



EcoStruxure Panel Server

Guía de ciberseguridad

Pasarela Modbus y concentrador de dispositivos inalámbricos, registrador de datos y servidor de energía

EcoStruxure ofrece una arquitectura y plataforma compatibles con el IoT.

DOCA0211ES-14
01/2026



Información legal

La información proporcionada en este documento contiene descripciones generales, características técnicas o recomendaciones relacionadas con productos o soluciones.

Este documento no pretende sustituir a un estudio detallado o un plan de desarrollo o esquemático específico de operaciones o sitios. No debe usarse para determinar la adecuación o la fiabilidad de los productos o las soluciones para aplicaciones de usuario específicas. Es responsabilidad del usuario realizar o solicitar a un experto profesional (integrador, especificador, etc.) que realice análisis de riesgos, evaluación y pruebas adecuados y completos de los productos o las soluciones con respecto a la aplicación o el uso específicos de dichos productos o dichas soluciones.

La marca Schneider Electric y cualquier otra marca comercial de Schneider Electric SE y sus filiales mencionadas en este documento son propiedad de Schneider Electric SE o sus filiales. Todas las otras marcas pueden ser marcas comerciales de sus respectivos propietarios.

Este documento y su contenido están protegidos por las leyes de copyright aplicables, y se proporcionan exclusivamente a título informativo. Ninguna parte de este documento puede ser reproducida o transmitida de cualquier forma o por cualquier medio (electrónico, mecánico, fotocopia, grabación u otro), para ningún propósito, sin el permiso previo por escrito de Schneider Electric.

Schneider Electric no otorga ningún derecho o licencia para el uso comercial del documento o su contenido, excepto por una licencia no exclusiva y personal para consultarla "tal cual".

Schneider Electric se reserva el derecho de realizar cambios o actualizaciones con respecto a o en el contenido de este documento o con respecto a o en el formato de dicho documento en cualquier momento sin previo aviso.

En la medida permitida por la ley aplicable, Schneider Electric y sus filiales no asumen ninguna responsabilidad u obligación por cualquier error u omisión en el contenido informativo de este documento o por el uso no previsto o el mal uso del contenido de dicho documento.

Tabla de contenido

Información de seguridad	5
Acerca del documento	6
Introducción a la ciberseguridad.....	9
Características del dispositivo	10
Acciones recomendadas para la ciberseguridad	12
Funciones del dispositivo.....	14
Seguridad de red.....	16
Seguridad de la aplicación en la nube	19
Seguridad física del dispositivo	21
Recomendaciones de seguridad para el mantenimiento	23
Glosario	25

Información de seguridad

Información importante

Lea atentamente estas instrucciones y observe el equipo para familiarizarse con el dispositivo antes de instalarlo, utilizarlo, revisarlo o realizar su mantenimiento. Los mensajes especiales que se ofrecen a continuación pueden aparecer a lo largo de la documentación o en el equipo para advertir de peligros potenciales, o para ofrecer información que aclara o simplifica los distintos procedimientos.



La inclusión de este icono en una etiqueta "Peligro" o "Advertencia" indica que existe un riesgo de descarga eléctrica, que puede provocar lesiones si no se siguen las instrucciones.



Éste es el icono de alerta de seguridad. Se utiliza para advertir de posibles riesgos de lesiones. Observe todos los mensajes que siguen a este icono para evitar posibles lesiones o incluso la muerte.

PELIGRO

PELIGRO indica una situación de peligro que, si no se evita, **provocará** lesiones graves o incluso la muerte.

ADVERTENCIA

ADVERTENCIA indica una situación de peligro que, si no se evita, **podría provocar** lesiones graves o incluso la muerte.

ATENCIÓN

ATENCIÓN indica una situación peligrosa que, si no se evita, **podría provocar** lesiones leves o moderadas.

AVISO

AVISO indica una situación potencialmente peligrosa que, si no se evita, **puede provocar** daños en el equipo.

Tenga en cuenta

La instalación, manejo, puesta en servicio y mantenimiento de equipos eléctricos deberán ser realizados sólo por personal cualificado. Schneider Electric no se hace responsable de ninguna de las consecuencias del uso de este material.

Una persona cualificada es aquella que cuenta con capacidad y conocimientos relativos a la construcción, el funcionamiento y la instalación de equipos eléctricos, y que ha sido formada en materia de seguridad para reconocer y evitar los riesgos que conllevan tales equipos.

Acerca del documento

Ámbito del documento

Esta guía proporciona información sobre aspectos de ciberseguridad en EcoStruxure™ Panel Server a fin de ayudar a los diseñadores y operadores de sistemas a promover un entorno de funcionamiento seguro para el producto.

En esta guía, no se abarca el tema general de cómo proteger su red de tecnología operativa o su red Ethernet empresarial. Para ver una introducción general a las amenazas de ciberseguridad y cómo afrontarlas, consulte [Información de ciberseguridad general](#), página 6.

NOTA: En esta guía, el término **seguridad** se utiliza para hacer referencia a la ciberseguridad.

Nota de validez

La información de esta guía es relevante para EcoStruxure Panel Server con la versión de firmware 002.005.000 o superior.

Información online

La información incluida en esta guía está sujeta a actualizaciones en cualquier momento. Schneider Electric recomienda encarecidamente tener la versión más reciente y actualizada que está disponible en www.se.com/ww/en/download.

Las características técnicas de los dispositivos que se describen en este documento también se encuentran online. Para acceder a la información online, vaya a la página de inicio de Schneider Electric en www.se.com.

