

SIEMENS

RED SIMÁTICA

Comunicación remota industrial

- Redes remotas

SINEMA Remote Connect - Servidor

Instrucciones de operación

Prefacio

Aplicación y propiedades

1

Requisitos para la operación

2

Instalación y puesta en marcha

3

Configurando con Web Gestión Basada

4

Conservación y mantenimiento

5

Apéndice A

A

apéndice B

B

Apéndice C

C

Apéndice D

D

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 **pueden** producirse 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.

Prefacio

Propósito de esta documentación

Este manual le ayuda a instalar, configurar y operar la aplicación SINEMA RC Server.

Validez de esta documentación

Este manual es válido para la siguiente versión de software:

- SINEMA Remote Connect a partir de la versión V3.0

Licencias

Las siguientes licencias están disponibles para el producto:

Nombre del producto	número de artículo de las licencias	Número de participantes configurables (usuarios y dispositivos)
Conexión remota SINEMA	6GK1720-1AH01-0BV0	4
Conexión remota SINEMA 64	6GK1722-1JH01-0BV0	+64
Conexión remota SINEMA 256	6GK1722-1MH01-0BV0	+256
Conexión remota SINEMA 1024	6GK1722-1QH01-0BV0	+1024

Los siguientes productos están disponibles para activar la conexión a SINEMA Remote Conectar servidor:

Nombre del producto	Número de artículo
LLAVE-PLUG SINEMA RC (SCALANCE M-800, SCALANCE S615)	6GK5908-0PB00
Licencia SINEMA RC UMC	6GK1724-2VH03-0BV0
Licencia SINEMA RC Client (1 cliente VPN)	6GK1721-1XG03-0AA0
Licencia de cliente SINEMA RC (OSD)	6GK1721-1XG03-0AK0
Licencia API SINEMA RC	6GK1724-3VH03-0BV0

Las siguientes licencias están disponibles para la conexión a UMC:

Licencia de software	Número de artículo
Licencia de alquiler del componente de gestión de usuarios (UMC) de TIA Portal para 100 cuentas de usuario y 365 días Certificado de Licencia para descargar	6ES7823-1UE30-0YA0
Licencia de alquiler del componente de gestión de usuarios (UMC) de TIA Portal para 4000 cuentas de usuario y 365 días Certificado de Licencia para descargar	6ES7823-1UE10-0YA0

Productos compatibles

En la sección "Nodos conectables (Página 24)" encontrará información sobre los nodos compatibles.

Abreviaturas/acrónimos y terminología

• CINE RC

En el resto del manual, el software "SINEMA Remote Connect" se abrevia como "SINEMA RC".

• SCALANCE M-800

Esta abreviatura se aplica a los siguientes dispositivos si el contenido de la descripción se aplica igualmente a estos dispositivos en el contexto relevante:

- SCALANCE M874-2
- SCALANCE M874-3
- SCALANCE M876-3
- SCALANCE M876-4
- ESCALANCE M812
- ESCALANCE M816

• UMC

Esta abreviatura se utiliza para "Componente de gestión de usuarios", una base de datos para la administración central de los datos de los usuarios.

• API

Esta abreviatura significa "Interfaz de programación de aplicaciones", una interfaz AP basada en HTTP a través de la cual puede configurar el WBM del servidor SINEMA RC.

Nuevo en esta versión

- Dirección IPv6 para el servidor SINEMA RC
- Interfaz AP basada en HTTP
- Nueva estructura del menú "Sistema"
- Nuevo menú "Servicios"
- Conexión basada en la nube
- Compatibilidad con
- DHCP • Registro de los eventos del cortafuegos • Descarga del software SINEMA RC Client del servidor SINEMA RC •
- Visualización de los textos informativos específicos del cliente en la pantalla de inicio de sesión del servidor • Aplicación del logotipo específico del cliente en la pantalla del SINEMA RC Client

Experiencia requerida

Para poder configurar y operar el sistema descrito en este documento, necesita experiencia con los siguientes productos, sistemas y tecnologías:

- SIMATIC NET - Redes remotas
- Comunicación basada en IP
- STEP 7 Básico/Profesional
- SIMATIC S7

Más documentación

- Manual de instrucciones "SINEMA Remote Connect Client"

Este manual le ayuda a instalar, configurar y operar la aplicación SINEMA RC Client.

- Primeros pasos "SINEMA Remote Connect"

A partir de un ejemplo, se muestra la configuración de SINEMA Remote Connect.

- Primeros pasos "Servidor API SINEMA Remote Connect"

Este manual le ayuda con la configuración WBM del servidor SINEMA RC a través de la interfaz AP.

- Primeros pasos "Instalación en la nube de SINEMA RC"

Este manual le ayuda con la instalación de SINEMA RC en la nube.

Encontrará el manual en las páginas de Internet de Siemens Industry Online Support

- *Manual de usuario de la interfaz de usuario web de UMC*

Este manual lo ayuda a crear y administrar cuentas de usuario en la UMC.

Manuales actuales y más información

Encontrará los manuales actuales y más información sobre productos de redes remotas en las páginas de Internet de Siemens Industry Online Support:

- Usando la función de búsqueda:

Enlace al soporte en línea de la industria de

Siemens (<https://support.industry.siemens.com/cs/ww/en/ps/21816>)

Introduzca el ID de entrada del manual correspondiente como elemento de búsqueda.

- a través de la navegación en el área "Redes remotas":

Enlace al área "Redes remotas" (<https://support.industry.siemens.com/cs/ww/en/ps/21778>)

Vaya al grupo de productos requerido y realice los siguientes ajustes:

Pestaña "Lista de entradas", Tipo de entrada "Manuales"

Prefacio

Encontrará la documentación de los productos relevantes aquí en el medio de almacenamiento de datos que se envía con algunos productos:

- CD del producto/DVD del producto
- Colección de manuales SIMATIC NET

Condiciones de la licencia

Nota**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 los siguientes documentos en el soporte de datos suministrado:

- OSS_SINEMA-RC_86.pdf

Informacion de seguridad

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

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

Desmantelamiento

Apague el dispositivo correctamente para evitar que personas no autorizadas accedan a datos confidenciales en la memoria del dispositivo.

Para hacer esto, restablezca la configuración de fábrica en el dispositivo.

Restaure también la configuración de fábrica en el medio de almacenamiento.

Capacitación, Servicio y Soporte

Encontrará información sobre Formación, Servicio y Soporte en el documento multilingüe "DC_support_99.pdf" en el soporte de datos suministrado con la documentación.

Glosario SIMATIC NET

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

Aquí encontrará el glosario SIMATIC NET:

- Colección de manuales SIMATIC NET o DVD del producto

El DVD se envía con ciertos productos SIMATIC NET.

- En Internet con el siguiente ID de entrada:

50305045 (<https://support.industry.siemens.com/cs/ww/en/view/50305045>)

Marcas registradas

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

® están

SINEMA, ESCALANCE

Prefacio

Tabla de contenido

Prefacio.....	3
1 Aplicación y propiedades	13
1.1 Solicitud	13
1.2 Vista general de las funciones.....	14
1.3 Concepto de usuario.....	15
1.4 Ejemplo de configuración	17
1.4.1 TeleControl con SINEMA RC	17
1.5 Distribución automática de certificados y firmware	19
1.5.1 Actualización automática de certificados y firmware	19
1.5.2 Actualización de certificados con conexión de reserva.....	21
2 Requisitos para el funcionamiento	23
2.1 Requisitos	23
2.2 Nodos conectables	24
2.3 Información de licencia	26
2.4 Caracteres permitidos.....	27
2.5 Datos de rendimiento	28
3 Instalación y puesta en marcha	29
3.1 Recomendaciones de seguridad.....	29
3.2 Instalación del servidor SINEMA RC	33
3.3 Primera puesta en servicio de equipos finales con WBM	35
4 Configuración con administración basada en web	37
4.1 Apertura de Administración basada en web	37
4.2 Inicio del WBM.....	37
4.2.1 Iniciar sesión con nombre de usuario y contraseña	37
4.2.2 Inicio de sesión con UMC	39
4.2.3 Inicio de sesión con la tarjeta inteligente/certificados de usuario	41
4.3 Disposición de la ventana	44
4.4 Selección de idioma.....	47
4.5 Sistema	47
4.5.1 Visión de conjunto.....	47
4.5.2 Tronco.....	48
4.5.2.1 Registrar mensajes	48
4.5.2.2 Archivos de registro	50
4.5.2.3 Registro de cortafuegos.....	50

Tabla de contenido

4.5.3	Configuración de la red.....	51
4.5.3.1	Interfaces	51
4.5.3.2	DNS.....	53
4.5.3.3	Servidor web	54
4.5.3.4	Hacer ping.....	55
4.5.3.5	Rutas estáticas	55
4.5.4	Espacios de direcciones	56
4.5.4.1	Espacio de direcciones de red	56
4.5.4.2	Espacios de direcciones VPN.....	57
4.5.5	Fecha y hora.....	58
4.5.6	Mensajes SMS y correos electrónicos.....	59
4.5.6.1	Proveedor de puerta de enlace SMS	59
4.5.6.2	Configuración de correo electrónico	60
4.5.7	Licencias.....	62
4.5.7.1	Resumen	62
4.5.7.2	Licencias en línea	63
4.5.7.3	Licencias fuera de línea	64
4.5.8	Actualizar	sesenta y cinco
4.5.9	Copia de seguridad y restauración	67
4.5.9.1	Copias de seguridad.....	67
4.5.9.2	Ajustes.....	69
4.5.10	Gestión de energía.....	70
4.5.10.1	Administración de energía	70
4.5.10.2	Partición de arranque	70
4.5.11	Ajustes.....	71
4.5.11.1	Información del servidor	71
4.5.11.2	Cierre de sesión automático	72
4.6	Conexiones remotas	72
4.6.1	Administrar dispositivos	72
4.6.1.1	Descripción general de la gestión de dispositivos	72
4.6.1.2	Creación de un nuevo dispositivo	75
4.6.1.3	Actualización de dispositivos	80
4.6.2	Grupos de participantes	81
4.6.3	Relaciones de comunicación	82
4.6.4	Asignación de un nodo a un grupo	84
4.7	Cuentas de usuario	84
4.7.1	Vista general de las cuentas de usuario	84
4.7.2	Gestión de roles y derechos	86
4.7.3	Crear un nuevo usuario	88
4.7.4	Acuerdo del Usuario.....	92
4.7.5	Software de cliente	92
4.7.5.1	Software de cliente	92
4.7.5.2	Configuración del cliente	93
4.7.5.3	Licencias de cliente.....	94
4.8	Servicios.....	94
4.8.1	FUEGO	94
4.8.2	Configuración de UMC	95
4.8.3	Carga del servidor	96
4.8.4	Cliente Syslog	97
4.8.5	Inicio de sesión de depuración.....	98

4.9	Seguridad	100
4.9.1	Gestión de certificados.....	100
4.9.1.1	Descripción general de la gestión de certificados	100
4.9.1.2	certificado CA	101
4.9.1.3	Certificado de servidor.....	102
4.9.1.4	Importación del certificado del servidor web.....	103
4.9.1.5	Certificado de dispositivo	105
4.9.1.6	Configuración de los certificados	106
4.9.2	Conexiones VPN.....	107
4.9.2.1	Configuración básica de VPN.....	107
4.9.2.2	Configuración de OpenVPN.....	107
4.9.2.3	Realización de la configuración de IPsec	108
4.9.2.4	Creación de perfiles IPsec.....	110
4.9.3	Gestión de certificados PKI.....	111
4.9.3.1	Certificado CA de PKI	111
4.9.3.2	Bloqueo de tarjeta inteligente/certificado de usuario.....	112
4.9.4	Gestión de certificados Syslog.....	114
4.9.4	Certificados CA de Syslog.....	114
.4.1	Certificados de Syslog.....	116
4.9.4.2	4.9.4.3 Revocación de certificados de Syslog	117
4.10	Mi cuenta.....	119
4.10.1	Certificado de usuario.....	119
4.10.2	Cambia la contraseña	120
4.10.3	Descargar software de cliente	120
5	Conservación y mantenimiento	123
5.1	Copia de seguridad y restauración de la configuración del sistema	123
5.2	Actualización del sistema V1.2 > V1.3.....	125
5.3	Actualización del sistema V2.0 > V2.1.....	130
5.4	Actualización del sistema V2.1 > V3.0.....	133
A	Apéndice A	135
A.1	Conexión OpenVPN a un dispositivo iOS.....	135
B	Apéndice B.....	137
B.1	Habilitación de la dirección de correo electrónico	137
B.2	Monitoreo y tiempo de respuesta de mensajes SMS de despertador	138
C	Apéndice C.....	139
C.1	Mensajes de Syslog.....	139
C.1.1	Etiquetas en los mensajes de Syslog	139
C.1.2	Lista de mensajes de Syslog	140
C.1.2.1	Identificación y autenticación de usuarios humanos	140
C.1.2.2	Gestión de cuentas de usuario	140
C.1.2.3	Gestión de los identificadores	143
C.1.2.4	Intentos de inicio de sesión fallidos	144
C.1.2.5	Acceso a través de redes no confiables	145
C.1.2.6	Identificación y autenticación de dispositivos	146
C.1.2.7	No repudio	146
C.1.2.8	Copia de seguridad de datos en el sistema de automatización (copia de seguridad)	147

Tabla de contenido

C.1.2.9	Restauración del sistema de automatización	148
C.1.2.10	Configuración de seguridad de red y TI	151
C.1.2.11	Estado del sistema	152
D Apéndice D		153
D.1	Cifrados utilizados	153
Índice		157

Aplicación y propiedades

1.1 Solicitud

Uso del servidor SINEMA Remote Connect

SINEMA RC Server proporciona una gestión de conexión de extremo a extremo de redes distribuidas a través de Internet. Esto también incluye el acceso remoto seguro a las redes subyacentes con fines de mantenimiento, control y diagnóstico. La comunicación entre SINEMA RC Server y los participantes remotos se realiza a través de un túnel VPN teniendo en cuenta los derechos de acceso almacenados. La conexión se establece codificada mediante IPsec u OpenVPN.

El SINEMA RC Server se puede configurar a través de Web Based Management (WBM).

La conexión al WBM a través de Internet/WAN se realiza a través del protocolo HTTPS. Para establecer una conexión con el WBM del servidor, los usuarios deben iniciar sesión ingresando un nombre de usuario y contraseña o con una tarjeta inteligente.

Productos compatibles

Los siguientes productos son adecuados para la conexión al SINEMA RC Server:

- SCALANCE M874, SCALANCE M876, SCALANCE M816, SCALANCE M826, SCALANCE M804PB
- SCALANCE S615
- Cliente SINEMA RC
- SCALANCE S602, SCALANCE S612, SCALANCE S623, SCALANCE S627-2M
- SCALANCE SC632-2C, SCALANCE SC636-2C, SCALANCE SC642-2C, SCALANCE SC646-2C
- CP 1200
- CP 1543-1, CP 1543-1SP
- RM 1224
- RTU3010C, RTU3030C, RTU3031C, RTU3041C

En el apartado "Estaciones conectables (Página 24)" encontrará información sobre qué versiones de producto y SINEMA RC son compatibles entre sí.

Aplicación y propiedades**1.2 Resumen de funciones****Concepto de protección**

Para proteger el servidor SINEMA RC de accesos no autorizados, el acceso al sistema está protegido de varias formas:

- Autenticación
 - El acceso está protegido con contraseña introduciendo el nombre de usuario y la contraseña, consulte la sección "Crear un nuevo usuario (Página 88)".
 - El acceso se logra mediante una tarjeta inteligente con un procedimiento de PIN (Número de Identificación Personal). Para comprobar la identidad se utiliza un certificado.
- Derechos y funciones de los usuarios

Los derechos de acceso dependientes de la tarea se especifican mediante roles y derechos de usuario. Para obtener información más detallada, consulte el apartado "Gestión de roles y derechos (Página 86)".

1.2 Resumen de funciones

Configuración del servidor SINEMA Remote Connect

El servidor SINEMA RC se puede configurar a través de una gestión basada en web (WBM). Además, a través de la interfaz AP basada en HTTP, puede acceder al WBM del servidor SINEMA RC y configurar solicitudes API con él. Para ello, necesita una licencia API con la que pueda habilitar el servidor API en el servidor SINEMA RC. Puede encontrar información adicional en la sección "API (Página 94)".

Configuración del servidor SINEMA RC

En el WBM, puede utilizar las siguientes funciones:

- Configuración básica del sistema
 - Ajustes del sistema y parámetros de dirección
 - Idioma del WBM
- Especificación de usuarios, grupos y sus derechos
 - Creación de usuarios y dispositivos, incluida la asignación de contraseñas
 - Creación y asignación de roles y derechos
 - Asignación de grupos de participantes
- Configuración de conexiones
 - Creación de relaciones de comunicación entre los grupos participantes

Puesta en marcha/configuración de dispositivos finales

- Puede crear configuraciones parciales globalmente para los dispositivos finales. Esto incluye, por ejemplo, la configuración de NAT, etc.
- A través del servidor, la información de configuración se puede cargar en el dispositivo final.

Gestión del servidor

- Cambiar la configuración del sistema o de los participantes
- Activar/desactivar conexiones entre participantes

Gestión de conexiones

- Visualización de todas las conexiones disponibles en línea y fuera de línea
- Configuración de conexión con creación de certificados
- Establecimiento y terminación de conexiones
- Enviar un mensaje SMS de activación a un dispositivo, por ejemplo, para establecer una conexión segura

1.3

Concepto de usuario

SINEMA RC Server dispone de un amplio sistema de derechos de acceso. Este sistema permite al administrador conceder o denegar el acceso de los usuarios a determinados objetos del programa de forma individual y según las necesidades. Durante la configuración, debe tener en cuenta los siguientes criterios en el rol:

- Seguridad de la red
- Experiencia de TI de los usuarios
- La necesidad de ciertas funciones
- La facilidad de uso

Nota**La gestión de derechos es una de las tareas más importantes de un administrador**

Por lo tanto, esto debe planificarse y configurarse para cumplir con los requisitos específicos teniendo en cuenta los aspectos relevantes para la seguridad. Le recomendamos encarecidamente que se familiarice con el concepto de usuarios y roles de SINEMA RC Server. Las configuraciones nuevas o modificadas siempre deben verificarse en términos de su efecto previsto.

Lo esencial

Los derechos de acceso en SINEMA RC se especifican mediante los siguientes objetos:

- Usuarios
- Funciones
- Derechos
- Grupos de participantes

En principio, se aplica lo siguiente: A

cada usuario se le pueden asignar ciertos derechos.

A cada rol se le pueden asignar varios derechos que se transfieren automáticamente a todos sus miembros (usuarios, grupos de participantes).

Aplicación y propiedades

1.3 Concepto de usuario

Cada usuario puede tener varios roles y ser miembro de varios grupos de participantes.

Usuarios

Para que un usuario creado pueda crear y administrar otros usuarios, el usuario debe tener asignado el derecho de usuario "Administrar usuarios".

usuario "administrador"

Por defecto, después de la instalación, el usuario predefinido "admin" está disponible. Con este nombre de usuario, puede iniciar sesión una vez después de la instalación. Después de esto, se le pedirá que cree un nuevo usuario. El rol de "administrador" se asigna automáticamente a este usuario recién creado.

El administrador tiene derecho a acceder a todas las funciones y puede configurar el sistema. Esto incluye crear usuarios y asignarles roles y derechos. Para obtener información más detallada, consulte el apartado "Gestión de roles y derechos (Página 86)".

El administrador aparece en la lista con las cuentas de usuario y no se puede editar ni eliminar. El nombre de usuario "admin" ya no está disponible.

Usuarios de UMC

SINEMA RC ofrece la posibilidad de utilizar los datos de usuario almacenados de forma centralizada en un servidor UMC. Además, el servidor UMC puede conectarse a Windows Active Directory y acceder a sus datos de usuario. El uso de los datos de usuario de UMC significa que no es necesario crear cuentas de usuario individuales localmente en SINEMA RC. El administrador solo necesita configurar una conexión con el UMC en el servidor SINEMA RC e ingresar el nombre del grupo de usuarios de UMC en la configuración de roles para el rol afectado. Los nombres de los grupos de usuarios de UMC en SINEMA RC deben coincidir exactamente con los nombres de los grupos de usuarios de UMC en UMC. Cuando un usuario de UMC inicia sesión en UMC, SINEMA RC establece una conexión con el servidor de UMC, accede a la cuenta de usuario a través del grupo de usuarios de UMC y crea un usuario temporal con el rol asignado.

Puede encontrar información sobre cómo crear y administrar cuentas de usuario en UMC en el "Manual de usuario de la interfaz de usuario web de UMC".

Licencias en SINEMA RC

Necesita una licencia UMC para poder utilizar el servidor UMC.

- Licencia de prueba

Con la licencia de prueba, tiene un uso ilimitado de UMC durante 14 días con fines de prueba y evaluación, pero no para uso productivo. Se excluyen todas las reclamaciones de responsabilidad. Una vez que la licencia de prueba haya caducado, deberá obtener una licencia de alquiler.

- Licencia de alquiler

Con una licencia de alquiler activada, puede utilizar UMC sin restricciones en SINEMA RC. La licencia de alquiler está disponible directamente como Certificado de Licencia (CoL).

Iniciar sesión

Las siguientes opciones están disponibles para iniciar sesión:

- Localmente al WBM
 - Iniciar sesión con nombre de usuario y contraseña
 - Iniciar sesión con la tarjeta inteligente
 - Inicio de sesión con certificado PKI
- A través de un servidor UMC
 - Iniciar sesión con nombre de usuario y contraseña

roles

En SINEMA Server, hay dos roles predefinidos disponibles con los derechos de acceso correspondientes.

Rol estándar	Descripción
administración	El rol tiene todos los derechos de acceso y no pertenece a un grupo de participantes.
usuario_vpn	El rol no tiene derechos de acceso y se asigna automáticamente al grupo de participantes. El rol solo puede establecer conexiones VPN con los participantes que pertenecen al grupo de participantes vpn_user_group.

grupo de participantes

en SINEMA RC Server hay disponible un grupo de participantes predefinido.

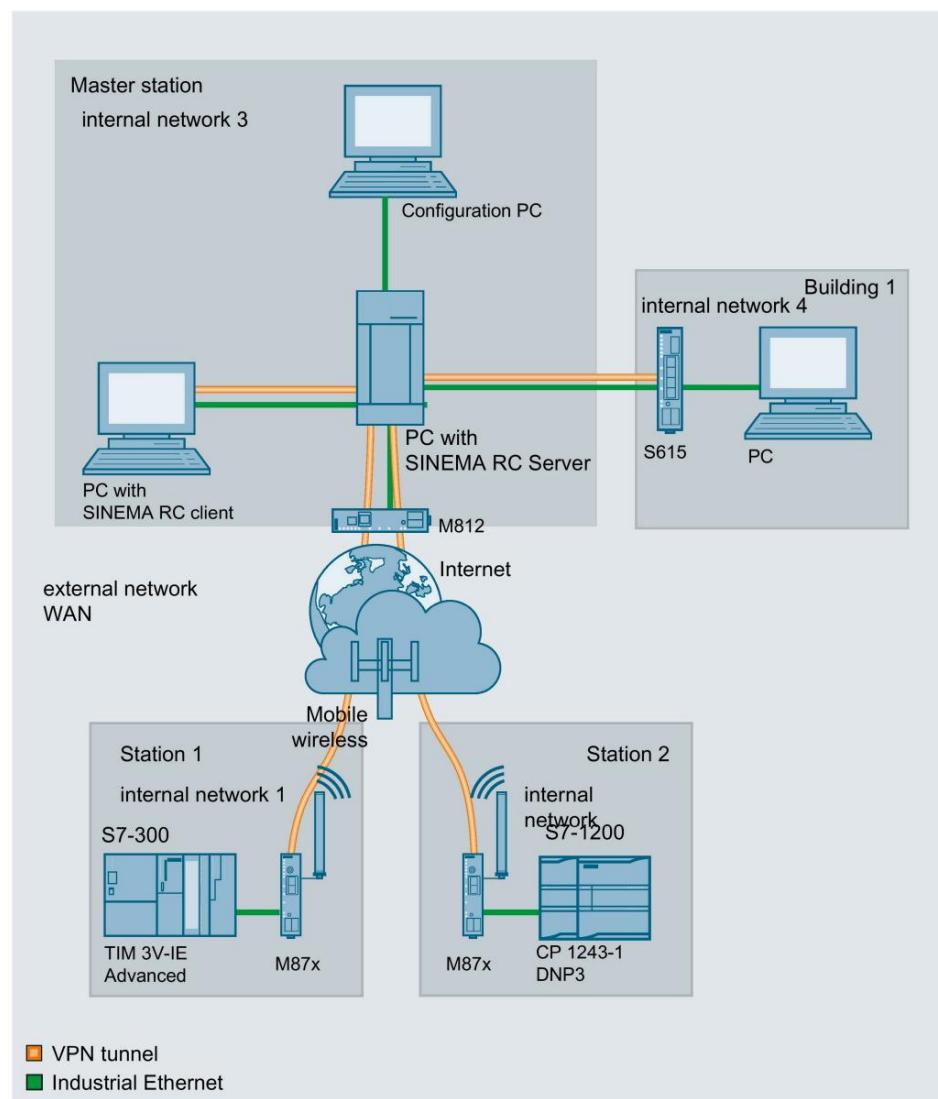
Grupo de participantes estándar	Descripción
vpn_user_group	No se permite la comunicación entre los nodos.

1.4 Ejemplo de configuración

1.4.1 TeleControl con SINEMA RC

En esta configuración, la estación maestra de mantenimiento remoto está conectada a Internet/intranet a través del servidor SINEMA RC. Las plantas se comunican a través de SCALANCE M o SCALANCE S615 que establecen un túnel VPN al servidor SINEMA RC. En la estación maestra, SINEMA RC Client establece un túnel VPN hacia SINEMA RC Server. Para establecer el túnel VPN, se utiliza OpenVPN.

Los dispositivos deben iniciar sesión en el servidor SINEMA RC. Para ello, está disponible un WBM. El túnel VPN entre el dispositivo y SINEMA RC Server se establece solo después de una autenticación exitosa. Según las relaciones de comunicación configuradas y los ajustes de seguridad, el servidor SINEMA RC conecta los túneles VPN individuales.

*Aplicación y propiedades 1.4**Ejemplo de configuración***Procedimiento**

Para poder acceder a una planta a través de una estación maestra de mantenimiento remoto, siga los pasos a continuación:

1. Establezca la conexión Ethernet entre el dispositivo y el PC de configuración conectado.
2. Establezca una conexión a la WAN.
3. Registre el nuevo dispositivo en SINEMA RC Server.
4. Configure la conexión con SINEMA RC Server en el dispositivo.
5. Ponga en funcionamiento el nuevo dispositivo.

Encontrará instrucciones sobre el procedimiento en Getting Started for SINEMA Remote Connect.

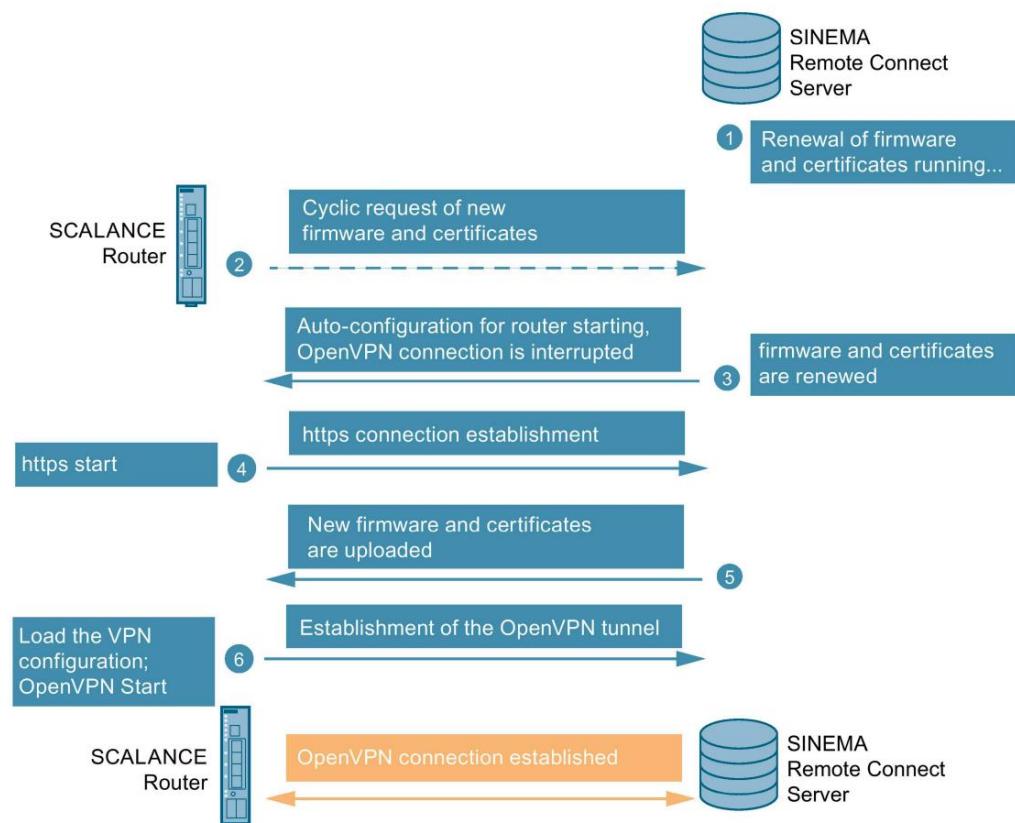
1.5 Distribución automática de certificados y firmware

1.5.1 Actualización automática de certificados y firmware

Si se establece una conexión entre SINEMA RC Server y el enrutador SCALANCE, el enrutador solicita automáticamente actualizaciones de firmware y certificados. Esta solicitud se realiza de forma cíclica en intervalos de tiempo específicos, que puede configurar como el parámetro "Intervalo de inscripción automática" en el enrutador. Para SCALANCE S615/M-800/SC-600, configure el parámetro en el WBM en "Sistema > SINEMA RC".

Puede encontrar información adicional sobre esto en el manual de configuración del dispositivo respectivo.

Procedimiento



1. Si hay actualizaciones de firmware y certificados disponibles, SINEMA RC Server las renueva automáticamente o el usuario puede renovarlas manualmente.
2. Después de un tiempo configurado en el enrutador, el enrutador SCALANCE pregunta cíclicamente al servidor si hay disponible un archivo de firmware más nuevo o si hay disponible un nuevo certificado. El intervalo de sondeo predeterminado es de 60 minutos.
3. Si se ha renovado el firmware o el certificado en el servidor, la autoconfiguración comienza: la conexión OpenVPN finaliza brevemente.
4. El router SCALANCE inicia la conexión https con el SINEMA RC Server.

Aplicación y propiedades

1.5 Distribución automática de certificados y firmware

5. El servidor SINEMA RC envía un archivo de configuración al enrutador SCALANCE. El router SCALANCE recibe el nuevo firmware y los certificados y los almacena.
6. El enrutador SCALANCE carga la configuración VPN completa y establece el túnel OpenVPN hacia el servidor.

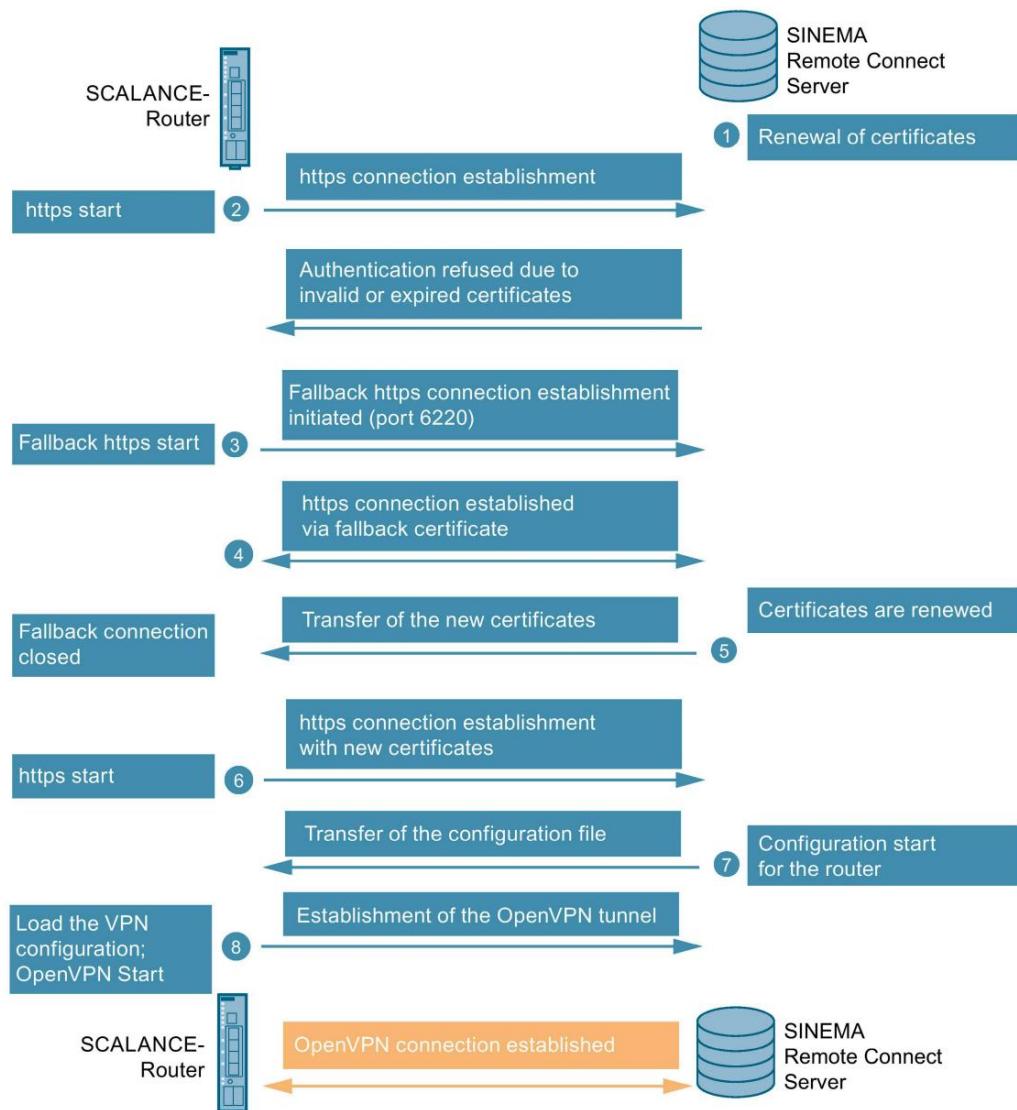
Resultado

La conexión VPN entre SINEMA RC Server y el enrutador SCALANCE está establecida.

1.5.2 Actualización de certificados con conexión alternativa

Debido a certificados caducados o no válidos, no es posible establecer una conexión a través de https. Como resultado, el enrutador SCALANCE no puede actualizar automáticamente los certificados relevantes. Para poder establecer la conexión entre el servidor y el enrutador a pesar de los certificados caducados o inválidos, la conexión alternativa se hace cargo durante este tiempo.

Procedimiento



1. Antes de que caduquen los certificados, SINEMA RC Server los renueva automáticamente o el usuario los renueva manualmente.
2. El enrutador SCALANCE intenta establecer una conexión https para que sea posible la configuración automática. Sin embargo, la conexión se rechaza porque el certificado del router SCALANCE no es válido o ha caducado.
3. A continuación, el router SCALANCE inicia una conexión alternativa.
La conexión alternativa es una conexión https a través de un puerto https separado (puerto 6220).

*Aplicación y propiedades**1.5 Distribución automática de certificados y firmware*

a través del cual el servidor envía un certificado alternativo al enrutador para su verificación. El enrutador ahora puede autenticar el servidor con el certificado alternativo.

4. Se establece una conexión https con el servidor.
5. El router SCALANCE puede recibir los nuevos certificados y los almacena en Certificados. Los certificados no válidos se eliminan automáticamente. La conexión alternativa ahora está completa.
6. La conexión con SINEMA RC Server ahora está establecida como de costumbre, pero con el nuevo certificados Para ello, el router SCALANCE establece una conexión https con el SINEMA RC Server. El servidor se identifica con su certificado de servidor web. El enrutador se autentica en el servidor mediante una huella digital o un certificado de CA.
7. El servidor ahora inicia la configuración automática para el enrutador. El enrutador recibe un archivo de configuración con los parámetros y certificados necesarios para configurar el túnel VPN, incluido el certificado del dispositivo y el certificado de reserva.
8. El enrutador SCALANCE carga la configuración VPN completa y establece el túnel OpenVPN hacia el servidor.

Resultado

La conexión VPN entre SINEMA RC Server y el enrutador SCALANCE está establecida.

