Application Note
RPS-API V2.3.0.6

1 Introduction

The RPS-API (Remote Programming Software Application Programming Interface) provides a RESTful interface for customers to integrate their applications with the configuration data stored in the RPS Database. This document describes how to install and configure RPS-API in a MS Windows development environment.

2 Feature Overview

The main service provides the RESTful Web API to search for panel attributes by control panel GUID. The control panel GUID is a unique ID that identifies a panel.

2.1 Panel, Area and Point attributes

The RPS-API allows for secured READ ONLY access to select Panel, Area and Point attributes.

Panel attributes include:

- Panel GUID
- Supported Languages
- Panel Language

Area attributes include:

- Area Number
- Area On property
- Area Name Text
- Exit Delay
- Force Arm/Bypass Max

Point attributes include:

- Point Number
- Area
- Profile
- Text
- Source
- RFID
- Output

Point Profile attributes include:

- Bypassable
- Entry Delay
- Point Type
- Response
- Circuit Style

2.2 Panel control attributes

The RPS-API allows you to control specific elements of the panel.

- Arm/Disarm Areas
- Bypass/Unbypass Points

2.2 Panel Connection, 3rd Party Integration/Automation attributes

The RPS-API allows for secured READ and WRITE access to select Panel Connection, 3rd Party Integration/Automation, and Panel User Assignments attributes.

Panel Connection attributes include:

- RPS Panel Data - View: Network IP details
- RPS Panel Data - View: Cellular details
- RPS Panel Data - View: Cloud ID details

3rd Party Integration/Automation attributes include:

- Automation Device
- Automation Passcode

User Assignments

Create, reset or delete users or individual User attributes include:

- Passcode
- Authority Level
- User Name
- User Group
- Card Data
- User Number

2 System requirements

3.1 Windows system

The following are the minimum requirements for your environment:

- Windows .NET 4.6 framework and higher
- Windows 8
- Windows Server 2012 R2 and higher
- 4 GB RAM

3.2 RPS (Remote Programming Software)

Install RPS-API on a machine that has RPS version 6.11 or higher installed. RPS-API does not require the RPS client application after installation but uses the configured connection to the RPS database.

RPS minimum version supported for use with RPS-API versions 2.2.27914 or higher:

- RPS 6.11 or higher to support full API and panel operations, including TCP Panel connections.
- RPS 6.04 to RPS 6.10 to support full API features with panel connections limited to and requiring UDP protocol.

3.3 Supported control panels

RPS-API supports the following control panels:

- B9512G, B8512G
- B6512, B5512, B4512, B3512
- D9412GV4, D7412GV4
  - GV4 1.00 through 1.00.010 (Step 3)
  - GV4 2.00 through 2.00.014 (Step 4)
- D9412GV3, D7412GV3
  - GV3 8.10 through 8.14 (Step 2)

Note: RPS-API does not support GV3 control panels 8.00 through 8.05 (Step 1). RPS-API can update the RPS database for these panels but cannot communicate with these panels.

3.4 Supported connections

The RPS-API Scheduler service supports the following RPS connections:

- IP
- Cellular
- Cloud
- WebConnect

3.5 Supported Network Protocols

When opening a panel connection, RPS-API version 2.1 (and higher) uses the System Configuration Settings saved in RPS. Using RPS version 6.07 (and higher), operators select one of three options:

- UDP Only
- TCP with fallback to UDP
- TCP Only

Using RPS version 6.06 and earlier, RPS-API will continue using the default UDP Only setting.

Note: Using RPS version 6.10 and lower with RPS-API 2.3.0.6 and higher will result in failed TCP connections to panel systems and requires configuring either the UDP Only or TCP with fallback to UDP setting.

3.6 Required Security Protocol

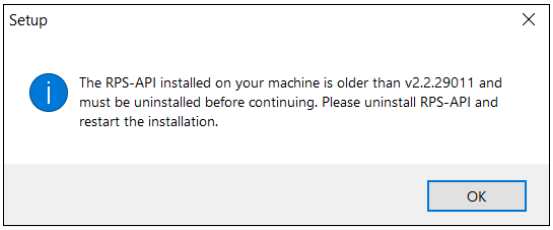
RPS-API version 2.2 and higher requires HTTPS. Version 2.2.27914 and higher only supports HTTPS to secure communications.

4 Installation

Perform the following steps to install RPS-API:

