EcoStruxure Automation Device Maintenance

Herramienta de actualización del firmware

Ayuda en línea

EIO0000004047.04
11/2022

www.se.com

Información legal

La marca Schneider Electric y cualquier otra marca comercial de Schneider Electric SE y sus filiales mencionadas en esta guía son propiedad de Schneider Electric SE o sus filiales. Todas las otras marcas pueden ser marcas comerciales de sus respectivos propietarios. Esta guía y su contenido están protegidos por las leyes de copyright aplicables, y se proporcionan exclusivamente a título informativo. Ninguna parte de este manual 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 concede ningún derecho o licencia para el uso comercial de la guía o su contenido, excepto por una licencia no exclusiva y personal para consultarla "tal cual".

La instalación, utilización, mantenimiento y reparación de los productos y equipos de Schneider Electric la debe realizar solo personal cualificado.

Debido a la evolución de las normativas, especificaciones y diseños con el tiempo, la información contenida en esta guía puede estar sujeta a cambios 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 material o por las consecuencias derivadas o resultantes del uso de la información contenida en el presente documento.

Como parte de un grupo de empresas responsables e inclusivas, estamos actualizando nuestras comunicaciones que contienen terminología no inclusiva. Sin embargo, hasta que completemos este proceso, es posible que nuestro contenido todavía contenga términos estandarizados del sector que pueden ser considerados inapropiados para nuestros clientes.

© 2022 - Schneider Electric. Todos los derechos reservados.

Tabla de contenido

Información de seguridad 5
- Cualificación del personal 5
- Uso correcto 6
- Antes de empezar 6
- Iniciar y probar 7
- Funcionamiento y ajustes 8
- Precauciones de seguridad 8

Acerca de este libro 10

Introducción 15
- Descripción general 15
- Requisitos del sistema 16
- Instalación 17

Conceptos básicos 18
- Pantalla de bienvenida 18

Interfaz de usuario de EcoStruxure Automation Device Maintenance 20
- Paquete de datos 20
- Dispositivo/Cargando 21
- Agregar dispositivo 23
- Configuración de ajustes 25
- Ventana de errores y advertencias 26
- Creación de un nuevo proyecto de EcoStruxure Automation Device Maintenance 27
- Guardado del proyecto 28
- Apertura del proyecto 29

Configuración de la herramienta EcoStruxure Automation Device Maintenance 32
- Configuración del modo de detección de dispositivos 32
- Configuración del explorador Modbus TCP 34
- Configuración del explorador DPWS 36
- Configuración de los parámetros de comunicación 37
- Configuración de ubicación de los paquetes 37
- Visualización de los archivos de registro 38
- Configuración del idioma 40
- Restablecimiento de la configuración de la aplicación 40

Configuración de las funciones de seguridad 41
- Características de seguridad 41
- Gestión de certificados 43
- Gestión de la infraestructura de clave pública (PKI) 48
- Activación del registro de mensajes de Syslog 49

Paquete de datos 51
- Ficha Paquete de datos 51

Dispositivo/Cargando 55
- Ficha **Dispositivo/Cargando** 55
- Agrupación de dispositivos en la LISTA DE DISPOSITIVOS 56
- Eliminación de dispositivos 57

Administración de credenciales de usuario 61
Acceso a extensiones 64
Supervisión del estado de detección de dispositivos 66
Ver/confirmar mensajes 67
Visualización de registros 68
Centro de actualizaciones 68
Actualización del firmware 69
Actualización del archivo de configuración de seguridad 71
Ciberseguridad 74
¿Qué es la ciberseguridad? 74
Directrices de Schneider Electric 76
Verificación de firmas digitales 78
Archivos que requieren desinstalación manual 79
Componentes utilizados por EcoStruxure Automation Device Maintenance 80
Glosario 83
Índice 86

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.

Cualificación del personal

Una persona cualificada es aquella que posee las siguientes cualificaciones:

- Habilidades y conocimientos relacionados con la construcción y el manejo de equipos eléctricos y su instalación.
- Conocimientos y experiencia en programación de control industrial.
- Ha recibido formación relacionada con la seguridad para poder detectar y evitar los riesgos implicados.

La persona cualificada debe ser capaz de detectar los peligros potenciales que pueden surgir de la parametrización, la modificación de valores de parámetros y, en general, de los equipos mecánicos, eléctricos o electrónicos. La persona cualificada debe estar familiarizada con los estándares, disposiciones y normativas para la prevención de accidentes industriales, que deberán seguir cuando diseñen e implementen el sistema.

Uso correcto

Este producto es una biblioteca que debe usarse junto con los sistemas de control y los segmentos de motor de estator largo previstos únicamente para la finalidad que se describe en la presente documentación conforme se aplica en el sector industrial.

Siga siempre las instrucciones aplicables de seguridad, las condiciones especificadas y los datos técnicos.

Antes de usar el producto, realice una evaluación de riesgos que incluya el uso específico. Aplique medidas de protección conformes al resultado obtenido.

Como el producto se utiliza como parte de un sistema general, deberá garantizar la seguridad del personal mediante el diseño de ese sistema general (por ejemplo, diseño de la máquina).

Cualquier otro uso no se ha previsto y puede ser peligroso.

Antes de empezar

No utilice este producto en maquinaria sin protección de punto de funcionamiento. La ausencia de protección de punto de funcionamiento en una máquina puede provocar lesiones graves al operador de dicha máquina.

⚠ ADVERTENCIA

EQUIPO SIN PROTECCIÓN

- No utilice este software ni los equipos de automatización relacionados en equipos que no dispongan de protección de punto de funcionamiento.
- No introduzca las manos u otras partes del cuerpo dentro de la maquinaria mientras está en funcionamiento.

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

Este equipo de automatización y el software relacionado se utilizan para controlar diversos procesos industriales. El tipo o modelo del equipo de automatización adecuado para cada uso varía en función de factores tales como las funciones de control necesarias, el grado de protección requerido, los métodos de producción, la existencia de condiciones poco habituales, las normativas gubernamentales, etc. En algunos usos, puede ser necesario más de un procesador, como en el caso de que se requiera redundancia de respaldo.

Solamente el usuario, el fabricante de la máquina o el integrador del sistema conocen las condiciones y los factores presentes durante la configuración, el funcionamiento y el mantenimiento de la máquina y, por consiguiente, pueden decidir el equipo asociado y las medidas de seguridad y los enclavamientos relacionados que se pueden utilizar de forma adecuada. Al seleccionar los equipos de automatización y control, así como el software relacionado para un uso determinado, el usuario deberá consultar los estándares y las normativas locales y nacionales aplicables. La publicación National Safety Council's Accident Prevention Manual (que goza de un gran reconocimiento en los Estados Unidos de América) también proporciona gran cantidad de información de utilidad.

En algunas aplicaciones, como en el caso de la maquinaria de embalaje, debe proporcionarse protección adicional al operador, como la protección de punto de funcionamiento. Esta medida es necesaria si existe la posibilidad de que las manos y otras partes del cuerpo del operador puedan introducirse y quedar atrapadas en áreas o puntos peligrosos, lo que puede provocar lesiones graves. Los productos de software por sí solos no pueden proteger al operador frente a posibles lesiones. Por este motivo, el software no se puede sustituir por la protección de punto de funcionamiento ni puede realizar la función de esta.

Asegúrese de que las medidas de seguridad y los enclavamientos mecánicos/eléctricos relacionados con la protección de punto de funcionamiento se hayan instalado y estén operativos antes de que los equipos entren en funcionamiento. Todos los enclavamientos y las medidas de seguridad relacionados con la protección de punto de funcionamiento deben estar coordinados con la programación del software y los equipos de automatización relacionados.

NOTA: La coordinación de las medidas de seguridad y los enclavamientos mecánicos/eléctricos para la protección de punto de funcionamiento está fuera del ámbito de la biblioteca de bloques de funciones, la guía de usuario del sistema o de otras instalaciones mencionadas en esta documentación.

Iniciar y probar

Antes de utilizar los equipos eléctricos de control y automatización para su funcionamiento normal tras la instalación, es necesario que personal cualificado lleve a cabo una prueba de inicio del sistema para verificar que los equipos funcionan correctamente. Es importante realizar los preparativos para una comprobación de estas características y disponer de suficiente tiempo para llevar a cabo las pruebas de forma completa y correcta.

⚠ADVERTENCIA

PELIGRO DE FUNCIONAMIENTO DEL EQUIPO

- Compruebe que se hayan seguido todos los procedimientos de instalación y configuración.
- Antes de realizar las pruebas de funcionamiento, retire de todos los dispositivos todos los bloqueos u otros medios de sujeción temporales utilizados para el transporte.
- Retire del equipo las herramientas, los medidores y el material de desecho que pueda haber.

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

Realice todas las pruebas de inicio recomendadas en la documentación del equipo. Guarde la documentación del equipo para consultarla en el futuro.

Las pruebas del software deben realizarse tanto en un entorno simulado como en un entorno real.

Verifique que no existen cortocircuitos ni conexiones a tierra temporales en todo el sistema que no estén instalados según la normativa local (de conformidad con National Electrical Code de EE. UU., por ejemplo). Si fuera necesario realizar pruebas de tensión de alto potencial, siga las recomendaciones de la documentación del equipo para evitar dañar el equipo fortuitamente.

Antes de dar tensión al equipo:

- Retire del equipo las herramientas, los medidores y el material de desecho que pueda haber.
- Cierre la puerta de la carcasa del equipo.
- Retire todas las conexiones a tierra temporales de las líneas de alimentación de entrada.
- Realice todas las pruebas iniciales recomendadas por el fabricante.

Funcionamiento y ajustes

Las precauciones siguientes proceden de NEMA Standards Publication ICS 7.1-1995 (prevalece la versión en inglés):

- Aunque se ha extremado la precaución en el diseño y la fabricación del equipo o en la selección y las especificaciones de los componentes, existen riesgos que pueden aparecer si el equipo se utiliza de forma inadecuada.
- En algunas ocasiones puede desajustarse el equipo, lo que provocaría un funcionamiento incorrecto o poco seguro. Utilice siempre las instrucciones del fabricante como guía para realizar los ajustes de funcionamiento. El personal que tenga acceso a estos ajustes debe estar familiarizado con las instrucciones del fabricante del equipo y con la maquinaria utilizada para los equipos eléctricos.
- El operador solo debe tener acceso a los ajustes de funcionamiento que realmente necesita. El acceso a los demás controles debe restringirse para evitar cambios no autorizados en las características de funcionamiento.

Precauciones de seguridad

Durante la instalación o el uso de este software, preste atención a los mensajes de seguridad que aparecen en el software y que están incluidos en la documentación. Los siguientes mensajes de seguridad se aplican a este software en su totalidad.

⚠ ADVERTENCIA

RIESGO DE FUNCIONAMIENTO IMPREVISTO DEL EQUIPO

- No utilice el software para control crítico o aplicaciones de protección donde la seguridad de las personas o del equipo depende del funcionamiento de la acción de control.
- No utilice el software para control de funciones de tiempo crítico. Puede producirse retardos de comunicación entre el momento en el que se inicia un control y cuando se aplica la acción.

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

⚠ ADVERTENCIA

RIESGO DE RESULTADOS DE DATOS IMPRECISOS

- Configure el software correctamente para obtener informes o datos precisos.
- No base las acciones de servicio o mantenimiento únicamente en los mensajes y la información visualizada en el software.
- No confíe únicamente en los mensajes e informes del software para determinar si el sistema funciona correctamente o cumple los estándares y requerimientos aplicables.
- Tenga en cuenta las implicaciones de los retardos de transmisiones o los fallos de enlaces de comunicación imprevistos.

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

⚠ADVERTENCIA

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

Siga las mejores prácticas de ciberseguridad.

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

NOTA: Para obtener información detallada sobre ciberseguridad, consulte el capítulo Ciberseguridad, página 74.

Acerca de este libro

Alcance del documento

Esta documentación describe la herramienta EcoStruxure Automation Device Maintenance. EcoStruxure Automation Device Maintenance puede transferir firmware de un PC a un dispositivo de Schneider Electric admitido. La herramienta admite la detección de dispositivos relevantes de la red y también permite identificar dichos dispositivos de manera manual si la detección de dispositivos no es posible.

Campo de aplicación

Este documento se ha actualizado para EcoStruxure Automation Device Maintenance versión 3.1.

Las características descritas en el presente documento, así como las descritas en los documentos incluidos a continuación en la sección Documentos relacionados, pueden consultarse en línea. Para acceder a la información en línea, diríjase a la página de inicio de Schneider Electric www.se.com/ww/en/download/. Para obtener documentación sobre EcoStruxure Automation Device Maintenance, escriba *EcoStruxure Automation Device Maintenance* en el cuadro de texto de búsqueda y presione la tecla **Entrar**.

Las características descritas en el presente documento deben coincidir con las características que aparecen en línea. De acuerdo con nuestra política de mejoras continuas, es posible que a lo largo del tiempo revisemos el contenido con el fin de elaborar documentos más claros y precisos. Si nota alguna diferencia entre el manual y la información online, utilice la información online como referencia.

Documentos relacionados

Título de la documentación	Número de referencia
Firmware Compatibility Rules, Modicon M580, Modicon Momentum, and Modicon X80 I/O Modules	EIO0000002634 (English)
Ciberseguridad - Plataforma de controladores Modicon - Manual de referencia	EIO0000001999 (English) EIO0000002001 (French) EIO0000002000 (German) EIO0000002003 (Spanish) EIO0000002002 (Italian) EIO0000002004 (Chinese)
Guía de especificaciones e implementaciones de Modbus - Manual de referencia	Modbus Application Protocol Specification
Perfil de dispositivos para servicios web - Manual de referencia	WSDD-DPWS

Título de la documentación	Número de referencia
EcoStruxure™ Control Expert, Modalidades de funcionamiento	33003101 (English) 33003102 (French) 33003103 (German) 33003104 (Spanish) 33003696 (Italian) 33003697 (Chinese)
EcoStruxure Automation Device Maintenance Manual del usuario de Altivar	JYT50472 (English) JYT50474 (French) JYT50482 (German) JYT50476 (Spanish) JYT50478 (Italian) JYT50483 (Chinese) JYT50484 (Turkish) JYT50485 (Portuguese)

Información relacionada con el producto

⚠ADVERTENCIA

PÉRDIDA DE CONTROL

- El diseñador del esquema de control debe tener en cuenta los posibles modos de fallo de rutas de control y, para ciertas funciones de control críticas, proporcionar los medios para lograr un estado seguro durante y después de un fallo de ruta. Funciones de control críticas son, por ejemplo, una parada de emergencia y una parada de sobrerrecorrido, un corte de alimentación y un reinicio.
- Para las funciones críticas de control deben proporcionarse rutas de control separadas o redundantes.
- Las rutas de control del sistema pueden incluir enlaces de comunicación. Deben tenerse en cuenta las implicaciones de los retrasos de transmisión no esperados o los fallos en el enlace.
- Tenga en cuenta todas las reglamentaciones para la prevención de accidentes y las directrices de seguridad locales.[1]
- Cada implementación de este equipo debe probarse de forma individual y exhaustiva antes de entrar en servicio.

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

[1] Para obtener información adicional, consulte NEMA ICS 1.1 (última edición), "Safety Guidelines for the Application, Installation, and Maintenance of Solid State Control" (Directrices de seguridad para la aplicación, la instalación y el mantenimiento del control de estado estático) y NEMA ICS 7.1 (última edición), "Safety Standards for Construction and Guide for Selection, Installation and Operation of Adjustable-Speed Drive Systems" (Estándares de seguridad para la construcción y guía para la selección, instalación y utilización de sistemas de unidades de velocidad ajustable) o su equivalente aplicable a la ubicación específica.

Antes de intentar proporcionar una solución (máquina o proceso) para una aplicación específica mediante las POU que se encuentran en la biblioteca, hay que tener en cuenta, aplicar y completar las prácticas recomendadas. Entre esas prácticas se incluyen, sin limitaciones, el análisis de riesgos, la seguridad funcional, la compatibilidad de los componentes, pruebas y validación del sistema en tanto estén relacionadas con esta biblioteca.

⚠ ADVERTENCIA

USO INCORRECTO DE LAS UNIDADES DE ORGANIZACIÓN DE PROGRAMA

- Realice un análisis de seguridad en la aplicación y los dispositivos instalados.
- Asegúrese de que las unidades de organización de programa (POU) sean compatibles con los dispositivos del sistema y que no se producen efectos imprevistos en el correcto funcionamiento del sistema.
- Utilice los parámetros adecuados, especialmente los valores límite y observe el desgaste de la máquina y el comportamiento de parada.
- Verifique que los sensores y accionadores sean compatibles con las POU seleccionadas.
- Pruebe exhaustivamente todas las funciones durante la verificación y la puesta en marcha en todas las modalidades de funcionamiento.
- Proporcione métodos independientes para las funciones de control críticas (parada de emergencia, condiciones para la superación de valores límite, etc.) de acuerdo con un análisis de seguridad, las reglas correspondientes y las normas.

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

⚠ ADVERTENCIA

FUNCIONAMIENTO IMPREVISTO DEL EQUIPO

- Utilice sólo software aprobado por Schneider Electric para este equipo.
- Actualice el programa de aplicación siempre que cambie la configuración de hardware física.

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

Las transferencias de archivos incompletas, como las transferencias de archivos de datos, aplicaciones o firmware, pueden tener consecuencias graves para la máquina o el controlador. Si desconecta la alimentación o se produce un corte de corriente o una interrupción de la comunicación durante una transferencia de archivos, la máquina puede quedar inoperativa o la aplicación puede intentar acceder a un archivo de datos dañado. Si se produce una interrupción, vuelva intentar la transferencia. Asegúrese de incluir en el análisis de riesgos el impacto de archivos de datos dañados.

⚠ ADVERTENCIA

FUNCIONAMIENTO IMPREVISTO DEL EQUIPO, PÉRDIDA DE DATOS O ARCHIVOS DAÑADOS

- No interrumpa una transferencia de datos en curso.
- Si la transferencia se interrumpiese por cualquier motivo, vuelva a iniciarla.
- No ponga la máquina en servicio hasta que la transferencia de archivos haya finalizado correctamente, a menos que haya tenido en cuenta los archivos dañados en el análisis de riesgo y haya realizado los pasos apropiados para evitar las posibles consecuencias graves derivadas de una transferencia de archivos fallida.

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

Se debe tener cuidado y adoptar las medidas adecuadas al utilizar esta biblioteca como control de la máquina, con el fin de evitar consecuencias no deseadas en el funcionamiento solicitado de máquinas, cambios de estado o alteración de la memoria de datos o de los elementos de funcionamiento de la máquina.

⚠ADVERTENCIA

FUNCIONAMIENTO IMPREVISTO DEL EQUIPO

- Coloque los dispositivos del sistema de control del operador cerca de la máquina o en un lugar en el que tenga una vista completa de la máquina.
- Proteja los comandos de operador contra el acceso sin autorización.
- Si el control remoto es un aspecto de diseño necesario en la aplicación, asegúrese de que un observador local, competente y cualificado esté presente al utilizarlo desde una ubicación remota.
- Configure e instale la entrada Ejecutar/Detener, si la tiene, u otros medios externos en la aplicación con el objetivo de mantener el control local sobre el inicio o la detención del dispositivo independientemente de los comandos remotos que se le hayan enviado.

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

Normas y términos utilizados

Los términos técnicos, símbolos y las descripciones correspondientes del presente manual o que aparecen en la parte interior o exterior de los propios productos se derivan, por lo general, de los términos y las definiciones de estándares internacionales.

En el área de los sistemas de seguridad funcional, unidades y automatización general se incluyen, pero sin limitarse a ellos, términos como *seguridad*, *función de seguridad*, *estado de seguridad*, *fallo*, *reinicio tras fallo*, *avería*, *funcionamiento incorrecto*, *error*, *mensaje de error*, *peligroso*, etc.

Estos estándares incluyen, entre otros:

Norma	Descripción
IEC 61131-2:2007	Controladores programables, parte 2: requisitos y ensayos de los equipos.
ISO 13849-1:2015	Seguridad de la maquinaria: componentes de los sistemas de control relacionados con la seguridad. Principios generales del diseño.
EN 61496-1:2013	Seguridad de las máquinas: equipos de protección electrosensibles. Parte 1: pruebas y requisitos generales.
ISO 12100:2010	Seguridad de las máquinas. Principios generales para el diseño. Evaluación del riesgo y reducción del riesgo
EN 60204-1:2006	Seguridad de las máquinas. Equipo eléctrico de las máquinas. Parte 1: requisitos generales
ISO 14119:2013	Seguridad de las máquinas. Dispositivos de bloqueo asociados con protecciones: principios de diseño y selección
ISO 13850:2015	Seguridad de las máquinas. Parada de emergencia: principios de diseño
IEC 62061:2015	Seguridad de las máquinas. Seguridad funcional de los sistemas de control eléctricos, electrónicos y electrónicos programables relacionados con la seguridad
IEC 61508-1:2010	Seguridad funcional de los sistemas eléctricos/electrónicos/electrónicos programables relacionados con la seguridad: requisitos generales.
IEC 61508-2:2010	Seguridad funcional de los sistemas eléctricos/electrónicos/electrónicos programables relacionados con la seguridad: requisitos para los sistemas eléctricos/electrónicos/electrónicos programables relacionados con la seguridad.
IEC 61508-3:2010	Seguridad funcional de los sistemas eléctricos/electrónicos/electrónicos programables relacionados con la seguridad: requisitos de software.
IEC 61784-3:2016	Redes de comunicación industrial - Perfiles - Parte 3: Buses de campo de seguridad funcionales - Reglas generales y definiciones de perfiles.
2006/42/EC	Directiva de maquinaria
2014/30/EU	Directiva de compatibilidad electromagnética
2014/35/EU	Directiva de baja tensión

Además, los términos utilizados en este documento se pueden usar de manera tangencial porque se obtienen de otros estándares como:

Norma	Descripción
Serie IEC 60034	Máquinas eléctricas giratorias
Serie IEC 61800	Accionamientos eléctricos de potencia de velocidad variable
Serie IEC 61158	Comunicación digital de datos para la medición y control: bus de campo para su uso en sistemas de control.

Por último, el término *zona de funcionamiento* se puede utilizar junto con la descripción de peligros específicos, y se define como tal para una *zona de peligro* o una *zona peligrosa* en la *Directiva de maquinaria* (*2006/42/EC*) e *ISO 12100:2010*.

NOTA: Los estándares mencionados anteriormente podrían o no aplicarse a los productos específicos citados en la presente documentación. Para obtener más información en relación con los diferentes estándares aplicables a los productos descritos en este documento, consulte las tablas de características de las referencias de dichos productos.

Introducción

Descripción general

Introducción

Con EcoStruxure Automation Device Maintenance puede actualizar los paquetes de firmware en varios dispositivos de manera simultánea. Los dispositivos pueden detectarse automáticamente o puede añadir el dispositivo manualmente si no se admite la detección automática de dispositivos o está desconectada en el dispositivo.

Los métodos de detección de dispositivos admitidos son:

- Código de función 43 de Modbus (Lectura de identificación de dispositivo)
- DPWS (Perfil de dispositivo para servicios web)

Características

EcoStruxure Automation Device Maintenance admite las siguientes características:

- Detección automática de dispositivos
- Identificación manual de dispositivos
- Funciones de seguridad
- Actualización de firmware para varios dispositivos de manera simultánea
- Administración de direcciones IP

Dispositivos Schneider Electric compatibles

Dispositivos Modicon:

- Modicon M340
- Modicon M580
- Modicon Momentum
- Módulos de E/S de Modicon X80

Dispositivos Altivar:

- Familia de productos Altivar
  - Unidades Altivar Process ATV6••
  - Unidades Altivar Process ATV9••
  - Unidades Altivar Machine ATV340
- Módulos opcionales Altivar:
  - VW3A3720 Ethernet
  - VW3A3721 MultiDrive-Link
  - VW3A3530D ATV dPAC
- Arrancadores progresivos Altivar:
  - Arrancador progresivo Altivar ATS480

Requisitos del sistema

Requisitos de hardware

Componente	Requisitos mínimos
CPU	Compatible conIntel® Core i3 o versión posterior
RAM	4 GB como mínimo; 8 GB o más recomendados
Espacio en disco duro	500 MB de espacio libre en disco

Requisitos de software

- Microsoft Windows® 10 Professional de 32 bits/64 bits o una versión posterior
- Microsoft Windows Server 2016 Standard de 64 bits
- Microsoft Windows Server 2019 Standard de 64 bits

Protocolos de comunicación

La herramienta admite los siguientes protocolos:

- FTP
- HTTP / HTTPS
- Modbus SL
- Modbus TCP
- OPC UA
- TCP
- UDP
- USB

Resolución de pantalla

Para visualizar el software con la mejor resolución de pantalla, utilice una resolución de pantalla de 1920 × 1080 píxeles. Se necesita, como mínimo, una resolución de pantalla de 1280 x 1024 píxeles.

Ciberseguridad

El software utiliza los siguientes puertos:

- DPWS (a través del puerto 3702)
- FTP (a través de los puertos 20, 21)
- HTTP (a través del puerto 80) / HTTPS (a través de los puertos 443 y 8080)
- Modbus (a través del puerto 502)
- OPC UA (a través del puerto 4840)

⚠ADVERTENCIA

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

Siga las prácticas recomendadas de ciberseguridad.

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

NOTA: Para obtener información detallada sobre ciberseguridad, consulte el capítulo Ciberseguridad, página 74.

Instalación

Procedimiento

Puede instalar el software descargando los archivos de instalación del sitio web Schneider Electric.

NOTA: Antes de hacer doble clic en el archivo AutomationDeviceMaintenance.exe, verifique la integridad del archivo como se describe en el capítulo Verificación de firmas digitales, página 78.

NOTA: Debe tener derechos de administrador para instalar el software.

