



RED SIMÁTICA

Administración de redes
SINEC INS




Instrucciones de operación

<u>Prefacio</u>	1
<u>Instalación e inicio de sesión</u>	2
<u>Servicios de red</u>	3
<u>Administracion del sistema</u>	4
<u>Mensajes de registro del sistema</u>	5
<u>Apéndice A</u>	A

Información legal

Sistema de avisos de advertencia

Este manual contiene avisos que debe observar para garantizar su seguridad personal, así como para evitar daños a la propiedad. Los avisos que se refieren a su seguridad personal están resaltados en el manual con un símbolo de alerta de seguridad, los avisos que se refieren únicamente a daños a la propiedad no tienen símbolo de alerta de seguridad. Estos avisos que se muestran a continuación están clasificados según el grado de peligro.

 PELIGRO
indica que se producirán lesiones personales graves o la muerte si no se toman las precauciones adecuadas.
 ADVERTENCIA
indica que se pueden producir lesiones personales graves o la muerte si no se toman las precauciones adecuadas.
 PRECAUCIÓN
indica que pueden producirse lesiones personales menores si no se toman las precauciones adecuadas.
AVISO
indica que pueden producirse daños materiales si no se toman las precauciones adecuadas.


Si hay más de un grado de peligro, se utilizará el aviso de advertencia que represente el mayor grado de peligro. Un aviso de advertencia de lesiones a personas con un símbolo de alerta de seguridad también puede incluir una advertencia relacionada con daños a la propiedad.

Personal calificado

El producto/sistema descrito en esta documentación solo puede ser operado por **personal calificado** para la tarea específica de acuerdo con la documentación relevante, en particular sus avisos de advertencia e instrucciones de seguridad. El personal cualificado es aquel que, en base a su formación y experiencia, es capaz de identificar riesgos y evitar peligros potenciales al trabajar con estos productos/sistemas.

Uso adecuado de los productos Siemens

Tenga en cuenta lo siguiente:

 ADVERTENCIA
Los productos de Siemens solo pueden utilizarse para las aplicaciones descritas en el catálogo y en la documentación técnica correspondiente. Si se utilizan productos y componentes de otros fabricantes, estos deben ser recomendados o aprobados por Siemens. Se requiere un transporte, almacenamiento, instalación, montaje, puesta en marcha, operación y mantenimiento adecuados para garantizar que los productos funcionen de forma segura y sin problemas. Deben cumplirse las condiciones ambientales admisibles. Se debe observar la información en la documentación correspondiente.

Marcas registradas

Todos los nombres identificados con ® son marcas registradas de Siemens AG. El resto de marcas registradas en esta publicación pueden ser marcas cuyo uso por parte de terceros para sus propios fines podría violar los derechos del titular.

Descargo de responsabilidad

Hemos revisado el contenido de esta publicación para garantizar la coherencia con el hardware y el software descritos. Dado que la variación no se puede excluir por completo, no podemos garantizar una consistencia total. Sin embargo, la información de esta publicación se revisa regularmente y las correcciones necesarias se incluyen en ediciones posteriores.

Tabla de contenido

1	Prefacio.....	5
1.1	Recomendaciones de seguridad.....	6
2	Instalación e inicio de sesión.....	9
2.1	Tipos de licencia	9
2.2	Requisitos del sistema.....	10
2.3	Puertos utilizados	11
2.4	Instalación.....	12
2.5	Migración	13
2.6	Desinstalación	14
2.7	Iniciar sesión.....	15
2.8	Página de inicio.....	dieciséis
2.9	Estructura de la interfaz de usuario	21
3	Servicios de red	23
3.1	servicio de registro del sistema	23
3.1.1	Mensajes de Syslog.....	23
3.1.2	Configuración de Syslog	25
3.1.3	Filtros de Syslog.....	31
3.2	Servicio RADIO	31
3.2.1	Configuración de RADIO.....	32
3.2.2	Configuración de relés.....	38
3.3	Servicio DHCP	39
3.3.1	Configuración de DHCP.....	39
3.3.2	Asignaciones de DHCP.....	43
3.4	Servicio NTP	44
3.5	Servicio TFTP	45
3.5.1	Configuración TFTP	45
3.5.2	Transferencia de archivos TFTP desde la interfaz de usuario web de SINEC INS al directorio TFTP	46
3.6	Servicio SFTP.....	47
3.6.1	Configuración de SFTP	47
3.6.2	Transferencia de archivos SFTP desde la interfaz de usuario web de SINEC INS al directorio SFTP	50
3.7	Servicio de DNS.....	52
3.7.1	Configuración de DNS.....	52
3.7.2	Zonas DNS.....	55
3.7.3	DNS recuerdos.....	56

4 **Administracion del sistema..... 59**

4.1 Configuración general 59

4.1.1 UCM 59

4.1.2 Licencia 59

4.1.2.1 Activación de licencias 60

4.1.2.2 Nodos de licencia usados 61

4.1.3 Certificados 61

4.1.4 Configuración del puerto HTTP(S) 63

4.2 Gestión de autorizaciones 64

4.2.1 Componentes 64

4.2.2 Usuarios sesenta y cinco

4.2.2.1 Grupos de usuarios de UMC sesenta y cinco

4.2.2.2 Usuarios locales sesenta y cinco

4.2.3 Funciones sesenta y cinco

4.2.4 Asignaciones de roles 66

5 **Mensajes de Syslog..... 67**

5.1 Estructura de los mensajes de Syslog 67

5.2 Etiquetas en los mensajes de Syslog 68

5.3 Lista de mensajes de Syslog relacionados con la seguridad 69

A Apéndice A 75

A.1 Descripción general de la importación y exportación de configuraciones 75

Índice..... .. 77

Prefacio

Propósito de este software

SINEC INS pone a disposición varios servicios de red y permite la configuración central de estos servicios a través de una interfaz web común.

Propósito de esta documentación

Este manual le ayuda a instalar y operar SINEC INS.

Ámbito de validez

La información de este documento se aplica a SINEC INS V1.0 SP1.

Marcas registradas

Los siguientes y posiblemente otros nombres no identificados por el signo de marca registrada son marcas registradas de Siemens AG:

SINEC, SIMATIC

Condiciones de la licencia

Nota

Software de código abierto

El producto contiene software de código abierto. Lea atentamente las condiciones de licencia del software de código abierto antes de utilizar el producto.

Encontrará las condiciones de la licencia en el siguiente documento en el soporte de datos suministrado:

OSS_SINEC-INS_99.pdf

Glosario SIMATIC NET

Las explicaciones de muchos de los términos especializados utilizados en esta documentación se pueden encontrar en el glosario SIMATIC NET.

Puede encontrar el glosario SIMATIC NET en Internet en nuestras páginas de Industry Online Support en la siguiente dirección:
ID de entrada 50305045 (<https://support.industry.siemens.com/cs/ww/en/view/50305045>)

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 cibernéticas, es necesario implementar, y mantener continuamente, un concepto de seguridad industrial holístico y de última generación. Los productos y soluciones de Siemens forman un elemento de este concepto.

Los clientes son responsables de evitar el acceso no autorizado a sus plantas, sistemas, máquinas y redes. Estos sistemas, máquinas y componentes solo deben conectarse a la red empresarial o a Internet si y solo en la medida en que sea necesario y con las medidas de seguridad adecuadas (cortafuegos y/o segmentación de la red) implementadas.

Puede encontrar más información sobre medidas de protección en el área de seguridad industrial visitando:

<https://www.siemens.com/industrialsecurity> (<https://www.siemens.com/industrialsecurity>).

Los productos y soluciones de Siemens se someten a un desarrollo continuo para hacerlos más seguros. Siemens recomienda enfáticamente realizar actualizaciones de productos tan pronto como estén disponibles y usar solo 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> (<https://www.siemens.com/industrialsecurity>).

1.1 Recomendaciones de seguridad

Para evitar el acceso no autorizado, tenga en cuenta las siguientes recomendaciones de seguridad.

General

- Debe realizar comprobaciones periódicas para asegurarse de que este producto cumple estos recomendaciones y/u otras pautas de seguridad interna.
- Evalúe su planta como un todo en términos de seguridad. Utilice un concepto de protección celular con productos adecuados.
- SINEC INS solo está diseñado para conexiones con redes confiables y no debe conectado directamente con redes como Internet. Tenga esto en cuenta en un concepto de seguridad integral para su planta.
- Mantenga actualizado el software que está utilizando. Compruebe periódicamente si hay actualizaciones de seguridad para el producto. Encontrará información al respecto en:
Enlace: (<https://www.siemens.com/industrialsecurity>)
- Active únicamente los servicios que necesite para su red.

- Siempre que sea posible, utilice siempre las variantes de servicios que proporcionen mayor seguridad (por ejemplo, Secure Syslog, extensión DNSSEC, listas de control de acceso (ACL) para DNS, etc.).
- Las conexiones a través de áreas de red no seguras deben protegerse mediante mecanismos de seguridad como SSL VPN.
- Siempre haga clic en el botón "Cerrar sesión" en la interfaz web cuando haya terminado de trabajar con SINEC INS.
- Restringir el acceso al SINEC INS al personal calificado.
- Utilice la administración de usuarios y roles de SINEC INS para configurar los derechos de los usuarios según sus autorizaciones, consulte la sección Gestión de autorizaciones (Página 64).

Usuarios, roles y contraseñas

- Definir reglas para el uso del software y asignación de contraseñas.
- Actualice periódicamente las contraseñas y claves para aumentar la seguridad.
- Cree usuarios y funciones que se adapten al ámbito de autorización requerido por cada usuario. No use solo el usuario predeterminado "SuperAdmin" y el rol predeterminado "Admin".
- Defina contraseñas únicas para cada nuevo usuario.
- Utilice únicamente contraseñas con una seguridad de contraseña alta. Evite las contraseñas débiles, por contraseña de ejemplo 1, 123456789, abcdefgh.
- Asegúrese de que todas las contraseñas estén protegidas y sean inaccesibles para personas no autorizadas.
personas
- No utilice la misma contraseña para diferentes usuarios y sistemas.

Prefacio

1.1 Recomendaciones de seguridad

Instalación e inicio de sesión

2.1 Tipos de licencia

Cada licencia SINEC INS contiene un número específico de nodos de licencia. La cantidad de nodos de licencia determina cuántos dispositivos pueden usar los servicios. Los nodos de licencia se identifican en función de las direcciones IP de los dispositivos. Dependiendo del servicio respectivo, la licencia tiene los siguientes efectos:

- Syslog: el servidor Syslog recibe mensajes Syslog solo de un número limitado de Clientes Syslog.
- RADIUS: solo puede configurar un número limitado de clientes RADIUS en la página "Servicios de red > Servicio RADIUS > Configuración RADIUS > Clientes RADIUS". los dispositivos finales y los usuarios RADIUS de los clientes RADIUS no cuentan como nodos de licencia.
- TFTP / SFTP: Estos servidores solo pueden ser utilizados por un número limitado de sus clientes. Descarga, carga y eliminación de datos a través de la interfaz web SINEC INS utiliza HTTPS y estas operaciones no están limitadas.
- DNS: el servidor DNS responde a las solicitudes de resolución de nombres de un número limitado de dispositivos.

Cada nodo de licencia puede usar los servicios especificados simultáneamente. No hay restricciones para usar los servicios DHCP y NTP.

Por defecto, SINEC INS incluye una licencia de demostración gratuita con 10 nodos de licencia. Para aumentar la cantidad de dispositivos que pueden usar el servicio Syslog, RADIUS, TFTP, SFTP y DNS, debe comprar una licencia. Están disponibles los siguientes tipos de licencia:

- SINEC INS Básico 50
- SINEC INS Básico 100
- SINEC INS Básico 250
- SINEC INS Básico 500
- SINEC INS Básico 1000
- SINEC INS Básico 5000

El número en el nombre de la licencia especifica cuántos nodos de licencia se pueden utilizar para los servicios de red SINEC INS. Las licencias se pueden combinar. Puede encontrar información sobre la activación de las licencias adquiridas en el apartado Licencia (Página 59).

2.2 Requisitos del sistema

Requisitos de hardware

Según el número de nodos utilizados, se aplican los siguientes requisitos de hardware:

Tabla 2- 1 Requisitos de hardware

Componente	Hasta 500 nodos	Hasta 5000 nodos	Más de 5000 nodos
Procesador	2 núcleos con 2,16 GHz x64	2 núcleos con 2,6 GHz x64 4 núcleos con 3,6 GHz x64	
memoria de trabajo	2GB	8 GB	16 GB
Espacio en disco duro	Disco duro de 128 GB	SSD de 256GB	SSD de 512GB

Nota

Compruebe el uso del disco duro con regularidad. Cuando su disco duro está lleno, ya no se puede garantizar el correcto funcionamiento de SINEC INS.

Requisitos de Software

Los siguientes requisitos se aplican al software que se utilizará:

Tabla 2- 2 Requisitos de software

Sistema operativo	<ul style="list-style-type: none">• Escritorio Linux Ubuntu 18.04.2 LTS (64 bits)• Servidor Linux Ubuntu 18.04.2 LTS (64 bits)• SO SIMATIC V1.3• RX1500 APE 1808 Debian 9.6.0
Idiomas del sistema operativo admitidos	<ul style="list-style-type: none">• Alemán• Inglés
navegador web	<ul style="list-style-type: none">• Google Chrome 67.0 o superior• Firefox 60.0 o superior• Microsoft Edge 41 o superior• Internet Explorer 11.0*
Resolución de la pantalla	1920 x 1080 píxeles (el tamaño se puede cambiar)
Plataformas de virtualización recomendadas	<ul style="list-style-type: none">• VMware Workstation Pro/Workstation Player 15.0• Oracle VirtualBox 6.0 <p>Puede encontrar más información en la siguiente sección.</p>

* El navegador web solo es compatible de forma limitada.

Limitaciones en el uso de plataformas de virtualización

Las plataformas de virtualización recomendadas VMware Workstation y VirtualBox ofrecen la posibilidad de utilizar instantáneas para almacenar el estado y los datos de la máquina virtual en un momento dado. Tenga en cuenta que las instantáneas no deben crearse durante la operación de SINEC INS.

Antes de tomar una instantánea, asegúrese de haber deshabilitado todos los servicios de red.

Cuando se restaura una instantánea en la máquina virtual, la dirección IP de la interfaz de red debe permanecer sin cambios. De lo contrario, debe volver a generar el certificado de SINEC INS.

2.3 Puertos utilizados

SINEC INS utiliza los siguientes puertos como puertos predeterminados para la comunicación. Tenga en cuenta que dos programas diferentes no pueden comunicarse al mismo tiempo a través del mismo puerto. Si, por ejemplo, otras aplicaciones o dispositivos SIMATIC utilizan uno de los puertos, este puerto no está disponible para SINEC INS.

Tabla 2- 3 Puertos utilizados

Servicio/Protocolo	Protocolo / Número de puerto	Estado del puerto predeterminado	Estado del puerto configurable	Número de puerto configurable	Auténtico ción	Cifrado
SFTP	TCP/22	Cerrado	sí	sí	sí	sí
DNS	UDP/53	Cerrado	sí	No	sí	No
DHCP	UDP/67	Cerrado	sí	No	No	No
TFTP	UDP/69	Cerrado	sí	sí	No	No
HTTP	TCP/80	Abierto	No	sí	No	No
Servidor NTP	UDP/123	Cerrado	sí	No	sí	sí
Cliente NTP	UDP/123	Cerrado	sí	No	sí	No
HTTPS	TCP/443	Abierto	No	sí	sí	sí
servidor de registro del sistema	UDP/514	Cerrado	sí	sí	No	No
Servidor Syslog seguro	TCP/6514	Cerrado	sí	sí	sí	sí
Relé de servidor Syslog	UDP/dinámico	Abierto (interno)	Sí	sí	sí	sí
Servidor de radio	UDP/1812	Cerrado	sí	sí	sí	sí
Servidor web	TCP/5053	Abierto (interno)	No	sí	sí	sí
Servidor de radio apoderado	UDP/dinámico	Abierto (interno)	Sí	sí	sí	sí
CodeMeter Linux	TCP/22350	Abierto (interno)	No	No	sí	sí
CodeMeter administrador web	TCP/22352	Abierto (interno)	No	No	sí	sí

2.4 Instalación

Validación de firma antes de la instalación

Antes de instalar SINEC INS, compruebe la integridad de los paquetes Debian validando sus firmas. Para ello, siga los pasos que se describen a continuación:

1. En la terminal de su sistema operativo, navegue hasta el directorio SINECINS_V1.0.1/deb que contiene el archivo "key.gpg".
2. Ejecute el siguiente comando para importar la clave pública: `gpg --importar clave.gpg`
3. En la terminal de su sistema operativo, navegue hasta el directorio que contiene los archivos "sinecins.deb" y "codemeter-lite_7.10.4196.501_amd64.deb".
4. Valide la firma de los paquetes Debian de la siguiente manera:
 - Para "sinecins.deb": `dpkg-sig --verificar sinecins.deb`
 - Para "codemeter-lite_7.10.4196.501_amd64.deb": `dpkg-sig --verificar codificador lite_7.10.4196.501_amd64.deb`

Si la validación de la firma fue exitosa, instale SINEC INS de acuerdo con las instrucciones de la sección a continuación.

Instalación

Nota

Distribución del teclado durante la instalación

Durante la instalación, se establece la distribución del teclado "Inglés (EE. UU., Internacional)".

Siga estos pasos para instalar SINEC INS:

1. Compruebe la conexión a Internet.

Si no hay una conexión a Internet activa para SIMATIC OS V1.3 y RX1500 APE 1808 Debian 9.6.0, asegúrese de que estén instalados los siguientes paquetes:

- sistema
- libusb-1.0-0
- libcap2-bin
- libpcap-dev
- libwrap0-dev
- libglib2.0-0
- libreadline7
- libncursesw6

2. Para instalar SINEC INS desde el DVD del producto, copie el contenido del DVD en un directorio local de su PC.

Para instalar la versión de descarga de SINEC INS, descomprima el contenido del archivo "SINECINS_V1.0.1.tar.gz".

3. En la terminal de su sistema operativo, navegue hasta el directorio SINECINS_V1.0.1 que contiene el archivo "install.sh".

4. Ejecute el siguiente comando:

- Para sistemas operativos Linux Ubuntu: `sudo ./install.sh`
- Para SIMATIC OS V1.3 y RX1500 APE 1808 Debian 9.6.0 (se requiere una conexión a Internet activa): `sudo ./installDebianPkgDeps.sh`

Ahora se instalará SINEC INS. Durante la instalación debe aceptar las condiciones de licencia y las recomendaciones de seguridad.

SINEC INS utiliza los siguientes puertos TCP como estándar:

- Puerto de interfaz de usuario web HTTPS TCP 443
- Puerto de interfaz de usuario web HTTP TCP 80
- Puerto de servidor HTTPS TCP 5053

Si alguno de estos puertos ya está en uso, la instalación se detiene y debe definir un puerto diferente para SINEC INS. El valor ingresado debe estar entre 1 - 65535 y aún no ocupado. Sin embargo, no recomendamos usar puertos estandarizados entre 1 y 1023 para HTTP(S). Tenga en cuenta que los puertos ingresados no pueden ser idénticos.

La instalación continúa cuando confirma la entrada.

Una vez completada la instalación, puede iniciar sesión en la interfaz web; consulte la sección Inicio de sesión (Página 15).

2.5 Migración

Una instalación existente de SINEC INS V1.0 se puede migrar a SINEC INS V1.0 SP1. La licencia básica respectiva todavía se utiliza después de la migración.

Las cuentas de usuario y los dispositivos creados previamente, así como las configuraciones para los servicios de red, se conservan después de la migración. Todos los nodos de licencia utilizados, con la excepción de los clientes RADIUS, se eliminan durante la migración. Todas las funciones permanecen disponibles.

