EcoStruxure Panel Server

Manual de cibersegurança

Concentrador de dispositivos sem Fios e gateway Modbus, datalogger e servidor de energia

EcoStruxure inclui uma plataforma e arquitetura compatível com IoT.

DOCA0211PT-13
07/2025

www.se.com

Informações legais

As informações fornecidas neste documento contêm descrições gerais, características técnicas e/ou recomendações relacionadas com produtos/soluções.

Este documento não deve substituir um estudo aprofundado ou um desenvolvimento operacional e num local específico ou um plano esquemático. Não deve ser utilizado para determinar a adequação ou fiabilidade dos produtos/soluções para aplicações específicas de utilizadores. O utilizador tem o dever de efetuar ou solicitar a um especialista profissional à sua escolha (integrador, supervisor ou semelhante) uma análise adequada e exaustiva do risco, avaliação e teste dos produtos/soluções no que respeita à aplicação específica ou utilização efetiva.

A marca Schneider Electric e quaisquer marcas comerciais da Schneider Electric SE e respetivas subsidiárias referidas no presente documento são propriedade da Schneider Electric SE ou das respetivas subsidiárias. Todas as outras marcas podem ser marcas comerciais do respetivo proprietário.

A Schneider Electric reserva-se o direito de efetuar alterações ou atualizações relativamente ou sobre o conteúdo do presente documento ou o respetivo formato, em qualquer altura sem aviso prévio.

Na medida do permitido pela legislação aplicável, a Schneider Electric e as respetivas subsidiárias não assumem qualquer responsabilidade ou obrigação por quaisquer erros ou omissões no conteúdo informativo do presente documento, bem como qualquer utilização indevida ou abusiva do respetivo conteúdo.

Conteúdos

Instruções de segurança 5
Acerca do documento 6
Introdução à cibersegurança 9
Caraterísticas do dispositivo 11
Funcionalidades do dispositivo.....13
Segurança de rede 16
Segurança de aplicações na nuvem.....19
Segurança física do dispositivo 20
Recomendações de segurança em termos de manutenção.....22
Glossário 25

Instruções de segurança

Informações importantes

Leia cuidadosamente estas instruções e observe o equipamento para se familiarizar com o dispositivo antes de o tentar instalar, utilizar, colocar em funcionamento ou efectuar a manutenção. As seguintes mensagens especiais podem surgir ao longo deste documento ou no equipamento para o avisar de possíveis perigos ou para lhe chamar a atenção relativamente a informação que esclareça ou simplifique os procedimentos.

A existência deste símbolo em um rótulo de segurança de “Perigo” ou “Atenção” indica perigo de choque elétrico, que pode resultar em ferimentos, se as instruções não forem seguidas.

Este é o símbolo de aviso de segurança. É utilizado para o alertar quanto a possíveis ferimentos pessoais. Obedeça a todas as mensagens de segurança que acompanham o símbolo para evitar possíveis ferimentos ou morte.

⚠ PERIGO

PERIGO indica uma situação perigosa que, se não for evitada, **resultará em** morte ou ferimentos graves.

⚠ ATENÇÃO

ATENÇÃO indica uma situação perigosa que, se não for evitada, **pode resultar em** morte ou ferimentos graves.

⚠ CUIDADO

CUIDADO indica uma situação perigosa que, se não for evitada, **pode resultar em** ferimentos leves ou moderados.

AVISO

AVISO é utilizado para abordar práticas não relacionadas com lesões corporais.

Nota

A instalação, utilização e manutenção do equipamento eléctrico devem ser efectuadas exclusivamente por pessoal qualificado. A Schneider Electric não assume qualquer responsabilidade pelas consequências resultantes da utilização deste material.

Uma pessoa qualificada possui aptidões e conhecimentos relacionados com o fabrico e o funcionamento do equipamento eléctrico e a sua instalação e recebeu formação de segurança para reconhecer e evitar os perigos envolvidos.

Acerca do documento

Âmbito do documento

Este manual fornece informações sobre os aspetos de cibersegurança do EcoStruxure™ Panel Server para ajudar designers de sistemas e operadores a promover um ambiente de funcionamento seguro para o produto.

Este manual não aborda o tópico mais abrangente sobre como proteger a sua rede de tecnologia operacional ou a rede Ethernet da sua empresa. Para uma introdução geral a ameaças de cibersegurança e como abordá-las, consulte Informações gerais de cibersegurança, página 6.

NOTA: Neste manual, o termo **segurança** é utilizado para referir-se à cibersegurança.

Nota de validade

As informações indicadas neste manual são relevantes para EcoStruxure Panel Server com versão de firmware 002.003.000 ou superior.

Informações online

É provável que a informação contida neste manual seja atualizada em qualquer altura. A Schneider Electric recomenda vivamente que tenha a versão mais recente e atualizada disponível em www.se.com/ww/en/download.

As características técnicas dos dispositivos descritos neste manual estão também indicadas online. Para aceder à informação online, vá para a página inicial da Schneider Electric em www.se.com.