Información general sobre ciberseguridad

En los últimos años, el creciente número de equipos y plantas de producción conectados a la red ha aumentado de la mano del potencial de las amenazas cibernéticas, como el acceso no autorizado, violaciones de datos e interrupciones operativas. Por lo tanto, es recomendable considerar todas las medidas de ciberseguridad posibles con el fin de ayudar a proteger los activos y los sistemas de dichas amenazas.

Para mantener sus productos de Schneider Electric seguros y protegidos, es conveniente que implemente las prácticas recomendadas de ciberseguridad que se indican en el documento [Cybersecurity Best Practices](#).

Schneider Electric proporciona información y asistencia adicionales:

- Suscríbase al [boletín de seguridad](#) de Schneider Electric .
- Consulta la página web de [Cybersecurity Support Portal](#) para:
 - Buscar notificaciones de seguridad.
 - Notificar vulnerabilidades e incidentes.
- Consulta la página web de [Schneider Electric Cybersecurity and Data Protection Posture](#) para:
 - Acceder a la perspectiva de ciberseguridad.
 - Obtener más información sobre la ciberseguridad en la academia de ciberseguridad.
 - Explorar los servicios de ciberseguridad de Schneider Electric.

Información de ciberseguridad relacionada con el producto

⚠ ADVERTENCIA

RIESGO POTENCIAL PARA LA DISPONIBILIDAD, LA INTEGRIDAD Y LA CONFIDENCIALIDAD DEL SISTEMA

- Desactive los puertos o servicios no utilizados para reducir al mínimo las vías de acceso de atacantes dañinos.
- Ponga los dispositivos en red tras varias capas de ciberdefensas (como cortafuegos, segmentación de red y protección y detección de intrusiones en red).
- Siga las prácticas recomendadas de ciberseguridad (por ejemplo, privilegio mínimo, separación de tareas) para evitar exposiciones no autorizadas, pérdidas, modificaciones de datos y registros o interrupciones de los servicios.

Si no se siguen estas instrucciones, pueden producirse lesiones graves, muerte o daños en el equipo.

Idiomas disponibles del documento

Este documento está disponible en los siguientes idiomas:

- Inglés (DOCA0211EN), idioma original
- Francés (DOCA0211FR)
- Alemán (DOCA0211DE)
- Italiano (DOCA0211IT)
- Portugués (DOCA0211PT)
- Español (DOCA0211ES)

Documentos relacionados

Título de la documentación	Número de referencia
<i>EcoStruxure Panel Server - Guía del usuario</i>	DOCA0172EN DOCA0172DE DOCA0172ES DOCA0172FR DOCA0172IT DOCA0172PT
<i>Prácticas recomendadas de ciberseguridad</i>	7EN52-0390
<i>EcoStruxure Power - Guide for Designing and Implementing a Cyber Secure Digital Power System - Technical Guide</i>	ESXP2TG003EN

Puede descargar estas publicaciones técnicas y otra información técnica de nuestro sitio web en www.se.com/ww/en/download/.

Información sobre terminología no inclusiva o insensible

Como empresa responsable e inclusiva, Schneider Electric actualiza constantemente sus comunicaciones y productos que contienen terminología no inclusiva o insensible. Sin embargo, a pesar de estos esfuerzos, nuestro contenido aún puede contener términos que algunos clientes consideren inapropiados.

Marcas comerciales

QR Code es una marca comercial registrada de DENSO WAVE INCORPORATED en Japón y otros países.

Introducción a la ciberseguridad

Área principal EcoStruxure

EcoStruxure es el sistema de plataforma y arquitectura compatible con el IoT, de uso inmediato, abierto e interoperativo de Schneider Electric. Está disponible para hogares, edificios, centros de datos, infraestructuras e industrias. Innovación a todos los niveles, desde los productos conectados hasta el control perimetral, y las aplicaciones, los análisis y los servicios.

Introducción

La ciberseguridad tiene como objetivo contribuir a proteger su red de comunicaciones y todos los equipos conectados a ella frente a ataques que puedan interrumpir las operaciones (disponibilidad), modificar la información (integridad) o revelar información confidencial (confidencialidad). El objetivo de la ciberseguridad es proporcionar mayores niveles de protección contra robo, corrupción, mal uso o accidentes de la información y los activos físicos y, a la vez, garantizar el acceso a los usuarios legítimos. Hay muchos aspectos que tener en cuenta por lo que respecta a la ciberseguridad, incluido el diseño de sistemas seguros, la restricción del acceso utilizando métodos físicos y digitales, la identificación de los usuarios y la implementación de procedimientos de seguridad y políticas de mejores prácticas.

Directrices de Schneider Electric

Además de las recomendaciones que se ofrecen en esta guía, que son específicas del Panel Server, debe seguir el método de defensa exhaustivo de Schneider Electric para la ciberseguridad y la información de ciberseguridad general, página 6.

Políticas y reglas de ciberseguridad de Schneider Electric

Schneider Electric usa un proceso Secure Development Lifecycle (SDL), un marco clave de desarrollo de productos que contribuye a garantizar que los productos sigan procesos de diseño seguros durante todas las etapas del ciclo de vida. El proceso SDL de Schneider Electric cumple IEC 62443-4-1.

El proceso SDL incluye lo siguiente:

- Prácticas SDL aplicadas a acciones de desarrollo internas, en toda la cadena de suministro.
- Revisión de seguridad final requerida para publicar el proyecto.
- Formación en seguridad para el personal que participa en el desarrollo de productos.