Requisitos para la operación

2.1 Requisitos

Requisitos de hardware

Componente	Mínimo requisitos	Requerimientos Recomendados	Requisitos recomendados para los límites máximos de configuración (ver más abajo)
Procesador	CPU de doble núcleo de 2,4 GHz	CPU de cuatro núcleos a 2,66 GHz	CPU de cuatro núcleos a 3,6 GHz 4 subprocesos y hyperthreading deshabilitado
RAM	2 GB	4 GB	8GB
Adaptador de red	1x	1x Nota: SINEMA RC El servidor admite hasta cuatro adaptadores de red.	1x GbpsEthernet Nota: SINEMA RC Server admite hasta cuatro adaptadores de red.
Disco duro	> 20GB	> 60GB	SSD de 250GB

Plataformas de virtualización

La aplicación SINEMA RC Server también se puede instalar en una máquina virtual (VM).

- VMware vSphere Hipervisor (ESXi) 6.5
- Estación de trabajo VMWare 14

Si desea instalar la aplicación SINEMA RC Server en una máquina virtual, cree una partición para un sistema Ubuntu de 64 bits. SINEMA RC en sí es una aplicación que ya trae consigo el sistema Ubuntu de 64 bits como sistema operativo y lo instala como un sistema operativo.

Límites máximos de configuración

Transferencia de datos general máxima para todos los dispositivos: 800 Mbps

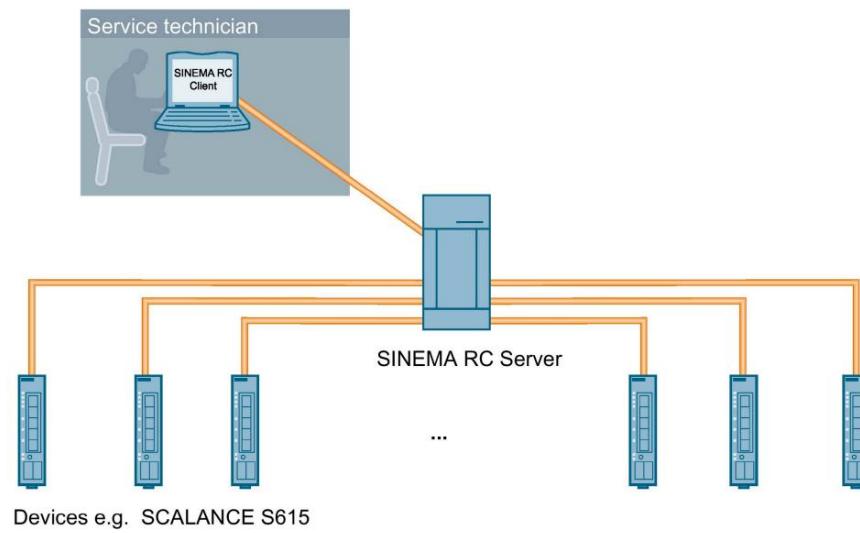
Número máximo de dispositivos y usuarios conectados simultáneamente para una subred por dispositivo: **1024**

Las combinaciones de usuario/dispositivo se pueden seleccionar libremente hasta la estructura de cantidad total máxima.

Dado que el número de subredes también depende de las relaciones de comunicación permitidas entre sí, por ejemplo, estas deben verificarse/cuestionarse y restringirse, cuando sea necesario. Si los dispositivos no necesitan comunicarse entre sí, debe suprimir la comunicación para garantizar un comportamiento óptimo de los dispositivos.

Requisitos para la operación

2.2 Nodos conectables

**2.2****Nodos conectables**

La conexión a SINEMA RC se puede establecer a través de varios medios, como redes inalámbricas móviles, DSL o infraestructuras de redes privadas existentes.

Los siguientes productos SCALANCE han sido probados para la conexión a SINEMA RC:

Cliente SINEMA RC

		Versión cliente SINEMA RC							
		1.0	1.0 SP1	1.0 SP2	1.0 SP3 +	SP4	2.0	2.1	3.0
CINE RC versión del servidor	1.0	-	-	-	-	-	-	-	-
	1.1	-	ÿ	-	-	-	-	-	-
	1.2	-	-	ÿ	-	-	-	-	-
	1.3	-	-	-	ÿ	-	-	-	-
	2.0	-	-	-	-	-	ÿ	-	-
	2.1	-	-	-	-	-	-	ÿ	-
	3.0	-	-	-	-	-	-	-	ÿ

Nodos conectables

Tipo de dispositivo	Nodo	Número de artículo	Versión de firmware	Establecimiento de conexión a la Servidor CINE RC					Sub redes (vlan)
				Despertar arriba SMS	Maldita sea la entrada	Para mamá ahora	IPsec abierto	vpn	
ESCALANCE S615	S615	6GK5615-0AA00-2AA2 a partir de 4.0	-	ÿ	ÿ	ÿ	ÿ	ÿ	desde
ESCALANCE	SC632-2C	6GK5632-2GS00-2AC2 a partir de 1.0	-	ÿ	ÿ	ÿ	-	ÿ 1)	257

Requisitos para la operación

2.2 Nodos conectables

Tipo de dispositivo	Nodo	Número de artículo	Versión de firmware	Establecimiento de conexión a la Servidor CINE RC					Sub redes (vlan)
				Despertar arriba SMS	Maldita sea la entrada	Para mamá ahora	IPsec abierto	vpn	
SC-600	SC636-2C	6GK5636-2GS00-2AC2 a partir	de 1,0	-	ÿ	ÿ	-	ÿ 1)	257
	SC642-2C	6GK5642-2GS00-2AC2 a partir	de 1,0	-	ÿ	ÿ	ÿ	ÿ 1)	257
	SC646-2C	6GK5646-2GS00-2AC2 a partir	de 1,0	-	ÿ	ÿ	ÿ	ÿ 1)	257
ESCALANCE S600 2)	S612	6GK5612-0BA10-2AA3 A partir	de 4.0.1.1	-	-	ÿ	ÿ	-	
	S623	6GK5623-0BA10-2AA3 A partir	de 4.0.1.1	-	-	ÿ	ÿ	-	
	S627-M	6GK5627-2BA10-2AA3 a partir	de 4.0.1.1	-	-	ÿ	ÿ	-	
ESCALANCE Móvil M800	M874-2	6GK5874-2AA00-2AA2 A partir	de 4.1	ÿ	ÿ	ÿ	ÿ	ÿ	decidido
	M874-3	6GK5874-3AA00-2AA2 A partir	de 4.1	ÿ	ÿ	ÿ	ÿ	ÿ	decidido
	M876-3	6GK5876-3AA02-2BA2 A partir	de 4.1	ÿ	ÿ	ÿ	ÿ	ÿ	decidido
	M876-4	6GK5876-4AA00-2BA2 (I) 6GK5876-4AA00-2DA2 (NAM) 3)	A partir de 4.1	ÿ	ÿ	ÿ	ÿ	ÿ	decidido
ESCALANCE Módems M816	M816-1	6GK5816-1AA00-2AA2 (UE) 6GK5816-1BA00-2AA2 (NAM) 3)	A partir de 4.2	-	ÿ	ÿ	ÿ	ÿ	decidido
ESCALANCE M804 PB	M804PB	6GK5804-0AP00-2AA2 a partir	de 6,0	-	ÿ	ÿ	ÿ	ÿ	decidido
SIMATIC CP1200	PC 1243-1	6GK7243-1BX30-0XE0 a partir	de 3.1	-	-	ÿ	-	ÿ	
	CP 1243-7 LTE	6GK7243-7KX30-0XE0 (I) 6GK7243-7SX30-0XE0 (NAM) 3)	A partir de 3.1	-	-	ÿ	-	ÿ	
	CP 1243-8 IRC	6GK7243-8RX30-0XE0 A partir	de 3.1	-	-	ÿ	-	ÿ	
SIMATIC CP 1543-1	CP 1543-1	6GK7543-1AX00-0XE0		-	-	ÿ	ÿ	-	1
SIMATIC CP ET 200SP	CP 1543SP-1 6GK7543-6WX00-0XE0	A partir de 2,0		-	-	ÿ	-	ÿ	
	CP 1542SP-1 IRC	6GK7542-6VX00-0XE0 a partir	de 2,0	-	-	ÿ	ÿ	ÿ	
SIMATIC RTU 3010C	RTU3010C	6NH3112-0BA00-0XX0		-	- 4)	ÿ	-	ÿ	
SIMATIC RTU 303XC	RTU3031C	6NH3112-3BB00-0XX0		ÿ	- 4)	ÿ	-	ÿ	
	RTU3030C	6NH3112-3BA00-0XX0		ÿ	- 4)	ÿ	-	ÿ	

Requisitos para la operación**2.3 Información de la licencia**

Tipo de dispositivo	Nodo	Número de artículo	Versión de firmware	Establecimiento de conexión a la Servidor CINE RC					Sub redes (vlan)
				Despertar arriba SMS	Maldita sea la entrada	Para mamá ahora	IPsec abierto	vpn	
SIMATIC RTU 3040C	RTU3041C 6NH3	112-4BB00-0XX0		ÿ	- 4)	ÿ	-	ÿ	
RUGGEDCOM \$1224	\$1224 LTE (4G)	6GK6108-4AM00-2BA2 (I) 6GK6108-4AM00-2DA2 (NAM) 3)	A partir de 4.1	ÿ	ÿ	ÿ	ÿ	ÿ	decisión

- 1) La conexión OpenVPN solo se puede establecer con el servidor SINEMA RC.
- 2) La configuración solo se puede realizar a través de SCT (IPsec) con las funciones de exportación/importación. Autoconfiguración con Open VPN no es posible.
- 3) América del Norte
- 4) La entrada digital del dispositivo no se utiliza para establecer una conexión con el SINEMA RC Server.

2.3 Información de licencia

Licencias

Distinguimos entre los siguientes tipos de licencia. El comportamiento del software difiere según el tipo de licencia:

Licencia tipos	Descripción
Manifestación	Las siguientes licencias ya están incluidas en la instalación del servidor SINEMA RC: <ul style="list-style-type: none"> • SINEMA Remote Connect 4: 4 participantes • Cliente SINEMA Remote Connect 1 El Certificado de Licencia determina el tipo de uso.
Actualizar	El uso está limitado al número especificado de participantes o clientes Con varias licencias, se agregan los participantes o clientes en "Número". Se puede aumentar el número de participantes con las siguientes licencias de conexión: <ul style="list-style-type: none"> • SINEMA Remote Connect 64: Esta licencia admite hasta +64 participantes. • SINEMA Remote Connect 256: Esta licencia admite hasta +256 participantes. • SINEMA Remote Connect 1024: esta licencia admite hasta +1024 participantes El número de Clientes SINEMA RC se puede ampliar con las siguientes licencias: <ul style="list-style-type: none"> • SW cliente SINEMA Remote Connect, +1 VPN
Prueba	El uso de UMC, API y otras conexiones de clientes está limitado a 30 días a partir del primer día de uso. El software solo puede utilizarse con fines de prueba y validación.
Único	El uso de UMC (Página 39) y API (Página 3) no tiene límite de tiempo.

Puede encontrar los números de artículo de las licencias en la sección "Prefacio (Página 3)".

Actualización de licencia

Para expandir la licencia a un mayor número de participantes/clientes, necesita una actualización a una nueva licencia. Para poder realizar una actualización de licencia, debe obtener una nueva clave de licencia e ingresar el número de licencia correspondiente en el WBM.

El procedimiento para activar la licencia en el WBM se describe en la sección "Resumen (Página 62)".

La cantidad de conexiones que se pueden establecer simultáneamente depende del rendimiento de la plataforma del servidor.

2.4 Caracteres permitidos

contraseñas

Al crear o cambiar las contraseñas, recuerde las siguientes reglas:

Caracteres permitidos de un conjunto de caracteres según ANSI X 3.4-1986	0123456789 A ... Z a ... z #\$/%&()^+,-./;:<=>?@[]_{}~^
Caracteres no permitidos	...
Longitud de la contraseña	mínimo 8 caracteres y máximo 128 caracteres

Nota**contraseñas**

Para mejorar la seguridad, asegúrese de que las contraseñas sean lo más largas posible.

Las contraseñas deben tener al menos 8 caracteres y contener caracteres especiales, mayúsculas y minúsculas, así como números.

Nombres de roles

Al crear o cambiar los nombres de los roles, recuerde las siguientes reglas:

Caracteres permitidos de un personaje colocar	0123456789 A ... Z a ... z _ - . +
Caracteres no permitidos	...
Longitud del nombre del rol	1 a 80 caracteres

Requisitos para la operación**2.5 Datos de rendimiento****Nombres de grupo**

Al crear o cambiar los nombres de los grupos, recuerde las siguientes reglas:

Caracteres permitidos de un conjunto de caracteres	0123456789 A ... Z a ... z . @ + - _
Caracteres no permitidos	...
Longitud del nombre del grupo	1 a 50 caracteres

Nombres de usuario y nombres de dispositivos

Al crear o cambiar los nombres, recuerde las siguientes reglas:

Caracteres permitidos de un conjunto de caracteres	0123456789 A ... Z a ... z _
Caracteres no permitidos	" `#\$%&()*+,-./;:<=>?@[{\}~^
No permitido para nombres de usuario	administración
No permitido para nombres de dispositivos	control
Longitud del nombre	1 a 30 caracteres

Nota**Nombres de usuario**

Para mejorar la seguridad, asegúrese de que los nombres de usuario sean lo más largos posible.

nombre de host

Caracteres permitidos de un conjunto de caracteres según ANSI X 3.4-1986	0123456789 A ... Z a ... z _.
--	-------------------------------------

2.5**Datos de rendimiento**

Número máximo de grupos de participantes	No limitado
Número máximo de participantes por grupo de participantes	No limitado
Número máximo de copias de seguridad locales	30
Número máximo de archivos de registro	100

Instalación y puesta en marcha

3.1 Recomendaciones de seguridad

Respete las siguientes recomendaciones de seguridad para evitar el acceso no autorizado al sistema.

General

- Debe realizar comprobaciones periódicas para asegurarse de que el dispositivo cumpla con estas recomendaciones y otras pautas de seguridad interna, si corresponde.
- Evalúe su planta como un todo en términos de seguridad. Utilice un concepto de protección celular con productos adecuados (<https://www.industry.siemens.com/topics/global/en/industrial-security/network-security/Pages/Default.aspx>).
- No conecte el dispositivo directamente a Internet. Opere el dispositivo dentro de un área protegida.

Acceso al servidor

- Restringir el acceso físico al SINEMA RC Server al personal cualificado.

SINEMA RC Server dispone de un amplio sistema de derechos de acceso. Este sistema le permite otorgar o denegar el acceso a ciertos objetos del programa de forma individual y según la necesidad.

Acceso físico

- Restrinja el acceso físico al dispositivo al personal calificado. Utiliza los mecanismos de seguridad del SINEMA RC.
- Proteja el servidor SINEMA RC de accesos no autorizados instalándolo en racks/control armarios / en salas de control que se pueden cerrar con llave.

Funciones de seguridad del software.

- Mantenga el software actualizado.
 - Compruebe periódicamente las actualizaciones de seguridad del producto. Puede encontrar información al respecto en (<https://support.industry.siemens.com/cs/ww/en/ps/21713/dl>).
- El archivo de actualización está firmado. Esto garantiza que solo se pueda descargar un archivo de actualización creado por Siemens.
 - Infórmese regularmente sobre las recomendaciones de seguridad publicadas por Siemens ProductCERT (<https://www.siemens.com/global/en/home/produkte/services/cert.html>).
- El SINEMA RC Server incluye una función de registro automático. Revisa esta información regularmente para el acceso no autorizado.

Instalación y puesta en marcha

3.1 Recomendaciones de seguridad

contraseñas

- Definir reglas para el uso de dispositivos y asignación de contraseñas.
- Actualice periódicamente las contraseñas para aumentar la seguridad.
- Utilice únicamente contraseñas con una seguridad de contraseña alta.
- Asegúrese de que todas las contraseñas estén protegidas y sean inaccesibles para el personal no autorizado.
- Se debe cambiar una contraseña si se sabe o se sospecha que se sabe por parte de personas no autorizadas.
- personas
- No utilice una contraseña para diferentes usuarios y sistemas.

Claves y certificados

Esta sección trata sobre las claves de seguridad y los certificados que necesita para establecer una conexión.

- El dispositivo contiene un certificado X.509 con clave preinstalado. Reemplace este certificado con un certificado hecho a sí mismo con clave. Le recomendamos que utilice un certificado firmado por una autoridad de certificación externa o interna confiable.
- Utilizar una autoridad de certificación que incluya la revocación y gestión de claves para firmar el certificados
- Asegúrese de que las claves privadas definidas por el usuario estén protegidas y sean inaccesibles para personas no autorizadas.
- personas
- Verificar certificados y huellas dactilares en el servidor y el cliente para evitar el "hombre en el medio" ataques
- Se recomienda que utilice certificados protegidos con contraseña en el formato PKCS#12
- Cambie las claves y los certificados de inmediato si existe una sospecha de compromiso.
- Le recomendamos que utilice certificados con una longitud de clave de 4096 bits.
- El producto es compatible con RSA 1024 - Longitud de clave de 8192 bits.

Protocolos disponibles

La siguiente lista le proporciona una descripción general de todos los servicios utilizados del producto.

Tenga esto en cuenta al configurar un cortafuegos.

La tabla incluye las siguientes columnas:

- Protocolo
- Todos los protocolos que admite el dispositivo

- Número de puerto

Número de puerto asignado al protocolo

- Estado del puerto

- Abierto

El puerto siempre está abierto y no se puede cerrar. Para usarlo, es necesaria la autenticación.

– Abierto (cuando está configurado)

El puerto está abierto si se ha configurado. Para usarlo, es necesaria la autenticación.

Servicio	Protocolo	Número de puerto	Estado del puerto preestablecido	Autenticación configurable			Cifrado
				ser vicio	Puerto		
HTTPS	TCP	443	Abierto	--	ÿ	ÿ	--
HTTPS para la inscripción automática de certificados	TCP	6220	Abierto	--	ÿ	ÿ	--
OpenVPN	UDP	1194	Abierto	ÿ	ÿ	ÿ	--
	TCP	5443	Abierto	ÿ	ÿ	ÿ	--
IPsec	ESP	n / A	Abierto	ÿ	--	ÿ	--
IPsec encapsulado ed	UDP	500	Abierto	ÿ	--	ÿ	--
IPsec encapsulado ed NAPT	UDP	4500	Abierto	ÿ	--	ÿ	--
SSH	TCP	22	Abierto (cuando está configurado)	--	ÿ	ÿ	ÿ
Syslog sobre TLS UDP	TCP	514	Solo saliente	--	ÿ	ÿ	ÿ

Tabla 3- 1 Servicios disponibles

Protocolo		Número de puerto	Estado del puerto	Puerto cambiante		autenticación
HTTPS	TCP	443	Abierto	ÿ	ÿ	
HTTPS para la inscripción automática de certificados	TCP	6220	Abierto	ÿ	ÿ	
OpenVPN	UDP	1194	Abierto	ÿ	ÿ	
	TCP	5443	Abierto	ÿ	ÿ	
IPsec	ESP	n / A	Abierto	--	ÿ	
UDP encapsulado IPsec		500	Abierto	--	ÿ	
IPsec encapsulado NAPT	UDP	4500	Abierto	--	ÿ	
SSH	TCP	22	Abierto (cuando está configurado)	ÿ	ÿ	

Instalación y puesta en marcha

3.1 Recomendaciones de seguridad

Protocolo		Número de puerto	Estado del puerto	Puerto cambiable	autenticación
Licencia	TCP UDP	22350	Abierto con activación de la licencia en línea del producto	--	ÿ
registro del sistema	UDP TCP	514	Solo saliente	ÿ ÿ	-- ÿ

Tabla 3- 2 Servicios utilizados

Protocolo		número de puerto ber	estado del puerto
NTP	UDP	123	Saliente cuando está configurado
DNS	TCP	53	Saliente cuando está configurado
Cliente de correo electrónico	TCP	25 u otro	Saliente
HTTPS - TCP de recuperación de CRL		según a URL	Extrovertido
HTTPS - activación de licencia	TCP	443	Saliente con activación de la licencia online del producto

3.2 Instalación del servidor SINEMA RC

Nota

Distribución del teclado durante la instalación

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

Requisito

- En el orden de inicio, el CD/DVD se configura como el primer medio de inicio.
- Se cumplen los requisitos de hardware.

Nueva instalación

AVISO

La reinstalación formatea el disco duro

La nueva instalación del servidor SINEMA RC incluye su propio sistema operativo, basado en Ubuntu 18.04 LTS. Si utiliza una PC en la que ya existe un sistema operativo, se formateará el disco duro. Esto significa que los datos existentes se pierden. Asegúrese de que se haya realizado una copia de seguridad de todos los datos importantes del PC.

1. Inserte el soporte de datos en la unidad.
2. Encienda la PC o reinicie el servidor.
La instalación comienza automáticamente.
3. En el siguiente cuadro de diálogo, seleccione la entrada "Instalar/Actualizar SINEMA Remote Connect Server".
Confirme la selección con la tecla ENTER.
Si ya hay una versión instalada, seleccione "Instalar - Instalación nueva" en el siguiente cuadro de diálogo.
No se adoptan las configuraciones anteriores del SINEMA RC Server.
4. Siga las instrucciones adicionales en la pantalla.

Durante la instalación, especifique la dirección IP, la máscara de red y la puerta de enlace para la interfaz WAN.
Alternativamente, seleccione la asignación dinámica de la dirección IP a través de DHCP.

Resultado

El servidor SINEMA RC está instalado. Inicie sesión con el usuario predefinido "admin".

Nota

Servidor SINEMA RC con conexión a la nube

Si descarga el servidor en la nube y desea configurar varios servidores a partir de una imagen, debe iniciar sesión con "admin" directamente después de la instalación y hacer esto. Esta es la única forma de garantizar que cada servidor tenga sus propios certificados.

Instalación y puesta en marcha

3.2 Instalación del servidor SINEMA RC

Antes de que pueda configurar más ajustes mediante WBM, se le solicitará que cree un nuevo usuario y verifique la configuración de la red. Tenga en cuenta que el inicio de sesión con "admin" ya no es posible después de esto.

Actualización de la versión del servidor

La actualización debe realizarse en el orden correcto: V1.0 > V1.1 >
V1.2 > V1.3 > V2.0 > V2.1 > V3.0.

Nota

Actualización del sistema V1.2 > V1.3

Debido a cambios en la instalación básica, una actualización de V1.2 a V 1.3 solo es posible utilizando el CD de instalación; consulte el apartado "Actualización del sistema V1.2 > V1.3 (Página 125)".

Nota

Actualización del sistema V2.0 > V2.1

Antes de actualizar la versión del software, debe liberar las licencias para "SINEMA RC (2.0)" y reactivarlas en la versión de servidor V2.1. El procedimiento se describe en el apartado "Actualización del sistema V2.0 > V2.1 (Página 130)".

Procedimiento

1. En la navegación, seleccione "Sistema > Actualizar".
2. Haga clic en el botón "Seleccionar archivo".
3. Navegue hasta el directorio de almacenamiento y seleccione Archivo *.tar.gz.
Confirme su selección con el botón "Abrir".
4. Haga clic en el botón "Importar".

Resultado

El sistema está actualizado. Según el tipo de actualización, se reinician funciones individuales o todo el sistema. Para verificar la versión después del reinicio, en la navegación, haga clic en "Sistema> Descripción general" y verifique la versión de software que se muestra.

Puede encontrar información más detallada en la sección "Actualización (Página 65)".

Ver también

Estaciones conectables (Página 24)

3.3 Primera puesta en marcha de equipos finales con WBM

Puesta en marcha del nodo a través del WBM

Procedimiento

1. Configure el nuevo dispositivo en SINEMA RC Server.

Para obtener información más detallada, consulte el apartado "Configuración del dispositivo (Página 75)".

– Especifique la información del dispositivo requerida. por ejemplo, nombre del dispositivo, fabricante, ubicación, etc.

– Configurar el modo de conexión VPN

– Introduzca la contraseña para identificar el dispositivo final durante el inicio de sesión.

– Asigne el dispositivo a un grupo de participantes.

Para obtener información más detallada, consulte la sección "Asignación de un nodo a un grupo (Página 84)".

Cuando se configura el dispositivo, el certificado se crea automáticamente.

Para obtener información más detallada, consulte la sección "Descripción general de la gestión de certificados (Página 100)".

2. Transfiera los ajustes de configuración de SINEMA RC Server al dispositivo.

– Para identificar el dispositivo en SINEMA RC Server, transfiera el certificado al dispositivo e ingrese la contraseña.

– Introduzca la dirección IP del SINEMA RC Server.

3. Ponga el dispositivo en funcionamiento.

Resultado

El dispositivo se conecta al servidor SINEMA RC. Cuando la conexión se ha establecido correctamente, se transfiere, por ejemplo, una dirección IP virtual.

Si es necesario, realice más pasos de configuración:

1. En el extremo del dispositivo, por ejemplo, configure las reglas de firewall, NAT, etc.

Puede encontrar instrucciones precisas paso a paso en el Getting Started de SINEMA Remote Connect y en el Getting Started del dispositivo correspondiente.

Instalación y puesta en marcha

3.3 Primera puesta en marcha de equipos finales con WBM

Configuración con administración basada en web

4.1 Apertura de la gestión basada en web

Llamar a la página de inicio del WBM

1. Abra el navegador web.
2. En la línea de dirección del navegador, introduzca <https://<dirección IP>> del SINEMA RC Server.
Ha especificado la dirección IP durante la instalación.

Si utiliza un puerto que no sea el 443 como puerto estándar HTTPS, introduzca el número de puerto junto con la dirección IP.
Se deben ingresar dos puntos ":" entre la dirección IP y el número de puerto como delimitador, por ejemplo: <https://192.168.234.1:6443>.

Nota

El puerto para acceder al servidor web se configura en la pestaña "Sistema > Configuración de red > Configuración del servidor web".

Resultado

Se abre la página de inicio del WBM.

4.2 Iniciar el WBM

4.2.1 Iniciar sesión con nombre de usuario y contraseña

Procedimiento

1. Introduzca un nombre de usuario configurado.

Puede encontrar información sobre el primer inicio de sesión en la siguiente sección "Inicio de sesión después de la nueva instalación".
2. Introduzca la contraseña correspondiente.

Puede encontrar información sobre el primer inicio de sesión en la siguiente sección "Inicio de sesión después de la nueva instalación".
3. Haga clic en el botón "Iniciar sesión".

Se abre la página de inicio del WBM. Es posible que se muestre un acuerdo de usuario, consulte la sección "Contrato de usuario (Página 92)". Si hace clic en el botón "Aceptar", aparece la página de inicio.

Cambiar la contraseña actual

Como usuario registrado, puede cambiar su contraseña actual; consulte el apartado "Cambiar la contraseña actual (Página 120)".

Inicio de sesión después de instalar nuevos

1. Después de una nueva instalación, ingrese "admin" como nombre de usuario y contraseña.

2. Haga clic en el botón "Iniciar sesión".

Se abre la página WBM "Cambiar contraseña".

3. Especifique el nombre de usuario y la contraseña del administrador.

La nueva contraseña debe tener al menos 8 caracteres y contener caracteres especiales, mayúsculas y minúsculas, así como números, consulte la sección "Caracteres permitidos"

(Página 27)". El nombre de usuario "admin" no está permitido. El rol de "administrador" se asigna automáticamente a este usuario recién creado.

El administrador tiene derecho a acceder a todas las funciones y puede configurar el sistema. Esto incluye crear usuarios y asignarles roles y derechos.

4. Haga clic en el botón "Guardar".

Después de guardar, iniciará sesión automáticamente con el administrador recién creado. El usuario "admin" ya no está disponible.

Una vez que haya iniciado sesión correctamente, aparecerá la página de inicio. Es posible que se muestre un acuerdo de usuario, consulte la sección "Contrato de usuario (Página 92)". Si hace clic en el botón "Aceptar", aparece la página de inicio.

Nota**Cambio de contraseña después del primer inicio de sesión de un usuario**

Después del primer inicio de sesión, un usuario configurado se reenvía automáticamente a una página en la que puede cambiar la contraseña. Sin este proceso, no es posible iniciar sesión en SINEMA RC Client.

Ingresar el nombre de usuario o la contraseña incorrectos

Si ingresa un nombre de usuario que no está configurado, se muestra un mensaje de error independientemente de la contraseña ingresada. Se puede ingresar un nombre de usuario o una variedad de nombres de usuario incorrectos cualquier número de veces sin que el sistema se bloquee.

Nota**Pérdida de la contraseña de administrador**

Ante una contraseña de administrador recién asignada o modificada y guárde la en un lugar seguro.

Si solo se configura un administrador, la pérdida de la contraseña de administrador significa que no se pueden realizar más tareas de administrador.

No hay posibilidad de restablecer la contraseña de administrador asignada.

Nota**Introducción incorrecta de la contraseña**

Si ingresa una contraseña incorrecta con el nombre de usuario, se muestra un mensaje de error.

Si ingresa una contraseña incorrecta, comienza un tiempo de bloqueo que se extiende con cada intento de iniciar sesión con una contraseña incorrecta.

4.2.2 Inicio de sesión con UMC

UMC (User Management Component) es una base de datos para la administración central de datos de usuario. UMC ofrece una gestión de usuarios eficiente que reduce la carga de trabajo para mantener los datos de los usuarios en la planta. UMC puede ser opcionalmente parte del dominio AD para que los datos del usuario puedan leerse directamente desde Microsoft Active Directory.

Si se configura un servidor UMC en SINEMA RC, un usuario creado en el UMC puede iniciar sesión en SINEMA RC con sus datos de acceso al UMC.

Cómo funciona

En primer lugar, se crea un usuario de UMC en el servidor de UMC y se asigna a uno o varios grupos de usuarios de UMC. El nombre del grupo de usuarios de UMC se encuentra más adelante en SINEMA RC.

El administrador configura la conexión con el servidor UMC en el servidor SINEMA RC y también crea un rol para el cual se ingresa además el nombre del grupo de usuarios UMC asociado con el usuario UMC.

Cuando un usuario de UMC inicia sesión en SINEMA RC utilizando su inicio de sesión de UMC, SINEMA RC establece una conexión con el servidor de UMC. SINEMA RC comprueba si el usuario está asignado a un grupo de usuarios UMC introducido en SINEMA RC y habilitado para la conexión.

El intercambio de datos entre los dos servidores solo es posible cuando los nombres de los grupos de usuarios de UMC en SINEMA RC coinciden exactamente con los nombres de los grupos de usuarios de UMC en UMC.

Nota**Etiquetado de un usuario UMC con prefijo**

Cada usuario de UMC recibe el prefijo "Umcuser_". La barra invertida "ÿ" en el nombre de usuario del usuario de un servidor UMC se convierte en un guion bajo "_" en SINEMA RC.

Licencias en el servidor UMC

- El servidor UMC forma parte del DVD de descarga/programa del programa SINEMA RC Client.
- Con la instalación del software, puede administrar hasta 10 cuentas de usuario sin licencia. Para más cuentas de usuario, necesita una licencia.

4.2 Inicio del WBM

- Puede acumular esta licencia. Si tiene varias licencias, la configuración permitida el límite para las cuentas de usuario se deriva de la suma de las licencias.
- La licencia es necesaria para el servidor de anillo del dominio del Componente de gestión de usuarios.
La licencia se ofrece como Licencia de Alquiler por 365 días. El Certificado de Licencia se puede descargar directamente.

Licencia de software	Número de artículo
Componente de gestión de usuarios del TIA Portal (UMC) Licencia de alquiler para 100 cuentas de usuario y 365 días Certificado de Licencia para descargar	6ES7823-1UE30-0YA0
Componente de gestión de usuarios del TIA Portal (UMC) Licencia de alquiler para 4000 cuentas de usuario y 365 días Certificado de Licencia para descargar	6ES7823-1UE10-0YA0

Requisitos en el servidor SINEMA RC

- Se crea un usuario en UMC y se asigna a un grupo de usuarios de UMC.
- Se activa una licencia SINEMA RC UMC válida (MLFB 6GK1724-2VH03-0BV0) o una licencia de prueba en SINEMA RC.
- La conexión con el servidor UMC se establece en el SINEMA RC, consulte la sección "Configuración UMC (Página 95)".
- Se crea un rol en SINEMA RC y utiliza el mismo nombre para el grupo de usuarios de UMC para que el usuario correspondiente está asignado en UMC, apartado "Gestión de roles y derechos (Página 86)".

Procedimiento

1. Seleccione la pestaña "Inicio de sesión de UMC" en la página web de inicio de sesión de SINEMA RC.
2. Ingrese el nombre de usuario de UMC.
3. Introduzca la contraseña correspondiente.
4. Haga clic en el botón "Iniciar sesión".

Nota**Cambiar los datos de un usuario de UMC**

Los usuarios de la UMC registrados en SINEMA RC no pueden editar sus datos de acceso y su perfil en SINEMA RC.

El administrador solo tiene los derechos para eliminar un usuario de UMC de la lista de usuarios o asignar el nombre de un grupo de usuarios de UMC a una función.

4.2.3

Iniciar sesión con la tarjeta inteligente / certificados de usuario

El inicio de sesión con la tarjeta inteligente corresponde a un sistema de seguridad de dos niveles.

El primer nivel es la posesión de la tarjeta y el segundo nivel es el número de identificación personal (PIN) para desbloquear la tarjeta inteligente. En la tarjeta inteligente debe estar el certificado PKI y la clave privada que le pertenece.

Como alternativa, el certificado PKI también puede estar en el disco duro del cliente SINEMA RC. Sin embargo, la clave privada no está protegida por la tarjeta inteligente, sino que debe protegerse con una medida adecuada diferente, por ejemplo, encriptación de la clave privada, medidas integradas en el navegador web.

Cadena de certificados al certificado raíz

Los certificados de una PKI suelen estar organizados jerárquicamente:

En la punta de la jerarquía están los certificados raíz. Son certificados que no están certificados por una autoridad certificadora de nivel superior. El propietario del certificado y el emisor del certificado raíz son idénticos. Los certificados raíz son de plena confianza, son el "ancla" de la confianza y, por lo tanto, el destinatario debe reconocerlos como certificados de confianza. Se almacenan en un área destinada a certificados de confianza.

Dependiendo de la PKI, la función de los certificados raíz puede ser, por ejemplo, firmar certificados de autoridades de certificación de nivel inferior, los llamados certificados intermedios. Esto transfiere la confianza del certificado raíz al certificado intermedio. Un certificado intermedio puede firmar un certificado como un certificado raíz. Por lo tanto, ambos se denominan "certificados CA". CA es el acrónimo de "Autoridad de Certificación".

Esta jerarquía puede continuar sobre varios certificados intermedios hasta el certificado de entidad final. El certificado de entidad final es el certificado del usuario a identificar. En la descripción restante el certificado de entidad final se conocerá como certificado PKI.

Durante la validación, la jerarquía se ejecuta en la dirección opuesta. Como se describió anteriormente, se identifica al emisor del certificado, se verifica la firma con la clave pública, luego se identifica el certificado del emisor del certificado de nivel superior hasta que la cadena de confianza se ha ejecutado hasta el certificado raíz.

Resumen: La cadena de certificados intermedios hasta el certificado raíz (la ruta del certificado) debe existir en el servidor SINEMA RC para permitir la validación del certificado PKI del usuario.

Cómo funciona

Una vez instalada la cadena de certificados en SINEMA RC Server, el usuario puede iniciar sesión con su certificado PKI. Despues de iniciar sesión correctamente, se realiza una verificación para establecer si el certificado PKI contenido del usuario es válido.

Luego se verifica si los atributos de las reglas de filtrado de DN de PKI están incluidos en el certificado de PKI.

*Configuración con administración basada en web***4.2 Inicio del WBM**

Existen los siguientes tipos de inicio de sesión:

- Identificación de usuario

si la regla de filtro PKI DN se aplica a un usuario, este usuario se registra en SINEMA RC Server con el nombre de usuario, consulte el capítulo "Crear nuevos usuarios (Página 88)".

- Usuarios temporales

Si la regla de filtro de PKI se aplica a un rol, se crea un usuario temporal. pkouser _X se utiliza como nombre de usuario. El usuario temporal recibe el derecho y el acceso a los grupos de participantes asignados al rol. Este usuario aparece en "Cuentas de usuario > Usuarios y funciones".

En el rol, también especifica cuándo se eliminará el usuario temporal, consulte la sección "Gestión de roles y derechos (Página 86)".

Inicio de sesión con tarjeta inteligente**Requisito**

- Un lector de tarjetas en la PC o notebook
- El lector de tarjetas está conectado de acuerdo con las instrucciones del fabricante y el controlador que le pertenece está instalado.
- La cadena de certificados PKI CA está instalada en el SINEMA RC Server, ver apartado "PKI CA certificado (Página 111)".
- Una tarjeta inteligente con un certificado PKI válido derivado de uno de los certificados PKI CA importado en SINEMA RC.
- Se han creado reglas de filtrado de DN de PKI.
- Para el usuario, se ha configurado el método de inicio de sesión correspondiente, consulte la sección "Crear un nuevo usuario (Página 88)".
- El software cliente (navegador web o cliente SINEMA RC) es capaz de comunicarse con el lector de tarjetas
 - Internet Explorer, Microsoft Edge y Google Chrome: use Windows Crypto API que reconoce automáticamente un lector de tarjetas adjunto.
 - Cliente Firefox y SINEMA RC: debe seleccionarse la DLL PKCS11 adecuada para la tarjeta Lector y tarjeta inteligente.

