to show the directory tree, or click 🔲 to hide it.

Client Selection Dropdown

The client selection dropdown list provides quick access to all of your clients and enables you to easily navigate between them.
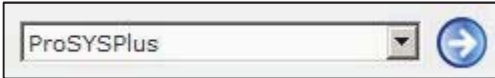
➢ **To navigate between your clients:**

1. Select a client from the drop down list.

2. Press ; a directory tree displays for the selected client.

Connection & Time-Elapsed Indicators

This indicates whether communication between the CS and the main panel has been established. The amount of connectivity time elapsed displays on the right.

- **Red** = no connection
- **Orange** = connecting
- **Green** = connected

Indicators for Troubles, System Status and Partitions

Indicates present troubles found in the system, system status, and partition status.

Connection Options between the Panel to the CS PC

The CS PC and the panel can communicate with each other via TCP/IP, GSM, and PSTN. Note that some RISCO systems may not support PSTN communication.

General Connection Parameters for the Panel

Regardless of the type of communication channel used to communicate from the main panel and the CS PC, configure the panel's general connection parameters:

➢ **To configure general connection parameters for the panel:**

1. Select **Configuration Software** from the directory tree.
2. Configure these parameters in the Security area:
   - **Access Code:** To communicate between the monitoring station and the installation. Code must be the same in the panel and the CS (default is 5678)
   - **Remote ID Code:** Use **0001** for an encrypted connection (**0000 is** for a non-encrypted connection)
   - **MS Lock:** It provides greater proprietary security when viewing and changing Monitoring Station parameters. This 6-digit code should be the same in the panel and the CS.
   - **Call Back:** Relevant for GSM and PSTN, select **Yes** to enable the panel to call the CS (to the telephone number/s that you enter). This provides more security for remote operations using the CS.
   - **Call Back Phone Numbers:** Define up to 3 numbers that the panel can call for CS communication
   - **Outbound GPRS/IP Connection** [For "CS Connect" via keypad]**:** Enter the IP address and port address of the CS PC. If you have an external router connected to the CS PC, then you should enter the IP address of the router. **NOTE:** If you enter the IP address of the external router, ensure that the port forwarding (from the router to the CS PC) is configured correctly.
   - **Controls [LightSYS, ProSYS Plus]:** Select the **User Initialed Call** checkbox in order to enable the installer to use "CS Connect" (via the keypad) – CS should be in the **Wait for Call** state for this.
   - **Controls**: **[Agility, WiComm]:** To enable communication between the main panel and the CS, select from the following: **Enable CS (via GPRS (out), Enable CS via GPRS (Listener mode), Enable CS (via GSM-CSD), Enable CS (via Ethernet (IP), Enable CS via Modem (PSTN).** The CS should be in the **Wait for Call** state for this.

Connecting the CS PC to the Main Panel

Local "Direct" Connection

- **Agility, LightSYS:** USB-to-RS232 (3-pin) cable
- **ProSYS Plus:** USB-to-USB cable
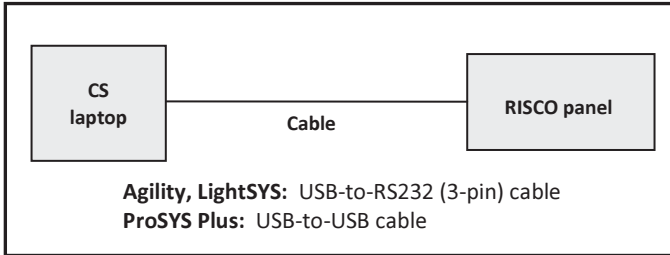
➢ **To establish a Direct connection:**

1. Connect the cable to the USB port on your laptop/PC, and the other end to the connector (USB or RS232, depending on the system) on the main panel.

2. Power up your laptop/PC and activate the Configuration Software.

➢ **To configure Direct connection parameters:**

- Define Direct communication parameters (see page *22*).

Remote PSTN Connection

NOTE: Some RISCO systems may not support PSTN communication.

Agility, LightSYS: connect to main panel via Line & Set screw terminals
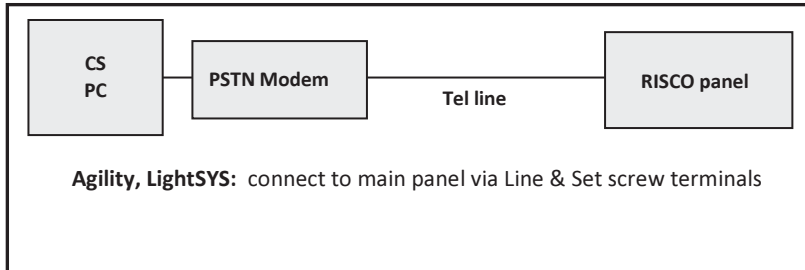
> **To establish a remote PSTN connection:**

1. Connect the modem to your PC and telephone line.
2. Check that you hear a dial tone, and then hang up.
3. Power-up your PC and modem and then activate the Configuration Software.

> **To configure PSTN connection parameters:**

1. Define PSTN communication parameters (see page 22).
2. From **Connection Settings** in the directory tree, you set the pa of the CS PC. In the Modem area, enter the phone number. You can also edit the pause between dialing interval and select the checkbox to enable using an answering machine.
3. Select **Configuration Software** from the directory tree to set the parameters of the panel.

   NOTE: After the CS connects to the panel, the panel will ask the CS for the call back phone number. The panel will only call back the phone numbers defined in the panel.

4. In the **Call Back** area, first enable call back by selecting its checkbox, and then enter from 1 to 3 call back numbers.
5. **[LightSYS]:** In the **Modem Protocol Type** area, select among the PSTN modem options: **V21** (via Hayes-compatible modem), or **Bell** (via MD12 modem).

Remote GSM Connection

NOTE: Remote configuration via GSM requires a GSM/GPRS module installed in the main panel.

> **To establish a remote GSM connection:**

1. Connect the GSM/PSTN modem to your computer. You can use a cellular phone as your computer modem.
2. Power up your PC and activate the Configuration software.

> **To configure GSM connection parameters:**

1. Define GSM communication parameters (see page 22).
2. From **Connection Settings** in the directory tree, you set the parameters of the CS PC. In the GSM area, enter the **CSD** telephone number and **SMS** telephone number.
3. Select **Configuration Software** from the directory tree to set the parameters of the panel.
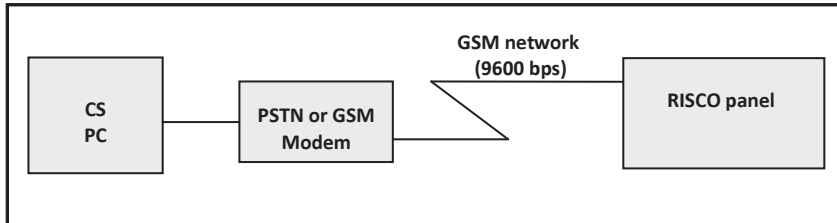
   NOTE: After the CS connects to the panel, the panel will ask the CS for the call back phone number. The panel will only call back the phone numbers defined in the panel.
4. In the **Call Back** area, first enable call back by selecting its checkbox, and then enter from 1 to 3 call back numbers.

Remote TCP/IP Connection

NOTE: Remote configuration via IP requires an IP module installed in the main panel.
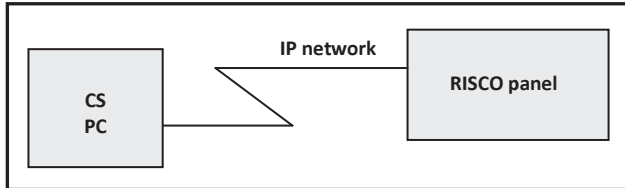
➢ **To establish a remote IP network connection:**

1. Connect the RISCO system to the IP network by plugging an appropriate IP cable plug into the RJ-45 connector on the IP module.

2. Power up your computer and activate the Configuration software.

➢ **To configure TCP/IP connection parameters:**

1. Define TCP/IP communication parameters (see page *22*).

2. From **Connection Settings** in the directory tree, you set the parameters of the CS PC. In the TCP/IP area, the IP address and port number are the same as you may have already entered in the Configuration dialog box for TCP/IP (Communication menu > Configuration > TCP/IP).

3. Select **Configuration Software** from the directory tree to set the parameters of the panel. In the **Outbound GPRS/IP Connection** area, enter the following:

   • **Destination Entry Host IP:** Enter the IP address of the router/gateway of the system

   • **Destination Entry Host Port:** Enter the port on the router/gateway of the system. **NOTE:** This port must be open on the router's firewall.

Remote GPRS Connection

Remote configuration via GPRS requires a GSM/GPRS module installed in the main panel.
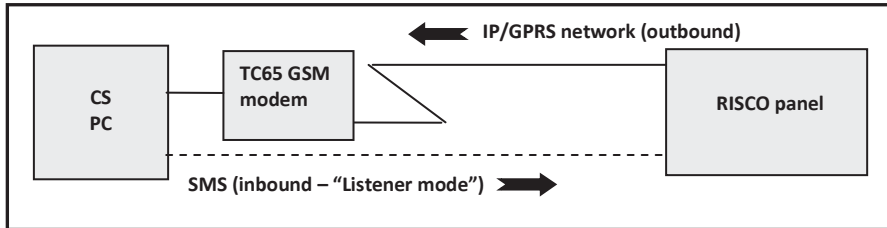
> **To establish a GPRS connection:**

1. Connect your computer to the IP network.

2. Connect the GPRS/GSM Module to the GSM network.

3. Power up your PC and activate the Configuration software.

4. Define GPRS communication parameters (see page xx).

> **To configure GPRS connection parameters:**

1. From **Connection Settings** in the directory tree, in the GSM area, enter the **CSD** telephone number and **SMS** telephone number.

2. Go to **Communication menu > Configuration > GPRS >** select the **target IP address** from the dropdown list, define the **port** (default is 1000) > click **OK.**

3. Go to **Communication menu > Configuration > Wait for Call >** select the **By GSM Module** option > for inbound, select **Using GPRS** > select **Fetch automatically** (default is enabled) > click **OK.**

4. To connect the system panel to your PC, send an SMS message to the GSM/GPRS module in the system panel:

   a. Click the arrow of the Connect ( ) icon, and then select **GPRS** from the popup list.

   b. Click the icon. The following message appears, which is compiled of the installer code, the word GPRS, Entry Host IP, Entry Host Port:

Waiting For Connection...