Informações gerais de segurança cibernética

Nos últimos anos, o número crescente de máquinas em rede e fábricas de produção tem registado um aumento correspondente do potencial de ameaças cibernéticas, como acesso não autorizado, violações de dados e interrupções operacionais. Deve, portanto, considerar todas as medidas de cibersegurança possíveis para ajudar a proteger ativos e sistemas dessas ameaças.

Para ajudar a manter os seus produtos Schneider Electric seguros e protegidos, é do seu interesse implementar as melhores práticas de cibersegurança, conforme descrito no documento Cybersecurity Best Practices.

A Schneider Electric fornece informação e assistência adicionais:

- Subscreva a newsletter de segurança da Schneider Electric.
- Visite a página Web do Cybersecurity Support Portal para:
  - Localizar Notificações de segurança.
  - Comunicar vulnerabilidades e incidentes.
- Visite a página Web do Schneider Electric Cybersecurity and Data Protection Posture para:
  - Aceder à postura de cibersegurança.
  - Saber mais sobre cibersegurança na Academia de Segurança Cibernética.
  - Explorar os serviços de cibersegurança da Schneider Electric.

Informações de cibersegurança relacionadas com o produto

⚠ATENÇÃO
RISCO POTENCIAL DE DISPONIBILIDADE, INTEGRIDADE E CONFIDENCIALIDADE • Desative portas/serviços não utilizados para ajudar a minimizar o acesso a atacantes maliciosos. • Coloque os dispositivos ligados à rede atrás de várias camadas de defesa cibernética (como firewalls, segmentação de rede e deteção de intrusão e proteção da rede). • Utilize as melhores práticas de cibersegurança (por exemplo, menos privilégios, separação de funções) para ajudar a evitar a exposição não autorizada, perda, alteração de dados e registos ou interrupção dos serviços. **O não cumprimento destas instruções pode resultar em morte, lesões graves ou danos no equipamento.**

Idiomas disponíveis do documento

O documento está disponível nos seguintes idiomas:

- Inglês (DOCA0211EN), idioma original
- Francês (DOCA0211FR)
- Alemão (DOCA0211DE)
- Italiano (DOCA0211IT)
- Português (DOCA0211PT)
- Espanhol (DOCA0211ES)

Documentos relacionados

Título da documentação	Número de referência
EcoStruxure Panel Server - Manual do utilizador	DOCA0172EN DOCA0172DE DOCA0172ES DOCA0172FR DOCA0172IT DOCA0172PT
Melhores práticas de cibersegurança	7EN52-0390
EcoStruxure Power - Guide for Designing and Implementing a Cyber Secure Digital Power System - Technical Guide	ESXP2TG003EN

Pode transferir estas publicações técnicas e outras informações técnicas a partir do nosso Website em www.se.com/ww/en/download/.

Informação sobre terminologia não inclusiva ou não sensível

Como empresa responsável e inclusiva, a Schneider Electric está constantemente a atualizar as suas comunicações e produtos que contêm terminologia não inclusiva ou insensível. No entanto, apesar destes esforços, o nosso conteúdo pode conter termos que são considerados inadequados por alguns clientes.

Marcas comerciais

QR Code é uma marca comercial registada da DENSO WAVE INCORPORATED no Japão e noutros países.

Introdução à cibersegurança

EcoStruxure Intervalo principal

A EcoStruxure é a plataforma e arquitetura interoperável, plug-and-play, aberta e compatível com IoT da Schneider Electric para habitação, edifícios, centros de dados, infraestruturas e indústrias. Inovação a todos os níveis, desde produtos ligados a controlo de ponta e aplicações, análises e serviços.

Tópicos relacionados

- Introdução à cibersegurança (Parent Topic)

Introdução

A cibersegurança destina-se a ajudar a proteger a sua rede de comunicações e todos os equipamentos a ela ligados de ataques que possam afetar as operações (disponibilidade), modificar a informação (integridade) ou fornecer informações confidenciais (confidencialidade). O objetivo da cibersegurança é fornecer níveis reforçados de proteção para informações e ativos físicos contra roubo, corrupção, uso indevido ou acidentes, além de manter o acesso aos seus utilizadores. Existem muitos aspetos da cibersegurança, incluindo conceção de sistemas seguros, restrição do acesso através de métodos físicos e digitais, identificação de utilizadores, bem como implementação de procedimentos de segurança e de políticas de melhores práticas.

Tópicos relacionados

- Introdução à cibersegurança (Parent Topic)

Diretrizes da Schneider Electric

Além das recomendações indicadas neste manual que são específicas da Panel Server, deve seguir a abordagem aprofundada da defesa à cibersegurança da Schneider Electric e as informações gerais de cibersegurança, página 6.