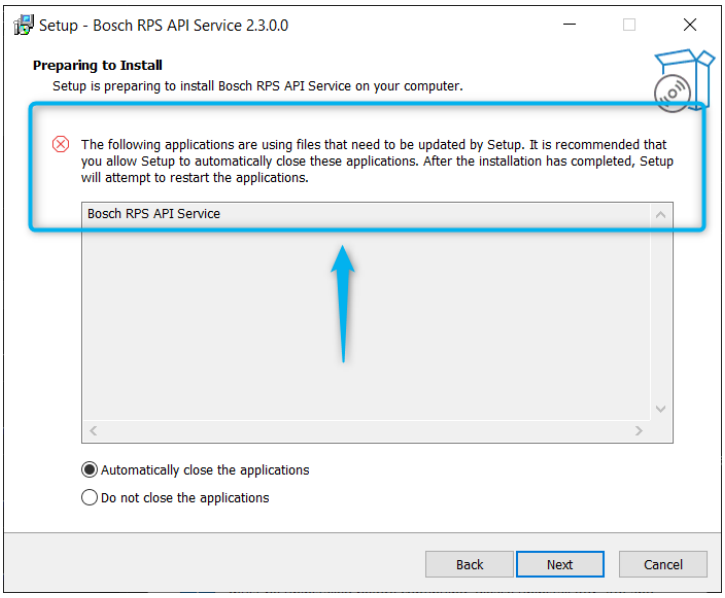
1. Download and save the installer to your local machine.
2. Run the **Bosch_RPS_API_Setup_v2.3.0.6.exe** installer.
3. The installer wizard opens to the EULA (End User License Agreement) screen. Read and select **I accept the agreement**. When finished, click **Next**.

- If the machine is missing any dependencies, you will receive an error message. If the message notifies you of a missing software package, install the package and re-run the installer.
- If the machine previously had RPS-API installed and the installed version is older than 2.2.29011, you must manually uninstall the previous version of RPS-API. Then, re-run the installer. This is due to a technology compatibility issue.

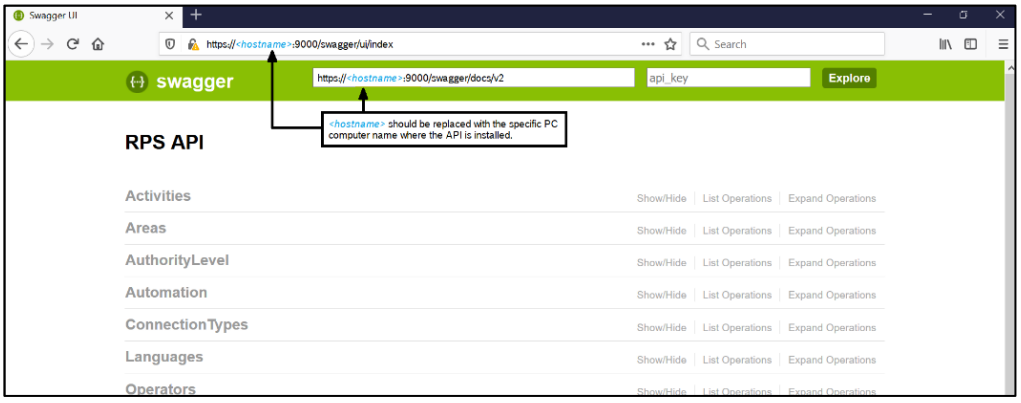


4. Click **Install**.

- If a application message shows on the **Preparing to Install** screen, the RPS-API might be running on the machine. Select **Automatically close the applications** to stop any instances of RPS-API and continue with the new installation.



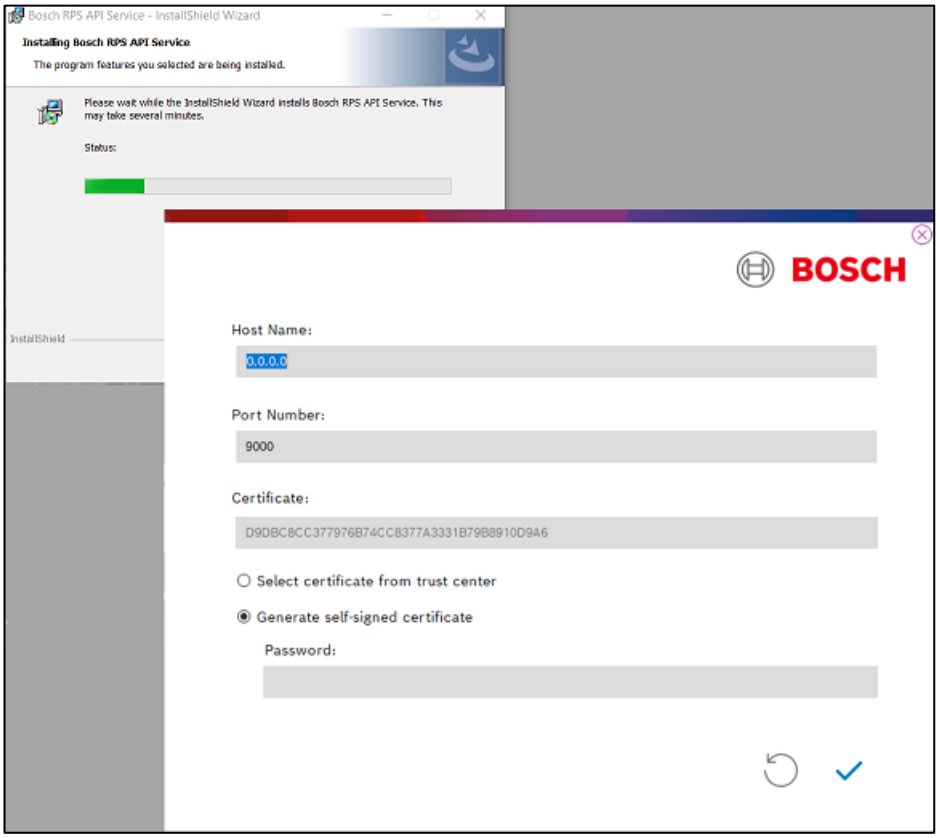
5. After finishing the installation and configuring HTTPS, the installer saves the OSS report to your machine. This report can be found at **C:\Program Files (x86)\Bosch\Bosch RPS API Service\OSS\RPSAPI-V2.3-OSS.html**.
6. To verify that RPS-API is running, access the **https://*<hostname>*:9000/swagger/ui/index** URL in a browser to open the Swagger documentation web page. Note that *<hostname>* is the computer name where the API is installed.



