

SIEMENS
Ingenuity for life



SINEC NMS Firmware Management

SINEC NMS V1.0 SP1

<https://support.industry.siemens.com/cs/ww/de/view/109762792>

Siemens
Industry
Online
Support



Información legal

Uso de ejemplos de aplicación.

Los ejemplos de aplicación ilustran la solución de tareas de automatización a través de una interacción de varios componentes en forma de módulos de texto, gráficos y/o software. Los ejemplos de aplicación son un servicio gratuito de Siemens AG y/o una subsidiaria de Siemens AG ("Siemens"). No son vinculantes y no pretenden ser completos o funcionales con respecto a la configuración y el equipamiento. Los ejemplos de aplicación simplemente ofrecen ayuda con tareas típicas; no constituyen soluciones específicas para el cliente. Usted mismo es responsable del funcionamiento correcto y seguro de los productos de acuerdo con las normas vigentes y también debe verificar la función del ejemplo de aplicación respectivo y personalizarlo para su sistema.

Siemens le otorga el derecho no exclusivo, no sublicenciable e intransferible de que los ejemplos de aplicación sean utilizados por personal técnicamente capacitado. Cualquier cambio en los ejemplos de aplicación es su responsabilidad. Solo se permite compartir los ejemplos de aplicación con terceros o copiar los ejemplos de aplicación o extractos de los mismos en combinación con sus propios productos.

Los ejemplos de aplicación no están obligados a someterse a las pruebas e inspecciones de calidad habituales de un producto facturable; pueden tener defectos funcionales y de rendimiento, así como errores. Es su responsabilidad usarlos de tal manera que cualquier mal funcionamiento que pueda ocurrir no resulte en daños a la propiedad o lesiones a las personas.

Descargo de responsabilidad

Siemens no asumirá ninguna responsabilidad, por ningún motivo legal, incluida, entre otras, la responsabilidad por la usabilidad, disponibilidad, integridad y ausencia de defectos de los ejemplos de aplicación, así como por la información relacionada, los datos de configuración y rendimiento y cualquier daño causado por ello. . Esto no se aplicará en casos de responsabilidad obligatoria, por ejemplo, en virtud de la Ley alemana de responsabilidad por productos defectuosos, o en casos de dolo, negligencia grave o muerte culposa, lesiones corporales o daños a la salud, incumplimiento de una garantía, incumplimiento fraudulento. -revelación de un defecto o incumplimiento culposo de obligaciones contractuales materiales. No obstante, las reclamaciones por daños derivados del incumplimiento de obligaciones contractuales materiales se limitarán a los daños previsibles típicos del tipo de acuerdo, a menos que la responsabilidad surja de dolo o negligencia grave o se base en la pérdida de la vida, lesiones corporales o daños a la salud. Las disposiciones anteriores no implican ningún cambio en la carga de la prueba en su perjuicio. Deberá indemnizar a Siemens frente a reclamaciones existentes o futuras de terceros a este respecto, excepto cuando Siemens sea responsable obligatorio.

Al utilizar los ejemplos de aplicación, reconoce que Siemens no se hace responsable de ningún daño más allá de las disposiciones de responsabilidad descritas.

Otra información

Siemens se reserva el derecho de realizar cambios en los ejemplos de aplicación en cualquier momento sin previo aviso. En caso de discrepancias entre las sugerencias de los ejemplos de aplicación y otras publicaciones de Siemens, como catálogos, prevalecerá el contenido de la otra documentación.

Los términos de uso de Siemens (<https://support.industry.siemens.com>) también se aplicará.

Información de seguridad

Siemens ofrece productos y soluciones con funciones de seguridad industrial que respaldan el funcionamiento seguro de plantas, sistemas, máquinas y redes.

Para proteger plantas, sistemas, máquinas y redes contra amenazas ciberneticas, es necesario implementar, y mantener continuamente, un concepto de seguridad industrial holístico y de última generación.

Los productos y soluciones de Siemens constituyen un elemento de dicho concepto.

Los clientes son responsables de evitar el acceso no autorizado a sus plantas, sistemas, máquinas y redes. Dichos sistemas, máquinas y componentes solo deben conectarse a una red empresarial oa Internet si y en la medida en que dicha conexión sea necesaria y solo cuando estén implementadas las medidas de seguridad adecuadas (por ejemplo, cortafuegos y/o segmentación de la red).

Para obtener información adicional sobre las medidas de seguridad industrial que pueden implementarse, visite <https://www.siemens.com/industrialsecurity>.

Los productos y soluciones de Siemens se someten a un desarrollo continuo para hacerlos más seguros.

Siemens recomienda enfáticamente que las actualizaciones del producto se apliquen tan pronto como estén disponibles y que se utilicen las últimas versiones del producto. El uso de versiones de productos que ya no son compatibles y la falta de aplicación de las últimas actualizaciones puede aumentar la exposición del cliente a las ciberamenazas.

Para mantenerse informado sobre las actualizaciones de productos, suscríbase a la fuente RSS de Siemens Industrial Security en: <https://www.siemens.com/industrialsecurity>.

Tabla de contenido

Tabla de contenido

Información legal.....	2
1 Introducción.....	4
1.1 Descripción general.....	4
1.2 Principio de funcionamiento.....	4
1.3 Componentes utilizados.....	5
2 Configuración de hardware	6
3 Ingeniería	7
3.1 Requerimientos básicos	7
3.2 Descarga de archivos de firmware	12
3.3 Crear contenedor de firmware.....	13
3.4 Creación de una política para la actualización del firmware	18
4 Información útil	30
4.1 Política	30
4.1.1 Configuración basada en reglas globales o locales	31
4.2 Programación (Disparador)	32
4.3 Condiciones del dispositivo	34
4.3.1 Copia de seguridad de dispositivos individuales	35
4.3.2 Copia de seguridad de dispositivos del mismo tipo	36
4.3.3 Copia de seguridad de varios dispositivos en el área de dispositivos	37
4.3.4 Comodines.....	40
4.4 Estrategias de políticas y manejo de errores	41
4.4.1 Estrategias de política	41
4.4.2 Manejo de errores de reglas	43
4.5 Tareas.....	45
4.5.1 Tarea: Establecer servidor SSH	45
4.5.2 Tarea: Cargar firmware en el dispositivo	46
4.5.3 Tarea: Tiempo de espera de activación	47
5 Apéndice	48
5.1 Servicio y soporte	48
5.2 Enlaces y literatura	49
5.3 Modificar la documentación	49

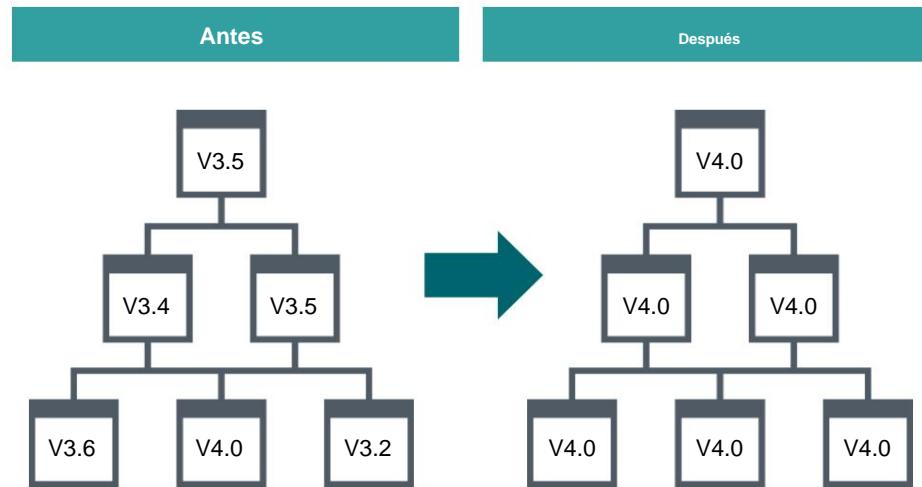
1. Introducción

1 Introducción

1.1 Descripción general

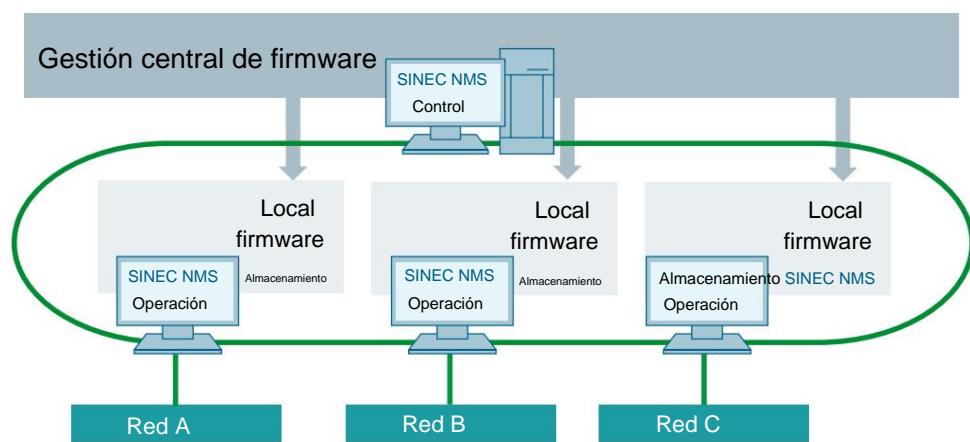
Es posible que un administrador de red necesite ajustar las versiones de firmware de los componentes de la red para reflejar las nuevas funciones o las políticas globales de la empresa. SINEC NMS le ofrece la posibilidad de gestionar las versiones de firmware de forma centralizada para reducir el esfuerzo y garantizar que las versiones de firmware estén actualizadas.

Figura 1-1



1.2 Principio de funcionamiento

Figura 1-2



SINEC NMS ofrece la posibilidad de cargar archivos de firmware en componentes SCALANCE y RUGGEDCOM. En el sistema SINEC NMS, los archivos de firmware se administran de forma centralizada en contenedores de firmware en el Control y se pueden implementar en toda la planta a través de políticas. El firmware se puede cargar en el dispositivo de forma manual o programar a través de una política. Al hacerlo, SINEC NMS tiene en cuenta la topología para proporcionar un proceso de actualización fluido. Cada cambio en los contenedores de firmware en el Control es

 1. Introducción

sincronizado automáticamente con las Operaciones. Cuando se realizan cambios importantes en los contenedores de firmware, la sincronización con Operations puede llevar algún tiempo.

1.3 Componentes utilizados

Este ejemplo de aplicación se creó utilizando estos componentes de hardware y software:

Tabla 1-1

Componentes	Número de artículo	Dirección IP	enrutador	Nota
XB208	6GK5 208-0BA00-2AB2	172.16.0.2	172.16.0.1	
CPU 317-2 PN/PD	6ES7 317-2EK14-0AB0	172.16.0.5	172.16.0.1	
CPU 1513-1 NP	6ES7 516-3FN01-0AB0	172.16.0.3	172.16.0.1	
XB208	6GK5 208-0BA00-2AB2	192.168.0.2	192.168.0.1	
W761-1 RJ45 6GK5 761-1FC00-0AA0		192.168.0.14	192.168.0.1	
W722-1 RJ45 6GK5 722-1FC00-0AA0		192.168.0.13	192.168.0.1	
CPU 1212C		192.168.0.10	192.168.0.1	
ET 200SP	6ES7 155-6AU00-0BN0	192.168.0.11	192.168.0.1	
XM408-4C	6GK5 408-8GR00-2AM2	10.0.0.1		
Control & Operación 1		10.0.1.4	10.0.1.1	Se admite cualquier SIMATIC IPC que cumpla los requisitos de software.
Operación 2		10.0.2.3	10.0.2.1	

Este ejemplo de aplicación consta de los siguientes componentes:

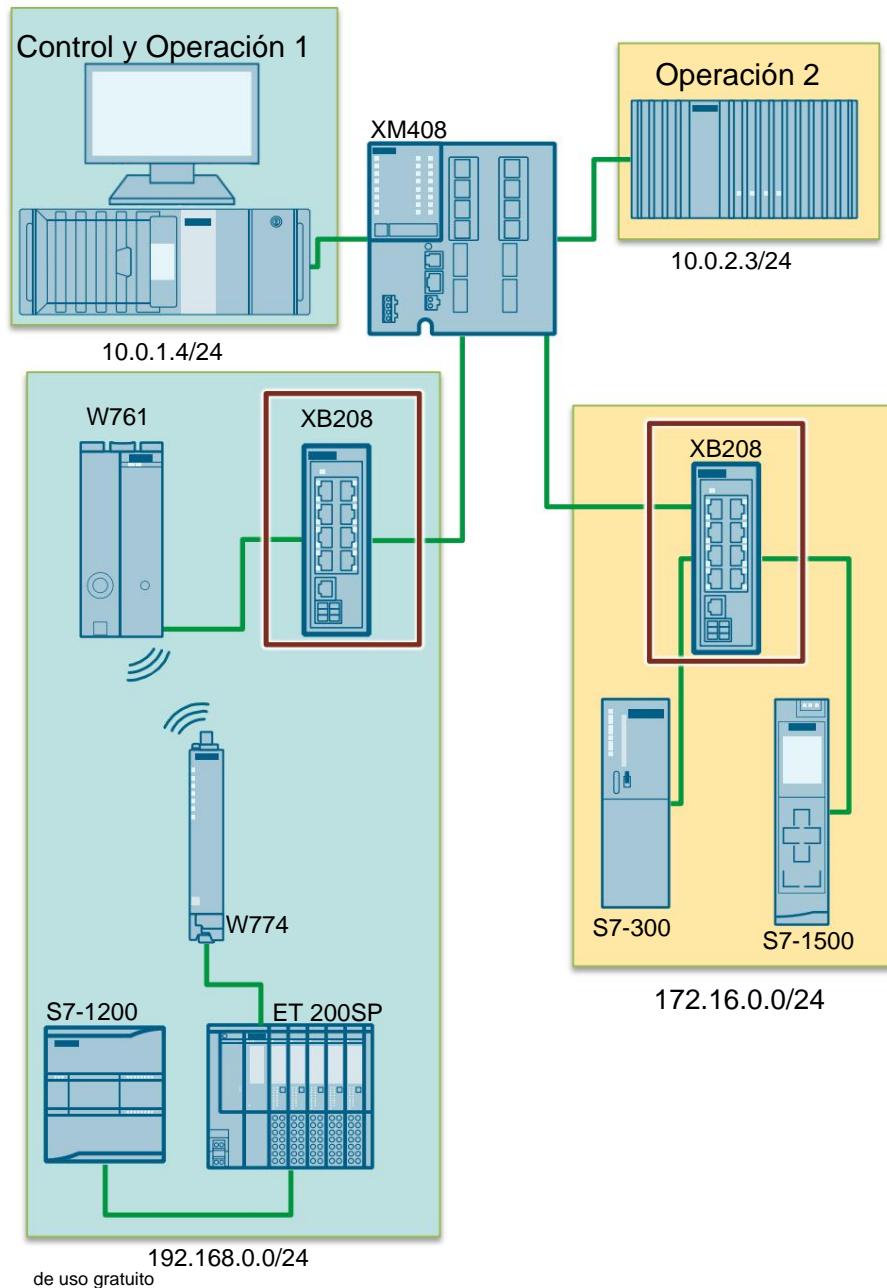
Tabla 1-2

Componentes	Nombre del archivo	Nota
Este documento	109762792_SINEC_NMS_Firmware_V1_0.es	

2 Configuración de hardware**2 configuración de hardware**

En el siguiente documento, se cargará una actualización de firmware desde el XB208. La actualización del firmware se almacena en el Control. Aquí se utiliza la misma configuración de hardware que en el artículo *Primeros pasos "Comprender y utilizar SINEC NMS"*.

