Remote Security Control
Remote Security Certificate Builder

BOSCH

en Reference Guide

Table of contents

1   Introduction

This document contains instructions for a trained installer to properly obtain, install, configure, and operate the Remote Security Certificate Builder v1.3 and higher, required for use with Remote Security Control v2.2 and higher. Remote Security Control works with some Bosch control panels, and all optional peripheral devices for those compatible control panels. Review this document and those listed in this section for more information.

1.1   About documentation

Throughout this document, the words "remote programming software" refer to all Bosch programming applications compatible with Remote Security Certificate Builder (RPS and A-Link Plus). Throughout this document, the words "control panel" refer to all Bosch control panels compatible with Remote Security Certificate Builder (GV4 Series, B Series, Solution 2000/3000).

Copyright
This document is the intellectual property of Bosch Security Systems, Inc. and is protected by copyright. All rights reserved.

Trademarks
All hardware and software product names used in this document are likely to be registered trademarks and must be treated accordingly.

1.1.1   Related documentation

To obtain any of the documents listed in this section, download them from the web.
Downloading documentation:
1.   Go to the Bosch website (us.boschsecurity.com).
2.   In the Search text box on the right side of the page, enter the CTN for the product for which you wish to download the documentation.
3.   Press [ENTER].
4.   If you see the desired document in the search results, click the link for the document to open it. Otherwise, click the desired product's Product Page button. The product page opens with the Details tab selected.
5.   Click on the Documents tab, and then click the desired language listed to the right of the desired document.

Call Bosch Security Systems, Inc., Technical Support (1-800-289-0096) if you need additional assistance.

Documents

Remote Security Certificate Builder Datasheet (P/N: 5903555851)#
Remote Security Certificate Builder Installation Guide (P/N: F01U262845)#
Remote Security Control Quick Reference Guide (P/N: F01U281304)# (this document)
Remote Security Certificate Builder Help*
RPS (D5500CU) Help*
ITS-ALINK-PLUS User Guide (P/N: F01U165466)#
*Within the application. #On www.boschsecurity.com.

2   Planning

This section includes compatibility, requirements, and configuration information for an RSC system.

2.1   Compatibility

Compatible control panels
–   B5512/B5512E, B4512/B4512E, and B3512/B3512E ("E" variants require an Ethernet or cellular module)
–   D9412GV4, D7412GV4, and D7212GV4
–   Solution 2000/3000 (ICP-SOL2-P/ICP-SOL3-P) (requires an Ethernet module)

Hardware requirements
–   A wireless router
–   For WAN applications, a wireless router connected to the internet
–   For WAN applications, a 3G or 4G plan for the Android or Apple iOS device

Compatible devices for certificates
–   Android devices with Android version 2.3 (Gingerbread) or newer
–   iPhone, iPod Touch, iPad with Apple iOS 4.5 or newer

Compatible remote programming software
–   Remote Programming Software v5.15.4 and higher
–   A-Link Plus Remote programming Software v4.5 and higher

Required software
–   Remote Security Control
–   Remote Security Certificate Builder
–   Remote programming software

Notice!

Refer to the Remote Security Certificate Builder or the remote programming software datasheet or installation guide for computer hardware requirements for those programs.

2.2   Software download and installation

Download and install the Remote Security Control app and Remote Security Certificate Builder.

2.2.1   Remote Security Control

Downloading Remote Security Control for Apple:
–   Use Apple iTunes, download the app from the iTunes store by searching on Remote Security Control, and then syncing to your Apple iOS device.
- or -
–   Use the App Store on your Apple iOS device by locating and installing the Remote Security Control.

Downloading Remote Security Control for Android:
–   Use the Play Store on your Android device by locating and installing the Bosch Remote Security Control.

You must have a valid certificate prior to using Remote Security Control.