Características del dispositivo

Descripción general

El EcoStruxure Panel Server está equipado con funciones de seguridad. Estas funciones están en estado preconfigurado y pueden modificarse para adaptarlas a las necesidades de su instalación. El Panel Server solo debe configurarlo y establecerlo personal cualificado, ya que deshabilitar o cambiar ajustes afecta a la seguridad general de Panel Server y a la seguridad de su red.

Use esta guía junto con DOCA0172•• *EcoStruxure Panel Server - Guía del usuario*, página 7 para obtener información detallada sobre la configuración de las funciones y los ajustes de Panel Server.

Interfaces del EcoStruxure Panel Server

La siguiente tabla resume las arquitecturas de comunicación disponibles con Panel Server por modelo:

Característica		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	PAS600PWD 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	
Ethernet 10/100BASE-T	Un puerto RJ45	✓	-	-	-	-	-	-	-	-	-	-	-	-	-	
	Dos puertos RJ45	-	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
Conectividad Modbus TCP/IP aguas arriba		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
Conectividad Wi-Fi aguas arriba		✓	✓	✓	✓	✓	✓	-	-	✓	✓	✓	✓	✓	✓	
Conectividad Modbus TCP/IP aguas abajo		-	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
Conectividad IEEE 802.15.4 aguas abajo		✓	✓	✓	✓	✓	✓	-	-	✓	✓	✓	✓	✓	✓	
Conectividad Modbus-SL aguas abajo		-	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
Dos entradas digitales (para WAGES [agua, aire, gas, electricidad o vapor])		-	-	-	-	✓	✓	✓	-	-	-	✓	✓	-	-	
Antena externa Wi-Fi		-	✓	✓	✓	✓	✓	-	-	✓	✓	✓	✓	✓	✓	
Antena externa IEEE 802.15.4		-	-	✓	-	-	✓	-	-	✓	✓	✓	✓	✓	✓	
Punto de acceso Wi-Fi		✓	✓	✓	✓	✓	✓	-	-	✓	✓	✓	✓	✓	✓	
Notificación de alarmas por correo electrónico		-	-	-	-	-	-	-	-	✓	✓	✓	✓	✓	✓	
Publicación en servidor SFTP o HTTPS		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	

Convención

En adelante, el EcoStruxure Panel Server pasará a denominarse Panel Server.

Protocolos compatibles

El EcoStruxure Panel Server admite los siguientes protocolos:

- DHCP para el direccionamiento IP en la red
- DNS para la resolución de nombres de red
- DPWS para la detección de redes
- HTTPS (TLS v1.2) para configuración a través de herramientas de configuración y páginas web integradas
- IEEE 802.15.4 para comunicación inalámbrica con comunicación por radiofrecuencia de banda ISM 2,4 GHz (no disponible para modelos Wired by Design)
- Modbus TCP y Modbus-SL para comunicaciones con otros dispositivos de tecnología operativa (OT)
- NTP para la sincronización horaria
- RSTP para permitir topologías en anillo Ethernet sólidas en aplicaciones críticas
- SFTP para la publicación de archivos CSV en un servidor SFTP
- Cliente VPN para acceso remoto (abierto al Centro de Atención al Cliente de Schneider Electric)
- WPA2 y WPA para comunicación Wi-Fi (no disponible para modelos Wired by Design)

Funciones de seguridad

El EcoStruxure Panel Server admite las siguientes funciones de seguridad:

- Solo el firmware firmado digitalmente por Schneider Electric puede instalarse en Panel Server.
- En cada arranque, la firma digital del firmware se valida antes de la ejecución para garantizar que no se ha manipulado.
- Las contraseñas de usuario se almacenan como contraseñas con sal y hash (SHA256).
- Para borrar toda la información de Panel Server, use el botón Reiniciar.
- El dispositivo tiene un reloj interno y recuerda su fecha y hora durante unos meses sin alimentación.
- La clave de autenticidad de Panel Server se almacena en un chip Common Criteria CC EAL6+ muy seguro.

Acciones recomendadas para la ciberseguridad

Su dispositivo está diseñado para utilizarse en un entorno protegido que emplea una estrategia de defensa en profundidad.

Para contribuir a proteger el dispositivo, deberá tomar medidas específicas en todas las fases del ciclo de vida del proyecto.

NOTA: La siguiente es una lista no exhaustiva de las posibles medidas de ciberseguridad que se recomienda tomar. Su propósito es servir de punto de partida para mejorar la seguridad del dispositivo en un entorno protegido. No obstante, deberá consultar con expertos en ciberseguridad para planificar, configurar, operar, mantener y desmantelar el dispositivo en función de sus necesidades específicas.

La siguiente tabla enumera las acciones recomendadas en cada fase del ciclo de vida para contribuir a proteger su dispositivo en un entorno protegido:

Fase del ciclo de vida	Acción recomendada	Función en la estrategia de defensa en profundidad
Planificar	Estudiar la percepción sobre ciberseguridad, página 6	Use los recursos disponibles para aumentar el conocimiento y la percepción sobre ciberseguridad.
	Estudie las suposiciones sobre la defensa en profundidad del sistema. Seguir las recomendaciones de esta guía	Entienda las medidas de seguridad que se prevé que se apliquen en el entorno externo en el que va a utilizarse el dispositivo. Estas incluyen, entre otras: - Seguridad del sitio y de la ubicación del dispositivo - Seguridad de la red
	Revisar las funciones de seguridad del dispositivo Consulte <i>Capacidades de seguridad</i> en Guía de usuario de DOCA0172** Panel Server, página 7.	Entienda cómo pueden utilizarse las funciones de seguridad del dispositivo en un entorno protegido.
	Revisar los riesgos de seguridad y los controles de compensación Consulte <i>Capacidades de seguridad</i> en Guía de usuario de DOCA0172** Panel Server, página 7.	Comprenda los riesgos de seguridad conocidos y los controles de compensación para ayudar a reducir al mínimo los riesgos.
Instalar y configurar	Comprobar el estado de la etiqueta antimanipulación antes de instalar el dispositivo, página 21	La etiqueta antimanipulación impide que se modifique el dispositivo antes de su instalación.
	Seguir las instrucciones de instalación, página 21	Ayuda a reducir el acceso físico no autorizado.
	En el primer inicio de sesión, cambiar la contraseña predeterminada Consulte <i>Gestión de usuarios</i> en Guía de usuario de DOCA0172** Panel Server, página 7.	Ayuda a reducir los accesos no autorizados. Los ajustes de cuenta predeterminados suelen ser una causa frecuente de accesos no autorizados por parte de usuarios malintencionados.
	Cambiar la contraseña de usuario de Panel Server y la contraseña del punto de acceso Wi-Fi Consulte <i>Gestión de usuarios y Punto de acceso Wi-Fi</i> en Guía de usuario de DOCA0172** Panel Server, página 7.	Crear contraseñas seguras siguiendo las directrices Los ajustes de cuenta predeterminados y las contraseñas no seguras suelen ser una causa frecuente de accesos no autorizados por parte de usuarios malintencionados.
	Deshabilitar los protocolos y los puertos que no se usen, página 14	Deshabilite los protocolos y los puertos de comunicación innecesarios y que no se utilicen, por ejemplo, Wi-Fi, punto de acceso Wi-Fi, IEEE.802.15.4.
Operar	Cifrar los archivos de configuración de copia de seguridad, página 21	Utilice contraseñas seguras para cifrar los archivos de copia de seguridad de la configuración. Los archivos desprotegidos y las contraseñas no seguras pueden causar accesos no autorizados por parte de usuarios malintencionados
	Gestionar el acceso a los dominios, página 19	Limite el acceso a los dominios conocidos y necesarios, según sus necesidades.
	Notificar incidentes o vulnerabilidades de ciberseguridad, página 6	Notifique cualquier actividad sospechosa, incidente de ciberseguridad o vulnerabilidad en la página web del Portal de asistencia de ciberseguridad de Schneider Electric.
Mantener	Mantener el firmware actualizado Consulte <i>Actualización de firmware</i> en Guía de usuario de DOCA0172** Panel Server, página 7.	Actualice a la versión más reciente del firmware para beneficiarse de sus parches de seguridad.

Fase del ciclo de vida	Acción recomendada	Función en la estrategia de defensa en profundidad
	Consultar el registro de auditoría para detectar comportamientos inesperados Consulte <i>Registros de diagnóstico</i> en Guía de usuario de DOCA0172** Panel Server, página 7.	Consulte los registros de auditoría para detectar actividades inesperadas y para contribuir a identificar la causa de brechas de ciberseguridad que podrían provocar incidentes de ciberseguridad.
	Comprobar regularmente el estado de la etiqueta antimanipulación, página 21	La etiqueta antimanipulación impide que se modifique el dispositivo.
	Comprobar los dispositivos conectados para asegurarse de que no haya dispositivos desconocidos, página 18	Localice y elimine los dispositivos desconocidos para ayudar a proteger el sistema contra brechas de ciberseguridad.
	Mantener actualizada la seguridad de redes	Ayuda a minimizar los puntos de ataque y reduce la probabilidad de experimentar vulnerabilidades.
	Realizar auditorías de seguridad	Ayuda a verificar el estado de seguridad del sistema.
Desmantelar	Restablecer el dispositivo con la configuración de fábrica Consulte <i>Recomendaciones de seguridad para el desmantelamiento</i> en Guía de usuario de DOCA0172** Panel Server, página 7.	Ayuda a evitar una posible revelación de datos.

Funciones del dispositivo

Actualización de firmware

Actualice EcoStruxure Panel Server a la versión de firmware más reciente para obtener las funciones más recientes y tener actualizados los parches de seguridad. Todo el firmware diseñado para EcoStruxure Panel Server está firmado con la infraestructura de clave pública (PKI) de Schneider Electric para contribuir a garantizar la integridad y la autenticidad del firmware que se ejecuta en EcoStruxure Panel Server. Para que la PKI funcione correctamente, mantenga sincronizada la fecha del dispositivo (consulte [Fecha y hora](#), página 14).

Si desea que recibir información sobre actualizaciones de seguridad, regístrese en [Security Notifications](#) en Cybersecurity Support Portal de Schneider Electric.

Fecha y hora

Es importante mantener la fecha y la hora sincronizadas para los siguientes propósitos:

- Para evitar errores en los certificados y las firmas digitales en el EcoStruxure Panel Server
- Para proporcionar una marca de tiempo precisa en los registros de auditoría para ayudar a la seguridad forense

Para obtener más información sobre la fecha y la hora, consulte [DOCA0172](#)•• *EcoStruxure Panel Server - Guía del usuario*, página 7.

Desactivar funciones no utilizadas

EcoStruxure Panel Server le permite desactivar los puertos y los servicios no utilizados para contribuir a reducir al mínimo las vías de acceso de atacantes dañinos.