Send SMS message
'0132GPRS172.16.18.88:1000' to number
'057773333' or initiate from keypad

Send SMS   **Cancel**
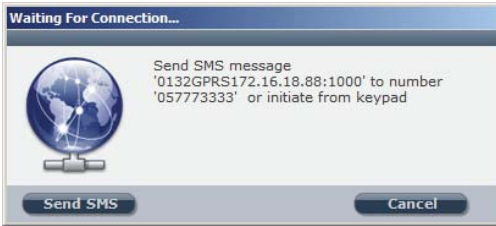
c. Send an SMS by either clicking **Send SMS** to send automatically via a
    TC65 external GSM modem, or send the SMS using a mobile telephone to
    the device's GSM phone number (for example:
    0132GPRS172.16.16.75:1000); the RISCO system will respond to the
    communication request based on the information in the SMS.

Defining Parameters for Communication Options

Define parameters for communication between the CS computer and the panel. Communication can be established either locally or remotely, via these options:

- **Locally:** Direct
- **Remotely:** GSM, PSTN (modem), TCP/IP, GPRS, and Wait for Call.

Direct Communication

➢ **To define direct communication parameters:**

1. From the Communication menu, select **Configuration;** the Configuration dialog box appears.

2. Select the **Direct** communication channel from the drop down list and configure the following parameters as needed:
   - **Port:** Select the relevant port
   - **Baud Rate:** 38400 (Agility and WiComm default), 115200 (LightSYS and ProSYS Plus default)
   - **Data Bits:** 8 (default)
   - **Parity:** None (default)
   - **Stop Bit:** 2 (default)
   - **Handshake:** None (default)
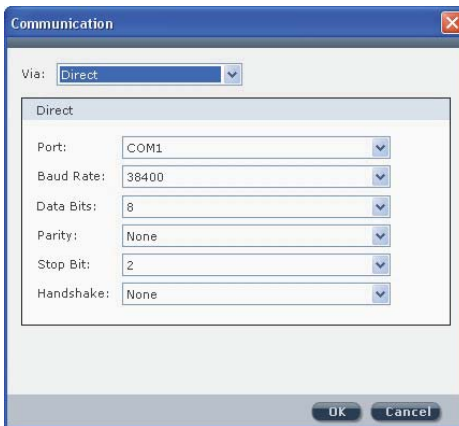
3. In the directory tree, go to **Configuration Software > Security** area, and ensure that the Remote ID Code value is set to **0001** (standard encryption), then click **OK**.

PSTN Communication

NOTE: Some RISCO systems may not support PSTN communication.

➢ **To define PSTN communication parameters:**

1. From the Communication menu, select **Configuration;** the Configuration dialog box appears.

2. Select the **PSTN** (Modem) communication channel from the drop down list and configure the following parameters as needed:
    *   **Port:** Select the relevant port
    *   **Baud Rate:** 2400 (default)
    *   **Data Bits:** 8 (default)
    *   **Parity:** None (default)
    *   **Stop Bit:** 1 (default)
    *   **Handshake:** None (default)
    *   **Modem:** Select the relevant Modem from the Modem dropdown list
    *   **Callback Phone:** Enter the callback telephone number

3. Click **OK.**

GSM Communication

➢ **To define Remote GSM communication parameters:**

1. From the Communication menu, select **Configuration;** the Configuration dialog box appears.

2. Select the **GSM** communication channel from the drop down list and configure the following parameters as needed:

   - **Port:** Select the relevant port
   - **Baud Rate:** 9600 (default)
   - **Data Bits:** 8 (default)
   - **Parity:** None (default)
   - **Stop Bit:** 1 (default)
   - **Handshake:** Set to None (default)
   - **Modem:** select the modem used
   - **Callback Phone:** Enter the callback telephone number

3. Click **OK**.

TCP/IP Communication

➢ **To define TCP/IP communication parameters:**

1. From the Communication menu, select **Configuration;** the Configuration dialog box appears.

2. Select the **TCP/IP** communication channel from the drop down list and configure the following parameters as needed:
   - **IP Address:** The PC's IP address displays by default. In case of two network interface cards, select the relevant IP address from the drop-down list
   - **Port:** Select the relevant port

   NOTE: If there is no port forwarding, then the IP address and port values in these fields should be the same as what appears in the Wait for Call window.

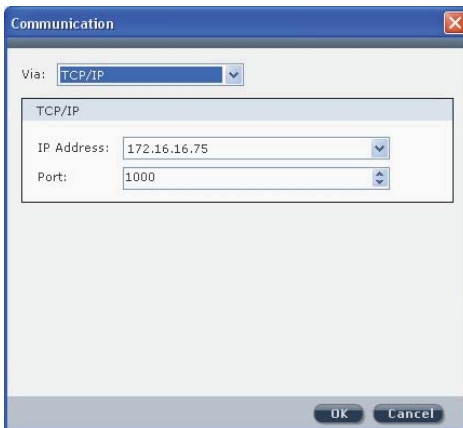| Communication		✕
Via: TCP/IP ▼		
TCP/IP		
IP Address: 172.16.16.75 ▼		
Port: 1000 ▲▼		
	OK	Cancel

3. Click **OK**.

GPRS Communication

➢ **To define GPRS parameters:**

1. From the Communication menu, select **Configuration;** the Configuration dialog box appears.

2. Select the **GPRS** communication channel from the drop down list and configure the following parameters as needed:

   - **IP Address:** The PC's IP address displays by default. In the case of two network interface cards select the relevant IP address from the drop down list.
   - **Port:** Select the port on your PC that the router will forward the RISCO system data to.

   NOTE: This port must be open on the local PC's firewall.

   NOTE: If there is no port forwarding, then the IP address and port values in these fields should be the same as what appears in the Wait for Call window.
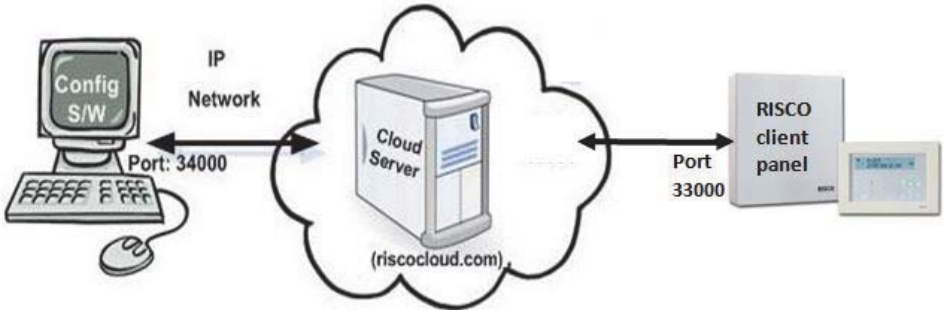

3. Click **OK**.

Cloud Connections

RISCO Cloud connectivity enables doing the following from a remote location:

- Modifying an installation's configuration
- Obtaining status information
- Issuing main panel commands

Enabling Cloud Communication

➢ **To enable cloud communication:**

- **[Agility, WiComm]:** In the directory tree select **System > Basic tab**, and in the Communication Controls area, select **Cloud Enable**
- **[LightSYS, ProSYS Plus]:** In the directory tree select **System,** and in the Communication Controls tab, select **Cloud Enable**

Establishing IP Network Communication from the CS PC to the Cloud Server

➢ **To establish IP network communication from the CS host PC to the RISCO Cloud server:**

In the directory tree select **Connection Settings,** and in the **Cloud** area configure the following:
- **IP Address (domain): riscocloud.com** (IP domain of the RISCO cloud server)
- **Port: 34000**
- **CPID:** Enter the 11-digit control panel ID number (per the sticker on the panel) without spaces or dashes

Establishing Communication between a Client Panel and the Cloud Server

➢ **To establish communication between a client panel and the Cloud server:**

In the directory tree select **Cloud,** and then configure the following::

- **Channel**: From the dropdown list, select the primary communication channel as either **IP Ethernet only** or **IP GPRS only.**
- **IP Address (domain): www.riscocloud.com**
- **IP Port:** Specify the port as **33000**
- **Password:** RISCO Cloud default is **AAAAAA.** If using another Cloud, enter a password comprised of up to 16 alphanumeric characters.
- **Backup area:** For both monitoring station (MS) and Follow-Me destinations (FM), you can select their respective checkbox(s) to utilize both primary and backup communication channels simultaneously for sending events.
- **Controls area:** Select the respective checkboxes to enable arming and/or disarming from the iRISCO Smartphone and Web user apps.

Chapter 3: Main Menus

Client Menu

Creating a New Client

➢ **To create a new client:**

1. From the main menu, select **Client >New** or click the 🔧 icon in the tool bar; the Client dialog box appears:

2. Select the RISCO system from the dropdown.

3. From the **Personal Information tab,** it is mandatory to enter a name in the Name field. Then select the relevant customer ID from the **Customer** drop down list.

NOTE: If the selected Customer ID settings differ from that of the panel to which it connects, a message will display to inform you

4. Enter the **Time Details** information, and then click **OK.**

5. Make sure the **Load Client After Create** checkbox is selected in order to load the new client after you finish creating it.

6. From the **Connection Settings** tab (or if the system is using the Cloud, instead click on **Connection Settings** from the directory tree), now configure the communication mode parameters for connecting the CS PC to the client's system panel.

    NOTE: If, for example, the client can connect via GSM and TCP/IP, choose either one of those two options to connect to that client.

7. Enter the relevant information according to your selection. For **GSM** or **Modem** selection enter the Customer phone number. For **TCP/IP** selection enter the IP address and port. For connection via the Cloud, enter **IP address, port** (default is **34000**), and the CPDI (the control panel's 11-digit ID).

   NOTE: You must define the port in the communication configuration **before** selecting it here (see page 37).

8. Click **OK**; the new client will appear in the client dropdown list:

   ProSYSPlus

Find Client

1. From the Client menu select **Find Client,** or click 🔍 **;** the Client Selection dialog box appears.

2. Click the relevant client from the list, and then click **Select**.

Refresh

• From the Client menu select **refresh** or click 🔄 to refresh screen data.

Close

• From the main menu, select **Client > close** to exit the current client.

Remove

• From the Client menu select **Remove**, then select from the list client(s) to remove from the CA database, and then click **Remove.**

View Previous Screen

• From the Client menu select **View Previous Screen,** or click 📄 to return to the previous screen.

Save Current Screen

• From Client menu select **Save Current Screen** or click 💾 to save current screen.

Save

- From the Client menu select **Save,** or click 🖫 . If "Not validated" appears, the client information cannot be saved due to screen(s) that are incomplete –for example, if there are fields indicated in red (mandatory) that are not filled in.

Save as…

- From the Client menu select **Save as….**

Backup

- From the Client menu select **Backup > Export** to export a client's information (for example, to backup files).
- From Client menu, select **Backup > Import** to import previously saved client files.

Logout

- From the Client menu select **Logout** to log out of the CS.

Exit

- From the Client menu select **Exit** to exit the CS.

View Menu

- From the View menu select **Explorer Tree** or click 🔙 to open/close the directory tree.