Tópicos relacionados

- Introdução à cibersegurança (Parent Topic)

Políticas e regras de cibersegurança da Schneider Electric

A Schneider Electric utiliza um processo de Ciclo de vida de desenvolvimento seguro (SDL), uma estrutura principal baseada no desenvolvimento de produtos que ajuda a garantir que os produtos seguem processos de design seguros em todas as fases do ciclo de vida. O processo SDL da Schneider Electric está em conformidade com IEC 62443-4-1.

O processo SDL inclui o seguinte:

- Práticas SDL aplicadas a ações de desenvolvimento interno, em toda a cadeia de abastecimento.
- Revisão de segurança final necessária para o lançamento do projeto.
- Formação em segurança para o pessoal envolvido no desenvolvimento do produto.

Tópicos relacionados

- Introdução à cibersegurança (Parent Topic)

Caraterísticas do dispositivo

Descrição geral

O EcoStruxure Panel Server está equipado com funcionalidades de segurança ativadas. Estas funcionalidades encontram-se num estado predefinido e podem ser modificadas para satisfazer as suas necessidades de instalação. O Panel Server só deve ser configurado e definido por pessoal qualificado, uma vez que a desativação ou alteração das definições afeta a robustez da segurança em geral do Panel Server e da segurança da sua rede.

Consulte este manual em conjunto com o DOCA0172•• *EcoStruxure Panel Server - Manual do utilizador*, página 7 para obter uma configuração pormenorizada das funções e definições do Panel Server.

Interfaces do EcoStruxure Panel Server

A tabela seguinte resume as arquiteturas de comunicação disponíveis no Panel Server por modelo:

Caraterística		**EcoStruxure Panel Server**													
		Entry	**Universal**							**Advanced**					
		PAS400	**PAS600 HW: V1.0**	**PAS600 HW: V2.0**	**PAS600T HW: V1.0**	**PAS600L HW: V1.0**	**PAS600L HW: V2.0**	**PAS600LWD HW: V2.0**	**PAS600LWD HW: V2.0**	**PAS800 HW: V1.0**	**PAS800 HW: V2.0**	**PAS800L HW: V1.0**	**PAS800L HW: V2.0**	**PAS800P HW: V1.0**	**PAS800P HW: V2.0**
10/100BASE-T Ethernet	Uma porta RJ45	✓	-	-	-	-	-	-	-	-	-	-	-	-	-
	Duas portas RJ45	-	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Conetividade Modbus TCP/IP a montante		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Conetividade Wi-Fi a montante		✓	✓	✓	✓	✓	✓	-	-	✓	✓	✓	✓	✓	✓
Conetividade Modbus TCP/IP a jusante		-	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Conetividade IEEE 802.15.4 a jusante		✓	✓	✓	✓	✓	✓	-	-	✓	✓	✓	✓	✓	✓
Conetividade Modbus-SL a jusante		-	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Duas entradas digitais (para WAGES (água, ar, gás, eletricidade, vapor))		-	-	-	-	✓	✓	✓	-	-	-	✓	✓	-	-
Antena de Wi-Fi interna		-	✓	✓	✓	✓	✓	-	-	✓	✓	✓	✓	✓	✓
Antena externa IEEE 802.15.4		-	-	✓	-	-	✓	-	-	✓	✓	✓	✓	✓	✓
Ponto de acesso Wi-Fi		✓	✓	✓	✓	✓	✓	-	-	✓	✓	✓	✓	✓	✓
Notificação de alarmes por e-mail		-	-	-	-	-	-	-	-	✓	✓	✓	✓	✓	✓
Publicação no servidor SFTP ou HTTPS		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Convenção

O EcoStruxure Panel Server é doravante referido como Panel Server.

Protocolos suportados

O EcoStruxure Panel Server suporta os seguintes protocolos:

- DHCP para endereçamento IP de rede
- DNS para resolução de nomes de rede
- DPWS para deteção de rede
- HTTPS (TLS v1.2) para configuração através de ferramentas de configuração e páginas Web integradas
- IEEE 802.15.4 para comunicação sem fios utilizando comunicação por radiofrequência banda ISM 2.4 GHz (não disponível para os modelos Wired by Design)
- Modbus TCP e Modbus-SL para comunicações com outros dispositivos de tecnologia operacional (OT)
- NTP para sincronização de hora
- RSTP para permitir topologias em anel Ethernet robustas para aplicações críticas
- SFTP para publicação de ficheiros .CSV num servidor SFTP
- Cliente VPN para acesso remoto (aberto ao Centro de apoio ao cliente da Schneider Electric)
- WPA2 e WPA para comunicação Wi-Fi (não disponível para os modelos Wired by Design)

Funcionalidades de segurança

O EcoStruxure Panel Server suporta as seguintes funcionalidades de segurança:

- Apenas o firmware com assinatura digital da Schneider Electric pode ser instalado no Panel Server.
- Em cada inicialização, a assinatura digital do firmware é validada antes da execução, para ajudar a garantir que não foi adulterada.
- As palavras-passe do utilizador são armazenadas como palavras-passe em salt e em hash (SHA256).
- O botão Reiniciar permite apagar todas as informações do Panel Server.
- O dispositivo tem um relógio interno e memoriza a data e hora durante alguns meses sem energia.
- A chave de autenticidade do Panel Server é armazenada num chip com certificação Common Criteria CC EAL6+ de elevada segurança.