Se recomienda desactivar:

- Activación e infraestructura del Wi-Fi. El Wi-Fi puede desactivarse permanentemente si es necesario.
- Punto de acceso Wi-Fi (activado de forma predeterminada). Si el punto de acceso está desactivado, pulsar el botón en la parte frontal del Panel Server no activará el punto de acceso. La desactivación de la activación del Wi-Fi también desactiva el punto de acceso Wi-Fi e interrumpe cualquier conexión activa.
- IEEE 802.15.4 (no activo de forma predeterminada). El IEEE 802.15.4 se puede desactivar de forma permanente.
- Servicios de pasarela Modbus (activados de forma predeterminada). Se puede desactivar en cada interfaz (Ethernet 1, Ethernet 2 o Wi-Fi) de las páginas web de Panel Server.
- DPWS (protocolo de detección sobre IP v4/6; activo de forma predeterminada).
- Protocolo de árbol de expansión rápida RSTP (no activado de forma predeterminada)

NOTA: Wi-Fi e IEEE 802.15.4 no están disponibles de forma nativa en modelos Wired by Design (WD) que no cuentan con un chipset inalámbrico.

Para obtener más información sobre cómo deshabilitar las funciones sin utilizar de EcoStruxure Panel Server, consulte [DOCA0172](#)•• *EcoStruxure Panel Server - Guía del usuario*, página 7.

Puertos TCP

Los siguientes puertos TCP se utilizan en EcoStruxure Panel Server:

- Puerto 443: HTTPS
- Puerto 502: Modbus
- Puerto 5357: DPWS (puede cambiarse)

NOTA: El Panel Server no incorpora ningún tipo de servidor SSH.

Registros de auditoría

EcoStruxure Panel Server genera registros de auditoría que registran eventos como actualizaciones de firmware e intentos de inicio de sesión no válidos.

Los registros no contienen información personal.

Para detectar comportamientos inesperados (por ejemplo, reinicios frecuentes, actualizaciones incorrectas del firmware o intentos de inicio de sesión no válidos), se recomienda supervisar periódicamente los registros de auditoría. Para obtener más información sobre los registros de diagnóstico, consulte

DOCA0172• *EcoStruxure Panel Server - Guía del usuario*, página 7.

Eliminación del dispositivo

EcoStruxure Panel Server contiene información confidencial configurada durante la puesta en marcha, valores de datos recientes y registros. Por ejemplo, esta información puede incluir la topología del dispositivo Modbus, las redes inalámbricas, las contraseñas Wi-Fi o los consumos de energía medidos.

Es necesario realizar un restablecimiento de los ajustes predeterminados antes de eliminar EcoStruxure Panel Server. Debe tener acceso físico para apagar y encender EcoStruxure Panel Server durante la ejecución de este procedimiento. Consulte cómo restablecer los ajustes de fábrica de EcoStruxure Panel Server en DOCA0172• *EcoStruxure Panel Server - Guía del usuario*, página 7.

Seguridad de red

Introducción

El EcoStruxure Panel Server no está diseñado para soportar la exposición directa al Internet público. Debe instalarse como mínimo tras la traducción de direcciones de red (NAT) o, preferiblemente, tras varios cortafuegos. Si desea más información, consulte los siguientes sitios web:

- Servicios de consultoría de ciberseguridad de Schneider Electric
- Instituto Nacional de Estándares y Tecnología de los Estados Unidos (NIST)
- Agencia de la Unión Europea para la Ciberseguridad (ENISA)

Segmentación de red

El EcoStruxure Panel Server es una pasarela. Crea un puente entre redes distintas. La segmentación de la red ayuda a garantizar la ciberdefensa. Para mejorar la segmentación de la red, Panel Server Universal y Advanced disponen de dos puertos Ethernet. Se pueden emplear de forma independiente para tener un puerto dedicado a las tecnologías de la información (TI) y otro a la tecnología operativa (OT). La segmentación de la red le permite mantener segmentadas las redes OT y de TI, ya que los paquetes de red no se reenvían de un lado al otro.

Se recomienda configurar la red por separado (para obtener más información acerca de los ajustes de red, consulte [DOCA0172•• EcoStruxure Panel Server - Guía del usuario](#), página 7).

Esto le permite conectar Panel Server a lo siguiente:

- Dispositivos OT aguas abajo a través de Modbus TCP en un puerto Ethernet.
- PC de TI aguas arriba con SCADA y puesta en marcha de aplicaciones de software en el otro puerto Ethernet.

HTTPS y Modbus están disponibles en las interfaces Ethernet de Panel Server (ETH1, ETH2) y Wi-Fi.

La siguiente tabla presenta la configuración predeterminada para cada interfaz:

Interfaz		Modbus
Ethernet en topología conmutada		Activada
Ethernet en topología independiente	Puerto ETH1	Activado
	Puerto ETH2	Desactivado
Infraestructura Wi-Fi		Desactivado
Punto de acceso Wi-Fi		No disponible

Se recomienda inhabilitar el servicio Modbus en las redes donde no se utiliza. Para obtener más información acerca de la activación del servicio, consulte [DOCA0172•• EcoStruxure Panel Server - Guía del usuario](#), página 7.

Certificado de servidor web del producto

Para admitir comunicaciones HTTP seguras, EcoStruxure Panel Server tiene un certificado X.509v3 de forma predeterminada. Este certificado contribuye a garantizar la integridad y la confidencialidad a la hora de configurar la comunicación HTTPS.

Los navegadores solo reconocen certificados para sitios web públicos. Como Panel Server se instala en una red de área local (LAN), los navegadores no

pueden distinguir un Panel Server de otro. Por lo tanto, aparece un mensaje de seguridad en el navegador al conectarse a Panel Server.