Procedimiento

Proceda de la siguiente manera para migrar SINEC INS:

1. Descomprima el contenido del archivo "SINECINS_V1.0.1.tar.gz".
2. Siga el procedimiento descrito en el apartado "Instalación (Página 12)".

Antes de la migración, confirme el mensaje sobre el proceso de actualización con "y" o "sí". Puede finalizar el proceso de migración con "n" o "no".

Durante la migración, se le solicitará:

- Aceptar las condiciones de la licencia y las recomendaciones de seguridad.
- Para especificar nuevos puertos HTTP(S) si los puertos HTTP(S) estandarizados ya están siendo utilizados por otra aplicación; consulte la sección "Instalación (Página 12)".

No hay servicios de red disponibles durante la migración.

3. Verifique el estado de los servicios de red después de la migración.

2.6 Desinstalando

Siga estos pasos para desinstalar SINEC INS:

1. En la página "Administración del sistema > Licencia > Licencias", libere las licencias para poder reutilizar las claves de licencia usadas para activar las licencias después de la desinstalación; consulte el apartado "Licencias (Página 60)".
2. En la terminal de su sistema operativo, navegue hasta el directorio que contiene el archivo "uninstall.sh". Encontrará este archivo en el DVD de producto de SINEC INS y en la carpeta de descarga "SINECINS_V1.0.1.tar.gz".
3. Ejecute el siguiente comando:

```
sudo ./uninstall.sh
```

Ahora se desinstalará SINEC INS y todos los servicios asociados.

Después de la desinstalación, se le preguntará si desea eliminar el contenedor de licencias con licencias activadas o conservarlo en el dispositivo en el que está instalado SINEC INS.

2.7

Iniciar sesión

La interfaz web de SINEC INS se puede llamar a través de la dirección IP o la URL del PC/dispositivo en el que está instalado SINEC INS. El acceso a la interfaz web de SINEC INS se realiza a través del protocolo HTTPS.

Se recomienda vaciar la memoria caché del navegador antes de acceder a la interfaz web de SINEC INS.

Nota

Verifique el estado de los servicios de red después de cada reinicio de SINEC INS.

Puede seleccionar el idioma deseado en la página de inicio.

Inicio de sesión inicial

La primera vez que inicie sesión en SINEC INS, utilice el siguiente usuario local y la contraseña correspondiente:

Tabla 2- 4 Datos de usuario para el primer inicio de sesión

Nombre de usuario	superadministrador
Clave	sinecinas

Después de iniciar sesión en SINEC INS por primera vez, se le redirigirá a una página en la que debe cambiar la contraseña. Utilice una contraseña segura y asegúrese de anotarla.

Si se pierde la contraseña, puede ser necesario reinstalar SINEC INS.

Opciones de inicio de sesión

Después del primer inicio de sesión, el inicio de sesión en SINEC INS puede realizarse con un usuario local o con un usuario configurado en UMC.

Iniciar sesión con UMC

UMC son las siglas de User Management Component, una base de datos para la administración central de los datos de los usuarios. Si se crea un usuario en UMC y se asigna a un grupo de usuarios de UMC, este usuario puede iniciar sesión en SINEC INS con su nombre de usuario y contraseña de UMC. Para ello, el servidor UMC debe estar activado en SINEC INS en "Administración del sistema > Configuración general > UMC" y la conexión con el servidor UMC debe estar configurada. Además, se debe crear el grupo de usuarios UMC en SINEC INS en la página "Administración del sistema" > "Usuarios" en la pestaña "Grupos de usuarios UMC". El nombre del grupo de usuarios de UMC especificado en SINEC INS debe corresponder al nombre del grupo de usuarios en UMC. Si la autenticación a través del servidor UMC está activada, SINEC INS intenta realizar el inicio de sesión con un usuario UMC. Si falla el inicio de sesión con un usuario de UMC, SINEC INS intenta realizar el inicio de sesión con un usuario local.

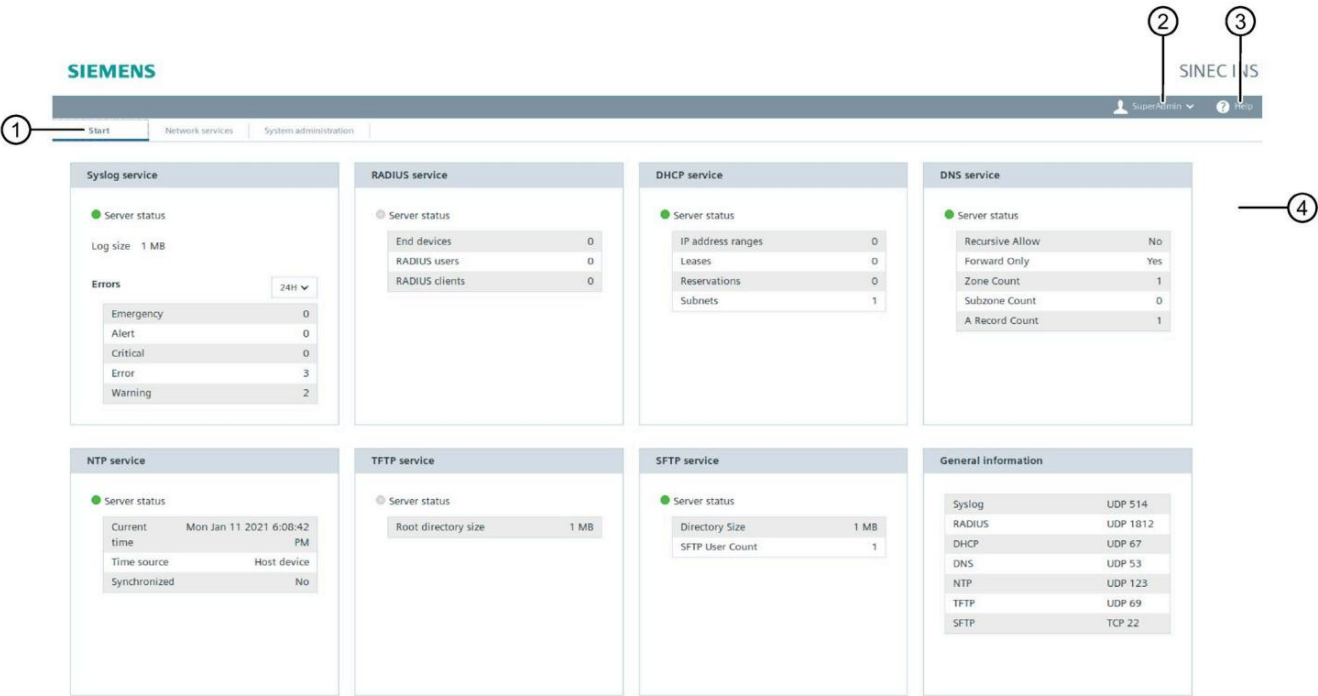
UMC no está incluido en el alcance del producto SINEC INS y debe instalarse por separado.

Para obtener información sobre la configuración de grupos de usuarios UMC en SINEC INS, consulte el capítulo Grupos de usuarios UMC (Página 65).

2.8 **Página de inicio**

Después de un inicio de sesión exitoso, se muestra la página de inicio. No puede configurar nada en esta página.

La página de inicio es el tablero de SINEC INS. Contiene una descripción general de la información básica sobre los servicios de red disponibles y se actualiza cada 60 segundos. La visualización de la página de inicio es individual y se adapta a las autorizaciones del usuario respectivo. Por lo tanto, la página de inicio solo muestra aquellos servicios de red para los que el usuario registrado está configurado con el derecho "Ver" o "Editar". Los usuarios con el derecho "Editar", y para algunos servicios de red también con el derecho "Ver", pueden cambiar a un servicio haciendo clic en el servicio en el tablero.



- Navegación
- Menú de usuario, consulte la sección a continuación
- Botón para acceder a la ayuda en línea
- Área de contenido, consulte la sección a continuación

Figura 2-1 Página de inicio de SINEC INS

Menú del Usuario

El menú de usuario muestra el nombre del usuario que ha iniciado sesión y contiene las siguientes funciones:

- Perfil (solo para usuarios locales)

Abre una ventana que muestra los detalles del usuario que ha iniciado sesión. La contraseña del usuario registrado se puede cambiar mediante el botón "Cambiar contraseña".

- Idioma

Selección del idioma de la interfaz de usuario

- Cerrar sesión

Cierra la sesión del usuario de SINEC INS.

- Información de versión

Muestra la versión instalada de SINEC INS.

Área de contenido

Los servicios de red disponibles y la información general se muestran en el área de contenido de la página de inicio.

Puede encontrar información detallada sobre los servicios de red individuales en la sección Servicios de red (Página 23).

servicio de registro del sistema

Se muestra la siguiente información:

- El estado del servidor

- Símbolo verde: el servidor Syslog está habilitado.

- Símbolo amarillo: no se puede acceder al directorio de registro o al directorio de archivo especificado.

Se utiliza el directorio predeterminado "/opt/sinecins/bin/syslog-ng/logs" en lugar del directorio de registro. Se utiliza el directorio predeterminado "/opt/sinecins/bin/syslog-ng/archive" en lugar del directorio de archivo.

- Símbolo gris: el servidor Syslog está deshabilitado.

- Tamaño del registro

Tamaño del archivo de registro en MB para mensajes Syslog.

- Errores

Esta tabla especifica la cantidad de mensajes Syslog que tienen las siguientes gravedades:

- 0: Emergencia
- 1: Alerta
- 2: Crítico
- 3: Error
- 4: Advertencia

El período de tiempo a partir del cual se originan los mensajes de Syslog recibidos se puede seleccionar en la lista desplegable.

servicio RADIO

Se muestra la siguiente información:

- El estado del servidor

- Símbolo verde: el servidor RADIUS está habilitado.
- Símbolo gris: el servidor RADIUS está deshabilitado.

- Dispositivos finales

Especifica el número de dispositivos finales configurados de clientes RADIUS.

- Usuarios de RADIUS

Especifica la cantidad de usuarios de RADIUS configurados que se requieren para la autenticación de usuarios.

- Clientes RADIUS

Especifica el número de clientes RADIUS configurados. El servidor RADIUS acepta solicitudes de autenticación de estos clientes RADIUS.

servicio DHCP

Se muestra la siguiente información:

- El estado del servidor

- Símbolo verde: El servidor DHCP está habilitado.
- Símbolo gris: el servidor DHCP está deshabilitado.

- Rangos de direcciones IP

Especifica la cantidad de rangos de direcciones IP a partir de los cuales el servidor DHCP puede asignar direcciones IP a los clientes DHCP.

- Arrendamientos

Especifica el número de dispositivos a los que el servidor DHCP concede actualmente direcciones IP.

- Reservas

Especifica el número de dispositivos para los que el servidor DHCP reserva actualmente direcciones IP.

- Subredes

Especifica el número de subredes en las que SINEC INS puede realizar asignaciones de direcciones IP.

servicio NTP

Se muestra la siguiente información:

- El estado del servidor

- Símbolo verde: El servidor NTP está habilitado.
- Símbolo gris: el servidor NTP está deshabilitado.

- Tiempo actual

Especifica la hora que el servidor NTP utiliza como hora actual.

- Fuente de tiempo

Especifica la fuente de tiempo SINEC INS que se utiliza para la hora actual.

- Sincronizado

Especifica si la hora está sincronizada entre SINEC INS y la fuente de tiempo utilizada.

- Última sincronización (si la hora está sincronizada entre SINEC INS y la hora fuente)

Especifica en segundos cuándo tuvo lugar la última sincronización entre SINEC INS y la fuente horaria.

- Servidor de sincronización

Dirección IP de la fuente de tiempo

Servicio TFTP

Se muestra la siguiente información:

- El estado del servidor

- Símbolo verde: El servidor TFTP está habilitado.
- Símbolo gris: el servidor TFTP está deshabilitado.

- Tamaño del directorio raíz

Especifica el tamaño del directorio raíz.

Servicio SFTP

Se muestra la siguiente información:

- El estado del servidor
 - Símbolo verde: El servidor SFTP está habilitado.
 - Símbolo gris: el servidor SFTP está deshabilitado.
- Tamaño del directorio

Especifica el tamaño del directorio SFTP.
- Usuarios de SFTP

Especifica el número de usuarios de SFTP.

servicio DNS

Se muestra la siguiente información:

- El estado del servidor
 - Símbolo verde: El servidor DNS está habilitado.
 - Símbolo gris: el servidor DNS está deshabilitado.
- Solicitudes de DNS recursivas
 - Sí No

Especifica si se habilitan más servidores de nombres para resoluciones recursivas de nombres de dominio.
- Solo reenviar
 - Sí: SINEC INS no intenta ponerse en contacto con otros servidores de nombres para responder a la solicitud de resolución de nombres si el propio SINEC INS o el servidor de nombres configurado no puede dar una respuesta.
 - No: SINEC INS intenta contactar con otros servidores de nombres, incluido el DNS raíz servidor, para responder a la solicitud de resolución de nombres si el propio SINEC INS o el servidor de nombres configurado no pueden dar una respuesta. Esta opción se utiliza para buscar dominios en Internet.
- Zonas DNS

Especifica el número de zonas DNS configuradas.
- Sub-zonas

Especifica el número de subzonas DNS configuradas.
- A recuerdos

Especifica el número de registros A configurados.

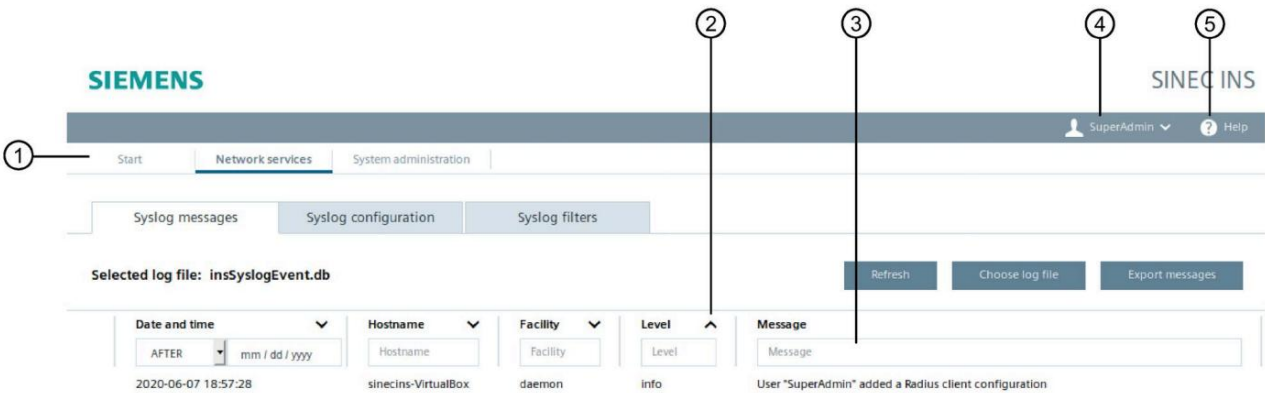
Información general

Los puertos que se utilizan actualmente para los servicios de red individuales se muestran en este área.

2.9 Estructura de la interfaz de usuario

SINEC INS se puede configurar a través de una interfaz de usuario. Los derechos de las funciones de un usuario determinan qué servicios de red y funciones del sistema están disponibles para este usuario en la interfaz de usuario.

La siguiente figura muestra elementos esenciales de la interfaz de usuario de SINEC INS utilizando la página para mensajes Syslog recibidos.



- Navegación
- Iconos para la clasificación ascendente/descendente del contenido de las columnas
- Cuadro de entrada para el filtrado de texto del contenido de la columna
- Menú de usuario
- Botón para llamar a la ayuda en línea

Figura 2-2 Interfaz de usuario de SINEC INS

En todas las páginas de WBM con tablas, aquí se muestra la opción para ordenar y filtrar las entradas de la tabla.

Servicios de red

3.1

servicio de registro del sistema

SINEC INS se puede utilizar como servidor Syslog y recibir mensajes Syslog de dispositivos u otros clientes Syslog en la red. SINEC INS también puede funcionar como relé Syslog y reenviar los mensajes Syslog recibidos a otros servidores Syslog o sistemas Siemens. Ambas rutas de comunicación se pueden proteger con TLS. SINEC INS admite la funcionalidad de servidor Syslog según RFC 5424 y RFC 3164 y la funcionalidad de cliente Syslog según RFC 5424.

Nota

Cuando los mensajes de Syslog se transfieren a través de TCP, SINEC INS admite el método de trama no transparente. El método de conteo de octetos según RFC 6587 no es compatible con SINEC INS.

3.1.1

Mensajes de registro del sistema

Los mensajes Syslog que SINEC INS recibió de dispositivos u otros servidores Syslog se muestran en la página "Servicios de red > Servicio Syslog > Mensajes Syslog". Los mensajes de Syslog se guardan con la hora UTC del sistema del servidor Syslog. La hora se muestra de acuerdo con la zona horaria del navegador respectivo en la PC. Además de los mensajes Syslog de los dispositivos de red, también se muestran los mensajes internos generados por SINEC INS. Cuando hace clic en una entrada en la página "Mensajes de Syslog", el mensaje asociado se muestra en su totalidad.

Para recibir mensajes Syslog, debe habilitar el servidor Syslog y especificar la interfaz y el puerto a través del cual SINEC INS debe recibir mensajes Syslog en la página "Servicios de red > Servicio Syslog > Configuración Syslog".

Controles del operador

Los siguientes controles del operador están disponibles encima de la mesa:

- Actualizar

Actualiza la tabla con mensajes Syslog

- Elija el archivo de registro

Abre un cuadro de diálogo en el que puede seleccionar el archivo de registro cuyos mensajes Syslog se van a desplegar.

Los mensajes Syslog recibidos siempre se guardan en el archivo de registro "insSyslogEvent.db". Este archivo se mueve a un directorio de archivo tan pronto como se exceda el límite máximo configurado. Todos los archivos de registro en el directorio de archivos de registro y en el directorio de archivo están disponibles para su selección en el cuadro de diálogo. Cuando hay varios archivos de registro, puede buscar el nombre del archivo. Configure estos dos directorios, así como el tamaño máximo del archivo de registro en la página "Servicios de red > Servicio Syslog > Configuración de Syslog".

• Exportar mensajes

Exporta los mensajes de Syslog mostrados a un archivo CSV.

Puede encontrar una descripción general de la exportación de mensajes Syslog en la sección "Descripción general de importar y exportar configuraciones (Página 75)".

Exhibición de Instalaciones

El origen de los mensajes se muestra en forma abreviada en el campo de la facilidad. La siguiente tabla asigna los nombres de las instalaciones que se muestran en SINEC INS a los nombres especificados en RFC 5424:

Tabla 3- 1 Instalaciones de Syslog

Código numérico	Nombre de la instalación en SINEC INS	Nombre de la instalación en RFC 5424
0	centro	mensajes del núcleo
1	usuario	mensajes a nivel de usuario
2	correo	sistema de correo
3	demonio	demonios del sistema
4	syslog de seguridad/autorización	mensajes de seguridad/autorización
5		mensajes generados internamente por syslogd
6	lpr	subsistema de impresora de línea
7	noticias	subsistema de noticias de la red
8	uucp	subsistema UUCP
9	demonio del reloj	demonio del reloj
10	seguridad/autorización ftp ntp	mensajes de seguridad/autorización
11	registro auditoría registro alerta	Demonio FTP
12	reloj daemon (nota 2)	subsistema NTP
13		auditoría de registro
14		alerta de registro
15		demonio de reloj (nota 2)
16-23	local0..local7	instalaciones de uso local (local0-local7)

Visualización de gravedades

La gravedad de los mensajes se muestra en el campo de gravedad. La siguiente tabla asigna los nombres de gravedad que se muestran en SINEC INS a los nombres especificados en RFC 5424:

Tabla 3- 2 Severidades de Syslog

Código numérico	Nombre de la gravedad en SINEC INS	Nombre de gravedad en RFC 5424
0	emergencia	Emergencia
1	alerta	Alerta
2	crítico	Crítico
3	error	Error
4	advertencia	Advertencia
5	aviso	Aviso
6	información	Informativo
7	depurar	Depurar

3.1.2

Configuración de registro del sistema

Los usuarios que tienen el derecho de "Editar" para el servicio Syslog pueden configurar el servidor Syslog. Los siguientes parámetros están disponibles para configurar el servidor Syslog en la página "Servicios de red > Servicio Syslog > Configuración de Syslog": • Activar servidor Syslog

Habilita o deshabilita el servidor Syslog.