Siga el procedimiento para instalar el software:

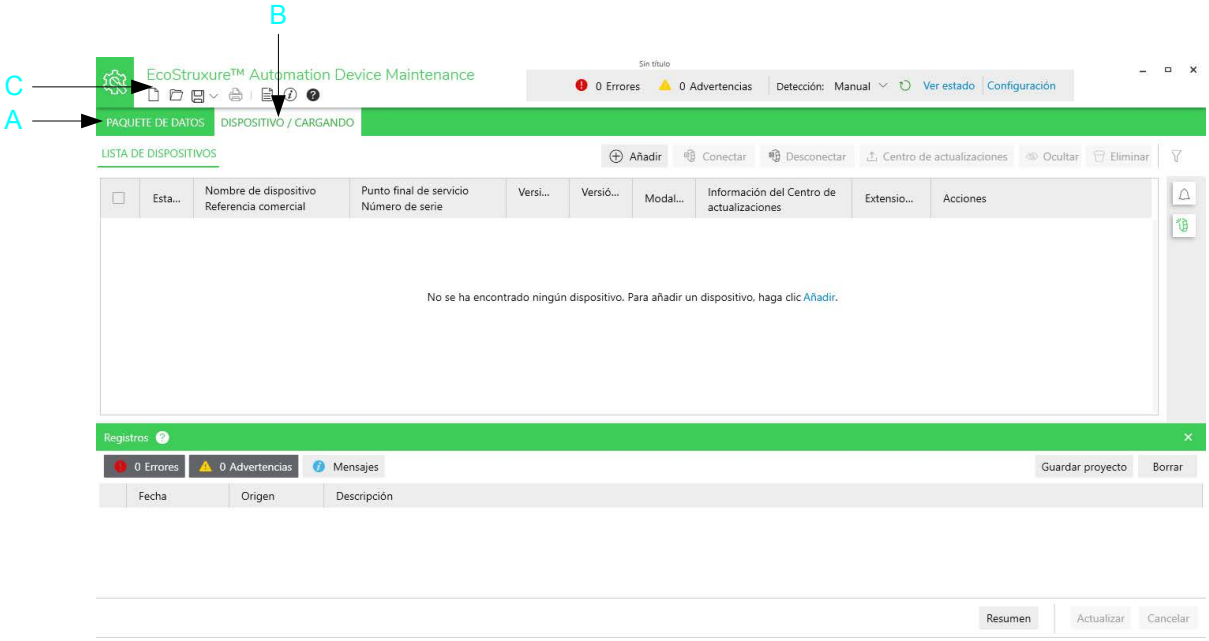
Paso	Acción
1	Localice los archivos de instalación utilizando Windows Explorer tras descargar los archivos.
2	Haga doble clic en el archivo de instalación de EcoStruxure Automation Device Maintenance. Se mostrará **InstallShield Wizard**.
3	Siga las instrucciones de **InstallShield Wizard** para completar la instalación.

Conceptos básicos

Pantalla de bienvenida

Descripción general

Tras el arranque inicial, EcoStruxure Automation Device Maintenance muestra la pantalla siguiente para actualizar los paquetes de firmware en varios dispositivos. Al cerrar la herramienta, se guardará el estado actual de la interfaz de usuario. Así, EcoStruxure Automation Device Maintenance mostrará la vista que había al cerrar la herramienta por última vez cuando vuelva a iniciarla.



Número	Nombre	Función
A	**Paquete de datos**	Muestra el contenido del repositorio del paquete de datos.
B	**Dispositivo/Cargando**	Muestra los detalles de los dispositivos detectados o identificados manualmente.
C	**Barra de herramientas**	Muestra el conjunto de iconos para ejecutar funciones.

Barra de herramientas

La barra de herramientas permite el acceso a las funciones generales de EcoStruxure Automation Device Maintenance.

Elemento	Nombre	Descripción
	Nuevo proyecto	Permite crear un nuevo proyecto de EcoStruxure Automation Device Maintenance, página 27.
	Abrir	Permite abrir un existing project, página 29.
	Guardar	Permite guardar la project settings, página 28.
	Imprimir	La característica no está disponible en esta versión.
	Registros	Le permite ver la información del registro.
	Acerca de	Permite el acceso a: • Información de EcoStruxure Automation Device Maintenance • Copiar detalles • Contrato de licencia • Información sobre componentes • Información del sistema
	Ayuda	Permite el acceso a la ayuda en línea.
	Error	Permite ver los errores detectados , página 26.
	Advertencia	Permite ver las advertencias detectadas , página 26.
	Detección	Permite activar la detección cuando la modalidad de detección de dispositivos está establecida en **Manual**.
–	**Manual/Automático**	Seleccione en la lista la modalidad de detección **Manual** o **Automático**. Para obtener más información, consulte el capítulo *Configuración de la modalidad de detección de dispositivos*, página 32.
–	**Ajustes**	Permite configurar **Configuración**.

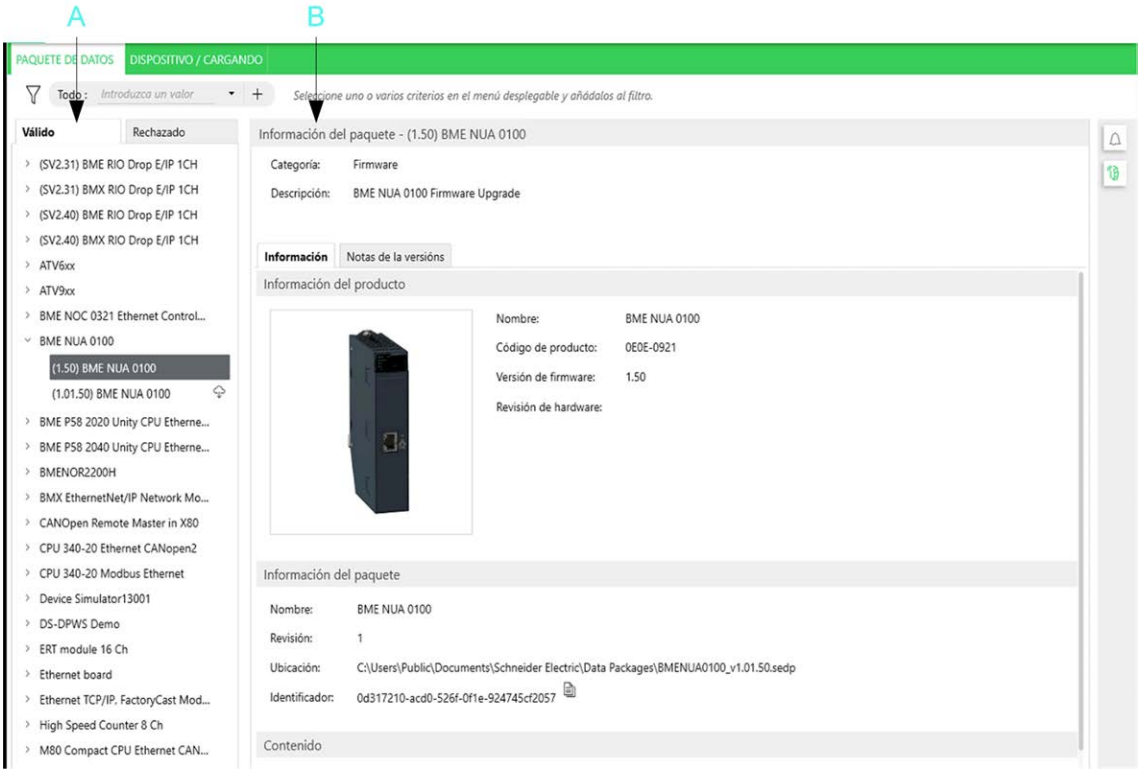
Botones

Botón	Descripción
Resumen	Después de realizar una actualización, haga clic en el botón **Resumen** para recuperar información sobre los dispositivos actualizados.
Actualizar	Después de haber realizado los ajustes para actualizar el firmware, página 69 o actualizar el archivo de configuración de seguridad, página 71, haga clic en el botón **Actualizar** para iniciar el proceso de actualización tal como está configurado.
Cancelar	El botón **Cancelar** le permite cancelar una operación de actualización.

Interfaz de usuario de EcoStruxure Automation Device Maintenance

Paquete de datos

La característica **Paquete de datos** contiene el repositorio del paquete y muestra los paquetes de firmware disponibles en la herramienta.



Número	Nombre	Descripción
A	Lista **PAQUETE DE DATOS** con las fichas **Válido** y **Rechazado**	Muestra la lista de paquetes de firmware disponibles localmente. Los paquetes disponibles en la red se mostrarán siempre que esté instalado el complemento necesario. Para obtener más información, consulte el capítulo *Ficha Paquete de datos*, página 51.
B	**Información del paquete**	Muestra la descripción y el contenido del paquete de datos seleccionado con información estática en la parte superior que indica la **Categoría** y la **Descripción** y con las dos fichas **Información** y **Notas de la versión** en la parte inferior. Para obtener más información, consulte el capítulo *Ficha Paquete de datos*, página 51.

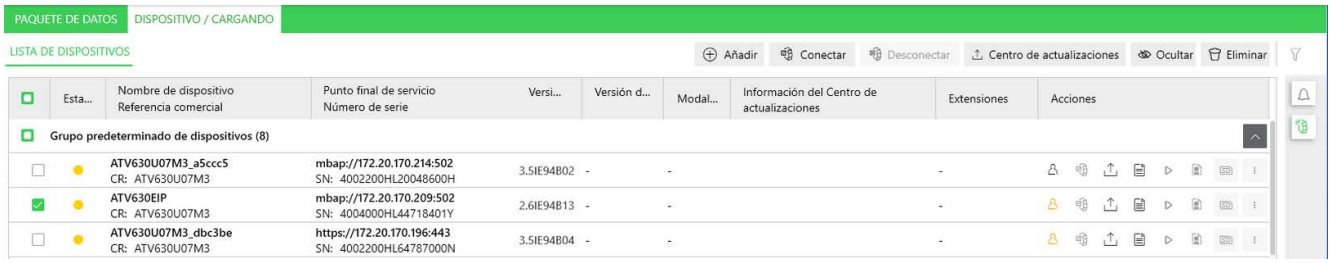
Dispositivo/Cargando

Descripción general

La ficha **Dispositivo/Cargando** muestra los detalles de los dispositivos conocidos por la herramienta.

NOTA: La información que se muestra en esta ficha solo se actualiza automáticamente si el modo de detección está configurado en **Automático**.

Haga clic en el icono de la barra de herramientas para mostrar los valores más recientes.



Botones de la ficha:

Botón	Descripción
Add	Haga clic en el botón **Añadir** para añadir un dispositivo nuevo. Para obtener más información, consulte Agregar dispositivo, página 23.
Conectar	Haga clic en el botón **Conectar** para establecer una conexión con el dispositivo o dispositivos seleccionados.
Desconectar	Haga clic en el botón **Desconectar** para finalizar la conexión con el dispositivo o dispositivos seleccionados.
Centro de actualizaciones	Haga clic en el botón **Centro de actualizaciones** para abrir el cuadro de diálogo **Centro de actualizaciones**. Le permite configurar los ajustes para realizar una actualización del firmware o una actualización del archivo de configuración de seguridad del dispositivo o dispositivos seleccionados. Para obtener más información, consulte **Centro de actualizaciones**, página 68.
Hide	Haga clic en el botón **Ocultar** para ocultar los dispositivos detectados. Para obtener más información, consulte Vista Dispositivo/Cargando, página 55.
Dispose	Haga clic en el botón **Desechar** para descartar el dispositivo o dispositivos detectados. Para obtener más información, consulte Vista Dispositivo/Cargando, página 55.
	Haga clic en el botón **Área de notificaciones** para ver el área de notificaciones en el lado derecho de la ficha **Dispositivo/Cargando**. Para obtener más información, consulte *Visualización/confirmación de mensajes*, página 67.
	Haga clic en el botón **Estado de detección de dispositivos** para ver la vista **Estado de detección de dispositivos** en el lado derecho de la ficha **Dispositivo/Cargando**. Para obtener más información, consulte *Supervisión del estado de detección de dispositivos*, página 66.

Elementos de la tabla:

Elemento	Descripción
Grupo	Puede asignar los dispositivos que se muestran en la **LISTA DE DISPOSITIVOS** a distintos grupos, tal como se describe en el capítulo Agrupación de dispositivos en la LISTA DE DISPOSITIVOS, página 56. Para seleccionar todos los dispositivos que pertenecen a un **Grupo**, marque la casilla de verificación del **Grupo**.
Casillas de verificación	Marque varias casillas de verificación en el lado izquierdo para realizar la misma operación en varios dispositivos simultáneamente, como **Conectar**/**Desconectar** u operaciones de actualización.

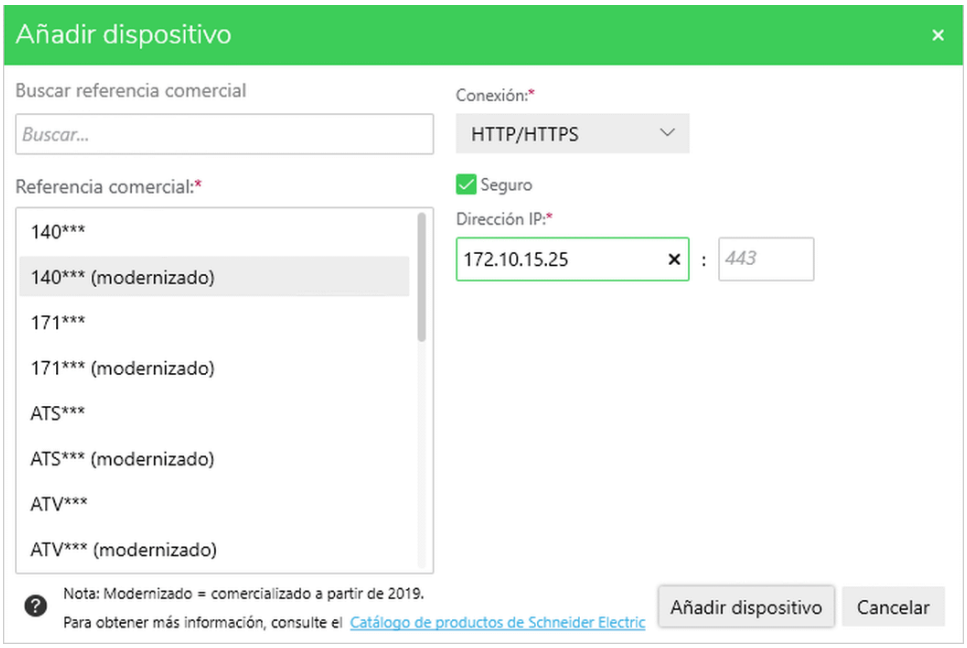
Elemento	Descripción
Estado	Muestra el estado del dispositivo: • **Gris**: el dispositivo está desconectado de la red. • **Amarillo**: el dispositivo está conectado a la red, pero no se han introducido credenciales válidas. • **Verde**: se han introducido credenciales válidas. • **Azul**: la herramienta está cargando contenido en el dispositivo. • **Rojo**: el dispositivo se está reiniciando después de descargar el firmware para completar la instalación.
Nombre del dispositivo **Referencia comercial**	Muestra el nombre y la referencia comercial (**CR**) del dispositivo. **NOTA:** Si asignó un **Nombre descriptivo** a su dispositivo, este nombre definido por el usuario solo se mostrará si el protocolo de comunicación admite este parámetro. Modbus TCP, por ejemplo, no lo admite.
Punto final de servicio **Número de serie**	Muestra la dirección del punto final de servicio como URI (identificador uniforme de recursos) y el número de serie (**SN**) del dispositivo.
Versión de firmware	Muestra la versión actual del firmware del dispositivo.
Modalidad	Solo disponible tras iniciar sesión: Indica el modo del dispositivo: **RUN, STOP, BUSY, NOCONF, RESERVED, ENTERED, LOADING, COMPLETED, REQUIRERESTART, ERROR**. El contenido de esta celda se actualiza periódicamente. **NOTA:** En función del número de dispositivos a los que esté conectado, la supervisión de este modo puede afectar al ancho de banda de la red.
Información del Centro de actualizaciones	Muestra los ajustes de actualización que se han configurado en el cuadro de diálogo **Centro de actualizaciones**: **Firmware seleccionado**, **Configuración de seguridad seleccionada**, **El firmware se ha actualizado correctamente**, **La actualización del firmware se ha cancelado**, **El firmware no se ha actualizado**. Para obtener más información, consulte **Centro de actualizaciones**, página 68.
Extensiones	Los dispositivos modulares proporcionan un enlace (Extensiones) que le permite acceder a las extensiones individuales del dispositivo. Para obtener más información, consulte Acceso a extensiones, página 64.
Acciones	Se muestran iconos que corresponden a cada dispositivo, para que se realicen operaciones distintas específicas de cada dispositivo:
	Haga clic en el icono **Definir credenciales** e introduzca las credenciales para conectarse al dispositivo en el cuadro de diálogo **Definir credenciales**. El icono negro indica que no se ha almacenado ninguna credencial para el dispositivo. El icono amarillo indica que se han almacenado credenciales, pero que no se ha iniciado sesión en el dispositivo. Otra opción es configurar credenciales globales para el proyecto mediante **Configuración > Proyecto > Ajustes de credenciales de usuario**. Para obtener más información, consulte Administración de credenciales de usuario, página 61.
	Cuando el icono **Definir credenciales** está de color verde, indica que las credenciales del dispositivo se han validado y que el inicio de sesión se ha realizado correctamente.
	Si el icono **Definir credenciales** está de color rojo, indica que el intento de iniciar sesión en el dispositivo no ha tenido éxito. Vuelva a ejecutar el procedimiento de inicio de sesión y asegúrese de utilizar las credenciales correctas.
	Haga clic en el icono **Conectar**/**Desconectar** para establecer o finalizar una conexión con el dispositivo.
	Haga clic en el icono **Centro de actualizaciones** para abrir el cuadro de diálogo **Centro de actualizaciones**. Le permite configurar los ajustes para realizar una actualización del firmware o una actualización del archivo de configuración de seguridad del dispositivo. Para obtener más información, consulte **Centro de actualizaciones**, página 68.
	Haga clic en el icono **Registro del dispositivo** para ver la información de registro.
	Haga clic en el icono **Iniciar dispositivo** para iniciar el dispositivo. **NOTA:** Realice una prueba de puesta en marcha antes de usar el equipo de control eléctrico y automatización para operaciones normales después de la instalación o actualización. Para obtener más información, consulte Iniciar y probar, página 7.
	Muestra el estado del certificado. • Gris: Certificado de confianza • Rojo: Certificado no de confianza Haga clic en el icono **Certificado del dispositivo** para abrir el cuadro de diálogo **Información del certificado**. Para obtener más información, consulte Gestión del estado de confianza de certificados en la ficha **Dispositivo/Cargando**, página 47.

Elemento	Descripción
	Indica que el dispositivo está equipado con una tarjeta de memoria SD. Haga clic en este icono para descargar directamente el software en la tarjeta de memoria SD.
	Haga clic en el icono **Opciones adicionales del dispositivo** para ver una lista de comandos disponibles para los dispositivos después de iniciar sesión correctamente. Para obtener más información, consulte *Detalles disponibles después de iniciar sesión*, página 56.
Progreso	Muestra el estado del progreso de actualización del firmware.

Agregar dispositivo

Descripción general

El cuadro de diálogo **Agregar dispositivo** se abre al hacer clic en el botón + Add de la ficha **Dispositivo/Carga** o al hacer clic en **No se encontró ningún dispositivo**. **Para agregar un dispositivo, haga clic aquí** en el vínculo que aparece cuando la lista de dispositivos está vacía, por ejemplo, si crea un proyecto nuevo.



Le permite añadir dispositivos manualmente si EcoStruxure Automation Device Maintenance no puede detectarlos automáticamente, ya sea porque el dispositivo no admite la detección o porque la función de detección está desactivada. Para hacerlo, seleccione la referencia comercial.

De forma predeterminada, la lista de **Referencias comerciales** solo contiene plantillas de referencias comerciales (como **BME****, **BMX**** o **Cualquier dispositivo)**. En este caso, tiene dos opciones:

- Seleccionar la plantilla que coincida con su producto: Por ejemplo, para BMEP582020, seleccione **BME***** en la lista.

  NOTA: Se presentan dos variantes para cada plantilla que cubren la versión antigua (por ejemplo, **BME****) y la versión reciente (por ejemplo, **BME*** (modernizado)**). Se diferencian en los protocolos compatibles. Por lo tanto, si no encuentra el protocolo de su elección en la lista **Conexión**, seleccione la segunda opción proporcionada para su producto.

- Para completar la lista con referencias comerciales de los dispositivos que está utilizando, copie los paquetes de datos correspondientes en la carpeta que configuró como **Repositorio local** en el cuadro de diálogo **Configuración > Configuración del paquete** (para obtener más información, consulte el capítuloConfiguración de ubicación de los paquetes, página 37). A continuación, en la tabla se mostrarán referencias específicas (como **BMEP582020** o **BMXNOR0200**).

Componente	Descripción
Referencia comercial	Seleccione el número de **Referencia comercial** de su dispositivo en la lista y especifique la información del dispositivo de acuerdo con el protocolo seleccionado en la lista **Conexión** del lado derecho.
Conexión	Seleccione en la lista el protocolo empleado para la comunicación: • **HTTP/HTTPS** • **MODBUS (SL)** • **MODBUS (TCP)** • **OPC UA** • **FTP** • **USB** Los parámetros variarán en función del protocolo seleccionado.
Seguridad	Esta opción solo está disponible para la comunicación **HTTP/HTTPS**: Seleccione esta opción si el dispositivo está conectado a través de una conexión segura (HTTPS).
Dirección IP	Introduzca la dirección IP del dispositivo que desea añadir, así como el puerto empleado para la comunicación.
ID de la unidad	Esta opción solo está disponible para la comunicación **MODBUS (TCP)**: Introduzca el nodo de identificación de la unidad para la comunicación Modbus TCP. Para obtener más información sobre las especificaciones de Modbus, consulte Modbus Specifications and Implementation Guides.

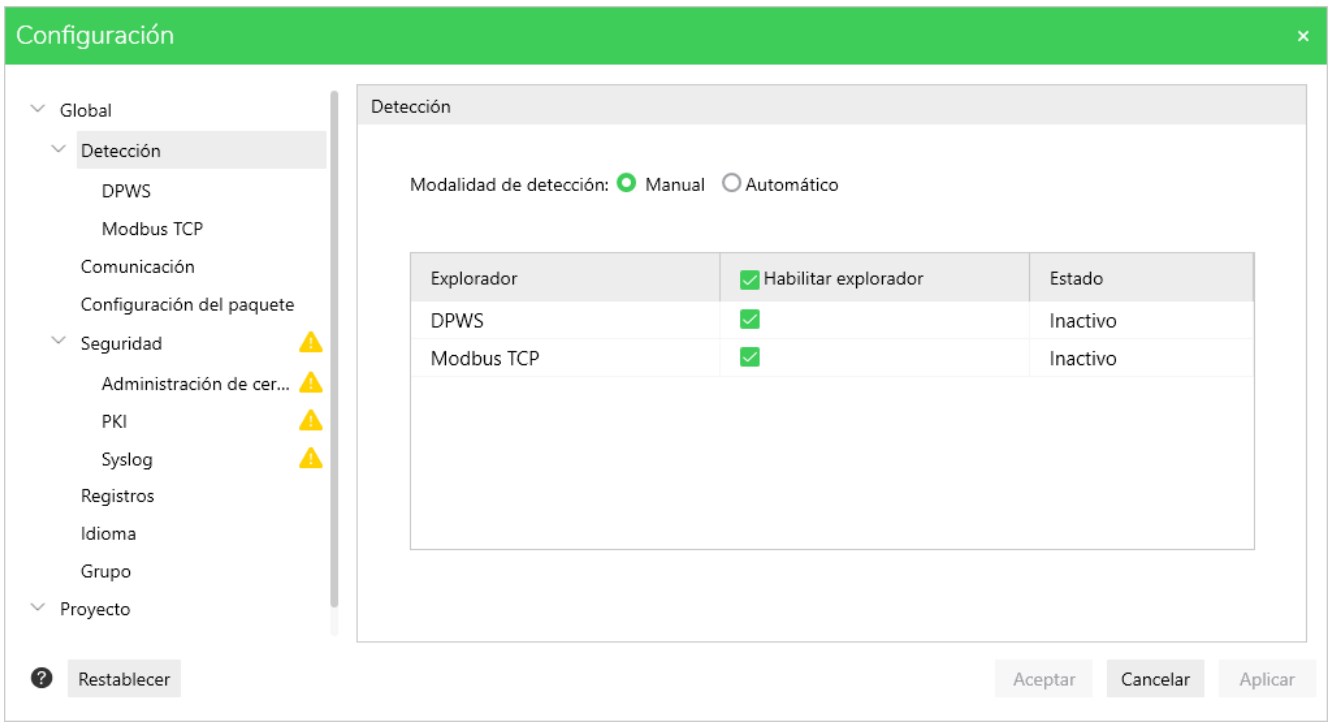
NOTA: EcoStruxure Automation Device Maintenance versión V3.1 y versiones posteriores permiten la inclusión de dispositivos mediante la referencia comercial. Si intenta abrir archivos de proyecto creados con EcoStruxure Automation Device Maintenance V3.0 y versiones anteriores que contienen dispositivos sin referencia comercial, se le pedirá que seleccione una referencia comercial para cada dispositivo desconocido.

Consulte también Apertura del proyecto, página 29.

Configuración de ajustes

Descripción general

La página **Ajustes** permite configurar los ajustes generales.