Figura 2-1



3 Ingeniería

3.1 Requerimientos básicos

Para utilizar las funciones en SINEC NMS, se deben cumplir los siguientes requisitos básicos:

1. La función de actualización de firmware es compatible con los siguientes dispositivos.

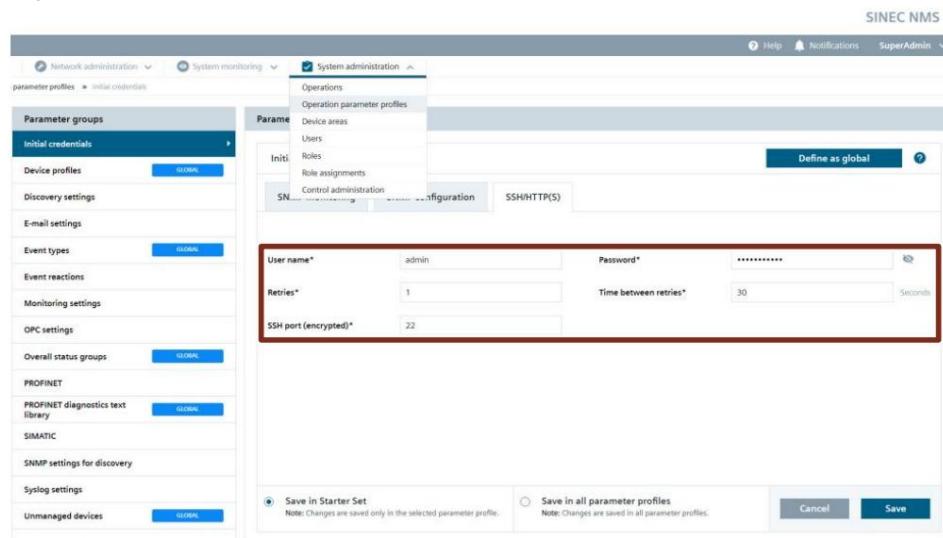
Tabla 3-1

Sistema operativo	familia de dispositivos
VxWorks	ESCALANCE X
MSPS	ESCALANCE X
VxWorks	ESCALANCE W-700
MSPS	SCALANCE W-700 / 1700
MSPS	SCALANCE S615, SC-600
MSPS	SCALANCE M-800
RUGGEDCOM RS	
RUGGEDCOM RX	

3 Ingeniería

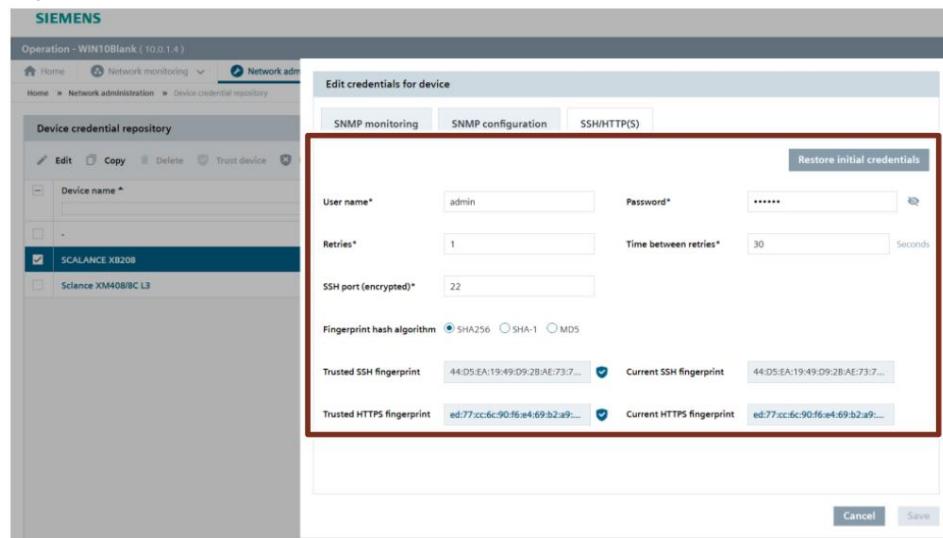
2. SINEC NMS requiere datos de inicio de sesión del dispositivo para establecer una conexión con los dispositivos a través de SSH y SNMP. Puede definir los datos de inicio de sesión en el menú "Perfil de parámetros de operación" en Control, en el grupo de parámetros "Datos iniciales de inicio de sesión". En la pestaña SSH/HTTP(S), puede ingresar los valores deseados y guardarlos en el perfil de parámetros.

Figura 3-1



Además, los datos de inicio de sesión se pueden almacenar y editar en el directorio de datos de inicio de sesión del dispositivo de Operation para cada dispositivo individual. Si no se almacenan datos de inicio de sesión específicos en el directorio de datos de inicio de sesión del dispositivo, los datos de inicio de sesión iniciales se transfieren al directorio de datos de inicio de sesión del dispositivo y se utilizan para el inicio de sesión.

Figura 3-2

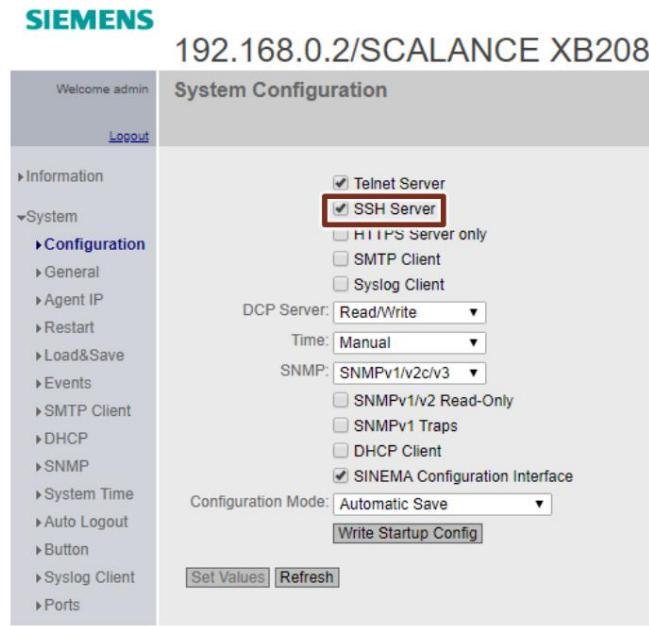


de uso gratuito

3 Ingeniería

3. El servidor SSH debe estar habilitado en el dispositivo (SCALANCE XB208).

Figura 3-3

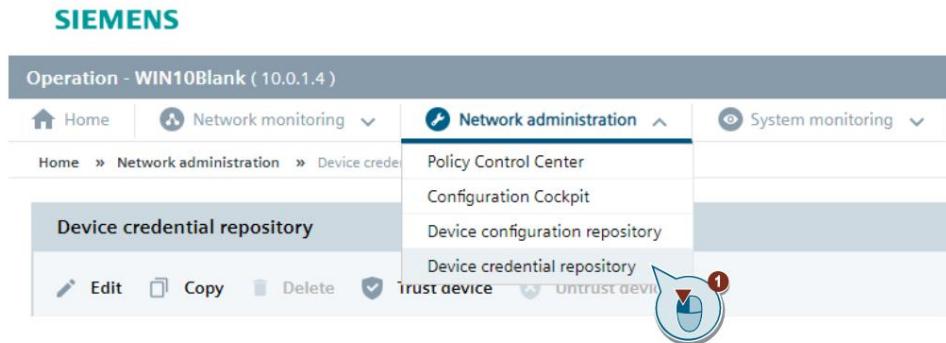


de uso gratuito

3 Ingeniería

4. El dispositivo debe designarse como de confianza. Haga clic en "Administración de red > Directorio de datos de inicio de sesión del dispositivo" en la Operación.

Figura 3-4



Seleccione el dispositivo y haga clic en "Confiar en el dispositivo".

Figura 3-5

The screenshot shows the 'Device credential repository' table. The columns are: Device name, Device type, In monitoring, Trust state. The first row has a checked checkbox and a blue circular icon with a red '2'. The second row has an unchecked checkbox and a blue circular icon with a red '1'. The third row has a checked checkbox and a blue circular icon with a red '2'. The fourth row has an unchecked checkbox and a blue circular icon with a red '1'. The 'Trust state' column for the first two rows is 'Yes' and 'Untrusted' respectively, while the last two rows are 'Yes' and 'Trusted'.

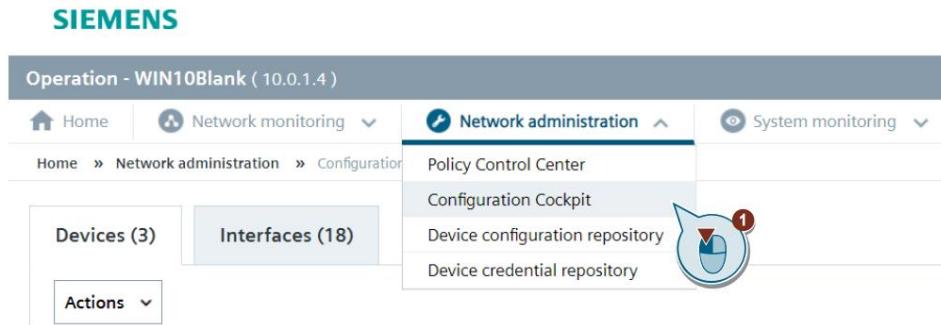
	Device name	Device type	In monitoring	Trust state
<input type="checkbox"/>	SCALANCE XB208 10.0.1.4	Management Station	Yes	Untrusted
<input checked="" type="checkbox"/>	SCALANCE XB208 PN (OBAA00-2AB2) 192.168.0.2	SCALANCE XB208 PN (OBAA00-2AB2)	Yes	Untrusted
<input type="checkbox"/>	SCALANCE XM408-8C (8GR00-2AM2) 10.0.1.1	SCALANCE XM408-8C (8GR00-2AM2)	Yes	Trusted

de uso gratuito

3 Ingeniería

5. Solo los dispositivos para los que se permite el acceso a la configuración se incluyen en el política. Vaya a la página "Administración de red > Cabina de configuración" de la Operación respectiva.

Figura 3-6



Utilice el botón "Permitir acceso a la configuración" para determinar qué dispositivos deben tener el estado "Permitido".

Figura 3-7

The screenshot shows the 'Configuration Cockpit' page under 'Network administration'. It displays a table of devices with columns for Status, IP address, System name, Configuration access status, and Management status. One row is highlighted, showing an IP address of 192.168.0.2/24, a system name of SCALANCE XB208, and a configuration access status of 'Blocked'. The 'Blocked' button in this row is highlighted with a red box.

	Status	IP address	System name	Configuration access	Management status
<input type="checkbox"/>	OK	10.0.1.4/24		Allowed	Monitored
<input checked="" type="checkbox"/>	OK	192.168.0.2/24	SCALANCE XB208	Blocked	Monitored
<input type="checkbox"/>	OK	10.0.1.1/24	Scalance XM408/BC L3	Allowed	Managed

Nota Hay disponible una licencia de prueba para familiarizarse con SINEC NMS y probarlo. Esto admite un máximo de tres dispositivos del estado de gestión "Administrado". Una licencia de este tipo es estándar y válida por un período de 21 días. Esta licencia se activa automáticamente si el administrador de licencias de automatización no encuentra ningún otro tipo de licencia durante la primera puesta en marcha de SINEC NMS. Un sistema con una licencia de prueba vencida se puede reactivar agregando una licencia completa.

de uso gratuito

3.2 Descarga de archivos de firmware

1. Los archivos de firmware actuales se pueden encontrar en [Siemens Industry Online Support](#).
2. Introduzca el número de artículo del dispositivo en el campo de búsqueda. Seleccione "Descargar" como el tipo de entrada. Abre la página de entrada actual.

Figura 3-8

The screenshot shows the Siemens Industry Online Support interface. In the search bar, the text '6GK5 208-0BA00-2AB2' is entered. Below the search bar, a dropdown menu shows 'Downloaded (14)'. The main area displays a list of 14 entries. The first entry is highlighted with a blue circle and the number '3'. Callouts numbered 1, 2, and 3 point to the search bar, the download filter, and the first search result respectively.