Funcionalidades do dispositivo

Atualização de firmware

Atualize o EcoStruxure Panel Server para a versão mais recente do firmware para obter as funcionalidades mais recentes e mantenha-se atualizado com as correções de segurança. Todo o firmware concebido para o EcoStruxure Panel Server é assinado pela Infraestrutura de chaves públicas (PKI) da Schneider Electric para garantir a integridade e autenticidade do firmware executado no EcoStruxure Panel Server. Para um funcionamento PKI adequado, mantenha a data do dispositivo sincronizada (consulte Data e hora, página 13).

Para ser informado sobre atualizações de segurança, efetue o registo em Security Notifications no Portal de apoio à cibersegurança da Schneider Electric.

Tópicos relacionados

- Funcionalidades do dispositivo (Parent Topic)

Data e hora

É importante manter a data e a hora sincronizadas para os seguintes fins:

- Para evitar erros em certificados e assinaturas digitais no EcoStruxure Panel Server
- Para fornecer um carimbo de data/hora preciso nos registos de auditoria para ajudar a segurança forense

Para obter mais informações sobre data e hora, consulte o DOCA0172•• *EcoStruxure Panel Server - Manual do utilizador*, página 7.

Tópicos relacionados

- Funcionalidades do dispositivo (Parent Topic)

Desativar funcionalidades não utilizadas

O EcoStruxure Panel Server permite desativar portas/serviços não utilizados para ajudar a minimizar os caminhos para atacantes maliciosos.

É recomendável desativar:

- Ativação Wi-Fi e infraestrutura Wi-Fi. A Wi-Fi pode ser desativada de maneira permanente, se necessário.
- Ponto de acesso Wi-Fi (ativado por predefinição). Quando o ponto de acesso estiver desativado, premir o botão na parte dianteira do Panel Server não aciona a ativação do ponto de acesso. A desativação da ativação Wi-Fi também desativa o ponto de acesso Wi-Fi e interrompe qualquer ligação ativa.
- IEEE 802.15.4 (não ativa por predefinição). A norma IEEE 802.15.4 pode ser desativada de maneira permanente.
- Serviços de gateway Modbus (ativos por predefinição). Pode ser desativado em cada interface (Ethernet 1, Ethernet 2 e/ou Wi-Fi) nas páginas Web do Panel Server.
- Protocolo de deteção DPWS através de IP v4/6 (ativo por predefinição)
- RSTP Rapid Spanning Tree Protocol (não ativo por predefinição)

  NOTA: Wi-Fi e IEEE 802.15.4 estão indisponíveis nativamente nos modelos Wired by Design (WD), que não têm chipset sem fios.

Para obter mais informações sobre como desativar as funcionalidades não utilizadas do EcoStruxure Panel Server, consulte DOCA0172•• *EcoStruxure Panel Server - Manual do utilizador*, página 7.

Tópicos relacionados

- Funcionalidades do dispositivo (Parent Topic)

Portas TCP

As seguintes portas TCP são utilizadas no EcoStruxure Panel Server:

- Porta 443: HTTPS
- Porta 502: Modbus
- Porta 5357: DPWS (pode ser alterada)

NOTA: O Panel Server não integra qualquer tipo de servidor SSH.

Tópicos relacionados

- Funcionalidades do dispositivo (Parent Topic)

Registos de auditoria

O EcoStruxure Panel Server gera registos de auditoria que registam eventos como tentativas de início de sessão inválidas e atualização de firmware.

Os registos não contêm quaisquer informações pessoais.

Para detetar comportamentos inesperados (por exemplo, reinicialização frequente, atualização de firmware incorreta ou tentativas de início de sessão inválidas), é recomendável monitorizar registos de auditoria com frequência. Para obter mais informações sobre registos de diagnósticos, consulte DOCA0172•• *EcoStruxure Panel Server - Manual do utilizador*, página 7.

Tópicos relacionados

- Funcionalidades do dispositivo (Parent Topic)

Eliminação do dispositivo

O EcoStruxure Panel Server contém informações confidenciais configuradas durante a colocação em funcionamento, registos e valores de dados recentes. Por exemplo, estas informações podem incluir topologia de dispositivos Modbus, redes sem fios, palavras-passe Wi-Fi ou consumos de energia medidos.

É necessário executar uma reposição de fábrica antes de eliminar o EcoStruxure Panel Server. Quando executar este procedimento, deve ter acesso físico para reiniciar o ciclo de energia EcoStruxure Panel Server. Veja como repor o EcoStruxure Panel Server para as definições de fábrica no DOCA0172•• *EcoStruxure Panel Server - Manual do utilizador*, página 7.