Componentes	Descripción
Discovery	Seleccione la herramienta para configurar la modalidad de detección. Para obtener más información, consulte Configuración del modo de detección de dispositivos, página 32.
DPWS	Seleccione la herramienta para configurar los detalles del explorador DPWS. Para obtener más información, consulte Configuración del explorador DPWS, página 36.
Modbus TCP	Seleccione la herramienta para configurar los detalles del explorador de Modbus. Para obtener más información, consulte Configuración del explorador Modbus TCP, página 34.
Communication	Seleccione para configurar los parámetros de comunicación. Para obtener más información, consulte Configuración de los parámetros de comunicación, página 37.
Configuración del paquete	Seleccione la herramienta para configurar los ajustes de paquete. Para obtener más información, consulte Configuración de ubicación de los paquetes, página 37.
Seguridad	Seleccione la opción para activar el modo de protección y para mostrar las notificaciones relacionadas con características de seguridad como la comunicación cifrada mediante certificados, paquetes seguros o compatibilidad con syslog. Para obtener más información, consulte Características de seguridad, página 41.
Administración de certificados	Seleccione para inscribir el certificado de aplicación de EcoStruxure Automation Device Maintenance y administrar el estado de confianza de los certificados digitales de los socios de comunicación. Para obtener más información, consulte Gestión de certificados, página 43.
PKI	Seleccione para configurar una infraestructura de clave pública (PKI). Para obtener más información, consulte Gestión de la infraestructura de clave pública (PKI), página 48.
Registros	Seleccione para ver los archivos de registro de EcoStruxure Automation Device Maintenance y configurar los parámetros de registro. Para obtener más información, consulte Visualización de los archivos de registro, página 38.
Idioma	Seleccione la herramienta para configurar el idioma deseado. Para obtener más información, consulte Configuración del idioma, página 40.
Grupo	Seleccione para agrupar los dispositivos que se muestran en la **LISTA DE DISPOSITIVOS**. Para obtener más información, consulte Agrupación de dispositivos en la LISTA DE DISPOSITIVOS, página 56.
Proyecto > Ajustes de credenciales de usuario	Seleccione esta opción para introducir credenciales globales para los dispositivos del proyecto. Para obtener más información, consulte Administración de credenciales de usuario, página 61.

Aplicar modificaciones

Siempre que modifique la configuración en una ficha de la página **Configuración**, esta ficha se marca con el icono de actualización que indica que algunas modificaciones en esta página aún no se han aplicado.

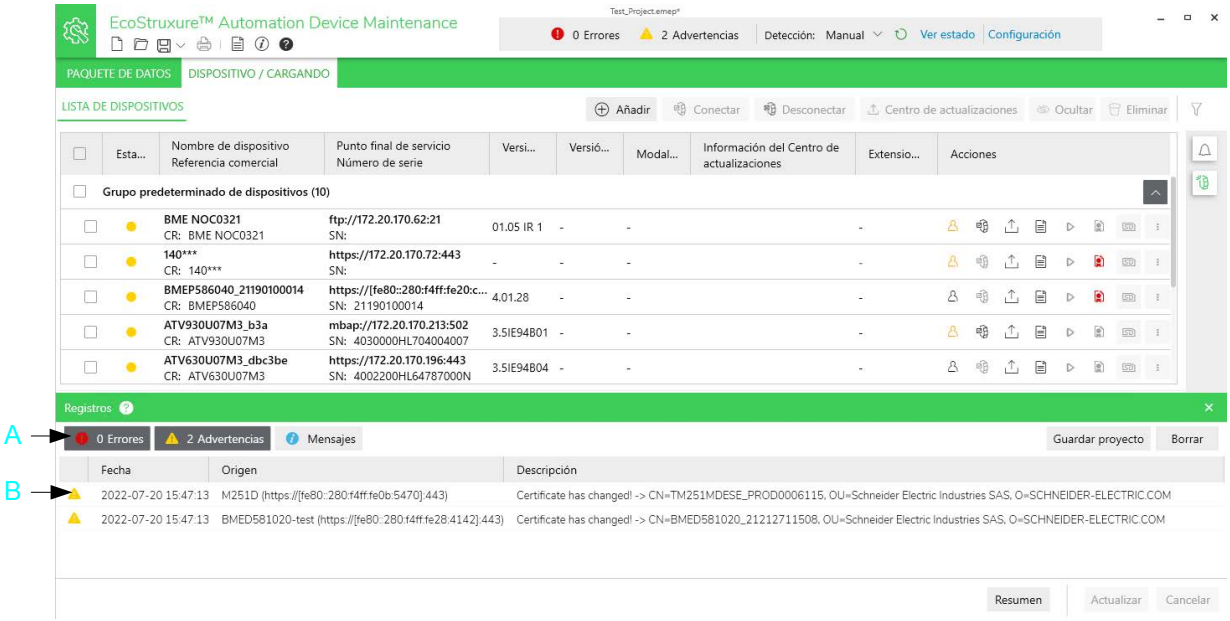
Para aplicar las modificaciones a esta página, haga clic en el botón **Aplicar**.

Para aplicar las modificaciones realizadas en todas las fichas y cerrar la página **Configuración**, haga clic en el botón **Aceptar**.

Ventana de errores y advertencias

Descripción general

Puede visualizar detalles de los errores detectados en la herramienta en una ventana de registros acumulados. El registro de errores proporciona los detalles para corregir el error detectado relacionado con el dispositivo seleccionado. No puede proseguir con la actualización del firmware para los dispositivos seleccionados a menos que se resuelvan los errores detectados.



Número	Nombre	Descripción
A	Estado de error y advertencia	Muestra el número de errores detectados y advertencias detectadas.
B	**Registros**	Muestra el número de errores detectados y advertencias detectadas con la descripción.

Visualización de registros de error y advertencias

Paso	Acción
1	Haga clic en el estado **Errores** o **Advertencias** en la barra de herramientas. En la ventana **Registros** se muestra la información siguiente: • Número de errores detectados, advertencias detectadas e información. • Descripción de los errores detectados.
2	Seleccione el error detectado, la advertencia detectada y los mensajes informativos de su elección.

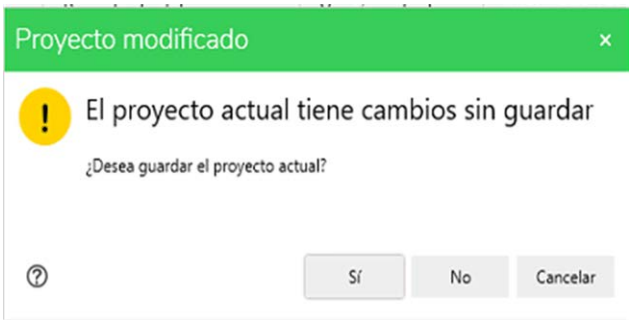
Paso	Acción
3	Haga clic en **Guardar** para guardar el error detectado, advertencia detectada o información seleccionados.
4	Haga clic en **Borrar** para eliminar todos los mensajes acerca de errores detectados y advertencias detectadas del registro.

Creación de un nuevo proyecto de EcoStruxure Automation Device Maintenance

Procedimiento

Esta función permite crear un nuevo proyecto de EcoStruxure Automation Device Maintenance.

Siga los pasos que se indican a continuación para crear un proyecto:

Paso	Acción
1	Haga clic en el icono . **Resultado**: Aparecerá el cuadro de diálogo **Proyecto modificado** si hay abierto un proyecto modificado y que aún no se ha guardado.
2	En el cuadro de diálogo **Proyecto modificado**, haga clic en **Sí** para guardar los cambios en el proyecto abierto o en **No** para cerrar el proyecto sin guardar.  **Resultado**: Se cierra el proyecto abierto y se abre un nuevo proyecto que muestra la ficha **Dispositivo/Cargando** con la lista de dispositivos vacía.

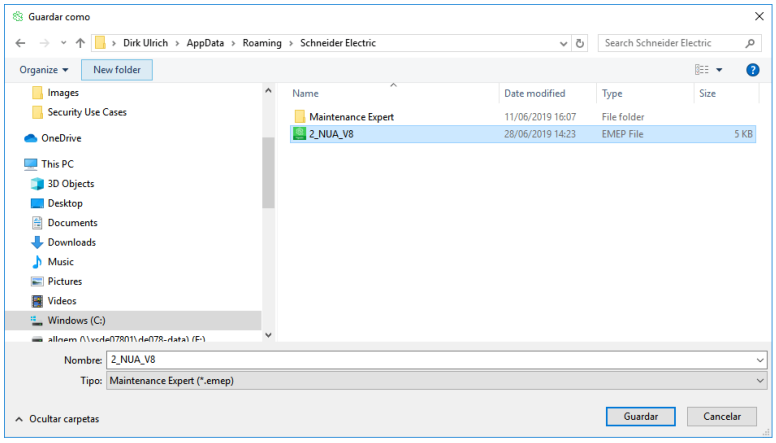
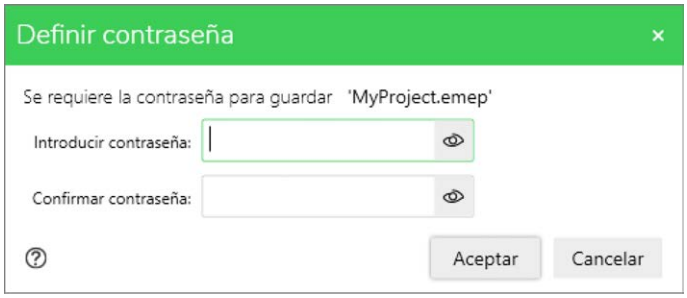
Al crear un nuevo proyecto, se ejecutan automáticamente las siguientes tareas:

- La modalidad de detección se establece en **Manual**.
- Las entradas del archivo de registro se borran.

Guardado del proyecto

Esta característica permite guardar una copia del proyecto actual con un nombre distinto o en una ubicación distinta. La ventaja es que no es necesario añadir los dispositivos una y otra vez cuando se abre la herramienta EcoStruxure Automation Device Maintenance.

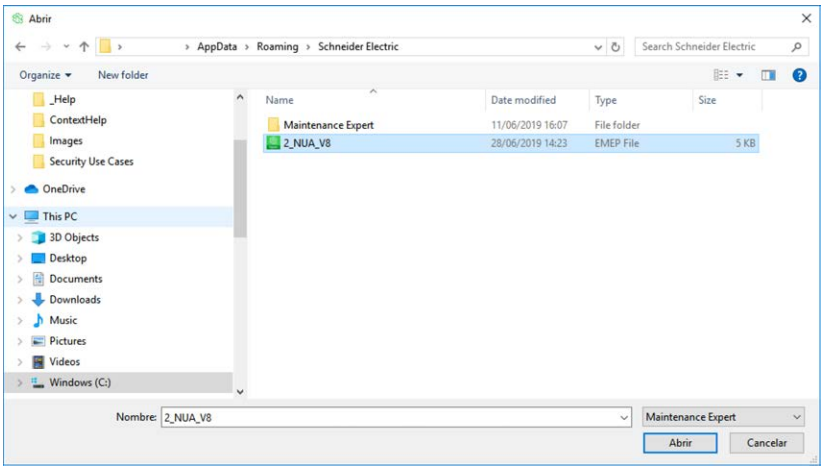
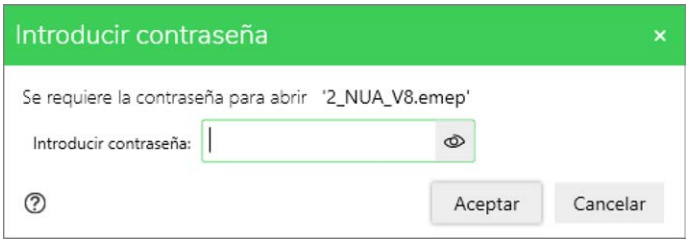
Siga los pasos siguientes para guardar los ajustes del proyecto:

Paso	Acción
1	Haga clic en el icono .
2	Para guardar los cambios del proyecto actual, haga clic en **Guardar**. Para guardar una copia del proyecto, haga clic en **Guardar como**.
3	Seleccione la carpeta en la que desea guardar el proyecto e introduzca el **Nombre de archivo**. 
4	Haga clic en **Guardar** e introduzca la misma contraseña en ambos campos del cuadro de diálogo **Definir contraseña**. 
5	Haga clic en **Aceptar** para continuar.

Apertura del proyecto

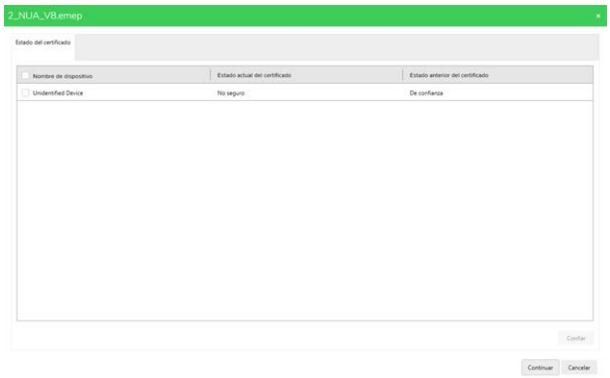
Apertura de un proyecto

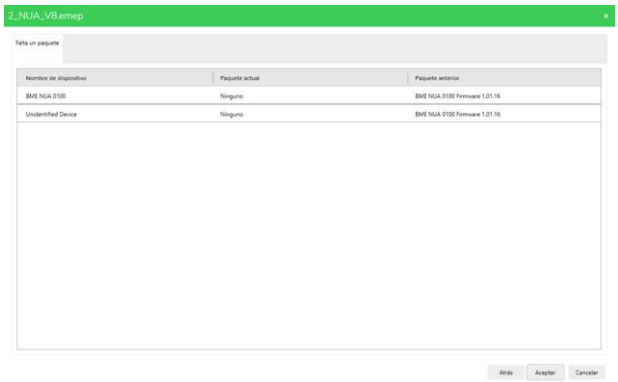
Para abrir un proyecto, siga los pasos que se describen a continuación.

Paso	Acción
1	Haga clic en el icono . 
2	Seleccione la carpeta y el proyecto. Haga clic en **Abrir** e introduzca la contraseña. 
3	Haga clic en **Aceptar** para abrir el proyecto.

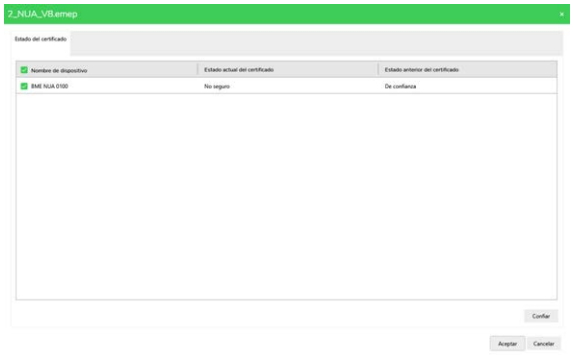
Pasos opcionales para archivos de proyecto creados en otro ordenador

Si intenta abrir un archivo de proyecto creado en otro ordenador, la herramienta indica opcionalmente diferencias del estado de confianza del certificado y diferencias de disponibilidad del paquete.



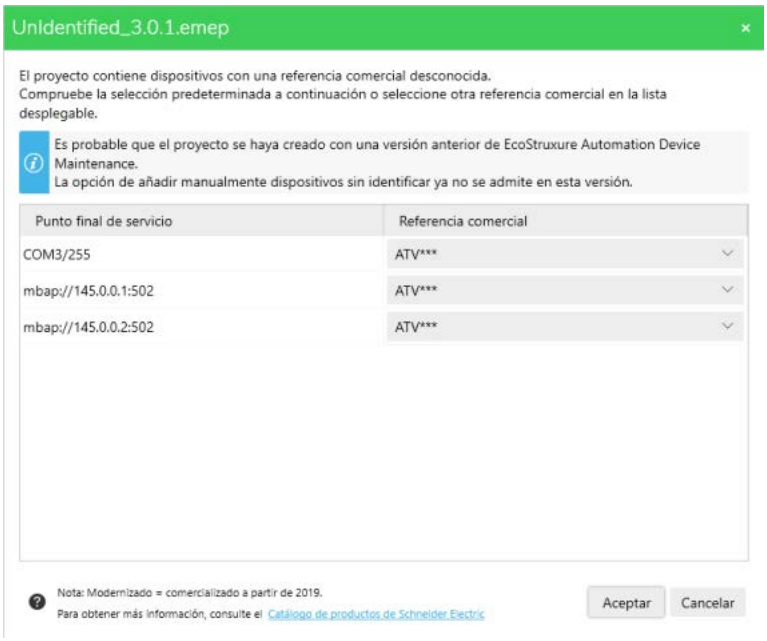


En este caso, proceda como se indica a continuación:

Paso	Acción
4	Seleccione los dispositivos que desea establecer como de confianza y haga clic en **Confiar**.
5	Haga clic en **Continuar**. 
6	Haga clic en **Aceptar** para abrir el proyecto al que le faltan paquetes o haga clic en **Cancel**.

Paso opcional para archivos de proyecto con dispositivos no identificados

Si intenta abrir archivos de proyecto creados con EcoStruxure Automation Device Maintenance V3.0 y versiones anteriores que contienen dispositivos sin referencia comercial, aparecerá un cuadro de diálogo en el que se le solicitará que seleccione una referencia comercial para cada dispositivo desconocido de la lista:



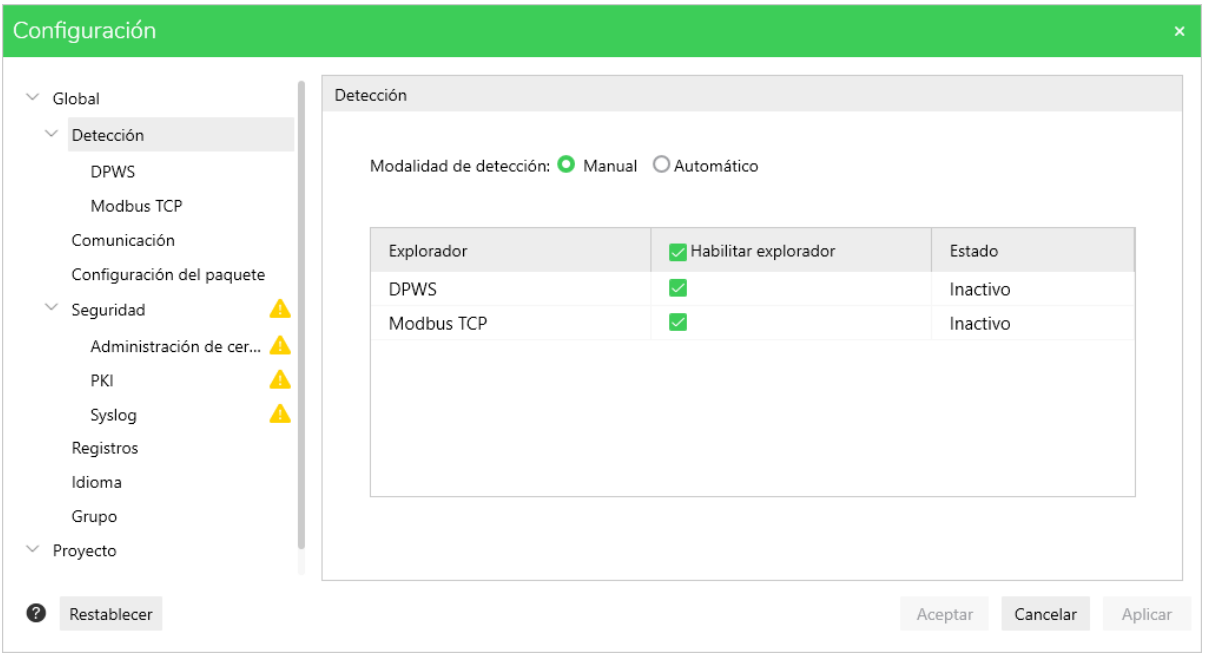
Seleccione las referencias comerciales que desee y haga clic en **Aceptar** para abrir el proyecto.

Configuración de la herramienta EcoStruxure Automation Device Maintenance

Configuración del modo de detección de dispositivos

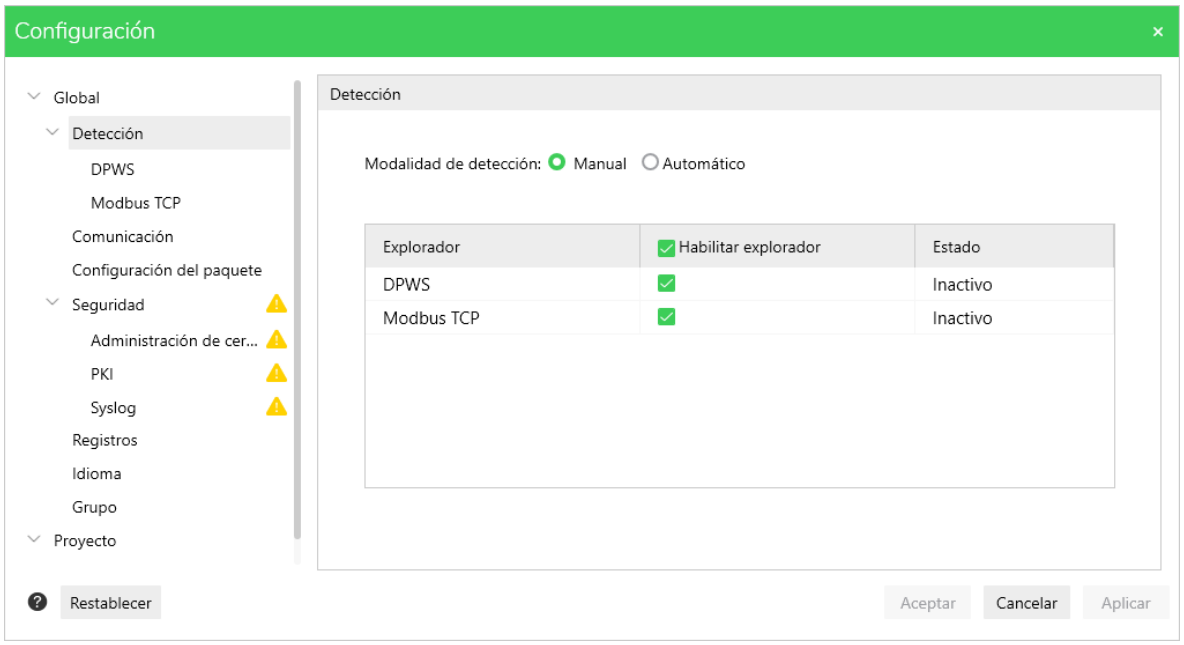
Configuración del modo de detección automática

Puede seleccionar la modalidad de detección de dispositivos como **Automático** o **Manual**. En el caso de detección **automático**, la herramienta enviará información periódicamente a través de la red en segundo plano y recibirá información de los dispositivos que respondan.

Paso	Acción
1	Haga clic en el menú **Configuración** de la parte superior central de la página **Inicio**.
2	Haga clic en la opción **Detección**. 
3	Seleccione la modalidad **Automático**.
4	Seleccione los escáneres que formarán parte de la detección. Utilice este ajuste para evitar que se escaneen los dispositivos que desee evitar.
5	Haga clic en **Aplicar** y, a continuación, haga clic en **Aceptar**.

Configuración de la modalidad de detección manual

Puede seleccionar la modalidad de detección como **Manual** para detectar los dispositivos conectados a la red cuando sea necesario.

Paso	Acción
1	Haga clic en el menú **Configuración** de la parte superior central de la página **Inicio**.
2	Haga clic en la opción **Detección**. 
3	Seleccione la modalidad **Manual**.
4	Seleccione los escáneres que formarán parte de la detección. Utilice este ajuste para evitar que se escaneen los dispositivos que desee evitar.
5	Haga clic en **Aplicar** y, a continuación, haga clic en **Aceptar**.

Configuración del explorador Modbus TCP

Descripción general

El explorador **Modbus TCP** envía peticiones del código de función Modbus 43 a todas las direcciones IP de un rango definido por una **dirección IP de inicio** y una **dirección IP final.**.

Puede configurar los siguientes parámetros de **TCP Modbus**:

Elemento	Valor predeterminado	Descripción
Sección **Dirección IP**:		
Parámetro **Nombre de rango**	–	Nombre opcional del rango de direcciones.
Parámetro **Dirección IP inicial**	127.0.0.1	Primera dirección del rango de la exploración de direcciones.
Parámetro **Dirección IP final**	127.0.0.1	Última dirección del rango de la exploración de direcciones.
Botón **Importar**	–	Haga clic en el botón **Importar** para importar un archivo de configuración disponible en formato .csv (consulte el siguiente ejemplo de archivo de configuración de importación, página 34). **NOTA:** Con este comando se sobrescriben los valores de configuración actuales. Asegúrese, por tanto, de realizar una copia de seguridad de los valores antes de ejecutar esta función. **Resultado**: Se abrirá el cuadro de diálogo **Abrir archivo** de Windows que le permitirá explorar la red para encontrar el archivo csv. Haga clic en **Abrir** para importar los valores de configuración del archivo. Para aplicar los nuevos valores de configuración, haga clic en **Aplicar** o en **Aceptar**.
Botón **+ Añadir**	–	Haga clic en el botón **+ Añadir** para crear un nuevo rango de direcciones. **Resultado**: Se añade una nueva línea a la tabla con: **Nombre de rango = Predeterminado** **Dirección IP de inicio = 127.0.0.1** **Dirección IP final = 127.0.0.1**
Casilla de verificación	–	Active o desactive una casilla de verificación para incluir o excluir el rango seleccionado para la exploración de Modbus.
Botón de papelera	–	Haga clic en el botón de la papelera para eliminar el rango seleccionado, es decir, la línea de la tabla.
Sección **Configuración avanzada**:		
Parámetro **Puerto inicial**	502	Primer puerto del rango de exploración de puertos.
Parámetro **Puerto final**	502	Último puerto del rango de exploración de puertos.
Parámetro **Tiempo de espera**	4000	Tiempo de espera máximo entre el envío de un comando ping a un dispositivo y la recepción de la respuesta.
Parámetro **ID de la unidad**	255	ID de la unidad Modbus utilizada para acceder al dispositivo.