3. Descarga el archivo y descomprímelo.

Figura 3-9

This screenshot shows a download page for a firmware update. The file name is 'Firmware_XB-200_XC-200_XP-200_XR-300WG_XF200BA_V04.02.00.00_06.01.56_OSS.zip', which is 22.6 MB in size. Below the file name, there is a 'Hash:' section with a link to 'Firmware_XB-200_XC-200_XP-200_XR-300WG_XF200BA_V04.02.00.00_06.01.56_OSS.zip.txt'. There is also a 'GSDML:' section with a link to 'GSDML.zip' (226.3 KB). Callouts numbered 1, 2, and 3 point to the file name, hash, and GSDML link respectively.

Nota

Tenga en cuenta qué versión de firmware es compatible. Puede encontrar información sobre nuevas versiones de firmware en el archivo "Léame" de SINEC NMS o en el HSP actual.

Se pueden descargar versiones de firmware más recientes, pero puede haber limitaciones en la funcionalidad, como la copia de seguridad de la configuración.

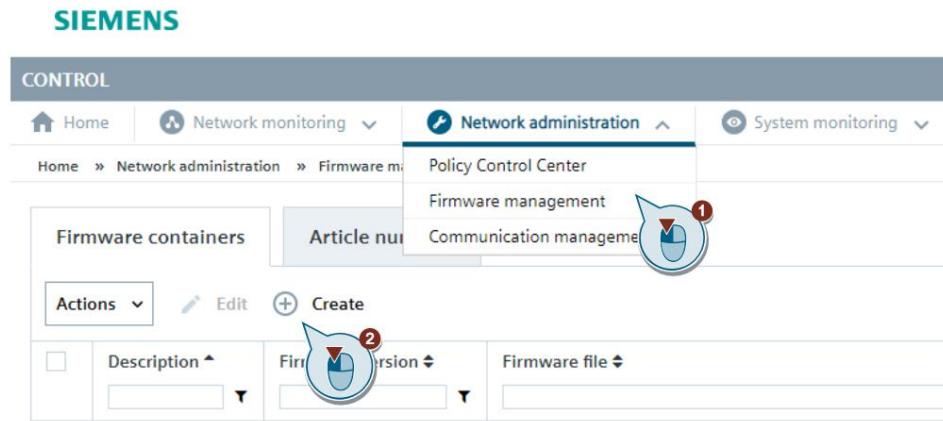
de uso gratuito

3.3 Crear contenedor de firmware

Los archivos de firmware del dispositivo se pueden gestionar de forma centralizada en Gestión de firmware en el Control. Cualquier cambio en la gestión de firmware se sincroniza automáticamente con las operaciones correspondientes. Puede descargar archivos de firmware existentes a los dispositivos correspondientes a través de políticas o configuraciones individuales.

1. Abra el menú "Administración de red > Gestión de firmware" en el Control. Se abre la Gestión de firmware. Haga clic en el botón "Crear" para crear un nuevo contenedor de firmware.

Figura 3-10



2. Introduzca una descripción para el contenedor de firmware. Haga clic en el botón "Agregar archivo".

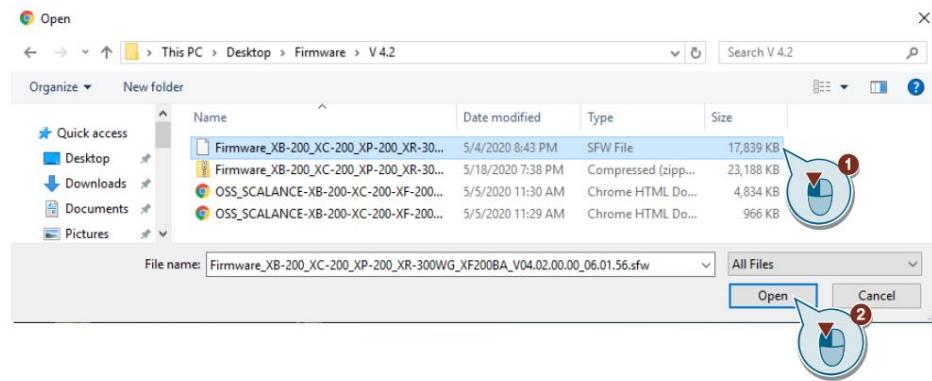
Figura 3-11

Description*	Release time stamp*
SCALANCE XB200_XC200_XP200_XR300WG_XF200BA_V4.2	mm/dd/yyyy hh:mm
Version*	Compatible firmware version
	Compatible hardware version
Firmware file and documents Compatibility	
Firmware file Move up Move down Modify Delete Add file	
NO FIRMWARE FILE AVAILABLE	

3 Ingeniería

3. Seleccione el archivo de firmware.

Figura 3-12



4. Haga clic en el botón "Compatibilidad". Al cargar archivos de firmware en SINEC NMS, la información de compatibilidad del dispositivo se lee automáticamente. Esto se aplica a dispositivos MSPS y dispositivos Ruggedcom. Para dispositivos VxWorks, esta información debe actualizarse manualmente. Compruebe si el número de artículo adecuado está disponible para su dispositivo.

Figura 3-13

Article number	Device type	User-defined
6GK5 208-0BA00-2AB2	SCALANCE XB208 PN (0BA00-2AB2)	No
6GK5 326-2Q500-3RR3		No
6GK5 208-0GA00-2FC2	SCALANCE XC208 PN G EEC (GA00-2FC2)	No
6GK5 216-4BS00-2AC2	SCALANCE XC216-4C (BS00-2AC2)	No
6GK5 216-0BA00-2TB2	SCALANCE XB216 (0BA00-2TB2)	No
6CKE 206-2C500-2AC2	SCALANCE XC206-2C500-2AC2	No

de uso gratuito
Note: To be able to save the firmware container, article numbers must be selected in the "Compatibility" tab.

Cancel **Save**

3 Ingeniería

5. Haga clic en el botón "Guardar".

Figura 3-14

The screenshot shows the 'Create firmware container' interface. At the top, there are fields for 'Description*' (SCALANCE XB200_XC200_XP200_XR300WG_XF200BA_V4.2) and 'Release time stamp*' (04/24/2020 19:30). Below these are fields for 'Version*' (4.2.0.0), 'Compatible firmware version' (0.0.0.0), and 'Compatible hardware version'. The 'Compatibility' tab is selected. A note at the bottom states: 'Note: To be able to save the firmware container, article numbers must be selected in the "Compatibility" tab.' There is a 'Save' button with a red circled '1' icon indicating pending changes.

6. Para mostrar las diferentes configuraciones, se creó un segundo contenedor de firmware en este ejemplo (firmware V4.1). Para la configuración del segundo contenedor de firmware, se repitieron los pasos 1 a 5.

Figura 3-15

The screenshot shows the SINEC NMS interface under 'Firmware management'. It displays a list of 'Firmware containers (2)'. The first container, 'dé uso gratuito', has two entries: 'SCALANCE XB200_XC200_XP200_XR300WG_XF200BA_V4.1' (Firmware version 4.1.0.0) and 'SCALANCE XB200_XC200_XP200_XR300WG_XF200BA_V4.2' (Firmware version 4.2.0.0). The second container, 'SCALANCE XB200_XC200_XP200_XR300WG_XF200BA_V4.2', is highlighted with a red border. The top right corner shows 'Capacity : 33.5 MB / 10 GB'.

3 Ingeniería

7. Seleccione el menú "Números de artículo". Seleccione el número de artículo de su dispositivo y asigne una "Versión de firmware de referencia". Haga clic en el botón "Editar etiquetas".

Figura 3-16

Article number	Device type	Available firmware versions	Latest firmware version	Reference firmware version
<input checked="" type="checkbox"/> 6GK5 208-0BA00-2AB2	SCALANCE XB208 PN (BA00-2AB2)	4.2.0.0, 4.1.0.0	4.2.0.0	4.1.0.0
<input type="checkbox"/> 6GK5 208-0BA00-2AC2	SCALANCE XC208 PN (BA00-2AC2)	4.1.0.0, 4.2.0.0	4.2.0.0	-
<input type="checkbox"/> 6GK5 208-0BA00-2FC2	SCALANCE XC208 PN EEC (BA00-2FC2)	4.1.0.0, 4.2.0.0	4.2.0.0	-
<input type="checkbox"/> 6GK5 208-0BA00-2TB2	SCALANCE XB208 (BA00-2TB2)	4.1.0.0, 4.2.0.0	4.2.0.0	-
<input type="checkbox"/> 6GK5 208-0GA00-2AC2	SCALANCE XC208 PN G (GA00-2AC2)	4.1.0.0, 4.2.0.0	4.2.0.0	-
<input type="checkbox"/> 6GK5 208-0GA00-2FC2	SCALANCE XC208 PN EEC (GA00-2...)	4.2.0.0, 4.1.0.0	4.2.0.0	-

8. Asigne un nombre a la "etiqueta". Haga clic en el botón "Aceptar".

Figura 3-17

Version 4.1.0.0	XB208 V4100
Version 4.2.0.0	XB208 V4200

Cancel OK

de uso gratuito

3 Ingeniería

9. Ahora ha configurado 4 parámetros con los que puede vincular la tarea "Cargar firmware en el dispositivo" con el contenedor de firmware. La siguiente sección le mostrará cómo crear una política con una tarea.

Figura 3-18

Tabla 3-2

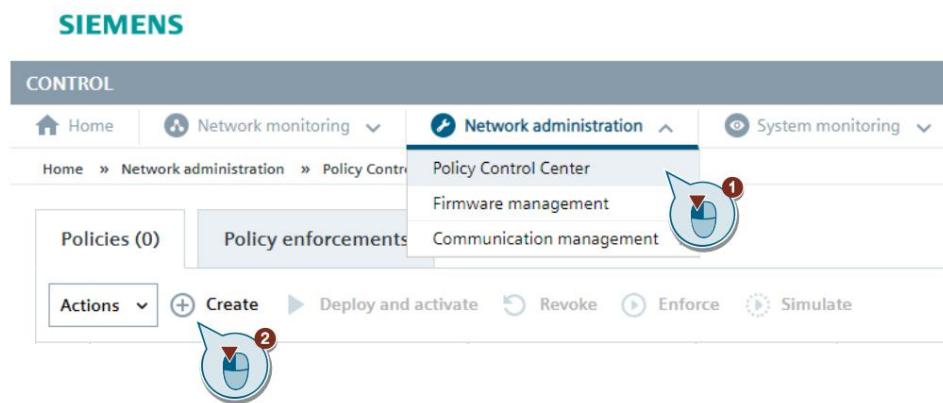
Parámetro	Ejemplo
Versión de firmware de referencia	4.1.0.0
Versión de firmware más reciente	4.2.0.0
Versiones de firmware disponibles	4.2.0.0 o 4.1.0.0
Firmware con etiqueta	XB208 V4100 o XB208 V4200

de uso gratuito

3.4**Creación de una política para la actualización de firmware**

1. El Centro de control de políticas está disponible en la página "Administración de red > Centro de control de políticas". Las políticas globales se pueden administrar y ejecutar en el Centro de control de políticas. Abra el Centro de control de políticas. Cree una nueva política haciendo clic en el botón "Crear".

Figura 3-19

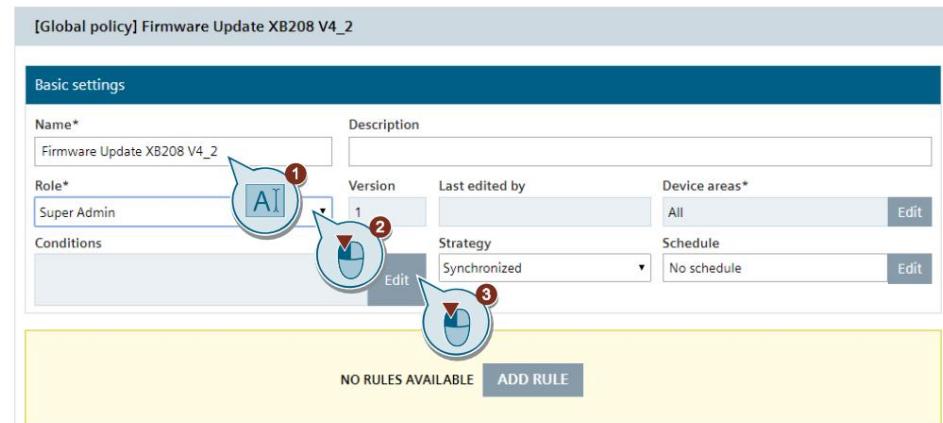


2. Defina un nombre para la política. Opcionalmente, puede ingresar una descripción de la política junto al nombre de la política.

Por ejemplo, seleccione su SuperAdmin como rol; esto fue creado durante la instalación. La función de política seleccionada determina qué usuarios pueden trabajar con esta función de política. Solo los usuarios que tienen la función de política seleccionada, o una función superior a la política, pueden acceder a la política. Los permisos fundamentales que tiene un usuario al acceder a las políticas se definen en la Gestión de permisos.

Haga clic en el botón "Editar" para definir una condición de dispositivo.