Una conexión con cable directa ayuda a proteger la vía de comunicación con Panel Server. Para obtener más información sobre el primer acceso a las páginas web del EcoStruxure Panel Server desde el PC, consulte DOCA0172**
EcoStruxure Panel Server - Guía del usuario, página 7.

Huella digital de la clave del servidor SFTP

Si publica sus datos en un servidor SFTP, asegúrese de que la huella digital de la clave, que se muestra al configurar la dirección del servidor, coincida con la clave SFTP del servidor.

Si renueva la clave SFTP del servidor, el Panel Server ya no podrá enviar los archivos porque la conexión no se autenticará. Debe volver a configurar la publicación del Panel Server para grabar la nueva huella digital de la clave SFTP.

Red inalámbrica

Los protocolos de radio son vulnerables a las infracciones de la seguridad física. Por ejemplo, un ataque por denegación de servicio puede interferir intencionadamente con la señal de radio mediante un emisor de radio potente situado cerca.

Por lo tanto, se recomienda adaptar la seguridad física a la importancia de la información que depende de los protocolos de radio. Para ello, las redes inalámbricas (Wi-Fi e IEEE 802.15.4) se pueden desactivar de forma permanente en el Panel Server. Si cree que nunca necesitará redes inalámbricas (Wi-Fi e IEEE 802.15.4), únicamente en este caso podrá desactivarlas de forma permanente. Para obtener más información sobre la desactivación permanente y concurrente de las redes inalámbricas, consulte DOCA0172** *EcoStruxure Panel Server - Guía del usuario, página 7.*

NOTA: Los modelos Wired by Design (WD) de Panel Server le permiten cumplir políticas no inalámbricas, ya que no contienen ningún chipset inalámbrico.

Se recomienda:

- Utilice el código de instalación para detectar dispositivos inalámbricos. Para obtener más información, consulte DOCA0172** *EcoStruxure Panel Server - Guía del usuario, página 7*
- Realice la puesta en marcha de los dispositivos inalámbricos IEEE 802.15.4 en un lugar protegido de los transmisores de radio no autorizados, como una sala de administración.

Para la red Wi-Fi, se recomienda utilizar el protocolo WPA2 (Wi-Fi Protected Access versión 2).

NOTA: El Protocolo de integridad de clave temporal (TKIP) no es compatible.

Acceso remoto (VPN)

El Panel Server proporciona una función de acceso remoto que permite al centro de atención al cliente (CCC) de Schneider Electric conectarse a las páginas web de Panel Server.

El acceso no está habilitado de forma predeterminada y requiere que el firewall habilite la conexión. Para obtener más información, consulte *Extremos esperados, página 19.*

La función de acceso remoto se basa en una VPN de capa 3 que, por diseño, no proporciona acceso a la red, sino solo a Panel Server. Además, solo HTTPS está autorizado para ser tunelizado a través de esta VPN.

Dispositivos conectados

Se recomienda comprobar periódicamente la lista de dispositivos conectados a la red IEEE 802.15.4 del Panel Server . Si hay un dispositivo conectado desconocido, localícelo y quítelo. También puede reconstruir la red y reconectar solo los dispositivos identificados.

Seguridad de la aplicación en la nube

Seguridad de datos en movimiento

Schneider Electric con aplicaciones EcoStruxure en la nube implementa prácticas recomendadas, como:

- Todas las comunicaciones que tienen como origen y destino EcoStruxure Panel Server con sistemas internos de Schneider Electric o sistemas externos de terceros están cifradas con HTTPS (el nivel mínimo requerido es TLS 1.2).
- Los certificados que participan en estas sesiones cifradas utilizan el algoritmo hash seguro SHA 256. Esto se aplica a las comunicaciones entre la aplicación de Panel Server y los servidores de las plataformas en la nube de Microsoft Azure.

Seguridad de datos en reposo

Schneider Electric sigue las prácticas recomendadas para crear soluciones seguras y limitar el riesgo de que los datos se comprometan de manera significativa a la vez que protege la privacidad, el control y la autonomía de los datos de cada cliente independientemente de cualquier otro.

Todas las credenciales y tokens de sistema a sistema se almacenan y cifran en plataformas en la nube de Microsoft Azure.

Extremos esperados

Schneider Electric recomienda solo permitir el acceso a los dominios requeridos en función de sus necesidades.

En la tabla siguiente se enumeran los nombres de dominio y los protocolos utilizados cuando Panel Server se conecta a la nube.

Nombre del dominio	Protocolo	Descripción
cbBootStrap.gl.StruXureWareCloud.com	HTTPS (puerto TCP 443)	Se utiliza en la primera conexión de Panel Server a la nube (o después de un restablecimiento de los ajustes de fábrica) para autenticar y registrar Panel Server.
etp.prod.StruXureWareCloud.com	HTTPS (puerto TCP 443)	Se utiliza para descargar las actualizaciones de firmware.
cnm-ih-na.Azure-devices.net	HTTPS (puerto TCP 443)	Se utiliza para la comunicación de Panel Server con servicios en la nube de Schneider Electric, como configuración, datos o alarmas.
RemoteShell.rsp.Schneider-Electric.com	HTTPS (puerto TCP 443)	Permite que el centro de asistencia al cliente de Schneider Electric acceda de forma remota a las páginas web del Panel Server mediante VPN.
cnmdapiappstna.Blob.Core.Windows.net	HTTPS (puerto TCP 443)	Permite al Panel Server cargar registros y archivos de diagnóstico cuando así lo solicite el Centro de Atención al Cliente de Schneider Electric.
cnmiothubappstna.Blob.Core.Windows.net/file-upload	HTTPS (puerto TCP 443)	Permite al Panel Server cargar una topología en los servicios en la nube de Schneider Electric.
time.gl.StruXureWareCloud.com	Puerto NTP (UDP) 123)	El servidor NTP permite mantener sincronizado el reloj del Panel Server.