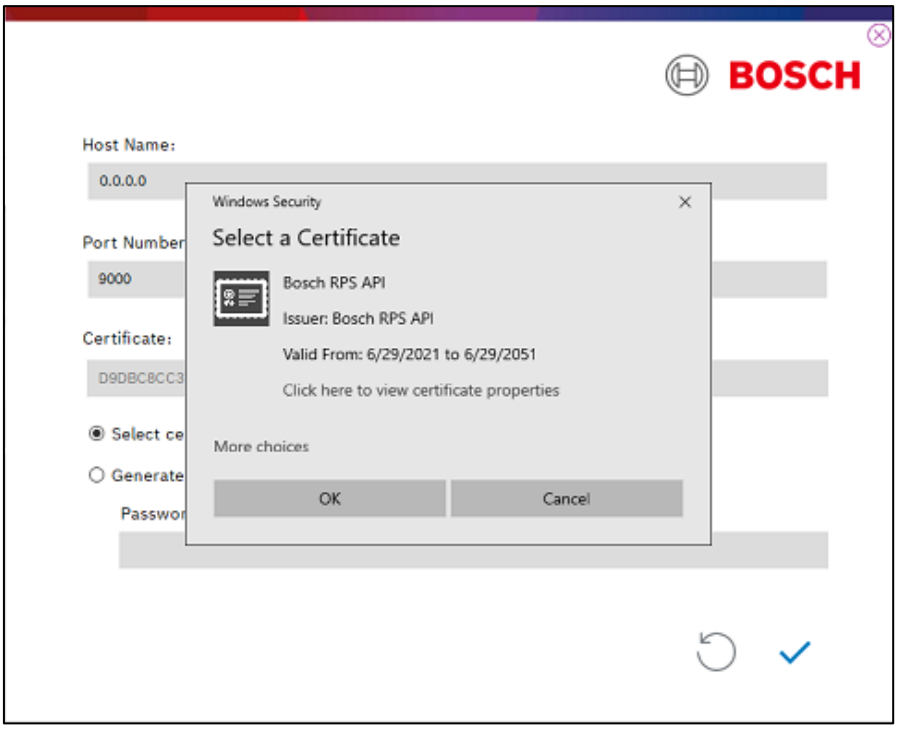
4.1 HTTPS Configuration Tool

The RPS-API 2.3.0.6 installation provides an HTTPS configuration tool guide you through the HTTPS set up.

1. In the configuration tool, edit these entries as needed:
   - **Host Name** - default value = 0.0.0.0. Change this entry when you want to have a specific domain name for RPS-API, which relates to the DNS/Router settings. For more information, reference the netsh command in Windows. You can also use this command to manually set up HTTPS for RPS-API. Avoid using localhost or 127.0.0.1 for the host name as it makes RPS-API inaccessible from another machine.
   - **Port Number -** default value = 9000. The entry port number for RPS-API.
   - **Select certificate from trust center** - if you have a certificate for the Web server, use this entry to select an installed certificate from LocalMachine/Personal repository. Select **More choices** to select a certificate from a list. Once selected, the thumbprint is shown in the certificate field.