Communication Menu

Send

When online, you can send the settings (a specific screen's settings, or settings from all screens) from the CS to the connected RISCO system.

➢ **To send data from a currently displayed screen to the RISCO system:**

- From the Communication menu select **Send > Screen,** or click 🔃 .

➢ **To send data from all the screens to the RISCO system:**

- From the Communication menu select **Send > All.**

> **To send data from specific, multiple screens to the RISCO system:**

1. From the Communication menu select **Send > Selection**; the Screens Selection dialog box appears.

2. Check the relevant screens, and then click **OK**.
   -OR-

   Right-click from within the tabular data cell, and then click **Send.**

Receive

When online, you can transmit information from the RISCO system to the CS.

> **To receive data for the currently displayed screen from the RISCO system:**

- From the Communication menu select **Receive > Screen**, or click .

> **To receive data for all screens from the RISCO system:**
- From the Communication menu select **Receive > All**.

> **To receive data for specific, multiple screens from the RISCO system:**

1. From the Communication menu select **Receive > Selection**; the Screens Selection dialog box appears.

2. Check the relevant screens, and then click **OK**.

   -OR-

   Right-click from within the table and then click **Set All List** to select categories to receive data, or select **Get All List** to view data from the selected categories.

Screen	Progress
Remote Controls	Done
KeyPads	Done
Sirens	Done
Proximity Key Reader	Acquiring...
Power Supply	Acquiring...
Codes	Done
PSTN	Done
GSM	Done
TCP/IP	Done
LRT	Done
Monitoring Station	Done
Configuration Software	Done
Follow Me	Done
Audio	Done
Scheduler	

Receiving...

Elapsed Time: 00:20:07

Cancel

Receiving...

Screen Name: **Status**

Elapsed Time: 00:16:26

Cancel

CS Restore Defaults

Used for restoring factory defaults.

➢ **To restore default values for the current screen:**

- From the Communication menu select **Restore Defaults > Screen,** or click 🖋 .

➢ **To restore default values for all screens:**

- From the Communication menu select **Restore Defaults > All.**

➢ **To restore default values to specific, multiple screens simultaneously:**

1. From the Communication menu select **Restore Defaults > Selection**.
2. Select the checkbox(s) for the relevant screens, and then click **OK**.

Verify

➢ **To verify if CS data is identical to the data in the RISCO system:**

1. When online, from the Communication menu select **Verify,** and then select the relevant option:
   - **Screen:** Verifies the current screen
   - **All:** Verifies all the screens
   - **Selection:** Verifies selected screens. From the dialog box, check the relevant checkboxes, and then click **OK.**
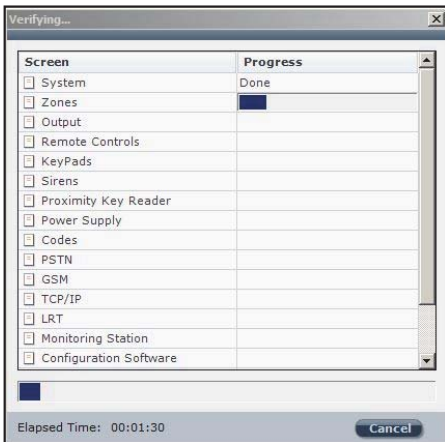
2. When verification is complete the Compare Verify Viewer dialog box displays all inconsistent parameters as well as any differences found between the CS values, the RISCO system values, and the default values:

3. To accept a value, right-click the relevant line, then select one of the following:

    -   Leave Screen Values
    -   Apply Device Changes (RISCO system values)
    -   Restore Default Changes

NOTES:

-   To accept all changes made to the client, right-click the client name.
-   To accept all changes under a specific branch, right-click the relevant branch. For example, to accept the changes made to the Quick Arm and Allow Bypass parameters (see figure above), right-click Controls.
-   The Compare Verify Viewer dialog box closes as soon as there are no inconsistencies left.

Exporting Verification Results

➢ **To export a report of results:**

1. After verification is complete, right-click to select the type of file to save the report as: **HTML, Text** or **CSV.**

2. To export the file click **Export**.

Connect / Disconnect

From the Communication menu, select **Connect** or **Disconnect,** or click .
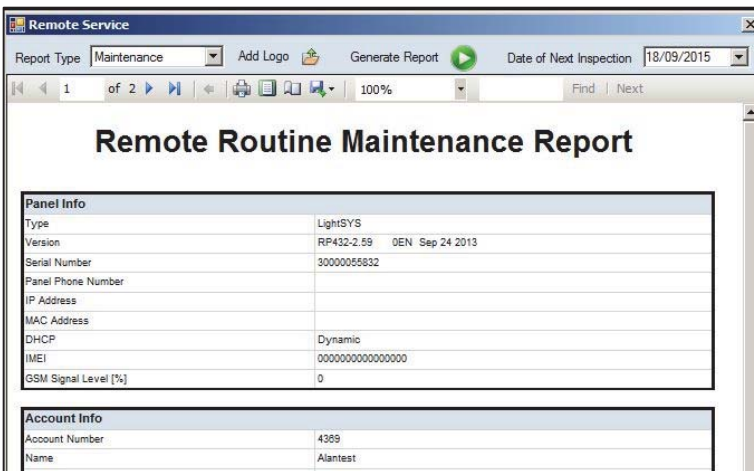
Configuration

See *Defining Parameters for Communication Options,* page *22.*

Tools Menu

Remote Routine Inspection (RRI) Service

Use this tool to schedule, generate, print, and export **Remote Routine Maintenance** reports and **Remote Routine Exception** reports.

> ➤ **To use the RRI feature:**

1. First select a report type – **Maintenance** or **Exception** (lists values that are outside of the acceptable parameters)

2. Click **Generate** to generate a system-level report. The following displays:

   - **[Maintenance report]:** Panel info, Account info, Inspection, System Power, System State, System Panel, Last Partition Set and Unset, Last Zone Activation, Wireless Batteries Status, RSI (Wireless Zone Signal). Use the scroll arrows to scroll between the pages.

   - **[Exception report]:** Maintenance report]: Panel info, Account info, Inspection, System Power, Devices

3. You can customize the report by adding a company logo – click **Add Logo** to browse for the logo image; the report will print with the logo automatically inserted. To delete the logo from the report, click **Remove Logo**.

4. You can click the **Page Setup** icon to edit the report page parameters, and click the **Print Layout** icon to view a "print preview."

5. You can export the report file – click **Export,** then browse for the location to export it to.

6. To schedule a date for a future report to be generated, click the **Date of Next Inspection** dropdown arrow**,** and select a date.

Authorization

Each person authorized to use the Configuration Software should be registered and assigned a password. When the Configuration Software is activated the first time, use the default password to use is 123. Access to the users list can be denied to all users except for the default user (administrator) who is listed first in the user list. It is highly recommended to change the default password to one that is confidential, and also establish passwords for all users.

> **To add a new CS user:**

1. From the main menu select **Tools > Authorization**; the Authorization dialog box appears.
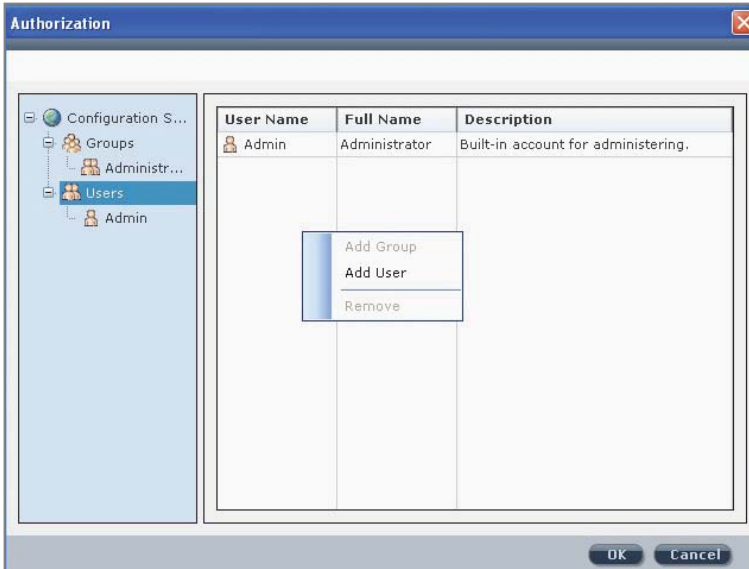
1. To add a new authorized user, select **Users**, right-click it, and then select **Add User;** the New User dialog box appears.

2. Enter the relevant information and click **OK**.

> **To remove a user:**

• Select a user to remove from the list, right-click it, and then select **Remove.**

> **To add a new group:**

1. Select **Groups** from the Authorization directory, right click it, and then select **Add Group;** the New Group dialog box appears:

2. Enter a name and description for this group, and then click the **Access Rights** to define user rights for this group; the Access Rights dialog box appears:
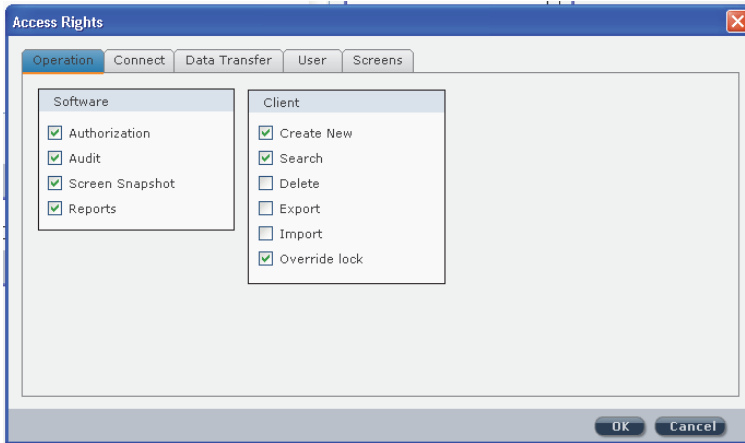
3. Define this group's user rights according to the parameters in each of the 5 tabs: **Operation, Connect, Data Transfer, User** and **Screens**.

4. Click **OK** to return to the New Group dialog box.

5. Click **OK** to return to the Authorization dialog box; the new group appears in the list.

Report

➢ **To generate and print reports:**

1. To generate reports, go to **Tools** > **Reports** and select **Screen**, **All**, or **Selection**; the Report Viewer screen appears:

2. To print the report, click **Print.**

Screen

If technical support is needed it is possible to send an image of a particular screen to the customer support team.

➢ **To capture a screen:**

• From main menu select **Tools > Screen > Capture**, or from the tool bar click .

➢ **To load a screen for the customer support team:**

• From the main menu select **Tools > Screen > Load**, or from the tool bar click .

Audit

The Audit feature stores a list of user actions.