Tópicos relacionados

- Funcionalidades do dispositivo (Parent Topic)

Segurança de rede

Introdução

O EcoStruxure Panel Server não foi concebido para resistir à exposição direta à Internet pública. Deve ser instalado pelo menos atrás da Tradução de endereços de rede (NAT) ou, de preferência, atrás de várias firewalls. Para obter mais informações, consulte os seguintes Websites:

- Serviços de consultoria de cibersegurança da Schneider Electric
- Instituto Nacional de Normas e Tecnologia (NIST)
- Agência da União Europeia para a Cibersegurança (ENISA)

Segmentação de rede

O EcoStruxure Panel Server é um gateway. Cria uma ponte entre redes diferentes. A segmentação de rede ajuda a garantir a defesa cibernética. Para melhorar a segmentação da rede, Panel Server Universal e Advanced incluem duas portas Ethernet. Podem ser otimizadas no modo separado para terem uma porta dedicada à tecnologia de informação (TI) e uma porta dedicada à tecnologia operacional (TO). A segmentação de rede permite-lhe manter as redes de TO e TI segmentadas, uma vez que os pacotes de rede não são encaminhados de um lado para o outro.

É recomendável configurar a rede no modo Separado (para obter mais informações sobre definições de rede, consulte o DOCA0172•• *EcoStruxure Panel Server - Manual do utilizador*, página 7).

Isto permite-lhe ligar o Panel Server a:

- dispositivos OT a jusante através do TCP Modbus numa porta Ethernet.
- PC de TI a montante com SCADA e aplicações de software em funcionamento na outra porta Ethernet.

HTTPS e Modbus estão disponíveis em interfaces Ethernet do Panel Server (ETH1, ETH2) e Wi-Fi.

A tabela seguinte apresenta a predefinição para cada interface:

Interface		**Modbus**
Ethernet em topologia comutada		Ativado
Ethernet em topologia separada	Porta ETH1	Ativado
	Porta ETH2	Desativada
Infraestrutura Wi-Fi		Desativada
Ponto de acesso Wi-Fi		Não disponível

É recomendável desativar o serviço Modbus em redes onde não seja utilizado. Para obter mais informações sobre a ativação do serviço, consulte DOCA0172•• *EcoStruxure Panel Server - Manual do utilizador*, página 7.

Certificado do servidor Web do produto

Para suportar comunicações seguras HTTP, o EcoStruxure Panel Server está equipado com um certificado X.509v3 por predefinição. Este certificado ajuda a garantir a integridade e a confidencialidade para configurar a comunicação HTTPS.

Os browsers reconhecem apenas certificados para Websites públicos. Uma vez que o Panel Server está instalado numa rede local (LAN), os Web browsers não conseguem distinguir um Panel Server de outro. Por conseguinte, é apresentada uma mensagem de segurança no Web browser quando estabelecer ligação ao Panel Server.

Uma ligação com fios direta ajuda a proteger o caminho de comunicação com o Panel Server. Para obter mais informações sobre o primeiro acesso a páginas Web EcoStruxure Panel Server através do PC, consulte DOCA0172•• *EcoStruxure Panel Server - Manual do utilizador*, página 7.

Impressão digital por chave do servidor SFTP

Se publicar os dados num servidor SFTP, certifique-se de que a impressão digital chave, apresentada quando configura o endereço do servidor, corresponde à chave SFTP do servidor.

Se renovar a chave SFTP no servidor, o Panel Server deixa de poder enviar os ficheiros, uma vez que a ligação não será autenticada. Deve configurar novamente a publicação para que o Panel Server grave a nossa impressão digital da chave SFTP.

Rede sem fios

Os protocolos de rádio são vulneráveis a violações de segurança física. Por exemplo, um ataque de recusa de serviço pode bloquear o sinal de rádio através de um potente emissor de rádio localizado nas proximidades.

Por conseguinte, é recomendável que adapte a sua segurança física ao nível crítico das informações que dependem de protocolos de rádio. Para este efeito, as redes sem fios (Wi-Fi e IEEE 802.15.4) podem ser desativadas permanentemente no Panel Server. Se estiver confiante de que nunca vai necessitar de redes sem fios (Wi-Fi e IEEE 802.15.4), e apenas neste caso, pode desativá-las de maneira permanente. Para obter mais informações sobre a desativação permanente e simultânea das redes sem fios, consulte DOCA0172•• *EcoStruxure Panel Server - Manual do utilizador*, página 7.

NOTA: Os modelos Wired by Design (WD) do Panel Server permitem-lhe cumprir as políticas sem fios, uma vez que não contêm chipset sem fios.

É recomendável que:

- Utilize o código de instalação para detetar dispositivos sem fios. Para obter mais informações, consulte DOCA0172•• *EcoStruxure Panel Server - Manual do utilizador*, página 7
- Execute a colocação em funcionamento de dispositivos sem fios IEEE 802.15.4 num local seguro contra transmissores de rádio não autorizados, como uma sala de administrador.

No que respeita à rede Wi-Fi, é recomendável a utilização do protocolo WPA2 (Wi-Fi Protected Access, versão 2).

