

Whitepaper


Remote Programming Software Secure Installation

Overview

This white paper provides basic to advanced best practices to assist customers that wish to secure their RPS installation(s) and access for RPS operators to program panel systems.

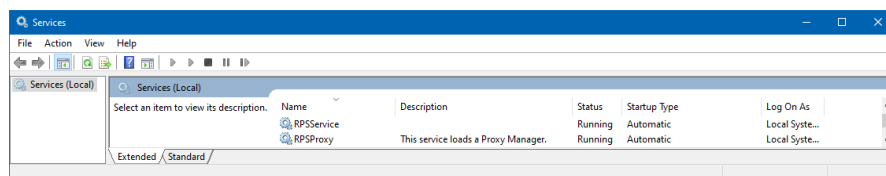
Best practices include controls that limit RPS application permissions, operator access and RPS feature use as well as the ability to access a panel system and perform panel programming.

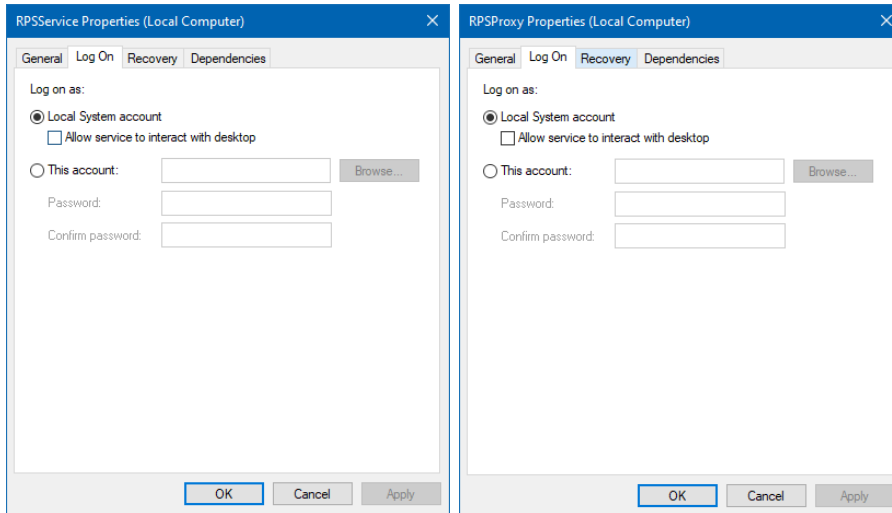
Implementation of these controls includes using and applying minimum security levels to:

- 1.) RPS Windows services user (Figure X) During RPS install, an RPSSvc windows user will be created with the minimum permissions required to run and operate RPS. If this is unsuccessful, RPS will log any failures and assign the Windows System user to start the RPS services.
- 2.) RPS Operators (Figure 1) In RPS, go to Lists >Operators, and click  (New icon) in the toolbar.
- 3.) RPS application features using the RPS System Configuration settings. (In RPS, go to Config>Workstation Specific>Security) (Figure 2)
- 4.) RPS Operator Password Policy (Figure 2 and Figure Y) In RPS, go to Config>System>Work Station Specific>Security>RPS Operator Password Policy
- 5.) RPS programming parameters using Panel View> Security settings. This granular level of Security is first enabled by first selecting Edit>Security inside the panel record. Specific View and Edit restrictions can be applied by selecting <F5> while in a specific programming parameter field. (Figure 3.1 and Figure 3.2)

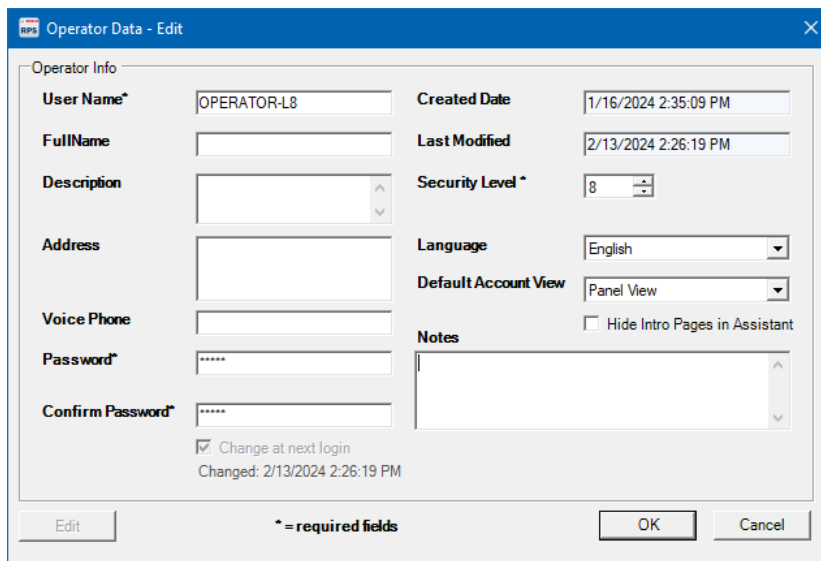
When minimum security levels are applied to an RPS application feature or applied to a panel programming parameter, only RPS Operators with the same Security Level (or higher) will be allowed to access that application feature or be able to view or edit that panel programming.