➢ **To execute an audit trail:**

1. From the main menu select **Tools > Audit**, the Audit Trail dialog box appears:
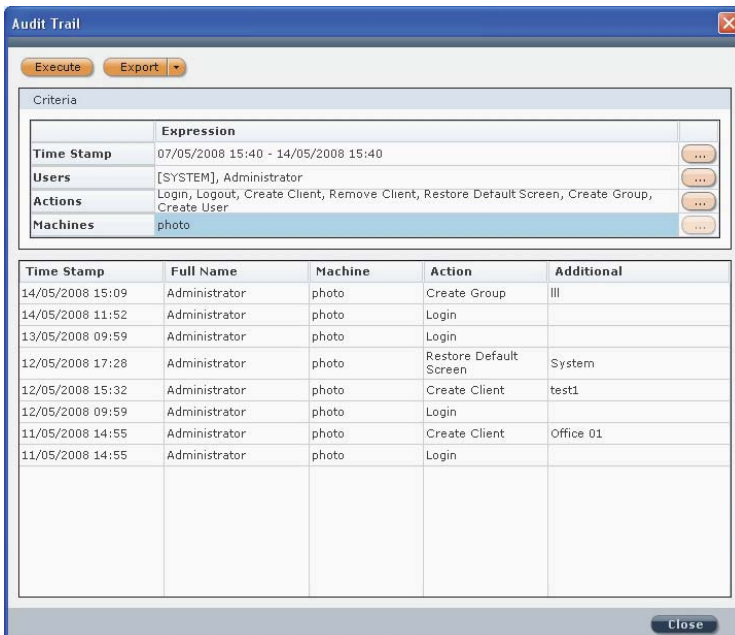
2. Click 〔...〕 to filter the audit trail according to time span, users, actions and machines, and then click **OK** after each selection.

3. To execute an audit trail, click **Execute.**

4. To export the results, right-click 〔▾〕 and save the file as **HTML, text,** or **CSV**.

5. To export the file, click **Export.**

Help Menu

About

View information about the installed CS version.

Chapter 4: Connection Settings

See *Creating a New Client*, page *29*.

Chapter 5: System Overview

[Agility, WiComm]: The **Overview** feature provides an overview of the client's system. The screen displays the following:

- All the accessories (zones, remote controls, keypads, sirens, I/O modules) connected to the client's system and their diagnostics. To view the diagnostic information, stand above the relevant icon, a pop-up box appears with information such as the accessory's name, serial number and assigned partition number.

- The connection types available to the client's system in the communication section.

- The ▤ icon displays the RSSI signal intensity level.

NOTE: This screen does not display any status information. For status information, see the *Status* screen on page *63*.
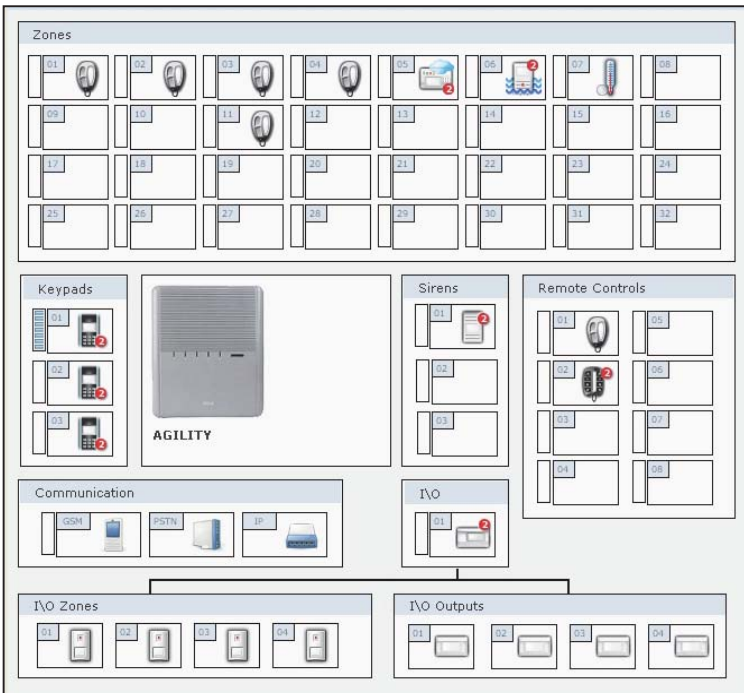
Chapter 6: System Configuration

You can send a configuration to a client, receive a configuration at the CS PC from a client system, and also restore default values for parameters.

➢ **To send a configuration to the client system:**

• Right-click inside a field that is configured, and then select **Send;** the setting is sent to the client system.

➢ **To receive configuration data from the client system:**

• Right-click inside a field, and then select **Receive;** the field is populated with data per the client system.

➢ **To restore default values:**

• Right click inside a field, and then select **Restore Defaults;** the field is populated with the default setting.

System

From all tabs in the **System** screen, various system parameters can be configured. Of the following features, the ones available differ slightly per RISCO system:

• **Timers:** Enter the preferred value (and select seconds or minutes from the dropdown). To display the value range tool tip, hover the cursor above the relevant parameter's dropdown list.

• **Wireless:** Set the jamming time and RX supervision time for wireless

• **Controls/Basic Controls:** Check the preferred checkboxes for Basic Controls. For additional Agility and WiComm configuration options, click Advanced Controls.

• **Communication Controls:** Select whether to enable monitoring station, Configuration Software, Follow Me destinations, and Cloud communication.

• **Automatic Clock Synchronization:** As needed, edit the host IP address, NTP server port, time zone (GMT), and protocol for automatic time update (NTP or Daytime)

• **Sounds:** Set the system sound options.

• **Main Speaker Volume:** Set the main panel speaker volume.

- **Language Settings:** Set the text language.
- **Labels:** Set the system labels for partitions.
- **Pictures Destination:** Set the primary and backup communication channel, host address, port, user name and password
- **Settings:** Set parameters for system settings.
- **Service Information:** Edit the information as needed.
- Firmware Update/Main Unit Software Upgrade: Edit the firmware upgrade information.
- **Main Unit:** Set parameters for various system settings, such as end-of-line termination resistance values, language and voice options, system firmware upgrade information, and service information.

Zones (Wireless, Bus, and Relay)

Wireless, bus, and wired relay zones can be configured via the Configuration software in the following screens (not all of the following screens are available for each RISCO system):

NOTE: Right-click inside a field to display additional parameters that you may need to configure.

- **Label:** the zone description, or label. Click to edit it.
- **Channel:** displays the system device's ID information (zone type, bus line, physical installer-set ID of the expansion module, and the index number of the device on the expansion module).
- **Type:** the zone type
- **Sound / Sound at Arm:** sound options for arming
- **Termination:** end-of-line termination resistance options (for wired non-bus zones only)
- **Group:** group options
- **Partition:** partition options
- **[Agility, WiComm]:** Sequential Confirmation screen, Zone Crossing screen, Soak Test screen, and Serial Code screen (Serial Code is read-only, to add a device to the system go to the Radio Device Allocation screen while online)

Output

[LightSYS, ProSYS Plus]: Configure the following output parameters (see the system's installation manual for more details):

NOTE: Right-click inside a field to display additional parameters for configuration.

- **Label:** the output description, or label. Click to edit it.
- **Pattern:** from the dropdown select Pulse Normally Closed, Latch Normally Closed, Pulse Normally Open, Latch Normally Open
- **Pulse:** the pulse time
- **Type:** output type
- **Follow Event:** activates output upon this event

Remote Controls

In the **Controls** area, you can enable **Instant Arm** (instant full arming), **Instant Stay** (instant partial arming), and **Disarm Using Code** (disarming with code).

In the **Parameters** area, for each keyfob number in use, configure the following parameters (may differ per RISCO system):

NOTE: Right-click inside a field to display additional, configurable parameters.

- **Label /Belongs To:** the user's description, or label
- **Partition /User Partition:** the partition(s) the user can operate
- **Serial Code/Serial Number:** the device's 11-digit serial number (for allocation)
- **Parent Control [Agility, WiComm]:** to enable parent control (when keypad/remote control is activated, it sends a message to the Follow Me destination – for tracking when children arrive at home, for example.

Keypads

NOTE: Right-click inside a field to display additional parameters that you may need to configure.

[LightSYS, ProSYS Plus]: In the **Controls** area, select the **RF Wake Up** checkbox to enable the system to wake up the 2-way keypad up during exit/entry times or when failing to set the system. In the **Keypads** area, specify the keypad number(s) in the system, their labels, the corresponding types, and the assigned partitions and masking. In the **Macro Keys** area, define macro strings for keypads.

[Agility, WiComm]: In the **Keypads** area, specify the keypad number(s) in the system, the serial code (11-digit code for allocation), the keys to be used for emergency, and the function keys (for specifying the type of emergency – panic, or listen & talk). In the **Macro Keys** area, for the relevant keypad number(s), specify which key to use to activate the macro ("Assigned To"), the macro labels, and the macro strings.

Sirens

NOTE: Right-click inside a field to display additional parameters that you may need to configure.

[LightSYS, ProSYS Plus]: In the **Sounders area,** for each siren number in use, specify the label, type, audible, squawk, squawk strobe, and partitions. In the **Scheduler area,** specify up to 2 start and stop times for the LUM8 and SIRN2 sirens.

[Agility, WiComm]: For each siren number in use, specify the label, serial code (for allocation), partition(s), type, supervision, alarm volume, and squawk volume.

Proximity Key Reader

[LightSYS, ProSYS Plus]: For each power supply expansion module in use, specify a label, type, bell/LS, and partition(s).

I/O Expander

[Agility, WiComm]: In the **Controls** area, select checkboxes to enable Quick output operation, I/O expander supervision. In the **Common Parameter** area, enter the I/O expander's 11-digit serial code (for allocation).

In the **Zones** tab, for each I/O expander used specify label, partitions, type, sound.

In the **Outputs** tab, specify the parameters in the **Output Parameters** area, the **X-10 Outputs Parameters** area, and press **DTMF** to assign output via DTMF.

DTMF Control

DTMF Digit No.	Assign Output
1	Output 01
2	Output 02
3	Output 03
4	Output 04
5	X10: Output 01
6	X10: Output 02
7	X10: Output 03
8	X10: Output 04

OK   Cancel

Power Supply

[LightSYS, ProSYS Plus]: For each Proximity key reader in use, specify a label, type, partition(s), Configure the parameters for the Power Supply: **label, type, Bell/LS, Partition.**

Chapter 7: Codes

Configure the codes for all system users, such as installer, sub-installer, Grand Master (Master), users, cleaner, maid, guard, arm-only (armer), duress, UO controller and bypass unit.

