

# Manual de Segurança da Série SV2

## FOLHA DE DADOS DO PRODUTO



**OBSERVAÇÃO:** O conjunto eletrônico principal da válvula pode ser substituído em campo e, como tal, essa etiqueta deve ser violada para substituí-lo.

As válvulas da série SV2 são projetadas para fornecer vários recursos de segurança para evitar o uso incorreto remotamente. No entanto, é importante lembrar que a segurança física é absolutamente essencial para evitar muitas ameaças locais.

Ao instalar um dispositivo, selecione sempre um local físico com acesso limitado ou até mesmo restrito. Recomenda-se trancar o dispositivo em um gabinete fechado com acesso permitido apenas ao pessoal aprovado e treinado.

Além disso, é altamente recomendável manter toda a fiação do dispositivo fisicamente segura. Um exemplo de fiação correta e incorreta é mostrado na Fig. 1.

## INTRODUÇÃO

Este documento fornece informações de segurança para as válvulas e acessórios da série SV2.

Veja a seguir uma lista com publicações relacionadas:

- 32-00029, Manual do usuário da série SV2
- 32-00031, Manual do usuário da ferramenta de HMI/PC

## Proteção do dispositivo físico

### ⚠ AVISO DE CIBERSEGURANÇA

Os produtos da série SV2 contêm componentes eletrônicos e software. O profissional de instalação e os administradores do local devem tomar precauções para proporcionar proteção contra acesso não autorizado à válvula e à interface de programação para modificação de parâmetros (se aplicável).

O acesso autorizado não deve ser permitido no momento de alterações na interface de fiação da válvula, substituição de peças e alterações no hardware ou software do dispositivo. O não cumprimento dessas especificações pode causar riscos à segurança.

Uma etiqueta que evidencia violações foi colocada dentro do gabinete elétrico da válvula para indicar o acesso. Ela fica entre o conjunto eletrônico principal da válvula e o gabinete elétrico.

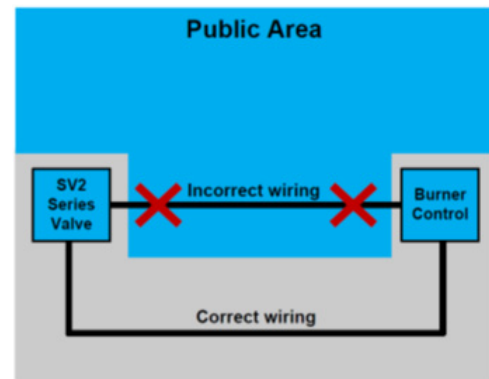


Fig. 1. Exemplos de fiação corretos e incorretos

### ⚠ CUIDADO

Quando a fiação não está protegida, uma pessoa não autorizada pode adulterar a fiação do dispositivo, resultando em um comportamento perigoso. Esta regra aplica-se à fiação específica de produtos da série SV2, mas também se aplica a qualquer outro equipamento controlado.



32-00151P-02

**OBSERVAÇÃO:** Este produto pode conter ou ser derivado de materiais, incluindo software, de terceiros. Os materiais de terceiros podem estar sujeitos a licenças, avisos, restrições e obrigações impostas pelo licenciante. As licenças, avisos, restrições e obrigações, se houver, podem ser encontradas nos materiais que acompanham o produto, nos documentos ou arquivos que acompanham tais materiais de terceiros, em um arquivo chamado `third_party_licenses` na mídia que contém o produto, ou em <http://www.honeywell.com/ps/thirdpartylicenses>

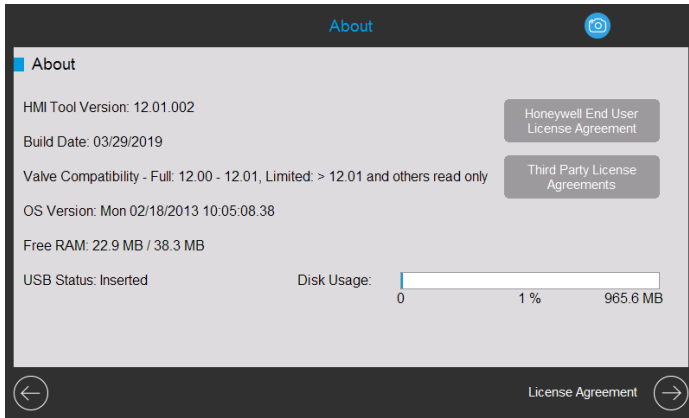


Fig. 2. Sobre a página com contratos de licença.

