SV2 Series Security Manual

PRODUCT DATA SHEET

INTRODUCTION

This document provides security information for the SV2 Series valves and accessories.

Other applicable publications are:

- 32-00029, SV2 Series User Manual
- 32-00031, HMI/PC Tool User Manual
- 32-00241, User Interface EULA License

Physical device Protection

⚠ CYBER SECURITY NOTICE

SV2 Series products contain electronics and software. Care should be taken by the installer / facility management to guard against unauthorized access to the valve and to the programming interface for parameter modification (if applicable).

Unauthorized access to change the valve wiring interface, replace parts, change device hardware or software should not be permitted. Failure to do so may pose a safety risk.

A tamper evident label has been placed inside the valve electrical enclosure to indicate if access has occurred. The label resides between the valve main electronics assembly and the electrical enclosure which houses it.

NOTE: The valve main electronics assembly is field replaceable and as such, this seal must be broken in order to replace it.

The SV2 series valves are designed to provide various security features to avoid being misused remotely. However, it is important to remember that physical security is absolutely essential to avoid many local threats.

When installing a device, always select a physical location with limited or even restricted access. It is recommended to lock the device in an enclosed cabinet with access allowed only to approved and trained personnel.

Also, it is strongly advised to keep all the wiring of the device physically secure. An example of correct and incorrect wiring is shown in Fig. 1.

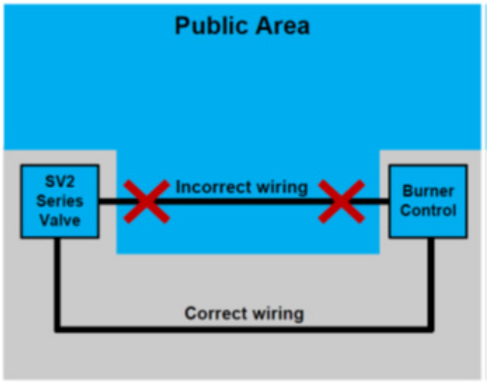
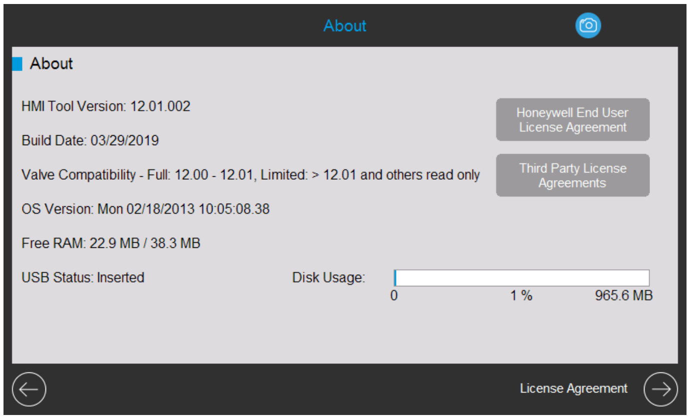


Fig. 1. Correct and incorrect wiring examples

⚠ CAUTION

When wiring is unsecured, an unauthorized person might tamper with wiring of the device, resulting in dangerous behavior. This rule applies to SV2 Series products specific wiring, but also applies to any other controlled equipment.

NOTE: This product may contain or be derived from materials, including software, of third parties. The third party materials may be subject to licenses, notices, restrictions and obligations imposed by the licensor. The licenses, notices, restrictions and obligations, if any, may be found in the materials accompanying the product, in the documents or files accompanying such third party materials, in a file named third_party_licenses on the media containing the product, or at http://www.honeywell.com/ps/thirdpartylicenses.


About
Honeywell End User License Agreement
Third Party License Agreements
License Agreement

About

HMI Tool Version: 12.01.002

Build Date: 03/29/2019

Valve Compatibility - Full: 12.00 - 12.01, Limited: > 12.01 and others read only

OS Version: Mon 02/18/2013 10:05:08.38

Free RAM: 22.9 MB / 38.3 MB

USB Status: Inserted

Disk Usage: 0 1 % 965.6 MB

Fig. 2. About page with license agreements.

SV2 Series Accessory Modules

The SV2 Series valves support connection of accessory modules providing advanced functionality. They include the Fuel/Air Ratio Module and Pressure Module. These modules utilize external wiring, which once tampered with, might affect device functionality in a dangerous way, limit it or completely disable it.

Although it might not be obvious, the Fuel/Air Ratio Module also utilizes external piping, which in case of unauthorized modification, might cause device failure.

MODBUS® COMMUNICATION

For SV2 Series configuration and device monitoring, Modbus communication utilizing an RS-485 BUS is used. This communication requires special attention when it comes to security.