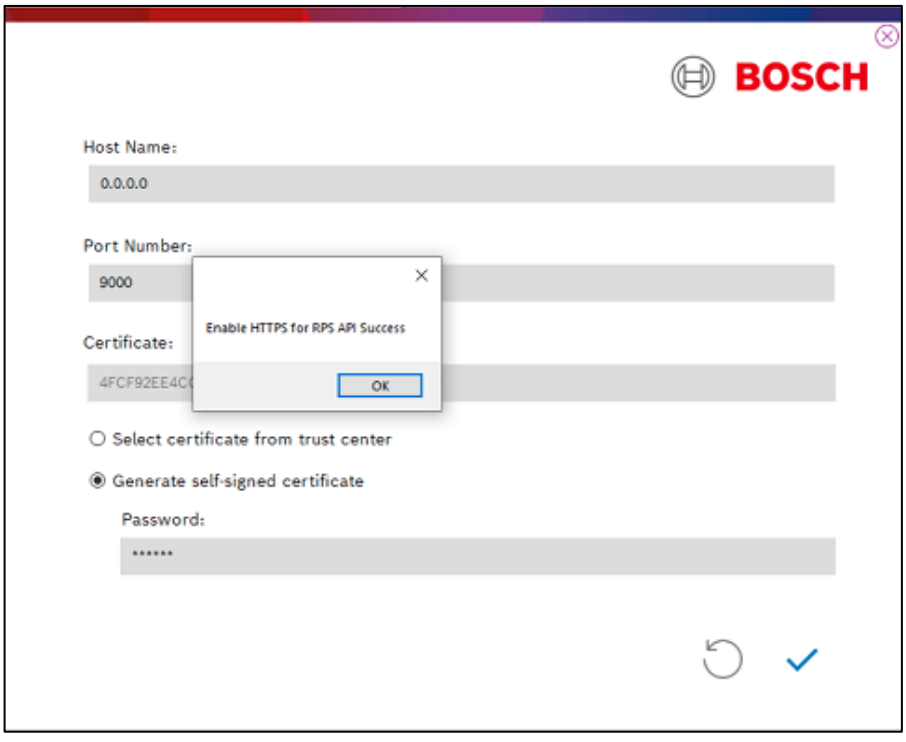


2. Select **Generate a self-signed certificate**. Make sure that you enter the password for the certificate, as the password field cannot be empty.



3. Click ✓ to process. The configuration tool generates a server certificate for the RPS-API set up. When finished, a success message displays. Click **OK**.

   If you already set up HTTPS for RPS-API or if you want to manually set it up, click ⊗ to exit the configuration tool.



Self-signed certificate and untrusted CA warning

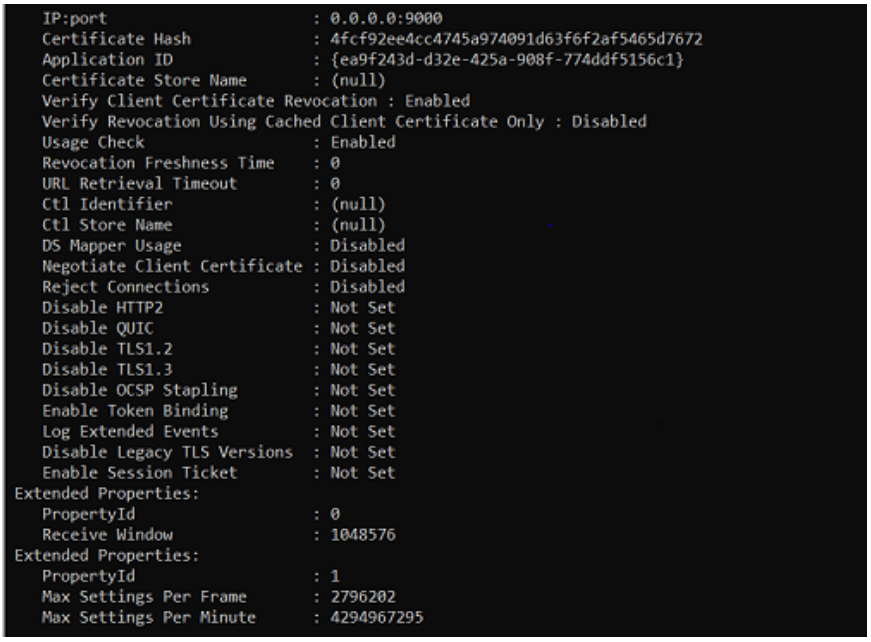
When you install the RPS-API version 2.3.0.6 or higher and select to generate a self-signed certificate, the installation will install the certificate and set up RPS-API using the HTTPS **netsh** command. On the client side, the self-signed certificate is not issued from a trusted authority, so browsers or your application will receive an untrusted CA (Certificate Authority) warning.

To fix the untrusted CA warning, install the self-signed certificate on the client machine and modify your application to ignore the warning.

4.2 Verify HTTPS is enabled

With administrator permission, open a Windows command prompt. Type and execute the commands:

1. **netsh http show sslcert**



2. **netsh http show urlacl**

After the certificate is installed, you might need the certificate for your clients. Locate the generated certificates (if you selected the generate self-signed certificate option) in this path:

%appdata%\Roaming\Bosch RPS-API

For example:

c:\users\<name>\AppData\Roaming\Bosch RPS-API)

5 Enable HTTPS

RPS-API version 2.2.27914 and higher only supports HTTPS to secure communications. During the installation, the HTTPS configuration tool will guide you through the setup of HTTPS. See section 4.1 HTTPS Configuration Tool for information.

To enable HTTPS for RPS-API, you must have an SSL certificate, and then install the certificate to the local machine. The following files are available for you to use:

- Setup_HTTPS_RPSApi.ps1 (MS PowerShell)
- Setup_HTTPS_RPSApi.bat (batch file)

After you install the certificate, use the batch file (Setup_HTTPS_RPSApi.bat) to enable HTTPS for RPS-API.

1. Install the SSL certificate to LocalMachine\root.
2. Stop the RPS-API service.
3. Change the EnableHTTPS configuration to 1 in HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Bosch\RPSAPI\Setup.
4. Copy the thumbprint of the certificate.
5. Paste the thumbprint into $certHash=''<thumbprint>'' in either the Setup_HTTPS_RPSApi.ps1 or Setup_HTTPS_RPSApi.bat file.
6. If RPS-API is not running in port 9000, change the $port setting in either Setup_HTTPS_RPSApi.ps1 or Setup_HTTPS_RPSApi.bat file.
7. Run Setup_HTTPS_RPSApi.ps1 or Setup_HTTPS_RPSApi.bat with administrator permission.
8. Start the RPS-API service.