Procedimiento

1. Inserte su tarjeta inteligente en el dispositivo lector.
2. Haga clic en el símbolo de la tarjeta.
3. Introduzca su PIN y haga clic en "Iniciar sesión".

Es posible que se muestre un acuerdo de usuario, consulte la sección "Contrato de usuario (Página 92)". Si hace clic en el botón "Aceptar", aparece la página de inicio.

Iniciar sesión con un certificado de usuario

Requisito

- La cadena de certificados PKI CA está instalada en el SINEMA RC Server, ver apartado "PKI CA certificado (Página 111)".
- En el PC existe el certificado de usuario válido derivado de uno de los certificados PKI CA importados a SINEMA RC.
- Se han creado reglas de filtrado de DN de PKI.
- Para el usuario, se ha configurado el método de inicio de sesión correspondiente, consulte la sección "Crear un nuevo usuario (Página 88)".

Procedimiento

1. Navegue hasta el directorio de almacenamiento del certificado PKI.
2. Seleccione el archivo del certificado y haga clic en el botón "Abrir".
Si el archivo está protegido con contraseña, ingrese la contraseña.
3. Haga clic en el botón "Iniciar sesión". Es posible que se muestre un acuerdo de usuario, consulte la sección "Acuerdo de usuario (Página 92)". Si hace clic en el botón "Aceptar", aparece la página de inicio.

Resultado

Durante el inicio de sesión, se realiza una verificación para establecer si el certificado PKI es válido. Luego se verifica si los atributos de las reglas de filtrado de DN de PKI están incluidos en el certificado de PKI.

- Identificación de usuario

Si la regla de filtro PKI DN se aplica precisamente a un usuario, la tarjeta PKI con este nombre de usuario se registra en el SINEMA RC Server, consulte el apartado "Crear un nuevo usuario (Página 88)".

- Usuarios temporales

Si la regla de filtro de DN de PKI se aplica a un rol, se crea un usuario temporal "carduser_X". El usuario temporal aparece en "Cuentas de usuario > Usuarios y roles". El usuario recibe los derechos y el acceso a los grupos de participantes asignados al rol.

En el rol, también especifica cuándo se eliminará el usuario temporal, consulte la sección "Gestión de roles y derechos". También puede eliminar el usuario temporal en "Cuentas de usuario > Usuarios y funciones".

Bloqueo de tarjeta inteligente/certificado de usuario

Para bloquear a los usuarios, tiene las siguientes opciones:

- Lista de revocación
- Lista negra de DN de PKI
- Certificado de usuario caducado
- Bloqueo automático de la Smartcard tras introducir varias veces el PIN erróneo. Solo el emisor de la tarjeta inteligente puede liberar esto nuevamente.

Configuración con administración basada en web

4.3 Diseño de la ventana

Encontrará más información sobre la lista de revocación de certificados y la lista negra de DN de PKI en la sección "Bloqueo de tarjeta inteligente / certificado de usuario".

Reglas de filtrado de DN de PKI

Los atributos de los nombres (Distinguished Name según el estándar X.509) se utilizan como criterios de filtrado para las reglas de filtrado.

Especifique las reglas de filtrado de DN de PKI para el usuario y el rol.

La siguiente tabla muestra varios ejemplos:

Regla de filtro de DN de PKI	Descripción
Para el usuario "JohnDoe" se define la siguiente regla de filtrado: CN = max johndoe, O = PD, O = Siemens, C = DE	Los valores de atributo existen en el certificado de usuario. El sistema señala al usuario de la tarjeta inteligente como usuario "JohnDoe" a quien se le asigna el rol de "administrador". El rol tiene todos los derechos de acceso.
Para el rol "Servicio" se define la siguiente regla de filtrado: CN=*,OU=Servicio_Grupo_Planta_1,O=Siemens,C=DE	Solo los usuarios de tarjetas PKI obtienen acceso para quienes existen los valores de atributos relevantes para OU, O y C. Esto restringe el acceso a un determinado grupo de servicios. El sistema crea un usuario temporal que recibe los derechos asignados al rol "Servicio". Este usuario aparece en "Cuentas de usuario > Usuarios y funciones".
Para el rol "Servicio" se define la siguiente regla de filtrado: CN = *, O = *, O = *, C = DE	En este caso, solo existe la restricción a C = DE. Como marcador de posición se utiliza el carácter **.

4.3 Disposición de la ventana

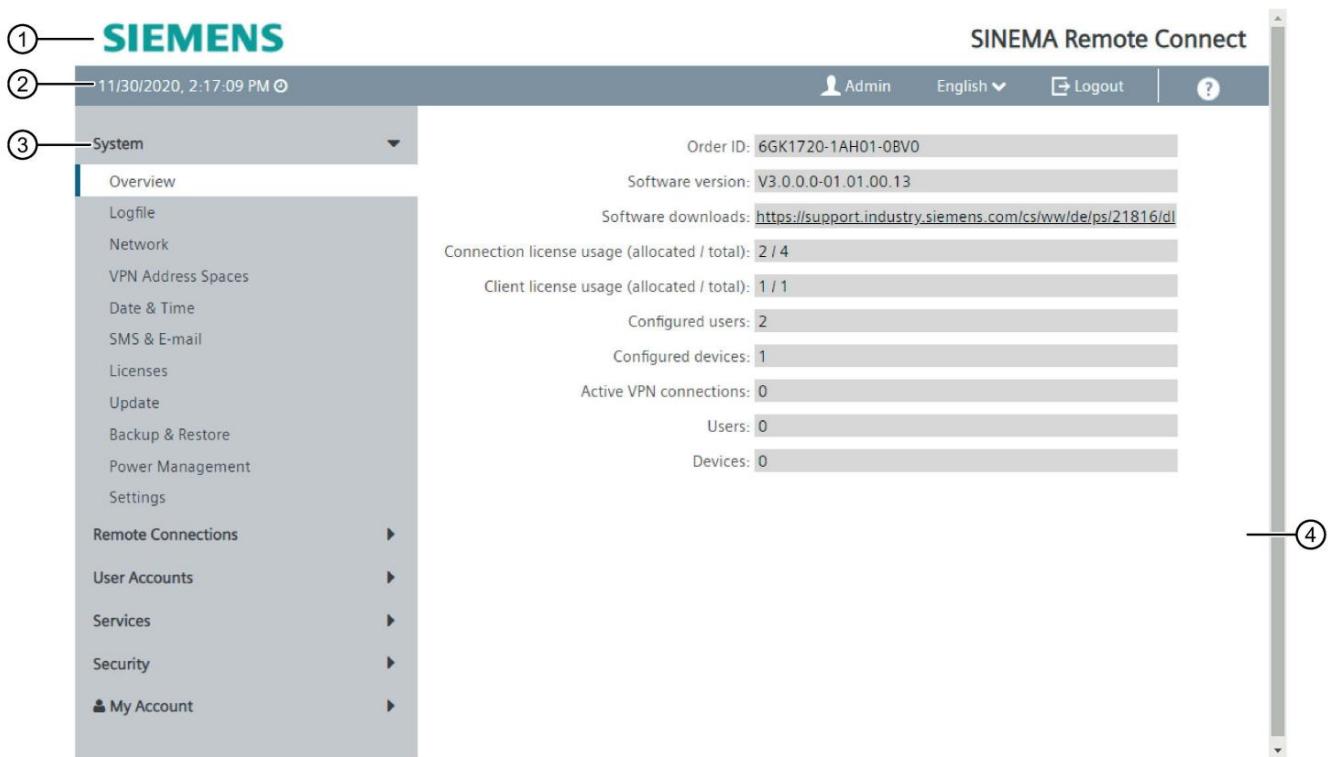
Vista de la página de inicio

Si ingresa la dirección IP de SINEMA Remote Connect, la página de inicio se muestra después de iniciar sesión correctamente.
No puede configurar nada en esta página.

Diseño general de la página WBM

Las siguientes áreas están generalmente disponibles en cada página de WBM:

- Área de encabezado (1): Área superior
- Área de visualización (2): Área superior
- Zona de navegación (3): Zona izquierda
- Área de contenido (4): Área central



Área de encabezado ↴

Lo siguiente está disponible en el área de encabezado:

- Logotipo de Siemens AG
- Nombre del producto

Área de visualización ↴

La parte izquierda del área de visualización contiene los siguientes campos:

- Hora y fecha del sistema

Puede cambiar el contenido de esta pantalla con "Sistema > Hora del sistema".

La parte derecha del área de visualización contiene los siguientes campos y botones:

- Visualización del nombre de usuario con el que ha iniciado sesión.
- Lista desplegable para la selección de idioma.

Se muestra el idioma actual del WBM.

- Cerrar sesión

Botón para cerrar sesión en el WBM. Puede cerrar sesión desde cualquier página de WBM.

- ?

Abre la ayuda en línea en una nueva ventana del navegador.

Área de navegación

En el área de navegación, tiene varios menús disponibles. Haga clic en los menús individuales para mostrar los submenús. Los submenús contienen páginas en las que hay información disponible para usted o con las que puede crear configuraciones. Estas páginas siempre se muestran en el contenido.

Nota

Es posible que no todos los submenús estén disponibles, ya que esto depende de los derechos que se le hayan asignado. Para obtener información más detallada sobre el concepto de usuario, consulte el apartado "Concepto de usuario (Página 15)".

Área de contenido

El área de contenido incluye páginas con campos de entrada o visualización que se muestran según los menús en los que se hizo clic en el área de navegación.

- En el área de navegación, haga clic en un menú para mostrar las páginas del WBM en el área de contenido.

Botones que necesita a menudo

Las páginas del WBM contienen los siguientes botones estándar:

- **Salir del submenú con**  "Diálogo de salida"

Para salir de nuevo de un submenú y volver al menú principal, utilice el botón "Salir del diálogo".

- **Cambiar la configuración con "Guardar"**

Las páginas de WBM en las que puede realizar ajustes tienen el botón "Guardar". Haga clic en el botón para guardar los datos que ha ingresado.

Nota

Para cambiar la configuración, necesita los derechos de usuario adecuados que se describen en la sección "Administrar funciones y derechos (Página 86)".

Nota

Los cambios tienen efecto inmediato. Sin embargo, puede tomar algún tiempo antes de que los cambios se guarden en la configuración.

- **Creación de entradas con "Crear"**

Las páginas de WBM en las que puede crear nuevas entradas tienen el botón "Crear". Haga clic en este botón para crear una nueva entrada.

- **Crear entradas con "Copiar"**

Las páginas de WBM en las que puede copiar entradas tienen el botón "Copiar". Haga clic en este botón para copiar la entrada deseada.

- **Borrar entradas con "Borrar"**

Las páginas de WBM en las que puede borrar entradas tienen el botón "Borrar". Haga clic en este botón para eliminar las entradas seleccionadas anteriormente. La eliminación también da como resultado una actualización de la página en el WBM.

- **Búsqueda dentro de una lista**

En las listas de resumen de los dispositivos, usuarios, roles y grupos de participantes, puede buscar determinadas entradas. Para hacer esto, ingrese el nombre o parte del nombre en el cuadro de búsqueda. Luego presione la tecla ENTER en su teclado.

- **Avance página con "Siguiente"**

El número de registros de datos que se pueden mostrar en una página es limitado. Haga clic en el botón "Siguiente" para avanzar en la página a través de los registros de datos.

- **Volver a la página con "Anterior"**

El número de registros de datos que se pueden mostrar en una página es limitado. Haga clic en el botón "Anterior" para retroceder a través de los registros de datos.

- **Botón "Mostrar todo"**

Puede mostrar todas las entradas en páginas con una gran cantidad de registros de datos. Haga clic en "Mostrar todo" para mostrar todas las entradas en la página. Tenga en cuenta que mostrar todos los mensajes puede llevar algún tiempo.

- **Lista desplegable para seleccionar el número de entradas mostradas**

Puede establecer el número de entradas mostradas para páginas con una gran cantidad de registros de datos. Seleccione el número deseado de entradas de la lista desplegable para mostrarlas.

4.4 Selección de idioma

Elegir lenguaje

1. En el área de encabezado a la derecha, abra la lista desplegable para la configuración de idioma.
2. Seleccione el idioma requerido.

Resultado

La interfaz de usuario de SINEMA RC Server se muestra en el idioma seleccionado independientemente del navegador web que se utilice.

Si el idioma no se cambia inmediatamente, use la tecla de función "F5".

4.5 Sistema

4.5.1 Visión de conjunto

Después de iniciar sesión en el WBM, aparece la descripción general del sistema. Esta página contiene una descripción general de la configuración del dispositivo.

Llamando a la página web

En la navegación, seleccione "Sistema > Resumen".

Configuración con administración basada en web

4.5 Sistema

Entradas mostradas

Se muestran las siguientes entradas:

Campo	Sentido
Solicitar ID	Muestra el número de artículo del software actual.
Versión del software	Muestra el número de versión del software actual.
Descarga de software	Muestra el enlace para descargar la versión actual del software. Al hacer clic en este enlace, accederá a la página de soporte en línea de Siemens Industry con la versión de software actual. Aquí puede verificar si su versión de software está actualizada o descargar la versión actual.
Uso de licencias de conexión (asignado/total)	Muestra el número de participantes actualmente activos y cuántos participantes se pueden configurar en total.
Uso de licencias de cliente (asignado/total)	Muestra el número de conexiones SINEMA RC Client actualmente activas y cuántas conexiones cliente son posibles en total.
Usuarios configurados	Muestra el número de usuarios creados en el proyecto.
Dispositivos configurados	Muestra el número de dispositivos creados en el proyecto.
Conexiones VPN activas	Muestra el número de conexiones VPN activas.
Usuarios	Muestra el número de conexiones VPN activas a los usuarios creados en el proyecto.
Dispositivos	Muestra el número de conexiones VPN activas a los dispositivos creados en el proyecto.

4.5.2

Tronco

4.5.2.1 Registrar mensajes

Los eventos del sistema que han ocurrido se guardan en los mensajes de registro. Éstos incluyen:

- Inicios de sesión en el sistema
- Cambios en la configuración
- Establecimiento de conexión
- Interrupción de conexiones
- Mensajes operativos

Llamando a la página web

En la navegación, seleccione "Sistema > Archivo de registro" y la pestaña "Mensajes de registro".

Entradas mostradas

Se muestran las siguientes entradas:

Campo	Sentido
Fecha	Muestra la fecha y la hora.
Nivel de mensaje	Soñ posibles los siguientes niveles de mensaje: <ul style="list-style-type: none"> • Emergencia • Alerta • Crítico • Error, por ejemplo, cuando falla la exportación del certificado del servidor • Advertencia, por ejemplo, cuando se elimina una CA • Aviso, por ejemplo, cuando se crea una CA • Información, por ejemplo, cuando un usuario ha iniciado sesión • Depurar
Función	Muestra el estado operativo codificado.
Categoría	Muestra la categoría del mensaje de registro.
Mensaje	Muestra información sobre el evento que ocurrió.

Filtrado de entradas de registro

1. Ingrese el período deseado en los campos "Desde" / "Hasta".
2. Seleccione el nivel requerido de la lista desplegable "Nivel de mensaje".
3. Seleccione la categoría requerida en la lista desplegable "Categoría".
4. Haga clic en el botón "Aplicar filtro".

Resultado

La pantalla se actualiza de acuerdo con la configuración de filtro seleccionada. Solo se muestran las entradas seleccionadas.

Guardar entradas de registro**Nota****Guardar entradas de registro**

El registro se guarda en el archivo de registro después de llegar a 1.000.000 de entradas. Además de esto, un registro semanal se guarda y archiva semanalmente.

Para exportar las entradas del registro, haga clic en el botón Exportar. Navegue hasta el directorio de almacenamiento y guarde el archivo de registro actual en formato *.csv. Todas las entradas se exportan incluso si ha filtrado las entradas.

*Configuración con administración basada en web***4.5 Sistema**

Puede, por ejemplo, enviar los datos con una solicitud de soporte.

Nota**Proteger los archivos de registro exportados del acceso no autorizado**

Los archivos de registro exportados pueden contener información relevante para la seguridad. Por lo tanto, debe asegurarse de que estos archivos estén protegidos contra el acceso no autorizado. Recuerde esto especialmente cuando entregue los archivos.

4.5.2.2**Archivos de registro**

El registro se guarda en el archivo de registro después de llegar a 1000000 de mensajes de registro. Es posible un máximo de 100 archivos de registro.

Llamando a la página web

En la navegación, seleccione "Sistema > Registro", la pestaña "Archivo de registro".

Entradas mostradas

Se muestran las siguientes entradas:

Campo	Sentido
Fecha	Muestra la fecha y la hora.
Tamaño	Muestra el tamaño del archivo de registro.
Comportamiento	Puede administrar las entradas del archivo de registro utilizando los siguientes botones: <ul style="list-style-type: none"> •  Exporte y guarde el archivo de registro seleccionado como un archivo. •  Elimina el archivo de registro seleccionado de la lista.

4.5.2.3**Registro de cortafuegos**

En esta página, puede permitir que los eventos se introduzcan en un archivo de registro para el cortafuegos. Esta información puede resultarle útil a la hora de solucionar problemas de conexión a través de un cortafuegos.

Llamando a la página web

En la navegación, seleccione "Sistema > Archivo de registro" y la pestaña "Registro de firewall".

Entradas mostradas

Realice los siguientes ajustes. Luego haga clic en el botón "Guardar":

Campo	Sentido
Nombre del archivo	Muestra el nombre de archivo del registro del cortafuegos. El nombre del archivo "firewall.log" se almacena en el sistema y no se puede cambiar aquí. Puede cambiar el nombre del archivo durante la exportación.
Paquetes descartados de protocolo	Cuando está habilitado, se emite información sobre los paquetes descartados.
Conexión exitosa del protocolo	Cuando está habilitado, se emite información sobre las conexiones exitosas.
Protocolo de paquetes rechazados	Cuando está habilitado, se genera información sobre los paquetes rechazados.

Exportación de registros de cortafuegos

Con el botón "Exportar", puede descargar el archivo de registro a su PC, por ejemplo, para enviarlo con una solicitud de soporte.

1. Haga clic en el botón "Exportar".

Se abre un cuadro de diálogo para guardar el archivo de registro actual.

2. Navegue hasta el directorio donde desea guardar el archivo y confirme con "Guardar".

4.5.3 Configuración de la red

4.5.3.1 Interfaces

Nota

Direcciones IPv4 y máscara de subred según RFC 1918

Las direcciones IPv4 y las máscaras de subred de fábrica se pueden cambiar según sea necesario, pero deben cumplir con la especificación RFC 1918.

Nota

Para poder acceder al SINEMA RC a través del enrutador de Internet, en el enrutador se debe configurar el reenvío de puertos para los siguientes puertos:

- Para el WBM, consulte Configuración del servidor web (Página 54).
 - para el puerto HTTPS TCP 443 (preestablecido, se puede cambiar)
- Para establecer el túnel OpenVPN, consulte Configuración de OpenVPN (Página 107)
 - el puerto UDP 1194 (preestablecido, se puede cambiar)
 - el puerto TCP 5443 (preestablecido, se puede cambiar)
- Para la actualización del certificado, el puerto TCP 6220 (preajuste del puerto alternativo, se puede cambiar)
- Para el establecimiento del túnel VPN IPsec
 - Puerto UDP 500 (no se puede cambiar) y puerto UDP 4500 (no se puede cambiar)
 - Protocolo IP ESP (protocolo de capa 3)

Llamando a la página web

En la navegación, seleccione "Sistema > Configuración de red" y la pestaña "Interfaces".

Configuración de una interfaz

Realice los siguientes ajustes y luego haga clic en "Guardar":

Campo	Sentido
Activar la interfaz	La interfaz WAN no se puede desactivar. Las interfaces LAN son opcionales y se pueden desactivar.
Interfaz	Seleccione la interfaz a configurar. Si selecciona la interfaz WAN, se requieren entradas adicionales, consulte la tabla "Configuración adicional de la interfaz WAN".
Dirección MAC	Muestra la dirección MAC de la interfaz seleccionada. Es ingresado automáticamente por el sistema.
MTU	MTU (Unidad máxima de transmisión) especifica el tamaño máximo del paquete. Si los paquetes son más largos que la MTU establecida, se fragmentan. El tamaño máximo es de 1500 bytes. Introduzca un valor ≥ 1 500.
Usar DHCP	Habilita la asignación de una dirección IP de la interfaz a través del DHCP servidor.
dirección IP	Introduzca la dirección IPv4 de la interfaz. La dirección IP debe ser única. La entrada es posible cuando la opción "Usar DHCP" está deshabilitada.
Máscara de red	Introduzca la máscara de subred de la subred que está creando. La entrada es posible cuando la opción "Usar DHCP" está deshabilitada.
enmascarado	Habilita el enmascaramiento para una interfaz LAN.

Configuraciones adicionales para la interfaz WAN

Campo	Sentido
Configuración para IPv4	
Puerta de enlace predeterminada	<p>Cuando se opera una VPN a través de Internet, generalmente se requieren direcciones IPv4 adicionales para las puertas de enlace de Internet, como los enruteadores DSL. En la VPN, los módulos individuales deben conocer las direcciones IP públicas de los módulos asociados a los que se puede acceder a través de Internet.</p> <p>Introduzca la dirección IP de la puerta de enlace.</p>
SINEMA Remote Connect se encuentra detrás de un dispositivo NAT con una dirección IP fija	<p>Si selecciona la casilla de verificación, puede ingresar la dirección IPv4 de WAN externa de la puerta de enlace de Internet.</p>
Dirección IP de la WAN	<p>La dirección IPv4 WAN a través de la cual se puede acceder a SINEMA RC. Esta puede ser, por ejemplo, la dirección WAN IPv4 de un enruteador DSL a través del cual SINEMA RC está conectado a Internet.</p>
Configuración para IPv6	
Activar IPv6	También activa IPv6 en la interfaz WAN.
Usar SLAAC para IPv6	Utiliza la configuración automática de direcciones sin estado (SLAAC) para IPv6.
dirección IPv6	<p>Introduzca una dirección IPv6 de la interfaz.</p>
Dirección IPv6 de enlace local	<p>Si se activa "Usar SLAAC para IPv6" en la interfaz, se forma automáticamente una dirección IPv6 local de enlace</p>
Longitud del prefijo de subred	<p>El prefijo IPv6 representa el identificador de subred.</p> <p>Introduzca el número de bits de la izquierda que pertenecen al prefijo.</p> <p>Los prefijos y las direcciones IPv6 se especifican de la misma manera que con la notación CIDR (enrutamiento entre dominios sin clase) para IPv4.</p> <p>Ejemplo: 2001:0db8:1234::1111/48 Introduzca la</p>
Puerta de enlace predeterminada	<p>dirección IPv6 de la puerta de enlace a través de la cual se puede acceder a esta dirección de red.</p>

4.5.3.2 DNS

Los clientes VPN también pueden acceder al SINEMA RC Server utilizando un nombre de host. Para hacer esto, especifique un nombre de host, por ejemplo, sinemarc.example.org

Para la resolución de nombres, especifique el servidor DNS. Esta configuración se adopta en la configuración VPN de los clientes.

La configuración también es necesaria para obtener la licencia.

Llamando a la página web

En el panel de navegación, seleccione "Sistema > Configuración de red" y la pestaña "DNS".

*Configuración con administración basada en web***4.5 Sistema****Crear un nuevo servidor DNS**

Realice los siguientes ajustes y luego haga clic en "Guardar":

Campo	Sentido
nombre de host	Introduzca el nombre de host con el que se puede acceder a SINEMA RC, p. ej., sinemarc.example.org
Host resoluble externamente nombre	Cuando está activado, el nombre de host se incluye en la configuración de VPN y en la configuración de los clientes de VPN.
Servidor DNS principal	Introduzca la dirección IPv4 del servidor DNS principal.
Servidor DNS secundario	Ingrese la dirección IPv4 del servidor DNS secundario que luego se usa si no se puede acceder al servidor DNS principal.

4.5.3.3 Servidor web**Llamando a la página web**

En la navegación, seleccione "Sistema > Configuración de red" y la pestaña "Servidor web".

Configuración del servidor web

Realice los siguientes ajustes y luego haga clic en "Guardar":

Campo	Sentido
puerto HTTPS	Especifique a través de qué puerto HTTPS se realizará el acceso remoto al WBM. Puerto predeterminado HTTPS
puerto alternativo	443 Especifique el puerto alternativo. Este puerto lo utilizan los dispositivos OpenVPN que actualizan las configuraciones mediante el mecanismo de inscripción automática (intervalo de actualización). Si no se puede acceder a estos dispositivos a través del puerto HTTPS, la actualización se realiza a través del puerto alternativo. Puerto predeterminado alternativo
Bloquear el acceso al servidor web desde interfaz WAN	6220 Cuando está habilitado, se deniega el acceso remoto al WBM.

Cambio de números de puerto

Si cambia los números de puerto, utilice puertos del rango de números 1024 ... 65535.

Seleccione un puerto libre que no se utilice de otra manera, por ejemplo, por el puerto TCP en OpenVPN

Los puertos 0 ... 1023 están estandarizados (puertos bien conocidos). De los puertos registrados a partir de 1024, por ejemplo no. 1024 está reservado.

Si usa otro puerto como el puerto predeterminado 443, se debe ingresar el número de puerto junto con la dirección IP. Se deben ingresar dos puntos ":" entre la dirección IP y el número de puerto como delimitador.

Ejemplo:

Si se puede acceder a SINEMA RC a través de Internet a través de la dirección IP 192.144.112.5, y además de este número de puerto se especificó 6443 para el acceso remoto, se debe especificar la siguiente información para la estación remota en el navegador web:

- <https://192.144.112.5:6443>

4.5.3.4**Silbido**

En esta página, comprueba con un ping si se puede acceder a un dispositivo específico en la red.

Llamando a la página web

En la navegación, seleccione "Sistema > Configuración de red" y la pestaña "Ping".

Establecer ping

Realice los siguientes ajustes:

Campo	Sentido
dirección IP	Introduzca la dirección IP del dispositivo.
Repetir	Introduzca el número de reintentos de ping.
Se acabó el tiempo	Ingrese el tiempo de espera dentro del cual el ping verifica el dispositivo.
Salida de ping	Muestra si se puede acceder al dispositivo a través de la dirección especificada.

Haga clic en el botón "Ping" para iniciar el ping.

Resultado

Ping envía solicitudes de ping a la dirección IP para verificar y recibe respuestas del dispositivo de destino, si se puede alcanzar. Una vez transcurrido el tiempo de espera, recibirá un mensaje de estado.

4.5.3.5**Rutas estáticas**

En esta página, define rutas estáticas para la comunicación entre subredes.

Requisito

- Al usuario se le ha asignado el derecho "Editar parámetros del sistema".

Llamando a la página web

En la navegación, seleccione "Sistema > Configuración de red" y la pestaña "Configuración de rutas estáticas".

*Configuración con administración basada en web***4.5 Sistema****Creación de rutas estáticas**

Realice los siguientes ajustes y luego haga clic en "Guardar":

Campo	Sentido
Red de destino	Introduzca la dirección de red del destino al que se puede llegar a través de esta ruta.
Máscara de red	Introduzca la máscara de red del destino.
Puerta	Introduzca la dirección IP de la puerta de enlace a través de la cual se puede acceder a esta dirección de red.
Interfaz	Especifique la interfaz a través de la cual se alcanza la dirección de red del destino.

Resultado

La ruta estática para la comunicación está configurada. La ruta se ingresa en la siguiente tabla.

Nota

Solo las rutas estáticas con la interfaz LAN se reenvían a los dispositivos, a diferencia de las que tienen la interfaz WAN.

Entradas mostradas

Se muestran las siguientes entradas:

Campo	Sentido
Destino La red	Muestra la dirección de destino de la ruta.
Máscara de red	Muestra la máscara de red de la ruta.
Puerta	Muestra la puerta de enlace de la ruta.
Interfaz	Muestra la interfaz de la ruta.

4.5.4**Espacios de direcciones****4.5.4.1****espacio de direcciones de red**

Defina el espacio de direcciones para la LAN local virtual en esta página.

Nota

La primera dirección IP del espacio de direcciones siempre se asigna al SINEMA RC Server.

Llamando a la página web

En la navegación, seleccione "Conexiones remotas > Espacios de direcciones > Subred virtual".

Administrar el espacio de direcciones

1. Haga clic en "Activar espacio de direcciones de red" para establecer la configuración de la subred virtual.

2. Configure el espacio de direcciones para la subred virtual:

Campo	Sentido
dirección de inicio	Dirección de inicio del espacio de direcciones.
Máscara de red	La máscara de red que pertenece al espacio de direcciones.
dirección final	Dirección final del espacio de direcciones El espacio de direcciones está limitado por la dirección de inicio y la máscara de red. La dirección final debe estar dentro de este rango.
Redes disponibles (en total)	Muestra el número de redes disponibles determinado a partir de la dirección inicial y la dirección final.

3. Haga clic en el botón "Guardar".

4.5.4.2**Espacios de direcciones VPN**

Usted define los espacios de direcciones para TCP, UDP e IPsec en esta página. Cuando un cliente VPN inicia sesión en SINEMA RC Server, recibe una dirección IP del espacio de direcciones mientras dura la conexión.

Nota

- La primera dirección IP del espacio de direcciones siempre se asigna al SINEMA RC Server.
- El máximo espacio de direcciones posible comprende 65535 direcciones. La dirección de inicio del espacio de direcciones debe seleccionarse de tal manera que se utilicen al menos dos direcciones del espacio de direcciones.

Llamando a la página web

En la navegación, seleccione "Conexiones remotas > Espacios de direcciones".

Administrar el espacio de direcciones

En las pestañas "OpenVPN" e "IPsec", puede realizar los siguientes ajustes para los espacios de direcciones:

Campo	Sentido
Dirección IP de inicio	Dirección de inicio del espacio de direcciones.
Máscara de red	La máscara de red que pertenece al espacio de direcciones.
Dirección IP final	Dirección final del espacio de direcciones La dirección final se calcula a partir de la máscara de red y la dirección inicial y no se puede configurar.
Uso (IPs asignadas / del total)	Se muestran los siguientes valores: <ul style="list-style-type: none"> • Número de direcciones IP asignadas • Número de direcciones IP disponibles

*Configuración con administración basada en web***4.5 Sistema**

Campo	Sentido
Activar dirección IP fija espacio	Cuando está habilitado, al dispositivo se le puede asignar una dirección IP fija desde el espacio de direcciones.
Protocolo IP fijo	Solo con OpenVPN: <ul style="list-style-type: none">• TCP: se aplica a las conexiones OpenVPN a través de TCP• UDP: se aplica a conexiones OpenVPN a través de UDP
Ubicación del espacio de direcciones IP fijas	<ul style="list-style-type: none">• Primero: las direcciones IP fijas son del área de inicio del espacio de direcciones. La primera dirección IP está reservada para SINEMA RC Server.• La primera dirección IP fija es siempre la segunda dirección IP después de la dirección IP de inicio.• Último: las direcciones IP fijas son del área final del espacio de direcciones. La última dirección IP fija es siempre la dirección IP final.
Longitud del espacio de direcciones IP fijas	Número de direcciones IP fijas

4.5.5 Fecha y hora

Para comprobar la validez de los certificados y las marcas de tiempo de las entradas del registro, se conservan la fecha y la hora actuales. Puede configurar la hora del sistema manualmente o sincronizarla automáticamente con un servidor NTP. Solo un método puede estar activo a la vez.

Llamando a la página web

En la navegación, seleccione "Sistema > Fecha y hora".

Configurar la hora manualmente

Realice los siguientes ajustes en la pestaña "Manual":

Campo	Sentido
hora del sistema	Muestra la hora actual del sistema en el formato "DD.MM.YYYY HH:MM". La visualización depende del idioma configurado.
Usar tiempo de PC	Haga clic en el botón para usar la configuración de hora de la PC.

Configuración automática de la hora del día con NTP

Para la sincronización de la hora del día a través de NTP, realice los siguientes ajustes en la pestaña "NTP":

Campo	Sentido
Activar	Si está habilitado, la sincronización horaria automática se realiza a través de NTP.
hora del sistema	Muestra la hora actual del sistema en el formato "DD.MM.YYYY HH:MM". La visualización depende del idioma configurado.

Campo	Sentido
Última hora de sincronización	Muestra la hora de la última sincronización. • Hora en formato "DD.MM.AAAA HH:MM" O • no sincronizado
Zona horaria	Introduzca la zona horaria que está utilizando en el formato "+/- HH:MM". La zona horaria se relaciona con la hora mundial estándar UTC.
Servidor NTP principal	Introduzca la dirección IP o el nombre de host del servidor NTP principal.
Servidor NTP secundario	Ingrese la dirección IP o el nombre de host del servidor NTP secundario primario es.

Para aplicar la configuración seleccionada, haga clic en el botón "Guardar":

4.5.6 Mensajes SMS y correos electrónicos

4.5.6.1 Proveedor de puerta de enlace de SMS

Para despertar una estación, SINEMA RC Server envía un correo electrónico. El correo electrónico se envía a una puerta de enlace SMS. La puerta de enlace SMS convierte el correo electrónico en un mensaje SMS y lo transfiere al dispositivo, por ejemplo, un M87x. Cuando se acepta el mensaje SMS, el dispositivo establece la conexión con el servidor SINEMA RC.

El requisito es que la tarjeta SIM del dispositivo esté preparada para recibir el mensaje SMS. Encontrará más información al respecto en el manual de configuración del dispositivo.

Nota

La hora a la que se enviará el mensaje SMS de activación a la estación no se puede predecir con precisión y depende de la carga actual de la red. Debido a eventos especiales, un mensaje SMS puede tardar mucho en llegar. Tenga esto en cuenta cuando envíe el mensaje SMS de activación, consulte la sección "Seguimiento y tiempo de respuesta de los mensajes SMS de activación (Página 138)".

Llamando a la página web

En la navegación, seleccione "Sistema > SMS y correo electrónico > Proveedor de puerta de enlace SMS".

Entradas mostradas

Se muestra una lista de los proveedores de puerta de enlace de SMS ya existentes. Por defecto, los datos de cuatro proveedores de red ya están configurados.

Campo	Sentido
Nombre	Nombre del proveedor de puerta de enlace de SMS
Habla a	Dirección de correo electrónico del destinatario del mensaje SMS La dirección de correo electrónico generalmente se compone del número de llamada de la tarjeta SIM y el nombre de la puerta de enlace de SMS. El requisito es que la dirección de correo electrónico esté activada, "Activar la dirección de correo electrónico (Página 137)" Consulte con su proveedor de red si es necesario o no enviar un mensaje SMS de activación. Con el marcador de posición \$\$SMS-NO, el número de teléfono se utiliza automáticamente en el dispositivo.
Número de remitente	Identificación que se transfiere en el correo electrónico.
Tema	Asunto del correo electrónico
CC	Dirección de correo electrónico de otro destinatario El destinatario recibe sólo un correo electrónico. Esto podría ser, por ejemplo, un técnico de servicio que siempre quiere estar informado cuando se activa un determinado dispositivo.
Texto	\$MSG: el texto del mensaje SMS de activación se introduce automáticamente. Según el proveedor de red, el texto del asunto o el cuadro de texto se envía como mensaje SMS. Puede obtener información más detallada sobre esto de su proveedor de red.
Comportamiento	 Abra la descripción general para cambiar el proveedor de la puerta de enlace de SMS.

Creación de un proveedor de puerta de enlace de SMS

1. Haga clic en el botón "Crear".
2. En el siguiente cuadro de diálogo, ingrese un nombre.
3. En "Dirección", ingrese la dirección de correo electrónico del destinatario. Para el número de teléfono, utilice el marcador de posición "\$\$SMS-NO".
4. Para "Asunto" o "Texto", ingrese un marcador de posición "\$MSG". Esto depende de su proveedor de red.
5. Haga clic en el botón "Crear".

4.5.6.2**Ajustes del correo electrónico**

En esta página, especifica si un correo electrónico se reenvía directamente al destinatario o a través de un servidor de retransmisión SMTP. También puede especificar que la transferencia del correo electrónico se realice a través de una conexión cifrada.

Nota**Envío a través de un servidor de retransmisión SMTP**

Para enviar el correo electrónico, se recomienda utilizar un servidor de retransmisión SMTP. Si utiliza el método de transmisión "Directo", es posible que el correo electrónico se clasifique como no seguro. Entonces el correo electrónico se bloquea y no llega.

Llamando a la página web

En la navegación, seleccione "Sistema > SMS y correo electrónico > Configuración".