Figura 3-20

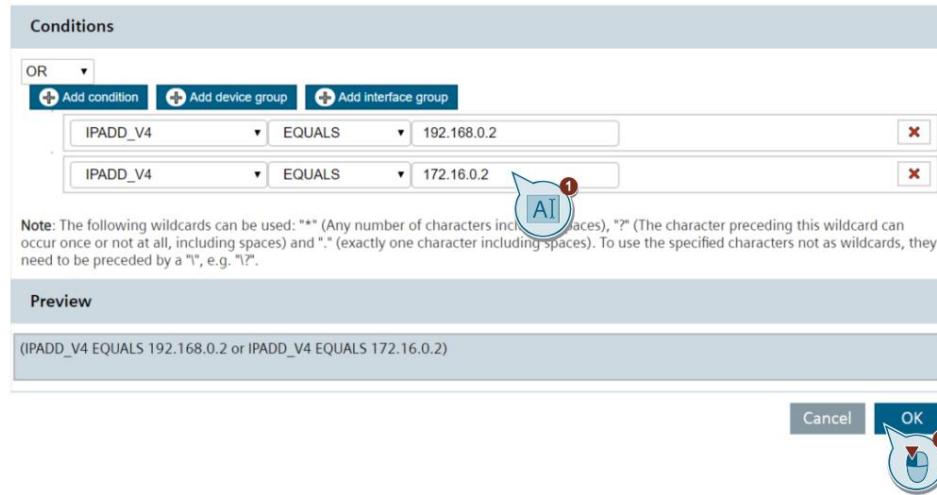


de uso gratuito

3 Ingeniería

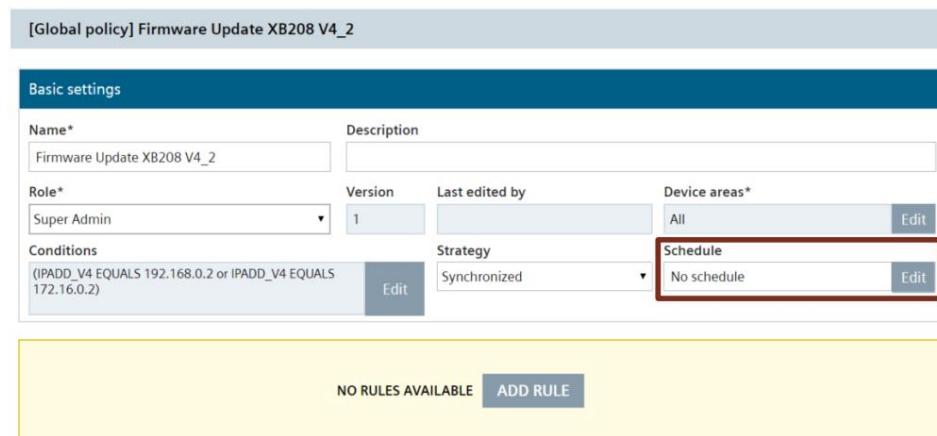
3. Aquí filtramos las condiciones por dirección IP del Scalance XB208. Puede encontrar información adicional sobre las condiciones individuales en las [Condiciones del dispositivo](#) sección.

Figura 3-21



4. En la pestaña "Programación", puede definir una programación (disparador). Si no lo hace configura un horario, la política solo se puede ejecutar manualmente usando la acción "Aplicar". Puede encontrar información adicional en el [Programa \(Disparador\)](#) sección.

Figura 3-22

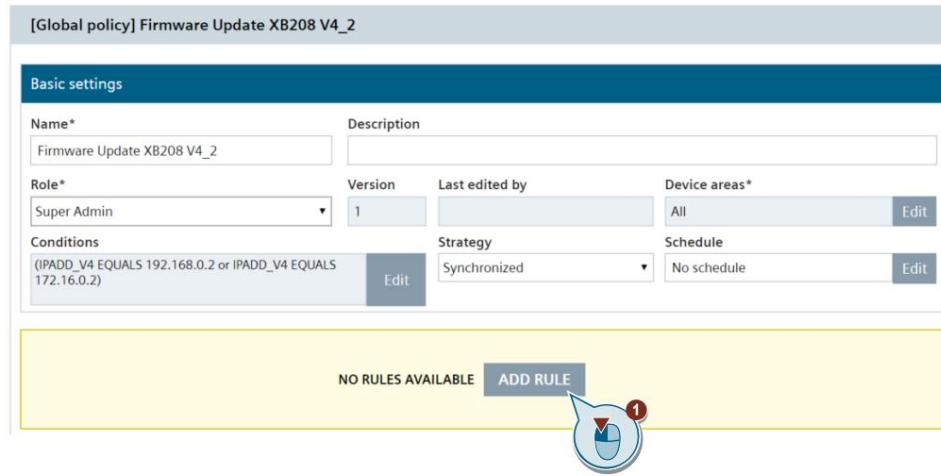


de uso gratuito

3 Ingeniería

5. Haga clic en el botón "Agregar regla".

Figura 3-23



6. Asigne un nombre de regla. Configure "Dispositivos" como el tipo de regla. Las tareas para dispositivos o las tareas para interfaces de dispositivos están disponibles según el tipo de regla seleccionado. Opcionalmente, puede ingresar una descripción de la regla junto al nombre de la regla. Haga clic en el botón "Aceptar".

Figura 3-24

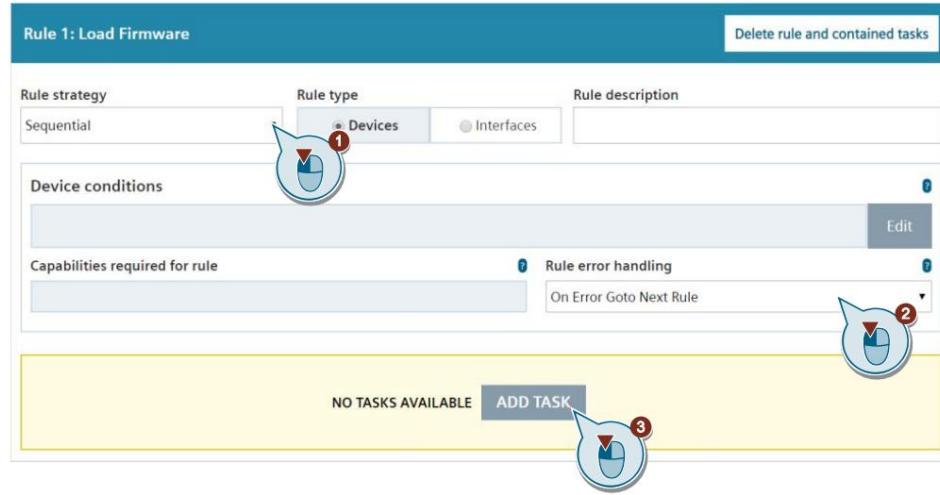


de uso gratuito

3 Ingeniería

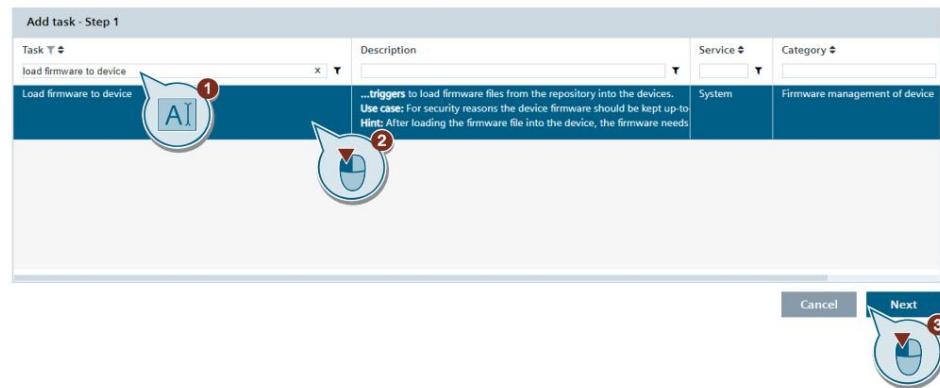
7. Seleccione una "estrategia de reglas". Defina una regla para el manejo de errores. Puede encontrar información detallada sobre este tema en la sección [Estrategias de políticas y manejo de errores](#).
Haga clic en el botón "Agregar tarea"

Figura 3-25



8. Seleccione la tarea "Cargar firmware en el dispositivo". Haga clic en el botón "Siguiente". Adicional
Se pueden agregar tareas si es necesario.

Figura 3-26



de uso gratuito

3 Ingeniería

9. La tarea "Cargar firmware en el dispositivo" tiene 6 parámetros.

Tabla 3-3

Parámetro	Explicación
Tiempo de espera de transferencia (s)	El tiempo de espera de transferencia es el período de tiempo que el dispositivo tiene disponible para ejecutar la política. Si la política no se ejecuta completamente dentro de este período de tiempo, la política devuelve un error. Si tiene una conexión lenta, se recomienda aumentar este período de tiempo.
Sobrescribir firmware	Siempre: el firmware siempre se carga en el dispositivo. Solo si es diferente: el firmware solo se carga cuando se cambia el dispositivo.
Usar firmware de referencia	La versión de firmware de referencia se selecciona desde la Gestión de firmware.
Utilice el firmware más reciente	La última versión de firmware se selecciona desde la Gestión de firmware.
Usar una versión de firmware específica	Se selecciona una versión de firmware específica desde la Gestión de firmware.
Usar firmware etiquetado con	El firmware con una etiqueta se selecciona desde la Gestión de firmware.

Figura 3-27

Edit parameters (Load firmware to device)-Step 2

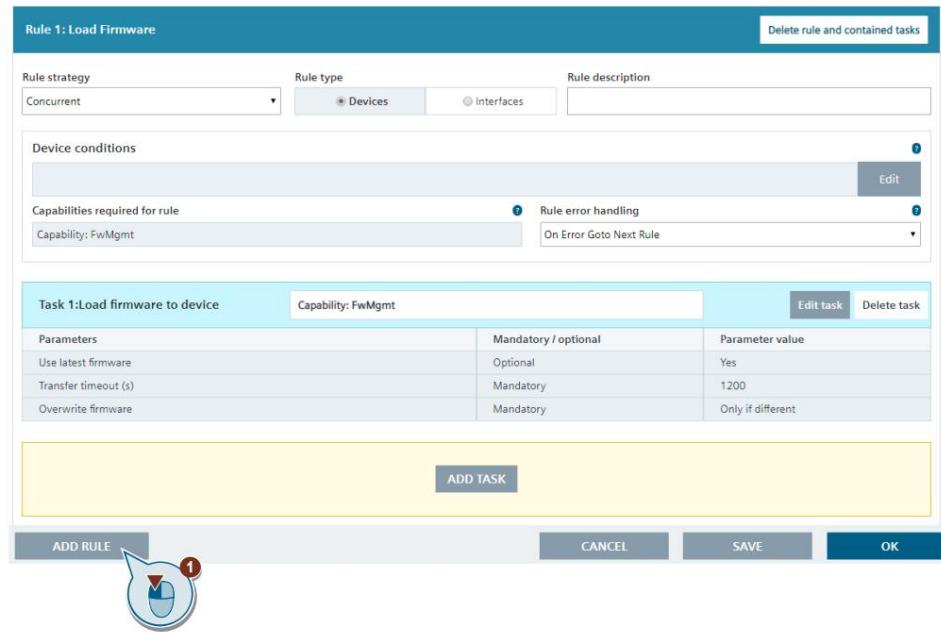
Parameter	Mandatory / optional	Parameter value	Default value
<input checked="" type="checkbox"/> Transfer timeout (s)	Mandatory	1200	1200
<input checked="" type="checkbox"/> Overwrite firmware	Mandatory	Only if different	Only if different
<input type="checkbox"/> Use reference firmware	Optional	--	
<input checked="" type="checkbox"/> Use latest firmware	Optional	Yes	Yes
<input type="checkbox"/> Use specific firmware version	Optional		
<input type="checkbox"/> Use firmware tagged with	Optional		

◀ Back Cancel OK

3 Ingeniería

10. Haga clic en el botón "Regla"

Figura 3-28



11. Asigne un nombre de regla. Configure "Dispositivos" como el tipo de regla. Las tareas para dispositivos o las tareas para interfaces de dispositivos están disponibles según el tipo de regla seleccionado. Opcionalmente, puede ingresar una descripción de la regla junto al nombre de la regla. Haga clic en el botón "Aceptar".

Figura 3-29

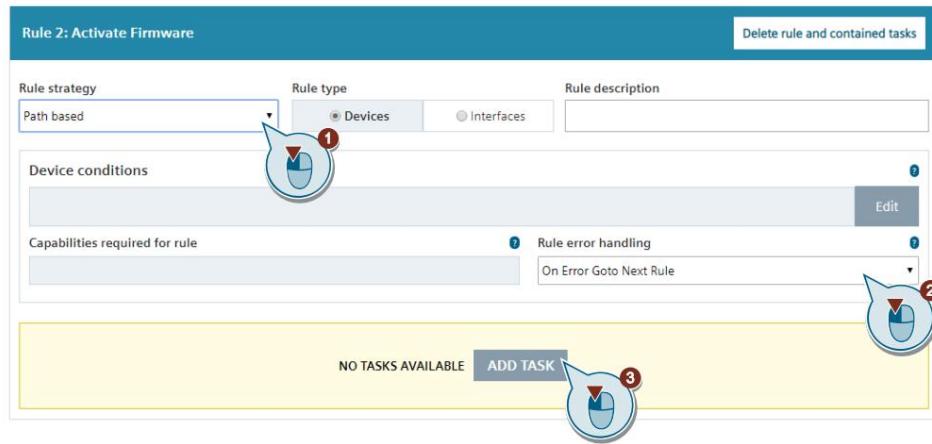


de uso gratuito

3 Ingeniería

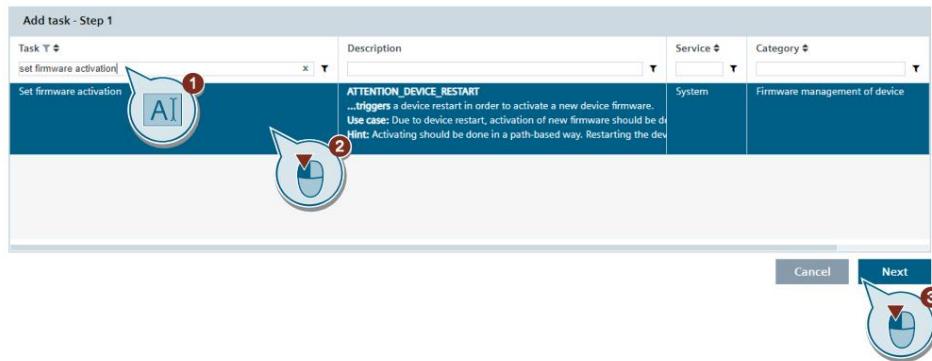
12. Seleccione una "estrategia de reglas". Defina una regla para el manejo de errores. Puede encontrar información detallada sobre este tema en la sección [Estrategias de políticas y manejo de errores](#). Haga clic en el botón "Agregar tarea"

Figura 3-30



13. Seleccione la tarea "Establecer activación de firmware". Haga clic en el botón "Siguiente". Se pueden agregar tareas adicionales si es necesario.