## Módulos de acessórios da série SV2

As válvulas da série SV2 suportam a conexão de módulos de acessórios, oferecendo funcionalidade avançada. Eles incluem o módulo de relação combustível/ar e o módulo de pressão. Esses módulos utilizam fiação externa que, uma vez adulterada, pode afetar a funcionalidade do dispositivo de maneira perigosa, limitá-lo ou desativá-lo completamente.

Embora possa não ser óbvio, o módulo de relação combustível/ar também utiliza tubulação externa que, em caso de modificação não autorizada, pode causar falhas no dispositivo.

## MODIFICAÇÃO MODBUS®

Para a configuração da série SV2 e o monitoramento do dispositivo, é utilizada a comunicação Modbus utilizando um barramento RS-485. Esta comunicação requer atenção especial quando se trata de segurança.

## Comunicação segura vs. Não segura

O protocolo Modbus, por sua natureza, não é seguro e não fornece nenhum meio nativo de segurança, no entanto, a versão 10 do firmware em execução da série SV2 suporta o Modbus seguro, que é uma extensão de propriedade da Honeywell do protocolo padrão.

O Modbus seguro suporta a validação de integridade de mensagens, de modo que não podem ser afuniladas por ninguém que esteja acessando o conduto RS-485. No entanto, este protocolo não protege os dados do dispositivo contra a leitura por pessoal não autorizado.

## Gerenciamento de sessão

As válvulas da série SV2 e as ferramentas de HMI/PC suportam uma sessão segura quando o Modbus seguro é usado. Isso significa que, quando o usuário faz login com uma senha para os níveis de acesso do Instalador ou do OEM, um túnel seguro é estabelecido entre o aplicativo do cliente HMI/PC do usuário e a válvula da série SV2. Consulte as Figuras 2-4.

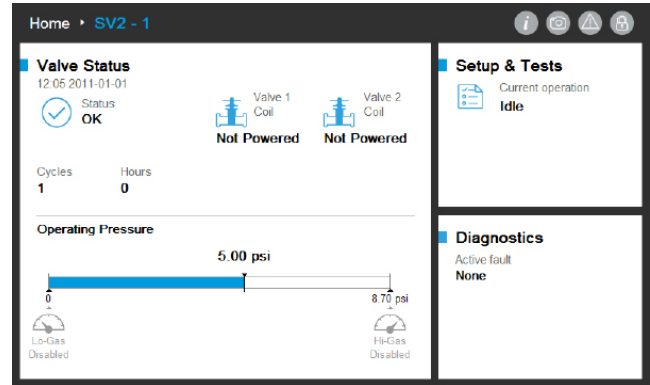


Fig. 3. Sessão não estabelecida. O usuário não está conectado.

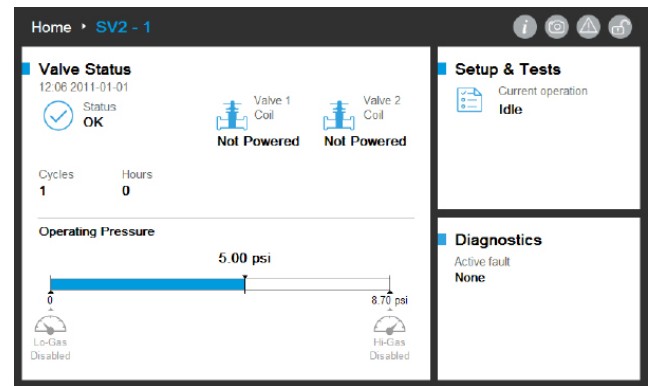


Fig. 4. Sessão estabelecida. O usuário está conectado como Instalador.

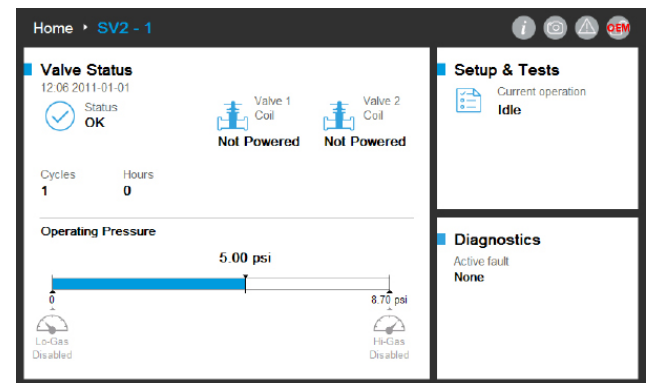


Fig. 5. Sessão estabelecida. O usuário está conectado como OEM.