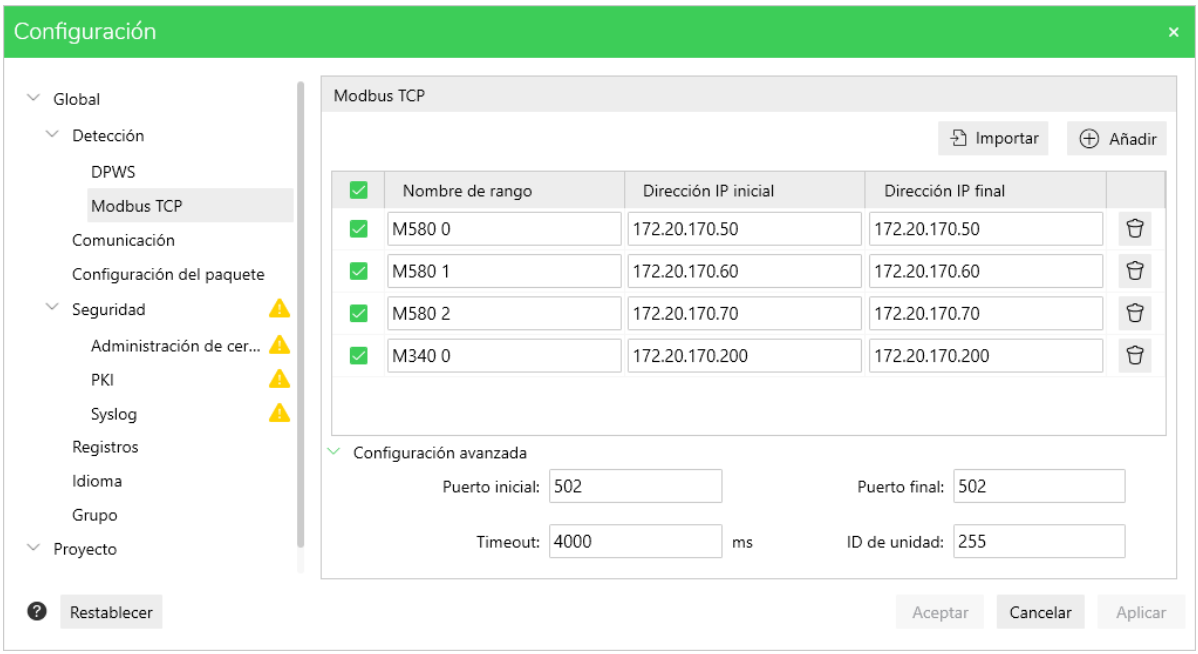
Ejemplo de un archivo de configuración de importación

El formato del archivo de configuración en formato .csv deberá ser compatible con el siguiente ejemplo:

```
enabled;name;start;end
1;range 1;127.0.0.1;127.0.0.1
1;range 2;127.0.0.2;127.0.0.2
```

Configuración del explorador TCP Modbus

Siga los pasos siguientes para configurar el explorador **TCP Modbus**:

Paso	Acción
1	Amplíe el menú **Detección** de la página **Configuración**.
2	Seleccione el nodo **TCP Modbus**.
3	En el lado derecho de la vista **TCP Modbus**, haga clic en el botón **Añadir** para crear un nuevo rango de direcciones.
4	Haga clic en el botón **Importar** para importar un archivo de configuración o para configurar los siguientes parámetros: • **Nombre del rango** • **Dirección IP inicial** • **Dirección IP final** • **Puerto inicial** • **Puerto final** • **Tiempo de espera** • **ID de la unidad** 
5	Haga clic en **Aplicar** para aplicar los valores de configuración de Modbus TCP o en **Aceptar** para aplicar todas las modificaciones realizadas en los valores de la aplicación y cerrar el cuadro de diálogo **Configuración**.

Configuración del explorador DPWS

Descripción general

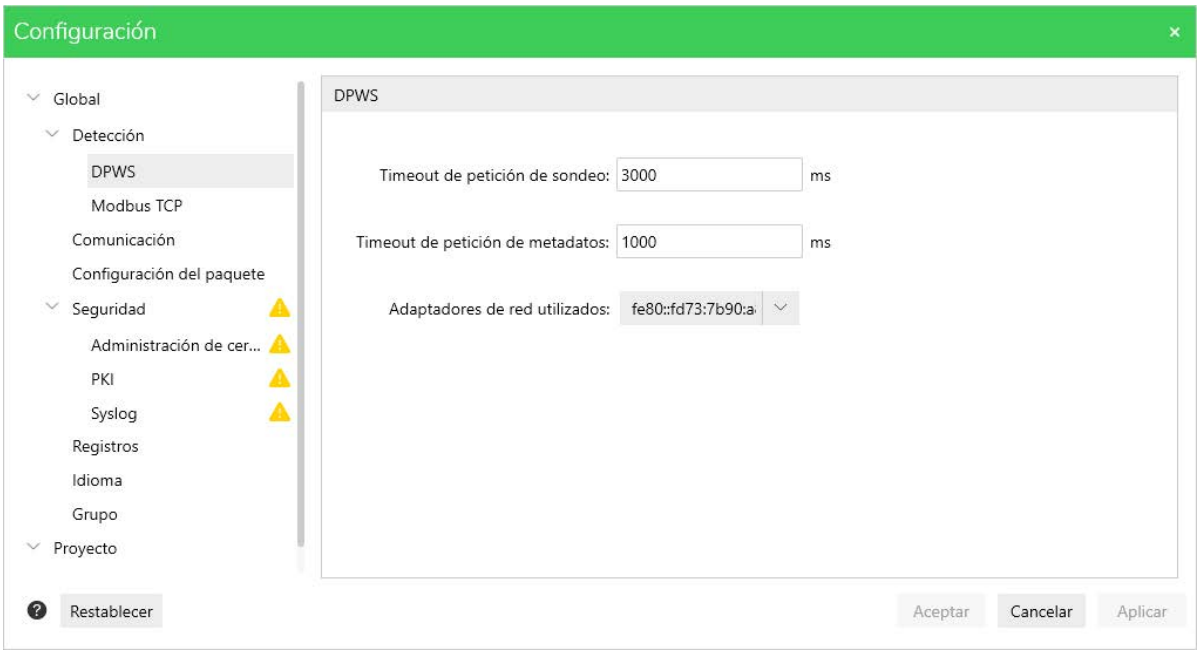
El explorador **DPWS** es una implementación del lado del cliente del estándar **DPWS** que permite detectar dispositivos compatibles con DPWS.

Para obtener más información sobre el estándar DPWS, consulte http://docs.oasis-open.org/ws-dd/ns/dpws/2009/01.

Puede configurar los siguientes parámetros de **DPWS**:

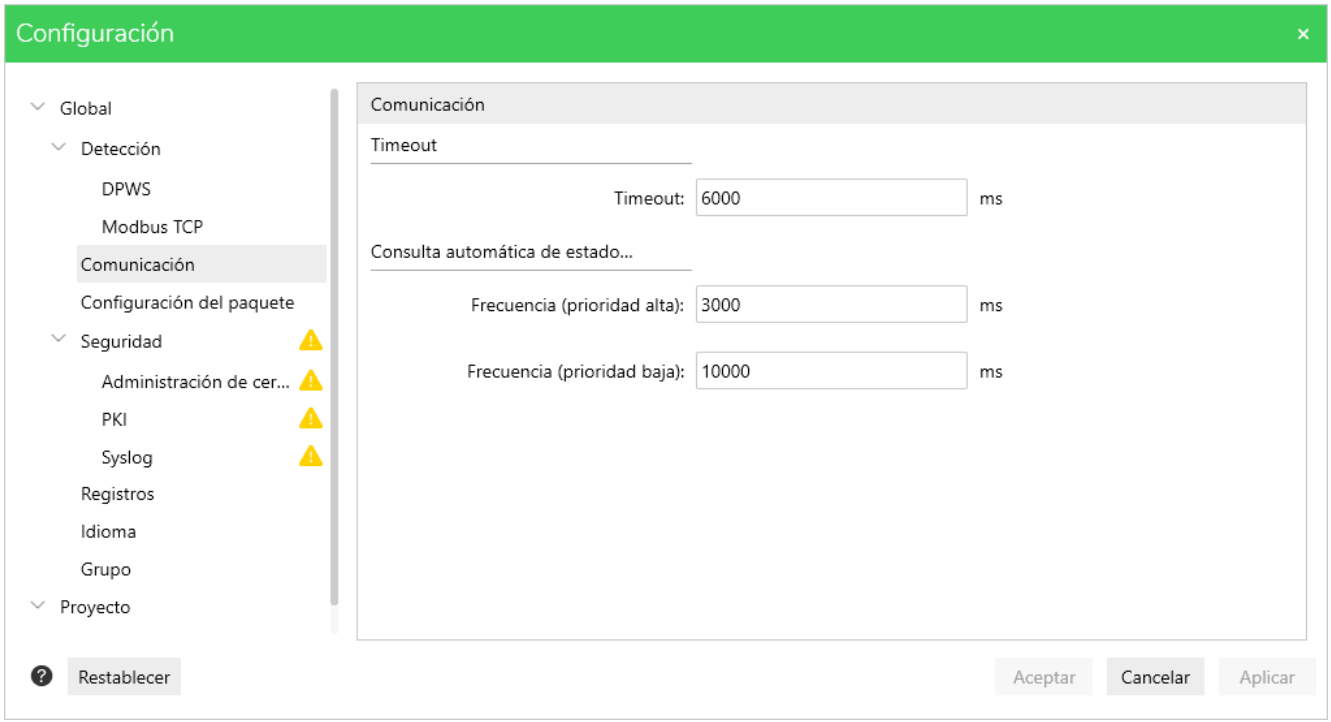
Parámetro	Valor predetermina-do	Descripción
Timeout de petición de sondeo	3000 ms	Tiempo de espera máximo entre el envío de una solicitud de sondeo y la recepción de las respuestas de sondeo coincidentes desde los dispositivos.
Timeout de petición de metadatos	1000 ms	Tiempo de espera máximo entre el envío de una solicitud de metadatos y la recepción de la respuesta desde el dispositivo.
Adaptadores de red utilizados	–	Lista de adaptadores de red utilizados para el envío de solicitudes de sondeo de **DPWS**.

Siga los pasos siguientes para configurar el explorador **DPWS**:

Paso	Acción
1	Amplíe el menú **Detección** de la página **Configuración**.
2	Seleccione **DPWS** e introduzca los detalles siguientes: • **Timeout de petición de sondeo** • **Timeout de petición de metadatos** • **Adaptadores de red utilizados** 
3	Haga clic en **Aplicar** y, a continuación, haga clic en **Aceptar**.

Configuración de los parámetros de comunicación

Descripción general



Es posible configurar los siguientes parámetros para la comunicación entre EcoStruxure Automation Device Maintenance y los dispositivos:

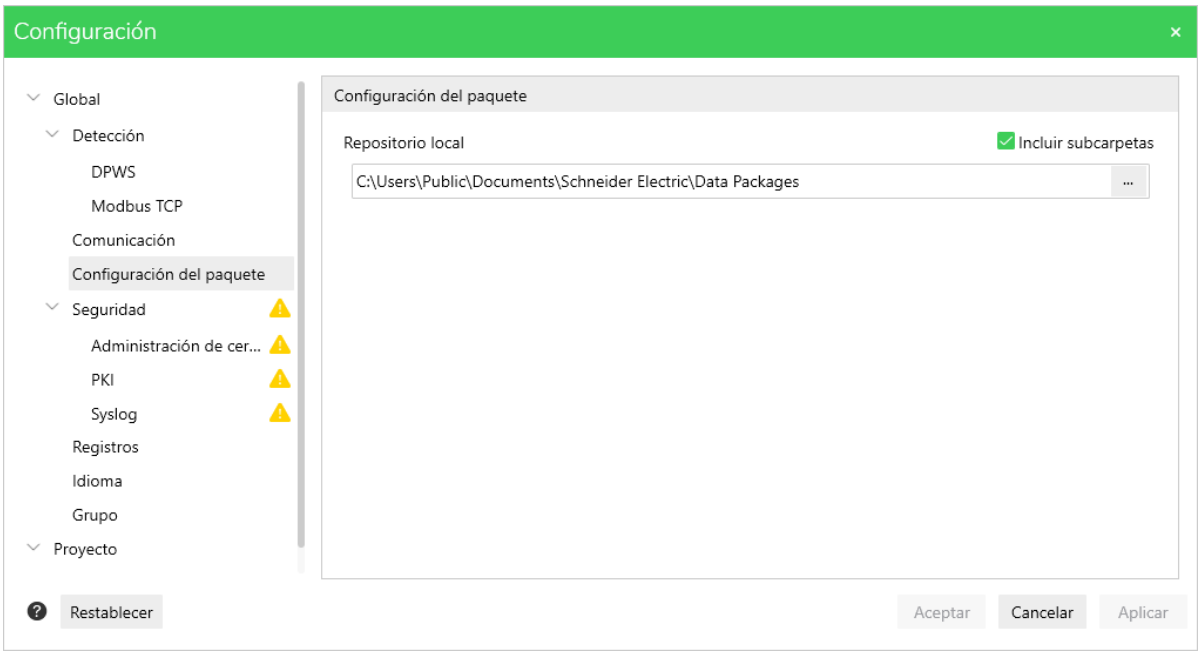
Parámetro	Valor predeterminado	Descripción
Sección **Tiempo de espera**:		
Tiempo de espera	6000 ms	Tiempo de espera máximo tras el envío o la recepción por parte de EcoStruxure Automation Device Maintenance de peticiones o respuestas (por ejemplo, actualizaciones del firmware o configuración de los parámetros de IP). En el caso de los tiempos de espera que se aplican a peticiones de detección, consulte el Explorador Modbus TCP, página 34 y el Explorador DPWS, página 36.
Sección**Consulta automática de estado de dispositivo**: Estos parámetros definen la frecuencia del envío de solicitudes de sondeo a dispositivos detectados para mantener actualizado el estado del dispositivo, página 21:		
Frecuencia (prioridad alta):	3000 ms	El sondeo de alta prioridad se utiliza al ejecutar actualizaciones del firmware. Permite acelerar la detección del dispositivo una vez que se ha reiniciado.
Frecuencia (prioridad baja):	10.000 ms	La prioridad baja, que incluye ciclos de sondeo de menor frecuencia, se emplea en el funcionamiento normal.

Configuración de ubicación de los paquetes

Puede configurar la ruta de acceso de los paquetes de datos de firmware disponibles en la herramienta. Esto permite actualizar las versiones de firmware del dispositivo. Además, la referencia comercial específica proporcionada por cada paquete de datos se añade a la lista **Referencia comercial** del cuadro de diálogo **Agregar dispositivo**, página 23.

Cambiar ubicación del paquete

Siga los pasos siguientes para cambiar la ubicación de los paquetes:

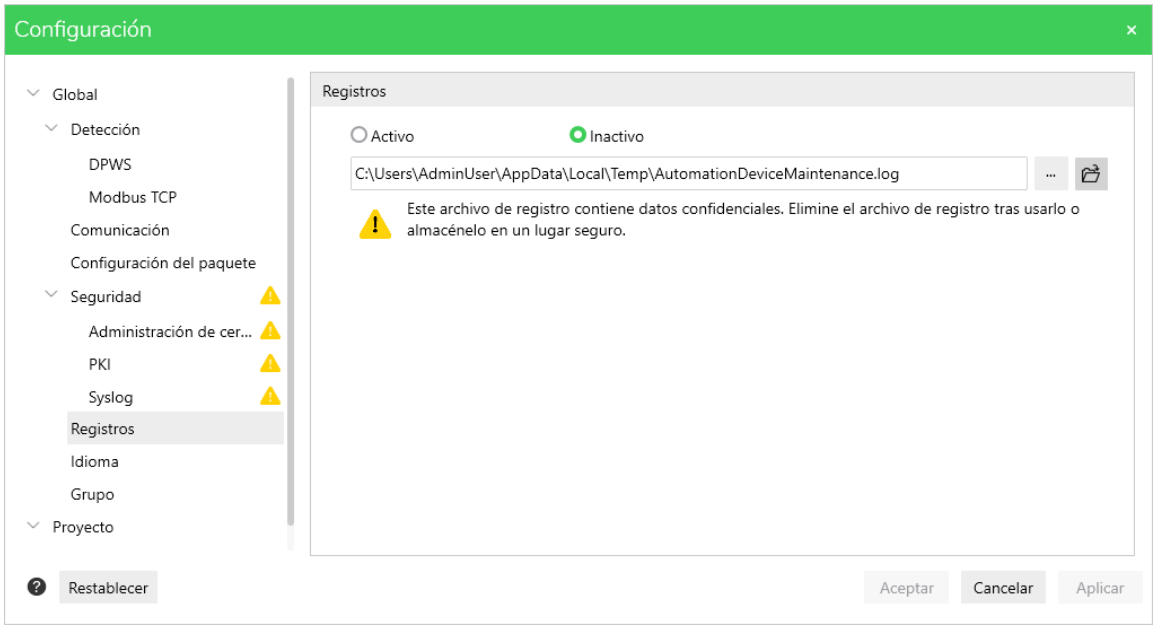
Paso	Acción
1	Haga clic en el menú **Configuración** de la parte superior central de la página **Inicio**.
2	Seleccione la opción **Configuración del paquete**.
3	Seleccione la ruta para cambiar la ubicación del **Repositorio local**.
4	Haga clic en el icono ... y seleccione la carpeta de destino para cambiar la ruta. 
5	Haga clic en **Aplicar** y, a continuación, haga clic en **Aceptar**.

Visualización de los archivos de registro

Puede visualizar los registros almacenados y analizarlos para hallar detalles para el dispositivo seleccionado.

Siga los pasos siguientes para visualizar los registros:

Paso	Acción
1	Haga clic en el menú **Configuración** de la parte superior central de la página Inicio.
2	Seleccione la opción **Registros**.
3	Establezca la característica de creación de registros como **Activa**/**Inactiva**.
4	Seleccione la ruta de acceso para cambiar la ubicación del archivo de registro.

Paso	Acción
5	Haga clic en el icono y seleccione la carpeta de destino para cambiar la ruta.  **NOTA:** Para obtener más información sobre la notificación de ciberseguridad, consulte Recomendación para mejorar la ciberseguridad, página 68.
6	Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

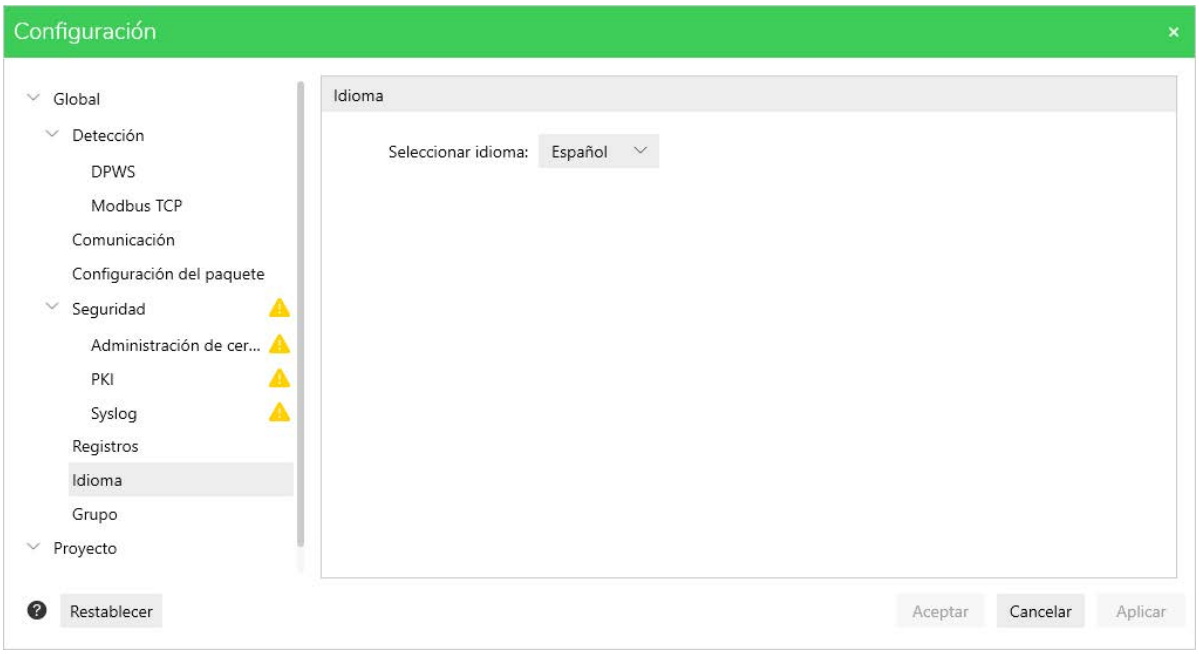
Configuración del idioma

Puede seleccionar el idioma con el que desea visualizar el contenido de la herramienta EcoStruxure Automation Device Maintenance.

Son compatibles los siguientes lenguajes:

- Inglés
- Alemán
- Francés
- Español
- Italiano
- Chino

Siga los pasos siguientes para establecer el idioma:

Paso	Acción
1	Haga clic en el menú **Configuración** de la parte superior central de la página **Inicio**.
2	Seleccione la opción **Idioma**.
3	Haga clic en el idioma deseado de la lista desplegable **Seleccionar idioma**. 
4	Haga clic en **Aplicar** y, a continuación, haga clic en **Aceptar**. **NOTA:** Reinicie EcoStruxure Automation Device Maintenance para aplicar los cambios de idioma.

Restablecimiento de la configuración de la aplicación

Descripción general

Los cuadros de diálogo del menú **Configuración** incluyen un botón **Resetear** en la esquina inferior izquierda.

Haga clic en el botón **Resetear** para restablecer los valores de configuración de toda la aplicación que ajustó mediante el menú **Configuración** a sus valores predeterminados.

Configuración de las funciones de seguridad

Descripción general

Las prácticas recomendadas y las soluciones de ciberseguridad evolucionan constantemente, en función de la información más reciente disponible. Como criterio de diseño, Schneider Electric incorpora conocimientos y técnicas actualizados para contribuir a que los productos sean más resilientes ante los ciberataques. El enfoque de seguridad por diseño incluye la implementación de mecanismos para mitigar las amenazas, reducir las vulnerabilidades explotables y protegerse ante filtraciones de datos y ciberataques evitables.

NOTA:

Para mantener los productos de Schneider Electric seguros y protegidos, es conveniente que implemente las prácticas recomendadas de ciberseguridad que se indican en el documento *Prácticas recomendadas de ciberseguridad*, incluido en el Schneider Electric website.

Debido al rápido aumento del número de redes de equipos y plantas, las amenazas potenciales también aumentan rápidamente. Por lo tanto, tenga muy en cuenta todas las posibles medidas de seguridad.

Las medidas de seguridad son necesarias para contribuir a proteger los datos y los canales de comunicación frente al acceso no autorizado.

NOTA: Antes de configurar las funciones de seguridad, consulte a su administrador de seguridad para que le ayude a asegurarse de que está utilizando la configuración de seguridad correcta.

Características de seguridad

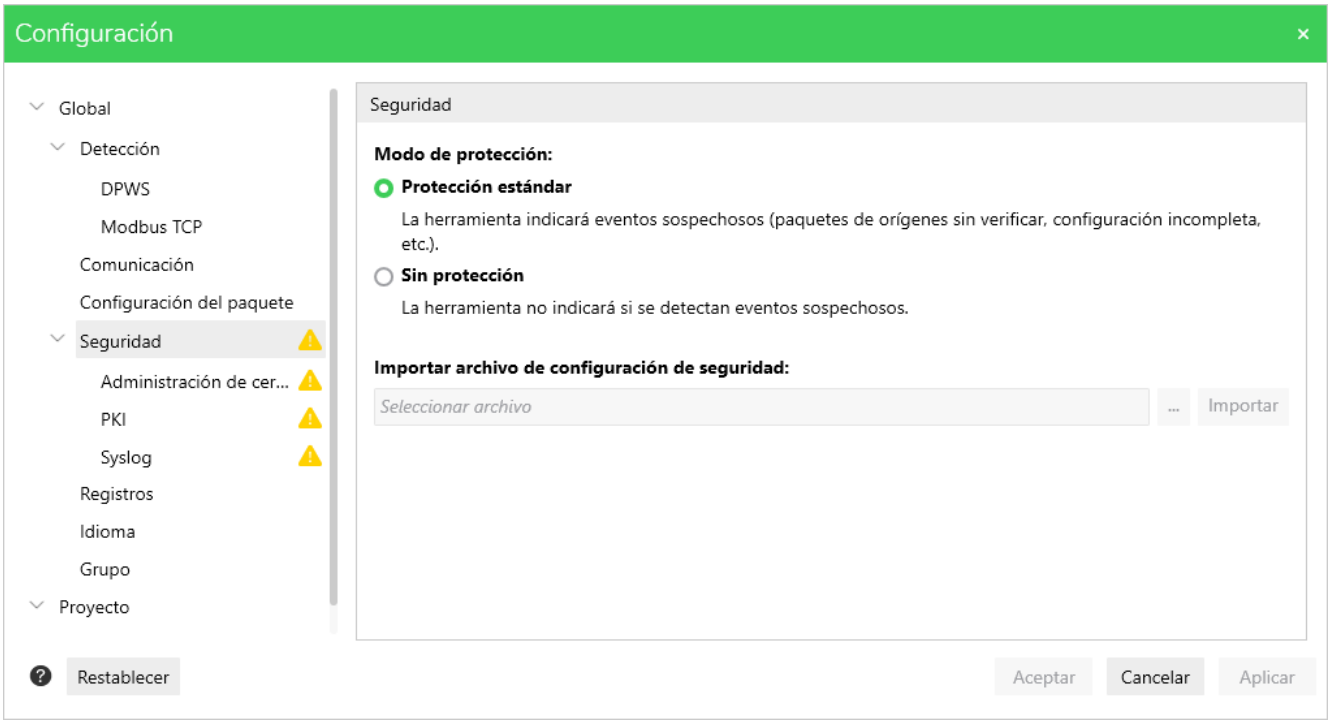
Descripción general

EcoStruxure Automation Device Maintenance admite las siguientes funciones de seguridad:

- Comunicación cifrada mediante certificados digitales en una infraestructura de clave pública (PKI).
- Gestión de paquetes de datos seguros (SEDPS) de Schneider Electric con firma digital.
- Protocolo de red Syslog.