Note: If the certificate is not signed, the browser or Postman will block the connection. To verify the function, disable the HTTPS verify function in the browser or client application.

6 Sample Code

Preformatted sample code with basic calls to RPS-API is included in a Postman collection. To view and test the sample code, download and import the collection into Postman.

The RPSAPI-PostmanExamples.json collection is located in the install directory: Bosch > Bosch RPS API Service > Samples.

The imported Postman calls allow you to check if RPS-API is running by making simple REST calls. The calls provided are a subset of the RPS-API functionality, but include tasks such as getting a panel, setting a user on a panel, arming and disarming a panel.

Notes:

- Set and save any variables to avoid retyping with each call. (See Image 6.1, Image 6.2)
- Run a few specific calls to set key operating variables:
  1. **Get Token** to receive and set the Token variable
  2. **Get a panel using panelname** to set a specific panel
     - **Get all panels** if you prefer all panels
- Run your tests. Some calls will auto-save results to variables.

Image 6.1 Review and set any variables

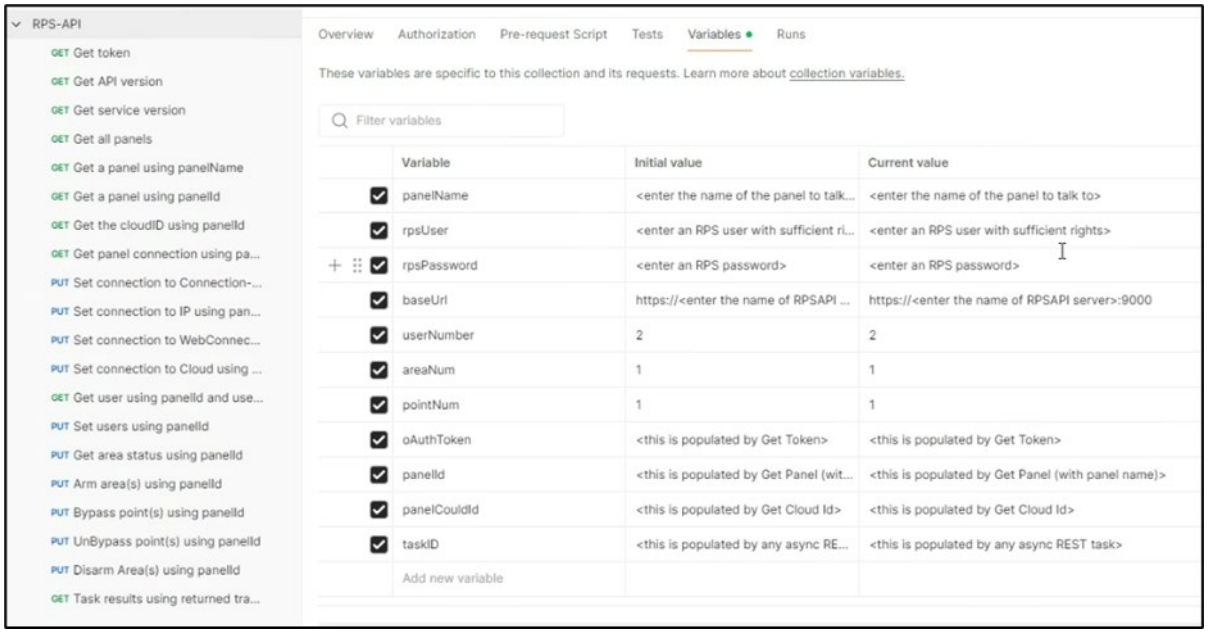


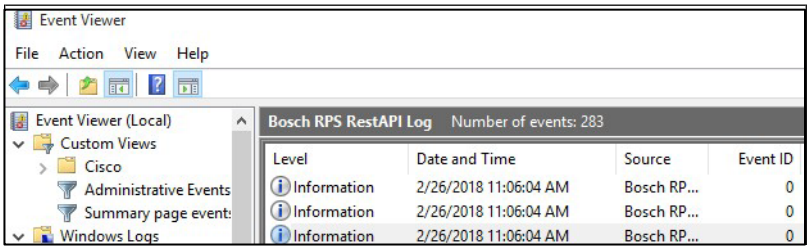
Image 6.2 Sample call using the baseURL set variable

7 Error log

RPS-API writes installation and run time information, warnings, and errors to the Windows Event Log (Bosch RPS RestAPI Log).

For troubleshooting purposes, the log configuration file is available for configuring where to log errors and the error level to log.

Use the Windows Event Viewer to view this information.



8 Error status definitions

The tables in this section contain HTTP and RPS error reference information.