Uma sessão deve ser estabelecida e usada para poder fazer qualquer alteração na configuração da válvula. Por exemplo, configurações típicas são:

1. Verificação de segurança de dados de configuração críticos
2. Comissionamento de configuração de válvula de pré-mistura
3. Configuração do módulo de pressão
4. Configuração de segurança (configuração de senha, modificação de privilégios de acesso)
5. Configuração de prova de fechamento
6. Sequência de provas de válvula
7. Unidades (pressão, volume e vazamento)
8. Configurações gerais da válvula (endereço Modbus, taxa de baud)

**OBSERVAÇÕES:**

- Apenas uma sessão pode estar ativa por vez. Em outras palavras, quando um usuário está conectado, outro precisa esperar até que a sessão anterior seja encerrada.
- Uma sessão segura será encerrada se nenhuma comunicação segura for recebida dentro de 20 segundos após a última mensagem segura.
- Uma sessão segura será encerrada pela ferramenta de HMI/PC da série SV2 se o usuário estiver inativo por mais de 10 minutos.

**Gerenciamento de senha/chave**

Uma senha é a frase ou sequência de caracteres que precisam cumprir as seguintes regras:

- Pelo menos doze caracteres
- Pelo menos uma letra maiúscula e uma minúscula
- Pelo menos um número
- Não inclua caracteres especiais

As válvulas da série SV2 são fornecidas com as senhas pré-configuradas padrão do OEM e do Instalador. Essas senhas devem ser alteradas antes que a válvula possa ser usada em um aplicativo sem observação do usuário.

Esquecer de alterar a senha padrão resulta em bloqueio persistente quando a sessão segura é finalizada. Esta é uma medida de segurança que evita o uso de uma válvula no modo inseguro (sem a configuração correta da senha). Consulte as Figuras 5-8.

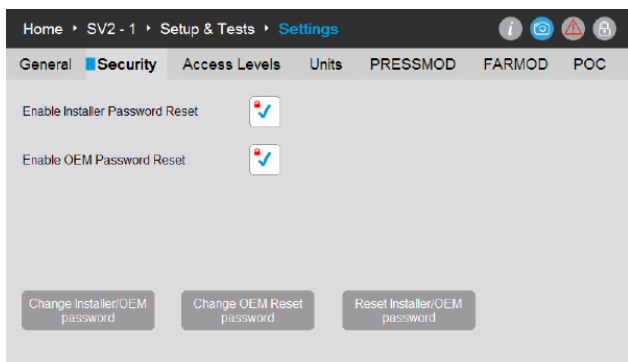


Fig. 6. As senhas do OEM, da Redefinição do OEM e do Instalador podem ser alteradas na página Segurança.

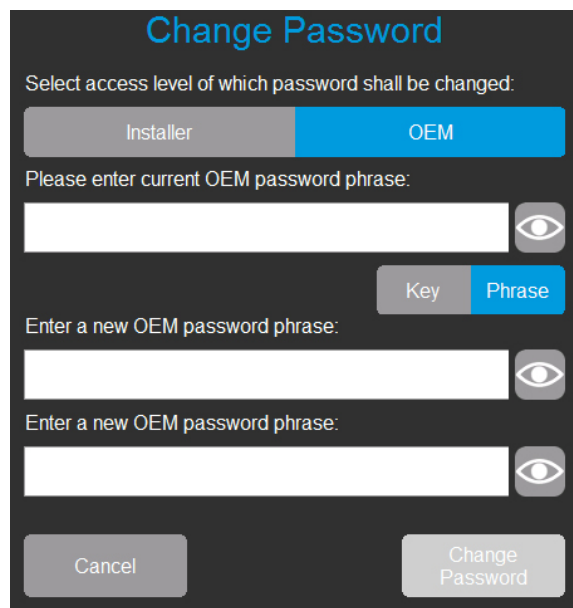


Fig. 7. O usuário conectado como OEM pode alterar a senha do Instalador ou do OEM. O usuário insere a senha atual do OEM e a nova senha duas vezes.