In the **Codes** area you can do the following:

- Set the length for all codes (4 digits or 6 digits)
- Set the Installer and Sub-Installer codes
- Set the DTMF code

In the **Users** area, you can do the following:

- **Label:** In the Label column, click on a user number and edit it accordingly.
- Authority level: Double-click the Authority Level field for a user, and select an authority level option from the dropdown list.
- **Partition:** Click the partition(s) the user will be allowed to operate.
- Code: Click in a code field; the Set User Password dialog appears where you edit the code.
- **Parent Control [Agility, WiComm]:** Select the checkbox for the users who are allowed to use the Parent Control feature (upon keypad/remote control activation, a message is sent to the Follow Me destination – used for tracking when children arrive at home, for example).
- **Proximity Tag:** Enter a proximity tag number for a user by double clicking in the Proximity Tag field and entering the relevant number.

Chapter 8: Communication

The following configurable communication parameters vary per RISCO system:

Configuring PSTN Parameters

NOTE: Some RISCO systems may not support PSTN communication.

- **Timers:** specify PSTN Loss Delay time, Wait for Dial Tone time (in seconds)
- **Parameters:** specify dial method, Rings Before Answer (number of rings before answering), Area Code, and PBX Prefix, call wait
- **Controls:** Answer Machine Override, Alarm Line Cut

Configuring GSM Parameters

- **Timers**: specify GSM loss delay, low RSSI GSM duration, GSM network loss. SIM expiration time, Keep Alive (MS Polling), and the schedule for primary, secondary and backup communication channels
- **Controls:** disable/enable GSM, enable/disable caller ID
- **Parameters:** specify SIM PIN code, SIM phone number, SMS center phone, and GSM network (signal) sensitivity (RSSI)
- **Prepaid SIM:** specify "get credit by" method, phone to send credit request, SMS credit message, and phone to receive SMS credit message
- **GPRS:** specify the APN definitions (APN, user name, password), E-mail server definitions (mail host, SMTP port number, SMPT user name, and SMPT password), and GSM/GPRS Module Email Address
- **Listener GPRS/IP Connection:** specify host subnet address, listener port number

Configuring TCP/IP Parameters

- **Automatic IP (DHCP):** specify if using Automatic IP (DHCP), IP address, subnet mask, gateway address, DNS primary address, DNS secondary address, IP port
- **Controls [Agility, WiComm]:** select checkbox to disable IP, or clear it to enable IP
- **Email Server:** specify the mail host, SMTP port, Email address, and User Authentication details (SMPT user name and password)
- **Parameters:** specify the network name, and Keep Alive (MS Polling) schedule for primary, secondary and backup communication channels

Configuring LRT Parameters

- **[LightSYS, ProSYS Plus]:** For long-range radio transmission (LRT), specify the 6-digit account number, system number, periodic test, timer for No Communication Timeout, and select the checkbox to enable bypassing low battery trouble.

Monitoring Station

Configure the monitoring station parameters in this screen (parameters vary per RISCO system).

To view the lists of the Report Codes, click **Report Codes.**

NOTE: Report codes can only be edited with the Configuration Software.

NOTE: For a detailed list of all available report codes refer to relevant RISCO system Report Code appendix.

Connections

	Type	Channel	Account	Phone	IP Address	IP Port
Monitoring Station 1	Voice	PSTN/GSM	001111			0
Monitoring Station 2	Voice	PSTN/GSM	002222			0
Monitoring Station 3	Voice	PSTN/GSM	003333			0

Parameters

MS Retries:	8
Alarm Restore:	On Bell Timed
MS1 SIA IP Encryption Key:	0001020304050
MS2 SIA IP Encryption Key:	0001020304050
MS3 SIA IP Encryption Key:	0001020304050
MS1 SIA IP Receiver Number:	0000
MS2 SIA IP Receiver Number:	0000
MS3 SIA IP Receiver Number:	0000
MS1 SIA IP Receiver Line Number:	0000
MS2 SIA IP Receiver Line Number:	0000
MS3 SIA IP Receiver Line Number:	0000

Controls

☐ Handshake
☐ Kiss Off
☐ Random Periodic Test
☐ SIA with Text
☐ SIA IP + CPID
☐ SIA with Partition

Communication Format

Format:
Contact ID

Report Codes...

Timers

Cancel Delay:	5
Abort Alarm:	15
Listen In:	120
No Arm:	0

Confirmation

Confirm Delay:	0
Confirm Time Window:	30

Periodic Test

Time:	0 : 0
Recurrence:	Do Not Call

Report Split

Arm/Disarm:	Call MS1 & MS2 As Backup
MS Urgent:	Call MS1 & MS2 As Backup
MS Non Urgent:	Call MS1 & MS2 As Backup

Report Codes [Contact ID]

Alarms | Main Troubles | Arm/Disarm | Zones | Keypads | Remote Controls | Sirens | I/O Expander | Miscellaneous

Emergency

	Event Code	Restore Code
Panic	120	120
Fire	115	115
Medical	100	100
Duress	121	121
Box Tamper	137	137
Confirmed Alarm	139	
Recent Close		
Confirmed Hold Up Alarm		

Configuration Software

See the sections under *Connecting the CS PC to the Main Panel,* page *15.*

Follow Me

Follow Me Tab

Configure the following for each Follow Me destination from the **Follow Me tab:**

- To enter a **label, phone number,** and **email address,** double click the respective field and edit / enter the information for each Follow Me user.
- To change an option in the **Type** or **Channel** columns, double-click the relevant field in the relevant line and select an option from the dropdown list that appears.
- To enable **Remote Listen** and **Remote Program** features, select the checkbox(s)
- Select the **partition(s)** that, upon alarm activation, will activate Follow Me reporting
- Configure additional parameters in these areas: **Controls, Parameters, Periodic Test**

Events Tab

Configure the following for each Follow Me destination from the **Events tab:**

- From the **Category** dropdown list, select a category that will generate Follow Me notification
- In the **Events area**, select the checkboxes for the event types (within the category) that will generate Follow Me notification. Repeat for the different categories.
- In the **Restore Events** area, choose the restore events that will be reported to each Follow Me destination.

Cloud

See *Establishing IP Network Communication from a Panel to the Cloud Server,* page …

Chapter 9: Audio

Define voice message parameters in the Audio screen, which is divided into the following sections:

- **Audio Messages**: Select a voice message to be assigned to a **zone**, **partition**, **output** or **macro**. When an event occurs this voice message will be heard accordingly. To assign location-specific messages, first select the language from the language dropdown list. Then double-click the relevant fields under the message number columns and select the locations/descriptors from the dropdown list.
- **Local Announcements (Local Messages):** Upon event occurrence, the system can announce the security situation to occupants of the premises by sounding a local announcement message. This announcement message can be enabled or disabled, per event. Enable a message announcement by checking the relevant checkbox.

Chapter 10: Scheduler

Define multiple weekly schedules for arming or activating utility outputs.

No.	Name	Type	Activation	Inactivity Timer
1	SCHEDULE 01	Arm/Disarm	☑	☐
2	SCHEDULE 02	Arm/Disarm	☑	☐
3	SCHEDULE 03	Arm/Disarm	☑	☐
4	SCHEDULE 04	Arm/Disarm	☑	☐
5	SCHEDULE 05	Arm/Disarm	☑	☐
6	SCHEDULE 06	Arm/Disarm	☑	☐
7	SCHEDULE 07	Arm/Disarm	☑	☐
8	SCHEDULE 08	Arm/Disarm	☑	☐
9	SCHEDULE 09	Arm/Disarm	☑	☐
10	SCHEDULE 10	Arm/Disarm	☑	☐
11	SCHEDULE 11	Arm/Disarm	☑	☐
12	SCHEDULE 12	Arm/Disarm	☑	☐

Parameters

SCHEDULE 01

	Start Time 1	Stop Time 1	Start Time 2	Stop Time 2
Sunday	00:00	00:00	00:00	00:00
Monday	00:00	00:00	00:00	00:00
Tuesday	00:00	00:00	00:00	00:00
Wednesday	00:00	00:00	00:00	00:00
Thursday	00:00	00:00	00:00	00:00
Friday	00:00	00:00	00:00	00:00
Saturday	00:00	00:00	00:00	00:00

Partitions For Schedule: 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32

Arming Mode: Away

Define schedule parameters from the following sections:

- **Scheduler [LightSYS, ProSYS Plus]:** For each schedule, double-click the Name field to edit it. Double-click the **Type** column and select from the dropdown list: Arm/Disarm or Utility Output. Clear the Activation checkbox to cancel the schedule without deleting it, and select the Inactivity Timer checkbox to automatically arm the zone if no signal is received according to the Inactive Timer time definition.
- **Scheduler [Agility, WiComm]:** For each schedule, double-click Label field to edit. Double-click the **Type** column and select from the dropdown list: Arm/Disarm, Utility Output or User Limit. Clear the Enable checkbox to cancel the schedule without deleting it.
- **Parameters:** For each schedule (2 possible), define up to two start times and two stop times for each day of the week by double-clicking on the relevant field and entering (or scrolling to) the desired times. Select the relevant partition(s) by checking the partition checkboxes, and select the arming mode from the Arming Mode (Stay, Away) from the dropdown list.

NOTE: To revert to defaults, in both Scheduler and Parameters, you can right-click in a field and select Restore Defaults.

- **Vacations button:** From the Vacations screen, for multiple vacations you can define their labels, start and stop days/times, as well as partitions, and then select the respective checkbox to enable the schedule (or clear the checkbox to disable it).

Activities

NOTE: All the operations under Activities can be performed only when the main panel is connected to the Configuration Software. Ensure the USB cable is connected, and then from the main menu select **Communication > Connect**.

Allocation – for LightSYS & ProSYS Plus

Here you can perform various system scans/searches and also allocate system components (bus devices and wireless devices) – both automatically and manually. You also delete system components that are no longer in use from this screen.
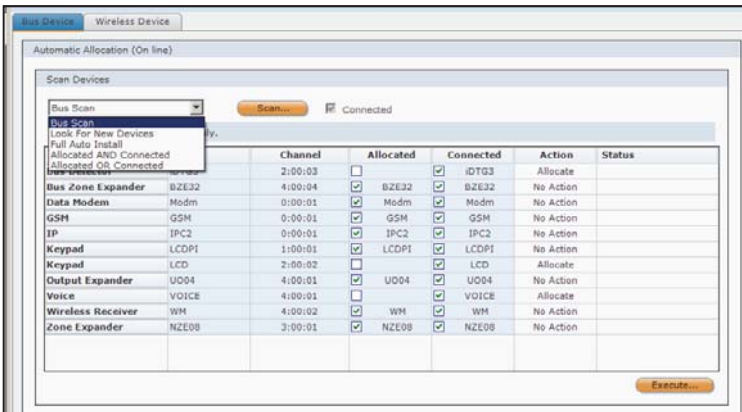
Bus Devices

➢ **From the Bus Device tab, you can do the following in the Scan Devices area:**

1. From the dropdown list, select a scan, search, or full auto-allocation to perform; the respective "status" checkboxes will display – "Connected" and/or "Allocated."