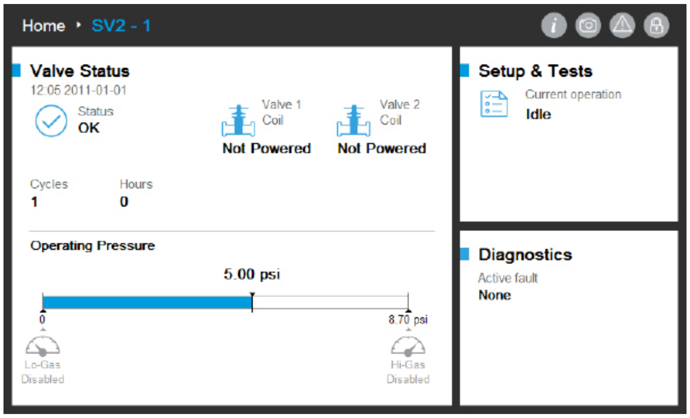
Secure vs. Unsecure Communication

Modbus protocol from its nature is unsecure and does not provide any native means for security, however SV2 Series running firmware version 10 and later supports Secured Modbus, which is a Honeywell proprietary extension of the standard protocol.

Secured Modbus supports integrity validation of messages so they cannot be tapered by anyone accessing the RS-485 conduit. However, this protocol does not protect device data against reading by unauthorized personnel.

Session Management

The SV2 Series valves and HMI/PC Tools support a secured session when Secured Modbus is used. This means that when the user logs in with a password for either the Installer or OEM access levels, a secured tunnel is established between the user HMI/PC client application and the SV2 Series valve. Refer to Figs. 2-4.



Valve Status 12:05 2011-01-01

Status OK

Valve 1 Coil Not Powered

Valve 2 Coil Not Powered

Cycles 1

Hours 0

Operating Pressure 5.00 psi

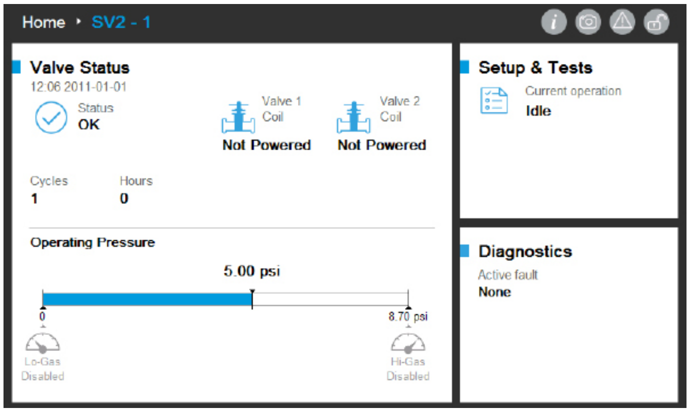
Lo-Gas Disabled

Hi-Gas Disabled

Current operation Idle

Active fault None

Fig. 3. Session is not established. User is not logged in.



Valve Status 12:06 2011-01-01

Status OK

Valve 1 Coil Not Powered

Valve 2 Coil Not Powered

Cycles 1

Hours 0

Operating Pressure 5.00 psi

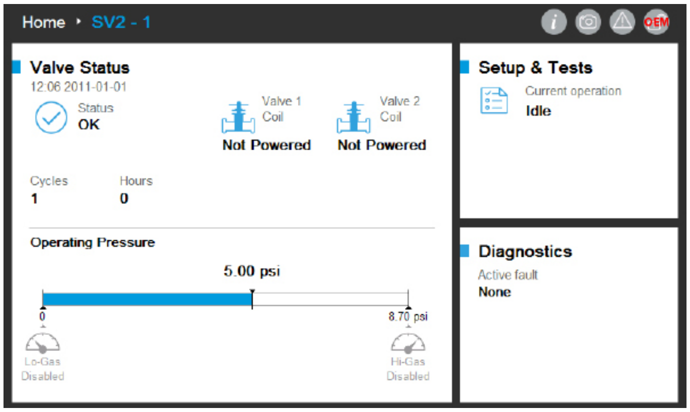
Lo-Gas Disabled

Hi-Gas Disabled

Current operation Idle

Active fault None

Fig. 4. Session is established. User is logged as Installer.



Valve Status 12:06 2011-01-01

Status OK

Valve 1 Coil Not Powered

Valve 2 Coil Not Powered

Cycles 1

Hours 0

Operating Pressure 5.00 psi

Lo-Gas Disabled

Hi-Gas Disabled

Current operation Idle

Active fault None

Fig. 5. Session is established. User is logged as OEM.