NOTA: Los nombres de dominio no distinguen entre mayúsculas y minúsculas.

Seguridad física del dispositivo

Etiqueta antimanipulación

El EcoStruxure Panel Server tiene una etiqueta de indicación de alteración que protege la seguridad física del dispositivo. Debe estar limpia y no mostrar ningún signo de manipulación (por ejemplo, roturas, rasgones o arañazos). Schneider Electric recomienda no usar dispositivos claramente manipulados.

Instalación

Para contribuir a garantizar la seguridad física del dispositivo, se recomienda la siguiente instalación:

- Instale EcoStruxure Panel Server en un armario protegido adecuadamente según el nivel de riesgo de su instalación (por ejemplo, un armario con candado o llave).
- Si EcoStruxure Panel Server se monta en un cuadro eléctrico, instale dicho cuadro en una sala segura (por ejemplo, con puerta cerrada o cámara).

NOTA: La protección de la seguridad física del dispositivo incluye la protección del código QR. El código QR proporciona acceso al código de dispositivo del Panel Server, que debe considerarse como una credencial para el dispositivo. Se utiliza:

- En la reclamación segura del dispositivo para aplicaciones en la nube
- Como contraseña para conectarse al punto de acceso Wi-Fi

Gestión de contraseñas

Para ayudar a proteger el dispositivo de ataques malintencionados, cambie la contraseña de usuario del Panel Server y la contraseña del punto de acceso Wi-Fi mediante las páginas web de Panel Server.

La contraseña de usuario y la contraseña de SupportUser deben cumplir las siguientes reglas:

- Entre 8 y 50 caracteres
- Debe contener al menos tres de los siguientes tipos de caracteres:
 - Mayúsculas
 - Minúsculas
 - Dígitos
 - Caracteres especiales (limitados a espacios y !"#\$%&'()*+,-./:;<=>?@[\\]^_`{|}~)

La contraseña del punto de acceso Wi-Fi debe cumplir las siguientes reglas:

- Entre 8 y 32 caracteres
- Debe contener al menos uno de los siguientes tipos de caracteres:
 - Mayúsculas
 - Minúsculas
 - Dígitos
- Puede contener caracteres especiales (limitados a espacios y !"#\$%&'()*+,-./:;<=>?@[\\]^_`{|}~)

Función de copia de seguridad

Al descargar un archivo de copia de seguridad, cifre el archivo con una contraseña segura, formada por:

- Entre 6 y 32 caracteres
- Al menos uno de cada uno de los siguientes tipos de caracteres:
 - Mayúsculas
 - Minúsculas
- Caracteres especiales (limitados a espacios y !"#\$%&'()*+,-./:;<=>?@[]_`{|}~)

Recomendaciones de seguridad para el mantenimiento

Operaciones de mantenimiento

Durante la vida útil de EcoStruxure Panel Server, se recomienda realizar las siguientes operaciones con regularidad:

- Comprobar la seguridad física de EcoStruxure Panel Server (consulte la etiqueta antimanipulación, página 21).
- Asegurarse de tener la actualización de firmware más reciente. Debe haberse registrado para recibir notificaciones de seguridad, página 14.
- Comprobar los dispositivos conectados, página 18 para asegurarse de que no haya dispositivos desconocidos.
- Consultar los registros de auditoría, página 15 para comprobar que no haya comportamientos inesperados, como intentos de inicio de sesión no válidos o re arranques frecuentes.
- Comprobar la fecha y la hora, página 14 para no desviarse de la fecha actual.
- Asegúrese de que todos los servicios y funciones innecesarios están desactivados, página 14.

Verificación de las funciones de seguridad

Las pruebas siguientes le permiten verificar el funcionamiento previsto de las funciones de seguridad a través de las páginas web de EcoStruxure Panel Server.

Autenticación web

1. Intente iniciar sesión en las páginas web de EcoStruxure Panel Server sin contraseña o introduzca una contraseña incorrecta.
Resultado: EcoStruxure Panel Server no proporciona acceso a las páginas web.
2. Repita esta operación 9 veces más.
Resultado: EcoStruxure Panel Server se bloquea durante 10 minutos.
3. Inténtelo de nuevo 5 veces.
Resultado: EcoStruxure Panel Server se bloquea durante 60 minutos.

Autorización web

1. Inicie sesión en las páginas web de EcoStruxure Panel Server.
2. Guarde como marcador una página web (por ejemplo, **Configuración**)
3. Abra una ventana de navegación privada en el navegador y abra la página web anteriormente guardada como marcador.
Resultado: no podrá acceder a la página web, pero se le redirigirá a la página de inicio de sesión.

Auditar

1. Tras realizar todas o algunas de las pruebas anteriores, acceda a la página web Registros.
2. Descargue los archivos de registro.
3. Compruebe que los intentos fallidos estén presentes en los registros.

Actualización del firmware

1. Vaya a la página web **Actualización de firmware**.
2. Cargue un archivo aleatorio (por ejemplo, una imagen o un documento de texto).
Resultado: EcoStruxure Panel Server informa de una firma incorrecta.
3. Acceda a los registros de auditoría.
4. Compruebe que la actualización del firmware que ha fallado esté presente en los registros.