2. Press **Scan** to run the scan/search or full auto install; the resulting status for each discovered device displays in the various fields.

3. For the devices that are found, you can double-click their **Action** field and select from the dropdown list: **Allocate, Delete,** or **No action.**

4. Click **Execute;** the updated results for these devices will display, including the status (status field).

➢ **From the Bus Device tab, you can do the following in the Manual Allocation (Online) area:**

1. In the Accessory field, select a component (for allocating manually or deleting) from the dropdown list; depending on the component type, additional parameters may display.

2. Configure the additional parameters (for allocation), if any.

3. In the Type field, select the type / model of the component you want to manually allocate, or select **None** to delete its existing allocation.

4. From the Indexed / Indexed (logic position) field, manually select the index number

   - OR-

   [ProSYS Plus]: Select **Auto** to automatically assign an index number (if allocating).

5. **[ProSYS Plus]:** In the Bus ID field enter the RISCO bus line ID (1—4 available).

6. **[ProSYS Plus]:** In the Physical Address (D.S.) field enter the installer-set sequential ID that corresponds to the device's individual DIP switch settings.

7. Click **Execute.** You can perform another Bus scan (from the Bus Device tab) to view and confirm the results (for both allocations and deletions).

Wireless Devices

From the **Wireless Device tab,** you can allocate and delete wireless (RF) devices used in the system by entering the device's 11-digit serial code, or by sending an RF transmission from the device.

> ➢ **To allocate or delete wireless devices:**

1. In the Allocation area, from the Operation dropdown list, for the wireless device select **Allocate** or **Delete** (to delete a single device).

2. From the Accessory dropdown list, select the type of wireless device – zone (detector), keypad, keyfob, or siren.

3. If the wireless device is connected to the system via a wireless expander module, from the Select Receiver dropdown select the receiver (wireless expander) index number it is connect to.

4. In the Indexed field, select the devices index number

5. If deleting, press **Execute.**

6. If allocating, from the Allocate By dropdown list, select the allocation method – **By RF** or **By Serial.**

7. **[Allocating By Serial]:** In the Serial Code field, enter the 11-digit serial code, and now press **Execute.**

   NOTE: The serial number can also be found on the device.

8. **[Allocating by RF transmission]:** In the Allocation area, select the index number, then in the "Allocate By" field select the **By RF** option, and now press **Execute.**

9. Activate the device, and send a transmission per the following chart (note that not all devices in the chart may apply to your system):

Wireless Device (1-way and 2-way)	To send an RF transmission:
Detectors : • **WatchOUT** • **BWare** • **iWave** • **iWise** • **Door-Window Contacts (Dual Channel, Pulse Count, Universal)** • **Shock** • **Glassbreak**	Insert battery. Press and hold the tamper switch for at least 3 seconds.
Smoke & heat detectors	Insert battery. Transmission is sent automatically within 10 seconds.
Gas detectors	Insert battery. Within 10 seconds, press and hold the test button for 3 seconds.
CO detectors	Insert battery. Within 10 seconds, press and hold the test button for 3 seconds.
Flood detectors	Insert battery. Press both tamper buttons (back and cover) for at least 3 seconds.
WL beams	Insert battery. Press tamper spring for 5 seconds. Observe DIP switch settings according to model and tamper usage.
Sirens (Round Indoor siren, Lumin8 siren, Outside sirens)	Insert battery. Press and hold the tamper switch for 3 seconds.
2-way, 8-button remote control	Press both buttons (🔒 and 🔓) for at least 7 seconds.
4-button rolling code keyfob	Press and hold 🔒 for at least 5 seconds (the LED lights up twice during the 5 seconds - the second time indicates the transmission is being sent).
2-button panic keyfob	Press both buttons for at least 7 seconds.
Wristband panic transmitter	Press both buttons for at least 7 seconds. The red LED lights up upon transmission.
2-Way WL Slim Keypad	Press and hold both buttons (🏠 and 🔒) for at least 7 seconds.

> **To delete multiple RF devices:**

1. In the Delete RF Device area, select the checkbox(s) of the receivers (wireless expander modules) for which you want all their connected wireless devices deleted.

2. If you have multiple wireless expander modules and want to delete the connected devices for all of them, select the Check/Uncheck checkbox.

3. Press **Execute.**

Radio Device Allocation – for Agility & WiComm

You can allocate / delete the wireless (RF) devices used in the system – either by entering the device's 11-digit serial code, or by sending an RF transmission from the device.

> **To allocate wireless devices:**

- **[To allocate by serial code]:** In the **Allocation** area enter the 11-digit serial code, then manually select the index number (or select **Automatic** to have the next available index number assigned automatically), and now press **Allocate.**
  NOTE: To view the 11-digit serial code, in the **Identification** area, click **Read Code** and then active the device; the code and accessory type display in the respective fields.

- **[To allocate by RF transmission]:** In the **Allocation** area, select the index number (or select **Automatic** to automatically to have the next available index number assigned automatically), then press **Allocate.** Now activate the device, and send a transmission:
  NOTE: The main unit will acknowledge the sent transmission with a sound. When the system recognizes the device the Radio Device Allocation screen indicates that the status of allocation has been successful

Wireless device	Transmission procedure
2-Way LCD Keypad	Press ⬜ and ⬜ simultaneously for at least 2 seconds
2-Way Slim Keypad	Press 🏠 and 🔒 simultaneously for at least 2 seconds.
PIR Detectors: • **PIR** • **PIR camera** • **PIR-pet** • **PIR-pet camera**	Press the tamper switch for 3 seconds.
Curtain detector	After inserting battery, close the bracket and wait 3 seconds.
1-Way Magnetic Contact Detectors	Press the tamper switch for 3 seconds.
2-Way Magnetic Contact Detectors	Press the tamper switch for 3 seconds. **NOTE:** After programming parameters for this device and exiting Programming mode, press the Tamper switch for 3 seconds, and then wait 1 minute for the main panel to download the parameters from the detector
2-Way Remote Control	Press ⬜ and ⬜ simultaneously for at least 2 seconds
1-Way Keyfob	Click 🔒 for at least 2 seconds
Smoke Detector	After inserting battery, transmission is send automatically within 10 seconds.
Siren	Press the reset switch on the siren. After a squawk sounds, you have 10 seconds to press on the tamper switch for at least 3 seconds.
Gas Detector	Transmission is automatically sent 10 seconds after connecting to power supply, or after pressing the test button for 3 seconds (if pressed within 10 minutes of applying electrical power).
CO (carbon monoxide) Detector	Press back tamper switch for 3 seconds. Alternatively, transmission is automatically sent 10 seconds after installing battery.
2-Button Panic Keyfob	Press both buttons for at least 7 seconds
Wrist Band Panic Transmitter	Press the button for at least 7 seconds.

➢ **To delete wireless devices:**

• To delete an existing allocation(s), in the **Delete RF Device** area, enter the 11-digit serial code, index number and accessory type, then press **Delete** (or press **Delete All** for deleting all wireless devices in the system).

Status

The Status screen displays the system status including any troubles, and it enables you to send commands to each partition and zone. Changes initiated in this screen are immediately transmitted and reflected in the system settings display.
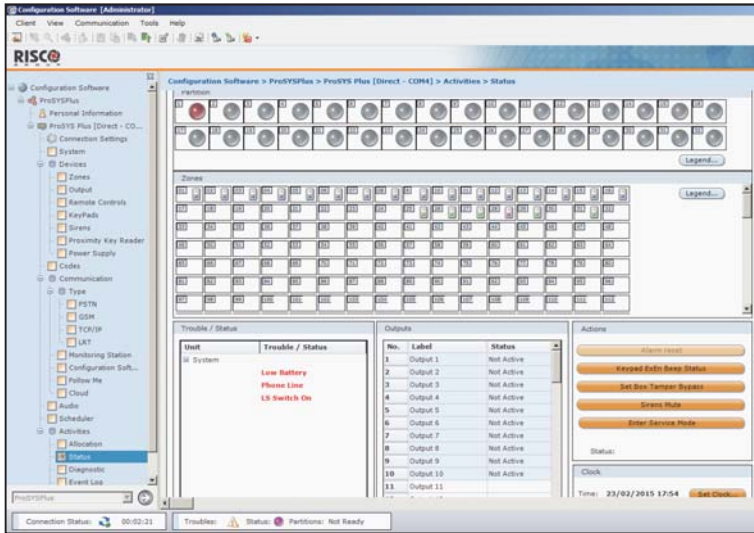
The Status screen is divided into the following sections:

- **Partition area:** View the status of all the partitions in your system (click **Legend** to view status conventions). Arm/disarm partition(s) that are in Ready state by right-clicking the relevant partition(s) and selecting **Arm**, **Arm All, or Disarm All.**
- **Zones area:** View the status of all the zones in your system. Click **Legend** to view status conventions. To view zone information, double-click a zone status icon. To bypass a zone, right-click on a zone status icon, and then select **Bypass.**
- **Expanders area [Agility, WiComm]:** If you have defined zones 33 to 36 in your system, you can view their status according to the color coded key.
- **Trouble / Status area:** View system and component-level trouble/status messages.

- **Outputs area:** View the status of the output devices. To activate/deactivate the output, right-click the relevant output and select **Activate** or **Deactivate.** **NOTE:** The status screen does not display the status (Open/Closed) of those U/O's that have been defined as latched.

- **Actions area**: Click the active button bars to change existing parameter settings.

- **Clock area:** Click **Set Clock** to edit the time.

Diagnostic (Testing)

| Main Unit | Bus Device | Communication | Wireless | Bus Test |

Main Unit

Panel Version:	RP512-0.16 0EN Feb 15 2015
File System Version:	0.16 15/02/15
Battery Voltage [VDC]:	0
Serial Number:	00000000000
Panel ID:	

Zones on Board

No.	Label	Resistance [KOhm]	Voltage [VDC]
1	Zone 001		0
2	Zone 002		0
3	Zone 003		0
4	Zone 004		0
5	Zone 005		0
6	Zone 006		0
7	Zone 007		0
8	Zone 008		0

Test

[LightSYS, ProSYS Plus]: You can perform the following diagnostic tests:

- **Main Unit tab:** To test and display the resistance in ohms (K Ohm), and the voltage (V DC) for all the onboard zones (zones on the panel PCB), click **Test.**
- **Bus Device tab:** To test bus devices (bus detectors, zone expanders, sirens, power supply modules, and LRT module), first select the bus device from the dropdown list, then select other applicable parameters from the fields that display (i.e. bus device ID), and now click **Test.**
- **Communication tab:** To test the IP and GSM communication modules, from the Communication Type dropdown list select a module, and then click **Test.**
- **Wireless tab:** From the Category dropdown list, select what wireless entities to test – receiver (wireless expander), zones, remote controls, keypads, or sirens – and then click **Test.** For the Receiver (wireless expander) you can also click **Calibration** to test the background noise level.
- **Bus Test tab:** Click **Test** to perform a system bus test.