A session has to be established and used to be able to make any changes to the valve configuration. For instance, typical configurations are:

1. Safety verification of critical configuration data
2. Premix valve configuration commissioning
3. Pressure Module configuration
4. Security configuration (password setup, access privileges modification)
5. Proof of closure configuration
6. Valve Proving Sequence
7. Units (Pressure, Volume and Leakage)
8. Valve General settings (Modbus Address, Baud Rate)

NOTES:

- Only one session can be active at a time. In other words, when one user is logged in, another needs to wait until the previous session is terminated.
- A secured session is terminated if no secure communication is received within 20 seconds after the last secure message.
- A secured session is terminated by the SV2 Series HMI/ PC Tool if the user is inactive longer than 10 minutes.

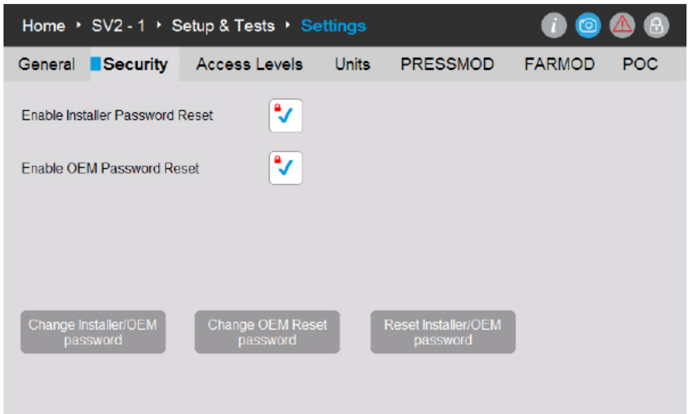
Password / Key Management

A password is the phrase or string of characters which need to fulfill the following rules:

- At least twelve characters long
- At least one capital and one lower case letter
- At least one number
- No special characters

The SV2 Series valves are shipped with default OEM and Installer passwords pre-configured. These passwords have to be changed before the valve can be used in an application without user observation.

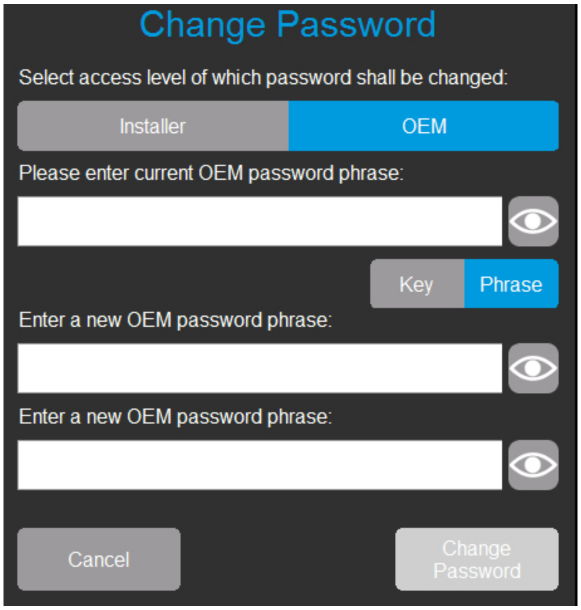
Forgetting to change the default password results in persistent lockout when the secured session is terminated. This is a security measure that avoids using a valve in unsecure mode (without proper password configuration). Refer to Figs. 5-8.


Home ‣ SV2 - 1 ‣ Setup & Tests ‣ Settings
General
Security
Access Levels
Units
PRESSMOD
FARMOD
POC
Change Installer/OEM password
Change OEM Reset password
Reset Installer/OEM password

Enable Installer Password Reset ☑

Enable OEM Password Reset ☑

Fig. 6. **OEM, OEM Reset and Installer passwords can be changed on Security page.**


Change Password

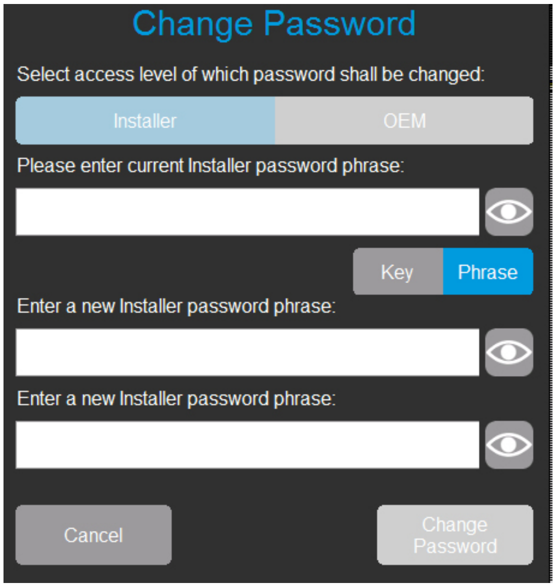
Select access level of which password shall be changed:

Please enter current OEM password phrase:

Enter a new OEM password phrase:

Enter a new OEM password phrase:

Fig. 7. **User logged in as OEM can change Installer or OEM password. User enters current OEM password and new password twice.**


Change Password

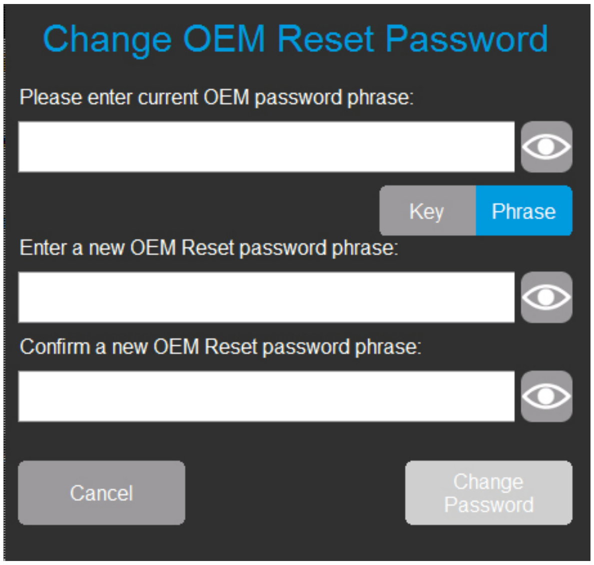
Select access level of which password shall be changed:

Please enter current Installer password phrase:

Enter a new Installer password phrase:

Enter a new Installer password phrase:

Fig. 8. User logged in as Installer can change only Installer password. User enters current Installer password and new password twice.


Change OEM Reset Password

Please enter current OEM password phrase:

Enter a new OEM Reset password phrase:

Confirm a new OEM Reset password phrase:

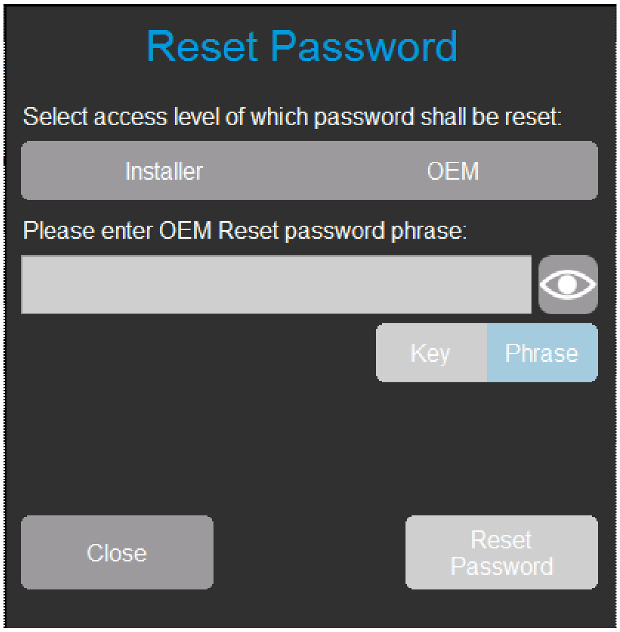
Fig. 9. User logged in as OEM can change also OEM Reset password. User enters current OEM password and new OEM Reset password twice

Password Reset

Should the Installer and/or OEM main access level passwords be lost, password reset is possible, if the reset mechanisms were enabled by the OEM. Refer to Fig. 5. The reset mechanism will vary between the Installer and OEM levels. Note that cycling of the valve or user interface power will not defeat this methodology.

The password reset mechanism simply allows the appropriate user to reset the current password(s) back to the Honeywell factory default value(s). Once the password(s) are reset, the user can then log in and assign new password(s).

After reset to the default value, if the OEM + Installer main and OEM reset passwords are not set to new non-default values, the valve will be in lockout status and will not be operational unless the OEM user is logged in. The applicable password(s) must be configured in order to clear the fault code(s).


Reset Password

Select access level of which password shall be reset:

Please enter OEM Reset password phrase:

Fig. 10. Unlogged user selects Access Level of password to be reset. User enters valid reset password phrase.

By default, the password reset feature for both the Installer and the OEM is disabled and has to be enabled upon initial configuration of every device by the OEM or original owner as indicated in Fig. 5.