8.1 HTTP error codes

HTTP Status	HTTP Methods	Error Message
(200) OK	ALL	SUCCESS – the entity body contains a representation of the requested resource.
(400) BAD REQUEST	ALL	Client Error – the request cannot be fulfilled due to bad syntax
(401) UNAUTHORIZED	ALL	Client Error – the request requires user authentication.
(403) FORBIDDEN	ALL	Client Error – the user is not allowed to perform the request.

8.2 RPS-API status codes

Error Code	Status Message
(0) SUCCESS	Request successful.
(20010) PANEL_NO_LOCK	Panel is not locked.
(20020) PANEL_PENDING	Panel has pending updates.
(20030) PANEL_PROCESSING	Panel is synchronizing.
(40110) UNAUTHORIZED_ACCESS	Authorization has been denied for this request
(40310) USER_HAS_NO_PERMISSION	User does not have permission to operate, please check the security level
(40320) IP_ADDR_BLOCKING	P Address is not allowed to access RPS-API.
(40050) NOT_SUPPORTED_SETTING	RPS-API Command is not supported by this panel model.
(40051) SETTING_INVALID	Setting is invalid and cannot be applied.
(40052) SETTING_OUT_OF_RANGE	Setting is out of range and cannot be applied.
(40053) SETTING_CONFLICT	Setting conflicts with another configured setting and cannot be applied.
(40054) ACTION_INVALID	JSON format is invalid and cannot be parsed or applied.
(40055) RPSAPI_START_SERVICE_FAILED	Starting the RPS-API service failed.
(40056) RPSAPI_READ_REGISTRY_FAILED	Reading the RPS-API registry failed.
(40057) RPSAPI_WRITE_ACTIVITY_FAILED	Writing the RPS-API activity log failed.
(40058) FILE_NOT_FOUND	Cannot find specific file.
(40060) RPS_VERSION_NOT_SUPPORTED	This version of RPS is not supported, please update.
(40062) DB_OPERATE_FAILED	Unable to connect to the database, please check the RPS settings.
(40070) PANEL_DOES_NOT_EXIST	Panel does not exist, please check panel GUID or name.
(40071) PANEL_OFF_LINE	Unable to connect to the panel.
(40072) PANEL_READ_ONLY	Panel is locked by another operator.
(40073) PANEL_NOT_SUPPORT	Panel is not supported, please check panel GUID or name.
(40074) AREA_NOT_EXISTS	Selected area does not exist in this control panel.
(40075) POINT_NOT_EXISTS	Selected point does not exist in this control panel.
(40076) USER_NOT_EXISTS	Selected user does not exist in this control panel.
(40077) PANEL_INTERNAL_EXCEPTION	Detected panel internal exception.

Error Code	Status Message
(40078) PANEL_DATA_LOCK	Configuration data for panel is locked.
(40079) POINTPROFILE_NOT_EXISTS	Selected point profile does not exist on this panel.
(40080) DATA_TYPE_NOT_MATCH	Requested data type does not match.
(40081) DATA_NOT_FOUND	Requested data is not found.
(40082) DATA_ALREADY_EXISTS	Data already exists.
(40083) PANEL_BUSY	Panel is updating, in use by another user or application.
(40084) PANEL_CONNECT_RETRY	Panel may not be able to connect, please retry.
(40085) OPERATOR_NOT_EXISTS	Operator setting was not found in database.
(40086) PASSCODE_NOT_MATCH	Requested passcode does not match.
(40087) SERVICE_STOPPED	Service is not running.
(40088) SERVICE_BUSY	Service is busy.
(40099) UNKNOWN_ERROR	Unknown Error, please check the event log.

9 Troubleshooting

9.1 RPS-API is updating the old RPS Database

If the RPS database is changed using the RPS system configuration utility, the API service(s) will require a reboot to connect to the new RPS database.

9.2 Cannot Edit User0 Authorities

User WRITE capabilities are restricted for User0 to ensure system access and authorities for this default user are maintained. For User0, Passcode, User Name, User Group and Language are available for edit.

9.3 Deleting users fails when passcode is left blank

When deleting a user, it is possible to include the user's passcode for verification. If the passcode is not going to be used, the full "user: { }" block should be omitted and only the user "index" number should be included in the panelUserList array.

For example, if deleting user 2, the body of the request should look like:

```
{
  "panelUserList": [
    {
      "index": 2
    }
  ],
  "priority": "HIGH"
}
```

9.4 RPS-API is not connecting to panels using TCP as expected

If Network Protocol details are changed using the RPS system configuration utility, the API service(s) will require a restart to connect using the new RPS settings.

Connections using TCP require control panel firmware 3.07 or higher and B465 communicator firmware 2.01 or higher. For environments that include lower firmware versions, connections will require the RPS Network Protocol set to TCP with fallback to UD or UDP only.

9.5 RPS-API requests to set Automation results in a "Value out of Range" error

Setting Automation requires that the target panel system support the configuration settings that are applied. Automation settings for GV3 panel systems are not available or supported.12

9.6 Client using HTTP to connect to RPS-API 2.2 version cannot reach server

If the client used HTTP to connect to the RPS-API version 2.2.27914, it will be unable to reach the server.

RPS-API version 2.2.27914 and higher requires HTTPS.