2.2.2 Remote Security Certificate Builder

Downloading the installation files:
1. Go to the Bosch website (us.boschsecurity.com).
2. Click on the Products tab and select Intrusion Alarm Systems.
3. On the right side of the page, under Online Tools, click the Remote Security Certificate Builder link.
4. After reviewing the required prerequisites, click Install.
5. Save the install file to your computer hard drive.

Installing Remote Security Certificate Builder:
1. After completing the download, double-click the setup.exe file.
2. When the Application Install dialog box appears, click Install.
3. The Installing Remote Security Certificate Builder dialog box indicates the installation progress.
4. When the installation finishes, Remote Security Certificate Builder launches.

2.2.3 Remote Security Certificate Builder application updates

Every time you launch Remote Security Certificate Builder, it checks for updated application versions. If the Remote Security Certificate Builder locates a new version, the Update Available dialog box appears.
Click OK to install the update or click Skip if you do not wish to update at this time. The Remote Security Certificate Builder application window opens.

2.3 Configure the network

– When configuring a wireless router to connect to an Android or an iOS device in a WAN configuration for use with a GV4 Series v1.xx control panel, the data sent from the Android or iOS device to the public IP needs to be port forwarded to the internal LAN IP (forward UDP port 7700). Refer to the port forwarding section in your router instruction manual for more information.
– When configuring a wireless router to connect to an Android or an iOS device in a WAN configuration for use with GV4 Series 2.xx, B Series, and Solution 2000/3000 control panels, enable UPnP in the router configuration settings. This automatically configures connected devices. Refer to the port forwarding section in your router instruction manual for more information on UPnP.

For required parameters in remote programming software, refer to *Wireless networking parameters, page 7*.

2.4 Remote programming software parameters

Certificate data
To allow a user to connect to and exchange configuration parameters with a control panel using Remote Security Control, you collect the following information using Remote Security Certificate Builder:

Parameter	GV4 Series 2.xx	GV4 Series 1.xx	B Series	Solution 2000/3000
RPS passcode		X		
Application passcode	X		X	

Parameter	GV4 Series 2.xx	GV4 Series 1.xx	B Series	Solution 2000/3000
A-Link Plus/RSC passcode				X
Control panel IP address or host name	X	X	X	X
Control panel port number	X	X	X	X
Control panel account type	X	X	X	X
Control panel account or Customer number	X	X	X	X
Datalock code		X		
Encryption (AES Key setting)	X	X*	X	
*GV4 Series v1.xx control panels offer limited support for RPS Encryption parameters. To use encryption with the Remote Security Certificate Builder and GV4 Series v1.xx control panels, turn encryption On (Yes) and program the encryption key to something other than Default.				

Notice!

Set the Application passcode in RPS from within the control panel account. Go to Automation to find the Application Passcode entry. The default passcode is "Bosch_RSC".

Set the A-Link Plus/RSC passcode in A-Link Plus within Control Panel Configuration > Comm > Network Config > A-Link/RSC Password. The default passcode is "0000000000".

All changes to the Application Passcode within RPS or the A-Link /RSC Password in A-Link Plus require a new certificate for the Android or iOS device.

For information on locating and setting other required parameters, refer to *Build Remote Certificate wizard use, page 11*.

Wireless networking parameters

The certificate automatically validates the IP address settings configured in the control panel account. Before building a certificate, ensure the IP Address/HostName in the control panel account matches the IP Address/HostName set in the destination control panel or interface module.

In RPS, find these settings in the RPS Panel List window. Select the control panel account, click View and select the Network tab.

In A-Link Plus, find these settings in Customer List. Double-click the control panel account and set the IP and Port.

3   Remote Security Certificate Builder use

The Compatible Panel Accounts window of Remote Security Certificate Builder shows all control panels in the connected database that are compatible with Remote Security Certificate Builder. From this page, select the control panel you wish to configure, and then build a certificate.