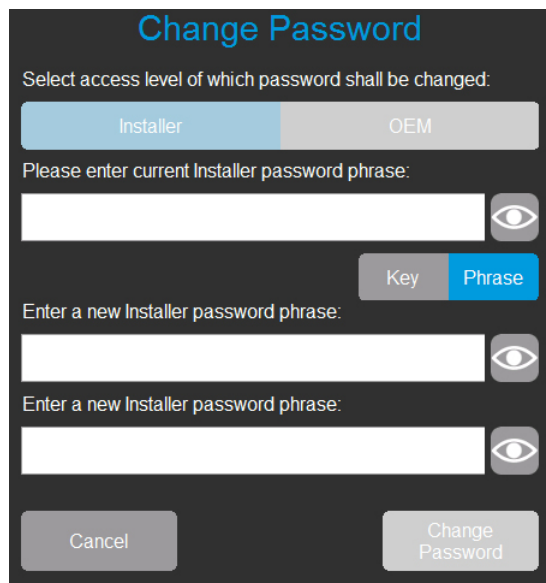


Fig. 8. O usuário conectado como Instalador pode alterar apenas a senha do Instalador. O usuário insere a senha atual do Instalador e a nova senha duas vezes.

Fig. 9. O usuário conectado como OEM também pode alterar a senha da Redefinição do OEM. O usuário insere a senha atual do OEM e a nova senha da Redefinição do OEM duas vezes.

## Redefinição de senha

Se as senhas do nível de acesso principal do Instalador e/ou do OEM forem perdidas, será possível redefinir a senha se os mecanismos de redefinição forem habilitados pelo OEM. Consulte a Fig. 5. O mecanismo de redefinição variará entre os níveis do Instalador e do OEM. Lembre-se que o ciclo da válvula ou a potência da interface do usuário não anula essa metodologia.

O mecanismo de redefinição de senha permite que o usuário apropriado reconfigure as senhas atuais aos valores padrão de fábrica da Honeywell. Depois que as senhas forem redefinidas, o usuário poderá fazer login e atribuir novas senhas.

Após redefinir para o valor padrão, se as senhas do OEM + Instalador e da Redefinição do OEM não estiverem definidas como novos valores não-padrão, a válvula ficará em status de bloqueio e não estará operacional a menos que o usuário do OEM esteja conectado. As senhas aplicáveis devem ser configuradas para limpar os códigos de falha.

Fig. 10. O usuário não conectado seleciona o nível de acesso da senha a ser redefinida. O usuário digita uma frase válida de senha de redefinição.

Por padrão, o recurso de redefinição de senha para o Instalador e o OEM é desativado e deve ser ativado na configuração inicial de cada dispositivo pelo OEM ou pelo proprietário original, conforme indicado na Figura 5.

### OBSERVAÇÕES:

- O OEM pode optar por ativar ou desativar a função de redefinição de senha do OEM. Consulte a Figura 5.
  - Se estiver ativada, a senha principal do OEM será perdida, o OEM poderá reconfigurar as senhas para os padrões de fábrica da Honeywell e reatribuir novas senhas
  - Se estiver desativado e a senha principal do OEM for perdida, o OEM não poderá redefinir a senha e será efetivamente impedido de editar a válvula no nível do OEM.
  - Se a senha principal do nível do Instalador for conhecida, o OEM poderá acessar a válvula usando-a e editar os parâmetros aos quais concederam o acesso do Instalador.
  - Para possibilitar a edição no nível do OEM novamente, os principais eletrônicos da válvula teriam que ser substituídos e a válvula completamente reprogramada nos níveis de OEM e Instalador.

## Proteção de senha

Para evitar que uma senha de sessão seja adivinhada por tentativas aleatórias, todas as senhas são protegidas por um mecanismo de detecção de força bruta. Esse mecanismo desativa temporariamente o login na conta e na válvula afetadas. Os dispositivos precisam ser desligados ou a pessoa que faz login precisa aguardar pelo menos um minuto antes da próxima tentativa.

Se isso ocorrer, as falhas serão anunciadas na página de diagnósticos da ferramenta de HMI/PC. Existem quatro códigos de falha possíveis associados a essa instância:

- Conta do Instalador temporariamente desativada
- Conta do OEM temporariamente desativada
- Recurso de redefinição de senha do Instalador temporariamente desativado
- Recurso de redefinição de senha do OEM temporariamente desativado

## Práticas recomendadas

Recomenda-se sempre usar senhas fortes e difíceis de adivinhar. Consulte a seção Gerenciamento de senhas/chaves no início deste documento.

## Gerenciamento de contas

Existem duas contas de usuário implementadas nas válvulas da série SV2. Essas contas são:

1. Instalador
2. OEM

A conta do Instalador é considerada subsidiária à conta do OEM. Em outras palavras, todos os recursos acessíveis pelo Instalador podem ser controlados pelo OEM.

Por outro lado, os recursos acessíveis pelo OEM podem ser usados apenas pelo OEM.