Deshabilite el servidor Syslog antes de configurarlo o realizar cambios en la configuración. Tú habilite el servidor Syslog nuevamente después de la configuración.

• Interfaces de entrada

– Habilitar el adaptador de red para el servicio Syslog

Selección del adaptador de red a través del cual el servidor Syslog debe recibir Syslog mensajes Cambios en la configuración del adaptador de red en el sistema operativo SINEC INS solo los aplica después de reiniciar el servicio Syslog.

– Protocolo

Selección del protocolo de transporte a través del cual el servidor Syslog debe recibir Mensajes de registro del sistema.

- Puerto

Entrada del puerto a través del cual el servidor Syslog debe recibir mensajes Syslog. Asegúrese de que otra aplicación no esté utilizando el puerto especificado.

– Filtro de registro del sistema

Selección del filtro a aplicar a los mensajes Syslog recibidos. El registro del sistema filtros que se configuraron en la página "Servicios de red > Servicio Syslog > Los filtros Syslog" están disponibles para su selección; consulte la sección Filtros Syslog (Página 31).

- Relé Syslog

- Habilitar el relé Syslog

Si activa esta opción, el servidor Syslog reenvía los mensajes Syslog recibidos a los servidores Syslog especificados. Los mensajes de Syslog se pueden reenviar hasta a cinco servidores Syslog. Antes de reenviar a otro servidor Syslog, se puede aplicar un filtro a los mensajes Syslog. Los filtros de Syslog que se configuraron en la página "Servicios de red > Servicio de Syslog > Filtros de Syslog" están disponibles para su selección; ver apartado Filtros Syslog (Página 31).

Cuando se reenvían los mensajes Syslog, SINEC INS utiliza el nombre de host del mensaje Syslog recibido. Si el mensaje Syslog recibido no contiene un nombre de host, SINEC INS utiliza la dirección IP desde la que se envió el mensaje.

- Inicio sesión

- Tamaño máximo del archivo de registro

Los mensajes Syslog recibidos por el servidor Syslog se guardan en el archivo "insSyslogEvent.db". Cuando este archivo de registro alcanza el tamaño indicado aquí, se mueve al directorio de archivo especificado en el cuadro de entrada "Directorio de archivo". A continuación, SINEC INS vuelve a crear el archivo "insSyslogEvent.db" en el directorio especificado en el campo de entrada "Directorio de registro" para poder recibir más mensajes Syslog.

- Directorio de registro

Directorio en el que se guarda el archivo de registro "insSyslogEvent.db". Los mensajes de Syslog recibidos se guardan en este archivo. Se recomienda que guarde los archivos de registro localmente y no en una unidad de red. En la página "Servicios de red > Servicio Syslog > Mensajes Syslog", puede seleccionar los archivos de registro ubicados en el directorio de registro especificado y en el directorio de archivo especificado.

Si no se puede acceder al directorio de registro especificado, se utiliza el directorio predeterminado "/opt/sinecins/bin/syslog-ng/logs". Este estado se muestra en la página de inicio con un símbolo amarillo para el servidor Syslog.

- Directorio de archivo

Directorio en el que se archiva el archivo de registro "insSyslogEvent.db" después de haber alcanzado el tamaño máximo especificado. En este directorio, el archivo recibe la marca de tiempo actual como prefijo en su nombre. Se recomienda archivar los archivos de registro localmente y no en una unidad de red. En la página "Servicios de red > Servicio Syslog > Mensajes Syslog", puede seleccionar los archivos de registro ubicados en el directorio de registro especificado y en el directorio de archivo especificado.

Si no se puede acceder al directorio de archivo especificado, se utiliza el directorio predeterminado "/opt/sinecins/bin/syslog-ng/archive". Este estado se muestra en la página de inicio con un símbolo amarillo para el servidor Syslog.

- Administrar el directorio de archivos

Las siguientes opciones están disponibles:

Número máximo de archivos: después de alcanzar el número especificado de archivos de registro, un nuevo archivo de registro reemplaza al archivo de registro más antiguo en cada caso.

Antigüedad máxima del archivo: después de alcanzar la antigüedad del archivo especificada en días, SINEC INS elimina los archivos de registro.

Autenticación basada en certificados

La comunicación entre los clientes de Syslog y el servidor de Syslog se puede cifrar con TLS. La siguiente figura muestra una ilustración del procedimiento de autenticación basado en certificados:

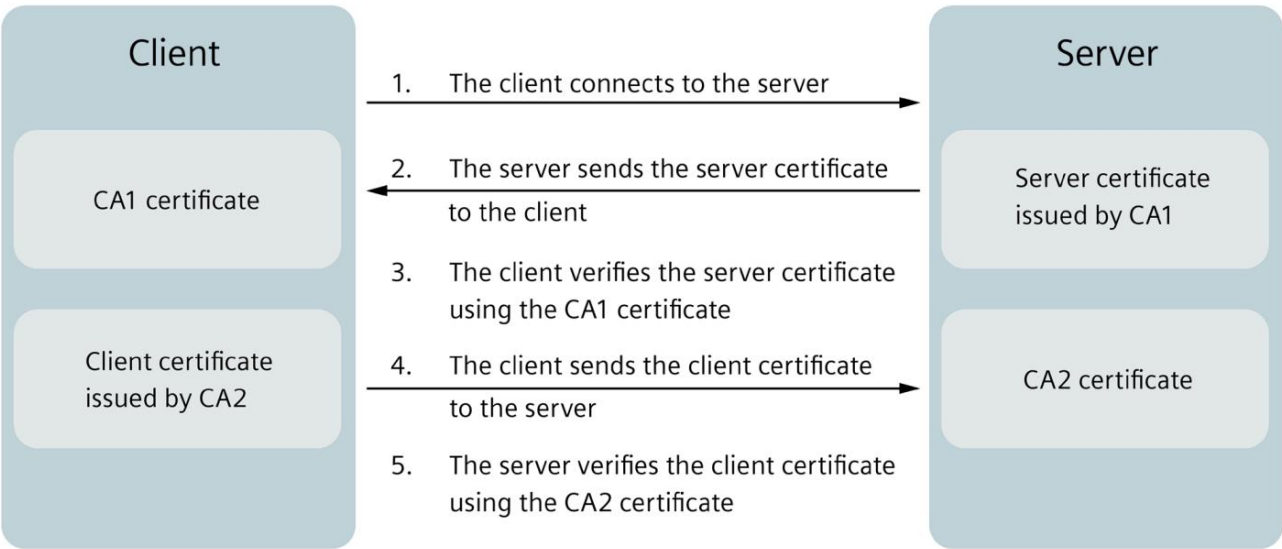


Figura 3-1 Autenticación basada en certificados

Nota

Requisitos de los certificados

La propiedad "Nombre común" o "subject_alt_name" debe contener el nombre de host o la dirección IP del servidor Syslog. De lo contrario, no se podrá establecer la conexión cifrada entre el cliente Syslog y el servidor Syslog.

Las claves con protección de contraseña no son compatibles con SINEC INS.

Asegúrese de que los certificados se renueven antes de su fecha de vencimiento.

Nota

Derechos de acceso para archivos de certificados

Observe los derechos de acceso para los certificados SSL que se utilizan para Secure Syslog.

Ejemplo:

- rwx-r--r-- para todos los archivos excepto el archivo de enlace simbólico
- rwx-rwx-rwx para el archivo de enlace simbólico

Nota

Interfaz de entrada para Secure Syslog

Para Secure Syslog, la interfaz de entrada debe cambiarse al puerto TCP 6514.

- Servidor Syslog seguro

Con las opciones de esta área de diálogo, puede proteger la comunicación entre los clientes Syslog y el servidor Syslog de SINEC INS. Los certificados y claves no son proporcionados por SINEC INS. Debe generarlos de acuerdo con sus propios requisitos y ponerlos a disposición de SINEC INS y de los clientes de Syslog. Solo se permiten certificados en formato *.pem y *.key.

En el área "Interfaz de entrada", asegúrese de que se seleccionó el protocolo TCP para una comunicación segura.

Están disponibles los siguientes ajustes:

- Habilitar el servidor Syslog seguro

Activa la comunicación segura de clientes Syslog con el servidor Syslog de SINEC INS. Todas las interfaces de entrada reciben posteriormente mensajes Syslog seguros.

- Servidor Syslog seguro con TLS

Si habilita esta opción, TLS se utiliza para registrar mensajes Syslog cifrados.

Antes de que comience la comunicación, los clientes de Syslog autentican el servidor de Syslog en función de su certificado. Para ello, debe especificar la ruta al certificado del servidor Syslog en el cuadro de entrada "Certificado del servidor Syslog". El certificado autofirmado del servidor Syslog o CA que creó el certificado del servidor Syslog debe ser conocido por los clientes Syslog para la autenticación del servidor Syslog. Para que el servidor Syslog descifre los mensajes de Syslog, se debe especificar la ruta a la clave privada asociada en el cuadro de entrada "Clave privada".

- Habilitar la autenticación mutua con TLS

Si habilita esta opción, TLS se utiliza para registrar mensajes Syslog cifrados.

Antes de que comience la comunicación, los clientes de Syslog autentican el servidor de Syslog en función de su certificado. Para ello, debe especificar la ruta al certificado del servidor Syslog en el cuadro de entrada "Certificado del servidor Syslog". El certificado autofirmado del servidor Syslog o CA que creó el certificado del servidor Syslog debe ser conocido por los clientes Syslog para la autenticación del servidor Syslog. Para que el servidor Syslog descifre los mensajes de Syslog, se debe especificar la ruta a la clave privada asociada en el cuadro de entrada "Clave privada".

Además, antes de que comience la comunicación, el servidor Syslog autentica a los clientes Syslog en función de sus certificados. Para ello, debe especificar en el cuadro de entrada "Directorio de certificado de CA del cliente" el directorio que contiene los certificados autofirmados de los clientes Syslog o las CA que crearon los certificados de los clientes Syslog. Luego, debe generar un valor hash para cada uno de estos certificados de acuerdo con las instrucciones a continuación y vincular el valor hash con el certificado correspondiente.

- Certificado de servidor Syslog

Ruta al certificado que usan los clientes Syslog para autenticar el servidor Syslog.
El certificado autofirmado del servidor Syslog o la CA que creó el
El certificado del servidor Syslog debe ser conocido por los clientes Syslog.

- Llave privada

Ruta a la clave privada que utiliza el servidor Syslog para descifrar los mensajes Syslog recibidos.

- Directorio de certificados CA del cliente (solo activo cuando la opción "Habilitar autenticación mutua con TLS" está activada)

Ruta al directorio que contiene los certificados autofirmados de los clientes Syslog o los certificados de las CA que crearon los certificados de los clientes Syslog.

Siga estos pasos para que el servidor Syslog pueda autenticar a los clientes Syslog en función de sus certificados:

1. Copie los certificados autofirmados de los clientes de Syslog o los certificados de CA en el directorio especificado.
2. Ejecute el siguiente comando para cada certificado para generar un valor hash alfanumérico para el certificado: `openssl x509 -noout -hash -in cacert.pem`
3. Ejecute el siguiente comando para establecer un enlace simbólico entre el certificado y el valor hash creado: `ln -s cacert.pem <valor hash>.0`

- Cliente Syslog seguro

Cuando se utiliza SINEC INS como relé Syslog, puede proteger la comunicación entre SINEC INS como cliente Syslog y otros servidores Syslog con las opciones de esta área de diálogo. Los certificados y claves no son proporcionados por SINEC INS. Debe generarlos de acuerdo con sus propios requisitos y ponerlos a disposición de SINEC INS y de los servidores Syslog. Están disponibles los siguientes ajustes:

- Habilitar cliente Syslog seguro

Activa la comunicación segura entre SINEC INS como cliente Syslog y otros servidores Syslog. Los mensajes Syslog seguros se envían a todos los Syslog configurados.
servidores.

- Cifrar mensajes de Syslog con TLS

Si activa esta opción, TLS se utiliza para cifrar la comunicación entre SINEC INS como cliente Syslog y otros servidores Syslog.

Antes de que comience la comunicación, el cliente Syslog autentica los servidores Syslog en función de sus certificados. Para ello, debe especificar en el cuadro de entrada "Directorio de certificados de CA de servidores" el directorio que contiene los certificados autofirmados de los servidores Syslog o los certificados de las CA que crearon los certificados de los servidores Syslog. Luego, debe generar un valor hash para cada uno de estos certificados de acuerdo con las instrucciones a continuación y vincular el valor hash con el certificado correspondiente.

- Habilitar la autenticación mutua con TLS

Si activa esta opción, TLS se utiliza para cifrar la comunicación entre SINEC INS como cliente Syslog y otros servidores Syslog.

Antes de que comience la comunicación, el cliente Syslog autentica los servidores Syslog en función de sus certificados. Para ello, debe especificar en el cuadro de entrada "Directorio de certificados de CA de servidores" el directorio que contiene los certificados autofirmados de los servidores Syslog o los certificados de las CA que crearon los certificados de los servidores Syslog. Luego, debe generar un valor hash para cada uno de estos certificados de acuerdo con las instrucciones a continuación y vincular el valor hash con el certificado correspondiente.

Además, antes de que comience la comunicación, los servidores de Syslog autentican al cliente de Syslog en función de su certificado. Para ello, debe especificar la ruta al certificado del cliente Syslog en el cuadro de entrada "Certificado del cliente Syslog". El certificado autofirmado del cliente Syslog o CA que creó el certificado del cliente Syslog debe ser conocido por los servidores Syslog para la autenticación del cliente Syslog. Para que el cliente Syslog descifre los datos del protocolo de enlace TLS, se debe especificar la ruta a la clave privada asociada en el cuadro de entrada "Clave privada".

– Directorio de certificados de CA de servidores

Ruta al directorio que contiene los certificados autofirmados de los servidores Syslog o los certificados de las CA que crearon los certificados de los servidores Syslog. Siga estos pasos para que el cliente Syslog pueda autenticar los servidores Syslog en base a sus certificados:

1. Copie los certificados autofirmados de los servidores Syslog o los certificados de CA en el directorio especificado.
2. Ejecute el siguiente comando para cada certificado para generar un valor hash alfanumérico para el certificado:
openssl x509 -noout -hash -in cacert.pem
3. Ejecute el siguiente comando para establecer un vínculo simbólico entre el certificado y el valor hash creado:
En -s cacert.pem <valor hash>.0

– Certificado de cliente Syslog (solo activo cuando la opción "Habilitar autenticación mutua con la opción TLS" está activada)

Ruta al certificado que usan los servidores Syslog para autenticar al cliente Syslog. El certificado autofirmado del cliente Syslog o CA que creó el certificado de el cliente Syslog debe ser conocido por los servidores Syslog.

– Clave privada (solo activa cuando la opción "Habilitar autenticación mutua con TLS" Está activado)

Ruta a la clave privada que utiliza el cliente de Syslog para descifrar los datos intercambiados en el contexto del protocolo de enlace TLS.

Nota

Para aplicar la configuración después de completar la configuración de Secure Syslog, debe deshabilitar el servidor Syslog y habilitarlo nuevamente.

3.1.3

Filtros de registro del sistema

En la página "Servicios de red > Servicio Syslog > Filtros Syslog", puede crear los filtros que se pueden aplicar a los mensajes Syslog recibidos y reenviados por SINEC INS.
Un filtro puede contener varias condiciones que se pueden establecer para propiedades como la gravedad y la instalación de los mensajes de Syslog. Puede vincular estas condiciones con los operadores OR o AND.

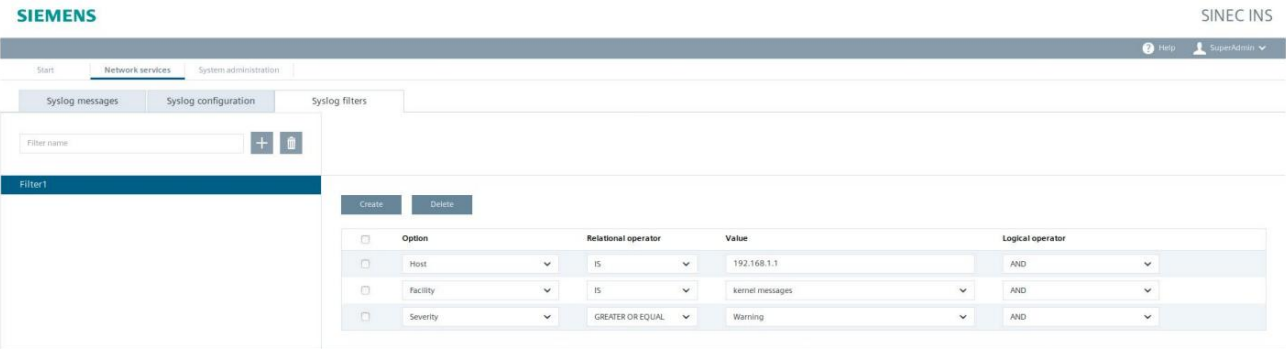


Figura 3-2 Filtro Syslog

En la página "Servicios de red > Servicio Syslog > Configuración de Syslog", puede seleccionar filtros creados para los adaptadores de red a través de los cuales el servidor Syslog recibe mensajes Syslog. Los filtros también se pueden aplicar a los mensajes de Syslog que se reenviarán a otros servidores de Syslog.

3.2 servicio RADIO

SINEC INS se puede utilizar como servidor RADIUS. RADIUS es un protocolo para la autenticación, autorización y contabilidad de usuarios y dispositivos mediante servidores en los que se pueden almacenar de forma centralizada los nombres de usuario, las contraseñas y la información del dispositivo. El uso de un servidor RADIUS puede aumentar la protección de estos datos. SINEC INS admite la autenticación y autorización de usuarios y dispositivos y puede reenviar solicitudes RADIUS a otros RADIUS servidores.

Las siguientes aplicaciones son compatibles con SINEC INS:

- Autenticación de usuario

Un usuario ingresa su nombre de usuario y contraseña en la página de inicio de sesión de WBM/SSH/Telnet de un dispositivo. Los datos del usuario son enviados por el dispositivo al servidor RADIUS de SINEC INS. SINEC INS comprueba si los datos del usuario están presentes en el servidor RADIUS. PAPILLA (Password Authentication Protocol) es el único protocolo de autenticación utilizado por SINEC INS.

- Autenticación basada en puerto

Un dispositivo final está conectado al puerto de un dispositivo cliente RADIUS. El dispositivo final se autentica para acceder al dispositivo cliente RADIUS con el modo configurado para el puerto. Los siguientes modos de autenticación de puertos son compatibles con SINEC INS:

- Dirección MAC

SINEC INS comprueba si la dirección MAC del dispositivo final está presente en SINEC INS en "Servicios de red > Servicio RADIUS > Configuración RADIUS > Dispositivos finales RADIUS".