Figura 3-31

**Nota**

El dispositivo se reinicia después de la tarea "Establecer activación de firmware".

de uso gratuito

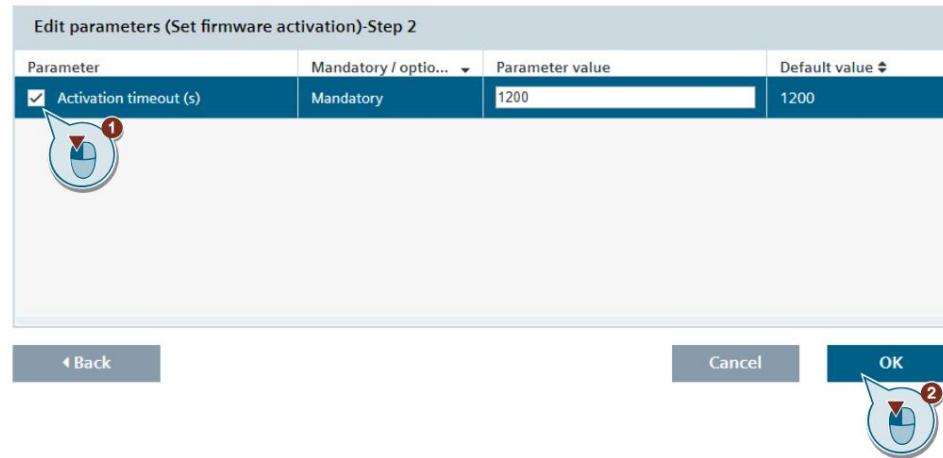
3 Ingeniería

14. La tarea "Establecer activación de firmware" tiene 1 parámetro.

Tabla 3-4

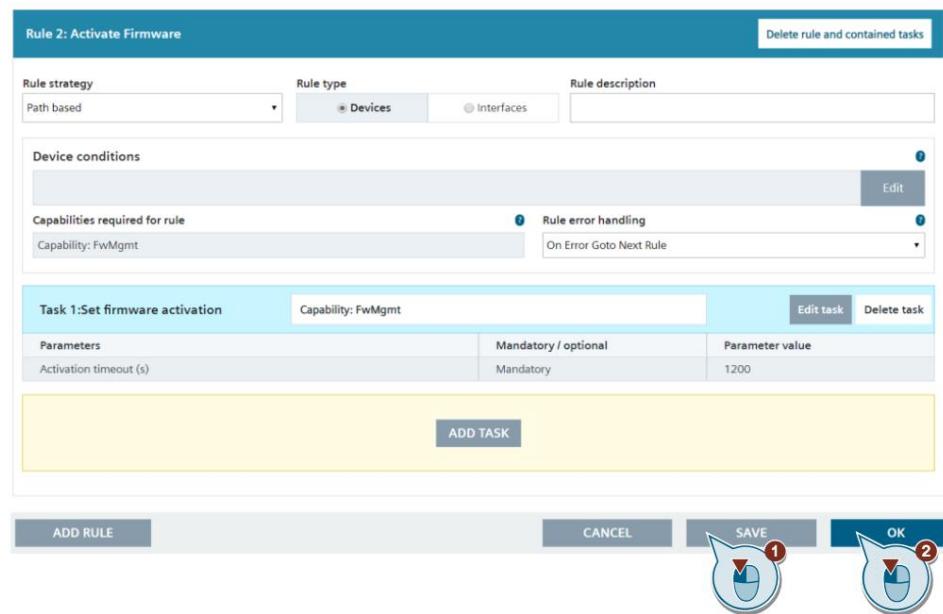
Parámetro	Explicación
Tiempo de espera de activación (s)	El tiempo de espera de activación es el tiempo que el dispositivo tiene disponible para activar el firmware.

Figura 3-32



15. Haga clic en los botones "Guardar" y "Aceptar".

Figura 3-33



de uso gratuito

3 Ingeniería

16. La política ahora debe implementarse y activarse en la Operación antes de que pueda ejecutarse o simularse allí. Haga clic en el botón "Implementar y activar". La política se establece en el estado "Activado". En este estado, la política se puede ejecutar según un cronograma configurado o manualmente.

Figura 3-34

Name	State	Deployed	Consistent
Firmware Update XB208 V4_2	Ready to deploy	NO	YES

17. Haga clic en el botón "Simular". La política seleccionada luego produce un informe de simulación. Los informes de simulación le permiten predecir el resultado de la aplicación de políticas sin tener que aplicar la política en sí. Los informes de simulación indican qué tarea se aplica a qué dispositivo o interfaz. Solo se pueden simular políticas que se encuentran en el estado "Activado".

Nota

Debe haber al menos 1 minuto entre el inicio de las simulaciones de políticas.

Figura 3-35

Name	State	Deployed	Consistent	Enforcement state	Last enforcement steps	Simulated version
Firmware Update XB208 V4_2	Activated	YES	YES	-	-	-

de uso gratuito

3 Ingeniería

18. Haga clic en "Informe de simulación".

Figura 3-36

Name	State	Deployed	Consistent	Last enforcement state	Last enforcement steps	Simulated version
Firmware Update XB208 V4_2	Activated	YES	YES	-	-	2 (07/13/2020 17:19)

19. Se abre el informe de simulación. La sección "General" contiene un resumen de las propiedades de la política configurada, la hora en que se simuló la política y la cantidad de dispositivos a los que se aplicó la política.

Figura 3-37

General - Simulation report

Name:	Firmware Update XB208 V4_2
Description:	
Role:	Super Admin
Last edited by:	SuperAdmin 07/13/2020 17:15:23
Number of rules:	2
Version:	2
Enforced by:	SuperAdmin
Strategy:	Synchronized
Simulated on:	07/13/2020 17:19
Affected devices:	2
Affected devices per rule:	Load Firmware: Affected devices: 2 , Tasks: 1 , Enforcement steps: 2 Activate Firmware: Affected devices: 2 , Tasks: 1 , Enforcement steps: 2
General information:	--
Display policy configuration	
de uso gratuito	

3 Ingeniería

La sección "Informe de simulación" muestra los resultados del informe de simulación.

Figura 3-38

Simulation report - WIN10Blank									
Name:	Load Firmware								
Rule:	1								
Description:									
Rule type:	Device Rule								
Summary:	Number of Matching Devices : 2								
Conditions:	Conditions: (IPADD_V4 EQUALS 192.168.0.2 or IPADD_V4 EQUALS 172.16.0.2) Required capabilities: FwMgmt								
Rule strategy:	Sequential								
Rule error handling:	On Error Goto Next Rule								
Device	Device type	Enforcement order	Port	Task	Parameters	Value			
SCALANCE XB208 / 172.16.0.2	SCALANCE XB208 PN (DBA00-2AB2)	1	-	Load firmware to device	Use latest firmware Transfer timeout (s) 2400 Overwrite firmware Only if different Server address 10.0.1.4 Server port 69 File name FW0111Firmware_XB-200_XC-200_XP-200_XR-300WG_XF200SA_V04.02.00_00_06.01.56.sfw	Yes			
SCALANCE XB208 / 192.168.0.2	SCALANCE XB208 PN (DBA00-2AB2)	2	-	Load firmware to device	Use latest firmware Transfer timeout (s) 2400 Overwrite firmware Only if different Server address 10.0.1.4 Server port 69 File name FW0111Firmware_XB-200_XC-200_XP-200_XR-300WG_XF200SA_V04.02.00_00_06.01.56.sfw	Yes			
Name:	Activate Firmware								
Rule:	2								
Description:									
Rule type:	Device Rule								
Summary:	Number of Matching Devices : 2								
Conditions:	Conditions: (IPADD_V4 EQUALS 192.168.0.2 or IPADD_V4 EQUALS 172.16.0.2) Required capabilities: FwMgmt								
Rule strategy:	Path based								
Rule error handling:	On Error Goto Next Rule								
Device	Device type	Enforcement order	Port	Task	Parameters	Value			
SCALANCE XB208 / 172.16.0.2	SCALANCE XB208 PN (DBA00-2AB2)	1	-	Set firmware activation	Activation timeout (s) 2400				
SCALANCE XB208 / 192.168.0.2	SCALANCE XB208 PN (DBA00-2AB2)	2	-	Set firmware activation	Activation timeout (s) 2400				

de uso gratuito

3 Ingeniería

20. Haga clic en el botón "Aplicar". La política se inicia manualmente y se establece en el Estado "Activado".

Nota

Debe permitir al menos 1 minuto entre el inicio de la implementación de políticas.

Figura 3-39

Name	State	Deployed	Consistent	Last enforcement state	Last enforcement steps
Firmware Update XB208 V4_2	Activated	YES	YES	-	-

21. Verifique la aplicación. La política se ha aplicado con éxito.

Figura 3-40

Name	State	Deployed	Consistent	Last enforcement state	Last enforcement steps
Firmware Update XB208 V4_2	Activated	YES	YES	Success	4(0/100)

de uso gratuito

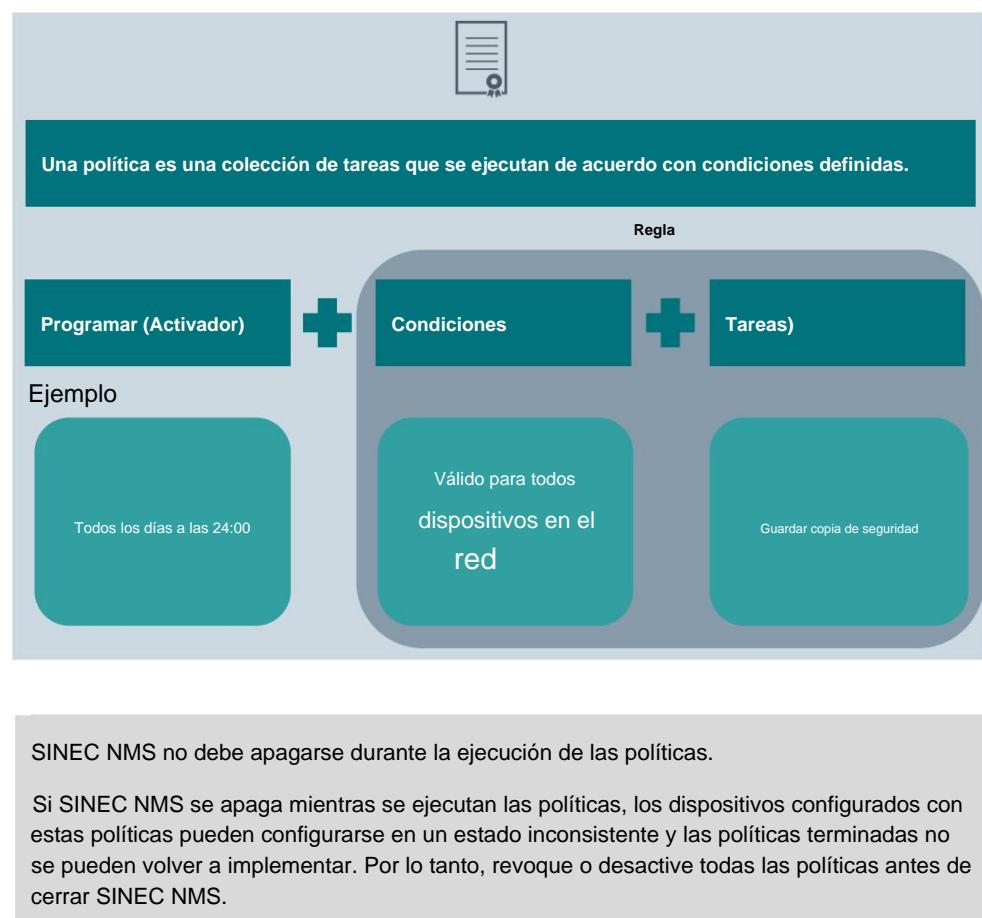
4 Información útil

4 Información útil

4.1 Política

Una política se puede utilizar para planificar y realizar tareas para configurar y administrar dispositivos. Los dispositivos y tareas de una política se pueden combinar libremente dentro del alcance de los permisos existentes. El rango de dispositivos que se pueden configurar está determinado por las condiciones. Las políticas se pueden implementar de forma programada o manualmente. Antes de ejecutar una política, SINEC NMS utiliza las funciones disponibles del dispositivo para determinar qué tareas se pueden ejecutar en qué dispositivos. Usando simulaciones de políticas, esta información se puede determinar sin tener que ejecutar la política.

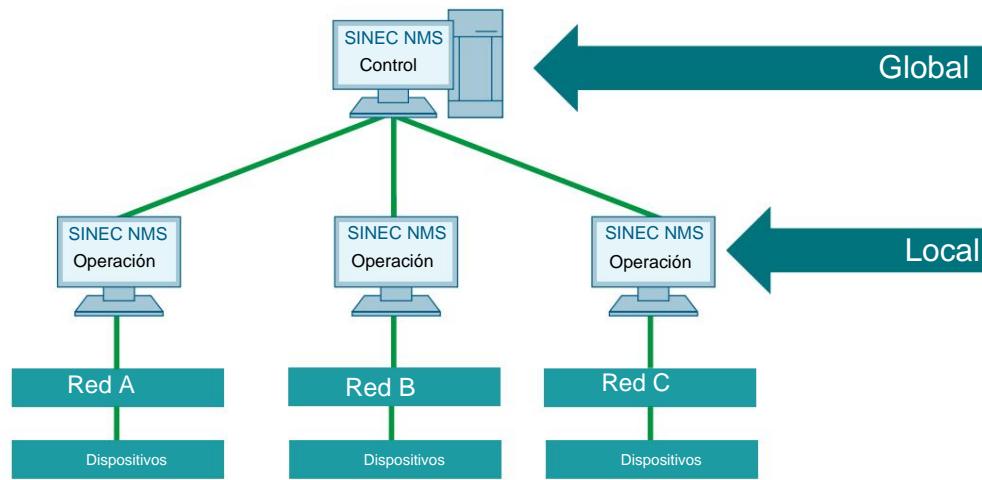
Figura 4-1



4 Información útil

4.1.1 Configuración basada en reglas globales o locales

Figura 4-2



Las políticas globales se configuran en el Control, luego se implementan en todas las Operaciones involucradas y luego se ejecutan en estas Operaciones. Las políticas globales son visibles en el Control y en las Operaciones involucradas.