NOTA: O protocolo TKIP (Temporal Key Integrity Protocol) não é suportado.

Acesso remoto (VPN)

O Panel Server fornece uma funcionalidade de acesso remoto que permite ao Centro de apoio ao cliente (CCC) do Schneider Electric para ligação a páginas Web do Panel Server.

O acesso não está ativado por predefinição e requer que a firewall ative a ligação. Para obter mais informações, consulte Pontos finais esperados, página 19.

A funcionalidade de acesso remoto depende de uma VPN de 3 camadas que, por conceção, não fornece acesso à rede, mas apenas ao Panel Server. Além disso, apenas HTTPS tem autorização para ligação através desta VPN.

Dispositivos ligados

É recomendável que verifique regularmente a lista de dispositivos ligados à rede IEEE 802.15.4 do Panel Server. No caso de um dispositivo ligado desconhecido, localize-o e remova-o. Pode também reconstruir a rede e voltar a ligar apenas os dispositivos identificados.

Segurança de aplicações na nuvem

Segurança de dados em movimento

O Schneider Electric com aplicações na nuvem EcoStruxure implementam as melhores práticas, tais como:

- Todas as comunicações de e para EcoStruxure Panel Server with sistemas Schneider Electric internos ou sistemas externos de terceiros são encriptados utilizando HTTPS (o nível mínimo necessário é TLS 1.2).
- Os certificados envolvidos nestas sessões encriptadas tiram partido do algoritmo hash seguro SHA 256. Isto aplica-se às comunicações entre a aplicação Panel Server e os servidores nas plataformas na nuvem do Microsoft Azure.

Segurança de dados em pausa

A Schneider Electric segue as melhores práticas para criar soluções seguras e limitar o risco dos dados serem comprometidos de maneira significativa, ao mesmo que protege a privacidade, o controlo e a autonomia dos dados de cada cliente independentemente de qualquer outro.

Todas as credenciais e tokens de sistema para o sistema são armazenados e encriptados nas plataformas na nuvem do Microsoft Azure.

Pontos finais previstos

A Schneider Electric recomenda a permissão de acesso apenas aos domínios necessários de acordo com as suas necessidades.

A seguinte tabela lista os nomes de domínio e protocolos utilizados quando o Panel Server estabelece ligação à nuvem.

Nome de domínio	Protocolo	Descrição
cbBootStrap.gl.StruXureWareCloud.com	HTTPS (porta TCP 443)	Utilizado na primeira ligação do Panel Server à nuvem (ou após uma reposição de fábrica) para autenticar e registar o Panel Server.
etp.prod.StruXureWareCloud.com	HTTPS (porta TCP 443)	Utilizado para transferir a atualização de firmware.
cnm-ih-na.Dispositivos-Azure.net	HTTPS (porta TCP 443)	Utilizado para comunicação do Panel Server com serviços em nuvem da Schneider Electric, como configuração, dados ou alarmes.
RemoteShell.rsp.Schneider-Electric.com	HTTPS (porta TCP 443)	Permite que o Centro de atendimento ao cliente da Schneider Electric aceda de maneira remota às páginas Web do Panel Server através da VPN.
cnmdapiappstna.Blob.Core.Windows.net	HTTPS (porta TCP 443)	Permite que o Panel Server carregue registos e ficheiros de diagnóstico a pedido do Centro de atendimento ao cliente da Schneider Electric.
cnmiothubappstna.Blob.Core.Windows.net/file-upload	HTTPS (porta TCP 443)	Permite que o Panel Server carregue uma topologia para os serviços em nuvem da Schneider Electric.
time.gl.StruXureWareCloud.com	Porta NTP (UDP) 123)	O servidor NTP permite que o relógio do Panel Server permaneça sincronizado.

NOTA: Os nomes de domínio não são sensíveis a maiúsculas e minúsculas.

Segurança física do dispositivo

Etiqueta de indicação de adulteração

O EcoStruxure Panel Server tem uma etiqueta de indicação de adulteração que ajuda a proteger a segurança física do dispositivo. Deve estar limpa e não apresentar sinais de adulteração (por exemplo, rasgos, danos ou riscos). A Schneider Electric não aconselha a utilização de um dispositivo que tenha sido visivelmente adulterado.

Instalação

Para ajudar a proteger a segurança física do dispositivo, aconselha-se a seguinte instalação:

- Instale o EcoStruxure Panel Server num armário protegido de maneira adequada ao nível de risco da instalação (por exemplo, um armário com cadeado ou chave).
- Se o EcoStruxure Panel Server estiver montado num quadro elétrico, instale o quadro elétrico numa sala segura (por exemplo, com porta ou câmara bloqueada).