9.7 Connections to panels fail with TCP authentication message

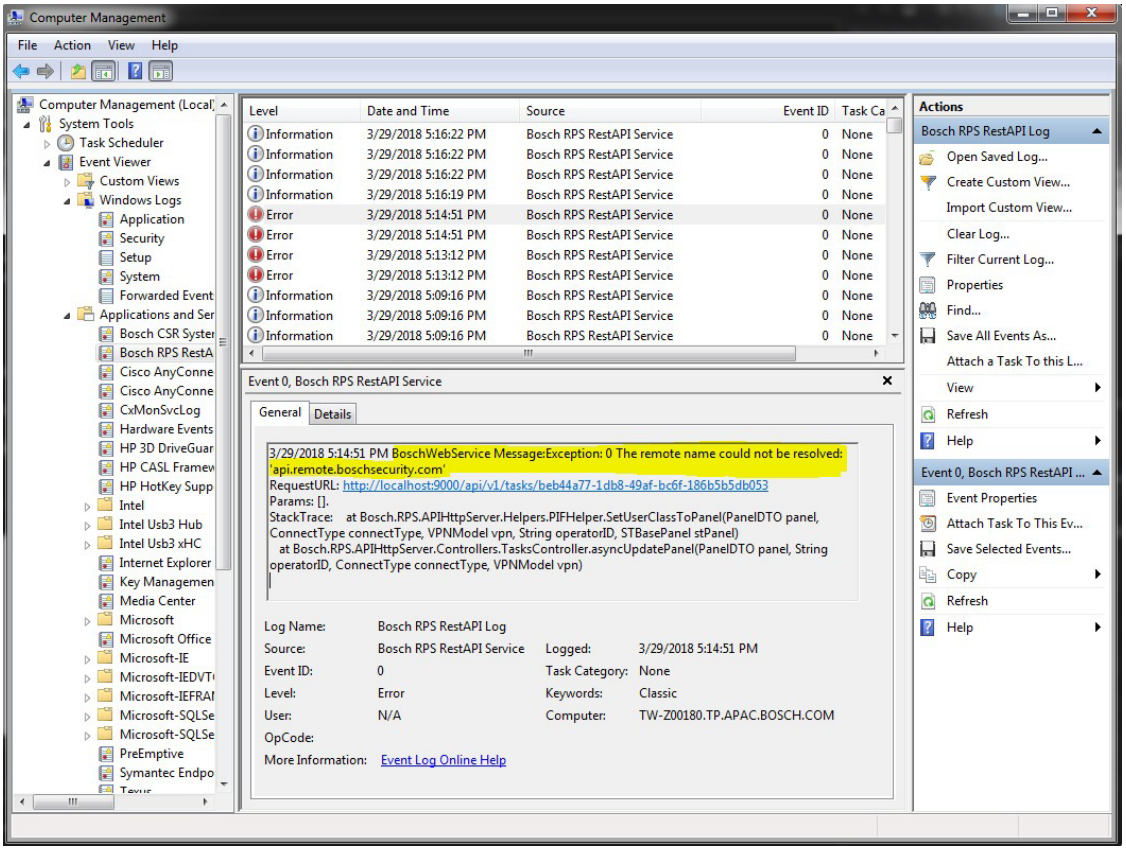
Update RPS to version 6.11 or higher or select the UDP only or TCP with fallback to UDP setting.

9.8 Cloud panel not updating

If a user cannot connect to the Cloud panel, then the Windows service is unable to connect to CBS via HTTPS. The user must have the proper permissions to use HTTPS or a specific account can be configured for the RPS-API service. See Figure 1 and 2 on the next page for examples.