Activación/desactivación del modo de protección

Si trabaja en una red protegida y no utiliza funciones de seguridad, las notificaciones relativas a las funciones de seguridad (por ejemplo, los signos de exclamación amarillos) se pueden deshabilitar mediante la opción **Seguridad** de la página **Configuración**.



Paso	Acción
1	Haga clic en el menú **Configuración** de la parte superior central de la página **Inicio**.
2	Seleccione la opción **Seguridad**.
3	Seleccione la opción para activar el modo de protección y para mostrar notificaciones relativas a las funciones de seguridad.

Importación de un archivo de configuración de seguridad

EcoStruxure Automation Device Maintenance le permite importar los ajustes de configuración de seguridad que haya configurado globalmente para su red dentro de la aplicación de EcoStruxure Cybersecurity Admin Expert. Si esta configuración está disponible como archivo, importe el archivo de la siguiente manera:

Paso	Acción
1	Haga clic en el menú **Configuración** de la parte superior central de la página **Inicio**.
2	Seleccione la opción **Seguridad**.
3	En la sección **Importar archivo de configuración de seguridad**, haga clic en el botón **Importar** para desplazarse hasta el archivo de configuración de seguridad.
4	Haga clic en **Abrir** para importar los ajustes de configuración de seguridad del archivo.

Para actualizar el archivo de configuración de seguridad, utilice el **Centro de actualizaciones** como se describe en el capítulo Actualización del archivo de configuración de seguridad, página 71.

Gestión de certificados

Descripción general

Los certificados digitales son necesarios para la comunicación protegida mediante protocolos correspondientes (por ejemplo, HTTPS) en una infraestructura de clave pública (PKI).

En el contexto de TLS, los certificados pueden utilizarse para comprobar la identidad de los participantes en la comunicación. Los certificados se envían mientras se establece la conexión, lo que se conoce como protocolo de enlace de TLS. El envío del certificado es opcional para el cliente (en este caso, el certificado de aplicación de EcoStruxure Automation Device Maintenance), a menos que el servidor solicite el certificado de cliente. El servidor envía su certificado siempre. La conexión con el participante en la comunicación solo podrá establecerse si el resultado de la comprobación del certificado es positivo.

EcoStruxure Automation Device Maintenance admite los siguientes modos de confianza de certificados:

- Modo de confianza manual: Puede confiar o desconfiar manualmente de los certificados de los participantes de la comunicación protegida. El estado de confianza se gestiona en las fichas **Certificados de confianza** / **Certificados no de confianza** del cuadro de diálogo **Administración de certificados**, página 46.
- Modo de confianza de lista de permitidos: Puede importar una lista de permitidos con el archivo de configuración de seguridad, página 42. A continuación, EcoStruxure Automation Device Maintenance confiará en los certificados de esta lista automáticamente.
- Entidad de certificación (CA)/modo de confianza de inscripción: EcoStruxure Automation Device Maintenance confía automáticamente en los certificados inscritos con certificados de la CA que están disponibles en la carpeta **Entidades de certificación raíz de confianza** del **Almacén de certificados** de Windows.

Consideraciones sobre el uso de certificados

Tenga en cuenta lo siguiente cuando use certificados para proteger las comunicaciones:

- Es necesario administrar los certificados, pues tienen una validez limitada y, por lo tanto, deben actualizarse cada cierto tiempo. Tenga esto en cuenta respecto al ciclo de vida de su máquina o su control.
- La configuración de fecha y hora del equipo Windows se usa para comprobar si el certificado sigue siendo válido. Compruebe la configuración en intervalos regulares a través de Windows **Inicio > Configuración > Hora e idioma > Fecha y hora**.
- Si el equipo que ejecuta EcoStruxure Automation Device Maintenance está permanentemente desconectado, debe actualizar la **Lista de revocación de certificados** (CRL) manualmente en intervalos regulares. Para ello, conéctese a su punto de distribución de CRL, descargue la CRL más reciente e instálela en su PC.

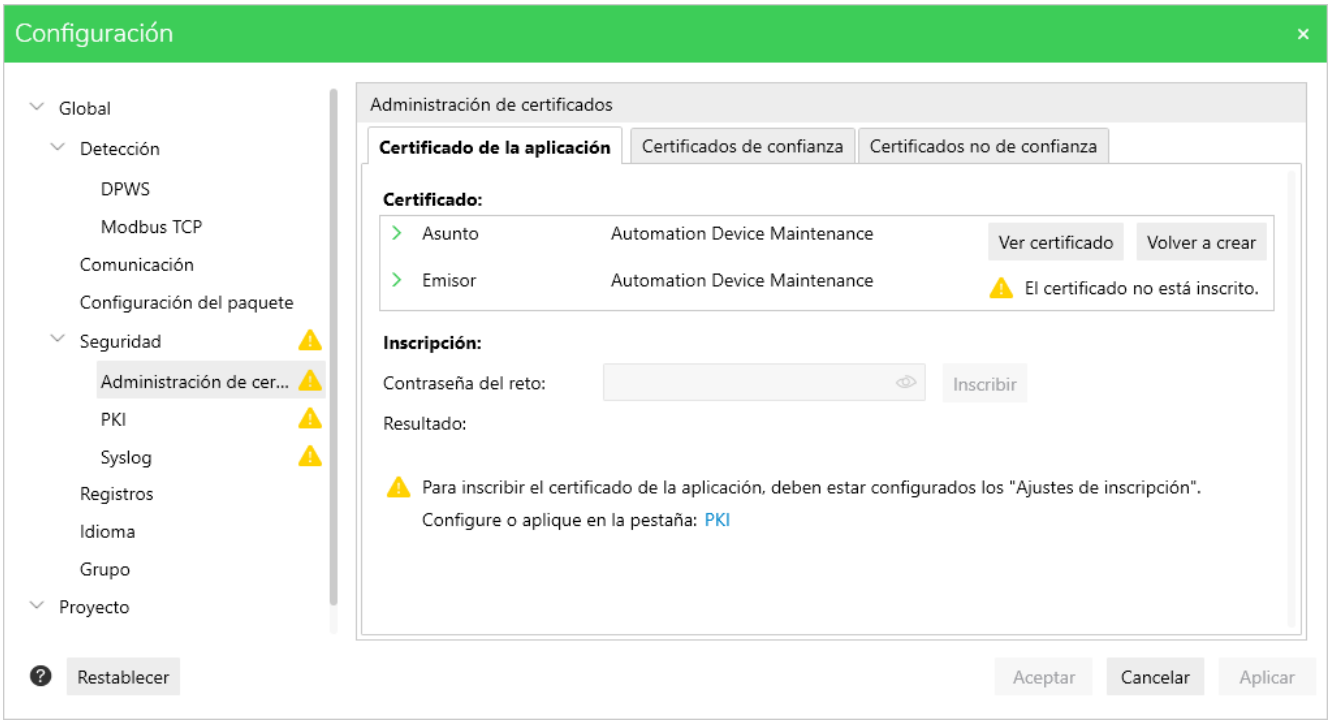
  Para obtener la dirección URL correcta del punto de distribución de CRL, consulte el administrador de seguridad.
- También puede declarar certificados como no de confianza en EcoStruxure Automation Device Maintenance, por ejemplo, a través del cuadro de diálogo **Gestión de certificados**, página 46.

Cuadro de diálogo Gestión de certificados

Tras la instalación inicial, se encuentra disponible un certificado de aplicación autofirmado predeterminado para EcoStruxure Automation Device Maintenance.

El cuadro de diálogo **Gestión de certificados** ofrece las siguientes opciones para el certificado de aplicación:

- Volver a crear el certificado de aplicación autofirmado y asignar propiedades individuales (consulte Volver a crear el certificado de aplicación autofirmado, página 44).
- Inscribir el certificado de aplicación para asignar una firma digital de una entidad de certificación (CA) y crear una cadena de confianza (consulte Inscripción del certificado de aplicación, página 45).
- Gestionar el estado de confianza de los certificados digitales de los socios de comunicación (consulte Gestión del estado de confianza de los certificados, página 46).



Volver a crear el certificado de aplicación autofirmado

Siga los pasos siguientes para volver a crear el certificado de aplicación predeterminado y asignar las propiedades individuales:

Paso	Acción
1	Haga clic en el menú **Configuración** de la parte superior central de la página **Inicio**.
2	Seleccione la opción **Seguridad > Gestión de certificados**.
3	En la ficha **Certificado de aplicación**, haga clic en el botón **Volver a crear**. **Resultado**: Se abrirá el cuadro de diálogo **Crear certificado**.
4	Escriba las propiedades que desee asignar al certificado y haga clic en el botón **Aceptar**. **Resultado**: El certificado autofirmado de EcoStruxure Automation Device Maintenance se presenta a otros participantes de la comunicación con las propiedades que ha definido.

Inscripción del certificado de aplicación

Para crear una cadena de confianza, el certificado de aplicación de EcoStruxure Automation Device Maintenance debe estar inscrito y firmado digitalmente por una entidad de certificación (CA).

Para inscribir el certificado, configure en primer lugar la **configuración de inscripción** tal y como se ofrece en la opción **Configuración** > **Seguridad** > **PKI**, página 48.

A continuación, siga los pasos siguientes para inscribir el certificado de aplicación de EcoStruxure Automation Device Maintenance:

Paso	Acción
1	Haga clic en el menú **Configuración** de la parte superior central de la página **Inicio**.
2	Seleccione la opción **Seguridad** > **Gestión de certificados**.
3	En la ficha **Certificado de aplicación**, compruebe que el certificado de la aplicación aún está autofirmado y todavía no está inscrito: • En la sección **Certificado**, tanto **Asunto** como **Emisor** muestran el mismo contenido: **Automation Device Maintenance**. • La notificación **El certificado no está inscrito** se muestra en la línea **Emisor**.
4	Escriba la contraseña de la CA en el cuadro de texto **Contraseña de comprobación**. Esta contraseña se utiliza para autorizar la solicitud de inscripción. Para obtener más información, consulte al administrador de redes industriales.
5	Haga clic en **Inscribir**. **Resultado**: EcoStruxure Automation Device Maintenance envía una solicitud de firma de certificado del certificado de la aplicación junto con la comprobación de contraseña a la CA. Si la contraseña no es correcta, se devolverá un mensaje de **Inscripción incorrecta**. **NOTA:** Este procedimiento sustituye el certificado de aplicación autofirmado predeterminado por un nuevo certificado firmado. No se puede deshacer la sustitución.
6	Verifique si el proceso se ha completado correctamente: • **Resultado:** En la ficha **Certificado de aplicación**, se mostrará **La inscripción se realizó correctamente**. • En la ficha **General** del cuadro de diálogo **Información del certificado**, la entrada **Emisor** ha cambiado al nombre de la CA, por ejemplo, *INT-DEV-SUB-CA*. • La ficha **ruta de certificación** del cuadro de diálogo **Información del certificado** indica la CA raíz y las CA subordinadas en una estructura jerárquica en función de la configuración de la PKI. El certificado de entidad final en la parte inferior de la estructura jerárquica es el certificado de EcoStruxure Automation Device Maintenance con las siguientes entradas: ◦ CN (Common Name) = Automation Device Maintenance ◦ O (Organization) = Schneider Electric

Gestión del estado de confianza de los certificados

Las fichas **Certificados de confianza** y **Certificados en los que no se confía** del cuadro de diálogo **Gestión de certificados** le permiten administrar el estado de confianza de los certificados disponibles en el EcoStruxure Automation Device Maintenance.

En ambas fichas, se muestra cada certificado con la siguiente información:

Componente	Descripción
Objeto	Proporciona información general sobre el certificado: • CN = Nombre común • OU = Unidad organizativa
Nombre del dispositivo	Proporciona el nombre del dispositivo tal y como se muestra en la **LISTA DE DISPOSITIVOS** de la ficha **Dispositivo/Carga**. Si el certificado no pertenece a un dispositivo, se muestra **n/a**.
Punto final de servicio	La información sobre el punto final de servicio se proporciona para los dispositivos que se utilizan en la sesión actual de EcoStruxure Automation Device Maintenance. Si el certificado no pertenece a un dispositivo, se muestra **n/a**.
Acción	Permite abrir el cuadro de diálogo **Información del certificado** a través del vínculo **Ver certificado**.
Estado de los certificados	Indica el estado del certificado: • **De confianza** • **No de confianza**

Puede realizar las siguientes acciones en los certificados:

- Para desconfiar de los certificados, seleccione uno o más certificados en la ficha **Certificados de confianza** y haga clic en el botón **No confiar**.
- Para confiar en los certificados, seleccione uno o más certificados en la ficha **Certificados no de confianza** y haga clic en el botón **Confiar**. Para confiar temporalmente en los certificados seleccionados, seleccione la opción **Confiar en esta sesión**.
- Para eliminar certificados, seleccione uno o más certificados en la ficha **Certificados de confianza** o **Certificados en los que no se confía** y haga clic en el botón **Eliminar**.

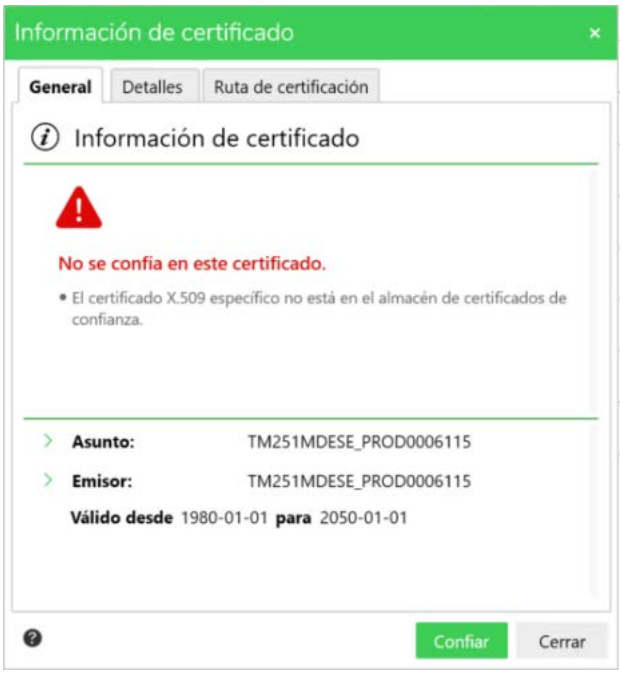
  NOTA: Los certificados de dispositivos que se están utilizando en la sesión actual de EcoStruxure Automation Device Maintenance no se pueden eliminar directamente. Los certificados se transfieren temporalmente a la lista de **Certificados en los que no se confía** y se quitarán cuando EcoStruxure Automation Device Maintenance se cierre.

  NOTA: Al ejecutar este comando, se quitan los certificados seleccionados del PC con Windows. También se quitarán del **Almacén de certificados** de Windows.

Gestión del estado de confianza de certificados en la ficha Dispositivo/Cargando

También puede confiar o desconfiar de los certificados de los dispositivos en la ficha **Dispositivo/Cargando**.

Siga estos pasos para confiar en el certificado del dispositivo en la ficha **Dispositivo/Cargando**:

Paso	Acción
1	Haga clic en el icono **Certificado del dispositivo** correspondiente al dispositivo.  **NOTA:** Puede establecer como de confianza el certificado del servidor temporalmente.
2	Seleccione la casilla de verificación para **Confiar en el certificado del dispositivo temporalmente durante la sesión actual**.
3	Haga clic en **Confiar en el certificado del dispositivo**.

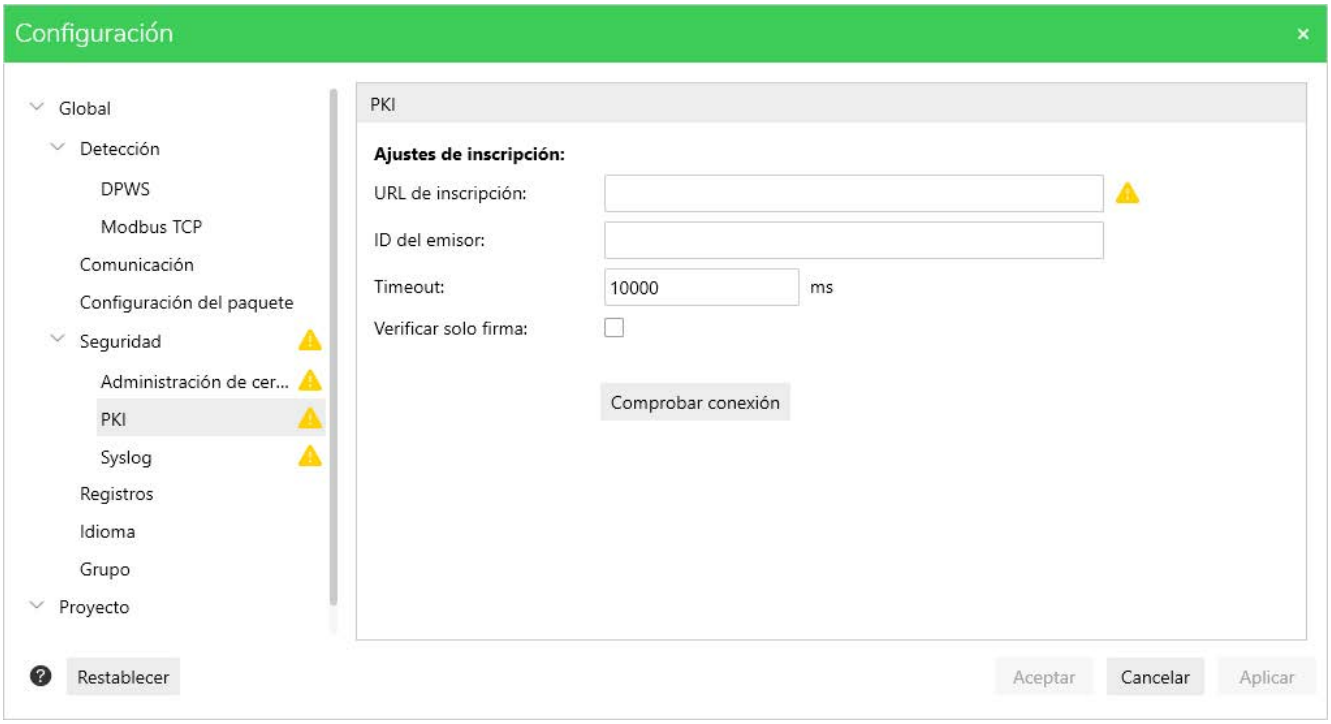
Siga estos pasos para dejar de confiar en el certificado del dispositivo en la ficha **Dispositivo/Cargando**:

Paso	Acción
1	Haga clic en el icono **Certificado del dispositivo** correspondiente al dispositivo.
2	Haga clic en **Revocar la confianza del certificado del dispositivo**.

Gestión de la infraestructura de clave pública (PKI)

Configuración para la inscripción del certificado de aplicación

Si la opción **Seguridad** está habilitada en el cuadro de diálogo **Seguridad** de la página **Configuración**, el cuadro de diálogo **PKI** le permite configurar la conexión con la entidad de certificación (CA) para inscribir el certificado de aplicación de EcoStruxure Automation Device Maintenance.



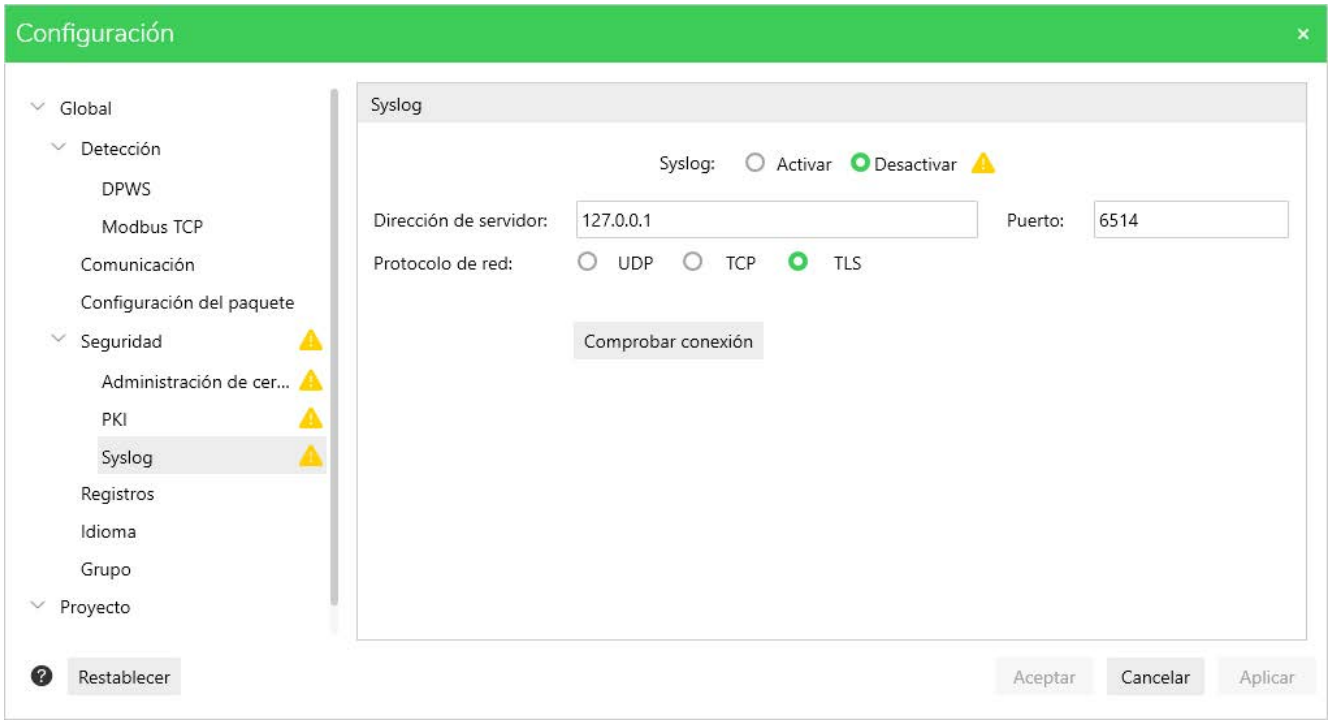
Componente	Descripción
URL de inscripción	Especifique el localizador de recursos uniforme (URL) de la entidad de certificación (CA) que emitirá el certificado.
ID del emisor	Especifique el identificador del emisor de su entidad de certificación.
Tiempo de espera	Introduzca un tiempo de espera (en milisegundos) que se corresponda con sus velocidades de transferencia de Internet. Valor predeterminado: 10.000 ms
Comprobar solo firma	Si esta opción no está seleccionada, el certificado de la CA debe estar disponible como certificado de confianza en el **Almacén de certificados**de Windows. Para comprobar solo las firmas digitales, seleccione esta opción.
Botón **Comprobar conexión**	Haga clic en el botón **Comprobar conexión** para establecer una conexión con el sitio web de la entidad de certificación (CA).
Botón **Ver certificado**	Una vez establecida correctamente la conexión con la CA, aparecerá el botón **Ver certificado**. Haga clic en el botón para abrir el cuadro de diálogo **Información del certificado** y compruebe los atributos del certificado para garantizar que está conectado a la CA correcta.

Si la conexión con el sitio web de la CA se ha establecido correctamente, seleccione la opción **Seguridad > Administración de certificados** y continúe con la inscripción del certificado de aplicación.

Activación del registro de mensajes de Syslog

Descripción general

El cuadro de diálogo de **Syslog** le permite activar la función de syslog y configurar EcoStruxure Automation Device Maintenance como cliente de syslog. EcoStruxure Automation Device Maintenance proporcionará un subconjunto de los mensajes de registro que genera al servidor syslog correspondiente mediante la configuración de syslog establecida en este cuadro de diálogo.



Activación del registro de mensajes de Syslog

Siga los pasos siguientes para activar la función de syslog y configurar la conexión con el servidor de syslog:

Paso	Acción
1	Haga clic en el menú **Configuración** de la parte superior central de la página **Inicio**.
2	Seleccione la opción **Seguridad** > **Syslog**.
3	Seleccione la opción **Habilitar** para activar la función de syslog.
4	En el cuadro de texto **Dirección del servidor**, introduzca la dirección IP de su servidor de syslog.
5	Ingrese el **puerto** que el servidor está supervisando para los mensajes de syslog de los clientes.
6	Seleccione la opción **Protocolo de red**: • **UDP** (Protocolo de datagrama de usuario) • **TCP** (Protocolo de control de transmisión) • **TLS** (Seguridad de la capa de transporte)
7	Para conexiones TCP o TLS, puede hacer clic de manera opcional en el botón **Comprobar conexión** para verificar la conexión con el servidor de syslog. **Resultados**: Para conexiones TCP: Aparece un mensaje que indica si se ha establecido una conexión con el servidor. Para conexiones TLS: • Aparece un mensaje que indica si se ha establecido una conexión con el servidor. • Un icono indica si el certificado del servidor de syslog ya está declarado como de confianza. Si el certificado no es de confianza, haga clic en el icono para abrir el cuadro de diálogo **Información del certificado** que le permite verificar el certificado y declararlo de confianza. **NOTA:** Como UDP se basa en un modelo de comunicación sin conexión, EcoStruxure Automation Device Maintenance no puede proporcionar una solución para verificar la conexión. Debe verificar manualmente si se reciben mensajes de syslog en el servidor que especificó.