Configuración del cliente SMTP

Seleccione la casilla de verificación "Activar cliente de correo electrónico" y realice los siguientes ajustes. Luego haga clic en el botón "Guardar":

Campo	Sentido
Método de entrega	Directo: el correo electrónico se reenvía directamente al servidor SMTP. Mediante servidor de retransmisión: el correo electrónico se reenvía a través de un servidor de retransmisión SMTP al destinatario. Realice los ajustes adicionales enumerados en la siguiente tabla.
Máxima vida en el cola(s)	Tiempo máximo en segundos que el remitente espera una respuesta del servidor de correo. Cuando transcurre el tiempo, se cancela la transferencia del correo electrónico.
Remitente	La dirección de correo electrónico especificada como remitente al transferir al servicio de correo es. Con el método de entrega "A través del servidor de retransmisión", se especifica la dirección de correo electrónico de la cuenta de usuario del servidor de retransmisión SMTP respectivo.

Configuraciones adicionales para el método de entrega "Vía servidor de retransmisión"

Introduzca los siguientes datos de acceso adicionales del servidor SMTP:

Campo	Sentido
Servicio de retransmisión SMTP es	Ingrese el nombre o la dirección IP del servidor de retransmisión SMTP que está destinado a reenviar los correos electrónicos recibidos.
El servicio de retransmisión SMTP es el puerto	Especifique el puerto en el que el servidor de retransmisión SMTP acepta conexiones. Como predeterminado, el puerto 587 está configurado para que el correo se reciba solo de usuarios autenticados.
Capa de transporte Seguridad (TLS)	Especifique si los correos electrónicos se transmitirán encriptados a través de TLS: <ul style="list-style-type: none"> • Oportunista: La transmisión del correo electrónico se puede cifrar a través de TLS. Si el servidor de correo receptor no admite la transferencia cifrada, el correo electrónico se reenvía a través de una conexión no cifrada. <p>Esta configuración se usa automáticamente si ha seleccionado "Directo" como método de entrega.</p> <ul style="list-style-type: none"> • Encuadernación: La transmisión del correo electrónico se cifra mediante TLS. Si el servidor de correo receptor no admite la transferencia cifrada, el correo electrónico no se reenvía.
El servidor requiere autenticación	Algunos servidores de retransmisión SMTP requieren un inicio de sesión. Introduzca el nombre de usuario y la contraseña. Algunos proveedores utilizan la dirección de correo electrónico como nombre de usuario. Obtendrá información más detallada de su proveedor.
Nombre de usuario	Nombre de usuario para acceder al servidor de retransmisión SMTP
Clave	Contraseña para acceder al servidor de retransmisión SMTP

Envío de un correo electrónico de prueba

Después de la configuración, puede enviar un correo electrónico de prueba en la pestaña "Correo electrónico de prueba". Para ello, introduce el Destinatario, el Asunto y un texto. Luego haga clic en el botón "Enviar".

4.5.7 Licencias

4.5.7.1 Visión de conjunto

En esta página obtiene una descripción general de las licencias existentes. Puede activar nuevos paquetes de licencia en las pestañas "Activación en línea" y "Activación fuera de línea". Encontrará un resumen de las licencias disponibles en el apartado "Información de licencia (Página 26)".

Llamando a la página web

En el área de navegación, seleccione "Sistema > Licencias".

Entradas mostradas

En la pestaña "Descripción general" se muestra una lista de las licencias existentes:

Campo	Sentido
Número	Números de licencias que están actualmente activadas. En este campo, puede reducir el número de licencias activadas si es necesario. Las licencias liberadas se vuelven a reservar en el número de licencia.
Tipo de licencia	Nombre del paquete de licencia
Número de licencia	Número de licencia utilizado cuando se activó la licencia.
Fecha de activacion	Fecha en que se activó la licencia.
Valor de la licencia	Número de participantes actualmente activados / número de licencias activadas. El número de licencias activadas determina cuántos participantes se pueden configurar en total.
Estado	<ul style="list-style-type: none"> Activa: la licencia está activada y se está utilizando. Bloqueada: la licencia no es válida o está dañada, por ejemplo, si ha cambiado el equipo de hardware.
Comportamiento	 Obtiene una descripción general de la información de la licencia. Esto también se muestra para los usuarios con el derecho "solo lectura".

Liberación de la licencia en línea

Puede liberar licencias no utilizadas o licencias parciales para activarlas en otro sistema, por ejemplo.

Nota

Antes de cambiar de sistema, debe devolver las licencias en línea porque no están incluidas en una copia de seguridad.

Requisitos

- Hay una conexión a Internet.
- Se configura un servidor DNS válido. El servidor DNS se configura en "Sistema > Red > DNS".
- No se utiliza la licencia o licencia parcial.

Procedimiento

1. Haga clic en la pestaña "Resumen".
2. Seleccione la casilla de verificación de la licencia en línea correspondiente e ingrese el número de licencias activadas. licencias, en su caso.
3. Haga clic en el botón "Liberar licencia".

Las licencias de cliente se liberan de la siguiente manera: El número de licencias que se liberan es la diferencia entre el último valor y el valor actual. Las licencias liberadas se vuelven a reservar en el número de licencia. El valor de la licencia se actualiza.

Resultado

Las licencias vuelven a ser gratuitas y se pueden volver a activar en este sistema o en otro sistema.

4.5.7.2**Licencias en línea**

En esta página, puede activar paquetes de licencias en línea.

Llamando a la página web

En la navegación, seleccione "Sistema > Licencias" y la "Activación en línea".

Activación de licencia en línea**Requisitos**

- Hay una conexión a Internet.
- Se configura un servidor DNS válido. El servidor DNS se configura en "Sistema > Red > DNS".

Procedimiento

1. Ingrese el número de licencia correspondiente a la licencia en línea.
2. Haga clic en el botón "Comprobar licencia".

El sistema comprueba si el número de licencia es válido y qué paquete de licencia está activado. Despues de una verificación exitosa, se muestran el tipo de licencia y el valor de la licencia.
El valor de la licencia muestra el número de licencias disponibles.

3. Para licencias de cliente adicionales: Ingrese el número de licencias a activar en el "Número" campo.
4. Haga clic en el botón "Activar licencia" para confirmar la activación de la licencia en línea.

El valor de la licencia en la tabla de resumen se actualiza al número de licencias activadas en este paso.

Resultado

La licencia se activa y se muestra en la pestaña "Descripción general".

Para desactivar las licencias en línea, cambie el número de licencias activadas en la pestaña "Descripción general (Página 62)".

4.5.7.3**Licencias fuera de línea**

En esta página, puede activar nuevos paquetes de licencias sin conexión y desactivar licencias existentes.

Llamando a la página web

En la navegación, seleccione "Sistema > Licencias" y la "Activación en línea".

Licencia fuera de línea**Activar licencia sin conexión**

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

2. Navegue hasta el directorio de almacenamiento donde está almacenado el archivo "sinemarc.WibuCmRaC".

3. Póngase en contacto con Atención al cliente a través de:

– Solicitud de soporte (<https://support.industry.siemens.com/cs/my?l=en-US>)

Cree una nueva solicitud de soporte. Introduzca "Licencia SINEMA" en la barra de búsqueda y haga clic en "Buscar". En "Autorización", seleccione la casilla de verificación "Licencia SINEMA" y haga clic en "Siguiente".

Rellene el formulario "Descripción del problema". Proporcione el número de licencia del paquete de licencia y adjunte el archivo "sinemarc.WibuCmRaC". Haga clic en Siguiente".

Introduce tus datos de contacto y haz clic en "Enviar".

- Correo electrónico (support.automation@siemens.com)

Ingrase la palabra clave "Licencia SINEMA" en la línea de asunto. Proporcione el número de licencia del paquete de licencia en el correo electrónico y adjunte el archivo "sinemarc.WibuCmRaC".

– Teléfono (+49 911 895 7222)

Tenga a mano el número de licencia del paquete de licencia.

4. Si el paquete de licencias está activado, recibirá la licencia sin conexión "sinemarc.WibuCmRaU"

Por correo electrónico. Guarde el archivo en su directorio de almacenamiento.

5. Haga clic en el botón "Seleccionar archivo".

6. Navegue hasta el directorio de almacenamiento y seleccione el archivo "sinemarc.WibuCmRaU".

7. Confirme su selección con el botón "Abrir" y haga clic en el botón "Importar actualización de licencia".

Resultado

La licencia se importa y se muestra en el resumen de licencias existentes.

Nota

Con la activación sin conexión, todas las licencias están siempre activadas. No es posible especificar el número a activar.

Desactivar licencia sin conexión

1. Póngase en contacto con el servicio de atención al cliente por correo electrónico (support.automation@siemens.com).

Ingrese la palabra clave "Licencia SINEMA" 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 de licencia sin conexión".

2. Seleccione la licencia sin conexión necesaria.

3. Haga clic en el botón "Liberar licencia".

Resultado

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

4.5.8**Actualizar**

Si hay una nueva versión disponible para SINEMA RC Server, puede encontrar la actualización en las páginas de Internet de Siemens Industry Online Support con el siguiente ID: 21816 (<https://support.industry.siemens.com/cs/ww/en /ps/21816/dl>)

Actualizar archivos

Los archivos de actualización están firmados y encriptados. Esto garantiza que solo los archivos de actualización creados por Siemens se puedan descargar en el dispositivo. La actualización automática no es posible, los archivos de actualización solo se proporcionan a través de SIOS.

La actualización debe realizarse en el orden correcto: V1.0 > V1.1 > V1.2 >
V1.3 > V2.0 > V2.1 > V3.0

Nota**Actualización del sistema V1.2 > V1.3**

Debido a cambios en la instalación básica, una actualización de V1.2 a V 1.3 solo es posible utilizando el CD de instalación.

Nota**Actualización del sistema V2.0 > V2.1**

Antes de actualizar la versión del software, debe liberar las licencias para "SINEMA RC (2.0)" y reactivarlas en la versión de servidor V2.1. El procedimiento se describe en el apartado "Actualización del sistema V2.0 > V2.1 (Página 130)".

Llamando a la página web

En la navegación, seleccione "Sistema > Actualizar > Actualización del sistema".

Requisito

- Al usuario se le ha asignado el derecho "Editar parámetros del sistema". • Se ha descargado la última versión de SINEMA RC. El archivo de actualización tiene el formato *.tar.gz.
- El usuario tiene acceso al directorio de almacenamiento.

Actualización del sistema

Procedimiento

1. Haga clic en el botón "Seleccionar archivo".
2. Navegue hasta el directorio de almacenamiento y seleccione el archivo *.tar.gz.
3. Confirme su selección con el botón "Abrir".
4. Haga clic en el botón "Importar".

Resultado

El sistema está actualizado. Según el tipo de actualización, se reinician funciones individuales o todo el sistema. Para verificar la versión después del reinicio, en la navegación, haga clic en "Sistema> Descripción general" y verifique la versión de software que se muestra.

4.5.9 Copia de seguridad y restauración**4.5.9.1 copias de seguridad**

Puede realizar hasta 30 copias de seguridad de la configuración del sistema del SINEMA RC Server y recargarlas cuando sea necesario. Las copias de seguridad individuales se guardan en formato *.backup y se pueden importar a otro sistema con la misma versión de SINEMA RC.

Puede encontrar información adicional

- En la sección "Mantenimiento y servicio".
- En Internet con el siguiente ID de entrada: 109748144
<https://support.industry.siemens.com/cs/ww/de/view/109748144/en>

Requisito para la creación de copias de seguridad

- Al usuario se le ha asignado el derecho "Crear copias de seguridad".
- Los ajustes para la copia de seguridad están configurados.

Llamando a la página web

En la navegación, seleccione "Sistema > Copia de seguridad y restauración > Copias de seguridad".

Entradas mostradas

En la pestaña "Copias de seguridad", se muestra una lista de las copias de seguridad existentes:

Campo	Sentido
Fecha	Fecha en la que se creó la copia de seguridad
Nombre del creador	Nombre del usuario que creó la copia de seguridad
Tamaño	Tamaño de archivo de la copia de seguridad
Comentario	Comentar la copia de seguridad. El texto se puede introducir al crear o importar una copia de seguridad.

Configuración con administración basada en web

4.5 Sistema

Campo	Sentido
Estado	<ul style="list-style-type: none"> • Listo Se ha creado la copia de seguridad. • Restaurar: se restaura la configuración del sistema de la copia de seguridad seleccionada.
Comportamiento	 Para esta acción, necesita el derecho de usuario "Restaurar el sistema". SINEMA RC Server toma la configuración del sistema de la copia de seguridad seleccionada y continúa trabajando con ella. Todos los ajustes realizados hasta este momento que no se hayan guardado en una copia de seguridad se perderán.
	 Exportar y guardar la copia de seguridad seleccionada como archivo (*.backup).

Creación de una nueva copia de seguridad**Requisito**

- Los ajustes para las copias de seguridad están configurados.

Con esta función, crea una nueva copia de seguridad con la configuración actual del sistema.

1. Haga clic en el botón "Crear nueva copia de seguridad".
2. En el cuadro de diálogo siguiente, si es necesario, introduzca un comentario sobre la copia de seguridad.
3. Haga clic en el botón "Finalizar".

Resultado

La copia de seguridad se crea y se muestra en la lista de copias de seguridad.

Nota**Ajustes que no se toman**

Las siguientes configuraciones no se respaldan:

- Configuración de red (excepción: puerto HTTPS)
- Mensajes de registro

Importación de la copia de seguridad**Nota**

La clave de codificación debe ser idéntica en ambos sistemas. Una copia de seguridad codificada con la clave (x) no se puede importar en un sistema con la clave (y).

Con esta función se carga una copia de seguridad previamente creada que se guardó como archivo.

1. Haga clic en el botón "Importar copia de seguridad".
2. En el cuadro de diálogo siguiente, si es necesario, introduzca un comentario sobre la copia de seguridad.
3. Haga clic en el botón "Seleccionar archivo".
4. Seleccione el archivo requerido en el formato *.backup y confirme su selección con "Abrir" botón.

5. Haga clic en el botón "Finalizar".

6. En "Acciones" haga clic en el botón "Restaurar" para adoptar la configuración del sistema del seleccionado
Copia de respaldo.

Resultado

SINEMA RC Server toma la configuración del sistema de la copia de seguridad seleccionada y continúa trabajando con esta configuración.
Todos los ajustes realizados hasta este momento que no se hayan guardado en una copia de seguridad se perderán.

Ver también

[Ajustes \(Página 69\)](#)

4.5.9.2

Ajustes

Utilice esta página para establecer la configuración de las copias de seguridad.

Llamando a la página web

En la navegación, seleccione "Sistema > Copia de seguridad y restauración > Configuración".

Entradas mostradas

En la pestaña "Configuración", configura los datos para la copia de seguridad:

Campo	Sentido
Número máximo de copias de seguridad locales	Número máximo de copias de seguridad locales permitidas Se permite una entrada entre 10 y 30. Cuando se alcanza el número máximo, se sobrescribe la copia de seguridad más antigua.
Intervalo de respaldo automático	Habilita la copia de seguridad automática si se va a realizar una copia de seguridad del sistema a intervalos regulares. Las siguientes entradas son posibles: <ul style="list-style-type: none"> • Discapacitado • A diario • Todos los domingos • Cada Sábado • Cada primer día del mes
Automático tiempo de copia de seguridad (UTC)	Información de tiempo para el guardado automático
Clave de encriptación	Clave de cifrado para cifrar una copia de seguridad La clave de cifrado debe tener al menos 8 caracteres e incluir caracteres especiales, mayúsculas y minúsculas, así como números, consulte la sección "Caracteres permitidos".
Confirmar clave de cifrado	La clave de cifrado debe introducirse dos veces.

Configuración de ajustes para copias de seguridad**Requisito**

- Al usuario se le ha asignado el derecho "Editar parámetros del sistema".

Procedimiento

1. Introduzca el número de copias de seguridad permitidas.
2. Seleccione la entrada adecuada en la lista desplegable "Intervalo de copia de seguridad automática" para crear copias de seguridad automáticamente.
3. Ingrese el tiempo para la copia de seguridad automática.
4. Introduzca una "Clave de codificación" con la que se cifra la copia de seguridad.
5. Confirme la "clave de cifrado".
6. Haga clic en el botón "Guardar".

4.5.10 Administración de energía**4.5.10.1 Administración de energía**

El sistema se puede reiniciar o apagar en esta página. También puede definir una partición de arranque para el reinicio.

Llamando a la página web

En la navegación, seleccione "Sistema > Administración de energía".

Administración de energía

El sistema se puede reiniciar o apagar con los siguientes botones:

- Reiniciar el sistema
- Apagado del sistema

4.5.10.2 Partición de arranque

Esta página está disponible a partir de la versión 3.0 y muestra la versión del servidor SINEMA RC instalada actualmente. A partir de la versión 3.1, siempre están disponibles las dos versiones de servidor SINEMA RC instaladas más recientemente: la versión actual y la versión anterior. La versión anterior sirve como copia de seguridad.

Llamando a la página web

En la navegación, seleccione "Sistema > Administración de energía > Partición de arranque".

Definición de la partición de arranque

1. Haga clic en la casilla de verificación de la versión con la que debe iniciarse el sistema operativo.
2. Guarde su selección con "Guardar".

Resultado

La partición seleccionada se inicia después del siguiente reinicio del sistema.

4.5.11 Ajustes

4.5.11.1 información del servidor

En esta página, puede crear su propio texto de información que se muestra en la pantalla de inicio de sesión del servidor SINEMA RC.

Llamando a la página web

Seleccione "Sistema > Configuración > Información del servidor" en la navegación.

Requisito

- Al usuario se le ha asignado el derecho "Editar parámetros del sistema".

Creación de un texto de información del servidor

1. Seleccione la casilla de verificación "Mostrar texto de información del servidor en la pantalla de inicio de sesión".
2. Introduzca el texto y confirme su entrada con "Guardar". El texto puede tener un máximo de 250 caracteres largos.

El texto se muestra encima de la pantalla de inicio de sesión del servidor SINEMA RC. Este texto se puede mostrar en el cuadro de información del servidor en SINEMA RC Client.

4.5.11.2**Cierre de sesión automático**

Puede definir el tiempo de la sesión en esta página.

Llamando a la página web

Seleccione "Sistema > Configuración > Cierre de sesión automático" en la navegación.

Requisito

- Al usuario se le ha asignado el derecho "Editar parámetros del sistema".

Configuración del intervalo de tiempo

1. Introduzca el tiempo en minutos. El valor introducido debe estar entre 1 y 60.
2. Confirme la entrada con "Guardar".

Una vez transcurrido el tiempo, el servidor finaliza la sesión.

4.6 Conexiones remotas**4.6.1****Administrar dispositivos****4.6.1.1****Descripción general de la administración de dispositivos**

Las entradas de dispositivos existentes se enumeran en forma tabular en esta página. La información más importante de cada dispositivo se muestra en diferentes columnas. Utilice el botón encima de la tabla para mostrar u ocultar las columnas y cambiar su orden.

Cuando crea el dispositivo, puede usar grupos de participantes para restringir el acceso a nodos específicos. Antes de crear los dispositivos, tiene sentido crear los grupos individuales primero (consulte la sección "Crear grupos de participantes (Página 81)").

Nota

Tenga en cuenta que un dispositivo debe asignarse al menos a un grupo de participantes.

Si el dispositivo no está asignado a ningún grupo de participantes, solo los usuarios con el derecho "Administrar dispositivos" pueden editarlo.

Requisito

- Al usuario se le ha asignado el derecho "Administrar dispositivos".

Llamando a la página web

En la navegación, seleccione "Conexiones remotas > Dispositivo".

Entradas mostradas

Campo	Sentido
Nombre del dispositivo	Muestra el nombre del dispositivo.
Identificación del dispositivo	El ID del dispositivo se crea automáticamente cuando se crea el dispositivo. Necesario para iniciar sesión en SINEMA RC Server.
dirección VPN	La dirección IP del dispositivo utilizado durante la comunicación a través de VPN. La dirección es asignada automáticamente por SINEMA RC. Si la comunicación a través de VPN no está activa, se muestra "ninguno".
subred remota	La dirección IP de la subred remota. Si la opción "Subredes locales conectadas" no está activada, se muestra "ninguna", consulte el apartado "Crear un nuevo dispositivo (Página 75)". Si se crean varias direcciones IP, se muestran una debajo de la otra.
subred virtual	La subred que coincide con la dirección IP NAT del dispositivo. Si la opción "NAT para subred local" no está activada, se muestra "ninguno", consulte el apartado "Crear un nuevo dispositivo (Página 75)". Si se crean varias direcciones IP, se muestran una debajo de la otra.
Estado	 Online  Offline Discalpidadado
Último acceso	Indica cuándo se inició sesión por última vez en el dispositivo.
Ubicación	Ubicación del dispositivo. Este puede ser, por ejemplo, el lugar de instalación del dispositivo.
Tipo de conexión	Muestra cuándo se establecerá la conexión. <ul style="list-style-type: none"> • Permanente: La conexión VPN existe permanentemente. • Entrada digital: La conexión VPN se establece tan pronto como hay una señal en la "entrada digital" del dispositivo. • SMS de despertador (M-800) o SMS de despertador (RTU 3030) Envía un SMS al dispositivo. La conexión se establece tan pronto como el dispositivo recibe el SMS. • SMS despertador / Entrada digital (M-800) La conexión se establece a través de la entrada digital o mediante un comando SMS.
Tipo de dispositivo	Muestra la designación de tipo del dispositivo.
Vendedor	Muestra el fabricante del dispositivo.
protocolo vpn	Muestra qué protocolo se está utilizando para la conexión VPN. 1. OpenVPN: La conexión se establecerá a través de OpenVPN. 2. IPsec: La conexión se establecerá vía IPsec.
Proveedor de puerta de enlace de SMS	Solo para M800 Mobile, RTU 303xC, RM1224 Muestra el proveedor de puerta de enlace de SMS. Puede configurar el proveedor de puerta de enlace SMS en "Sistema > Correo electrónico y SMS".

Campo	Sentido
Comentario	Muestra el comentario.
Comportamiento	 Obtiene una visión general de la información del dispositivo. La información del dispositivo contiene el ID del dispositivo y la huella digital. Estos dos datos deben introducirse en el dispositivo. Durante el establecimiento de la conexión, el dispositivo se autentica con SINEMA RC Server utilizando esta información.
	 Editar la configuración del dispositivo
	 El archivo de configuración con la configuración de OpenVPN para este dispositivo se crea y se puede guardar. El archivo se puede exportar al dispositivo final.
	 Se crea un archivo PKCS#12 protegido con contraseña y se puede guardar. El certificado se deriva de la última CA válida. El archivo contiene la clave privada del dispositivo con el certificado correspondiente. El archivo se puede exportar al dispositivo final. Cuando se solicite la contraseña, introduzca la contraseña que especificó cuando creó el dispositivo (consulte la sección "Crear un nuevo dispositivo (Página 75)").
	 El certificado y la clave se almacenan como texto ASCII codificado en Base64.
	 Desactivar dispositivo • Si el dispositivo está conectado, la conexión existente también se desactiva. • Si el dispositivo intenta establecer una conexión VPN, el dispositivo lo ignora. Servidor de CINE RC.
	 Activar dispositivo. El dispositivo puede establecer una conexión VPN con el SINEMA RC Server.
	 Solo disponible con el tipo de conexión "Wake-up SMS" o "Digital input & Wake-up SMS". • Si el dispositivo no está conectado, SINEMA RC Server envía el mensaje SMS de activación al dispositivo.

Crear un dispositivo

Haga clic en el botón "Crear" y configure los ajustes necesarios, consulte Creación de un nuevo dispositivo (Página 75).

Filtrado de entradas

1. Seleccione una entrada en "Filtro de búsqueda".
2. Introduzca un término de búsqueda o parte del término de búsqueda en el cuadro de búsqueda.
3. Para limitar aún más la búsqueda, seleccione la casilla de verificación "Coincidencia precisa".

Cuando se selecciona, se tienen en cuenta mayúsculas y minúsculas y se busca la palabra de búsqueda completa.

Los resultados de la búsqueda coincidirán exactamente con el término de búsqueda ingresado.

4. Haga clic en el botón "Aplicar filtro".

Resultado

La lista se actualiza en función de los ajustes realizados. Para volver a mostrar todas las entradas, haga clic en el botón "Mostrar todo".

4.6.1.2 Creando un nuevo dispositivo**Configuración de dispositivo**

Usted establece la configuración para el dispositivo deseado en esta página. Los ajustes se dividen en áreas que se pueden contraer y expandir para mayor claridad.

**Llamando a la página web**

En la navegación, seleccione "Conexiones remotas > Dispositivo".

Procedimiento

1. Haga clic en el botón "Crear".
2. Configure la **Información general del dispositivo**:

Campo	Sentido
Nombre del dispositivo	<p>Ingrés un nombre.</p> <p>El nombre debe cumplir las siguientes condiciones:</p> <ul style="list-style-type: none"> • Debe ser único • debe comenzar con una letra. • Se permiten los siguientes caracteres: az, AZ, 0-9 y – • "conn" no se puede utilizar como nombre.
Clave	Introduzca una contraseña y confirme esta contraseña.
Confirmar contraseña	Consulte también las directrices en el apartado "Caracteres permitidos (Página 27)".
Vendedor	Puede introducir el fabricante del dispositivo.
Escribe	<p>Seleccione el tipo de nodo de la lista.</p> <p>Si su tipo de dispositivo no se muestra o no lo sabe, seleccione "Otro".</p> <p>Todas las funciones ahora están habilitadas.</p>
Proveedor de puerta de enlace de SMS	<p>Solo para M800 Móvil, RTU 303xC, RM1224</p> <p>Seleccione el proveedor de puerta de enlace de SMS. Puede configurar el proveedor de puerta de enlace SMS en "Sistema > Correo electrónico y SMS".</p>
número GSM	<p>Solo para M800 Móvil, RTU 303xC, RM1224</p> <p>Introduzca el número de teléfono del nodo al que se envía el SMS de activación.</p>

*Configuración con administración basada en web***4.6 Conexiones remotas**

Campo	Sentido
identificación del remitente	Solo con RTU 303xC Este ID identifica el servidor SINEMA RC ante la RTU. El ID también debe configurarse en la RTU.
Ubicación	Puede introducir la ubicación de instalación del dispositivo.
Comentario	Puede ingresar un comentario.

3. Configure los **ajustes de VPN:**

Campo	Sentido
protocolo vpn	Especifique qué protocolo se utilizará para la conexión VPN. La selección depende del tipo de dispositivo seleccionado. <ul style="list-style-type: none"> • OpenVPN: La conexión se establecerá a través de OpenVPN. Configure los ajustes en "Seguridad > Ajustes básicos de VPN > Abrir VPN". • IPsec: La conexión se establecerá a través de IPsec.
Tipo de conexión	Especifique cuándo se establecerá la conexión VPN. La selección depende del tipo de dispositivo seleccionado. <ul style="list-style-type: none"> • Permanente <ul style="list-style-type: none"> El dispositivo establece una conexión VPN con el SINEMA RC Server. El túnel VPN se mantiene permanentemente. • Entrada digital <ul style="list-style-type: none"> El establecimiento de la conexión se controla a través de la entrada digital (DI) del dispositivo. • SMS de activación (SCALANCE M-800) / SMS de activación (RTU) <ul style="list-style-type: none"> Cuando el dispositivo recibe un SMS de activación, establece una conexión con el servidor SINEMA RC. • Entrada digital / SMS de activación (SCALANCE M-800) <ul style="list-style-type: none"> El establecimiento de la conexión se controla a través de la entrada digital o mediante un SMS de activación.
Solicitar dirección VPN	Cuando esta opción está habilitada, se solicita una dirección VPN durante el establecimiento de la conexión. <ul style="list-style-type: none"> • OpenVPN: la configuración siempre está seleccionada y no se puede cambiar. • IPsec: active o desactive la opción.
Usar dirección VPN fija	Si se selecciona esta opción, puede asignar una dirección VPN fija al dispositivo. A través de la conexión VPN, siempre se puede acceder al dispositivo en esta dirección VPN. <p>Esto solo es posible cuando el parámetro "Activar espacio de direcciones IP fijas" está habilitado.</p> <p>El parámetro depende del modo de conexión VPN.</p> <ul style="list-style-type: none"> • OpenVPN: Conexiones remotas > Espacios de direcciones > OpenVPN • IPsec: Conexiones remotas > Espacios de direcciones > IPsec
Dirección VPN fija	Ingrese la dirección VPN deseada.

4. Configure parámetros adicionales para la conexión VPN.

La máscara de configuración depende del protocolo VPN seleccionado.

– Conexión OpenVPN

Para configurar los parámetros, habilite "Parámetros de conexión".

Campo	Sentido
dirección IP	dirección IP de la conexión Introduzca la dirección IP a través de la cual se puede acceder al SINEMA RC Server.
Puerto	Introduzca el puerto en el que SINEMA RC Server recibe la conexión OpenVPN.
Protocolo	Especifique si la conexión OpenVPN se realiza a través de TCP o UDP.

– Conexión IPsec

Campo	Sentido
perfil IPsec	Solo se puede seleccionar en el modo de conexión "IPsec". Los perfiles IPsec se configuran en "Seguridad > Configuración básica de VPN > Perfil IPsec".
Certificado	<ul style="list-style-type: none"> • Certificado predeterminado Se utiliza el certificado CA del SINEMA Remote Connect Server para la autenticación. Debe exportar el certificado, ya que es necesario para la configuración de los dispositivos. El certificado se exporta a través de "Seguridad > Gestión de certificados > Certificado CA". • Certificados importados Solo se pueden seleccionar certificados importados con IPsec VPN. Puede importar certificados a través de "Seguridad > Gestión de certificados > Certificado de dispositivo".
ID local	IPsec utiliza el ID local y el ID remoto para identificar de forma exclusiva a los socios (punto final de VPN) durante el establecimiento de una conexión VPN.
identificación remota	Solo se requiere si el socio del túnel VPN evalúa la entrada.

5. Configure el acceso total.

Las subredes y los nodos accesibles a través del dispositivo son miembros de este grupo de participantes. Puede asignar uno o más grupos de participantes.

Seleccione el grupo de usuarios deseado y haga clic en el botón "Agregar". Para eliminar, haga clic en .

6. Si no necesita más configuraciones de red, haga clic en "Finalizar rápido".

Si necesita más configuraciones de red, haga clic en "Siguiente". El requisito previo es que el dispositivo admita subredes.

Configuración con administración basada en web

4.6 Conexiones remotas

Configuración de la red

Esta página solo está disponible para los tipos de dispositivos que admiten las subredes. Encontrará información sobre su dispositivo en el apartado "Estaciones conectables (Página 24)".

En esta página, define las subredes y los nodos a los que se puede acceder a través del dispositivo y quién puede acceder a ellos.

Requisito

- El dispositivo admite subredes.

Procedimiento

1. Si el dispositivo es una puerta de enlace, active "El dispositivo es una puerta de enlace de red". Si el dispositivo no funciona como una puerta de enlace de red, se fuerza un NAT de origen en el dispositivo con esta configuración.
2. En el cuadro de entrada "Nombre de subred", ingrese un nombre válido y haga clic en "Agregar".

Se crea el área "Nombre de subred [Nombre de subred]". Para eliminar, haga clic en .

3. Configure la subred:

Campo	Sentido
Grupos de participantes	Seleccione el grupo de participantes que tiene acceso a la subred y haga clic en el botón "Agregar". Puede asignar uno o más grupos de participantes. Para eliminar, haga clic en  .
IP de subred	Introduzca la dirección IPv4 de la subred accesible desde el dispositivo.
Máscara de subred	Especifique la máscara de red de la subred.

4. Especifique el mecanismo NAT para el "modo NAT":

- Sin

Para una comunicación IP transparente a través del túnel OpenVPN sin NAT. Los dispositivos que se comunican entre sí siempre utilizan la dirección IP explícita del interlocutor de comunicación.

- 1: 1 NA

La dirección IP de red de la subred remota está representada por una dirección IP de red virtual. Las direcciones IP de la red se convierten en el dispositivo remoto. La dirección IP del host permanece sin cambios. La dirección IP virtual debe usarse para dirigirse a un nodo en la subred remota.

- NAT para anfitriones locales

La dirección IP del dispositivo en la subred remota está oculta detrás de una dirección IP dedicada. Las direcciones IP del dispositivo se convierten en el dispositivo remoto. Puede especificar la dirección IP virtual dedicada para dirigirse a un nodo en la subred remota.

5. Si ha habilitado el modo NAT, configure la subred virtual:

Campo	Sentido
IP de subred virtual	Especifique la dirección IP para la subred virtual. Si el espacio de direcciones de red está habilitado, la dirección de inicio se ingresa automáticamente. Puede personalizar esta dirección.
Máscara de subred virtual	Solo disponible con "NAT para hosts locales": Introduzca la máscara de red de la subred virtual.

6. Ingrese un nombre único para "Nombre de nodo" y haga clic en "Agregar".

Se crea el área "Nodo [nombre de nodo]". Para eliminar, haga clic en .



7. Configure el nodo:

Campo	Sentido
Nombre del nodo	Muestra el nombre que le asignó al nodo.
IP del dispositivo terminal	Especifique la dirección IP del nodo. La dirección IP debe estar en la subred configurada.
IP del dispositivo terminal virtual	1: 1 NA La dirección IP virtual se ingresa automáticamente. • NAT para hosts locales Especifique las direcciones IPv4 NAT traducidas.
grupo de participantes	Seleccione el grupo de participantes remotos que tiene acceso al dispositivo y haga clic en "Agregar". Puede asignar uno o más grupos de participantes. Para eliminar, haga clic en .

8. Haga clic en el botón "Guardar".

Configuración de una plantilla con configuración de red

Para transferir la misma configuración de red a otros dispositivos, puede crear una plantilla en "Configuración de plantilla" y usarla.

Botón	Sentido
Guardar la configuración como plantilla	Para guardar la configuración de red en una plantilla, haga clic en el botón "Guardar configuración como plantilla". Nota: Cuando se guarda una nueva plantilla, la plantilla existente se sobrescribe con nuevos valores.
Cargar configuración desde plantilla	Para copiar la configuración de red desde la plantilla, haga clic en el botón "Cargar configuración". Nota: Cuando se carga la plantilla, todas las configuraciones nuevas se sobreescritan con los valores de la plantilla sin previo aviso. Las subredes recién creadas se eliminan si la plantilla no las contiene.

Al crear la plantilla, tenga en cuenta que solo está disponible la última plantilla guardada.

Los siguientes valores se ingresan en la plantilla:

- Configuración para "El dispositivo es una puerta de enlace de red".
- Nombre de subred y asignación de grupos de participantes

Configuración con administración basada en web

4.6 Conexiones remotas

- Dirección IP de subred y máscara de subred

Si el modo NAT se establece en "sin", esta información debe ser única. Adapte la información antes de guardar la configuración de red.

- Modo NAT seleccionado

- IP de subred virtual y máscara de subred virtual Si la

subred virtual está activada, estos valores no se toman de la plantilla, sino que se completan automáticamente con la siguiente dirección libre. Si NAT no está habilitado, ingrese los valores antes de guardar la configuración de red.

- Nombre del nodo

- IP del dispositivo terminal

- IP del dispositivo terminal virtual

El cálculo continúa automáticamente con la siguiente dirección IP libre.

- Asignación de los grupos de participantes

4.6.1.3

Actualización de dispositivos

Puede encontrar información sobre el estado del firmware cargado en esta página.

Llamando a la página web

En la navegación, seleccione "Conexiones remotas > Actualización de dispositivos > Dispositivos".

Entradas mostradas

Se muestra una lista de información sobre la versión de firmware instalada.

Campo	Sentido	
Nombre del dispositivo	Muestra el nombre del dispositivo.	
Última versión de firmware conocida	La versión de firmware que el dispositivo transfirió al SINEMA RC Server.	
Última solicitud conocida del firmware	Información sobre cuándo el dispositivo solicitó el firmware por última vez.	
Estado		Online: el dispositivo está conectado a SINEMA RC Server a través de VPN.
		Fuera de línea: el dispositivo no está conectado a SINEMA RC Server a través de VPN.
	Discapacitado	El dispositivo está deshabilitado.
Comportamiento		Desactivar dispositivo <ul style="list-style-type: none"> • Si el dispositivo está conectado, la conexión existente también se desactiva.
		Vuelva a activar el dispositivo.

Actualización de firmware

1. Haga clic en la pestaña "Archivo de firmware".
2. Haga clic en el botón "Seleccionar archivo".
3. Navegue hasta el directorio de almacenamiento y seleccione el archivo de actualización (*.swf). Confirma tu selección con el botón "Abrir".
4. Haga clic en el botón "Importar".
5. Haga clic en la pestaña "Dispositivos".
6. Seleccione los dispositivos que desea actualizar.
7. Haga clic en el botón "Guardar".

Resultado:

Después de guardar, SINEMA RC Server envía la solicitud al dispositivo para cargar el nuevo firmware. El dispositivo descarga el firmware y se reinicia.