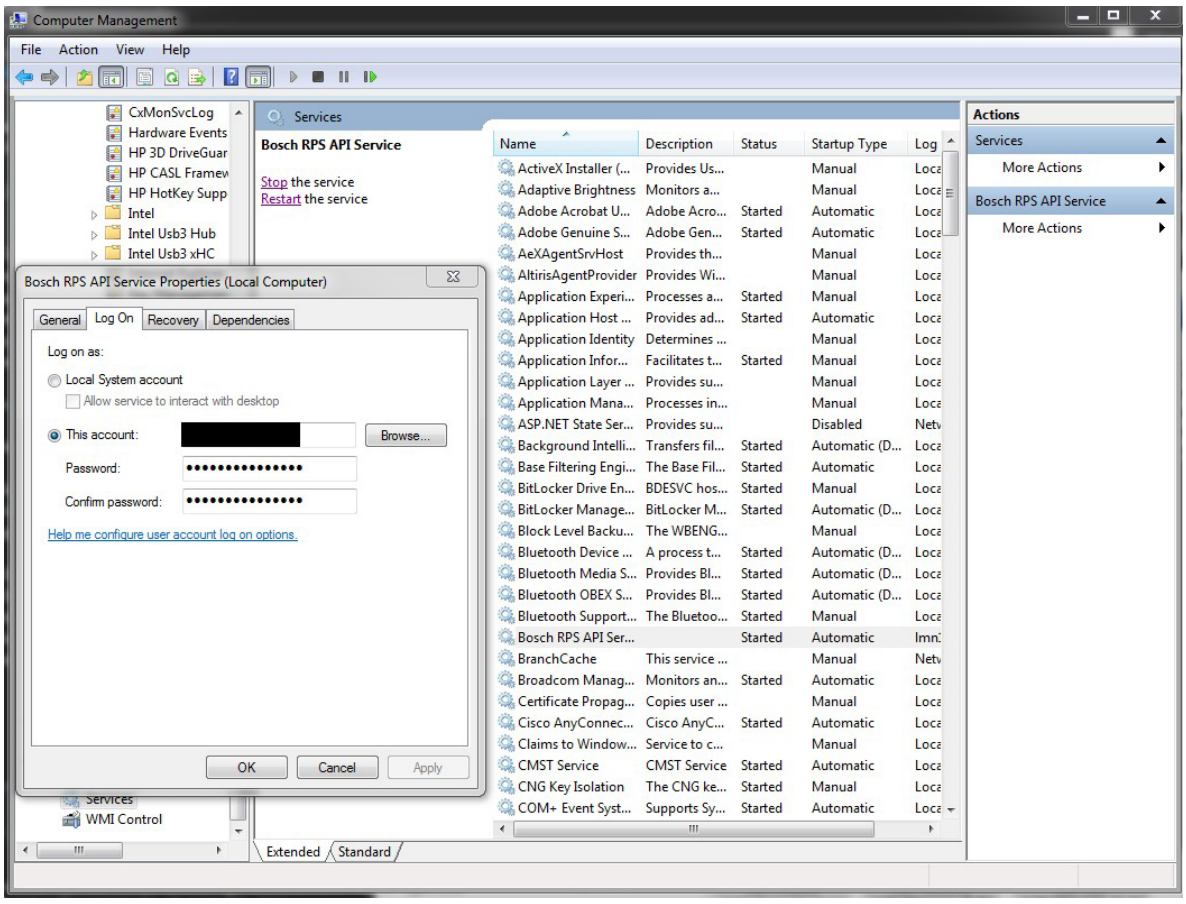
- If the RPS-API cannot update the Cloud panel, make sure that the Bosch RPS RestAPI Service has the proper permissions to use HTTPS.

Figure 1



- If the default Local System account does not have the correct permissions, you can configure the RPS-API service to use a specific account.

Figure 2



9.9 Self-signed certificate storage

RPS-API self-signed certificates are stored in this folder location:

C:\users\<name>\AppData\Roaming\Bosch RPS-API

9.10 Remove self-signed certificates

To remove sslceret and urlacl binding to the RPS-API, do 1 of these solutions:

- Solution 1 - manually use netsh to configure the sslcert and urlacl.
- Solution 2 - with administrator permission, access the Windows command prompt and run the HttsConfiguraiton.exe with the uninstall parameter:

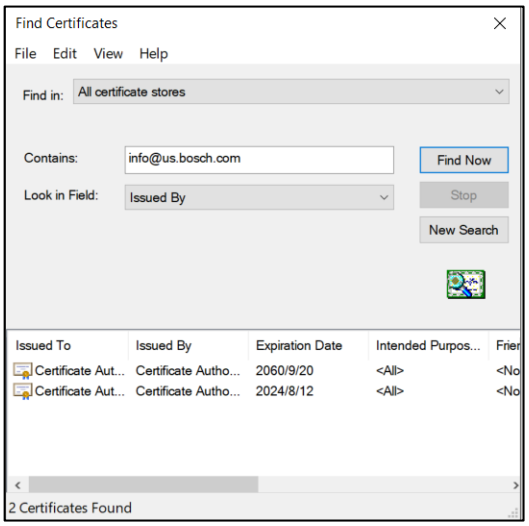
```
C:\Program Files (x86)\Robert Bosch\Bosch RPS API Service>.\HttpsConfigurationTool.exe uninstall
```

9.11 Delete certificates to downgrade RPS and RPS-API

Downgrading RPS-API/RPS is not typically recommended. If there is a reason to downgrade RPS to a version lower than 6.11 and RPS-API version 2.2.27914, use the steps in this section to manually remove the control panel connection certificates.

To remove certificates used for panel connection:

1. Open Windows search and type **Run**.
2. Type **mmc** and click **OK**.
3. In the File menu of the Console window, select **Add/Remove Snap-in**.
4. Select **Certificates** and click **Add**.
5. Select **Computer account.**
6. Click **Finish** and **OK**. The application will show the installed certificates.
7. In the tree, right-click **Certificates (Local computer)**, select **Find Certificates**.
8. Search for **info@us.bosch.com** in the Issued by field. There should be 2 certificates found.
9. Right-click the certificates and select **Delete** to remove them.
   Note: New certificates will be installed with RPS version 6.11 or higher and RPS-API version 2.2.x or higher.



9.12 Updated panel IP address is not being used during the panel connection

If you change a panel IP address and then immediately connect to the panel, in some cases the API will continue to use the previous IP address of the panel. To correct this, restart the RPS-API.

Bosch Security Systems B.V.
Torenallee 49
5617 BA Eindhoven
Netherlands
www.boschsecurity.com