NOTES:

- **The OEM can choose to enable or disable the OEM password reset function. Refer to Fig. 5.**
  - **If it is enabled the main OEM password is lost, the OEM can reset the passwords back to the Honeywell factory defaults and re-assign new passwords**
  - **If it is disabled and the main OEM password is lost, the OEM will not be able to reset the password and will effectively be locked out of editing the valve at the OEM level.**
  - **If the Installer level main password is known, the OEM can access the valve using it and edit the parameters to which they have granted the Installer access.**
  - **In order to make OEM level editing possible again, the valve main electronics would have to be replaced and the valve completely re-programmed at both the OEM and Installer levels.**

Password Protection

To avoid the chance that a session password is guessed by random attempts, all passwords are protected by a brute-force detection mechanism. This mechanism temporarily disables the login to the affected account and valve. The devices either need to be power-cycled or the person logging in has to wait at least one minute before the next attempt.

If this occurs, faults will be annunciated on the HMI/PC Tool Diagnostics page. There are four possible fault codes associated with this instance:

- Installer account temporarily disabled
- OEM account temporarily disabled
- Installer password reset feature temporarily disabled
- OEM password reset feature temporarily disabled

Best Practices

It is recommended to always use strong, hard-to-guess passwords. Please refer to the Password / Key Management section earlier in this document.

Account Management

There are two user accounts implemented in the SV2 Series valves. These accounts are:

1. Installer
2. OEM

The Installer account is considered to be subsidiary to the OEM account. In other words, all features accessible by the Installer can be controlled by the OEM.

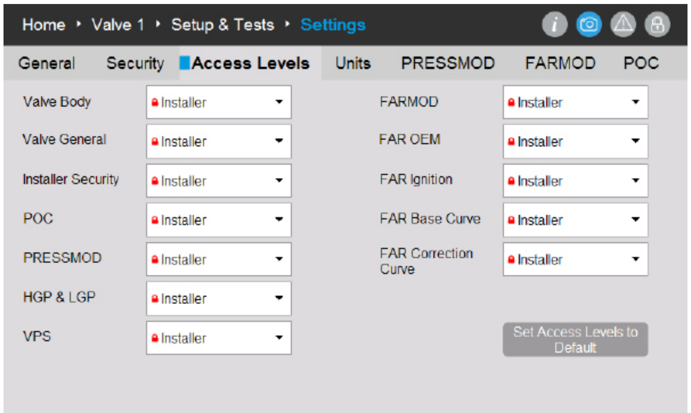
In contrast, features accessible by the OEM can be used by the OEM only.

User accounts cannot be removed or added and their intended purpose is as follows:

1. OEM account is used to configure critical valve features such as configuration of the Pressure Module, the Fuel/Air Module, Fuel/Air ignition and Fuel/Air base curves.
2. Installer account is used to configure less critical features such as functional limits or application specific variables.

Access Management

By default, access privileges are configurable for every critical feature. The default user level for all safety features is configured to Installer and should be raised to the OEM user level based on application specifics. Configuration can be done using the Honeywell HMI Tool or PC Tool as indicated in Fig. 11:


Home ‣ Valve 1 ‣ Setup & Tests ‣ Settings
General
Security
Access Levels
Units
PRESSMOD
FARMOD
POC
Set Access Levels to Default

Valve Body	Installer	FARMOD	Installer
Valve General	Installer	FAR OEM	Installer
Installer Security	Installer	FAR Ignition	Installer
POC	Installer	FAR Base Curve	Installer
PRESSMOD	Installer	FAR Correction Curve	Installer
HGP & LGP	Installer		
VPS	Installer		

Fig. 11. Access Levels page. Each configuration group could be set to Installer, OEM or Read-Only.

Remote Connection Security vs. Physical Security

To keep remote connection via communication secured, it is important to consider the following items which apply mainly for initial device configuration:

- When device is physically accessible to a potential attacker, the Installer reset password can be obtained by the attacker by reading it from the sticker on the back side of the valve's main electronics assembly and later used.
- When a session is established using the default password in the valve, it can never be considered as secure. It is recommended that initial passwords for the OEM and the Installer accounts be set with no other devices present on the RS-485 network on which the valve in connected.

HMI AND PC TOOLS

To keep the SV2 Series valves and the user interface tools secure it is essential to provide reliable and secure user access to them. For that reason, several security measures should be used with the PC Tool and HMI Tool as described below.

HMI Security

Any standalone SV2 Series HMI should always be kept physically secure; the same physical security recommendations apply to it as for the SV2 Series valve. Refer to the Physical Device Protection section earlier in this document.

PC Tool Security

The PC Tool is designed to run on computers with Microsoft® Windows operating systems. When connecting a computer to an SV2 Series valve, any applicable PC security issues might pose a security risk to the valve. For that reason, it is always recommended to follow security practices as outlined below:

1. Always use an operating system supported by Microsoft.
2. Always keep the system updated with the latest security patches.
3. Aways have antivirus software and a firewall installed and up to date.
4. Use the whitelisting feature enabled in the PC's operating system.
5. Never use applications from an unreliable source or cracked applications.
6. Make sure that USB drives or any other accessories connected to the PC come from a reliable source and do not contain harmful hardware or software (e.g. key loggers, memory scanners, etc).
7. Disable all unnecessary services, ports and user accounts on the PC to avoid remote attack.