Paquete de datos

Ficha Paquete de datos

Tipos de paquetes de datos compatibles

Se admiten los siguientes tipos de archivo:

- *.fwp
- *.ldx
- *.sedp
- *.sedps

Paquetes de datos protegidos

EcoStruxure Automation Device Maintenance admite paquetes de datos *.sedps (Schneider Electric Data Package Secure) que están firmados digitalmente: Cuando el modo de protección está habilitado, EcoStruxure Automation Device Maintenance verifica que se ha comprobado el origen del paquete y muestra notificaciones de seguridad si la firma no es correcta. Para obtener una descripción general de la gestión de certificados, consulte el capítulo Gestión de certificados, página 43.

Si se activa el modo de protección, página 42, se aplica lo siguiente:

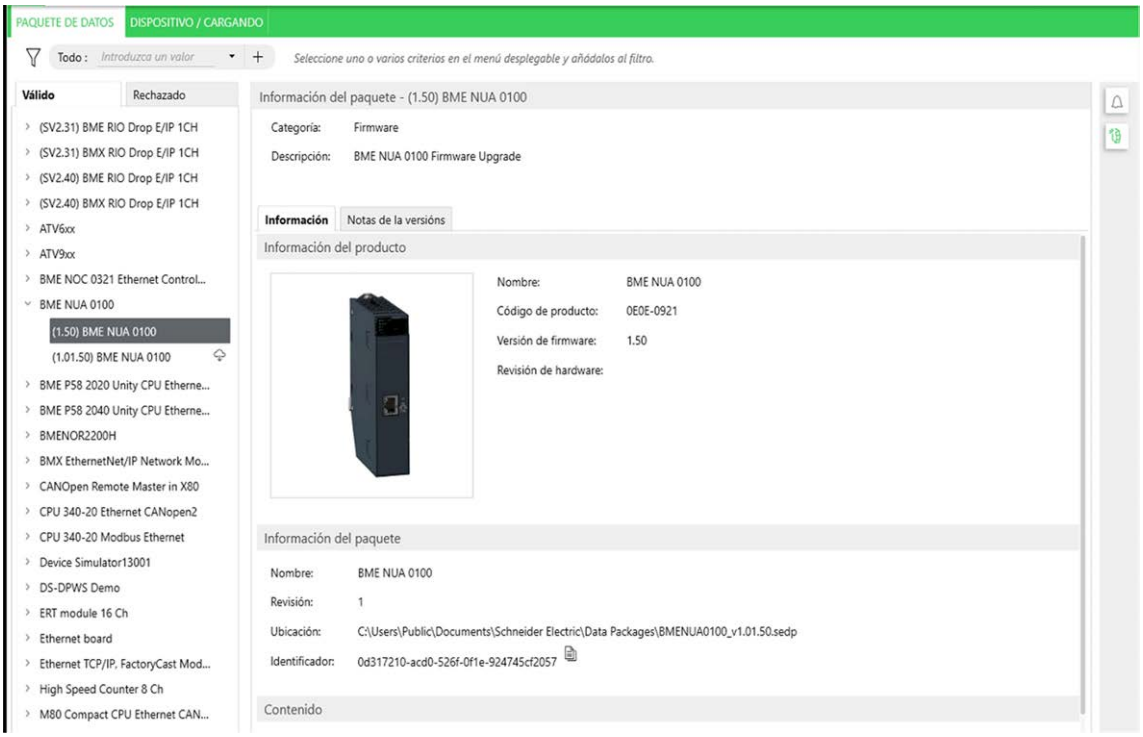
- Los siguientes archivos de paquete están marcados con el icono de notificación amarillo en la lista de paquetes de la ficha **Paquete de datos** y el mensaje **No se puede verificar la cadena de confianza del paquete** se muestra en el lado derecho:
  - Archivos de paquete sin firmar.
  - Archivos de paquete autofirmados.
  - Archivos de paquete que usan un certificado raíz que no es de confianza.
- Estos paquetes también se marcan en la ficha **Dispositivo/Carga** mediante el icono de notificación amarillo.
- Si intenta realizar un proceso de actualización del firmware con uno de estos paquetes de datos, el proceso se pone en pausa y se muestra el mensaje **No se puede verificar la cadena de confianza del paquete seleccionado. La descarga puede dañar el dispositivo. ¿Desea continuar?** en el área de notificaciones, página 67. Lea atentamente el mensaje y evalúe los riesgos. Después de confirmar el mensaje, el proceso continuará.
- Si intenta realizar un proceso de actualización del firmware con uno de estos paquetes de datos, los errores detectados se mostrarán en la ventana **Registros**, página 68.

AVISO
DISPOSITIVOS DAÑADOS Compruebe detenidamente si el paquete de datos procede de una fuente de confianza, dado que la descarga de un paquete de datos manipulado puede dañar el dispositivo. **Si no se siguen estas instrucciones, pueden producirse daños en el equipo.**

Descripción general de la ficha Paquete de datos

Puede visualizar el contenido de la biblioteca de paquetes de datos para localizar detalles de los paquetes individuales y el contenido.

En el lado izquierdo de la ficha se muestra la lista de paquetes de datos disponibles localmente agrupados por familia de dispositivos. En el lado derecho de la ficha se muestran los detalles del paquete seleccionado.



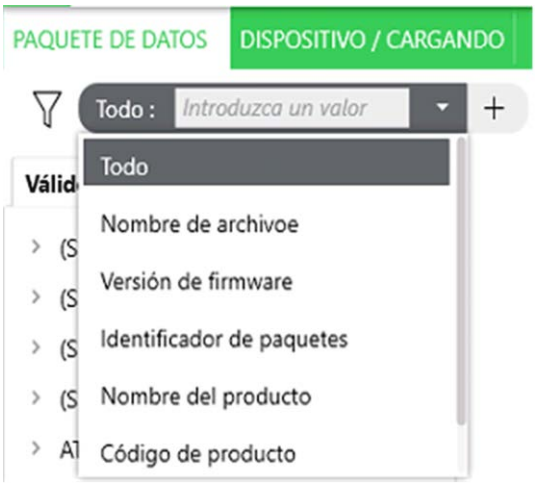
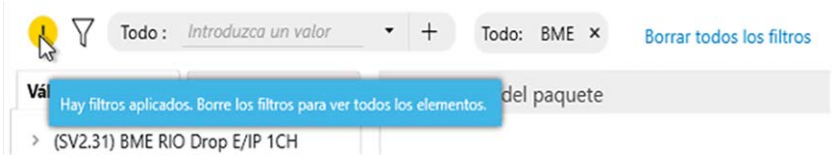
Lista de paquetes de datos

La lista de paquetes de datos de lado izquierdo se compone de dos fichas:

- En la ficha **Válido** se enumeran los paquetes de datos disponibles localmente en el PC agrupados por familia de dispositivos.
- En la ficha **Rechazado**, en cambio, se enumeran los paquetes de datos descargados en el PC que no se pueden procesar por algún motivo. Dado que el archivo del paquete de datos podría haberse dañado durante el proceso de descarga, puede resultar útil descargarlo nuevamente. Si, al hacerlo, no se resuelve el problema, póngase en contacto con su representante de Schneider Electric para obtener más ayuda.

Filtrado de la lista de paquetes de datos

Si desea reducir el número de paquetes de datos que se muestran en la lista, puede aplicar los siguientes criterios de búsqueda:

Paso	Acción
1	Introduzca una cadena en el campo de texto **Todo**. Para limitar la búsqueda a una propiedad específica del paquete de datos, puede también abrir la lista y seleccionar un criterio de búsqueda. 
2	Haga clic en el botón con el signo más del lado derecho de la lista de búsqueda para iniciar la búsqueda. **Resultado**: La lista de paquetes de datos muestra entradas que cumplen el criterio de búsqueda especificado. Se mostrará un icono amarillo a la izquierda del cuadro de búsqueda para indicar que se ha aplicado un filtro y que las entradas de la lista se han reducido por tanto a aquellos paquetes de datos que coinciden con el criterio de búsqueda. 
3	Repita los pasos 1 y 2 para definir otro filtro. Los filtros se combinan mediante AND. **Resultado**: La lista de paquetes de datos muestra entradas que cumplen ambos criterios de búsqueda.
4	Para borrar un filtro individual, haga clic en el botón de cruz correspondiente a dicho filtro. Si desea eliminar todos los filtros que ha definido, haga clic en el enlace **Borrar todos los filtros**. Se mostrará la lista completa de paquetes de datos.

Información del paquete

En la **Información del paquete** del lado derecho se proporciona información sobre el paquete de datos seleccionado de la lista de paquetes de datos.

En la parte superior se incluye la siguiente información:

- **Categoría**
- **Descripción**

En la ficha **Información** se muestran los siguientes detalles:

- Sección **Información del producto**:
  - Imagen (si está disponible en el paquete de datos)
  - **Name**
  - **Código de producto**
  - **Versión de firmware**
  - **Revisión de hardware**
- Sección **Información del paquete**:
  - **Name**
  - **Revisión**
  - **Ubicación**
  - **Identificador**: El botón **Copiar en el portapapeles** permite copiar la cadena identificadora en el portapapeles de su PC.
- Sección **Contenido**: Ofrece el contenido del paquete de datos de una lista.

En la ficha **Notas de la versión** se mostrará contenido siempre que el paquete de datos contenga un documento con la etiqueta `ReleaseNotes`. En caso contrario, la ficha se mostrará vacía.

Dispositivo/Cargando

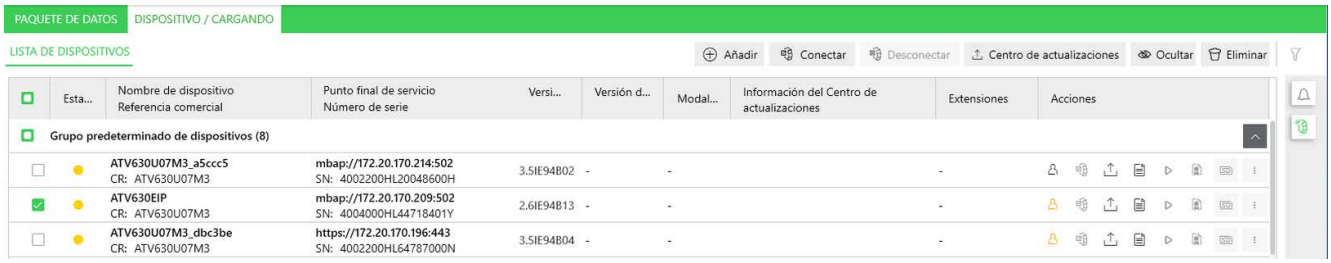
Ficha Dispositivo/Cargando

Descripción general

EcoStruxure Automation Device Maintenance muestra una serie de propiedades del dispositivo (como nombre del dispositivo, punto final de servicio, versión de firmware) en la ficha **Dispositivo/Cargando**.

NOTA: La información que se muestra en esta ficha solo se actualiza automáticamente si el modo de detección está configurado en **Automático**.

Haga clic en el icono de la barra de herramientas para mostrar los valores más recientes.



Para obtener información sobre los detalles mostrados para los dispositivos, consulte el capítulo Dispositivo/Cargando, página 21.

Detalles disponibles después de iniciar sesión

Una vez que haya iniciado sesión correctamente en un dispositivo y el estado del dispositivo haya cambiado a verde, haga clic en el botón para obtener acceso a los siguientes comandos para cada dispositivo:

Comando	Descripción
Óptica	El dispositivo emite una señal óptica que permite identificarlo en un bastidor de hardware para los modelos que admitan esta funcionalidad.
Óptica y acústica	El dispositivo emite una señal óptica y acústica que permite identificarlo en un bastidor de hardware para los modelos que admitan esta funcionalidad.
Propiedades	Abre otro cuadro de diálogo de **Propiedades** con información adicional sobre el dispositivo en diferentes fichas: • En la ficha **Información del dispositivo** se proporciona información general acerca del dispositivo: ◦ **ID del producto** ◦ **Nombre del producto** ◦ **Versión de firmware** ◦ **Revisión de hardware** ◦ **ID del hardware** ◦ **Dirección MAC** • En la ficha **Estado del dispositivo** se incluye información sobre el estado actual del dispositivo. • En la ficha **Configuración** se incluye información sobre los ajustes de configuración del dispositivo. Si el dispositivo lo admite, los ajustes de configuración pueden modificarse en esta ficha. **NOTA:** Las modificaciones de los ajustes de configuración pueden requerir un reinicio del dispositivo que puede provocar que el controlador se configure en el estado STOP. Los efectos se indican mediante mensajes que se muestran en el área de notificaciones. Lea atentamente cada mensaje y confirme que ha evaluado los riesgos. Después de confirmar cada mensaje, el proceso continuará. La información de **Propiedades** que se muestre dependerá del dispositivo en cuestión. Para obtener más información, consulte la documentación de usuario del dispositivo.

Agrupación de dispositivos en la LISTA DE DISPOSITIVOS

Descripción general

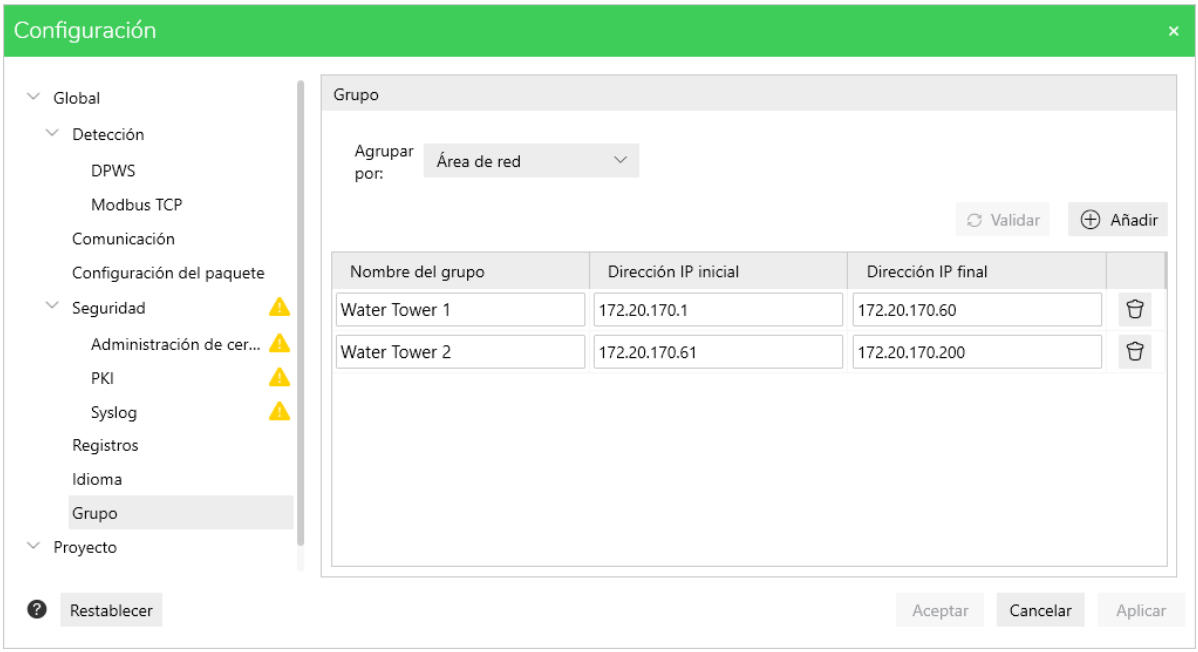
EcoStruxure Automation Device Maintenance permite estructurar los dispositivos mostrados en la **LISTA DE DISPOSITIVOS** mediante la creación de grupos.

EcoStruxure Automation Device Maintenance V3.0 permite la agrupación según las direcciones IP de los dispositivos mediante la definición de los rangos de direcciones IP. Se podrían agregar criterios de agrupación adicionales con versiones posteriores a EcoStruxure Automation Device Maintenance.

NOTA: Esta función de agrupación es exclusiva de las direcciones IPv4. El estándar IPv6 no es compatible con EcoStruxure Automation Device Maintenance V3.0.

Creación de grupos

Siga los pasos siguientes para agrupar dispositivos:

Paso	Acción
1	Seleccione la opción **Grupo** en la página **Configuración**.
2	Expanda la lista **Agrupar por** y seleccione la opción **Área de red**.
3	Haga clic en el botón **+ Añadir** para crear un nuevo rango de direcciones. **Resultado**: Se muestra una tabla con una línea vacía.
4	En la celda **Nombre de grupo** , introduzca un nombre para el grupo de dispositivos.
5	En la celda **Dirección IP inicial**, introduzca la primera dirección IP del rango de direcciones para su grupo de dispositivos.
6	En la celda **Dirección IP final**, escriba la última dirección IP del rango de direcciones para su grupo de dispositivos. 
7	Haga clic en el botón **+ Agregar** para crear otro grupo. O bien Haga clic en **Aplicar** para aplicar la configuración de **Grupo**. O bien Haga clic en **Aceptar** para aplicar todas las modificaciones de la configuración de la aplicación y para cerrar el cuadro de diálogo **Configuración**.

Eliminación de dispositivos

Descripción general

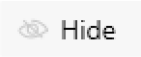
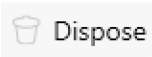
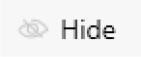
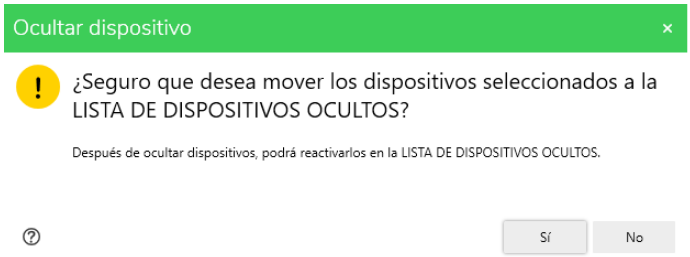
Puede eliminar los dispositivos ocultando temporalmente o descartándolos permanentemente en la ficha **Lista de dispositivos** del menú **Dispositivo/ Cargando**.

El dispositivo se puede eliminar a través de las siguientes acciones:

- Ocultación de un dispositivo activo
- Descarte de un dispositivo activo
- Descarte de un dispositivo oculto

Ocultación de un dispositivo activo

Siga los pasos siguientes para ocultar un dispositivo activo:

Paso	Acción
1	Haga clic en la ficha **Dispositivo/Cargando**. Los dispositivos activos detectados se listan en la ficha **Lista de dispositivos**.
2	En la ficha **Dispositivo/Cargando**: • seleccione un solo dispositivo haciendo clic en una celda de la fila del dispositivo. O • Seleccione varios dispositivos marcando las casillas de verificación que se encuentran a la izquierda de cada fila o seleccionando todo el **Grupo**.
3	Los iconos siguientes se activan para los dispositivos seleccionados: •  • 
4	Haga clic en el icono  . Se mostrará el mensaje **Ocultar dispositivo**. 
5	Haga clic en **Sí** para continuar. El dispositivo seleccionado se desplaza a la ficha **Lista de dispositivos ocultos**. **NOTA:** Puede reactivar los dispositivos ocultos desde **Lista de dispositivos ocultos**.

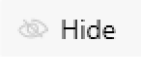
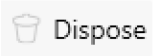
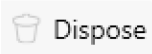
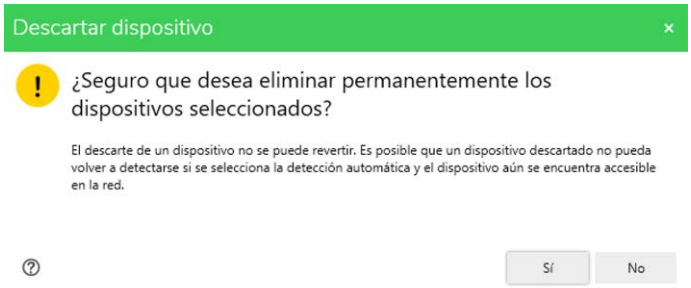
Visualización de un dispositivo oculto

Siga los pasos siguientes para visualizar un dispositivo oculto:

Paso	Acción
1	Haga clic en la ficha **Dispositivo/Cargando**. Los dispositivos ocultos se listan en la ficha **Lista de dispositivos ocultos**.
2	• seleccione un solo dispositivo haciendo clic en una celda de la fila del dispositivo. O • Seleccione varios dispositivos marcando las casillas de verificación que se encuentran a la izquierda de cada fila o seleccionando todo el **Grupo**.
3	Los iconos siguientes se activan para los dispositivos seleccionados: • Unhide • Dispose
4	Haga clic en el icono Unhide. El dispositivo seleccionado se desplaza a la ficha **Lista de dispositivos**.

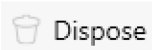
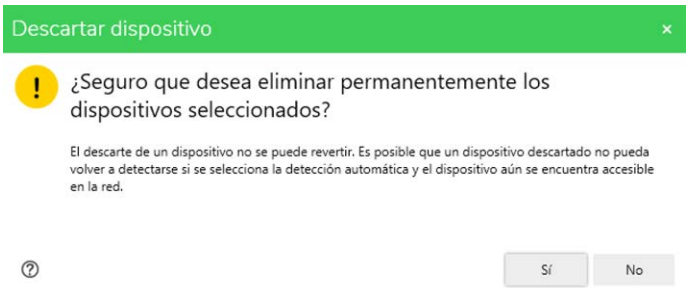
Descarte de un dispositivo activo

Siga los pasos siguientes para descartar un dispositivo activo:

Paso	Acción
1	Haga clic en la ficha **Dispositivo/Cargando**. Los dispositivos activos detectados se listan en la ficha **Lista de dispositivos**.
2	• seleccione un solo dispositivo haciendo clic en una celda de la fila del dispositivo. O • Seleccione varios dispositivos marcando las casillas de verificación que se encuentran a la izquierda de cada fila o seleccionando todo el **Grupo**.
3	Los iconos siguientes se activan para los dispositivos seleccionados: •  • 
4	Haga clic en el icono  . Se mostrará el mensaje **Descartar dispositivo**. 
5	Haga clic en **Sí** para continuar. **NOTA:** Al seleccionar **Sí**, se descarta permanentemente el dispositivo de la herramienta y para volver a tener el dispositivo disponible en la herramienta debe llevarse a cabo una detección o volver a añadirlo manualmente.

Descarte de un dispositivo oculto

Siga los pasos siguientes para descartar un dispositivo oculto:

Paso	Acción
1	Haga clic en la ficha **Dispositivo/Cargando**. Los dispositivos ocultos se listan en la ficha **Lista de dispositivos ocultos**.
2	• seleccione un solo dispositivo haciendo clic en una celda de la fila del dispositivo. O • Seleccione varios dispositivos marcando las casillas de verificación que se encuentran a la izquierda de cada fila o seleccionando todo el **Grupo**.
3	Los iconos siguientes se activan para los dispositivos seleccionados: • • 
4	Haga clic en el icono . Se mostrará el mensaje **Descartar dispositivo**. 
5	Haga clic en **Sí** para continuar. **NOTA:** Al seleccionar **Sí**, se descartará el dispositivo permanentemente de la herramienta y no se podrá recuperar.

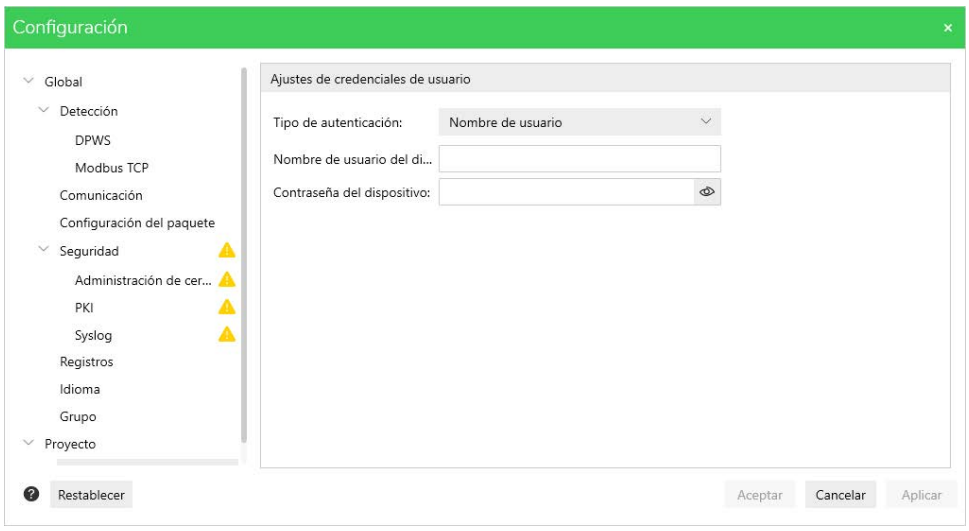
Administración de credenciales de usuario

Descripción general

EcoStruxure Automation Device Maintenance le permite especificar credenciales para el acceso autorizado a los dispositivos globalmente para el proyecto y de forma individual para cada dispositivo.

Administración global de credenciales de usuario

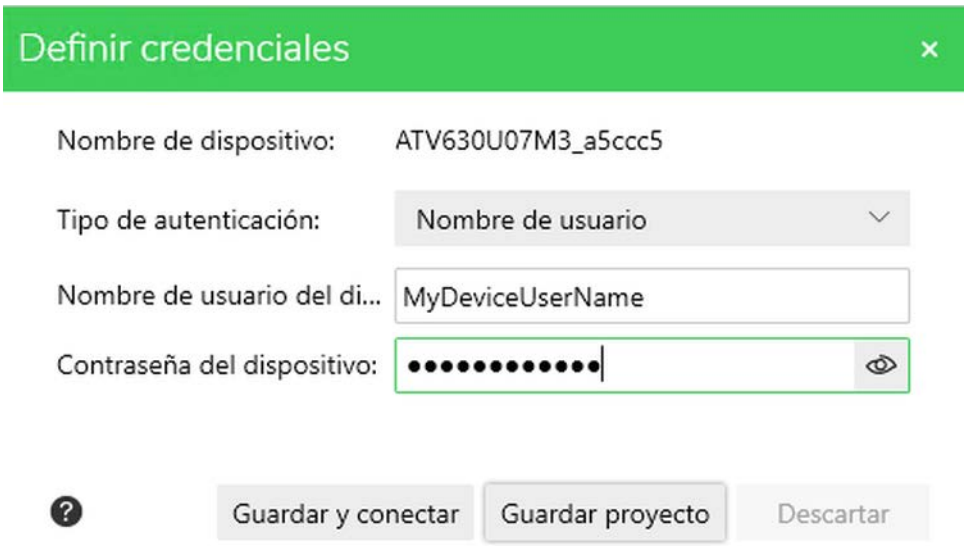
Para administrar las credenciales de usuario de manera global para el proyecto, vaya a la página **Configuración** y seleccione la opción **Proyecto > Ajustes de credenciales de usuario**.