  NOTA: A proteção da segurança física do dispositivo inclui a proteção do código QR. O código QR permite acesso ao código do dispositivo do Panel Server, que deve ser considerado como uma credencial para o dispositivo. É utilizado:

  - Na reivindicação segura do dispositivo para aplicações na nuvem
  - Como palavra-passe para ligação ao ponto de acesso Wi-Fi

Gestão de palavras-passe

Para ajudar a proteger o dispositivo de ataques maliciosos, altere a palavra-passe de utilizador e palavra-passe do ponto de acesso Wi-Fi Panel Server utilizando as páginas Web Panel Server.

A palavra-passe de utilizador e a palavra-passe de SupportUser devem estar em conformidade com as seguintes regras:

- Entre 8 e 50 carateres
- Deve conter pelo menos três dos seguintes tipos de carateres:
  - Maiúsculas
  - Minúsculas
  - Dígitos
  - Carateres especiais (limitados ao caráter de espaço e !"#$%&'()*+,-./:;<=>?@[\]^_`{|}~)

A palavra-passe do ponto de acesso Wi-Fi deve estar em conformidade com as seguintes regras:

- Entre 8 e 32 carateres
- Deve conter pelo menos um dos seguintes tipos de carateres:
  - Maiúsculas
  - Minúsculas
  - Dígitos
- Pode conter carateres especiais (limitados a carateres de espaço e !"#$%&'()*+,-./:;<=>?@[]^_`{|}~)

Função de cópia de segurança

Quando transferir um ficheiro de cópia de segurança, encripte o ficheiro com uma palavra-passe segura, composta por:

- Entre 6 e 32 carateres
- Pelo menos um dos seguintes tipos de carateres:
  - Maiúsculas
  - Minúsculas
- Carateres especiais (limitados ao caráter de espaço e !"#$%&'()*+,-./:;<=>?@[]^_`{|}~)

Recomendações de segurança em termos de manutenção

Tópicos relacionados

- Operações de manutenção
- Verificação da funcionalidade de segurança

Operações de manutenção

Ao longo da vida útil do EcoStruxure Panel Server, é recomendável realizar com frequência as seguintes operações:

- Verifique a segurança física do EcoStruxure Panel Server (consulte a etiqueta indicadora de adulteração, página 20).
- Certifique-se de que tem a atualização de firmware mais recente. Deve efetuar o registo para receber notificações de segurança, página 13.
- Verifique a presença de dispositivos desconhecidos nos dispositivos ligados, página 18.
- Verifique se existem comportamentos inesperados nos registos de auditoria, página 15, tais como tentativas de início de sessão inválidas ou reinicialização frequente.
- Verifique a data e a hora, página 13 para evitar desvios da data atual.
- Certifique-se de que todos os serviços e funcionalidades desnecessários estão desativados, página 13.

Tópicos relacionados

- Recomendações de segurança em termos de manutenção (Parent Topic)

Verificação da funcionalidade de segurança

Os seguintes testes permitem-lhe verificar o funcionamento pretendido das funções de segurança através das páginas Web do EcoStruxure Panel Server.

Autenticação Web

1. Tente iniciar sessão nas páginas Web EcoStruxure Panel Serversem palavra--passe ou introduza uma palavra-passe incorreta.

   Resultado: O EcoStruxure Panel Server não lhe fornece acesso às páginas Web.
2. Repita esta ação mais 9 vezes.

   Resultado: O EcoStruxure Panel Server bloqueia durante 10 minutos.
3. Tente novamente 5 vezes.

   Resultado: O EcoStruxure Panel Server bloqueia durante 60 minutos.

Autorização Web

1. Inicie sessão nas páginas Web EcoStruxure Panel Server.
2. Marcar uma página Web (por exemplo, **Definições**)

3. Abra uma janela de navegação privada no browser e abra a página Web marcada anteriormente.

   Resultado: Não é possível aceder à página Web, mas é redirecionado para a página de início de sessão.

Auditoria

1. Após alguns ou todos os testes anteriores, aceda à página Web Registos.
2. Transfira os ficheiros de registo.
3. Verifique se as tentativas falhadas estão indicadas nos registos.

Atualização de firmware

1. Vá para a página Web **Atualização de firmware**.
2. Carregue um ficheiro aleatório (por exemplo, uma imagem ou um documento de texto).

   Resultado: O EcoStruxure Panel Server comunica uma assinatura incorreta.
3. Aceda aos registos de auditoria.
4. Verifique se a atualização de firmware falhada está presente nos registos.

Desativar serviços

1. Para aceder ao menu para desativar os serviços, selecione **Definições > Comunicação de rede > DPWS**.
2. Ligue um PC com o sistema operativo Windows à mesma rede local.
3. Clique em Rede a partir do Explorador de ficheiros.

   Resultado: O EcoStruxure Panel Server não foi detetado e, por conseguinte, não aparece na lista de dispositivos na rede.

Desativar serviços sem fios

Para aceder aos menus para desativar temporariamente os serviços sem fios:

- No que respeita à Wi-Fi, navegue para **Definições > Comunicação de rede > Wi-Fi**, clique no botão **Ativação da Wi-Fi** e guarde as alterações.