3.1   Configuration

Prior to logging in to a remote programming database through Remote Security Certificate Builder, you must configure the database settings. The settings, which include the database location, name, and authentication information (depending on the remote programming software used), allow Remote Security Certificate Builder to connect with the database.

Notice!

For RPS, if you do not know the database location (server name), the database name, or authentication method, you can view the database settings within RPS by selecting Config > System, and then viewing the information on the File Locations tab. For information on RPS and authentication, refer to *RPS Database settings and authentication, page 9*.

For A-Link Plus, if you do not know the database path, find it in C:\Program Files(x86)\Bosch Security System\A-Link Plus\DataBase.

---

1.   Select Start > (All) Programs > Bosch > Remote Security Certificate Builder. The Remote Security Certificate Builder application window launches.
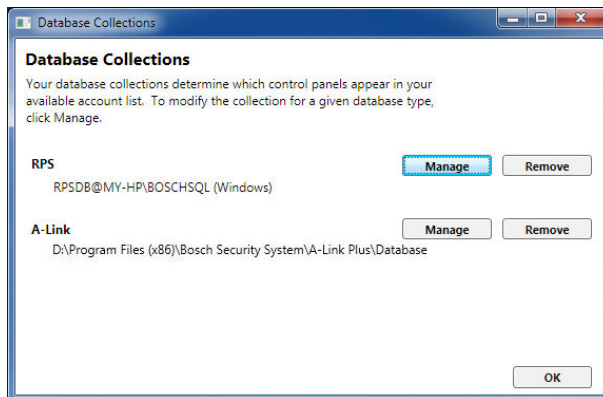2.   Click the Database Settings button. The Database Settings dialog box opens.

Figure 3.1: Database Collections dialog box

3.   Click the Manage button for the database you wish to use. The corresponding Settings dialog box appears.
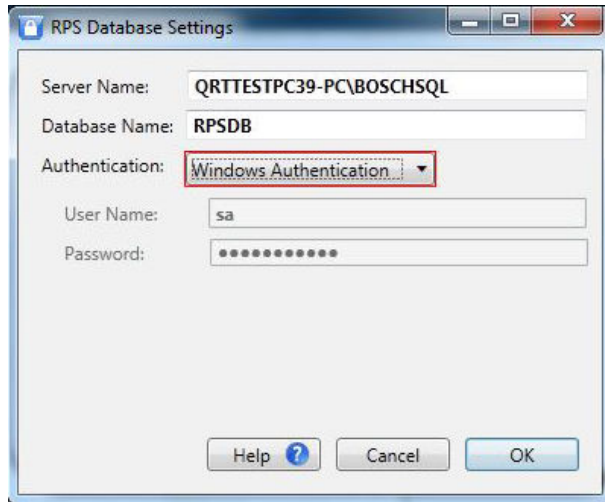
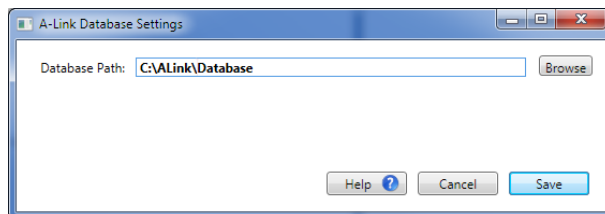**Figure 3.2: RPS Database Settings dialog box**

Figure 3.3: A-Link Database Settings dialog box

4.   Enter the appropriate information in the text boxes, or browse to and select the correct database.
5.   Click OK.

The dialog box closes and returns to the Remote Security Certificate Builder application window. You can now log in to access the desired database.

3.1.1   RPS Database settings and authentication

Database connection failed (Windows 7 / Windows 8)

When RPS is installed on Windows 7 or 8, the User Account Control (UAC) settings prohibit Windows Authentication as a connection method to the SQL database.