As contas de usuário não podem ser removidas ou adicionadas e sua finalidade é a seguinte:

1. A conta do OEM é usada para configurar recursos críticos da válvula, como a configuração das variáveis do módulo de pressão, módulo de combustível/ar, ignição de combustível/ar e base de combustível/ar.
2. A conta do Instalador é usada para configurar recursos menos críticos, como limites funcionais ou variáveis específicas do aplicativo.

## Gerenciamento de acesso

Por padrão, os privilégios de acesso são configuráveis para todos os recursos críticos. O nível de usuário padrão para todos os recursos de segurança é configurado para o Instalador e deve ser elevado para o nível de usuário do OEM com base em aplicativos específicos. A configuração pode ser feita usando a ferramenta de HMI ou PC da Honeywell, conforme indicado na Fig. 11:

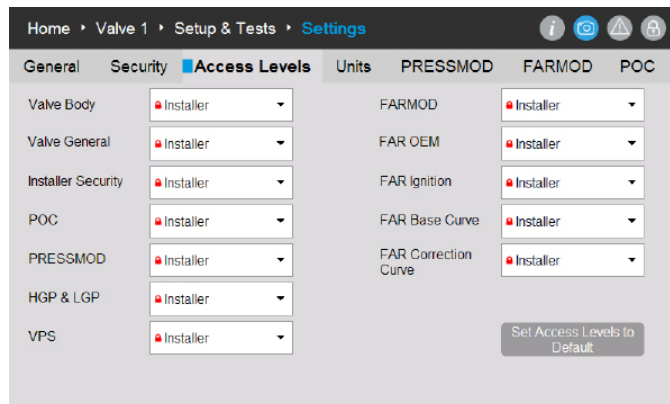


Fig. 11. Página de níveis de acesso. Cada grupo de configuração pode ser definido como Instalador, OEM ou Somente leitura.

## Segurança de conexão remota versus segurança física

Para manter a conexão remota via comunicação segura, é importante considerar os seguintes itens que se aplicam principalmente à configuração inicial do dispositivo:

- Quando o dispositivo está fisicamente acessível a um invasor em potencial, a senha de redefinição do Instalador pode ser obtida pelo invasor, lendo-o no adesivo na parte traseira do conjunto principal de componentes eletrônicos da válvula e depois usado.
- Quando uma sessão é estabelecida usando a senha padrão na válvula, ela nunca pode ser considerada segura. Recomenda-se que as senhas iniciais das contas do OEM e do Instalador sejam configuradas sem que outros dispositivos estejam presentes na rede RS-485 nos quais a válvula está conectada.

## FERRAMENTAS DE HMI E PC

Para manter as válvulas da série SV2 e as ferramentas de interface do usuário seguras, é essencial fornecer acesso confiável e seguro aos usuários. Por essa razão, várias medidas de segurança devem ser usadas com a ferramenta de PC e HMI, conforme descrito abaixo.

## Segurança de HMI

Qualquer HMI autônomo da série SV2 deve sempre ser mantido fisicamente seguro. As mesmas recomendações de segurança física se aplicam à válvula da série SV2. Consulte a seção Proteção de dispositivos físicos, anteriormente neste documento.



## Segurança da ferramenta de PC

A ferramenta de PC é projetada para funcionar em computadores com sistemas operacionais Microsoft® Windows. Ao conectar um computador a uma válvula da série SV2, qualquer problema de segurança do PC aplicável pode representar um risco de segurança para a válvula. Por esse motivo, é sempre recomendável seguir as práticas de segurança descritas abaixo:

1. Use sempre um sistema operacional suportado pela Microsoft.
2. Mantenha sempre o sistema atualizado com os patches de segurança mais recentes.
3. Tenha sempre o software antivírus e o firewall instalados e atualizados.
4. Use o recurso de lista de permissões ativado no sistema operacional do PC.
5. Nunca use aplicativos de uma fonte não confiável ou aplicativos quebrados.
6. Certifique-se de que as unidades USB ou quaisquer outros acessórios conectados ao PC sejam provenientes de uma fonte confiável e não contenham hardware ou software prejudicial (por exemplo, key loggers, scanners de memória, etc.).
7. Desative todos os serviços desnecessários, portas e contas de usuário no PC para evitar ataques remotos.

Um arquivo de instalação ou arquivo binário de aplicativo é assinado por uma chave da Honeywell para garantir que o instalador/aplicativo da Ferramenta de PC seja proveniente de uma fonte verificada. No entanto, embora a assinatura ofereça um bom nível de segurança, é sempre recomendável usar somente o instalador/aplicativo Ferramenta de PC fornecido diretamente pela Honeywell ou por um OEM/Instalador autorizado da Honeywell.