Las políticas locales se configuran directamente en las Operaciones sobre las que se van a ejecutar. Las políticas locales solo son visibles en su operación asociada, esto también se aplica a las instalaciones de un solo nodo.

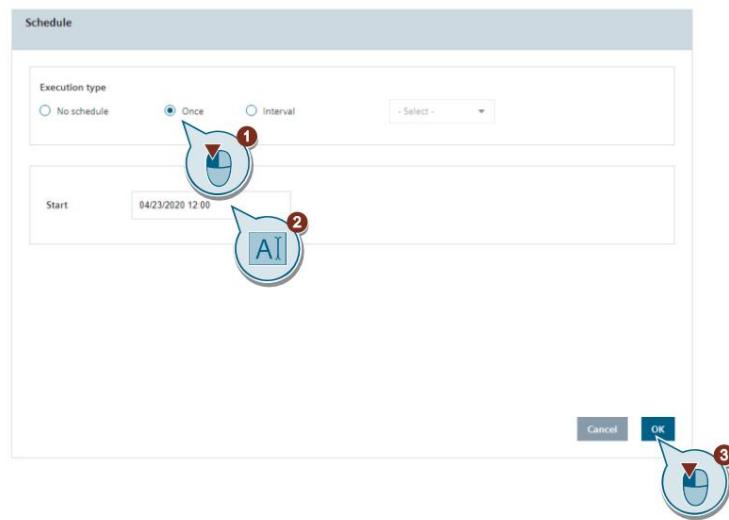
Irrestricto

4.2 Programar (Activador)

Disparador de una sola vez

Puede ejecutar una política una vez en un día específico a una hora específica. Seleccione "Una vez" como tipo de ejecución. Especifique una fecha y hora. Haga clic en el botón "Aceptar".

Figura 4-3



Periodo de tiempo

Puede ejecutar una política varias veces durante un período de tiempo. Seleccione "Intervalo" como tipo de ejecución. Seleccione los minutos, horas, días, semanas, meses o años como unidad de tiempo. Introduzca la frecuencia con la que se puede repetir una unidad de tiempo. Especifique una hora de inicio. Hay varias opciones disponibles para la hora de finalización:

- Puede ingresar una hora de finalización definida en el campo de entrada.

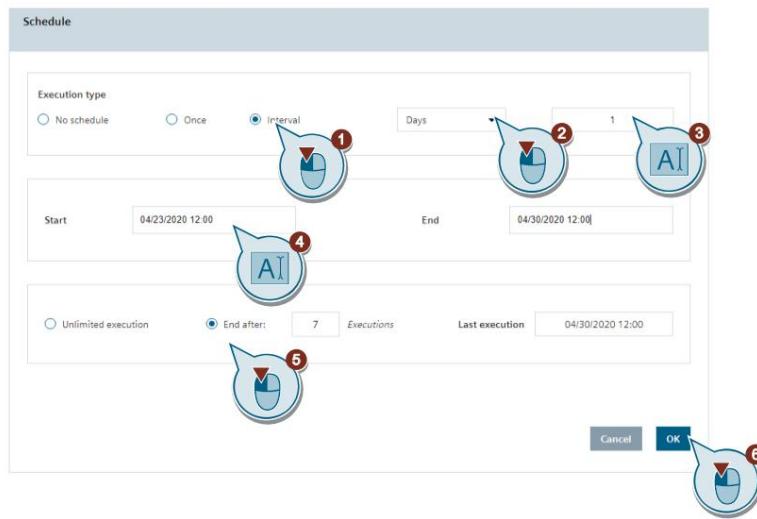
- Puede hacer cumplir la política indefinidamente.
- O la política finaliza después de n ejecuciones.

Haga clic en el botón "Aceptar".

de uso gratuito

4 Información útil

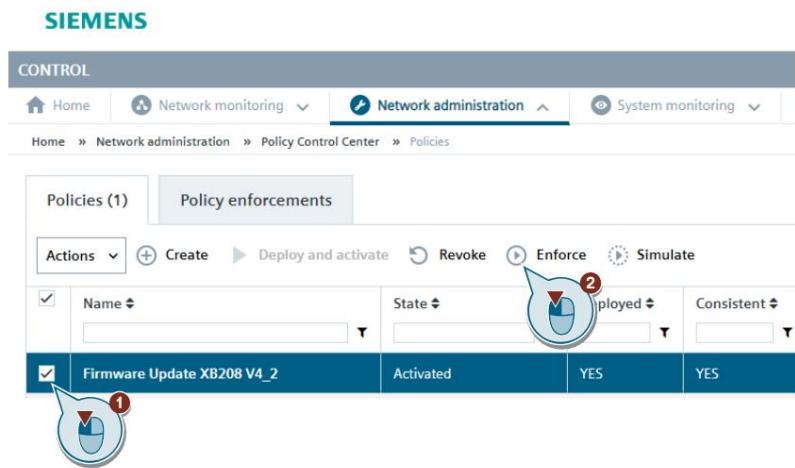
Figura 4-4



Gatillo manual

También puede iniciar una política manualmente una vez que se implementa y activa. Haga clic en el botón "Aplicar" para la activación manual.

Figura 4-5



de uso gratuito

4.3 Condiciones del dispositivo

Con las condiciones de la política, puede seleccionar dispositivos de las áreas de dispositivos configurados en función de propiedades como direcciones IP o números de artículo.

Se pueden buscar las siguientes condiciones del dispositivo:

- IPADD_V4
- IPADD_V6 •
- UBICACIÓN_SISTEMA •
- NOMBRE_PROFNET •
- NOMBRE_SISTEMA •
- NÚMERO_DE_ARTÍCULO •
- VERSIÓN_DE_FIRMWARE •
- VERSIÓN_DE_HARDWARE •
- PERSONA_DE_CONTACTO •
- NÚMERO_DE_SERIE •
- NOMBRE_DE_OPERACIÓN •
- IPV4_CIDR • TOTAL_PUERTOS •
- IPADD_EXTERNO •
- CATEGORÍA_DISPOSITIVO •
- TIPO_DISPOSITIVO

A continuación se muestran ejemplos de cómo utilizar las condiciones del dispositivo.

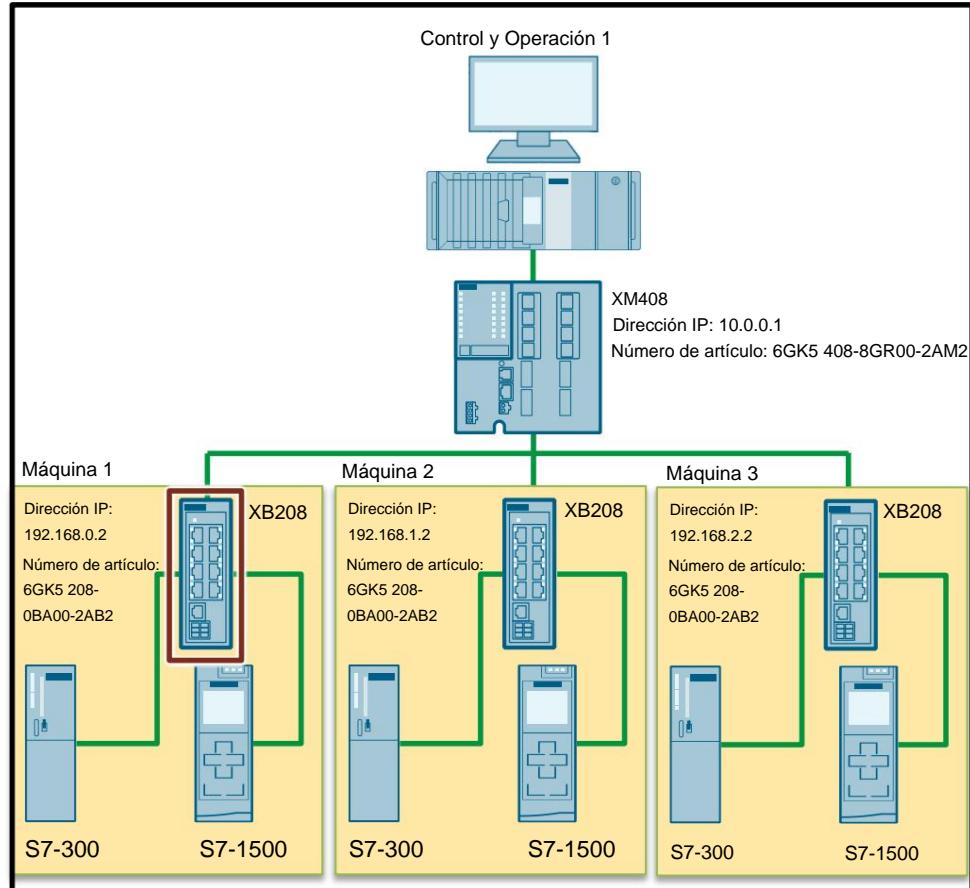
4 Información útil

4.3.1 Copia de seguridad de dispositivos individuales

Para la copia de seguridad de dispositivos individuales, se recomienda la siguiente condición: • IPADD_V4 EQUALS 192.168.0.2

Figura 4-6

Piso 1



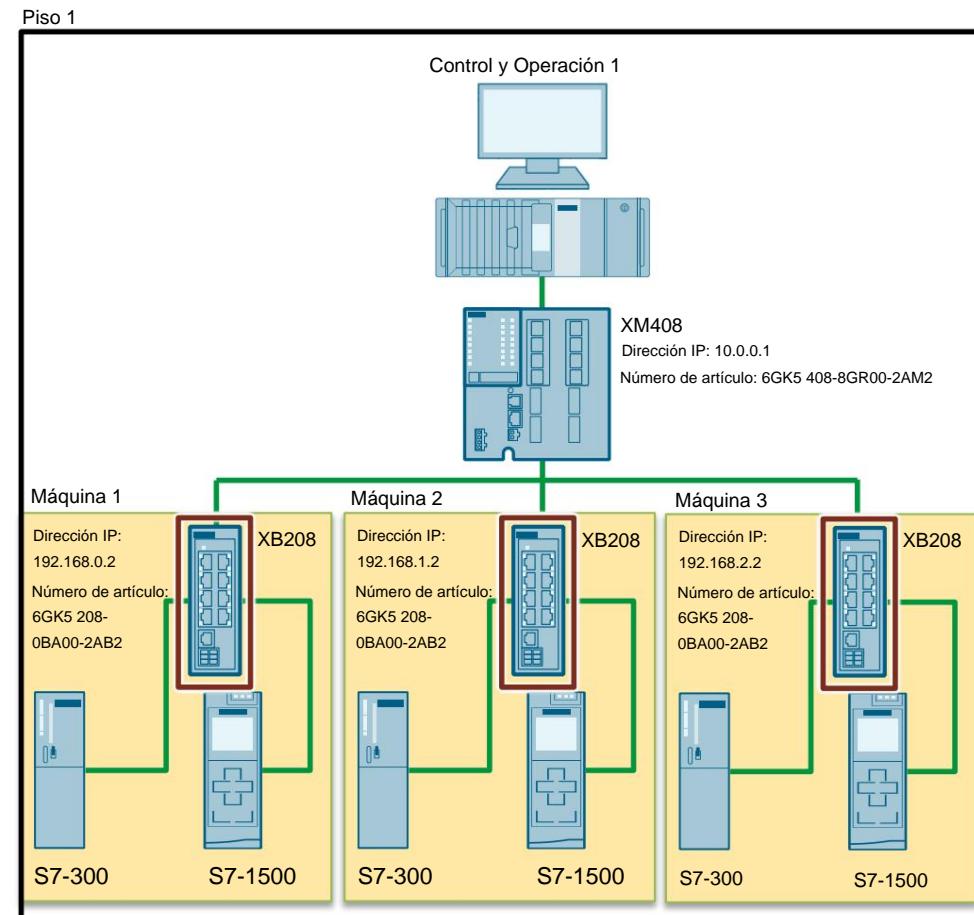
Irrestricto

4 Información útil

4.3.2 Copia de seguridad de dispositivos del mismo tipo

- NÚMERO_DE_ARTÍCULO IGUAL A 6GK5 208-0BA00-2AB2 O por la combinación de diferentes condiciones del dispositivo:
- IPADD_V4 IGUAL A 192.168.0.2 o IPADD_V4 IGUAL A 192.168.1.2 o IPADD_V4 IGUAL A 192.168.2.2