(Figure X) Start>All apps>Windows Administrative Tools>Services

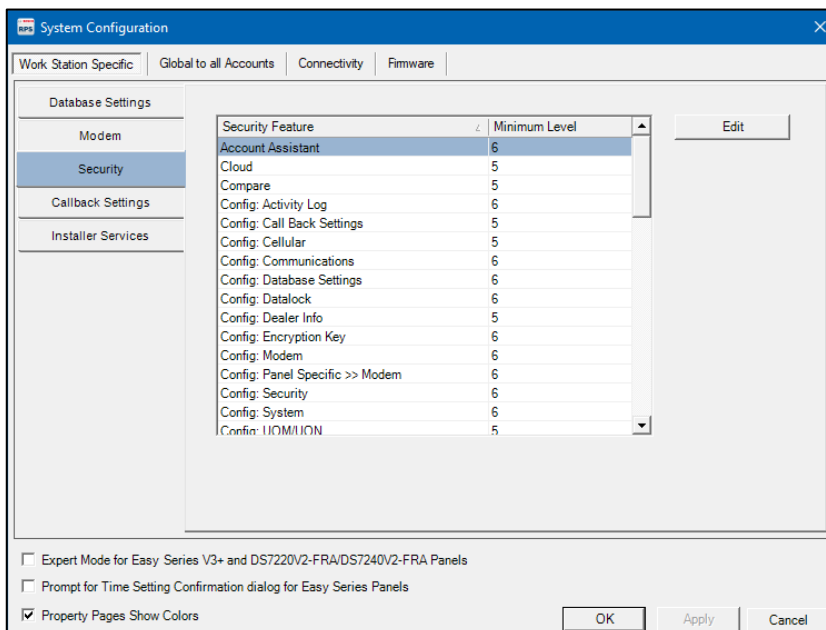




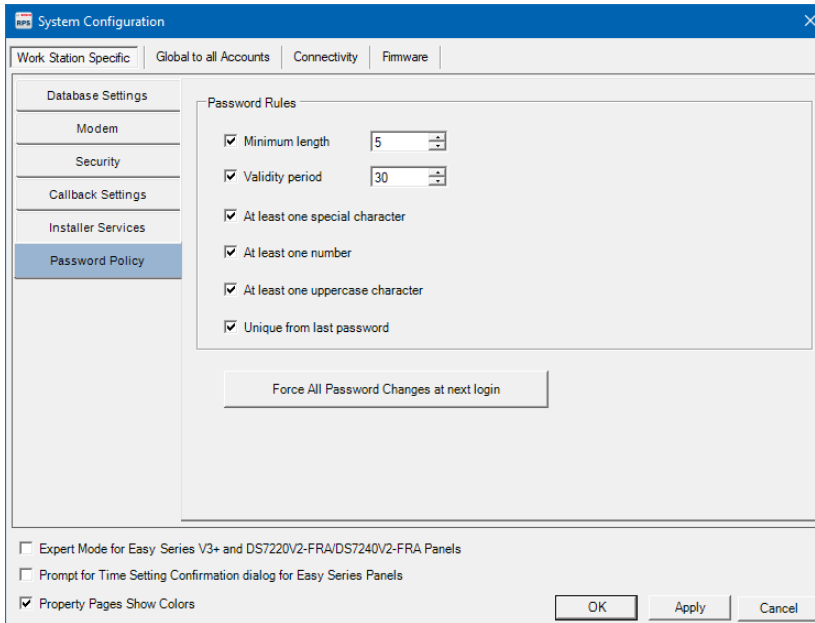
(Figure 1) Lists>Operators>  (New icon)