## Lista de verificação de segurança da ferramenta de PC

Para usar este aplicativo com segurança, certifique-se de que:

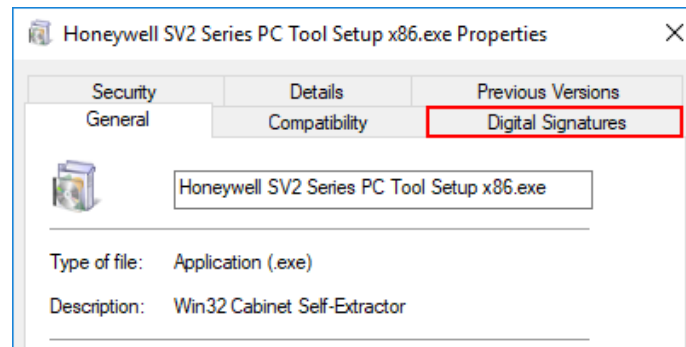
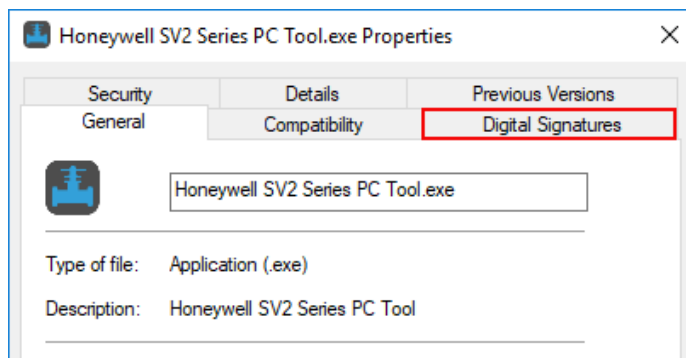
1. Você está usando apenas um aplicativo assinado e confiável (consulte a seção Verificação de origem do aplicativo)
2. Se possível, use a lista de permissões de aplicativos (consulte a seção Aplicativos de lista de permissões)
3. Você está usando proteção antivírus junto com um firewall configurado adequadamente se o computador estiver conectado à Internet.
4. Assegure-se de que o PC no qual você executa o aplicativo possui proteção por senha, para que o pessoal não autorizado não possa usá-lo.
5. Assegure-se de que o acesso físico por pessoal não autorizado ao seu sistema seja eliminado ou limitado (PC -> RS485 -> Modbus -> Válvula da série SV2).
6. A ferramenta de PC deve ser instalada automaticamente na pasta padrão "Arquivos de programa" do Microsoft Windows. Este local de instalação é pré-selecionado no instalador da ferramenta de PC. Se um local de instalação diferente for selecionado, o usuário deverá configurar as permissões de segurança (por exemplo, para o administrador) para garantir que a instalação da ferramenta de PC não seja adulterada por pessoas não autorizadas.

## Verificação de origem do instalador/aplicativo de ferramenta de PC

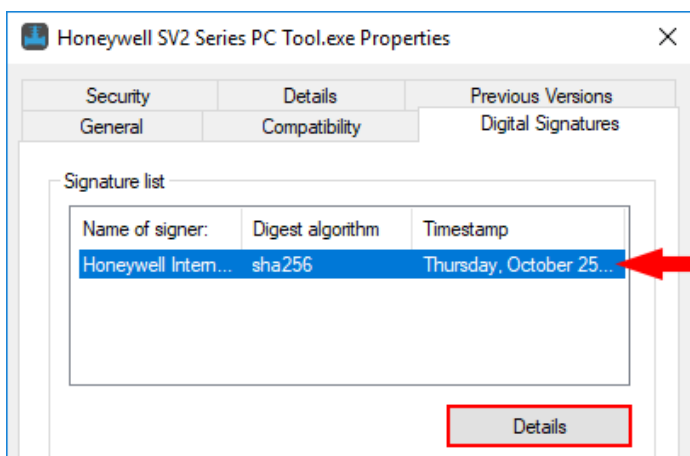
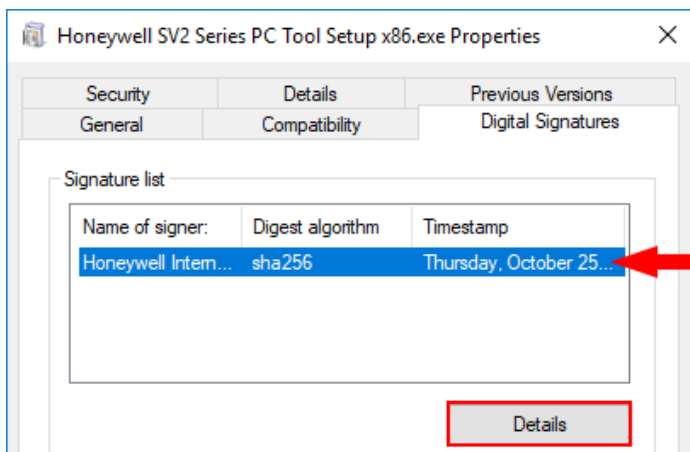
O instalador/aplicativo é fornecido com uma assinatura digital. Essa assinatura será verificada após o download de uma nova versão do instalador/aplicativo ou se houver qualquer suspeita sobre a origem do instalador/aplicativo.