La versión de firmware actual se introduce en la tabla bajo "Última versión de firmware conocida".

Cada actualización del dispositivo se documenta en los "Mensajes del archivo de registro" en "Sistema > Archivo de registro".

4.6.2 Grupos de participantes

Los usuarios, dispositivos, dispositivos finales y subredes se pueden agrupar en grupos de participantes. Los nodos también se pueden asignar a varios grupos de participantes. También especifica si la comunicación entre los participantes de un grupo individual está permitida o prohibida.

Una vez creados los grupos de participantes, puede definir las relaciones de comunicación entre los grupos; véase el apartado "Relaciones de comunicación (Página 82)".

Requisito para crear grupos de participantes

- Al usuario se le ha asignado el derecho "Gestionar conexiones remotas".

Llamando a la página web

En la navegación, seleccione "Conexiones remotas > Grupos de participantes".

Entradas mostradas

Se muestra una lista de los grupos de participantes que ya se han creado:

Campo	Sentido
Nombre del grupo	nombre del grupo
Los miembros pueden comunicarse	Indica que los miembros de este grupo pueden comunicarse entre sí.
Interfaces Ethernet accesibles	Muestra la interfaz LAN a través de la cual se puede acceder al túnel VPN.
Número de usuarios	Número de usuarios asignados al grupo.

Configuración con administración basada en web

4.6 Conexiones remotas

Campo	Sentido
Número de dispositivos	Número de dispositivos asignados al grupo.
Número de subredes	Número de subredes asignadas al grupo.
Número de nodos	Número de nodos asignados al grupo.
Número de roles	Número de roles asignados al grupo.
Comportamiento	 Abrir lista de miembros. En la lista se muestran todos los dispositivos y usuarios pertenecientes al grupo de participantes y su estado (en línea o fuera de línea).
	 Abra la vista general para cambiar la configuración de los grupos de participantes.
	 Abra el resumen para modificar las relaciones de comunicación.

Crear nuevo grupo de participantes

1. Haga clic en el botón "Crear".
2. Ingrese un nombre de grupo y, opcionalmente, una descripción en el siguiente cuadro de diálogo.
3. Especifique si los miembros del grupo pueden comunicarse entre sí.
4. Especifique a qué interfaz LAN se puede acceder a través del túnel VPN.
5. Haga clic en el botón "Guardar".

Resultado

El grupo de participantes ha sido creado. Ha especificado si la comunicación entre los miembros de este grupo está permitida o prohibida.

Cambiar la configuración de los grupos de participantes

1. Cambie la configuración del grupo de participantes relevante.
2. Luego haga clic en el botón "Guardar".

Filtrado de entradas

1. Seleccione una entrada en "Filtro de búsqueda".
2. Introduzca un nombre o parte del nombre en el cuadro de búsqueda.
3. Haga clic en el botón "Aplicar filtro".

Resultado

La lista se actualiza en función de los ajustes realizados. Para volver a mostrar todas las entradas, haga clic en el botón "Mostrar todo".

4.6.3**Relaciones de comunicación**

Usted define las relaciones de comunicación entre los grupos en esta página.

Requisito

- Al usuario se le ha asignado el derecho "Gestionar conexiones remotas".
- Se han creado grupos de participantes.

Llamando a la página web

En la navegación, seleccione "Conexiones remotas > Relaciones de comunicación".

Entradas mostradas

Se muestra una lista de las relaciones de comunicación ya creadas:

Campo	Sentido
Grupo de origen	Nombre del grupo de origen
Grupo de destino	Nombres de los grupos de destino cuyos miembros pueden comunicarse con los miembros del grupo de origen.
Comportamiento	 Abra la vista general para cambiar la configuración de los grupos de participantes.

Crear relaciones de comunicación entre los grupos participantes

1. Especifique el grupo de origen. Para este grupo, haga clic en el icono .
2. En la página siguiente, define los grupos de destino a los que se permiten conexiones del grupo fuente.
3. Haga clic en el botón "Guardar".

Resultado

Se especifica la comunicación entre los grupos de participantes. Ha especificado si la comunicación entre los miembros de este grupo está permitida o prohibida.

Cambiar las relaciones de comunicación entre los grupos de participantes

1. En la navegación, seleccione "Conexiones remotas > Relaciones de comunicación".
2. Haga clic en el  icono. Cambie las relaciones de comunicación relevantes y luego haga clic en "Guardar" botón.

Filtrado de entradas

1. Seleccione una entrada en "Filtro de búsqueda".
2. Introduzca un nombre o parte del nombre en el cuadro de búsqueda.
3. Haga clic en el botón "Aplicar filtro".

Resultado

La lista se actualiza en función de los ajustes realizados. Para volver a mostrar todas las entradas, haga clic en el botón "Mostrar todo".

4.6.4 Asignación de un nodo a un grupo

Asignar usuarios a uno o más grupos

1. Haga clic en el  icono en la vista general del usuario.

Se muestran los grupos de participantes que ya se han creado.

2. Seleccione el grupo o grupos a los que se asignará el participante.
3. Haga clic en el botón "Guardar".

Asigne dispositivos, subredes o nodos a uno o más grupos.

1. Haga clic en el  icono en la vista general del dispositivo.

Se abre la configuración general del dispositivo.

2. En "Acceso total", seleccione el grupo de usuarios deseado y haga clic en el botón "Agregar".
3. Haga clic en el botón "Guardar".
4. Si el dispositivo admite subredes, puede asignar las subredes y los nodos accesibles a través del dispositivo a los grupos de participantes en la configuración de red.
Seleccione el grupo de participantes que tiene acceso a la subred o nodo y haga clic en el botón "Agregar".

5. Haga clic en el botón "Guardar".

4.7 Cuentas de usuario

4.7.1 Resumen de las cuentas de usuario

Requisito para crear y cambiar usuarios

Al usuario se le ha asignado el derecho "Gestionar usuarios".

Llamando a la página web

En la navegación, seleccione "Cuentas de usuario > Usuarios y roles".

Entradas mostradas

Se muestra una lista de los usuarios que ya se han creado junto con su estado. Además, se muestran los usuarios temporales que se crean al iniciar sesión con Smartcard o el certificado PKI.

Campo	Sentido	
Nombre de usuario	El nombre asignado al usuario. El nombre de usuario debe ser único en todo el sistema y se puede cambiar. Consulte la nota en la sección "Crear un nuevo usuario (Página 88)".	
dirección VPN	La dirección IP del dispositivo utilizado durante la comunicación a través de VPN. La dirección es asignada automáticamente por SINEMA RC. Si la comunicación a través de VPN no está activa, se muestra "ninguno".	
Primer nombre	Nombre del usuario	
Apellido	Apellido del usuario	
Cuenta creada Fecha y hora	en que se creó esta cuenta de usuario	
Último acceso	Fecha y hora del último inicio de sesión	
Estado	 Online  Offline Discapacitado	El usuario está registrado en SINEMA RC. El usuario no está registrado en SINEMA RC. El usuario está deshabilitado.
protocolo vpn	Muestra qué protocolo se está utilizando para la conexión VPN.	
Comportamiento	     Resumen de la configuración del usuario. La configuración del usuario también se muestra para los usuarios con el derecho "solo lectura". Cambiar la configuración del usuario. Esto incluye cambiar los datos de contacto, asignar nuevos roles y derechos y cambiar la contraseña. Edite el grupo de participantes al que está asignado el usuario seleccionado. El usuario puede ser asignado a uno o más grupos. Desactivar usuario. Si el usuario está en línea, la conexión VPN existente también se desactiva. Cuando el usuario intenta iniciar sesión, se muestra el mensaje "La cuenta está desactivada". Vuelva a activar el usuario. El usuario puede volver a iniciar sesión en el servidor SINEMA RC.	

Filtrado de entradas

- Seleccione una entrada en el menú emergente "Filtro de búsqueda".
- Introduzca un término de búsqueda o parte del término de búsqueda en el cuadro de búsqueda.
- Para limitar aún más la búsqueda, seleccione la casilla de verificación "Coincidencia precisa".

Cuando se selecciona, se tienen en cuenta mayúsculas y minúsculas y se busca la palabra de búsqueda completa.

Los resultados de la búsqueda coincidirán exactamente con el término de búsqueda ingresado.

- Haga clic en el botón "Aplicar filtro".

Resultado

Configuración con administración basada en web

4.7 Cuentas de usuario

La lista se actualiza en función de los ajustes realizados. Para volver a mostrar todas las entradas, haga clic en el botón "Mostrar todo".

4.7.2 Administrar roles y derechos

Requisito para crear roles

Al usuario se le ha asignado el derecho "Gestionar usuarios".

Entradas mostradas

Se muestra una lista de los roles creados.

Campo	Sentido	Llamando a la página web
Nombre de rol	Nombre del rol	-
Administrar espacios de direcciones	Editar parámetros de los espacios de direcciones	Conexiones remotas > Dirección espacios
Crear copias de seguridad	Crear, eliminar, exportar e importar una copia de seguridad	Sistema > Copia de seguridad y restauración
Restaurar sistema	Restaurar el sistema basado en el archivo de sistema guardado	Sistema > Copia de seguridad y Sistema Restaurar
fuerza como	Cuando finaliza el túnel VPN entre SINEMA RC Client y el servidor, se solicita al usuario que introduzca un comentario. Solo entonces se puede cerrar la sesión actual. El comentario se registra en el registro del SINEMA RC Server.	Cliente SINEMA RC
Administrar actualizaciones de firmware	Cargue el archivo de actualización con el nuevo firmware en el dispositivo e inicie el proceso de actualización.	Sistema > Dispositivos-Actualización
Administrar dispositivos	Crear nuevos dispositivos; editar y eliminar dispositivos ya creados; crear grupos de participantes y asignarles dispositivos; crear y descargar un archivo de configuración con la configuración de VPN para el dispositivo	Conexiones remotas > Dispositivos
Gestionar conexiones remotas	Definir relaciones de comunicación: Comunicación entre participantes dentro de un grupo de participantes y grupos de participantes entre sí	Conexiones remotas > Grupos de participantes Conexiones remotas > Relaciones de comunicación
Editar parámetros del sistema	Leer, crear y eliminar parámetros del sistema. Los parámetros del sistema incluyen: <ul style="list-style-type: none">• Visión de conjunto• Registro de eventos• Servidor web• Licencias• La red• Actualización del sistema• Fecha y hora del día• VPN• Número máximo y clave de codificación para la copia de seguridad copias	

Campo	Sentido	Llamando a la página web
Gestión de certificados	Crear nuevos certificados de CA y certificados de servidor; editar y eliminar certificados existentes	Seguridad > Certificados
Administrar usuarios y roles	Cree nuevos usuarios y roles, edite y elimine usuarios y roles existentes; asignar derechos y cambiar sus propios derechos asignados	Cuentas de usuario > Usuarios y roles
Descargar software de cliente	Descargar el software Cliente SINEMA RC	Cuentas de usuario > Software de cliente
Política de contraseñas	Pauta para la asignación de contraseñas	
Política de PKI	Directrices para el certificado PKI	
Política de UMC	Muestra si el acceso a la UMC está activado o no	

Creando un nuevo rol

1. Abra la pestaña "Funciones".
2. Haga clic en el botón "Crear".
3. Introduzca un nombre de función.
4. Asigne derechos al rol de acuerdo con la siguiente tabla. Haga clic en el botón "Siguiente".
5. Active las membresías de grupos relevantes. Haga clic en el botón "Siguiente".
6. Especifique la política de contraseñas:

Campo	Descripción
La contraseña caduca (en días)	Especifica que la contraseña caduca después de un período determinado. <ul style="list-style-type: none"> • Nunca (establecido como predeterminado) • 30 días • 90 días • 360 días 14 días antes de la expiración, el usuario recibe un correo electrónico. Requisito: <ul style="list-style-type: none"> • Se configura una dirección de correo electrónico para el usuario. • El cliente SMTP está configurado.
Reutilizando la misma contraseña •	0: la configuración está deshabilitada <ul style="list-style-type: none"> • 1 - 5: si, por ejemplo, ingresa 3, la contraseña actual solo se puede reutilizar después de 3 contraseñas diferentes. Por defecto, se establece 3.
El usuario debe cambiar la contraseña después del primer inicio de sesión	Especifica si un usuario necesita cambiar su contraseña después del primer inicio de sesión.

Configuración con administración basada en web

4.7 Cuentas de usuario

7. Especifique la configuración para el inicio de sesión con el certificado PKI.

Campo	Descripción
Regla de filtro de DN de PKI	<p>Criterios de filtro según los cuales se realiza una verificación en el inicio de sesión.</p> <p>Los atributos de los nombres (Distinguished Name según el estándar X.509) se utilizan como criterios de filtrado. Esto requiere que los atributos estén incluidos en el certificado PKI del usuario.</p> <p>Para obtener información más detallada, consulte la sección "Iniciar sesión con el Certificados de tarjeta inteligente/PKI".</p>
Eliminar usuarios temporales (en horas)	<ul style="list-style-type: none"> • 0: el ajuste está deshabilitado. El usuario temporal debe ser eliminado a mano. • 1 - 72 horas: Cuando vence el tiempo, se elimina el usuario temporal.

8. Si esta función debe activarse para los inicios de sesión de UMC, seleccione la casilla de verificación "Activado" y defina la siguiente configuración:

Campo	Descripción
grupo de usuarios de UMC	Introduzca el nombre del grupo de usuarios de UMC. El nombre ingresado debe coincidir con el nombre en el servidor UMC.
Eliminar usuarios temporales (en horas)	<ul style="list-style-type: none"> • 1 - 9999 horas: Cuando expira el tiempo, se elimina el usuario temporal.

9. Haga clic en el botón "Finalizar".

4.7.3 Crear un nuevo usuario

Crear un nuevo usuario

1. Abra la pestaña "Usuarios".
2. Haga clic en el botón "Crear".

3. Configurar los datos de contacto

- Introduzca la información necesaria en la pestaña "Datos de contacto". Una casilla obligatoria es la de "Usuario nombre".
- El resto de datos de contacto es opcional y puede ser introducido y modificado por los propios usuarios.

Nota

Nombres de usuario

El nombre de usuario debe cumplir las siguientes condiciones:

- Debe ser único
- debe comenzar con una letra.
- Se permiten los siguientes caracteres: az, AZ, 0-9 y • No se permite el siguiente nombre de usuario: admin

Nombres de usuario: administrador

Por defecto, después de la instalación, el usuario predefinido "admin" está disponible.

- admin: puede iniciar sesión una vez después de la instalación con este nombre de usuario y la contraseña "admin". Después de esto, se le pedirá que cree un nuevo usuario. El rol de "administrador" se asigna a este usuario automáticamente. Este administrador tiene derecho a acceder a todas las funciones y puede configurar el sistema. Esto incluye crear usuarios y asignarles roles y derechos. El usuario "admin" ya no está disponible.

Cambiar un nombre de usuario

Puede cambiar el nombre de usuario más adelante. Si cambia el nombre de usuario, debe cambiar la contraseña o el usuario debe iniciar sesión para generar un nuevo certificado y un nuevo archivo PKCS#12.

*Configuración con administración basada en web**4.7 Cuentas de usuario*

- Especifique cómo el usuario puede iniciar sesión en SINEMA RC Server:

Campo	Sentido
Método de inicio de sesión	<ul style="list-style-type: none"> • Clave <p>Iniciar sesión con nombre de usuario y contraseña</p> <ul style="list-style-type: none"> • PKI <p>Iniciar sesión solo con certificado PKI</p>
Regla de filtro de DN de PKI	<p>Solo se requiere al iniciar sesión con el certificado PKI.</p> <p>Criterios de filtro según los cuales se realiza una verificación en el inicio de sesión.</p> <p>Los atributos de los nombres (Distinguished Name según el estándar X.509) se utilizan como criterios de filtrado. Esto requiere que los atributos estén incluidos en el certificado de entidad final del usuario.</p> <p>Como marcador de posición utilice el carácter **.</p>

- Haga clic en el botón "Siguiente".

4. Asignar derechos y roles

- Cesión de derechos mediante asignación de roles:

Haga clic y seleccione el rol requerido en la lista desplegable. Haga clic en "Agregar".

El usuario recibe los derechos asignados al rol. Para asignar derechos adicionales al usuario, haga clic en la casilla de verificación frente al derecho respectivo.

Para cancelar la asignación de funciones, vuelva a hacer clic en la casilla de verificación de la función.

- Cesión de derechos sin asignación de roles:

Si no ha seleccionado un rol, habilite los derechos correspondientes haciendo clic en la casilla de verificación.

- Haga clic en el botón "Siguiente".

5. Crear membresías grupales

- Seleccione uno o más grupos de participantes a los que se asignará el dispositivo. Encontrará información sobre cómo crear grupos de participantes en el apartado "Crear grupos de participantes (Página 81)".

- Haga clic en el botón "Siguiente".

6. Configurar el modo de conexión VPN

Establezca los siguientes parámetros:

Campo	Sentido
Solicitar dirección IP virtual	Cuando está habilitado, se solicita una dirección IP virtual durante el establecimiento de la conexión.
Dirección IP fija	La dirección IP que siempre se asigna al usuario. Esto solo es posible cuando el parámetro "Activar espacio de direcciones IP fijas" está habilitado. <ul style="list-style-type: none"> • OpenVPN: Conexiones remotas > Espacios de direcciones > OpenVPN
Parámetros de conexión de OpenVPN	Solo es necesario cuando la dirección IP WAN del SINEMA RC Server se traduce con NAT. <ul style="list-style-type: none"> • Dirección IP de la conexión Introduzca la dirección IP a través de la cual se puede acceder al SINEMA RC Server. • Puerto de la conexión Introduzca el puerto en el que SINEMA RC Server recibe la conexión OpenVPN. • Protocolo IP Especifique si la conexión OpenVPN se ejecuta a través de TCP o UDP. • Acciones Para eliminar, haga clic en  para acciones

7. Especificación de la contraseña

Introduzca una contraseña y confírmela. La contraseña asignada puede ser cambiada posteriormente por el usuario correspondiente, consulte la sección "Cambiar la contraseña actual (Página 120)".

8. Haga clic en el botón "Finalizar".

Cambiar la configuración del usuario

Cambie la configuración de usuario correspondiente. Luego haga clic en el botón "Guardar".

Nota

Cambiar el método de inicio de sesión

Si cambia el método de inicio de sesión de contraseña a PKI, la contraseña configurada se elimina.

4.7.4**Acuerdo del Usuario**

En esta página puede ingresar un acuerdo de usuario.

Campo	Sentido
opción de visualización	<ul style="list-style-type: none"> • Nunca El acuerdo de usuario no se muestra. • Primer inicio de sesión Cuando el usuario inicia sesión por primera vez, se muestra el acuerdo de usuario. Después de aceptar el acuerdo de usuario, el usuario puede acceder al WBM del SINEMA RC Server. • Cada inicio de sesión Cada vez que el usuario inicia sesión, se muestra el acuerdo de usuario. Después de aceptar el acuerdo de usuario, el usuario puede acceder al WBM del SINEMA RC Server.
Mensaje	<p>En el editor, ingrese el texto para el acuerdo de usuario. En la barra de herramientas hay herramientas disponibles para dar formato al texto. Los símbolos proporcionan información breve en forma de información sobre herramientas.</p> <p>Después de hacer su entrada, haga clic en el botón "Guardar".</p>
Exportar	Exporta la versión seleccionada del acuerdo de usuario.

Nota**Acuerdo de usuario modificado**

Si cambia el acuerdo de usuario mientras los usuarios están registrados en SINEMA RC Client, este cambio no tendrá efecto inmediato para estos usuarios. Estos usuarios permanecen conectados después de realizar el cambio en el acuerdo de usuario.

El acuerdo de usuario modificado se muestra solo cuando estos usuarios inician sesión nuevamente. Despues de aceptar el acuerdo de usuario, estos usuarios pueden acceder al WBM del SINEMA RC Server.

4.7.5**software de cliente****4.7.5.1****software de cliente**

En esta página puede cargar el software de instalación del cliente SINEMA RC en el servidor SINEMA RC.

Requisito

- El usuario tiene acceso al directorio de almacenamiento.

Llamando a la página web

En la navegación, seleccione "Cuentas de usuario > Software de cliente".

Importación de software de cliente

Procedimiento

1. Haga clic en "Seleccionar archivo" en la pestaña "Software de cliente".
2. Navegue hasta el directorio de almacenamiento y seleccione el archivo que desea cargar (*.exe). Confirmar tu selección con el botón "Abrir".
3. Haga clic en el botón "Importar".

Resultado

El software SINEMA RC Client se carga en el servidor SINEMA RC. Se muestran el nombre del archivo y la huella digital con SHA256. Verifique los campos mostrados.

4.7.5.2 Configuración del cliente

En la pestaña "Configuración del cliente", puede cargar su propia imagen de logotipo en formato PNG, JPEG o BMP. Esta imagen se muestra en la interfaz del cliente en lugar del logotipo de SIEMENS. Para evitar distorsiones o recortes de imágenes, utilice imágenes con una relación de aspecto de 2 : 1 (alto x ancho), por ejemplo, 200 x 100 px o 600 x 300 px.

Requisito

- El usuario tiene acceso al directorio de almacenamiento.

Llamando a la página web

En la navegación, seleccione "Cuentas de usuario > Software de cliente" y la pestaña "Configuración de cliente".

Configuración del cliente

1. Haga clic en "Seleccionar archivo" en la pestaña "Configuración del cliente".
2. Navegue hasta el directorio de almacenamiento y seleccione el archivo de imagen que desea cargar. Confirmar tu selección con el botón "Abrir".
3. Haga clic en el botón "Importar".

Resultado

La imagen se carga en el servidor SINEMA RC. Se muestran el nombre del archivo y la vista en miniatura. El logotipo se aplica la próxima vez que se inicie el cliente. Puede volver a la imagen estándar con el botón "Restablecer logotipo predeterminado".

4.7.5.3 Licencias de cliente

En la pestaña "Licencias de cliente", recibe una descripción general de los inicios de sesión de los clientes. También puede administrar estas entradas.

Para conexiones de dos clientes SINEMA RC, necesita la licencia de cliente SINEMA RC (MLFB 6GK1721-1XG03-0AA0 o 6GK1721-1XG03-0AK0 para OSD).

Llamando a la página web

En la navegación, seleccione "Cuentas de usuario > Software de cliente" y la pestaña "Licencias de cliente".

Gestión de licencias de clientes

En la pestaña "Licencias de cliente" se muestra una descripción general de los inicios de sesión de los clientes:

Campo	Sentido
ID del sistema del cliente	Muestra el ID del sistema cliente en el servidor.
Nombre del dispositivo cliente	Muestra el nombre de la PC desde la cual el cliente inició sesión en el servidor.
Último acceso	Muestra la marca de tiempo del inicio de sesión del cliente con la fecha y la hora.
Último usuario conectado	Muestra el nombre del usuario que estableció por última vez la conexión del cliente al servidor.

Para eliminar una entrada de la tabla, seleccione la casilla de verificación frente a la entrada que desea eliminar y haga clic en el botón "Eliminar".

4.8 Servicios

4.8.1 FUEGO

En esta página, configura el servidor API SINEMA RC, que responde a las solicitudes API del cliente API.

Requisito

Para poder utilizar esta función, necesita la licencia SINEMA RC API (MLFB 6GK1724-3VH03-0BV0).

Puede probar la función de forma gratuita durante un período de 14 días. Para ello, debe activar la licencia de prueba. Encontrará más información en el apartado "Vista general (Página 62)" y en el manual Getting Started "SINEMA Remote Connect API server".

Llamando a la página web

En la navegación, seleccione "Servicios > API".

Configuración del servidor API

Seleccione la casilla de verificación "Servidor API" y realice la siguiente configuración:

Campo	Sentido
Tiempo de vencimiento del token API en días	Ingrese el tiempo de vencimiento del token de autenticación.

Haga clic en "Guardar" para guardar la configuración.

Resultado

El servidor API está configurado. A través de la API, puede acceder al WBM del servidor SINEMA RC para configurarlo.

Puede encontrar más información sobre la configuración del WBM del servidor SINEMA RC con API en el Getting Started "SINEMA RC API server".

4.8.2

Configuración de UMC

En esta página, configura la conexión al servidor UMC.

Requisito

Para poder utilizar esta función, necesita la licencia SINEMA RC UMC (n.º de pedido 6GK1724-2VH03-0BV0).

Puede probar la función de forma gratuita durante un período de 14 días. Para ello, debe activar la licencia de prueba. Encontrará más información en el apartado "Iniciar sesión con UMC (Página 39)".

Llamando a la página web

En la navegación, seleccione "Servicios > Configuración de UMC".

Configuración de la conexión al servidor UMC

Seleccione la casilla de verificación "Servidor UMC" y realice los siguientes ajustes:

Campo	Sentido
Dirección IP del servidor UMC	Ingrese la dirección IP del servidor UMC.
Puerto del servidor UMC	Ingrese el número de puerto del servidor UMC.

Haga clic en "Guardar" para guardar la configuración.

Resultado

La conexión con el servidor de UMC se establece cuando un usuario de UMC inicia sesión.

4.8.3**Carga del servidor**

Esta página le brinda la opción de cargar archivos de configuración o mensajes de archivos de registro a un servidor SFTP. SFTP significa Protocolo seguro de transferencia de archivos, pero a menudo se confunde con el Protocolo simple de transferencia de archivos. El servidor SFTP utiliza un protocolo separado que permite la transferencia de archivos a través de una conexión SSH segura.

Llamando a la página web

En la navegación, seleccione "Servicios > Cargar servidor".

Entradas mostradas

Realice la siguiente configuración en la pestaña "Cargar configuración del servidor". Luego haga clic en el botón "Guardar".

Campo	Sentido
Carga automática de archivos	Cuando está activado, los archivos recién generados se cargan en el SFTP servidor.
Archivos para subir	Especifique qué tipos de archivos se van a cargar: <ul style="list-style-type: none"> • Configuración • Archivos de registro • Archivos de configuración y registro
Nombre del servidor SFTP	Dirección IP o FQDN del servidor SFTP Si utiliza un puerto que no sea el puerto estándar 22, introduzca el número de puerto junto con la dirección IP. Se ingresan dos puntos ":" como separador entre la dirección IP y el número de puerto, por ejemplo: 192.168.234.1:622.
Servidor SFTP de huellas dactilares	Visualización de la huella digital actual (última conexión de trabajo) Si la huella dactilar cambia, por ejemplo, después de renovar la huella dactilar, la función se desactiva y se introduce un mensaje de advertencia a tal efecto en el registro. Para poder volver a cargar archivos en el servidor SFTP, debe habilitar la carga automática de archivos y verificar si la nueva huella digital coincide con la del servidor SFTP.
Subir directorio	Al usuario se le asigna un directorio de almacenamiento, el llamado directorio de inicio. Si no ingresa nada, el archivo se carga directamente en el directorio de inicio. Para cargar el archivo en un subdirectorío, especifique el subdirectorío. <u>Siempre que el subdirectorío se cree en el directorio de inicio.</u>
Nombre de usuario	Nombre de usuario para acceder al servidor SFTP
Clave	Contraseña de acceso al servidor SFTP
Subir archivos antiguos	Botón para cargar todos los archivos actualmente presentes en el servidor SFTP

Después de guardar la configuración, los archivos recién generados se transfieren automáticamente al servidor SFTP.

Para cargar los archivos actuales al servidor SFTP, haga clic en el botón "Cargar archivos antiguos".

4.8.4

cliente de registro del sistema

En esta página, configura el cliente Syslog en el servidor SINEMA RC para establecer la conexión con el servidor Syslog y comprobar su estado de conexión.

Llamando a la página web

En la navegación, seleccione "Servicios > Cliente Syslog".

Establecimiento de una conexión con el servidor Syslog

Realice los siguientes ajustes y luego haga clic en "Guardar y comprobar la conexión":

Campo	Sentido
ID de cliente (nombre de host)	Introduzca la dirección IP del servidor SINEMA RC. Con esta dirección IP, SINEMA RC se identifica como cliente Syslog en el Syslog servidor.
Dirección IP del servidor Syslog	Introduzca la dirección IP del servidor Syslog.
Puerto del servidor Syslog	Introduzca el número de puerto del servidor Syslog.
Protocolo	Seleccione el protocolo IP deseado (TCP (TLS) o UDP) de la lista.
El servidor Syslog solicita la autenticación del cliente	Cuando está habilitado, el servidor Syslog requiere la autenticación del cliente. Se debe especificar un certificado de conexión en el campo a continuación para este propósito. Esta configuración se utiliza para la autenticación mutua entre el cliente Syslog y el servidor Syslog (autenticación de servidor y cliente) y solo es relevante para el protocolo TCP (TLS) seleccionado. Esta casilla de verificación no se puede activar para el protocolo UDP seleccionado.
Certificado de conexión Selección	Seleccione el certificado del servidor Syslog con el que se establece la conexión. Puede importar certificados a través de la página web "Seguridad > Gestión de certificados Syslog"; ver apartado "Gestión de certificados Syslog (Página 114)".

Nota

No hay certificado adecuado para la conexión

Si no se encuentra ningún certificado adecuado en la gestión de certificados Syslog, se muestra el certificado del servidor Syslog.

En este caso, tiene la opción de agregar esto a SINEMA RC con "Aceptar" y autorizar la conexión Syslog con "Guardar y verificar conexión".

Con "Rechazar", niega el uso del certificado respectivo.

Resultado

Se establece la conexión con el servidor Syslog recién creado. Los parámetros de conexión y el estado se muestran en una tabla.

Entradas mostradas

Se muestran las siguientes entradas:

Campo	Sentido										
dirección IP de la conexión	Muestra la dirección IP del servidor Syslog.										
Puerto de conexión	Muestra el número del puerto de conexión.										
protocolo IP	Muestra el protocolo IP utilizado.										
Estado	<p>Muestra el estado de la conexión con el servidor Syslog. Son posibles los siguientes estados:</p> <ul style="list-style-type: none"> • Conexiones sobre UDP: <ul style="list-style-type: none"> - "—" No es posible la supervisión de la conexión a través de UDP. • Conexiones sobre TCP (TLS): <ul style="list-style-type: none"> - En línea Establecer una conexión con el servidor Syslog. - Desconectado Se interrumpe una conexión establecida con el servidor Syslog, por ejemplo, si el servidor Syslog ya no está disponible. - Rechazado Si ocurre durante una verificación de conexión, por ejemplo, usando el  botón, certificado que no es válido o ha caducado o que el servidor Syslog no responde. - Discapacitado La conexión con el servidor Syslog está deshabilitada. - Certificado eliminado Se elimina un certificado de Syslog basado en el cual se establece la conexión. 										
Comportamiento	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="text-align: center; padding: 5px;"></td><td style="padding: 5px;">Comprobar conexión con el servidor Syslog (sólo con conexiones sobre TCP (TLS)).</td></tr> <tr> <td style="text-align: center; padding: 5px;"></td><td style="padding: 5px;">Descargar certificado de cliente Syslog desde SINEMA RC.</td></tr> <tr> <td style="text-align: center; padding: 5px;"></td><td style="padding: 5px;">Haga clic en este botón para desactivar el servidor Syslog.</td></tr> <tr> <td style="text-align: center; padding: 5px;"></td><td style="padding: 5px;">El servidor Syslog está deshabilitado y no se le envía ningún mensaje. Haga clic en este botón para habilitar el servidor Syslog.</td></tr> <tr> <td style="text-align: center; padding: 5px;"></td><td style="padding: 5px;">Quite el servidor Syslog de la lista. La configuración del servidor Syslog se elimina inmediatamente.</td></tr> </table>		Comprobar conexión con el servidor Syslog (sólo con conexiones sobre TCP (TLS)).		Descargar certificado de cliente Syslog desde SINEMA RC.		Haga clic en este botón para desactivar el servidor Syslog.		El servidor Syslog está deshabilitado y no se le envía ningún mensaje. Haga clic en este botón para habilitar el servidor Syslog.		Quite el servidor Syslog de la lista. La configuración del servidor Syslog se elimina inmediatamente.
	Comprobar conexión con el servidor Syslog (sólo con conexiones sobre TCP (TLS)).										
	Descargar certificado de cliente Syslog desde SINEMA RC.										
	Haga clic en este botón para desactivar el servidor Syslog.										
	El servidor Syslog está deshabilitado y no se le envía ningún mensaje. Haga clic en este botón para habilitar el servidor Syslog.										
	Quite el servidor Syslog de la lista. La configuración del servidor Syslog se elimina inmediatamente.										

4.8.5

Inicio de sesión de depuración

Puede otorgar a su contacto de Siemens acceso al servidor SINEMA RC durante un cierto período de tiempo a través del inicio de sesión de depuración.

El contacto en Siemens solo puede acceder a los datos si proporciona información sobre el puerto y la contraseña y habilita la función.

Llamando a la página web

En la navegación, seleccione "Servicios > Inicio de sesión de depuración".

Configuración del inicio de sesión de depuración

1. Seleccione la casilla de verificación "Habilitar inicio de sesión de depuración" y realice los siguientes ajustes:

Campo	Sentido
Tiempo de espera de inicio de sesión de depuración (minutos)	Especifique la duración del acceso. Cuando transcurre este tiempo, el usuario se desconecta automáticamente.
Puerto de inicio de sesión de depuración	Especifique el puerto TCP a través del cual se accede al sistema de SINEMA RC Server. Es posible que deba configurar el reenvío de PUERTOS a SINEMA RC en el enrutador de Internet.
Contraseña de inicio de sesión de depuración	Introduce la contraseña. La nueva contraseña debe tener al menos 8 caracteres y contener caracteres especiales, mayúsculas y minúsculas, así como números, consulte la sección "Caracteres permitidos (Página 27)".
Confirmar contraseña de inicio de sesión de depuración	Confirme esta contraseña.

2. Haga clic en "Guardar" para guardar la configuración.

Cuando se guardan los ajustes, el tiempo restante se muestra en el cuadro "Tiempo restante (minutos)".

Desactivar inicio de sesión de depuración

1. Deshabilite "Habilitar inicio de sesión de depuración".

2. Haga clic en el botón "Guardar".

La configuración vuelve a los valores predeterminados y la contraseña se elimina.

Configuración con administración basada en web

4.9 Seguridad

4.9 Seguridad**4.9.1 Gestión de certificados****4.9.1.1 Descripción general de la gestión de certificados****Tipos de certificados**

SINEMA RC utiliza diferentes certificados para autenticar los distintos nodos al establecer una conexión VPN. Éstos incluyen:

Certificado	Se utiliza para ...	Expediente escribe	Descripción en la sección...
Certificados CA	<p>El certificado CA es un certificado emitido por la "Autoridad de certificación" del que se derivan los certificados.</p> <p>Para que se derive un certificado, a cada certificado de CA le pertenece una clave privada. Los certificados derivados se firman con la clave privada.</p> <p>La firma del certificado derivado se comprueba con la clave pública del certificado CA.</p> <p>Cuando se instala SINEMA RC Server, se genera un certificado CA.</p> <p>Cuando sea necesario, el certificado de CA se puede renovar.</p> <p>Los certificados de servidor, dispositivo y usuario se derivan del certificado CA actualmente válido.</p> <p>El intercambio de claves entre el dispositivo y la puerta de enlace VPN del socio se realiza automáticamente al establecer la conexión OpenVPN. No es necesario el intercambio manual de archivos clave.</p>	*.crt	Certificados CA (Página 101)
Certificado de servidor	Se requieren certificados de servidor para establecer una comunicación segura (p. ej., HTTPS, VPN...) entre el dispositivo y otro participante de la red. El certificado del servidor es un certificado SSL encriptado.	*.p12	Certificado de servidor (Página 102)
Certificado de dispositivo	Los certificados de dispositivo y las claves correspondientes solo se crean cuando el usuario tiene los derechos adecuados.	*.p12	Descripción general de la administración de dispositivos (Página 72)
Certificado de usuario	SINEMA RC Server crea un certificado personal para cada usuario creado. Obtiene una descripción general del certificado de usuario en la página "Mi cuenta > Certificado de usuario".	*.p12 .pem	Certificado de usuario (Página 119)
Certificación PKI CA	Para el inicio de sesión con el certificado PKI.	* Certificado CA	.pem PKI (Página 111)
Syslog del servidor CA certificado	Para la autenticación en el servidor Syslog.	*.crt	Certificados Syslog CA (Página 114)

Tipos de archivo

Tipo de archivo	Descripción
*.crt	Archivo que contiene el certificado.
*.p12 *.pfx	Los formatos *.p12 y *.pfx se utilizan para guardar el certificado junto con la clave privada. La clave privada con el certificado correspondiente se almacena protegida con contraseña. La CA crea un archivo de certificado (PKCS12) para ambos extremos de una conexión VPN con la extensión de archivo ".p12". Este archivo de certificado contiene la clave pública y privada de la estación local, el certificado firmado de la CA y la clave pública de la CA.
*.pem	Certificado y/o clave como texto ASCII codificado en Base64.
*.clave	Clave privada codificada en Base64 desprotegida

Funciones adicionales

Además, junto con los certificados también están disponibles las siguientes funciones:

- Exportación de certificados usados
- Importación de certificados
- Renovación de certificados vencidos
- Sustitución de las autoridades de certificación existentes

Nota**Fecha actual y hora actual del día en los dispositivos**

Cuando utilice una comunicación segura (por ejemplo, HTTPS, VPN...), asegúrese de que los dispositivos involucrados tengan la hora y la fecha actuales. De lo contrario, los certificados utilizados no se evaluarán como válidos y la comunicación segura no funcionará.