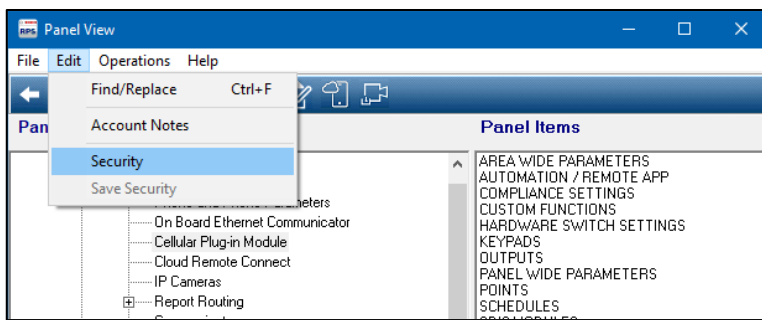
(Figure 2) Config>Work Station Specific > Security



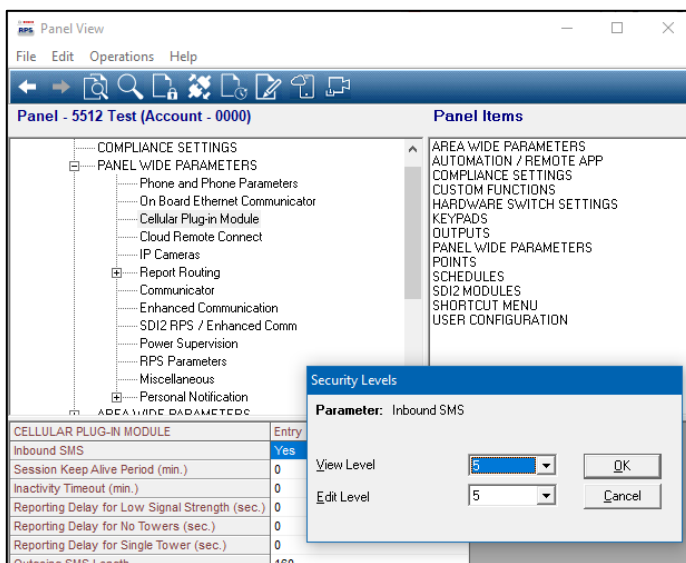
(Figure Y) Config>Work Station Specific>Security>RPS Operator Password Policy



(Figure 3.1) Open Panel View > Edit > Security



(Figure 3.2) Example: Panel Wide Parameters>Inbound SMS parameter, press F5



1.) Control the start, stop of the RPS Windows Services

Allow RPS install to create a local Windows user to start/stop services

- RPS installer will create local windows user with limited permissions
- RPS installer will assign RPSSvc user to start/stop RPSProxy Windows service
- RPS installer will assign RPSSvc user to start/stop RPSService Windows service

Create and assign a Windows user to start/stop RPS services

- Create your own local Windows or Domain user with the required Windows permissions (see RPS Help)
 - Use Windows Users and Groups to establish a Windows user with local permissions.
- Assign the Windows user to start/stop RPSProxy Windows service.
 - Edit the service Logon as user in Windows by going to Start>All apps>Windows Administrative Tools>Services>RPSProxy
- Assign the Windows user to start/stop RPSService Windows service
 - Edit the service Logon as user in Windows by going to Start>All apps>Windows Administrative Tools>Services>RPSService

2.) Control the ability to access, use RPS application features

Control who can log into RPS

- Limit RPS software install locations
- Change the RPS software default administrator account and password
- Do not have users share RPS Operator accounts to log in
- Create individual RPS operator accounts for each intended user

Control who can create and modify other RPS Operators

Apply limits to who can manage RPS Operators using the RPS System Configuration, Security Minimum Level settings. Set the minimum security level of these specific settings higher than the Security Level of any RPS Operators you do not want to have access. In RPS, go to Config>System>Work Station Specific>Security:

- Lists: Operators, Delete
- Lists: Operators, New
- Lists: Operators, View/Edit

Control which application settings operators can see in RPS

Limit what settings the RPS Operators can control by applying Security Level(s) to each RPS Operator account and configuring minimum level (Min Level) parameters to specific RPS Application Settings. Configure your RPS Operators with lower security level(s) than the RPS application features you do not want them to have access to use. In RPS, go to Config>System>Work Station Specific>Security to modify these parameters.

3.) Control the ability to access, modify panel accounts

Control who can use RPS to add, delete, view/edit panel accounts

Restrict the viewing of panel record lists to specific RPS Operators only. Change the Min Level to higher than the RPS Operators you want to restrict. The default level is 5. In RPS, go to Config>System>Work Station Specific> Security:

- Lists: Panels, Delete

- Lists: Panels, New
- Lists: Panels, View/Edit.