Figura 4-7



Irrestricto

4 Información útil

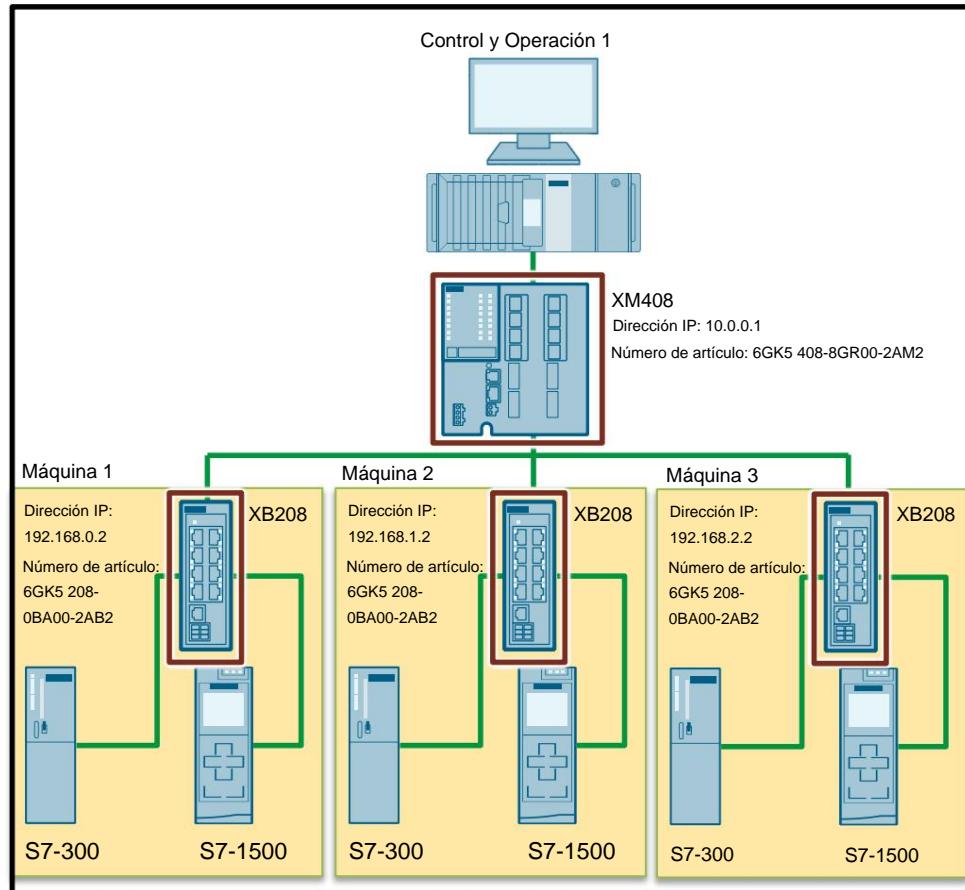
4.3.3

Copia de seguridad de varios dispositivos en el área de dispositivos

Se pueden almacenar varios dispositivos en un área de dispositivos. Esto ahorra tiempo al configurar varias políticas en la misma área de dispositivos. En la página "Administración del sistema > Áreas de dispositivos", se pueden crear o eliminar áreas de dispositivos y se pueden especificar las operaciones y las condiciones del dispositivo de un área de dispositivo.

Figura 4-8

Piso 1



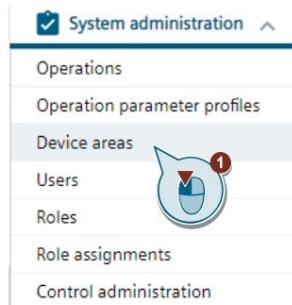
Irrestricto

4 Información útil

Configuración

1. En el Control, abra la página "Administración del sistema > Áreas de dispositivos".

Figura 4-9



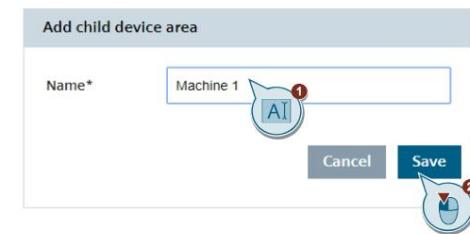
2. Haga clic en el botón "Añadir área de dispositivos secundaria".

Figura 4-10



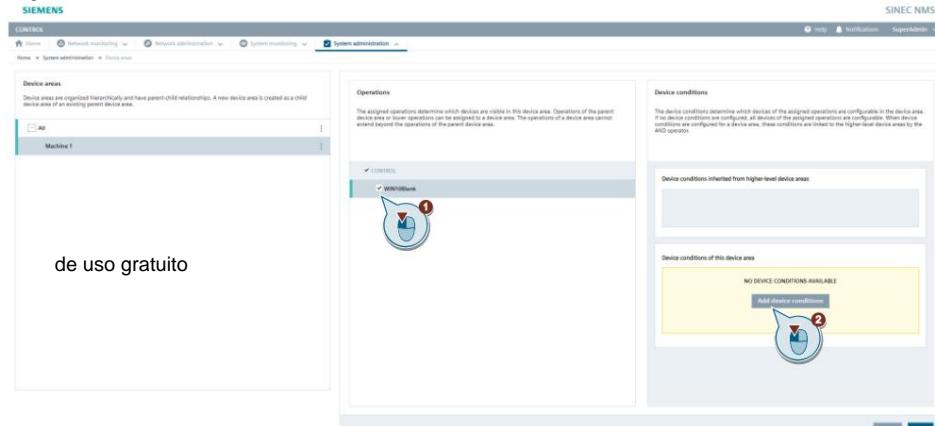
3. Asigne un nombre al área del dispositivo.

Figura 4-11



4. Seleccione la Operación a la que se aplicará el área del dispositivo. Haga clic en "Añadir estado del dispositivo".

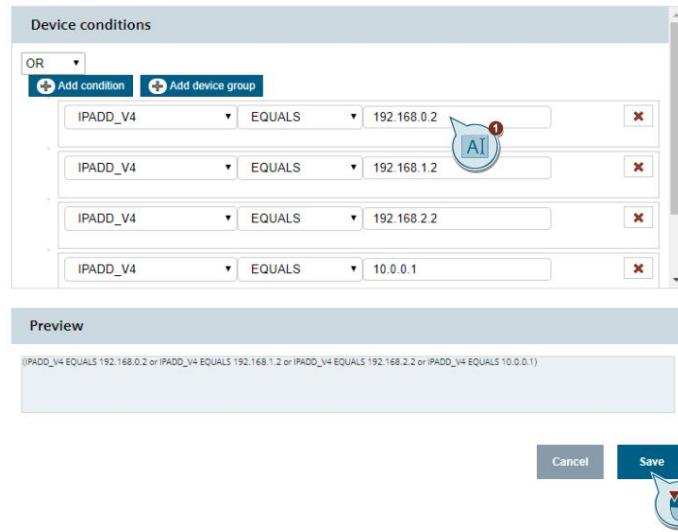
Figura 4-12



4 Información útil

5. Cree una condición de dispositivo. Haga clic en el botón "Guardar".

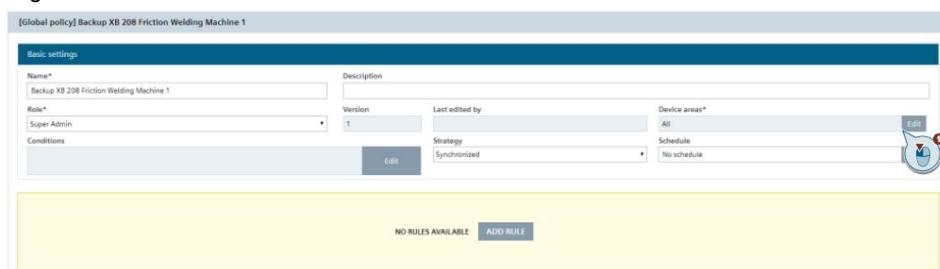
Figura 4-13



6. Haga clic en el botón "Guardar" en el área del dispositivo.

7. Seleccione el área del dispositivo en la política.

Figura 4-14



8. Seleccione el área del dispositivo creado.

Figura 4-15



4.3.4 comodines

Los comodines se pueden utilizar en algunas condiciones. Cuando está permitido, se pueden utilizar los siguientes comodines:

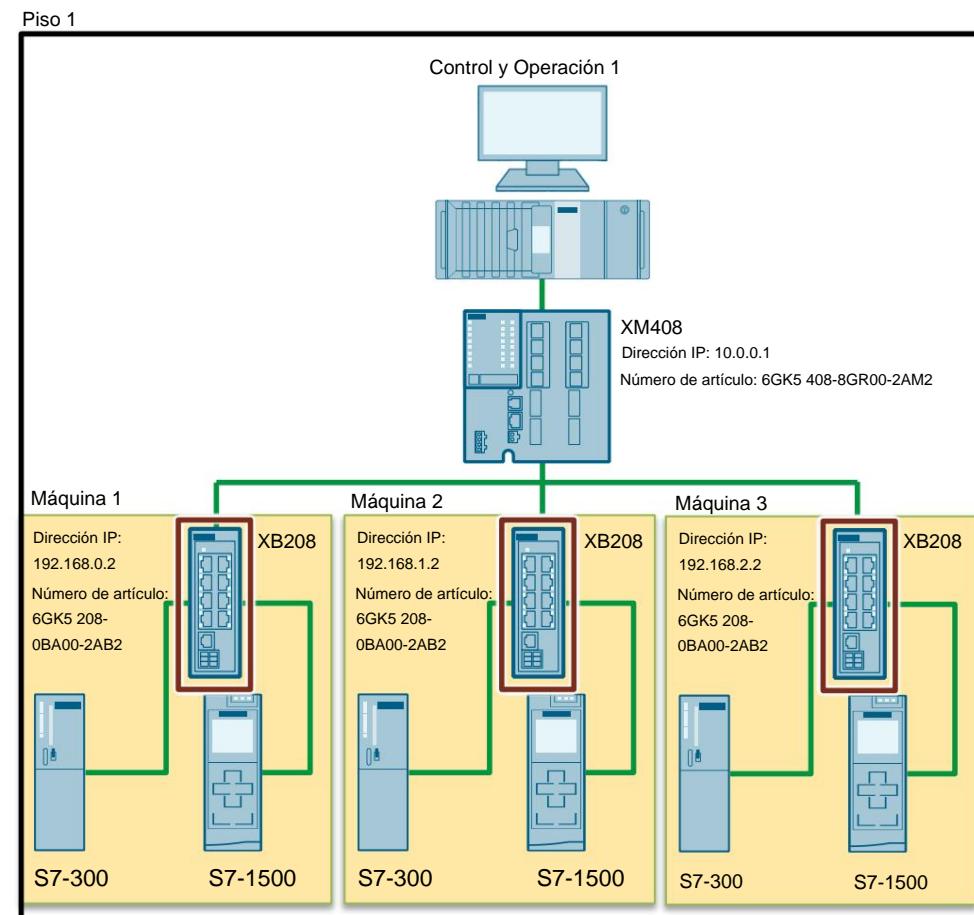
- * (Cualquier número de caracteres, incluidos los espacios en blanco)
- ? (El carácter que precede a este comodín no puede aparecer o solo puede aparecer una vez, incluidos los espacios en blanco)
- . (Exactamente un carácter, incluidos los espacios en blanco)

Para evitar que estos caracteres se utilicen como comodines, deben seguir a "\", por ejemplo, "\?".

Ejemplo:

IPV4_CIDR IGUAL A 192.168.1.1/16: Los dispositivos e interfaces cuyas direcciones IP comienzan con 192.168 cumplen con las condiciones de la política.

Figura 4-16



4 Información útil

4.4 Estrategias de políticas y manejo de errores

4.4.1 Estrategias de política

La estrategia de política determina el orden en que se aplica la regla a los dispositivos. Se puede seleccionar una de las siguientes estrategias de política para una política.

Figura 4-17



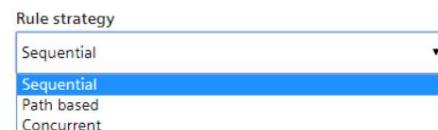
no sincronizado

La política se ejecuta simultáneamente para todos los dispositivos en la Operación. Una vez que se hayan ejecutado todas las tareas de una regla para un dispositivo, el dispositivo ejecutará la siguiente regla. Esta estrategia puede acortar el tiempo de ejecución de la política, pero, según las tareas específicas, la funcionalidad de la red puede verse afectada temporalmente. Este es el caso, por ejemplo, si la actualización del firmware de un interruptor se realiza en un momento inoportuno y el dispositivo debe reiniciarse posteriormente.

sincronizado

Solo después de que se haya ejecutado una regla para todos los dispositivos en la operación, la aplicación de la política continúa con la siguiente regla.

Figura 4-18



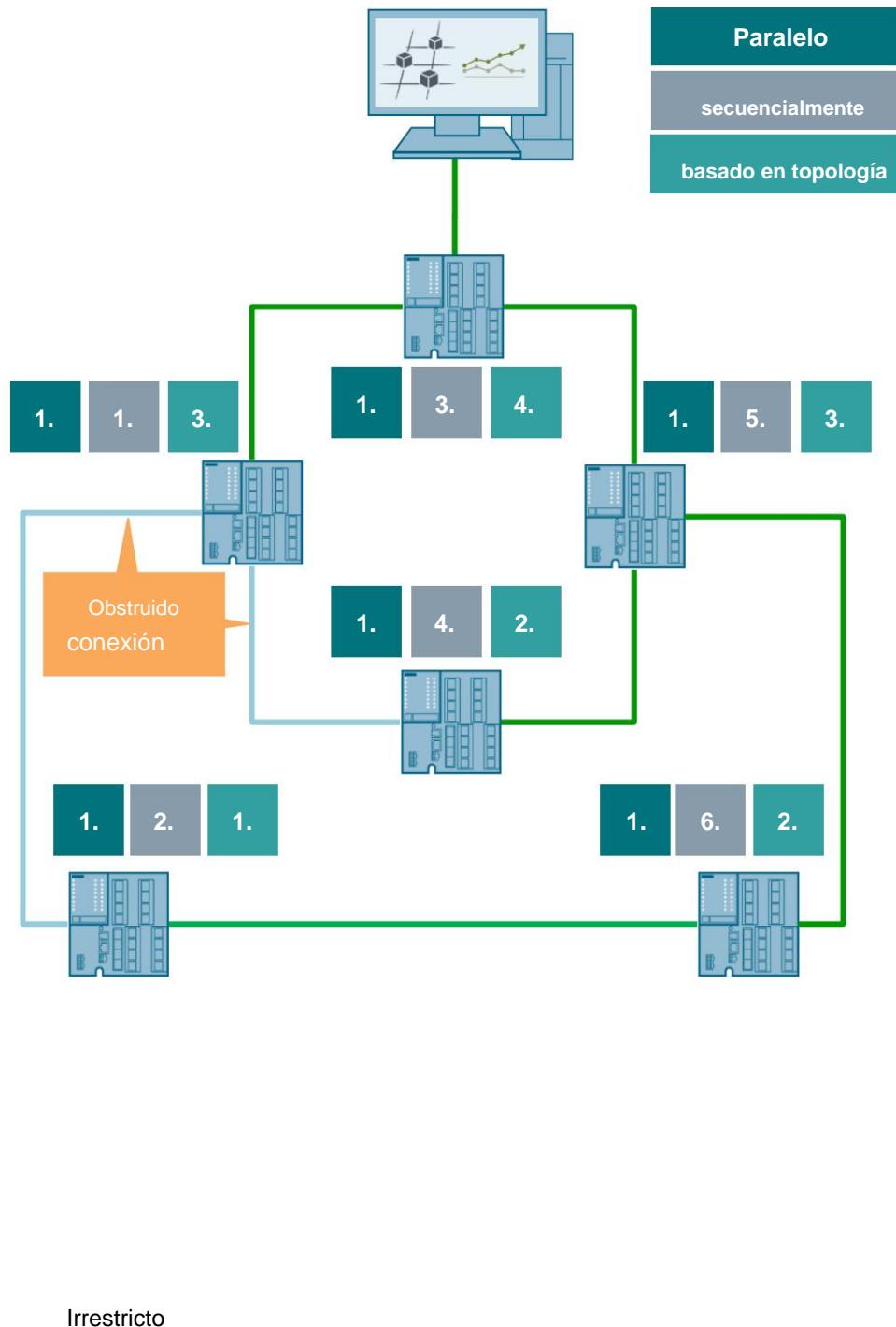
- **Secuencialmente:** la regla se aplica a los dispositivos afectados uno tras otro
- **Paralelo:** la regla se aplica simultáneamente a los dispositivos relevantes.
- **Basado en topología:** la regla se aplica a los dispositivos relevantes en el orden en que los dispositivos están dispuestos en la topología. Los dispositivos que están a más saltos de la operación se procesan antes que los dispositivos que están a menos saltos de la operación. Los dispositivos a la misma distancia de la Operación se procesan simultáneamente (en paralelo). Para usar esta opción, la topología de referencia se debe crear en la operación y la operación debe tener una conexión a la red en la topología.