[Agility, WiComm]: The Testing screen enables testing and displaying the RSSI signal strength level (and noise level calibration), battery voltage level and version / serial number of RISCO system components: main panel, zones, bus and wireless devices, and communication and I/O modules.

> ➢ **To perform diagnostic testing:**

1. First establish communication between the main unit and the Configuration software by selecting **Communication > Connect** from the main menu.

2. From the Testing screen, select the tab of what you want to be tested (main unit, zones, remote controls, keypads, sirens, GSM, I/O, IP)

3. Click **Test** (or you can click **Test All** to test the main panel and all the other components); the relevant results will display (such as RSSI level, version, serial number, battery voltage)

   NOTE: The RSSI level results will display from 0 – 100%

4. Click **Calibration** to measure and display the background noise level.

Event Log

> **To view all events in the system:**

1. From the Order By dropdown, select **ascending** or **descending** to view results.

2. To filter the dates, select the **Filter** checkbox and edit the date and time

3. Click **Read;** a list of all the events appears.

> **To export the Event Log:**

1. After viewing an event log, click **Export** and choose a type of file from the drop-down list: HTML, Text or CSV; the Save As dialog box appears.

2. Select a destination, enter a file name, then click **Save**.

Main Unit Upgrade (Main Panel Firmware Upgrade)

You can perform a firmware upgrade to the main panel via IP or GPRS.

➢ **To view the firmware version currently installed:**

1. Go to: **Diagnostics > Panel version**.

2. Ensure your system's main panel is connected to your computer.

3. From the directory tree, select **Main Unit Upgrade**; the Upgrade Channel screen displays:

4. Depending on your panel's primary mode of communication, select to upgrade through **IP** or **GPRS,** and then press **Upgrade;** the Remote Upgrade dialog appears:

5. Enter the Upgrade password (available from your local RISCO branch), and then click **Upgrade;** the keypad displays "system in installation" while the upload is taking place.

Appendix A: Deleting and Installing CS Versions

Periodically check to ensure you have the latest version of CS installed, which is available to upload from the RISCO website: **www.riscogroup.com**

To upgrade your Configuration Software version, do the following steps:

Step 1: Backing Up Clients

Before uninstalling an out-dated Configuration Software version, perform a backup of all client information.

➢ **To backup client information:**

1. Log in to the Configuration Software.
2. Go to **Client → Backup → Export,** and then select the individual checkboxes of the clients to back up, or to back up all clients click **Select All.**
3. Click **Export,** and then choose a location where to save the backup file.
4. Click **Save**.

Step 2: Uninstalling an Outdated CS Version

➢ **To uninstall the current CS version:**

• From your computer, go to **Control Panel,** and uninstall the **Configuration Software** program.

Step 3: Installing a New CS Version

• Install the most recent CS version from the RISCO website: **www.riscogroup.com**

Appendix B: SQL Server Express Edition 2005 Management

Use the non-default SQL Server Express Edition 2005 database if your system requires support for multiple concurrent connections or enhanced performance or if the present installation is an upgrade of an existing SQLSEE installation.

This appendix documents the SQLSEE installation and upgrade procedures, as well as troubleshooting.

Initializing and Installing the SQL Express Edition Database

➤ **To initialize and install the SQL Express Edition database:**

1. Go to: **Programs > RISCO Group > Configuration Software > System Organizer** window **> Install SQL Engine** directory tree option, and click **Start** as per the following:
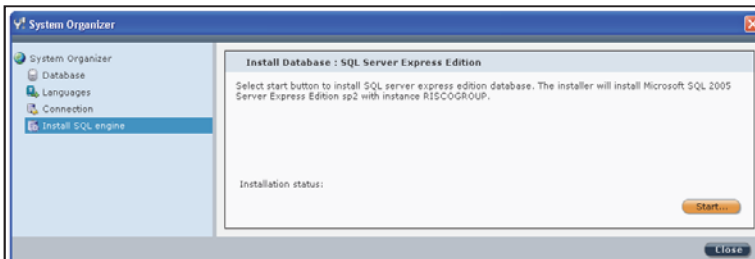
2. Upon successful instance creation, the message "Installation status: RISCOGROUP instance exists" displays.

3. Click the **Database** directory tree option, and then click ; the Select Database dialog displays

4. Select **SqlExpressEdition** from the dropdown list, and then click **Select.**
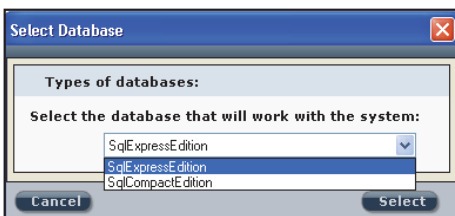
Microsoft SQL Server Installation Troubleshooting

If the Microsoft SQL Server 2005 has failed to install, here are some procedures that can be performed for troubleshooting:

- Assigning Microsoft SQL Server 2005 Administrator Privileges to a User
- Uninstalling RISCOGROUP instance on the Microsoft SQL Server 2005
- Uninstalling Microsoft SQL Server 2005 Common Components

Assigning Microsoft SQL Server 2005 Administrator Privileges to a User

If Microsoft SQL Server 2005 fails to install, it is possible that the logged-on user may not have administrator privileges to the Microsoft SQL Server 2005.

➢ **To assign Microsoft SQL Server 2005 administrator privileges to a user:**

For Win XP OS:
1. Go to **Start → Programs → Microsoft SQL Server 2005 → Configuration Tools → SQL Server Surface Area Configuration.**
2. Click the **Add New Administrator** link; the name of the currently logged-on user appears in the top-right of the window.
3. Click ⟩⟩ to move the left box contents over to the right box, and then click **OK;** the currently logged-on user now has administration privileges.

For Win 7 OS:
1. Right-click the CS desktop icon and select **Properties.**
2. In the Compatibility tab, select the **Privilege Level—Run this program as an administrator** checkbox.
   NOTE: If Microsoft SQL Express 2005 SP2 continues to fail to install, please contact customer support services.

Uninstalling RISCOGROUP instance on the Microsoft SQL Server 2005

If Microsoft SQL Server 2005 fails to install, try to uninstall the RISCOGROUP instance on the Microsoft SQL Server 2005.

NOTES:

- Do not uninstall the RISCOGROUP instance if you have other RISCO Group software programs installed on your computer.
- All existing clients will be deleted when uninstalling the RISCOGROUP instance on the Microsoft SQL Server 2005.
- Before removing the RISCOGROUP instance on the Microsoft SQL Server 2005, be sure to backup all existing databases.

➢ **To uninstall the RISCOGROUP instance on the Microsoft SQL Server 2005:**

1. **[Windows XP]:** Go to **Start → Settings → Control Panel → Add/Remove Programs.**
2. **[Windows Vista]:** Go to **Start → Settings → Control Panel → Program and Features.**
3. Double-click **Microsoft SQL Server 2005**; the Component Selection dialog box appears:
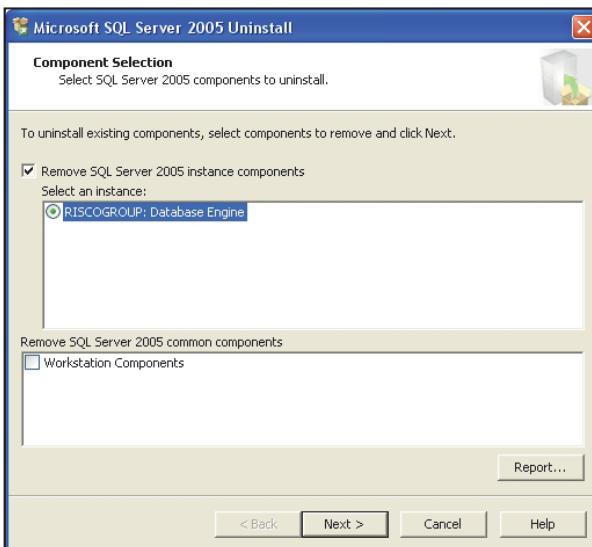
4. Select **RISCOGROUP: Database Engine,** and then click **Next.**

5. When uninstall is complete, go to: **My Computer → C → Program Files → Microsoft SQL Server → MSSQL.x → MSSQL → Data.**

   NOTE: There may be several MSSQL.x folders on your computer. If so, you need to check in which of these folders the MSSQL → Data folders appear.

6. If present, delete the following files:

   - **ConfigurationSoftware_Data**

   - **ConfigurationSoftware_Log**

Uninstalling Microsoft SQL Server 2005 Common Components

➢ **To remove all Microsoft SQL Server 2005 common components:**

1. In the Component Selection dialog box, select the **Workstation Components** checkbox

2. Click **Next.**

NOTE: For more information please refer to Microsoft's Help and Support for the SQL Server 2005.

Reinstalling Microsoft SQL Server 2005

➢ **To reinstall the Microsoft SQL Server 2005:**

1. Uninstall the Configuration Software (see…).

2. Reinstall the Configuration Software (see …); after the Microsoft SQL Server 2005 reinstallation will begin automatically.