Control who can use RPS to create or export panel accounts

Restrict the ability to export and/or backup panel accounts to specific RPS Operators only. Change the Min Level to higher than the RPS Operators that you want to restrict. The default level is 5. In RPS, go to Config>System>Work Station Specific>Security:

- Lists: Panels, Backup/Restore
- File: Import/Export

Control who can use RPS to connect to panel accounts

- Modify your RPS Operator security level to restrict your RPS Operators from viewing panels. Change the Min Level to higher than the RPS Operators that you want to restrict from connecting to panels. The default level is 5. In RPS, go to Config>System>Work Station Specific>Security>Lists: Panels, View/Edit.
- Limit the panel to only accept RPS connections from a specific RPS workstation IP address. In RPS, open the panel programming using Panel Wide Parameters>SDI2 RPS/Enhanced Communication>RPS Address Verification and change the parameter to **Yes**. Enter the RPS workstation IP address in the IP Network Address parameter.
- Require a manual keypad confirmation for each remote RPS connection. In RPS, open the panel programming and set the Panel Wide Parameters>SDI2 RPS/Enhanced Communication>Answer RPS Over Network? and change the parameter to **No**. Future RPS connection attempts will require keypad confirmation using local keypad menu selection Actions>RPS>Answer.
- Restrict which Panel Users are allowed to use the keypad to confirm a remote RPS connection. In RPS, open the panel programming to set the User Configuration>Authority Levels>Remote Program and set the security/authority level to the level higher than the Authority Level assigned to Panel Users you want to restrict.
- Maintain the RPS passcode as a panel unique, non-default passcode.
- Establish non-default Datalock codes. In RPS, go to Config>System>Global to all Accounts>Datalock.
- Do not provide USB security dongles for G Series panels. Without a USB Security dongle, RPS will not be able to connect to G Series panels.

Control RPS Operator Passwords

- Modify your RPS Operator security level to restrict which RPS Operators can manage the RPS Operator Password Policy. . Change the Min Level to higher than the RPS Operators that you want to restrict from managing the Policy. In RPS, go to Config>System>Work Station Specific>Security>RPS Operator Password Policy
- Use the RPS Operator Password Policy to enforce password rules and your desired level of complexity
- Use a Validity period rule to require RPS Operators change their password regularly.
- Use the “Force All Password Changes at next logon” when setting / updating a password policy to ensure all existing Operators are covered by the Policy.
- If an RPS Operator forgets their password, an administrator is required to provide a new password to the RPS Operator.

Control who can see RPS passcodes

- Limit RPS Operators from viewing and or editing the RPS Passcode used to connect to Panels by modifying the required security level. In RPS, open the panel programming and use the enhanced security settings <F5> to set the View/Edit security levels of Panel Wide

Parameters>RPS Parameters>RPS Passcode to a higher level than the RPS Operators you want to restrict.

Control how panel users passcodes can be modified

- Limit RPS Operators who can edit user passcodes. In RPS, open panel programming and use the enhanced security settings <F5> to set the View security levels of User Configuration>User Assignments [Passcodes]>Passcode to a higher level than the RPS Operators you want to restrict.
- Limit RPS Operators from seeing Panel User Passcodes. In RPS, go to Config>System>Work Station Specific>Security>Mask User Passcodes and change the security level to a higher level than the RPS Operators you want to restrict.
- Allow / Remove permission for Panel users to change their passcode.

Control which panel users can create/set/enable other panel users and passcodes

- Limit Panel Users that are allowed to create or edit other panel users and passcodes. In RPS, open panel programming and set User Configuration>Authority Levels>Add User Passcode/Card/Level and Delete User Passcode/Card/Level parameters. Enable these only for Authority Levels higher than the Panel Users you wish to restrict.

4.) Other resources/options

- Access the help system and F1 context sensitive help available in RPS.
- Use RPS-LITE as an alternative to RPS to limit what options and access Operators have available
- View the [Panel Account Security](#) video and other online resources.
- When installing RPS with SQL Express to use SQL Server Authentication, set a unique password for your sa account.
 - Starting with RPSv6.11, new installations can use the RPS default or create your own custom SQL sa passcode.

Bosch Security Systems B.V.

Torenallee 49

5617 BA Eindhoven

Netherlands

www.boschsecurity.com

© Bosch Security Systems B.V., 2024