An installer file or application binary file is signed by a Honeywell key to provide assurance that the PC Tool installer/application is coming from a verified source. However, although the signature is providing a good level of security, it is always recommended to use only the PC Tool installer/application provided directly by Honeywell or an authorized Honeywell OEM/Installer.

PC Tool Security Checklist

To safely use this application, please ensure that you meet the following:

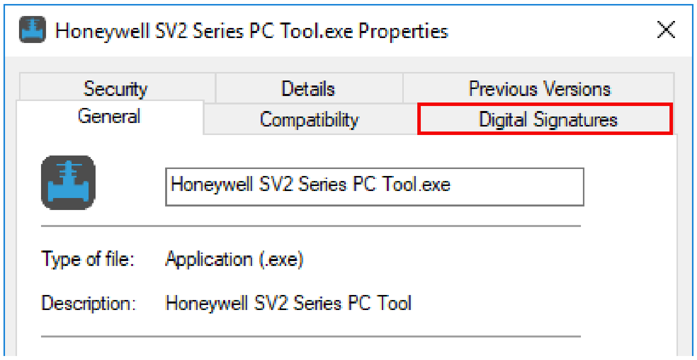
1. You are using only a trusted, signed application (see section Application Origin verification)
2. If possible use whitelisting of applications (see section Whitelisting Applications)
3. You are using antivirus protection along with a properly configured firewall if the PC is connected to the internet.
4. Ensure the PC which you run the application on has password protection so unauthorized personnel cannot use it.
5. Ensure that physical access by unauthorized personnel to your system is eliminated or limited (PC -> RS485 -> Modbus -> SV2 Series Valve).
6. The PC Tool should automatically be installed in the Microsoft Windows ` Program Files' standard folder. This installation location is pre-selected in the PC Tool installer. If a different installation location is selected, the user shall configure the security permissions (e.g. to administrator) to ensure that the PC Tool installation will not be tampered with by unauthorized personnel.

PC Tool Installer/Application Origin Verification

The installer/application is provided with a digital signature. This signature will be checked after downloading a new version of the installer/application, or if any suspicion is present about the installer's/application's origin.

The signature can be checked by following these steps:

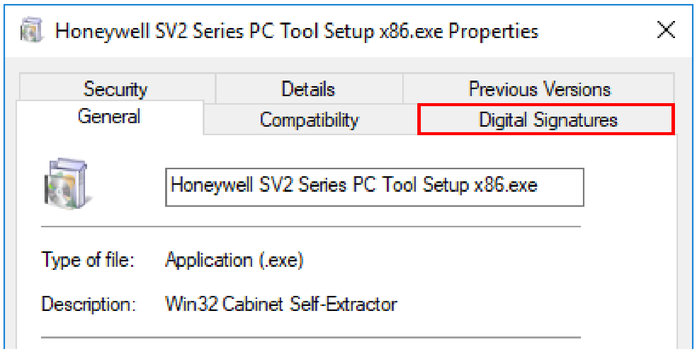
1. Click on the "Honeywell SV2 Series PC Tool Setup x86.exe" / "Honeywell SV2 Series PC Tool Setup x64.exe" / "SV2 Series PC Tool.exe" with right mouse button, and click "Properties"
2. Extract contents of "usb_root.zip" and click on the "app.exe" with right mouse, and click "Properties".
3. On Properties window click "Digital signatures". If tab is not present, jump to step 5).



Honeywell SV2 Series PC Tool.exe

Type of file: Application (.exe)