  Resultado: Na interface de gestão do ponto de acesso de Wi-Fi, não existe um EcoStruxure Panel Server ligado.
- No que respeita a IEEE 802.15.4, navegue para **Definições > Dispositivos sem fios > Configuração de rede**, clique no cursor deslize **Ativação sem fios** e guarde as alterações.

  Resultado: Todos os dispositivos sem fios listados em **Definições > Dispositivos sem fios > Dispositivos sem fios** indicam o estado **Não ligado** após um determinado período de tempo, dependendo do dispositivo sem fios (consulte a documentação do dispositivo para obter mais detalhes).

Tópicos relacionados

- Recomendações de segurança em termos de manutenção (Parent Topic)

Glossário

C

Código de instalação:

Um código único de 36 carateres associado a um dispositivo Modbus que lhe permite iniciar uma deteção do dispositivo com maior segurança a partir do Panel Server.

D

DHCP - Protocolo de configuração dinâmica do anfitrião:

Um protocolo de gestão de rede utilizado em redes de protocolo Internet para atribuir automaticamente endereços IP e outros parâmetros de comunicação aos dispositivos ligados à rede, utilizando uma arquitetura de cliente/servidor.

DPWS - Perfil de dispositivos para serviços Web:

Conjunto mínimo de restrições de implementação que ajuda a ativar mensagens seguras do serviço Web, deteção, descrição e eventos em dispositivos com recursos restritos.

H

HTTP - Protocolo de transferência de hipertexto:

Um protocolo de rede que gere a entrega de ficheiros e dados na World Wide Web.

HTTPS - Protocolo de transferência de hipertexto seguro:

Uma variante do protocolo de transferência Web padrão (HTTP) que adiciona uma camada de segurança aos dados em trânsito através de uma ligação de protocolo SSL (Secure Socket Layer) ou TLS (Transport Layer Security).

I

IEEE 802.15.4:

Norma definida pelo IEEE e utilizada pelo EcoStruxure Panel Server para comunicar com dispositivos sem fios.

IP - Protocolo de Internet:

Os endereços IP são utilizados para identificar dispositivos ligados à intranet da empresa ou à Internet.

L

LAN - Rede local:

Refere-se à intranet da empresa ou à rede de TI.

M

Modbus TCP/IP:

Um protocolo que fornece comunicação cliente/servidor entre dispositivos e TCP/ /IP que fornece comunicações através de uma ligação Ethernet.

N

NTP - Protocolo de tempo de rede:

Um protocolo de rede para sincronização de relógio entre sistemas informáticos através de redes de dados de latência variável e comutadas por pacotes.

P

PKI - Infraestrutura de chave pública:

Define um conjunto de serviços utilizados para gerar e autenticar assinaturas digitais. A infraestrutura de chave pública é concebida para garantir a confidencialidade, integridade e autenticidade da informação.

Política de segurança:

A política de segurança do sistema são as definições de segurança aplicadas em todo o sistema protegido. Uma política de segurança refere-se, em geral, à utilização de normas. É utilizada para definir qualquer configuração relacionada com a segurança partilhada entre todos os dispositivos.

R

RSTP - Protocolo Rapid Spanning Tree:

Um protocolo de rede que promove uma elevada disponibilidade e topologia sem ciclo nas redes Ethernet.

S

SCADA - Supervisory control and data acquisition:

Refere-se a sistemas concebidos para obter dados em tempo real sobre processos de produção e equipamentos para monitorizá-los e controlá-los a nível remoto.

SDL - Ciclo de vida do desenvolvimento seguro:

Uma estrutura de desenvolvimento de produto que ajuda a garantir que os produtos seguem processos de design seguros em todas as fases do ciclo de vida.

SFTP - Secure File Transfer Protocol:

Uma versão segura do Protocolo de transferência de ficheiros que facilita o acesso a dados e a transferência de dados através de um fluxo de dados de Secure Shell (SSH).

T

TCP/IP - Transmission control protocol/Internet protocol:

Refere-se ao conjunto de protocolos utilizados para comunicação através da Internet.

TI - Tecnologias da informação:

Refere-se aos sistemas informáticos e à rede de informação da empresa por oposição à sua rede de TO (tecnologia operacional).

TO - Tecnologia operacional:

Refere-se aos sistemas de hardware e software que a empresa utiliza para monitorizar e controlar diretamente os processos e equipamentos de produção, também apelidada de rede de controlo industrial (IC). A TO é frequentemente utilizada para referir-se à rede operacional da empresa em vez da respetiva rede de TI.

V

VPN - Rede privada virtual:

A VPN é utilizada para estabelecer um “túnel” seguro/privado entre um ponto de acesso externo autenticado e a rede empresarial fidedigna.

Schneider Electric
35 rue Joseph Monier
92500 Rueil Malmaison
França

+ 33 (0) 1 41 29 70 00

www.se.com

Como as normas, especificações e desenhos são periodicamente actualizados, solicite a confirmação das informações incluídas nesta publicação.

DOCA0211PT-13