Desactivación de servicios

1. Si desea acceder al menú para desactivar servicios, seleccione **Configuración > Comunicación de red > DPWS**.
2. Conecte un PC con el sistema operativo Windows a la misma red local.
3. Haga clic en Red en el Explorador de archivos.
Resultado: EcoStruxure Panel Server no se detecta, por lo que no aparece en la lista de dispositivos de la red.

Desactivación de los servicios inalámbricos

Para acceder a los menús y desactivar temporalmente los servicios inalámbricos:

- Para Wi-Fi, vaya a **Configuración > Comunicación de red > Wi-Fi**, haga clic en el control deslizante **Activación de Wi-Fi** y guarde los cambios.
Resultado: En su interfaz de gestión de puntos de acceso Wi-Fi, no hay ningún EcoStruxure Panel Server conectado.
- Para IEEE 802.15.4, vaya a **Configuración > Dispositivos inalámbricos > Configuración de red**, haga clic en el control deslizante **Activación inalámbrica** y guarde los cambios.
Resultado: Todos los dispositivos inalámbricos incluidos en **Configuración > Dispositivos inalámbricos > Dispositivos inalámbricos** indicarán el estado **No conectado** después de un determinado tiempo, dependiendo del dispositivo inalámbrico (consulte la documentación del dispositivo para obtener más detalles).

Glosario

C

Código de instalación:

Un código único de 36 caracteres asociado a un dispositivo Modbus que le permite iniciar la detección del dispositivo con mayor seguridad desde el Panel Server.

D

DHCP: protocolo de configuración dinámica de host:

Protocolo de administración de redes utilizado en redes de protocolo de Internet para asignar automáticamente direcciones IP y otros parámetros de comunicación a dispositivos conectados a la red mediante una arquitectura cliente-servidor.

DPWS: Devices Profile for Web Services (perfil de dispositivos para servicios web):

Conjunto mínimo de restricciones de implementación que ayudan a permitir de manera segura los servicios web de mensajería, detección, descripción y eventos en los dispositivos de recursos restringidos.

H

HTTP: protocolo de transferencia de hipertexto:

Protocolo de red que gestiona la entrega de archivos y datos en la World Wide Web.

HTTPS: protocolo seguro de transferencia de hipertexto:

Variante del protocolo de transferencia web estándar (HTTP) que añade una capa de seguridad a los datos que se transportan a través de una conexión de protocolo de capa de sockets seguros (SSL) o seguridad de la capa de transporte (TLS).

I

IEEE 802.15.4:

Estándar definido por IEEE y utilizado por el EcoStruxure Panel Server para comunicarse con dispositivos inalámbricos.

IP : protocolo de Internet:

Las direcciones IP se utilizan para identificar dispositivos conectados a la intranet de la empresa o a Internet.

L

LAN: red de área local:

Hace referencia a la intranet o la red de TI de la empresa.

M

Modbus TCP/IP:

Protocolo que proporciona comunicación cliente/servidor entre dispositivos y TCP/IP que proporciona comunicaciones a través de una conexión Ethernet.

N

NTP: protocolo de tiempo de red:

Un protocolo de red para la sincronización horaria entre sistemas informáticos con redes de datos de latencia variable y conmutación de paquetes.

O

OT: tecnología operativa:

Hace referencia a los sistemas de hardware y software que la empresa utiliza para supervisar y controlar directamente los procesos y equipos de producción, lo que también se conoce como red de control industrial (IC). OT se suele utilizar para hacer referencia a la red operativa de la empresa, en contraposición a su red de TI.

P

PKI: infraestructura de clave pública:

Define un conjunto de servicios que se utilizan para generar y autenticar firmas digitales. Una infraestructura de clave pública está diseñada para garantizar la confidencialidad, la integridad y la autenticidad de la información.

Política de seguridad:

La política de seguridad de un sistema es la configuración de seguridad aplicada en todo el sistema protegido. Las políticas de seguridad suelen hacer referencia al uso de normas. Se usan para definir la configuración de seguridad compartida por todos los dispositivos.

R

RSTP: protocolo de árbol de expansión rápido:

Un protocolo de red que promueve una alta disponibilidad y una topología sin bucles en las redes Ethernet.

S

SCADA - Supervisory control and data acquisition:

Hace referencia a los sistemas diseñados para obtener datos en tiempo real sobre los procesos y equipos de producción para supervisarlos y controlarlos remotamente.

SDL: ciclo de vida seguro del desarrollo:

Un marco de desarrollo de productos que ayuda a garantizar que los productos sigan procesos de diseño seguros en todas las etapas del ciclo de vida.

SFTP - Secure File Transfer Protocol:

Una versión segura del protocolo de transferencia de archivos que facilita el acceso a los datos y su transferencia mediante un flujo de datos de Secure Shell (SSH).

T

TCP/IP - Transmission control protocol/Internet protocol:

Hace referencia al conjunto de protocolos que se utilizan para las comunicaciones por Internet.

TI: tecnologías de la información:

Hace referencia a los sistemas de información y a la red de información de la empresa en contraposición a su red de OT (tecnología operativa).

V

VPN: red privada virtual:

Las VPN se utilizan para establecer un "túnel" protegido o privado entre un punto de acceso externo autenticado y la red empresarial de confianza.

Schneider Electric
35 rue Joseph Monier
92500 Rueil Malmaison
Francia

+ 33 (0) 1 41 29 70 00

www.se.com

Debido a que las normas, especificaciones y diseños cambian periódicamente, solicite la confirmación de la información dada en esta publicación.

© 2026 Schneider Electric. Reservados todos los derechos.

DOCA0211ES-14