de uso gratuito

4 Información útil**Ejemplo**

El siguiente ejemplo muestra cómo el procesamiento de estrategias de políticas puede ser paralelo, secuencial o basado en topología.

Figura 4-19



4 Información útil

4.4.2 Manejo de errores de reglas

Dentro de cada regla, las estrategias de manejo de errores de reglas definen el comportamiento en caso de un error de ejecución.

Figura 4-20



1. En caso de error: Terminar la ejecución de la política en el dispositivo

La ejecución de la política finaliza después de que surge el error.

2. En caso de error: Ir a la regla siguiente

La ejecución de la política continúa con la siguiente regla para este dispositivo. Otras tareas para la regla en la que ocurrió el error ya no se procesan para el dispositivo.

3. En caso de error: continuar con la siguiente ejecución para el dispositivo

La ejecución de la política continúa con la siguiente tarea para este dispositivo. Si no hay otra tarea en la regla, la aplicación de la política continúa con la siguiente tarea.

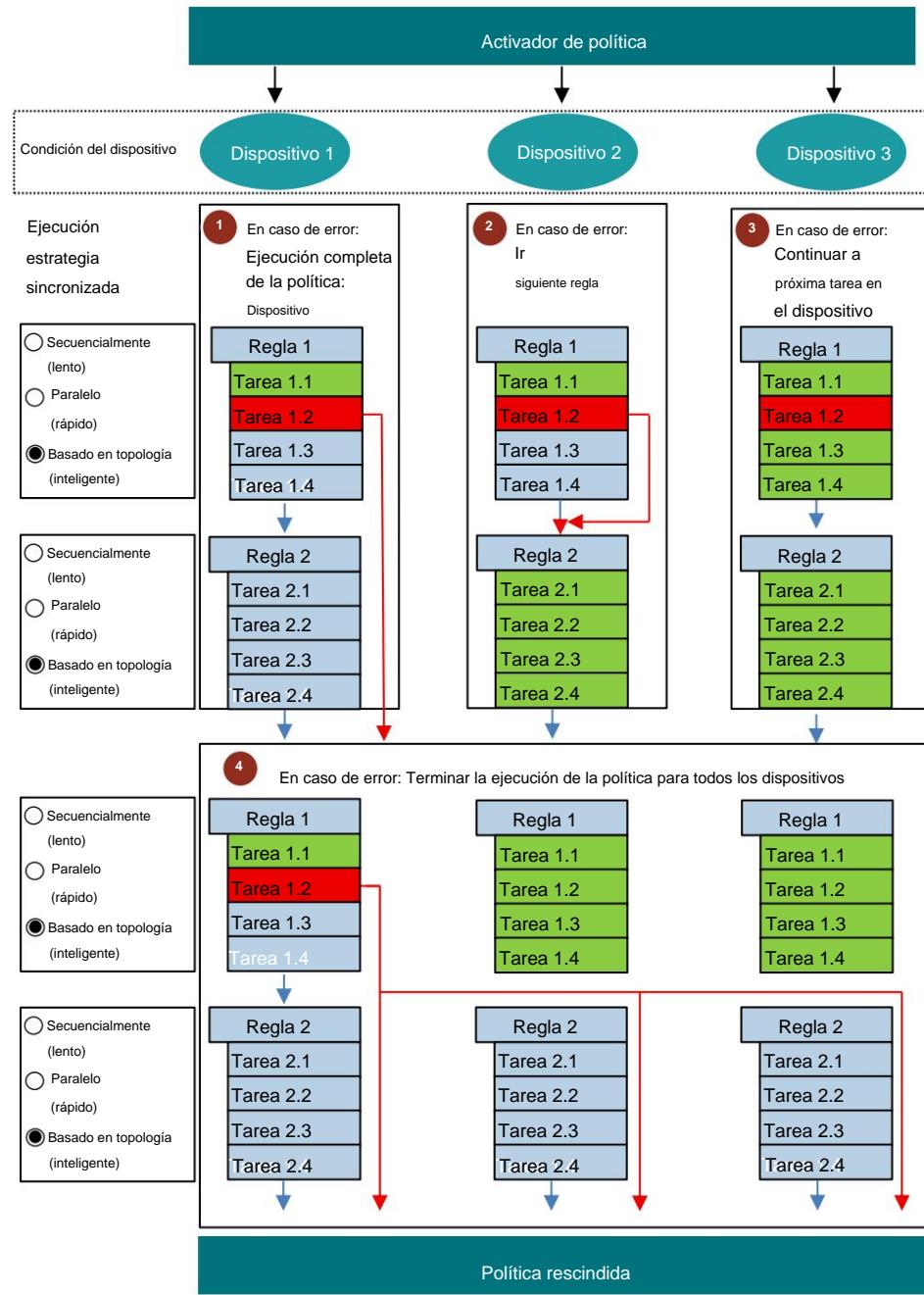
4. En caso de error: Terminar la ejecución de la política para todos los dispositivos

La ejecución de la política finaliza para el dispositivo en el que se produjo el error después de la tarea afectada. Para todos los demás dispositivos en la Operación, la política finaliza después de que se ejecuta la regla.

de uso gratuito

4 Información útil

Figura 4-21



Irrestricto

4 Información útil

4.5 Tareas**Nota**

Las tareas disponibles dependen del rol de política configurado y del tipo de regla seleccionado.

4.5.1 Tarea: Establecer servidor SSH

Además de los datos de inicio de sesión SSH, SINEC NMS requiere acceso al servidor SSH de los dispositivos respectivos. Puede activarlos fácilmente con la tarea de política "Establecer servidor SSH".

Figura 4-22

The screenshot shows the 'Add task - Step 1' dialog. In the 'Task' field, 'set ssh server' is selected. The 'Description' field contains the note: "...defines if the device can be accessed via encrypted CLI. Use case: CLI is a common interface in order to manage network devices. Hint: SINEC NMS needs to have this secure access in order to perform device management tasks." The 'Service' dropdown is set to 'System', 'Category' to 'SSH server configuration', and 'Capability' to 'SSH'.

Parámetro

Figura 4-23

The screenshot shows the 'Edit parameters (Set SSH server)-Step 2' dialog. The 'Parameter' column lists 'Enable'. The 'Mandatory / optional' dropdown shows 'Mandatory'. The 'Parameter value' dropdown shows 'Yes'. The 'Default value' dropdown also shows 'Yes'.

Tabla 4-1

Parámetro	Explicación
Permitir	Sí: habilita la propiedad del dispositivo del servidor SSH. No: deshabilita la propiedad del dispositivo del servidor SSH.

4 Información útil

4.5.2 Tarea: Cargar firmware en el dispositivo

Puede transferir un archivo de firmware a un dispositivo con la tarea de política "Cargar firmware en el dispositivo".

Figura 4-24

Add task - Step 1			
Task	Description	Service	Category
load firmware to device			
Load firmware to device	...triggers to load firmware files from the repository into the devices. Use case: For security reasons the device firmware should be kept up-to-date. Hint: After loading the firmware file into the device, the firmware needs	System	Firmware management of device

Parámetro

Figura 4-25

Parameter	Mandatory / optional	Parameter value	Default value
<input checked="" type="checkbox"/> Transfer timeout (s)	Mandatory	1200	1200
<input checked="" type="checkbox"/> Overwrite firmware	Mandatory	Only if different	Only if different
<input type="checkbox"/> Use reference firmware	Optional	--	
<input checked="" type="checkbox"/> Use latest firmware	Optional	Yes	Yes
<input type="checkbox"/> Use specific firmware version	Optional		
<input type="checkbox"/> Use firmware tagged with	Optional		

Tabla 4-2

Parámetro	Explicación
Tiempo de espera de transferencia (s)	El tiempo de espera de transferencia es el período de tiempo que el dispositivo tiene disponible para ejecutar la política. Si la política no se ejecuta completamente dentro de este período de tiempo, la política devuelve un error. Si tiene una conexión lenta, se recomienda aumentar este período de tiempo.
Sobrescribir firmware	Siempre: el firmware siempre se carga en el dispositivo. Solo si es diferente: el firmware solo se carga cuando se cambia el dispositivo.
Usar firmware de referencia	La versión de firmware de referencia se selecciona desde la Gestión de firmware.
Utilice el firmware más reciente	La última versión de firmware se selecciona desde la Gestión de firmware.
Usar una versión de firmware específica	Se selecciona una versión de firmware específica desde la Gestión de firmware.
Usar firmware etiquetado con	El firmware con una etiqueta se selecciona desde la Gestión de firmware.

de uso gratuito

de uso gratuito

4 Información útil

4.5.3

Tarea: Tiempo de espera de activación

Puede utilizar la tarea de política "Tiempo de espera de activación" para activar un archivo de firmware en un dispositivo.

Figura 4-26

Add task - Step 1			
Task	Description	Service	Category
set firmware activation	ATTENTION_DEVICE_RESTART ...triggers a device restart in order to activate a new device firmware. Use case: Due to device restart, activation of new firmware should be done in a path-based way. Hint: Activating should be done in a path-based way. Restarting the dev	System	Firmware management of device

Parámetro

Figura 4-27

Edit parameters (Set firmware activation)-Step 2			
Parameter	Mandatory / option...	Parameter value	Default value
<input checked="" type="checkbox"/> Activation timeout (s)	Mandatory	1200	1200

Tabla 4-3

Parámetro	Explicación
Tiempo de espera de activación (s)	El tiempo de espera de activación es el tiempo que el dispositivo tiene disponible para activar el firmware.

de uso gratuito

5 Apéndice

5 Apéndice

5.1 Servicio y soporte

Soporte en línea de la industria

¿Tiene alguna pregunta o necesita ayuda?

Siemens Industry Online Support ofrece acceso las 24 horas a todo nuestro servicio, soporte y conocimientos técnicos y cartera.

Industry Online Support es la dirección central para obtener información sobre nuestros productos, soluciones y servicios.

Información de productos, manuales, descargas, preguntas frecuentes, ejemplos de aplicación y videos: toda la información está accesible con unos pocos clics del ratón: <https://support.industry.siemens.com>

Apoyo técnico

El Soporte técnico de Siemens Industry le brinda un soporte rápido y competente con respecto a todas las consultas técnicas con numerosas ofertas a medida, que van desde soporte básico hasta contratos de soporte individuales. Envíe sus consultas al Soporte Técnico a través del formulario web:

www.siemens.com/industry/supportrequest

SITRAIN – Formación para la Industria

Le apoyamos con nuestros cursos de formación disponibles en todo el mundo para la industria con experiencia práctica, métodos de aprendizaje innovadores y un concepto que se adapta a las necesidades específicas del cliente.

Para obtener más información sobre nuestras capacitaciones y cursos ofrecidos, así como sus ubicaciones y fechas, consulte nuestra página web:
www.siemens.com/sitrain

oferta de servicio

Nuestra gama de servicios incluye lo siguiente:

- Servicios de datos de planta
- Servicios de repuestos
- Servicios de reparación
- Servicios in situ y de mantenimiento
- Servicios de reacondicionamiento y modernización
- Programas y contratos de servicios

Puede encontrar información detallada sobre nuestra gama de servicios en la página web del catálogo de servicios:

<https://support.industry.siemens.com/cs/sc>

Aplicación de soporte en línea de la industria

Recibirá un soporte óptimo esté donde esté con la aplicación "Siemens Industry Online Support". La aplicación está disponible para Apple iOS, Android y Windows Phone: <https://support.industry.siemens.com/cs/ww/en/sc/2067>

5 Apéndice

5.2 Enlaces y literatura

Tabla 5-1

No.	Tema
\1\	Asistencia en línea de la industria de Siemens https://support.industry.siemens.com
\2\	Enlace a la página de entrada del ejemplo de aplicación https://support.industry.siemens.com/cs/ww/en/view/109762792
\3\	

5.3 Cambiar documentación

Tabla 5-2

Versión	Fecha	Modificaciones
V1.0	07/2020	Primera versión