If your RPS settings have been configured to Windows Authentication on a Windows 7 or 8 operating system, when attempting to open RPS, the **Database Connection Failed** dialog box appears**.** To correct this, either change your **RPS Database Settings** to **SQL Server Authentication** or **Run as Administrator.**

SQL Server authentication

1.   Click **OK** on the **Error** dialog box.
2.   Enter your SQL authentication password in the **Enter Password** field**.** (On a new installation, the default Password for the **sa** User Name is **RPSsql12345**.)
3.   For a new database installation, enter a **SQL Database Name,** click **Create Database**, then click **OK**. For an existing database installation, click **OK**.
4.   The RPS **Login Information** dialog box opens, enabling you to access the SQL database.

Run as Administrator (Windows 7 / Windows 8)

1.   Click **OK** on the **Error** dialog box.
2.   On the **Database Settings** dialog box, click **Cancel**. (The RPS window closes.)
3.   Right click on the RPS shortcut on the desktop.
4.   Choose **Run as Administrator**.

5.   The RPS **Login Information** dialog box opens, enabling you to access the SQL database. For more information on RPS default user credentials, refer to *RPS Help* or the *RPS (D5500CU) Installation Guide* (P/N: 4998141259).

3.2   Log in

> **Notice!**
>
> During the log in process, Remote Security Certificate Builder attempts to independently authorize the user to access each of the configured remote programming applications. For applications that require hardware security devices, Remote Security Certificate Builder performs additional security checks.
>
> To access Remote Security Certificate Builder, log in with proper credentials to authorize the specified user to at least one configured application.

> **Notice!**
>
> For control panels using RPS, limit access to Remote Security Certificate Builder to authorized individuals only because the application contains provisions for setting passwords. Establish appropriate security levels and set passwords before allowing operating personnel access to Remote Security Certificate Builder. To set the security level for Remote Security Certificate Builder access, within RPS select Config > System, and then locate Manage Credentials on the Security tab.

> **Notice!**
>
> For control panels using A-Link Plus, limit access to Remote Security Certificate Builder to authorized individuals only because the application contains provisions for setting passwords. To allow an A-Link Plus user to access Remote Security Certificate Builder access, within A-Link Plus, select User > Operator Settings, select the desired user or click Add to add a new one, and then click Modify Level and add the Make RPC certificate option. The default user, admin, has the Make RPC certificate option by default.

Logging into Remote Security Certificate Builder:
1.   Select Start > (All) Programs > Bosch > Remote Security Certificate Builder. The Remote Security Certificate Builder application window opens.
2.   To configure Remote Security Certificate Builder during the first use, refer to *Configuration, page 8*. To log in, enter your remote programming software user name and password.
3.   Click Login (or press [Enter]) to continue.
If you enter incorrect credentials, the window indicates that login failed.
If your login attempt succeeds, the Compatible Panel Accounts window opens.

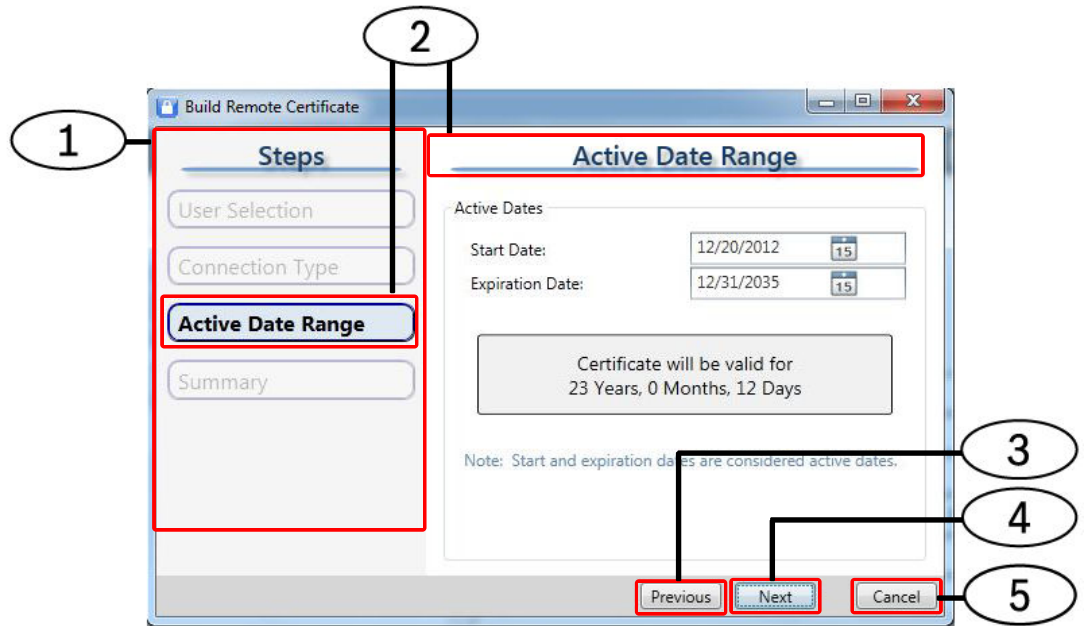## 3.3   Build Remote Certificate wizard overview