4.9.1.2 Certificados CA**Llamando a la página web**

En la navegación, seleccione "Seguridad > Certificados".

Entradas mostradas

En la pestaña "Certificados CA", puede ver una descripción general de los certificados CA:

Campo	Sentido
Certificados CA nombre	El nombre de la CA es generado automáticamente por el sistema.
Tiempo de expiración	Muestra cuánto tiempo es válido el certificado de CA. Puede especificar la fecha de validez en la pestaña "Configuración". Allí, también puede establecer cuántos días antes de que caduque el certificado de CA, se renovará automáticamente.

*Configuración con administración basada en web***4.9 Seguridad**

Campo	Sentido
Estado	Activo: el certificado de CA es válido. Fuera de servicio: se generó un certificado de CA más nuevo o el certificado de CA caducó.
Comportamiento	 Llamar información de CA Obtiene información sobre la CA seleccionada. Esto también se muestra para los usuarios con el derecho "solo lectura".
	 Exportación de un certificado de CA Al hacer clic en el ícono, se exporta el certificado CA (*.crt). El archivo, por ejemplo, se exporta al dispositivo final o al servidor de destino.

Renovación de un certificado de CA

Con el botón "Nuevo certificado de CA", puede, cuando sea necesario, por ejemplo, con certificados comprometidos, generar un nuevo certificado.

Eliminación de un certificado de CA

Los certificados de CA con el estado "Fuera de servicio" se pueden eliminar. Para ello, seleccione el certificado correspondiente en la vista general y haga clic en el botón "Eliminar".

4.9.1.3 Certificado de servidor**Llamando a la página web**

En la navegación, seleccione "Seguridad > Certificados".

Entradas mostradas

En las pestañas "Certificado de servidor web" y "Certificado de servidor VPN", puede ver una descripción general de los certificados:

Campo	Sentido
Número de serie	Número para identificar el certificado. El número de serie se incrementa automáticamente en uno cuando se crea el certificado.
Nombre común	El nombre se toma de la configuración de la red: <ul style="list-style-type: none">• El nombre DNS si ha activado la opción "Nombre de host que se puede resolver externamente" y ha introducido un valor (consulte el apartado "DNS (Página 53)").• La dirección IP de la interfaz WAN o LAN, consulte el capítulo "Interfaces (Página 51)".
Editor	Visualización de la autoridad certificadora que emitió el certificado.
Válida desde	Fecha a partir de la cual el certificado es válido.
Válido hasta	Fecha en que caduca el certificado.
Longitud de clave (bits)	Longitud de clave que se estableció en "Configuración" cuando se generó este certificado.
Método de firma	Método de firma con la clave de firma correspondiente ("valor hash") que se configuró en "Configuración" cuando se generó este certificado.
Huella dactilar SHA1	Huella digital con SHA1 como algoritmo hash

Campo	Sentido
Huella dactilar SHA256	Huella digital con SHA256 (SH2) como algoritmo hash
Nombres alternativos	<ul style="list-style-type: none"> • IP: la dirección IP de la interfaz WAN, consulte el apartado "Interfaces (Página 51)". • IP: la dirección IP WAN si ha activado la función "SINEMA Remote Connect se encuentra detrás de un dispositivo NAT" y ha introducido una dirección IP, consulte el capítulo "Interfaces (Página 51)". • DNS: el nombre DNS cuando ha activado la opción "Nombre de host que se puede resolver externamente" y ha introducido un valor (consulte la sección "DNS (Página 53)").

Renovación del certificado del servidor web y el certificado del servidor VPN

Con el botón "Renovar", puede cuando sea necesario, por ejemplo, con certificados comprometidos, generar un nuevo certificado. Los certificados se derivan del certificado CA actualmente válido. El número de serie se incrementa automáticamente en uno.

Importación del certificado del servidor web

Con el botón "Importar", puede importar certificados CA para el cifrado del tráfico de datos.

4.9.1.4 Importación del certificado del servidor web

Si no desea utilizar el certificado de servidor web emitido por SINEMA RC, aquí puede importar un certificado de servidor web de una autoridad de certificación externa. El certificado del servidor web puede, por ejemplo, ser emitido por una autoridad de certificación interna de la empresa o por una autoridad de certificación pública.

Nota

Cifrado compatible

SINEMA RC admite certificados de servidor web cifrados según RSA (Rivest, Shamir und Adleman).

4.9 Seguridad

Para importar el certificado del servidor web, necesita los siguientes archivos:

- Archivo de certificado

Ejemplos del contenido de un archivo de certificado (.crt, .pem)

-----INICIAR CERTIFICADO----- -----FIN DEL CERTIFICADO-----

-----COMENZAR EL CERTIFICADO X509----- -----FIN DEL CERTIFICADO X509-----

- Archivo de clave

El archivo de clave RSA que pertenece al archivo de certificado.

Ejemplos del contenido de un archivo de certificado de un archivo de clave (.pem, .key)

Encriptado:

-----COMENZAR CLAVE PRIVADA ENCRYPTADA----- ... -----FIN DE LA CLAVE PRIVADA ENCRYPTADA-----

Sin cifrar:

-----COMENZAR CLAVE PRIVADA----- ... -----FIN CLAVE PRIVADA RSA-----

-----COMENZAR LA CLAVE PRIVADA DE RSA----- ... -----FIN CLAVE PRIVADA RSA-----

- archivo de cadena CA

Este archivo contiene los certificados de todas las autoridades de certificación involucradas. En base a la cadena de certificados, se comprueba la validez del certificado del servidor web.

Ejemplos del contenido de un archivo de cadena de CA (.crt, .pem):

Varios bloques de certificados uno tras otro:

-----INICIAR CERTIFICADO----- -----FIN DEL CERTIFICADO-----

-----INICIAR CERTIFICADO----- -----FIN DEL CERTIFICADO-----

-----INICIAR CERTIFICADO----- -----FIN DEL CERTIFICADO-----

Procedimiento

1. Para importar el certificado, haga clic en el botón "Seleccionar archivo" en "Seleccionar el archivo del certificado".
2. Seleccione el archivo de certificado y confirme su selección con el botón "Abrir".
3. Haga clic en el botón "Seleccionar archivo" en "Seleccionar el archivo de clave".
4. Seleccione el archivo clave correspondiente y confirme su selección con el botón "Abrir".
5. Para importar el certificado de una autoridad de certificación de rango superior, haga clic en "Seleccionar archivo" botón en "Seleccionar el archivo de la cadena CA".
6. Seleccione el archivo del certificado CA y confirme su selección con el botón "Abrir".
7. Para archivos protegidos con contraseña, ingrese la contraseña especificada para el archivo y repita la entrada.

8. Haga clic en el botón "Siguiente".

Los detalles del certificado firmado se muestran en la pestaña "Activar certificado". Puede, por ejemplo, comprobar si el certificado sigue siendo válido.

Campo	Sentido
Número de serie	Número para identificar el certificado. El número de serie se incrementa automáticamente en uno cuando se crea el certificado.
Nombre común	Nombre del solicitante
Editor	Visualización de la autoridad certificadora que emitió el certificado.
Válida desde	Fecha a partir de la cual el certificado es válido.
Válido hasta	Fecha en que caduca el certificado.
Longitud de clave	Especifica la longitud de la clave que se utiliza.
Método de firma	Especifica qué método de firma digital con la clave de firma correspondiente ("valor hash") se utilizó para el certificado.

9. Para finalmente importar los archivos, haga clic en el botón "Importar".

4.9.1.5 Certificado de dispositivo

Llamando a la página web

En la navegación, seleccione "Seguridad > Certificados" y la pestaña "Certificado de dispositivo".

Entradas mostradas

En la pestaña "Certificado de dispositivo", puede ver una descripción general de los certificados importados:

Campo	Sentido
Escribe	Tipo del archivo cargado. Encontrará más información en el apartado "Resumen de la gestión de certificados (Página 100)".
Nombre común	Nombre del solicitante
Estado	Visualización de si el certificado es válido o ya ha caducado.
Tema	Visualización del titular obtenido a partir del nombre común (CN).
Editor	Visualización de la autoridad certificadora que emitió el certificado.
Válida desde	Fecha a partir de la cual el certificado es válido.
Válido hasta	Fecha en que caduca el certificado.
Utilizar	La función que utiliza el certificado.

Importación de certificados de dispositivo

1. Para importar certificados de dispositivos, haga clic en el botón "Importar".
2. Seleccione el archivo PKCS12 (*.p12) y confirme su selección con el botón "Abrir".
3. Los archivos están protegidos con contraseña. Para cargar los archivos en el dispositivo, ingrese la contraseña y repetir la entrada.

*Configuración con administración basada en web***4.9 Seguridad**

4. Haga clic en el botón "Siguiente".

Los detalles del certificado CA se muestran en la pestaña "Activar certificado". Puede, por ejemplo, comprobar si el certificado sigue siendo válido.

Campo	Sentido
Número de serie	Número para identificar el certificado. El número de serie se incrementa automáticamente en uno cuando se crea el certificado.
Nombre común	Nombre del solicitante
Emitido por	Visualización de la autoridad certificadora que emitió el certificado.
Válida desde	Fecha a partir de la cual el certificado es válido.
Válido hasta	Fecha en que caduca el certificado.
Longitud de clave	Especifica la longitud de la clave que se utiliza.
Método de firma	Especifica qué método de firma digital con la clave de firma correspondiente ("valor hash") se utilizó para el certificado.

5. Para cargar los archivos en SINEMA RC Server, haga clic en el botón "Importar".

Resultado:

El archivo PKCS12 se importa al servidor SINEMA RC. Este archivo de certificado contiene el certificado del participante y el certificado firmado de la autoridad de certificación.

4.9.1.6 Configuración de los certificados**Llamando a la página web**

En la navegación, seleccione "Seguridad > Certificados".

Cambiar la configuración

Los cambios realizados en la pestaña "Configuración" solo se utilizan al renovar el certificado del servidor: Los cambios no se aplican a los certificados existentes. En las pestañas "Certificado de servidor web" y "Certificado de servidor VPN" puede utilizar el botón "Renovar" para generar un nuevo certificado de servidor.

Campo	Sentido
Longitud de clave preferida (bits)	Seleccione el número de bits de las distintas claves posibles para el procedimiento.
Método hash preferido	Seleccione el método hash para el certificado: SHA256 o SHA512
Renovación del certificado de CA (días antes del vencimiento)	Especifique cuántos días antes de que caduque se renovará automáticamente el certificado. Por defecto, el certificado CA del servidor tiene una validez de 10 años. Si, por ejemplo, especifica 365 días, se generará un nuevo certificado de CA después de 9 años. El certificado de CA anterior está "Fuera de servicio" pero es válido por otros 365 días. Los clientes que utilizan este certificado de CA pueden continuar iniciando sesión con él durante otros 365 días. Después de este tiempo, el certificado de CA cuenta como "Caducado" y los clientes deben usar el nuevo certificado de CA.
Validez de los certificados de cliente (días)	Especifique por cuántos días será válido el certificado. Ya no se puede utilizar un certificado cuya CA ya haya caducado.

4.9.2 conexiones VPN

4.9.2.1 Configuración básica de VPN

Configuración básica de VPN

OpenVPN es un programa para establecer una conexión TLS cifrada. OpenSSL se utiliza para el cifrado.

Archivo OpenVPN

Cuando se crea un dispositivo o usuario, automáticamente se genera un archivo de configuración con la extensión *.ovpn. El archivo contiene varios parámetros necesarios para una conexión con el servidor.

Estos incluyen, por ejemplo, los certificados; consulte la sección "Descripción general de la gestión de certificados (Página 100)".

El archivo debe cargarse en el participante de la red remota con la que SINEMA RC Server establece una conexión VPN.

El cliente SINEMA RC siempre obtiene estos datos automáticamente. El S615 obtiene los datos automáticamente o se debe cargar el archivo. Esto depende de la configuración.

Descargar un archivo OpenVPN

Para dispositivos, el archivo se llama en la lista de dispositivos; consulte el apartado "Vista general de la gestión de dispositivos (Página 72)".

Para los usuarios, el archivo se llama en la cuenta de usuario personal (consulte la sección "Certificado de usuario (Página 119)").

4.9.2.2 Configuración de OpenVPN

Requisito para cambiar la configuración de OpenVPN

Al usuario se le ha asignado el derecho "Editar parámetros del sistema".

Llamando a la página web

En la navegación, seleccione "Seguridad > OpenVPN".

Configuración de OpenVPN

Configure los siguientes ajustes que son válidos para todas las conexiones OpenVPN después de haber guardado:

Campo	Sentido
Activar	Cuando está habilitado, se utiliza OpenVPN.
Estado	Muestra si OpenVPN está activado o desactivado.

*Configuración con administración basada en web***4.9 Seguridad**

Campo	Sentido
puerto TCP	Especifique el puerto en el que SINEMA RC Server acepta conexiones TCP. Suponiendo que las tramas TCP se puedan enviar a este puerto. En un enrutador DSL preconectado, por ejemplo, se debe ingresar la asignación de puertos.
el puerto UDP	Especifique el puerto en el que SINEMA RC Server acepta conexiones UDP. Suponiendo que las tramas UDP se puedan enviar a este puerto. En un enrutador DSL preconectado, por ejemplo, se debe ingresar la asignación de puertos.
Mantener vivo el intervalo (s)	Ingrese el intervalo en segundos en el que los socios de conexión envían paquetes de mantenimiento activo. Esta configuración se transfiere automáticamente al cliente cuando se establece la conexión. Los paquetes de mantenimiento de vida se envían solo cuando no hubo comunicación durante el último intervalo. Si no hay respuesta al paquete, el interlocutor de la comunicación supone una interrupción en la conexión o que el interlocutor de la comunicación no funciona. Las medidas se toman de acuerdo con el ajuste "Tiempo de espera de conexión".
Tiempo de espera de conexión (s)	Especifique el tiempo máximo en segundos que el socio de comunicación espera una respuesta del servidor antes de que se considere que la conexión se ha interrumpido. Esta configuración se transfiere automáticamente al cliente cuando se establece la conexión. La detección de una interrupción de la conexión se logra con paquetes de mantenimiento de vida (consulte la configuración "Intervalo de mantenimiento de vida"). Si el cliente detecta una interrupción de la conexión, reacciona restableciendo la conexión cuando haya transcurrido el tiempo de espera de la conexión. En el servidor, el tiempo de espera de conexión establecido se duplica. Una vez transcurrido el tiempo de espera de la conexión duplicada, el servidor considera que la conexión con el cliente se ha interrumpido.
Longitud de clave DH	Seleccione el protocolo de intercambio de claves Diffie-Hellman que se utilizará entre los socios de comunicación.
Cifrar	Selección del algoritmo para el cifrado de los datos transferidos. Están disponibles los siguientes: <ul style="list-style-type: none">• AES-128, 192, 256: Estándar de cifrado avanzado (longitud de clave de 128, 192 o 256 bits, modo CBC)• DES-EDE, DES-EDE3: Estándar de cifrado de datos (longitud de clave de 128 o 192 bits, modo CBC)
método hash	Selección del algoritmo de autenticación: SHA-1, 256, 512: algoritmo hash seguro 1, 256 o 512
mín. versión TLS	Especifique la versión de TLS.
Interfaz	La interfaz que forma el punto final de VPN local. A través de esta interfaz se establece la conexión OpenVPN con el socio OpenVPN (SINEMA RC Client, dispositivo). • WAN: Conexión solo a través de la interfaz WAN <ul style="list-style-type: none">• LAN 1-n: Conexión a través de las interfaces LAN disponibles:• WAN + LAN 1-n: Conexión a través de todas las interfaces

4.9.2.3 Configuración de IPsec**Requisito para cambiar la configuración de IPsec VPN**

Al usuario se le ha asignado el derecho "Editar parámetros del sistema".

Llamando a la página web

En la navegación, seleccione "Seguridad > IPsec".

Configuración de los ajustes básicos de IPsec

En la pestaña "IPsec", configure los siguientes ajustes que son válidos para todos los perfiles VPN IPsec después de haberlos guardado:

Campo	Sentido
Activar	Cuando está activado, se utiliza IPsec.
Estado	Muestra si IPsec está activado o desactivado.
Intervalo después de la(s) consulta(s) DPD	Periodo tras el cual se envían las consultas DPD. Estas consultas prueban si la estación remota aún es accesible o no.
Tiempo de espera después de la(s) consulta(s) DPD	Si no hay respuesta a la consulta DPD, la conexión VPN a la estación remota se declara inválida una vez transcurrido este intervalo de tiempo.
Interfaz	<p>La interfaz es el punto final local de la conexión VPN. A través de esta interfaz se establece la conexión VPN con el socio VPN (cliente SINEMA RC, dispositivo).</p> <ul style="list-style-type: none"> • WAN: Conexión solo a través de la interfaz WAN • LAN 1-n: Conexión a través de las interfaces LAN disponibles • WAN + LAN 1-n: Conexión a través de todas las interfaces

perfiles IPsec

A los dispositivos y usuarios se les asignan perfiles IPsec. Los perfiles contienen los ajustes de la fase 1 y la fase 2.

En la pestaña "Perfiles IPsec" se muestra una lista de los perfiles IPsec que ya se han creado junto con su estado:

Campo	Sentido
Nombre de perfil	El nombre asignado al perfil IPsec. El nombre debe ser único en todo el sistema y no se puede cambiar, consulte la sección "Creación de perfiles IPsec (Página 110)"
Intercambio de llaves	Método de intercambio de claves
como	Configuración de la Fase 1 - IKE (KE/Intercambio de claves)
ESP	Configuración de la Fase 2 - ESP (autenticación)
Comportamiento	 Descripción general del perfil IPsec. Esto también se muestra para los usuarios con el derecho "solo lectura".  Cambiar un perfil IPsec. Esto también incluye cambiar la configuración de la Fase 1 y la Fase 2.

Con el botón "Crear", puede crear nuevos perfiles IPsec, consulte "Creación de perfiles IPsec (Página 110)".

Con el botón "Copiar" creas una copia del perfil seleccionado en el que adaptas parámetros y que puedes guardar como nuevo perfil IPsec. Los perfiles IPsec creados se eliminan con "Eliminar".

4.9.2.4 Creación de perfiles IPsec

Requisito para cambiar la configuración de IPsec VPN

Al usuario se le ha asignado el derecho "Editar parámetros del sistema".

Creación de un nuevo perfil IPsec

1. Abra la pestaña "Perfil IPsec"
2. Haga clic en el botón "Crear".
3. Ingrese un nombre para el perfil IPsec.
4. En Método de intercambio de claves, especifique si se utilizará IKEv2 o IKEv1.
5. Realice los ajustes de la Fase 1 - IKE (SA/Intercambio de claves):

Campo	Sentido
Algoritmo de cifrado:	La selección depende de la fase y el método de intercambio de claves. (IKE)
Algoritmo hash	Selección del algoritmo de autenticación: SHA 1, 256, 384, 512
Derivación de claves	Seleccione el grupo Diffie-Hellmann (DH) requerido a partir del cual se generará una clave.
Toda la vida	El tiempo de vida de la autenticación. Cuando haya transcurrido el tiempo, los puntos finales de VPN involucrados deben autenticarse entre sí nuevamente y generar una nueva clave.

6. Realice los ajustes de la Fase 2 - ESP (autenticación):

Campo	Sentido
Protocolo	Selección del protocolo AH: El encabezado de autenticación IP (AH) maneja la autenticación e identificación de la fuente. ESP: la carga útil de seguridad de encapsulación (ESP) cifra los datos.
Algoritmo de cifrado:	La selección depende de la fase y el método de intercambio de claves (IKE)
Algoritmo hash	Selección del algoritmo de autenticación: SHA 1, 256, 384, 512
Derivación de claves	Seleccione el grupo Diffie-Hellmann (DH) requerido a partir del cual se generará una clave.
Toda la vida	El tiempo de vida de la autenticación. Cuando haya transcurrido el tiempo, los puntos finales de VPN involucrados deben autenticarse entre sí nuevamente y generar una nueva clave.

7. Haga clic en "Crear".

Cambiar un perfil IPsec

Cambie la configuración de usuario correspondiente. Luego haga clic en el botón "Guardar".

Algoritmo de cifrado

	Fase 1		Fase 2	
	IKEv1	IKEv2	IKEv1	IKEv2
3DES	X	X	X	X
AES128 CBC	X	X	X	X
AES192 CBC	X	X	X	X
AES256 CBC	X	X	X	X
CTR AES128	-	X	X	X
CTR AES192	-	X	X	X
CTR AES256	-	X	X	X
AES128 CCM 16	-	X	X	X
AES192 MCC 16	-	X	X	X
AES256 CCM 16	-	X	X	X
AES128 GCM 16	-	X	X	X
AES192 GCM 16	-	X	X	X
AES256 GCM 16	-	X	X	X

x: es compatible

-: no es apoyado

4.9.3 Gestión de certificados PKI

4.9.3.1 Certificación PKI CA

Llamando a la página web

En la navegación, seleccione "Seguridad > PKI".

Entradas mostradas

En la pestaña "Certificados de CA PKI", puede ver una descripción general de los certificados importados:

Campo	Sentido
Nombre común	Nombre del solicitante, por ejemplo, el nombre de usuario
Estado	Muestra si el certificado es válido o ya ha caducado.
Tipo de certificado	Tipo de certificado importado
Tema	Propietario de la clave privada asignada en el certificado
Editor	Visualización de la autoridad certificadora que emitió el certificado.
Válida desde	Fecha a partir de la cual el certificado es válido.
Válido hasta	Fecha en que caduca el certificado.
Huella dactilar	Suma de comprobación del certificado para garantizar la integridad

Para eliminar un certificado de CA de PKI, seleccione la casilla de verificación frente al certificado que desea eliminar y haga clic en el botón "Eliminar".

Importación de certificados de CA de PKI

1. Para importar certificados de CA PKI, haga clic en el botón "Importar".
2. Seleccione el archivo del certificado CA (*.crl) y confirme su selección con el botón "Abrir".
3. Para cargar el archivo en SINEMA RC Server, haga clic en el botón "Guardar".

Resultado:

El archivo de certificado se importa al servidor SINEMA RC. El certificado PKI CA se muestra en la siguiente pestaña "Certificado PKI CA".

4.9.3.2**Bloqueo de tarjeta inteligente/certificado de usuario**

Para bloquear a los usuarios, tiene dos opciones:

- Lista de revocación de certificados (CRL)
- Lista negra de DN de PKI

Llamando a la página web

En la navegación, seleccione "Seguridad > PKI".

Lista de revocación de certificados

Los certificados de salida que ya no son válidos aparecen en una lista de revocación de certificados. Si, por ejemplo, los empleados dejan la empresa, sus certificados se recuperan y se incluyen en la lista. Entonces ya no es posible iniciar sesión con este certificado.

Para que se utilice la lista de revocaciones, active la comprobación de CRL en la pestaña "Configuración".

En la pestaña "Lista de revocación", puede ver una descripción general de las listas de revocación disponibles:

Campo	Sentido
Editor	Visualización de la autoridad de certificación que emitió la lista de revocación del certificado.
Números de serie revocados	Muestra los números de serie revocados.
Última actualización	Fecha en la que se actualizó por última vez la lista de revocación de certificados.
Próxima actualización	Fecha en la que se actualizará próximamente la lista de revocación de certificados.
Origen	Muestra de dónde se origina la lista de revocación de certificados: Archivo: Se importó la lista de revocación de certificados URL: la lista de revocación de certificados se almacena en el punto de distribución.

Importación o eliminación de la lista de revocación de certificados**Importar**

1. En la pestaña "Lista de revocaciones", haga clic en el botón "Importar".
2. Haga clic en el botón "Seleccionar archivo" y seleccione la lista de revocación de certificados. Generalmente, el archivo tiene la extensión *.crl.

Confirme su selección con el botón "Abrir".

3. Para importar la lista de revocación de certificados, haga clic en el botón "Guardar".

Borrar

1. Seleccione la casilla de verificación frente a la lista de revocación de certificados que desea eliminar.
2. Haga clic en el botón "Eliminar".

Obtención de la lista de revocación de certificados de forma automática

En un certificado según el estándar X.509v3, puede especificar un punto de distribución de la lista de revocación de certificados. Para ello, especifique una URL en el atributo "Punto de distribución de CRL" en la que se almacena la CRL actual de esta autoridad de certificación. Para usar esta función, el atributo debe existir en el certificado de CA PKI.

A determinados intervalos, SINEMA RC descarga el archivo y lo utiliza. El intervalo se especifica en la pestaña "Configuración".

Configuración de la lista de revocación de certificados

Campo	Sentido
Activar comprobación de CRL	Cuando está habilitado, la validez del certificado de usuario se comprueba en función de la lista de revocación de certificados.
Intervalo de actualización de CRL (min)	Especifique los intervalos en los que se comprueban los cambios en la lista de revocación de certificados. Si hay cambios, la lista de revocación de certificados se descarga desde el punto de distribución.
Permitir CRL faltante	<ul style="list-style-type: none"> • Discapacitado <p>Cada certificado de CA de PKI requiere una lista de revocación de certificados válida. Si falta, los certificados de usuario derivados del certificado de CA de PKI no son válidos.</p> <ul style="list-style-type: none"> • Activado: <p>Cuando está habilitado, se permite la ausencia de la lista de revocación de certificados. Tenga en cuenta que si falta la lista de revocación de certificados, se permiten todos los certificados de usuario derivados del certificado PKI CA.</p>

Lista negra de DN de PKI

El usuario está bloqueado si existe una regla de filtro de DN de PKI correspondiente en la lista negra de DN de PKI.

1. Haga clic en la pestaña "Lista negra de DN de PKI".
2. Introduzca la regla de filtrado correspondiente en "PKI DN". Los atributos de los nombres (Distinguidos Nombre según al estándar X.509) se utilizan como criterios de filtro. Esto requiere que los atributos estén incluidos en el certificado PKI del usuario. Para obtener información más detallada, consulte la sección "Inicio de sesión con los certificados Smartcard / PKI".
3. Haga clic en "Agregar".

Resultado:

Las entradas creadas se enumeran en la página:

Campo	Sentido
filtro DN	Muestra la regla de filtro de DN de PKI.
Usuario desactivado	Muestra los usuarios a los que se aplica la regla y que, por tanto, están bloqueados.

Para eliminar una regla de filtro de DN de PKI, seleccione la casilla de verificación frente a la entrada que desea eliminar y haga clic en el botón "Eliminar".

4.9.4 Gestión de certificados Syslog

4.9.4.1 Certificados CA de Syslog

Puede importar el certificado de CA necesario para la autenticación del servidor Syslog en esta página.

Nota

Importación de los certificados de CA

Importe primero los certificados de CA del servidor Syslog. Si carga los certificados de Syslog más tarde, no será posible ejecutar algunas funciones, como la inspección en cadena o la lista de revocación de certificados.

Sin embargo, es posible la conexión sin certificados de CA del servidor Syslog importados.

Tipos de autenticación Syslog

Durante una **autenticación del servidor Syslog**, el cliente Syslog verifica la identidad del servidor Syslog utilizando el certificado del servidor CA Syslog.

Como opción, se puede realizar la autenticación mutua entre el cliente y el servidor (**autenticación de servidor y cliente**). En este caso, el servidor Syslog solicita el certificado del cliente Syslog después de la autenticación del servidor Syslog para verificar la identidad del cliente Syslog. La verificación del certificado se realiza de acuerdo con RFC 5280. Para la autenticación del servidor y del cliente, se debe importar el certificado del cliente Syslog; consulte "Importación de certificados Syslog". Estos certificados se pueden seleccionar como certificados de conexión para el cliente Syslog, consulte "Cliente Syslog (Página 97)".

Requisito

- El usuario tiene asignado el derecho "Gestión de certificados".

Llamando a la página web

En la navegación, seleccione "Seguridad > Syslog".

Entradas mostradas

En la pestaña "Administración de certificados de CA de Syslog", puede ver una descripción general de los certificados de CA importados:

Campo	Sentido
Nombre común	Nombre del solicitante, por ejemplo, el nombre de usuario
Estado	Muestra si el certificado es válido o ya ha caducado
Tipo de certificado	Tipo de certificado importado
Tema	Propietario de la clave privada asignada en el certificado
Editor	Visualización de la autoridad certificadora que emitió el certificado
Válida desde	Fecha a partir de la cual el certificado es válido
Válido hasta	Fecha en que caduca el certificado
Huella dactilar	Suma de comprobación del certificado para garantizar la integridad
Comportamiento	 Certificado de exportación

Importación de certificados Syslog

- Para importar certificados Syslog, haga clic en el botón "Importar".

Se muestra la página de diálogo para importar certificados. Puede cargar los siguientes archivos:

- Certificado CA del servidor Syslog (obligatorio)
- Certificado de cliente Syslog (opcional)
- Clave privada del cliente Syslog (opcional)

- Haga clic en el botón "Seleccionar archivo" para importar el tipo de certificado.

Navegue hasta el directorio de almacenamiento y seleccione el archivo correspondiente. Confirme su selección con el botón "Abrir".

- Para cargar los archivos en el servidor SINEMA RC, haga clic en el botón "Guardar".

Resultado

El archivo de certificado se importa al servidor SINEMA RC. El certificado Syslog se muestra en la tabla.

Nota

Parámetros incorrectos del certificado del servidor

La conexión cifrada entre el servidor y el cliente falla si el "commonName" o el parámetro del certificado del servidor "subject_alt_name" no contiene ni el nombre de host ni la dirección IP del servidor (por ejemplo, CN = 192.168.10.10).

Nota

Renovación de certificados

SINEMA RC no renueva los certificados automáticamente. Para evitar problemas con los certificados, actualice los archivos de certificados caducados manualmente en el servidor Syslog y el servidor SINEMA RC.

4.9.4.2**Certificados de Syslog**

En esta página, puede importar los certificados de cliente de Syslog y administrar los certificados importados. Para la autenticación, el servidor Syslog solicita el certificado del cliente Syslog para verificar la identidad del cliente Syslog.

Requisito

- El usuario tiene asignado el derecho "Gestión de certificados".

Llamando a la página web

En la navegación, seleccione "Seguridad > Syslog".

Entradas mostradas

En la pestaña "Certificados de Syslog", puede ver una descripción general de los certificados de Syslog importados:

Campo	Sentido
Nombre común	Nombre del solicitante, por ejemplo, el nombre de usuario
Estado	Válido: se utiliza el certificado. No válido: el certificado no se utiliza. Se generó un certificado más nuevo o el certificado caducó.
Tipo de certificado	Tipo de certificado importado
Tema	Propietario de la clave privada asignada en el certificado
Editor	Visualización de la autoridad certificadora que emitió el certificado.
Válida desde	Fecha a partir de la cual el certificado es válido.
Válido hasta	Fecha en que caduca el certificado.
Huella dactilar	Suma de comprobación del certificado para garantizar la integridad
Comportamiento	 Certificado de exportación  Renovar certificado

Importación de certificados Syslog

1. Para importar certificados Syslog, haga clic en el botón "Importar".

Se muestra la página de diálogo para importar certificados. Puede cargar los siguientes archivos:

- Certificado CA del servidor Syslog (obligatorio)
- Certificado de cliente Syslog (opcional)
- Clave privada del cliente Syslog (opcional)

2. Haga clic en el botón "Seleccionar archivo" para importar el tipo de certificado.
Navegue hasta el directorio de almacenamiento y seleccione el archivo correspondiente. Confirme su selección con el botón "Abrir".
3. Para cargar los archivos en el servidor SINEMA RC, haga clic en el botón "Guardar".

Resultado

El archivo de certificado se importa al servidor SINEMA RC. El certificado Syslog se muestra en la tabla.

Nota**Parámetros incorrectos del certificado del servidor**

La conexión cifrada entre el servidor y el cliente falla si el "commonName" o el parámetro del certificado del servidor "subject_alt_name" no contiene ni el nombre de host ni la dirección IP del servidor (por ejemplo, CN = 192.168.10.10).

Nota**Renovación de certificados**

SINEMA RC no renueva los certificados automáticamente. Para evitar problemas con los certificados, actualice los archivos de certificados caducados manualmente en el servidor Syslog y el servidor SINEMA RC.

Eliminación de certificados de Syslog

Puede eliminar los certificados caducados mediante el botón "Eliminar".

1. Seleccione la casilla de verificación del certificado que desea eliminar.
2. Haga clic en el botón "Eliminar".

4.9.4.3**Revocación de certificados de Syslog**

Puede revocar usuarios mediante la Lista de revocación de certificados (CRL) de Syslog.

Llamando a la página web

En la navegación, seleccione "Seguridad > Syslog > Lista de revocación de Syslog".

Lista de revocación de certificados

Los certificados de salida que ya no son válidos aparecen en una lista de revocación de certificados. Si, por ejemplo, los empleados dejan la empresa, sus certificados se recuperan y se incluyen en la lista. Entonces ya no es posible iniciar sesión con este certificado.

Para que se utilice la lista de revocaciones, active la comprobación de CRL en la pestaña "Configuración".

En la pestaña "Lista de revocación de Syslog", puede ver una descripción general de las listas de revocación disponibles:

Campo	Sentido
Editor	Visualización de la autoridad de certificación que emitió la lista de revocación del certificado.
Números de serie revocados	Muestra los números de serie revocados.
Última actualización	Fecha en la que se actualizó por última vez la lista de revocación de certificados.

Configuración con administración basada en web

4.9 Seguridad

Campo	Sentido
Próxima actualización	Fecha en la que se actualizará próximamente la lista de revocación de certificados.
Origen	Muestra de dónde se origina la lista de revocación de certificados: Archivo: Se importó la lista de revocación de certificados URL: la lista de revocación de certificados se almacena en el punto de distribución.

Importación o eliminación de la lista de revocación de certificados

Importar

1. En la pestaña "Lista de revocación de Syslog", haga clic en el botón "Importar".
2. Haga clic en el botón "Seleccionar archivo" y seleccione la lista de revocación de certificados.

Generalmente, el archivo tiene la extensión *.crl.

Confirme su selección con el botón "Abrir".

3. Para importar la lista de revocación de certificados, haga clic en el botón "Guardar".

Borrar

1. Seleccione la casilla de verificación frente a la lista de revocación de certificados que desea eliminar.
2. Haga clic en el botón "Eliminar".

Obtención de la lista de revocación de certificados de forma automática

En un certificado según el estándar X.509v3, puede especificar un punto de distribución de la lista de revocación de certificados. Para ello, especifique una URL en el atributo "Punto de distribución de CRL" en la que se almacena la CRL actual de esta autoridad de certificación. Para usar esta función, el atributo debe existir en el certificado Syslog.

A determinados intervalos SINEMA RC descarga el archivo y lo utiliza. El intervalo se especifica en la pestaña "Configuración".

Configuración de la lista de revocación de certificados

Campo	Sentido
Activar comprobación de CRL	Cuando está habilitado, la validez del certificado de usuario se comprueba en función de la lista de revocación de certificados.
Intervalo de actualización de CRL (min)	Especifique los intervalos en los que se comprueban los cambios en la lista de revocación de certificados. Si hay cambios, la lista de revocación de certificados se descarga desde el punto de distribución.
Permitir CRL faltante	<ul style="list-style-type: none"> • Discapacitado <p>Cada certificado de Syslog requiere una lista de revocación de certificados válida. Si falta, los certificados de usuario derivados del certificado Syslog no son válidos.</p> • Activado <p>Cuando está habilitado, se permite la ausencia de la lista de revocación de certificados. Tenga en cuenta que si falta la lista de revocación de certificados, se permiten todos los certificados de usuario derivados del certificado Syslog.</p>

4.10 Mi cuenta

4.10.1 Certificado de usuario

Llamando a la página web

En la navegación, seleccione "Mi cuenta > Certificado de usuario".

Entradas mostradas

En la pestaña "Detalles", verá una descripción general del certificado de usuario derivado del certificado de CA:

Campo	Sentido
Número de serie	Número para identificar el certificado. El número de serie se asigna automáticamente cuando se crea el certificado.
Nombre común	El nombre utilizado es generado automáticamente por el sistema.
Editor	Visualización de la autoridad certificadora que emitió el certificado. El sistema utiliza el último certificado CA válido.
Válida desde	Fecha a partir de la cual el certificado es válido.
Válido hasta	Fecha en que caduca el certificado.
Longitud de clave (bits)	Especifica la longitud de la clave que se utiliza. El valor se puede establecer en el menú "Seguridad > Certificados", pestaña "Configuración" en "Longitud de clave preferida".
Método de firma	Especifica qué método de firma digital con la clave de firma correspondiente ("valor hash") se utilizó para el certificado. El valor se puede establecer en el menú "Seguridad > Certificados", pestaña "Configuración" en "Método hash preferido".