Seleccione **Tipo de autenticación > Nombre de usuario** o **Tipo de autenticación > Personalizado** y especifique las credenciales según corresponda. Haga clic en **Aceptar** para guardar las credenciales. Al hacerlo, el icono **Definir credenciales** de los dispositivos correspondientes de la página **Dispositivo/Cargando** se establece en amarillo y puede hacer clic en el icono **Conectar** o en el botón Conectar para iniciar sesión sin volver a escribir las credenciales.

Administración de credenciales de usuario por dispositivo

Para administrar las credenciales de usuario de cada dispositivo por separado, abra la página **Dispositivo/Cargando** y haga clic en el icono **Definir credenciales** en la fila de dispositivos de la tabla:



Puede hacer clic en **Guardar y conectar** para guardar las credenciales y establecer una conexión con el dispositivo. Después de iniciar sesión correctamente, el icono **Definir credenciales** cambia a verde. Otra opción es hacer clic en **Guardar** para guardar las credenciales de este dispositivo para iniciar sesión más adelante. En este caso, el icono **Definir credenciales** cambia a color amarillo y puede hacer clic en el icono **Conectar** o en el botón Conectar para iniciar sesión sin volver a introducir las credenciales.

Parámetros de credencial de usuario

Los parámetros mostrados son específicos del dispositivo y solicitan las credenciales necesarias para iniciar sesión en el dispositivo en cuestión. Para obtener más información, consulte la documentación de usuario del dispositivo.

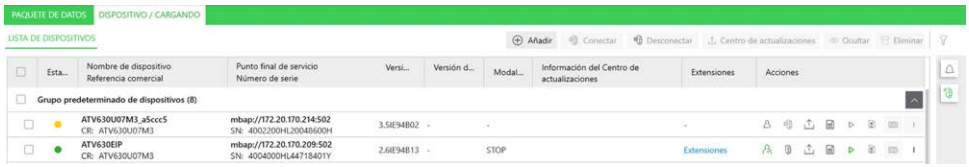
Para iniciar sesión en los controladores Modicon M340, Modicon M580 o Momentum, se requieren tres contraseñas. Para obtener más información sobre la contraseña de protección de la aplicación, la contraseña de almacenamiento de datos y la contraseña de protección del firmware, consulte los capítulos correspondientes del *EcoStruxure Control Expert Operating Modes* or the legacy *Unity Pro Operating Modes* manual. Los enlaces de descarga de las traducciones de este manual se proporcionan en la lista de documentos relacionados de esta ayuda en línea, página 10.

Acceso a extensiones

Descripción general

Un dispositivo modular de la **LISTA DE DISPOSITIVOS** de la ficha **Dispositivo/ Cargando** proporciona un enlace que permite acceder a las extensiones individuales del dispositivo.

Ejemplo de dispositivo modular:



Si es compatible con el dispositivo, el enlace **Extensiones** (Extensiones) abre una nueva ficha **Extensiones** y proporciona los dispositivos modulares agrupados por **Extensión**.

Ambas fichas proporcionan acceso al cuadro de diálogo **Centro de actualizaciones** (a través del icono **Centro de actualizaciones** o el botón **Centro de actualizaciones** Centro de actualizaciones) que le permite seleccionar el paquete de datos de firmware con el botón **Firmware**.

En el caso de los dispositivos que no pueden cargar las extensiones bajo demanda al hacer clic en el enlace **Extensiones**, siga el proceso descrito en la siguiente sección para acceder a extensiones individuales.

Acceso manual a extensiones

En el caso de los dispositivos que no pueden cargar las extensiones bajo demanda al hacer clic en el enlace **Extensiones**, proceda de la siguiente manera:

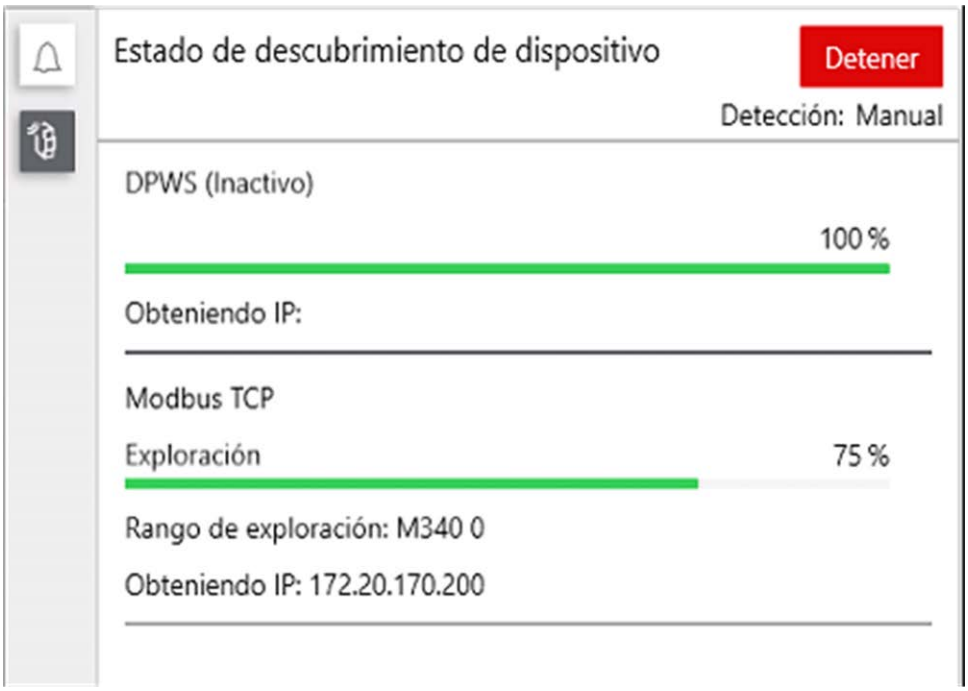
Paso	Acción
1	Haga clic en el enlace **Extensiones** del dispositivo modular. **Resultado**: Se abrirá la ficha **Extensiones**. Si el dispositivo no puede cargar las extensiones bajo demanda al hacer clic en el enlace **Extensiones**, se proporciona un botón **Agregar**.
2	Haga clic en el botón **Agregar** o en el enlace **No se encontró ningún módulo. Para agregar un módulo haga clic aquí**. **Resultado**: Se abrirá el cuadro de diálogo **Agregar módulo**.
3	En el cuadro de diálogo **Agregar módulo**, configure los parámetros para acceder a las extensiones del dispositivo: • Número de **Bastidor** • Número de **Ranura**
4	Haga clic en el botón **Aceptar** para iniciar la exploración de detección. Cuando se detecten correctamente las extensiones, aparecerá la ficha **Extensiones**.
5	Cierre la ficha **Extensiones**.

Supervisión del estado de detección de dispositivos

Descripción general

Siempre que se esté ejecutando el proceso de detección de dispositivos, puede recuperar el estado de este proceso al hacer clic en el botón de la ficha **Dispositivo/Carga**.

Se muestra la vista **Estado de descubrimiento de dispositivo** en el lado derecho:



Se muestra la siguiente información:

- Información del progreso de cada explorador.
- Si se han configurado diferentes rangos para un mismo explorador, la información de progreso se muestra de manera individual para cada rango (por ejemplo, para el explorador Modbus TCP, página 34).

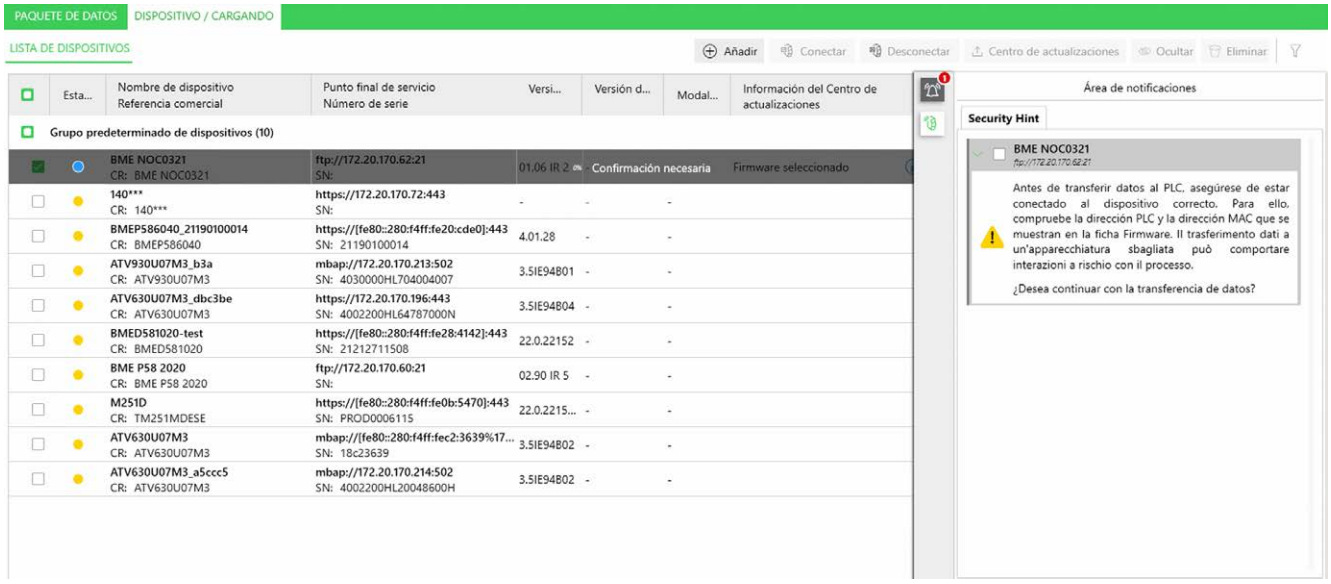
El botón **Iniciar**/**Detener** permite iniciar una detección manual de dispositivos o detener un proceso de detección de dispositivos en ejecución directamente desde esta vista.

Ver/confirmar mensajes

Descripción general

Algunos de los procesos que ejecuta EcoStruxure Automation Device Maintenance requieren interacción por parte del usuario. Cuando sea necesaria una confirmación, el proceso, como por ejemplo la actualización del firmware, se detiene y se muestra un mensaje en el área de notificaciones. Lea atentamente cada mensaje y confirme que ha evaluado los riesgos. Después de confirmar cada mensaje, el proceso continuará.

Para abrir el área de notificaciones, haga clic en el botón de la ficha **Dispositivo/Cargando**.



En el área de notificaciones se pueden mostrar dos tipos distintos de mensajes:

- Mensajes de confirmación: seleccione el mensaje marcando la casilla de verificación y haga clic en **Confirmar** para confirmar el mensaje y reanudar el proceso en ejecución, o haga clic en **Rechazar** para detener el proceso.
- Mensajes de notificación: seleccione el mensaje marcando la casilla de verificación y haga clic en **Aceptar** para confirmar el mensaje y reanudar el proceso en ejecución.

La opción **No mostrar notificaciones** permite deshabilitar la visualización de mensajes de notificación. Si se selecciona esta opción, los procesos se ejecutarán automáticamente sin interrupciones para aquellas interacciones de usuario que asuman que se confirman los mensajes.

NOTA: Active esta opción solo si está trabajando en el modo de mantenimiento y el operador ha comprobado el estado de seguridad de su máquina o del entorno del proceso.

Visualización de registros

Puede ver los registros almacenados y analizarlos para obtener información detallada sobre el dispositivo seleccionado.

La información del registro se puede visualizar en las secciones siguientes:

- Para cada dispositivo de la página **Dispositivo/Cargando**
- Para todo el proyecto en la ventana **Registros**

  NOTA: En la ventana **Registros** se muestran los errores detectados, las advertencias detectadas y los mensajes de información en una única ventana.

Para ver los registros exclusivos del dispositivo seleccionado, haga lo siguiente:

Paso	Acción
1	Acceda a la página **Dispositivo/Cargando**.
2	Haga clic en el icono **Registro del dispositivo** de un dispositivo. **Resultado**: Se abre directamente una pequeña vista de **Información de registro** en la tabla debajo de la fila del dispositivo. Utilice la barra de desplazamiento del lado derecho para ver todas las entradas de registro, si es necesario.

Para ocultar la **Información de registro** de un dispositivo, vuelva a hacer clic en el icono **Registro del dispositivo**.

Recomendación para mejorar la ciberseguridad

El archivo de registro suele contener datos sensibles tales como

- Direcciones de dispositivos
- Nombres de dispositivos
- Detalles de la tipología de red
- Detalles de la configuración de red

Se almacena en el disco duro del PC. Se elimina el archivo de registro en cuanto ya no es necesario o se almacena en un lugar seguro, en el que no es posible el acceso sin autorización.

Centro de actualizaciones

Descripción general

El cuadro de diálogo **Centro de actualizaciones** le permite configurar los ajustes para realizar una actualización del firmware o de un archivo de configuración de seguridad. Estos ajustes de configuración se pueden aplicar a un dispositivo concreto o a varios dispositivos simultáneamente.

- Para realizar actualizaciones en un dispositivo concreto, haga clic en el icono **Centro de actualizaciones** en la fila de dispositivo de la tabla de la ficha **Dispositivo/Cargando**.
- Para realizar actualizaciones de diferentes dispositivos del proyecto simultáneamente, seleccione los dispositivos en la ficha **Dispositivo/Cargando** y haga clic en el botón **Centro de actualizaciones** Centro de actualizaciones de la barra de botones.

Cuadro de diálogo Centro de actualizaciones

Ambas operaciones abren el cuadro de diálogo **Centro de actualizaciones**, que permite seleccionar:

- **Firmware**: permite configurar los ajustes para actualizar el firmware del dispositivo o dispositivos seleccionados. Para obtener más información, consulte Actualización del firmware, página 69.
- **Seguridad**: permite configurar los ajustes para actualizar el archivo de configuración de seguridad del dispositivo o dispositivos seleccionados. Para obtener más información, consulte Actualización del archivo de configuración de seguridad, página 71.
- **Restablecer**: permite restablecer la configuración de actualización del dispositivo o dispositivos seleccionados.

Para confirmar los ajustes y cerrar el cuadro de diálogo **Centro de actualizaciones**, haga clic en el botón **Guardar**. Como resultado, la configuración que ha establecido se indica en las celdas **Información del centro de actualizaciones** del dispositivo o dispositivos en la ficha **Dispositivo/Cargando** , página 21.

Para ejecutar el proceso de actualización según se haya configurado, haga clic en el botón **Actualizar**.

Actualización del firmware

Descripción general

EcoStruxure Automation Device Maintenance le permite actualizar el firmware de los dispositivos que se muestran en la ficha **Dispositivo/Cargando**.

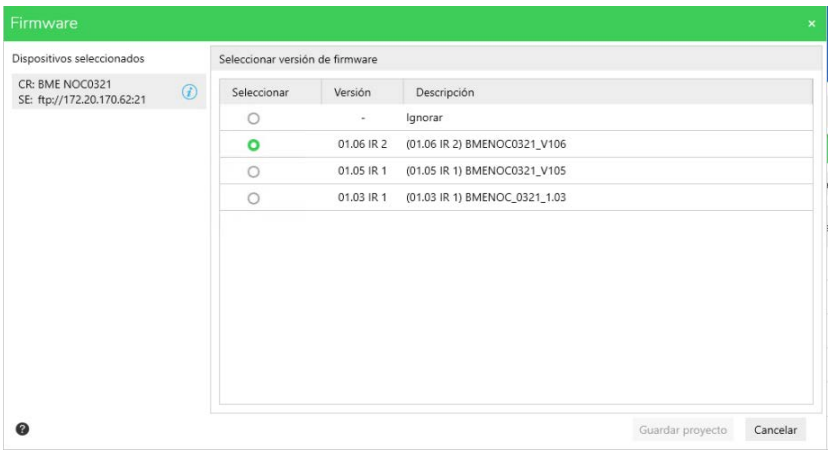
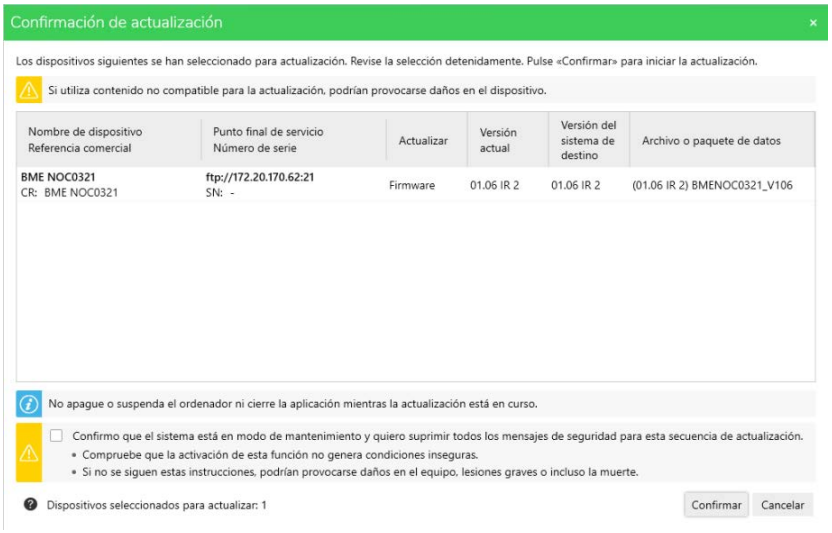
Para actualizar el firmware de los dispositivos modulares, puede acceder a las extensiones individuales tal y como se describe en el capítulo Acceso a extensiones, página 64.

Puede seleccionar paquetes de datos para varias extensiones módulos de bastidor. EcoStruxure Automation Device Maintenance actualizará de manera simultánea el firmware de esos dispositivos.

> **NOTA:** Si realiza una actualización simultánea del controlador y los módulos, asegúrese de que no reiniciar el controlador mientras está en marcha la actualización de los módulos. Vea a continuación un mensaje importante de peligro.

Actualización del firmware

Ejecute los siguientes pasos para actualizar el firmware:

Paso	Acción
1	Acceda a la página **Dispositivo/Cargando**.
2a	Para realizar actualizaciones en un dispositivo concreto, haga clic en el icono del **Centro de actualizaciones** en la fila del dispositivo.
2b	Para realizar actualizaciones de varios dispositivos del proyecto de forma simultánea, marque las casillas de verificación de los dispositivos o marque la casilla de verificación de todo el **Grupo** y haga clic en el botón **Centro de actualizaciones** Centro de actualizaciones de la barra de botones.
3	En el cuadro de diálogo **Centro de actualizaciones**, haga clic en el botón **Firmware**.
4	En el cuadro de diálogo **Firmware**, seleccione el paquete de datos de firmware de cada dispositivo. 
5	Haga clic en **Guardar** para guardar la configuración de actualización de firmware y cerrar el cuadro de diálogo **Firmware**. **Resultado**: La celda o celdas **Información del centro de actualizaciones** del dispositivo o dispositivos de la ficha Dispositivo/Cargando, página 21 muestra el texto **Firmware seleccionado**.
6	Haga clic en el botón **Actualizar** de la ficha **Dispositivo/Cargando** para iniciar el proceso de actualización. **Resultado**: Aparecerá el cuadro de diálogo **Confirmación de actualización**. 
7	En el cuadro de diálogo **Confirmación de actualización**, revise cuidadosamente la lista de dispositivos seleccionados para la actualización y verifique los ajustes que ha realizado.

Paso	Acción
8	Haga clic en el botón **Confirmar** para iniciar el proceso de actualización. **Resultado**: Se inicia el proceso de actualización del firmware. Cuando sea necesaria la interacción por parte del usuario, el proceso se detendrá y se mostrará un mensaje en el área de notificaciones, página 67. Lea atentamente cada mensaje y confirme que ha evaluado los riesgos. Después de confirmar cada mensaje, el proceso continuará.
9	Una vez que el proceso de firmware se haya completado correctamente, haga clic en el botón **Resumen**, página 19 de la parte inferior de EcoStruxure Automation Device Maintenance para mostrar el cuadro de diálogo **Resumen de actualización**. Contiene información sobre el estado de actualización de cada dispositivo, indicando la versión anterior y de destino, así como el paquete/archivo de datos.

AVISO

DISPOSITIVOS DAÑADOS

No apague el PC ni cierre la aplicación y asegúrese de que el PC no entra en modo de suspensión mientras se ejecuta el proceso de actualización del firmware, dado que la interrupción del proceso puede dañar el dispositivo.

Si no se siguen estas instrucciones, pueden producirse daños en el equipo.

Si lo desea, puede marcar la casilla de verificación **Confirmo que el sistema está en modo de mantenimiento y quiero suprimir todos los mensajes de seguridad para esta secuencia de actualización.** Esto ayuda a evitar que el proceso se detenga.

NOTA: Active esta opción solo si está trabajando en el modo de mantenimiento y el operador ha comprobado el estado de seguridad de su máquina o del entorno del proceso.

Una vez que el proceso de firmware se haya completado correctamente, para los controladores puede hacer clic en el icono **Iniciar dispositivo** en la ficha **Dispositivo/Cargando**, página 21 para iniciar el dispositivo.

NOTA: Realice una prueba de puesta en marcha antes de usar el equipo de control eléctrico y automatización para operaciones normales después de la instalación o actualización. Para obtener más información, consulte Iniciar y probar, página 7.

Actualización del archivo de configuración de seguridad

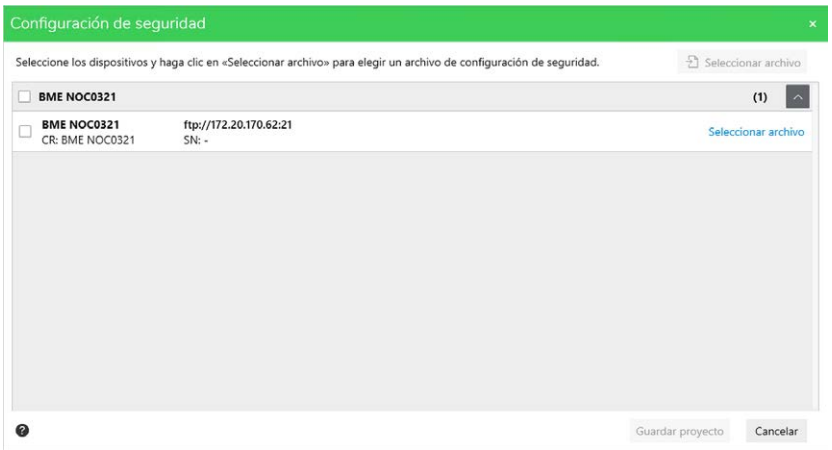
Descripción general

EcoStruxure Automation Device Maintenance le permite actualizar el archivo de configuración de seguridad que contiene los ajustes de configuración de seguridad que ha configurado globalmente para su red dentro de la aplicación EcoStruxure Cybersecurity Admin Expert.

NOTA: El nuevo archivo de configuración de seguridad puede asignar nuevas credenciales al dispositivo o dispositivos. Para los próximos inicios de sesión, se solicitarán las nuevas credenciales.

Actualización del archivo de configuración de seguridad

Para actualizar el archivo de configuración de seguridad, siga los pasos que se describen a continuación.

Paso	Acción
1	Acceda a la página **Dispositivo/Cargando**.
2a	Para realizar actualizaciones en un dispositivo concreto, haga clic en el icono del **Centro de actualizaciones** en la fila del dispositivo.
2b	Para realizar actualizaciones de varios dispositivos del proyecto de forma simultánea, marque las casillas de verificación de los dispositivos o marque la casilla de verificación de todo el **Grupo** y haga clic en el botón **Centro de actualizaciones** Centro de actualizaciones de la barra de botones.
3	En el cuadro de diálogo **Centro de actualizaciones**, haga clic en el botón **Seguridad**.
4	En el cuadro de diálogo **Configuración de seguridad**, seleccione un dispositivo concreto y haga clic en el enlace **Seleccionar archivo** para este dispositivo o seleccione varios dispositivos y haga clic en el botón **Seleccionar archivo** de la parte superior del cuadro de diálogo.  **Resultado**: Se muestra un cuadro de diálogo de apertura de archivo de Windows que permite buscar el archivo de configuración de seguridad en la red.
5	Seleccione el archivo de configuración de seguridad y haga clic en el botón **Abrir**. **Resultado**: El cuadro de diálogo **Configuración de seguridad** muestra los dispositivos con los archivos seleccionados.
6	Haga clic en el botón **Guardar** para guardar la configuración y cerrar el cuadro de diálogo **Configuración de seguridad**. **Resultado**: La celda o celdas de **Información del Centro de actualizaciones** del dispositivo o dispositivos de la ficha **Dispositivo/Cargando**, página 21 muestran el texto **Configuración de seguridad seleccionada**.
7	Haga clic en el botón **Actualizar** de la ficha **Dispositivo/Cargando** para iniciar el proceso de actualización. **Resultado**: Aparecerá el cuadro de diálogo **Confirmación de actualización**.
8	En el cuadro de diálogo **Confirmación de actualización**, revise cuidadosamente la lista de dispositivos seleccionados para la actualización y verifique los ajustes que ha realizado.
9	Haga clic en el botón **Confirmar** para iniciar el proceso de actualización. **Resultado**: Se inicia el proceso de actualización. Cuando sea necesaria la interacción por parte del usuario, el proceso se detendrá y se mostrará un mensaje en el área de notificaciones, página 67. Lea atentamente cada mensaje y confirme que ha evaluado los riesgos. Después de confirmar cada mensaje, el proceso continuará.