- 802.1X (PAE)

El dispositivo final se autentica mediante uno de los siguientes protocolos:

EAP-MD5: SINEC INS no puede procesar consultas EAP-MD5 como servidor RADIUS, pero puede reenviar la solicitud a otros servidores RADIUS. Para un reenvío exitoso, se debe configurar un grupo de usuarios RADIUS correspondiente en SINEC INS para el nombre de usuario especificado en "Servicios de red > Servicio RADIUS > Configuración de retransmisión".

EAP-TLS / EAP-TTLS / EAP-PEAP: SINEC INS no puede procesar los certificados proporcionados, pero puede reenviar la solicitud de autenticación a otros servidores RADIUS.

Para un reenvío exitoso, se debe configurar un grupo de usuarios RADIUS correspondiente en SINEC INS en "Servicios de red > Servicio RADIUS > Configuración de relés".

- Autenticación de usuario con servidor UMC

Los usuarios en el servidor UMC se pueden usar para la autenticación RADIUS. Por lo tanto, un usuario de UMC puede iniciar sesión en dispositivos SIEMENS a través del servidor RADIUS utilizando su nombre de usuario y contraseña. Cuando un usuario de UMC inicia sesión en el cliente RADIUS, la solicitud de autenticación se envía al servidor RADIUS. Cuando la autenticación RADIUS con el servidor UMC está habilitada, la solicitud de autenticación se envía al servidor UMC. Para una autenticación exitosa, la configuración de los clientes RADIUS debe configurarse en consecuencia; consulte el apartado "Configuración RADIUS (Página 32)".

3.2.1 configuración de RADIUS

Los usuarios que tienen el derecho de "Editar" para el servicio RADIUS pueden configurar el servidor RADIUS y pueden exportar e importar configuraciones. Encontrará una descripción general de la exportación e importación de configuraciones en el apartado "Resumen de la importación y exportación de configuraciones (Página 75)".

Los siguientes parámetros están disponibles para configurar el servidor RADIUS en el
Página "Servicios de red > Servicio RADIUS > Configuración de RADIUS":

- **Habilitar el servidor RADIUS**

Habilita o deshabilita el servidor RADIUS

Deshabilite el servidor RADIUS antes de configurarlo o realizar cambios en la configuración.

Vuelva a habilitar el servidor RADIUS después de la configuración.

- **Botón "Exportar configuraciones"**

Botón para exportar las configuraciones de usuarios RADIUS, clientes RADIUS y dispositivos finales. Los archivos creados se utilizan para realizar copias de seguridad de las configuraciones.

Después de la exportación, recibirá un archivo ZIP "sinecinsRadiusConfiguration.zip" con tres configuraciones en formato CSV para usuarios, clientes y dispositivos finales.

Los archivos CSV exportados de los usuarios de RADIUS "sinecinsRadiusUsers.csv" y de los clientes de RADIUS "sinecinsRadiusClients.csv" están encriptados por SINEC INS. El archivo CSV exportado desde los dispositivos finales RADIUS "sinecinsRadiusEndDevices.csv" no está cifrado y el usuario puede editarlo. Después de la exportación, el CSV se edita con el sistema operativo. Tenga en cuenta que los nombres de los tres archivos CSV, así como los nombres y el orden de las columnas que contienen, no se pueden cambiar después de la exportación. De lo contrario, no será posible importar las configuraciones posteriormente.

- **Botón "Importar configuraciones"**

Botón para importar las configuraciones de usuarios RADIUS, clientes RADIUS y dispositivos finales.

Puede importar configuraciones previamente exportadas para usuarios, clientes y dispositivos finales desde un archivo ZIP a SINEC INS.

Siga estos pasos para importar la configuración de RADIUS:

1. Deshabilite el servidor RADIUS antes de la importación.
2. Haga clic en "Importar configuraciones".

Se muestra la ventana de diálogo "Importar configuraciones".
3. En el navegador, navegue hasta el directorio que contiene el
Archivo de configuración "sinecinsRadiusConfiguration.zip" a cargar. Haga doble clic en el archivo ZIP correspondiente para aplicarlo. Tenga en cuenta que ninguno de los nombres de archivo se puede cambiar. De lo contrario, se cancelará la importación.
4. Seleccione la casilla de verificación "Anular configuraciones existentes" para sobrescribir las entradas existentes.

La sobrescritura se basa en el nombre de usuario especificado para los usuarios RADIUS, en el nombre del cliente y la dirección IP del cliente especificados para los clientes RADIUS y en la dirección MAC especificada para los dispositivos finales.

Si ha cambiado el nombre de VLAN o la ID de VLAN para un dispositivo final en el archivo sin cifrar "sinecinsRadiusEndDevices.csv", el nombre de VLAN anterior o la ID de VLAN anterior se sobrescribirán si se selecciona la opción "Anular configuraciones existentes".

5. Haga clic en "Importar".

Todas las configuraciones de RADIUS para usuarios, clientes y dispositivos finales se importan a SINEC INS.

Tenga en cuenta que todos los usuarios de RADIUS se importan con el estado "habilitado", independientemente de si tenían el estado "habilitado" o "deshabilitado" antes de la exportación.

Durante la importación, los resultados del proceso de importación se registran en un archivo de registro. El archivo de registro se guarda automáticamente en el navegador de la PC del usuario. El servicio Syslog registra cada proceso de importación.

Tenga en cuenta que la cantidad de clientes RADIUS está limitada por la licencia disponible. Si se supera el número máximo de clientes RADIUS, se detiene la adición de más clientes RADIUS. Esta información se registra.

- Interfaces de entrada

- Habilitar el adaptador de red para el servicio RADIUS

- Selección del adaptador de red a través del cual el servidor RADIUS debe recibir solicitudes de autenticación. SINEC INS solo aplica los cambios en la configuración del adaptador de red en el sistema operativo después de reiniciar el servicio RADIUS.

- Puerto

- Entrada del puerto UDP a través del cual el servidor RADIUS debe recibir solicitudes de autenticación. Asegúrese de que otra aplicación no esté utilizando el puerto especificado.

- Usuarios de RADIUS

Los datos de usuario que se necesitan para la autenticación del usuario se pueden administrar en esta área de diálogo. Con el botón "Crear", puede crear nuevos usuarios de RADIUS. Para ello, introduzca el nombre de usuario y la contraseña y confirme la contraseña. Utilice contraseñas con una seguridad de contraseña alta. Para asignar permisos de escritura al usuario en el dispositivo, habilite la opción "Usuario administrativo". Cuando el servidor RADIUS recibe una solicitud de autenticación de un dispositivo, verifica si los datos de usuario especificados están presentes en esta área de diálogo. Si los datos del usuario están presentes, el usuario recibe acceso al dispositivo.

Se muestra un estado "habilitado/deshabilitado" para los usuarios de RADIUS configurados y se pueden filtrar por estado.

- Botones "Habilitar" y "Deshabilitar"

Puede habilitar o deshabilitar usuarios de RADIUS previamente seleccionados con estos botones. Un usuario recién creado recibe el estado "habilitado" de forma predeterminada. Los botones están disponibles cuando se selecciona al menos un usuario de RADIUS en la lista.

- Botón "Importar usuarios de RADIUS"

El botón para importar datos de usuario de RADIUS se encuentra a la derecha en el área "Usuarios de RADIUS".

Puede importar datos de usuario RADIUS creados previamente desde un archivo CSV a SINEC INS.

Siga estos pasos para importar los usuarios de RADIUS:

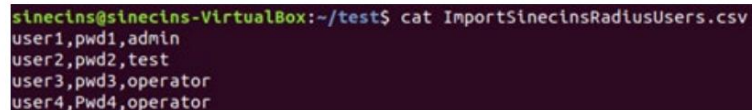
1. Primero, cree un archivo CSV con los datos del usuario. Para hacer esto, ingrese los datos de los usuarios de RADIUS en una tabla y luego guarde la tabla como archivo CSV. La tabla **no debe tener encabezado** y contener los datos en el siguiente orden:

- Primera columna: Nombre de usuario
- Segunda columna: Contraseña correspondiente
- Tercera columna: tipo de usuario, por ejemplo, administrador u operador (las entradas no distinguen entre mayúsculas y minúsculas)

Si no se ingresa ningún tipo de usuario o se ingresa un tipo de usuario diferente a "admin", SINEC INS lo convierte automáticamente al tipo de usuario "Operador". El tipo de usuario "admin" recibe permisos de escritura para clientes RADIUS y el tipo de usuario "Operador" recibe permisos de lectura. Los nombres de usuario y contraseñas especificados deben ser válidos. De lo contrario, no se guarda ningún dato.

Tenga en cuenta que la cantidad de usuarios de RADIUS que se importarán desde un archivo CSV está limitada a un máximo. 10000.

El delimitador de columna del archivo CSV debe ser ",", (coma).



```
sinecins@sinecins-VirtualBox:~/test$ cat ImportSinecinsRadiusUsers.csv
user1,pwd1,admin
user2,pwd2,test
user3,pwd3,operator
user4,Pwd4,operator
```

Figura 3-3 Ejemplo de un archivo CSV para importar los usuarios de RADIUS

2. Deshabilite el servidor RADIUS antes de la importación.
3. Haga clic en "Importar usuarios de RADIUS".

Aparece el cuadro de diálogo "Importar usuarios de RADIUS".
4. Navegue en el navegador hasta el directorio en el que se encuentra el archivo CSV que se va a cargar.

Haga doble clic en el archivo deseado para aplicarlo.
5. Haga clic en "Importar".

Los datos de usuario de RADIUS se importan a SINEC INS.

Durante la importación, los resultados del proceso de importación se registran en un archivo de registro. El registro El archivo se guarda automáticamente en el navegador del PC del usuario. El servicio Syslog registra cada proceso de importación. Se registra la información de los usuarios no agregados.

Si se supera el número máximo de entradas, se detiene la adición de más usuarios de RADIUS y no se registran las entradas superfluas.

• Clientes RADIUS

Todos los dispositivos que envían solicitudes de autenticación al servidor RADIUS deben ser conocidos por el servidor RADIUS. Con el botón "Crear", puede dar a conocer estos dispositivos al servidor RADIUS creándolos como clientes RADIUS con nombres y direcciones IP. Para cada cliente RADIUS, se debe especificar un secreto compartido que también debe configurarse en el cliente RADIUS. Los nombres de los clientes especificados no necesitan coincidir con los nombres de los dispositivos.

Seleccione la casilla de verificación "Atributo de autenticador de mensajes compatible" si el cliente RADIUS puede enviar un atributo de autenticador de mensajes para los requisitos de acceso. Esto activa un mecanismo de seguridad RADIUS. Luego, el cliente RADIUS necesita calcular una clave con HMAC MD5 de su propio paquete de solicitud y agregarla al atributo Message-Authenticator como firma. El servidor RADIUS valida el paquete. Si la verificación tiene éxito, el cliente RADIUS recibe una respuesta del servidor RADIUS. Si la verificación falla debido a un atributo del autenticador de mensajes incorrecto o faltante, la solicitud de acceso RADIUS se descarta. Todos los dispositivos SCALANCE compatibles generan automáticamente un atributo Message-Authenticator y lo agregan al paquete de solicitud. Deje seleccionada la casilla de verificación "Atributo de autenticador de mensajes compatible" para los dispositivos SCALANCE. Los dispositivos RUGGEDCOM, por el contrario, **no** tienen esta opción. Por este motivo, debe desmarcar esta casilla de verificación para dispositivos RUGGEDCOM; de lo contrario, el servidor RADIUS no puede responder a los dispositivos RUGGEDCOM.

Tenga en cuenta que la cantidad de clientes RADIUS configurables está limitada por la presente licencia.

- Botón "Importar clientes Radius"

El botón para importar datos de clientes RADIUS se encuentra a la derecha en "RADIUS área de clientes".

Puede importar datos creados previamente de clientes RADIUS desde un archivo CSV a SINEC EN S. El procedimiento es idéntico a la importación de usuarios RADIUS; ver el "Radio de importación usuarios" arriba. La tabla **no debe tener encabezado** y contener los datos en el siguiente orden:

- Primera columna: Nombre del cliente RADIUS
- Segunda columna: dirección IP del cliente RADIUS
- Tercera columna: Secreto compartido correspondiente
- Cuarta columna: "sí" o "no" (no distingue entre mayúsculas y minúsculas)
 - "sí", si el atributo Message-Authenticator está habilitado en el cliente RADIUS (p. ej. para dispositivos SCALANCE)
 - "no", si el atributo Message-Authenticator está deshabilitado en el cliente RADIUS (por ejemplo, para dispositivos RUGGEDCOM).

Si la cuarta columna no contiene una entrada o contiene una entrada que no sea "sí" o "no", SINEC INS la convierte automáticamente a "sí".

Los nombres de usuario y direcciones IP especificados deben ser válidos. De lo contrario, no se guarda ningún dato.

El delimitador de columna del archivo CSV debe ser "," (coma). El máximo. el número de usuarios de RADIUS que se importarán desde un archivo CSV es 10000.

- VLAN invitada

La VLAN invitada permite que los dispositivos finales desconocidos accedan al cliente RADIUS especificando el nombre de la VLAN invitada o el ID de la VLAN invitada.

Habilite esta opción si desea que el dispositivo final tenga permiso en la VLAN invitada si falla la autenticación. El dispositivo solo se puede asignar a la VLAN correspondiente si la VLAN se ha creado en el dispositivo. De lo contrario, se rechaza la autenticación.

Asegúrese de que la opción "Asignación de VLAN de RADIUS permitida" también esté habilitada en el propio dispositivo para que el dispositivo pueda autenticarse en la VLAN invitada.

- Habilitar VLAN invitada

Habilita o deshabilita la VLAN invitada.

- Nombre de VLAN/ID de VLAN

Entrada del nombre de VLAN o la ID de VLAN para la VLAN invitada

El nombre de VLAN/ID de VLAN se puede manejar de manera diferente según la configuración del cliente. Verifique la configuración del cliente para evitar la autorización no intencional.

- Dispositivos finales

Los dispositivos finales que están conectados al puerto de un cliente RADIUS se pueden autenticar en función de su dirección MAC. En el área de diálogo "Dispositivos finales" puede especificar las direcciones MAC de estos dispositivos finales. La VLAN invitada también se puede asignar a un dispositivo final.

Si especifica además el nombre de VLAN o la ID de VLAN para un dispositivo final, la respuesta de SINEC INS a la solicitud de un cliente RADIUS también contiene la información de VLAN especificada. El cliente RADIUS puede verificar si la VLAN especificada corresponde a la VLAN del dispositivo final que está conectado al puerto respectivo.

- Botón "Importar dispositivos de radio"

El botón para importar dispositivos finales se encuentra a la derecha en el área "Dispositivos finales".

Puede importar datos creados anteriormente de dispositivos finales desde un archivo CSV a SINEC INS. El procedimiento es idéntico a la importación de usuarios RADIUS; vea el botón "Importar usuarios de radio" arriba. La tabla **no debe tener encabezado** y contener los datos en el siguiente orden:

- Primera columna: dirección MAC o

"-" ":" se puede utilizar para las direcciones MAC.

- Segunda columna: nombre de VLAN/ID de VLAN

Las direcciones MAC especificadas y los nombres de VLAN/ID de VLAN deben ser válidos. De lo contrario, no se guarda ningún dato.

El delimitador de columna del archivo CSV debe ser ",", (coma). El máximo, el número de usuarios de RADIUS que se importarán desde un archivo CSV es 10000.

```
sinecins@sinecins-VirtualBox:~/test$ cat sinecinsRadiusEndDevices.csv
12:F4:8D:E3:47:03,VLAN1
10-F4-8D-E3-47-12,VLAN2
```

Figura 3-4 Ejemplo de un archivo CSV para importar los dispositivos finales

- Habilite la autenticación Radius con el servidor UMC

Los datos de inicio de sesión de los usuarios de UMC se pueden usar para la autenticación RADIUS para acceder a los dispositivos, siempre que estos dispositivos puedan enviar el atributo Message-Authenticator en sus solicitudes de autenticación RADIUS. Las solicitudes de autenticación de RADIUS sin un atributo de autenticación de mensajes solo se editan con usuarios de RADIUS locales.

Para poder usar la autenticación RADIUS con el servidor UMC, debe asegurarse en el lado del cliente RADIUS de que el cliente RADIUS admita la autorización en el modo específico del proveedor y que la autenticación RADIUS esté configurada según el modo específico del proveedor. Los nombres de los grupos de usuarios en el cliente RADIUS deben coincidir exactamente con los nombres de los grupos de usuarios en el servidor UMC.

Si la solicitud de autenticación a través del servidor UMC tiene éxito, SINEC INS devuelve un mensaje de aceptación de acceso con el nombre del grupo de usuarios UMC del usuario UMC que se va a autorizar e intenta autenticar el cliente RADIUS.

- Habilite la autenticación Radius con el servidor UMC

Habilita o deshabilita la autenticación RADIUS a través del servidor UMC

- Botón "Configurar servidor UMC"

Con este botón, puede cambiar a la página de configuración de UMC para configurar el servidor UMC o habilitar el inicio de sesión en SINEC INS allí a través del servidor UMC; consulte la sección "UMC (Página 59)".

Para la autenticación RADIUS a través del servidor UMC, solo es necesario especificar la dirección del servidor UMC. Si no desea utilizar la autenticación RADIUS a través del servidor UMC, debe deshabilitar esta función después de configurar el servidor UMC mediante el control deslizante "Habilitar la autenticación Radius con el servidor UMC". El control deslizante en la página de configuración de UMC en "Administración del sistema > Configuración general > UMC" se usa para habilitar el inicio de sesión en SINEC INS a través de UMC. Para ello, necesita el derecho "Editar" para la "Configuración general".

3.2.2 Configuración de relés

Los usuarios que tienen el derecho de "Editar" para el servicio RADIUS pueden configurar el reenvío de solicitudes RADIUS a otros servidores RADIUS en la página "Servicios de red > Servicio RADIUS > Configuración de retransmisión".

Es posible que la función de retransmisión no esté disponible con la autenticación RADIUS habilitada a través de UMC.

Están disponibles los siguientes elementos de control:

- Grupos de usuarios de RADIUS

SINEC INS reenvía una solicitud RADIUS a otros servidores RADIUS si el nombre de usuario de la solicitud RADIUS pertenece a uno de los grupos de usuarios RADIUS especificados y se especifica de la siguiente manera:

- Usuario@grupo de usuarios RADIUS

El grupo de usuarios de RADIUS debe contener el carácter ".", por ejemplo mycompany.com

- Grupo de usuarios/usuario de RADIUS

- Grupo de usuarios de RADIUS y usuario

Ejemplo: El grupo de usuarios RADIUS "siemens.com" está configurado en SINEC INS. Si una solicitud RADIUS contiene el nombre de usuario "testuser@siemens.com", esta solicitud RADIUS se reenvía.

- Grupos de servidores RADIUS de retransmisión

En esta área, configura los servidores RADIUS a los que se deben reenviar las solicitudes RADIUS. Combine estos servidores RADIUS en grupos de servidores RADIUS de retransmisión.

- Asignación de relés

En esta área, define qué grupos de usuarios RADIUS deben asignarse a qué grupos de servidores RADIUS de retransmisión. Una solicitud RADIUS con un nombre de usuario que pertenece a un grupo de usuarios RADIUS se reenvía a todos los servidores RADIUS de los grupos de servidores RADIUS de retransmisión asociados.

3.3 Servicio DHCP

SINEC INS se puede utilizar como servidor DHCP y asignar direcciones IP a los dispositivos de la red. Las direcciones IP se pueden asignar a dispositivos desde rangos de direcciones IP configurables o se pueden reservar para las direcciones MAC de los dispositivos.

3.3.1 Configuración DHCP

Los usuarios que tienen el derecho de "Editar" para el servicio DHCP pueden configurar el servidor DHCP en la página "Servicios de red > Servicio DHCP > Configuración de DHCP".