A assinatura pode ser verificada seguindo estas etapas:

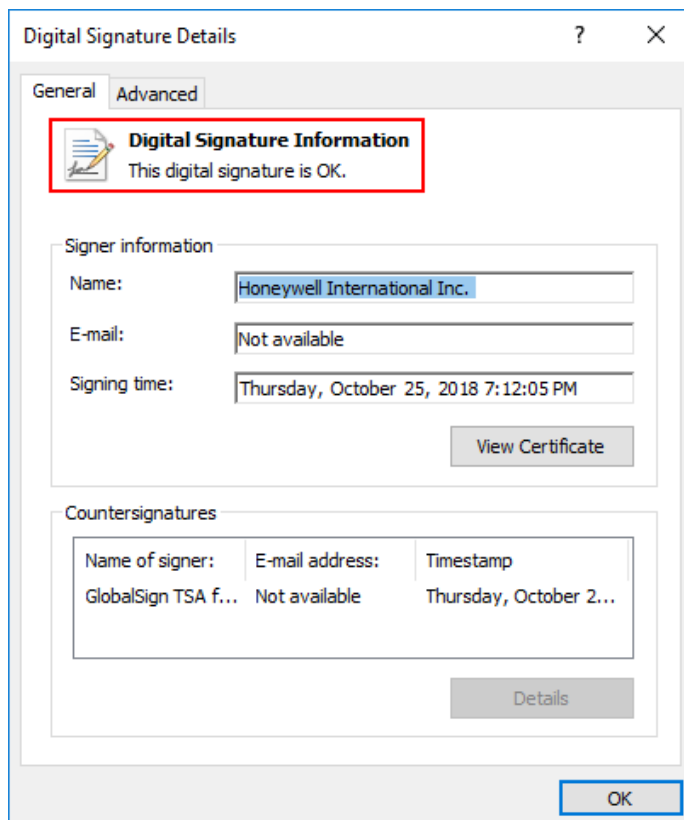
1. Clique no botão "HoneywellSV2SeriesPCToolSetupx86.exe" / "Honeywell SV2 Series PC Tool Setup x64.exe" com o botão direito do mouse e clique em "Propriedades"
2. Extraia o conteúdo de "usb\_root.zip" e clique no "app.exe" com o botão direito do mouse e clique em "Propriedades".
3. Na janela Propriedades, clique em "Assinaturas digitais". Se a guia não estiver presente, pule para a etapa 5).



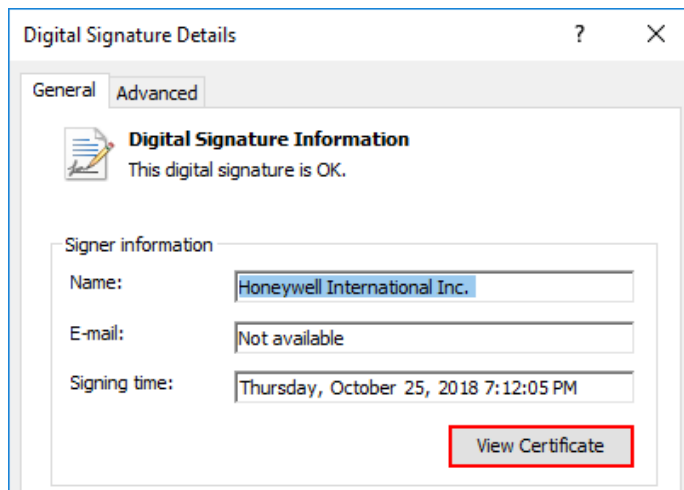
4. Na guia “Assinaturas digitais”, o único item na “Lista de assinaturas” deve ser nomeado “Honeywell International Inc.”. Clique no item e depois no botão “Detalhes”.