Renovación de un certificado de usuario

Nota

Sólo renovar certificados válidos

No puede renovar un certificado que ya ha caducado. Si intenta renovar un certificado caducado, la autoridad de certificación rechazará la solicitud. Cuando un certificado ya ha caducado, en lugar de renovar el certificado existente, debe solicitar un nuevo certificado.

Con el botón "Renovar", puede cuando sea necesario, por ejemplo, con certificados comprometidos, generar un nuevo certificado.

Para ello introduzca la contraseña de usuario correspondiente. El número de serie se incrementa automáticamente en uno.

*Configuración con administración basada en web***4.10 Mi cuenta****Exportación de un certificado de usuario**

Puede descargar el certificado personal en la pestaña "Exportar". Éstos incluyen:

Campo	Sentido
PKCS#12	Descargue un contenedor en el formato de intercambio de información personal (PFX).
PEM	Descargue el certificado y la clave como texto ASCII codificado en Base64.
OVPN	Descargue la configuración de OpenVPN para el usuario.

4.10.2 Cambia la contraseña**Cambiar la contraseña actual**

Como usuario registrado, puede cambiar su contraseña actual:

1. En la navegación, seleccione "Mi cuenta > Cambiar contraseña".
2. Introduzca la contraseña anterior.
3. Introduzca la nueva contraseña y confírmela.

El nuevo debe tener al menos 8 caracteres y contener caracteres especiales, mayúsculas y minúsculas, así como números. Ver también la sección "Caracteres permitidos (Página 27)".

4.10.3 Descargar software de cliente

En esta página, puede descargar SINEMA RC Client desde el servidor SINEMA RC a su PC.

Requisito

- Al usuario se le ha asignado el derecho "Descargar software de cliente".
- Se cargó un paquete de software de cliente en el servidor.

Llamando a la página web

En la navegación, seleccione "Mi cuenta > Software de cliente".

Descargar software de cliente

Procedimiento

1. Compruebe la versión de software mostrada del SINEMA RC Client y la huella digital.
2. Haga clic en el botón "Descargar".

Se abre un cuadro de diálogo para abrir y guardar archivos. Siga las instrucciones del cuadro de diálogo para guardar el software del cliente en la PC del usuario.

Resultado

El SINEMA RC Client se descarga en su PC.

Dependiendo de la configuración, el archivo también se puede cargar en la carpeta de descarga.

Conservación y mantenimiento

5.1

Copia de seguridad y restauración de la configuración del sistema

En la copia de seguridad se guardan los ajustes actuales del sistema de SINEMA RC Server, p. ej. dispositivos configurados, usuarios.

Nota

Ajustes que no se toman

Las siguientes configuraciones no se respaldan:

- Configuración de la red
- Mensajes de registro

Con la copia de seguridad, puede restaurar la configuración del sistema del servidor dentro de una versión SINEMA RC o transferirla a otro servidor. Una copia de seguridad creada en una versión SINEMA RC, por ejemplo, 1.2, no se puede leer en un sistema con SINEMA RC versión V1.3. Puede encontrar información adicional en Internet con el siguiente ID de entrada: 109748144 (<https://support.industry.siemens.com/cs/ww/de/view/109748144/en>)

Configuración de ajustes

Requisito:

- Al usuario se le ha asignado el derecho "Editar parámetros del sistema".

Procedimiento

1. En el panel de navegación "Sistema > Copia de seguridad y restauración", seleccione la pestaña "Configuración".

Introduzca el número de copias de seguridad permitidas.

Se permite una entrada entre 10 y 30. Cuando se alcanza el número máximo, se sobrescribe la copia de seguridad más antigua.

2. Si se debe realizar una copia de seguridad del sistema a intervalos regulares, especifique el intervalo y el tiempo para la copia de seguridad.

3. Introduzca una "clave de cifrado".

La clave de codificación debe tener al menos 8 caracteres y contener caracteres especiales, mayúsculas y minúsculas, así como números, consulte la sección "Caracteres permitidos (Página 27)".

4. Confirme la clave de codificación.

5. Haga clic en el botón "Guardar".

Conservación y mantenimiento**5.1 Copia de seguridad y restauración de la configuración del sistema****Copia de seguridad de configuraciones****Requisito**

- Al usuario se le ha asignado el derecho "Crear copias de seguridad".
- Los ajustes para la copia de seguridad están configurados.

Procedimiento

1. En el panel de navegación, seleccione "Sistema > > Copia de seguridad y restauración".
2. Haga clic en el botón "Crear nueva copia de seguridad".
3. En el cuadro de diálogo siguiente, introduzca un comentario sobre la copia de seguridad.
4. Haga clic en el botón "Finalizar".

Resultado

Se ha creado una copia de seguridad (*.backup) con la configuración del sistema del SINEMA RC Server.

Restauración de la configuración**Requisito**

- En el sistema está instalada la versión SINEMA RC con la que se realizó la copia de seguridad creada.

Importación de la copia de seguridad

1. En el panel de navegación "Sistema > Copia de seguridad y restauración", seleccione la pestaña "Configuración".
2. Introduzca la misma clave de codificación con la que se creó la copia de seguridad y guarde la configuración.
3. Haga clic en el botón "Importar copia de seguridad".
4. Haga clic en el botón "Examinar".
5. Seleccione el archivo requerido en el formato *.backup y confirme su selección con "Abrir" botón.
6. Haga clic en el botón "Finalizar". La copia de seguridad se muestra en la vista general.
7. Haga clic en el botón "Restaurar" para adoptar la configuración del sistema de la copia de seguridad seleccionada.

Haga clic en el botón "Restaurar" en el siguiente cuadro de diálogo.

Resultado

- La copia de seguridad se importó al mismo servidor/hardware con la instalación existente
SINEMA RC Server toma la configuración del sistema de la copia de seguridad seleccionada y continúa trabajando con ella.
Todos los ajustes realizados hasta este momento que no se hayan guardado en una copia de seguridad se perderán.
- La copia de seguridad se importó a otro servidor/hardware con una nueva instalación y la misma configuración de la red
Después de una transferencia exitosa, el sistema se reinicia y se abre la página de inicio de sesión del SINEMA RC Server.
Los certificados respaldados se importan.
- La copia de seguridad se importó a un servidor/hardware diferente y una nueva instalación con diferentes configuraciones de red.

Después del reinicio, se abre la página de inicio de sesión de SINEMA RC Server. Los certificados no se importan sino que se crean nuevos.

5.2 Actualización del sistema V1.2 > V1.3

Procedimiento

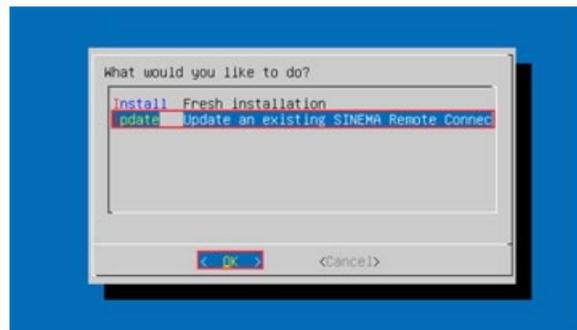
1. Realice una copia de seguridad de su configuración con SINEMA RC Server V1.2 WBM y exporte este archivo de copia de seguridad a su PC o servidor SFTP.
Puede encontrar información más detallada al respecto en las secciones "Backup & Restore" y "Upload Server (Página 96)".
2. Inserte el soporte de datos V1.3 en la unidad.
3. Navegue hasta el menú WBM "Sistema > Actualizar (Página 65)".
Reinicie a través de "Gestión de energía (Página 65)".
La instalación comienza automáticamente.
4. Seleccione la entrada "Instalar/Actualizar SINEMA Remote Connect Server" en el siguiente cuadro de diálogo.
Confirme la selección con la tecla ENTER.



Conservación y mantenimiento

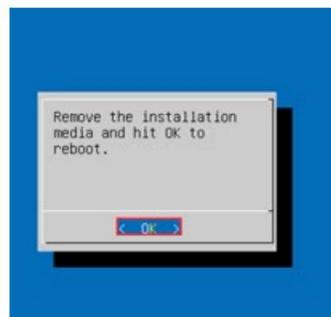
5.2 Actualización del sistema V1.2 > V1.3

5. En el siguiente cuadro de diálogo, seleccione la entrada "Actualizar - Actualizar un SINEMA Remote Connect existente" y haga clic en el botón <Aceptar>.



Se actualizó el servidor SINEMA RC a la versión V1.3. Después de la instalación de esta actualización, hay dos particiones de arranque disponibles. Una partición aún contiene su servidor operativo versión V1.2. Otra partición ahora contiene un servidor operativo versión V1.3 con la misma configuración de servidor, incluidos dispositivos, usuarios y certificados. Sin embargo, su licencia SINEMA RC Server no se transfirió automáticamente a V1.3. Para habilitarlo en su nuevo servidor V1.3, primero debe liberar la licencia en la versión V1.2.

6. Extraiga el disco V1.3 de la unidad y haga clic en el botón <Aceptar>.



Reinicie el servidor. En el menú de inicio, puede ver las particiones de ambas versiones de servidor V1.2 y V1.3.

7. Seleccione "SINEMA RC (1.2.0)" en el menú de arranque y confirme su selección con ENTER llave.



8. Inicie sesión con sus credenciales de usuario y navegue hasta el menú "Sistema > Licencias (Página 62)".
 Liberar las licencias para reactivarlas en servidor versión V1.3.

SIEMENS SINEMA Remote Connect

Logged on as "Admin!"

Log off

Licenses

License type	Ticket number	Activation date	License value	Status	Actions
<input type="checkbox"/> Demo License	00000-00000-00000-00000-00000	-	4 / 4	Active	
<input checked="" type="checkbox"/> SINEMA RC connections	M8BHD-XXXXXXXXXX	Dec. 1, 2017, 10:53 a.m.	15 / 64	Active	

A

Conservación y mantenimiento

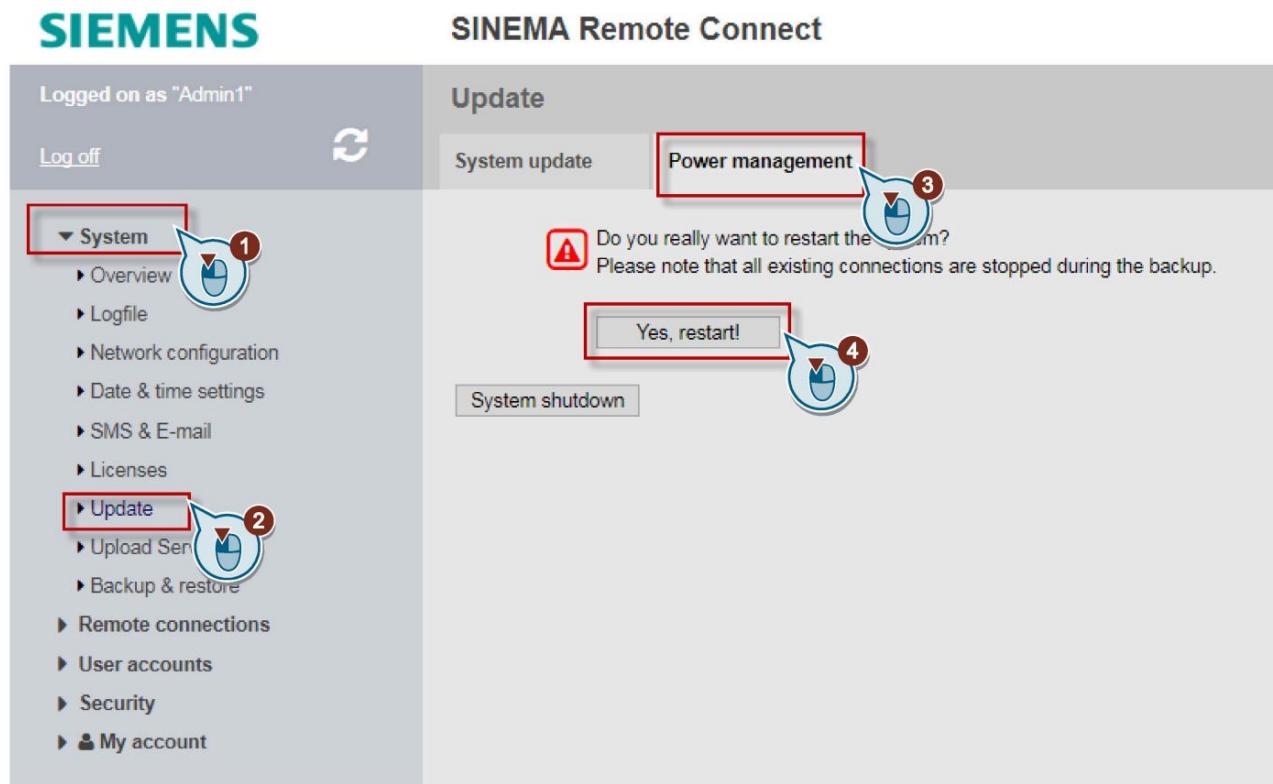
5.2 Actualización del sistema V1.2 > V1.3

Nota

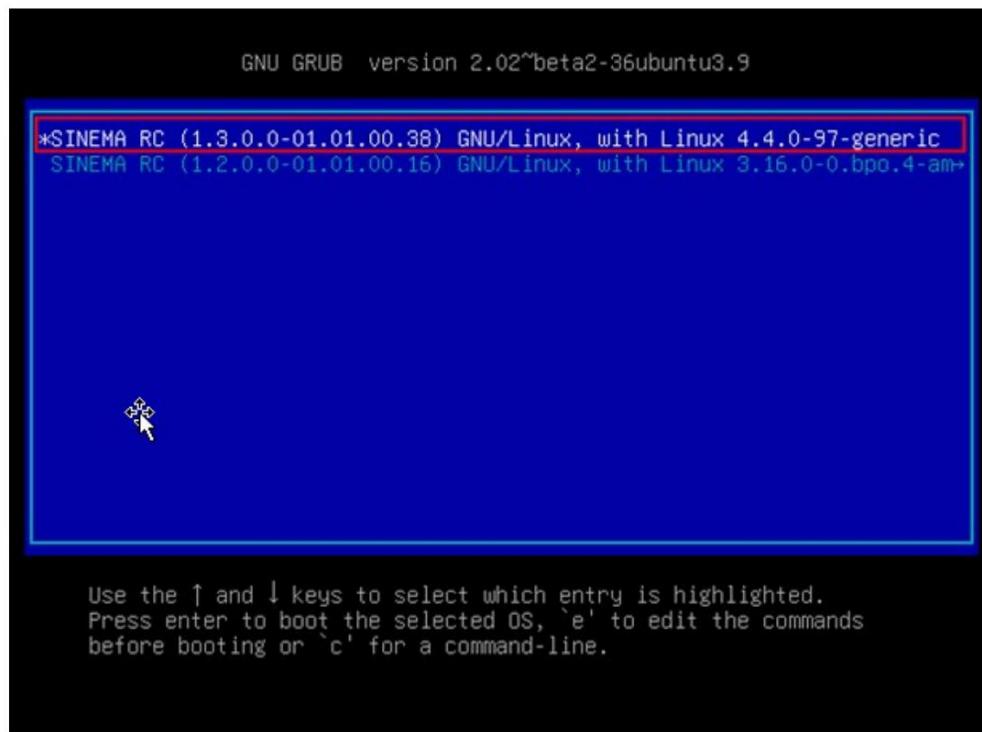
Si no es posible desactivar la licencia en WBM (p. ej., no hay conexión con el servidor de licencias), póngase en contacto con el servicio de atención al cliente a través de una solicitud de soporte (<https://support.industry.siemens.com/cs/my?lc=en-US>). Luego, todos los pasos posteriores se coordinan con Atención al cliente para reactivar la licencia.

9. Navegue hasta el menú WBM "Sistema > Actualizar (Página 65)".

Realice un reinicio a través de "Gestión de energía (Página 65)".



10. Seleccione "SINEMA RC (1.3.0)" en el menú de inicio y confirme su selección con ENTER llave.



11. Inicie sesión con sus credenciales de usuario y navegue nuevamente al menú "Sistema > Licencias (Página 62)".

Activar las licencias.

Puede seleccionar entre la activación sin conexión o en línea. Encontrará más información al respecto en el apartado "Gestionar licencias (Página 62)".

License type	License number	Activation date	License value	Status	Actions
<input type="checkbox"/> Demo License	00000-00000-00000-00000-00000	-	0 / 4	Active	

Conservación y mantenimiento

5.3 Actualización del sistema V2.0 > V2.1

Resultado

Se ha actualizado el servidor SINEMA RC y su licencia a la versión V1.3. Se conservan las configuraciones anteriores del servidor. Además de esta versión actualizada del servidor, hay otra partición en la PC con la versión original del servidor V1.2 como respaldo. La versión del servidor V1.2 aún se puede iniciar desde el menú de inicio de la PC si es necesario deshacer la actualización. No se pueden crear más dispositivos o usuarios en la versión de servidor V1.2. Cuando reinicia el servidor, siempre se utiliza la última partición que se inició.

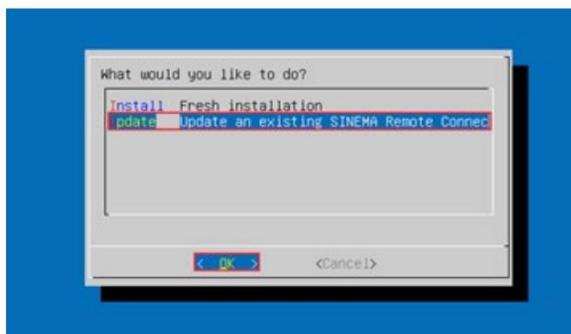
5.3 Actualización del sistema V2.0 > V2.1

Procedimiento

1. Realice una copia de seguridad de su configuración con el servidor SINEMA RC V2.0 WBM y exporte este archivo de copia de seguridad a su PC o servidor SFTP.
Puede encontrar información más detallada al respecto en las secciones "Backup & Restore" y "Upload Server (Página 96)".
2. Navegue hasta el menú WBM "Sistema > Actualizar (Página 65)".
Reinicie a través de "Gestión de energía (Página 65)".
La instalación comienza automáticamente.
3. Seleccione la entrada "Instalar/Actualizar SINEMA Remote Connect Server" en el siguiente cuadro de diálogo.
Confirme la selección con la tecla ENTER.



4. En el siguiente cuadro de diálogo, seleccione la entrada "Actualizar - Actualizar un SINEMA Remote Connect existente" y haga clic en el botón <Aceptar>.



5. Seleccione "SINEMA RC (2.0)" en el menú de arranque y confirme su selección con ENTER llave.
6. Inicie sesión con sus credenciales de usuario y navegue hasta el menú "Sistema > Licencias (Página 62)". Liberar las licencias de "SINEMA RC (2.0)" para reactivarlas posteriormente en la versión de servidor V2.1.

License type	Ticket number	Activation date	License value	Status	Actions
<input type="checkbox"/> Demo License	0000-0000-0000-0000-0000	-	4 / 4	Active	
<input checked="" type="checkbox"/> SINEMA RC connections	M8BHD-	Dec. 1, 2017, 10:53 a.m.	15 / 64	Active	

Nota

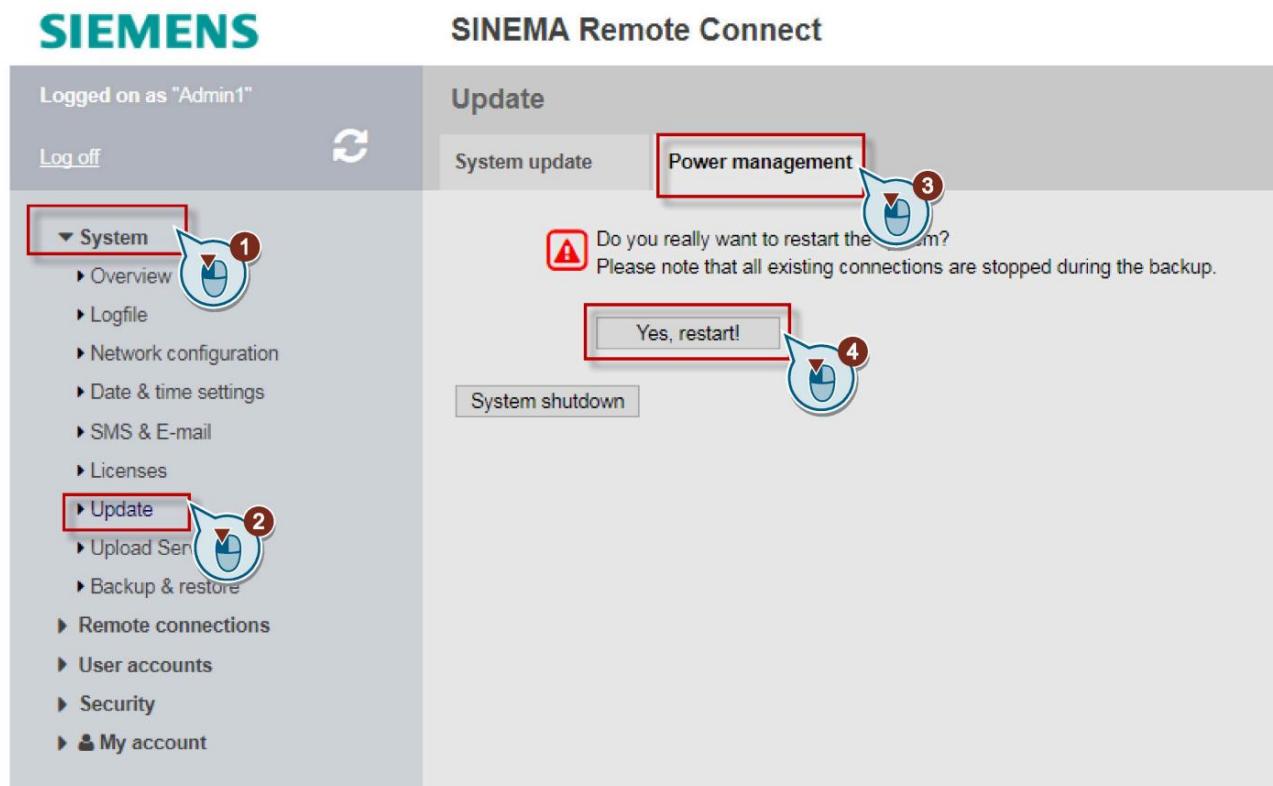
Si no es posible desactivar la licencia en WBM (p. ej., no hay conexión con el servidor de licencias), póngase en contacto con el servicio de atención al cliente a través de una solicitud de soporte (<https://support.industry.siemens.com/cs/my?lc=en-US>). Luego, todos los pasos posteriores se coordinan con Atención al cliente para reactivar la licencia.

Conservación y mantenimiento

5.3 Actualización del sistema V2.0 > V2.1

7. Navegue hasta el menú WBM "Sistema > Actualizar (Página 65)".

Realice un reinicio a través de "Gestión de energía (Página 65)".



8. Seleccione "SINEMA RC (2.1)" en el menú de arranque y confirme su selección con ENTER llave.
9. Inicie sesión con sus credenciales de usuario y navegue nuevamente hasta el menú "Sistema> Licencias (Página 62)".
Activar las licencias.
Puede seleccionar entre la activación sin conexión o en línea. Encontrará más información al respecto en el apartado "Gestionar licencias (Página 62)".

The screenshot shows the SINEMA Remote Connect web interface. On the left, there's a sidebar with a navigation tree under 'System' (marked with a red box and number 1). The 'Licenses' item is selected and highlighted with a red box (marked with a red box and number 2). The main content area is titled 'Licenses'. It shows a table with one row for a 'Demo License' (marked with a red box and number 3a). Below the table is a section for 'Online license activation' with a 'Activate License' button. To the right, there's a larger box for 'Offline license activation' containing three steps: 'Step 1: Export License Container', 'Step 2: Contact Siemens Industry Support', and 'Step 3: Datei auswählen | Keine ausgewählt Import License Update' (marked with a red box and number 3b).

Resultado

Se ha actualizado el servidor SINEMA RC y su licencia a la versión 2.1. Se conservan las configuraciones anteriores del servidor.

5.4 Actualización del sistema V2.1 > V3.0

En la página "Sistema > Actualizar" puede actualizar el servidor SINEMA RC V2.1 a la versión V3.0. Despu s de la actualizaci n, reinicia el servidor. Se conservan las configuraciones anteriores del servidor. Puede encontrar informaci n adicional en la secci n "Actualizaci n (P gina 65)".

A

Apéndice A

A.1 Conexión OpenVPN a un dispositivo iOS

Para establecer una conexión OpenVPN a un dispositivo iOS, siga los pasos a continuación:

1. Inicie sesión en SINEMA RC Server con sus datos de usuario.
2. En la navegación, seleccione "Mi cuenta > Certificado de usuario" y haga clic en la pestaña "Exportaciones".
3. Exporte los siguientes archivos a un directorio local en su PC:
 - PEM: Certificado y clave como texto ASCII codificado en Base64
 - OVPN: configuración de OpenVPN para el usuario

Al hacer clic en los archivos, se descargan inmediatamente.
4. Abra el archivo pem con un editor, por ejemplo, Notepad ++, y seleccione todo con el acceso directo "CTRL + A".
Copie el texto seleccionado al portapapeles usando el atajo "CTRL + C".
5. Abra el archivo opvn y haga clic en la línea libre delante de la etiqueta "<pkcs12>". Pegue el contenido del portapapeles en esta ubicación con el atajo "CTRL + V".
6. Haga clic en el botón "Mostrar todos los caracteres" para ocultar los caracteres de formato.
7. Elimine los espacios superfluos y los saltos de línea después de la etiqueta "</ca>".
8. Guarde los cambios en el archivo opvn.
9. Cargue el archivo opvn en el dispositivo iOS. También puede enviarse a sí mismo el archivo en un correo electrónico.
10. Cuando abre el archivo opvn, se le pregunta si desea abrirlo con la aplicación.
Confirmar esto. La nueva configuración se ofrece para aplicar en la aplicación "OpenVPN-Connect".
Haga clic en el ícono verde más. Debe confirmar que permite que la aplicación OpenVPN configure conexiones VPN con el código de su iPad.
11. Se abre el perfil. Se requiere la contraseña para el certificado. En el campo correspondiente, introduzca la contraseña que definió para el nuevo usuario en SINEMA Remote Connect Server.
12. Si todos los componentes están configurados, el túnel VPN se puede inicializar entre la tableta (aplicación "OpenVPN-Connect") y SINEMA Remote Connect Server.
13. Cuando se establezca la conexión, podrá acceder al WBM de SINEMA RC.

Apéndice A

A.1 Conexión OpenVPN a un dispositivo iOS

B

apéndice B

B.1

Habilitación de la dirección de correo electrónico

Para recibir el correo electrónico, con algunos proveedores de red, primero se debe habilitar la dirección de correo electrónico del destinatario del mensaje SMS.

Para habilitar la dirección de correo electrónico, normalmente envía un texto de activación especial a un número abreviado de su proveedor de red. Encontrará varios ejemplos en la siguiente tabla "SMS de activación y desactivación".

Recibirá un SMS de respuesta con la dirección de correo electrónico que contiene el número de teléfono y el Nombre de la puerta de enlace de SMS de su operador de red:

12345@<Dominio del proveedor de SMS>.<Dominio de nivel superior>

Nota

Consulte con su proveedor de red si es necesario o no enviar mensajes SMS de activación y desactivación. Su proveedor de red le informará sobre los textos y el número corto.

Tabla B-1 SMS de activación y desactivación (ejemplos)

	E-Plus	O2 Alemania	T-Mobile	Vodafone
puerta de enlace SMS nombre	smsmail.eplus.de	o2online.de	t-mobile-sms.de vodafone-sms.de	
Habilitación Enviar SMS con texto a número corto	Texto: INICIO Número corto: 7676245	Texto: ABIERTO Número corto: 6245	Texto: ABIERTO Número corto: 8000	Texto: ABIERTO Número corto: 3400
Desactivando Enviar SMS con texto a número corto	Texto: PARAR Número corto: 7676245	Texto: PARAR Número corto: 6245	Texto: CERRAR Número corto: 8000	Texto: CERRAR Número corto: 3400

Ver también

Proveedor de puerta de enlace SMS (Página 59)

apéndice B

B.2 Seguimiento y tiempo de respuesta de mensajes SMS de despertador

B.2 Monitoreo y tiempo de respuesta de mensajes SMS de despertador

Possibles causas de intentos fallidos de reactivación

Si una estación no se puede despertar, existen diferentes razones posibles para ello.

- **Bloques de tiempo de los proveedores de puerta de enlace de SMS**

Para activar un mensaje SMS de activación, haga clic en "Conexiones remotas > Administrar dispositivos".

Como defensa contra el spam, algunos proveedores de red filtran los mensajes SMS con el mismo contenido enviado al mismo suscriptor dentro de un tiempo limitado, por ejemplo, 1 minuto.

Si intenta reactivar un dispositivo repetidamente porque no establece una conexión en poco tiempo, espere un tiempo adecuado entre repeticiones. Compruebe las entradas del registro. Mensajes como "El correo parecía ser SPAM u olvidado" indican que este es el caso.

Si es necesario, consulte con su proveedor de red.

- **No ejecutado**

El trabajo de reactivación se transfirió a SINEMA RC pero no se ejecutó. Compruebe las conexiones de SINEMA RC Server, incluida la conexión a Internet.

- **Respuesta negativa**

La puerta de enlace SMS no ha recibido el mensaje.

El éxito del envío de un correo electrónico de activación a la puerta de enlace SMS se puede detectar a través de un mensaje de registro. Si no se recibe la confirmación y se muestra este estado, hay una interrupción en la ruta entre SINEMA RC Server y la puerta de enlace SMS.

C

Apéndice C

C.1

Mensajes de registro del sistema

Visor de eventos

Los mensajes de Syslog se guardan localmente en el Visor de eventos de Microsoft Windows y no se envían a un servidor de Syslog.

1. Introduzca "Visor de eventos" en la línea de búsqueda del menú de inicio.
2. Haga clic en la entrada "Visor de eventos" para iniciar el Visor de eventos.
3. Haga clic en la entrada "Siemens Automation" para "Registros de aplicaciones y servicios".

Las entradas de registro se enumeran en forma tabular. Cuando hace clic en una entrada, la vista detallada se abre en el área inferior de la ventana.

C.1.1 Etiquetas en mensajes Syslog

Los mensajes de Syslog pueden contener variables que se llenan dinámicamente con los datos del evento respectivo. Estas variables se muestran entre llaves {variable} en el campo "Texto del mensaje" en la sección "Lista de mensajes Syslog (Página 140)".

Las siguientes variables ocurren en los mensajes de Syslog:

Parámetro	Descripción	Formato	Posibles valores o ejemplo
Nombre de usuario	Cadena que identifica al usuario autenticado en base a su nombre sin espacios	%s	Peter_Maier
dirección IP	Dirección IPv4 o IPv6	Dirección IP según RFC1035 o RFC4291 Sección 2.2	192.168.10.128
Nombre de usuario de destino	Cadena para el nombre del usuario de destino. Este no es el usuario autenticado.	%s	Peter_Maier
Nombre del dispositivo	Cadena para el nombre del dispositivo	%s	S615_1
Nombre de usuario temporal	Cadena para el nombre del usuario temporal	%s	Peter_Maier
Cierto parámetros	Cadena para los parámetros del certificado	%s	
Papel	Cadena para el nombre del rol de grupo	%s	Consultoría técnica
Grupo	Cadena para el nombre del grupo	%s	Servicio_TI
Nombre del CN	Cadena para el nombre de host del parámetro del servidor "commonName"	%s	Servidor 1 192.168.10.10
Detalle de configuración	Cadena para la configuración con espacios	%s	la configuración de DNS la configuración de copia de seguridad etc

Apéndice C**C.1 Mensajes de Syslog**

Parámetro	Descripción	Formato	Posibles valores o ejemplo
Nombre del archivo	Cadena para el nombre del archivo	%s	2019_04_03_09_53_2 3.copia de seguridad
Versión del archivo	Cadena para la versión del archivo	%s	2019_06_13_23_00_0 1.copia de seguridad
Versión del software	Cadena para la versión de software instalada	%s	V3.0.0-01.01.00.04
Versión de software de destino	Cadena para la versión de software cargada	%s	V3.0.0-01.01.00.01
Versión del software fuente	Cadena para la versión de software instalada	%s	V2.0.1.0-01.01.00.04
Número de versión	Cadena para la versión del acuerdo de usuario	%D	1

C.1.2 Lista de mensajes de Syslog**C.1.2.1 Identificación y autenticación de usuarios humanos**

Mensaje de texto	{Nombre de usuario} ha iniciado sesión
Ejemplo	"Peter_Maier" ha iniciado sesión
Explicación	Un usuario ha iniciado sesión correctamente en el servidor a través de la interfaz web.
Gravedad	Información
Instalaciones	local0
Estándar	Referencia IEC 62443-3-3: SR 1.1

Mensaje de texto	La solicitud de autenticación de {dirección IP} ha fallado La solicitud de
Ejemplo	autenticación de 192.168.0.1 ha fallado
Explicación	Falló el inicio de sesión en el servidor a través de la interfaz web. Nombre de usuario incorrecto o contraseña incorrecta ingresada durante el inicio de sesión remoto.
Gravedad	Error
Instalaciones	local0
Estándar	Referencia IEC 62443-3-3: SR 1.1

Mensaje de texto	{Nombre de usuario} se ha desconectado
Ejemplo	"Peter_Meier" se ha desconectado
Explicación	Un usuario cerró la sesión a través de la interfaz web, ya sea de forma manual o automática debido a un tiempo de espera. Sesión de usuario completada - sesión cerrada.
Gravedad	Información
Instalaciones	local0
Estándar	Referencia IEC 62443-3-3: SR 1.1

C.1.2.2 Gestión de cuentas de usuario

Mensaje de texto	{Nombre de usuario} ha desactivado al usuario: {Nombre de usuario de destino}
Ejemplo	"Admin" ha desactivado al usuario "Peter_Maier"

Explicación	Un usuario ha inhabilitado una cuenta de usuario.
Gravedad	Aviso
Instalaciones	local0
Estándar	Referencia IEC 62443-3-3: SR 1.3

Mensaje de texto	{Nombre de usuario} ha desactivado el dispositivo {Nombre del dispositivo}
Ejemplo	"Admin" ha desactivado el dispositivo "S615_1"
Explicación	Un usuario ha inhabilitado una cuenta de dispositivo.
Gravedad	Aviso
Instalaciones	local0
Estándar	Referencia IEC 62443-3-3: SR 1.3

Mensaje de texto	{Nombre de usuario} ha creado el usuario {Nombre de usuario de destino}
Ejemplo	"Admin" ha creado el usuario "Peter_Maier"
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	{Nombre de usuario temporal} se ha creado con {parámetros de certificado}
Ejemplo	"temp_user" ha sido creado con DN= "xxxx"
Explicación	Se creó una cuenta de usuario temporal.
Gravedad	Información
Instalaciones	local0
Estándar	Referencia IEC 62443-3-3: SR 1.3

Mensaje de texto	{Nombre de usuario} ha creado el dispositivo {Nombre del dispositivo}
Ejemplo	"Admin" ha creado el dispositivo "S615_1"
Explicación	Un usuario creó una cuenta de dispositivo.
Gravedad	Aviso
Instalaciones	local0
Estándar	Referencia IEC 62443-3-3: SR 1.3

Mensaje de texto	{Nombre de usuario} ha editado el usuario {Nombre de usuario de destino}
Ejemplo	"Admin" ha editado el usuario "Peter_Maier"
Explicación	Un usuario ha cambiado una cuenta de usuario existente o ha asignado una función diferente a esta cuenta.
Gravedad	Aviso
Instalaciones	local0
Estándar	Referencia IEC 62443-3-3: SR 1.3

Mensaje de texto	{Nombre de usuario} ha editado el dispositivo: {Nombre del dispositivo}
Ejemplo	"Admin" ha editado el dispositivo: "S_615"
Explicación	Un usuario ha cambiado una cuenta de dispositivo existente.
Gravedad	Aviso
Instalaciones	local0
Estándar	Referencia IEC 62443-3-3: SR 1.3

Apéndice C**C.1 Mensajes de Syslog**

Mensaje de texto	{Nombre de usuario} ha eliminado al usuario {Nombre de usuario de destino}
Ejemplo	"Admin" ha eliminado al usuario "Peter_Maier"
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	{Nombre de usuario} ha eliminado el dispositivo {Nombre del dispositivo}
Ejemplo	"Administrador" ha eliminado el dispositivo "S615_1"
Explicación	Un usuario ha eliminado una cuenta de dispositivo existente.
Gravedad	Aviso
Instalaciones	local0
Estándar	Referencia IEC 62443-3-3: SR 1.3