Están disponibles los siguientes elementos de control:

- Habilitar servidor DHCP

Activa/desactiva el servidor DHCP.

Deshabilite el servidor DHCP antes de configurarlo o realizar cambios en la configuración. Vuelva a habilitar el servidor DHCP después de la configuración.

- Subredes

En esta área de diálogo se configuran las subredes en las que SINEC INS debe realizar las asignaciones de direcciones IP. Según las subredes especificadas, puede definir en los "Rangos de direcciones IP" los rangos de direcciones IP de estas subredes a partir de las cuales se asignarán las direcciones IP.

Las direcciones de red de los adaptadores de red disponibles están predefinidas por SINEC INS en el área de diálogo "Subredes". Dependiendo del adaptador de red a través del cual SINEC INS recibe una solicitud de dirección IP de un cliente DHCP, SINEC INS ofrece al cliente DHCP una dirección IP del rango de direcciones IP asociado.

Además de las direcciones de red predefinidas, puede especificar manualmente subredes a las que se puede acceder a través de un enrutador. Cuando se configura un Agente de retransmisión DHCP en el enrutador, SINEC INS utiliza la dirección IP del Agente de retransmisión en el mensaje DHCPDISCOVER para reconocer la subred en la que debe realizarse la asignación de la dirección IP.

Configura una nueva subred con el botón "Crear". Puede modificar los parámetros en las subredes configuradas con el botón "Editar".

Introduzca los siguientes parámetros en el cuadro de diálogo para configurar una subred nueva o existente:

- Dirección IP

Primera dirección IP de la subred en la que SINEC INS va a realizar las asignaciones de direcciones IP. La dirección de red de la subred depende de la máscara de subred utilizada.

- Máscara de subred

Máscara para determinar la parte de la red y la parte del host de la dirección IP especificada. La primera dirección IP de una subred se puede determinar utilizando la máscara de subred.

Puede definir parámetros adicionales en "Opciones":

- servidores DNS

Direcciones IP de servidores DNS que se envían al cliente DHCP como parte de la concesión de direcciones IP.

- Enrutadores

Direcciones IP de enrutadores que se envían al cliente DHCP como parte de la concesión de direcciones IP.

- Servidores NTP

Direcciones IP de servidores NTP que se envían al cliente DHCP como parte de la concesión de direcciones IP.

- Servidor TFTP

Dirección IP del servidor TFTP que se envía al cliente DHCP como parte de la concesión de la dirección IP.

- Dirección de Difusión

Dirección IP que se utiliza como dirección IP de difusión de la subred. Solo se permite una dirección IP. Si no desea asignar una dirección de transmisión específica, el dispositivo utiliza automáticamente la última dirección IP de la subred.

– Tiempo de concesión predeterminado (segundos)

Periodo de tiempo durante el cual se arrienda una dirección IP a un cliente DHCP cuando el cliente DHCP no solicita un tiempo de arriendo específico a SINEC INS.

– Tiempo máximo de arrendamiento (segundos)

El tiempo máximo que un cliente DHCP puede solicitar para arrendar una dirección IP de SINEC INS.

- Rangos de direcciones IP

En esta área de diálogo se ingresa, en base a las subredes configuradas, los rangos de direcciones IP a partir de los cuales SINEC INS debe asignar direcciones IP a los clientes DHCP. Puede especificar un máximo de un rango de direcciones IP por subred.

- Reservas de direcciones IP

En esta área de diálogo puede reservar direcciones IP para clientes DHCP. Los clientes DHCP se identifican en función de sus direcciones MAC. Una dirección IP reservada para un cliente DHCP no se asigna a ningún otro cliente DHCP por parte de SINEC INS.

Nota

No use direcciones IP de rangos IP dinámicos para reservas de direcciones IP.

Utilice el botón de flecha en el encabezado para actualizar la lista de reservas de direcciones IP.

Configura una nueva reserva de dirección con el botón "Crear". Puede modificar los parámetros en las reservas de direcciones configuradas con el botón "Editar".

Se pueden especificar los siguientes parámetros:

- Nombre

Nombre de la reserva de dirección IP. Este nombre solo se utiliza para la visualización en SINEC INS y no afecta a la configuración del cliente DHCP.

- Dirección MAC

Dirección MAC del cliente DHCP para el que se reserva la dirección IP.

– Subredes

Selección de la subred en la que se va a reservar la dirección IP. Configure las subredes que están disponibles para la selección en el área de diálogo "Subredes", consulte la sección anterior.

- Dirección IP

Dirección IP que se reservará para el cliente DHCP.

– Nombre de host

Nombre de host que se asigna al cliente DHCP.

– Identificación del cliente

Identificador de cliente que se asigna al cliente DHCP.

– servidores DNS

Direcciones IP de servidores DNS que se envían al cliente DHCP como parte de la concesión de direcciones IP. Los parámetros configurados aquí sobrescriben los parámetros configurados para la subred asociada.

– Enrutadores

Direcciones IP de enrutadores que se envían al cliente DHCP como parte de la concesión de direcciones IP. Los parámetros configurados aquí sobrescriben los parámetros configurados para la subred asociada.

– Servidores NTP

Direcciones IP de servidores NTP que se envían al cliente DHCP como parte de la concesión de direcciones IP. Los parámetros configurados aquí sobrescriben los parámetros configurados para la subred asociada.

– Servidor TFTP

Dirección IP del servidor TFTP que se envía al cliente DHCP como parte de la concesión de la dirección IP. El parámetro configurado aquí sobrescribe el parámetro configurado para la subred asociada.

- Dirección de Difusión

Dirección IP que se utiliza como dirección IP de difusión de la subred. Solo se permite una dirección IP. El parámetro configurado aquí sobrescribe el parámetro configurado para la subred asociada. Si no desea asignar una dirección de transmisión específica, el dispositivo utiliza automáticamente la última dirección IP de la subred.

- Nombre de dominio

Nombre de dominio que se envía al cliente DHCP como parte de la concesión de la dirección IP.

– Archivo de arranque

Ruta al archivo que debe ejecutar el cliente DHCP.

– Tiempo de concesión predeterminado (segundos)

Periodo de tiempo durante el cual se arrienda una dirección IP al cliente DHCP cuando el cliente DHCP no solicita un tiempo de arriendo específico a SINEC INS. El parámetro configurado aquí sobrescribe el parámetro configurado para la subred asociada.

– Tiempo máximo de arrendamiento (segundos)

El tiempo máximo que el cliente DHCP puede solicitar para arrendar una dirección IP de SINEC INS. El parámetro configurado aquí sobrescribe el parámetro configurado para la subred asociada.

• Botón "Exportar configuraciones"

Botón para exportar las reservas de direcciones IP para clientes DHCP. El archivo creado se utiliza para hacer una copia de seguridad de la configuración.

Después de la exportación, recibirá un archivo ZIP "sinecinsDhcpClients.zip" con todas las configuraciones del cliente DHCP en formato CSV.

El archivo CSV exportado "sinecinsDhcpClients.csv" no está cifrado y el usuario puede editarlo. Después de la exportación, el CSV se edita con el sistema operativo. Tenga en cuenta que el nombre del archivo CSV, así como los nombres y el orden de las columnas contenidas no se pueden cambiar después de la exportación. De lo contrario, no será posible importar las configuraciones posteriormente.

- Botón "Importar configuraciones"

Botón para importar las reservas de direcciones IP para clientes DHCP

Los usuarios con el derecho de "Editar" pueden importar reservas de direcciones IP previamente exportadas para Clientes DHCP desde un archivo ZIP a SINEC INS.

Siga estos pasos para importar las reservas de direcciones IP:

1. Desactive el servidor DHCP antes de la importación.

2. Haga clic en "Importar configuraciones".

Se muestra la ventana de diálogo "Importar configuraciones".

3. En el navegador, navegue hasta el directorio que contiene "sinecinsDhcpClients.zip" archivo de configuración a cargar. Haga doble clic en el archivo ZIP correspondiente para aplicarlo.

4. Seleccione la casilla de verificación "Anular configuraciones existentes" para sobrescribir las entradas existentes.

Para las reservas de direcciones IP, la sobrescritura se basa en el nombre.

5. Haga clic en "Importar".

Todas las reservas de direcciones IP se importan a SINEC INS.

Durante la importación, los resultados del proceso de importación se registran en un archivo de registro. El registro

El archivo se guarda automáticamente en la PC del usuario. Cada proceso de importación es registrado por el

servicio de registro de sistema.

Encontrará una descripción general de la exportación e importación de configuraciones en el apartado "Resumen de la importación y exportación de configuraciones (Página 75)".

3.3.2 asignaciones DHCP

Las asignaciones de direcciones IP a los dispositivos se muestran en la página "Servicios de red > Servicio DHCP > Asignaciones de DHCP". La información en la columna "Tipo" especifica si la dirección IP se arrienda a un dispositivo desde un rango de direcciones IP configurado o si se "reserva" para la dirección MAC de un dispositivo. Puede configurar rangos de direcciones IP para la asignación dinámica en la página "Servicios de red > Servicio DHCP > Configuración DHCP" en el área "Rangos de direcciones IP" y para reservas de direcciones IP estáticas en el área "Reservas de direcciones IP".

Los usuarios con el derecho de "Editar" para el servicio DHCP pueden actualizar la página usando el botón "Actualizar" y convertir una asignación de dirección IP alquilada en reservada con el botón "Reservar dirección IP".

Una dirección IP reservada no se puede volver a reservar mediante el botón "Reservar dirección IP".

3.4 servicio NTP

SINEC INS se puede utilizar como servidor NTP y proporciona la hora actual a los dispositivos de la red. Como fuente de la hora actual, SINEC INS puede utilizar la hora del PC host o la hora de otro servidor NTP. Para garantizar que los clientes NTP obtengan la hora de un servidor NTP confiable, los paquetes de datos NTP se pueden proteger con algoritmos hash.

AVISO

Fuente de tiempo Servidor NTP (detección de "tiempo insano")
Cuando SINEC INS utiliza un servidor NTP diferente como fuente horaria y detecta una diferencia horaria de más de 1000 segundos entre el servidor NTP y el PC en el que está instalado SINEC INS, SINEC INS clasifica el servidor NTP como una fuente horaria no fiable y cancela el NTP Servicio. Asegúrese de que la diferencia de tiempo entre los servidores NTP y la PC SINEC INS sea inferior a 1000 segundos.

Los usuarios que tienen el derecho de "Editar" para el servicio NTP pueden configurar el servidor NTP en la página "Servicios de red > Servicio NTP".

Los siguientes parámetros están disponibles para configurar el servidor NTP:

- **Habilitar servidor NTP**
Habilita o deshabilita el servidor NTP.

Deshabilite el servidor NTP antes de configurarlo o realizar cambios en la configuración. Vuelva a habilitar el servidor NTP después de la configuración.
- **Interfaces de entrada**
Selección del adaptador de red a través del cual el servidor NTP debe recibir solicitudes NTP.
SINEC INS solo aplica los cambios en la configuración del adaptador de red en el sistema operativo después de reiniciar el servicio NTP.
- **Fuente de tiempo**
En esta área de diálogo, usted especifica qué hora utiliza SINEC INS como la hora actual y la proporciona a los clientes NTP a pedido.
 - **Dispositivo anfitrión**
SINEC INS utiliza la hora del dispositivo en el que está instalado SINEC INS como hora actual.
 - **servidor NTP**
SINEC INS utiliza la hora de un servidor NTP configurado como hora actual. El primer servidor NTP de la lista al que puede acceder SINEC INS se utiliza como fuente de tiempo. Si SINEC INS no puede llegar a ninguno de los servidores NTP configurados, SINEC INS utiliza el dispositivo host como fuente de tiempo.

Si SINEC INS debe autenticar un servidor NTP antes de utilizar la hora, introduzca el ID de clave de una clave NTP que haya configurado en el área de diálogo "Claves NTP". Para una autenticación exitosa a través de SINEC INS, la misma clave NTP debe estar instalada en este servidor NTP.

- Claves NTP

En esta área de diálogo puede configurar claves NTP. Estas claves NTP se pueden utilizar para la autenticación de servidores NTP a través de SINEC INS o para la autenticación de SINEC INS a través de clientes NTP. Asegúrese de que las claves NTP estén configuradas en el servidor NTP y en los clientes NTP.

Tenga en cuenta que, si la clave NTP ingresada tiene más de 20 caracteres, SINEC INS considera que este valor es hexadecimal. En este caso, debe seleccionar la configuración de clave NTP hexadecimal en su dispositivo.

3.5 Servicio TFTP

SINEC INS se puede utilizar como servidor TFTP para el intercambio de archivos entre clientes TFTP dentro de un área de red local.

3.5.1 Configuración TFTP

Los usuarios que tienen el derecho de "Editar" para el servicio TFTP pueden configurar el servidor TFTP. Los siguientes parámetros están disponibles para configurar el servidor TFTP en la página "Servicios de red > Servicio TFTP > Configuración TFTP":

- Habilitar servidor TFTP

Habilita o deshabilita el servidor TFTP.

Deshabilite el servidor TFTP antes de configurarlo o realizar cambios en la configuración. Vuelva a habilitar el servidor TFTP después de la configuración.

- Interfaces de entrada

- Habilitar el adaptador de red para el servicio TFTP

Selección del adaptador de red a través del cual el servidor TFTP debe recibir solicitudes TFTP. Cuando selecciona la entrada "Todos / 0.0.0.0", el servidor TFTP recibe solicitudes TFTP de todos los adaptadores de red. SINEC INS solo aplica los cambios en la configuración del adaptador de red en el sistema operativo después de reiniciar el servicio TFTP.

- Puerto

Especificación del puerto a través del cual el servidor TFTP debe recibir solicitudes TFTP.

- Directorio raíz TFTP

Visualización de la ruta al directorio raíz del servidor TFTP. Por razones de seguridad, el directorio raíz del servidor TFTP no se puede cambiar.

3.5.2 Transferencia de archivos TFTP desde la interfaz de usuario web de SINEC INS al directorio TFTP

Los usuarios que tienen el derecho de "Ver" para el servicio TFTP pueden ver los archivos y carpetas en el servidor TFTP en la página "Servicios de red > Servicio TFTP > Transferencia de archivos". Puede administrar los archivos usando la lista desplegable "Seleccione una acción". El protocolo HTTPS se utiliza para ejecutar estas acciones en SINEC INS. Los nuevos directorios solo se pueden crear a través del sistema operativo. Para directorios creados, puede navegar a directorios de nivel inferior haciendo doble clic en un directorio. Para volver a un directorio de nivel superior, haga doble clic en ".." en la primera línea del directorio. La ruta de navegación al directorio actual se muestra encima de la lista de archivos para facilitar la orientación.

Las siguientes acciones están disponibles en la lista desplegable "Seleccionar una acción":

- Actualizar

Actualiza la interfaz web

- Cargar/Descargar/Eliminar

Con estas acciones, puede cargar, descargar o eliminar uno o más archivos seleccionados.

Nota

SINEC INS debe tener derechos de acceso de lectura para cargar los archivos. De lo contrario, la transferencia de archivos fallará.

Para cargar un archivo, proceda de la siguiente

manera: 1. Seleccione la acción "Cargar" en la lista desplegable.

Aparecerá el cuadro de diálogo "Cargar".

2. Navegue en el navegador hasta el directorio en el que se encuentra el archivo a cargar.

Haga doble clic en el archivo deseado para aplicarlo.

Puede seleccionar varios archivos.

3. Haga clic en "Cargar" para cargar el archivo en el servidor TFTP.

El archivo se guarda en el directorio TFTP actual.

Cada proceso de carga es registrado por el servicio Syslog.

Para descargar un archivo, proceda de la siguiente manera:

1. Seleccione el archivo requerido de la lista de archivos. Haga clic en la casilla de verificación correspondiente.

Puede seleccionar varios archivos.

2. Seleccione "Descargar" en la lista desplegable.

3. Navegue hasta el directorio donde desea guardar el archivo y confirme el guardado.

Cada proceso de descarga es registrado por el servicio Syslog.

3.6 Servicio SFTP

SINEC INS se puede utilizar como servidor SFTP para el intercambio de archivos cifrados entre clientes SFTP.

Este tipo de transferencia de datos está protegido contra el acceso no autorizado mediante el uso de una clave privada.

El servicio SFTP se puede utilizar, por ejemplo, para actualizaciones de firmware en dispositivos de red o para realizar copias de seguridad y restaurar archivos de configuración para dispositivos de red.

El puerto predeterminado para el servidor SFTP es TCP 22. El número de puerto es configurable.

3.6.1 Configuración de SFTP

Los usuarios que tienen el derecho de "Editar" para el servicio SFTP pueden configurar el servidor SFTP y pueden exportar e importar configuraciones. Encontrará una descripción general de la exportación e importación de configuraciones en el apartado "Resumen de la importación y exportación de configuraciones (Página 75)".

Los siguientes parámetros están disponibles para configurar el servidor SFTP en la página "Servicios de red > Servicio SFTP > Configuración SFTP":

- **Habilitar servidor SFTP**

Habilita o deshabilita el servidor SFTP.

Deshabilite el servidor SFTP antes de configurarlo o realizar cambios en la configuración. Vuelva a habilitar el servidor SFTP después de la configuración.

- **Botón "Exportar configuración"**

Botón para exportar la configuración SFTP. El archivo creado se utiliza para hacer una copia de seguridad de los detalles del usuario.

Después de la exportación, recibe un archivo ZIP "sinecinsSftpUserBackup.zip" con configuraciones de usuario. Este archivo ZIP se descarga en su dispositivo a través del navegador.

Los archivos CSV exportados con usuarios SFTP son encriptados por SINEC INS.

- **Botón "Importar configuración"**

Botón para importar la configuración SFTP

Puede importar una configuración SFTP previamente exportada desde un archivo ZIP a SINEC INS.

Siga estos pasos para importar la configuración de SFTP:

1. Deshabilite el servidor SFTP antes de la importación.
2. Haga clic en "Importar configuración".

Se muestra la ventana de diálogo "Importar configuración".

3. Haga clic en "Elegir archivo" y navegue en el navegador hasta el directorio que contiene el Archivo de configuración "sinecinsSftpUserBackup.zip" a cargar. Haga doble clic en el archivo ZIP correspondiente para aplicarlo.

4. Haga clic en "Importar".

Todas las configuraciones de SFTP para los usuarios se importan a SINEC INS. Después de una importación exitosa, el archivo ZIP de SINEC INS se extrae y descifra.

Si una configuración para importar ya está presente en la base de datos, no se importará.

Tenga en cuenta que se puede importar un máximo de 10000 usuarios SFTP al mismo tiempo. Si se supera el número máximo de usuarios de SFTP, se detiene la adición de más usuarios de SFTP.

Durante la importación, los resultados del proceso de importación se registran en un archivo de registro. El archivo de registro se guarda automáticamente en el navegador de la PC del usuario. El servicio Syslog registra cada proceso de importación. Se registra toda la información sobre los usuarios no agregados.

- Interfaces de entrada

Si un dispositivo host tiene varias interfaces de red, puede habilitar las interfaces de red deseadas para el servidor SFTP. De manera predeterminada, todas las interfaces de red disponibles están habilitadas. SINEC INS utiliza el puerto TCP 22 para el servidor SFTP. Este puerto se puede configurar.

- Habilitar el adaptador de red para el servicio SFTP

Selección de los adaptadores de red disponibles a través de los cuales el servidor SFTP debe recibir solicitudes SFTP. SINEC INS solo aplica los cambios en la configuración del adaptador de red en el sistema operativo después de reiniciar el servicio SFTP.

- Puerto

Especificación del puerto TCP a través del cual el servidor SFTP debe recibir solicitudes SFTP. Asegúrese de que otra aplicación no esté utilizando el puerto especificado.