Description: Honeywell SV2 Series PC Tool

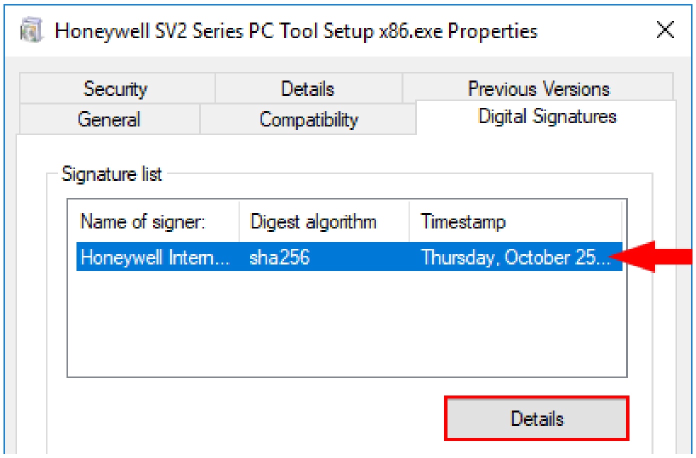


Honeywell SV2 Series PC Tool Setup x86.exe

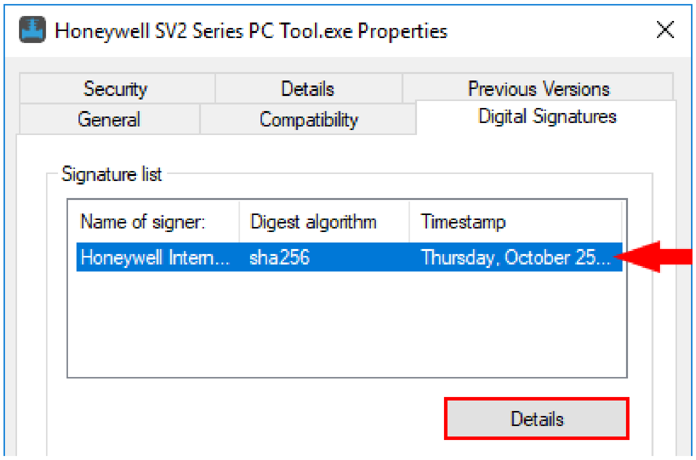
Type of file: Application (.exe)

Description: Win32 Cabinet Self-Extractor

4. On “Digital signatures” tab, the only item in “Signature list” should be Named “Honeywell International Inc.” Click on the item, and click the “Details” button.

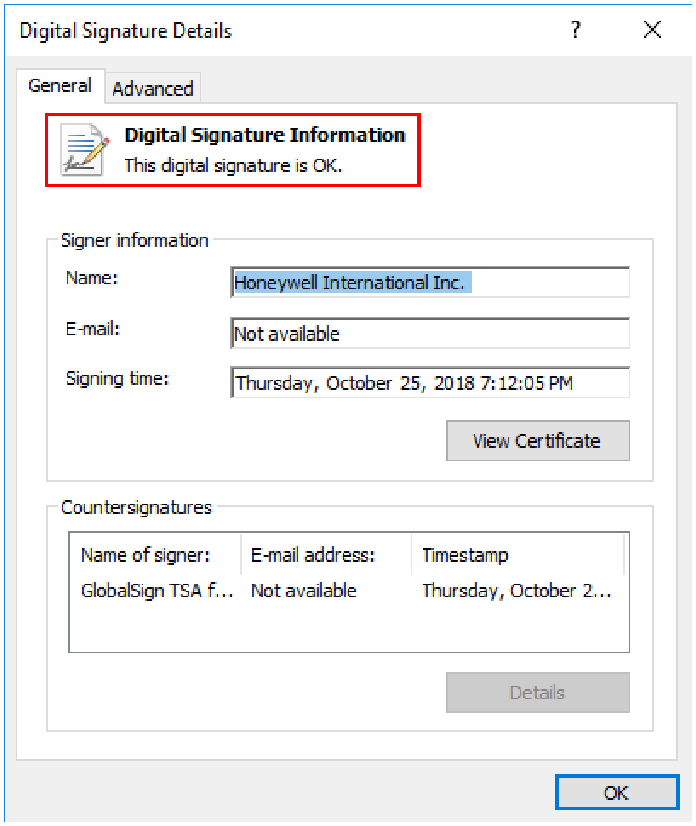


Name of signer:	Digest algorithm	Timestamp
Honeywell Intern...	sha256	Thursday, October 25...



Name of signer:	Digest algorithm	Timestamp
Honeywell Intern...	sha256	Thursday, October 25...

5. On the “Digital Signature Details” window, check the “Digital Signature Information”. It should say “This digital signature is OK.”



Digital Signature Information

This digital signature is OK.

Signer information

Name: Honeywell International Inc.

E-mail: Not available

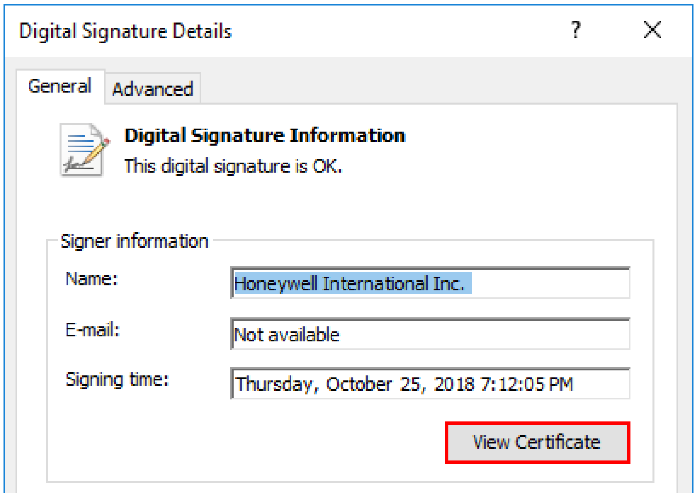
Signing time: Thursday, October 25, 2018 7:12:05 PM

Countersignatures

Name of signer:	E-mail address:	Timestamp
GlobalSign TSA f...	Not available	Thursday, October 2...