Mensaje de texto	El usuario temporal {Nombre de usuario} se eliminó
Ejemplo	Se elimina el usuario temporal "Temp_User"
Explicación	Se eliminó una cuenta de usuario temporal existente.
Gravedad	Información
Instalaciones	local0
Estándar	Referencia IEC 62443-3-3: SR 1.3

Mensaje de texto	Usuario(s) temporal(es) {Nombre de usuario} asociado(s) con el(las) rol(es) {Role} eliminado por {Nombre de usuario}
Ejemplo	Usuario(s) temporal(es) "Temp_User" asociado(s) con la(s) función(es) "Soporte" eliminado por "Administrador"
Explicación	Un usuario ha eliminado una cuenta de usuario existente.
Gravedad	Información
Instalaciones	local0
Estándar	Referencia IEC 62443-3-3: SR 1.3

Mensaje de texto	{Nombre de usuario} cambió la contraseña del dispositivo: {Nombre del dispositivo}
Ejemplo	"Admin" cambió la contraseña del dispositivo: "S615_1"
Explicación	Un usuario ha cambiado la contraseña de un dispositivo.
Gravedad	Aviso
Instalaciones	local0
Estándar	Referencia IEC 62443-3-3: SR 1.3

Mensaje de texto	La contraseña de usuario de depuración cambió
Ejemplo	La contraseña de usuario de depuración cambió
Explicación	Un usuario autenticado cambió la contraseña de la cuenta de depuración.
Gravedad	Aviso
Instalaciones	local0
Estándar	Referencia IEC 62443-3-3: SR 1.3

Mensaje de texto	{Nombre de usuario} ha activado al usuario: {Nombre de usuario de destino}
Ejemplo	"Admin" ha activado el usuario: "Peter_Maier"
Explicación	Un usuario ha activado la cuenta de otro usuario.
Gravedad	Aviso
Instalaciones	local0
Estándar	Referencia IEC 62443-3-3: SR 1.3

Mensaje de texto	{Nombre de usuario} ha activado el dispositivo {Nombre del dispositivo}
Ejemplo	"Admin" ha activado el dispositivo "S615_1"
Explicación	Un usuario ha habilitado una cuenta de dispositivo.
Gravedad	Aviso
Instalaciones	local0
Estándar	Referencia IEC 62443-3-3: SR 1.3

C.1.2.3 Gestión de los identificadores

Mensaje de texto	El usuario {Nombre de usuario} ha creado el rol {Rol}
Ejemplo	El usuario "Admin" ha creado el rol "Technical_Consulting"
Explicación	El usuario creó un nuevo rol.
Gravedad	Aviso
Instalaciones	local0
Estándar	Referencia IEC 62443-3-3: SR 1.3

Mensaje de texto	El usuario {Nombre de usuario} ha eliminado el rol {Role}
Ejemplo	El usuario "Admin" ha eliminado el rol "Technical_Consulting"
Explicación	El usuario ha eliminado un rol existente.
Gravedad	Aviso
Instalaciones	local0
Estándar	Referencia IEC 62443-3-3: SR 1.3

Mensaje de texto	El usuario {Nombre de usuario} ha editado el rol {Rol}
Ejemplo	El usuario "Admin" ha editado el rol "Technical_Consulting"
Explicación	El usuario ha cambiado el rol.
Gravedad	Aviso
Instalaciones	local0
Estándar	Referencia IEC 62443-3-3: SR 1.3

Mensaje de texto	El usuario {nombre de usuario} ha creado el grupo {Group}
Ejemplo	El usuario "Admin" ha creado el grupo "IT_Service"

Apéndice C**C.1 Mensajes de Syslog**

Explicación	El usuario ha creado un grupo de usuarios.
Gravedad	Aviso
Instalaciones	local0
Estándar	Referencia IEC 62443-3-3: SR 1.4

Mensaje de texto	El usuario {nombre de usuario} ha eliminado el grupo {Group}
Ejemplo	El usuario "Admin" ha eliminado el grupo "IT_Service"
Explicación	El usuario ha eliminado el grupo de usuarios.
Gravedad	Aviso
Instalaciones	local0
Estándar	Referencia IEC 62443-3-3: SR 1.4

Mensaje de texto	El usuario {nombre de usuario} ha editado el grupo {Group}
Ejemplo	El usuario "Admin" ha editado el grupo "IT_Service"
Explicación	El usuario ha cambiado de grupo de usuarios.
Gravedad	Aviso
Instalaciones	local0
Estándar	Referencia IEC 62443-3-3: SR 1.4

Mensaje de texto	El usuario {nombre de usuario} ha editado los destinos de comunicación del grupo {Group}
Ejemplo	El usuario "Admin" ha editado los destinos de comunicación del grupo "IT_Service"
Explicación	El usuario cambió los objetivos de comunicación del grupo de usuarios.
Gravedad	Aviso
Instalaciones	local0
Estándar	Referencia IEC 62443-3-3: SR 1.4

C.1.2.4 Intentos fallidos de inicio de sesión

Mensaje de texto	El bloqueo de fuerza bruta está activado para {Nombre de usuario}
Ejemplo	El bloqueo de fuerza bruta está activado para "Peter_Maier"
Explicación	Después de varios intentos de inicio de sesión fallidos, la cuenta de usuario correspondiente se bloquea durante un tiempo específico. La configuración predeterminada para el número de intentos fallidos de inicio de sesión después de los cuales se bloquea la cuenta de usuario es 10.
Gravedad	Advertencia
Instalaciones	local0
Estándar	IEC 62443-3-3 Referencia: SR 1.11

Mensaje de texto	El bloqueo de fuerza bruta está desactivado para {Nombre de usuario}
Ejemplo	El bloqueo de fuerza bruta está desactivado para "Peter_Maier"
Explicación	La cuenta de usuario está desbloqueada.
Gravedad	Advertencia
Instalaciones	local0
Estándar	IEC 62443-3-3 Referencia: SR 1.11

C.1.2.5 Acceso a través de redes no confiables

Mensaje de texto	{Nombre de usuario} rechazado debido a una versión de cliente no compatible
Ejemplo	"Peter_Maier" rechazado debido a una versión de cliente no compatible
Explicación	El inicio de sesión del usuario del cliente fue rechazado debido a un conflicto de versiones.
Gravedad	Aviso
Instalaciones	local0
Estándar	IEC 62443-3-3 Referencia: SR 1.11

Mensaje de texto	{Nombre} conectado a través de OpenVPN
Ejemplo	Peter_Maier@8.1 conectado a través de OpenVPN
Explicación	Se establece la conexión OpenVPN a un dispositivo o usuario.
Gravedad	Información
Instalaciones	local0
Estándar	Referencia IEC 62443-3-3: n/a (NERC-CIP 005-R1)

Mensaje de texto	{Name} desconectado a través de OpenVPN
Ejemplo	Peter_Maier@8.1 desconectado a través de OpenVPN
Explicación	La conexión OpenVPN a un dispositivo o usuario está cerrada.
Gravedad	Información
Instalaciones	local0
Estándar	Referencia IEC 62443-3-3: n/a (NERC-CIP 005-R1)

Mensaje de texto	{Nombre del dispositivo} conectado a través de IPsec
Ejemplo	"S615_1" conectado a través de IPsec
Explicación	Se establece la conexión IPsec a un dispositivo.
Gravedad	Información
Instalaciones	local0
Estándar	Referencia IEC 62443-3-3: n/a (NERC-CIP 005-R1)

Mensaje de texto	{Nombre del dispositivo} desconectado a través de IPsec
Ejemplo	"S615_1" desconectado a través de IPsec
Explicación	La conexión IPsec a un dispositivo está cerrada.
Gravedad	Información
Instalaciones	local0
Estándar	Referencia IEC 62443-3-3: n/a (NERC-CIP 005-R1)

Apéndice C**C.1 Mensajes de Syslog****C.1.2.6 Identificación y autenticación de dispositivos**

Mensaje de texto	Ningún cliente válido con CN {Nombre de CN}
Ejemplo	Ningún cliente válido con CN Device1
Explicación	La autenticación del dispositivo falló.
Gravedad	Error
Instalaciones	local0
Estándar	Referencia IEC 62443-3-3: SR 1.2

Mensaje de texto	El participante con CN {nombre CN} no puede establecer una conexión OpenVPN
Ejemplo	El participante con CN Device1 no puede establecer una conexión OpenVPN
Explicación	La autenticación del dispositivo falló.
Gravedad	Advertencia
Instalaciones	local0
Estándar	Referencia IEC 62443-3-3: SR 1.2

C.1.2.7 no repudio

Mensaje de texto	{Nombre de usuario} ha cambiado {Detalle de configuración}
Ejemplos	"Administrador" ha cambiado la hora del sistema al 03/04/2019, 11:44:46 "Administrador" ha cambiado la configuración de la interfaz de red "Administrador" ha cambiado la configuración de DNS "Administrador" ha cambiado la configuración del servidor de carga "Administrador" ha cambiado la configuración de copia de seguridad
Explicación	El usuario cambió ciertos datos de configuración. Cualquier configuración se puede especificar en el servidor como detalles de configuración.
Gravedad	Aviso
Instalaciones	local0
Estándar	IEC 62443-3-3 Referencia: SR 2.12

Mensaje de texto	{Nombre de usuario} reinicia el sistema
Ejemplos	"Administrador" reinicia el sistema
Explicación	El usuario reinicia el sistema.
Gravedad	Aviso
Instalaciones	local0
Estándar	IEC 62443-3-3 Referencia: SR 2.12

Mensaje de texto	{Nombre de usuario} ha exportado los mensajes de registro
Ejemplos	"Admin" ha exportado los mensajes de registro
Explicación	El usuario exportó mensajes de registro.
Gravedad	Aviso
Instalaciones	local0
Estándar	IEC 62443-3-3 Referencia: SR 2.12

Mensaje de texto	Verificación de conexión al servidor syslog {dirección IP} exitosa
Ejemplos	Verificación de conexión al servidor syslog "172.168.16.10" exitosa

Explicación	La verificación de la conexión con el servidor Syslog se completó con éxito.
Gravedad	Información
Instalaciones	local0
Estándar	IEC 62443-3-3 Referencia: SR 2.12

Mensaje de texto	La verificación de conexión con el servidor syslog (dirección IP) falló
Ejemplos	La comprobación de conexión con el servidor syslog "172.168.16.10" falló
Explicación	La comprobación de la conexión con el servidor Syslog falló.
Gravedad	Información
Instalaciones	local0
Estándar	IEC 62443-3-3 Referencia: SR 2.12

C.1.2.8 Copia de seguridad de datos en el sistema de automatización (copia de seguridad)

Mensaje de texto	{Nombre de usuario} ha creado la copia de seguridad: {Nombre de archivo}
Ejemplo	"Administrador" ha creado la copia de seguridad: "2019_04_03_09_53_23.backup"
Explicación	El usuario ha creado una copia de seguridad en el servidor.
Gravedad	Aviso
Instalaciones	local0
Estándar	IEC 62443-3-3 Referencia: SR7.3

Mensaje de texto	Se ha creado una copia de seguridad automática: {Nombre de archivo}
Ejemplo	Se ha creado una copia de seguridad automática: "2019_04_03_09_53_23.backup"
Explicación	Se creó una copia de seguridad automática en el servidor.
Gravedad	Información
Instalaciones	local0
Estándar	IEC 62443-3-3 Referencia: SR7.3

Mensaje de texto	{Nombre de usuario} ha importado la copia de seguridad: {Nombre de archivo}
Ejemplo	"Admin" ha importado la copia de seguridad: "2019_04_03_09_53_23.backup"
Explicación	El usuario importó una copia de seguridad.
Gravedad	Aviso
Instalaciones	local0
Estándar	IEC 62443-3-3 Referencia: SR7.3

Mensaje de texto	{Nombre de usuario} ha eliminado la copia de seguridad: {Nombre de archivo}
Ejemplo	"Administrador" ha eliminado la copia de seguridad: "2019_04_03_09_53_23.backup"
Explicación	El usuario ha eliminado una copia de seguridad en el servidor.
Gravedad	Aviso
Instalaciones	local0
Estándar	IEC 62443-3-3 Referencia: SR7.3

Apéndice C**C.1 Mensajes de Syslog****C.1.2.9 Restauración del sistema de automatización.**

Mensaje de texto	Restaurar copia de seguridad fallida
Ejemplo	Restaurar copia de seguridad fallida
Explicación	El sistema no pudo utilizar el archivo de copia de seguridad para la restauración.
Gravedad	Error
Instalaciones	local0
Estándar	IEC 62443-3-3 Referencia: SR 7.4

Mensaje de texto	Copia de seguridad no válida cargada, rechazando...
Ejemplo	Copia de seguridad no válida cargada, rechazando...
Explicación	La restauración falló. El archivo de copia de seguridad cargado no es compatible con el sistema.
Gravedad	Advertencia
Instalaciones	local0
Estándar	IEC 62443-3-3 Referencia: SR7.4

Mensaje de texto	El recuento de recursos de licencia no es suficiente para restaurar
Ejemplo	El recuento de recursos de licencia no es suficiente para restaurar
Explicación	La restauración falló debido a la falta de licencias.
Gravedad	Advertencia
Instalaciones	local0
Estándar	IEC 62443-3-3 Referencia: SR 7.4

Mensaje de texto	{Nombre de usuario} ha iniciado la restauración de la copia de seguridad: {Nombre de archivo}
Ejemplo	"Admin" ha iniciado la restauración de la copia de seguridad: "2019_06_13_23_00_01.backup"
Explicación	El usuario inició la restauración de una copia de seguridad.
Gravedad	Aviso
Instalaciones	local0
Estándar	IEC 62443-3-3 Referencia: SR7.4

Mensaje de texto	Versión de copia de seguridad restaurada: {Versión de archivo}
Ejemplo	Versión de copia de seguridad restaurada: "2019_06_13_23_00_01.backup"
Explicación	Muestra la información de la versión del archivo de copia de seguridad cargado.
Gravedad	Aviso
Instalaciones	local0
Estándar	IEC 62443-3-3 Referencia: SR7.4

Mensaje de texto	Importación de firmware exitosa: {Nombre de archivo}
Ejemplo	Importación de firmware exitosa: "SCALANCE_M800_S615_V06.02.00_30.01_estc.sfw"
Explicación	El firmware del dispositivo fue importado con éxito por el usuario.
Gravedad	Información
Instalaciones	local0
Estándar	IEC 62443-3-3 Referencia: SR 7.4

Mensaje de texto	{Nombre del dispositivo} solicita el firmware
Ejemplo	"S615_1" solicita el firmware
Explicación	El dispositivo solicitó el firmware.

Gravedad	Aviso
Instalaciones	local0
Estándar	IEC 62443-3-3 Referencia: SR 7.4

Mensaje de texto	{Nombre del dispositivo} ha comenzado a descargar el firmware
Ejemplo	"S615_1" ha comenzado a descargar el firmware
Explicación	El dispositivo está descargando el firmware.
Gravedad	Aviso
Instalaciones	local0
Estándar	IEC 62443-3-3 Referencia: SR 7.4

Mensaje de texto	{Nombre del dispositivo} completó la descarga del firmware
Ejemplo	"S615_1" ha completado la descarga del firmware
Explicación	El dispositivo completó la descarga del firmware.
Gravedad	Aviso
Instalaciones	local0
Estándar	IEC 62443-3-3 Referencia: SR 7.4

Mensaje de texto	Importación de firmware fallida: ¡Tipo de archivo de firmware desconocido!
Ejemplo	Importación de firmware fallida: ¡Tipo de archivo de firmware desconocido!
Explicación	La importación del firmware falló debido a un tipo de archivo de firmware no válido.
Gravedad	Error
Instalaciones	local0
Estándar	IEC 62443-3-3 Referencia: SR 7.4

Mensaje de texto	Importación de firmware fallida: ¡Falló la verificación de integridad!
Ejemplo	Importación de firmware fallida: ¡Falló la verificación de integridad!
Explicación	La importación del firmware falló durante la verificación de integridad.
Gravedad	Error
Instalaciones	local0
Estándar	IEC 62443-3-3 Referencia: SR 7.4

Mensaje de texto	No hay archivo de firmware importado en la tienda
Ejemplo	No hay archivo de firmware importado en la tienda
Explicación	No se puede iniciar la actualización del dispositivo porque no se ha importado ningún archivo de firmware.
Gravedad	Error
Instalaciones	local0
Estándar	IEC 62443-3-3 Referencia: SR 7.4

Apéndice C**C.1 Mensajes de Syslog**

Mensaje de texto	{Nombre de usuario} ha subido la actualización
Ejemplo	"Administrador" ha subido la actualización.
Explicación	El usuario ha subido una actualización del servidor.
Gravedad	Aviso
Instalaciones	local0
Estándar	IEC 62443-3-3 Referencia: SR 7.4

Mensaje de texto	Actualización de SINEMA RC a la versión: {Versión de software}
Ejemplo	Actualización de SINEMA RC a la versión: 2.0.1.0-01.01.00.04
Explicación	El servidor se está actualizando a la versión especificada.
Gravedad	Información
Instalaciones	local0
Estándar	IEC 62443-3-3 Referencia: SR 7.4

Mensaje de texto	Actualización aplicada con éxito
Ejemplo	Actualización aplicada con éxito
Explicación	El servidor se actualizó con éxito.
Gravedad	Información
Instalaciones	local0
Estándar	IEC 62443-3-3 Referencia: SR 7.4

Mensaje de texto	El paquete de actualización no es aplicable. La(s) versión(es) de destino es {versión de software de destino}, mientras que la versión instalada es {versión de software de origen}
Ejemplo	El paquete de actualización no es aplicable. Las versiones de destino son V1.3.0.0-01.01.00.38, V2.0.0.0-01.01.00.21, mientras que la versión instalada es V2.0.1.0-01.01.00.04
Explicación	La activación del software falló. La actualización de software cargada no es compatible con la versión instalada.
Gravedad	Advertencia
Instalaciones	local0
Estándar	IEC 62443-3-3 Referencia: SR 7.4

Mensaje de texto	¡Error al aplicar la actualización del sistema!
Ejemplo	¡Error al aplicar la actualización del sistema!
Explicación	La actualización del servidor falló.
Gravedad	Error
Instalaciones	local0
Estándar	IEC 62443-3-3 Referencia: SR 7.4

C.1.2.10 Configuración de seguridad de red y TI

Mensaje de texto	Información del dispositivo enviada a {Nombre de usuario}
Ejemplo	Información del dispositivo enviada a "Peter_Maier"
Explicación	La información del dispositivo se envía al usuario del cliente a través del mecanismo de configuración automática.
Gravedad	Aviso
Instalaciones	local0
Estándar	IEC 62443-3-3 Referencia: SR 1.11

Mensaje de texto	La configuración de OpenVPN se envió a {Nombre de usuario}
Ejemplo	La configuración de OpenVPN fue enviada a "Peter_Maier"
Explicación	La configuración de OpenVPN se envía al usuario del cliente a través del mecanismo de configuración automática.
Gravedad	Aviso
Instalaciones	local0
Estándar	IEC 62443-3-3 Referencia: SR 1.11

Mensaje de texto	El usuario {Nombre de usuario} no pudo iniciar sesión en el cliente desde {dirección IP}: no se encontró el usuario
Ejemplo	HTTPS: el usuario "Administrador" no pudo iniciar sesión en el cliente desde "192.168.1.105": no se encontró el usuario
Explicación	El usuario del cliente no puede iniciar sesión en el servidor.
Gravedad	Error
Instalaciones	local0
Estándar	IEC 62443-3-3 Referencia: SR 1.13

Mensaje de texto	Envío actualización de ruta a {dirección IP}
Ejemplo	Envío actualización de ruta a 192.168.1.20
Explicación	La actualización de la ruta se envió a un dispositivo o a un usuario debido a cambios de configuración.
Gravedad	Información
Instalaciones	local0
Estándar	IEC 62443-3-3 Referencia: SR 1.11

Mensaje de texto	Archivo(s) cargado(s) correctamente {Nombres de archivo} a la carpeta en {dirección IP}
Ejemplo	Archivos cargados con éxito "2019_04_03_09_53_23.backup, 2019_04_03_09_53_23.backup" a la carpeta en "192.168.1.110"
Explicación	Los archivos se cargaron correctamente en el servidor de carga (servidor SFTP).
Gravedad	Aviso
Instalaciones	local0
Estándar	IEC 62443-3-3 Referencia: SR7.3

Mensaje de texto	{Protocolo}: ¡Error en la carga! No se puede acceder al servidor de carga
Ejemplo	¡Subida fallida! El servidor no es accesible
Explicación	El archivo no se pudo cargar en el servidor de carga (servidor SFTP).
Gravedad	Error
Instalaciones	local0
Estándar	IEC 62443-3-3 Referencia: SR7.3

Apéndice C**C.1 Mensajes de Syslog**

Mensaje de texto	No se pudieron cargar los archivos {nombre de archivo} a la carpeta en {dirección IP}
Ejemplo	Error al cargar los archivos "2019_04_03_09_53_23.backup, 2019_04_03_09_53_23.backup" a la carpeta en "192.168.10.10"
Explicación	El archivo no se pudo cargar en el servidor de carga (servidor SFTP).
Gravedad	Error
Instalaciones	local0
Estándar	IEC 62443-3-3 Referencia: SR7.3

Mensaje de texto	{Nombre de usuario} ha aceptado el acuerdo de usuario {Número de versión}
Ejemplo	"Peter_Maier" ha aceptado el acuerdo de usuario 1
Explicación	El usuario aceptó el acuerdo de usuario.
Gravedad	Información
Instalaciones	local0
Estándar	IEC 62443-3-3: SR 7.6

Mensaje de texto	{Nombre de usuario} ha rechazado el acuerdo de usuario {Número de versión}.
Ejemplo	"Peter_Maier" ha rechazado el acuerdo de usuario 1
Explicación	El usuario rechazó el acuerdo de usuario.
Gravedad	Información
Instalaciones	local0
Estándar	Referencia IEC 62443-3-3: SR 7.6

C.1.2.11 Estado del sistema

Mensaje de texto	Estado de conexión del servidor Syslog {Dirección IP} "En línea"
Ejemplo	Estado de conexión del servidor Syslog 192.168.50.10 "En línea"
Explicación	Se cambió el estado de un servidor Syslog.
Gravedad	Información
Instalaciones	local0
Estándar	CEI 62443-3-3

Mensaje de texto	Estado de conexión del servidor Syslog {Dirección IP} "En línea"
Ejemplo	Estado de conexión del servidor Syslog 192.168.50.10 "En línea"
Explicación	Se cambió el estado de un servidor Syslog.
Gravedad	Información
Instalaciones	local0
Estándar	CEI 62443-3-3

D

Apéndice D

D.1 Cifrados utilizados

Los conjuntos de cifrado que utiliza el servidor SINEMA RC se enumeran en las siguientes tablas.

Mecanismos de seguridad soportados para autenticación WBM

Nombre de configuración del cifrado en SINEMA RC	Nombre compatible con RFC	método de cifrado
AND-RSA-AES256-GCM SHA384	TLS_DHE_RSA_CON_AES_256_GCM_SHA384	AES según RFC3268, TLS v1.2
AND-RSA-AES256-SHA	TLS_DHE_RSA_CON_AES_256_CBC_SHA256	AES según RFC3268, TLS v1.2
AES256-GCM-SHA384	TLS_RSA_CON_AES_256_GCM_SHA384	AES según RFC3268, TLS v1.2
AES256-SHA	TLS_RSA_WITH_AES_256_CBC_SHA256	AES según RFC3268, TLS v1.2
AND-RSA-AES128-GCM SHA256	TLS_DHE_RSA_CON_AES_128_GCM_SHA256	AES según RFC3268, TLS v1.2
AND-RSA-AES128-SHA	TLS_DHE_RSA_CON_AES_128_CBC_SHA256	AES según RFC3268, TLS v1.2
AES128-GCM-SHA256	TLS_RSA_CON_AES_128_GCM_SHA256	AES según RFC3268, TLS v1.2
AES128-SHA	TLS_RSA_WITH_AES_128_CBC_SHA256	AES según RFC3268, TLS v1.2

Mecanismos de seguridad compatibles con la autenticación SSH (inicio de sesión de depuración)

- DIFFIE-HELLMAN-GROUP-EXCHANGE-SHA256
- SSH-RSA
- RSA-SHA2-512
- RSA-SHA2-256
- AES256-CTR
- HMAC-SHA2-256-ETM@OPENSSH.COM

Mecanismos de seguridad compatibles con la autenticación SFTP

- AES128-CTR
- AES192-CTR
- AES256-CTR
- AES128-CBC

Apéndice D**D.1 Cifrados utilizados**

- 3DES-CBC
- HMAC-MD5
- HMAC-SHA1
- UMAC-64@OPENSSH.COM

Mecanismos de seguridad admitidos para autenticación SMTP (correo electrónico), cliente y Syslog

Nombre de configuración del cifrado en SINEMA RC	Nombre compatible con RFC	método de cifrado
AES128-SHA	TLS_RSA_CON_AES_128_CBC_SHA	AES según RFC3268, TLS v1.0
AES256-SHA	TLS_RSA_CON_AES_256_CBC_SHA	AES según RFC3268, TLS v1.1
AND-RSA-AES128-SHA	TLS_DHE_RSA_CON_AES_128_CBC_SHA	AES según RFC3268, TLS v1.10
AND-RSA-AES256-SHA	TLS_DHE_RSA_CON_AES_256_CBC_SHA	AES según RFC3268, TLS v1.11
ECDHE-RSA-CHACHA20-POLY1305 TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256	TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256	ChaCha20-Poly1305, TLS v1.2
ECDHE-ECDSA-CHACHA20-POLY1305	TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256	ChaCha20-Poly1305, TLS v1.3
AND-RSA-CHACHA20-POLY1305	TLS_DHE_RSA_CON_CHACHA20_POLY1305_SHA256	ChaCha20-Poly1305, TLS v1.4
PSK-CHACHA20-POLY1305	TLS_PSK_WITH_CHACHA20_POLY1305_SHA256	ChaCha20-Poly1305, TLS v1.5
ECDHE-PSK-CHACHA20-POLY1305 TLS_ECDHE_PSK_WITH_CHACHA20_POLY1305_SHA256	TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256	ChaCha20-Poly1305, TLS v1.6
AND-PSK-CHACHA20-POLY1305	TLS_DHE_PSK_WITH_CHACHA20_POLY1305_SHA256	ChaCha20-Poly1305, TLS v1.7
RSA-PSK-CHACHA20-POLY1305	TLS_RSA_PSK_WITH_CHACHA20_POLY1305_SHA256	ChaCha20-Poly1305, TLS v1.8
ECDHE-ECDSA-AES128-SHA	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	Conjuntos de cifrado de curva elíptica
ECDHE-ECDSA-AES256-SHA	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	Conjuntos de cifrado de curva elíptica
ECDHE-RSA-AES128-SHA	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	Conjuntos de cifrado de curva elíptica
ECDHE-RSA-AES256-SHA	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	Conjuntos de cifrado de curva elíptica
AND-PSK-AES128-CBC-SHA	DHE_PSK_CON_AES_128_CBC_SHA	Clave precompartida (PSK)
AND-PSK-AES128-CBC-SHA256	DHE_PSK_CON_AES_128_CBC_SHA256	Clave precompartida (PSK)
AND-PSK-AES128-GCM-SHA256	DHE_PSK_CON_AES_128_GCM_SHA256	Clave precompartida (PSK)
AND-PSK-AES256-CBC-SHA	DHE_PSK_CON_AES_256_CBC_SHA	Clave precompartida (PSK)
AND-PSK-AES256-CBC-SHA384	DHE_PSK_CON_AES_256_CBC_SHA384	Clave precompartida (PSK)
AND-PSK-AES256-GCM-SHA384	DHE_PSK_CON_AES_256_GCM_SHA384	Clave precompartida (PSK)
ECDHE-PSK-AES128-CBC-SHA	ECDHE_PSK_CON_AES_128_CBC_SHA	Clave precompartida (PSK)
ECDHE-PSK-AES128-CBC-SHA256	ECDHE_PSK_WITH_AES_128_CBC_SHA256	Clave precompartida (PSK)
ECDHE-PSK-AES256-CBC-SHA	ECDHE_PSK_CON_AES_256_CBC_SHA	Clave precompartida (PSK)
ECDHE-PSK-AES256-CBC-SHA384	ECDHE_PSK_WITH_AES_256_CBC_SHA384	Clave precompartida (PSK)
PSK-AES128-CBC-SHA	PSK_CON_AES_128_CBC_SHA	Clave precompartida (PSK)
PSK-AES128-CBC-SHA256	PSK_CON_AES_128_CBC_SHA256	Clave precompartida (PSK)
PSK-AES128-GCM-SHA256	PSK_CON_AES_128_GCM_SHA256	Clave precompartida (PSK)
PSK-AES256-CBC-SHA	PSK_CON_AES_256_CBC_SHA	Clave precompartida (PSK)

Nombre de configuración del cifrado en SINEMA RC	Nombre compatible con RFC	método de cifrado
PSK-AES256-CBC-SHA384	V1.2 PSK_WITH_AES_256_CBC_SHA384	Clave precompartida (PSK)
PSK-AES256-GCM-SHA384	PSK_WITH_AES_256_GCM_SHA384	Clave precompartida (PSK)
RSA-PSK-AES128-CBC-SHA	RSA_PSK_WITH_AES_128_CBC_SHA	Clave precompartida (PSK)
RSA-PSK-AES128-CBC-SHA256	RSA_PSK_WITH_AES_128_CBC_SHA256	Clave precompartida (PSK)
RSA-PSK-AES128-GCM-SHA256	RSA_PSK_WITH_AES_128_GCM_SHA256	Clave precompartida (PSK)
RSA-PSK-AES256-CBC-SHA	RSA_PSK_WITH_AES_256_CBC_SHA	Clave precompartida (PSK)
RSA-PSK-AES256-CBC-SHA384	RSA_PSK_WITH_AES_256_CBC_SHA384	Clave precompartida (PSK)
RSA-PSK-AES256-GCM-SHA384	RSA_PSK_WITH_AES_256_GCM_SHA384	Clave precompartida (PSK)
SRP-AES-128-CBC-SHA	TLS_SRPSHA_WITH_AES_128_CBC_SHA	cifrados SRP
SRP-AES-256-CBC-SHA	SRP_SHA_WITH_AES_256_CBC_SHA	cifrados SRP
SRP-RSA-AES-128-CBC-SHA	TLS_SRPSHA_RSA_WITH_AES_128_CBC_SHA	cifrados SRP
SRP-RSA-AES-256-CBC-SHA	TLS_SRPSHA_RSA_WITH_AES_256_CBC_SHA	cifrados SRP
AES128-GCM-SHA256	TLS_RSA_WITH_AES_128_GCM_SHA256	TLS v1.2
AES128-SHA256	TLS_RSA_WITH_AES_128_CBC_SHA256	TLS v1.2
AES256-GCM-SHA384	TLS_RSA_WITH_AES_256_GCM_SHA384	TLS v1.2
AES256-SHA256	TLS_RSA_WITH_AES_256_CBC_SHA256	TLS v1.2
AND-RSA-AES128-GCM-SHA256	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 TLS	
AND-RSA-AES128-SHA256	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 TLS v1.2	
AND-RSA-AES256-GCM-SHA384	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 TLS v1.2	
AND-RSA-AES256-SHA256	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 TLS v1.2	
ECDHE-ECDSA-AES128-GCM SHA256	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	TLS v1.2
ECDHE-ECDSA-AES128-SHA256	TLS_ECDHE_ECDSA_CON_AES_128_CBC_SHA256	TLS v1.2
ECDHE-ECDSA-AES256-GCM SHA384	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	TLS v1.2
ECDHE-ECDSA-AES256-SHA384	TLS_ECDHE_ECDSA_CON_AES_256_CBC_SHA384	TLS v1.2
ECDHE-RSA-AES128-GCM-SHA256 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 TLS v1.2	
ECDHE-RSA-AES128-SHA256 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 TLS v1.2	
ECDHE-RSA-AES256-GCM-SHA384 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 TLS v1.2	
ECDHE-RSA-AES256-SHA384 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 TLS v1.2	
TLS_AES_256_GCM_SHA384	TLS_AES_256_GCM_SHA384 TLS v1.3	
TLS_AES_128_GCM_SHA256	TLS_AES_128_GCM_SHA256	TLS v1.3
TLS_CHACHA20_POLY1305_SHA256	TLS_CHACHA20_POLY1305_SHA256	TLS v1.3

Apéndice D

D.1 Cifrados utilizados

Índice

A

Abreviaturas/acrónimos, 4
Contraseña de administrador, 38
pérdida, 38
servidor API
configurar, 95
número de artículo, 3

B

Copia de respaldo
Crear, 68, 124
Importación, 68
Número máximo, 70
Partición de arranque, 71

C

ca, 101
certificado CA, 100
Exportación, 102
Autoridad de certificación, 101
Cambiar idioma, 47
Cambiar grupo de participantes, 82
Crear grupo de participantes, 82
Creación de un proveedor de puerta de enlace SMS, 60

D

Definición de términos, 4
Eliminación certificada de CA, 102
Dispositivo
Creando, 75
Certificado de dispositivo, 100
generación, 74
Nombre del dispositivo
Caracteres permitidos y longitud, 28
DNS, 53, 103
Descarga del archivo de configuración, 74, 107, 120

Y

Entradas
Creando, 46

Borrar, 46
ahorro, 46
Registro de eventos
Registro de cortafuegos, 51
Archivos de registro, 50
Mensajes de registro, 49

F

Filtrar
Lista de dispositivos, 74, 82
lista de usuarios, 85
Registro de cortafuegos, 50
Actualización de firmware, 80

G

Glosario, 7
Nombre del grupo
Caracteres permitidos y longitud, 27

H

método hash, 106
nombre de host
Directrices, 28 https,
37

I

IPsec
Configurar espacio de direcciones, 57
perfiles IPsec
Crear, 110

P

Longitud de clave, 106

L

Licencia
licencias existentes, 62
Número de licencia, 62
Actualización de licencia, 27

Índice

Licencias (TCSB), 3

archivos de registro, 50

METRO

Unidad de transmisión máxima, 52

Requisitos mínimos, 23

UTM, 52

norte

La red

Configuración, 78

interfaz, 52

adaptador de red, 23

PNT, 58

O

Licencia fuera de línea

activar, 64

liberación, 64

Licencia en línea

activar, 63

liberación, 62

VPN abierta, 107, 108

Archivo de configuración, 107

Archivo de configuración (dispositivo), 74

Archivo de configuración (usuario), 120

Configurar espacio de direcciones, 57

Descarga del archivo de configuración, 107

Archivo OpenVPN, 120

PAGES

Grupo de participantes

Usuario de VPN,

17 grupos de participantes, 15

administrador de contraseñas,

38 directriz, ¡error!

Marcador no definido.

Entrada no válida, 38

Pérdida, 38 Usuarios,

14, 91 Caracteres

permitidos, 28 Configuración de

ping, 55 Certificados PKI CA, 111

Procesador, 23 Concepto de

protección, 14

R

RAM, 23

Requisitos recomendados, 23, 23

Renovación de un certificado de CA, 102

Derechos, 15

Papel

administrador, 17

usuario de VPN, 17

Nombre de rol

Caracteres permitidos y longitud, 27

papeles, 15

Ejecutar una búsqueda, 47

S

Servidor

Subir archivos, 96

Certificado de servidor, 100, 102

Renovando, 103

Certificado de servidor, 100, 102

Información del servidor, 71

Servicio y soporte, 7

SHA256, 106

SHA512, 106

Glosario SIMATIC NET, 7

Manual SIMATIC NET, 5

Página de inicio, 44

Rutas estáticas, 56

certificado de Syslog, 115

Borrar, 117

Certificados Syslog, 116

Mensajes de registro del sistema

variables, 139

servidor de registro del sistema

Parámetros de conexión, 97

Sistema

reiniciar, 70

Ajustes, 71

apagar, 70

Resumen del sistema, 47

T

Número de billete, 62

Tiempo, 101

manualmente, 58

PNT, 58

Formación, 7

t

UMC

- Crear grupo de usuarios UMC, 88 Inicio
- de sesión, 39 Servidor UMC Parámetros
- de conexión, 95 Certificado de usuario, 100
- Exportación, 120 Resumen, 119
- Renovación, 119 Nombre de usuario Directriz,

Fehler! Textmarke nicht definiert.

Nombre de usuario: entrada no válida,

- Derechos de los usuarios, 86
 - Administrar dispositivos, 86
 - Administrar un dispositivo, 72
 - Gestión de usuarios, 87
- Usuarios, 15
 - Derechos, 14
 - papeles, 14
- Derechos de los usuarios, 14

v

subred virtual

- Configurar espacio de direcciones, 57

vpn

VPN abierta, 107, 108

EN

SMS de despertador

Intentos fallidos, 138.

Dirección IP de WAN, 103

externa, 53

WBM

Botones, 46

Disposición de la ventana, 44

interfaz de usuario web, 37

Entrada incorrecta, nombre de usuario, 38

Índice