- Configuraciones de SFTP

- Directorio raíz del servidor SFTP

Muestra el directorio raíz del servidor SFTP de SINEC INS.

La ruta predeterminada "/opt/sinecins/bin/proftpd/var/sftpboot" la establece SINEC INS y no se puede cambiar.

- Habilitar limitación de velocidad saliente/entrante

Habilita las casillas de entrada para la máxima velocidad de transmisión de datos

Puede configurar la velocidad de carga y descarga del servidor SFTP para satisfacer sus necesidades. El valor debe estar entre 10 y 1000000 Kbps para la carga y descarga. Si la limitación de velocidad no está habilitada, los archivos se transfieren con la máxima velocidad posible.

– Velocidad máxima de entrada del servidor (KB/seg)

Especificación de la velocidad máxima de descarga

El valor máximo es 1000000 Kbps = 1 Gbps.

– Velocidad máxima de salida del servidor (KB/seg)

Especificación de la velocidad máxima de subida

El valor máximo es 1000000 Kbps = 1 Gbps.

– Botón "Guardar"

Guarda los cambios en las entradas de limitación de velocidad.

• Usuarios de SFTP

Los datos de usuario necesarios para la autenticación de usuarios en el servidor SFTP se pueden administrar en esta área de diálogo. Cuando el servidor SFTP recibe una solicitud de autenticación de un usuario SFTP, verifica si el usuario especificado y la contraseña asociada están configurados en esta área de diálogo. Si los datos de usuario relevantes están presentes, el usuario recibe acceso al servidor SFTP y puede cargar archivos al servidor y descargar los archivos almacenados en el servidor.

Al crear un usuario SFTP, tenga en cuenta que, para evitar posibles conexiones SFTP desde el host de Linux, el nombre de usuario no puede ser idéntico al nombre del host de Linux.

• Botón "Importar usuarios SFTP"

El botón para importar datos de usuario SFTP se encuentra a la derecha en "Usuarios SFTP" área.

Puede importar detalles de usuario SFTP creados previamente desde un archivo CSV a SINEC INS.

Siga estos pasos para importar los usuarios de SFTP:

1. Primero, cree un archivo CSV con los usuarios SFTP que se van a importar. Para ello, introduzca los datos de los usuarios de SFTP en una tabla y luego guarde la tabla como archivo CSV.

La tabla **no debe tener encabezado** y contener los datos en el siguiente orden:

– Primera columna: Nombre de usuario

– Segunda columna: Contraseña correspondiente

Los nombres de usuario y contraseñas especificados deben ser válidos. De lo contrario, no se guarda ningún dato.

Tenga en cuenta que la cantidad de usuarios SFTP que se importarán desde un archivo CSV es limitada a máx. 10000.

El delimitador de columna del archivo CSV debe ser "," (coma).

2. Deshabilite el servidor SFTP antes de la importación.

3. Haga clic en "Importar usuarios SFTP".

Aparece el cuadro de diálogo "Importar usuarios SFTP".

4. Navegue en el navegador hasta el directorio en el que se encuentra el archivo CSV que se va a cargar. Haga doble clic en el archivo deseado para aplicarlo.

5. Haga clic en "Importar".

Los datos de usuario de SFTP se importan a SINEC INS.

Durante la importación, los resultados del proceso de importación se registran en un archivo de registro. El registro El archivo se guarda automáticamente en el navegador del PC del usuario. Si un usuario a importar es ya presente en la base de datos, no se importará.

El servicio Syslog registra cada proceso de importación. La información sobre los usuarios no añadido se registra.

Si se excede el número máximo de entradas, se agregarán más usuarios SFTP. las entradas detenidas y superfluas no se registran.

- Claves SFTP SSH

El cliente puede usar una clave de host para verificar la identidad del host para asegurarse de que el se estableció la conexión con el host correcto (el servidor SFTP). SINEC INS genera pares de claves SSH con los algoritmos RSA y DSA. La longitud de una clave RSA es de al menos 2048 bits y la longitud de una clave DSA es de 1024 bits.

En esta área, puede ver las claves públicas o regenerar un par de claves SSH.

- Claves públicas RSA

Cuadro de visualización con la clave de host RSA pública actual

- Claves públicas DSA

Cuadro de visualización con la clave de host DSA pública actual

- Botón "Copiar"

Botón para copiar la clave de host pública relevante en el portapapeles

- Botón "Regenerar pares de claves SSH"

Botón para regenerar los pares de claves

Una vez confirmada la operación, las claves de host públicas y privadas se renuevan el la interfaz de usuario con algoritmos RSA y DSA.

3.6.2

Transferencia de archivos SFTP desde la interfaz de usuario web de SINEC INS al directorio SFTP

Los usuarios que tienen el derecho de "Ver" para el servicio SFTP pueden administrar directorios SFTP y cargar y descargar archivos en el servidor SFTP. El protocolo HTTPS se utiliza para ejecutar estas acciones en SINEC INS.

Los archivos y las carpetas SFTP del servidor SFTP se muestran en la página "Servicios de red > Servicio SFTP > Transferencia de archivos". La lista desplegable "Seleccione una acción" contiene acciones disponibles con las que puede administrar los directorios y archivos. Al hacer doble clic en un directorio, navega paso a paso a directorios de nivel inferior. Para volver a un directorio de nivel superior, haga doble clic en ".." en la primera línea del directorio. La ruta de navegación al directorio actual se muestra encima de la lista de archivos para facilitar la orientación.

Las siguientes acciones están disponibles en la lista desplegable "Seleccionar una acción":

- Actualizar

Actualiza la interfaz web

- Subir descargar

Con estas acciones, puede cargar uno o más archivos seleccionados en el directorio SFTP actual y descargarlos desde el directorio a su PC.

Nota

SINEC INS debe tener derechos de acceso de lectura para cargar los archivos. De lo contrario, la transferencia de archivos fallará.

- Moverse

Puede mover uno o más archivos a un directorio SFTP creado.

- Crear el directorio

Puede crear un nuevo directorio en el directorio SFTP actual.

En el área de diálogo, ingrese el nombre del directorio y guárdelo.

- Borrar

Puede eliminar uno o más archivos seleccionados en el directorio SFTP actual.

Para cargar un archivo, proceda de la siguiente

manera: 1. Navegue hasta el directorio SFTP en el que desea cargar el archivo deseado.

2. Seleccione la acción "Cargar" en la lista desplegable.

Aparecerá el cuadro de diálogo "Cargar".

3. En el navegador de su sistema operativo, navegue hasta el directorio en el que se encuentra el archivo se encuentra cargado. Haga doble clic en el archivo deseado para aplicarlo.

Puede seleccionar varios archivos. El máximo. El tamaño de los archivos a cargar es de 1024 MB.

4. Haga clic en "Cargar" para cargar el archivo en el servidor SFTP. El archivo se guarda en el actual Directorio SFTP.

Cada proceso de carga es registrado por el servicio Syslog.

Para descargar un archivo, proceda de la siguiente

manera: 1. Navegue hasta el directorio SFTP en el que se encuentra el archivo que desea descargar.

2. Seleccione el archivo. Haga clic en la casilla de verificación correspondiente.

Puede seleccionar varios archivos. Los directorios no se pueden descargar.

3. Seleccione la acción "Descargar" en la lista desplegable.

4. En el navegador de su sistema operativo, navegue hasta el directorio en el que desea guarde el archivo y confirme guardar.

Cada proceso de descarga es registrado por el servicio Syslog.

Para mover un archivo, proceda de la siguiente manera:

1. Navegue hasta el directorio SFTP en el que se encuentra el archivo que se va a mover.
2. Seleccione el archivo.

Puede seleccionar varios archivos.

3. Seleccione la acción "Mover" en la lista desplegable.

Aparece el cuadro de diálogo "Mover".

4. Seleccione el directorio de destino de la lista o navegue con un doble clic hasta el directorio de destino al que desea mover el archivo. Si desea mover el archivo al directorio raíz, no seleccione ninguna de las entradas de la lista. Con el botón "Atrás" puede volver paso a paso al directorio superior.

5. Haga clic en "Mover".

Cada proceso de movimiento es registrado por el servicio Syslog.

3.7 servicio DNS

SINEC INS se puede utilizar como servidor DNS y responder a solicitudes de resolución de nombres de dispositivos o usuarios en la red.

El puerto predeterminado para el servidor DNS, a través del cual debe recibir solicitudes, es UDP 53. El número de puerto no es configurable. Para poder habilitar el servicio DNS, asegúrese de que el puerto UDP 53 no esté siendo utilizado por otra aplicación.

3.7.1 Configuración DNS

Los usuarios que tienen el derecho de "Editar" para el servicio DNS pueden configurar el servidor DNS.

Los siguientes parámetros están disponibles para configurar el servidor DNS en la página "Servicios de red > Servicio DNS > Configuración DNS":

- **Habilitar servidor DNS**

Habilita o deshabilita el servidor DNS

Si el servidor DNS está habilitado, se debe definir al menos una zona y los registros A correspondientes. De lo contrario, el servidor DNS no puede resolver ningún nombre de dominio.

Deshabilite el servidor DNS antes de configurarlo o realizar cambios en la configuración. Vuelva a habilitar el servidor DNS después de la configuración.

- Interfaces de entrada

SINEC INS utiliza el puerto UDP 53 para el servidor DNS. Este puerto no se puede configurar. Si un dispositivo host tiene varias interfaces de red, puede habilitarlas para el servidor DNS.

De manera predeterminada, todos los adaptadores de red disponibles están habilitados.

- Habilitar el adaptador de red para el servicio DNS

Selección de los adaptadores de red a través de los cuales el servidor DNS debe recibir DNS peticiones. SINEC INS solo aplica los cambios en la configuración del adaptador de red en el sistema operativo después de reiniciar el servicio DNS.

- Lista de control de acceso (ACL)

Con las listas de control de acceso (ACL), se puede restringir el acceso al servidor DNS y el se puede aumentar la seguridad del servicio DNS. En las ACL, los dispositivos que pueden solicitar nombres de dominio y realizar solicitudes recursivas están definidos por sus direcciones IP.

Configure sus listas de control de acceso en esta área de diálogo.

Crea una nueva ACL con el botón "Crear". Puede modificar los parámetros en una ACL configurada con el botón "Editar". Las ACL que utilizan las solicitudes o zonas de DNS recursivas no se pueden eliminar. Para poder eliminar una ACL, primero debe eliminar su uso.

Ingrese los siguientes parámetros en el cuadro de diálogo para configurar una ACL nueva o existente:

- nombre de ACL

Nombre de la LCA

- Subredes / direcciones IP

Dirección de subred válida o dirección IPv4 del dispositivo

- Botón "Agregar nuevo"

Puede ingresar hasta diez direcciones IP y de subred adicionales con el botón "Agregar nuevo".

- Solicitudes de DNS recursivas

Si SINEC INS no puede responder por sí mismo a una solicitud de resolución de nombres, SINEC INS puede reenviar esta solicitud de DNS a otros servidores de nombres.

En esta área de diálogo, configura los siguientes parámetros para solicitudes DNS recursivas:

- Permitir solicitudes DNS recursivas de

Habilita o deshabilita las solicitudes de DNS recursivas a los servidores de nombres configurados en esta sección

- Botones "Crear", "Editar" y "Eliminar"

Configura un nuevo servidor de nombres recursivo con el botón "Crear". Puede crear un total de cinco servidores de nombres. Puede modificar los parámetros en un servidor de nombres configurado con el botón "Editar".

Introduzca los siguientes parámetros en el cuadro de diálogo para configurar un nombre nuevo o existente servidor:

- Nombre del servidor

- Dirección IP

Dirección IPv4 válida del servidor de nombres

– Permitir consulta desde

- Cualquier dirección IP

Seleccionada de forma predeterminada. Todos los usuarios y dispositivos pueden realizar solicitudes de DNS recursivas.

- Lista de control de

acceso Si se define al menos una ACL, esta opción se puede habilitar y la entrada ACL deseada se puede seleccionar de la lista desplegable. Solo los dispositivos ingresados en la ACL están autorizados a realizar solicitudes recursivas en este caso.

– Solo reenviar

SINEC INS primero verifica los registros DNS guardados y responde a la solicitud de DNS cuando ha encontrado el registro A correspondiente. Si la búsqueda falla, SINEC INS reenvía la solicitud a los servidores de nombres configurados. Si uno de los servidores de nombres direccionados tiene la información solicitada, la solicitud de DNS se resuelve y el usuario puede llegar al dispositivo con el nombre de dominio ingresado en el navegador.

- "Solo reenviar" activado: si ni SINEC INS ni los servidores de nombres configurados pueden responder a la solicitud de DNS, SINEC INS no vuelve a intentar contactar con otros servidores de nombres.

- "Solo reenviar" desactivado: si ni SINEC INS ni los servidores de nombres configurados pueden responder a la solicitud de DNS, SINEC INS intenta ponerse en contacto con otros servidores de nombres, incluido el servidor DNS raíz, para buscar información. Si la computadora host SINEC INS está conectada a Internet, SINEC INS también puede reenviar solicitudes de DNS al servidor de nombres, como el DNS público de Google. Esto significa que los dispositivos reciben respuestas si solicitan un nombre de dominio como www.google.com.

- Habilitar extensión DNSSEC

Habilita la extensión de seguridad del protocolo DNS para firmar los datos DNS.

Si está habilitado, la seguridad está garantizada al resolver los nombres de dominio. Si el servidor de nombres direccionado ha resuelto el nombre de dominio, asegura los datos a enviar con su firma digital. SINEC INS valida la firma. Si la autenticación es exitosa, SINEC INS confía en los datos contenidos en la respuesta y los reenvía al usuario. Luego, el usuario puede llegar al dispositivo con el nombre de dominio ingresado en el navegador. Si la autenticación falla, los datos recibidos del servidor de nombres se descartan.

Si se configuran varios servidores de nombres, la solicitud de DNS se reenvía secuencialmente al siguiente servidor de nombres hasta que se resuelva o no.

Si el servidor de nombres direccionado no admite una extensión DNSSEC pero está habilitada en SINEC INS, se rechaza la respuesta del servidor de nombres.

3.7.2 zonas DNS

Para poder resolver un nombre de dominio, el servidor DNS requiere la zona asignada al dominio que se busca. Los usuarios que tienen el derecho de "Editar" para el servicio DNS pueden configurar zonas DNS. Los usuarios con el derecho "Ver" pueden ver "Zonas DNS".

Los siguientes parámetros están disponibles para configurar las zonas DNS en la página "Servicios de red > Servicio DNS > Zonas DNS":

- Zonas DNS

En esta área de diálogo, configura las zonas DNS para definir un dominio en el árbol de dominios.

Configuras una nueva zona con el botón "Crear". Puede modificar los parámetros en una zona configurada con el botón "Editar".

Introduzca los siguientes parámetros en el cuadro de diálogo para configurar una zona nueva o existente:

- Nombre de la zona

- Permitir consulta desde

- Cualquier dirección IP

Seleccionado por defecto

- Lista de control de acceso

Si se define al menos una ACL, esta opción se puede habilitar y la entrada ACL deseada se puede seleccionar de la lista desplegable.

- Sub-zonas

Las subzonas de DNS se configuran en esta área de diálogo. Las subzonas generalmente se definen para subdominios.

Ejemplo: un dominio se divide en zonas DNS según la ubicación geográfica (Europa, Asia, América del Norte, etc.). Las subzonas pueden representar diferentes áreas dentro de cada zona DNS, por ejemplo, producción, marketing, ventas, etc.

Configuras una nueva subzona con el botón "Crear". Puede modificar los parámetros en una subzona configurada con el botón "Editar".

Ingrese los siguientes parámetros en el cuadro de diálogo para configurar un sub nuevo o existente zona:

- Nombre de la subzona

- Seleccionar zona principal

Selección de una zona principal de la lista desplegable

Nota

Eliminación de una zona

Cuando se elimina una zona o subzona, tenga en cuenta que también se eliminan todas las configuraciones asociadas, como las subzonas y los registros DNS.

3.7.3 DNS recuerdos

Los registros DNS son entradas en la base de datos de un servidor DNS en las que se asigna un nombre de dominio a cada dirección IP conocida por el servidor. El servidor busca sus registros DNS para responder a una solicitud de resolución de nombres.

Los usuarios que tienen el derecho de "Editar" para el servicio DNS pueden configurar registros DNS en la página "Servicios de red > Servicio DNS > Registros DNS".

Para poder crear registros DNS, primero debe configurar las zonas DNS en la página "Servicios de red > Servicio DNS > Registros DNS", a la que se asignan los registros DNS creados aquí. Los usuarios con el derecho "Ver" pueden ver los registros DNS.

Los siguientes parámetros están disponibles en esta página para configurar los registros DNS:

- A recuerdos

En esta área de diálogo, configura los registros A para asignar una dirección IP a un dominio.

- Seleccionar zona

Selección de una zona o una subzona de la lista desplegable

- Configure un nuevo registro A con el botón "Crear". Puedes modificar parámetros en un registro A configurado con el botón "Editar".

Ingrese los siguientes parámetros en el cuadro de diálogo para configurar un A nuevo o existente registro:

- Nombre de dominio

Nombre del dominio. Se permiten los siguientes caracteres: "az", ".", y "-". A el nombre de dominio no puede comenzar ni terminar con "-" y ".".

- Dirección IP

Dirección IPv4 para el dominio relevante

- Comentar

Texto opcional

Después de haber creado un registro A para una dirección IP, puede comunicarse con el dispositivo a través de su FQDN (Nombre de dominio totalmente calificado).

Si se crea una ACL para una zona, solo el dispositivo cuyas direcciones IP se especifican en la ACL puede recibir respuestas a sus solicitudes de DNS.

- Botón "Exportar registros A"

Botón para exportar los registros A de las zonas seleccionadas. Los usuarios con el derecho "Editar" pueden exportar registros A.

Siga estos pasos para exportar los registros A:

1. En la lista desplegable, seleccione la zona para la que desea exportar los registros A.
2. Haga clic en "Exportar registros A".

Después de la exportación, recibe un archivo CSV que contiene registros A para la zona seleccionada con pares de nombre de dominio (domain) y dirección IP (ip). El archivo CSV se descarga a su dispositivo a través del navegador. El nombre del archivo corresponde al nombre del archivo seleccionado. zona.

El archivo CSV exportado no está encriptado por SINEC INS.

• Botón "Importar registros A"

Botón para importar los registros A de la zona seleccionada. Los usuarios con el derecho "Editar" pueden importar registros A.

Siga estos pasos para importar los registros A:

1. Si no dispone de ningún archivo CSV exportado previamente con registros A, créelo en el siguiente manera:

Ingrese los registros A que consisten en el nombre de dominio y su dirección IPv4 en una tabla y luego guarde la tabla como archivo CSV.

La tabla debe tener dos columnas y contener un encabezado con los títulos "dominio, ip".

El delimitador de columna del archivo CSV debe ser "," (coma).

2. Deshabilite el servidor DNS antes de la importación.

3. En la lista desplegable, seleccione la zona o subzona para la que desea importar el archivo CSV con registros A.

4. Haga clic en "Importar registros A".

Aparecerá el cuadro de diálogo "Importar registros A".

5. Haga clic en "Elegir archivo" y navegue en el navegador hasta el directorio que contiene el archivo CSV para ser cargado. Haga doble clic en el archivo CSV correspondiente para aplicarlo.

6. Haga clic en "Importar".

Se importan nuevos registros A para la zona afectada en SINEC INS.

Si un registro A para importar ya está presente en la base de datos, no se importará, pero se registrará en el archivo de registro.

Durante la importación, los resultados del proceso de importación se registran en un archivo de registro. El registro El archivo se guarda automáticamente en el navegador del PC del usuario. El servicio Syslog registra cada proceso de importación.