AVISO

DISPOSITIVOS DAÑADOS

No apague el PC ni cierre la aplicación y asegúrese de que el PC no entra en modo de suspensión mientras se ejecuta el proceso de actualización del firmware, dado que la interrupción del proceso puede dañar el dispositivo.

Si no se siguen estas instrucciones, pueden producirse daños en el equipo.

Si lo desea, puede marcar la casilla de verificación **Confirmo que el sistema está en modo de mantenimiento y quiero suprimir todos los mensajes de seguridad para esta secuencia de actualización.** Esto ayuda a evitar que el proceso se detenga.

NOTA: Active esta opción solo si está trabajando en el modo de mantenimiento y el operador ha comprobado el estado de seguridad de su máquina o del entorno del proceso.

Ciberseguridad

Introducción

La ciberseguridad es una rama de la administración de redes que se ocupa de los ataques en o desde sistemas informáticos que pueden causar interrupciones accidentales o intencionadas. El objetivo de la ciberseguridad es contribuir a aumentar los niveles de protección de la información y los activos físicos ante el robo, la corrupción, el uso inapropiado o los accidentes, al tiempo que se mantiene el acceso para sus usuarios previstos.

No existe ningún método único de ciberseguridad que resulte adecuado. Schneider Electric recomienda un método de defensa exhaustivo. Concebido por la National Security Agency (NSA), este método protege la red en varias capas con funciones de seguridad, dispositivos y procesos. Los componentes básicos de este método son:

- evaluación del riesgo
- un plan de seguridad elaborado según los resultados de la evaluación de riesgo
- una campaña de formación en varias fases
- separación física de las redes industriales y las redes de empresa utilizadas en una zona desmilitarizada (DMZ) y rutas de acceso para establecer otras zonas de seguridad
- control de acceso al sistema
- endurecimiento del dispositivo
- seguimiento y mantenimiento de la red

En este capítulo se definen los elementos que le ayudan a configurar un sistema menos susceptible a sufrir ciberataques. Para obtener información detallada sobre el enfoque de defensa en profundidad, consulte la *nota técnica del sistema*: *¿Cómo puedo... Reduzca la vulnerabilidad a los ciberataques* en el sitio webSchneider Electric website.

¿Qué es la ciberseguridad?

Descripción general

Las ciberamenazas son acciones deliberadas o accidentes que pueden interrumpir el funcionamiento normal de redes y sistemas informáticos. Estas acciones pueden iniciarse desde dentro del sitio físico o desde una localización externa. Los desafíos a la seguridad para el entorno de control incluyen:

- diversos límites físicos y lógicos
- múltiples sitios y grandes áreas geográficas
- efectos adversos de la implementación de seguridad en la disponibilidad de procesos
- mayor exposición a gusanos y virus al migrar de los sistemas empresariales a los sistemas de control, a medida que las comunicaciones de control empresarial se vuelven más abiertas
- mayor exposición a software malintencionado desde dispositivos USB, ordenadores portátiles de proveedores y servicio técnico, y red empresarial
- impacto directo de los sistemas de control en sistemas mecánicos y físicos

Fuentes de ciberataques

Implemente un plan de ciberseguridad que pueda contrarrestar varias fuentes potenciales de ciberataques e incidentes, incluyendo:

Origen	Descripción
interno	• comportamiento inapropiado del empleado o contratista • empleado o contratista insatisfecho
oportunista externo (no dirigido)	• script kiddies* • hackers aficionados • programadores de virus
deliberado externo (dirigido)	• grupos criminales • activistas • terroristas • agencias de estados extranjeros
accidental	
* término anglófono en jerga para designar a hackers que utilizan scripts malintencionados programados por otros sin poseer un conocimiento exhaustivo de su funcionamiento o su impacto potencial en un sistema.	

Un ciberataque deliberado sobre un sistema de control puede ser ejecutado para conseguir una serie de resultados maliciosos, entre ellos:

- perturbar el proceso productivo bloqueando o retrasando el flujo de información.
- dañar, deshabilitar o apagar el equipo para que la producción tenga un impacto negativo en el entorno
- modificar o deshabilitar los sistemas de seguridad para causar un daño intencionado

¿Cómo consiguen acceder los atacantes?

Un ciberatacante elude las defensas del perímetro para obtener acceso a la red del sistema de control. Los puntos de acceso comunes incluyen:

- acceso de marcación a los dispositivos de la unidad de terminal remoto (RTU)
- puntos de acceso del proveedor (como los puntos de acceso del soporte técnico)
- productos de red controlados informáticamente
- red privada virtual de empresa (VPN)
- vínculos de la base de datos
- cortafuegos mal configurados
- servicios compartidos

Certificaciones de ciberseguridad

Schneider Electric ha desarrollado unas directrices de ciberseguridad según las siguientes recomendaciones:

- Achilles
- ISA Secure

Para preguntas, noticias o informar sobre problemas de vulnerabilidad

Para enviar una pregunta sobre ciberseguridad, recibir las últimas noticias de Schneider Electric o informar sobre problemas de vulnerabilidad, visite nuestro website.

Directrices de Schneider Electric

Introducción

El sistema de su PC puede ejecutar varias aplicaciones para mejorar la seguridad en su entorno de control. El sistema viene con una configuración predeterminada de fábrica que debe reconfigurarse para que coincida con la recomendación de Schneider Electric de emplear un método de defensa exhaustivo para el endurecimiento de los dispositivos.

En las siguientes directrices se describen procedimientos llevados a cabo en un sistema operativo Windows. Solamente se recogen a modo de ejemplo. Su sistema operativo y aplicación podrían necesitar procedimientos o requisitos diferentes.

Proteger estaciones de trabajo de ingeniería

Los clientes pueden elegir entre distintos sistemas informáticos disponibles en el mercado para satisfacer las necesidades de su estación de trabajo de ingeniería. Entre las técnicas clave para proteger los sistemas se incluyen:

- Gestión de una contraseña sólida.
- Gestión de cuentas de usuario.
- Métodos de privilegios mínimos aplicados a aplicaciones y cuentas de usuario.
- Eliminación o deshabilitación de servicios sin usar.
- Eliminación de privilegios de gestión remota.
- Gestión sistemática de parches.

Deshabilitar tarjetas de interfaz de red no utilizadas

Verifique que las tarjetas de interfaz de red que no necesite la aplicación estén deshabilitadas. Por ejemplo, si su sistema tiene 2 tarjetas y la aplicación utiliza solo una, verifique que la otra tarjeta de red (conexión de área local 2) está deshabilitada.

Para deshabilitar una tarjeta de red en Windows:

Paso	Acción
1	Abra **Panel de control** > **Redes e Internet** > **Centro de redes y recursos compartidos** > **Cambiar configuración del adaptador**.
2	Haga clic con el botón derecho en la conexión no utilizada. Seleccione **Deshabilitar**.

Configuración de la conexión de área local

Varias configuraciones de red de Windows proporcionan una mayor seguridad de acuerdo con el método de defensa exhaustivo que recomienda Schneider Electric.

En los sistemas Windows, acceda a estos ajustes abriendo **Panel de control > Redes e Internet > Centro de redes y recursos compartidos > Cambiar configuración del adaptador > Conexión de área local (x).**

Esta lista es un ejemplo de los cambios en la configuración que podría realizar en su sistema en la pantalla **Propiedades de conexión de área local**:

- Deshabilite todas las pilas IPv6 en sus respectivas tarjetas de red. (Este ejemplo de sistema no requiere el rango de direcciones de IPv6, y si se deshabilitan las pilas IPV6 se limita la vulnerabilidad a los posibles riesgos de seguridad para el IPv6).
- Deshabilite **Uso compartido de archivos e impresoras para la red de Microsoft**.

Las recomendaciones de Schneider Electric para una defensa exhaustiva incluyen:

- Definir solo direcciones IPv4, máscaras de subred y pasarelas estáticas.
- No utilice DHCP ni DNS en la sala de control.

Gestión del Firewall de Windows

Las recomendaciones del enfoque de defensa en profundidad de Schneider Electric incluyen habilitar el firewall del host de Windows en todos los PC del sistema. Habilite los firewalls para cualquier perfil público o privado de la lista.

Se recomienda que el usuario defina las reglas de cortafuegos que rechacen las conexiones desde o hacia cualquier host externo desconocido/no seguro.

Deshabilitar el protocolo de escritorio remoto

Entre las recomendaciones de método de defensa en profundidad de Schneider Electric se incluye deshabilitar el protocolo de escritorio remoto (RDP), a menos que su aplicación requiera el RDP.

Lleve a cabo los siguientes pasos para deshabilitar el protocolo para sistemas con Windows 10:

Paso	Acción
1	Haga clic con el botón derecho en el botón **Inicio** de Windows y ejecute el comando **Sistema**.
2	En el menú **Configuración**, ejecute el comando **Escritorio remoto**.
3	En la vista **Escritorio remoto**, desactive **Habilitar escritorio remoto** (cambiar a **Off**).

Para otros sistemas operativos de Windows, lleve a cabo procedimientos equivalentes.

Actualizar las directivas de seguridad

Actualice las directivas de seguridad de los PC en su sistema escribiendo `gpupdate` en una ventana de comando. Para obtener más información, consulte la documentación de Microsoft sobre `gpupdate`.

Deshabilitar LANMAN y NTLM

El protocolo Microsoft LAN Manager (LANMAN o LM) y su sucesor NT LAN Manager (NTLM) presentan vulnerabilidades que hacen desaconsejable su uso en aplicaciones de control.

Los pasos siguientes describen cómo inhabilitar LM y NTLM en un sistema Windows:

Paso	Acción
1	En una ventana de comandos, ejecute `secpol.msc` para abrir la ventana **Directiva de seguridad local**.
2	Abra **Configuración de seguridad** > **Directivas locales** > **Opciones de seguridad**.
3	Seleccione **Send NTLMv2 response only (Enviar respuesta NTLMv2 solamente)**. **Refuse LM & NTLM (Rechazar LM y NTLM)** en el campo **Network Security: LAN Manger authentication level (Seguridad de red: nivel de autenticación de administrador LAN)**.
4	Seleccione la casilla de verificación **Network Security: Do not store LAN Manager hash value on next password change (Seguridad de red: no almacenar valor de hash de LAN Manager en el próximo cambio de contraseña)**.
5	En una ventana de comando, escriba `gpupdate` para realizar el cambio de directivas de seguridad.

Administrar actualizaciones

Antes de la implementación, actualice todos los sistemas operativos del PC utilizando las herramientas de la página web **Windows Update** de Microsoft. Para acceder a esta herramienta en Windows, seleccione **Inicio > Todos los programas > Windows Update**.

Verificación de firmas digitales

Verificación de la integridad de EcoStruxure Automation Device Maintenance tras la descarga

Después de descargar el archivo ejecutable de EcoStruxure Automation Device Maintenance del sitio web de Schneider Electric, verifique la integridad del archivo. Para ello, siga los pasos siguientes:

Paso	Acción
1	Haga clic con el botón derecho en el archivo AutomationDeviceMaintenance.exe y ejecute el comando **Propiedades** en el menú contextual.
2	En el cuadro de diálogo **AutomationDeviceMaintenance.exe Properties** seleccione la ficha **Firmas digitales**.
3	En la **Lista de firmas**, seleccione **Schneider Electric USA, INC.** y haga clic en el botón **Detalles** para ver los **Detalles de la firma digital**.
4	En el cuadro de diálogo **Detalles de la firma digital**, asegúrese de que se muestra el siguiente mensaje: **Esta firma digital es correcta.**

Ahora puede hacer doble clic en el archivo .exe para iniciar EcoStruxure Automation Device Maintenance.

Verificación de los componentes durante la puesta en marcha

Cuando se inicia EcoStruxure Automation Device Maintenance, se analiza cada biblioteca de enlace dinámico (DLL) cargada para verificar si es de confianza o no. Se trata de una característica de seguridad integrada contra los ciberataques, que también se emplea para aumentar el nivel de confianza.

Qué hacer si se detectan componentes que no son de confianza

Si se detectan componentes que no son de confianza, se cancela el inicio de EcoStruxure Automation Device Maintenance y se muestra un mensaje que indica que se ha detectado una excepción.

En este caso, tiene las siguientes opciones:

- Reinstale EcoStruxure Automation Device Maintenance.
- Si tiene la menor sospecha de que esto ha sido causado por un ciberataque, consulte el portalSchneider Electric Cybersecurity services portal para obtener más información o asistencia.

Para encontrar el componente que provoca el problema, puede utilizar una herramienta de depuración, como WinDbg: Ejecute la herramienta de depuración, inicie EcoStruxure Automation Device Maintenance y observe el contenido del archivo de registro en busca de las entradas que indican que no se puede determinar la validez de la firma de código de una DLL.

Archivos que requieren desinstalación manual

Descripción general

Cuando se desinstala EcoStruxure Automation Device Maintenance del PC, los archivos de programa se eliminan automáticamente, pero hay algunos archivos específicos del usuario que debe gestionar de forma individual para evitar problemas de ciberseguridad.

Archivo de configuración de EcoStruxure Automation Device Maintenance

El archivo de configuración de EcoStruxure Automation Device Maintenance *AutomationDeviceMaintenanceSettings.emes* se crea con EcoStruxure Automation Device Maintenance para almacenar la configuración que se define en el cuadro de diálogo **Configuración** (por ejemplo, rangos de exploración de Modbus TCP o ajustes de detección). No se elimina del PC con la desinstalación de EcoStruxure Automation Device Maintenance, sino que debe eliminarse manualmente.

Elimínelo de la carpeta *%APPDATA%\Schneider Electric\Automation Device Maintenance* con el Explorador de Windows u otras herramientas del sistema de archivos.

Certificados

El certificado de EcoStruxure Automation Device Maintenance y los **Certificados de confianza** y **Certificados no de confianza** gestionados en el cuadro de diálogo **Configuración** , en **Seguridad > Gestión de certificados** (consulte también Cuadro de diálogo **Gestión de certificados**, página 44) se eliminan del

PC con Windows con la desinstalación de EcoStruxure Automation Device Maintenance. También se eliminan del almacén de certificados de Windows.

Paquetes de datos

Los paquetes de datos, página 20 que se han guardado localmente no se eliminarán del PC con la desinstalación de EcoStruxure Automation Device Maintenance. De forma predeterminada, los paquetes de datos se almacenan en la carpeta *%PUBLIC%\Public Documents\Schneider Electric\Data Packages*. Puede configurar su propia ruta en el cuadro de diálogo **Configuración > Configuración del paquete**, página 37.

Elimine la carpeta predeterminada o la configurada manualmente mediante el Explorador de Windows u otras herramientas de sistema de archivos.

Archivos del proyecto de EcoStruxure Automation Device Maintenance

Los archivos del proyecto de EcoStruxure Automation Device Maintenance no se eliminan del PC al desinstalar EcoStruxure Automation Device Maintenance. Busque archivos con la extensión **.emep* y elimínelos manualmente o guárdelos para utilizarlos más tarde en un lugar seguro, en el que no sea posible el acceso no autorizado.

Archivos de registro

Los archivos de registro que se han guardado localmente en la ruta especificada en el cuadro de diálogo **Configuración > Registros**, página 38 no se eliminan del PC al desinstalar EcoStruxure Automation Device Maintenance. Quite la carpeta manualmente con el Explorador de Windows u otras herramientas de sistema de archivos o guarde los archivos de registro para utilizarlos más adelante en un lugar seguro en el que no sea posible el acceso no autorizado.

Componentes utilizados por EcoStruxure Automation Device Maintenance

Descripción general

EcoStruxure Automation Device Maintenance proporciona una descripción general de los componentes y las versiones actuales. Si se detecta una excepción, esta lista de componentes y versiones puede ayudar a encontrar el componente que podría ser la causa.

Recuperación de una lista de componentes

Para recuperar una lista de los componentes cargados por EcoStruxure Automation Device Maintenance, siga estos pasos:

Paso	Acción
1	Haga clic en el botón **Acerca de** de la barra de herramientas. **Resultado**: Se abrirá el cuadro de diálogo **Acerca de**.
2	Haga clic en el enlace **Información del componente**. **Resultado**: Se abrirá el cuadro de diálogo **Información del componente**. Acerca de × Información de componente Nombre de componente / Versión / Descripción AutomationDeviceMaintenance / 3.0.154.0 / General BrandIdentity / 4.19.0.2175 / General ServiceCommon / 3.1.3.0 / General log4net / 2.0.11.0 / General PackageCommon / 3.0.4.0 / General Org.Schneider.FWChecker / 2.5.2.0 / General Org.Schneider.Crypto / 2.5.2.0 / General Asn1Parser / 2.5.2.0 / General SE.CS.PKI.Common / 1.0.6.0 / General PackageDescriptionLibrary / 3.1.1.0 / General Volver a Acerca de Copiar detalles Life Is On Schneider Electric Aceptar
3	Haga clic en el vínculo **Copiar detalles** para copiar la lista de componentes y versiones en el portapapeles. Ahora puede pegar el contenido en un archivo *.txt que le permita buscar cómodamente componentes específicos y las versiones correspondientes.

Glosario

C

Certificado de dispositivo:

Certificado de llaves público X.509 utilizado por la herramienta y el dispositivo para establecer un canal de comunicación seguro (por ejemplo, HTTPS).

D

Detección de dispositivos:

Detección automática de dispositivos y los servicios que ofrecen dichos dispositivos en una red informática.

DHCP: Protocolo de configuración dinámica de host (del inglés "Dynamic Host Configuration Protocol").

Dirección IP:

Dirección de un dispositivo de acuerdo con los estándares del protocolo IP. Puede ser en formato de dirección IPv4 o IPv6.

DNS: Domain Name System (sistema de nombres de dominio)

DPWS:

Perfil de dispositivo para servicios web (Device Profile for Web Services): estándar para la detección y la descripción de dispositivos que admiten servicios web.

F

Familia de dispositivos:

Grupo de dispositivos de tipo similar: cada familia de dispositivos se identifica con un ID de producto.

H

HTTP:

«Hypertext Transfer Protocol» (protocolo de transferencia de hipertexto)

HTTPS:

«Hypertext Transfer Protocol Secure» (protocolo seguro de transferencia de hipertexto), conocido también como HTTP sobre TLS.

I

ICS: Control y sistemas industriales

ID de producto:

Identificador de producto, identifica la familia de productos a la que pertenece un dispositivo.

IEC:

(*International Electrotechnical Commission*) Una organización de estándares internacional sin ánimo de lucro y no gubernamental que prepara y publica estándares internacionales para todas las tecnologías eléctricas, electrónicas y relacionadas.

IP:

Protocolo de Internet

ISO: Organización Internacional de Normalización

N

NEMA:

(*National Electrical Manufacturers Association*) El estándar para el rendimiento de diversas clases de carcasas eléctricas. Los estándares de NEMA abarcan la resistencia a la corrosión, la capacidad de protección contra la lluvia y la inmersión, etc. Para los países adheridos a IEC, la norma IEC 60529 clasifica el grado de protección contra la entrada de las carcasas.

O

OPC UA:

OPC Unified Architecture: OPC UA es un estándar de interoperabilidad para el intercambio seguro y fiable de datos en el espacio de automatización industrial. Es un protocolo de comunicación independiente de la plataforma que usa el modelo servidor/cliente. La conexión entre el cliente y el servidor suele basarse en el fiable protocolo de capas de transporte (TCP, Transmission Control Protocol, protocolo de control de transmisión).

Para obtener más información sobre OPC, especialmente OPC UA, consulte la página web oficial de OPC Foundationhttps://opcfoundation.org.

P

Paquete de datos, Paquete de firmware:

Un paquete de datos es un archivo utilizado para el intercambio de contenido entre la herramienta y los dispositivos. Puede estar en formato SEDP. Un paquete de datos contiene paquete(s) de firmware, pero también contiene configuración, aplicaciones PLC, etc.

PLC:

(*controlador lógico programable*) Un ordenador industrial que se usa para automatizar procesos industriales, de fabricación y otros procesos electromecánicos. Los PLCs se diferencian de los ordenadores comunes en que están diseñados de forma que tienen varias matrices de entrada y salida, y que disponen de especificaciones más sólidas contra los golpes, las vibraciones, la temperatura, las interferencias eléctricas, etc.

POU:

(*unidad de organización de programas*) Una declaración variable en el código fuente y el conjunto de instrucciones correspondiente. Las POUs facilitan la reutilización modular de programas de software, funciones y bloques de funciones. Una vez declaradas, cada una de las POUs está disponible para las otras.

S

SEDP:

Schneider Electric Data Package (paquete de datos de Schneider Electric), formato de archivo estandarizado para el intercambio de contenido entre las herramientas de software y los dispositivos.

T

TCP:

«Transmission Control Protocol» (protocolo de control de transmisión)

TLS:

«Transport Layer Security» (seguridad de la capa de transporte)

U

UDP: Protocolo de datagramas de usuario (del inglés “User Datagram Protocol”).

URL:

«Uniform Resource Locator» (localizador uniforme de recursos):

Índice

A

acceso a extensiones 64
actualización del archive de configuración de seguridad 71
actualizar firmware 69
Administración de certificados 43
Advertencia
  guardar, borrar 26
agregar dispositivo 23
Agrupar dispositivos 56
aplicación de modificaciones 26
Archivo AutomationDeviceMaintenanceSettings.emes 79
Archivo csv para importación 34
archivo de configuración de seguridad 41, 71
archivos de proyecto con dispositivos no identificados 31
archivos de proyecto de otro ordenador 30
Archivos fwp del paquete 51
Archivos ldx del paquete 51
Archivos sedp del paquete 51
Archivos sedps del paquete 51
archivos sedps del paquete seguros 51
área de notificaciones 67

B

barra de herramientas
  acerca de, ayuda, detección 19
Botón **Aceptar** 26
Botón **Aplicar** 26
Botón **Copiar en el portapapeles** 54
búsqueda
  manual, automático 25

C

CA 43
Centro de actualizaciones 68
certificado
  validar, confiar, dejar de confiar, quitar 43
Certificado de aplicación 43
certificado de dispositivo
  de confianza, no de confianza 21
certificados 43
ciberseguridad 74
  certificaciones 74
  conexión de área local 77
  cortafuegos 77
  directrices 76
  escritorio remoto 77
  introducción 74
  LANMAN / NTLM 78
  tarjetas de interfaz de red 76
componentes y versiones 80
Comunicación HTTP/HTTPS 23
comunicación Modbus TCP 23
confiar en el certificado 43
configuración
  Configuración de comunicación 37
  detección 32
  detección, Modbus, configuración de paquete, idioma, certificado 25
  Explorador DPWS 36
  idioma, cambiar 40
  Modbus TCP 34
  ubicación de paquete 37
contraseñas 61, 69
copiar el identificador 54
credenciales 25, 61, 69
Cuadro de diálogo **Confirmación de actualización** 69
cuadro de diálogo de inicio de sesión 61
Cuadro de diálogo **Firmware** 69
Cuadro de diálogo **Inicio de sesión del dispositivo** 61
Cuadro de diálogo **Proyecto modificado** 27
Cuadro de diálogo **Resumen de actualización** 69

D

datos
  firmware, configurar 52
dejar de confiar en el certificado 43
desinstalación 79
detección
  automático, manual 32
detección de dispositivos
  Modbus, DPWS (perfil de dispositivo para servicios web) 15
dispositivo
  actualización, opciones de configuración, credenciales 61
dispositivo/carga
  nombre del dispositivo, estado, paquete de datos 21
dispositivos compatibles 15
dispositivos modulares 64
DLL no de confianza 78

E

eliminación de archivos 79
eliminar certificado 43
Entidad de certificación 43
error
  error, advertencia 19
Error
  guardar,borrar 26
Estado de detección de dispositivos 66
excepción 78
Explorador DPWS
  petición de sondeo, petición de metadatos, adaptadores de red 36
extensiones 64

F

Ficha **Dispositivo/Cargando** 55
ficha **Extensiones** 64
firmware
  actualización, dispositivo/carga, paquete de datos 69
  versión, información de actualización, progreso 21
frecuencia de sondeo 37
funciones de seguridad 41

H

hardware
  CPU, RAM, HDD 16

I

icono de actualización 26
identificador
  Copia 54
Importar archivo csv 34
importar archivo de configuración 34
Importar archivo de configuración de seguridad 41
importar un archivo de configuración 34
inferior 21
información
  guardar, borrar 26
  paquete, producto 52
información del componente 80
Infraestructura de clave pública (PKI) 48
inicio de sesión para la actualización del firmware ... 69
inscribir certificado de aplicación 43
instalación
  procedimiento, asistente para la instalación, instalación, acuerdo de licencia 17

M

mensajes de confirmación 67
mensajes de notificación 67
Modbus TCP
  ID de la unidad, tiempo de espera de ping agotado, puerto 34
modificaciones en la página **Configuración** 26
módulos de bastidor 64

N

nuevo proyecto 27

O

Opción **grupo** 56

P

pantalla de bienvenida
  paquete de datos, dispositivo/carga, barra de herramientas 18
paquete de datos 51
  nombre del paquete, información del paquete 20
paquete de firmware
  información del paquete, nombre del paquete 18
Paquetes de datos **rechazados** 52
Paquetes de datos **válidos** 52
PKI 48
project
  abrir 29
  abrir, guardar 19
  guardar 28
protocolos de comunicación 16
proyecto
  nuevo 27

Q

quitar certificado 43

R

registros
  inferior 68
Repositorio local 37
requisitos del sistema
  hardware, software, protocolos de comunicación, resolución de pantalla, ciberseguridad 16
restablecer configuración de aplicación 40

S

Software
  características, paquetes de firmware compatibles 15
Supervisión del estado de detección de dispositivos 66
syslog 49

T

Tarjeta de memoria SD 21
TCP 49
timeout
  Configuración de comunicación 37
TLS 49

U

ubicación del paquete
  sumar 38
UDP 49

Schneider Electric
35 rue Joseph Monier
92500 Rueil Malmaison
France

+ 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.

© 2022 Schneider Electric. Reservados todos los derechos.

EIO0000004047.04