Figure 3.4: Build Remote Certificate wizard overview

Callout	Name	Brief description of use
1	Steps pane	Lists the steps in the wizard
2	Current step indicators	Indicate the current step
3	Previous button	Move to the previous step
4	Next button	Move to the next step
5	Cancel button	Close the Build Remote Certificate wizard

3.4   Build Remote Certificate wizard use

Launch the Build Remote Certificate wizard to create a certificate. In the Compatible Panel Accounts area, locate the account for which you wish to make a certificate. Then, double-click on the account, or highlight the account and then click the Build Certificate button or select File > Build Certificate. The Build Remote Certificate wizard opens.

The Steps pane lists all the steps in the wizard, and highlights the current step. The field on the right side of the wizard allows you to configure the certificate. Use the Next and Previous buttons, when enabled, to move through the wizard. Refer to *Build Remote Certificate wizard overview, page 11*.

Notice!

For GV4 Series and B Series control panels, the Build Remote Certificate wizard requires specific programming parameters set in the Panel Data section of RPS. From RPS – Panel List, select the control panel account and click View. Click Edit to modify these parameters. These parameters are:

- For GV4 Series 1.xx control panels, an IP address and a Datalock code.
- For GV4 Series 2.xx control panels, an IP address.
- For B Series control panels, a cellular IP address for a cellular certificate or an Ethernet IP address for an Ethernet certificate.

Notice!

For Solution 2000/3000 control panels, the Build Remote Certificate wizard requires specific programming parameters set in the Panel Data section of A-Link Plus. From the A-Link Plus Customer List, double-click the control panel account to modify these parameters. These parameters are:

- Control panel IP address
- Control panel port

3.4.1   User Selection page

In the first step of the wizard, select the user for whom you wish to create a certificate, and then click Next. You can identify users by User # or Name.

3.4.2   Connection Type page

In the second step of the wizard, select the connection method for the control panel to use to connect to the network, and then click Next.

The Connection Type page enables only the methods available for your control panel; unavailable connection types are disabled.

3.4.3   Active Date Range page

In the Active Date Range step of the wizard, set the dates for which you wish the user's certificate to remain active, and click Next.

3.4.4   Summary page

In the final step of the wizard, use the Summary page to view a summary of your selections in the previous pages, and to confirm that the wizard successfully created the certificate with those selections. You can click the Previous button to make changes and recreate the certificate.

From the Summary page, you prepare to send the certificate to the user. You can do one of the following:

– Generate a prewritten email using your default email client and your client email account, if they are configured on the Remote Security Certificate Builder computer. The email includes the following information:
  – User name
  – Account number
  – Instructions for copying the certificate to the Remote Security Control device and to install it.

  Generate the email, by clicking Create Email.