Tenga en cuenta que se pueden importar un máximo de 10000 registros A al mismo tiempo. Si se excede el número máximo de registros A, se detiene la adición de más registros A.

Esta información se registra.

Encontrará una descripción general de la exportación e importación de registros A en el apartado "Resumen de la importación y exportación de configuraciones (Página 75)".

• Registros CNAME

En esta área de diálogo, configura registros CNAME para asignar un dominio o subdominio adicional a un dominio. Por lo tanto, un registro CNAME hace referencia a un dominio existente y sirve para reenviar varios nombres a la misma dirección IP, como se muestra en el ejemplo de la tabla:

Dominio/Subdominio	tipo de registro	Destino
midominio.com	Un registro	111.222.333.444
correo.midominio.com	CNOMBRE	midominio.com
libreta de direcciones.midominio.com	CNAME	midominio.com
soporte.midominio.com	CNOMBRE	midominio.com

– Seleccionar zona

Selección de una zona o una subzona de la lista desplegable

– Configuras un nuevo registro CNAME con el botón "Crear". Puede modificar parámetros en un registro CNAME configurado con el botón "Editar".

Ingrese los siguientes parámetros en el cuadro de diálogo para configurar un nuevo o existente Registro CNAME:

- CNAME

El nombre de alias del dominio. Se permiten los siguientes caracteres: "az", ".", "y" "-".

- Nombre de

dominio El nombre real del dominio o subdominio al que el registro CNAME reenvía las solicitudes.

- Comentar

Texto opcional

Administración del sistema

4.1 Configuración general

4.1.1 UMC

En la página "Administración del sistema > Configuración general > UMC", puede especificar si SINEC INS debe conectarse a UMC. La conexión a UMC permite la autenticación a través de un sistema de administración de usuarios centralizado. Los usuarios de UMC se integran en SINEC INS utilizando sus grupos de usuarios de UMC y se asignan allí a los roles deseados. Encontrará información sobre la integración de grupos de usuarios UMC en SINEC INS en el capítulo Grupos de usuarios UMC (Página 65).

UMC no está incluido en el alcance del producto SINEC INS y debe instalarse por separado.

Configuración de UMC

Los usuarios que tienen el derecho de "Editar" para la "Configuración general" pueden configurar el servidor UMC en la página "Administración del sistema > Configuración general > UMC".

Los siguientes parámetros están disponibles aquí para configurar el servidor UMC:

- Habilitar inicio de sesión SINEC INS con servidor UMC

Habilita o deshabilita el ingreso a SINEC INS con el servidor UMC

- Configuración del servidor UMC

Dirección IP y puerto del servidor UMC a través del cual SINEC INS puede llegar al UMC servidor.

- Botón "Guardar"

Guarda los datos de configuración

4.1.2 Licencia

Puede activar las licencias adquiridas para SINEC INS en la página "Administración del sistema > Configuración general > Licencia > Licencias". La página "Administración del sistema > General ajustes > Licencia > Nodos de licencia usados" proporciona información sobre el número de licencias nodos que actualmente están siendo utilizados por las licencias SINEC INS activadas y qué servicios están actualmente en uso por los nodos de licencia.

Puede encontrar información general sobre la licencia SINEC INS en la sección Tipos de licencia (Página 9).

4.1.2.1 Activación de licencias

En la página "Administración del sistema > Licencia > Licencias", puede agregar licencias para SINEC INS a través de la activación en línea o fuera de línea y ver las licencias activas de SINEC INS en la PC/dispositivo.

Licencias activas

Esta área de diálogo muestra las licencias que se activaron en la PC/dispositivo a través de la activación en línea. La licencia de demostración de SINEC INS no se muestra en esta área de diálogo. Las licencias SINEC INS que fueron activadas a través de la activación en línea se pueden deshabilitar con el botón "Liberar". Se requiere una conexión a Internet activa para esta acción. Después de desactivar las licencias, se pueden usar en una PC/dispositivo diferente con la misma clave de licencia.

Activación en línea

En esta área de diálogo puede activar su licencia SINEC INS utilizando el código que recibió al comprar la licencia. Este tipo de activación requiere una conexión a Internet en el PC/dispositivo en el que está instalado SINEC INS.

Siga estos pasos para activar la licencia:

1. Introduzca el código en el campo de entrada "Código de licencia".
2. Haga clic en el botón "Comprobar".

Si el código ingresado es válido, se muestra el tipo de licencia asociado y el botón "Activar" se activará.

3. Haga clic en el botón "Activar" para activar la licencia SINEC INS.

Activación sin conexión

En esta área de diálogo puede activar su licencia SINEC INS utilizando un contenedor de licencia que exporta desde SINEC INS.

Siga estos pasos para activar la licencia:

1. Haga clic en el botón "Exportar contenedor de licencias".
2. Navegue hasta el directorio de almacenamiento donde se encuentra el archivo.
Se almacena "SINEC_INS_LICENSE_CONTAINER.WibuCmRaC".
3. Envíe el contenedor de licencias a Siemens Industry Online Support.

Siemens Industry Online Support verifica su solicitud y luego le devolverá el contenedor de licencia que puede usar para activar su licencia SINEC INS. Guarde el archivo en su directorio de almacenamiento.

4. Haga clic en el botón "Elegir archivo".
5. Navegue hasta el directorio de almacenamiento y seleccione el contenedor de licencias
"SINEC_INS_LICENSE_CONTAINER.WibuCmRaU".
6. Confirme su selección con el botón "Abrir" y haga clic en el botón "Importar licencia".

7. Haga clic en el botón "Exportar contenedor de licencias".

8. Envíe el contenedor de licencia exportado a Siemens Industry Online Support.

Siemens Industry Online Support también completará la activación de la licencia fuera de línea en el extremo de Wibu.

Resultado

La licencia sin conexión se importa.

Desactivar la licencia sin conexión

Póngase en contacto con el servicio de atención al cliente por correo electrónico (support.automation@siemens.com). Ingrese la palabra clave "Licencia SINEC INS" en la línea de asunto. Incluya el número de licencia del paquete de licencia que desea activar en el correo electrónico.

También puede ponerse en contacto con Atención al cliente mediante una Solicitud de soporte o por teléfono; consulte el procedimiento para "Activación sin conexión".

Resultado

La licencia sin conexión está desactivada. Para activar la licencia sin conexión en un sistema nuevo, siga los pasos en "Activación de licencia sin conexión".

4.1.2.2

Nodos de licencia usados

La página "Administración del sistema > Configuración general > Licencia > Nodos de licencia usados" proporciona información sobre el número de nodos de licencia que están siendo utilizados actualmente por las licencias SINEC INS activadas y qué servicios están siendo utilizados actualmente por los nodos de licencia. Puede usar el botón "Eliminar nodos" para eliminar las direcciones IP de la licencia y así liberar la licencia para otras direcciones IP. Esto tiene sentido después de los cambios de dirección IP de los clientes Syslog y TFTP. SINEC INS considera automáticamente las direcciones IP modificadas y eliminadas de los clientes RADIUS en los nodos de licencia utilizados. Un reinicio de SINEC INS elimina automáticamente el uso de los servicios Syslog, TFTP, SFTP y DNS a través de los nodos de licencia.

4.1.3

Certificados

Por defecto, SINEC INS contiene un certificado de servidor autofirmado para conexiones HTTPS que puede volver a generar en la página "Administración del sistema > Configuración general > Certificados". Vuelva a generar el certificado del servidor cuando haya cambiado la configuración del adaptador de red del PC en el que está instalado SINEC INS. Posteriormente deberá iniciar sesión nuevamente en SINEC INS. Compruebe también el estado de los servicios de red después de cada inicio de sesión.

Si desea utilizar su propio certificado para SINEC INS en lugar del certificado del servidor predeterminado, ingrese los parámetros de este certificado, copie los archivos de su certificado en los directorios especificados y luego haga clic en "Importar". El certificado a importar deberá cumplir con los siguientes requisitos:

- El certificado debe tener uno de los formatos admitidos; vea abajo.
- El Sujeto y el Emisor del certificado deben tener una entrada CN (Nombre común).

4.1 Configuración general

- Una Entidad final debe declararse como Entidad final y una Autoridad de certificación como Certificado autoridad en las restricciones básicas.
- Se admiten los siguientes algoritmos de firma:
 - sha1-con-RSA
 - sha224-con-RSA
 - sha256-con-RSA
 - sha384-con-RSA
 - sha512-con-RSA
- Se admiten las siguientes claves públicas:
 - RSA 2048 bits
 - Bit RSA 4096
- El cuadro Uso de clave no puede estar vacío.

Una vez importado el certificado, se vuelve a establecer la conexión con SINEC INS.

Actualice su navegador unos 30 segundos después de importar el certificado.

Según el tipo de certificado, ingrese los siguientes parámetros para el certificado que está importando:

- Tipo de certificado

Puede seleccionar entre los tipos crt/cer y p12. Los certificados en formato crt/cer deben codificarse con Base64.

Para certificados crt/cer:

- Ruta al certificado

Ruta al archivo del certificado.

- Ruta a la clave privada

Ruta a la clave privada del certificado en formato pem.

- Contraseña protegida

Seleccione esta casilla de verificación si la clave privada está protegida por una contraseña.

- Contraseña de clave privada

Al usar el símbolo del ojo al lado del cuadro de entrada, puede ocultar o mostrar la contraseña.

- Firmado por CA

Seleccione esta casilla de verificación cuando el certificado haya sido firmado por una autoridad de certificación (CA).

- Ruta al certificado de CA

Ruta al archivo de certificado de CA. Si hay una cadena de certificados de CA, esta cadena de certificados debe importarse.

Para certificados p12:

- Ruta al contenedor (para certificados p12)

Ruta al archivo contenedor del certificado.

- Contraseña protegida

Seleccione esta casilla de verificación si el contenedor está protegido por una contraseña.

- Contraseña del contenedor (para certificados p12)

Al usar el símbolo del ojo al lado del cuadro de entrada, puede ocultar o mostrar la contraseña.

- Firmado por CA

Seleccione esta casilla de verificación cuando el certificado haya sido firmado por una autoridad de certificación (CA).

- Ruta al certificado de CA

Ruta al archivo de certificado de CA. Si hay una cadena de certificados de CA, esta cadena de certificados debe ser importado.

4.1.4

Configuración del puerto HTTP(S)

SINEC INS utiliza los siguientes puertos TCP por defecto:

- Puerto TCP 5053 para conexión de servidor HTTPS
- Puerto TCP 443 para conexión de interfaz de usuario web HTTPS
- Puerto TCP 80 para conexión de interfaz de usuario web HTTP

Los usuarios que tienen el derecho de "Editar" para la configuración del sistema pueden definir los puertos HTTP(S) en la página "Administración del sistema > Configuración general > Configuración del puerto HTTP(S)". El valor ingresado debe estar entre 1 - 65535 y aún no ocupado.

Ingrese el número de puerto deseado en el cuadro de entrada correspondiente y confirme el cambio con el botón "Guardar". Asegúrese de que otra aplicación no esté utilizando el puerto especificado. Sin embargo, no recomendamos usar puertos estandarizados entre 1 y 1023 para HTTP(S). Tenga en cuenta que los puertos ingresados no pueden ser idénticos.

Después de que se actualiza un puerto, la sesión del usuario finaliza porque se reinician los servicios backend y/o frontend. Necesita iniciar sesión de nuevo.

4.2 Gestión de autorizaciones

4.2.1 Componentes

Los siguientes componentes son importantes para configurar las autorizaciones de usuario:

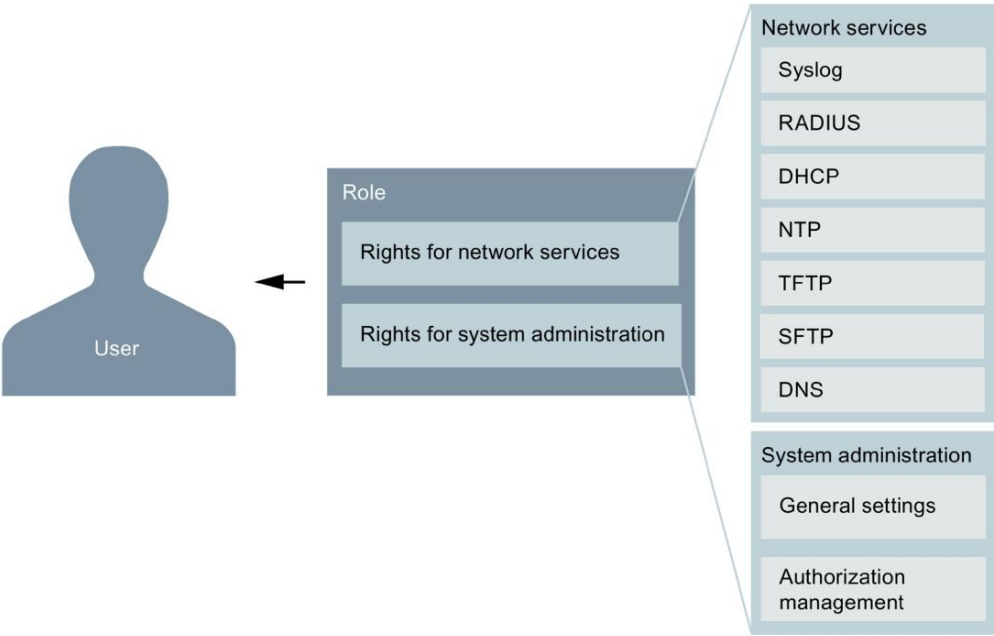


Figura 4-1 Componentes de gestión de autorizaciones

Se asignan uno o más roles a cada usuario. Cada función incluye derechos para la configuración de los servicios de red, así como para la administración del sistema.

Usuarios

Los usuarios pueden gestionarse de forma centralizada en el componente de gestión de usuarios (UMC) y luego usarse en SINEC INS o configurarse localmente en SINEC INS, consulte la sección Usuarios (Página 65).

El usuario "SuperAdmin" con el rol "admin" está disponible por defecto después de la instalación de SINEC INS. Este rol contiene todos los derechos para los servicios de red y para la administración del sistema. El usuario y el rol solo pueden ser editados o eliminados por el usuario "SuperAdmin". Puede encontrar información sobre las credenciales iniciales del usuario "SuperAdmin" en la sección Inicio de sesión (Página 15).

roles

Una función utiliza los derechos incluidos para determinar qué funciones están disponibles para el usuario, consulte la sección Funciones (Página 65).

Derechos

Hay derechos para los servicios de red y derechos para la administración del sistema. Los derechos para los servicios de red otorgan permiso para configurar servicios como RADIUS y NTP. Los derechos para la administración del sistema otorgan permiso para la configuración general y para gestión de autorizaciones. Mientras que la gestión de autorizaciones incluye la configuración de usuarios, funciones y asignaciones de funciones, la configuración general incluye la configuración de licencias y UMC, así como la configuración del certificado del servidor.

Los derechos se asignan a los roles en la página "Administración del sistema > Asignaciones de roles".

4.2.2 Usuarios

4.2.2.1 Grupos de usuarios de UMC

UMC (User Management Component) es una base de datos para la administración central de datos de usuario. En SINEC INS, los usuarios de UMC se pueden utilizar después de que se hayan incluido los grupos de usuarios de UMC especificando los nombres de los grupos de usuarios de UMC. El editor en "Administración del sistema > Usuarios > Grupos de usuarios de UMC" se puede utilizar para integrar los grupos de usuarios de UMC. El nombre especificado del grupo de usuarios de UMC en SINEC INS debe ser idéntico al nombre del grupo de usuarios de UMC en el servidor de UMC. Los nombres de los grupos de UMC distinguen entre mayúsculas y minúsculas.

El nombre del grupo de usuarios de UMC puede contener máx. 60 caracteres. Se permiten los siguientes caracteres: az, AZ, 0-9 y _ . / ' .

El usuario de un grupo de usuarios de UMC se puede utilizar para iniciar sesión cuando se configuró UMC y se especificaron los datos de dirección de UMC en SINEC INS en "Administración del sistema > Configuración general > UMC".

4.2.2.2 Usuarios locales

Como alternativa al empleo de usuarios de UMC, los usuarios se pueden configurar en "Administración del sistema > Usuarios > Usuarios locales". Los usuarios que se van a utilizar deben estar habilitados. El usuario definido por el sistema "SuperAdmin" solo se puede editar por sí mismo y no se puede eliminar.

4.2.3 roles

Puede crear, editar y eliminar roles en la página "Administración del sistema > Roles". El rol "admin" definido por el sistema solo puede ser editado por el usuario "SuperAdmin" y no puede ser eliminado.

4.2.4 **Asignaciones de roles**

En la página "Administración del sistema > Asignaciones de funciones", se pueden asignar grupos de usuarios de UMC y usuarios locales, así como derechos a las funciones que se crearon en la administración de funciones. Para que un usuario pueda iniciar sesión en SINEC INS, un usuario debe tener asignado un rol.

En la pestaña "Usuarios locales/grupos de usuarios de UMC asignados", los usuarios y grupos de usuarios de UMC deseados se asignan a un rol a través de los botones "Asignar grupos de usuarios de UMC" o "Asignar usuarios locales".

Las autorizaciones para la configuración de los servicios de red, así como los derechos para la administración del sistema, se asignan a un rol en la pestaña "Derechos".

Mensajes de registro del sistema

5.1 Estructura de los mensajes Syslog

SINEC INS admite RFC 5424 y RFC 3164 para recibir eventos. Por defecto, SINEC INS almacena los eventos en su propio servidor Syslog. Utilizando la funcionalidad de retransmisión, SINEC INS puede reenviar eventos a otros servidores Syslog. Los eventos se transfieren a este servidor Syslog de acuerdo con RFC 5424.

Un mensaje Syslog se compone de los siguientes parámetros:

Parámetro	Explicación
ENCABEZAMIENTO	
PRI	PRI contiene la prioridad codificada del mensaje Syslog, desglosada en Severidad (gravedad del mensaje) y Facilidad (origen del mensaje).
VERSIÓN	Número de versión de la especificación Syslog
MARCA DE TIEMPO	Marca de tiempo en el formato "2010-01-01T02:03:15.0003+02:00" como la hora local, incluida la zona horaria y la corrección para el horario de verano/hora estándar si es necesario.
NOMBRE DE HOST	Hace referencia a la computadora de origen con su FQDN, nombre de host o dirección IP. Dirección IPv4 según RFC1035: Bytes en representación decimal: XXX.XXX.XXX.XXX
NOMBRE DE LA APLICACIÓN	Dispositivo o aplicación desde donde se origina el mensaje. Se emite "-" si falta información.
PROCIDO	La identificación del proceso sirve para identificar claramente los procesos individuales, por ejemplo, durante el análisis y la resolución de problemas. Se emite "-" si falta información.
MSGID	ID para identificar el mensaje. Se emite "-" si falta información.
DATOS ESTRUCTURADOS	
tiempoCalidad	El elemento de datos estructurados "timeQuality" proporciona información sobre la hora del sistema. Ejemplo: [timeQuality tzKnown="0" isSynced="0"] El parámetro "tzKnown" indica si el remitente conoce su zona horaria (valor "1" = conocido; valor "0" = desconocido). El parámetro "isSynced" indica si el emisor está sincronizado con una fuente de tiempo externa fiable, por ejemplo, a través de NTP (valor "1" = sincronizado; valor "0" = no sincronizado).
GMS	
MENSAJE	Mensaje como cadena ASCII (inglés)

Nota

Información adicional

Puede leer información más detallada sobre la estructura de los mensajes Syslog y sobre el significado de los parámetros en RFC 5424 en: (<https://tools.ietf.org/html/rfc5424>)

5.2 Etiquetas en mensajes Syslog

5.2 Etiquetas en mensajes Syslog

El parámetro "MENSAJE" contiene etiquetas que se llenan dinámicamente con los datos del evento respectivo. Estas etiquetas se muestran entre corchetes {variable} en el campo "Texto del mensaje" en la sección "Lista de mensajes Syslog relacionados con la seguridad (Página 69)".