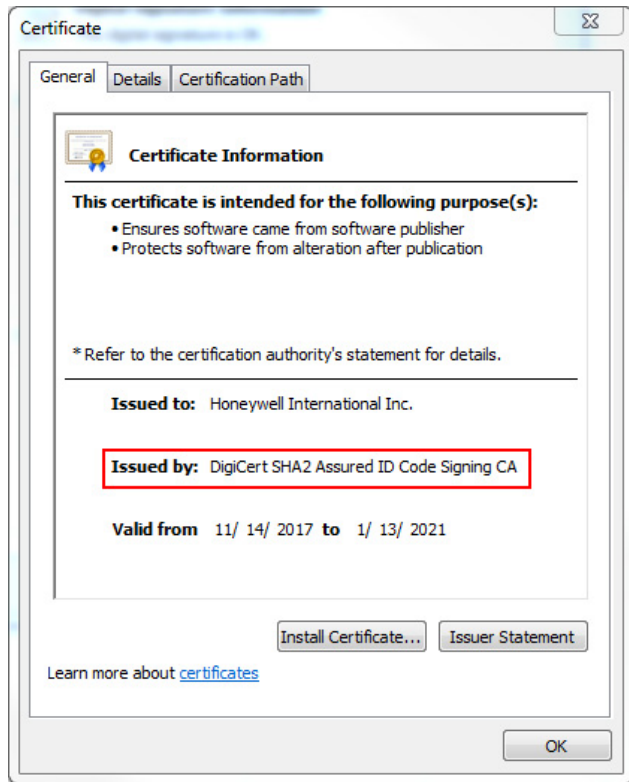
5. Na janela “Detalhes da assinatura digital”, verifique a “Informação de assinatura digital”. Deve dizer “Esta assinatura digital está OK”.



6. Se a assinatura não estiver OK ou não estiver presente (na etapa 2 sem guia de assinatura digital), o aplicativo não é confiável e deve ser excluído. Uma cópia nova e limpa pode ser baixada da fonte original.
7. Além disso, se você quiser verificar os detalhes do certificado, clique no botão “Visualizar certificado”.



8. A linha “Emitido por” nos detalhes do certificado deve conter “DigiCert”, que é o nome do provedor de certificado.



## Aplicativos de lista de permissões

A lista de permissões permite que o administrador defina uma lista de aplicativos desejados. Os aplicativos que não estão nessa lista não podem ser executados. A configuração de listas de permissões aumenta muito sua segurança e minimiza o risco de executar software não intencional em sua máquina. A lista de permissões está disponível como uma ferramenta incorporada nos sistemas operacionais do Windows (Windows 7, Windows 8) ou pode ser feita por software de terceiros.

## Relatório de falhas

Quando a ferramenta de HMI ou PC falha inesperadamente, um relatório de falha é criado. Os relatórios de falhas da ferramenta de PC estão localizados em C:\Users\\Documents\Honeywell\SV2 Series PC Tool\Crash reports\. O relatório de falha da ferramenta de HMI pode ser acessada na página Início/Configuração do display/Sobre. Consulte a Fig. 1. O relatório de falhas contém as seguintes informações:

- Versão e configuração da ferramenta de PC
- Versão do sistema operacional Microsoft Windows
- Versão do Microsoft .NET framework
- Exceção e rastreamento de pilha
- Lista de portas COM disponíveis
- Configuração total das válvulas

Para obter mais informações sobre este produto e sobre toda a linha de produtos da série SV2, consulte o Guia do usuário da série SV2 em nosso site: <https://combustion.honeywell.com/sv2>

### Para obter mais informações

A família de produtos Soluções térmicas Honeywell inclui Honeywell Combustion Safety, Eclipse, Exothermics, Hauck, Kromschröder e Maxon. Para saber mais sobre nossos produtos, acesse o site [ThermalSolutions.honeywell.com](https://ThermalSolutions.honeywell.com) ou entre em contato

### Honeywell Process Solutions

Soluções térmicas Honeywell (HTS)  
1250 West Sam Houston Parkway  
South Houston, TX 77042

[ThermalSolutions.honeywell.com](https://ThermalSolutions.honeywell.com)

® U.S. Registered Trademark.  
© 2019 Honeywell International Inc.  
32-00151P-02 Rev. 05-19  
Printed in USA