6. If the signature is not OK, or even not present (in step 2 no digital signature tab), the application is not trusted, and should be deleted. A new, clean copy can be downloaded from the original source.

7. Additionally, if you want to check the certificate’s details, click the “View Certificate” button.



Digital Signature Information

This digital signature is OK.

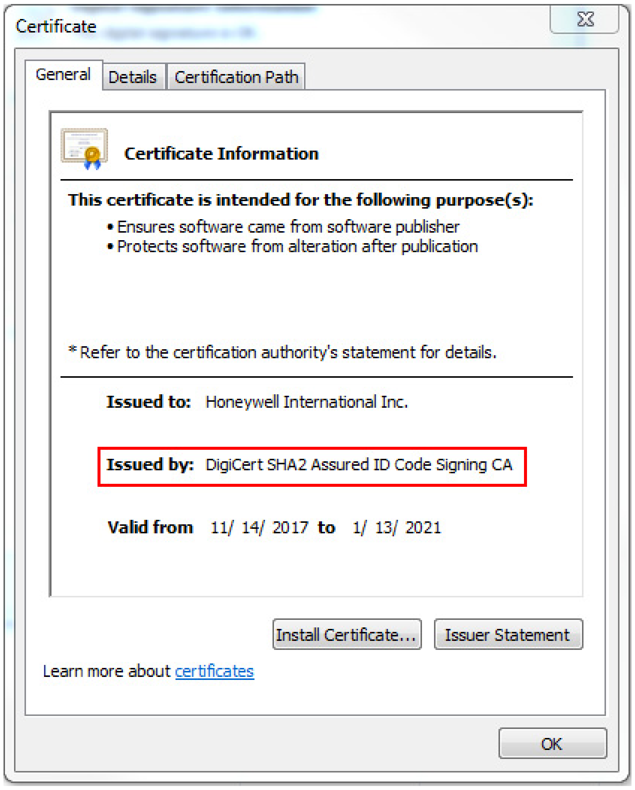
Signer information

Name: Honeywell International Inc.

E-mail: Not available

Signing time: Thursday, October 25, 2018 7:12:05 PM

8. The line “Issued by” in certificate’s details must contain “DigiCert”, which is the name of the certificate provider’s name.



Certificate Information

This certificate is intended for the following purpose(s):

- Ensures software came from software publisher
- Protects software from alteration after publication

* Refer to the certification authority's statement for details.

Issued to: Honeywell International Inc.

Issued by: DigiCert SHA2 Assured ID Code Signing CA

Valid from 11/ 14/ 2017 **to** 1/ 13/ 2021

Learn more about certificates

Whitelisting Applications

Whitelisting allows the administrator to set a list of wanted applications. Applications that are not on this list are not allowed to run. Setting up whitelisting highly increases your security, and minimizes the risk of running unintentional software on your machine. Whitelisting is available as a built-in tool in Windows operating systems (Windows 7, Windows 8), or can be done by third party software.

Crash Report

When the HMI or PC Tool unexpectedly crashes, a crash report is created. The PC Tool crash reports are located at C:\Users\<user>\Documents\Honeywell\SV2 Series PC Tool\Crash reports\. The HMI Tool crash report is accessible from the Home/Display Setup/About page. Refer to Fig. 2. The crash report contains the following information:

- PC Tool version and configuration
- Microsoft Windows OS version
- Microsoft .NET framework version
- Exception and stack trace
- List of available COM ports
- Full valve(s) configuration

For more information on this product and the entire SV2 Series product line, please refer to the SV2 Series User Guide located on our website at https://combustion.honeywell.com/sv2

For More Information

The Honeywell Thermal Solutions family of products includes Honeywell Combustion Safety, Eclipse, Exothermics, Hauck, Kromschröder and Maxon. To learn more about our products, visit ThermalSolutions.honeywell.com or contact your Honeywell Sales Engineer.

Honeywell Process Solutions
Honeywell Thermal Solutions (HTS)
1250 West Sam Houston Parkway
South Houston, TX 77042

ThermalSolutions.honeywell.com

32-00151-02 Rev. 05-19
Printed in USA