Las siguientes etiquetas aparecen en el parámetro "MESSAGE" de los mensajes de Syslog:

Etiqueta	Descripción	Formato Posible	Posibles valores o examen lleno
{Tipo de usuario}	Cadena que clasifica a los usuarios según el procedimiento de autenticación existente	%s	Local UMC
{Nombre de usuario}	Cadena que identifica al usuario autenticado en función de su nombre	%s	superadministrador
{Nombre de usuario de destino}	Cadena que identifica al usuario objetivo en función de su nombre	%s	usuario de prueba
{Nombre de rol}	Cadena que identifica un rol en función de su nombre.	%s	Administrador
{Tipo de operación}	Cadena para la designación de una operación	%s	agregado cambió actualizado eliminado editado importado exportado etc
{Tipo de servicio}	Cadena para la designación de un servicio de red SINEC INS	%s	RADIO, TFTP, Syslog, etc.
{Característica del servicio}	Cadena para la designación de una función del servicio de red	%s	Syslog Relay, clientes RADIUS, asignaciones de DHCP, etc.
{Activación de licencia Método}	Cadena para indicar el tipo de licencia actual	%s	Desconectado En línea
{Solicitar propietario Nombre}	Cadena para el nombre de usuario de autenticación WBM o Dirección MAC del dispositivo para la autenticación del puerto	%s	Estación1
{Nombre del cliente}	Cadena para el nombre de los clientes RADIUS	%s	SCALANCE_M876

5.3 Lista de mensajes Syslog relacionados con la seguridad

5.3

Lista de mensajes Syslog relacionados con la seguridad

Esta sección describe los mensajes Syslog relevantes para la seguridad. La estructura de los mensajes se basa en IEC 62443-3-3.

Identificación y autenticación de usuarios humanos

Mensaje de texto	{Tipo de usuario} Usuario {Nombre de usuario} conectado
Ejemplo	Usuario local "SuperAdmin" conectado
Explicación	Un usuario ha iniciado sesión correctamente.
Gravedad	Información
Instalaciones	local0
Estándar	Referencia IEC 62443-3-3: SR 1.1

Mensaje de texto	{Tipo de usuario} El usuario {Nombre de usuario} no pudo iniciar sesión
Ejemplo	El usuario local "SuperAdmin" no pudo iniciar sesión
Explicación	El inicio de sesión de un usuario falló.
Gravedad	Error
Instalaciones	local0
Estándar	Referencia IEC 62443-3-3: SR 1.1

Mensaje de texto	{Tipo de usuario} Usuario {Nombre de usuario} desconectado
Ejemplo	Usuario local "SuperAdmin" desconectado
Explicación	Un usuario ha cerrado sesión correctamente.
Gravedad	Información
Instalaciones	local0
Estándar	Referencia IEC 62443-3-3: SR 1.1

Gestión de cuentas de usuario

Mensaje de texto	{Tipo de usuario} El usuario {Nombre de usuario} cambió la contraseña del usuario {Tipo de usuario} {Nombre de usuario de destino}
Ejemplo	El usuario local "SuperAdmin" cambió la contraseña del usuario local "Tester"
Explicación	Un usuario ha cambiado la contraseña de otro usuario.
Gravedad	Aviso
Instalaciones	local0
Estándar	Referencia IEC 62443-3-3: SR 1.3

Mensaje de texto	{Tipo de usuario} Usuario {Nombre de usuario} deshabilitado {Tipo de usuario} usuario {Nombre de usuario de destino}
Ejemplo	Usuario local "SuperAdmin" deshabilitado Usuario local "Tester"
Explicación	Un usuario ha deshabilitado la cuenta de usuario de otro usuario.
Gravedad	Aviso
Instalaciones	local0
Estándar	Referencia IEC 62443-3-3: SR 1.3

Mensajes Syslog 5.3

Sistema de mensajes de seguridad

Mensaje de texto	{Tipo de usuario} Usuario {Nombre de usuario} creado {Tipo de usuario} usuario {Nombre de usuario de destino}
Ejemplo	Usuario local "SuperAdmin" creado Usuario local "Tester"
Explicación	Un usuario ha creado una cuenta de usuario.
Gravedad	Aviso
Instalaciones	local0
Estándar	Referencia IEC 62443-3-3: SR 1.3

Mensaje de texto	{Tipo de usuario} Usuario {Nombre de usuario} cambió {Tipo de usuario} usuario {Nombre de usuario de destino}
Ejemplo	El usuario local "SuperAdmin" cambió el usuario local "Tester"
Explicación	Un usuario ha cambiado una cuenta de usuario existente.
Gravedad	Aviso
Instalaciones	local0
Estándar	Referencia IEC 62443-3-3: SR 1.3

Mensaje de texto	{Tipo de usuario} Usuario {Nombre de usuario} cambió {Tipo de usuario} usuario {Nombre de usuario de destino} a {Nombre de usuario de destino}
Ejemplo	El usuario local "SuperAdmin" cambió el usuario local "Tester1" a "Tester2"
Explicación	Un usuario ha cambiado el nombre de un usuario existente.
Gravedad	Aviso
Instalaciones	local0
Estándar	Referencia IEC 62443-3-3: SR 1.3

Mensaje de texto	{Tipo de usuario} Usuario {Nombre de usuario} eliminado {Tipo de usuario} Usuario {Nombre de usuario de destino}
Ejemplo	Usuario local "SuperAdmin" eliminado Usuario local "Tester"
Explicación	Un usuario ha eliminado una cuenta de usuario existente.
Gravedad	Aviso
Instalaciones	local0
Estándar	Referencia IEC 62443-3-3: SR 1.3

Mensaje de texto	{Tipo de usuario} Usuario {Nombre de usuario} habilitado {Tipo de usuario} Usuario {Nombre de usuario de destino}
Ejemplo	Usuario local "SuperAdmin" habilitado Usuario local "Tester"
Explicación	Un usuario ha habilitado la cuenta de usuario de otro usuario.
Gravedad	Aviso
Instalaciones	local0
Estándar	Referencia IEC 62443-3-3: SR 1.3

Gestión de los identificadores

Mensaje de texto	{Tipo de usuario} El usuario {Nombre de usuario} agregó una coincidencia de rol de usuario
Ejemplo	El usuario local "SuperAdmin" agregó una coincidencia de rol de usuario
Explicación	Un usuario ha asignado los grupos de usuarios de UMC o los usuarios locales a un rol.
Gravedad	Aviso
Instalaciones	local0
Estándar	IEC 62443-3-3: SR 1.4

5.3 Lista de mensajes Syslog relacionados con la seguridad

Mensaje de texto	{Tipo de usuario} El usuario {Nombre de usuario} eliminó una coincidencia de rol de usuario
Ejemplo	El usuario local "SuperAdmin" eliminó una coincidencia de rol de usuario
Explicación	Un usuario ha eliminado la asignación de un rol a los grupos de usuarios de UMC o usuarios locales.
Gravedad	Aviso
Instalaciones	local0
Estándar	IEC 62443-3-3: SR 1.4

Mensaje de texto	{Tipo de usuario} Usuario {Nombre de usuario} rol creado {Nombre de rol}
Ejemplo	El usuario local "SuperAdmin" creó el rol "Servicio"
Explicación	Un usuario ha creado un rol.
Gravedad	Aviso
Instalaciones	local0
Estándar	IEC 62443-3-3: Referencia SR 1.4

Mensaje de texto	{Tipo de usuario} Usuario {Nombre de usuario} Rol eliminado {Nombre de rol}
Ejemplo	El usuario local "SuperAdmin" eliminó la función "Servicio"
Explicación	Un usuario ha eliminado un rol.
Gravedad	Aviso
Instalaciones	local0
Estándar	IEC 62443-3-3: Referencia SR 1.4

Mensaje de texto	{Tipo de usuario} Usuario {Nombre de usuario} Rol actualizado {Nombre de rol}
Ejemplo	Usuario local "SuperAdmin" rol actualizado "Servicio"
Explicación	Un usuario ha cambiado la configuración de un rol existente.
Gravedad	Aviso
Instalaciones	local0
Estándar	Referencia IEC 62443-3-3: SR 1.4

Mensaje de texto	{Tipo de usuario} Usuario {Nombre de usuario} rol actualizado {Nombre de rol} a {Nombre de rol}
Ejemplo	El usuario local "SuperAdmin" actualizó el rol "Service01" a "Service02"
Explicación	Un usuario ha cambiado el nombre de un rol existente.
Gravedad	Aviso
Instalaciones	local0
Estándar	Referencia IEC 62443-3-3: SR 1.4

Mensaje de texto	{Tipo de usuario} Usuario {Nombre de usuario} rol cambiado Derechos de {Nombre de rol}
Ejemplo	El usuario local "SuperAdmin" cambió el rol "SyslogAdmin" derechos
Explicación	Un usuario ha cambiado los derechos de un rol existente.
Gravedad	Aviso
Instalaciones	local0
Estándar	Referencia IEC 62443-3-3: SR 1.4

5.3 Lista de mensajes Syslog relacionados con la seguridad

Intentos de inicio de sesión fallidos

Mensaje de texto	La sesión del usuario {Tipo de usuario} {Nombre de usuario} finalizó después de 10 minutos de inactividad
Ejemplo	La sesión del usuario local "SuperAdmin" finalizó después de 10 minutos de inactividad
Explicación	Se cerró la sesión de un usuario por inactividad.
Gravedad	Advertencia
Instalaciones	local0
Estándar	Referencia IEC 62443-3-3: SR 2.5

Identificación y autenticación de dispositivos

Mensaje de texto	Se acepta la solicitud de autenticación de {Request Owner Name} para el cliente RADIUS {Client Name}
Ejemplo	Se acepta la solicitud de autenticación de "Estación 1" para el cliente Radius "SCALANCE_M876_1".
Explicación	El acceso al dispositivo se otorga debido a una autenticación 802.1X exitosa.
Gravedad	Información
Instalaciones	Seguridad/autorización
Estándar	Referencia IEC 62443-3-3: SR 1.2

Mensaje de texto	Solicitud de autenticación de {Request Owner Name} para el cliente RADIUS: {Client Name} rechazada
Ejemplo	Se rechaza la solicitud de autenticación de "Estación 1" para el cliente Radius "SCALANCE_M876_1".
Explicación	Se denegó el acceso al dispositivo debido a una autenticación 802.1X fallida.
Gravedad	Advertencia
Instalaciones	Seguridad/autorización
Estándar	Referencia IEC 62443-3-3: SR 1.2

Limitación del número de sesiones simultáneas

Mensaje de texto	Se superó el número máximo de 10 sesiones de inicio de sesión simultáneas
Ejemplo	Se superó el número máximo de 10 sesiones de inicio de sesión simultáneas
Explicación	Se ha superado el número máximo de sesiones web simultáneas.
Gravedad	Advertencia
Instalaciones	local0
Estándar	Referencia IEC 62443-3-3: SR 2.7

no negación

Mensaje de texto	Configuración de {Tipo de usuario} Usuario {Nombre de usuario} {Tipo de operación} {Tipo de servicio} {Característica del servicio}
Ejemplos	El usuario local "SuperAdmin" cambió la configuración de las interfaces de red de Syslog El usuario de UMC "Tester" actualizó una configuración de rangos de IP de DHCP El usuario local "SuperAdmin" agregó una configuración de IP específica del host DHCP El usuario local "SuperAdmin" eliminó una configuración de grupo de usuarios de retransmisión RADIUS
Explicación	Un usuario ha cambiado una configuración.
Gravedad	Información
Instalaciones	local0
Estándar	IEC 62443-3-3 Referencia: SR 2.12

5.3 Lista de mensajes Syslog relacionados con la seguridad

Mensaje de texto	{Tipo de usuario} El usuario {Nombre de usuario} activó una licencia de {Método de activación de licencia}
Ejemplo	El usuario local "SuperAdmin" activó una licencia en línea
Explicación	Un usuario ha habilitado una licencia.
Gravedad	Información
Instalaciones	local0
Estándar	IEC 62443-3-3 Referencia: SR 2.12

Mensaje de texto	{Tipo de usuario} El usuario {Nombre de usuario} liberó una licencia
Ejemplo	El usuario local "SuperAdmin" liberó una licencia
Explicación	Un usuario ha liberado una licencia.
Gravedad	Información
Instalaciones	local0
Estándar	IEC 62443-3-3 Referencia: SR 2.12

Integridad del software y de la información

Mensaje de texto	La verificación de integridad falló para el servicio {tipo de servicio}
Ejemplo	La verificación de integridad falló para el servicio Syslog
Explicación	La verificación de integridad falló.
Gravedad	Error
Instalaciones	local0
Estándar	Referencia IEC 62443-3-3: SR 3.4

5.3 Lista de mensajes Syslog relacionados con la seguridad

Apéndice A

A.1 Descripción general de la importación y exportación de configuraciones

Importación de configuraciones propias

Para algunos servicios de red, los usuarios que tienen el derecho de "Editar" para el servicio de red relevante pueden importar sus propios archivos CSV con datos de configuración. La siguiente tabla proporciona una descripción general de los datos y requisitos necesarios para importar las configuraciones. El orden de los datos se especifica en la columna "Número de columna y datos de entrada" y no se puede cambiar. Los nombres, contraseñas, direcciones IP y direcciones MAC especificadas deben ser válidos. De lo contrario, no se guarda ningún dato. El delimitador de columna en el archivo CSV debe ser "," (coma). El número de configuraciones a importar desde un archivo CSV no puede ser más de 10000 entradas. Antes de la importación, debe deshabilitar el servicio de red correspondiente.

Servicio	Botón para importar	Cabecera en el archivo CSV	Número de columna y datos de entrada	Comentario
Servicio RADIO > Configuración de RADIO	Importar radio nosotros	No	1. Nombre de usuario 2. Contraseña 3. administrador/operador	Los nombres de usuario y las contraseñas distinguen entre mayúsculas y minúsculas. El tipo de usuario "admin" recibe permisos de escritura para clientes RADIUS y el tipo de usuario "operador" recibe permisos de lectura.
	Importar clientes de radio	No	1. Nombre del cliente RADIUS 2. dirección IP 3. Secreto compartido 4. sí/no	Los nombres y los secretos compartidos distinguen entre mayúsculas y minúsculas. El parámetro "yes" habilita el atributo Message-Authenticator en el cliente RADIUS (p. ej., para dispositivos SCALANCE). El parámetro "no" desactiva el atributo Message Authenticator en el Cliente RADIUS (por ejemplo, para dispositivos RUGGEDCOM).
	Importe radius de vices	No	1. Dirección MAC 2. Nombre de VLAN/VLAN	"-" o ":" se puede utilizar para las direcciones MAC. Las direcciones MAC distinguen entre mayúsculas y minúsculas.
Servicio SFTP > Configuración de SFTP	Importar usuarios SFTP	No	1. Nombre de usuario 2. Contraseña	Los nombres de usuario y las contraseñas distinguen entre mayúsculas y minúsculas
Servicio DNS > DNS recuerdos	Importar registros A	Sí: dominio, ip	1. Nombre de dominio 2. Dirección IP del dominio	Los nombres de dominio distinguen entre mayúsculas y minúsculas

Exportación e importación de configuraciones SINEC INS

Los usuarios que tienen el derecho de "Editar" para el servicio de red relevante pueden exportar las configuraciones del servicio de red para hacer una copia de seguridad de los datos de configuración. El botón "Exportar configuraciones" está disponible para el servicio de red relevante para este propósito. Puede importar la configuración a SINEC INS con el botón "Importar configuraciones" del servicio de red respectivo. Antes de la importación, debe deshabilitar el servicio de red correspondiente. Algunos archivos CSV no están cifrados y los usuarios pueden editarlos. Después de la exportación, los archivos CSV se editan con el sistema operativo. Tenga en cuenta que los nombres de los archivos ZIP y CSV, así como los nombres y el orden de las columnas que contienen, no se pueden cambiar.

La siguiente tabla le ofrece una descripción general de los servicios de red para los que puede exportar las configuraciones con el botón "Exportar configuraciones":

Servicio	Nombre del archivo ZIP y contenido del archivo	Comentario
Servicio RADIO > configuración de RADIO	sinecinsRadiusConfiguration.zip • sinecinsRadiusUsers.csv • sinecinsRadiusClients.csv • sinecinsRadiusEndDevices.csv	Los "sinecinsRadiusUsers.csv" y "sinecinsRadiusClients.csv" están encriptados y no se pueden editar. El archivo "sinecinsRadiusEndDevices.csv" no está encriptado y puede ser editado por el usuario.
Servicio DHCP > Configuración DHCP > reservas de direcciones IP	sinecinsDhcpClients.zip • sinecinsDhcpClients.csv	El archivo CSV no está cifrado y el usuario puede editarlo.
Servicio SFTP > Configuración de SFTP	sinecinsSftpUserBackup.zip • sinecinsSftpUserBackup.csv	El archivo CSV está encriptado y no se puede editar

También puede exportar los archivos como archivos CSV con los siguientes servicios de red:

Servicio	Botón para exportar	Comentario
Servicio de registro del sistema > Mensajes de registro del sistema	Exportar mensajes	El archivo no está encriptado.
Servicio DNS > DNS recuerdos > A recuerdos	Exportar registros A	El archivo no está cifrado y puede ser editado por el usuario. Puede importar el archivo con "Importar registros A". El nombre del archivo se puede seleccionar libremente.

Índice

A

- Gestión de autorizaciones
 - Usuarios locales, 65
 - Asignación de roles, 66
 - papeles, 65
 - usuarios de UMC, 65

D

- servicio DHCP, 39
 - asignaciones DHCP, 43
 - configuración DHCP, 39
- servicio DNS
 - configuración DNS, 52
 - DNS records, 56
 - zonas DNS, 55

Y

- Exportación e importación de configuraciones
 - Resumen, 76

GRAMO

- Glosario, 5

H

- Configuración de
 - puertos HTTP(S), 63

I

- Importación de configuraciones
 - Resumen, 75
- Inicio de sesión inicial, 15
- Instalación, 12
 - Validación de firma, 12

I

- licencia, 59
 - Activación de una licencia, 60

SINEC INS

Instrucciones de servicio, 02/2021, C79000-G8976-C566-02

- Tipos de licencia, 9
- activación sin conexión, 60
- activación en línea, 60

METRO

- Migración, 13

norte

- servicio NTP, 44
 - configuración NTP, 44

PAGE

- Puertos utilizados, 11

R

- servicio RADIO, 31
 - configuración RADIO, 33
 - Configuración de relés, 39
- Eliminación, 14

S

- servicio SFTP, 47
 - transferencia de archivos, 50
 - configuración SFTP, 47
- Glosario SIMATIC NET, 5
- Configuración de registro del sistema
 - Syslog seguro, 27
- Mensajes de registro del sistema
 - Instalaciones, 24
 - Lista de mensajes Syslog relevantes para la seguridad, 69
 - parámetro, 67
 - Severidades, 25
 - variables, 68
- servicio syslog, 23
 - Configuración de Syslog, 25
 - filtro Syslog, 31
 - Mensajes de Syslog, 23
- Administración del sistema
 - Certificados, 61
 - licencia, 59
 - IMU, 59

Requisitos del sistema

- Requisitos de hardware, 10
- Requisitos de software, 10

T

servicio TFTP, 45

- configuración TFTP, 45

tu

configuración UMC, 59

Interfaz de usuario

- configuración, 21
- Página de inicio, 17

Usuarios

- Usuarios locales, 65
- usuarios de UMC, 65