> – Open Windows Explorer to the directory to which the wizard saved the certificate, with a single click. You can then drag and drop the certificate from the opened directory to the email.
> Open the file location directory by clicking Open File Location.

> **i** | **Notice!**
> Cellular certificates created for B Series control panels with cellular configured include "_Cell" in the file name for identification (for example, B5512_Site1_Cell).

When you finish creating the certificate for the desired account, click Finish.

4   Remote Security Control use

Prior to using Remote Security Control you must open the user's certificate on the user's compatible device. To open the certificate, the device must have an email client configured.

> **Notice!**
> You can open an unlimited number of certificates on an a device, allowing for multiple users on each device.

Opening the certificate for the user on the user's device:
1.   Open the received email on the device. (Use Gmail on Android devices.)
2.   Open the certificate file.
3.   Select Open in RS Control. Remote Security Control automatically opens to the Certificates section.
4.   Select the certificate you wish to use and tap Connect.
5.   Tap the empty numeric box to launch the keypad.
6.   Enter the user passcode for the user you selected when building the certificate.
7.   Tap Done.
8.   Tap Connect to Panel.
9.   Remote Security Control connects to the control panel, and the current status shows on the Security tab.

> **Notice!**
> For GV4 Series control panels, Remote Security Control and RPS cannot connect to the control panel at the same time.

4.1   Remote Security Control options overview

Once connected to the control panel, Remote Security Control can perform the following functions:
–   Turn the security system on and off
–   Secure, unlock, and cycle access doors (D9412GV4/D7412GV4 only)
–   Turn outputs on and off
–   View security system faults*
–   View area status

*For Solution 2000/3000 control panels, the system faults shown are only: System low battery, Phone line fault, AC Fail, and RF receiver missing.

4.2   Remote Security Control operation

Once connected to the control panel and viewing the Security screen, you can do the following:
–   Tap the padlock icon to turn on (arm) or turn off (disarm) the system.
–   Tap See Details, when available, to view system faults.
–   Work with the doors connected to the control panel by tapping Doors. The Doors screen shows the status of each door. Tap on a listed door to change its status. Depending on the door's current status, tap Secure, Unlock, or Cycle, if desired.
–   Work with the outputs connected to the control panel by tapping Outputs. The Outputs screen shows the status of each output. A solid blue circle indicates the output is On, and an empty circle indicates the output if Off. Use the All, On, and Off buttons to change the outputs shown. Tap on a listed output to change its status.

– To view area status and turn on (arm) or turn off (disarm) specific areas in a multiple area system, tap Advanced from the Security tab.
– To view control panel events, tap Events.
– To view IP cameras, tap Cameras. (For control panels that support IP cameras.)

When finished, tap Disconnect to disconnect from the control panel. (On Android, tap Disconnect and then tap Disconnect Now.)

5   Troubleshooting

This section includes troubleshooting tips.

5.1   Remote Security Certificate Builder error messages troubleshooting

Cannot login without security dongle. Please try again.
Connect a security block to the remote programming software network server or to the client itself. When using a D5370 as a network security block for use with all connected client machines, the generated broadcast message cannot cross subnets. Ensure all client machines are located in the same subnet as the programming database.

Login failed. Unable to authenticate or insufficient rights.
Verify that the operator User Name and password are correct.

Login failed. Unable to connect to the database.
Open the Database Settings and verify the server name, database name, and authentication User Name and password are correct.

5.2   Remote Security Control error messages

Cannot connect to the specified control panel
– For GV4 Series 2.xx, B Series, and Solution 2000/3000 control panels , verify that the application passcode setting located in the Automation section is set correctly. Refer to *Remote Security Certificate Builder, page 6*.
– Verify the passcode for the selected user.
– If using a Wi-Fi connection to connect to the control panel, verify the device is connected to the same network as the control panel or interface module.
– If connecting to a GV4 Series v1.xx control panel over a WAN, verify that port forwarding is set correctly in the router.