Appendix C: Configuration Software Error Codes

Unknown = 0	An unknown error has occurred
Engine_OpenFailed = 20001	Failed to open the Com/Serial port. Please check your Com/Serial port number selection.
Engine_Timeout = 20002	Panel is in reply Time Out error
Engine_DeviceGeneralError = 20005	Communication engine reported an error.
Engine_DeviceWriteError = 20006	Incorrect data received from Panel (may be junk)
Engine_ModemNoDailTone = 20007	There was no dial tone detected by the modem connected to this computer. Please check the PSTN connection with the Modem.
Engine_CouldNotOpenDirectPort = 20013	Direct port could not be opened.
Engine_CouldNotOpenTcpipPort = 20014	A TCP connection to the panel could not be established. Please check that the panel IP number is alive and that the correct panel IP is shown in the 'Connection Settings'. If connecting from WAN, check that relevant port forwarding has been applied to the router that the panel is connected to.
Engine_CouldNotOpenModemPort = 20015	The Modem port defined in [Communication][Configuration] could not be opened. Make sure the selected com port really exists on this computer.
Engine_CouldNotOpenGprsPort = 20016	GPRS port could not be opened.
Engine_CouldNotOpenGsmPort = 20017	The GSM port defined in [Communication][Configuration] could not be opened. Make sure the selected com port really exists on this computer.
Engine_NoCallbackNumber = 20018	The panel is defined to call back the CS, but there is no call back number defined in the panel.
Device_CRCError = 30004	Loss of data. Please check hardware.
Device_InvalidValue = 30006	Received bad data from the panel. This could indicate that CS is not enabled at the panel. Please check CS is enabled in System/Controls at the panel
Device_SystemInArmed = 30007	Cannot send data to panel while in Set condition

Device_SystemInAlarm = 30008	Cannot send data to panel while in Alarm condition
Device_DefaultJumperOn = 30009	DIP switch 2 (Default switch) is on!
Device_SystemNotInPROGMode = 30010	In order to change panel parameters, it should be in PROG mode (currently it's not in PROG mode)
Device_SystemInPROGMode = 30011	System is in PROG mode (notification from Panel) and CS, for example, can't connect to it.
Device_SystemNotReadyToArm = 30012	The current panel status prevents the system being Set. Please check panel Status .
Device_GeneralError = 30013	A general error occurred in the panel.
Device_OutputActivationError = 30014	Incorrect UO Operation
Device_SystemInRFAllocationMode = 30018	The requested operation cannot be performed because the panel is currently in Learn Mode.
Device_AccessoryNotExists = 30019	An attempt was made to send/receive data to/from a device that is not present at the panel
Device_TeolTerminationNotSupported = 30020	Connection rejected. Please check the values of resistors set.
Device_N21 = 30021	CS—panel message format is wrong
Device_N22 = 30022	Bus parameter is wrong
Device_N23 = 30023	Bus allocation failed
Device_CommandNotSupportedByZoneType = 30050	Value in CS request is not valid
Device_RejectsConnetion = 30051	Panel N06 error reply (value is not valid) on LCL command from CS
Device_AccessCodeMismatch = 30052	Access code mismatch
Device_NotSupportedInVersion = 30100	Command is not supported in current Panel version
Device_CommandNotSupported = 30505	Panel or selected accessory doesn't support this service.
Device_MismatchRemoteId = 30110	Remote ID between panel and CS is mismatched. CS will disconnect.
MainApplication_LoadClientFailed = 40001	Failed to load the chosen client from the database. If this problem persists, please perform a Windows restart.

MainApplication_DeviceSignatureNotFound = 40002	Did not receive understandable data from the panel. Please check your Remote ID and Remote Access codes.
MainApplication_VerifyError = 40004	Verification failed.
MainApplication_DeviceSignatureNotLoaded = 40005	Device signature is not defined, can't be read from client or xml file or not recognized
Database_IncorrectVersion = 50001	The current application version requires a database update. Please perform a database upgrade by using the Organizer application
Database_ConnectionFailed = 50002	Connection to DB has failed
Database_DataBaseNotSelectedOrInit = 50003	The database cannot be spoken to. If this is a new installation, please perform [Initialize] in the System organizer

Standard Limited Product Warranty

RISCO Ltd., its subsidiaries and affiliates ("**Risco**") guarantee Risco's hardware products to be free from defects in materials and workmanship when used and stored under normal conditions and in accordance with the instructions for use supplied by Risco, for a period of (i) 24 months from the date of connection to the Risco Cloud (for cloud connected products) or (ii) 24 months from production (for other products which are non-cloud connected), as the case may be (each, the "**Product Warranty Period**" respectively).

Contact with customers only. This Product Warranty is solely for the benefit of the customer who purchased the product directly from Risco, or from any authorized distributor of Risco. Nothing in this Warranty obligates Risco to accept product returns directly from end users that purchased the products for their own use from Risco's customer or from any installer of Risco, or otherwise provide warranty or other services to any such end user. Risco customer shall handle all interactions with its end users in connection with the Warranty, inter alia regarding the Warranty. Risco's customer shall make no warranties, representations, guarantees or statements to its customers or other third parties that suggest that Risco has any warranty or service obligation to, or any contractual privy with, any recipient of a product.

Return Material Authorization. In the event that a material defect in a product shall be discovered and reported during the Product Warranty Period, Risco shall, at its option, and at customer's expense, either: (i) accept return of the defective Product and repair or have repaired the defective Product, or (ii) accept return of the defective Product and provide a replacement product to the customer. The customer must obtain a Return Material Authorization ("**RMA**") number from Risco prior to returning any Product to Risco. The returned product must be accompanied with a detailed description of the defect discovered ("**Defect Description**") and must otherwise follow Risco's then-current RMA procedure in connection with any such return. If Risco determines in its reasonable discretion that any Product returned by customer conforms to the applicable warranty ("**Non-Defective Products**"), Risco will notify the customer of such determination and will return the applicable Product to customer at customer's expense. In addition, Risco may propose and assess customer a charge for testing and examination of Non-Defective Products.

Entire Liability. The repair or replacement of products in accordance with this warranty shall be Risco's entire liability and customer's sole and exclusive remedy in case a material defect in a product shall be discovered and reported as required herein. Risco's obligation and the Warranty are contingent upon the full payment by customer for such Product and upon a proven weekly testing and examination of the product functionality.

Limitations. The Product Warranty is the only warranty made by Risco with respect to the Products. The warranty is not transferable to any third party. To the maximum extent permitted by applicable law, the Product Warranty does not apply and will be void if: (i) the conditions set forth above are not met (including, but not limited to, full payment by customer for the product and a proven weekly testing and examination of the product functionality); (ii) if the Products or any part or component thereof: (a) have been subjected to improper operation or installation; (b) have been subject to neglect, abuse,

willful damage, abnormal working conditions, failure to follow Risco's instructions (whether oral or in writing); (c) have been misused, altered, modified or repaired without Risco's written approval or combined with, or installed on products, or equipment of the customer or of any third party; (d) have been damaged by any factor beyond Risco's reasonable control such as, but not limited to, power failure, electric power surges, or unsuitable third party components and the interaction of software therewith or (e) any delay or other failure in performance of the product attributable to any means of communications, provided by any third party service provider (including, but not limited to) GSM interruptions, lack of or internet outage and/or telephony failure.

BATTERIES ARE EXPLICITLY EXCLUDED FROM THE WARRANTY AND RISCO SHALL NOT BE HELD RESPONSIBLE OR LIABLE IN RELATION THERETO, AND THE ONLY WARRANTY APPLICABLE THERETO, IF ANY, IS THE BATTERY MANUFACTURER'S WARRANTY.

Risco makes no other warranty, expressed or implied, and makes no warranty of merchantability or of fitness for any particular purpose. For the sake of good order and avoidance of any doubt:

DISCLAIMER. EXCEPT FOR THE WARRANTIES SET FORTH HEREIN, RISCO AND ITS LICENSORS HEREBY DISCLAIM ALL EXPRESS, IMPLIED OR STATUTORY, REPRESENTATIONS, WARRANTIES, GUARANTEES, AND CONDITIONS WITH REGARD TO THE PRODUCTS, INCLUDING BUT NOT LIMITED TO ANY REPRESENTATIONS, WARRANTIES, GUARANTEES, AND CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND LOSS OF DATA. WITHOUT LIMITING THE GENERALITY OF THE FOREGOING, RISCO AND ITS LICENSORS DO NOT REPRESENT OR WARRANT THAT: (I) THE OPERATION OR USE OF THE PRODUCT WILL BE TIMELY, SECURE, UNINTERRUPTED OR ERROR-FREE; (ii) THAT ANY FILES, CONTENT OR INFORMATION OF ANY KIND THAT MAY BE ACCESSED THROUGH THE PRODUCT BY CUSTOMER OR END USER SHALL REMAIN SECURED OR NON DAMAGED. CUSTOMER ACKNOWLEDGES THAT NEITHER RISCO NOR ITS LICENSORS CONTROL THE TRANSFER OF DATA OVER COMMUNICATIONS FACILITIES, INCLUDING THE INTERNET, GSM OR OTHER MEANS OF COMMUNICATIONS AND THAT RISCO'S PRODUCTS, MAY BE SUBJECT TO LIMITATIONS, DELAYS, AND OTHER PROBLEMS INHERENT IN THE USE OF SUCH MEANS OF COMMUNICATIONS. RISCO IS NOT RESPONSIBLE FOR ANY DELAYS, DELIVERY FAILURES, OR OTHER DAMAGE RESULTING FROM SUCH PROBLEMS.

RISCO WARRANTS THAT ITS PRODUCTS DO NOT, TO THE BEST OF ITS KNOWLEDGE, INFRINGE UPON ANY PATENT, COPYRIGHT, TRADEMARK, TRADE SECRET OR OTHER INTELLECTUAL PROPERTY RIGHT

IN ANY EVENT RISCO SHALL NOT BE LIABLE FOR ANY AMOUNTS REPRESENTING LOST REVENUES OR PROFITS, PUNITIVE DAMAGES, OR FOR ANY OTHER INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL

DAMAGES, EVEN IF THEY WERE FORESEEABLE OR RISCO HAS BEEN INFORMED OF THEIR POTENTIAL.

Risco does not install or integrate the product in the end user security system and is therefore not responsible for and cannot guarantee the performance of the end user security system which uses the product.

Risco does not guarantee that the product will prevent any personal injury or property loss by burglary, robbery, fire or otherwise; or that the product will in all cases provide adequate warning or protection.

Customer understands that a correctly installed and maintained alarm may only reduce the risk of burglary, robbery or fire without warning, but is not an assurance or a guarantee that such an event will not occur or that there will be no personal injury or property loss as a result thereof. Consequently Risco shall have no liability for any personal injury, property damage or loss based on a claim that the product fails to give warning.

No employee or representative of Risco is authorized to change this warranty in any way or grant any other warranty.

Contacting RISCO Group

RISCO Group is committed to customer service and product support. You can contact us through our website **www.riscogroup.com** or as follows:

Australia
Tel: + 1-800-991-542
E-mail: support-au@riscogroup.com

Belgium (Benelux)
Tel: +32-2522-7622
E-mail: support-be@riscogroup.com

China (Shanghai)
Tel: +86-21-52-39-0066
E-mail: support-cn@riscogroup.com

France
Tel: +33-164-73-28-50
E-mail: support-fr@riscogroup.com

Israel
Tel: +972-3-963-7777
E-mail: support@riscogroup.com

Italy
Tel: +39-02-66590054
E-mail: support-it@riscogroup.com

Poland
Tel: +48-22-500-28-40
E-mail: support-pl@riscogroup.com

Spain
Tel: +34-91-490-2133
E-mail: support-es@riscogroup.com

United Kingdom
Tel: +44-(0)-161-655-5500
E-mail: support-uk@riscogroup.com

USA
Tel: +1-631-719-4400
E-mail: support-usa@riscogroup.com

5IN1159 C